3onedata
Make network communication more reliable

IES618 Series

Managed Industrial Ethernet Switch

User Manual

Document Version: 02

Issue Date: 10/21/2019

Industrial Ethernet communication solutions experts **3onedata Co., Ltd.**

Copyright © 2019 3onedata Co., Ltd. All rights reserved.

For this manual, all rights reserved by 3onedata Co., Ltd. No company or individual is allowed to duplicate or translate this manual in any forms without written permission issued by 3onedata Co., Ltd.

Trademark statement

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

Notes

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

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

3onedata
Make network communication more reliable

Please scan our QR code for more details

Embedded Industrial Ethernet Switch Modules

Embedded Serial Device Server Modules

Industry-specialized Products
(Rail Transit, Power, Smart City, Pipe Gallery…)

3onedata
Make network communication more reliable

Honor·Quality·Service

Layer 2 (Unmanaged) Managed Industrial Ethernet Switch

Layer 3 Managed Industrial Ethernet Switch

Industrial PoE Switch

BlueEyes pro

BlueEyes Pro Management Software

VSP Virtual Serial Port Management Software

SNMP Management Software

Modbus Gateway
Serial Device Server
Media Converter
CAN Device Server
Interface Converter

Industrial Wireless Products

3onedata Co., Ltd.

Headquarter address:	3/B, Zone 1, Baiwangxin High Technology Industrial Park, Song Bai Road, Nanshan District, Shenzhen, 518108, China
Technology support:	tech-support@3onedata.com
Service hotline:	+86-400-880-4496
E-mail:	sales@3onedata.com
Fax:	+86-0755-26703485
Website:	http://www.3onedata.com

Preface

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

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

Note

The manual print screen reference model is IES618-4F-2P (4 100M fiber ports + 4 100M copper ports, 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 follow:

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

Text Format Convention

Format	Description
“”	Words with "" represent the interface words. e.g.: "The port number".
>	Multiple paths are separated by the symbol ‘>’. For example, open local connection path description: open "Control Panel > Network Connection > Local Connection".
Light Blue Font	It represents the words clicked to achieve hyperlink. The font color is as follows: ‘Light Blue’.

Icon Convention

Format	Description

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	Conduct a necessary supplements and explanations for the description of operation content.
🔑 Key	Configuration, operation, or tips for device usage.
💡 Tips	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	6/27/2013	Product release
02	10/21/2019	Software upgrade, manual optimization

Content

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	Above 256 color
Browser	Above Internet Explorer 6.0
Operating System	Windows XP Windows 7

1.2 Set the IP Address of the Computer

The switch default management as follows:

IP Setting	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.

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

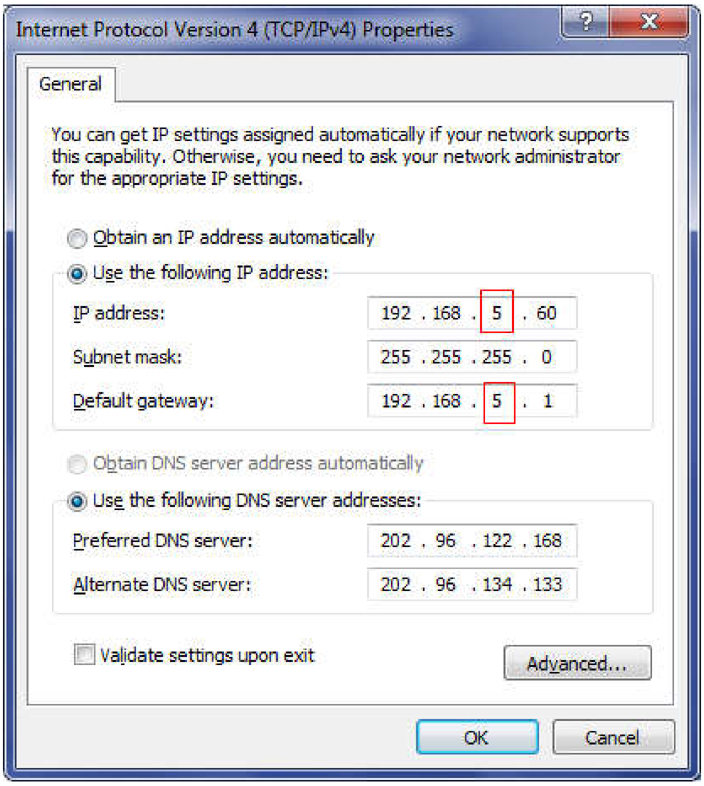
Eg: Assume that the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address to "1".

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".



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 5 . 60
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 5 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 202 . 96 . 122 . 168
Alternate DNS server: 202 . 96 . 134 . 133

□ Validate settings upon exit

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

Step 4 End.

1.3 Log in the Web Configuration Interface

Operation Steps

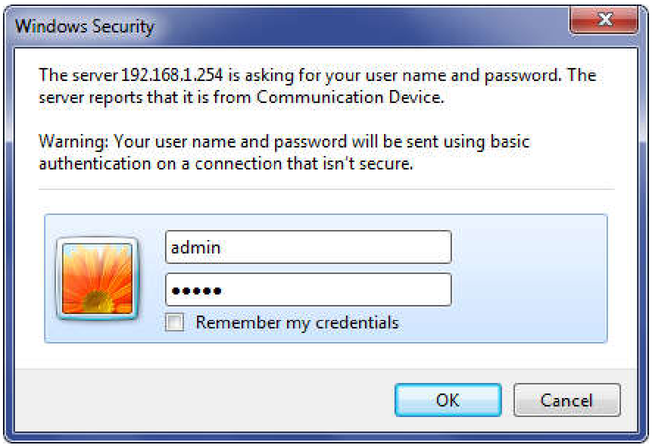
Login in the web configuration interface as follow:

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.



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

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

admin

•••••

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

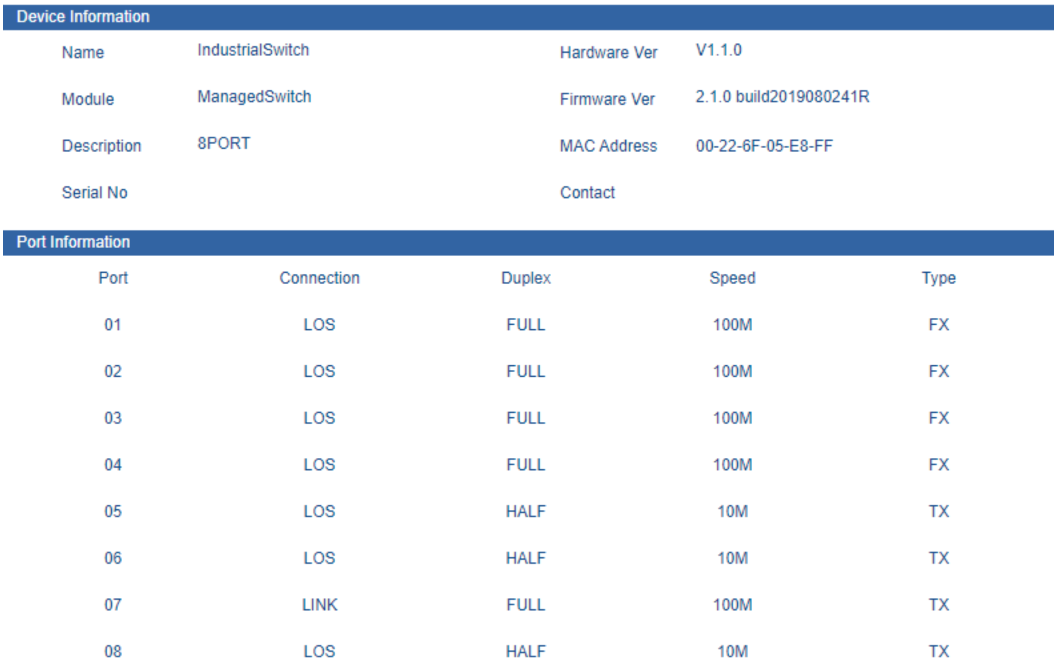
On the page of "System Information", user can check "Device Information" and "Port Information".

Operation Path

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

Interface description

Device information interface as follows:



Device Information

Name	IndustrialSwitch	Hardware Ver	V1.1.0
Module	ManagedSwitch	Firmware Ver	2.1.0 build2019080241R
Description	8PORT	MAC Address	00-22-6F-05-E8-FF
Serial No		Contact	

Port Information

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

Main elements configuration description of device information interface:

Interface Element	Description
Equipment information;	**Equipment information column.**

Interface Element	Description
Device name.	Display the device name.
Device model.	Display the device model.
Description	Display characters description of the device.
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 information.	Display the contact information of the device maintenance personnel.
Port Information	**Port information status column**
Port	Serial number of device port .
Link status	Port connection state, display state as follows: ● "LINK" represents connected port; ● "LOS" represents disconnected port.
Port state	Port work state, display state as follows: ● "HALF" represents the corresponding port is in the state of half-duplex; ● "FULL" represents corresponding port is in full duplex state.
Speed	Display the link speed of current port when it is connected.
Interface type.	Interface type. ● FX: fiber port; ● TX: copper port.

Note

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

3 Port Configuration

3.1 Port Setting

Function description

The "PoE Config" page mainly includes:

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

  Network congestion can cause packet loss, and flow control is a technology that prevents this from happening. After flow control function is configured, this device would send messages to the opposite device to notify it to stop sending messages if it has congestion. When the opposite device receives this message, it would stop sending messages to this device to avoid congestion no matter what its interface work speed is. Flow control can effectively prevent the impact on network caused by the instantaneous mass data in network to ensure the efficient and stable operation of user network.

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

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

Note

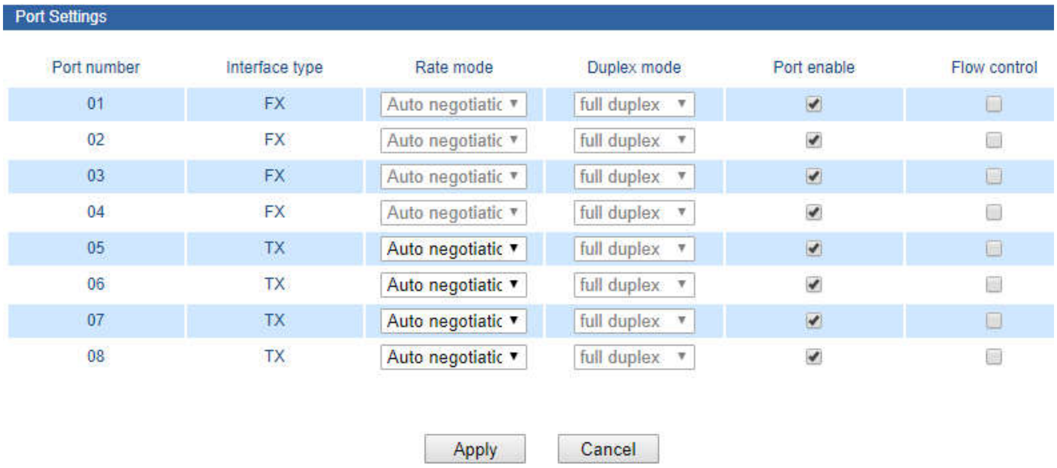
- The speed, duplex and flow control of this port take effects only when the port is enabled.
- After selecting automatic negotiation, speed and duplex will be gained via automatic negotiation.

Operation Path

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

Interface description

Port settings interface as follows:



Port Settings

Port number	Interface type	Rate mode	Duplex mode	Port enable	Flow control
01	FX	Auto negotiatic	full duplex	☑	☐
02	FX	Auto negotiatic	full duplex	☑	☐
03	FX	Auto negotiatic	full duplex	☑	☐
04	FX	Auto negotiatic	full duplex	☑	☐
05	TX	Auto negotiatic	full duplex	☑	☐
06	TX	Auto negotiatic	full duplex	☑	☐
07	TX	Auto negotiatic	full duplex	☑	☐
08	TX	Auto negotiatic	full duplex	☑	☐

Main elements configuration description of port settings interface:

Interface Element	Description
Port	Port number of the device.
Interface type.	According to the electrical properties of interface, the Ethernet interface of switch can be divided into: ● Copper port: transmit electrical signal via twisted-pair; ● Fiber port: transmit optical signal via optical fiber
Speed mode	Click the drop-down list box of “speed mode” to select port speed mode. ● Auto-negotiation: port can adjust to the transmission speed of the opposite port; ● 10M speed: the maximum supported speed is 10Mbit/s; ● 100M speed: the maximum supported speed is 100Mbit/s; Description: The copper ports of the switch are all MDI/MDIX self-adaptive ports, which support auto-negotiation.

Interface Element	Description
Duplex mode	Click the drop-down box of "duplex mode" to select the corresponding duplex mode of the port, options are as follows: ● Half-duplex: interface can only receive or send data at any time. ● Full-duplex: interface can receive and send data at the same time. Description: When the speed mode is "auto-negotiation", the port would match the duplex mode of corresponding port automatically.
Enable	Tick the check box to enable the port. Note: Unchecking the checkbox means this port is disabled and cannot forward data.
Flow control	Tick the check box to enable the flow control function of the port. ● Under full duplex mode, flow control method is IEEE 802.3x flow control. ● Under half duplex mode, flow control method is back pressure flow control.

Instance: Port Settings

for example: set port 1, port 2 and port3 as follows:

- Set port 1's "speed mode" to "auto-negotiation";
- Set port 2's "speed mode" to "100M speed", and "duplex mode" to "full duplex";
- Set port 3's "speed mode" to "10M speed", and "duplex mode" to "half duplex", and enable "flow control".

Operating steps

Step 1 Enter: "Main Menu > Port Config > Port Setting".

Step 2 Configure the parameter of port 1:

1. Check "Port Enable" checkbox.
2. Choose "automatic negotiation" as "speed mode" .

Note:

The default configuration of "speed mode" is "auto-negotiation".

Step 3 Configure the parameter of port 2:

1. Check "Port Enable" checkbox.
2. Select "100M speed" as "speed mode";
3. Choose "Full duplex" as "Duplex mode".

Step 4 Configure the parameter of port 3:

1. Check “Port Enable” checkbox.
2. Select “10M speed” as “speed mode”;
3. Choose “Half duplex” as “Duplex mode”.
4. Check “Flow control” checkbox.

Step 5 Click “Apply”.

Step 6 End.

3.2 Bandwidth Management

Function description

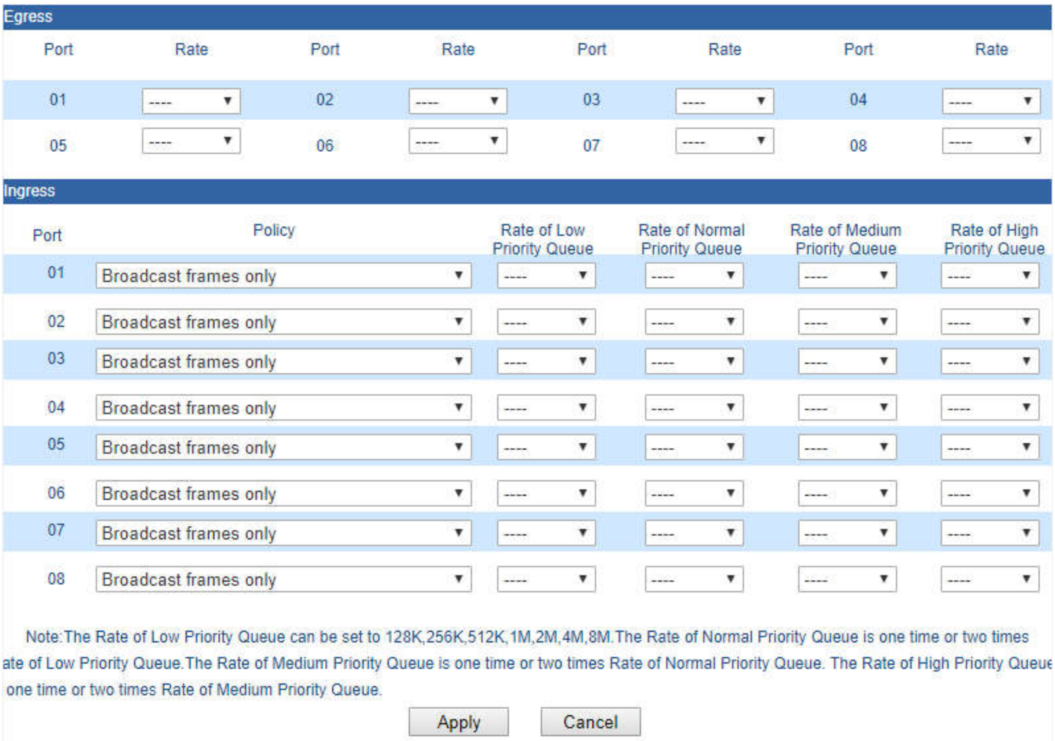
On the page of “Bandwidth Management”, the device can realize the port’s egress bandwidth settings and priority scheduling of ingress data packet.

