3onedata
Make network communication more reliable

IES5028 Series

Managed Industrial Ethernet Switch

User Manual

Version 02

Issue Date: 2019-11-26

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.

Notes

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

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

3onedata
Make network communication more reliable

Please scan our QR code for more details
Embedded Industrial Ethernet Switch Modules
Embedded Serial Device Server Modules
Industry-specialized Products
(Rail Transit, Power, Smart City, Pipe Gallery…)
3onedata
Make network communication more reliable
Honor·Quality·Service
Layer 2 (Unmanaged) Managed Industrial Ethernet Switch
Layer 3 Managed Industrial Ethernet Switch
Industrial PoE Switch
BlueEyes pro
BlueEyes Pro Management Software
VSP Virtual Serial Port Management Software
SNMP Management Software
Modbus Gateway
Serial Device Server
Media Converter
CAN Device Server
Interface Converter
Industrial Wireless Products

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:	+86-400-880-4496
E-mail:	sales@3onedata.com
Fax:	+86-0755-26703485
Website:	http://www.3onedata.com

Preface

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

- Product feature
- Network management method
- Network management relative principle overview

Readers

This manual mainly suits for engineers as follows:

- Network administrator responsible for network configuration and maintenance
- On-site technical support and maintenance staff
- Hardware engineer

Text Format Convention

Format	Description
“”	Words with "" represent the interface words. e.g.: "The port number".
>	Multi-level path is separated by ">". Such as opening the local connection path description: Open "Control Panel> Network Connection> Local Area Connection".
Light Blue Font	Represent the words click to achieve hyperlink. Font color as: "Light blue".
About This Chapter	The "About This Chapter" section provides links to each section and corresponding principles / operating chapters in this chapter.

Icon Convention

Format	Description
⚠ Notice	Reminder the announcements in the operation, improper

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

Revision Record

Version NO.	Revision Date	Revision Description
01	2019-11-26	Product release

Content

The First Part: Operation

1 Log in the Web Interface

1.1 WEB Browsing System Requirements

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

Hardware and Software	System Requirements
Resolution	Above 1024x768
Color	Above 256 color
Browser	Above Internet Explorer 6.0
Operating System	● Windows XP ● Windows 7 ● Windows 10

1.2 Setting IP Address of PC

The switch default management as follows:

IP Setting	Default Value
IP Address	192.168.1.254

IP Setting	Default Value
Subnet Mask	255.255.255.0

While configuring the switch via Web:

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

Notes:
While first configuring the switch, if it is a local configuration mode, please make sure that the network segment of current PC is 1.

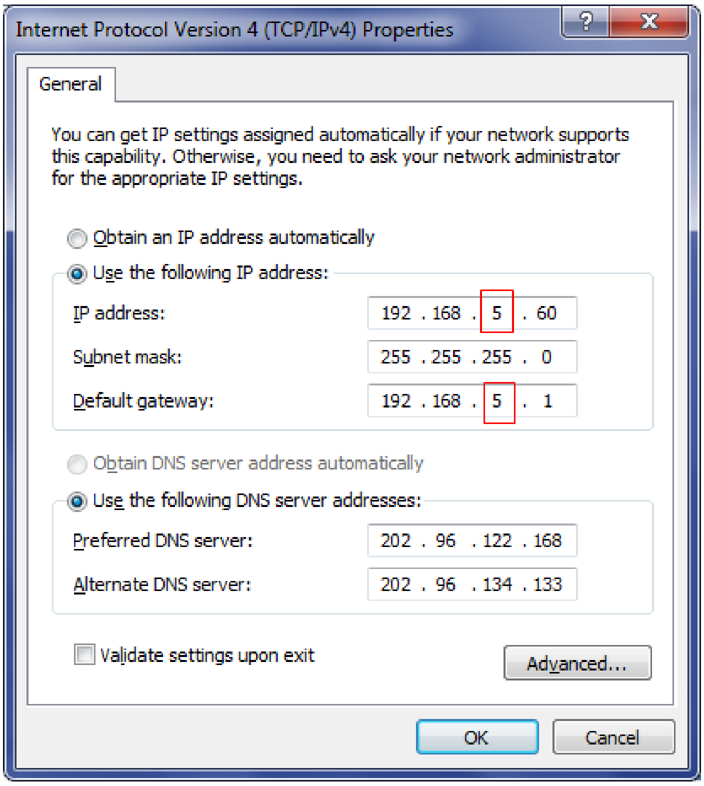
E.g.: Assume that the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address to "1".

Operation Steps

Amendment steps as follows:

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

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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 modifies successfully.

Step 4 End.

⚠ Notice

In windows system, if user adopts the advanced configuration function of IP address and accesses the switch device via setting IP dummy address, the following managed functions can't be achieved: IEEE 802.1x polling.

1.3 Log in the Web Configuration Interface

Operation Steps

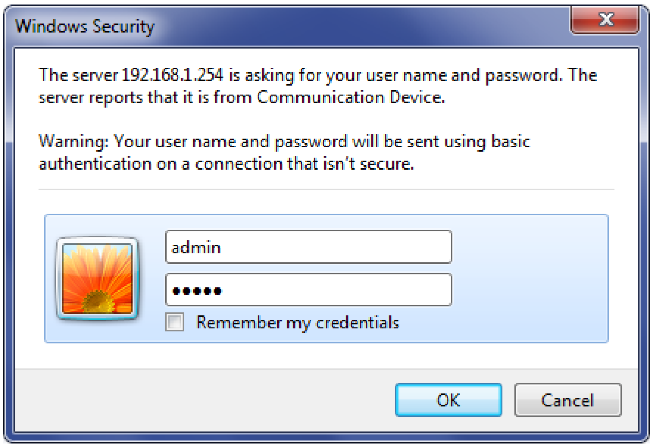
Login in the web configuration interface as follow:

Step 5 Run the computer browser.

Step 6 On the browser's address bar, type in the switch addresses "http://192.168.1.254 ".

Step 7 Click the “Enter” key.

Step 8 Pop-up a window as the figure below, enter the user name and password on the login window.



Windows Security

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

Notes:

- The default username and password are “admin”, please strictly distinguish capital and small letter while entering.
- Default username and password have the administrator privileges.
- WebServer will provide 3 times opportunities to enter username and password. If enter the error information for 3 times, the browser will display a "Access denied" to reject access message. Refresh the page and try again.

Step 9 Click "OK".

Step 10 End.

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

Notes:

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

2 System Configuration

2.1 System Information

Function Description

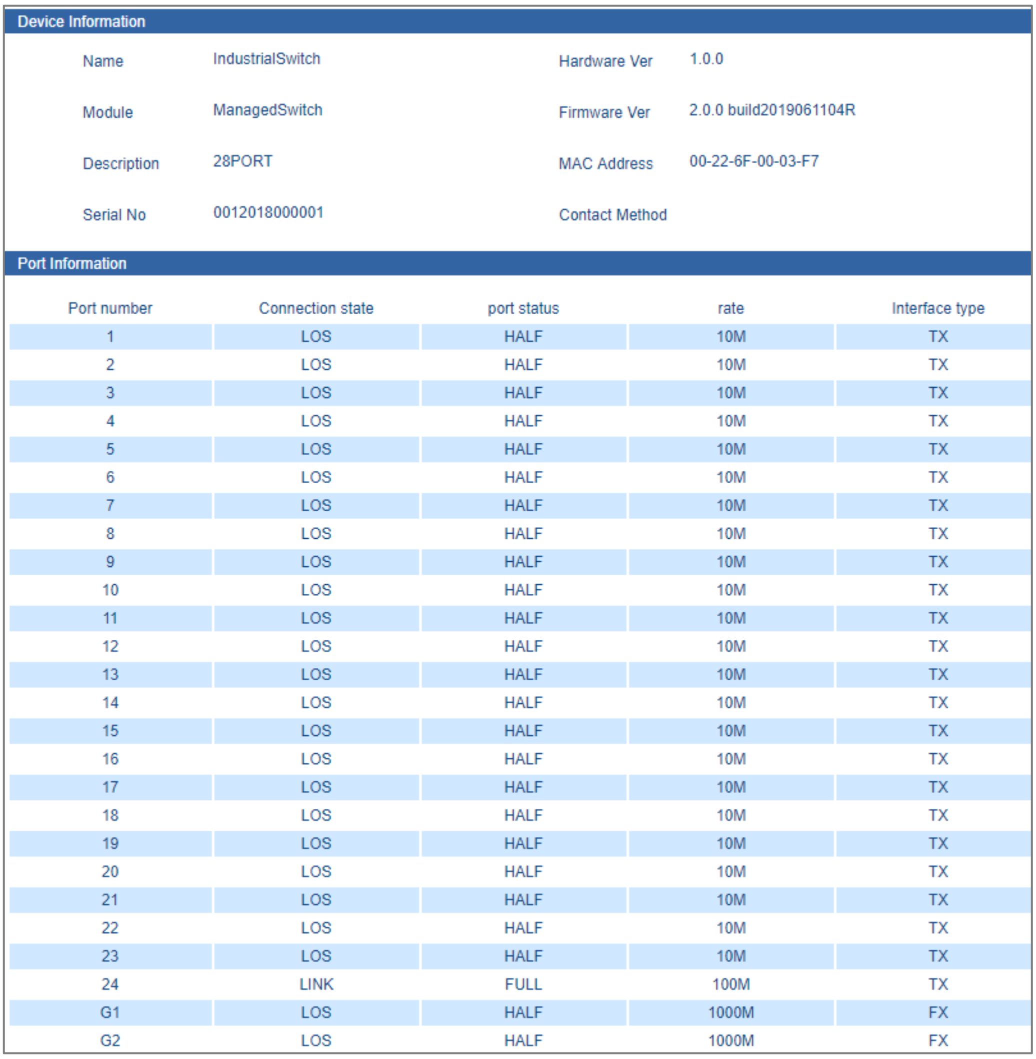
In "System Information" page, user can check "Device Information" and "Port Info".

Operation Path

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

Interface Description

System information interface as follows:



Device Information

Name	IndustrialSwitch	Hardware Ver	1.0.0
Module	ManagedSwitch	Firmware Ver	2.0.0 build2019061104R
Description	28PORT	MAC Address	00-22-6F-00-03-F7
Serial No	0012018000001	Contact Method	

Port Information

Port number	Connection state	port status	rate	Interface type
1	LOS	HALF	10M	TX
2	LOS	HALF	10M	TX
3	LOS	HALF	10M	TX
4	LOS	HALF	10M	TX
5	LOS	HALF	10M	TX
6	LOS	HALF	10M	TX
7	LOS	HALF	10M	TX
8	LOS	HALF	10M	TX
9	LOS	HALF	10M	TX
10	LOS	HALF	10M	TX
11	LOS	HALF	10M	TX
12	LOS	HALF	10M	TX
13	LOS	HALF	10M	TX
14	LOS	HALF	10M	TX
15	LOS	HALF	10M	TX
16	LOS	HALF	10M	TX
17	LOS	HALF	10M	TX
18	LOS	HALF	10M	TX
19	LOS	HALF	10M	TX
20	LOS	HALF	10M	TX
21	LOS	HALF	10M	TX
22	LOS	HALF	10M	TX
23	LOS	HALF	10M	TX
24	LINK	FULL	100M	TX
G1	LOS	HALF	1000M	FX
G2	LOS	HALF	1000M	FX

The main element configuration description of system information interface:

Interface Element	Description
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, pay attention to the hardware version limits in software version.
Firmware Ver	Current using software version information, updated software version has more functions.
MAC Address	Hardware address of device factory configuration.

Interface Element	Description
Contact Method	Display the contact information of the device maintenance personnel.
Port number	Display the number of the switch port.
Link status	Port connection state, display state as follows: ● "LINK" represents connected port; ● "LOS" represents disconnected port.
Port state	Port work state, display state as follows: ● "HALF" represents the corresponding port is in half-duplex state; ● "FULL" represents corresponding port is in full duplex state.
Speed	Display the current port link rate after port connection.
Interface type	Interface type, display port type as follows: ● TX; ● FX

Note

“Module”, “Name”, “Description” and “Contact Method” can be modified in "Main Menu > System Config > System Information".

3 Port Configuration

3.1 Port Settings

Function Description

The "Port Setting" page mainly includes:

- Check the port type: copper port or fiber port
- Configure the rate mode and duplex mode
- Port enable
- Flow control

Note

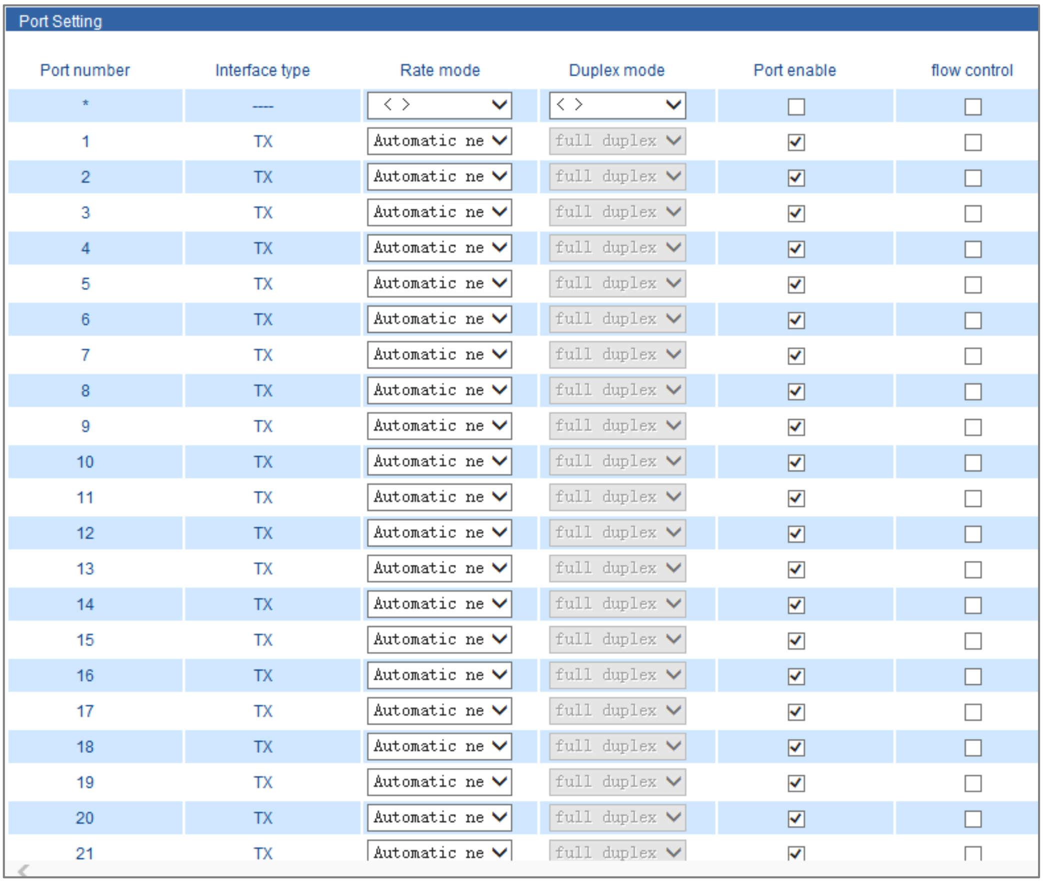
- Speed, duplex, flow control will take effect when the port is enabled.
- After selecting automated negotiation, speed and duplex will be gained via automated negotiation.

Operation Path

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

Interface Description

Port setting interface as follows:



Port Setting

Port number	Interface type	Rate mode	Duplex mode	Port enable	flow control
*	----	< >	< >	□	□
1	TX	Automatic ne	full duplex	☑	□
2	TX	Automatic ne	full duplex	☑	□
3	TX	Automatic ne	full duplex	☑	□
4	TX	Automatic ne	full duplex	☑	□
5	TX	Automatic ne	full duplex	☑	□
6	TX	Automatic ne	full duplex	☑	□
7	TX	Automatic ne	full duplex	☑	□
8	TX	Automatic ne	full duplex	☑	□
9	TX	Automatic ne	full duplex	☑	□
10	TX	Automatic ne	full duplex	☑	□
11	TX	Automatic ne	full duplex	☑	□
12	TX	Automatic ne	full duplex	☑	□
13	TX	Automatic ne	full duplex	☑	□
14	TX	Automatic ne	full duplex	☑	□
15	TX	Automatic ne	full duplex	☑	□
16	TX	Automatic ne	full duplex	☑	□
17	TX	Automatic ne	full duplex	☑	□
18	TX	Automatic ne	full duplex	☑	□
19	TX	Automatic ne	full duplex	☑	□
20	TX	Automatic ne	full duplex	☑	□
21	TX	Automatic ne	full duplex	☑	□

The main element configuration description of port setting interface:

Interface Element	Description
Port number	Display the device port number.
Interface type	Support two kinds of interface types: ● TX; ● FX.
Rate mode	Click the drop-down list box of “Rate mode” to select the port speed mode. ● Automatic negotiation: the port can automatically adjust the transmission speed of the opposite port. ● 10M rate: support the maximum rate of 10Mbit/s. ● 100M rate: support the maximum rate of 100Mbit/s. ● 1000M rate: support the maximum rate of 1000Mbit/s. Notes: ● All copper ports of the switch are MDI/MDIX self-adapting ports, and support automated negotiation speed mode. ● 1000M rate only suits for the Gigabit ports of the switch.

Interface Element	Description
Duplex	Click the drop-down list box of “Duplex” to select corresponding duplex mode of the port. Options as follows: ● Half duplex: the interface can only receive or send data at any time. ● Full duplex: the interface can receive or send data at the same time. Notes: When the speed mode is “AUTO”, the port will automatically match the opposite port mode, “Duplex” mode is disabled.
Enable	Enable Ethernet port. Note: If user doesn't check the port "Enable" checkbox, the port won't be connected to use.
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.

Examples: Port Settings

For example: configure the port 1, port 2 and port 3 as follows:

- “Rate mode” of port 1 is “Automatic negotiation”.
- “Rate mode” of port 2 is “100M”, “duplex mode” is “full duplex”.
- “Rate mode” of port 3 is “100M”, “duplex mode” is “full duplex”, and enable “flow control”.

Operating Steps

Step 1 Access to "Main Menu > Port Config > Port Setting".

Step 2 Configure the parameters of port 1:

1. Tick the check box of “Port enable”.
2. Select “Rate mode” as “Automatic negotiation”.

Notes:

The default configuration of “Rate mode” is “Automatic negotiation”.

Step 3 Configure the parameters of port 2:

1. Tick the check box of “Port enable”.
2. Select “Rate mode” as “100M”.
3. Select “duplex mode” as “full duplex”.

Step 4 Configure the parameters of port 3:

1. Tick the check box of “Port enable”.
2. Select “Rate mode” as “10M”.
3. Select “duplex mode” as “half duplex”.
4. Tick the check box of “flow control”.

Step 5 Click “set”.

Step 6 End.

3.2 Bandwidth Management

Function Description

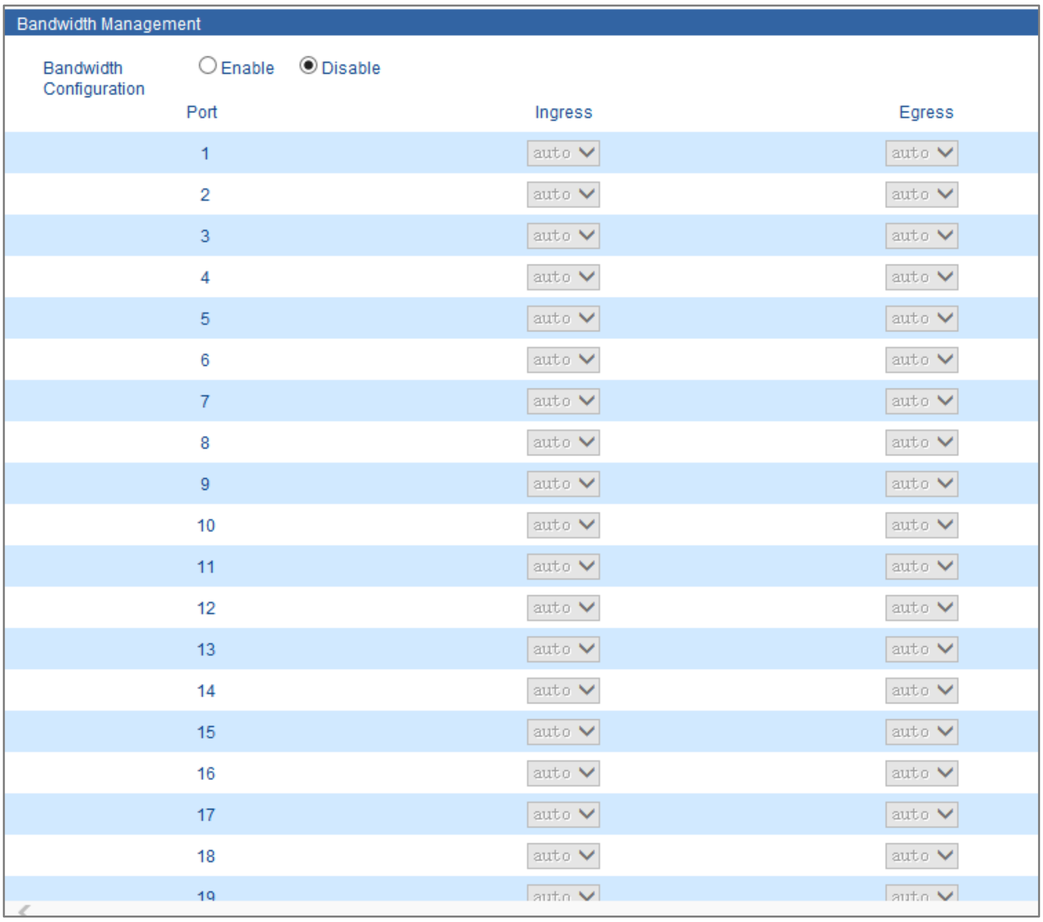
On the page of “Bandwidth Management”, user can limit the ingress and egress bandwidth speed of the port.

Operation Path

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

Interface Description

Bandwidth management interface as below:



Bandwidth Management

Bandwidth Configuration ○ Enable ● Disable

Port	Ingress	Egress
1	auto	auto
2	auto	auto
3	auto	auto
4	auto	auto
5	auto	auto
6	auto	auto
7	auto	auto
8	auto	auto
9	auto	auto
10	auto	auto
11	auto	auto
12	auto	auto
13	auto	auto
14	auto	auto
15	auto	auto
16	auto	auto
17	auto	auto
18	auto	auto
19	auto	auto

The main element configuration description of bandwidth management interface:

Interface Element	Description
Bandwidth configuration	Enable/disable bandwidth configuration.
Port	Port number of the device.
Ingress	Ingress speed is the limited port speed during data receiving.
Egress	Egress speed is the limited port speed during data transmitting.

Instance: bandwidth settings

For example: set both of the egress and ingress bandwidth of Port 1 to “4M”.

Operating steps

Step 1 Enter “Main Menu > Port Configuration > Bandwidth Management”.

Step 2 In the area of “Bandwidth Configuration”, click the option box of “Enable”.

Step 3 In the area of “Egress”, choose “4M” as the egress speed of Port 1.

Step 4 In the area of “Ingress”, choose “4M” as the ingress speed of Port 1.

Step 5 Click “Apply”.

Step 6 End.

Note

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

3.3 Storm Suppression

Function Description

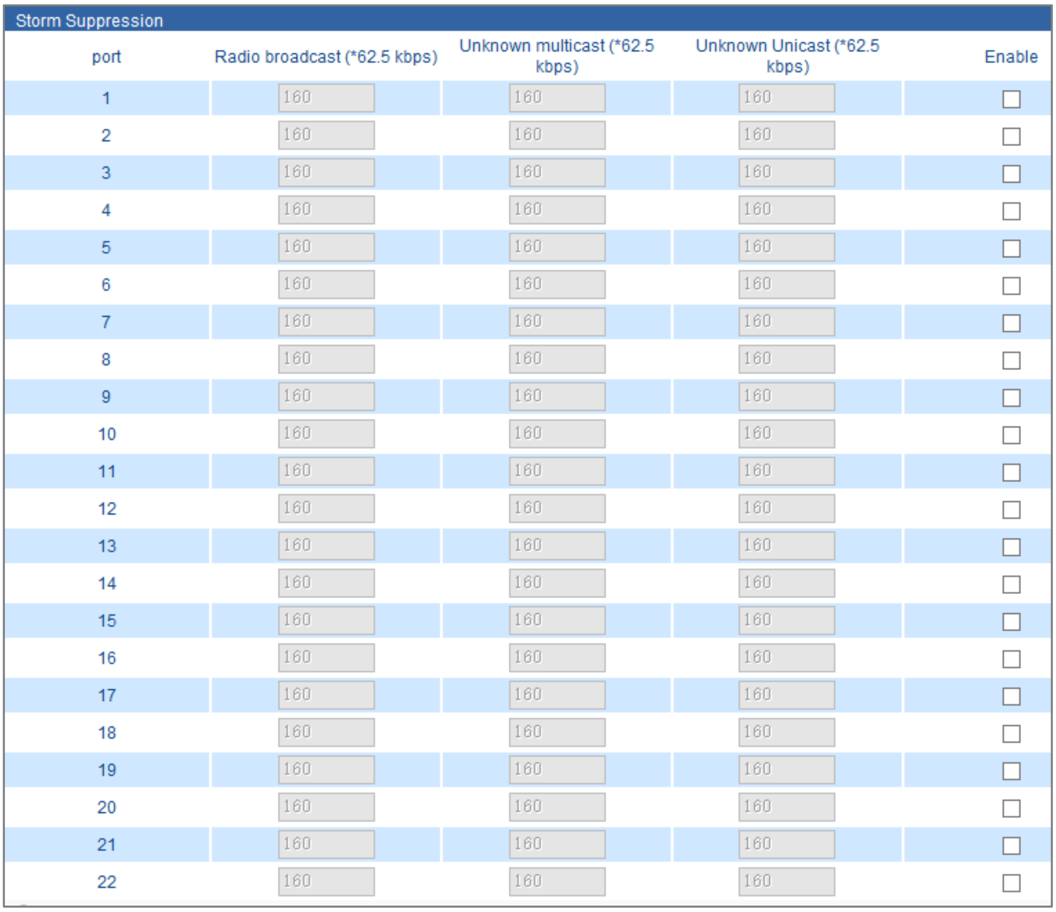
On the page of "Storm Suppression", user can achieve suppression of port broadcast storm.

