SICOM3016/3024/2024M/8000 Series Industrial Ethernet Switches Web Operation Manual

Kyland Technology Co., Ltd.

Publication Date: Mar. 2013

Version: V2.2

FAX: +86-10-88796678

Website: http://www.kyland.com

E-mail: support@kyland.com

Disclaimer:

Kyland Technology Co., Ltd. tries to keep the content in this manual as accurate and as up-to-date as possible. This document is not guaranteed to be error-free, and we reserve the right to amend it without notice.

Contents

Preface

This manual mainly introduces the access methods and software features of SICOM3016/3024/2024M/8000 series industrial Ethernet switches, and details Web configuration methods.

Content Structure

The manual contains the following contents:

Chapter	Content
1. Product Introduction	➢ Overview ➢ Product models ➢ Software features
2. Switch Access	➢ View types ➢ Access through Console Port ➢ Access through Telnet ➢ Access through Web
3. Device Management	➢ Restart ➢ Logout
4. Device Status	➢ Basic information ➢ Port status ➢ Port statistics ➢ System operating information
5. Basic Configuration	➢ IP address ➢ Basic information ➢ Port configuration ➢ Password change ➢ Software update (FTP) ➢ Software version query ➢ Configuration upload/download
6. Advanced Configuration	➢ Port rate limiting

	➢ VLAN ➢ PVLAN ➢ Port mirroring ➢ Port trunk ➢ Link check ➢ Static multicast* ➢ IGMP Snooping ➢ ACL ➢ ARP ➢ SNMP ➢ DT-Ring* ➢ RSTP/STP ➢ RSTP/STP transparent transmission ➢ QoS ➢ MAC address aging time ➢ LLDP ➢ SNTP ➢ MSTP* ➢ Alarm ➢ Port traffic alarm ➢ GMRP* ➢ RMON* ➢ Unicast address configuration and query

Note:

* indicates the features not available on SICOM2024M and SICOM3024_V1.2.

Conventions in the manual

1. Text format conventions

Format	Description
< >	The content in < > is a button name. For example, click <Apply> button.
[ ]	The content in [ ] is a window name or a menu name. For example, click [File] menu item.
{ }	The content in { } is a portfolio. For example, {IP address, MAC address} means the IP address and MAC address are a portfolio and they can be configured and displayed together.
→	Multi-level menus are separated by "→". For example, Start → All Programs → Accessories. Click [Start] menu, click the sub menu [All programs], then click the submenu [Accessories].
/	Select one option from two or more options that are separated by "/". For example "Addition/Deduction" means addition or deduction.
~	It means a range. For example, "1~255" means the range from 1 to 255.

2. CLI conventions

Format	Description
Bold	Commands and keywords, for example, **show version**, appear in **bold** font.
Italic	Parameters for which you supply values are in *italic* font. For example, in the **show vlan** *vlan id* command, you need to supply the actual value of *vlan id*.

3. Symbol conventions

Symbol	Description
⚠ **Caution**	The matters need attention during the operation and configuration, and they are supplement to the operation description.
✎ **Note**	Necessary explanations to the operation description.
⚡ **Warning**	The matters call for special attention. Incorrect operation might cause

	data loss or damage to devices.

Product Documents

The documents of SICOM3016/3024/2024M/8000 series industrial Ethernet switches include:

Document	Content
SICOM3016 Series Industrial Ethernet Switches Hardware Installation Manual	Describes the hardware structure, hardware specifications, mounting and dismounting methods of SICOM3016.
SICOM3024 Series Industrial Ethernet Switches Hardware Installation Manual	Describes the hardware structure, hardware specifications, mounting and dismounting methods of SICOM3024.
SICOM2024M Series Industrial Ethernet Switches Hardware Installation Manual	Describes the hardware structure, hardware specifications, mounting and dismounting methods of SICOM2024M.
SICOM8000 Series Industrial Ethernet Switches Hardware Installation Manual	Describes the hardware structure, hardware specifications, mounting and dismounting methods of SICOM8000
SICOM3016/3024/2024M/8000 Series Industrial Ethernet Switches Web Operation Manual	Describes the switch software functions, Web configuration methods, and steps of all functions.

Document Obtainment

Product documents can be obtained by:

- ➢ CD shipped with the device
- ➢ Kyland website: www.kyland.com

1 Product Introduction

1.1 Overview

The series switches are applied in the power, rail transit, coal mining, and many other industries. SICOM8000 is developed particularly for military applications. The high-performance switching engine and solid closed housing enable the series switches to adapt to harsh and hazardous industrial environments. Moreover, they support MSTP and DT-Ring, securing reliable operation. With extensive ports, the series switches satisfy various customers' requirements.

1.2 Product Models

This series switches include:
SICOM3016
SICOM3024_ V1.6/V1.2 (V1.6/ V1.2 indicates the hardware version.)
SICOM2024M_V1.2 (V1.2 indicates the hardware version.)
SICOM8000

1.3 Software Features

This series switches provide abundant software features, satisfying customers' various requirements.

- Redundancy protocols: RSTP/STP, DT-Ring, and MSTP
- Multicast protocols: IGMP Snooping, GMRP, and static multicast
- Switching attributes: VLAN, PVLAN, QoS, and ARP
- Bandwidth management: port trunk, port rate limiting
- Security: ACL
- Synchronization protocol: SNTP
- Device management: FTP software update, configuration upload/download
- Device diagnosis: port mirroring, LLDP, link check

- Alarm function: port alarm, power alarm, ring alarm, IP/MAC address conflict alarm, and port traffic alarm
- Network management: management by CLI, Telnet, Web and Kyvision network management software, and SNMP network monitoring
- ...

2 Switch Access

You can access the switch by:

- Console port
- Telnet
- Web browser
- Kyvision management software

Kyvision network management software is designed by Kyland. For details, refer to its user manual.

2.1 View Types

When logging into the Command Line Interface (CLI) by the console port or Telnet, you can enter different views or switch between views by using the following commands.

Table 1 View Types

View Prompt	View Type	View Function	Command for View Switching
SWITCH>	User view	View recently used commands. View software version. View response information for ping operation.	Input "**enable**" to enter the management view.
SWITCH #	Management view	Upload/Download configuration file. Restore default configuration. View response information for ping	Input "**configure terminal**" to enter the configuration view from the management view. Input "**exit**" to return to the user view.

		operation. Restart the switch. Save current configuration. Display current configuration. Update software.	
SWITCH(config)#	Configuration view	Configure switch functions.	Input "**exit**" or "**end**" to return to the management view.

When the switch is configured through the CLI, "?" can be used to get command help. In the help information, there are different parameter description formats. For example, <1, 255> means a number range; <H.H.H.H> means an IP address; <H:H:H:H:H:H> means a MAC address; word<1,31> means a string range. In addition, ↑ and ↓ can be used to scroll through recently used commands.

2.2 Access through Console Port

You can access a switch by its console port and the hyper terminal of Windows OS or other software that supports serial port connection, such as HTT3.3. The following example shows how to use Hyper Terminal to access switch by console port.

1. Connect the serial port of a PC to the console port of the switch with a DB9-RJ45 cable.
2. Run the Hyper Terminal in Windows desktop. Click [Start] → [All Programs] → [Accessories] → [Communications] → [Hyper Terminal], as shown in Figure 1.

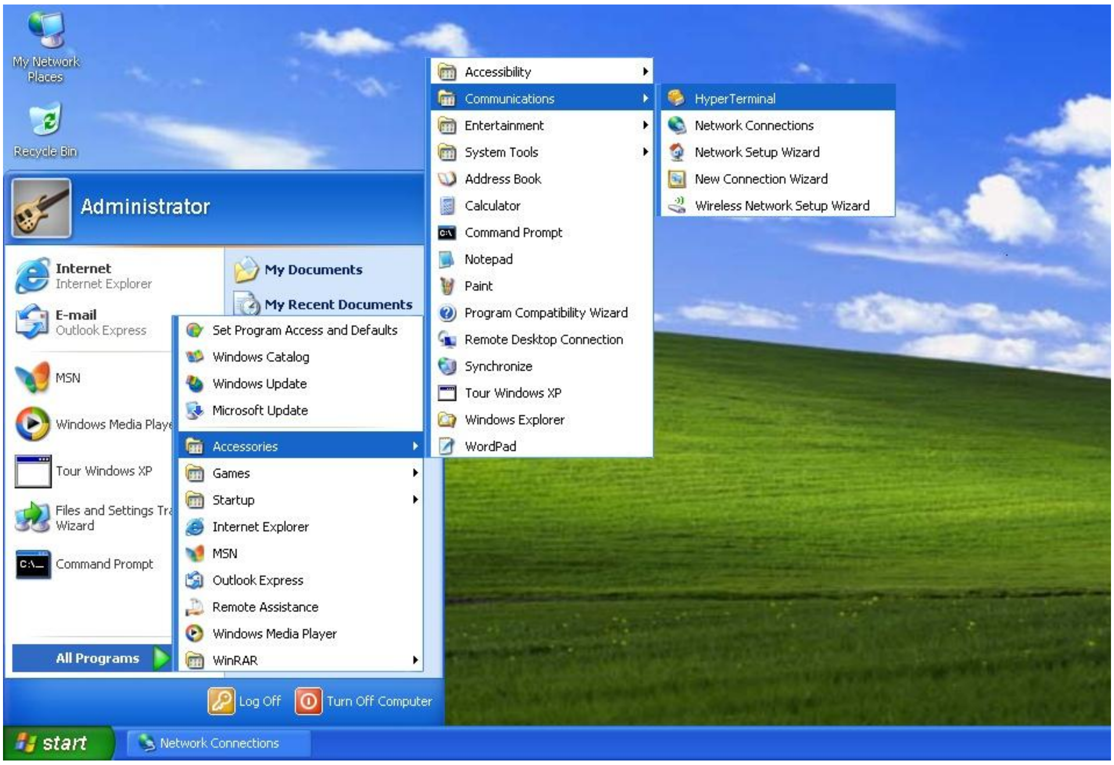
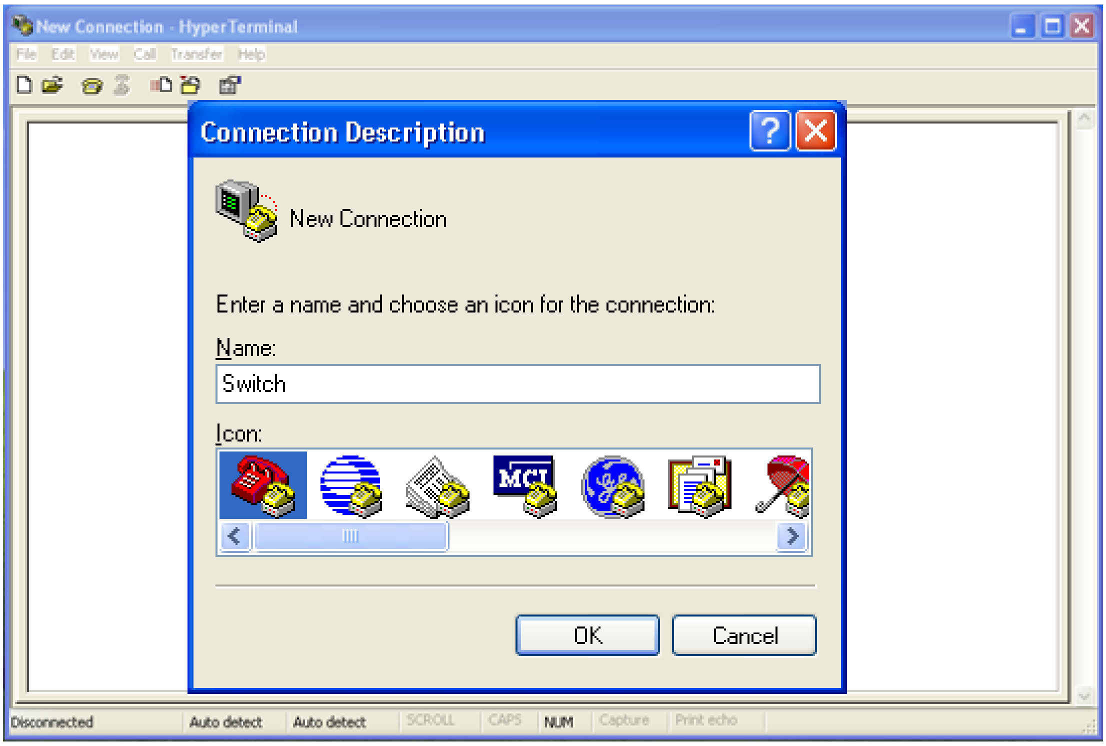


Figure 1 Starting the Hyper Terminal

3. Create a new connection "Switch", as shown in Figure 2.

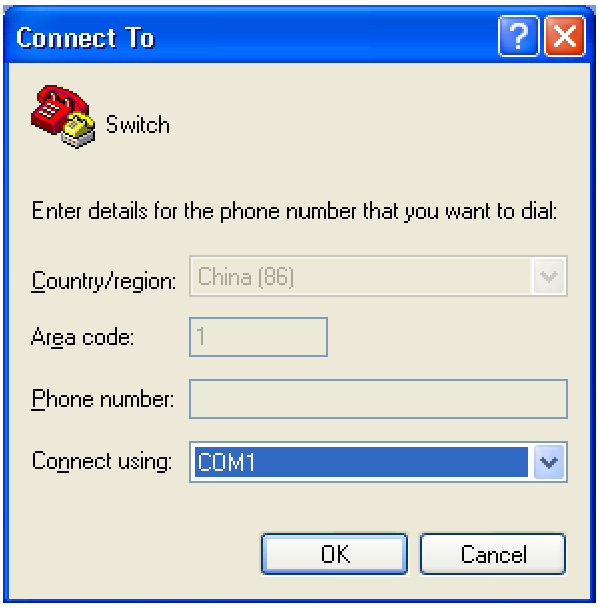


Enter a name and choose an icon for the connection:

Name: Switch

Figure 2 Creating a New Connection

4. Connect the communication port in use, as shown in Figure 3.



Connect To

Switch

Enter details for the phone number that you want to dial:

Country/region: China (86)

Area code: 1

Phone number:

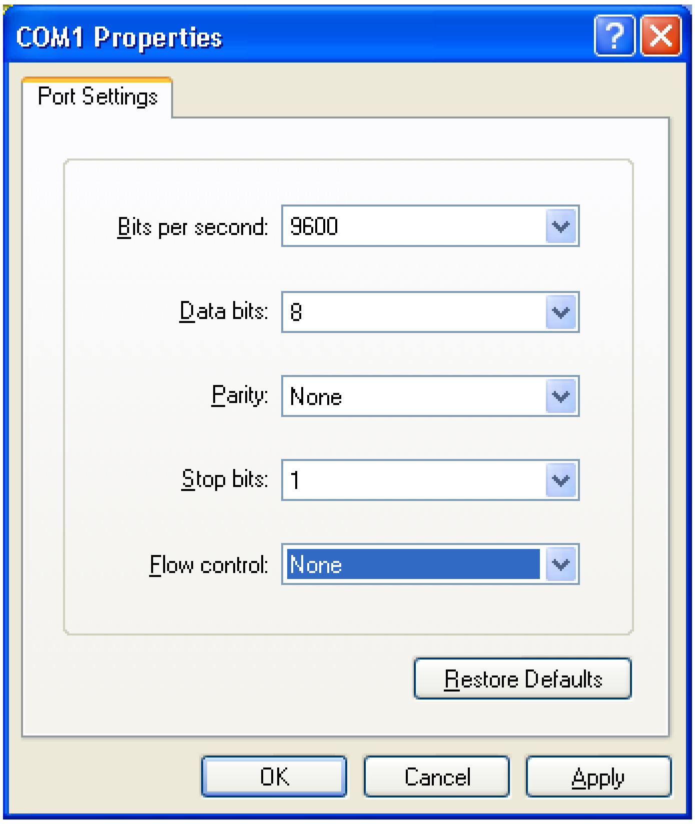
Connect using: COM1

Figure 3 Selecting the Communication Port

Note:

To confirm the communication port in use, right-click [My Computer] and click [Property] → [Hardware] → [Device Manager] → [Port].

5. Set port parameters (Bits per second: 9600, Data bits: 8, Parity: None, Stop bits: 1, and Flow control: None), as shown in Figure 4.