Operation Path

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

Interface description

Bandwidth management interface as below:



Egress

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

Ingress

Port	Policy	Rate of Low Priority Queue	Rate of Normal Priority Queue	Rate of Medium Priority Queue	Rate of High Priority Queue
01	Broadcast frames only	----	----	----	----
02	Broadcast frames only	----	----	----	----
03	Broadcast frames only	----	----	----	----
04	Broadcast frames only	----	----	----	----
05	Broadcast frames only	----	----	----	----
06	Broadcast frames only	----	----	----	----
07	Broadcast frames only	----	----	----	----
08	Broadcast frames only	----	----	----	----

Note:The Rate of Low Priority Queue can be set to 128K,256K,512K,1M,2M,4M,8M.The Rate of Normal Priority Queue is one time or two times ate of Low Priority Queue.The Rate of Medium Priority Queue is one time or two times Rate of Normal Priority Queue. The Rate of High Priority Queue one time or two times Rate of Medium Priority Queue.

The main element configuration description of bandwidth management interface:

Interface Element	Description
Port	Port number of the device.
Rate	Egress bandwidth is the bandwidth when the port sends data.

	Description: “----” represents no speed limit.
Limitation Packet Type	The data packets type of receiving bandwidth needs to be limited, options of drop-down list as follows: ● All frames: all kinds of data packets; ● Broadcast, Multicast and flood unicast frames: ● Broadcast and Multicast only; ● Broadcast frames only.
Rate of Low Priority Queue	Bandwidth settings of low priority queue.
Rate of Normal Priority Queue	Bandwidth settings of normal priority queue. The value could be the same to or twice of the bandwidth with the lowest priority.
Rate of Medium Priority Queue	Bandwidth settings of medium priority queue, the value could be the same to or twice of the bandwidth of normal priority queue.
Rate of High Priority Queue	Bandwidth settings of high priority queue, the value could be the same to or twice of the bandwidth of medium priority queue.

Instance: bandwidth settings

For example:

- Configure the egress bandwidth of port 1 as “4M”.
- Configure the ingress bandwidth of port 1 as “Broadcast only”, and set the bandwidth from low to high priority as follows: 1M, 2M, 4M, 8M.

Operating steps

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

Step 2 On the region of “Egress”, choose the egress bandwidth of port 1 as “4M”.

Step 3 On the region of “Ingress”, conduct following operations on the row of port 1:

1. Choose “Broadcast frames only” as “Limitation Packet Type”;
2. Choose “Rate of Low Priority Queue” as “1M”;
3. Choose “Rate of Normal Priority Queue” as “2M”;
4. Choose “Rate of Medium Priority Queue” as “4M”;
5. Choose “Rate of High Priority Queue” as “8M”.

Step 4 Click “Apply”.

Step 5 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.

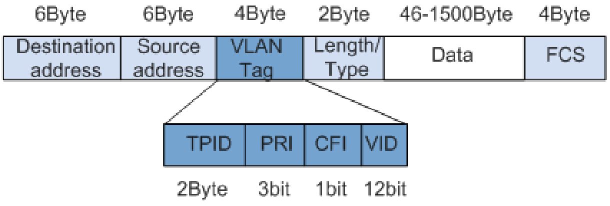
- Limit the broadcast domain;
- Increase the security of LAN;
- Improve the network stability;
- Flexibility construct virtual working team.

Port VLAN

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

IEEE802.1Q VLAN

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



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

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

Function description

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

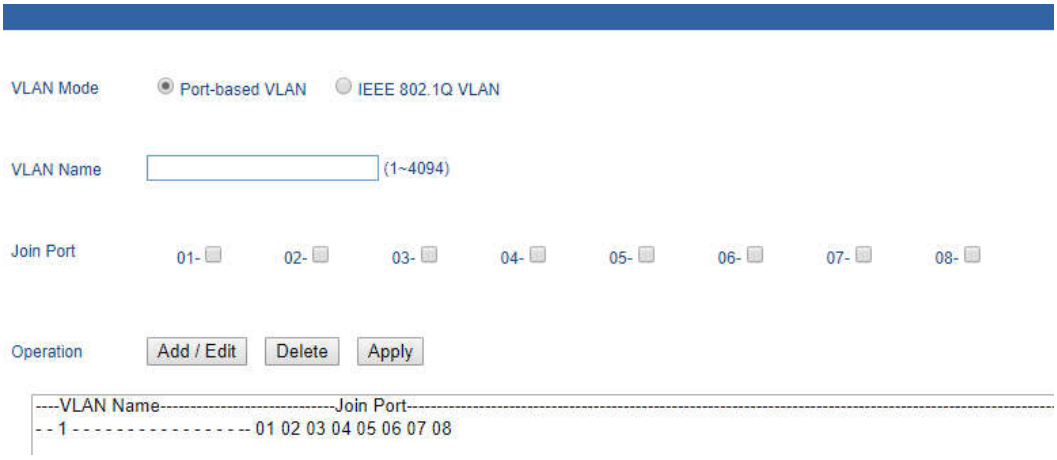
- Configure port type:
- Configure the port PVID;
- Create VLAN entry;
- Configure the port member type.

Operation Path

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

Interface Description 1: Port-based VLAN

Port-based VLAN interface as follows:



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

VLAN Name (1~4094)

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

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

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

Interface Element	Description
VLAN Mode	Choose VLAN type, options are: ● Port-based VLAN ● IEEE 802.1Q VLAN
VLAN name	Enter VLAN number in digital form. Description: Input range is 1~4094.
Port	Choose VLAN member.

Interface Element	Description
Operation	Add/edit, delete or save VLAN configuration information.

Instance: create port-based VLAN.

The steps of configuring port-based VLAN:

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

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

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

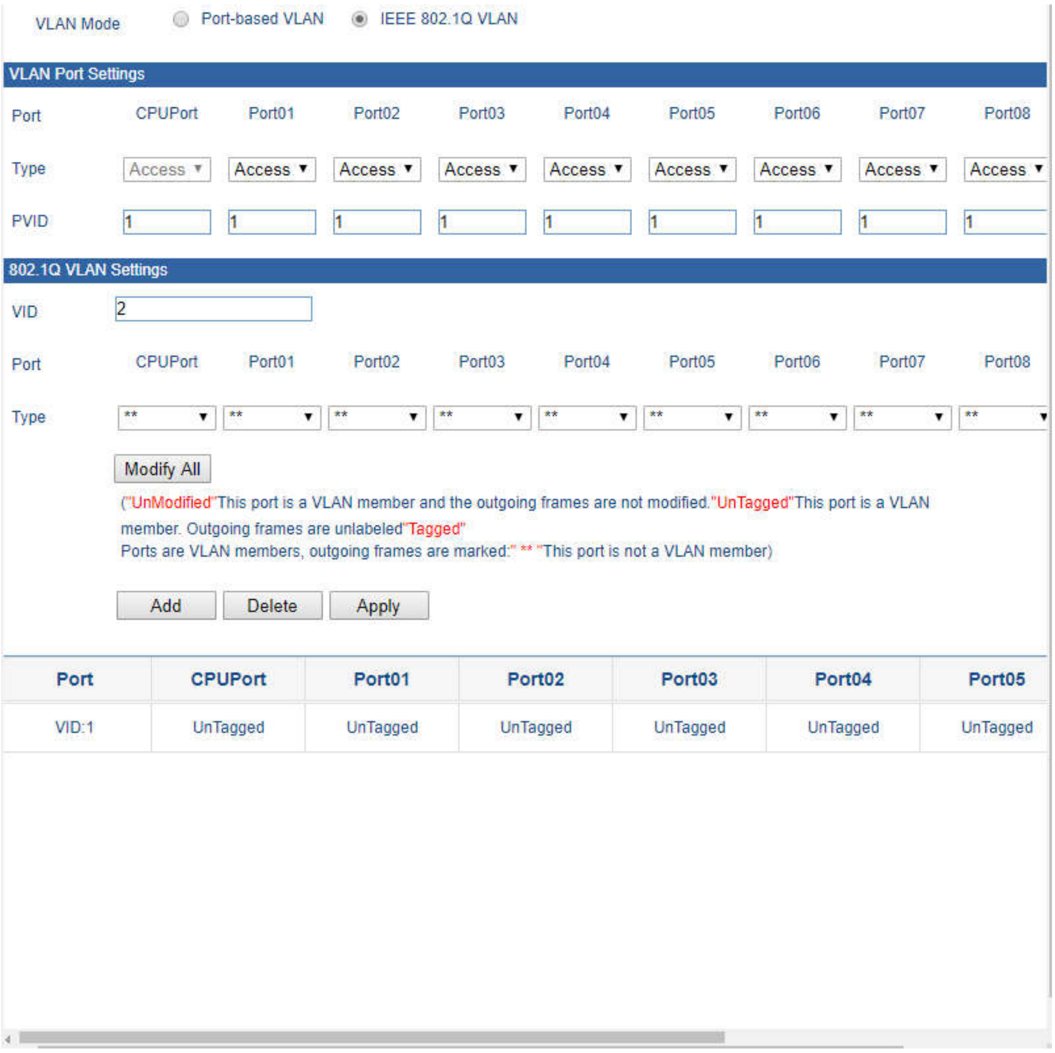
Step 4 Select VLAN member on the check box of “Join Port”, such as select port 2 and port 3.

Step 5 Click “Add/Edit”.

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

Interface Description: VLAN based on 802.1Q

Interface screenshot of VLAN based on 802.1Q as follows:



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

VLAN Port Settings

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

802.1Q VLAN Settings

VID 2

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

Modify All

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

Add Delete Apply

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

Main elements configuration descriptions of VLAN interface:

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

Interface Element	Description
	• If the port type is "access", PVID will replace the "VLAN ID" fields in the message. • If the port type is "trunk" and message is untagged, PVID will replace the "VLAN ID" fields in the message. • If the port type is "trunk" and message is tagged, the "VLAN ID" fields in the message will be reserved.
802.1Q VLAN Settings	**802.1Q VLAN Entry Settings Column**
VID	Port forwarding rule number, value range is 1-4094. Description: As for two ports that belong to the same VID; two ports with the same "VLAN ID" can communicate with each other.
Member type	There are three types of "VLAN ID" for data frames sent out by the port: ● Unmodify: when the data frame is sent out from the port, it will recover the "VLAN ID" of accessing to the switch. ● Untagged: remove the "VLAN ID" fields when the data frame is sent out from the port, ● Tagged: reserve "VLAN ID" fields when the data frame is sent out from the port.
Modify All	Quickly and simultaneously modify all member types.
Add	Add configured VLAN to VLAN member list.
Delete	Delete a VLAN item in the selected member list.
Save configuration	Apply VLAN configuration information.

VLAN configuration operations are introduced from the following five aspects:

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

Example: Create IEEE 802.1Q VLAN

Create a new IEEE 802.1Q VLAN.

Operating steps

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

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

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

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

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

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

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

Step 8 End.

Note

VLAN configuration will take effect after rebooting.

Example: Modify IEEE 802.1Q VLAN

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

Operating steps

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

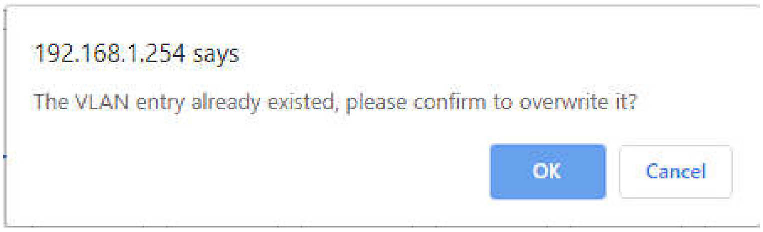
Step 2 In the column of "802.1Q VLAN Settings", click a VLAN entry to be modified in the "Port", such as VLAN1. And then the type of VLAN1 will display in the option of current VLAN entry settings.

Step 3 Modify the "VID" as required.

Step 4 Modify the "Type" as required.

Step 5 Click "Add" button.

Step 6 A prompt box pops up.



192.168.1.254 says

The VLAN entry already existed, please confirm to overwrite it?

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

Step 8 Click "Apply".

Step 9 Enter "Main Menu > System Management > Device Address".

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

Step 11 End.

Note

VLAN configuration will take effect after rebooting.

Example: Delete IEEE 802.1Q VLAN

The operation can delete existing VLAN

Operating steps

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

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

Step 3 Click “Delete” button.

Step 4 Click “Apply”.

Step 5 Enter “Main Menu > System Management > Device Address”.

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

Step 7 End.

Note

VLAN configuration will take effect after rebooting.

Example: IEEE 802.1Q VLAN Configuration for the Single Ring

Note

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

For example, create VLAN on the single ring composed of port 2~8, among which port 7 and port 8 are the ring network ports.

Operation steps as follows:

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

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

Description:

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

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

1. Configure the “Type” of port 7 as “Trunk”.
2. Configure the “Type” of port 8 as “Trunk”.

3. Set the “Port Type” of port 2-6 as “Access”.

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

1. Set the “PVID” of port 2-8 to “2”.

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

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

1. Set the “Member type” of port 2-6 to “Untagged”.
2. Configure the “Type” of port 7 as “Tagged”.
3. Configure the “Type” of port 8 as “Tagged”.

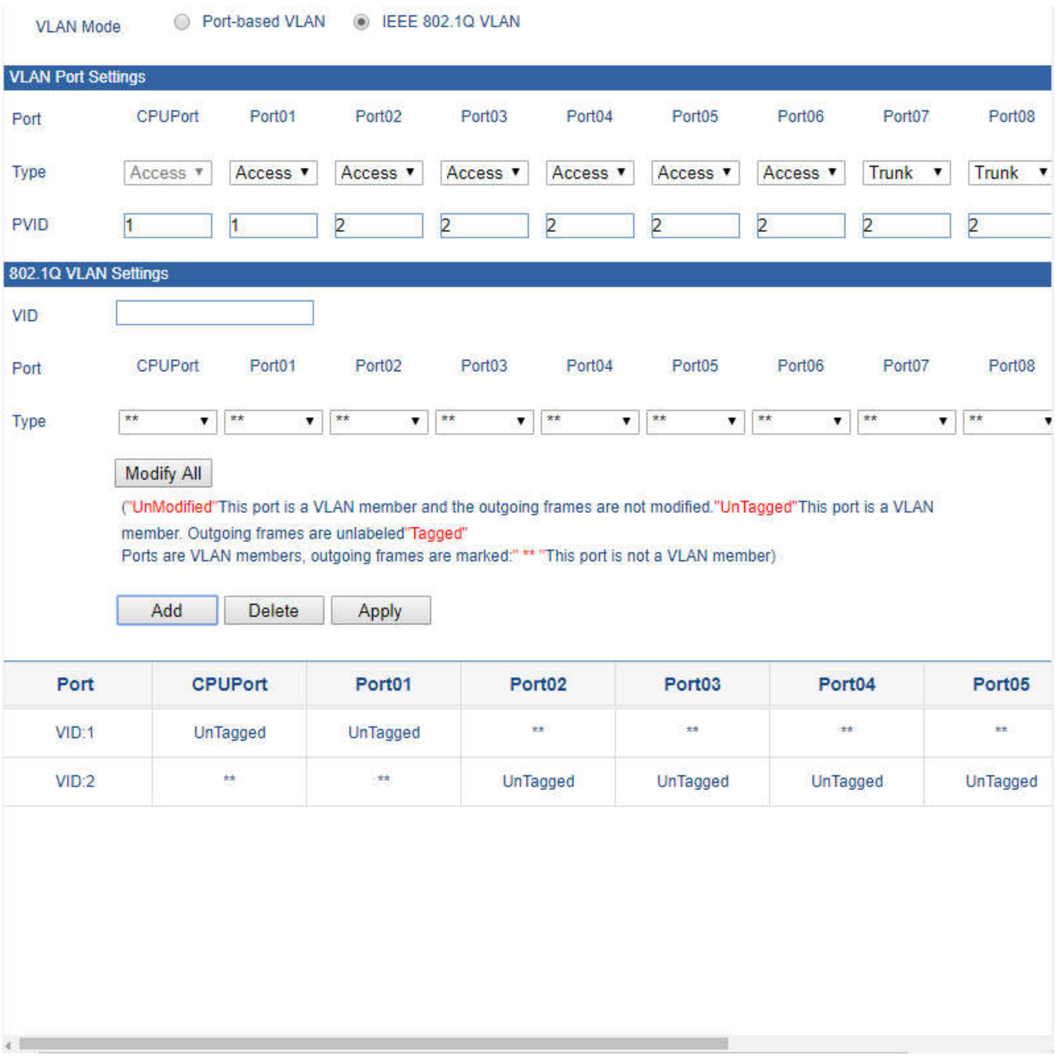
Step 7 Click “Add”.

Step 8 Click “Apply”.

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

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

Step 11 End.