Operation Path

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

Interface Description

Storm suppression interface as follows:



Storm Suppression

port	Radio broadcast (*62.5 kbps)	Unknown multicast (*62.5 kbps)	Unknown Unicast (*62.5 kbps)	Enable
1	160	160	160	□
2	160	160	160	□
3	160	160	160	□
4	160	160	160	□
5	160	160	160	□
6	160	160	160	□
7	160	160	160	□
8	160	160	160	□
9	160	160	160	□
10	160	160	160	□
11	160	160	160	□
12	160	160	160	□
13	160	160	160	□
14	160	160	160	□
15	160	160	160	□
16	160	160	160	□
17	160	160	160	□
18	160	160	160	□
19	160	160	160	□
20	160	160	160	□
21	160	160	160	□
22	160	160	160	□

Main elements configuration description of storm suppression interface:

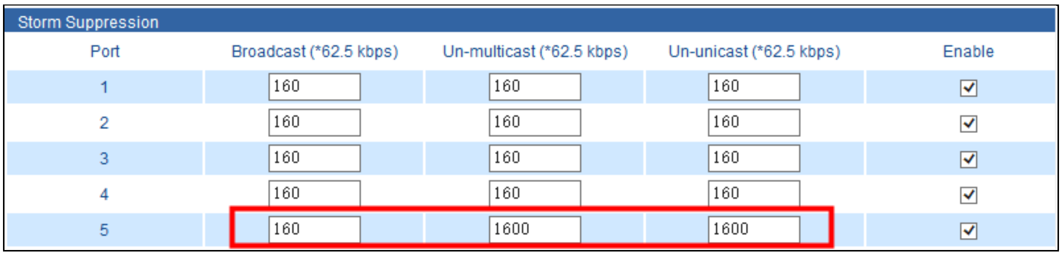
Interface Element	Description
Port	Display all Ethernet ports number of the device.
Broadcast (*62.5Kbps)	The device procedure can suppress the transmission speed of broadcast packet Notes: Broadcast packet, namely, the data frame with the destination address of FF-FF-FF-FF-FF-FF.
Un-multicast (*62.5kbps)	Port suppression to the transmission speed of unknown multicast data packet. Notes: Multicast packet, namely, data frame with the destination address of XX-XX-XX-XX-XX-XX, the second X is odd number (1, 3, 5, 7, 9, B, D, F).
Un-unicast (*62.5kbps)	Port suppression to the transmission speed of unknown unicast data packet. Notes: Unknown unicast packet, that is MAC address of the data frame doesn't exist in the internal index table of the device,

	which needs to be forwarded to all ports.
Enable	Tick the check box to enable storm suppression function of the port.

Example: Only Enable Broadcast Storm Suppression

For example:

- The broadcast speed is 160*62.5kbps=10000kbps=10Mbps.
- Under default configuration, the broadcast/unknown multicast/unknown unicast of each port are all in enabling suppression status, and the suppression speed is unified to 10Mbps.
- Only enable the "Broadcast Storm" suppression of port 5.



Storm Suppression

Port	Broadcast (*62.5 kbps)	Un-multicast (*62.5 kbps)	Un-unicast (*62.5 kbps)	Enable
1	160	160	160	☑
2	160	160	160	☑
3	160	160	160	☑
4	160	160	160	☑
5	160	1600	1600	☑

Operation Steps

Step 1 Click "Main Menu > Port Configuration > Storm Suppression".

Step 2 Tick corresponding "Enable" check box of port 5.

Step 3 Enter "160" in corresponding "Broadcast" text box of port 5.

Step 4 Enter "1600" in corresponding "Un-multicast" and "Un-unicast" text box of port 5. "Un-multicast" and "Un-unicast" will be uncontrolled.

Step 5 Click "Apply" to seperately enable the "Broadcast Storm" suppression of port 5.

Step 6 End.

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.

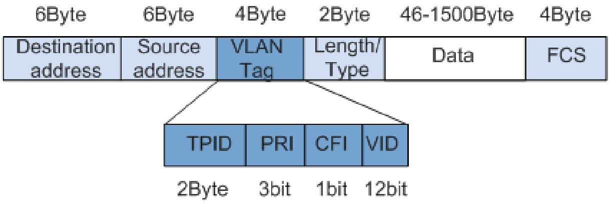
- Limit the broadcast domain;
- Increase the security of LAN;
- Improve the network stability;
- Flexiblely construct virtual working team.

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. VLAN ID value range is 0-4095. 0 and 4095 are reserved values of the protocol, so the valid value range of VLAN ID is 1-4094.

Function Description

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

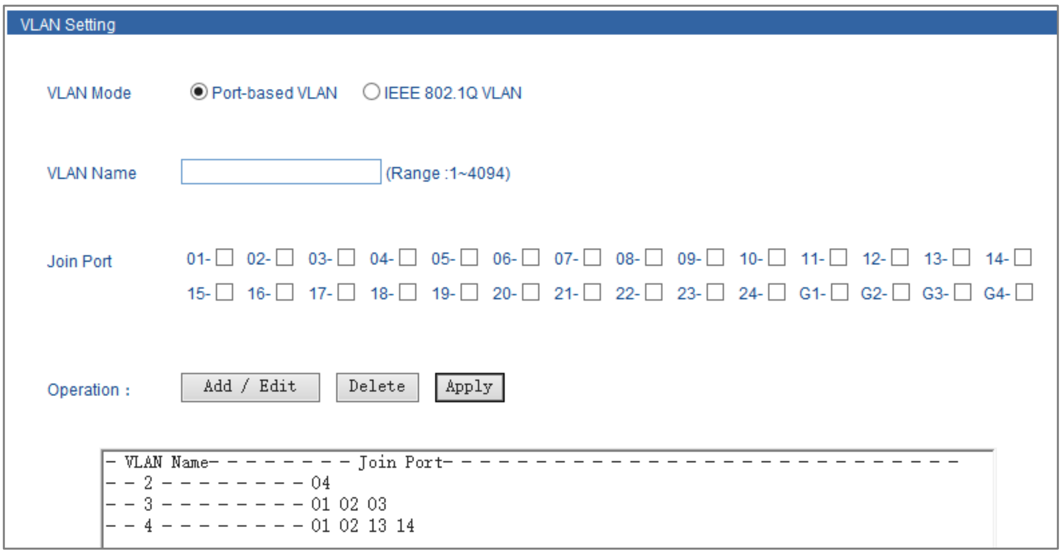
- Configure the port PVID;
- Create VLAN entry;
- Configure the port member type.

Operation Path

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

Interface Description 1: Port-based VLAN

Port-based VLAN interface as follows:



VLAN Setting

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

VLAN Name (Range :1~4094)

Join Port 01-□ 02-□ 03-□ 04-□ 05-□ 06-□ 07-□ 08-□ 09-□ 10-□ 11-□ 12-□ 13-□ 14-□
15-□ 16-□ 17-□ 18-□ 19-□ 20-□ 21-□ 22-□ 23-□ 24-□ G1-□ G2-□ G3-□ G4-□

Operation : Add / Edit | Delete | Apply

```
- VLAN Name- - - - - - - - Join Port- - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - 2 - - - - - - - - - 04
- - 3 - - - - - - - - - 01 02 03
- - 4 - - - - - - - - - 01 02 13 14
```

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

Interface Element	Description
VLAN Mode	Choose VLAN type, options are: ● Port-based VLAN ● IEEE 802.1Q VLAN
VLAN name	Enter VLAN number in digital form. 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 fill in the figure “3” to represent VLAN3.

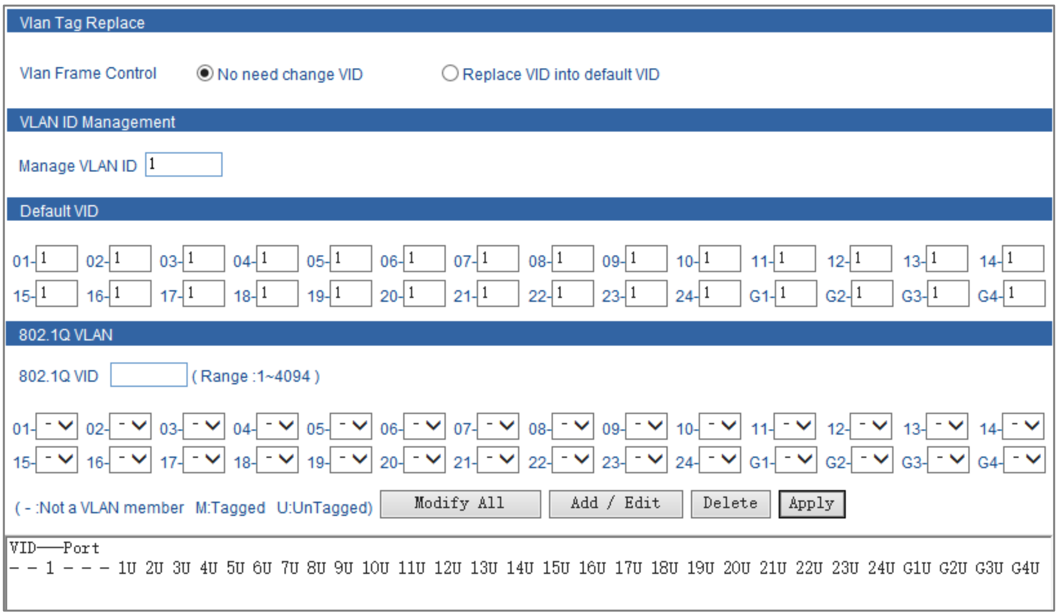
Step 4 Select VLAN member on the check box of “Join Port”, such as select port 2 and port 3.

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 Tag Replace

Vlan Frame Control ● No need change VID ○ Replace VID into default VID

VLAN ID Management

Manage VLAN ID 1

Default VID

01-1 02-1 03-1 04-1 05-1 06-1 07-1 08-1 09-1 10-1 11-1 12-1 13-1 14-1
15-1 16-1 17-1 18-1 19-1 20-1 21-1 22-1 23-1 24-1 G1-1 G2-1 G3-1 G4-1

802.1Q VLAN

802.1Q VID (Range :1~4094)

01- - 02- - 03- - 04- - 05- - 06- - 07- - 08- - 09- - 10- - 11- - 12- - 13- - 14- -
15- - 16- - 17- - 18- - 19- - 20- - 21- - 22- - 23- - 24- - G1- - G2- - G3- - G4- -

(- :Not a VLAN member M:Tagged U:UnTagged)

```
VID——Port
- - 1 - - - 1U 2U 3U 4U 5U 6U 7U 8U 9U 10U 11U 12U 13U 14U 15U 16U 17U 18U 19U 20U 21U 22U 23U 24U G1U G2U G3U G4U
```

The main element configuration description of 802.1Q Vlan interface:

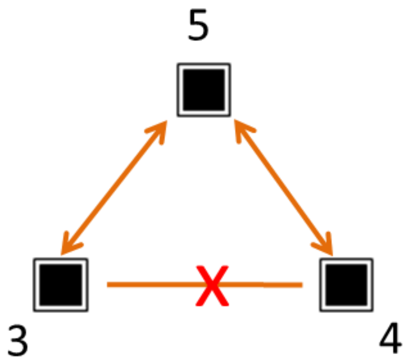
Interface Element	Description
VLAN mode	Choose VLAN mode, options are: ● Port-based VLAN: ● IEEE 802.1Q VLAN.
VLAN tag replace	**The configuration bar of VLAN tag replace**
VLAN frame control	Choose VLAN tag replace configuration, options are: ● No need change VID; ● Replace VID into default VID.
VLAN ID management	**The configuration bar of VLAN ID management**
Manage VLAN ID	Manage the VLAN ID of the device. Its value range is 1-4094.
Default VID	**The configuration bar of default VID**
802.1Q VID	VLAN ID number. Its value range is 1-4094.
Member type	There are three types of data frame laber that the port sends: ● 一: no forwarding, which is not as a member of this VLAN ID;

Interface Element	Description
	● M: forward and keep VLAN tag; ● U: forward but remove VLAN tag.
Modify all	Quickly modify all member type at the same time.
Add/edit	Add configurated VLAN to the list of VLAN member.
Delete	Delete one of the VLAN items in the selected member list.
Apply	Save VLAN configuration information.

4.1.1Instance: Typical VLAN Configuration

Instance

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?



Example 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.

Analyse the port forwarding entries design as below:

- Port 3

  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 U.

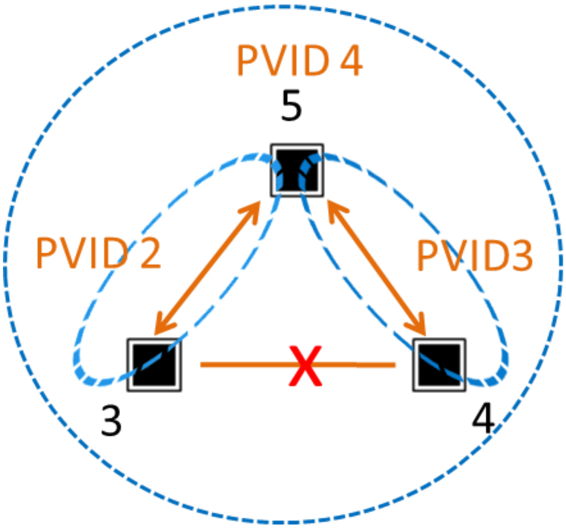
- Port 4

  Port 4 and Port 5 can communicate with each other. Port 4 forwarding entries include Port 4 and Port 5. Therefore, a forwarding entry PVID4 is designed, including Port 4 and Port 5. Configure the "Type" of Port 4 and Port 5 to U.

- Port 5

  Port 5 and Port 3, Port 4 can communicate with each other, Port 5 forwarding entries include Port 3, Port 4. Therefore, design a forwarding entry PVID5, including Port 3, Port 4. Configure the "Type" of Port 3 and Port 4 to U.

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



Operation Steps

Step 1 Enter “Main Menu>Layer 2 Config>VLAN”.

Step 2 Choose “IEEE 802.1Q VLAN” in the option box of “VLAN mode”.

Step 3 Choose “Replace VID into default VID” in the option box of “VLAN frame control”.

Step 4 In the “Default VID” area, enter 3, 4 and 5 respectly as the default VLAN “PVID” of Port3, Port4 and Port5.

Step 5 Enter 3 in “802.1Q VID” textbox.

Step 6 In the drop-down list of “member type”:

1. Set the member type of Port3 to U.
2. Set the member type of Port5 to U.

Step 7 Click “Add/edit” button to add VLAN entry to the “member list”.

Step 8 Enter 4 in “802.1Q VID” textbox.

Step 9 In the drop-down list of “member type”:

1. Set the member type of Port4 to U.
2. Set the member type of Port5 to U.

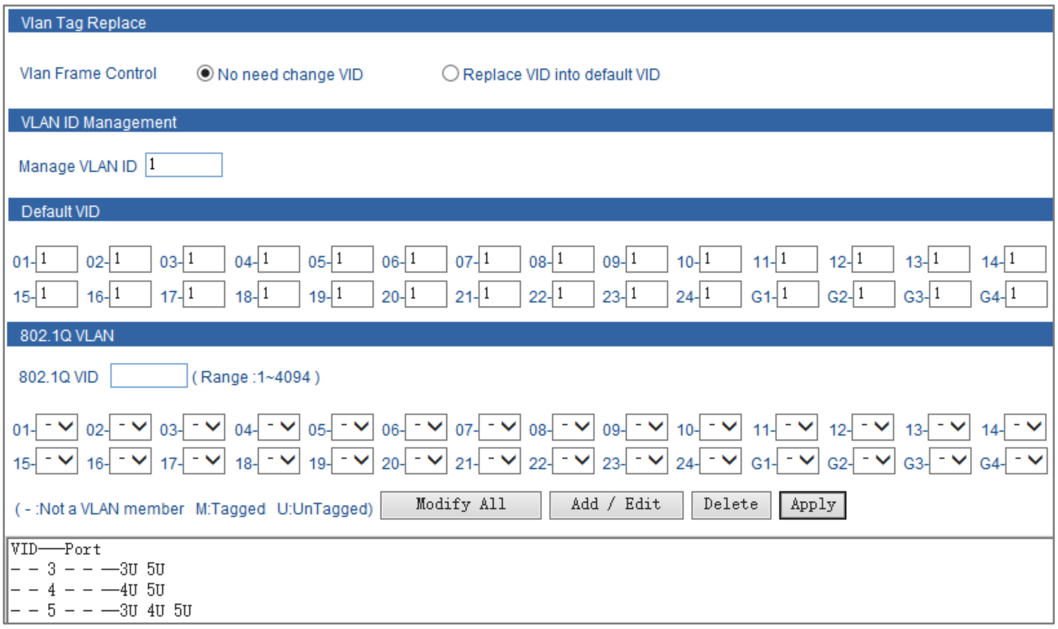
Step 10 Click “Add/edit” button to add VLAN entry to the “member list”.

Step 11 Enter 5 in “802.1Q VID” textbox.

Step 12 In the drop-down list of “member type”:

1. Set the member type of Port3 to U.
2. Set the member type of Port4 to U.
3. Set the member type of Port5 to U.

Step 13 Click “Add/edit” button to add VLAN entry to the “member list”.



Vlan Tag Replace

Vlan Frame Control ● No need change VID ○ Replace VID into default VID

VLAN ID Management

Manage VLAN ID 1

Default VID

01	02	03	04	05	06	07	08	09	10	11	12	13	14
1	1	1	1	1	1	1	1	1	1	1	1	1	1
15	16	17	18	19	20	21	22	23	24	G1	G2	G3	G4
1	1	1	1	1	1	1	1	1	1	1	1	1	1

802.1Q VLAN

802.1Q VID (Range :1~4094)

01	02	03	04	05	06	07	08	09	10	11	12	13	14
-	-	-	-	-	-	-	-	-	-	-	-	-	-
15	16	17	18	19	20	21	22	23	24	G1	G2	G3	G4
-	-	-	-	-	-	-	-	-	-	-	-	-	-

(- :Not a VLAN member M:Tagged U:UnTagged)

```
VID——Port
– – 3 – – —3U 5U
– – 4 – – —4U 5U
– – 5 – – —3U 4U 5U
```

Step 14 Click “Apply” button.

Step 15 End.

4.2 Multicast Filtering

4.2.1 Multicast Filtering

IGMP Snooping (Internet Group Management Protocol Snooping) is an IPv4 layer 2 multicast protocol. And it maintains the outcoming interface information of multicast packets via snooping the multicast protocol packets between layer 3 multicast device and user host. Then it can manage and control the forwarding of multicast data packets in the data link layer.

After configuring the IGMP Snooping, the layer 2 multicast device can snoop and analyze the IGMP packets between the multicast user and upstream router. User can establish layer 2 multicast forwarding items to control the forwarding of multicast data packets. It can prevent multicast data from being broadcast in the Layer 2 network.

IGMP snooping handles different packets in the following way:

- IGMP general query message: The IGMP querier periodically sends IGMP general queries to all hosts and routers on the local network segment to query which multicast groups are available on the network segment.
- IGMP report message: After receiving the IGMP general query message, the member responds to the IGMP report message. The member actively sends an IGMP report message to the IGMP querier to declare the join to the multicast group.
- IGMP Leave message: A member running IGMPv2 or IGMPv3 sends an IGMP Leave message to notify the IGMP querier that it has left a multicast group.

The GMRP Multicast Registration Protocol (GMRP) is an application of the Common Attribute Registration Protocol (GARP) for registering and deregistering multicast attributes. When a host wants to join an IP multicast group, it needs to send an IGMP join message, which is derived into a GMRP jion message. Once the GMRP join message is received, the switch will add the port that received the message to the appropriate multicast group. The switch sends the GMRP join information to all other hosts in the VLAN. One of the hosts serves as the multicast source. When the multicast source sends multicast information, the switch sends the multicast information via the port that joins in the multicast group.

Function Description

On the page of “Multicast Filtering”, user can conduct the following operations:

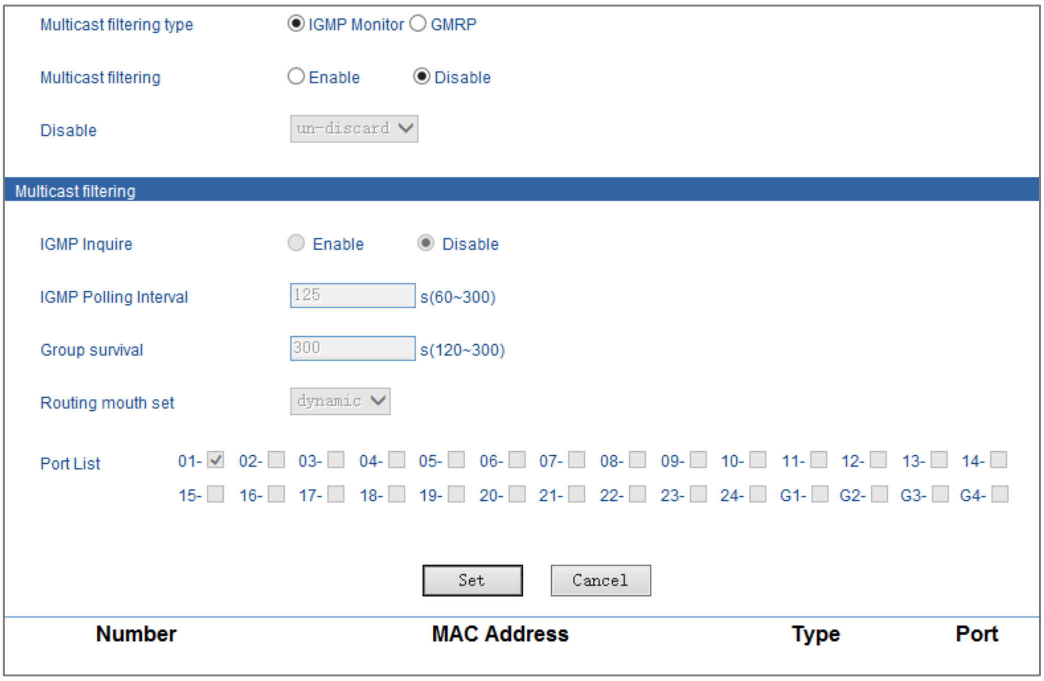
- Enable/disable IGMP Snooping.
- Enable/disable GMRP.
- Enable/disable IGMP Snooping query.
- Set IGMP Snooping query time interval.

Operation Path

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

Interface Description 1: IGMP snooping

IGMP Snooping interface as below:



Multicast filtering type ● IGMP Monitor ○ GMRP

Multicast filtering ○ Enable ● Disable

Disable un-discard

Multicast filtering

IGMP Inquire ○ Enable ● Disable

IGMP Polling Interval 125 s(60~300)

Group survival 300 s(120~300)

Routing mouth set dynamic

Port List 01- ☑ 02- □ 03- □ 04- □ 05- □ 06- □ 07- □ 08- □ 09- □ 10- □ 11- □ 12- □ 13- □ 14- □
15- □ 16- □ 17- □ 18- □ 19- □ 20- □ 21- □ 22- □ 23- □ 24- □ G1- □ G2- □ G3- □ G4- □

Number	MAC Address	Type	Port

The main element configuration description of IGMP Snooping interface:

Interface Element	Description
Multicast filtering type	Choose multicast filtering type, options are: • IGMP snooping; • GMRP.
Multicast filtering	Enable/disable multicast filtering function.
Unknown multicast	Choose the processing mode of unknown multicast, options are: • discard； • un-discard。
Multicast filtering	**The configuration bar of multicast filtering**
IGMP Query	The switch of IGMP query, options are: • Enable • Disable Notes: IGMP query means that router inquiring all hosts in subnet if they join some multicast groups.
IGMP query	IGMP query interval, unit: second. Notes:

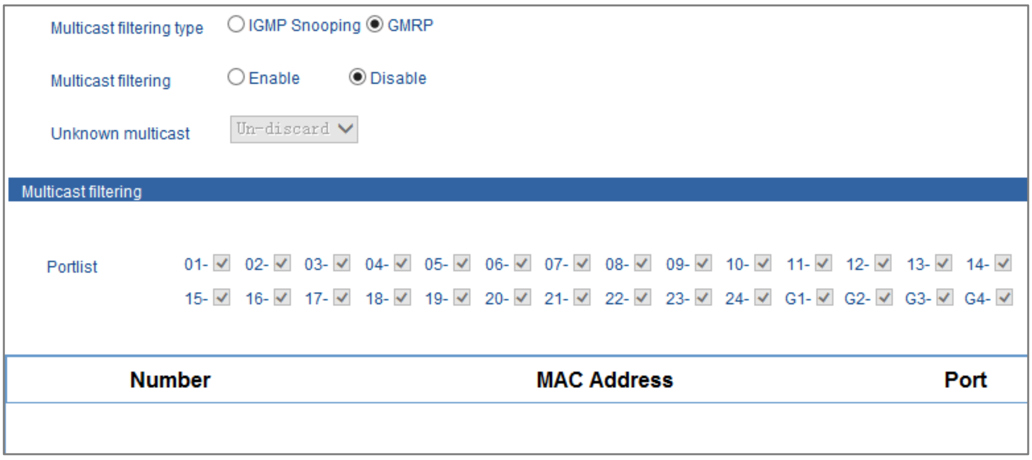
interval	The time range that can be entered is 60-300s.
Group survival	The maximum time that multicast members in device can survive from existence to not receiving any response. Unit: second. Notes: • IGMP snooping needs to be enabled before using this function. • The time range of group survival that can be set is 120-300s.
Routing mouth 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 list	The selection list of static routing port.

Note

- User needs 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.

Interface Description 2: GMRP

GMRP interface as below:



Multicast filtering type ○ IGMP Snooping ● GMRP

Multicast filtering ○ Enable ● Disable

Unknown multicast Un-discard

Multicast filtering

Portlist 01-☑ 02-☑ 03-☑ 04-☑ 05-☑ 06-☑ 07-☑ 08-☑ 09-☑ 10-☑ 11-☑ 12-☑ 13-☑ 14-☑
15-☑ 16-☑ 17-☑ 18-☑ 19-☑ 20-☑ 21-☑ 22-☑ 23-☑ 24-☑ G1-☑ G2-☑ G3-☑ G4-☑

Number	MAC Address	Port

The main element configuration description of GMRP interface:

Interface Element	Description
Multicast filtering type	Multicast filtering type, options are: ● IGMP snooping; ● GMRP.
Multicast filtering	The multicast filtering checkbox, options are: ● Enable; ● Disable.
Unknown multicast	Unknown multicast options are: ● discard； ● un-discard.
Multicast filtering	**The configuration bar of multicast filtering**
Port list	The checkbox of GMRP port list.

4.2.2 Static Multicast

Function Description

On the page of “Static Multicast”, user can configure the following functions:

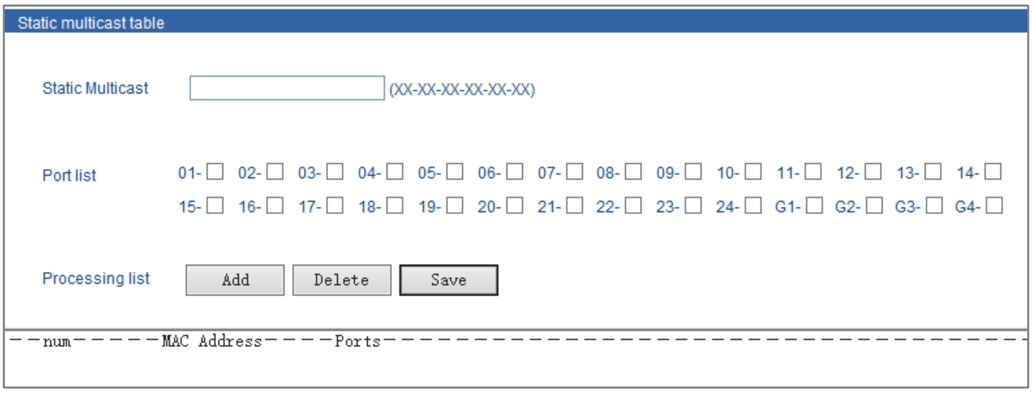
- Enable/disable IGMP Snooping or GMRP.
- Enable/disable multicast filtering.
- Configure the query interval of IGMP Snooping.

