



# 16/24 100M or 16/24 100M + 4 Gigabit Series Layer 2 Managed Industrial Ethernet Switch User Manual

Version 03

Issue Date: 4/13/2020

# Preface

This Switch User Manual has introduced:

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



Note

The manual print screen reference model is 4 Gigabit SFP + 12 100M copper ports + 12 100M fiber ports, 100~240VAC/DC redundant power supply, except the supported Ethernet port and power supply number and type, its interface function and operation is same to other models products.

## Readers






This manual mainly suits for engineers as follows:

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

## Text Format Convention

Format	Description
""	Words with "" represent the interface words. e.g.: "The port number".
>	Multi-level paths are separated by ">". Such as opening the local connection path description: Open "Control Panel> Network Connection> Local Area Connection".
Light Blue Font	It represents the words clicked to achieve hyperlink. The font color is as follows: 'Light Blue'.
About this chapter	The section 'about this chapter' provides links to various sections of this chapter, as well as links to the Principles Operations Section of this chapter.

## Icon Convention

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

## Port Convention

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

## Revision Record

Version NO.	Revision Date	Revision Description
01	2014-05	Product release
02	2016-05	Version upgrade
03	2020-04-13	Software upgrade, layout optimization

# Content

<b>PREFACE.....</b>	<b>1</b>
<b>CONTENT.....</b>	<b>1</b>
<b>1 LOG IN THE WEB INTERFACE.....</b>	<b>1</b>
1.1 WEB BROWSING SYSTEM REQUIREMENTS.....	1
1.2 SET THE IP ADDRESS OF THE COMPUTER.....	1
1.3 LOG IN THE WEB CONFIGURATION INTERFACE.....	2
<b>2 SYSTEM STATUS.....</b>	<b>4</b>
<b>3 PORT CONFIGURATION.....</b>	<b>7</b>
3.1 PORT SETTINGS.....	7
3.2 BANDWIDTH MANAGEMENT.....	10
3.3 STORM SUPPRESSION.....	12
<b>4 LAYER 2 FEATURES.....</b>	<b>15</b>
4.1 VLAN.....	15
4.1.1 Instance: typical VLAN configuration.....	18
4.2 MULTICAST FILTERING.....	21
4.2.1 Multicast Filtering.....	21
4.2.2 Static Multicast Table.....	24
<b>5 QOS.....</b>	<b>26</b>
5.1 QoS CLASSIFICATION.....	26
5.2 CoS MAPPING.....	29
5.3 DSCP Cos MAP QUEUE.....	31
<b>6 LINK BACKUP.....</b>	<b>33</b>
6.1 RAPID RING.....	33
6.1.1 Instance: create single ring.....	39
6.1.2 Instance: create coupling ring.....	40
6.1.3 Instance: creating chain.....	44
6.1.4 Creating Spanning Tree.....	48
6.2 PORT TRUNKING.....	53
<b>7 LLDP.....</b>	<b>56</b>
7.1 PARAMETERS CONFIGURATION.....	56
7.2 NEIGHBOR INFORMATION.....	58
<b>8 ACCESS CONTROL.....</b>	<b>60</b>
8.1 PASSWORD.....	60

8.2 DHCP SERVER.....	62
8.3 MAC PORT LOCK.....	64
8.4 SECURITY MANAGEMENT.....	65
8.4.1 MAC Filter.....	65
8.4.2 IP Address Filtering.....	66
<b>9 REMOTE MONITORING.....</b>	<b>68</b>
9.1 SNMP CONFIGURATION.....	68
9.2 E-MAIL ALARM.....	71
9.3 ALARM SETTINGS.....	73
<b>10 PORT STATISTICS.....</b>	<b>76</b>
10.1 RECEIVED FRAMES STATISTICS.....	76
10.2 TRANSMITTED FRAME STATISTICS.....	78
10.3 TOTAL FLOW STATISTIC.....	80
10.4 MAC ADDRESS TABLE.....	82
<b>11 NETWORK DIAGNOSIS.....</b>	<b>83</b>
11.1 PORT MIRROR.....	83
11.2 NETWORK DIAGNOSIS.....	84
<b>12 SYSTEM MANAGEMENT.....</b>	<b>87</b>
12.1 LOG INFORMATION.....	87
12.2 SNTP CONFIGURATION.....	88
12.3 DEVICE ADDRESS.....	89
12.4 SYSTEM INFORMATION ;.....	92
12.5 FILE MANAGEMENT.....	94
12.6 SYSTEM LOG OFF.....	96
<b>13 FAQ.....</b>	<b>98</b>
13.1 SIGN IN PROBLEMS.....	98
13.2 CONFIGURATION PROBLEM.....	98
13.3 ALARM PROBLEM.....	99
13.4 INDICATOR PROBLEM.....	99

# 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
CPU	Above Pentium 586
Memory	Above 128MB
Resolution	Above 1024x768
Color	256 color or above
Browser	Above Internet Explorer 6.0
Operating System	Windows XP Windows 7 or higher

## 1.2 Set the IP Address of the Computer

The switch default management as follows:

IP Settings	Default Value
IP address	192.168.1.254
Subnet mask.	255.255.255.0

While configuring the switch via Web:

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

Note:

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

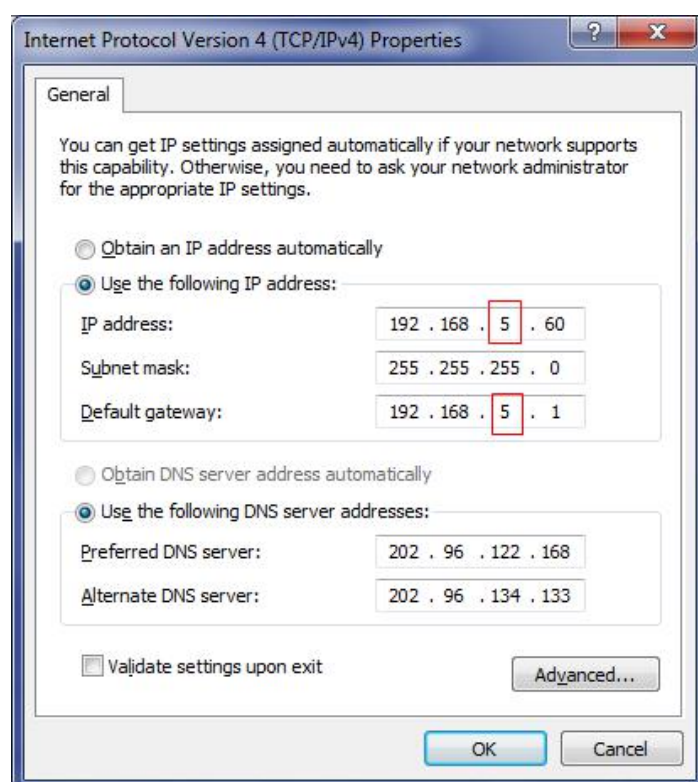
Eg: Assume that the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address to "1".

### Operation Steps

Amendment steps as 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".



**Step 3** Click "OK", IP address is modified successfully.

**Step 4** End.

## 1.3 Log in the Web Configuration Interface

### Operation Steps

Login in the web configuration interface as follow:

**Step 1** Run the computer browser.

**Step 2** On the address bar of browser, enter in the switch address "http://192.168.1.254".

**Step 3** Click the "Enter" key.

**Step 4** Pop up a window as the figure below, enter the user name and password on the login

window.



Note:

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

**Step 5** Click “OK”

**Step 6** End.

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

Note:

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



## 2 System Status

---

### Function Description

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

### Operation Path

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

### Interface Description

Device information interface as follows:

Device Information				
Name	IndustrialSwitch		Hardware Ver	V1.0.0
Module	ManagedSwitch		Firmware Ver	2.1.0 build2019072702R
Description	28PORT		MAC Address	00-22-6F-0D-5C-FD
Serial No	11		Contact Method	
Port Information				
Port number	Connection state	port status	rate	Interface type
1	LOS	FULL	100M	FX
2	LOS	FULL	100M	FX
3	LOS	FULL	100M	FX
4	LOS	FULL	100M	FX
5	LOS	FULL	100M	FX
6	LOS	FULL	100M	FX
7	LOS	FULL	100M	FX
8	LOS	FULL	100M	FX
9	LOS	FULL	100M	FX
10	LOS	FULL	100M	FX
11	LOS	FULL	100M	FX
12	LOS	FULL	100M	FX
13	LOS	HALF	10M	TX
14	LINK	FULL	100M	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	LOS	HALF	10M	TX
G1	LOS	HALF	1000M	FX
G2	LOS	HALF	1000M	FX
G3	LOS	HALF	1000M	FX
G4	LOS	HALF	1000M	FX

The main element configuration description of system status interface:

Interface Element	Description
<b>Device information</b>	<b>Device information status bar.</b>
Name	Display the device name.
Model.	Display the device model.
Description	Display characters description of the device.
Serial number.	SN code, product serial number.
Hardware Ver	Current hardware version information.
Firmware Ver	Current software version information.
MAC address;	Hardware address of device factory configuration.
Contact method	Display the contact information of the device maintenance personnel.
<b>Port Information</b>	<b>Port Information Status Bar.</b>

Interface Element	Description
Port	Number of device port.
Connection states	Port connection state, display state as follows: <ul style="list-style-type: none"><li>• "LINK" represents connected port;</li><li>• "LOS" represents disconnected port.</li></ul>
Port states	Port work state, display state as follows: <ul style="list-style-type: none"><li>• "HALF" represents the corresponding port is in the state of half-duplex;</li><li>• "FULL" represents corresponding port is in full duplex state.</li></ul>
rate	When a port is connected, the current rate of port link is displayed.
Interface type	Interface type. <ul style="list-style-type: none"><li>• Fiber port;</li><li>• Copper port.</li></ul>

**Note**

"Device model", "device name", "device description", "device number" and "contact information" can be modified in "Main Menu > Basic Settings > System Identification".

---

# 3 Port Configuration

---

## 3.1 Port Settings

### Function Description

The "Port Config" page mainly includes:

- View port type;
- Set speed mode and duplex mode;
- Port enablement;
- Flow control;

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

For half duplex and full duplex modes, flow control is realized in different ways:

- In half duplex mode, flow control is through the back pressure (backpressure) that usually called the back pressure count, which sending jamming signal to sending source to reduced its sending speed.
- In full duplex mode, flow control generally follows the IEEE 802.3x standard, the switch sends a "pause" frame to the information source to make it stop sending. When a source receives a "pause" frame, it will pause for a while before sending a message.