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

VLAN Port Settings

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

802.1Q VLAN Settings

VID

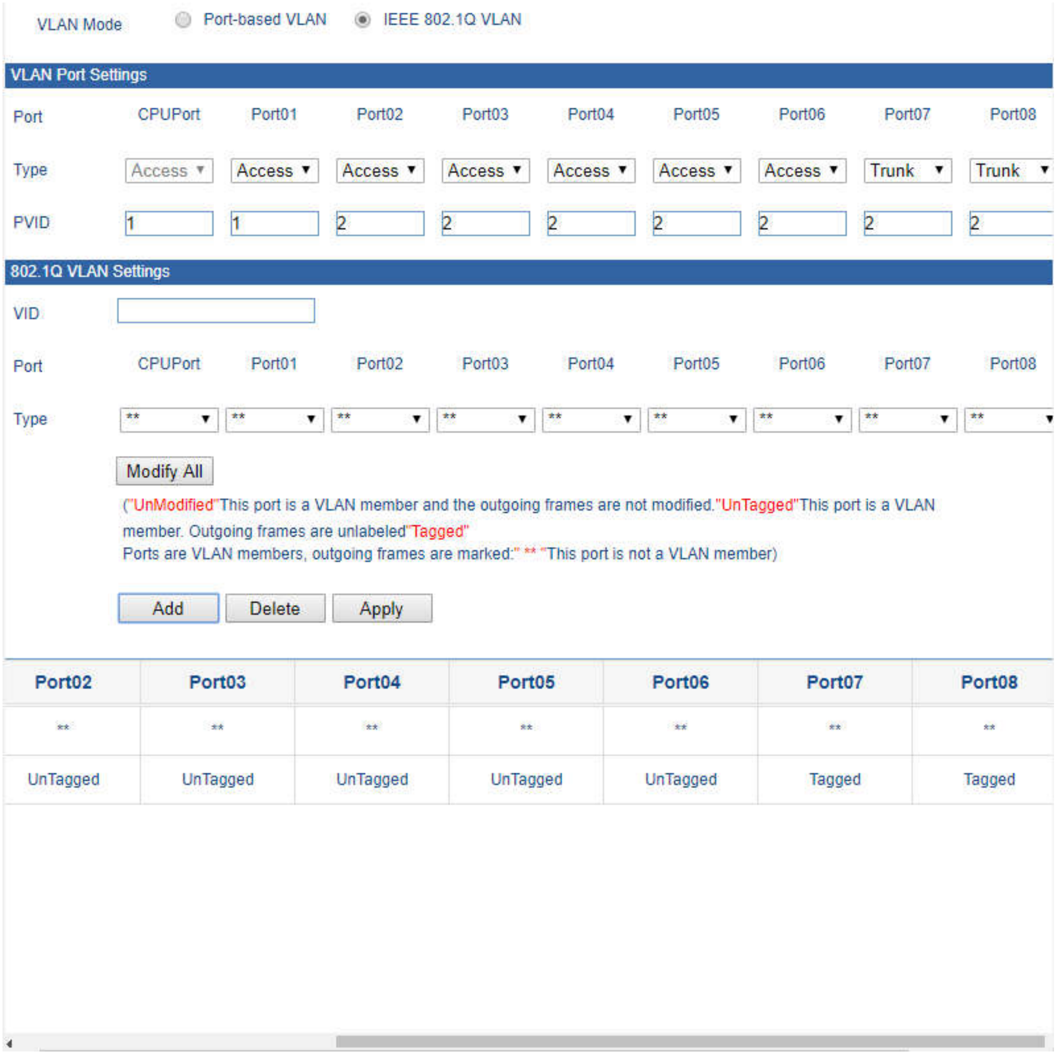
Port	CPUPort	Port01	Port02	Port03	Port04	Port05	Port06	Port07	Port08
Type	**	**	**	**	**	**	**	**	**

Modify All

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

Add Delete Apply

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



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

VLAN Port Settings

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

802.1Q VLAN Settings

VID

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

Modify All

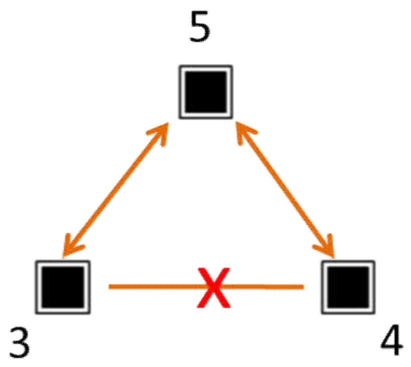
("UnModified"This port is a VLAN member and the outgoing frames are not modified."UnTagged"This port is a VLAN member. Outgoing frames are unlabeled"Tagged"
Ports are VLAN members, outgoing frames are marked:" ** "This port is not a VLAN member)

Add Delete Apply

Port02	Port03	Port04	Port05	Port06	Port07	Port08
**	**	**	**	**	**	**
UnTagged	UnTagged	UnTagged	UnTagged	UnTagged	Tagged	Tagged

Example: Typical IEEE 802.1Q VLAN Configuration

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



Instance analysis

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

Analyze the port forwarding entries design as below:

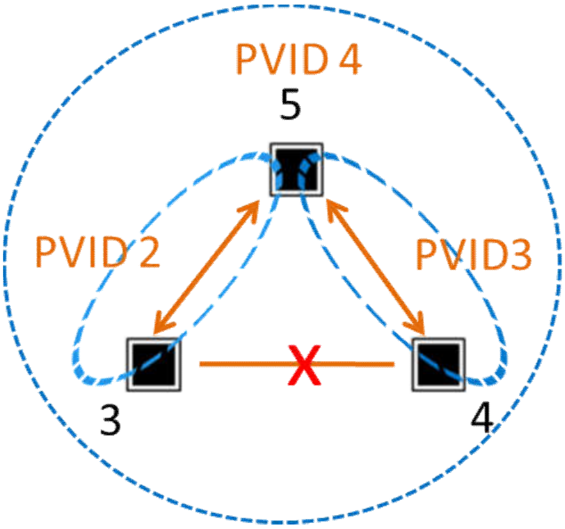
- Port3

  Port3 and Port5 can communicate with each other. Port3 forwarding entries include Port3 and Port5. Therefore, a forwarding entry PVID3 is designed, including Port 3 and Port 5. Configure the "Type" of Port 3 and Port 5 to U.
- Port4

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

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

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



Operating steps

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

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

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

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

Enter 2.

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

1. Configure the “Type” of Port3 as Untagged.
2. Configure the “Type” of Port5 as Untagged.

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

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

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

1. Configure the “Type” of Port4 as Untagged.
2. Configure the “Type” of Port5 as Untagged.

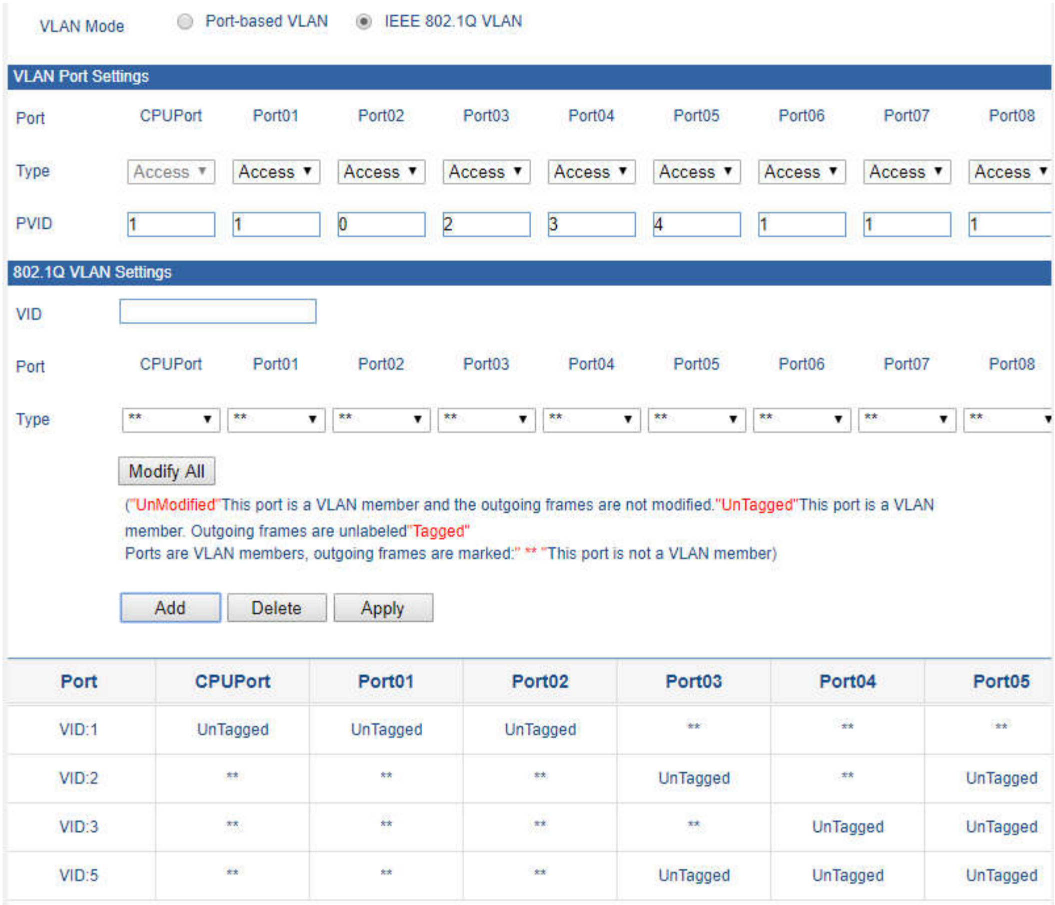
Step 9 Click “Add” button to add VLAN entry to the “Port”.

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

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

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

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



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

VLAN Port Settings

Port	CPUPort	Port01	Port02	Port03	Port04	Port05	Port06	Port07	Port08
Type	Access	Access	Access	Access	Access	Access	Access	Access	Access
PVID	1	1	0	2	3	4	1	1	1

802.1Q VLAN Settings

VID

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

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

Port	CPUPort	Port01	Port02	Port03	Port04	Port05
VID:1	UnTagged	UnTagged	UnTagged	**	**	**
VID:2	**	**	**	UnTagged	**	UnTagged
VID:3	**	**	**	**	UnTagged	UnTagged
VID:5	**	**	**	UnTagged	UnTagged	UnTagged

Step 13 Click “Apply”.

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

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

Step 16 End.

4.2 Multicast Filtering

4.2.1 IGMP snooping

IGMP Snooping (Internet Group Management Protocol Snooping) is a kind of IPv4 layer-2 multicast protocol. It maintains the outgoing information of multicast messages by snooping the multicast protocol messages transmitted between layer 3 multicast device and user host, so as to manage and control the forwarding of multicast data messages in data link layer.

After configuring IGMP Snooping, layer 2 multicast device can snoop and analyze the IGMP message between multicast user and upstream router, and create layer 2 multicast forwarding entries based on these information to control multicast data message forwarding. Which has prevented multicast data from broadcasting in layer 2 network.

The ways of IGMP Snooping processing different messages:

- IGMP General Query message: IGMP querier sends IGMP General Query messages to all hosts and routers in local network segment regularly to query which members of the multicast group are in this network segment.
- IGMP Report message: members respond with IGMP report messages when they receive IGMP IGMP General Query messages. Members send IGMP Report messages to IGMP querier proactively to declare joining this multicast group.
- IGMP Leave message: members that run IGMPv2 or IGMPv3 send IGMP leave report to notify IGMP querier that they have left some multicast groups.

Function description

On the “Multicast Filtering” page, user can:

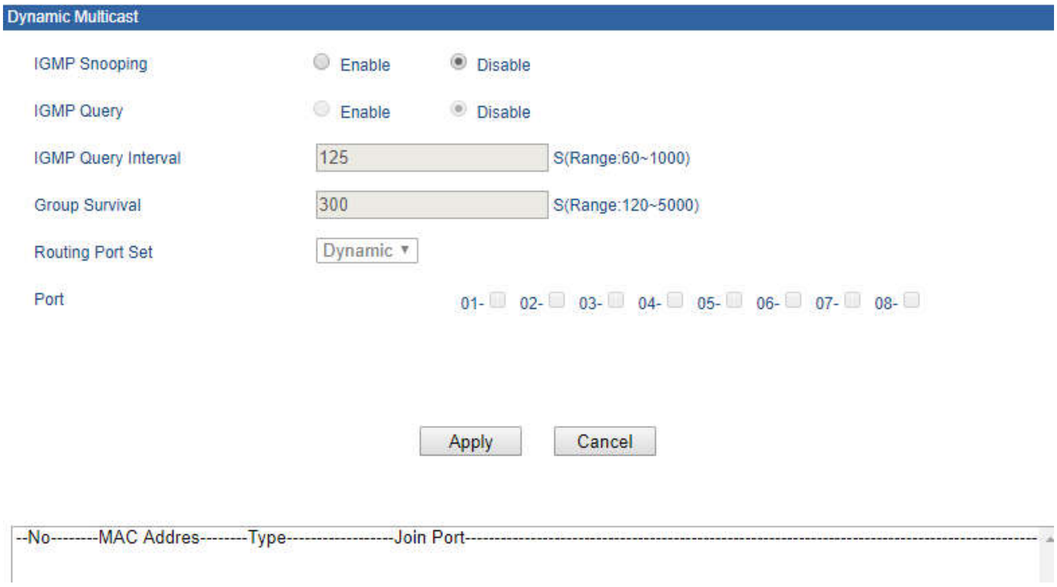
- Enable/disable IGMP snooping
- Enable/disable IGMP query
- Routing port settings

Operation Path

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

Interface description

Dynamic multicast interface as follows:



Dynamic Multicast

IGMP Snooping ○ Enable ● Disable

IGMP Query ○ Enable ● Disable

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

Group Survival 300 S(Range:120~5000)

Routing Port Set Dynamic ▾

Port 01-□ 02-□ 03-□ 04-□ 05-□ 06-□ 07-□ 08-□

Apply Cancel

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

The main element configuration description of dynamic multicast interface:

Interface Element	Description
IGMP snooping	The switch of IGMP snooping function, options are: ● Enable; ● Disable;

	Note: IGMP snooping means snooping the messages between user host and router, as well as tracking multicast information and the ports that have been applied for.
IGMP Query	The switch of IGMP query, options are: • Enable; • Disable; Note: IGMP query means that router inquiring all hosts in subnet if they join some multicast groups.
IGMP query interval	IGMP query interval, unit: second. Description: The time range that can be entered is 60-1000s.
Group survival	The maximum time that multicast members in device can survive from existence to not receiving any response. Unit: second. Description: • IGMP snooping needs to be enabled before using this function. • The time range of group survival that can be set is 120-5000s.
Routing port set	Choose the building mode of routing table, options are: • Dynamic routing, routing ports are dynamically acquired though switch. • Static routing, check the box of port in “port list” as routing port.

Note

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

4.2.2 Static Filtering

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

Function description

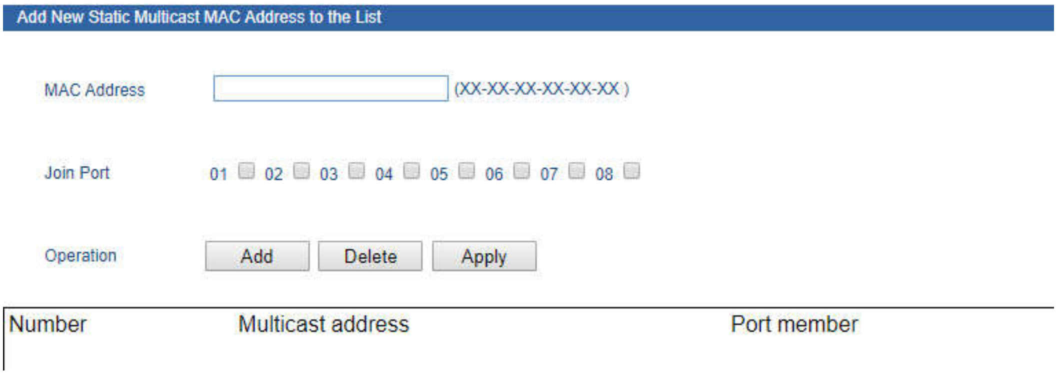
On the page of “Static Multicast”, user can configure the forwarding port list of static multicast.

Operation Path

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

Interface description

Static filtering interface as follows:



Add New Static Multicast MAC Address to the List

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

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

Operation Add Delete Apply

Number	Multicast address	Port member

Main elements configuration description of static filtering interface:

Interface Element	Description
MAC Address	Input “MAC Address”, and the format should be “XX-XX-XX-XX-XX-XX”. Description: • Low-order of the highest byte of multicast MAC address is 1, please don’t input non-multicast address. • Space and other illegal characters are not allowed for address format, otherwise alarm message will pop up.
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 "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

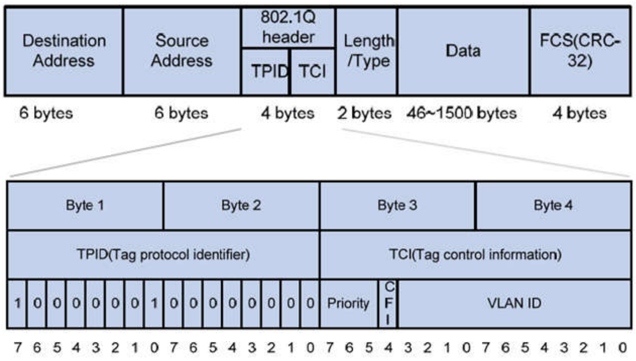
QoS(Quality of Service) is used to assess service provider's ability in meeting client service demands. As for network business, service quality includes transmission bandwidth, transfer delay, data packet loss rate and so on.