Operation Path

Open in order: “Main Menu > L2 Feature > Multicast Filtering > Static multicast table”.

Interface Description

Static filtering interface as follows:



Static multicast table

Static Multicast (XX-XX-XX-XX-XX-XX)

Port list 01-□ 02-□ 03-□ 04-□ 05-□ 06-□ 07-□ 08-□ 09-□ 10-□ 11-□ 12-□ 13-□ 14-□
15-□ 16-□ 17-□ 18-□ 19-□ 20-□ 21-□ 22-□ 23-□ 24-□ G1-□ G2-□ G3-□ G4-□

Processing list

--num-----MAC Address----Ports------------------------------------

Main elements configuration description of static multicast table interface:

Interface Element	Description
MAC Address	Input "MAC Address", and the format should be "XX-XX-XX-XX-XX-XX". Notes: • 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.

Operation steps 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":

a) Tick the check box after "1-";

b) Tick the check box after "2-";

c) Tick the check box after "3-".

Step 4 Click "Add".

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

Step 6 End.

5 QoS

5.1 QoS Classification

Function Description

On the page of QoS Classification, user can set:

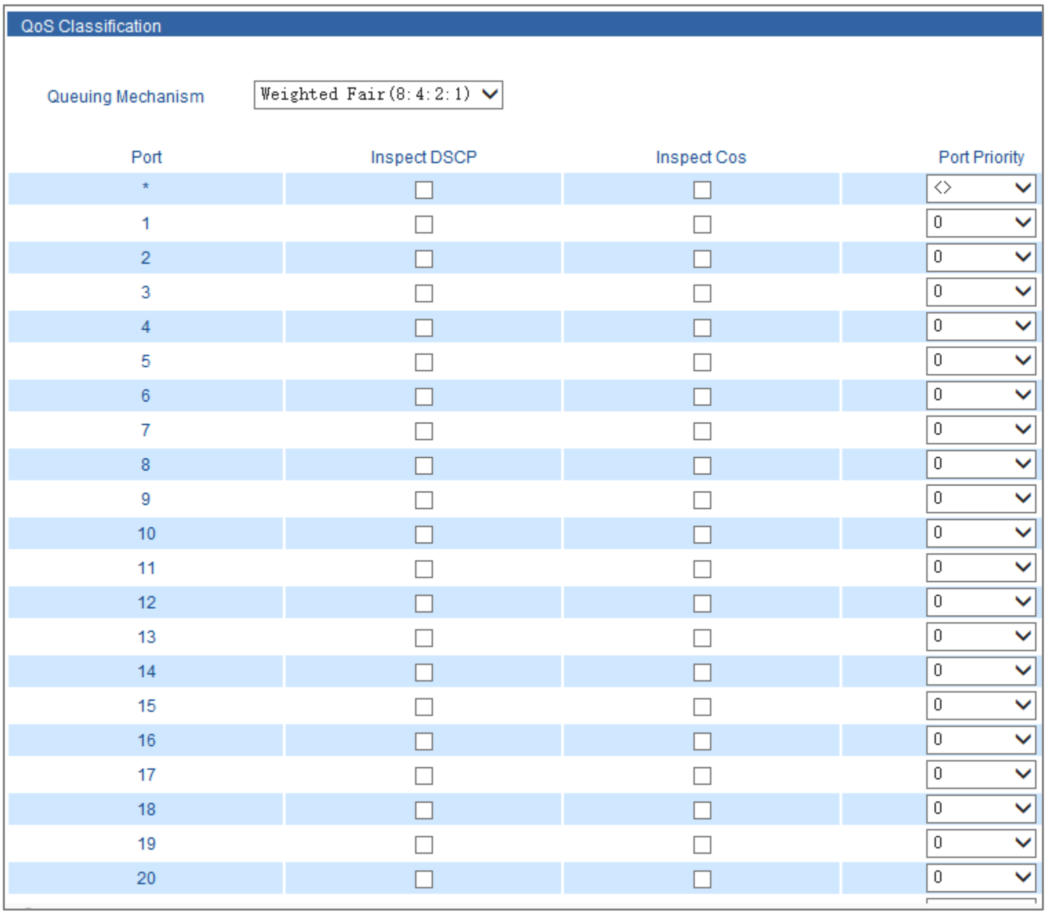
- Queuing mechanism
- Enable ToS
- Enable CoS
- Port priority

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	Inspect DSCP	Inspect Cos	Port Priority
*	□	□	<>
1	□	□	0
2	□	□	0
3	□	□	0
4	□	□	0
5	□	□	0
6	□	□	0
7	□	□	0
8	□	□	0
9	□	□	0
10	□	□	0
11	□	□	0
12	□	□	0
13	□	□	0
14	□	□	0
15	□	□	0
16	□	□	0
17	□	□	0
18	□	□	0
19	□	□	0
20	□	□	0

The main element configuration description of QoS classification interface:

Interface Element	Description
Queuing mechanism	Queuing scheduling setting, options are: • Weighted Fair (8:4:2:1): according to the queue's weighted value 8:4:2:1, weighted round-robin queue scheduling algorithm would schedule queues in turn to ensure that each queue can get some service time. • Strict (Strict Priority): Strict priority queue scheduling algorithm includes 4 queues and schedules in the decreasing order of priority. When the queue with fairly high priority is empty, then it would send groupings of queue with fairly low priority.
Port	Port number of switch.
Inspect ToS	After checking the checkbox, the priority of ToS would be checked during queue scheduling.
Inspect CoS	After checking the checkbox, the priority of CoS would be

Interface Element	Description
	checked during queue scheduling.
Default port priority	To configurate 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. Description: By default, switch would use port priority in place of the 802.1p priority the port comes with when receiving message to control the quality of service the messages deserve.

Note

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

Instance: QoS configuration

For example:

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

Operation steps

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

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

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

Step 4 Click "apply".

Step 5 Ends.

5.2 CoS Mapping

Function Description

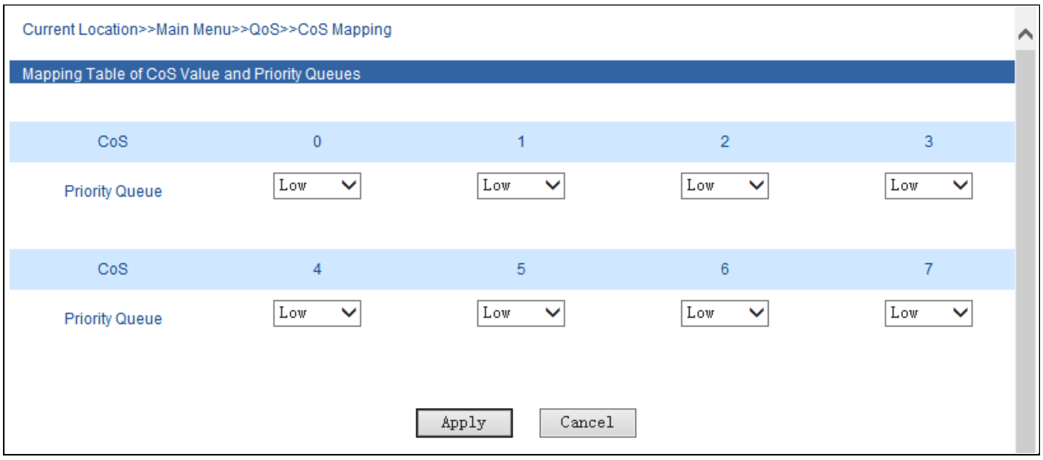
On the page of "CoS Mapping", user can configure the mapping relations between CoS value and priority queues.

Operation Path

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

Interface Description

Screenshot of CoS Mapping interface:



Current Location>>Main Menu>>QoS>>CoS Mapping

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 CoS mapping interface:

Interface Element	Description
CoS	Display CoS value.
Priority queue	Set the mapping between CoS value and priority queue, options 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 Ends.

5.3 DSCP Mapping

Function Description

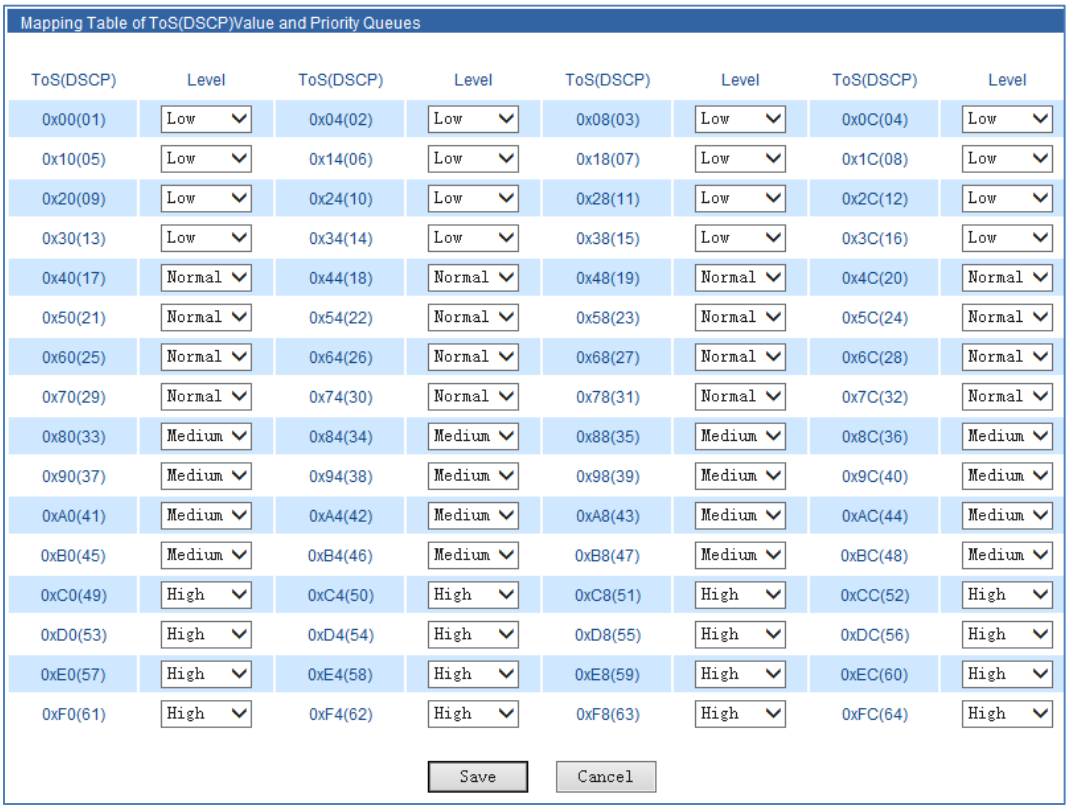
On the page of “DSCP Mapping”, user can configure the mapping relations between DSCP value and priority queue.

Operation Path

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

Interface Description

Screenshot of DSCP Mapping interface:



Mapping Table of ToS(DSCP)Value and Priority Queues

ToS(DSCP)	Level	ToS(DSCP)	Level	ToS(DSCP)	Level	ToS(DSCP)	Level
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)	Normal	0x44(18)	Normal	0x48(19)	Normal	0x4C(20)	Normal
0x50(21)	Normal	0x54(22)	Normal	0x58(23)	Normal	0x5C(24)	Normal
0x60(25)	Normal	0x64(26)	Normal	0x68(27)	Normal	0x6C(28)	Normal
0x70(29)	Normal	0x74(30)	Normal	0x78(31)	Normal	0x7C(32)	Normal
0x80(33)	Medium	0x84(34)	Medium	0x88(35)	Medium	0x8C(36)	Medium
0x90(37)	Medium	0x94(38)	Medium	0x98(39)	Medium	0x9C(40)	Medium
0xA0(41)	Medium	0xA4(42)	Medium	0xA8(43)	Medium	0xAC(44)	Medium
0xB0(45)	Medium	0xB4(46)	Medium	0xB8(47)	Medium	0xBC(48)	Medium
0xC0(49)	High	0xC4(50)	High	0xC8(51)	High	0xCC(52)	High
0xD0(53)	High	0xD4(54)	High	0xD8(55)	High	0xDC(56)	High
0xE0(57)	High	0xE4(58)	High	0xE8(59)	High	0xEC(60)	High
0xF0(61)	High	0xF4(62)	High	0xF8(63)	High	0xFC(64)	High

The main element configuration description of DSCP mapping interface:

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

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 > DSCP 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 Ends.

6 Link Backup

6.1 Rapid Ring

Function Description

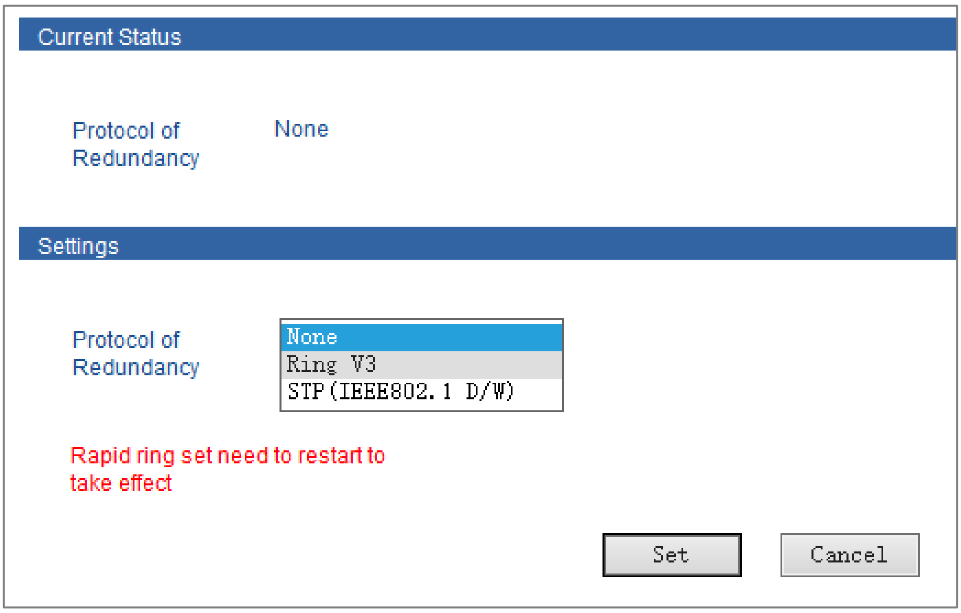
On the “Rapid ring” page, user can choose redundancy protocol and configure the ring network under this protocol quickly.

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 / Ring V3 / STP(IEEE802.1 D/W)

Rapid ring set need to restart to take effect

The main element configuration description of initial rapid ring interface:

Interface Element	Description
Protocol of redundancy	Choose the corresponding redundancy protocol. Options are: ● None: it means that the ring network function is disabled. ● Ring V3: single ring, coupling ring, chain and Dual homing are supported. ● STP (IEEE 802.1W/1D): spanning tree.

Function description of Ring V3

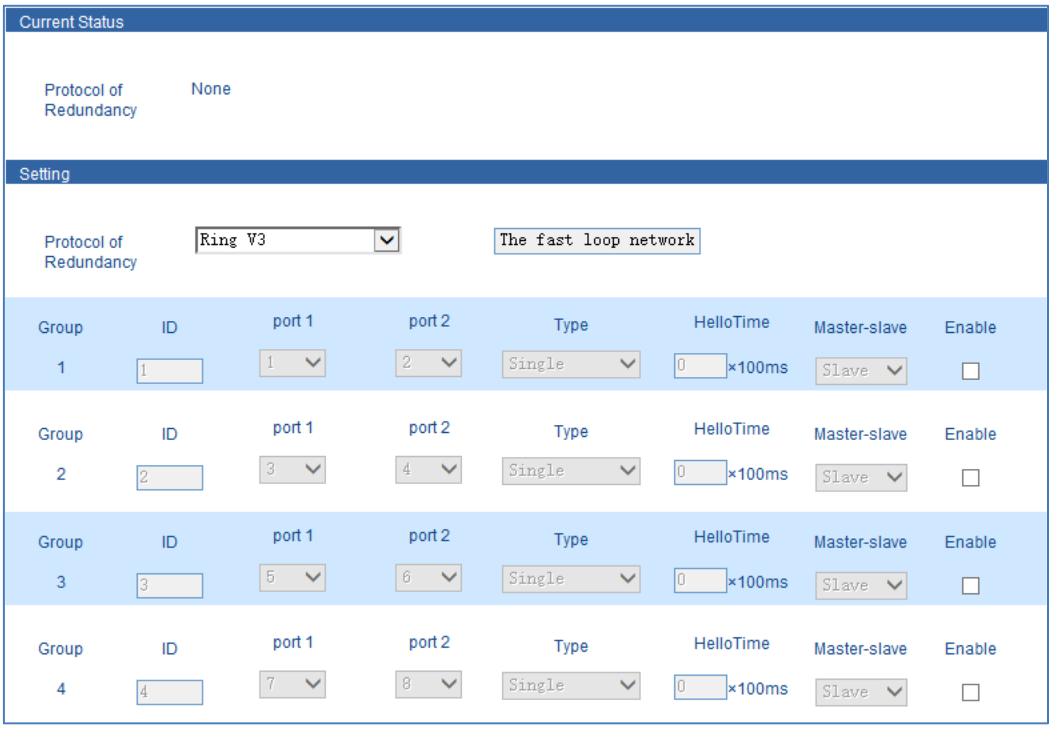
On the page of “rapid ring”, user can choose Ring V3 redundancy protocol and configure the ring network under this protocol quickly.

Operation Path

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

Interface Description

Initial rapid ring network interface as follows:



Current Status

Protocol of Redundancy: None

Setting

Protocol of Redundancy: Ring V3

The fast loop network

Group	ID	port 1	port 2	Type	HelloTime	Master-slave	Enable
1	1	1	2	Single	0 ×100ms	Slave	□
2	2	3	4	Single	0 ×100ms	Slave	□
3	3	5	6	Single	0 ×100ms	Slave	□
4	4	7	8	Single	0 ×100ms	Slave	□

The main element configuration description of Ring network interface:

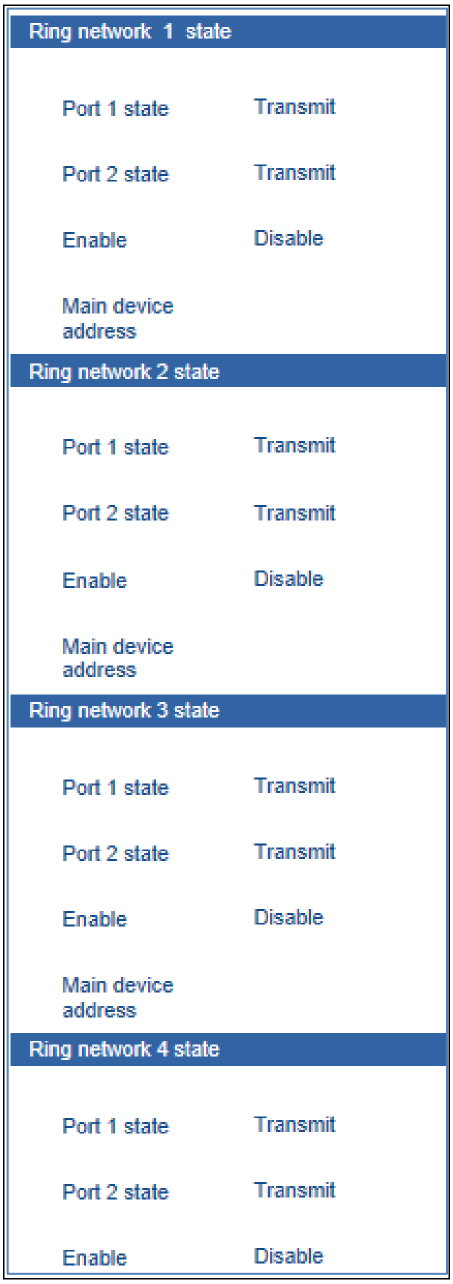
Interface Element	Description
Rapid ring state	Click “rapid ring state” to check the ring state of current ring network group configuration.
Group	Support Group 1-2 or Group 1-4, it means that the device

Interface Element	Description
	supports up to 2 or 4 groups. Notes: Device with less than 10 ports supports up to 2 rings, device with more than 10 ports supports 4 rings.
ID	When multiple switches form a ring, the current ring ID would be network ID. Different ring network has different ID.
Port 1	port 1 can be used for the formation of ring network in switch.
Coupling port	When the ring type is “Couple”, the coupling port would be the one connects different network ID.
Port 2	Port 2 can be used for the formation of ring network in switch.
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 network. • Single: single ring, using a continuous ring to connect all device together. • Couple: couple ring is a redundant structure used for connecting two independent networks. • Chain: chain can enhance user’s flexibility in constructing all types of redundant network topology via an advanced software technology. • Dual-homing: two adjacent rings share one switch. User could put one switch in two different networks or two different switching equipments in one network.
HelloTime	Hello_time is the 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. Notes: Some products don’t support Master-slave option, so their ring network is non-master station structure.

Interface Element	Description
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 network 1 state

Port 1 state	Transmit
Port 2 state	Transmit
Enable	Disable
Main device address	

Ring network 2 state

Port 1 state	Transmit
Port 2 state	Transmit
Enable	Disable
Main device address	

Ring network 3 state

Port 1 state	Transmit
Port 2 state	Transmit
Enable	Disable
Main device address	

Ring network 4 state

Port 1 state	Transmit
Port 2 state	Transmit
Enable	Disable

The main element configuration description of initial rapid ring interface

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

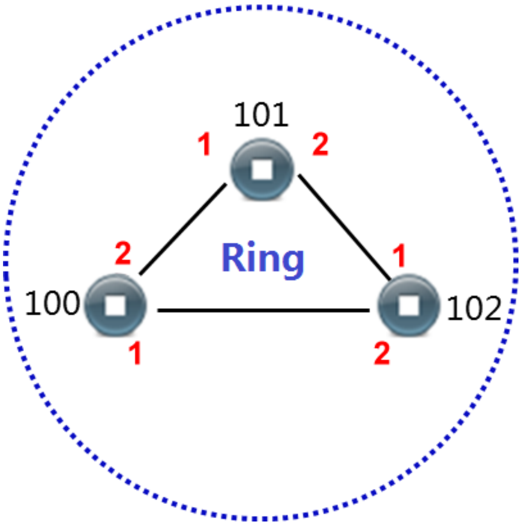
Single ring could be created when the redundant protocol is “Ring V1”, “Ring V2” or “Ring V3”. Here we take creating single ring in Ring V3 for example.

Note

Using Ring V1 and Ring V2 to create ring network is the same as using Ring V3.

Instance

For example: create the following single ring:



Instance analysis

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

Operation steps

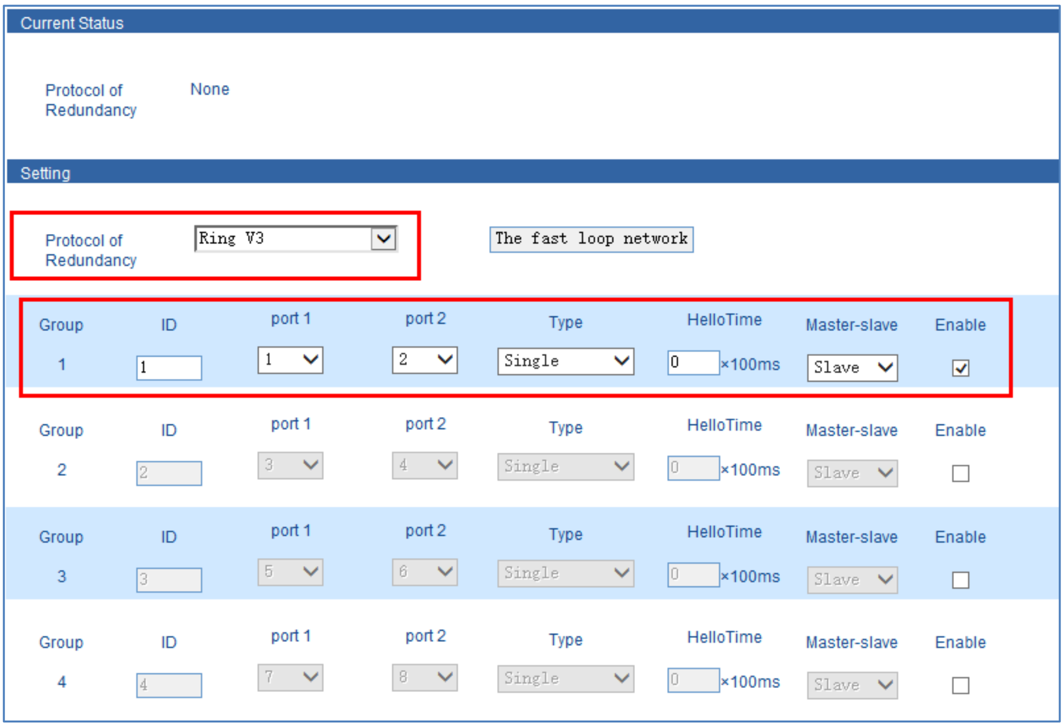
Configuring Device 100, 101 and 102 in the following steps:

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

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

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

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



Current Status

Protocol of Redundancy None

Setting

Protocol of Redundancy Ring V3

Group	ID	port 1	port 2	Type	HelloTime	Master-slave	Enable
1	1	1	2	Single	0 ×100ms	Slave	☑
2	2	3	4	Single	0 ×100ms	Slave	□
3	3	5	6	Single	0 ×100ms	Slave	□
4	4	7	8	Single	0 ×100ms	Slave	□

Step 5 Enter “1” in the “ID” textbox of “Group1”.

Step 6 Set “Port 1” as “01” and “Port 2” as “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.

⚠ Notice

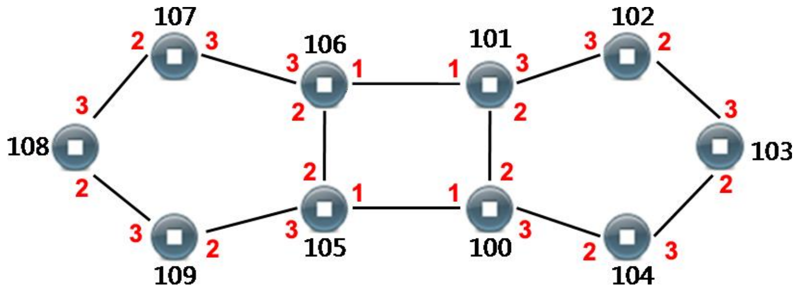
If the device exists the option of "Master-slave", the mode of one master multiple slaves is recommended to be used.

6.1.2 Instance: create coupling ring

Here we take creating coupling ring in Ring V3 for example.