Bits per second: 9600

Data bits: 8

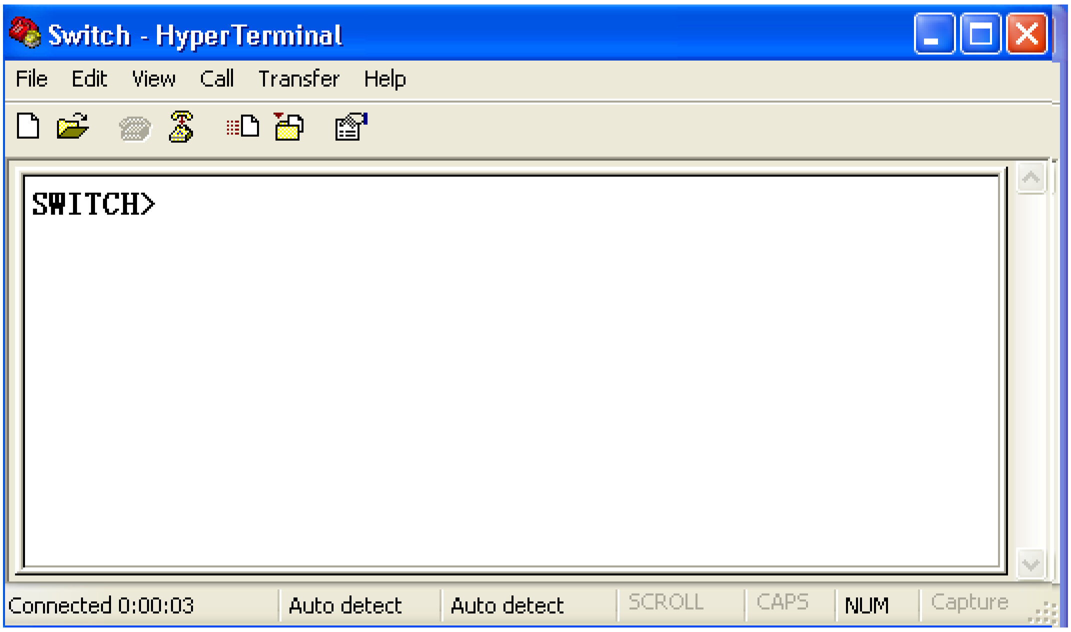
Parity: None

Stop bits: 1

Flow control: None

Figure 4 Setting Port Parameters

6. Click <OK>. The switch CLI is displayed. Press <Enter> to enter the user view, as shown in Figure 5.



```
SWITCH>
```

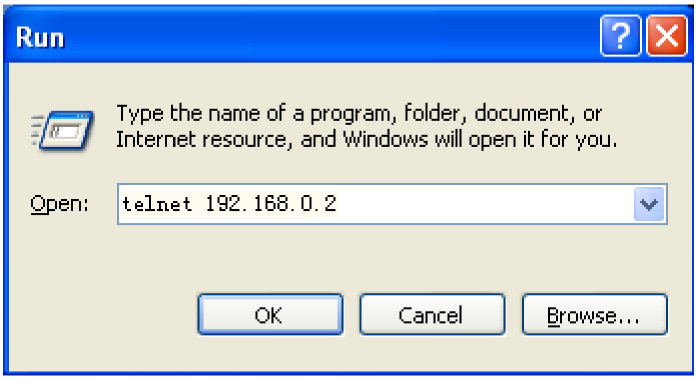
Connected 0:00:03 Auto detect Auto detect SCROLL CAPS NUM Capture

Figure 5 CLI

2.3 Access through Telnet

The precondition for accessing a switch by Telnet is the normal communication between the PC and the switch.

1. Enter "**telnet** *IP address*" in the Run dialog box, as shown in Figure 6.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

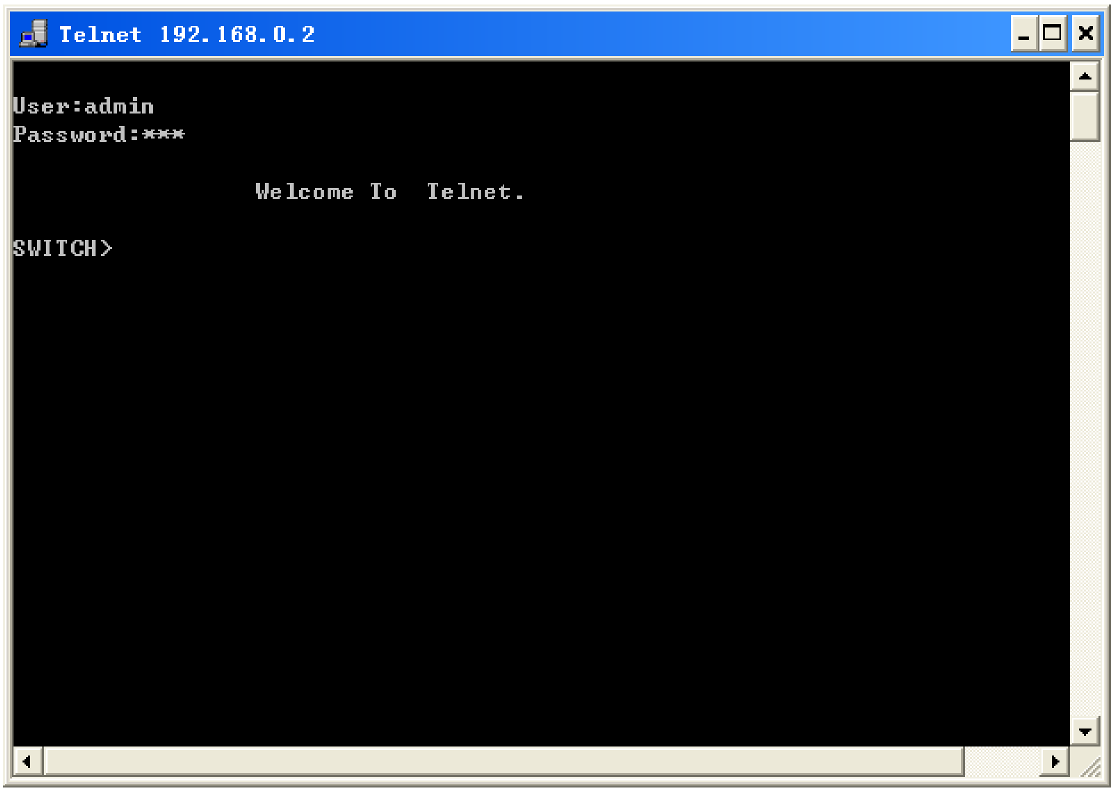
Open: telnet 192.168.0.2

Figure 6 Telnet Access

Note:

For details about how to confirm the switch IP address, see section 5.1 IP Address.

2. In the Telnet interface, press <Enter> to log in to the switch, as shown in Figure 7.



```
User:admin
Password:***

                  Welcome To  Telnet.

SWITCH>
```

Figure 7 Telnet Interface

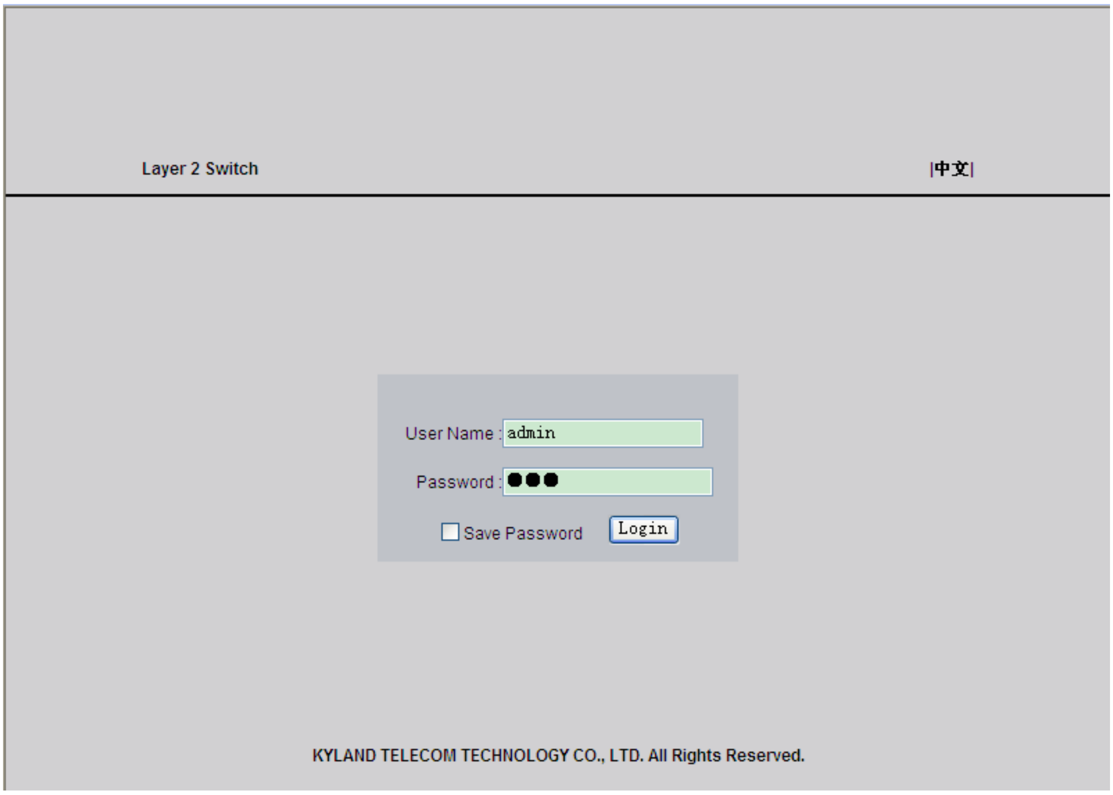
2.4 Access through Web

The precondition of accessing switch by Web is the normal communication of PC and switch.

Note:

IE8.0 or a later version is recommended for the best Web display results.

1. Input "IP address" in the browser address bar. The login interface is displayed, as shown in Figure 8. Input the default user name "admin" and password "123". Click <Login>.



Layer 2 Switch

|中文|

User Name : admin

Password : ●●●

□ Save Password

KYLAND TELECOM TECHNOLOGY CO., LTD. All Rights Reserved.

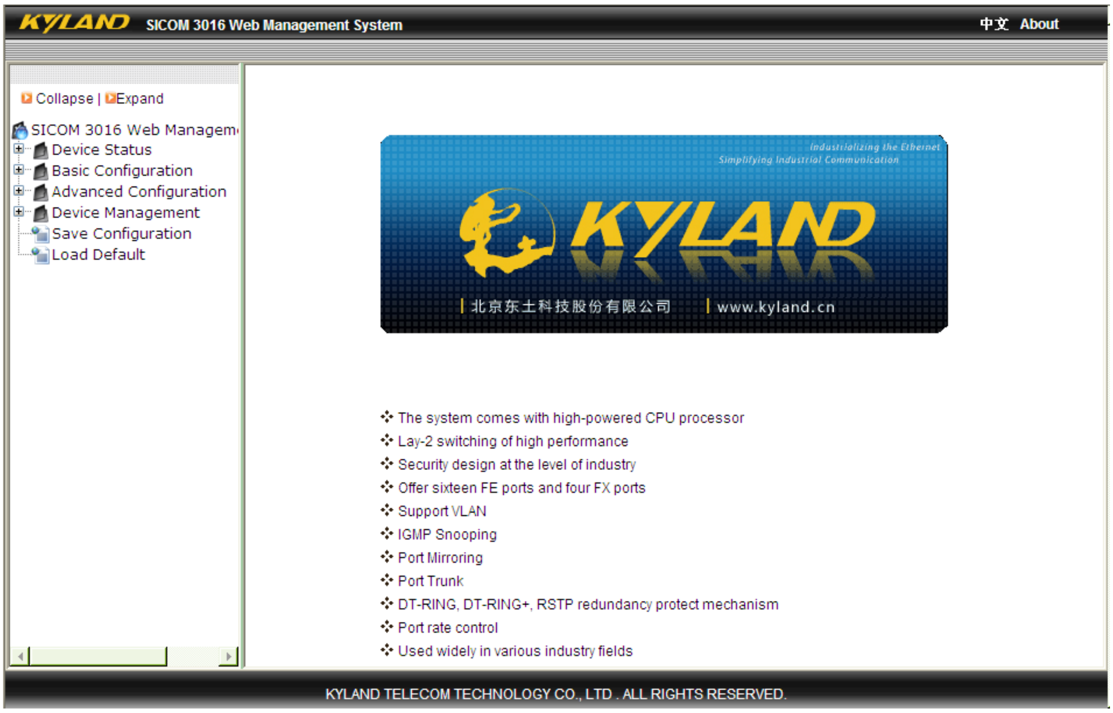
Figure 8 Web Login

The English login interface is displayed by default. You can click <中文> to change to the Chinese login interface.

Note:

For details about how to confirm the switch IP address, see section 5.1 IP Address.

2. After you log in successfully, there is a navigation tree on the left of the interface, as shown in Figure 9.



- The system comes with high-powered CPU processor
- Lay-2 switching of high performance
- Security design at the level of industry
- Offer sixteen FE ports and four FX ports
- Support VLAN
- IGMP Snooping
- Port Mirroring
- Port Trunk
- DT-RING, DT-RING+, RSTP redundancy protect mechanism
- Port rate control
- Used widely in various industry fields

Figure 9 Web Login

You can expand or collapse the navigation tree by clicking <Expand> or <Collapse> on the top of the navigation tree. You can perform corresponding operations by clicking [Save Settings] or [Load Default] in the top menu. In the upper right corner, you can click <中文> to switch to the Chinese interface and <Logout> to exit the Web interface.

CAUTION

Caution:

After you have restored the default settings, you need to restart the device to make settings take effect.

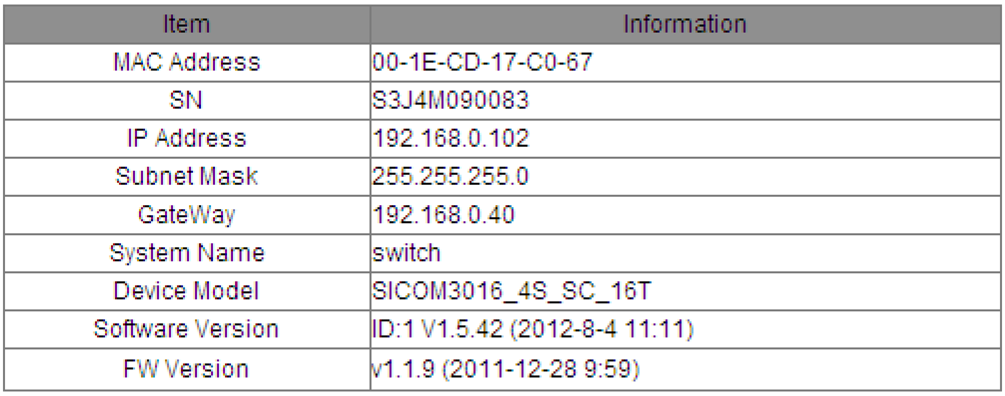
3 Device Management

Click [Device Management] → [Reboot]/[Logout]. You can reboot the device or exit the Web interface. Before rebooting the device, you need to save the current settings as required. If you have saved the settings, the switch automatically configures itself with the saved settings after restart. If you have not saved any settings, the switch restores the factory default settings after restart.

4 Device Status

4.1 Basic Information

The switch basic information includes the MAC address, SN, IP address, subnet mask, gateway, system name, device model, and software version, as shown in Figure 10.