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

Priority is used to tag the priority of message transmission.

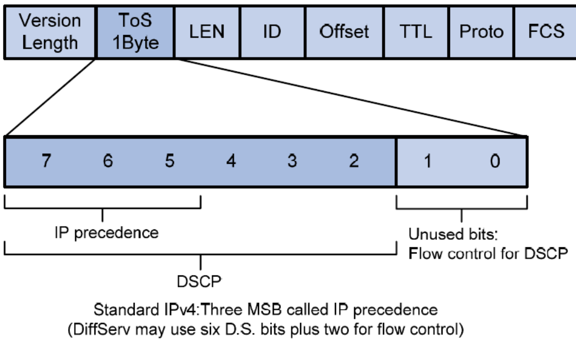
- CoS

  Ethernet has defined 8 service priorities (CoS, Class of Service) in the VLAN TAG of Ethernet frame header. 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) of IP message header is called DS (Differentiated Services) field, and DSCP priority uses the first 6 bits (0~5bit) of this field to represent, the value range is 0-63, the last 2 bits (6, 7bit) are reserved bits. The greater the priority level value, the higher the priority level.



Function description

On the page of QoS Classification, user can set:

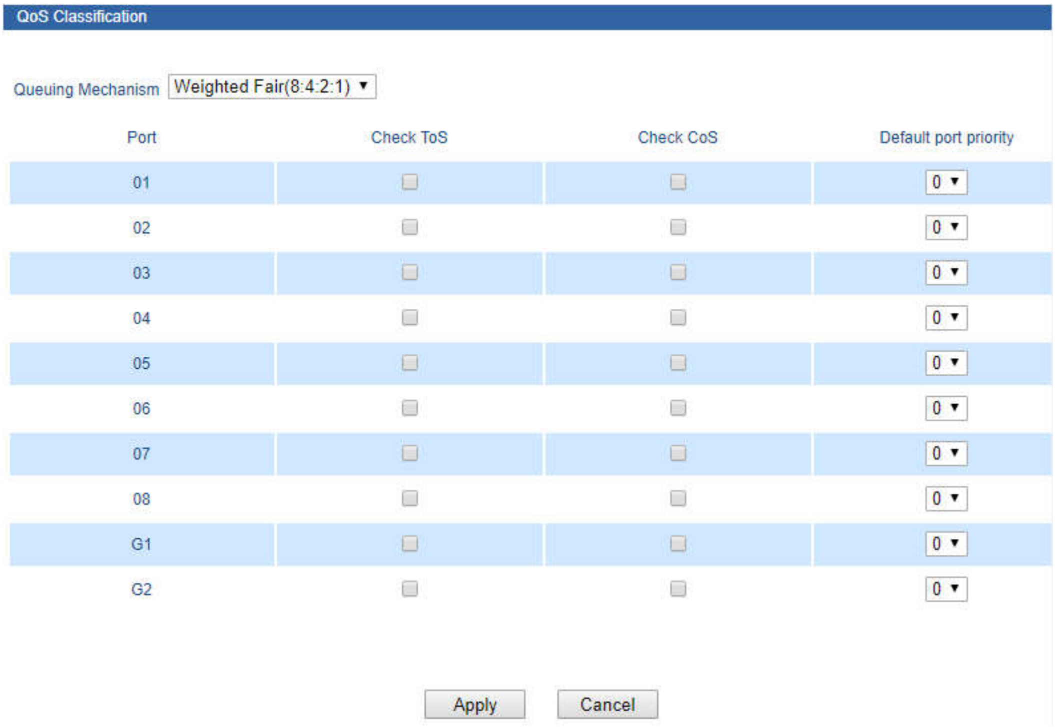
- Queuing mechanism
- Enable ToS
- Enable CoS
- Port priority

Operation Path

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

Interface description

Screenshot of QoS Classification interface:



QoS Classification

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

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

The main element configuration description of QoS classification interface:

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

Note

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

Instance: QoS configuration

For example:

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

Operating 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

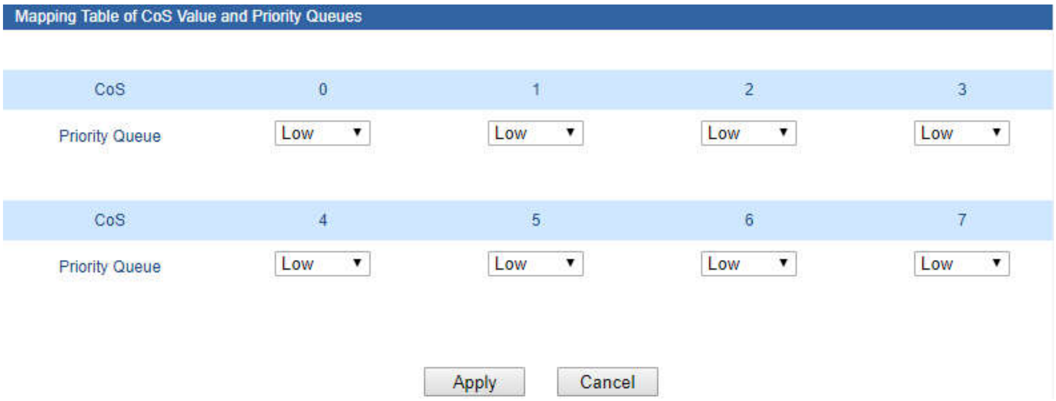
On the page of "CoS Mapping", user can configurate mapping between CoS value and priority queues.

Operation Path

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

Interface description

Screenshot of QoS Mapping interface:



Mapping Table of CoS Value and Priority Queues

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

The main element configuration description of QoS mapping interface:

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

Instance: CoS mapping configuration

For example:

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

Operating steps

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

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

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

Step 3 Click “Apply”.

Step 4 End.

5.3 ToS Mapping

Function description

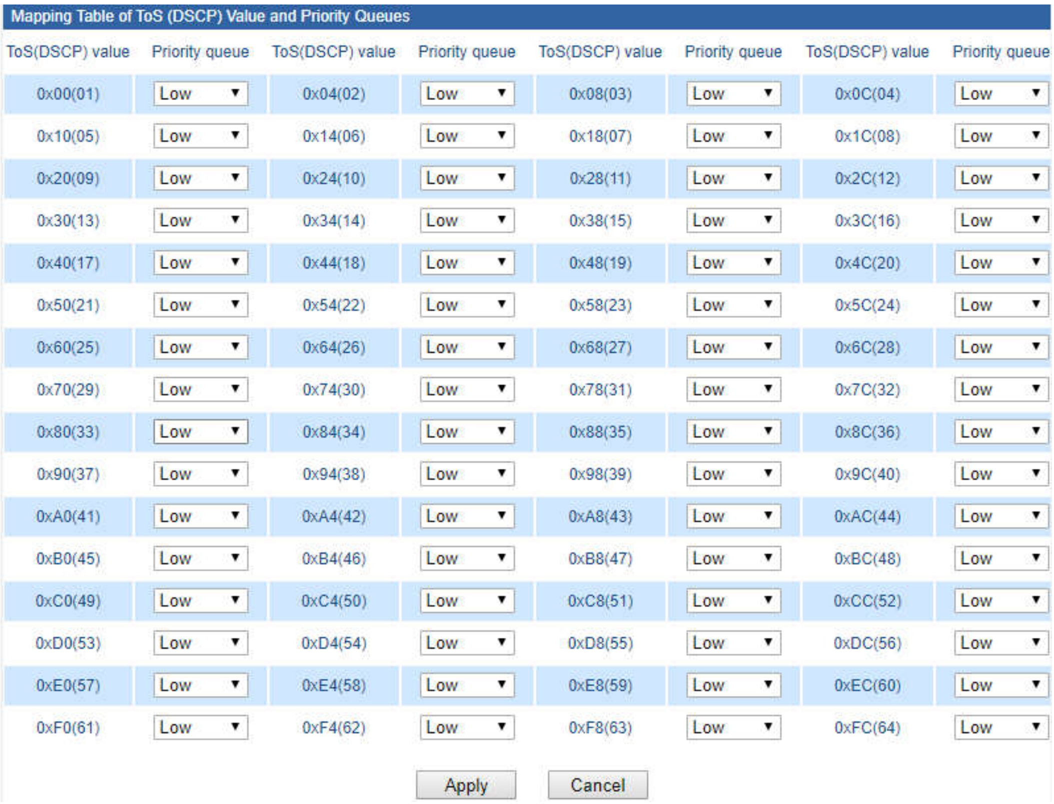
On the page of “CoS Mapping”, user can configurate mapping between CoS value and priority queue.

Operation Path

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

Interface description

Screenshot of ToS Mapping interface:



Mapping Table of ToS (DSCP) Value and Priority Queues

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

The main element configuration description of ToS mapping interface:

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

	● Low: low priority queue ● Normal: normal priority queue ● Medium: medium priority queue ● High: high priority queue

Instance: ToS mapping configuration

For example:

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

Operating 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 supported ring network protocols of switch are SW-Ring and RSTP.

- SW-Ring

  SW-Ring is a self-developed Ethernet ring network algorithm designed for highly reliable industrial control network application that requires link redundancy backup. It has Ethernet link redundancy and quick and automatic recovery from failure The Ring adopts non-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 address loop problem in switched network, STP (Spanning Tree Protocol) is put forward. 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 became 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

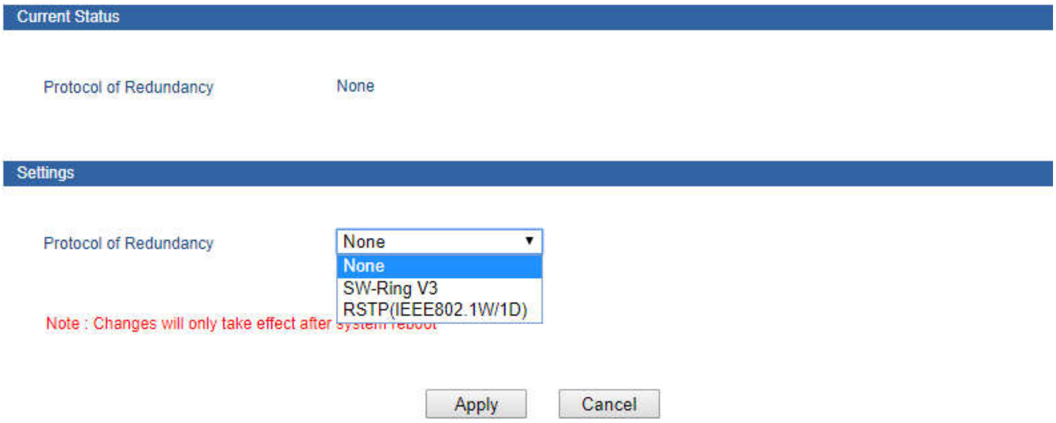
On the "Rapid ring" page, user can choose redundancy protocol and configure the ring network under this protocol quickly.

Operation Path

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

Interface description

Initial rapid ring interface as follows:



Current Status

Protocol of Redundancy: None

Settings

Protocol of Redundancy: None

Note : Changes will only take effect after system reboot

The main element configuration description of initial rapid ring interface:

Interface Element	Description

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

Function description of SW-Ring V3

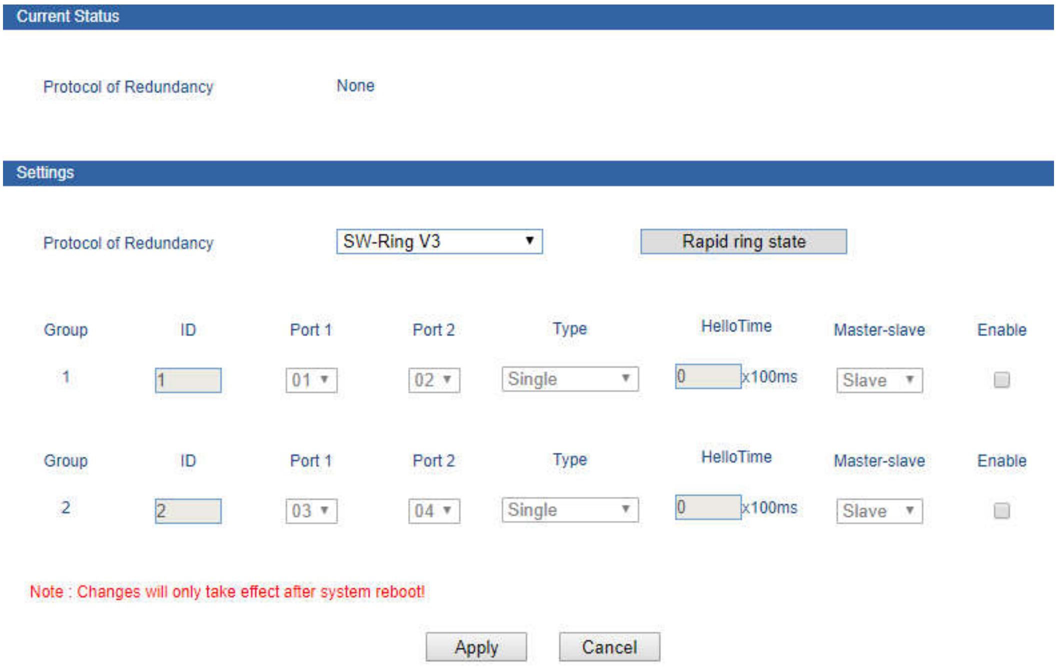
On the “rapid ring” page, user can choose Ring redundancy protocol and configure the ring network under this protocol quickly.

Operation Path

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

Interface description

SW-Ring network interface as follows:



Current Status

Protocol of Redundancy None

Settings

Protocol of Redundancy SW-Ring V3

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

Note : Changes will only take effect after system reboot!

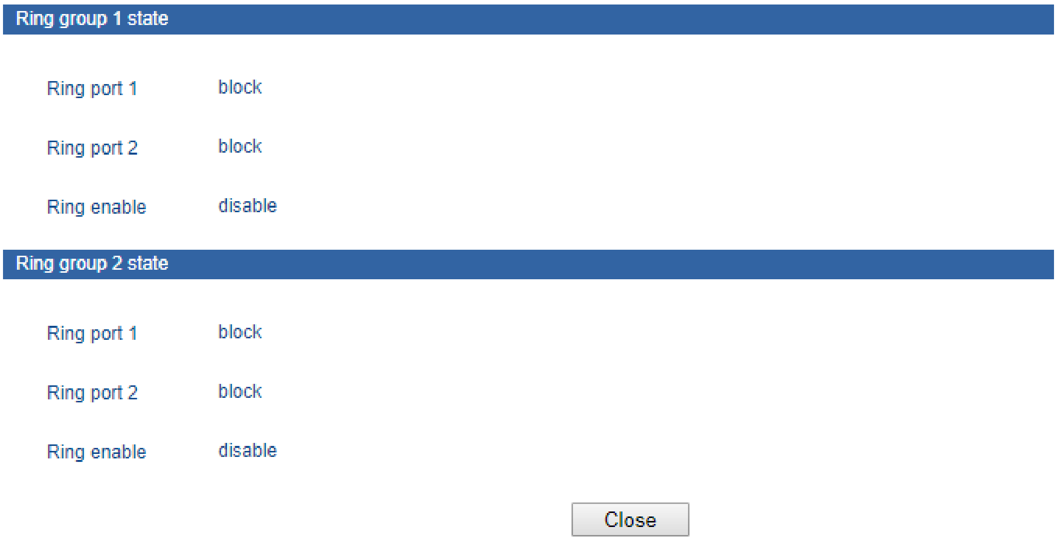
The main element configuration description of SW-Ring network interface:

Interface Element	Description

Interface Element	Description
Rapid ring state	Click “rapid ring state” to check the ring state of current ring network group configuration.
Ring group	Support Group 1-2 or Group 1-4, it means that the device supports up to 2 or 4 groups.
Network ID	When multiple switches form a ring, the current ring ID would be network ID. Different ring network has different ID.
Port 1	port 1 can be used for the formation of ring network in switch.
Coupling port	When the ring type is “Couple”, the coupling port would be the one connects different network ID.
Port 2	port 2 can be used for the formation of ring network in switch.
Control port	When the ring type is “Couple”, the control port would be the one in the link of the intersection of two rings.
Type	According to the requirement in the scene, user can choose different ring network. ● Single: single ring, using a continuous ring to connect all device together. ● Couple: couple ring is a redundant structure used for connecting two independent networks. ● Chain: chain can enhance user’s flexibility in constructing all types of redundant network topology via an advanced software technology. ● Dual-homing: two adjacent rings share one switch. User could put one switch in two different networks or two different switching equipments in one network.
HelloTime	Hello_time is the time interval of Hello packet transmission. It is a query packet sent to adjacent device via ring network port to confirm whether the connection is normal.
Master-slave	Single ring has master/slave device option. One-Master Multi-Slave mode is recommended in one single ring. When the device is set as master device and one end of it is backup link, it can enable backup link to ensure the normal operation of the network when failure occurs in ring network. Description: Some products don’t support Master-slave option, so their ring network is non-master station structure.
Enabled	Enable or disable the corresponding ring group.