**Note**

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

**Operation Path**

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

**Interface Description**

Port settings interface as follows:

Port Setting					
Port number	Interface type	Rate mode	Duplex mode	Port enable	flow control
*	----	< >	< >	<input type="checkbox"/>	<input type="checkbox"/>
1	FX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	FX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	FX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4	FX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5	FX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6	FX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
7	FX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8	FX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
9	FX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
10	FX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
11	FX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
12	FX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
13	TX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
14	TX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
15	TX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
16	TX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
17	TX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
18	TX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
19	TX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
20	TX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
21	TX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
22	TX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
23	TX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
24	TX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
G1	FX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
G2	FX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
G3	FX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>
G4	FX	Automatic neg	full duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Main elements configuration description of port settings interface:

Interface Element	Description
-------------------	-------------

Interface Element	Description
Port number	Display the port number of the device.
Interface type	<p>According to the electrical properties of the interface, the Ethernet interface of the switch can be divided into:</p> <ul style="list-style-type: none"> <li>• Copper port: transmission of electrical signals through twisted pair;</li> <li>• Fiber port: transmit optical signal via optical fiber</li> </ul>
Rate mode	<p>Click the drop-down list box of "speed mode" to select port speed mode.</p> <ul style="list-style-type: none"> <li>• Auto-Negotiation: the port can be automatically adjusted to the transmission speed of the opposite port;</li> <li>• 10M speed: the maximum supported speed is 10Mbit/s;</li> <li>• 100M speed: the maximum supported speed is 100Mbit/s;</li> </ul> <p>Note:</p> <ul style="list-style-type: none"> <li>• The copper ports of the switch are all MDI/MDIX self-adaptive ports, which support auto-negotiation.</li> <li>• 1000M speed applies only to the Gigabit ports of the switch.</li> </ul>
Duplex mode	<p>Click the "Duplex" drop-down list to select the duplex mode corresponding to the port. The options are as follows:</p> <ul style="list-style-type: none"> <li>• Half duplex: the interface can only receive or send data at any time.</li> <li>• Full duplex: the interface can receive and send data simultaneously.</li> </ul> <p>Note:</p> <p>When the speed mode is "Auto negotiation", the port automatically matches the opposite port duplex mode.</p>
Port enable	<p>Check the checkbox to enable the port.</p> <p>Note:</p> <p>Uncheck the checkbox means that the port is not enabled and cannot forward data.</p>
Flow Control	<p>Tick the check box to enable the flow control function of the port.</p> <ul style="list-style-type: none"> <li>• Under full duplex mode, flow control method is IEEE 802.3x flow control.</li> <li>• Under half duplex mode, flow control method is back pressure flow control.</li> </ul>

### Instance: Port Configuration

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

- Set the "Speed" of port 1 to "Auto".

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

### Operation Steps

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

**Step 2** Set the parameters of port 1:

1. Check the "Enable" check box;
2. Select "Auto" for "Speed".

Note:

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

**Step 3** Set the parameters of port 2:

1. Check the "Enable" check box;
2. Select "100M" for "Speed";
3. Select "Full" for "Duplex" .

**Step 4** Set the parameters of port 3:

1. Check the "Enable" check box;
2. Select "10M" for "Speed";
3. Select "Half " for "Duplex" .
4. Check the "Flow Control" check box.

**Step 5** Click "Apply".

**Step 6** End.

## 3.2 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	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
	Port	Ingress	Egress
	1	60M ▼	60M ▼
	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 ▼
	20	auto ▼	auto ▼
	21	auto ▼	auto ▼
	22	auto ▼	auto ▼
	23	auto ▼	auto ▼
	24	auto ▼	auto ▼
	G1	1000M ▼	auto ▼
	G2	auto ▼	auto ▼
	G3	auto ▼	auto ▼
	G4	auto ▼	auto ▼

The main element configuration description of bandwidth management interface:

Interface Element	Description
Bandwidth configuration	Enable/disable bandwidth configuration.
Port	Display the 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.
  - When using the port rate limit, packet loss should not occur unless the flow control is disabled. The representation of packet loss is the fluctuating transmission speed.
  - Port speed limit has high requirements on network cable quality, otherwise lots of conflict packets and broken packet would appear.
- 

## 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	100	160	160	<input checked="" type="checkbox"/>
2	160	160	160	<input type="checkbox"/>
3	160	160	160	<input type="checkbox"/>
4	160	160	160	<input type="checkbox"/>
5	160	160	160	<input type="checkbox"/>
6	160	160	160	<input type="checkbox"/>
7	160	160	160	<input type="checkbox"/>
8	160	160	160	<input type="checkbox"/>
9	160	160	160	<input type="checkbox"/>
10	160	160	160	<input type="checkbox"/>
11	160	160	160	<input type="checkbox"/>
12	160	160	160	<input type="checkbox"/>
13	160	160	160	<input type="checkbox"/>
14	160	160	160	<input type="checkbox"/>
15	160	160	160	<input type="checkbox"/>
16	160	160	160	<input type="checkbox"/>
17	160	160	160	<input type="checkbox"/>
18	160	160	160	<input type="checkbox"/>
19	160	160	160	<input type="checkbox"/>
20	160	160	160	<input type="checkbox"/>
21	160	160	160	<input type="checkbox"/>
22	160	160	160	<input type="checkbox"/>
23	160	160	160	<input type="checkbox"/>
24	160	160	160	<input type="checkbox"/>
G1	160	160	160	<input type="checkbox"/>
G2	160	160	160	<input type="checkbox"/>
G3	160	160	160	<input type="checkbox"/>
G4	160	160	160	<input type="checkbox"/>

Main elements configuration description of storm suppression interface:

Interface Element	Description
Port	Display all Ethernet ports number of the device.
Radio Broadcast (*62.5Kbps)	<p>The device procedure can suppress the transmission speed of broadcast packet</p> <p>Note: Broadcast packet, namely, the data frame with the destination address of FF-FF-FF-FF-FF-FF.</p>
Unknown-multicast (*62.5kbps)	<p>Port suppression to the transmission speed of unknown multicast data packet.</p> <p>Note: 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).</p>
Unknown -unicast	Port suppression to the transmission speed of unknown

(*62.5kbps)	unicast data packet. Note: 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  $160 \times 62.5 \text{ kbps} = 10000 \text{ kbps} = 10 \text{ Mbps}$ .
- 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	Radio broadcast (*62.5 kbps)	Unknown multicast (*62.5 kbps)	Unknown Unicast (*62.5 kbps)	Enable
1	160	160	160	<input type="checkbox"/>
2	160	160	160	<input type="checkbox"/>
3	160	160	160	<input type="checkbox"/>
4	160	160	160	<input type="checkbox"/>
5	160	160	160	<input type="checkbox"/>
6	160	160	160	<input type="checkbox"/>

### Operating 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 separately 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.

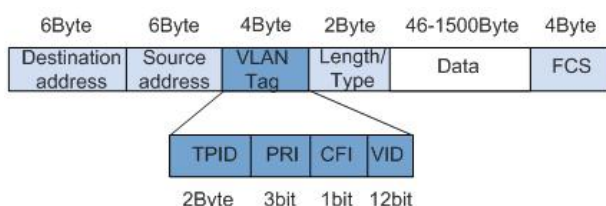
- Limit the broadcast domain;
- Increase the security of LAN;
- Improve the network stability;
- Flexibly construct virtual working team.

### Port VLAN

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

### IEEE802.1Q VLAN

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



- TPID: Tag Protocol Identifier represents the data frame type, when the value is 0x8100, it represents the VLAN data frame of IEEE 802.1Q.

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

### Function Description

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

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

### Operation Path

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

### Interface Description 1: Port-based VLAN

Port-based VLAN interface as follows:

The screenshot shows the 'VLAN Setting' window. At the top, 'VLAN Mode' has two radio buttons: 'Port-based VLAN' (selected) and 'IEEE 802.1Q VLAN'. Below this is a 'VLAN Name' text box with a '(Range :1~4094)' hint. Underneath is a 'Join Port' section with a grid of checkboxes for ports 01- through 24- and G1- through G4-. At the bottom, an 'Operation:' section contains three buttons: 'Add / Edit', 'Delete', and 'Apply'. Below the buttons is a summary table with two columns: 'VLAN Name' and 'Join Port'. The first row shows '1' in the VLAN Name column and a list of ports (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) in the Join Port column.

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

Interface Element	Description
VLAN Mode	Choose VLAN type, options are: <ul style="list-style-type: none"> <li>• Port-based VLAN</li> <li>• IEEE 802.1Q VLAN</li> </ul>
VLAN name	Enter VLAN number in digital form.
Join Port	Choose VLAN member.
Operation	Add/edit, delete or save VLAN configuration information.

The steps of configuring port-based VLAN:

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

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

**Step 3** Enter VLAN table items in the textbox of “VLAN Name”, such as 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 Mode ☐ Port-based VLAN ☒ IEEE 802.1Q VLAN

Vlan Tag Replace

Vlan Frame Control ☒ No need change VID ☐ Replace VID into default VID

VLAN ID Management

Manage VLAN ID

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 G3

The main element configuration description of 802.1Q Vlan interface:

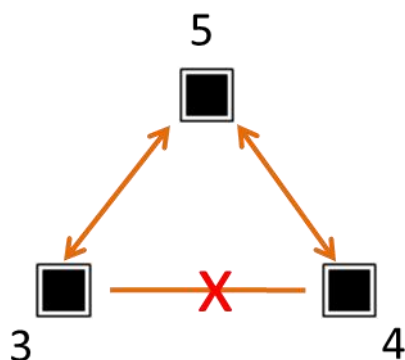
Interface Element	Description
VLAN Mode	Choose VLAN type, options are: <ul style="list-style-type: none"> <li>Port-based VLAN</li> <li>IEEE 802.1Q VLAN</li> </ul>
VLAN tag replace	The configuration bar of VLAN tag replace
VLAN frame control	Choose VLAN tag replace configuration, options are: <ul style="list-style-type: none"> <li>No need change VID;</li> <li>Replace VID into default VID.</li> </ul>
VLAN ID	The configuration bar of VLAN ID management

Interface Element	Description
<b>management</b>	
Manage VLAN ID	Manage the VLAN ID of the device. Its value range is 1-4094.
<b>The default VID configuration of the port</b>	<b>The configuration bar of default VID</b>
802.1Q VID	VLAN ID number. Its value range is 1-4094.
Member type	There are three types of data frame label that the port sends: <ul style="list-style-type: none"> <li>— : no forwarding, which is not as a member of this VLAN ID;</li> <li>M: forward and keep VLAN tag;</li> <li>U: forward but remove VLAN tag.</li> </ul>
Modify All	Quickly and simultaneously modify all member types.
Add/edit	Add configured VLAN to VLAN member list.
Delect	Delete a VLAN item in the selected member list.
Apply	Apply VLAN configuration information.