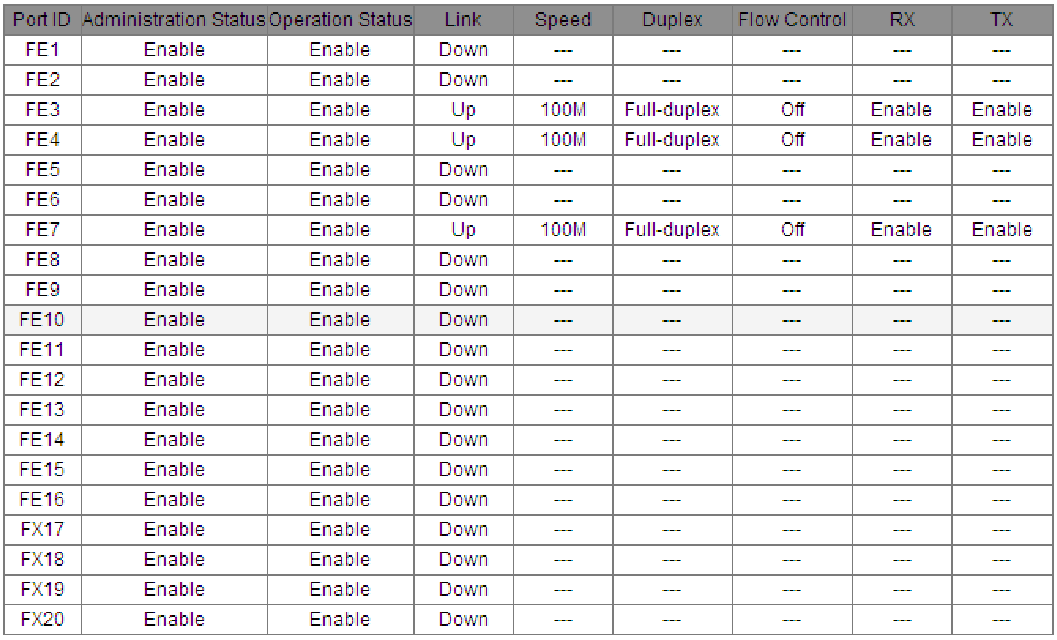


Item	Information
MAC Address	00-1E-CD-17-C0-67
SN	S3J4M090083
IP Address	192.168.0.102
Subnet Mask	255.255.255.0
GateWay	192.168.0.40
System Name	switch
Device Model	SICOM3016_4S_SC_16T
Software Version	ID:1 V1.5.42 (2012-8-4 11:11)
FW Version	v1.1.9 (2011-12-28 9:59)

Figure 10 Basic Information

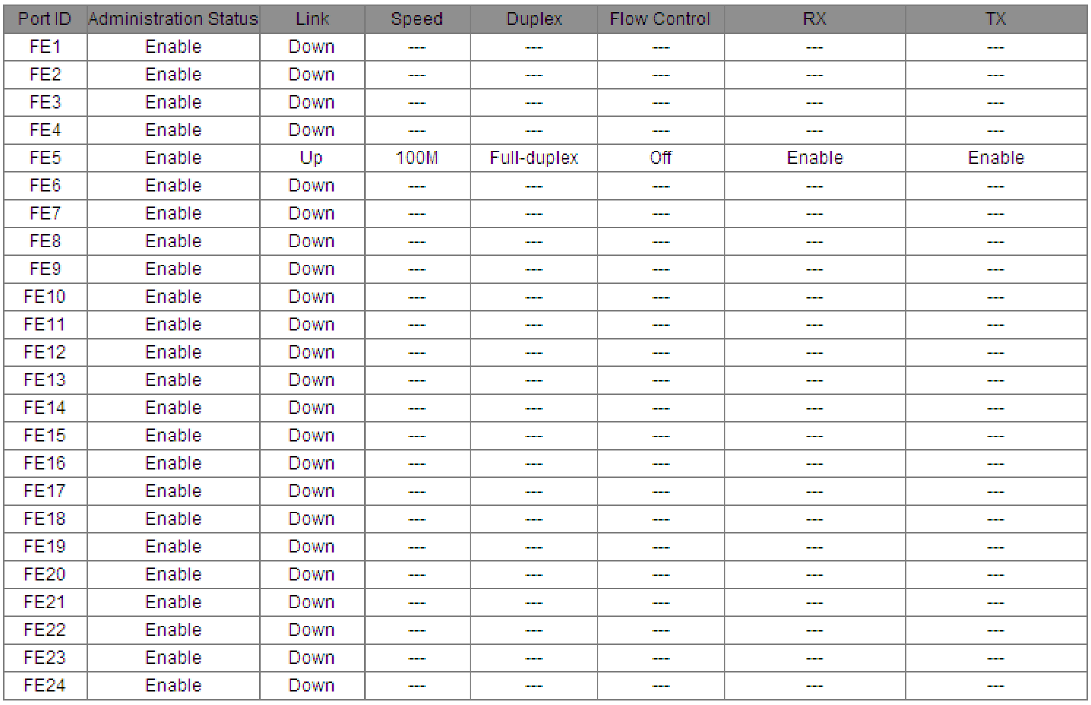
4.2 Port Status

Port status page displays the port number, port type, administration status, operation staus, link status, speed, duplex, and flow control, as shown in Figure 11 and Figure 12.



Port ID	Administration Status	Operation Status	Link	Speed	Duplex	Flow Control	RX	TX
FE1	Enable	Enable	Down	---	---	---	---	---
FE2	Enable	Enable	Down	---	---	---	---	---
FE3	Enable	Enable	Up	100M	Full-duplex	Off	Enable	Enable
FE4	Enable	Enable	Up	100M	Full-duplex	Off	Enable	Enable
FE5	Enable	Enable	Down	---	---	---	---	---
FE6	Enable	Enable	Down	---	---	---	---	---
FE7	Enable	Enable	Up	100M	Full-duplex	Off	Enable	Enable
FE8	Enable	Enable	Down	---	---	---	---	---
FE9	Enable	Enable	Down	---	---	---	---	---
FE10	Enable	Enable	Down	---	---	---	---	---
FE11	Enable	Enable	Down	---	---	---	---	---
FE12	Enable	Enable	Down	---	---	---	---	---
FE13	Enable	Enable	Down	---	---	---	---	---
FE14	Enable	Enable	Down	---	---	---	---	---
FE15	Enable	Enable	Down	---	---	---	---	---
FE16	Enable	Enable	Down	---	---	---	---	---
FX17	Enable	Enable	Down	---	---	---	---	---
FX18	Enable	Enable	Down	---	---	---	---	---
FX19	Enable	Enable	Down	---	---	---	---	---
FX20	Enable	Enable	Down	---	---	---	---	---

Figure 11 Port Status



Port ID	Administration Status	Link	Speed	Duplex	Flow Control	RX	TX
FE1	Enable	Down	---	---	---	---	---
FE2	Enable	Down	---	---	---	---	---
FE3	Enable	Down	---	---	---	---	---
FE4	Enable	Down	---	---	---	---	---
FE5	Enable	Up	100M	Full-duplex	Off	Enable	Enable
FE6	Enable	Down	---	---	---	---	---
FE7	Enable	Down	---	---	---	---	---
FE8	Enable	Down	---	---	---	---	---
FE9	Enable	Down	---	---	---	---	---
FE10	Enable	Down	---	---	---	---	---
FE11	Enable	Down	---	---	---	---	---
FE12	Enable	Down	---	---	---	---	---
FE13	Enable	Down	---	---	---	---	---
FE14	Enable	Down	---	---	---	---	---
FE15	Enable	Down	---	---	---	---	---
FE16	Enable	Down	---	---	---	---	---
FE17	Enable	Down	---	---	---	---	---
FE18	Enable	Down	---	---	---	---	---
FE19	Enable	Down	---	---	---	---	---
FE20	Enable	Down	---	---	---	---	---
FE21	Enable	Down	---	---	---	---	---
FE22	Enable	Down	---	---	---	---	---
FE23	Enable	Down	---	---	---	---	---
FE24	Enable	Down	---	---	---	---	---

Figure 12 Port Status (SICOM2024M)

Port ID

Display the type and ID of ports.

FE: 10/100Base-TX RJ45 port

FX: 100Base-FX port

GE: Gigabit RJ45 port

GX: Gigabit SFP slot

Administration Status

Display the administration status of ports.

Enable: The port is available and permits data transmission.

Disable: The port is locked without data transmission.

Operation Status

Display the operation status of ports.

Link

Display the link status of ports.

Up: The port is in LinkUp state and can communicate normally.

Down: The port is in LinkDown state and cannot communicate normally.

Speed

Display the communication speed of LinkUp ports.

Duplex

Display the duplex mode of LinkUp ports.

Full-duplex: The port can receive and transmit data at the same time.

Half-duplex: The port only receives or transmits data at the same time.

Flow Control

Display the flow control status of LinkUp ports.

RX

Options: Enable/Disable

Enable: The port can receive data.

Disable: The port cannot receive data.

TX

Options: Enable/Disable

Enable: The port can transmit data.

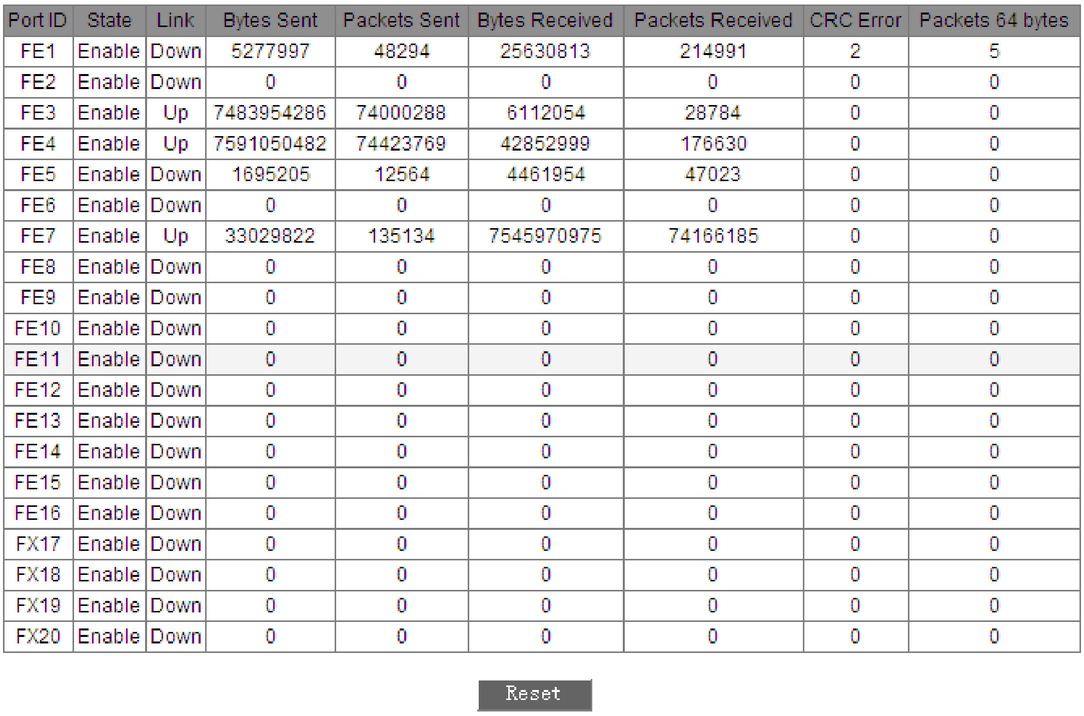
Disable: The port cannot transmit data.

Note:

For details about port settings, see section 5.3 Port Configuration.

4.3 Port Statistics

Port statistics cover the number of bytes/packets that each port sends/receives, CRC errors, and number of packets with less than 64 bytes, as shown in Figure 13.



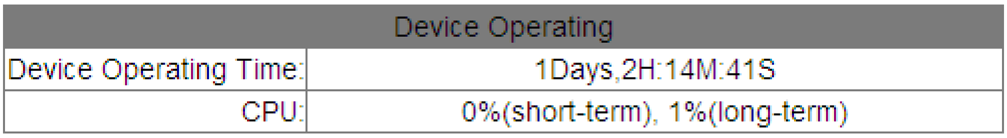
Port ID	State	Link	Bytes Sent	Packets Sent	Bytes Received	Packets Received	CRC Error	Packets 64 bytes
FE1	Enable	Down	5277997	48294	25630813	214991	2	5
FE2	Enable	Down	0	0	0	0	0	0
FE3	Enable	Up	7483954286	74000288	6112054	28784	0	0
FE4	Enable	Up	7591050482	74423769	42852999	176630	0	0
FE5	Enable	Down	1695205	12564	4461954	47023	0	0
FE6	Enable	Down	0	0	0	0	0	0
FE7	Enable	Up	33029822	135134	7545970975	74166185	0	0
FE8	Enable	Down	0	0	0	0	0	0
FE9	Enable	Down	0	0	0	0	0	0
FE10	Enable	Down	0	0	0	0	0	0
FE11	Enable	Down	0	0	0	0	0	0
FE12	Enable	Down	0	0	0	0	0	0
FE13	Enable	Down	0	0	0	0	0	0
FE14	Enable	Down	0	0	0	0	0	0
FE15	Enable	Down	0	0	0	0	0	0
FE16	Enable	Down	0	0	0	0	0	0
FX17	Enable	Down	0	0	0	0	0	0
FX18	Enable	Down	0	0	0	0	0	0
FX19	Enable	Down	0	0	0	0	0	0
FX20	Enable	Down	0	0	0	0	0	0

Figure 13 Port Statistics

You can click <Reset> to restart statistics collection.

4.4 System Operating Information

System operating information includes the device runtime and CPU usage, as shown in Figure 14.



Device Operating	
Device Operating Time:	1Days,2H:14M:41S
CPU:	0%(short-term), 1%(long-term)

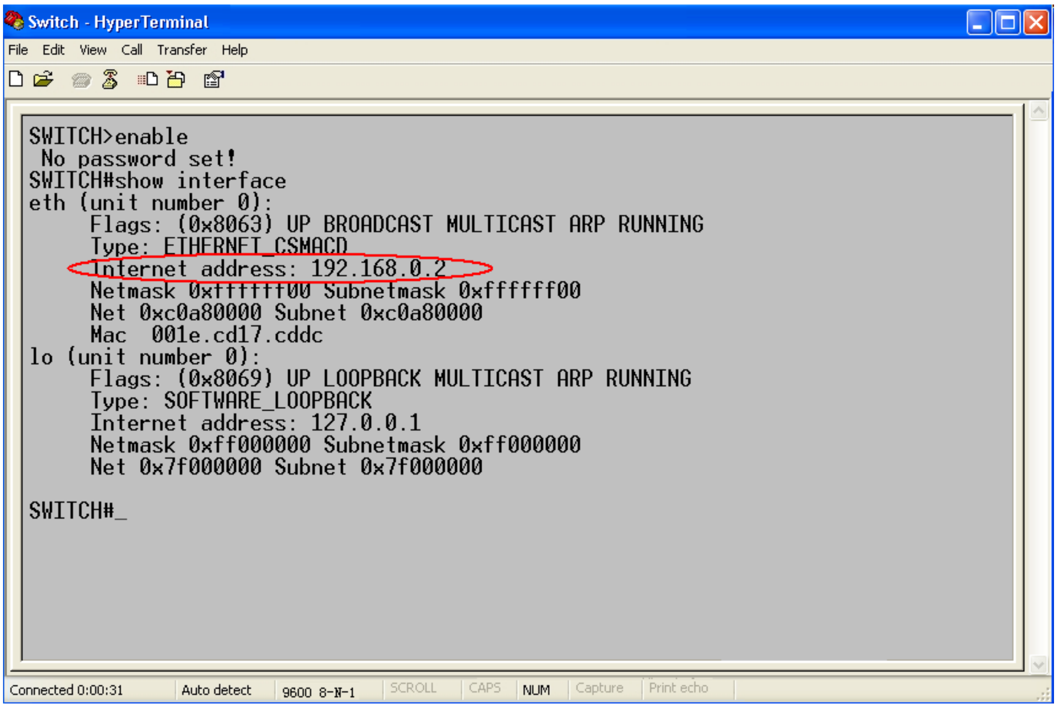
Figure 14 System Operating Information

5 Basic Configuration

5.1 IP Address

1. View the switch IP address by using the console port.

Log in to the switch CLI through the console port. Run the "**show interface**" command in the management view to view the switch IP address. As shown in Figure 15, the IP address is circled in red.



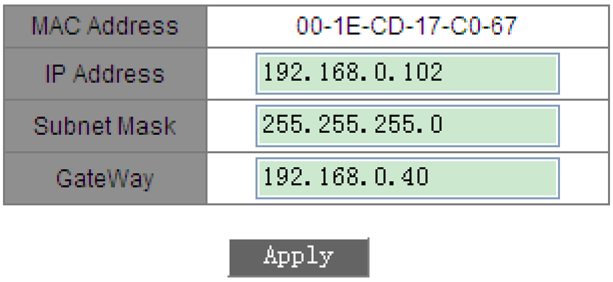
```
SWITCH>enable
 No password set!
SWITCH#show interface
eth (unit number 0):
     Flags: (0x8063) UP BROADCAST MULTICAST ARP RUNNING
     Type: ETHERNET_CSMACD
     Internet address: 192.168.0.2
     Netmask 0xffffff00 Subnetmask 0xffffff00
     Net 0xc0a80000 Subnet 0xc0a80000
     Mac  001e.cd17.cddc
lo (unit number 0):
     Flags: (0x8069) UP LOOPBACK MULTICAST ARP RUNNING
     Type: SOFTWARE_LOOPBACK
     Internet address: 127.0.0.1
     Netmask 0xff000000 Subnetmask 0xff000000
     Net 0x7f000000 Subnet 0x7f000000

SWITCH#_
```

Figure 15 Viewing IP Address

2. Set the IP address.

Switch IP address and gateway can be configured manually, as shown in Figure 16.