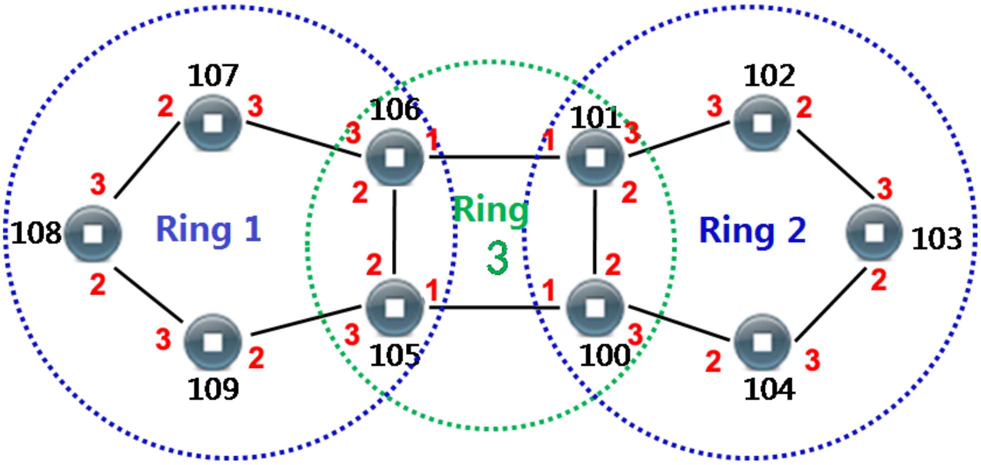
Instance

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

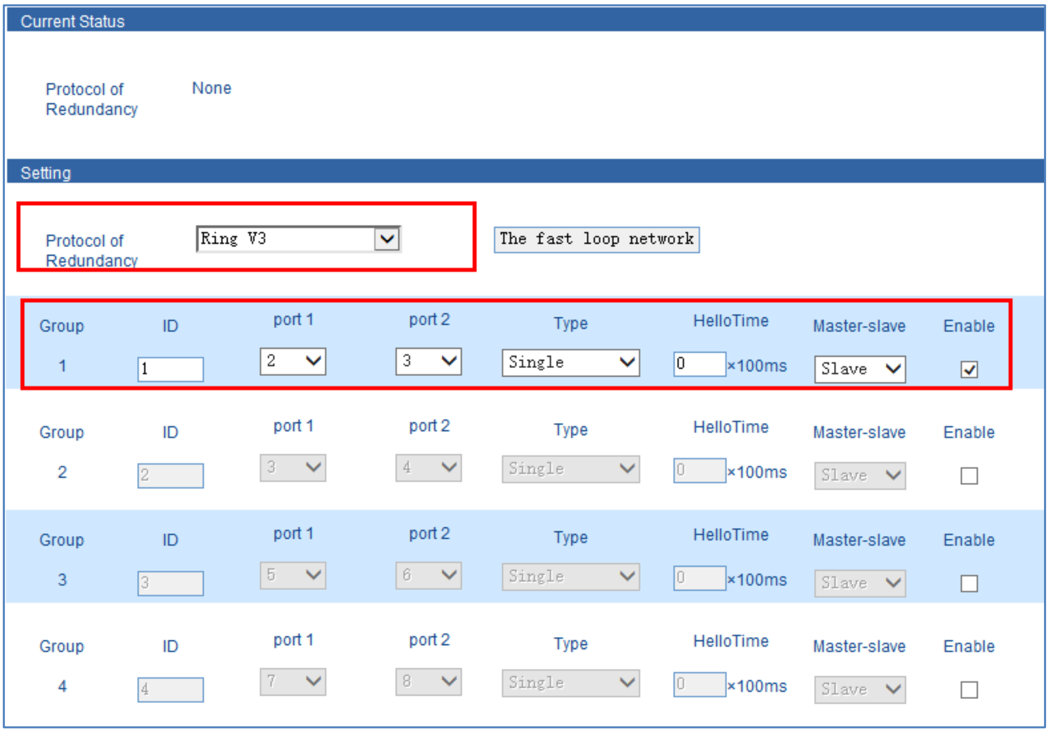
Configuring Device 105, 106, 107, 108 and 109 in the following steps respectively.

Step 1 Choose "Main Menu > Redundancy > Rapid Ring".

Step 2 In the "Settings" area of "Rapid Ring" page, choose "Ring V3" as "Protocol of Redundancy".

Step 3 Check the "Enable" box in the "Group 1".

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



Current Status

Protocol of Redundancy None

Setting

Protocol of Redundancy Ring V3 The fast loop network

Group	ID	port 1	port 2	Type	HelloTime	Master-slave	Enable
1	1	2	3	Single	0 ×100ms	Slave	☑
2	2	3	4	Single	0 ×100ms	Slave	□
3	3	5	6	Single	0 ×100ms	Slave	□
4	4	7	8	Single	0 ×100ms	Slave	□

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 Address".

Step 10 In the area of "reboot the device", click "reboot".

Step 11 End.

Operation Step 2: configuring Ring 2 in WEB interface

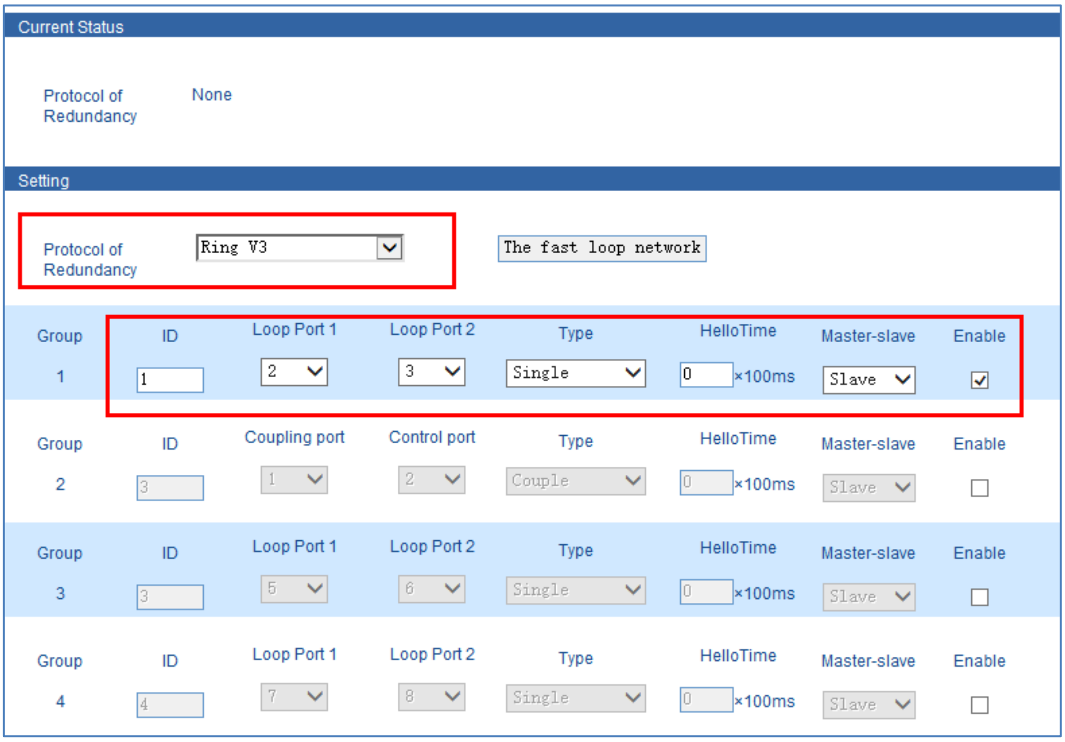
Configuring Device 100, 101, 102, 103 and 104 in the following steps respectively.

Step 1 Choose "Main Menu > Redundancy > Rapid Ring".

Step 2 In the "Settings" area of "Rapid Ring" page, choose "Ring V3" as "Protocol of Redundancy".

Step 3 Check the "Enable" box in the "Group 1".

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



Current Status

Protocol of Redundancy: None

Setting

Protocol of Redundancy: Ring V3 — The fast loop network

Group	ID	Loop Port 1	Loop Port 2	Type	HelloTime	Master-slave	Enable
1	1	2	3	Single	0 ×100ms	Slave	☑
Group	ID	Coupling port	Control port	Type	HelloTime	Master-slave	Enable
2	3	1	2	Couple	0 ×100ms	Slave	☐
Group	ID	Loop Port 1	Loop Port 2	Type	HelloTime	Master-slave	Enable
3	3	5	6	Single	0 ×100ms	Slave	☐
Group	ID	Loop Port 1	Loop Port 2	Type	HelloTime	Master-slave	Enable
4	4	7	8	Single	0 ×100ms	Slave	☐

Step 5 Enter "2" 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 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 Address”.

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 “Ring V3” as “Protocol of Redundancy”.

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

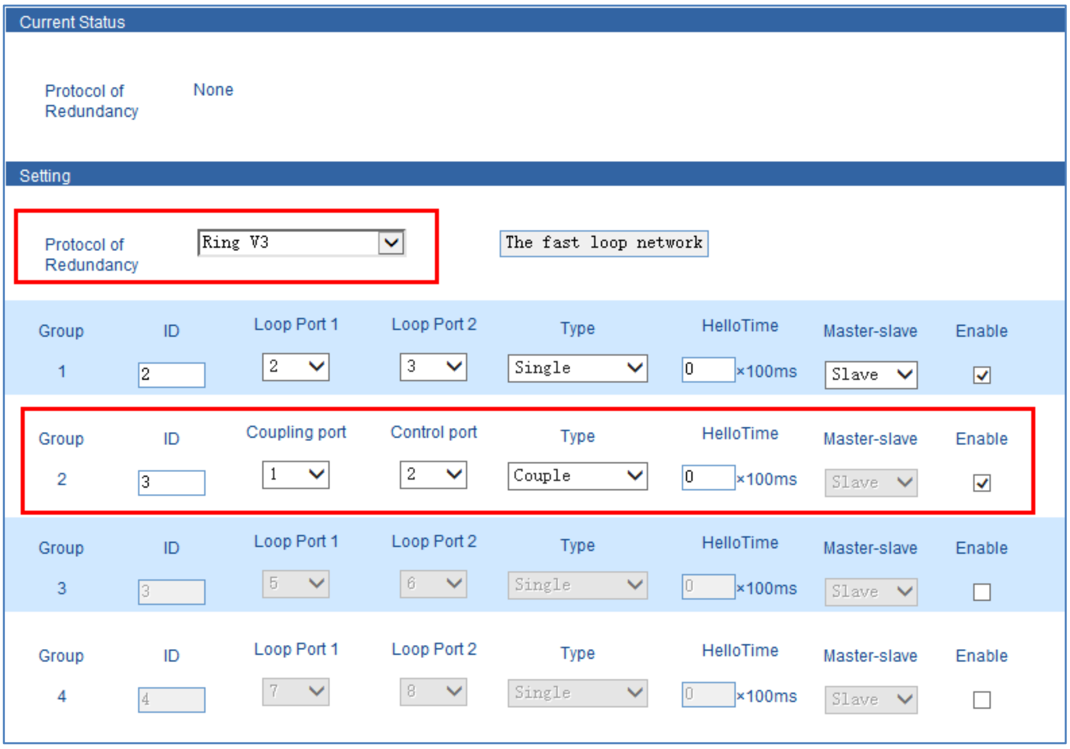
Step 6 Choose “1” in the drop-down list of “Coupling Port” of “Group 2”.

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

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

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

Step 10 End.



Current Status

Protocol of Redundancy: None

Setting

Protocol of Redundancy: Ring V3 — The fast loop network

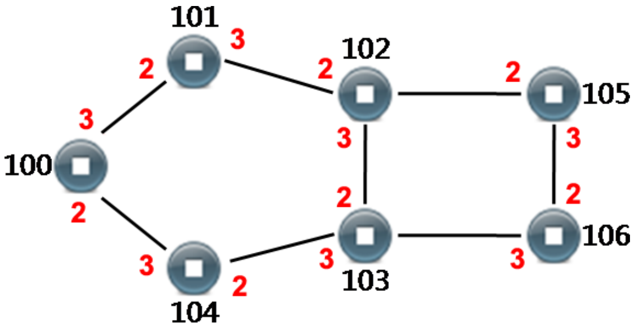
Group	ID	Loop Port 1	Loop Port 2	Type	HelloTime	Master-slave	Enable
1	2	2	3	Single	0 ×100ms	Slave	☑
Group	ID	Coupling port	Control port	Type	HelloTime	Master-slave	Enable
2	3	1	2	Couple	0 ×100ms	Slave	☑
Group	ID	Loop Port 1	Loop Port 2	Type	HelloTime	Master-slave	Enable
3	3	5	6	Single	0 ×100ms	Slave	□
Group	ID	Loop Port 1	Loop Port 2	Type	HelloTime	Master-slave	Enable
4	4	7	8	Single	0 ×100ms	Slave	□

Instance: creating chain

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

Instance

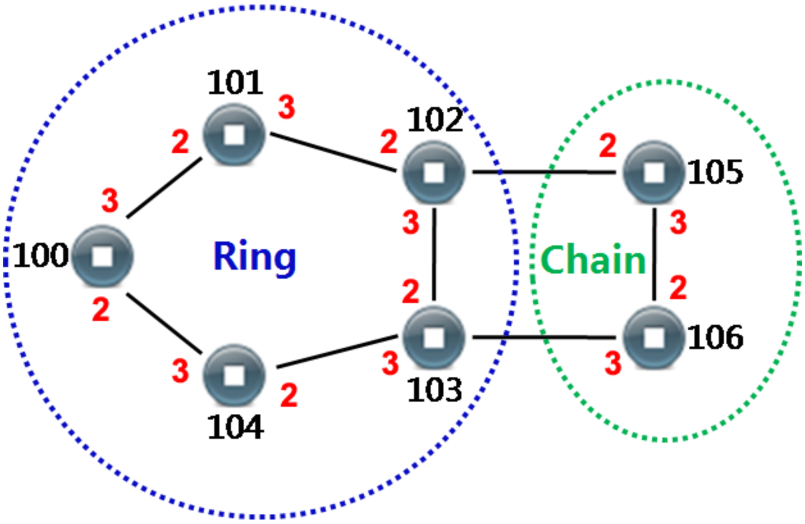
For example: creating chain. Its basic architecture is shown as below:



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 “Ring V3” as “Protocol of Redundancy”.

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

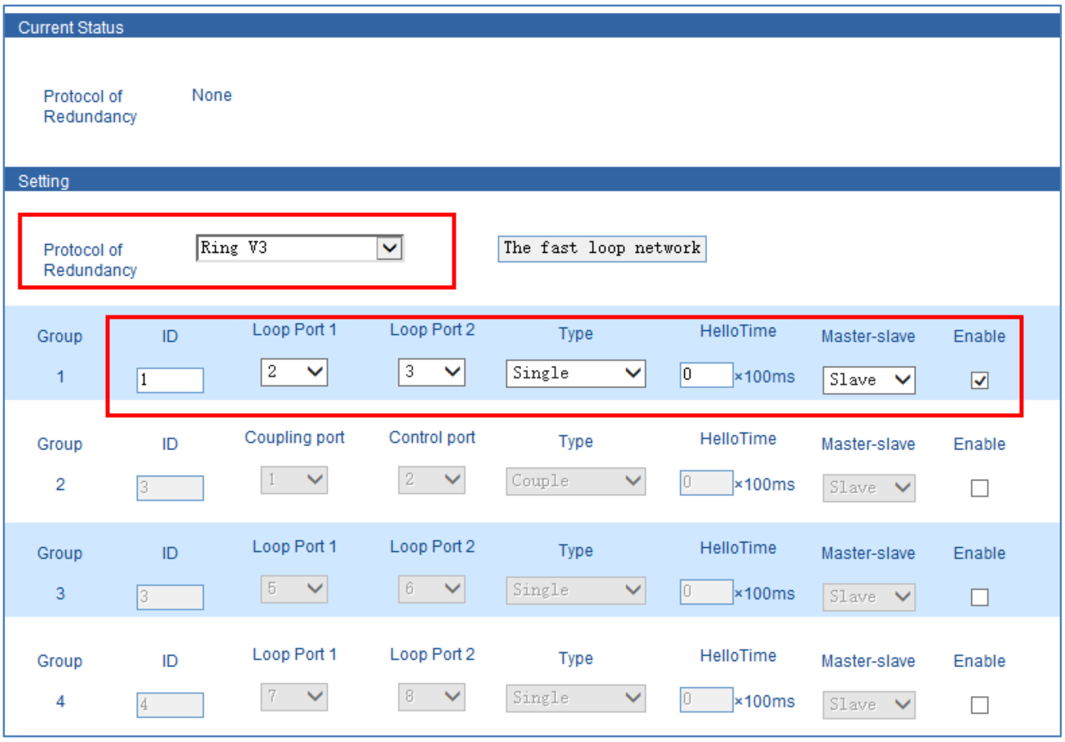
Step 4 In the “settings” area of “Rapid Ring”:

1. Set “Type” to “Single”;

2. Set “ID” to “1”;

3. Set “Port 1” to “2”;

4. Set “Port 2” to “3”;



Current Status

Protocol of Redundancy None

Setting

Protocol of Redundancy Ring V3 The fast loop network

Group	ID	Loop Port 1	Loop Port 2	Type	HelloTime	Master-slave	Enable
1	1	2	3	Single	0 ×100ms	Slave	☑
Group	ID	Coupling port	Control port	Type	HelloTime	Master-slave	Enable
2	3	1	2	Couple	0 ×100ms	Slave	□
Group	ID	Loop Port 1	Loop Port 2	Type	HelloTime	Master-slave	Enable
3	3	5	6	Single	0 ×100ms	Slave	□
Group	ID	Loop Port 1	Loop Port 2	Type	HelloTime	Master-slave	Enable
4	4	7	8	Single	0 ×100ms	Slave	□

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 Address”.

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”.

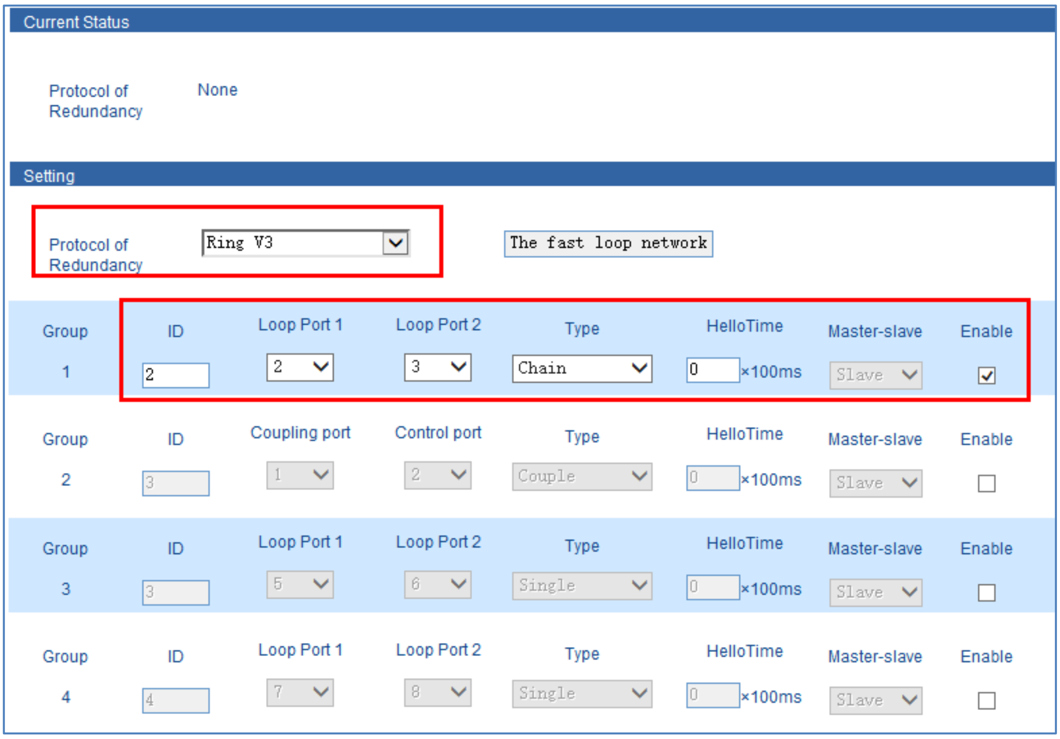
Step 2 In the “Settings” area of “Rapid Ring” page, choose “Ring V3” as “Protocol of Redundancy”.

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 “02” and set “Port 2” to “03”.



Current Status

Protocol of Redundancy: None

Setting

Protocol of Redundancy: Ring V3 — The fast loop network

Group	ID	Loop Port 1	Loop Port 2	Type	HelloTime	Master-slave	Enable
1	2	2	3	Chain	0 ×100ms	Slave	☑
Group	ID	Coupling port	Control port	Type	HelloTime	Master-slave	Enable
2	3	1	2	Couple	0 ×100ms	Slave	□
Group	ID	Loop Port 1	Loop Port 2	Type	HelloTime	Master-slave	Enable
3	3	5	6	Single	0 ×100ms	Slave	□
Group	ID	Loop Port 1	Loop Port 2	Type	HelloTime	Master-slave	Enable
4	4	7	8	Single	0 ×100ms	Slave	□

Note

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

Step 7 Click “Apply”.

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

Step 9 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.

6.1.3 Creating Spanning Tree

Function description

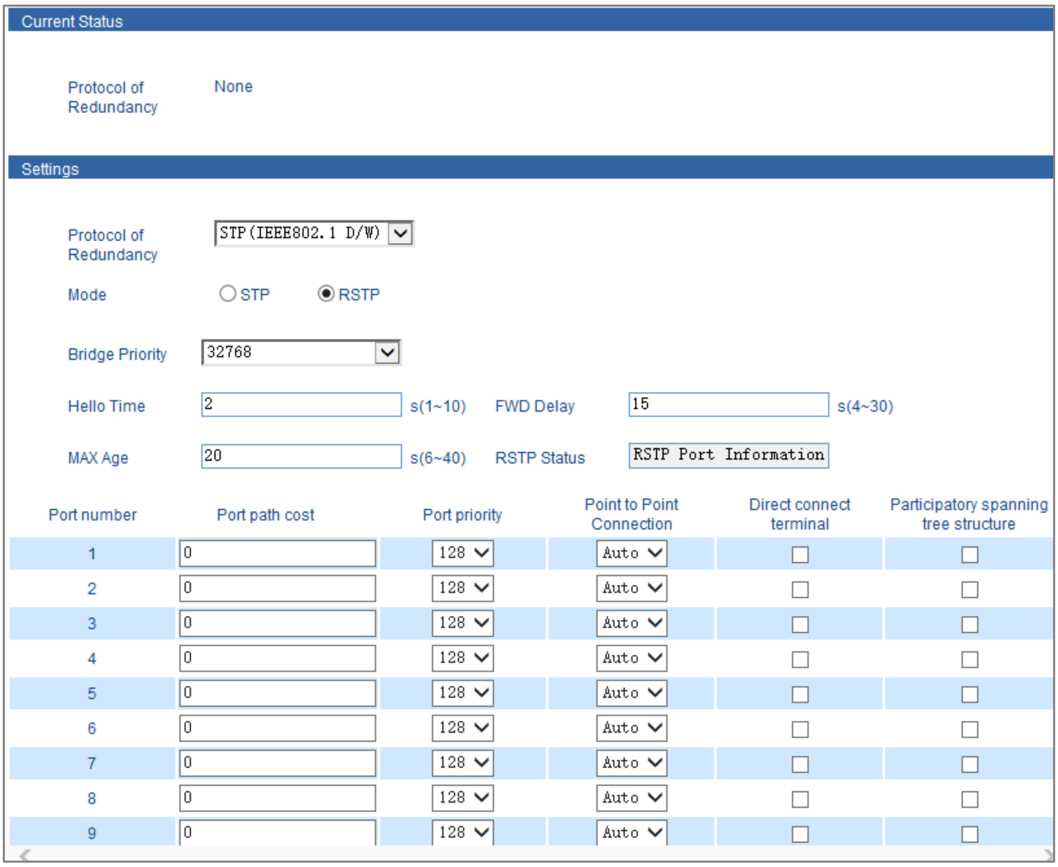
On the “Rapid ring” page, user can choose “RSTP (IEEE 802.1D/W)” as redundancy protocol to create spanning tree quickly.

Operation Path

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

Interface Description

Spanning tree interface as follows:



Current Status

Protocol of Redundancy: None

Settings

Protocol of Redundancy: STP(IEEE802.1 D/W)

Mode: ○ STP ● RSTP

Bridge Priority: 32768

Hello Time: 2 s(1~10) FWD Delay: 15 s(4~30)

MAX Age: 20 s(6~40) RSTP Status: RSTP Port Information

Port number	Port path cost	Port priority	Point to Point Connection	Direct connect terminal	Participatory spanning tree structure
1	0	128	Auto	□	□
2	0	128	Auto	□	□
3	0	128	Auto	□	□
4	0	128	Auto	□	□
5	0	128	Auto	□	□
6	0	128	Auto	□	□
7	0	128	Auto	□	□
8	0	128	Auto	□	□
9	0	128	Auto	□	□

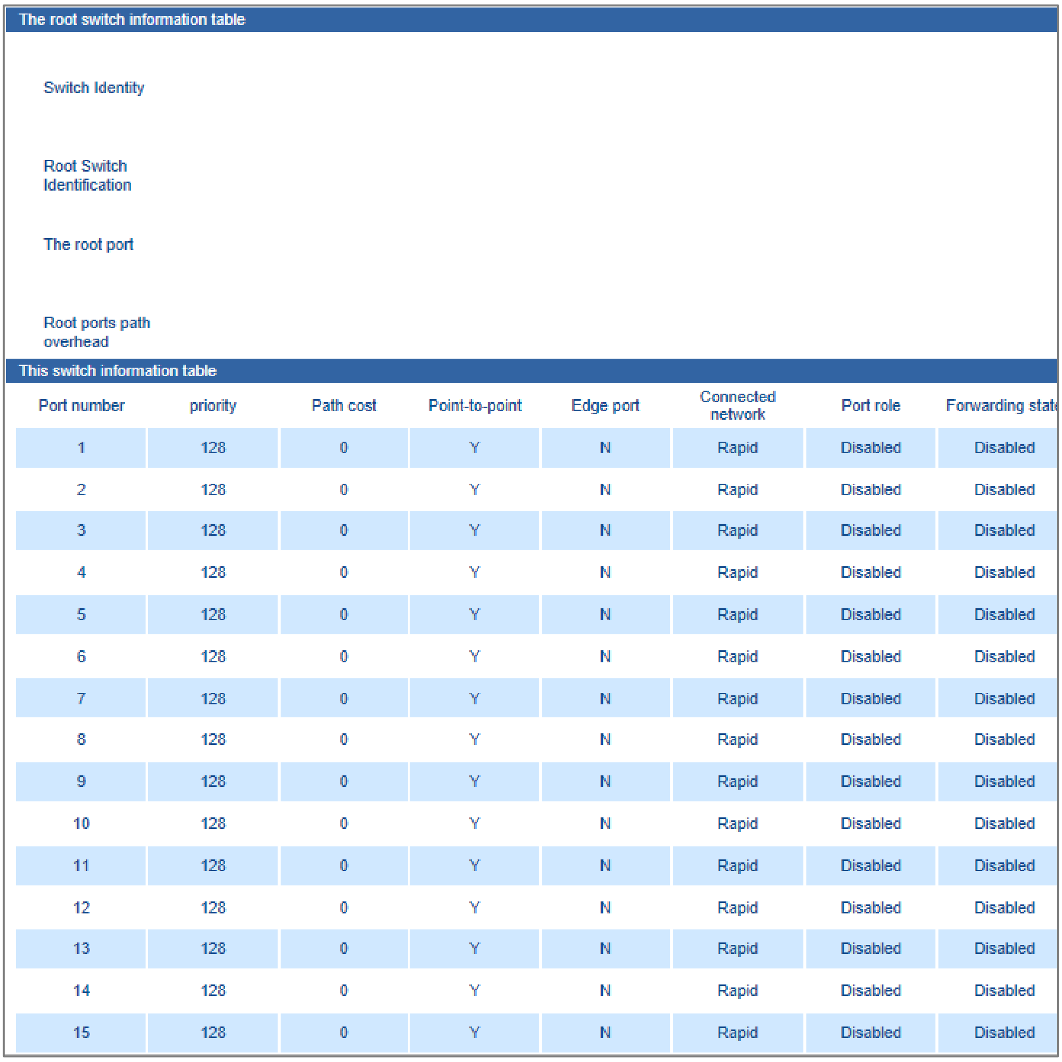
The main element configuration description of RSTP interface:

Interface Element	Description
Protocol of redundancy	Choose the algorithm of redundancy protocol, options are: • None: represents disabling ring network function;

	● Ring V1: supports single ring; ● Ring V2: supports single ring and coupling ring; ● 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	The transmission time interval of the BPDU data packet. Note: The protocol message that STP/RSTP adopts is BPDU (Bridge Protocol Data Unit).
FWD delay	The forward delay time that the port of switch maintains in transition state (listening and learning). Note: STP/RSTP adopts a mechanism of state transition. The newly-selected root port and specified port have to go through twice the Forward Delay time to enter the forwarding state.
MAX age	The lifetime of BPDU packets.
RSTP status	Button, used for checking the current status of rapid spanning tree.
Port	Displays the port number of the device.
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.
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.
Edge	The switch that is on the edge of network and connects to the

	terminal devices.
Port STP	Checking this checkbox. It represents participating in the operation of spanning tree protocol.