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

Rapid ring state interface as follows:



Ring group 1 state

Ring port 1	block
Ring port 2	block
Ring enable	disable

Ring group 2 state

Ring port 1	block
Ring port 2	block
Ring enable	disable

The main element configuration description of rapid ring interface

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

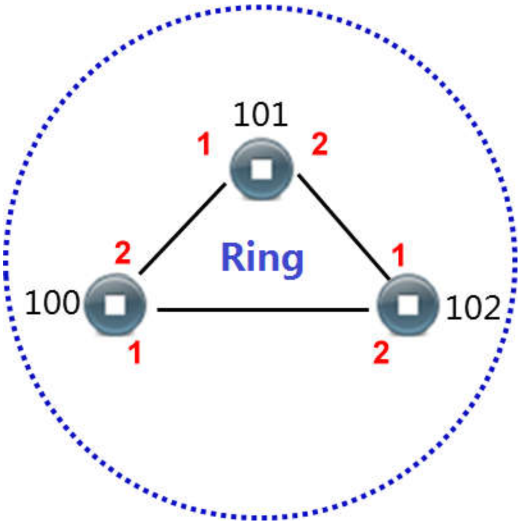
Now introduce the creation process respectively according to different ring network:

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

6.1.1 Instance: create single ring

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.

Operating steps

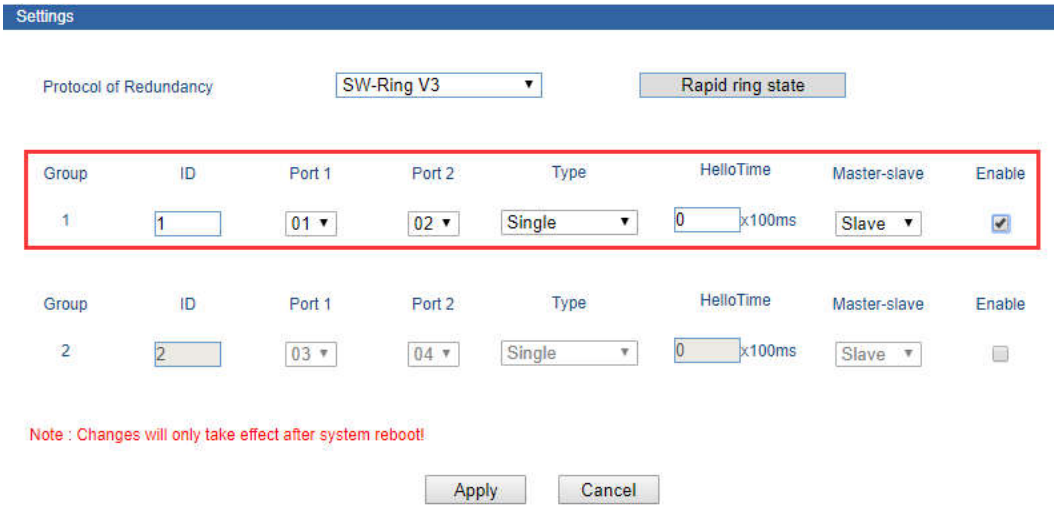
Configuring Device 100, 101 and 102 in the following steps:

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

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

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

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



Settings

Protocol of Redundancy: SW-Ring V3 ▾

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

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

Note : Changes will only take effect after system reboot!

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

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

Description:

“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".

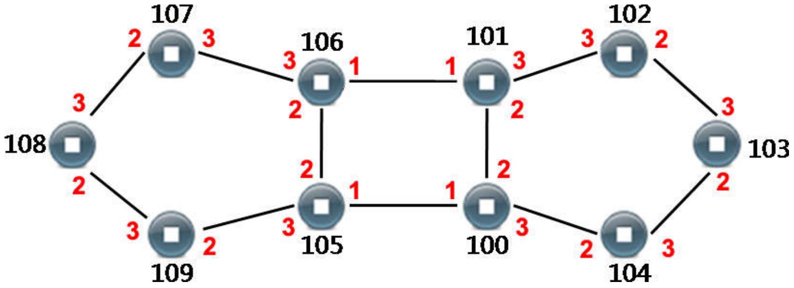
Step 10 On the column of "Device Reboot", click the button of "Reboot".

Step 11 End.

6.1.2 Instance: create coupling ring

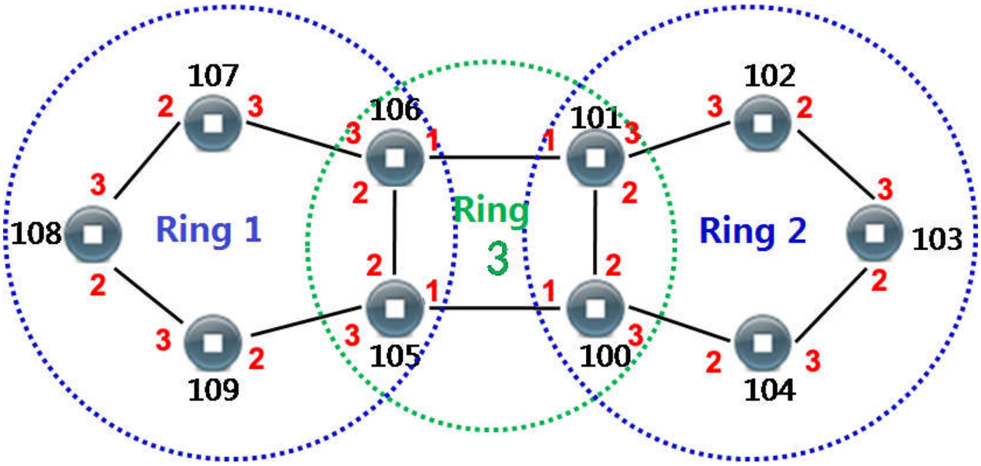
Instance

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

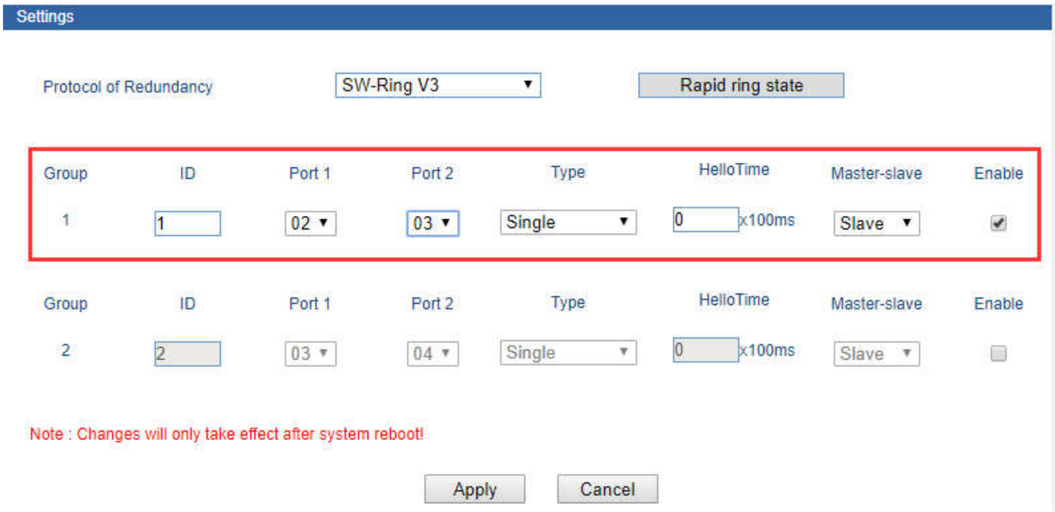
Configuring Device 105, 106, 107, 108 and 109 in the following steps respectively.

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

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

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

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



Settings

Protocol of Redundancy: SW-Ring V3

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

Note : Changes will only take effect after system reboot!

Step 5 Enter "1" into the "ID" textbox of "Group 1".

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

Description:

"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

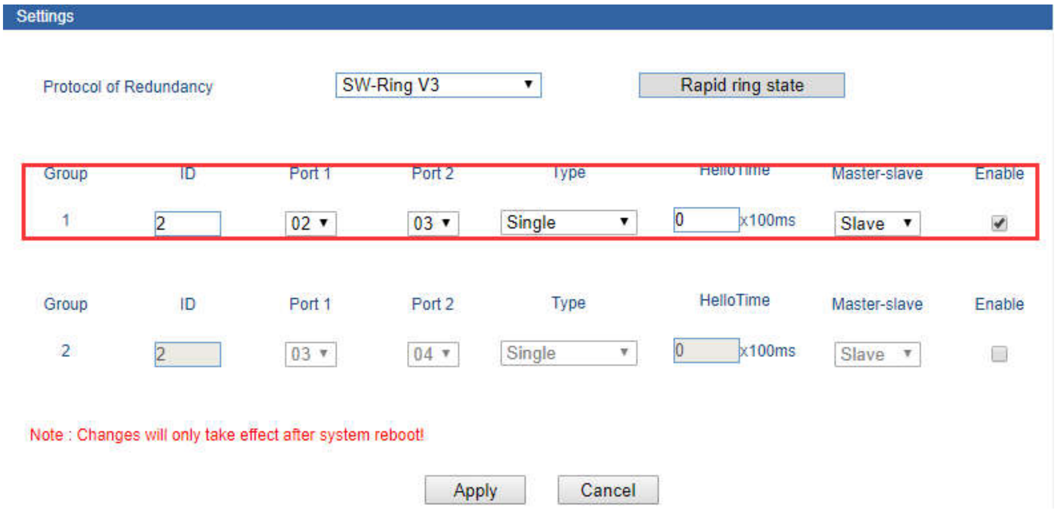
Configuring Device 100, 101, 102, 103 and 104 in the following steps respectively.

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

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

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

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



Settings

Protocol of Redundancy: SW-Ring V3 ▼ Rapid ring state

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

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

Note : Changes will only take effect after system reboot!

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

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

Description:

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

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

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

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

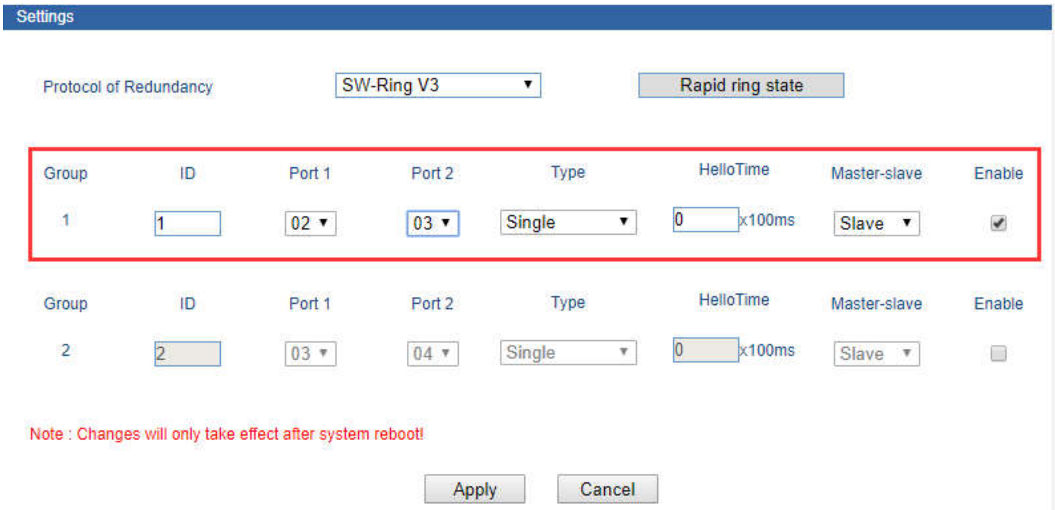
Step 6 Choose “1” in the drop-down list of “Coupling Port” of “Group 2”.

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



Settings

Protocol of Redundancy: SW-Ring V3 ▾ [Rapid ring state]

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

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

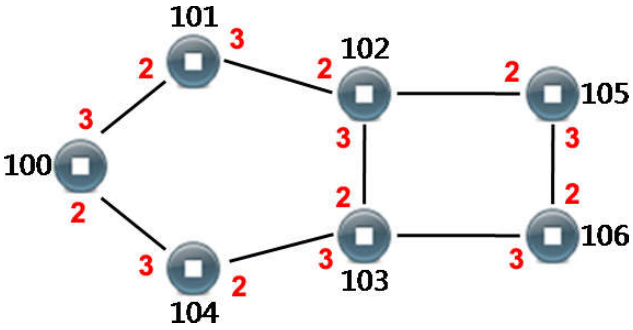
Note : Changes will only take effect after system reboot!

6.1.3 Instance: creating chain

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

Instance

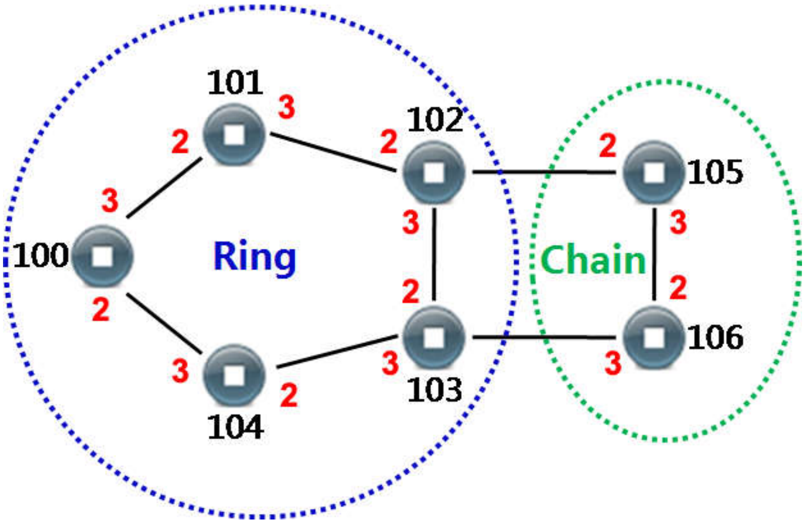
For example: creating chain. Its basic architecture is shown as below:



Instance analysis

Basic framework, we can make the following analyses:

- 100, 101, 102, 103 and 104 are in the ring. The ring network ports are 2 and 3. Device 100 is the master station, others are slave stations.
- Device 105 and 106 are in the chain. The ring network ports are 2 and 3.



Operation Step 1: creating ring

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

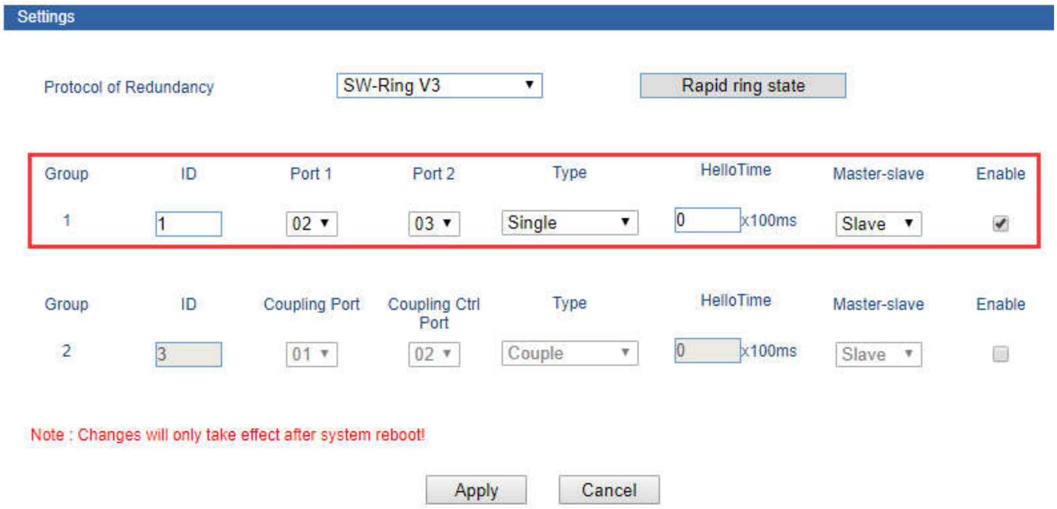
Step 1 Choose “Main Menu > Redundancy > Rapid Ring”.

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

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

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

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



Settings

Protocol of Redundancy: SW-Ring V3 ▾

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

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

Note : Changes will only take effect after system reboot!

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

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

Step 7 Click “Apply”.

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

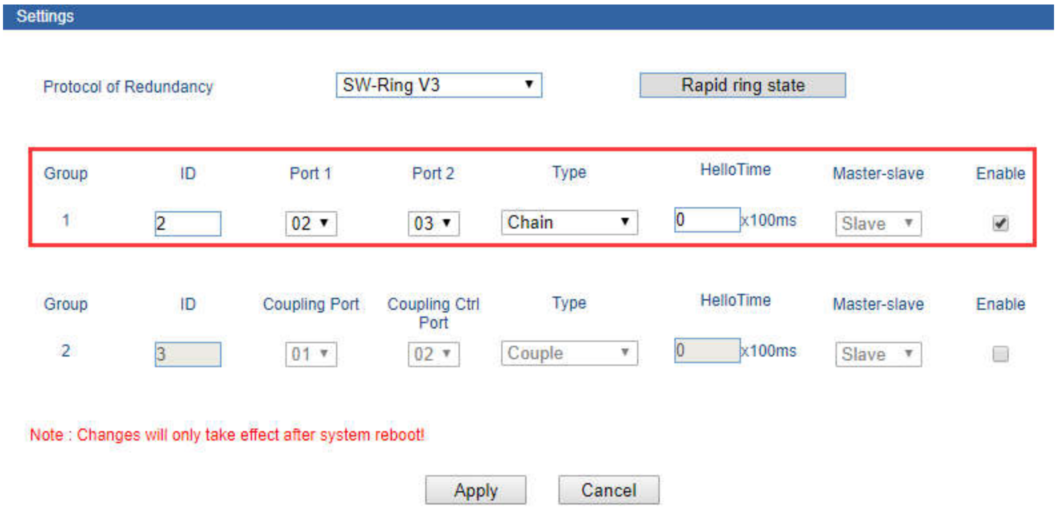
Step 2 In the “Settings” area of “Rapid Ring” page, choose “Ring V3” as “Protocol of Redundancy”.