### 4.1.1 Instance: typical VLAN configuration

#### Instance

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



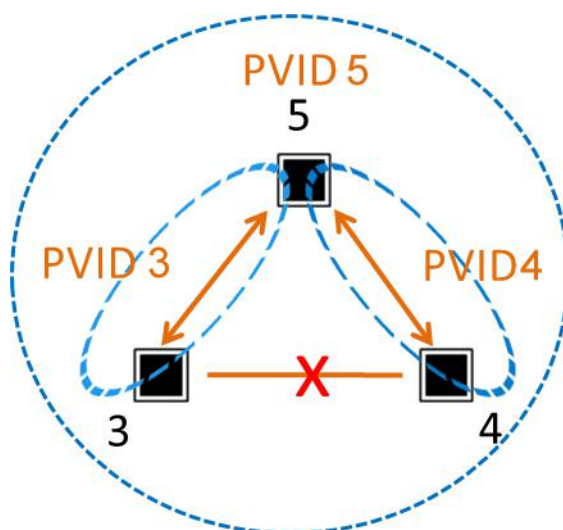
## Instance analysis

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

Analyse the port forwarding entries design as below:

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



## Operating Steps

**Step 1** Open "Main Menu > L2 Feature > 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 respectively 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 “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 “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 “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 Mode		<input type="radio"/> Port-based VLAN	<input checked="" type="radio"/> IEEE 802.1Q VLAN
Vlan Tag Replace			
Vlan Frame Control		<input checked="" type="radio"/> No need change VID	<input type="radio"/> Replace VID into default VID
VLAN ID Management			
Manage VLAN ID		<input type="text" value="1"/>	
Default VID			
01 - <input type="text" value="1"/>	02 - <input type="text" value="1"/>	03 - <input type="text" value="3"/>	04 - <input type="text" value="4"/>
05 - <input type="text" value="5"/>	06 - <input type="text" value="1"/>	07 - <input type="text" value="1"/>	08 - <input type="text" value="1"/>
09 - <input type="text" value="1"/>	10 - <input type="text" value="1"/>	11 - <input type="text" value="1"/>	12 - <input type="text" value="1"/>
13 - <input type="text" value="1"/>	14 - <input type="text" value="1"/>	15 - <input type="text" value="1"/>	16 - <input type="text" value="1"/>
17 - <input type="text" value="1"/>	18 - <input type="text" value="1"/>	19 - <input type="text" value="1"/>	20 - <input type="text" value="1"/>
21 - <input type="text" value="1"/>	22 - <input type="text" value="1"/>	23 - <input type="text" value="1"/>	24 - <input type="text" value="1"/>
G1 - <input type="text" value="1"/>	G2 - <input type="text" value="1"/>	G3 - <input type="text" value="1"/>	G4 - <input type="text" value="1"/>
802.1Q VLAN			
802.1Q VID		( Range : 1~4094 )	
01 - <input type="text" value="1"/>	02 - <input type="text" value="1"/>	03 - <input type="text" value="3"/>	04 - <input type="text" value="4"/>
05 - <input type="text" value="5"/>	06 - <input type="text" value="1"/>	07 - <input type="text" value="1"/>	08 - <input type="text" value="1"/>
09 - <input type="text" value="1"/>	10 - <input type="text" value="1"/>	11 - <input type="text" value="1"/>	12 - <input type="text" value="1"/>
13 - <input type="text" value="1"/>	14 - <input type="text" value="1"/>	15 - <input type="text" value="1"/>	16 - <input type="text" value="1"/>
17 - <input type="text" value="1"/>	18 - <input type="text" value="1"/>	19 - <input type="text" value="1"/>	20 - <input type="text" value="1"/>
21 - <input type="text" value="1"/>	22 - <input type="text" value="1"/>	23 - <input type="text" value="1"/>	24 - <input type="text" value="1"/>
G1 - <input type="text" value="1"/>	G2 - <input type="text" value="1"/>	G3 - <input type="text" value="1"/>	G4 - <input type="text" value="1"/>
(-:Not a VLAN member M:Tagged U:Untagged) <input type="button" value="Modify All"/> <input type="button" value="Add / Edit"/> <input type="button" value="Delete"/> <input type="button" value="Apply"/>			
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 G			
-- 3 --- 3U 5U			
-- 4 --- 4U 5U			
-- 5 --- 3U 4U 5U			

**Step 14** Click “Apply”.

**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. It maintains the egress interface information of Group broadcast by snooping for the multicast protocol messages sent between the layer 3 multicast device and the user host, so as to manage and control the forwarding of multicast data message in the data link layer.

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

Processing methods of different message by IGMP Snooping:

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

The GARP Multicast Registration Protocol (GMRP) is an application of the General Attribute Registration Protocol (GARP) to register and logout multicast attributes. When a host wants to join an IP multicast group, it needs to send an IGMP join information, The information evolves as a GMRP join information, once receiving GRMP join information, switch will add the port receiving the information to proper multicast group, Switch sends GMRP join information to other hosts in VLAN, among which one host as the multicast source, When the multicast source sends multicast information, switch will send the multicast information via the port that joins in the multicast group before.

#### Function Description

On the “Multicast Filtering” page, user can:

- Enable/disable IGMP Snooping;

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

### Operation Path

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

### Interface Description 1: IGMP snooping

IGMP Snooping interface as below:

Multicast filtering type	<input checked="" type="radio"/> IGMP Monitor <input type="radio"/> GMRP
Multicast filtering enable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Unknown multicast	<input type="text" value="un-discard"/>
<b>Multicast filtering</b>	
IGMP Inquire	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IGMP Polling Interval	<input type="text" value="123"/> s(60~300)
Group survival	<input type="text" value="300"/> s(120~300)
Route port set	<input type="text" value="dynamic"/>
Port List	01- <input checked="" type="checkbox"/> 02- <input type="checkbox"/> 03- <input type="checkbox"/> 04- <input type="checkbox"/> 05- <input type="checkbox"/> 06- <input type="checkbox"/> 07- <input type="checkbox"/> 08- <input type="checkbox"/> 09- <input type="checkbox"/> 10- <input type="checkbox"/> 11- <input type="checkbox"/> 12- <input type="checkbox"/> 13- <input type="checkbox"/> 14- <input type="checkbox"/> 15- <input type="checkbox"/> 16- <input type="checkbox"/> 17- <input type="checkbox"/> 18- <input type="checkbox"/> 19- <input type="checkbox"/> 20- <input type="checkbox"/> 21- <input type="checkbox"/> 22- <input type="checkbox"/> 23- <input type="checkbox"/> 24- <input type="checkbox"/> G1- <input type="checkbox"/> G2- <input type="checkbox"/> G3- <input type="checkbox"/> G4- <input type="checkbox"/>
<input type="button" value="Set"/> <input type="button" value="Cancel"/>	
<b>Number</b>	<b>MAC Address</b> <b>Type</b> <b>Port</b>

The main element configuration description of IGMP Snooping interface:

Interface Element	Description
Multicast filtering type	Choose multicast filtering type, options are: <ul style="list-style-type: none"> <li>• IGMP snooping;</li> <li>• GMRP.</li> </ul>
Multicast filtering	Enable/disable multicast filtering function.
Unknown multicast	Choose the processing mode of unknown multicast, options are: <ul style="list-style-type: none"> <li>• discard;</li> <li>• un-discard.</li> </ul>
<b>Multicast Filtering</b>	<b>The configuration bar of multicast filtering</b>
IGMP Query	The switch of IGMP query, options are: <ul style="list-style-type: none"> <li>• Enable;</li> <li>• Disable;</li> </ul> Note:

	IGMP query means that router inquiring all hosts in subnet if they join some multicast groups.
IGMP polling interval	IGMP query interval, unit: second. Note: 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. Note: <ul style="list-style-type: none"> <li>IGMP snooping needs to be enabled before using this function.</li> <li>The time range of group survival that can be set is 120-300s.</li> </ul>
Routing port set	Choose the building mode of routing table, options are: <ul style="list-style-type: none"> <li>Dynamic routing, routing ports are dynamically acquired though switch.</li> <li>Static routing, check the box of port in "port list" as routing port.</li> </ul>
Port list	The selection list of static routing port.



## Note

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

## Interface Description 2: GMRP

GMRP interface as below:

The image shows a configuration window for GMRP. At the top, there are three settings: 'Multicast filtering type' with radio buttons for 'IGMP Monitor' and 'GMRP' (selected); 'Multicast filtering' with radio buttons for 'Enable' and 'Disable' (selected); and 'Unknown multicast' with a dropdown menu set to 'Un-discard'. Below these is a section titled 'Multicast filtering' with a blue header. Under this header is a 'Portlist' section containing a grid of checkboxes for ports 01- through 24- and G1- through G4-. All checkboxes are checked. At the bottom of the window are 'Set' and 'Cancel' buttons.

The main element configuration description of GMRP interface:

Interface Element	Description
Multicast filtering type	Multicast filtering type, options are: <ul style="list-style-type: none"> <li>IGMP snooping;</li> <li>GMRP.</li> </ul>
Multicast filtering	The multicast filtering checkbox, options are: <ul style="list-style-type: none"> <li>Enable;</li> <li>Disable;</li> </ul>
Unknown multicast	Unknown multicast options are: <ul style="list-style-type: none"> <li>discard;</li> <li>un-discard.</li> </ul>
<b>Multicast Filtering</b>	<b>The configuration bar of multicast filtering</b>
Port list	The checkbox of GMRP port list.

## 4.2.2 Static Multicast Table

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

### Function Description

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

### Operation Path

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

### Interface Description

Static multicast interface as follows:

Static multicast table

Static Multicast  (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

The main element configuration description of static multicast interface:

Interface Element	Description
Static multicast MAC address	Input "Static multicast MAC address", and the format is "XX-XX-XX-XX-XX-XX". Note: <ul style="list-style-type: none"> <li>Low-order of the highest byte of multicast MAC address is 1. Entering non-multicast address is not allowed.</li> <li>Space and other illegal characters are not allowed for address format, otherwise alarm message will pop up.</li> </ul>
Port list	Tick the check box of corresponding port, it represents that corresponding port joins in the static multicast MAC address.
Processing list	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 "Static Multicast MAC Address:", input "01-00-00-00-00-01".

**Step 3** On the row of "Join Port":

1. Tick the check box after "1-";
2. Tick the check box after "2-";
3. Tick the check box after "3-".

**Step 4** Click "Add".

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

**Step 6** End.

# 5 QoS

## 5.1 QoS Classification

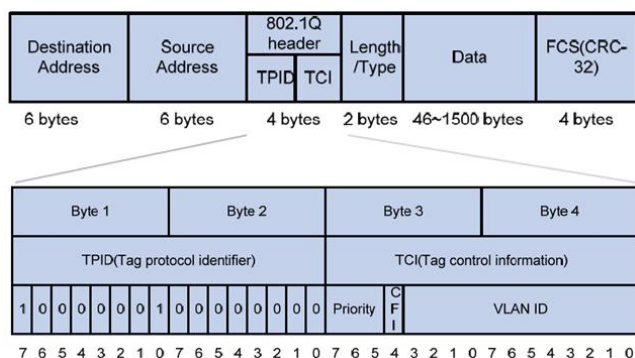
QoS (Quality of Service) is used to evaluate the ability of the service provider to meet the service needs of customers. As for network business, service quality includes transmission bandwidth, transfer delay, data packet loss rate and so on.