MAC Address	00-1E-CD-17-C0-67
IP Address	192.168.0.102
Subnet Mask	255.255.255.0
GateWay	192.168.0.40

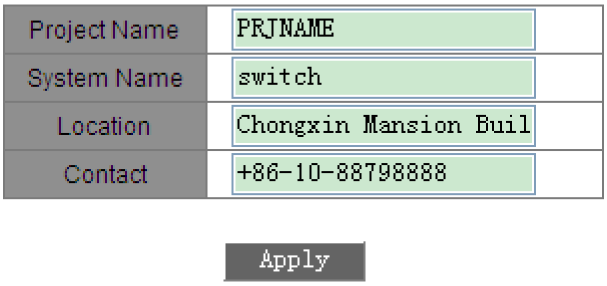
Figure 16 IP Address

Caution:

- IP address and gateway must be in the same network segment; otherwise, the IP address cannot be modified.
- For the series switches, the change in IP address will take effect only after the device is restarted.

5.2 Basic Information

Basic information includes the project name, system name, location and contact, as shown in Figure 17.



Project Name	PRJNAME
System Name	switch
Location	Chongxin Mansion Buil
Contact	+86-10-88798888

Figure 17 Device Information

Project Name

Range: 1~64 characters

System Name

Range: 1~32 characters

Location

Value: English/Chinese characters

Range: 1~255 characters (One Chinese character occupies the position of two English characters.)

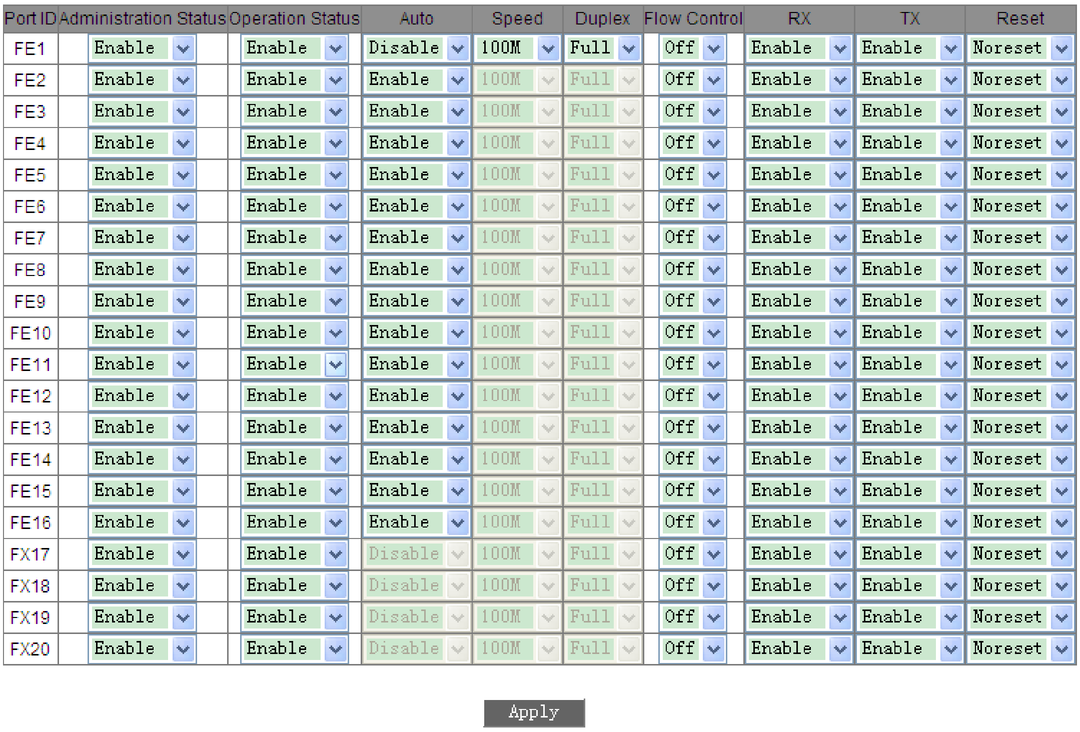
Contact

Value: English/Chinese characters

Range: 1~32 characters (One Chinese character occupies the position of two English characters.)

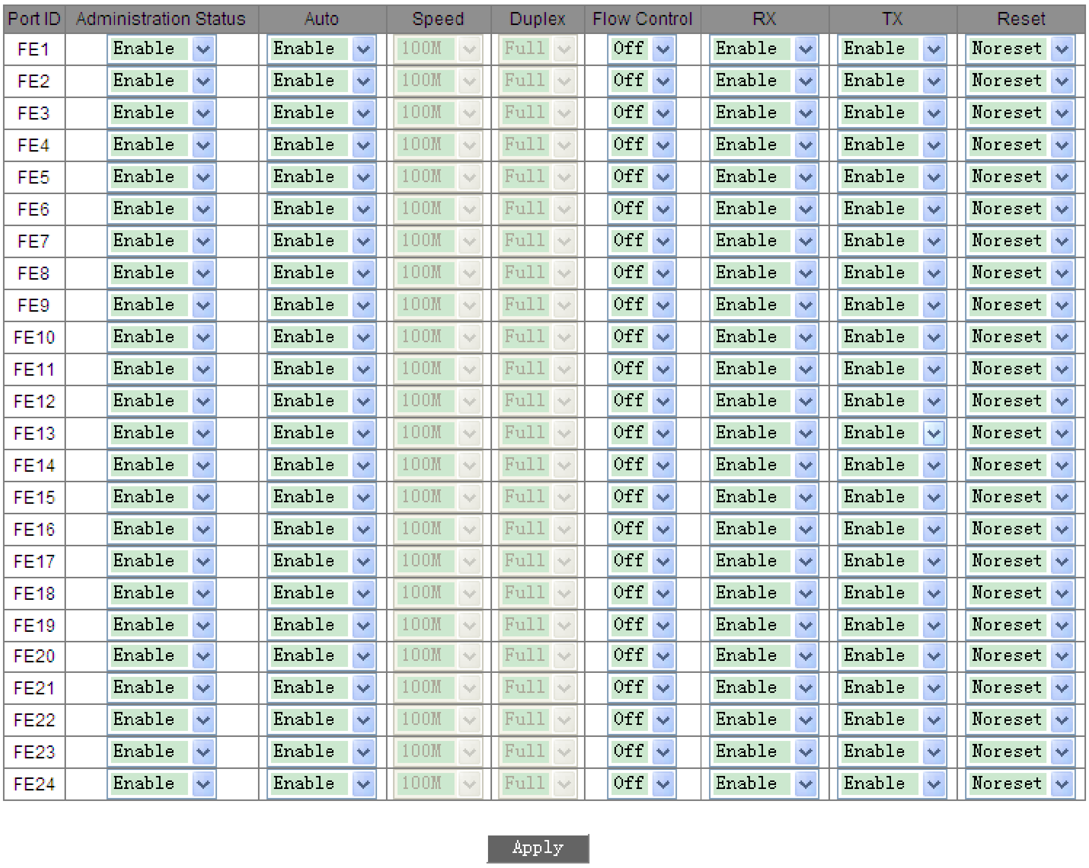
5.3 Port Configuration

In port configuration, you can configure port status, port speed, flow control, and other information, as shown in Figure 18 and Figure 19.



Port ID	Administration Status	Operation Status	Auto	Speed	Duplex	Flow Control	RX	TX	Reset
FE1	Enable	Enable	Disable	100M	Full	Off	Enable	Enable	Noreset
FE2	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE3	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE4	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE5	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE6	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE7	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE8	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE9	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE10	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE11	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE12	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE13	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE14	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE15	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE16	Enable	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FX17	Enable	Enable	Disable	100M	Full	Off	Enable	Enable	Noreset
FX18	Enable	Enable	Disable	100M	Full	Off	Enable	Enable	Noreset
FX19	Enable	Enable	Disable	100M	Full	Off	Enable	Enable	Noreset
FX20	Enable	Enable	Disable	100M	Full	Off	Enable	Enable	Noreset

Figure 18 Port Configuration



Port ID	Administration Status	Auto	Speed	Duplex	Flow Control	RX	TX	Reset
FE1	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE2	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE3	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE4	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE5	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE6	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE7	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE8	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE9	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE10	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE11	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE12	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE13	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE14	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE15	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE16	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE17	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE18	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE19	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE20	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE21	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE22	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE23	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset
FE24	Enable	Enable	100M	Full	Off	Enable	Enable	Noreset

Figure 19 Port Configuration (SICOM2024M)

Administration Status

Options: Enable/Disable

Default: Enable

Function: Allow data transmission on port or not.

Description: Enable indicates the port is enabled and permits data transmission; Disable indicates the port is disabled and disallows data transmission. This option directly affects the hardware status of the port and triggers port alarms.

Operation Status

Description: When the administration status is Enable, the operation status is set to Enable forcibly; when the administration status is Disable, the operation status is set to Disable forcibly.

Auto

Options: Enable/Disable

Default: Enable

Function: Configure the auto-negotiation status of ports.

Description: When Auto is set to Enable, the port speed and duplex mode will be automatically negotiated according to port connection status; when Auto is set to Disable, the port speed and duplex mode can be configured.

Caution:

100Base-FX ports are set to Disable forcibly.

Speed

Options: 10M/100M/1000M

Function: Configure the speed of ports forcibly.

Description: When Auto is set to Disable, the port speed can be configured.

Duplex

Options: Half/Full

Function: Configure the duplex mode of ports.

Description: When Auto is set to Disable, the port duplex mode can be configured.

Caution:

➢10/100Base-TX ports can be set to auto-negotiation, 10M&full duplex, 10M&half duplex, 100M&full duplex, or 100M&half duplex.

➢100Base-FX ports are set to 100M&full duplex.

➢1000M fiber ports can be set to auto-negotiation and 1000M&full duplex.

You are advised to enable auto-negotiation for each port to avoid the connection problems caused by mismatched port configuration. If you want to force port speed/duplex mode, please make sure the same speed configuration in the connected ports at both ends.

Flow Control

Options: Off/On

Default: Off

Function: Enable/Disable flow control function on the designated port.

Description: Once the flow control function is enabled, the port will inform the sender to slow the transmitting speed to avoid packet loss by algorithm or protocol when the port-received flow is bigger than the size of port cache. If the devices work in different duplex modes (half/full), their flow control is realized in different ways. If the devices work in full duplex mode, the receiving end will send a special frame (Pause frame) to inform the sending end to stop sending packets. When the sender receives the Pause frame, it will stop sending packets for a period of "wait time" carried in the Pause frame and continue sending packets once the "wait time" ends. If the devices work in half duplex mode, they support back pressure flow control. The receiving end creates a conflict or a carrier signal. When the sender detects the conflict or the carrier wave, it will take backoff to postpone the data transmission.

RX

Options: Enable/Disable

Default: Enable

Function: Allow the port to receive data or not.

Description: Enable indicates the port can receive data; Disable indicates the port cannot receive data.

TX

Options: Enable/Disable

Default: Enable

Function: Allow the port to receive data or not.

Description: Enable indicates the port can transmit data; Disable indicates the port cannot transmit data.

Reset

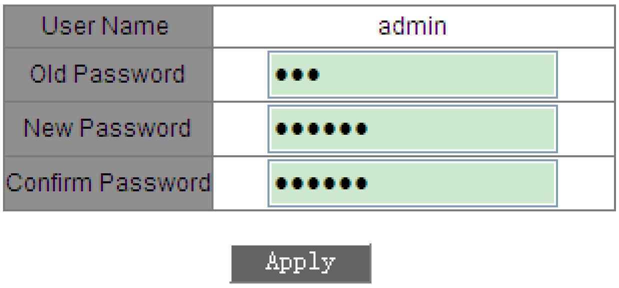
Options: Reset/Nonreset

Default: Nonreset

Function: Reset the port or not.

5.4 Password Change

You can change the password for user name "admin", as shown in Figure 20.



User Name	admin
Old Password	•••
New Password	••••••
Confirm Password	••••••

Figure 20 Changing the Password

5.5 Software Update

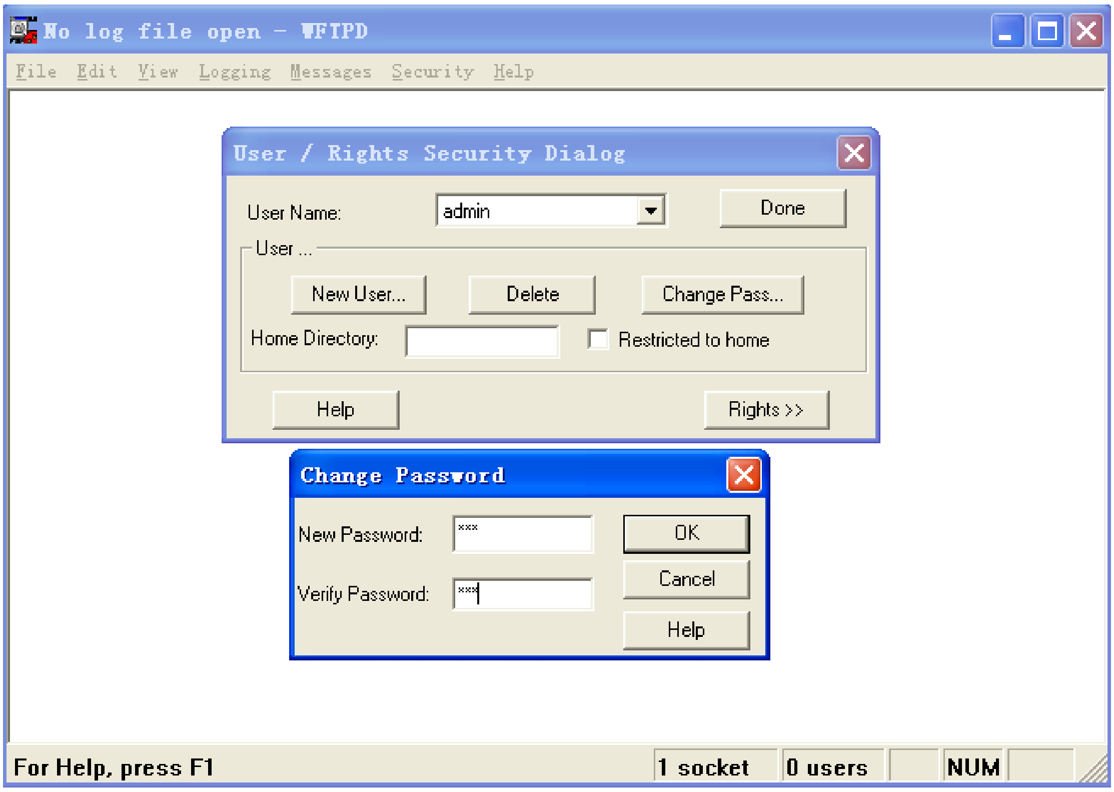
Software updates may help the switch to improve its performance. For this series switches, software updates include BootROM software version update and system software version update. The BootROM software version should be updated before the system software version. If the BootROM version does not change, you can update only the system software version.

The software version update requires an FTP server.

5.5.1 Software Update through FTP

Install an FTP server. The following uses WFTPD software as an example to introduce FTP server configuration and software update.

1. Click [Security] → [Users/Rights]. The "Users/Rights Security Dialog" dialog box is displayed. Click <New User> to create a new FTP user, as shown in Figure 21. Create a user name and password, for example, user name "admin" and password "123". Click <OK>.