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

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

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

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



Settings

Protocol of Redundancy: SW-Ring V3

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

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

Note : Changes will only take effect after system reboot!

Note

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

Step 7 Click “Apply”.

Step 8 Enter “Main Menu > System Management > Device 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

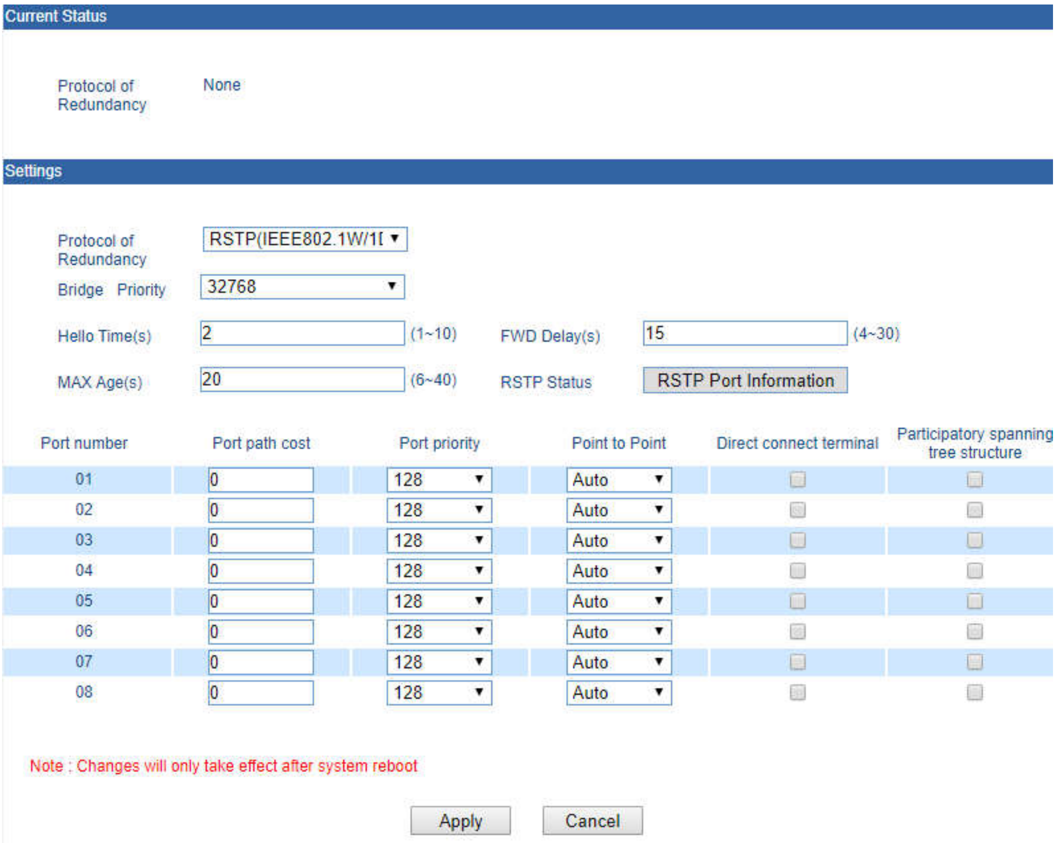
On the “Rapid ring” page, user can choose “RSTP (IEEE 802.1W/1D)” as redundancy protocol to create spanning tree quickly.

Operation Path

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

Interface description

RSTP interface as follows:



Current Status

Protocol of Redundancy: None

Settings

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

Bridge Priority: 32768 ▾

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

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

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

RSTP Status: RSTP Port Information

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

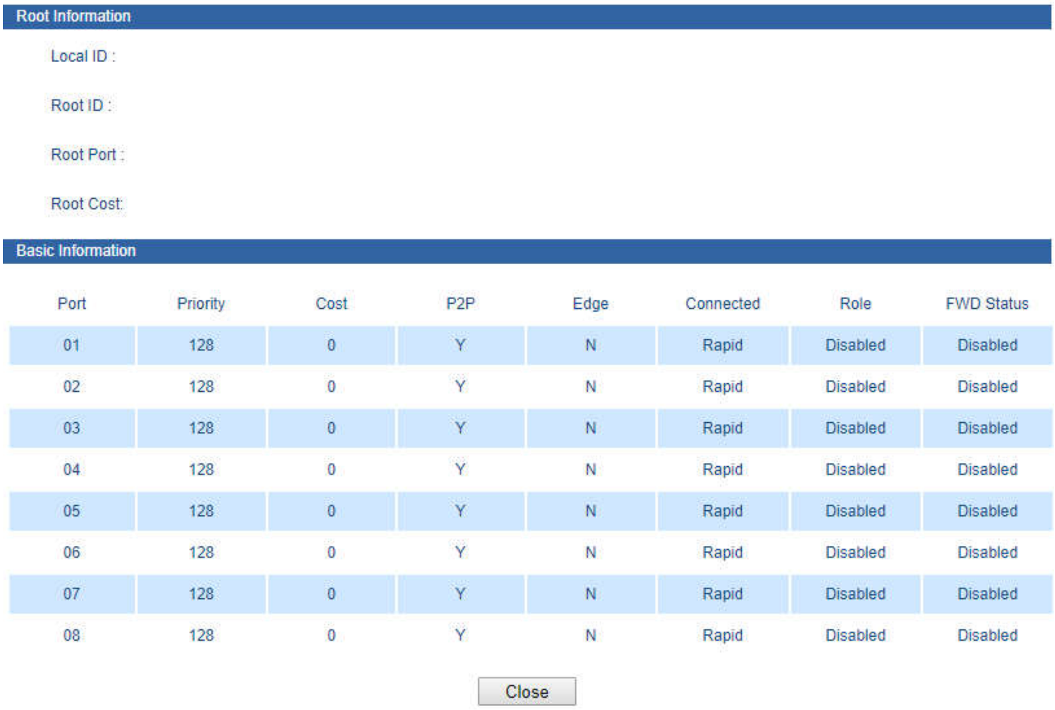
Note : Changes will only take effect after system reboot

The main element configuration description of RSTP interface:

Interface Element	Description
Redundancy protocol	Choose the algorithm of redundancy protocol, options are: ● None: it means that the ring network function is disabled. ● SW-Ring V3: supports single ring, coupling ring, chain and Dual_homing; ● RSTP (IEEE 802.1W/1D): rapid spanning tree.
Bridge priority	The priority of bridge. Description: In STP/RSTP network, the device with smallest bridge ID would be elected as root bridge. The bridge ID consists of bridge priority and bridge MAC address.
Hello time	The transmission time interval of the BPDU data packet. Description: The protocol message that STP/RSTP adopts is BPDU (Bridge Protocol Data Unit).
FWD delay	The forward delay time that the port of switch maintains in transition state (listening and learning). Description: STP/RSTP adopts a mechanism of state transition. The newly-selected root port and specified port have to go through twice the Forward Delay time to enter the forwarding state.
MAX age	The lifetime of BPDU packets.
RSTP status	Button, used for checking the current status of rapid spanning tree.
Port	Displays the port number of the device.
Cost	The path cost from network bridge to root bridge. Description: Path cost is a reference value for STP protocol to choose links. The path cost from a port to the root bridge is cumulated by the path cost it go through each port of each bridge.
Port priority	The priority of ports in bridge. The smaller the value, the higher the priority. Description: PID (Port ID) consists of two parts. The high 4 digits are port priorities, the low 12 digits are port numbers. In the case of same root path cost, it would not block the port with the smallest PID value, but the one with greater PID value.
P2P	The directly connected switch port, options are: ● Yes; ● No; ● Auto: adopt negotiation mechanism that could implement quick conversion of port states.

Interface Element	Description
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:



Root Information

Local ID :

Root ID :

Root Port :

Root Cost:

Basic Information

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

The main element configuration description of RSTP status interface:

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

	cost of root bridge is zero.
Basic information	**The display bar of basic information table**
Port	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	It is divided by whether the port forwards user flow and learns MAC address. • Discarding: neither forward user flow nor learn MAC address; • Learning: doesn’t forward user flow but learn MAC address; • Forwarding: forward user flow and learn MAC address; • Listening: neither forward user flow nor learn MAC address; but can receive and send configuration message; • Blocking: port only receives and processes BPDU, doesn’t forward user flow; • Disabled: blocked or physically disconnected.

Note

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

6.2 Port Trunking

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

Link aggregation technology mainly has the following three advantages:

- Increase bandwidth

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

  When some active links have fault, flow can be switched to other available member links, thus improving the stability of link aggregation interface.
- load sharing

  load sharing can be implemented on the active links of each member in one link aggregation group.

Function description

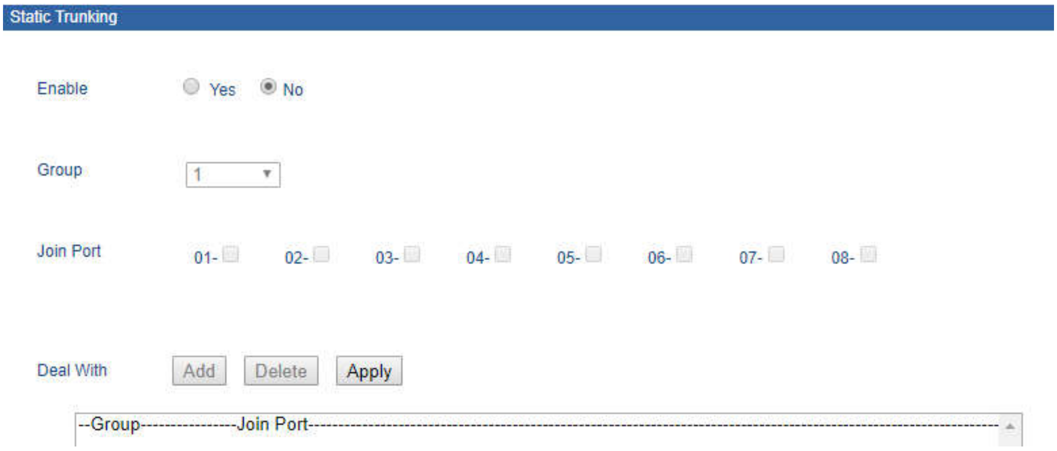
Binding multiple physical ports into one logical channel.

Operation Path

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

Interface description

Static Trunking interface as follows:



Static Trunking

Enable ○ Yes ● No

Group 1 ▾

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

Deal With

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

The main element configuration description of static trunking interface:

Interface Element	Description
Trunking configuration	Enable or disable trunking configuration.
Group	Choose trunking group.
Port list	Check the box of ports that join the trunking group.
Processing list	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.

Operating steps

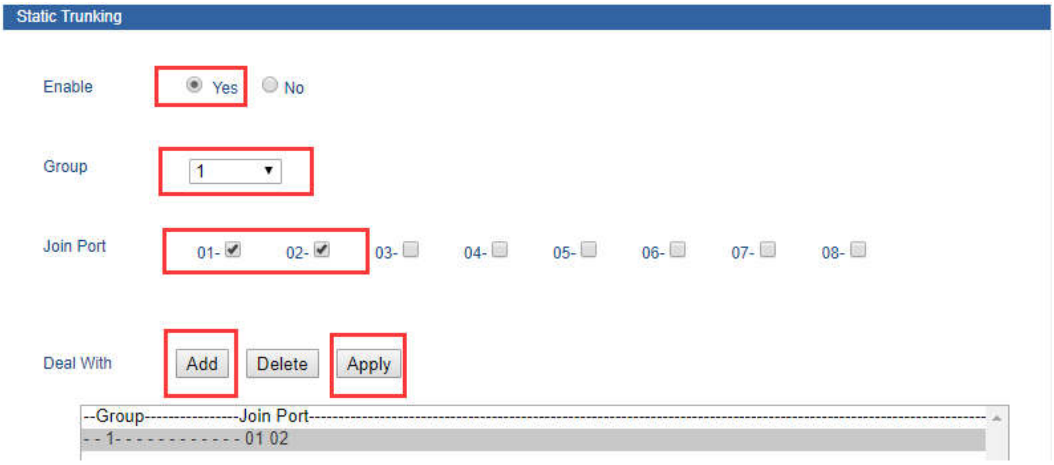
Configure switch A and switch B in the same way respectively.

Step 1 Log in Web configuration page.

Step 2 Choose "Main Menu > Redundancy > Port Trunking > Static Trunking".

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

Step 4 Choose "1" in the droplist of "Group".