The problem of service quality faced by traditional network is mainly caused by network congestion. The so-called congestion refers to the phenomenon that the forwarding rate decreases and extra delays are introduced due to the relative shortage of supply resources, thus leading to the decline of service quality. For congestion management, a queue technique is typically used, where traffic is classified using a queue algorithm and then sent out using a priority algorithm.

Priority is used to identify the priority of message transmission.

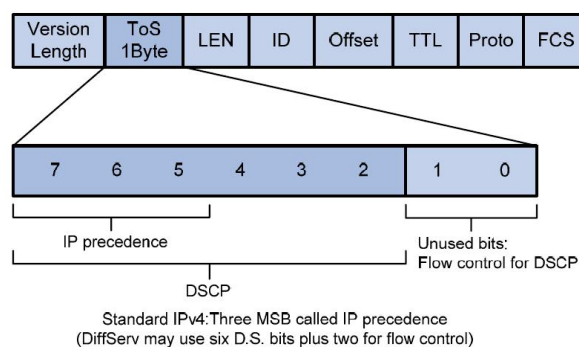
- CoS

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



- ToS

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



## Function Description

On the page of QoS Classification, user can set:

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

## Operation Path

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

## Interface Description

Screenshot of QoS Classification interface:



**QoS Classification**

Queuing Mechanism: **Weighted Fair(8:4:2:1)** ▼

Port	Inspect DSCP	Inspect Cos	Port Priority
*	<input type="checkbox"/>	<input type="checkbox"/>	<> ▼
1	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
2	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
3	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
4	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
5	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
6	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
7	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
8	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
9	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
10	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
11	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
12	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
13	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
14	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
15	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
16	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
17	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
18	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
19	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
20	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
21	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
22	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
23	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
24	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
G1	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
G2	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
G3	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼
G4	<input type="checkbox"/>	<input type="checkbox"/>	0 ▼

Save Cancel

The main element configuration description of QoS classification interface:

Interface Element	Description
Queuing mechanism	<p>Queuing scheduling setting, options are:</p> <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> </ul>
Port	Port number of switch.
Inspect ToS	After checking the checkbox, the priority of ToS would be inspected during queue scheduling.

Interface Element	Description
Inspect CoS	After checking the checkbox, the priority of CoS would be inspected during queue scheduling.
Port priority	<p>To configure default port priority for ports that haven't enabled ToS and CoS priority. The value range is 0-7. The higher the value, the higher the priority.</p> <p>Note: By default, switch would use port priority in place of the 802.1p priority the port comes with when receiving message to control the quality of service the messages deserve.</p>

**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**

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

**Operation Steps**

- Step 1** Open "Main Menu > QoS > QoS Classification".
- Step 2** On the page of classification, choose "Weight Fair (8:4:2:1)" in queuing mechanism.
- Step 3** On the line of port 1, check the checkbox of "inspect ToS".
- Step 4** Click "Apply".
- Step 5** End.

## 5.2 CoS Mapping

**Function Description**

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

**Operation Path**

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

**Interface Description**

Screenshot of QoS Mapping interface:

Cos Mapping				
Cos	0	1	2	3
Priority Queue	Low ▼	Low ▼	Normal ▼	Normal ▼
Cos	4	5	6	7
Priority Queue	Medium ▼	Medium ▼	High ▼	High ▼
<div>Save</div> <div>Cancel</div>				

The main element configuration description of QoS mapping interface:

Interface Element	Description
CoS	Display CoS value.
Priority	Set mapping between CoS value and priority queue, options are as follows: <ul style="list-style-type: none"> <li>Low: low priority queue</li> <li>Normal: normal priority queue</li> <li>Medium: medium priority queue</li> <li>High: high priority queue</li> </ul>

### Instance: CoS mapping configuration

For example:

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

### Operation Steps

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

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

1. When the CoS value is “0”, choose Low as the corresponding priority.
2. When the CoS value is “1”, choose Low as the corresponding priority.
3. When the CoS value is “2”, choose Normal as the corresponding priority.
4. When the CoS value is “3”, choose Normal as the corresponding priority.
5. When the CoS value is “4”, choose Medium as the corresponding priority.
6. When the CoS value is “5”, choose Medium as the corresponding priority.
7. When the CoS value is “6”, choose High as the corresponding priority.
8. When the CoS value is “7”, choose High as the corresponding priority.

**Step 3** Click “Apply”.

**Step 4** End.

## 5.3 DSCP Cos map queue

### Function Description

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

### Operation Path

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

### Interface Description

DSCP Mapping interface screenshot:

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)	It displays ToS (DSCP) in hexadecimal and decimal format simultaneously. The value in the bracket is decimal.
Level	Set mapping between ToS value and priority queue, options are as follows:

Interface Element	Description
	<ul style="list-style-type: none"> <li>Low: low priority queue</li> <li>Normal: normal priority queue</li> <li>Medium: medium priority queue</li> <li>High: high priority queue</li> </ul>

### Instance: ToS mapping configuration

For example:

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

### Operation Steps

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

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

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

**Step 3** Click “Apply”.

**Step 4** End.

# 6 Link Backup

## 6.1 Rapid Ring

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

- Ring

SW-Ring is an Ethernet Ring network algorithm developed and designed by the company for highly reliable industrial control network applications that require link redundancy backup. Features in Ethernet link redundancy, fast automatic recovery. Ring adopts no master station design. In a multi-ring network of up to 250 switches, the network self-recovery time is less than 20 milliseconds. Each port in this series of switches can be used as a ring port and connected with other switches. When an interruption occurs in the network connection, the SW-Ring redundant mechanism enables the backup link to quickly recover the network communication.

- RSTP

To solve the loop problem in switching network, Spanning Tree Protocol (STP) is proposed. Because of the slow speed of STP topological convergence, IEEE released 802.1W standard in 2001 which has defined RSTP (Rapid Spanning Tree Protocol). RSTP has made improvement on the basis of STP, which has achieved quick topological convergence of network. (The fastest speed could be in 1 second) The device that runs STP/RSTP protocol finds the loop in the network by interacting information, and be selective to congest a particular port, so eventually ring network structure will be pruned to a tree network structure without loop, thus preventing message from looping in the ring network, and the device from declining its processing ability caused by receiving the same message repetitively.

The working process of STP:

- First, elect the root bridge. The election basis is bridge ID combined by network bridge priority and network bridge MAC address. The network bridge with the smallest bridge ID would be the root bridge in the network, whose all ports are connected to the downstream bridge, so the roles of all ports has become specified ports.
- Next, the downstream network bridges that connect to the root bridge would choose a “strongest” brunch as the path to the root bridge separately, so the roles of the corresponding port would be root port. Loop this process to the edge of the network, a tree would be generated when the specified port and the root port are determined.
- when the spanning tree is stabled (default value is 30 seconds) after a while, the specified port and root port will enter forwarding state, and other ports will enter block state.
- STP BPDU would be sent from the specified ports of each network bridge regularly to maintain the state of link. If the network topology has changed, the spanning tree would be recalculated and the port state would be changed as well.

### Function Description

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

### Operation Path

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

### Interface Description

Initial rapid ring interface as follows:

The main element configuration description of initial rapid ring interface:

Interface Element	Description
Current status	Current status bar

Interface Element		Description
Protocol of redundancy	of	The current status of ring network protocol of the device.
<b>Settings</b>		<b>Settings bar</b>
Protocol of redundancy	of	Choose the corresponding redundancy protocol. Options: <ul style="list-style-type: none"> <li>• None: it means that the ring network function is disabled.</li> <li>• Ring V3: single ring, coupling ring, chain and Dual homing are supported.</li> <li>• STP (IEEE 802.1D/1W): spanning tree/rapid spanning tree.</li> </ul>

### Function description of Ring V3

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

### Operation Path

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

### Interface Description

Ring network interface as follows:



Current Status							
Protocol of Redundancy		Ring V3					
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	1	2	Single	0 *100ms	Slave	<input type="checkbox"/>
2	2	3	4	Single	0 *100ms	Slave	<input type="checkbox"/>
3	3	5	6	Single	0 *100ms	Slave	<input type="checkbox"/>
4	4	7	8	Single	0 *100ms	Slave	<input type="checkbox"/>
<p>Note : Changes will only take effect after system reboot</p>							
				Set		Cancel	

The main element configuration description of Ring network interface:

Interface Element	Description
The fast loop network	Click “The fast loop network” to check the ring state of current ring network group configuration.
Group	Support Group 1-4, it means that the device supports up to 4 groups.
ID	When multiple switches form a ring, the current ring ID would be network ID. Different ring network has different ID.
Loop 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	<p>According to the requirement in the scene, user can choose different ring network.</p> <ul style="list-style-type: none"> <li>Single: single ring, using a continuous ring to connect all device together.</li> <li>Couple: couple ring is a redundant structure used for</li> </ul>

Interface Element	Description
	<p>connecting two independent networks.</p> <ul style="list-style-type: none"> <li>Chain: chain can enhance user's flexibility in constructing all types of redundant network topology via an advanced software technology.</li> <li>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.</li> </ul>
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.
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
Main device address	

The main element configuration description of rapid ring interface

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

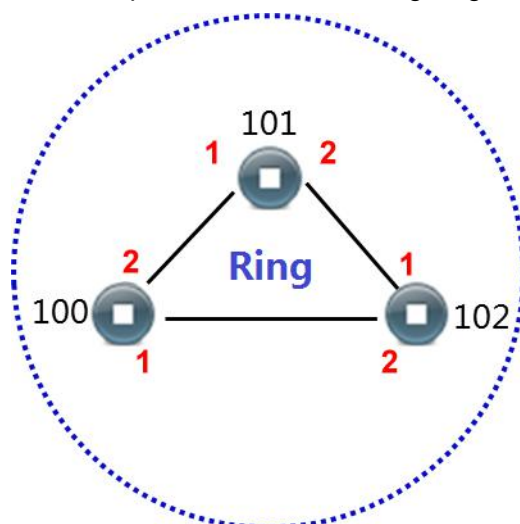
Now introduce the creation process respectively according to different ring network:

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

## 6.1.1 Instance: create single ring

### Instance

For example: create the following single ring:



### Instance analysis

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

### Operation Steps

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

- Step 1** Choose “Main Menu > Redundancy > Rapid Ring”.
- Step 2** In the 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”.