User Name: admin

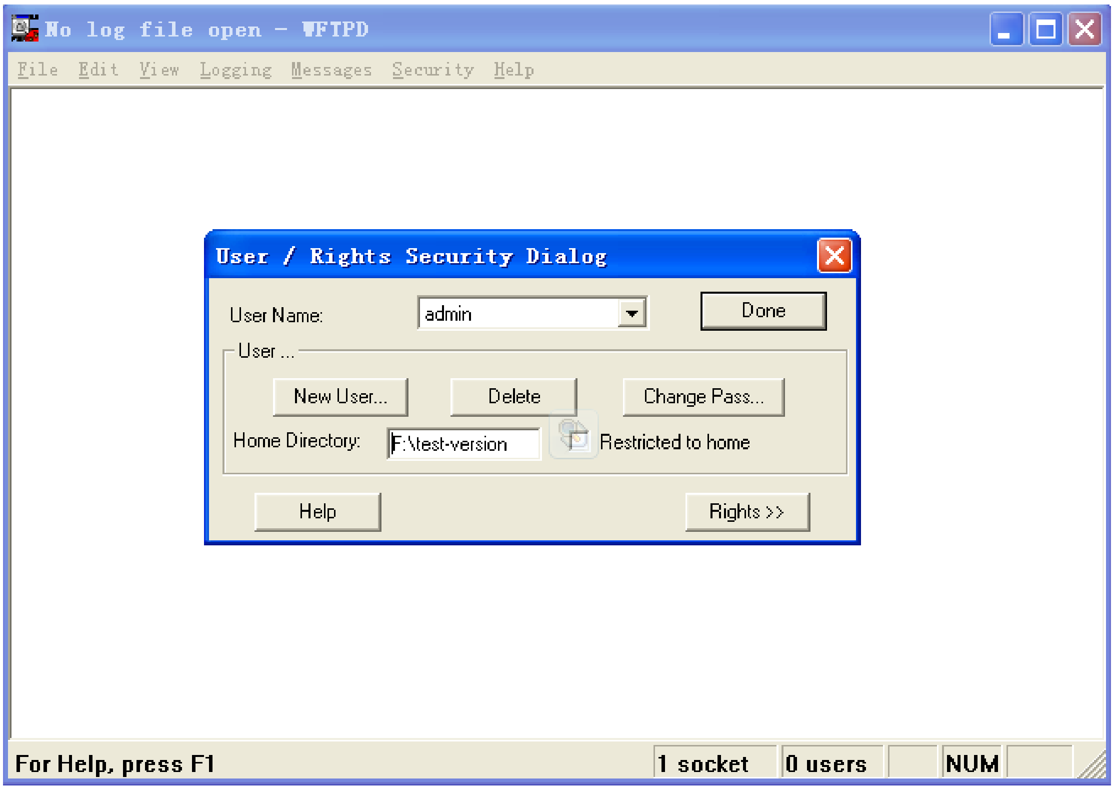
□ Restricted to home

New Password: ***

Verify Password: ***

Figure 21 Creating a New FTP User

2. Input the storage path of the update file in "Home Directory", as shown in Figure 22. Click <Done>.



User Name: admin

Home Directory: F:\test-version

Figure 22 File Location

3. To update the BootROM software, input the following command in the management view.

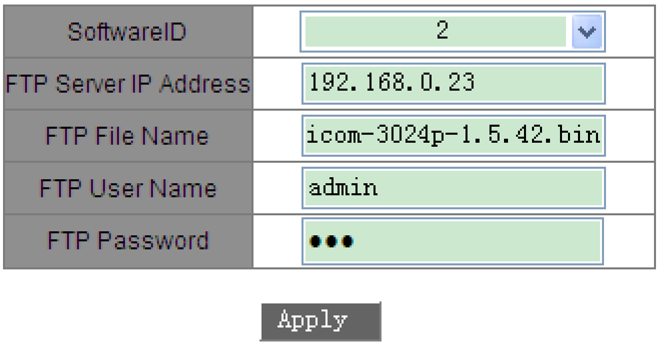
Switch#**update bootrom** *File_name Ftp_server_ip_address User_name Password*

Table 2 lists the parameter descriptions.

Table 2 Parameters for BootROM Update by FTP

Parameter	**Description**
File_name	Name of the BootROM version
Ftp_server_ip_address	IP address of the FTP server
User_name	Created FTP user name
Password	Created FTP password

4. Figure 23 shows the software update page. Enter the IP address of the FTP server, file name (on the server), FTP user name, and password. Click <Apply>.



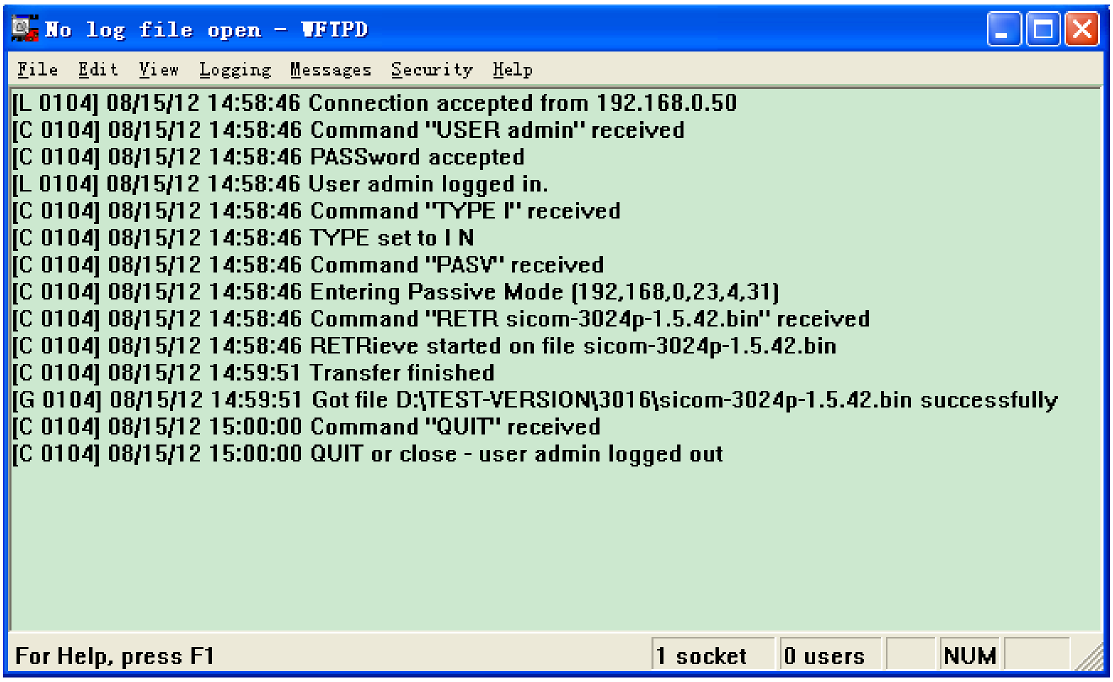
SoftwareID	2
FTP Server IP Address	192.168.0.23
FTP File Name	icom-3024p-1.5.42.bin
FTP User Name	admin
FTP Password	●●●

Figure 23 Software Update through FTP

Warning:

- Only the software version in inactive state can be used for update through Web.
- The file name must contain an extension. Otherwise, the update may fail.

5. Make sure the normal communication between the FTP server and the switch, as shown in Figure 24.



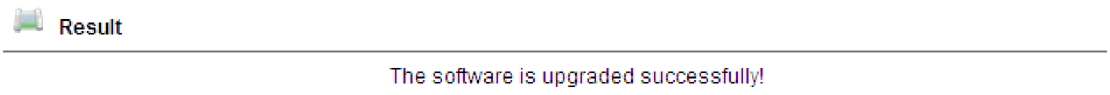
```
[L 0104] 08/15/12 14:58:46 Connection accepted from 192.168.0.50
[C 0104] 08/15/12 14:58:46 Command "USER admin" received
[C 0104] 08/15/12 14:58:46 PASSword accepted
[L 0104] 08/15/12 14:58:46 User admin logged in.
[C 0104] 08/15/12 14:58:46 Command "TYPE I" received
[C 0104] 08/15/12 14:58:46 TYPE set to I N
[C 0104] 08/15/12 14:58:46 Command "PASV" received
[C 0104] 08/15/12 14:58:46 Entering Passive Mode (192,168,0,23,4,31)
[C 0104] 08/15/12 14:58:46 Command "RETR sicom-3024p-1.5.42.bin" received
[C 0104] 08/15/12 14:58:46 RETRieve started on file sicom-3024p-1.5.42.bin
[C 0104] 08/15/12 14:59:51 Transfer finished
[G 0104] 08/15/12 14:59:51 Got file D:\TEST-VERSION\3016\sicom-3024p-1.5.42.bin successfully
[C 0104] 08/15/12 15:00:00 Command "QUIT" received
[C 0104] 08/15/12 15:00:00 QUIT or close - user admin logged out
```

Figure 24 Normal Communication between FTP Server and Switch

Caution:

To display update log information as shown in Figure 24, you need to click [Logging] → [Log Options] in WFTPD and select Enable Logging and the log information to be displayed.

6. When the update is completed as shown in Figure 25, please reboot the device and open the Switch Basic Information page to check whether the update succeeded and the new version is active.


Result

The software is upgraded successfully!

Figure 25 Successful Software Update through FTP

Warning:

➢In the software update process, keep the FTP server software running.

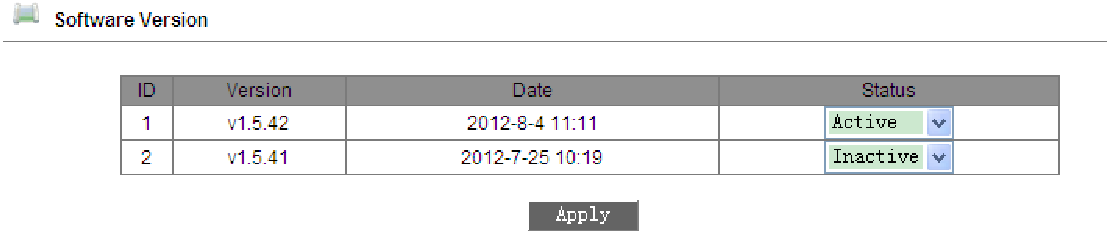
➢When update completes, reboot the device to make the new version take effect.

➢If update fails, do not reboot the device to avoid the loss of software file and startup anomaly.

5.6 Software Version Query

Two software versions can be downloaded to the switch, but only one can be in active state at a time. In the Web UI, you can update only the inactive version.

By querying software versions, you can learn the IDs, release dates, and statuses of the two versions, as shown in Figure 26.



Software Version

ID	Version	Date	Status
1	v1.5.42	2012-8-4 11:11	Active
2	v1.5.41	2012-7-25 10:19	Inactive

Figure 26 Software Version Query

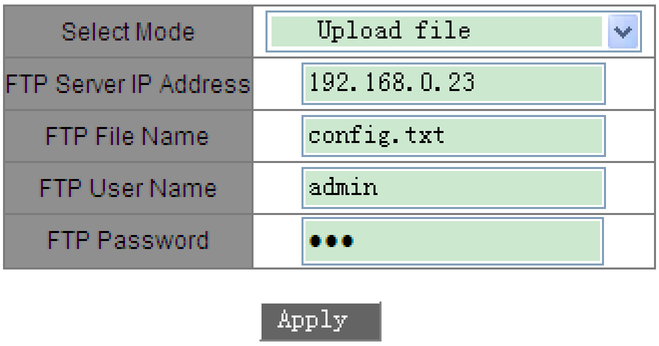
5.7 Configuration Upload/Download

Configuration backup function can save current switch configuration files on the server. When the switch configuration is changed, you can download the original configuration files from the server to switch through FTP.

File uploading is to upload the switch configuration files to the server and save them to *.doc and *.txt files. File downloading is to download the saved configuration files from the server to switch, as shown in Figure 27 and Figure 28.

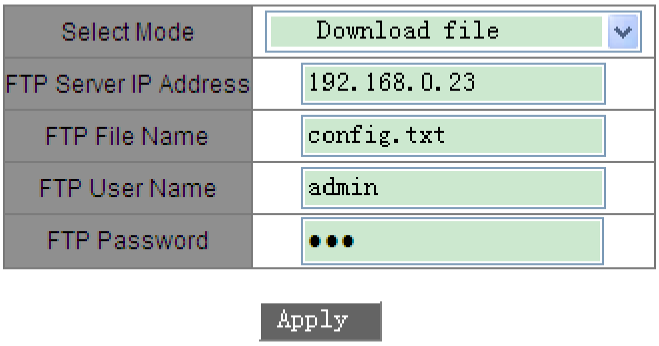
Caution:

After configuration file is downloaded to the switch, you need to restart the switch to make the configuration take effect.



Select Mode	Upload file
FTP Server IP Address	192.168.0.23
FTP File Name	config.txt
FTP User Name	admin
FTP Password	●●●

Figure 27 Configuration File Upload



Select Mode	Download file
FTP Server IP Address	192.168.0.23
FTP File Name	config.txt
FTP User Name	admin
FTP Password	●●●

Figure 28 Configuration File Download

6 Advanced Configuration

6.1 Port Rate Limiting

6.1.1 Overview

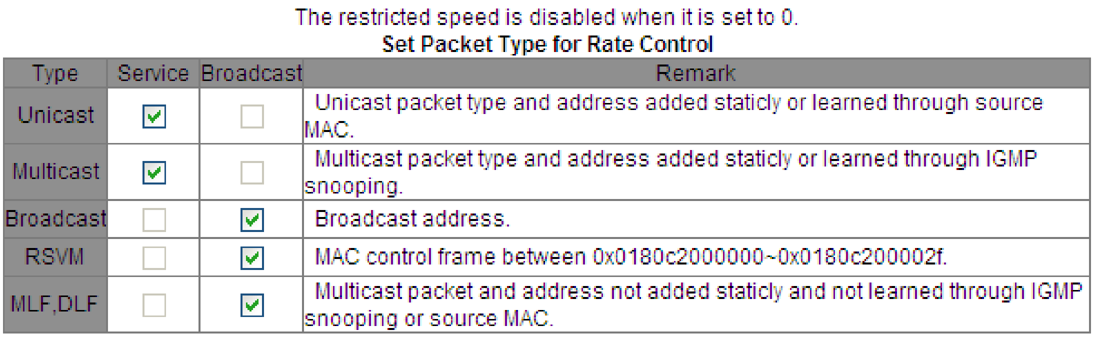
Port rate limiting is to limit the rate packets received or transmitted by a port and discard the packets whose rate exceeds the threshold. The function takes effect on all packets at the egress but only certain types of packets at the ingress.

The following packets are controlled at the ingress.

- Unicast packets: indicate the unicast packets added statically or whose source MAC addresses are learned.
- Multicast packets: indicate the packets added statically or learned through IGMP Snooping or GMRP.
- Broadcast packets: indicate the packets with the destination MAC address of FF:FF:FF:FF:FF:FF.
- Reserved multicast packets: indicate the packets with MAC addresses in the range of 0x0180c2000000 to 0x0180c200002f.
- Unknown multicast packets: indicate the packets neither added statically nor learned through IGMP Snooping or GMRP.
- Unknown unicast packets: indicate the packets neither added statically nor whose source MAC addresses are learned.
- Unknown source packets: indicate the packets with unknown source MAC addresses.

6.1.2 Web Configuration

1. Select the packet types for rate control, as shown in Figure 29 and Figure 30.

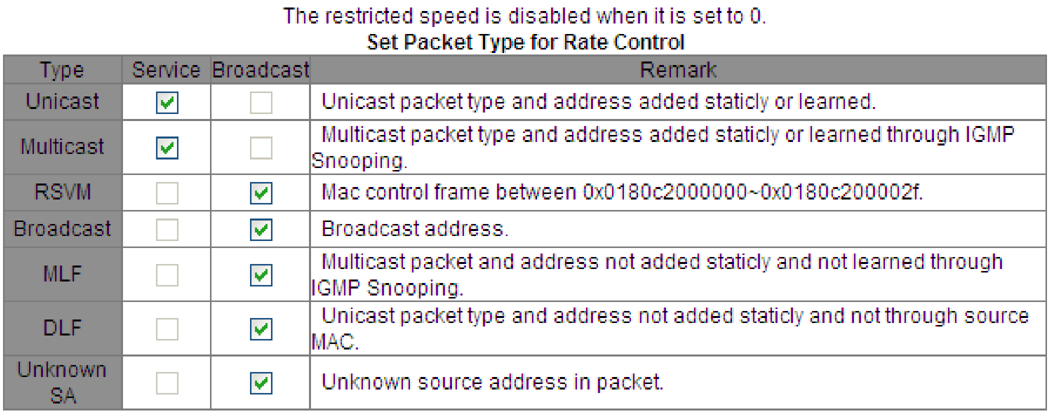


The restricted speed is disabled when it is set to 0.

Set Packet Type for Rate Control

Type	Service	Broadcast	Remark
Unicast	☑	□	Unicast packet type and address added staticly or learned through source MAC.
Multicast	☑	□	Multicast packet type and address added staticly or learned through IGMP snooping.
Broadcast	□	☑	Broadcast address.
RSVM	□	☑	MAC control frame between 0x0180c2000000~0x0180c200002f.
MLF,DLF	□	☑	Multicast packet and address not added staticly and not learned through IGMP snooping or source MAC.