Static Trunking

Enable ● Yes ○ No

Group 1

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

```
--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, network device’s types are increasing and their configurations are complex, a standard information communication platform is needed in order to make devices from different manufacturers find and exchange system and configuration information with each other in the network.

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

LLDP message sending mechanism

When LLDP function is enabled, the device would periodically send LLDP message to neighbor device. If device’s local configuration has changed, it would send LLDP message immediately to inform neighbor devices of changes in local information. 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

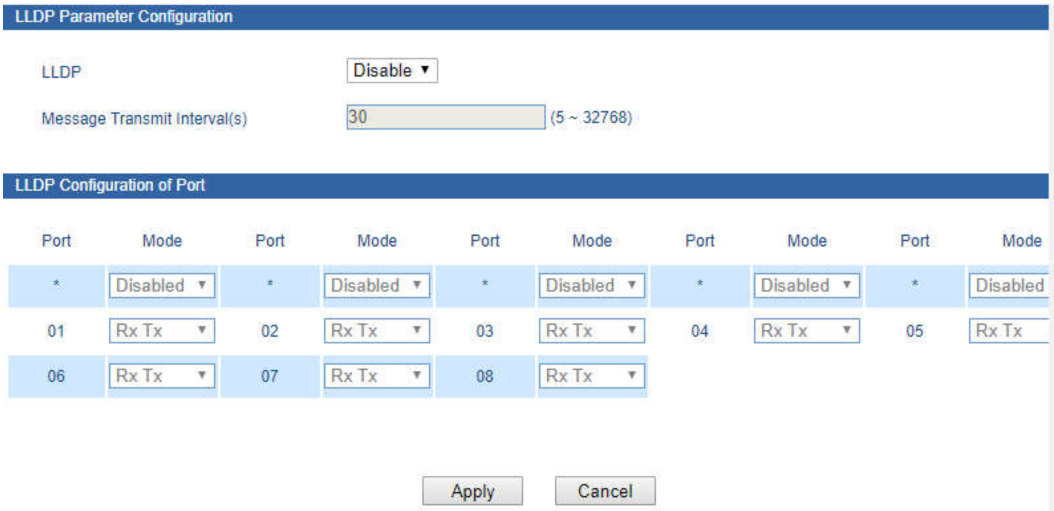
On the page of “Parameters Configuration”, user can configure LLDP function of the port and notify its device identity and performance in the local device.

Operation Path

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

Interface description

Parameter configuration interface as follows:



LLDP Parameter Configuration

LLDP: Disable

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

LLDP Configuration of Port

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

Main elements configuration description of parameter configuration interface:

Interface Element	Description
LLDP	Enable/disable LLDP function.
Interval time for messages sending (s)	Interval time for messages sending is 5-32768s. For preventing abounding LLDP sending caused by frequent changes of local information, next message should be delayed to send out after sending a LLDP message.
Mode	• Disable: disable LLDP function. • Tx Rx: send and receive LLDP message. • Tx only: periodically send LLDP message to neighbor device. • Rx only: check the validity of received LLDP and carried TLV, and configure the ageing time of neighbor device in the local device according to TTL (Time To Live) value in TLV.

7.2 Neighbor Information

Function description

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

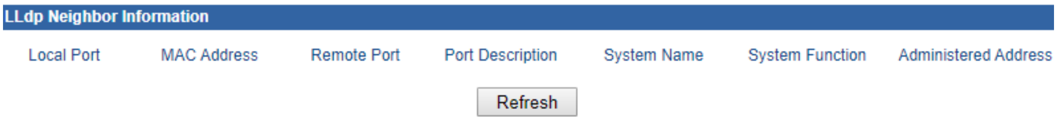
- MAC address;
- Remote port;
- Port description;
- System name;
- System function;
- Management address.

Operation Path

Open in order: " Main Menu > 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	Administered Address

Main elements configuration description of neighbor information interface:

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

8.1 Password

Company usually requires the administrators of monitoring devices and system or network are two roles. Their privileges should be separate, that is, the former is in charge of managing monitoring service only, and the latter is in charge of managing system or network only. Classification management provided by switch

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

Function description

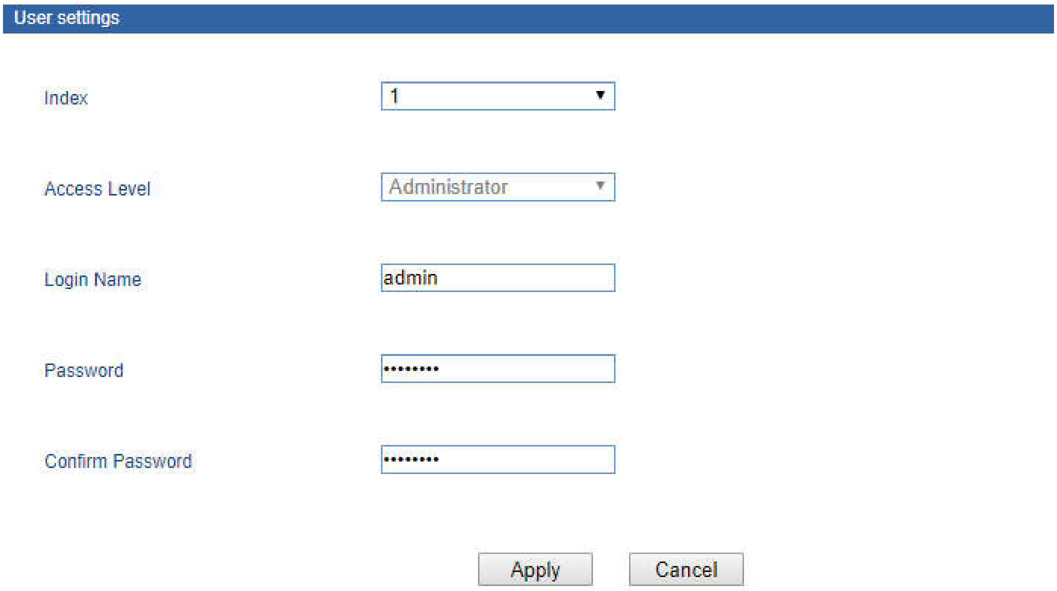
On the page of “Login Settings”, user can configure the login name, password and other parameters information of logging in to WEB configuration page.

Operation Path

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

Interface description

Login settings interface as follows:



User settings

Index	1
Access Level	Administrator
Login Name	admin
Password	••••••••
Confirm Password	••••••••

The main element configuration description of login settings interface:

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

⚠ Notice

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

For instance: create administrator

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

Operating steps

Step 1 Log in Web configuration page.

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

Step 3 On the “Login settings” page:

1. Choose “1” as “Index” number
2. Choose “administrator” as “access level”
3. Enter “admin8” as “login name”
4. Enter “admin8” as “password”
5. Enter “admin8” as “confirm password”.

Step 4 Click “Apply”.

Step 5 End.

9 Remote Monitoring

9.1 SNMP Configuration

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

SNMP System consists of NMS (Network Management System), Agent, Management object and MIB (Management Information Base).

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

As the network management center of the whole network, NMS manages devices. Each managed device includes Agent process, MIB and multiple managed objects that reside in 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 from 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	Response operation can return one or multiple parameters. This operation is issued by the Agent, which is the response operation of GetRequest, GetNextRequest, SetRequest and GetBulkRequest. After receiving the Get/Set instruction from NMS, the Agent completes the corresponding query/modification operation through MIB, and then uses Response operation to respond the information to NMS.
Trap	Trap information is the information sent by the Agent to NMS to inform the management process of the situation on the device end.
GetBulk	The GetBulk operation implements the NMS to query the information group of managed devices.
Inform	InformRequest is also managed device sending warning to NMS proactively. Different from Trap warning, the managed devices need NMS to respond InformResponse for affirmation after sending Inform warning.

Function description

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

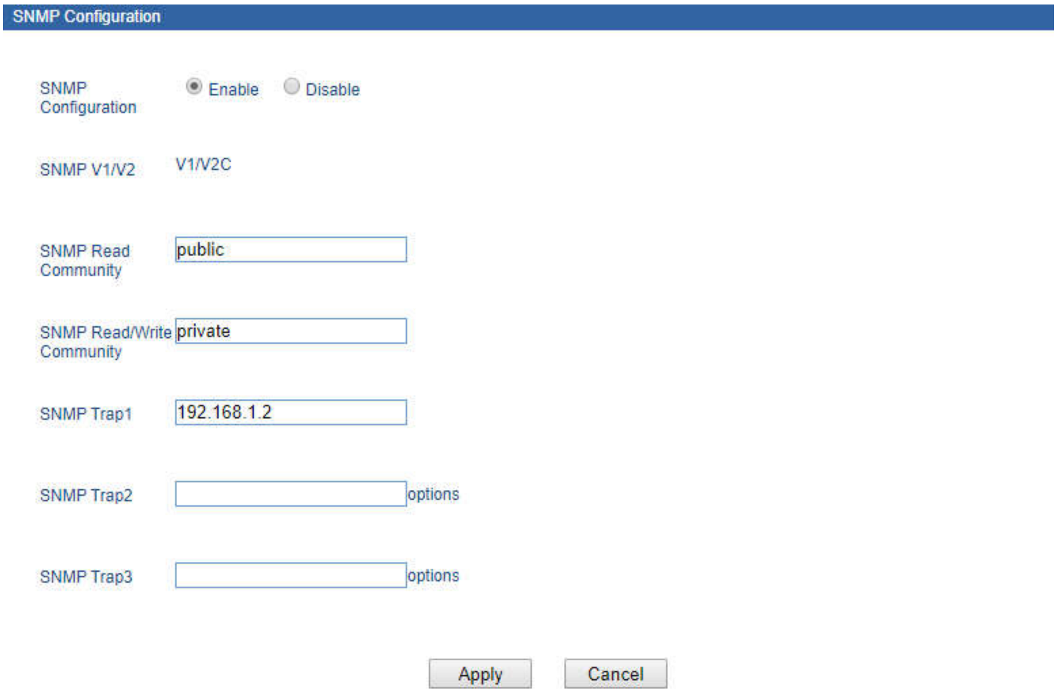
- Enable or disable SNMP configuration functions;
- Configure SNMP V1/V2 read-only community name;
- Configure SNMP V1/V2 read-only community name;
- Configure SNMP gateway.

Operation Path

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

Interface description

Interface screenshot of SNMP configuration as follows:



SNMP Configuration

SNMP Configuration	● Enable ○ Disable
SNMP V1/V2	V1/V2C
SNMP Read Community	public
SNMP Read/Write Community	private
SNMP Trap1	192.168.1.2
SNMP Trap2	options
SNMP Trap3	options

Main elements configuration description of SNMP configuration interface:

Interface Element	Description
SNMP Configuration	SNMP configuration function, options as follows: ● Enable; ● Disable;
SNMP version	SNMP supports the following version: ● SNMP V1: It adopts UDP protocol which can be used widely but will be insecure. ● SNMP V2c: Semantics has been enhanced, and it supports TCP protocol.
SNMP Read Community	Configure the read-only SNMP community name with the only operation permission of Get.
SNMP Read/Write Community	Configure the Read/Write SNMP community name with the operation permission of Get and Set.
SNMP Trap1	Configure Trap information destination IP address 1. Description: It will send out alarm during cold or warm start, port offline/online, power on/off.
SNMP Trap2	Configure Trap information destination IP address 2. Description: It will send out alarm during cold or warm start, port offline/online, power on/off.
SNMP Trap3	Configure Trap information destination IP address 3. Description: 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".

Operating steps

Step 1 Log in Web configuration page.

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 Relay Warning

Function description

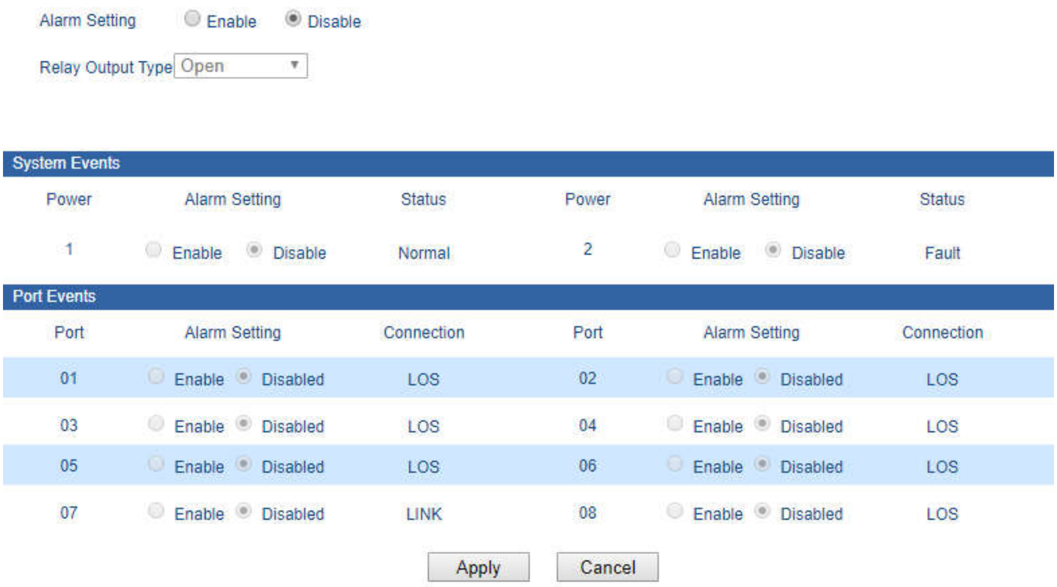
On the page of "Alarm Settings", user can configure power supply alarm and port alarm; when the equipment runs abnormally, it can promptly notify the administrator, and quickly repair the equipment status to avoid excessive loss.

Operation Path

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

Interface description

Relay warning interface as follows:



Alarm Setting ○ Enable ● Disable

Relay Output Type Open ▾

System Events

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

Port Events

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

Main elements configuration description of relay warning interface:

Interface Element	Description
Relay Warning	Configure alarm settings. Options as follows: • Enable; • Disable;
Relay Output Type	Click the drop-down list of "Relay Output Type", options as follows: • Normally open: when the relay is normal without alarm, it is in closed status; when alarm occurs, relay is in open status; • Normally closed: when the relay is normal without alarm, it is in open status; when alarm occurs, relay is in closed status.
System Events	**The power supply alarm setting bar**
Power	Display the power supply number of the device.
Relay Warning	Configure the alarm functions of the power supply. Options as follows: • Enable; • Disable; Note: • 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. • After enabling power supply alarm, the device will output alarm signal to hint abnormal operation of power supply when power supply runs abnormally.

Interface Element	Description
Power status	Display power supply’s current status ● Disable. ● Enable;
Port Events	**Port events column**
Port	Displays the port number of the device.
Relay Warning	Configure the port alarm function. Options as follows: ● Enable; ● Disable; Description 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.
Link status	Display port connection status of the device: ● Unlink ● Connected.

Instance Alert Settings

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

Operating steps

Step 1 Log in Web configuration page.

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

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

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

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

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

Step 6 Click “Apply”.

Step 7 End.

10 Port Statistics

10.1 Frame Statistics

Function description

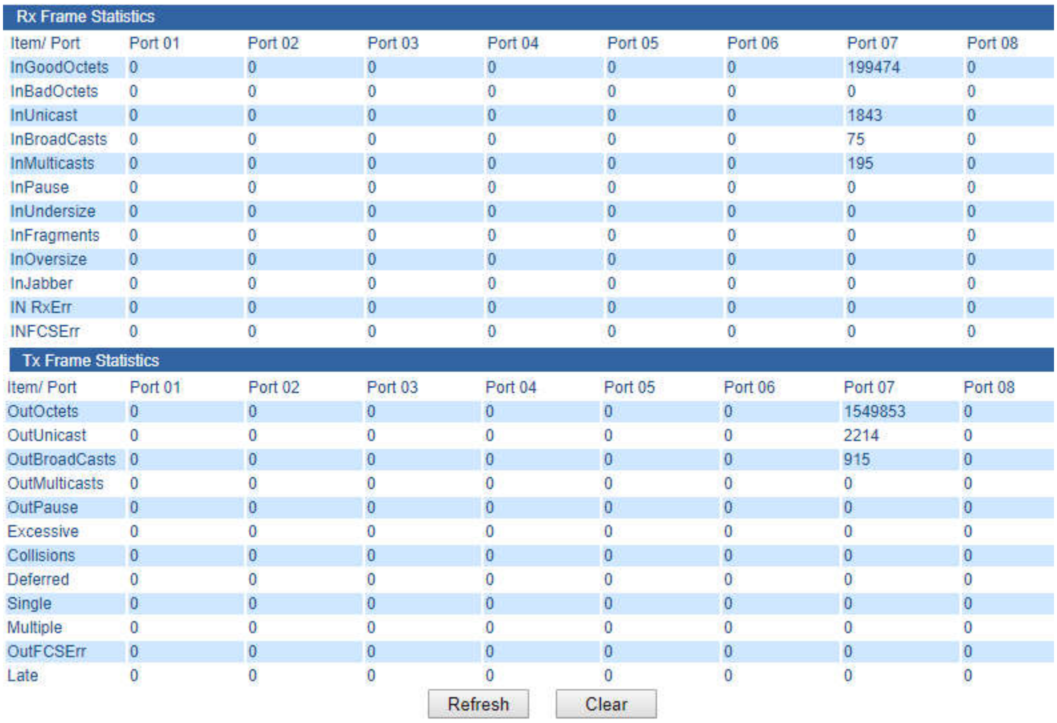
On the page of “Frame Statistics”, user can check frame statistics of sending/receiving data packets transmitted by the port within a period of time.

Operation Path

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

Interface description

Frames statistics interface as follows:



Rx Frame Statistics

Item/ Port	Port 01	Port 02	Port 03	Port 04	Port 05	Port 06	Port 07	Port 08
InGoodOctets	0	0	0	0	0	0	199474	0
InBadOctets	0	0	0	0	0	0	0	0
InUnicast	0	0	0	0	0	0	1843	0
InBroadCasts	0	0	0	0	0	0	75	0
InMulticasts	0	0	0	0	0	0	195	0
InPause	0	0	0	0	0	0	0	0
InUndersize	0	0	0	0	0	0	0	0
InFragments	0	0	0	0	0	0	0	0
InOversize	0	0	0	0	0	0	0	0
InJabber	0	0	0	0	0	0	0	0
IN RxErr	0	0	0	0	0	0	0	0
INFCSErr	0	0	0	0	0	0	0	0

Tx Frame Statistics

Item/ Port	Port 01	Port 02	Port 03	Port 04	Port 05	Port 06	Port 07	Port 08
OutOctets	0	0	0	0	0	0	1549853	0
OutUnicast	0	0	0	0	0	0	2214	0
OutBroadCasts	0	0	0	0	0	0	915	0
OutMulticasts	0	0	0	0	0	0	0	0
OutPause	0	0	0	0	0	0	0	0
Excessive	0	0	0	0	0	0	0	0
Collisions	0	0	0	0	0	0	0	0
Deferred	0	0	0	0	0	0	0	0
Single	0	0	0	0	0	0	0	0
Multiple	0	0	0	0	0	0	0	0
OutFCSErr	0	0	0	0	0	0	0	0
Late	0	0	0	0	0	0	0	0

Main elements configuration description of received frames statistics interface:

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

Main elements configuration description of transmitted frames statistics interface:

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

Interface Element	Description
	collision.
Multiple	Number of successfully output data frames after multiple times collision.
OutFCSErr	Number of output invalid FCS data frames.
Late	Number of output frames with the occurrence of collisions after 64 bytes.

11 Network Diagnosis

11.1 Port Mirror

Mirroring refers to copying a message that passes through a specified port (source port or mirror port) to another specified port (destination port or acquisition port). In the process of network operation and maintenance, 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 in order to facilitate business monitoring and fault location.

Function description

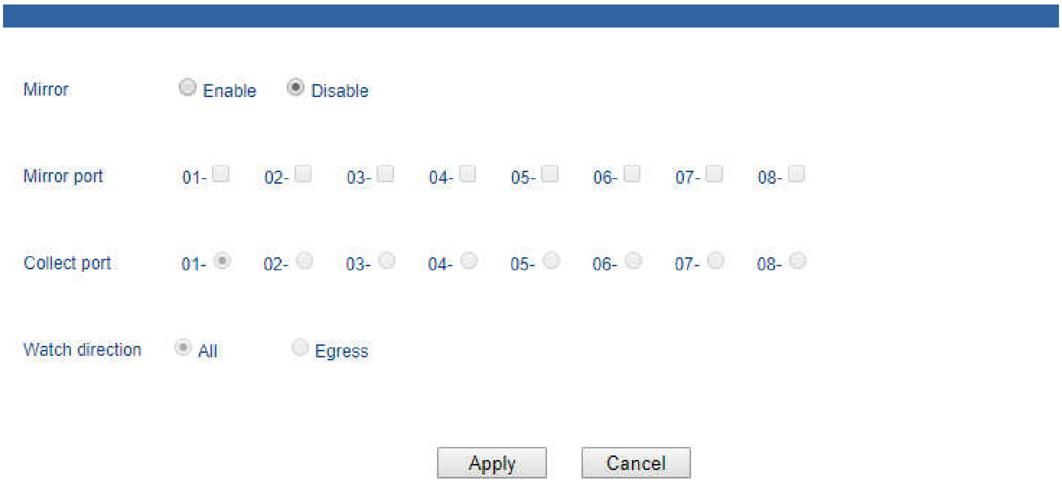