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	1	2	Single	0*100ms	Slave	<input checked="" type="checkbox"/>
2	2	3	4	Single	0*100ms	Slave	<input type="checkbox"/>
3	3	5	6	Single	0*100ms	Slave	<input type="checkbox"/>
4	4	7	8	Single	0*100ms	Slave	<input type="checkbox"/>

Note : Changes will only take effect after system reboot

Set    Cancel

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

**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”.

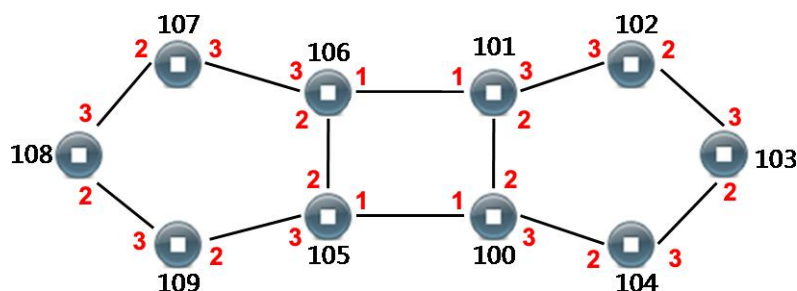
**Step 10** On the column of “Device Reboot”, click the button of “Reboot”.

**Step 11** End.

## 6.1.2 Instance: create coupling ring

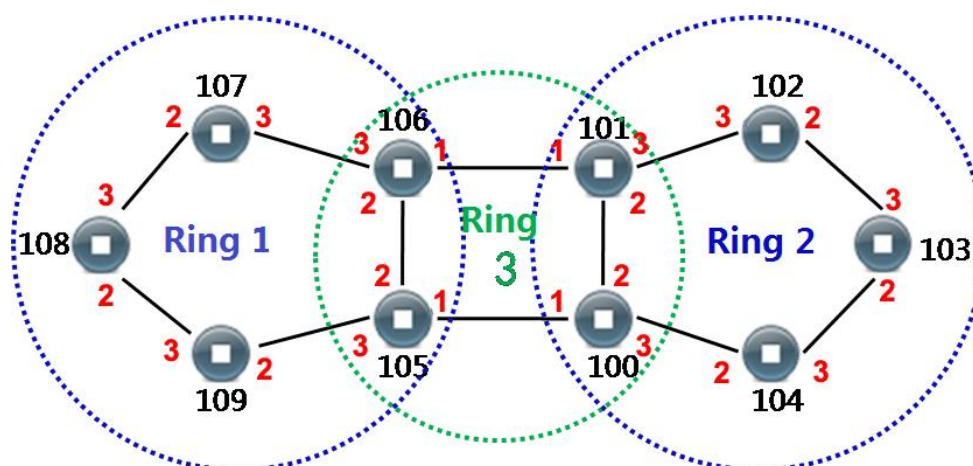
### Instance

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



### Instance analysis

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



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

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

### Operation Step 1: configuring Ring 1 in WEB interface

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

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

**Step 2** In the 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”.

Group	ID	Loop port 1	Loop port 2	Type	HelloTime	Master-slave	Enable
1	1	2	3	Single	0 *100ms	Slave	<input checked="" type="checkbox"/>
2	2	3	4	Single	0 *100ms	Slave	<input type="checkbox"/>
3	3	5	6	Single	0 *100ms	Slave	<input type="checkbox"/>
4	4	7	8	Single	0 *100ms	Slave	<input type="checkbox"/>

Note : Changes will only take effect after system reboot

Set Cancel

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

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	<input checked="" type="checkbox"/>
2	2	3	4	Single	0 *100ms	Slave	<input type="checkbox"/>
3	3	5	6	Single	0 *100ms	Slave	<input type="checkbox"/>
4	4	7	8	Single	0 *100ms	Slave	<input type="checkbox"/>

Note : Changes will only take effect after system reboot

Set Cancel

**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** On the column of “Device Reboot”, click the button of “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 setting area of the “Rapid Ring” page, choose “Ring V3” as the “protocol of redundancy”.

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

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

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

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

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

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



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

**Step 10** End.

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	<input checked="" type="checkbox"/>
2	3	1	2	Couple	0 *100ms	Slave	<input checked="" type="checkbox"/>
3	3	5	6	Single	0 *100ms	Slave	<input type="checkbox"/>
4	4	7	8	Single	0 *100ms	Slave	<input type="checkbox"/>

Note : Changes will only take effect after system reboot

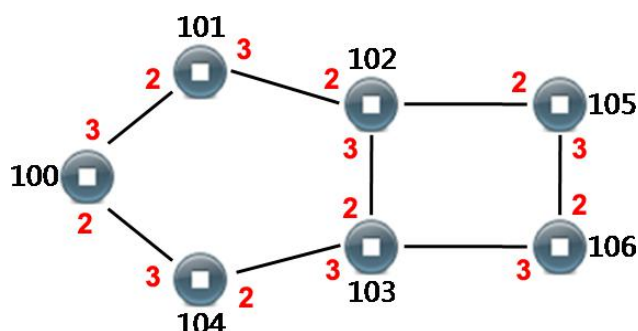
Set Cancel

### 6.1.3 Instance: creating chain

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

#### Instance

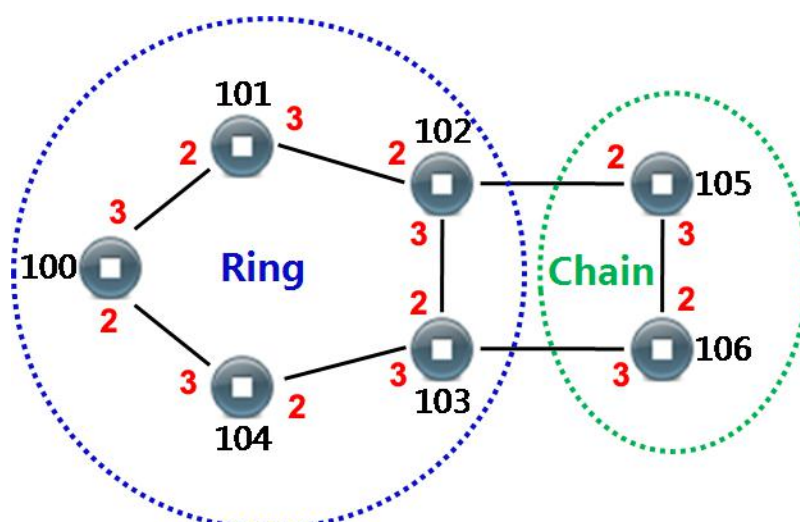
For example: creating chain. Its basic architecture is shown as below:



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

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

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

1. Set “Type” to “Single”;
2. Set “ID” to “1”;
3. Set “Port 1” to “2”;
4. Set “Port 2” to “3”;

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	<input checked="" type="checkbox"/>
2	3	1	2	Couple	0 *100ms	Slave	<input type="checkbox"/>
3	3	5	6	Single	0 *100ms	Slave	<input type="checkbox"/>
4	4	7	8	Single	0 *100ms	Slave	<input type="checkbox"/>

Note : Changes will only take effect after system reboot

Set Cancel

**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** On the column of “Device Reboot”, click the button of “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 setting area of the “Rapid Ring” page, choose “Ring V3” as the “protocol of redundancy”.

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

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

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

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

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	<input checked="" type="checkbox"/>
2	3	1	2	Couple	0 *100ms	Slave	<input type="checkbox"/>
3	3	5	6	Single	0 *100ms	Slave	<input type="checkbox"/>
4	4	7	8	Single	0 *100ms	Slave	<input type="checkbox"/>

Note : Changes will only take effect after system reboot

Set Cancel



#### Note

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

**Step 7** Click “Apply”.

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

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

**Step 10** End.



#### Notice

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

## 6.1.4 Creating Spanning Tree

### Function Description

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

### Operation Path

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

### Interface Description

RSTP 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	<input type="checkbox"/>	<input type="checkbox"/>
2	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>
3	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>
4	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>
5	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>
6	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>
7	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>
8	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>
9	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>
10	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>
11	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>
12	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>
13	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>
14	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>
15	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>
16	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>
17	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>
18	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>
19	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>
20	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>
21	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>
22	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>
23	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>
24	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>
G1	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>
G2	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>
G3	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>
G4	0	128	Auto	<input type="checkbox"/>	<input type="checkbox"/>

Notes : Changes will only take effect after system reboot

Apply

Cancel

The main element configuration description of RSTP interface:

Interface Element	Description
Protocol of redundancy	Choose the algorithm of redundancy protocol, options are: <ul style="list-style-type: none"> <li>None: it means that the ring network function is disabled.</li> </ul>

Interface Element	Description
	<ul style="list-style-type: none"> <li>SW-Ring V3: supports single ring, coupling ring, chain and Dual_homing;</li> <li>STP (IEEE 802.1D/1W): spanning tree/rapid spanning tree.</li> </ul>
Bridge priority	<p>The priority of bridge.</p> <p>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.</p>
Hello time	<p>The transmission time interval of the BPDU data packet.</p> <p>Note: The protocol message that STP/RSTP adopts is BPDU (Bridge Protocol Data Unit).</p>
FWD delay	<p>The forward delay time that the port of switch maintains in transition state (listening and learning).</p> <p>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.</p>
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	<p>The path cost from network bridge to root bridge.</p> <p>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.</p>
Port priority	<p>The priority of ports in bridge. The smaller the value, the higher the priority.</p> <p>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.</p>
P2P	<p>The directly connected switch port, options are:</p> <ul style="list-style-type: none"> <li>Yes;</li> <li>No;</li> <li>Auto: adopt negotiation mechanism that could implement quick conversion of port states.</li> </ul>
Directly connect to terminal	The switch that is on the edge of network and connects to the terminal devices.
Port STP	Checking this checkbox. It represents participating in the operation of spanning tree protocol.

RSTP status interface as follows:

The 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 state
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
16	128	0	Y	N	Rapid	Disabled	Disabled
17	128	0	Y	N	Rapid	Disabled	Disabled
18	128	0	Y	N	Rapid	Disabled	Disabled
19	128	0	Y	N	Rapid	Disabled	Disabled
20	128	0	Y	N	Rapid	Disabled	Disabled
21	128	0	Y	N	Rapid	Disabled	Disabled
22	128	0	Y	N	Rapid	Disabled	Disabled
23	128	0	Y	N	Rapid	Disabled	Disabled
24	128	0	Y	N	Rapid	Disabled	Disabled
G1	128	0	Y	N	Rapid	Disabled	Disabled
G2	128	0	Y	N	Rapid	Disabled	Disabled
G3	128	0	Y	N	Rapid	Disabled	Disabled
G4	128	0	Y	N	Rapid	Disabled	Disabled

Close

The main element configuration description of RSTP status interface:



Interface Element	Description
<b>Root information</b>	<b>The display bar of root information table</b>
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.
<b>Basic information</b>	<b>The display bar of basic information table</b>
Port	Displays the port number of the 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	<p>It is divided by whether the port forwards user flow and learns MAC address.</p> <ul style="list-style-type: none"> <li>Discarding: neither forward user flow nor learn MAC address;</li> <li>Learning: doesn't forward user flow but learn MAC address;</li> <li>Forwarding: forward user flow and learn MAC address;</li> <li>Listening: neither forward user flow nor learn MAC address; but can receive and send configuration message;</li> <li>Blocking: port only receives and processes BPDU,</li> </ul>

Interface Element	Description
	doesn't forward user flow; <ul style="list-style-type: none"> <li>Disabled: blocked or physically disconnected.</li> </ul>



Note

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

## 6.2 Port Trunking

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

Link aggregation technology mainly has the following three advantages:

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

### Function Description

Binding multiple physical ports into one logical channel.