Figure 29 Packet Types for Rate Control



The restricted speed is disabled when it is set to 0.

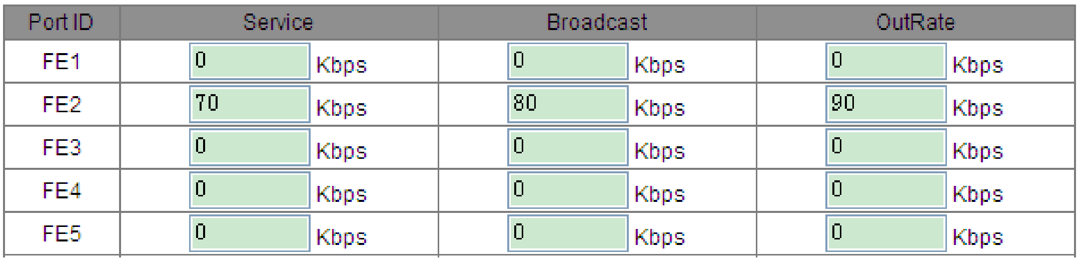
Set Packet Type for Rate Control

Type	Service	Broadcast	Remark
Unicast	☑	□	Unicast packet type and address added staticly or learned.
Multicast	☑	□	Multicast packet type and address added staticly or learned through IGMP Snooping.
RSVM	□	☑	Mac control frame between 0x0180c2000000~0x0180c200002f.
Broadcast	□	☑	Broadcast address.
MLF	□	☑	Multicast packet and address not added staticly and not learned through IGMP Snooping.
DLF	□	☑	Unicast packet type and address not added staticly and not through source MAC.
Unknown SA	□	☑	Unknown source address in packet.

Figure 30 Packet Types for Rate Control_SICOM8000

The receiver classifies rate control into two types: service rate control and broadcast rate control. Each packet can be added to only one rate control type.

2. Configure port rate control, as shown in Figure 31.



Port ID	Service	Broadcast	OutRate
FE1	0 Kbps	0 Kbps	0 Kbps
FE2	70 Kbps	80 Kbps	90 Kbps
FE3	0 Kbps	0 Kbps	0 Kbps
FE4	0 Kbps	0 Kbps	0 Kbps
FE5	0 Kbps	0 Kbps	0 Kbps

Figure 31 Port Rate Control

Service/Broadcast

Range: 64~1000000Kbps

Function: Configure rate control for packets on the port. Packets whose rate is higher than the specified value are discarded.

Description: The ingress rate for a 100M port ranges from 64 to 100000Kbps.

The ingress rate for a 1000M port ranges from 64 to 100000Kbps.

OutRate

Range: 64~1000000Kbps

Function: Limit the rate of packets forwarded by a port.

Description: The egress rate for a 100M port ranges from 64 to 100000Kbps.

The ingress rate for a 1000M port ranges from 64 to 100000Kbps.

Caution:

If a rate value is set to 0, rate control is disabled on the port.

6.1.3 Typical Configuration Example

Set the rate threshold of unicast and multicast packets on port 2 to 70Kbps, reserved multicast, unknown multicast, and unicast packets to 80Kbps, and outgoing rate to 90Kbps.

Configuration steps:

1. Select unicast and multicast packets in the Service column, and reserved multicast, unknown multicast, unicast, and broadcast packets in the Broadcast column, as shown in Figure 29 or Figure 30.
2. On port 2, set the service rate threshold to 70Kbps, broadcast rate threshold to 80Kbps, and outgoing rate to 90Kbps, as shown in Figure 31.

6.2 VLAN

6.2.1 Overview

One LAN can be divided into multiple logical Virtual Local Area Networks (VLANs). A device can only communicate with the devices on the same VLAN. As a result, broadcast packets are restricted to a VLAN, optimizing LAN security.

VLAN partition is not restricted by physical location. Each VLAN is regarded as a logical network. If a host in one VLAN needs to send data packets to a host in another VLAN, a router or layer-3 device must be involved.

6.2.2 Principle

To enable network devices to distinguish packets from different VLANs, fields for identifying VLANs need to be added to packets. At present, the most commonly used protocol for VLAN identification is IEEE802.1Q. Table 3 shows the structure of an 802.1Q frame.

Table 3 802.1Q Frame Structure

DA	SA	802.1Q Header				Length/Type	Data	FCS
		Type	PRI	CFI	VID			

A 4-byte 802.1Q header, as the VLAN tag, is added to the traditional Ethernet data frame.

Type: 16 bits. It is used to identify a data frame carrying a VLAN tag. The value is 0x8100.

PRI: three bits, identifying the 802.1p priority of a packet.

CFI: one bit. 0 indicates Ethernet, and 1 indicates token ring.

VID: 12 bits, indicating the VLAN number. The value ranges from 1 to 4093. 0, 4094, and 4095 are reserved values.

Note:

- VLAN 1 is the default VLAN and cannot be manually created and deleted.
- Reserved VLANs are reserved to realize specific functions by the system and cannot be manually created and deleted.

The packet containing 802.1Q header is a tagged packet; the one without 802.1Q header is an untagged packet. All packets carry an 802.1Q tag in the switch.

6.2.3 Port-based VLAN

VLAN partition can be either port-based or MAC address-based. This series switches support port-based VLAN partition. VLAN members can be defined based on switch ports. After a port is added to a specified VLAN, the port can forward the packets with the tag for the VLAN.

1.Port Type

Ports fall into two types according to how they handle VLAN tags when they forward packets.

- Untag port: Packets forwarded by an Untag port do not have VLAN tags. Untag ports are usually used to connect to terminals that do not support 802.1Q. By default, all switch ports are Untag ports and belong to VLAN1.
- Tag port: All packets forwarded by a Tag port carry a VLAN tag. Tag ports are usually used to connect network transmission devices.

2.PVID

Each port has a PVID. When receiving an untagged packet, a port adds a tag to the packet according to the PVID.

The port PVID is the VLAN ID of the Untag port. By default, all ports' PVID is VLAN 1.

Table 4 shows how the switch processes received and forwarded packets according to the port type and PVID.

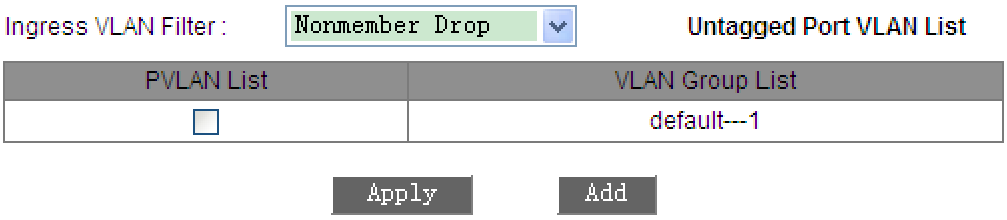
Table 4 Different Processing Modes for Packets

Processing Received Packets		**Processing Packets to Be Forwarded**	
Untagged packets	**Tagged packets**	**Port Type**	**Packet Processing**
Add PVID tags to untagged packets.	➢ If the VLAN ID in a packet is in the list of VLANs allowed through, accept the	Untag	Forward the packet after removing the tag.
		Tag	Keep the tag and forward the packet.

	packet. ➢ If the VLAN ID in a packet is not in the list of VLANs allowed through, discard the packet.		

6.2.4 Web Configuration

1.Configure the VLAN transparent transmission mode, as shown in Figure 32.



Ingress VLAN Filter : Nonmember Drop

Untagged Port VLAN List

PVLAN List	VLAN Group List
□	default---1

Figure 32 Configuring VLAN Transparent Transmission Mode

Ingress VLAN Filter

Options: Nonmember Drop/Nonmember Forward

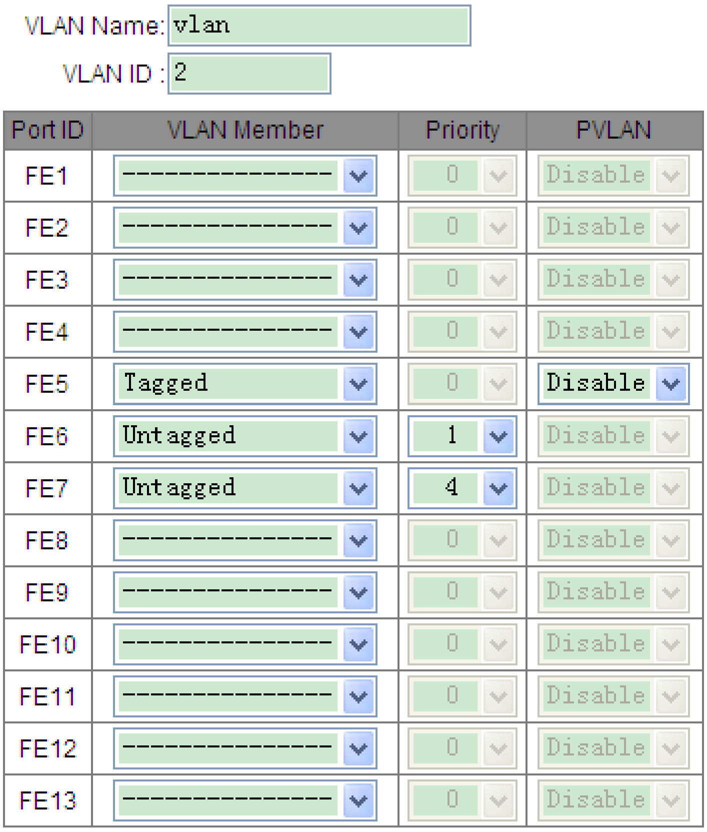
Default: Nonmember Drop

Function: Configure the VLAN transparent transmission mode.

Description: The transparent transmission mode indicates whether the switch checks incoming packets on a port. If Nonmember Drop is selected, a packet is discarded when the VLAN tag of the packet is different from the VLAN of the port. If Nonmember Forward is selected, a packet is accepted when the VLAN tag of the packet is identical with that of any other connected port on the switch; otherwise, the packet is discarded.

2.Create a VLAN.

Click <Add> in Figure 32 to create a VLAN. As shown in Figure 33, select the ports to be added to the VLAN and set port parameters.



VLAN Name: vlan

VLAN ID : 2

Port ID	VLAN Member	Priority	PVLAN
FE1	---------------	0	Disable
FE2	---------------	0	Disable
FE3	---------------	0	Disable
FE4	---------------	0	Disable
FE5	Tagged	0	Disable
FE6	Untagged	1	Disable
FE7	Untagged	4	Disable
FE8	---------------	0	Disable
FE9	---------------	0	Disable
FE10	---------------	0	Disable
FE11	---------------	0	Disable
FE12	---------------	0	Disable
FE13	---------------	0	Disable

Figure 33 VLAN Configuration

VLAN Name

Range: 1~31 characters

Function: Set the VLAN name.

VLAN ID

Range: 2~4093

Function: Configure the VLAN ID.

Description: VLAN ID is used to distinguish different VLANs. This series switches support a maximum of 256 VLANs.

VLAN Member

Options: Tagged/Untagged

Function: Select the type of the port in the VLAN.

Priority

Range: 0~7

Default: 0

Function: Set the default priority of the port. When adding an 802.1Q tag to an untagged packet, the value of the PRI field is the priority.

PVLAN

Options: Enable/Disable

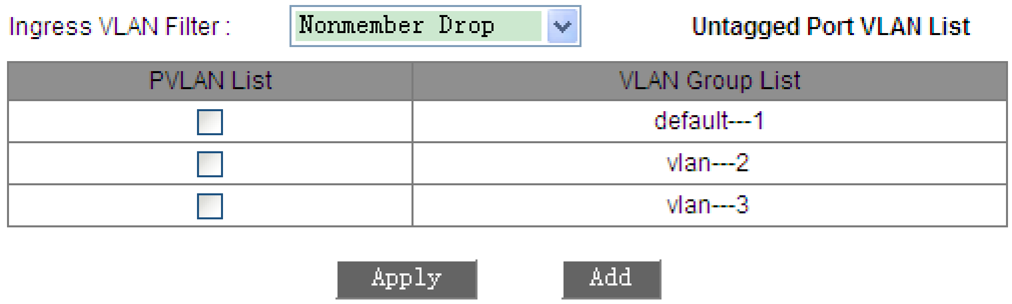
Default: Disable

Function: To add a Tag port to a VLAN, you need to enable or disable PVLAN. For details about PVLAN, see the next chapter.

Caution:

An Untag port can be added to only one VLAN. The VLAN ID is the PVID of the port. The default value is 1. A Tag port can be added to multiple VLANs.

3. View the VLAN list, as shown in Figure 34.



Ingress VLAN Filter : Nonmember Drop

Untagged Port VLAN List

PVLAN List	VLAN Group List
□	default---1
□	vlan---2
□	vlan---3

Figure 34 Viewing VLAN List

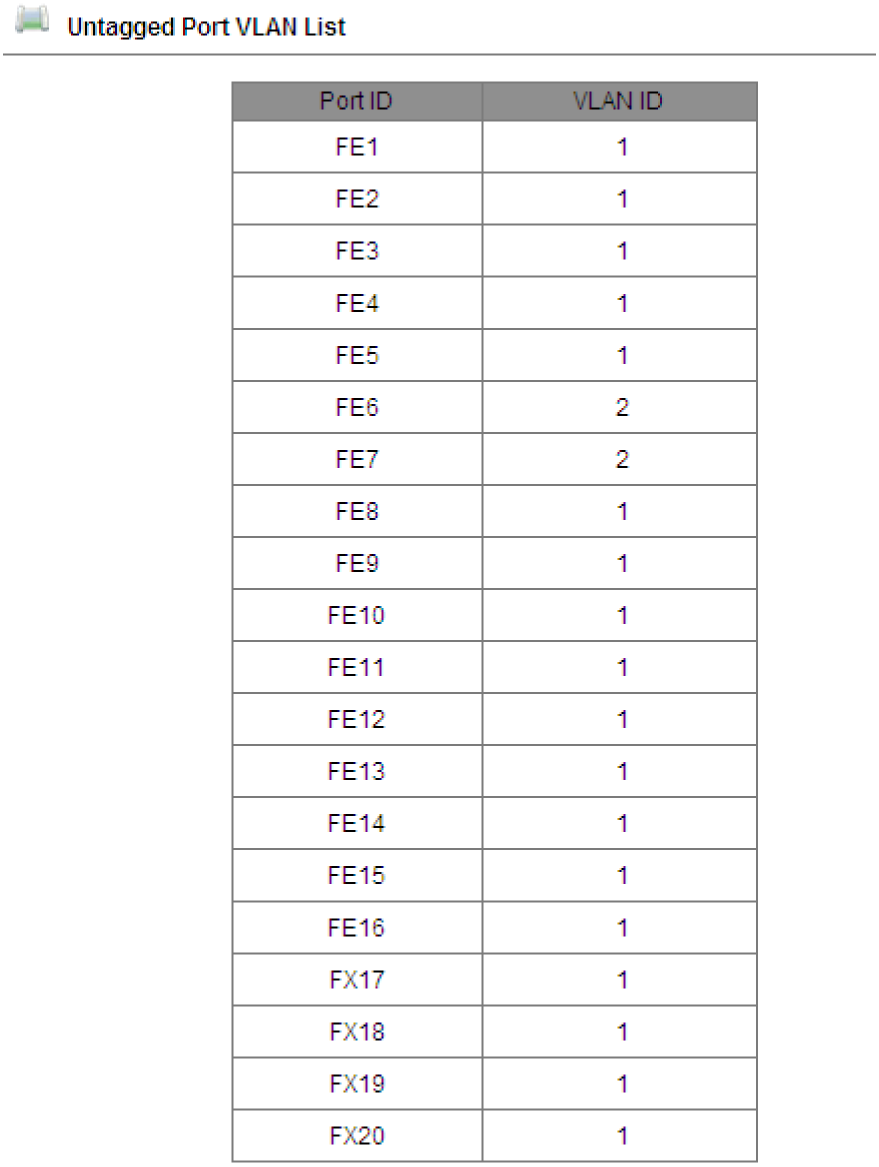
PVLAN List

Options: Select/Deselect

Function: Enable or disable the PVLAN function. For details, see the next chapter.

4. View the PVIDs of ports.

Click <Untagged Port VLAN List> in Figure 34. The following page is displayed.