On the “Port Mirror” page, user can enable or configure the correspondence between ingress data mirror and egress data mirror.

Operation Path

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

Interface description

Port mirror interface as follows:



Mirror	○ Enable	● Disable						
Mirror port	01- □	02- □	03- □	04- □	05- □	06- □	07- □	08- □
Collect port	01- ●	02- ○	03- ○	04- ○	05- ○	06- ○	07- ○	08- ○
Watch direction	● All	○ Egress						

The main element configuration description of port mirror interface:

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

For instance: port mirror configuration

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

Operating steps

Step 1 Log in Web configuration page.

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

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

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

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

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

Step 7 Click “Apply”.

Step 8 End.

12 System Management

12.1 Log Information

Function description

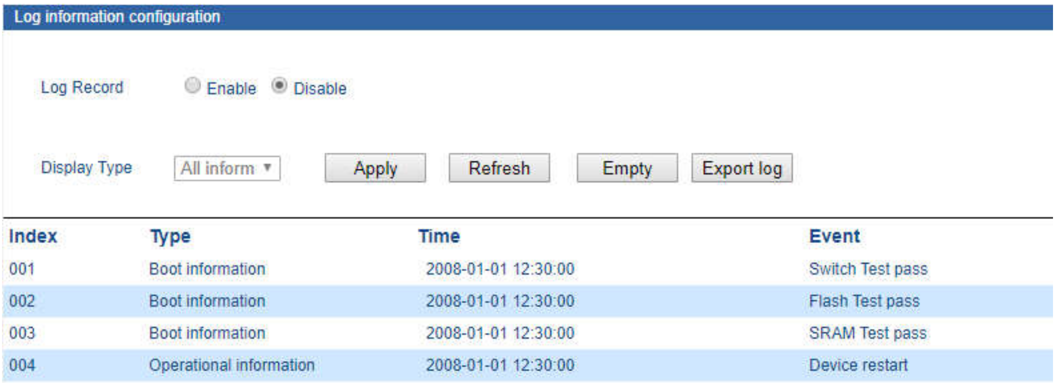
On the page of “Log information”, user can enable “log record” to check the status information of the device.

Operation Path

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

Interface description

Log information interface as follows:



Log Record ○ Enable ● Disable

Display Type All inform ▾

Index	Type	Time	Event
001	Boot information	2008-01-01 12:30:00	Switch Test pass
002	Boot information	2008-01-01 12:30:00	Flash Test pass
003	Boot information	2008-01-01 12:30:00	SRAM Test pass
004	Operational information	2008-01-01 12:30:00	Device restart

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 Time Configuration

Function description

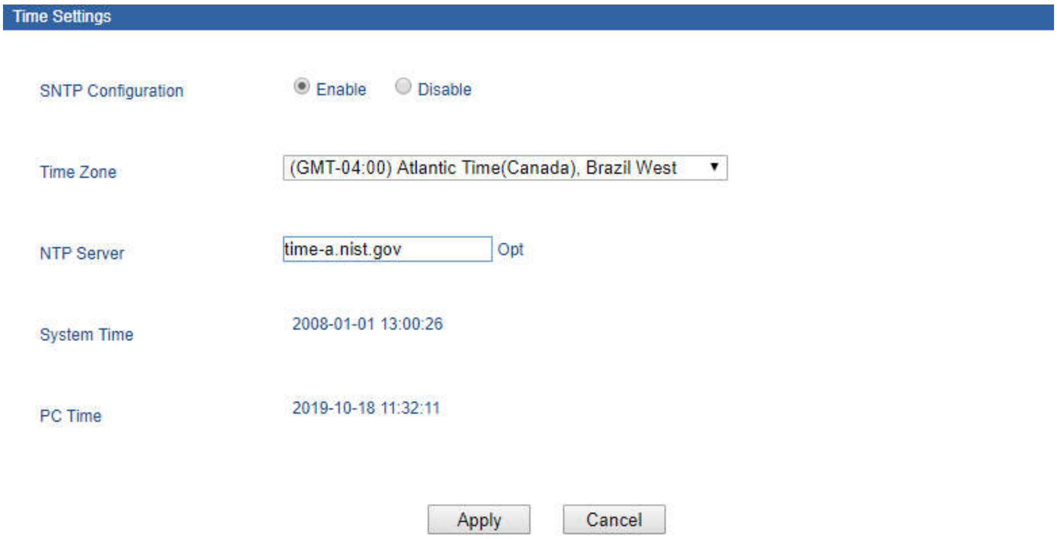
On the page of “Time Configuration”, user can check current PC time or system operation time, and select relative time zone.

Operation Path

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

Interface description

Time configuration interface as follows:



Time Settings

SNTP Configuration ● Enable ○ Disable

Time Zone (GMT-04:00) Atlantic Time(Canada), Brazil West

NTP Server time-a.nist.gov Opt

System Time 2008-01-01 13:00:26

PC Time 2019-10-18 11:32:11

Main elements configuration description of time configuration interface:

Interface Element	Description
Time Configuration	Enable or disable time configuration.
World time zone	Selection of standard time zone for countries in the world.
NTP Server	Host name or IP address that provides NTP timing and time service for user.
System Time	The time of the device itself, press “2008-01-01” to start operating after powered on.
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

- Thereinto, 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 32 digits that corresponds to IP address, some of them are 1 and others are 0 in these digits. 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

Gateway address is usually called default gateway. The default gateway is the default route, which is selected by the router when the destination address in the IP data packet can’t find other existing routes. All data packet whose destination is not in the routing table of the router would use the default route.

DNS Server

DNS’s full name is Domain Name Server, whose function is resolving domain name that is easy for us to remember to IP address that Internet can recognize. If our device needs to access some host names, it would need this server to resolve it to IP addresses.

Function description

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

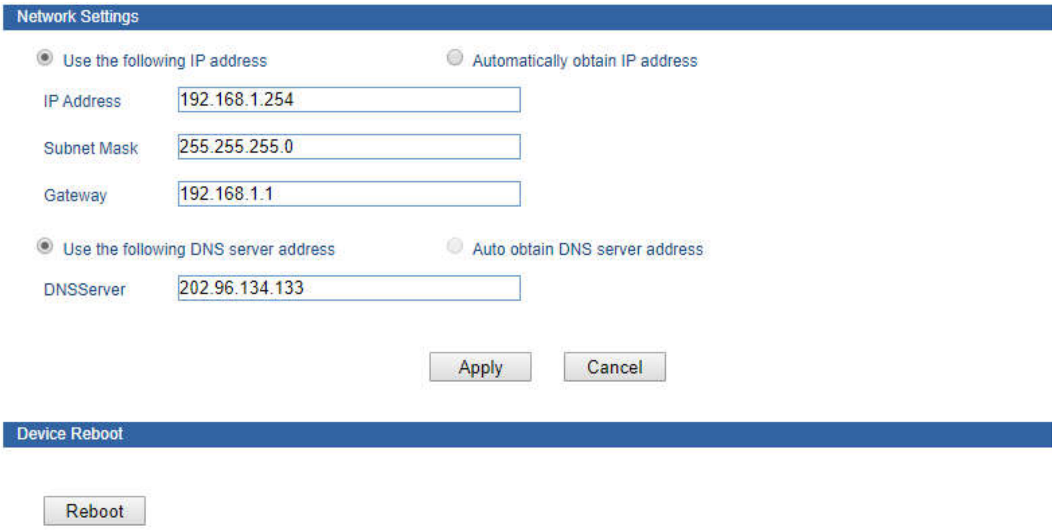
- Configure default IP address of the device;
- Configure netmask;
- Configure gateway address;
- Configure DNS server;
- Reboot the device.

Operation Path

Open in order: “Main Menu > Basic Settings > Network & Reboot”.

Interface description

Device address interface as follows:



Network Settings

● Use the following IP address ○ Automatically obtain IP address

IP Address: 192.168.1.254

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

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

DNSServer: 202.96.134.133

Device Reboot

Main elements configuration description of device address interface:

Interface Element	Description
Device Address	**Configuration column of the device address**
Use the following IP address	It represents that manually enabling configured IP address, netmask and gateway address.
Automatically obtain DNS server address	It represents that enabling the system automatical acquisition of the IP address of the device.
IP Address	Configure IP address of the device. Description 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. Description 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. Description 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. Description: When IP address is manual configuration, this option becomes gray and is not optional.
DNS server	Configure DNS server address.
Settings	Save the device address information. Description: Some devices may automatically reboot after configuration, and the configuration will take effect after rebooting.
Cancel	Cancel the modification of device address information.
Reboot the device.	**Configuration column of device reboot**
Reboot	Reboot the device

For Example: Manual Configuration

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

Operating steps

Step 1 Log in Web configuration page.

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.

Operating steps

Step 1 Log in Web configuration page.

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:

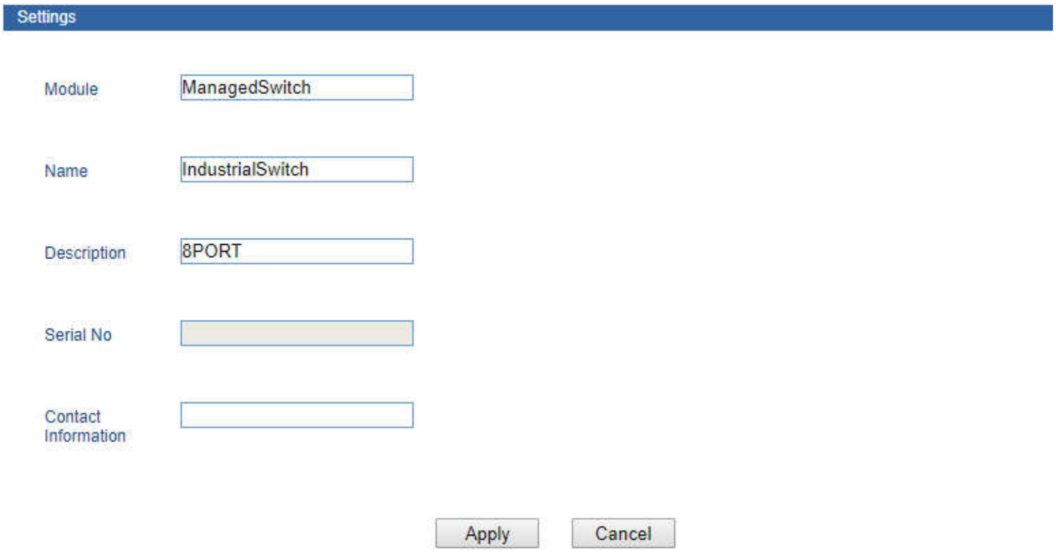
- Device model;
- Device name;
- Device description;
- Device number;
- Contact information.

Operation Path

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

Interface description

System information interface as follows:



Settings

Module: ManagedSwitch

Name: IndustrialSwitch

Description: 8PORT

Serial No:

Contact Information:

Main element configuration instructions in System Information interface.

Interface Elements	Description
Device model.	Configure the device model.
Device name.	Configure the device name to identify each device in the network.
Description	Configure the summary description of the device.
Device serial number.	Configure the device number. Description: • The number can be used for describing the installation position of the device; • The number length shouldn't be more than 30 bytes.
Contact information.	Configure the contact Information of the maintenance personnel of the device. Description: • Support the entering of Chinese characters, English letters, number, characters like "-", "_", "@", ",", "."; • The entering of blank space is not supported.

For Example: Device Information Configuration

For example: Configure the device according to following information:

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

Operating steps

Step 1 Log in Web configuration page.

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:

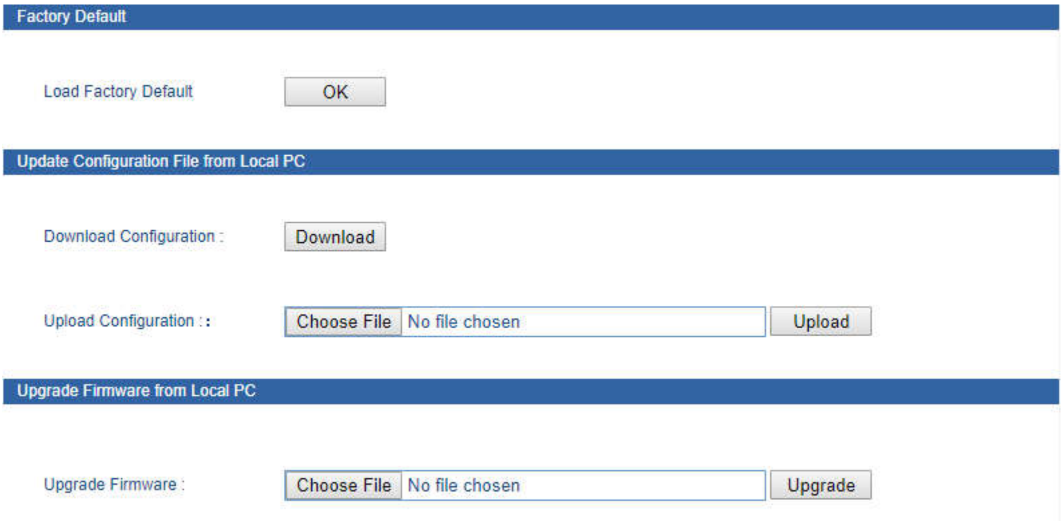
- Restore factory defaults;
- Upload and download configuration files;
- System upgrading.

Operation Path

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

Interface description

System File interface as follow:



Main element configuration instructions in System File interface.

Interface Element	Description
Restore factory setting	**Configuration column of restore factory defaults**
Load Factory Default	Restore factory defaults of the switch. Description: Restore factory defaults will cause all devices to be in the factory status, default IP address is "192.168.1.254".

Update Configuration File from Local PC	**Configuration column of configuration files**
Download Configuration	Download the configuration information files of current switch. Tips: Downloaded configuration files can be uploaded to other homogeneous devices, achieving repeated usage after one-time configuration.
Upload Configuration	Configure the switch via uploading configuration files information.
System upgrading.	**Configuration column of system upgrade**
Upgrade Firmware	Upgrade operating system of the switch.

⚠ Warning

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

Example: Download Configuration Files

For example: Download configuration files.

Operating steps

Step 1 Log in Web configuration page.

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.

Operating steps

Note

Please prepare the configuration files and then conduct uploading operation.

Step 1 Log in Web configuration page.

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

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

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

Step 5 Click "Open".

Step 6 Click "Upload".

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

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

Step 9 End.

12.6 System log off

Function description

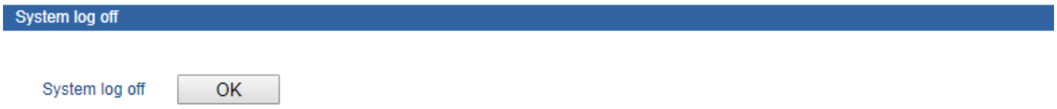
On the page of “System log off”, user can log off the login information of current user.

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.

Operating steps

Step 1 Log in Web configuration page.

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. **How about forget the login password?**
   For forgetting the login password, the password can be initialized by restoring factory setting, specific method is adopt BlueEyes_Ⅱ software to search and use restore factory setting function to initialize the password. Both of the initial user name and password are "admin".

3. **Is configuring via WEB browser same to configuring via BlueEyes_Ⅱ software?**
   Both configurations are the same, without conflict.

13.2 Configuration Problem

1. **How to configure the device restore default setting via DIP switch?**
   Turn the DIP switch 2 to ON position, and restore default setting after power on again.

2. **Why the bandwidth can't be increased after configure Trunking (port aggregation) function?**
   Check whether the port attributes set to Trunking are consistent, such as rate,

duplex mode, VLAN and other attributes.

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

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

13.3 Alarm Problem

1. **When the device alarms, except BlueEyes_II software nether alarm information display area will display alarm information, is there any other way to notify technical staffs?**
When the device alarms, monitoring host computer buzzer will continue to emit alarm sounds.

13.4 Indicator Problem

1. **Power indicator isn't bright, what's the reason?**
Possible reasons include:
    - Not connected to the power socket; troubleshooting, connected to the power socket.
    - Power supply or indicators faults; troubleshooting, change the power supply or device test.

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

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

Possible reasons include:

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

3. **Ethernet copper port 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.

14 Maintenance and Service

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

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

- Internet Service
- Call technical support office;
- Product repair or replacement;

14.1 Internet Service

More useful information and tips are available via our company's website. Website: http://www.3onedata.com

14.2 Service Hotline

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

14.3 Product repair or replacement;

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

3onedata
Make network communication more reliable

3onedata Co., Ltd.

Address: 3/B, Zone 1, Baiwangxin High Technology Industrial park, Nanshan District, Shenzhen, 518108 China

Tel: +86-755-26702668

E-mail: sales@3onedata.com

Fax: +86-755-26703485

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