### Operation Path

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

### Interface Description

Static Trunking interface as follows:

Static Trunking

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

Add / Edit
Delete
Apply

Group	Jion Port
1	01 03
2	02 04

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, In order to increase bandwidth, port 1 and port 2 of switch A and switch B can be trunked into a Trunking group.

### Operation Steps

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

**Step 1** Log into Web configuration interface.

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

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

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

**Static Trunking**

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

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

LLDP (Link Layer Discovery Protocol) is produced under such background, it provides a standard way of link layer discovery, The main capability, management address, device identification, interface identification and other information of the end device can be organized into different TLV (Type/Length/Value, Type/Length/Value), and encapsulated in LLDPDU (Link Layer Discovery Protocol Data Unit, Link Layer Discovery Protocol Data Unit) and distributed to the neighbor directly connected to it. After receiving the Information, the neighbor saves it in the form of standard MIB (Management Information Base) for the network Management system to query and judge the communication status of link.

### **LLDP message sending mechanism**

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

### **LLDP message receiving mechanism**

When enabling LLDP function, the device will check the validity of the received LLDP message and the TLV(Type/Length/Value) carried by it. After checking, the neighbor information will be saved in the local device, and the aging time of neighbor

information in the local device will be set according to the TTL(Time To Live) Value carried by TLV in the LLDPDU(LLDP Data Unit) message. If the received TTL value in the LLDPDU equals to zero, the neighbor information would be aged immediately.

### Function Description

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

### Operation Path

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

### Interface Description

Parameter configuration interface as follows:

LLDP Global Config									
LLDP		Disable ▼							
Message Transmit Interval(s)		30		(5 ~ 32768)					
LLDP Port 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 ▼				
<div>Set Cancel</div>									

Main elements configuration description of parameter configuration interface:

Interface Element	Description
<b>LLDP Global Configuration</b>	<b>LLDP Global Configuration Bar</b>
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.

Interface Element	Description
<b>LLDP Port Configuration</b>	<b>LLDP port configuration bar</b>
Mode	<ul style="list-style-type: none"> <li>• Disable: disable LLDP function.</li> <li>• Tx Rx: send and receive LLDP message.</li> <li>• Tx only: periodically send LLDP message to neighbor device.</li> <li>• Rx only: check the validity of received LLDP and carried TLV, and configure the ageing time of neighbor device in the local device according to TTL (Time To Live) value in TLV.</li> </ul>

## 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 > System Manage > LLDP > Neighbor Information".

### Interface Description

Neighbor information interface as follows:

LLDP Neighbor information						
Local port	MAC Address	Remote port	Port description	System Name	System function	Management address
Refresh						

Main elements configuration description of neighbor information interface:

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

Interface Element	Description
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 network topology and network management. Management address is released to public after being packaged in Management Address TLV of LLDP message.



# 8 Access Control

---

## 8.1 Password

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

- Observer: check permissions.
- System administrator: modify and view permissions.

### Function Description

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

### Operation Path

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

### Interface Description

Login settings interface as follows:

userpassword

Index

1

Access\_level

Administrator

Regular name

Regular Password

Login name

admin

Password

\*\*\*\*\*

Confirm Password

\*\*\*\*\*

Save

Cancel

The main element configuration description of login settings interface:

Interface Element	Description
Index	<p>The index number is corresponding to the access level.</p> <ul style="list-style-type: none"> <li>1: administrator</li> <li>2: administrator or observer</li> <li>3: administrator or observer</li> </ul>
Access level	<p>Access level settings, options:</p> <ul style="list-style-type: none"> <li>Administrator: check and modify permissions.</li> <li>Observer: check permissions.</li> </ul>
Regular name	<p>Login name for the current guest to log in to WEB configuration interface.</p>
Regular password	<p>Password for current guest to log in to WEB configuration interface.</p> <p>Note: The password should be a combination of letters less than 16 bytes.</p>
Login name	<p>Login name settings for guest to log in to WEB configuration interface again.</p>
Password	<p>Password settings for guest to log in to WEB configuration interface again.</p> <p>Note: The password should be a combination of letters less than 16 bytes.</p>
Confirm password	<p>Visitor password confirmed.</p>



Notice

---

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

---

### For instance: create administrator

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

### Operation Steps

- Step 1** Log into Web configuration interface.
- Step 2** Choose “Main Menu > Access Control > Login Settings”.
- Step 3** On the “Login settings” page:
1. Choose “2” 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 a technology used for centralized and dynamic user IP address management and configuration.

DHCP adopts client/server communication mode that the DHCP client submits configuration application to the DHCP server, then the server returns the configuration Information (including IP address, default gateway, DNS Server) allocated for the client. This can realize IP address allocation and centralized configuration management of other network 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  (Optional)

DNS1 Address  (Optional)

DNS2 Address  (Optional)

Tenancy term  hour (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

Number	IP Address	Port
--------	------------	------

The main element configuration description of DHCP server interface:

Interface Element	Description
DHCP Server	Enable/disable DHCP server function.
<b>DHCP Server Basic Information</b>	<b>The configuration bar of DHCP server basic information</b>
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.
DNS1 address	The DNS1 address that can be captured by DHCP client automatically.
DNS2 address	The DNS2 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).
<b>The distribution of static address table</b>	<b>The configuration bar of static address distribution table</b> Note: The IP address list that DHCP client can automatically capture in different ports.
IP Address	The specified IP address that can be captured by DHCP client automatically.
Join Port	Port list check box, check port binding with static IP

	address.
Processing list	Add/modify, delete or save configured static IP address and port entry.

## 8.3 MAC Port Lock

Physical MAC (Media Access Control) address exclusively identifies one terminal on the Ethernet. This address is a unique hardware address in the world.

### 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:

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.
Join Port	Display the corresponding ports of the device.
Processing list	Add/modify, delete static MAC address entry.



#### 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.

## 8.4 Security Management

### 8.4.1 MAC 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 > Access Ctrl > Security Management > MAC Filter".

#### Interface Description

MAC filter interface as follows:

Feature Set	
MAC Filter	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
	<input type="radio"/> Only rules list of MAC addresses will be allowed to pass <input checked="" type="radio"/> Only banned list of rules by MAC address
MAC Address filtering rules	
Goal MAC	<input type="text"/> (XX-XX-XX-XX-XX-XX)
Source MAC	<input type="text"/> (XX-XX-XX-XX-XX-XX)
Remarks	<input type="text"/> Choosable
Portlist	Check all <input type="checkbox"/> 1- <input type="checkbox"/> 2- <input type="checkbox"/> 3- <input type="checkbox"/> 4- <input type="checkbox"/> 5- <input type="checkbox"/> 6- <input type="checkbox"/> 7- <input type="checkbox"/> 8- <input type="checkbox"/> 9- <input type="checkbox"/> 10- <input type="checkbox"/> 11- <input type="checkbox"/> 12- <input type="checkbox"/> 13- <input type="checkbox"/> 14- <input type="checkbox"/> 15- <input type="checkbox"/> 16- <input type="checkbox"/> 17- <input type="checkbox"/> 18- <input type="checkbox"/> 19- <input type="checkbox"/> 20- <input type="checkbox"/> 21- <input type="checkbox"/> 22- <input type="checkbox"/> 23- <input type="checkbox"/> 24- <input type="checkbox"/> G1- <input type="checkbox"/> G2- <input type="checkbox"/> G3- <input type="checkbox"/> G4- <input type="checkbox"/>
Processing list	<input type="button" value="Add"/> <input type="button" value="Del"/> <input type="button" value="Save"/>
List	
Goal MAC	Source MAC
Remarks	Portlist

The main element configuration description of MAC filter interface:

Interface Element	Definition
<b>Feature set</b>	<b>Function setting area</b>
Mac Address Filtering	Enable or disable MAC address filtering. When the function is enabled, options are as follows: <ul style="list-style-type: none"> <li>Only enable the MAC addresses in the list of rules to pass</li> <li>Only disable the MAC addresses in the list of rules to pass</li> </ul>
<b>MAC address filtering rules</b>	<b>Configuration bar of MAC address filtering rules</b>

Interface Element	Definition
Destination MAC	Set the destination MAC address rules of MAC filtering: <ul style="list-style-type: none"> <li>When the list of rules is enabled, the data that takes this address as destination MAC address could be sent</li> <li>When the list of rules is disabled, the data that takes this address as destination MAC address couldn't be sent</li> </ul>
Source MAC	Set the source MAC address rules of MAC filtering: <ul style="list-style-type: none"> <li>When the list of rules is enabled, the data that takes this address as source MAC address could be sent</li> <li>When the list of rules is disabled, the data that takes this address as source MAC address couldn't be sent</li> </ul>
Remark	Add the remark information of the list of rules
Join Port	Check the box of ports that apply to MAC filtering rules
Processing list	Set the processing scheme of rules: <ul style="list-style-type: none"> <li>Add entry</li> <li>Delete entry</li> <li>Save configuration</li> </ul>
List of rules	Display the list of rules that have been set up

## 8.4.2 IP Address Filtering

### 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 > Access Ctrl > Security Management > IP Filter".

### Interface Description

IP filter interface as follows:

Feature Set	
IP Filter	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="radio"/> Only rules list of IP addresses will be allowed to pass <input checked="" type="radio"/> Only banned list of rules by IP address
IP Address filtering rules	
Goal IP	<input type="text"/>
Source IP	<input type="text"/>
Remarks	<input type="text"/> Choosable
Portlist	Check all <input type="checkbox"/> 1- <input type="checkbox"/> 2- <input type="checkbox"/> 3- <input type="checkbox"/> 4- <input type="checkbox"/> 5- <input type="checkbox"/> 6- <input type="checkbox"/> 7- <input type="checkbox"/> 8- <input type="checkbox"/> 9- <input type="checkbox"/> 10- <input type="checkbox"/> 11- <input type="checkbox"/> 12- <input type="checkbox"/> 13- <input type="checkbox"/> 14- <input type="checkbox"/> 15- <input type="checkbox"/> 16- <input type="checkbox"/> 17- <input type="checkbox"/> 18- <input type="checkbox"/> 19- <input type="checkbox"/> 20- <input type="checkbox"/> 21- <input type="checkbox"/> 22- <input type="checkbox"/> 23- <input type="checkbox"/> 24- <input type="checkbox"/> G1- <input type="checkbox"/> G2- <input type="checkbox"/> G3- <input type="checkbox"/> G4- <input type="checkbox"/>
Processing list	<input type="button" value="Add"/> <input type="button" value="Del"/> <input type="button" value="Save"/>
List of rules	
Goal IP	Source IP   Remarks   Portlist

Main element configuration instructions in IP Filtering interface

Interface Element	Definition
<b>Feature set</b>	<b>Function setting area</b>
IP Address Filtering	Enable or disable IP address filtering. When the function is enabled, options are as follows: <ul style="list-style-type: none"> <li>Only enable the IP addresses in the list of rules to pass</li> <li>Only disable the IP addresses in the list of rules to pass</li> </ul>
<b>IP address filtering rules</b>	<b>The configuration bar of IP address filtering rules</b>
Destination IP addresses.	Set the destination IP address rules of IP filtering: <ul style="list-style-type: none"> <li>When the list of rules is enabled, the data that takes this address as destination IP address could be sent</li> <li>When the list of rules is disabled, the data that takes this address as destination IP address couldn't be sent</li> </ul>
Source IP	Set the source IP address rules of IP filtering: <ul style="list-style-type: none"> <li>When the list of rules is enabled, the data that takes this address as source IP address could be sent</li> <li>When the list of rules is disabled, the data that takes this address as source IP address couldn't be sent</li> </ul>
Remark	Add the remark information of the list of rules
Join Port	Check the box of ports that apply to IP filtering rules
Processing list	Set the processing scheme of rules: <ul style="list-style-type: none"> <li>Add entry</li> <li>Delect entry</li> <li>Save configuration</li> </ul>
List of rules	Display the list of rules that have been set up



---

# 9 Remote Monitoring

---

## 9.1 SNMP Configuration

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

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

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

NMS as the network management center of the entire network, manages the equipments. Each managed device contains Agent processes, MIB, and multiple managed objects residing on the device. The NMS completes its instructions through interacting with the Agent running on the managed device, and the operation of the MIB on the device end by Agent.