RSTP status interface as follows:



The root switch information table

Switch Identity

Root Switch Identification

The root port

Root ports path overhead

This switch information table

Port number	priority	Path cost	Point-to-point	Edge port	Connected network	Port role	Forwarding stat
1	128	0	Y	N	Rapid	Disabled	Disabled
2	128	0	Y	N	Rapid	Disabled	Disabled
3	128	0	Y	N	Rapid	Disabled	Disabled
4	128	0	Y	N	Rapid	Disabled	Disabled
5	128	0	Y	N	Rapid	Disabled	Disabled
6	128	0	Y	N	Rapid	Disabled	Disabled
7	128	0	Y	N	Rapid	Disabled	Disabled
8	128	0	Y	N	Rapid	Disabled	Disabled
9	128	0	Y	N	Rapid	Disabled	Disabled
10	128	0	Y	N	Rapid	Disabled	Disabled
11	128	0	Y	N	Rapid	Disabled	Disabled
12	128	0	Y	N	Rapid	Disabled	Disabled
13	128	0	Y	N	Rapid	Disabled	Disabled
14	128	0	Y	N	Rapid	Disabled	Disabled
15	128	0	Y	N	Rapid	Disabled	Disabled

The main element configuration description of RSTP status interface:

Interface Element	Description
Root information	**The display bar of root information table**
Local ID	It displays the priority of this switch and MAC address information ID.
Root ID	It displays the priority of the root switch and MAC address

	information ID.
Root port	The port of the switch, which is not in the root bridge but nearest to it, is in charge of communicating with the root bridge. The path cost from this port to the root bridge is the lowest. When the path costs of multiple ports are the same, the one with the highest priority would be the root port.
Root cost	The root cost of a switch is the sum of root port cost and the root cost that data packet goes through all switches. The root cost of root bridge is zero.
Basic information	**The display bar of basic information table**
Port	It displays the port number of this device.
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 ERPS

Ethernet Ring Protection Switching (ERPS) is the Ethernet Ring Network Link Layer Technology with high reliability and stability. It can prevent the broadcast storm caused by data loop when the Ethernet ring is intact. When the Ethernet ring link failure occurs, it has high convergence speed that can rapidly recover the communication path between each node in the ring network.

Function Description

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

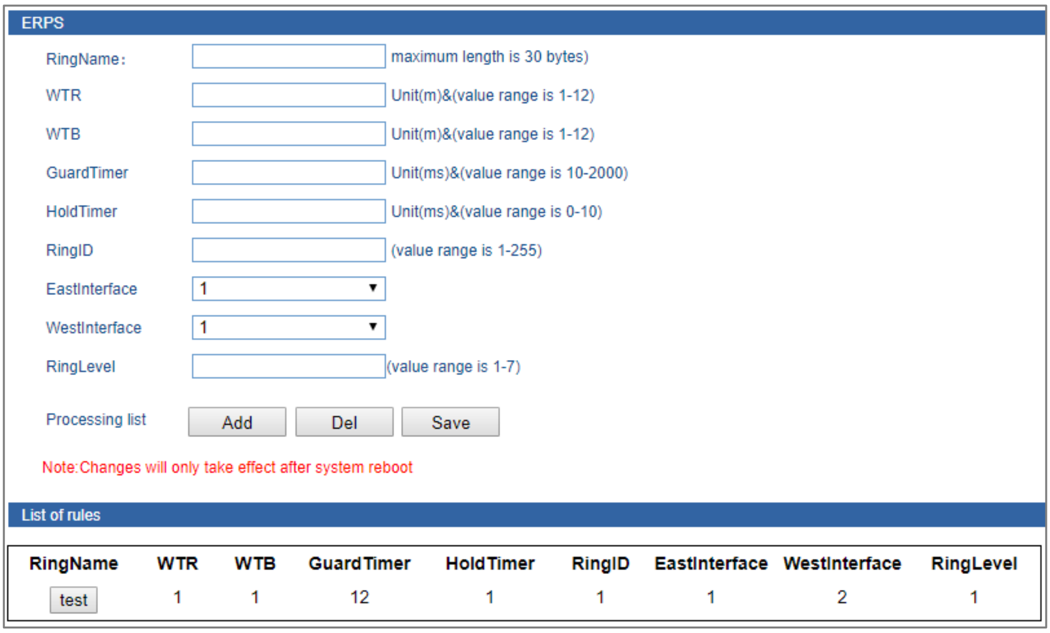
An Ethernet network topology connected in ring is called a ERPS Ring. It could be divided into main ring and subring. Every device in the ERPS ring is a node. The main node is in charge of blocking and opening ports on this node, preventing loops from forming.

Operation Path

Open in order: "Main Menu > Link Backup >ERPS”.

Interface Description1

ERPS interface as follows:



ERPS

RingName: maximum length is 30 bytes)

WTR Unit(m)&(value range is 1-12)

WTB Unit(m)&(value range is 1-12)

GuardTimer Unit(ms)&(value range is 10-2000)

HoldTimer Unit(ms)&(value range is 0-10)

RingID (value range is 1-255)

EastInterface 1

WestInterface 1

RingLevel (value range is 1-7)

Note:Changes will only take effect after system reboot

List of rules

RingName	WTR	WTB	GuardTimer	HoldTimer	RingID	EastInterface	WestInterface	RingLevel
test	1	1	12	1	1	1	2	1

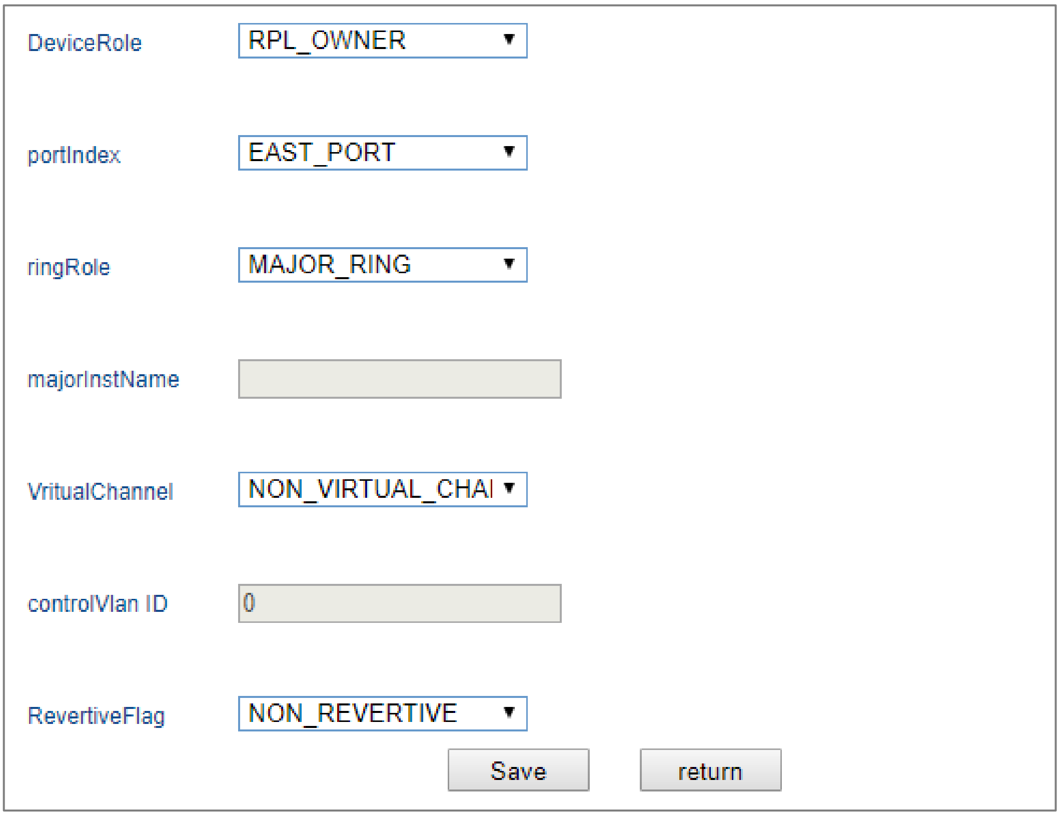
The main element configuration description of erps interface.

Interface Element	Description
ERPS	**ERPS configuration**
RingName	Name of ERPS and ring network, the maximum length is 30 bytes
WTR	WTR(Wait To Restore)timer, its value range is 1-12 minutes. Under revertive mode, the timer starts when the owner node in protection state receives NR packet. The owner node blocks the RPL port and unblocks the fault port after the timer expires.
WTB	WTB（Wait To Block）timer, its value range is 1-12 minutes. Under revertive mode, when the owner node is in MS (Manual Switch) or FS (Forced Switch) status, WTB timer will start if user carries out clean command on the owner node. After the timer expires, the owner node will block the RPL port and unblock temporary blocking port.
GuardTimer	Guard timer, its value range is 10-2000ms. The timer starts when the port detects the link restoration, before the timer expires, the port won’t deal with R-APS (Ring Automatic Protection Switching) packet.

Interface Element	Description
HoldTimer	Hold timer, its value range is 0-10ms. The timer starts when the port detects the link restoration, delay the fault report speed. When the link fails, the timer should report the fault if it exists after Hold timer expires.
RingID	The ID of ring network, its value range is 1-255
EastInterface	Ring network 1, its value range is 1-port number
WestInterface	Ring network 2, its value range is 1-port number
RingLevel	The higher the ring network level is, the greater the value is, its value range is 1-7
Operation	Click the button to operate: ● Add ● Delete
Ring List	The added ring could be displayed in this list. The ERPS configuration interface would pop up when clicking Ringname button

Interface Description 2

ERPS config interface as follows：



DeviceRole: RPL_OWNER

portIndex: EAST_PORT

ringRole: MAJOR_RING

majorInstName:

VritualChannel: NON_VIRTUAL_CHAI

controlVlan ID: 0

RevertiveFlag: NON_REVERTIVE

The main element configuration description of erps configuration interface.

Interface Element	Description
Device Role	Each device in ERPS ring is called a node. The node role is decided by user configuration, they are divided into following types: • RPL-Owner: owner node is responsible for blocking and unblocking the port in RPL of the node to prevent loop forming and conduct link switching. • RPL-Neighbor: neighbor node is connected to Owner node on RPL. Cooperating to the Owner node, it blocks and unblocks the ports on RPL of the node and conduct link switching. • Interconnection: interconnected node is the node to connect multiple rings in the multi-loop model, it belongs to the subring, and the primary ring has no interconnected node. In the link protocol packet upload mode between the two subring interconnected nodes, the subring protocol packet ends in the interconnected node, but the data packet won’t

Interface Element	Description
	end. • Other: normal node is the other node in addition to the above three nodes. Normal node is responsible for receiving and forwarding the protocol packet and data packet in the link.
RPL-Port	RPL (Ring Protection Link) port is the appointed ring network port for Owner node to establish RPL. Options: • EAST_PORT； • WEST_PORT。
Ring Role	Options of Ring Role drop-down box: • Major-ring: main ring network • Sub-ring: subring network
Major Instance Name	The major instance name could be set and need to be set as ERPS instance name only when the ring role is Sub-ring
Virtual Channel	After enable virtual channel, the subring protocol packet could transmit across the primary ring; otherwise, the subring protocol packet can only transmit in the ring. Options: • NON_VIRTUAL_CHANNEL; • VIRTUAL_CHANNEL.
Control VLAN	The VLAN channel of protocol packet, its value range is 1-4094
Revertive	Options: • Enable: In revertive mode, WTR timer starts when the owner node receives the link recovery packet after the clearing of fault. The timer will change from fault link protection status to idle status after timeout. • Disable: Irreversible mode: Owner node doesn’t conduct any action after receiving the link recovery packet and keeps the port status set before.

6.3 Loop Guard

Function Description

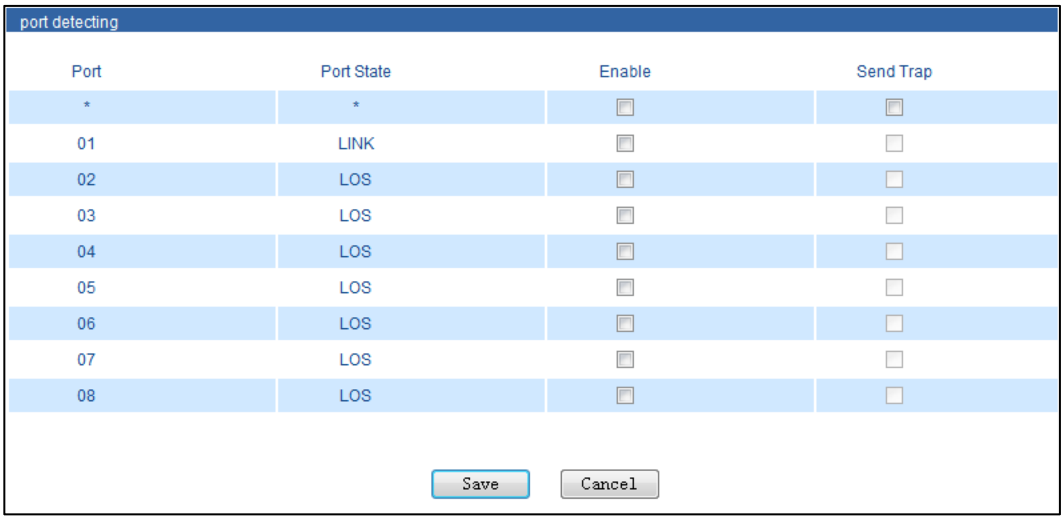
On the “Loop guard” page, user can configure related loop guard settings to prevent ring network storm.

Operation Path

Open in order: “Main Menu > Redundancy > Loop Guard”.

Interface Description

Loop guard interface as follows



port detecting

Port	Port State	Enable	Send Trap
*	*	□	□
01	LINK	□	□
02	LOS	□	□
03	LOS	□	□
04	LOS	□	□
05	LOS	□	□
06	LOS	□	□
07	LOS	□	□
08	LOS	□	□

The main element configuration description of loop guard interfaces

Interface Element	Description
Port	Display port number.
Port state	Display port's connection state: ● LOS: disconnected ● LINK: connected ● Self-loop ● Looping with port X (X presents port number)
Enable	Check the box to enable loop guard. When the ring network is not enabled on rapid ring page and ports are in a loop, enabling this function on any port will not cause storm. Notes: Ring network port cannot be set to loop detection port.
Send trap	Check the box to enable trap sending. When self-loop and looping occur, it would send TRAP alarm of SNMP. Notes: Before enabling this function, user needs to enable SNMP configuration function on SNMP configuration page and set SNMP Trap address. Then the trap sending function can take effect.

6.4 Port Trunking

6.4.1 Static Trunking

Function Description

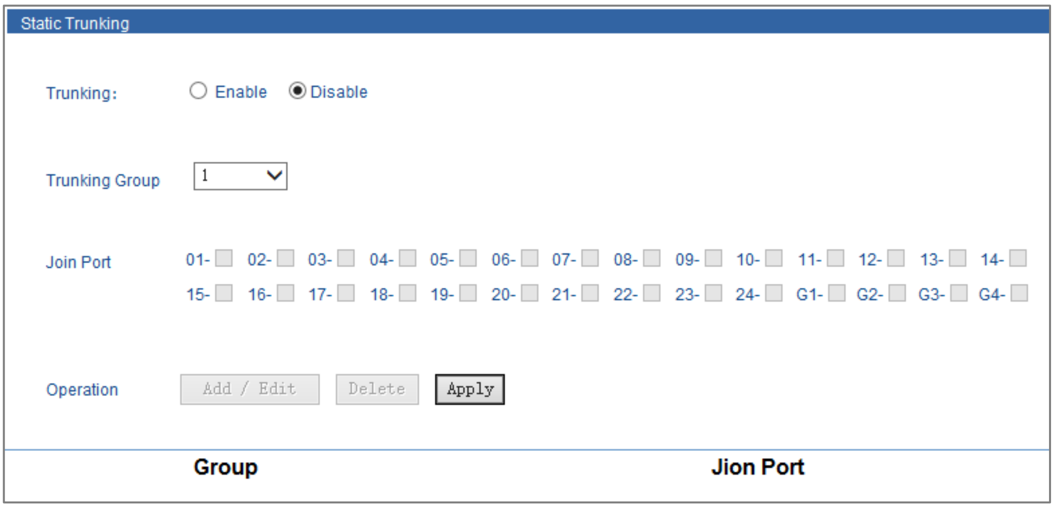
Binding multiple physical ports into one logical channel.

Operation Path

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

Interface Description

Static Trunking interface as follows:



Static Trunking

Trunking: ○ Enable ● Disable

Trunking Group 1

Join Port
01-□ 02-□ 03-□ 04-□ 05-□ 06-□ 07-□ 08-□ 09-□ 10-□ 11-□ 12-□ 13-□ 14-□
15-□ 16-□ 17-□ 18-□ 19-□ 20-□ 21-□ 22-□ 23-□ 24-□ G1-□ G2-□ G3-□ G4-□

Operation

Group	Jion Port

The main element configuration description of static trunking interface:

Interface Element	Description
Trunking	Enable or disable trunking configuration.
Trunking Group	Choose trunking group.
Join port	Check the box of ports that join the trunking group.
Operation	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, we could improve bandwidth by grouping them into a Trunking group.

Operation Steps

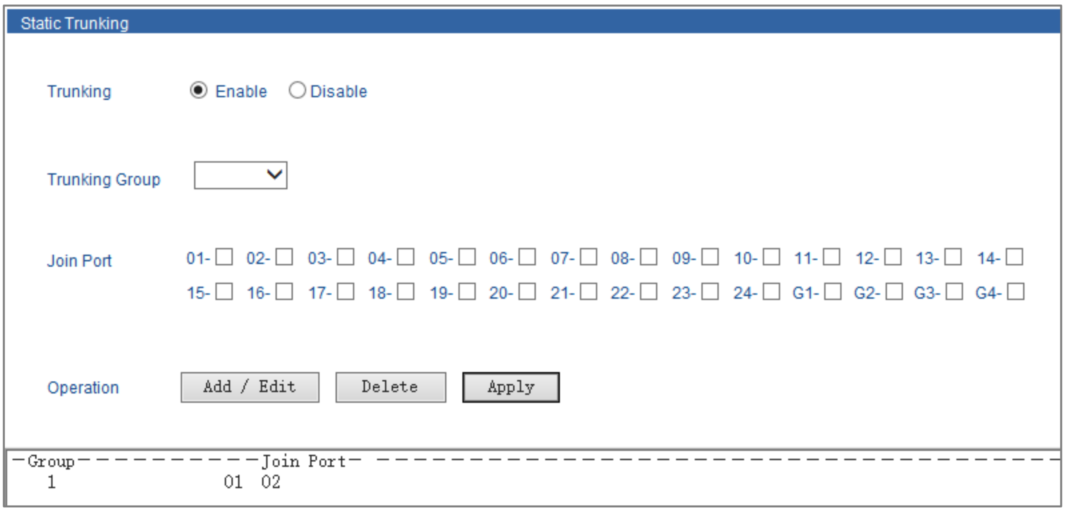
Configure switch A and switch B in the same way respectively.

Step 1 Log in Web configuration page.

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

Trunking ● Enable ○ Disable

Trunking Group

Join Port
01- □ 02- □ 03- □ 04- □ 05- □ 06- □ 07- □ 08- □ 09- □ 10- □ 11- □ 12- □ 13- □ 14- □
15- □ 16- □ 17- □ 18- □ 19- □ 20- □ 21- □ 22- □ 23- □ 24- □ G1- □ G2- □ G3- □ G4- □