Untagged Port VLAN List

Port ID	VLAN ID
FE1	1
FE2	1
FE3	1
FE4	1
FE5	1
FE6	2
FE7	2
FE8	1
FE9	1
FE10	1
FE11	1
FE12	1
FE13	1
FE14	1
FE15	1
FE16	1
FX17	1
FX18	1
FX19	1
FX20	1

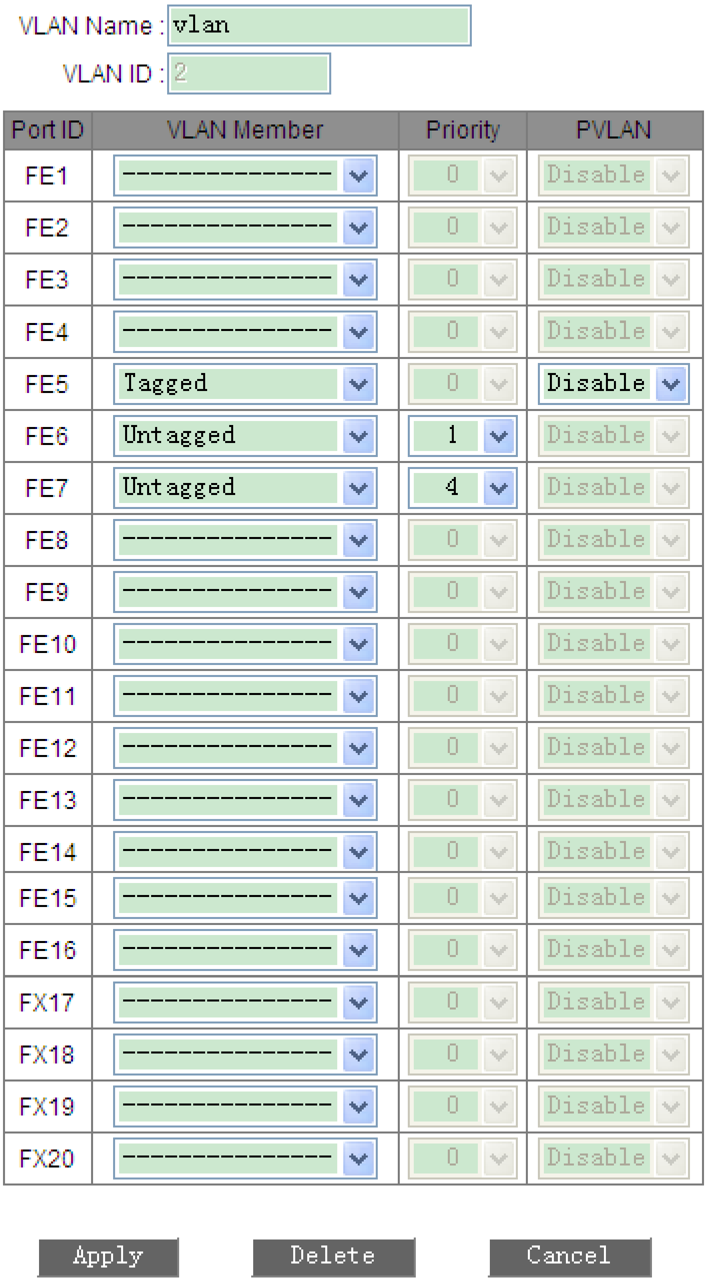
Figure 35 Port PVID List

Caution:

Each port must have an Untag attribute. If it is not set, the Untag port is in VLAN 1 by default.

5. Modify/Delete VLAN.

Click a VLAN list in Figure 34. You can modify or delete a created VLAN. Click <Delete> at the bottom. You can delete a VLAN directly, as shown in Figure 36.



VLAN Name : vlan

VLAN ID : 2

Port ID	VLAN Member	Priority	PVLAN
FE1	---------------	0	Disable
FE2	---------------	0	Disable
FE3	---------------	0	Disable
FE4	---------------	0	Disable
FE5	Tagged	0	Disable
FE6	Untagged	1	Disable
FE7	Untagged	4	Disable
FE8	---------------	0	Disable
FE9	---------------	0	Disable
FE10	---------------	0	Disable
FE11	---------------	0	Disable
FE12	---------------	0	Disable
FE13	---------------	0	Disable
FE14	---------------	0	Disable
FE15	---------------	0	Disable
FE16	---------------	0	Disable
FX17	---------------	0	Disable
FX18	---------------	0	Disable
FX19	---------------	0	Disable
FX20	---------------	0	Disable

Figure 36 Modifying/Deleting a created VLAN

6.2.5 Typical Configuration Example

As shown in Figure 37, the entire LAN is divided into 3 VLANs: VLAN2, VLAN100 and VLAN200. It is required that the devices in a same VLAN can communicate to each other, but different VLANs are isolated. The terminal PCs cannot distinguish Tag packets, so the ports on connecting Switch A and Switch B with PCs are set to Untag port. VLAN2, VLAN100 and VLAN200 packets need to be transmitted between Switch A and Switch B, so the ports connecting Switch A and Switch B should be set to Tag ports, permitting the packets of VLAN 2, VLAN 100 and VLAN 200 to pass through. Table 5 shows specific configuration.

Table 5 VLAN Configuration

Item	Configuration
VLAN2	Set port 1 and port 2 of Switch A and B to Untag ports, and port 7 to Tag port.
VLAN100	Set port 3 and port 4 of Switch A and B to Untag ports, and port 7 to Tag port.
VLAN200	Set port 5 and port 6 of Switch A and B to Untag ports, and port 7 to Tag port.

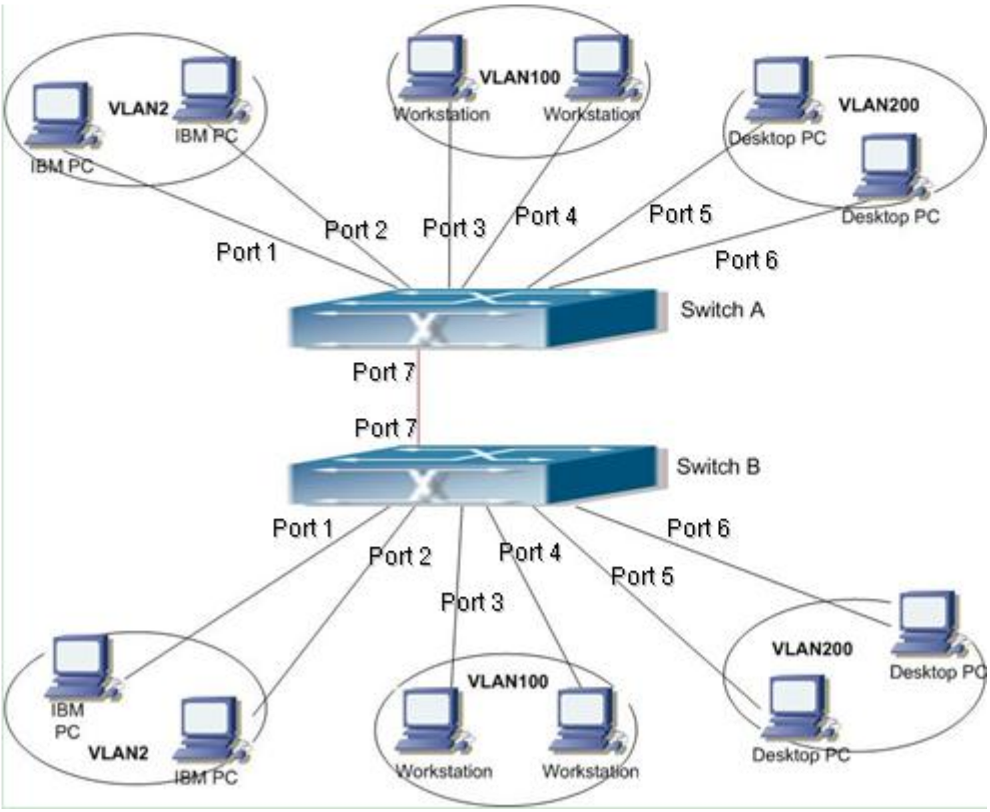


Figure 37 VLAN Application

Configurations on Switch A and Switch B:

1. Create VLAN 2, add port 1 and port 2 to VLAN 2 as Untag ports, and add port 7 into VLAN 2 as Tag port, as shown in Figure 33.

2. Create VLAN 100, add port 3 and port 4 to VLAN 100 as Untag ports, and add port 7 into VLAN 100 as Tag port, as shown in Figure 33.
3. Create VLAN 200, add port 5 and port 6 into VLAN 200 as Untag ports, and add port 7 into VLAN 200 as Tag port, as shown in Figure 33.

6.3 PVLAN

6.3.1 Overview

Private VLAN (PVLAN) uses two layers isolation technologies to realize the complex port traffic isolation function, achieving network security and broadcast domain isolation.

The upper VLAN is a shared domain VLAN in which ports are uplink ports. The lower VLANs are isolation domains in which ports are downlink ports. Downlink ports can be assigned to different isolation domains and they can communicate with the uplink port at the same time. Isolation domains cannot communicate to each other.

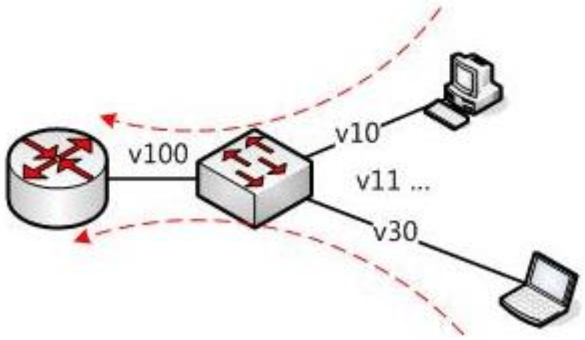


Figure 38 PVLAN Application

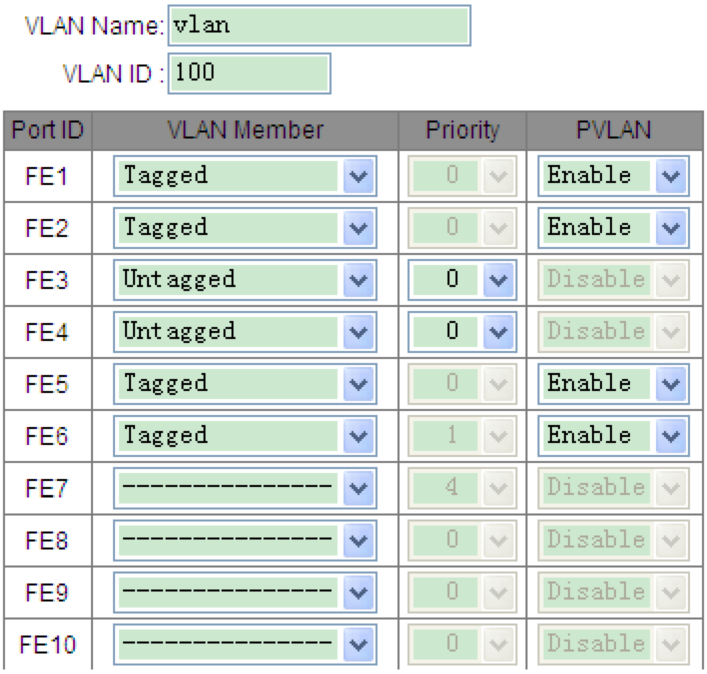
As shown in Figure 38, the shared domain is VLAN 100 and the isolation domains are VLAN 10 and VLAN 30; the devices in the isolation domains can communicate with the device in the shared domain, such as VLAN 10 can communicate with VLAN 100; VLAN 30 can also communicate with VLAN100, but the devices in different isolation domains cannot communicate with each other, such as VLAN 10 cannot communicate with VLAN 30.

Note:

When a PVLAN-enabled Tag port forwards a frame carrying a VLAN tag, the VLAN tag will be removed.

6.3.2 Web Configuration

1. Enable PVLAN on the port, as shown in Figure 39.



VLAN Name: vlan

VLAN ID : 100

Port ID	VLAN Member	Priority	PVLAN
FE1	Tagged	0	Enable
FE2	Tagged	0	Enable
FE3	Untagged	0	Disable
FE4	Untagged	0	Disable
FE5	Tagged	0	Enable
FE6	Tagged	1	Enable
FE7	---------------	4	Disable
FE8	---------------	0	Disable
FE9	---------------	0	Disable
FE10	---------------	0	Disable

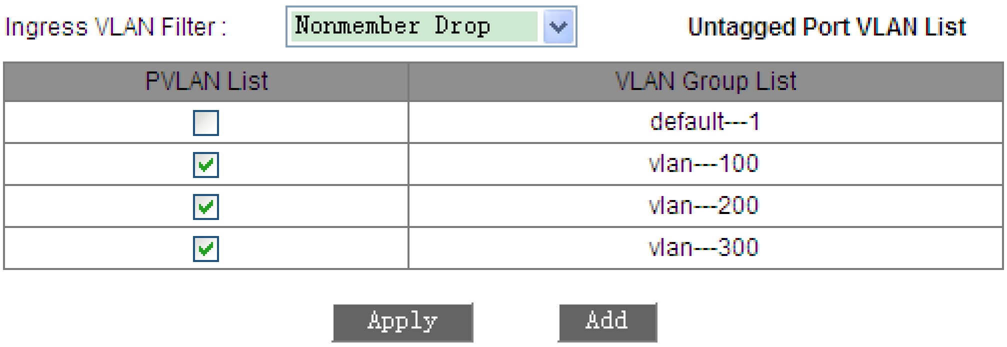
Figure 39 Enabling PVLAN

You should enable PVLAN on a Tag port in VLAN.

If the VLAN is a shared domain, the uplink port is an Untag port and the downlink port shall be added to the VLAN as a Tag port.

If the VLAN is an isolation domain, the downlink port is an Untag port and the uplink port shall be added to the VLAN as a Tag port.

2. Select the member VLANs of PVLAN, as shown in Figure 40.



Ingress VLAN Filter : Nonmember Drop

Untagged Port VLAN List

PVLAN List	VLAN Group List
□	default---1
☑	vlan---100
☑	vlan---200
☑	vlan---300

Figure 40 Selecting PVLAN Members

PVLAN List

Options: Select/Deselect

Default: Deselect

Function: Select PVLAN members.

Note:

Both shared and isolation domains are member VLANs of PVLAN.

6.3.3 Typical Configuration Example

Figure 41 shows a PVLAN application. VLAN300 is a shared domain and port 1 and port 2 are uplink ports; VLAN100 and VLAN200 are isolation domains and port 3, 4, 5 and 6 are downlink ports.

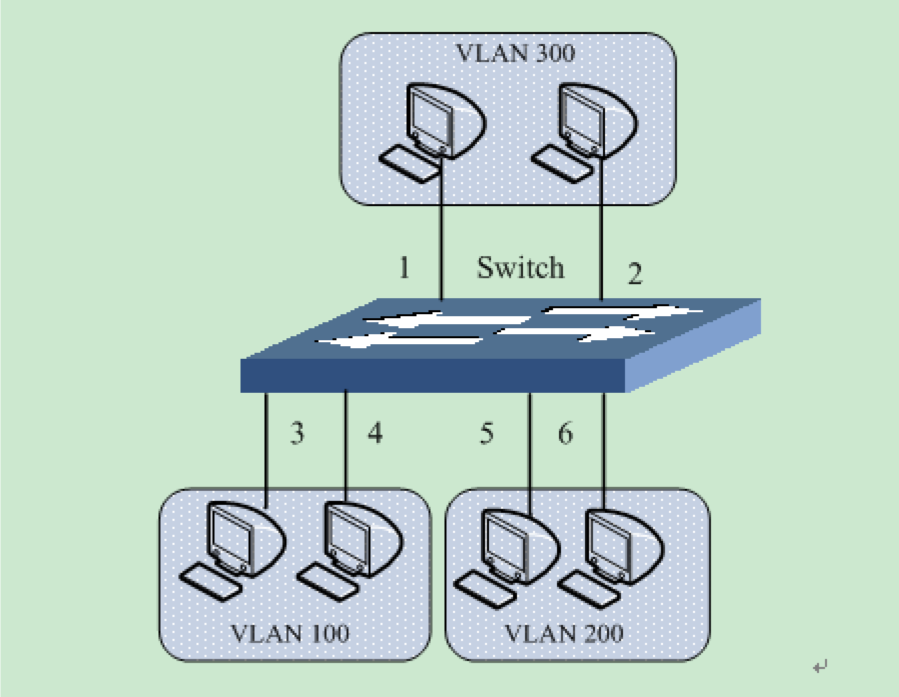


Figure 41 PVLAN Configuration Example

Configuration steps:

1. Configure the shared domain, VLAN 300, as shown in Figure 39.

Set port 1 and port 2 to Untag ports and add them to VLAN 300.