SNMPv1/SNMPv2c defines 7 operation types used to complete the information exchange between NMS and Agent. SNMPv1 version doesn't support GetBulk and Inform operation.

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

## Function Description

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

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

## Operation Path

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

## Interface Description

Interface screenshot of SNMP configuration as follows:

The image shows a 'SNMP Configuration' dialog box. At the top, there's a title bar. Below it, the 'SNMP Configuration' section has two radio buttons: 'Enable' (selected) and 'Disable'. The 'SNMP V1/V2' section is below. The 'SNMP Read Community' field contains the text 'public'. The 'SNMP Read/Write Community' field contains the text 'private'. The 'SNMP Gateway' field contains the IP address '192.168.1.1'. At the bottom right, there are 'Save' and 'Cancel' buttons.

Main elements configuration description of SNMP configuration interface:

Interface Element	Description
SNMP Configuration	SNMP configuration function, options as follows: <ul style="list-style-type: none"> <li>• Enable;</li> <li>• Disable;</li> </ul>
SNMP V1/V2C	SNMP supports the following version: <ul style="list-style-type: none"> <li>• SNMP V1: It adopts UDP protocol which can be used widely but will be insecure.</li> <li>• SNMP V2c: Semantics has been enhanced, and it supports TCP protocol.</li> </ul>
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	Configure the destination IP address of Trap information. Note: It will send out alarm during cold or warm start, port offline/online, power on/off.



#### Note

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

### Instance SNMP Configuration

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

### Operation Steps

- Step 1** Log into Web configuration interface.
- Step 2** Select "Main Menu > Remote Monitoring > SNMP Configuration".
- Step 3** On the displayed page of "SNMP Configuration":
  - 1. Select "enable" on the column of "SNMP Configuration";
  - 2. Select "Read-only community name" as "public";
  - 3. Select "Read/Write community name" as "private";
  - 4. Select "SNMP gateway" as "192.168.1.1".
- Step 4** Click "Apply".
- Step 5** End.

## 9.2 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:

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.

## 9.3 Alarm Settings

### Function Description

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

### Operation Path

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

### Interface Description

Alarm warning interface as follows:

Alarm Warning: ☐ Enable ☒ Disable

Relay Output Type:

System Events					
Power	Alarm Setting	Status	Power	Alarm Setting	Status
1	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Normal	2	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Fault

Port Events					
Port	Alarm Setting	Connection	Port	Alarm Setting	Connection
*	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	-----	*	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	-----
1	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los	2	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los
3	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los	4	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los
5	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los	6	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los
7	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los	8	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los
9	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los	10	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los
11	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los	12	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los
13	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los	14	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Link
15	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los	16	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los
17	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los	18	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los
19	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los	20	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los
21	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los	22	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los
23	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los	24	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los
G1	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los	G2	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los
G3	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los	G4	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Los

Main elements configuration description of alarm warning interface:

Interface Element	Description
Alarm Settings	Configure alarm settings. Options: <ul style="list-style-type: none"> <li>• Enable;</li> <li>• Disable;</li> </ul>

Interface Element	Description
Relay Output Type	<p>Click the drop-down list of "Relay Output Type", options as follows:</p> <ul style="list-style-type: none"> <li>Normally open: when the relay is normal without alarm, it is in closed status; when alarm occurs, relay is in open status;</li> <li>Normally closed: when the relay is normal without alarm, it is in open status; when alarm occurs, relay is in closed status.</li> </ul>
<b>Power supply alarm setting</b>	<b>The power supply alarm setting bar</b>
Power	Display the power supply number of the device.
Alarm Settings	<p>Configure the alarm functions of the power supply. Options:</p> <ul style="list-style-type: none"> <li>Enable;</li> <li>Disable;</li> </ul> <p>Note:</p> <ul style="list-style-type: none"> <li>DC provides 2 power supplies (AC without power supply alarm), when one power supply goes wrong, another power supply can supply electricity soon, dual power supply hot standby is supported.</li> <li>After enabling power supply alarm, the device will output alarm signal to hint abnormal operation of power supply when power supply runs abnormally.</li> </ul>
Power status	<p>Display current state of power supply:</p> <ul style="list-style-type: none"> <li>Fault;</li> <li>Normal.</li> </ul>
<b>Port Alarm Settings</b>	<b>Port events column</b>
Port	Displays the port number of the device.
Alarm Settings	<p>Configure the port alarm function. Options:</p> <ul style="list-style-type: none"> <li>Enable;</li> <li>Disable;</li> </ul> <p>Description</p> <p>After enabling port alarm, when the port is in abnormal status, such as connection or disconnection, the device will output a signal to hint the abnormal operation of the device.</p>
Link status	<p>Display port connection status of the device:</p> <ul style="list-style-type: none"> <li>Unlink</li> <li>Connected.</li> </ul>

## Instance Alarm Settings

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

### Operation Steps

**Step 1** Log into Web configuration interface.

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

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

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

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

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

**Step 6** Click "Apply".

**Step 7** End.



# 10 Port Statistics

---

## 10.1 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 packet	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	263	678	164	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	0	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
G3	0	0	0	0	0	0	0	0	0	0
G4	0	0	0	0	0	0	0	0	0	0

Main elements configuration description of received frames statistics interface:

Interface Element	Description
Unicast packet	Number of port received data packets whose address is unicast address.
Multicast packet	Number of port received data packets whose address is multicast address.
Broadcast packet	Number of port received data packets whose address is broadcast address.
Discard packet	Number of port received data packets which are normal but dropped due to security control.
Pause frame	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.
runts	Number of port received data packets whose length is less than 64 bytes, including the length of FCS.
Jumbo frame	Number of port received data packets whose length is more

Interface Element		Description
		than 1518 or 1522 (enable VLAN) bytes, including the length of FCS.
Erroneous short frame	ultra	Number of port received data packets whose length is less than 64 bytes, including the length of FCS.
Erroneous long frame	super	Number of port received data packets whose length is more than 1522 bytes, including the incorrect or deficient FCS.
Wrong frame	normal	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 packet	Multicast packet	Broadcast packet	Drop packet	Pause frame	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	369	0	3	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	0	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
G3	0	0	0	0	0	0	0	0	0	0
G4	0	0	0	0	0	0	0	0	0	0

Main elements configuration description of transmitted frames statistics interface:

Interface Element	Description
Unicast packet	Number of port transmitted data packets whose address is unicast address.
Multicast packet	Number of port transmitted data packets whose address is multicast address.
Broadcast packet	Number of port transmitted data packets whose address is broadcast address.
Drop packet	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 frame	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.
Collision	Collision frequency during port data transmission.
Multiple Collision	Number of successfully transmitted data packets with the

Interface Element	Description
	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 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	343212	121405	822	730	173	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	0	0	0	0	0	0
G1	0	0	0	0	0	0
G2	0	0	0	0	0	0
G3	0	0	0	0	0	0
G4	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.
Clear	Clear the counting of statistics frames.

## 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:

Number	MAC Address	Type	Port
--------	-------------	------	------

Main elements configuration description of MAC address table interface:

Interface Element	Description
Address display type	MAC address type: <ul style="list-style-type: none"> <li>Port: display MAC address information of the designated port.</li> <li>Auto: automatically display MAC address information of all ports.</li> </ul>
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	The total bytes of all data packets received by the port.



#### Note

- The address in this device calculates indexes according to the MAC address of the switch, so the VLAN values displayed in all MAC are 0;
- 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

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

### Function Description

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

### Operation Path

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

### Interface Description

Port mirror interface as follows:

Port Mirror		<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
<b>Ingress data mirror</b>			
Mirror Port	01- <input checked="" type="checkbox"/> 02- <input type="checkbox"/> 03- <input type="checkbox"/> 04- <input type="checkbox"/> 05- <input type="checkbox"/> 06- <input type="checkbox"/> 07- <input type="checkbox"/> 08- <input type="checkbox"/> 09- <input type="checkbox"/> 10- <input type="checkbox"/> 11- <input type="checkbox"/> 12- <input type="checkbox"/> 13- <input type="checkbox"/> 14- <input type="checkbox"/>		
	15- <input type="checkbox"/> 16- <input type="checkbox"/> 17- <input type="checkbox"/> 18- <input type="checkbox"/> 19- <input type="checkbox"/> 20- <input type="checkbox"/> 21- <input type="checkbox"/> 22- <input type="checkbox"/> 23- <input type="checkbox"/> 24- <input type="checkbox"/> G1- <input type="checkbox"/> G2- <input type="checkbox"/> G3- <input type="checkbox"/> G4- <input type="checkbox"/>		
<b>Egress data mirror</b>			
Mirror Port	01- <input type="checkbox"/> 02- <input checked="" type="checkbox"/> 03- <input type="checkbox"/> 04- <input type="checkbox"/> 05- <input type="checkbox"/> 06- <input type="checkbox"/> 07- <input type="checkbox"/> 08- <input type="checkbox"/> 09- <input type="checkbox"/> 10- <input type="checkbox"/> 11- <input type="checkbox"/> 12- <input type="checkbox"/> 13- <input type="checkbox"/> 14- <input type="checkbox"/>		
	15- <input type="checkbox"/> 16- <input type="checkbox"/> 17- <input type="checkbox"/> 18- <input type="checkbox"/> 19- <input type="checkbox"/> 20- <input type="checkbox"/> 21- <input type="checkbox"/> 22- <input type="checkbox"/> 23- <input type="checkbox"/> 24- <input type="checkbox"/> G1- <input type="checkbox"/> G2- <input type="checkbox"/> G3- <input type="checkbox"/> G4- <input type="checkbox"/>		
<b>Collect Port</b>			
Collect Port	01- <input type="radio"/> 02- <input type="radio"/> 03- <input checked="" type="radio"/> 04- <input type="radio"/> 05- <input type="radio"/> 06- <input type="radio"/> 07- <input type="radio"/> 08- <input type="radio"/> 09- <input type="radio"/> 10- <input type="radio"/> 11- <input type="radio"/> 12- <input type="radio"/> 13- <input type="radio"/> 14- <input type="radio"/>		
	15- <input type="radio"/> 16- <input type="radio"/> 17- <input type="radio"/> 18- <input type="radio"/> 19- <input type="radio"/> 20- <input type="radio"/> 21- <input type="radio"/> 22- <input type="radio"/> 23- <input type="radio"/> 24- <input type="radio"/> G1- <input type="radio"/> G2- <input type="radio"/> G3- <input type="radio"/> G4- <input type="radio"/>		
		<input type="button" value="Apply"/>	<input type="button" value="Cancel"/>