Operation

```
-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

Function Description

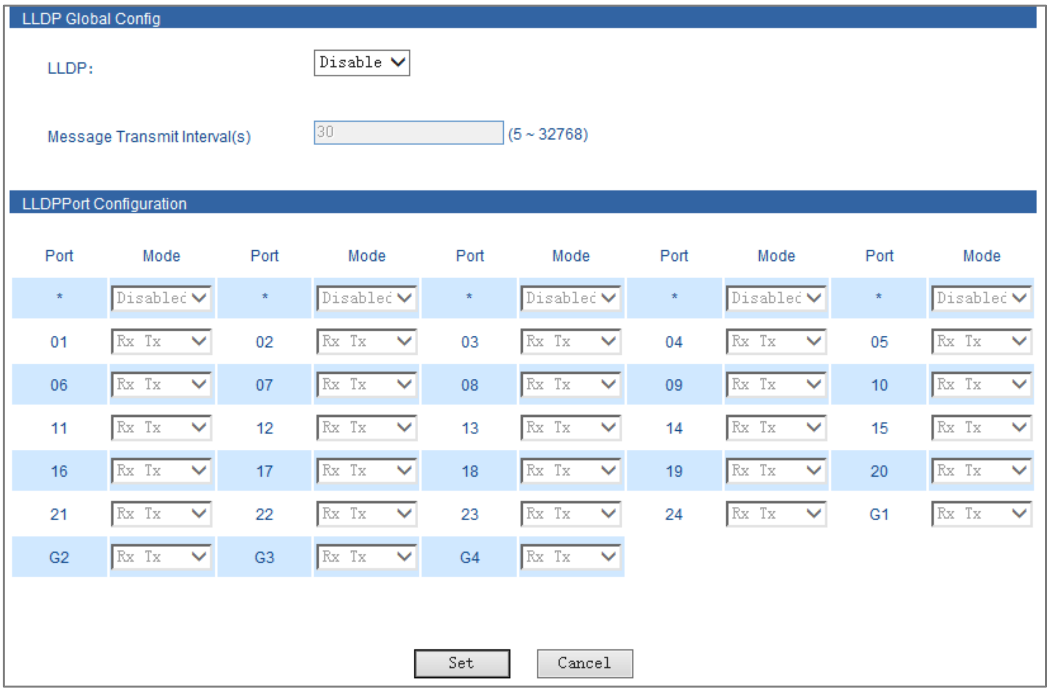
On the page of “Parameters Configuration”, user can configure LLDP function of the port and notify its device identity and performance in the local device.

Operation Path

Open in order: “Main Menu > LLDP > Parameter Configuration”.

Interface Description

Parameter configuration interface as follows:



LLDP Global Config

LLDP: Disable

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

LLDPPort Configuration

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	09	Rx Tx	10	Rx Tx
11	Rx Tx	12	Rx Tx	13	Rx Tx	14	Rx Tx	15	Rx Tx
16	Rx Tx	17	Rx Tx	18	Rx Tx	19	Rx Tx	20	Rx Tx
21	Rx Tx	22	Rx Tx	23	Rx Tx	24	Rx Tx	G1	Rx Tx
G2	Rx Tx	G3	Rx Tx	G4	Rx Tx				

Main elements configuration description of parameter configuration interface:

Interface Elements	Description
LLDP Global Config	**LLDP global configuration column**
LLDP	Enable/disable LLDP function.
Message Transmit Interval	Interval time for messages sending is 5-32768s. For preventing abounding LLDP sending caused by frequent changes of local information, next message should be delayed to send out after sending a LLDP message.
LLDP port configuration	**LLDP port configuration column**
Port	Display port number of the device
Mode	• Disable: disable LLDP function. • Tx Rx: send and receive LLDP message. • Tx only: periodically send LLDP message to neighbor device. • Rx only: conduct validity check to 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:

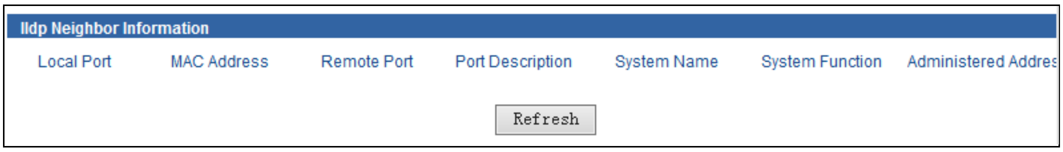
- MAC address;
- Remote port;
- Port description;
- System name;
- System function;
- Management address.

Operation Path

Open in order: “Main Menu > LLDP > Neighbor Information”.

Interface Description

Neighbor information interface as follows:



Main elements configuration description of neighbor information interface:

Interface Elements	Description
Local port	Corresponding local port number of the device.
MAC address	Discover corresponding MAC address of the neighbor device.
Remote port	Port number of neighbor device.
Port description	Port description information of the neighbor device.
System Name	System name of the neighbor device.
System function	System functions of the neighbor device.
Management address	Management addresses information of the neighbor device. Management address is the address provided for network management system to identify and manage the network devices. Management address can definitely identify a device, which is convenient for the drawing of

Interface Elements	Description
	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 User Password

Enterprises usually want to divide the permission of system (network) administrator and the one monitoring the device. That is, the former only takes charge of the management of monitoring services, and the latter is responsible for the system or network management. 3onedata switches provide hierarchical management as follows:

●Observer permission: permission to view.

●System administrator: permission to modify and view.

Function Description

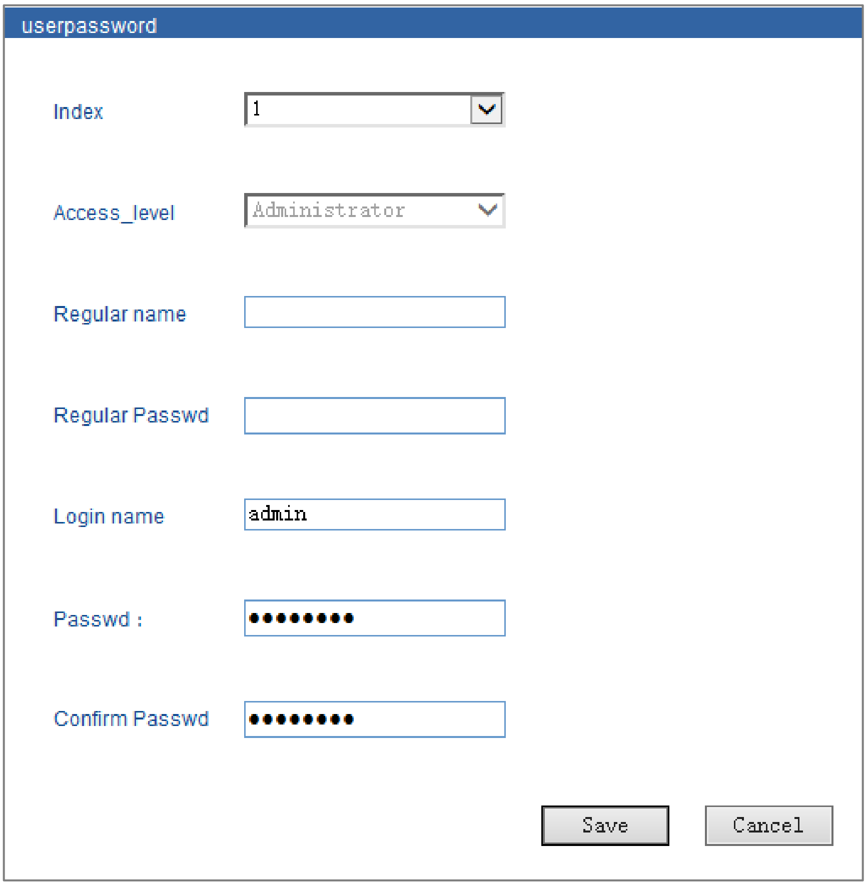
On the “User Password” page, user can configure the login name and password of logging in to WEB configuration page and other parameter information.

Operation Path

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

Interface Description

User password interface as follows:



userpassword

Index: 1

Access_level: Administrator

Regular name:

Regular Passwd:

Login name: admin

Passwd : ●●●●●●●●

Confirm Passwd: ●●●●●●●●

The main element configuration description of user password interface:

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

Password	Login password setting of WEB configuration interface. Note: The password should a combination of letters that less than 16 bytes.
Confirm password	Confirm 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 WEB configuration interface are “admin”.

For instance: create administrator

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

Operation Path

Step 1 Log in to 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 “regular name”
4. Enter “regular password”
5. Enter “admin8” as “login name”
6. Enter “admin8” as “password”
7. Enter “admin8” as “confirm password”.

Step 4 Click “apply”.

Step 5 End.

8.2 DHCP Server

DHCP (Dynamic Host Configuration Protocol) is the technology that intensively configures and dynamically manages the IP addresses of users.

DHCP adopts the client/server communication mode. The DHCP Client sends configuration application to the DHCP Server, and the server sends back the configuration information distributed for the DHCP Client (including IP address, default gateway, DNS Server). All of these can realize IP addresses distribution and concentrated configuration management of other networks parameters.

Function Description

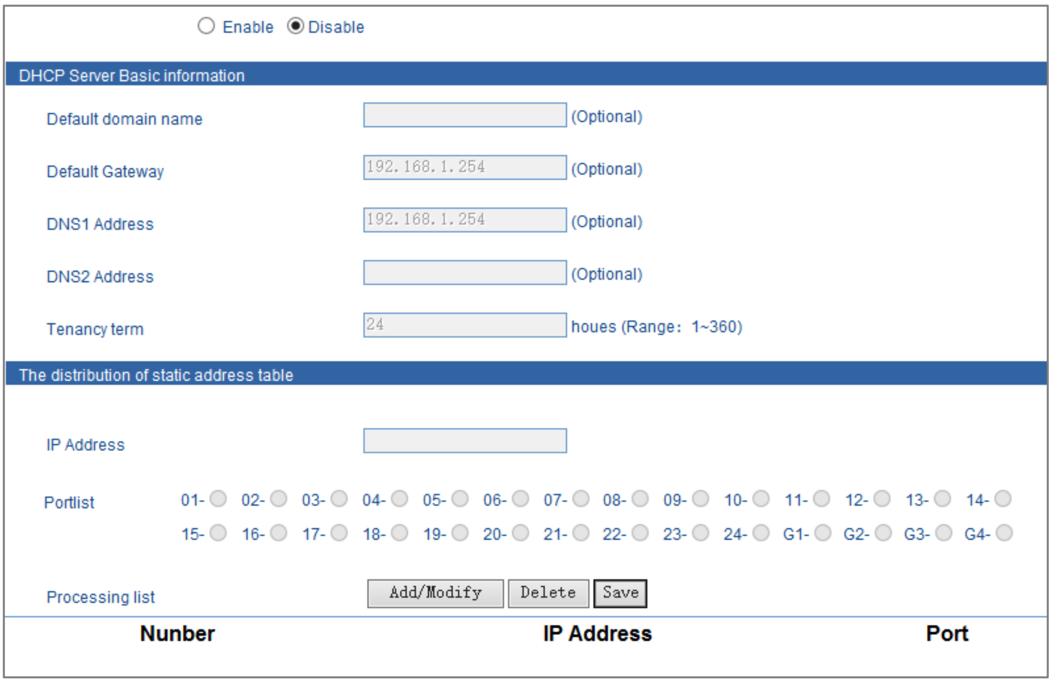
On the “DHCP Server” page, user can distribute network address statically.

Operation Path

Open in order: “Main Menu > Access Control > DHCP Server”.

Interface Description

DHCP Server interface as follows:



○ Enable ● Disable

DHCP Server Basic information

Default domain name (Optional)

Default Gateway 192.168.1.254 (Optional)

DNS1 Address 192.168.1.254 (Optional)

DNS2 Address (Optional)

Tenancy term 24 houes (Range: 1~360)

The distribution of static address table

IP Address

Portlist 01- ○ 02- ○ 03- ○ 04- ○ 05- ○ 06- ○ 07- ○ 08- ○ 09- ○ 10- ○ 11- ○ 12- ○ 13- ○ 14- ○
15- ○ 16- ○ 17- ○ 18- ○ 19- ○ 20- ○ 21- ○ 22- ○ 23- ○ 24- ○ G1- ○ G2- ○ G3- ○ G4- ○

Processing list

Nunber	IP Address	Port

The main element configuration description of DHCP server interface:

Interface Element	Description
DHCP Server	Enable/disable DHCP server function.
DHCP Server Basic Information	**The configuration bar of DHCP server basic information**
Default domain name	The domain name that can be captured by DHCP client automatically.
Default gateway	The gateway that can be captured by DHCP client automatically.
DNS address	The DNS address that can be captured by DHCP client

	automatically.
Tenancy term	The valid time that DHCP client can capture address automatically. 1-360 hour (optional).
The distribution of static address table	**The configuration bar of static address distribution table** Notes: The IP address list that DHCP client can automaticcaly capture in different ports.
IP address	The IP address that can be captured by DHCP client automatically.

8.3 Port Authentication

IEEE 802.1X protocol is a port-based network access control protocol, That is, accessed user equipment is authenticated on the port of LAN access device, so that user equipment controls the access to network resources.

IEEE 802.1x authentication system structure adopts "controllable port" and "uncontrollable port" logic function, which can achieve the separation of business and authentication. After user passes authentication, the business flow and authentication flow achieve separation, there exists no special requirements for subsequent data packet process, business can be flexible, and the business has great advantages in carrying out broadband multicast and other aspects; all businesses are not subject to the authentication method.

802.1X structure is mainly composed of three parts:

- Supplicant: User or client who wants to gain authentication;
- Authentication server: A typical example is RADIUS server;
- Authenticator: Interterminal equipment, such as wireless access point, switch and so on.

Function Description

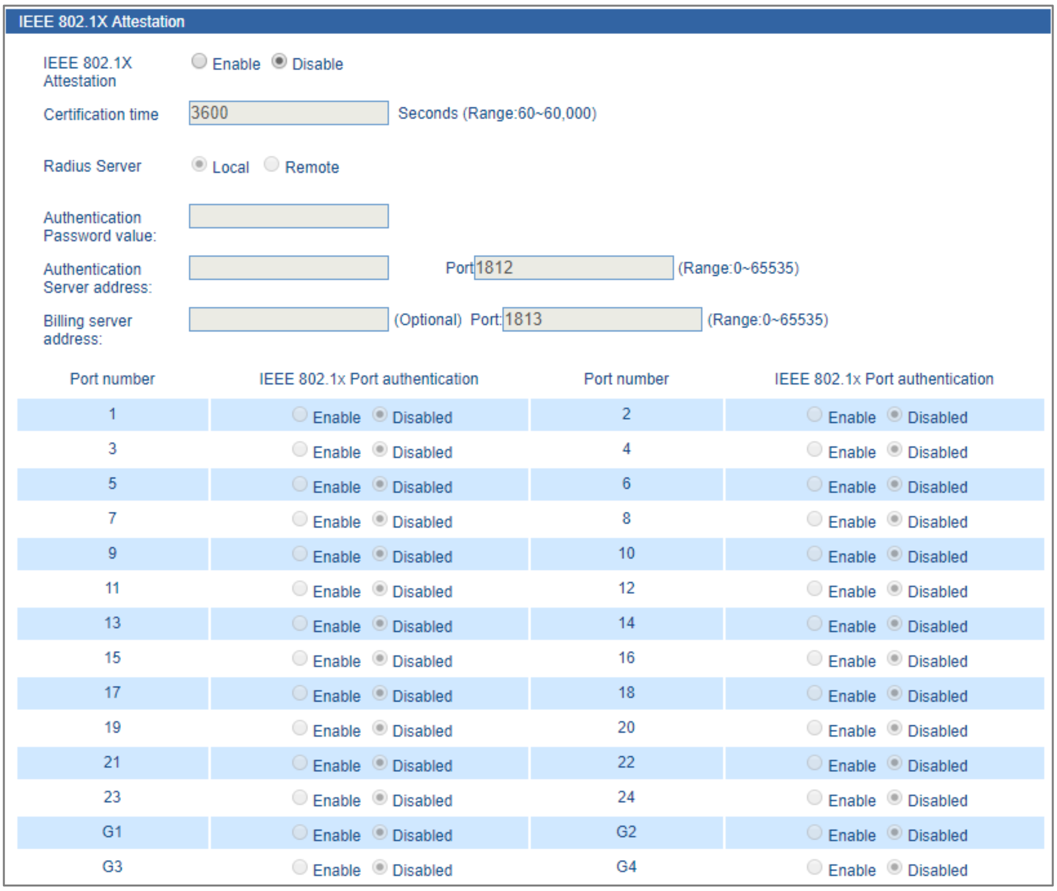
User can configure 802.1X authentication and Radius server parameter on the port authentication page.

Operation Path

Open in order: “Main Menu > Access Control > Port Authentication”.

Interface Description

The port authentication 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
1	○ Enable ● Disabled	2	○ Enable ● Disabled
3	○ Enable ● Disabled	4	○ Enable ● Disabled
5	○ Enable ● Disabled	6	○ Enable ● Disabled
7	○ Enable ● Disabled	8	○ Enable ● Disabled
9	○ Enable ● Disabled	10	○ Enable ● Disabled
11	○ Enable ● Disabled	12	○ Enable ● Disabled
13	○ Enable ● Disabled	14	○ Enable ● Disabled
15	○ Enable ● Disabled	16	○ Enable ● Disabled
17	○ Enable ● Disabled	18	○ Enable ● Disabled
19	○ Enable ● Disabled	20	○ Enable ● Disabled
21	○ Enable ● Disabled	22	○ Enable ● Disabled
23	○ Enable ● Disabled	24	○ Enable ● Disabled
G1	○ Enable ● Disabled	G2	○ Enable ● Disabled
G3	○ Enable ● Disabled	G4	○ Enable ● Disabled

The main element configuration description of global configuration interface.

Interface Element	Description
802.1X auth Config	**802.1X authentication configuration column**
802.1X authentication	802.1X authentication state setting: • Enable; • Disable.
Certification time	Interval range of authentication update is 60~60000, unit is second. The re-authentication period of 802.1x is used for enhancing the security of authentication.
Radius server	Configuration of local Radius server and remote Radius

Interface Element	Description
	server: • Local: built-in Radius server in the device. If choosing local Radius server, applicant will only use the username and password of internal Raduis database. • Remote: if using external Radius server, the IP address, port number and authentication shared password of the authentication server must be filled in.
Authentication password value	Used for device to access the shared password string of Radius server.
Authentication server address	IP address of Radius server.
Port number	Port of Radius server, default to 1812, value range is 1-65535.
Billing server address	Reserved
(optional) port number	Reserved
IEEE 802.1x port authentication	IEEE802.1X authentication status settings of each port: • Enable; • Disable.

8.4 Authentication Database

Function Description

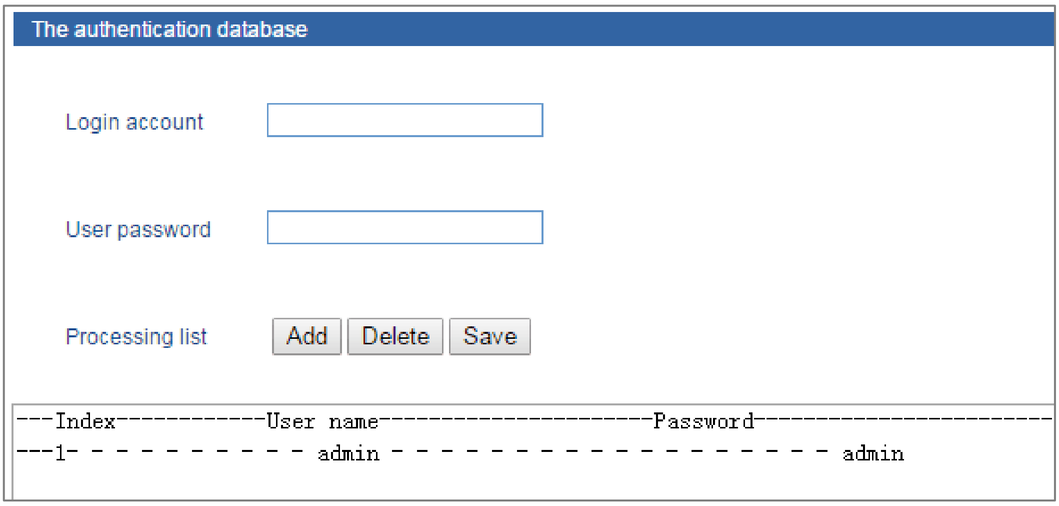
On the “Authentication Database” page, user can set the username and password for 802.1Q local authentication, and adding, deleting and saving user etc.

Operation Path

Open in order: “Main Menu > Access Control > Authentication Database”.

Interface Description

The authentication database interface is as follows:



Login account

User password

Processing list

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

The main element configuration description of authentication database interface.

Interface Element	Description
Login	Username of logging in local authentication
Password	User password for logging in local authentication
Processing list	Add, delete and save the configuration of authentication data

8.5 MAC Port Lock

Physical MAC (Media Access Control) address has identified a terminal on the Internet, and the address is the global unique hardware address.

Function Description

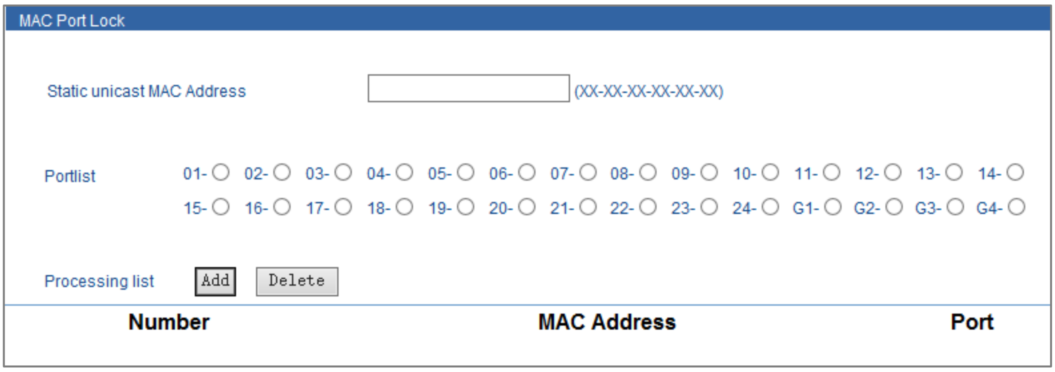
On the “MAC Port Lock” page, user can lock the MAC address of the port that connected to the device.

Operation Path

Open in order: “Main Menu > Access Control > MAC Port Lock”.

Interface Description

MAC port lock interface as follows:



MAC Port Lock

Static unicast MAC Address (XX-XX-XX-XX-XX-XX)

Portlist 01-○ 02-○ 03-○ 04-○ 05-○ 06-○ 07-○ 08-○ 09-○ 10-○ 11-○ 12-○ 13-○ 14-○
15-○ 16-○ 17-○ 18-○ 19-○ 20-○ 21-○ 22-○ 23-○ 24-○ G1-○ G2-○ G3-○ G4-○

Processing list

Number	MAC Address	Port

The main element configuration description of MAC port lock interface:

Interface Element	Description
Static unicast MAC address	The MAC address of the device that needs to be locked.
Port list	Display the corresponding ports of the device.
Processing list	Display the MAC address information of the locked ports.

Note

- Once it was added, the static address will remain in effect and be free from the limitation of maximum aging time until it is deleted.
- One MAC address corresponds to one port in static address table. If set, all data that send to this address will be forwarded to this port only.

8.6 Safety management

8.6.1MAC Filter

Function Description

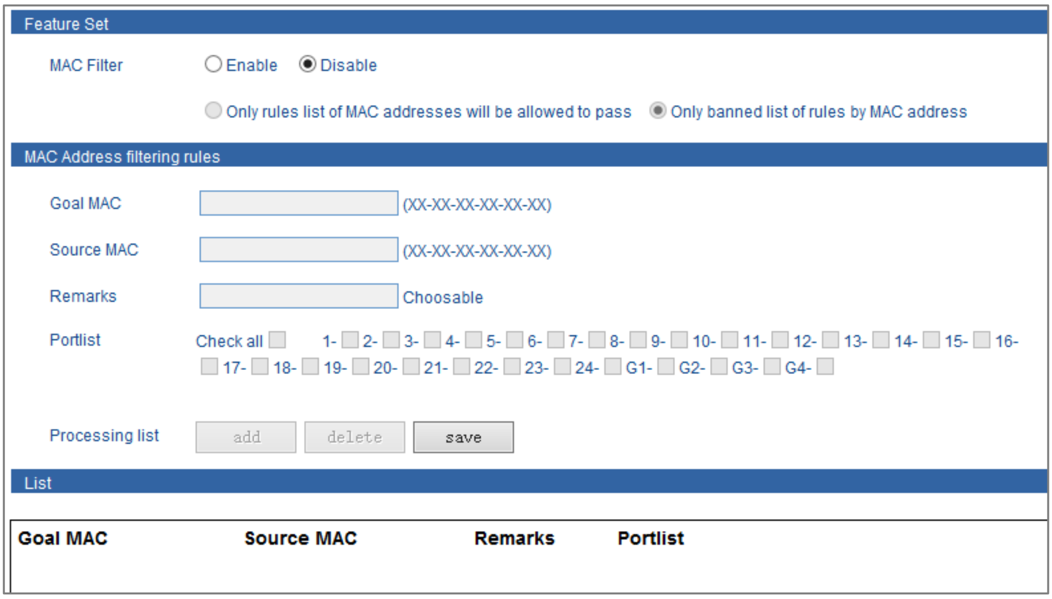
On the “MAC filter” page, user can control the receiving/sending data authority of the host connected to the switch port by setting the list of MAC address rules that enables or disables access.

Operation Path

Open in order: “Main Menu > Safety Management > MAC Filter”.

Interface Description

MAC filter interface as follows:



Feature Set

MAC Filter ○ Enable ● Disable

○ Only rules list of MAC addresses will be allowed to pass ● Only banned list of rules by MAC address

MAC Address filtering rules

Goal MAC (XX-XX-XX-XX-XX-XX)

Source MAC (XX-XX-XX-XX-XX-XX)

Remarks Choosable

Portlist Check all □ 1- □ 2- □ 3- □ 4- □ 5- □ 6- □ 7- □ 8- □ 9- □ 10- □ 11- □ 12- □ 13- □ 14- □ 15- □ 16-
□ 17- □ 18- □ 19- □ 20- □ 21- □ 22- □ 23- □ 24- □ G1- □ G2- □ G3- □ G4- □

Processing list

List

Goal MAC	Source MAC	Remarks	Portlist

The main element configuration description of MAC filter interface:

Interface Element	Description
Feature set	**Function setting area**
MAC filter	Enable or disable MAC address filtering. When the function is enabled, options are as follows: ● Only enable the MAC addresses in the list of rules to pass ● Only disable the MAC addresses in the list of rules to pass
MAC address filtering rules	**Configuration bar of MAC address filtering rules**
Destination MAC	Set the destination MAC address rules of MAC filtering: ● When the list of rules is enabled, the data that takes this address as destination MAC address could be sent ● When the list of rules is disabled, the data that takes this address as destination MAC address couldn’t be sent

Sourse MAC	Set the sourse MAC address rules of MAC filtering: ● When the list of rules is enabled, the data that takes this address as sourse MAC address could be sent ● When the list of rules is disabled, the data that takes this address as sourse MAC address couldn't be sent
Remarks	Add the remark information of the list of rules
Port list	Check the box of ports that apply to MAC filtering rules
Processing list	Set the processing scheme of rules: ● Add entry ● Delect entry ● Save configuration
List of rules	Display the list of rules that have been set up

8.6.2 IP Filter

Function Description

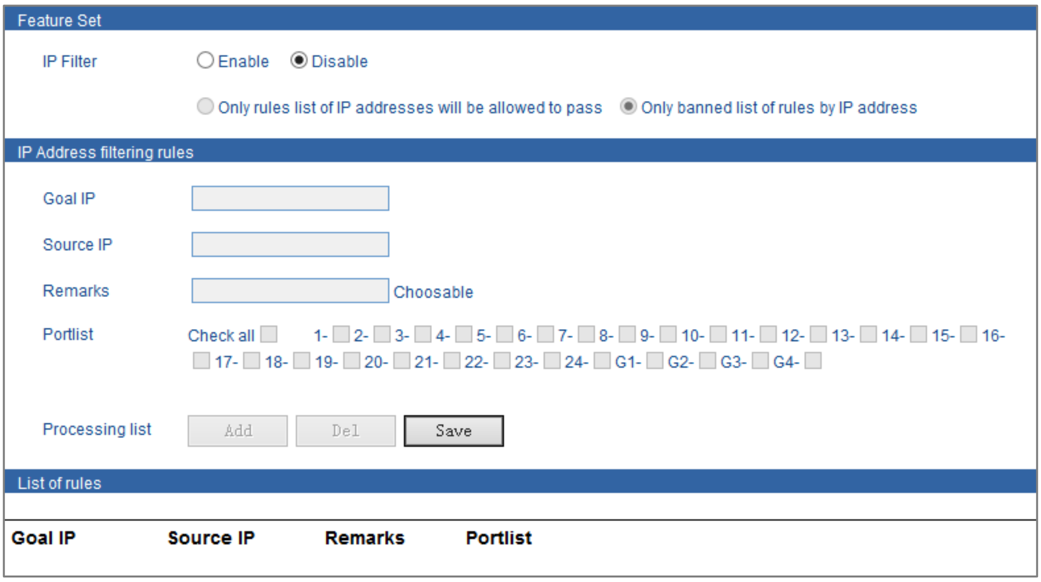
On the "IP filter" page, user can control the receiving/sending data authority of the host connected to the switch port by setting the list of IP address rules that enables or disables access.

Operation Path

Open in order: "Main Menu > Safety Management > IP Filter".

Interface Description

IP filter interface as follows:



Feature Set

IP Filter ○ Enable ● Disable

○ Only rules list of IP addresses will be allowed to pass ● Only banned list of rules by IP address

IP Address filtering rules

Goal IP

Source IP

Remarks Choosable

Portlist Check all □ 1- □ 2- □ 3- □ 4- □ 5- □ 6- □ 7- □ 8- □ 9- □ 10- □ 11- □ 12- □ 13- □ 14- □ 15- □ 16- □ 17- □ 18- □ 19- □ 20- □ 21- □ 22- □ 23- □ 24- □ G1- □ G2- □ G3- □ G4- □

Processing list Add Del Save

List of rules

Goal IP	Source IP	Remarks	Portlist

The main element configuration description of IP filter interface:

Interface Element	Description
Feature set	**Function setting area**
IP filter	Enable or disable IP address filtering. When the function is enabled, options are as follows: • Only enable the IP addresses in the list of rules to pass • Only disable the IP addresses in the list of rules to pass
IP address filtering rules	**The configuration bar of IP address filtering rules**
Destination IP	Set the destination IP address rules of IP filtering: • When the list of rules is enabled, the data that takes this address as destination IP address could be sent • When the list of rules is disabled, the data that takes this address as destination IP address couldn’t be sent
Sourse IP	Set the sourse IP address rules of IP filtering: • When the list of rules is enabled, the data that takes this address as sourse IP address could be sent • When the list of rules is disabled, the data that takes this address as sourse IP address couldn’t be sent
Remarks	Add the remark information of the list of rules
Port list	Check the box of ports that apply to IP filtering rules

Processing list	Set the processing scheme of rules: ● Add entry ● Delect entry ● Save configuration
List of rules	Display the list of rules that have been set up

9 Remote Monitoring

9.1 BlueEyes Configuration

Function Description

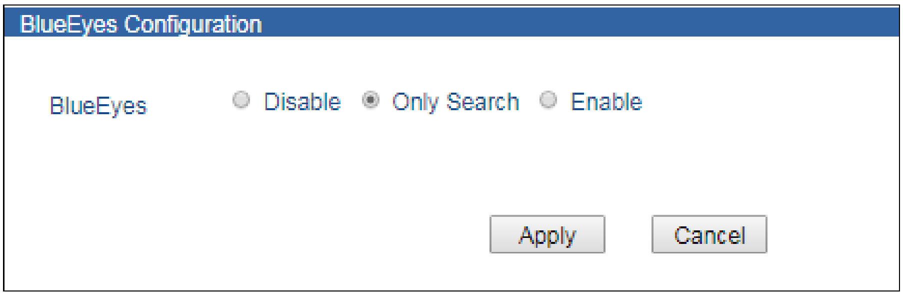
On the page of “BlueEyes Configration”, user can set the authority of BlueEyes tool to access this switch.

Operation Path

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

Interface Description

Interface screenshot of BlueEyes Configuration:



BlueEyes Configuration

BlueEyes ○ Disable ● Only Search ○ Enable

Main elements configuration description of BlueEyes configuration interface:

Interface Element	Description
BlueEyes	Check the authority of BlueEyes tool to access this switch: • Disable: BlueEyes tool cannot search this switch; • Only Search: BlueEyes can only search this switch but it cannot conduct parameter configuration; • Enable: BlueEyes tool can not only search this switch, but also conduct parameter configuration.

9.2 SNMP Configuration

Function Description

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

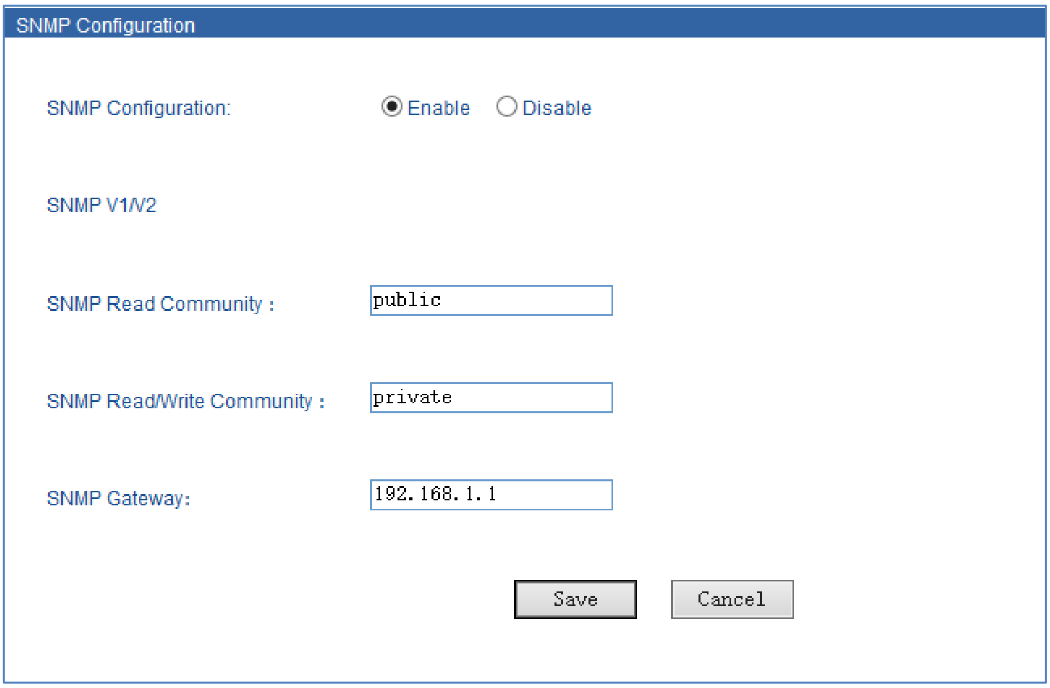
- Enable or disable SNMP configuration function;
- Configure SNMP V1/V2 read-only community name;
- Configure SNMP V1/V2 read-write community name;
- Configure SNMP Trap.

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

SNMP Read Community : public

SNMP Read/Write Community : private

SNMP Gateway: 192.168.1.1

Main elements configuration description of SNMP configuration interface:

Interface Element	Description
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 exists security issue. - SNMP V2: 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 Gateway	The destination IP address sent out by Trap messages.

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.

Example: SNMP Configuration

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

Operation Steps

Step 1 Log on to the 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. Select "SNMP gateway" as "192.168.1.1".

Step 4 Click "Apply".

Step 5 End.

9.3 E-mail Alarm

Function Description

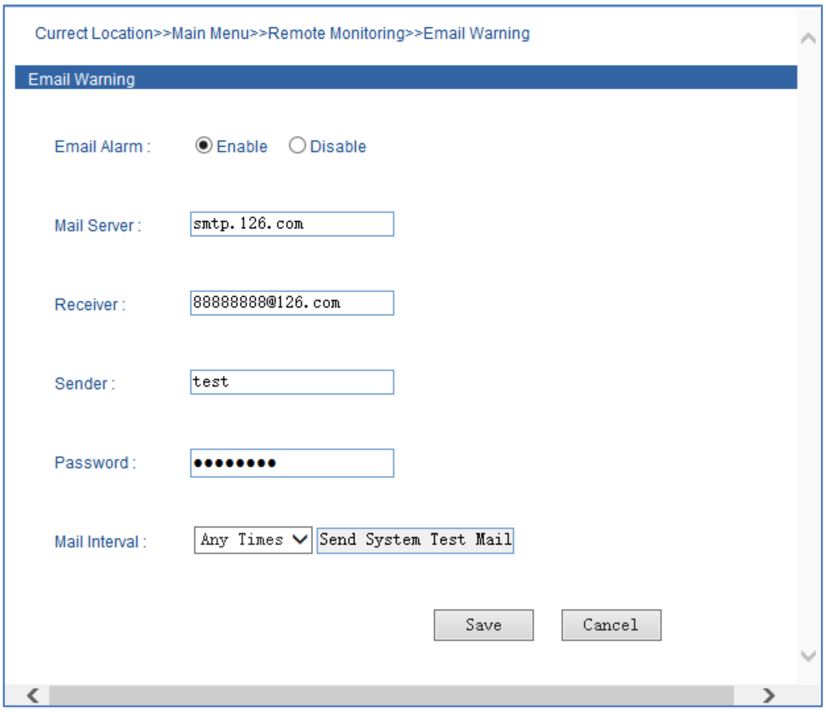
On the page of "E-mail Warning", user can enable remote alarm.

Operation Path

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

Interface Description

Interface screenshot of E-mail alarm configuration as follows:



Currect Location>>Main Menu>>Remote Monitoring>>Email Warning

Email Warning

Email Alarm : ● Enable ○ Disable

Mail Server : smtp.126.com

Receiver : 88888888@126.com

Sender : test

Password : ••••••••

Mail Interval : Any Times

Main elements configuration description of E-mail alarm configuration interface:

Interface Element	Description
E-mail Alarm	Enable/disable E-mail alarm.
Mail Server	Server address of used E-mail should be filled according to the account of used E-mail address. The host IP address or used host name that provides E-mail delivery service for the device.
Receiver	E-mail address used by abnormal event receiver.
Sender	E-mail address of sender, account name used for logging in to the E-mail server.
Password	E-mail password of sender, corresponding password used for logging in to the E-mail account.
Mail Interval	Interval time of sending E-mail.

Notice

While using E-mail alarm, user must ensure that the switch is connected to network normally and the gateway of switch is same to the one of LAN.

9.4 Relay Warning

Function Description

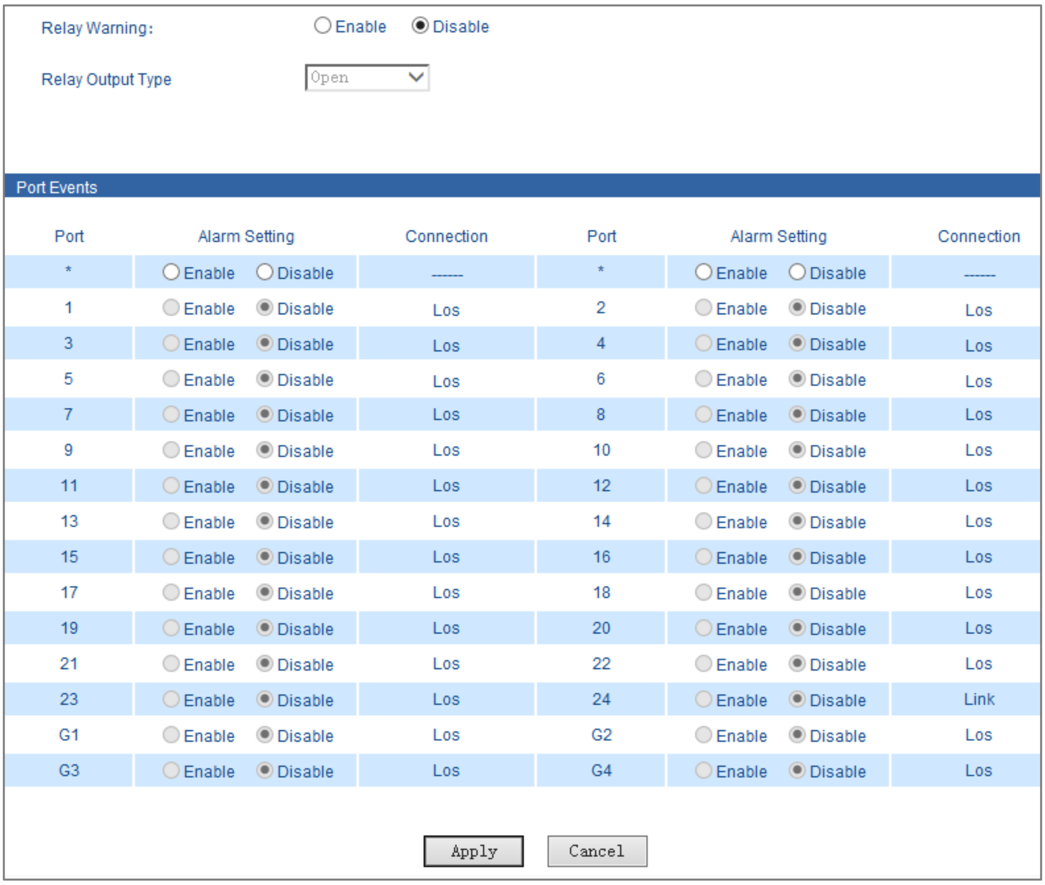
On the page of "Relay Warning", user can set power supply alarm, port alarm function; when the equipment is in abnormal state, it can promptly notify the administrator, and quickly repair the equipment status to avoid excessive losses.

Operation Path

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

Interface Description

Relay warning interface as follows:



Relay Warning: ○ Enable ● Disable

Relay Output Type: Open

Port Events

Port	Alarm Setting	Connection	Port	Alarm Setting	Connection
*	○ Enable ○ Disable	------	*	○ Enable ○ Disable	------
1	○ Enable ● Disable	Los	2	○ Enable ● Disable	Los
3	○ Enable ● Disable	Los	4	○ Enable ● Disable	Los
5	○ Enable ● Disable	Los	6	○ Enable ● Disable	Los
7	○ Enable ● Disable	Los	8	○ Enable ● Disable	Los
9	○ Enable ● Disable	Los	10	○ Enable ● Disable	Los
11	○ Enable ● Disable	Los	12	○ Enable ● Disable	Los
13	○ Enable ● Disable	Los	14	○ Enable ● Disable	Los
15	○ Enable ● Disable	Los	16	○ Enable ● Disable	Los
17	○ Enable ● Disable	Los	18	○ Enable ● Disable	Los
19	○ Enable ● Disable	Los	20	○ Enable ● Disable	Los
21	○ Enable ● Disable	Los	22	○ Enable ● Disable	Los
23	○ Enable ● Disable	Los	24	○ Enable ● Disable	Link
G1	○ Enable ● Disable	Los	G2	○ Enable ● Disable	Los
G3	○ Enable ● Disable	Los	G4	○ Enable ● Disable	Los

Main elements configuration description of relay warning interface:

Interface Element	Description
System Events	Configure alarm settings. Options as follows: ● Enable; ● Disable.
Relay Output Type	Click the drop-down list of "Relay Output Type", options as follows: ● Normally open: when it's normal without alarm, relay is in closed status; when alarm occurs, relay is in open status; ● Normally closed: when it's normal without alarm, relay is in open status; when alarm occurs, relay is in closed status.
Port Events	**Port events column**
Port	Display the device port number.
Alarm Setting	Configure the port alarm function. Options as follows: ● Enable; ● Disable. Note After enabling port alarm, when port is in abnormal status, such as connection or disconnection, the device will output a signal to hint the abnormal operation of device.
Connection	Display port connection status of the device: ● Unconnected; ● Connected.

Example: Alarm Configuration

For example: Enable alarm configuration, and alarm port is port 1.

Operation Steps

Step 1 Log on to the 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 "Port Events", select "Enable" the "Alarm Setting" of power 1.

Step 5 Click "Apply".

Step 6 End.

10 Port Statistics

10.1 Received Frames Statistics

Function Description

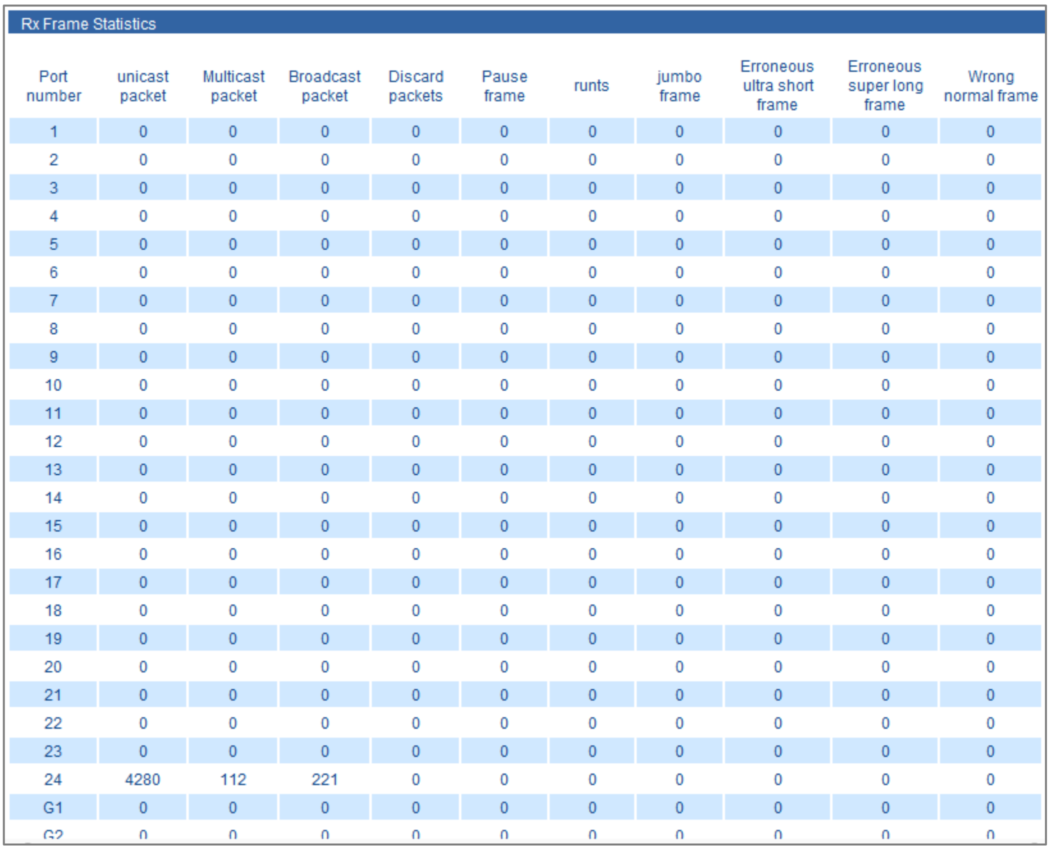
On the page of “Rx Frame Statistics”, user can check frame statistics of data packets received by the port within a period of time.

Operation Path

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

Interface Description

Received frames statistics interface as follows:



Rx Frame Statistics

Port number	unicast packet	Multicast packet	Broadcast packet	Discard packets	Pause frame	runts	jumbo frame	Erroneous ultra short frame	Erroneous super long frame	Wrong normal frame
1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0
24	4280	112	221	0	0	0	0	0	0	0
G1	0	0	0	0	0	0	0	0	0	0
G2	0	0	0	0	0	0	0	0	0	0

Main elements configuration description of received frames statistics interface:

Interface Elements	Description
Unicast	Number of port received data packets whose address is unicast address.
Multicast	Number of port received data packets whose address is multicast address.
Broadcast	Number of port received data packets whose address is broadcast address.
Drop	Number of port received data packets which are normal but dropped due to security control.
Pause	Port received Ethernet control frames with the protocol of 0x8808, under the status of full duplex; the data packet is used for controlling the frequency of port data sending.
UnderSize	Number of port received data packets whose length is less than 64 bytes, including the length of FCS.
OverSize	Number of port received data packets whose length is more

Interface Elements	Description
	than 1518 or 1522 (enable VLAN) bytes, including the length of FCS.
Fragments	Number of port received data packets whose length is less than 64 bytes, including the length of FCS.
Jabber	Number of port received data packets whose length is more than 1522 bytes, including the incorrect or deficient FCS.
SysbolErr	Number of port received data packets whose length is between 64 and 1518 or 1522 (enable VLAN) bytes, including the incorrect, deficient or invalid FCS.
Clear	Clear the counting of statistics frames.

10.2 Transmitted Frame Statistics

Function Description

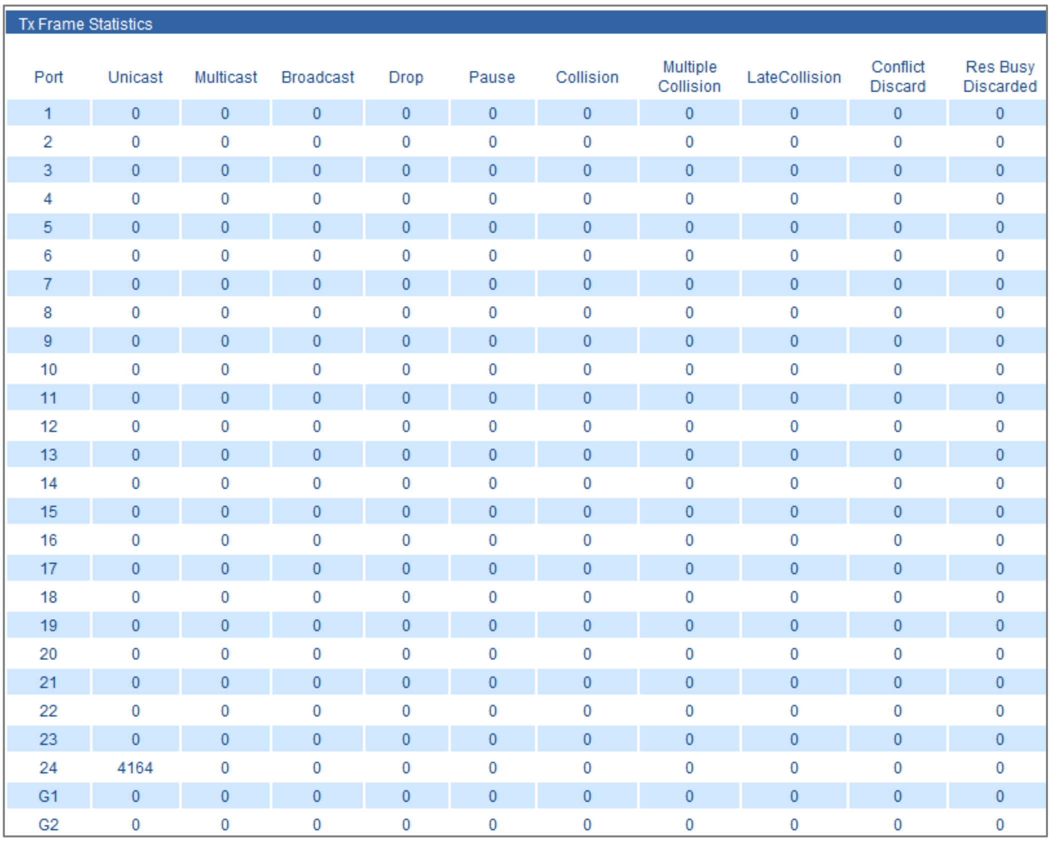
On the page of “Tx Frame Statistics”, user can check frame statistics of data packets transmitted by the port within a period of time.

Operation Path

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

Interface Description

Transmitted frames statistics interface as follows:



Tx Frame Statistics

Port	Unicast	Multicast	Broadcast	Drop	Pause	Collision	Multiple Collision	LateCollision	Conflict Discard	Res Busy Discarded
1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0
24	4164	0	0	0	0	0	0	0	0	0
G1	0	0	0	0	0	0	0	0	0	0
G2	0	0	0	0	0	0	0	0	0	0

Main elements configuration description of transmitted frames statistics interface:

Interface Element	Description
Unicast	Number of port transmitted data packets whose address is unicast address.
Multicast	Number of port transmitted data packets whose address is multicast address.
Broadcast	Number of port transmitted data packets whose address is broadcast address.
Drop	Number of port transmitted data packets which are normal but dropped due to insufficient resources or no internal condition for analysis (excluding data packets that are dropped due to collision).
Pause	Port received Ethernet control frames with the protocol of 0x8808, under full duplex status; the data packet is used for controlling the frequency of port data transmission.
Collision	Collision frequency during port data transmission.

Interface Element	Description
Multiple Collision	Number of successfully transmitted data packets with the collision frequency more than 1 during port data transmission.
LateCollision	Number of data packets with the detected collision during transmitting the data packets less than 64 bytes.
Res Busy Discarded	Number of data packets (Abundant data packets with low priority after enabling QoS) discarded due to deficient resources in the pop queue.
Clear	Clear the counting of statistics frames.

10.3 Total Flow Statistic

Function Description

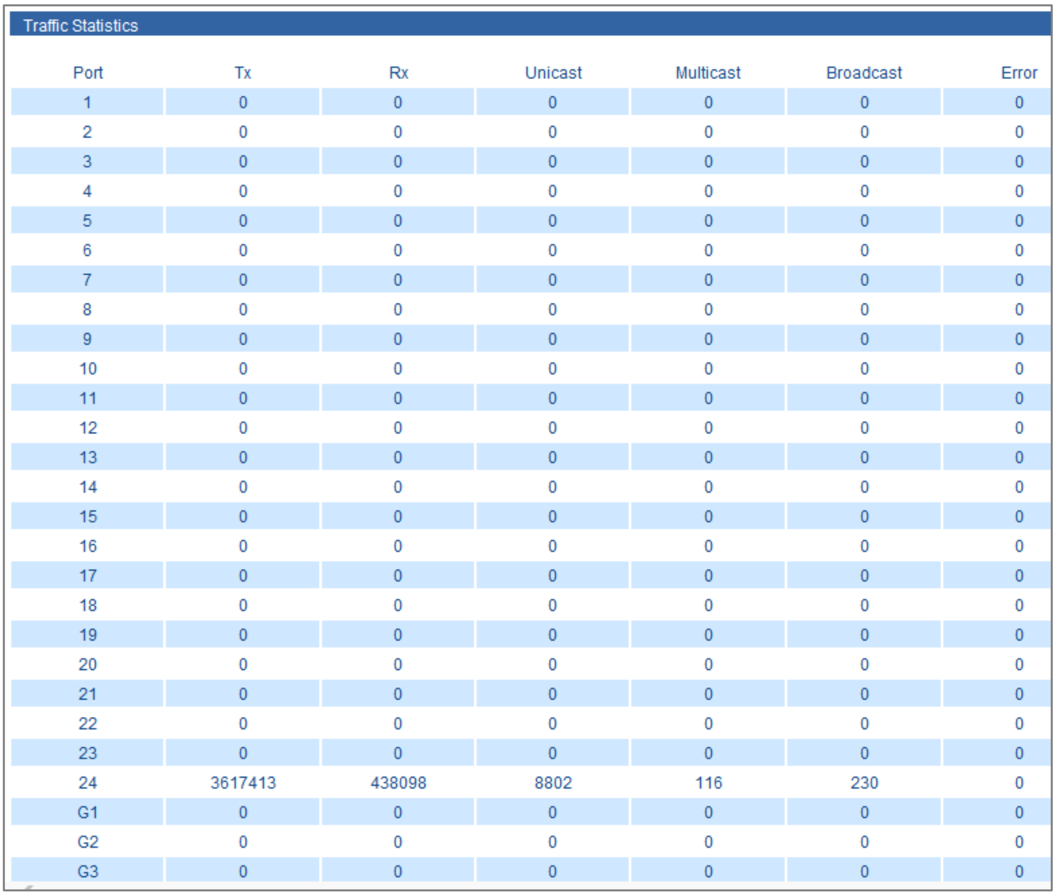
On the page of “Total Flow Statistic”, user can query the frame number of the total port data packet in a certain time.

Operation Path

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

Interface Description

Total flow statistic interface as below:



Traffic Statistics

Port	Tx	Rx	Unicast	Multicast	Broadcast	Error
1	0	0	0	0	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0
11	0	0	0	0	0	0
12	0	0	0	0	0	0
13	0	0	0	0	0	0
14	0	0	0	0	0	0
15	0	0	0	0	0	0
16	0	0	0	0	0	0
17	0	0	0	0	0	0
18	0	0	0	0	0	0
19	0	0	0	0	0	0
20	0	0	0	0	0	0
21	0	0	0	0	0	0
22	0	0	0	0	0	0
23	0	0	0	0	0	0
24	3617413	438098	8802	116	230	0
G1	0	0	0	0	0	0
G2	0	0	0	0	0	0
G3	0	0	0	0	0	0

The main element configuration description of total flow statistic interface:

Interface Element	Description
Tx	The total bytes of all data packets sent by the port.
Rx	The total bytes of all data packets received by the port.
Unicast	The number of data packets with unicast address as its port sending and receiving address.
Multicast	The number of data packets with multicast address as its port sending and receiving address.
Broadcast	The number of data packets with broadcast address as its port sending and receiving address.
Error	The number of data packets with error caused by various reasons in port sending and receiving address.
Reset	Reset the number of statistic frame.

10.4 MAC Address Table

Function Description

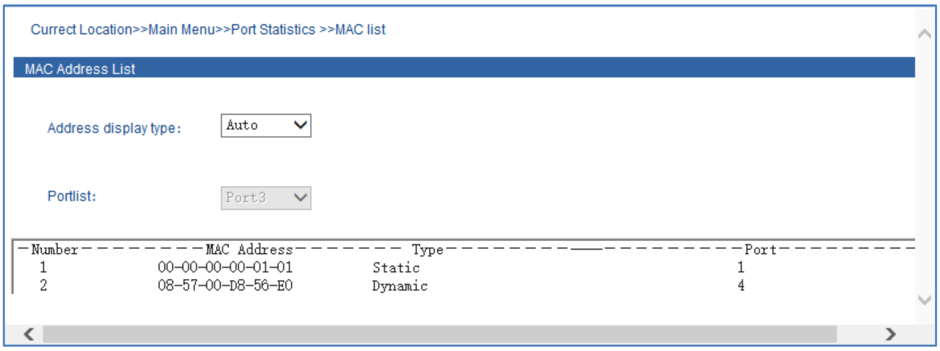
On the page of “MAC Address List”, user can check the port’s MAC address table information within a period of time.

Operation Path

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

Interface Description

Interface screenshot of MAC address table as follows:



Currect Location>>Main Menu>>Port Statistics >>MAC list

MAC Address List

Address display type: Auto

Portlist: Port3

```
—Number— — — — — — — — —MAC Address— — — — — — — Type— — — — — — — — — — — — — — — — — — —Port— — — — — — — — —
  1            00-00-00-00-01-01         Static                                          1
  2            08-57-00-D8-56-E0         Dynamic                                         4
```

Main elements configuration description of MAC address table interface:

Interface Element	Description
Address display type	MAC address type: • Port: display MAC address information of the designated port. • Auto: automatically display MAC address information of all ports.
Port list	When the address display type is port, user can select designated port number via drop-down list to check MAC address information.
Number	Total number of bytes of all data packets received by the port.

Note

- Permanent static address is configured in the port list of static MAC address, corresponding table items need to be modified when the port changes.
- Multicast address table is displayed in the items of IGMP snooping table, this address table items are all unicast addresses.
- The ageing time of MAC address is 300 seconds, the device system will eliminate all relative port list when the port is disconnected and MAC address surpasses the ageing time.

11 Network Diagnosis

11.1 Port Mirror

Port mirror refers to duplicate the packets from the appointed port (source port or mirror port) to another appointed port (destination port or collection port). In the process of network operation and maintenance, for the purpose of business monitoring and fault location, the network administrator analyzes the packets duplicated from the observed port via the network monitoring device and judges whether the business operated in the Internet is normal.

Function Description

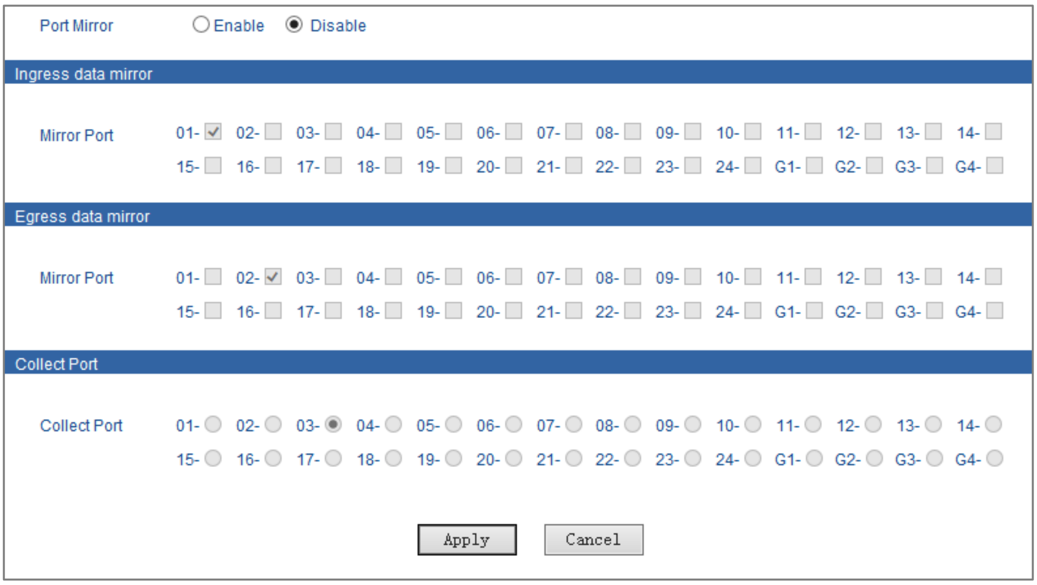
On the “Port Mirror” page, user can enable or configure the correspondence between ingress data mirror and egress data mirror.

Operation Path

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

Interface Description

Port mirror interface as follows:



Port Mirror ○ Enable ● Disable

Ingress data mirror

Mirror Port 01-☑ 02-□ 03-□ 04-□ 05-□ 06-□ 07-□ 08-□ 09-□ 10-□ 11-□ 12-□ 13-□ 14-□
15-□ 16-□ 17-□ 18-□ 19-□ 20-□ 21-□ 22-□ 23-□ 24-□ G1-□ G2-□ G3-□ G4-□

Egress data mirror

Mirror Port 01-□ 02-☑ 03-□ 04-□ 05-□ 06-□ 07-□ 08-□ 09-□ 10-□ 11-□ 12-□ 13-□ 14-□
15-□ 16-□ 17-□ 18-□ 19-□ 20-□ 21-□ 22-□ 23-□ 24-□ G1-□ G2-□ G3-□ G4-□

Collect Port

Collect Port 01-○ 02-○ 03-● 04-○ 05-○ 06-○ 07-○ 08-○ 09-○ 10-○ 11-○ 12-○ 13-○ 14-○
15-○ 16-○ 17-○ 18-○ 19-○ 20-○ 21-○ 22-○ 23-○ 24-○ G1-○ G2-○ G3-○ G4-○

The main element configuration description of port mirror interface:

Interface Element	Description
Port Mirror	Setting port mirror function, options are: • Enable; • Disable.
Ingress data mirror	**Configuration column of ingress data mirror.**
Mirror Port	Select the ingress data port that needs mirroring.
Egress data mirror	**Configuration column of egress data mirror.**
Mirror port	Choose the egress data port that needs mirroring.
Collect port	**Configuration column of collect port.**
Collect port	Configure the collect port after ingress/egress data mirror.

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 in to 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.

11.2 Network Diagnosis

Function Description

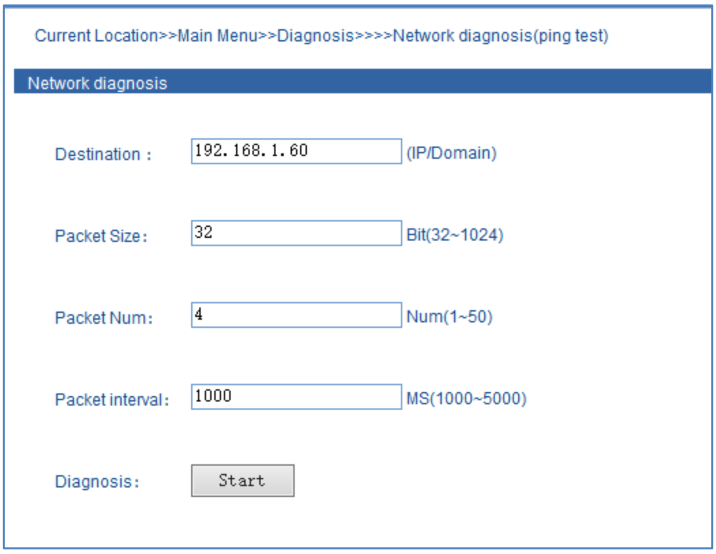
On the page of "Network diagnosis", user can use Ping test to Ping the IP or domain name of the opposite terminal, checking whether the network is connected.

Operation Path

Open in order: "Main Menu > Diagnosis > Network diagnosis (ping test)"

Interface Description

Network diagnosis interface screenshot as follows:



Current Location>>Main Menu>>Diagnosis>>>>Network diagnosis(ping test)

Network diagnosis

Destination : 192.168.1.60 (IP/Domain)

Packet Size: 32 Bit(32~1024)

Packet Num: 4 Num(1~50)

Packet interval: 1000 MS(1000~5000)

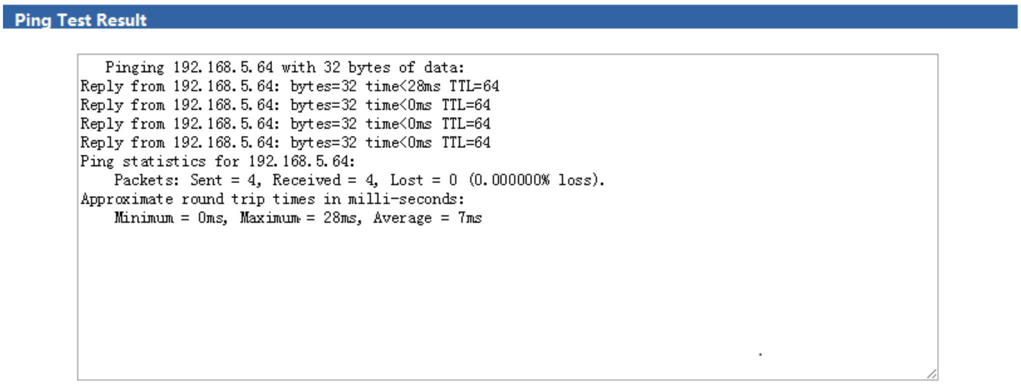
Diagnosis: Start

Main elements configuration description of network diagnosis interface:

Interface Element	Description
Destination	IP address or domain name of devices whose connectivity needs to be tested.
Packet Size	The packet size of Ping command is 32~1024 bytes.

Packet Num	Sending packets quantity of Ping command.
Packet interval	Packets transmission interval of Ping command.
Diagnosis	After filling in the destination, packet size, packet number and packet interval, user can click "Start" to initiate test.

Screenshot of Ping test result as follows:



```
   Pinging 192.168.5.64 with 32 bytes of data:
Reply from 192.168.5.64: bytes=32 time<28ms TTL=64
Reply from 192.168.5.64: bytes=32 time<0ms TTL=64
Reply from 192.168.5.64: bytes=32 time<0ms TTL=64
Reply from 192.168.5.64: bytes=32 time<0ms TTL=64
Ping statistics for 192.168.5.64:
    Packets: Sent = 4, Received = 4, Lost = 0 (0.000000% loss).
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 28ms, Average = 7ms
```

Main elements configuration description of network diagnosis interface:

Interface Element	Description
Destination	IP address or domain name of devices whose connectivity needs to be tested.
Packet Size	The packet size of Ping command is 32~1024 bytes.
Packet Num	Sending packets quantity of Ping command.
Packet interval	Packets transmission interval of Ping command.
Diagnosis	After filling in the destination, packet size, packet number and packet interval, user can click "Start" to initiate test. Notes: Test results show that no packet drop or time delay represents good network environment between these two devices when the switch sends data to the opposite terminal device.

11.3 SFP DDM Monitor

Function Description

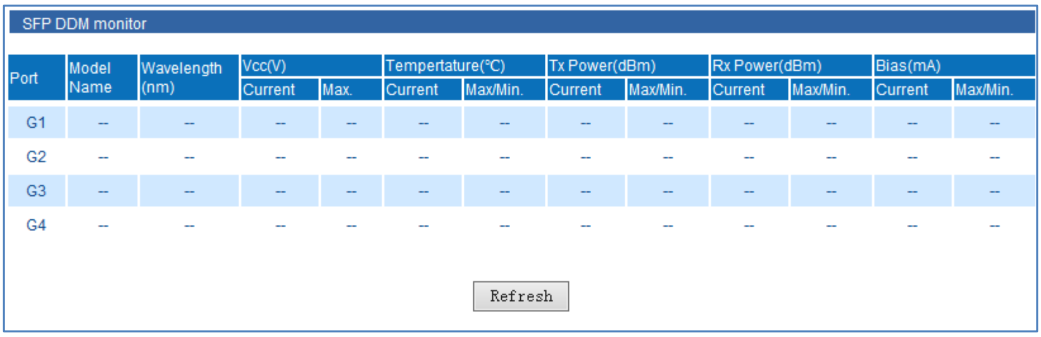
On the "SFP DDM" page, the DDM (Digital Diagnostic Monitor) function is supported. User can monitor SFP parameters in real time, which has greatly facilitated the troubleshooting process of fiber link and lowered the cost of on-site debugging.

Operation Path

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

Interface Description

SFP 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	--	--	--	--	--	--	--	--	--	--	--	--
G2	--	--	--	--	--	--	--	--	--	--	--	--
G3	--	--	--	--	--	--	--	--	--	--	--	--
G4	--	--	--	--	--	--	--	--	--	--	--	--

The main element configuration description of SFP DDM interface:

Interface Element	Description
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	Optical output power, referring to the output power of optical source in the sending end of optical module. The unit is dBm
RX Power	Optical input power, referring to the lowest optical power of receiving in certain rate and bit error rate. The unit is dBm.

Interface Element	Description
Bias	The bias current of laser. Its unit is mA.

12 System Management

12.1 Log Information

Function Description

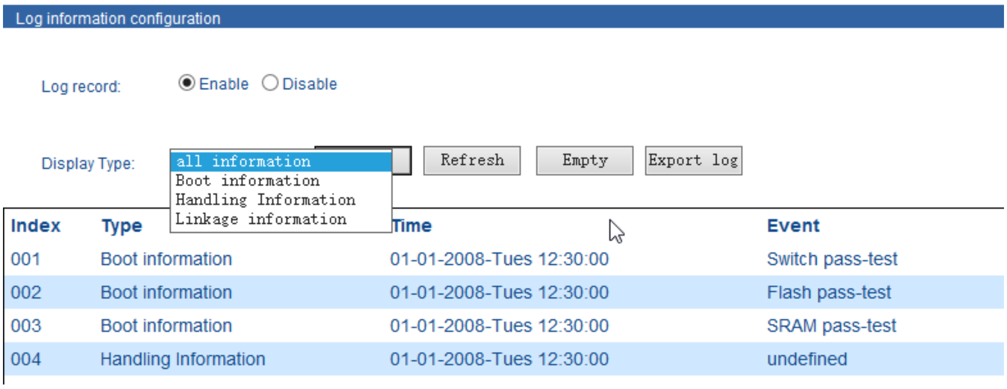
On the page of “Log information”, user can enable log record to check the device status information.

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 information [Refresh] [Empty] [Export log]

Index	Type	Time	Event
001	Boot information	01-01-2008-Tues 12:30:00	Switch pass-test
002	Boot information	01-01-2008-Tues 12:30:00	Flash pass-test
003	Boot information	01-01-2008-Tues 12:30:00	SRAM pass-test
004	Handling Information	01-01-2008-Tues 12:30:00	undefined

Main elements configuration description of log information interface:

Interface Elements	Description
Log record	Enable or disable log record.
Display Type	User can check the device booting, connection and

Interface Elements	Description
	operation information.

12.2 SNTP Configuration

Function Description

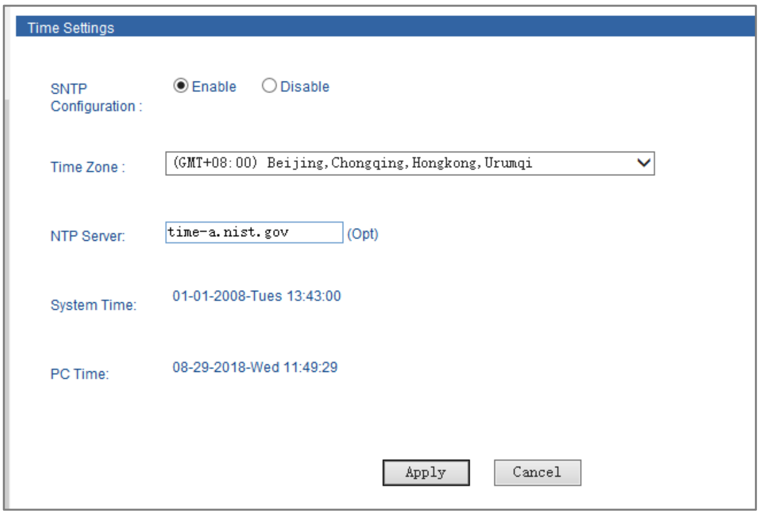
On the page of “Time Configuration”, user can check current PC time or system operation time, and select relative time zone.

Operation Path

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

Interface Description

Time configuration interface as follows:



SNTP Configuration : ● Enable ○ Disable

Time Zone : (GMT+08:00) Beijing,Chongqing,Hongkong,Urumqi

NTP Server: time-a.nist.gov (Opt)

System Time: 01-01-2008-Tues 13:43:00

PC Time: 08-29-2018-Wed 11:49:29

Main elements configuration description of time configuration interface:

Interface Elements	Description
SNTP Configuration	Enable or disable time configuration function.
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	Time of the device itself, after powering on, press

Interface Elements	Description
	"Tuesday, January 1, 2008" to manually or automatically use NTP updating.
PC Time	PC time of the visitor itself, the time display isn't relative to the switch itself.

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 Address

Function Description

On the page of "Network Settings", user can conduct following operations:

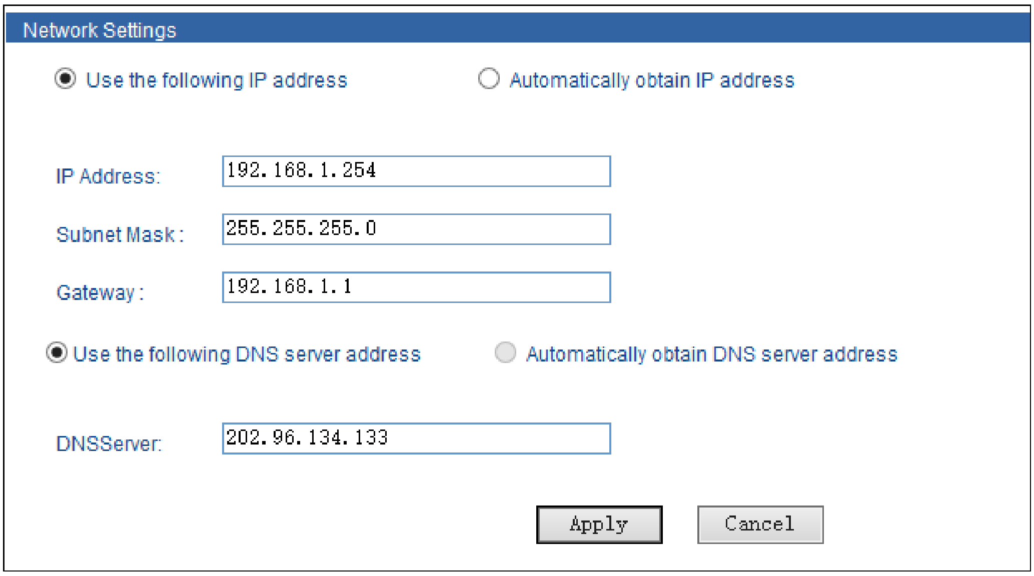
- Configure default IP address of the device;
- Configure netmask;
- Configure gateway address;
- Configure DNS server;
- Reboot the device.

Operation Path

Open in order: "Main Menu > Basic Settings > Network Settings".

Interface Description

Device address interface 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 ○ Automatically obtain DNS server address

DNSServer: 202.96.134.133

Main elements configuration description of device address interface:

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

Interface Elements	Description
Apply	Save the device address information. Notes: Some devices may automatically reboot after configuration, and the configuration will take effect after rebooting.
Cancel	Cancel the modification of device address information.

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 Login to the 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”.

a) Enter “192.168.5.88” in the textbox of “IP Address”.

b) 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 Login to the 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;

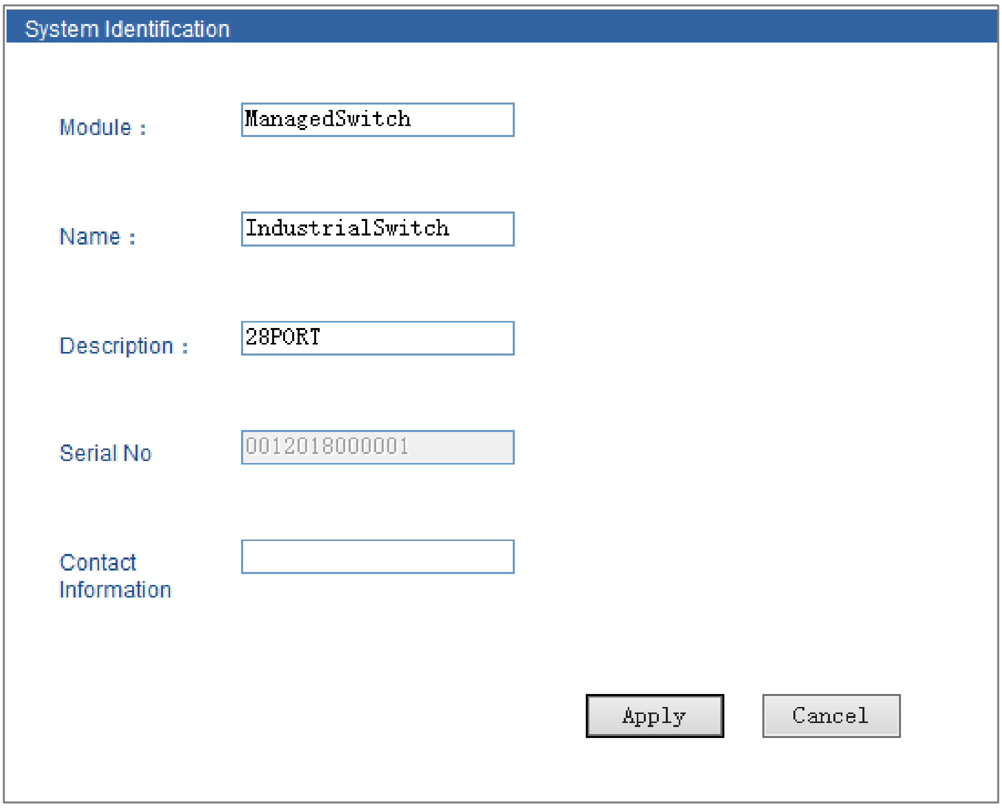
- Device description;
- Device number;
- Contact information.

Operation Path

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

Interface Description

System information interface as follows:



System Identification

Module : ManagedSwitch

Name : IndustrialSwitch

Description : 28PORT

Serial No 0012018000001

Contact Information

Main elements configuration description of system information interface:

Interface Elements	Description
Module	Configure the device model.
Name	Configure the device name to identify each device in the network.
Description	Configure the device summary description.
Serial No.	The serial number of the device, it defaults to gray and can’t be modified
Contact Information	Configure the contact Information of the device maintenance

	personnel. Notes: • 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 “SW-Switch”;
- “Description” is “8ports”.
- “Contact Information” is “0755-26702688”.

Operation Steps

Step 1 Login to the Web configuration interface.

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

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

a) Enter “Module” as “ManagedSwitch1”;

b) Enter “Name” as “SW-Switch”;

c) Enter “Description” as “8ports”.

d) Enter “Serial No.” as “SW001”.

e) Enter “Contact Information” as “0755-26702688”.

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:

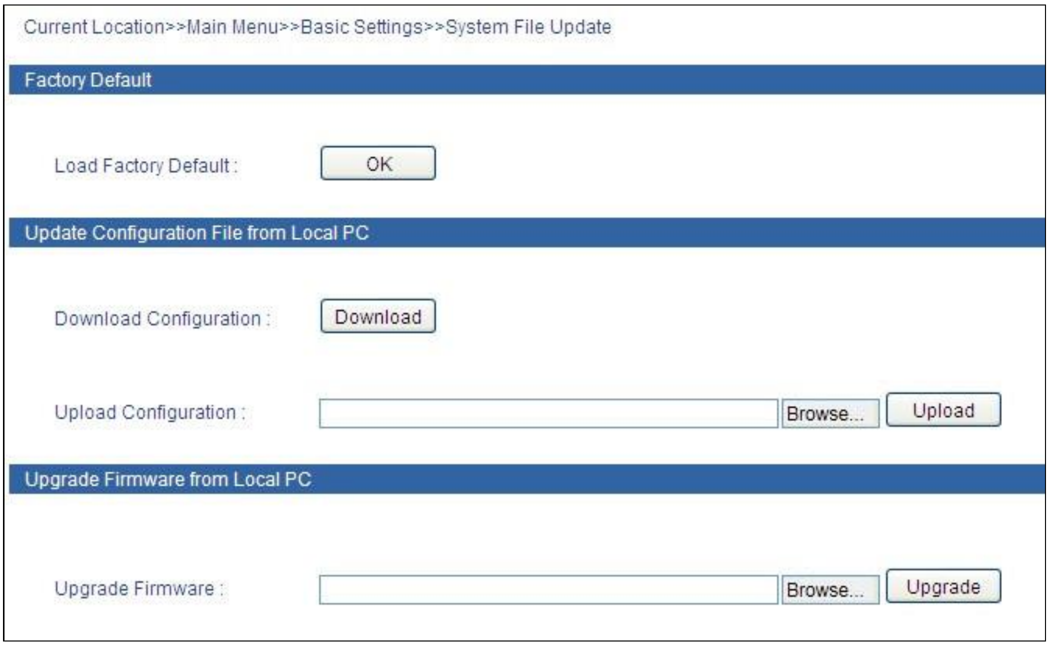
- Restore factory defaults;
- Upload and download configuration files;
- System upgrading.

Operation Path

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

Interface Description

File management interface as follows:



Current Location>>Main Menu>>Basic Settings>>System File Update

Main elements configuration description of file management interface:

Interface Element	Description
Factory Default	**Configuration column of restore factory defaults**
Load Factory Default	Restore factory defaults of the switch. Notes: Restore factory defaults will cause all devices status 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 on to the Web configuration interface.

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

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

Step 4 Click "Save (S)" on the pop-up dialog box of "File Download".

Step 5 Select save path on the pop-up dialog box of "Save as".

Step 6 Click "Apply".

Step 7 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 on to the Web configuration interface.

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

Step 3 On the region of "Update Configuration File from Local PC" 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

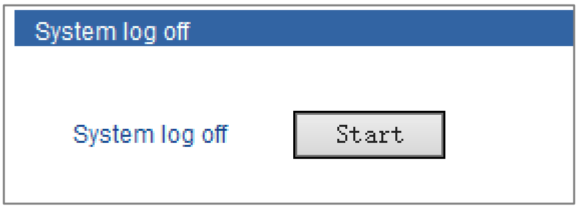
On the page of “System log off”, user can log off the login information of current user.

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 Elements	Description
System log off	Log off the login information of current user.

For example: Log off and change administrator to login

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

Operation Steps

Step 1 Login to the Web configuration interface.

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

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

Step 4 Conduct following operations on the pop-up login dialog box:

1. Enter “admin8” on the option box of “User name”.
2. Enter “admin8” on the option box of “Password”.

Step 5 Click “OK”.

Step 6 Alarm information is displayed on the pop-up dialog box of “messages from the webpage”, click “OK”.

Step 7 Login successfully to the WEB interface.

Step 8 End.

The Second Part: Frequently Asked Questions

13 FAQ

13.1 Sign in Problems

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

   Before access the WEB, please eliminate IE cache buffer and cookies. Otherwise, the webpage will display abnormally.

2. **How about forget the login password?**

   For forgetting the login password, the password can be initialized by restoring factory setting, specific method is adopt BlueEyes_Ⅱ software to search and use restore factory setting function to initialize the password. Both of 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. **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.

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

3. **How to deal with the problem that part of switch ports are impassable?**
   When some ports on the switch are impassable, it may be network cable, network adapter and switch port faults. User can locate the faults via following tests:
   - Connected computer and switch ports keep invariant, change other network cable;
   - Connected network cable and switch port keep invariant, change other computers;
   - Connected network cable and computer keep invariant, 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 Alarm Problem

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

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

13.4 Indicator Problem

1. **Power indicator isn't bright, what's the reason?**

   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 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. **The switch halts after communicate for a period time, and returns to normal after reboot, what's the reason?**

   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.

3onedata

Make network communication more reliable

3onedata Co., Ltd.

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

Technology support: tech-support@3onedata.com

Service hotline: +86-400-880-4496

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