The main element configuration description of port mirror interface:

Interface Element	Description
Port Mirror	Setting port mirror function, options are: <ul style="list-style-type: none"> <li>• Enable;</li> <li>• Disable;</li> </ul>
<b>Ingress data mirror</b>	<b>The configuration bar of ingress data mirror</b>
Mirror port	Choose the ingress data port that needs mirroring.
<b>Egress data mirror</b>	<b>The configuration bar of egress data mirror</b>
Mirror port	Choose the egress data port that needs mirroring.
<b>Collect port</b>	<b>The configuration bar of collect port</b>
Collect port	Configure the collect ports with ingress/egress data mirroring

#### For instance: port mirror configuration

For example: use port 5 to collect ingress data of port 1, port 2 and port 3, and egress data of port 4 at the same time.

#### Operating Steps

- Step 1** Log into Web configuration interface.
- Step 2** Choose "Main Menu > Diagnosis > Mirror".
- Step 3** On the "Mirror" page, choose "enable" in the "port mirror".
- Step 4** In the area of "ingress data mirror", choose "1", "2" and "3" as "mirror port".
- Step 5** In the area of "egress data mirror", choose "4" as "mirror port".
- Step 6** In the area of "collect port", choose "5" as "mirror port".
- 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:

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:

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.
Network Diagnosis	<p>After filling in the destination, packet size, packet number and packet interval, user can click "Start" to initiate test.</p> <p>Note: 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.</p>

# 12 System Management

## 12.1 Log Information

### Function Description

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

### Operation Path

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

### Interface Description

Log information interface as follows:

Index	Type	Time	Event
001	Operation information	2019/9/29 上午9:15:03	Enabling Ping Network Diagnosis
002	Operation information	2019/9/29 上午9:09:49	Successful landing system
003	Connection information	2019/9/29 上午8:44:56	The first power supply is back to normal
004	Connection information	2019/9/29 上午8:44:56	port14Go online
005	Boot information	2019/9/29 上午8:44:50	Switch Test pass
006	Boot information	2019/9/29 上午8:44:50	Flash Test pass
007	Boot information	2019/9/29 上午8:44:50	SRAM Test pass
008	Boot information	2019/9/29 上午8:44:50	RTC Test pass
009	Operation information	2019/9/29 上午8:44:50	Cold Start of System

Main elements configuration description of log information interface:

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

## 12.2 SNTP Configuration

### Function Description

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

### Operation Path

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

### Interface Description

SNTP configuration interface is as follows:

Main elements configuration description of time configuration interface:

Interface Element	Description
SNTP	Enable or disable time configuration.
Time zone	Selection of standard time zone for countries in the world.
NTP Server	Host name or IP address that provides NTP timing and time service for user.
System Time	Time of the device, after powering on, press “Tuesday, January 1, 2008” to manually or automatically initiate NTP

Interface Element	Description
	updating.
PC Time	PC time of the guest, the time display isn't relative to the switch.



Note

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

## 12.3 Device Address

### IP Address

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

Network Type	Address Range	Usable IP Network Range
A	0.0.0.0~126.255.255.255	1.0.0.0~126.0.0.0
B	128.0.0.0~191.255.255.255	128.0.0.0~191.254.0.0
C	192.0.0.0~223.255.255.255	192.0.0.0~223.255.254.0
D	224.0.0.0~239.255.255.255	-
E	240.0.0.0~246.255.255.255	-
Other addresses	255.255.255.255	255.255.255.255



Note

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

### Subnet Mask

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

### **Gateway**

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

### **DNS server**

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

## **Function Description**

On the page of "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 & Reboot".

## **Interface Description**

Device address interface as follows:

**Network Setting**

☒ Use the following IP address
 ☐ Automatically obtain IP address

IP Address:   
 Subnet Mask:   
 Gateway:

☒ Use the following DNS server address
 ☐ Automatically obtain DNS server address

DNSServer:

Apply Cancel

---

**Device Reboot**

Reboot

Main elements configuration description of device address interface:

Interface Element	Description
<b>Device Address</b>	<b>Configuration column of the device address</b>
Use the following IP address	It represents that manually enabling configured IP address, netmask and gateway address.
Automatically obtain DNS server address	It represents that enabling the system automatic acquisition of the IP address of the device.
IP Address	Configure IP address of the device. Note Default configured IP address is 192.168.1.254.
Subnet Mask	Configure subnet mask of the device. Description Default configured subnet mask is 255.255.255.0.
Gateway	Configure gateway address of the device. Note Default configured gateway address is 192.168.1.1.
Use the following DNS server address	Configure the acquisition form of DNS server address as manual configuration. Note Default configured DNS server address is 202.96.134.133.
Automatically obtain DNS server address	Configure the acquisition form of DNS server address as automatic acquisition. Note: When IP address is manual configuration, this option becomes gray and is not optional.
DNS server	Configure DNS server address.
Set	Save the device address information. Note: Some devices may automatically reboot after



Interface Element	Description
	configuration, and the configuration will take effect after rebooting.
Cancel	Cancel the modification of device address information.
<b>Device reboot</b>	<b>Configuration column of the device reboot</b>
Reboot	Reboot the device.

### For Example: Manual Configuration

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

### Operation Steps

- Step 1** Log into Web configuration interface.
- Step 2** Select “Main Menu > Basic Settings > Network & Reboot”.
- Step 3** On the “Network Settings” region of displayed page of “Device Management”, select “Use the following IP address”.
1. Enter “192.168.5.88” in the textbox of “IP Address”.
  2. Enter “192.168.5.1” in the textbox of “Gateway”.
- Step 4** Click “Apply”, system will automatically save the configuration.
- Step 5** End.

### For Example: Automatic Acquisition of IP

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

### Operation Steps

- Step 1** Log into Web configuration interface.
- Step 2** Select “Main Menu > Basic Settings > Network & Reboot”.
- Step 3** On the “Network Settings” region of displayed page of “Device Management”, select “Automatically obtain IP address”.
- Step 4** Click “Apply”, system will automatically save the configuration.
- Step 5** End.

## 12.4 System information;

### Function Description

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

- Device model;
- Device name;
- Device description;
- 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	11
Contact Method	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Main element configuration instructions in System Information interface.

Interface Element	Description
Model	Configure the device model.
Name	Configure the device name to identify each device in the network.
Description	Configure the summary description of the device.
Serial number	Configure the device number. Note: <ul style="list-style-type: none"> <li>The number can be used for describing the installation position of the device;</li> <li>The number length shouldn't be more than 30 bytes.</li> </ul>
Contact method	Configure the contact Information of the maintenance personnel of the device. Note: <ul style="list-style-type: none"> <li>Support the entering of Chinese characters, English letters, number, characters like “-”, “_”, “@”, “,”, “.”;</li> <li>The entering of blank space is not supported.</li> </ul>

## For Example: Device Information Configuration

For example: Configure the device according to following information:

- “Module” is “ManagedSwitch1”;

- “Name” is “IndustrialSwitch”;
- “Description” is “8ports”.

### Operation Steps

**Step 1** Log into Web configuration interface.

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

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

1. Enter “Module” as “ManagedSwitch1”;
2. Enter “Name” as “IndustrialSwitch”;
3. Enter “Description” as “8ports”.

**Step 4** Click “Apply” to save the configuration.

**Step 5** End.

## 12.5 File Management

### Function Description

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

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

### Operation Path

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

### Interface Description

System File interface as follow:

The screenshot displays the 'System File' interface with three main sections:

- Factory Default:** Contains a 'Factory Default' label and a 'Start' button.
- Update Configuration File from Local PC:** Contains a 'Download Configuration' label with a 'Download' button, and an 'Upload Configuration' label with a text input field, a 'Browse...' button, and an 'Upload' button.
- Upgrade Firmware from Local PC:** Contains an 'Upgrade Firmware' label with a text input field, a 'Browse...' button, and an 'Upgrade' button.

Main element configuration instructions in System File interface.

Interface Element	Description
Factory Default	Configuration column of restore factory defaults

Factory Default	Restore factory defaults of the switch. Note: Restore factory defaults will cause all devices to be in the factory status, default IP address is "192.168.1.254".
<b>Update Configuration File from Local PC</b>	<b>Configuration column of configuration files</b>
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.
<b>Upgrade firmware from local PC</b>	<b>Configuration column of system upgrade</b>
Upgrade Firmware	Upgrade operating system of the switch.

**Warning**

In the process of uploading configuration files or upgrading software, please don't click or configure other WEB page of the switch, or reboot the switch; otherwise, it will lead to failure of configuration files uploading or software upgrading, or even cause system breakdown of the switch.

**Example: Download Configuration Files**

For example: Download configuration files.

**Operation Steps**

- Step 1** Log into Web configuration interface.
- Step 2** Select "Main Menu > System Management > File Management".
- Step 3** On the region of "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 into 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 Log Off

### Function Description

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

### Operation Path

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

### Interface Description

System logout interface as follows:



Main elements configuration description of system logout interface:

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

**For example: Log off and change administrator to login**

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

**Operation Steps**

- Step 1** Log into Web configuration interface.
- Step 2** Select “Main Menu > Basic Settings > System log off”.
- Step 3** Click “OK” on the displayed page of “System log off”.
- 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 in the pop-up dialog box of "messages from the webpage", click "OK".
- Step 7** Login successfully to the WEB interface.
- Step 8** End.

# 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. **What should I do if I forget my 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. **How to configure the device restore default setting via DIP switch?**

Turn the DIN\_Rail device's DIP switch 2 to ON position, and restore default setting after power on again. Press rack-mounted device's RTS button, and restore default setting after power on again.

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

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

**3. 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.

**4. 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.

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

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

## 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 is in alarm, the device alarm light will be on and the state of the relay will change.

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

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

## **4. 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.