Set port 3 and port 4 to Tag ports and add them to VLAN 300. Enable PVLAN on the two ports.

Set port 5 and port 6 to Tag ports and add them to VLAN 300. Enable PVLAN on the two ports.

2. Configure VLAN 100, an isolation domain, as shown in Figure 39.

Set port 1 and port 2 to Tag ports and add them to VLAN 100. Enable PVLAN on the two ports.

Set port 3 and port 4 to Untag ports and add them to VLAN 100.

3. Configure VLAN 200, an isolation domain, as shown in Figure 39.

Set port 1 and port 2 to Tag ports and add them to VLAN 200. Enable PVLAN on the two ports.

Set port 5 and port 6 to Untag ports and add them to VLAN 200.

4. Set VLAN300, VLAN100 and VLAN200 to PVLAN members, as shown in Figure 40.

6.4 Port Mirroring

6.4.1 Overview

With port mirroring function, the switch copies all received or transmitted data frames in a port (mirroring source port) to another port (mirroring destination port). The mirroring destination port is connected to a protocol analyzer or RMON monitor for network monitoring, management, and fault diagnosis.

6.4.2 Description

A switch supports only one mirroring destination port but multiple source ports. Multiple source ports can be either in the same VLAN, or in different VLANs. Mirroring source port and destination port can be in the same VLAN or in different VLANs.

The source port and destination port cannot be the same port.

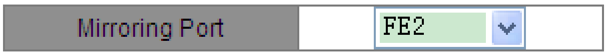
CAUTION

Caution:

- Port mirroring and Port Trunk are mutually exclusive. The mirroring source/destination port cannot be added into a Trunk group, while the ports added to a Trunk group cannot be set to a mirroring destination/source port.
- Port mirroring and port redundancy are mutually exclusive. The mirroring destination/source port cannot be set to a redundant port, while the redundant port cannot be set to a mirroring source/destination port.

6.4.3 Web Configuration

1. Select the mirroring destination port, as shown in Figure 42.



Mirroring Port: FE2

Figure 42 Selecting a Mirroring Port

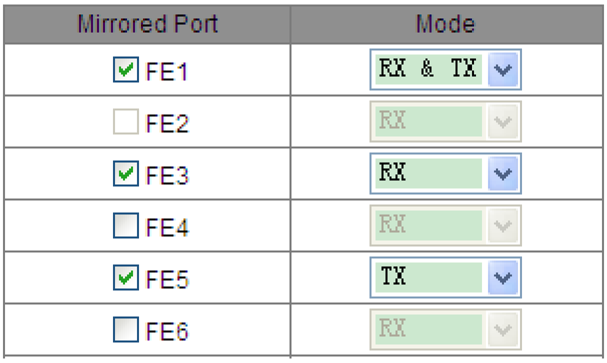
Mirroring Port

Options: Disable/A switch port

Default: Disable

Function: Select a port to be the mirroring destination port. There must be only one mirroring destination port.

2. Select mirroring source ports and the mirroring mode, as shown in Figure 43.



Mirrored Port	Mode
☑ FE1	RX & TX
☐ FE2	RX
☑ FE3	RX
☐ FE4	RX
☑ FE5	TX
☐ FE6	RX

Figure 43 Mirroring Source Port

Mode

Options: RX/TX/RX&TX

Function: Select the data to be mirrored.

TX indicates only the transmitted packets are mirrored in the source port.

RX indicates only the received packets are mirrored in the source port.

TX&RX indicates both transmitted and received packets are mirrored in the source port.

6.4.4 Typical Configuration Example

As shown in Figure 44, the mirroring destination port is port 2 and the mirroring source port is port 1. Both transmitted and received packets on port 1 are mirrored to port 2.

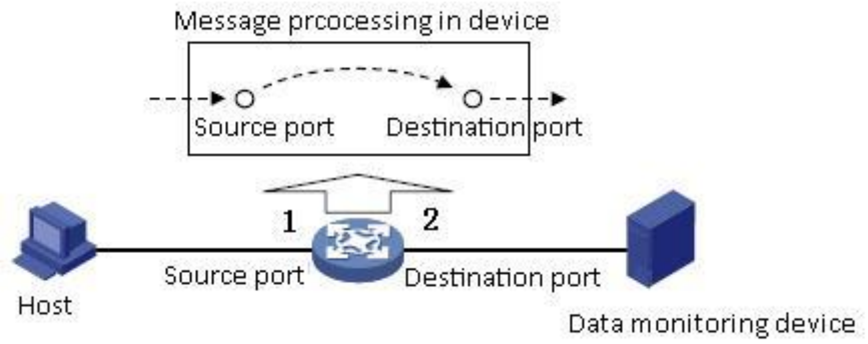


Figure 44 Port Mirroring Example

Configuration steps:

1. Set port 2 to the mirroring destination port, as shown in Figure 42.
2. Set port 1 to the mirroring source port and the port mirroring mode to TX&RX, as shown in Figure 43.

6.5 Port Trunk

6.5.1 Overview

Port trunk is to bind a group of physical ports that have the same configuration to a logical port. The member ports in a trunk group not only can share the flow to, but also can become a dynamic backup of each other to enhance the connection reliability.

6.5.2 Implementation

As shown in Figure 45, three ports in Switch A aggregate to a trunk group and the bandwidth of the trunk group is the total bandwidth of three ports.

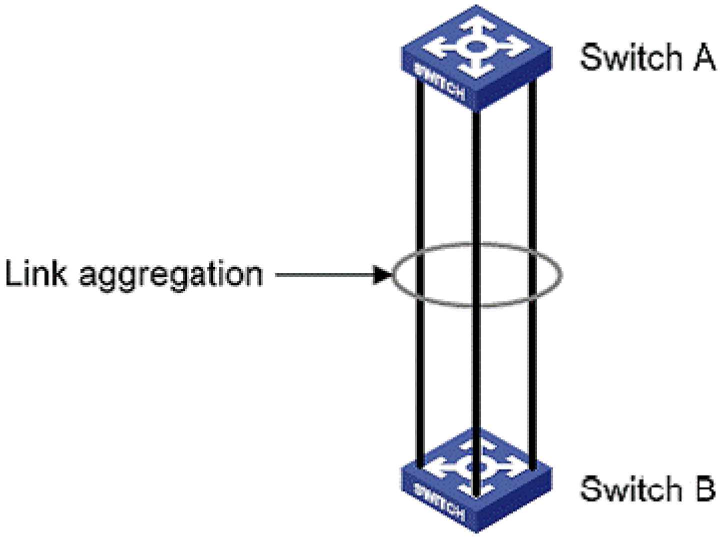


Figure 45 Port Trunk

If Switch A sends packets to Switch B by way of the aggregated link, Switch A determines the member port for transmitting the traffic based on the calculation result of load sharing. When one member port of the aggregated link fails, the traffic transmitted through the port is taken over by another normal port based on traffic sharing algorithm.

6.5.3 Description

Port trunk and the following port operations are mutually exclusive:

- Port trunk is mutually exclusive with port redundancy. A port added to a trunk group cannot be configured as a redundant port, while a redundant port cannot be added to a trunk group.
- Port trunk is mutually exclusive with port mirroring. A port added to a trunk group cannot be configured as a mirroring destination/source port.

In addition, the following operations are not recommended.

- Enable GMRP on a trunk port.
- Add a GMRP-enabled port to a trunk group.
- Add a trunk port to a static unicast/multicast entry.
- Add a port in a static unicast/multicast entry to a trunk group.

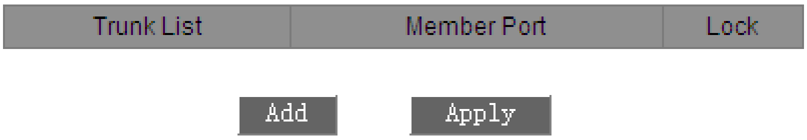
Caution:

- ➢ Gigabit ports of the series switches do not support port trunk.
- ➢ A port can be added to only one trunk group.

6.5.4 Web Configuration

1. Add Port Trunk.

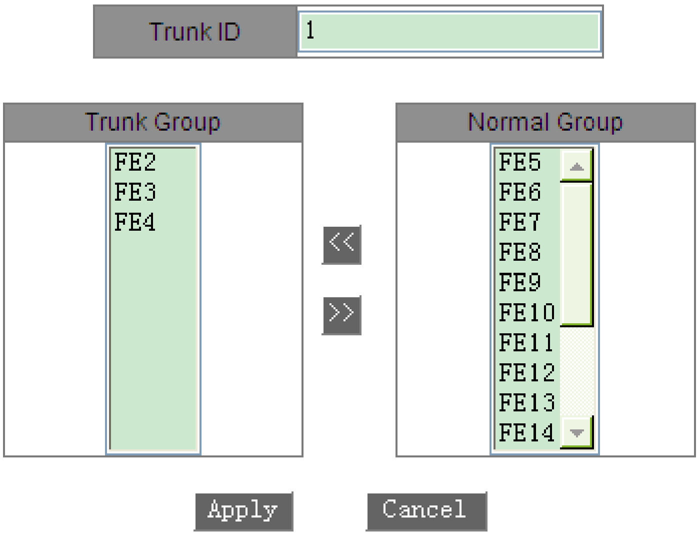
Click <Add> to add a trunk group, as shown in Figure 46.



Trunk List	Member Port	Lock

Figure 46 Adding a Trunk Group

2. Configure the trunk group, as shown in Figure 47.



Trunk ID: 1

Trunk Group	Normal Group
FE2 FE3 FE4	FE5 FE6 FE7 FE8 FE9 FE10 FE11 FE12 FE13 FE14

Figure 47 Configuring the Trunk Group

Trunk ID_ SICOM3016/3024/2024M

Range: 1~2

Function: Set the trunk group ID.

Description: The series switches support a maximum of 2 trunk groups. Each group can contain a maximum of 4 ports.

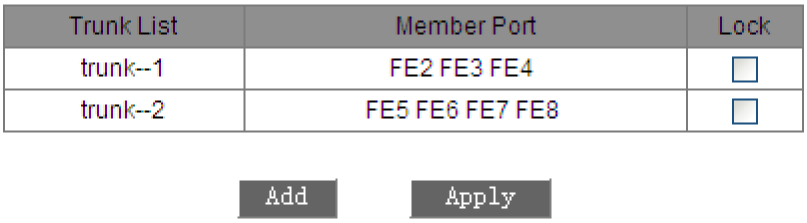
Trunk ID_ SICOM8000

Range: 1~6

Function: Set the trunk group ID.

Description: The series switches support a maximum of 6 trunk groups. Each group can contain a maximum of 4 ports.

3. View trunk group list, as shown in Figure 48.



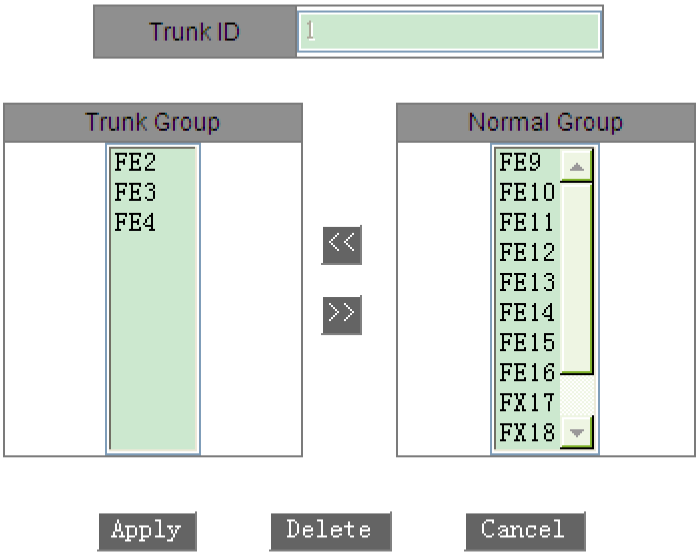
Trunk List	Member Port	Lock
trunk--1	FE2 FE3 FE4	□
trunk--2	FE5 FE6 FE7 FE8	□

Figure 48 Trunk Group List

Lock

Lock the member ports of a trunk group. After locked member ports are deleted from a trunk group, you must enable the ports manually to unlock the ports.

Click a trunk group in Figure 48. You can modify or delete the trunk group, as shown in Figure 49.



Trunk ID: 1

Trunk Group: FE2 FE3 FE4

Normal Group: FE9 FE10 FE11 FE12 FE13 FE14 FE15 FE16 FX17 FX18

Figure 49 Modifying/Deleting a Trunk Group

After modifying group member settings (add a new port to the group or delete a port member from the group), click <Apply> to make the modification take effect. If you click <Delete>, you can delete the group.

6.5.5 Typical Configuration Example

As shown in Figure 45, port 2, port 3, and port 4 of Switch A are connected to ports of Switch B respectively, forming trunk group 1 to achieve load balancing among ports.

Configuration steps:

1. Create trunk group 1 on Switch A and add port 2, port 3, and port 4 to the group, as shown in Figure 47.
2. Create trunk group 1 on Switch B and add port 2, port 3, and port 4 to the group, as shown in Figure 47.

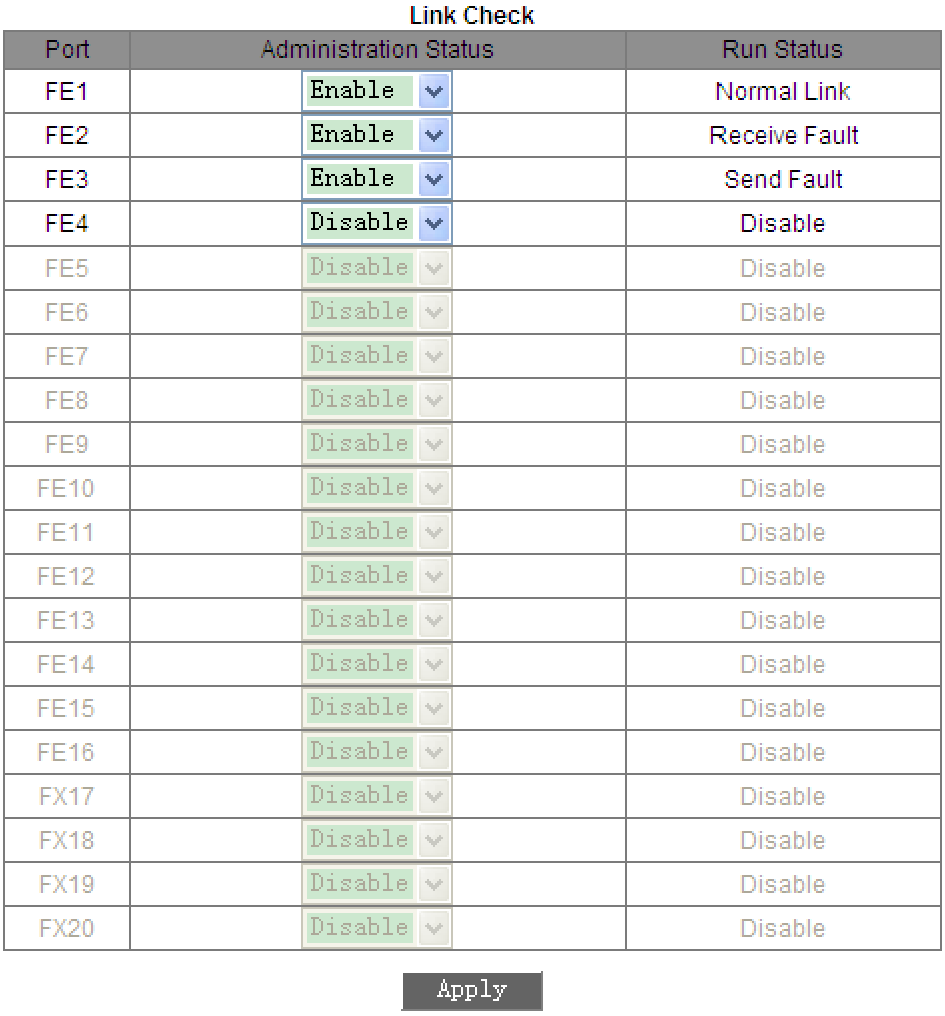
6.6 Link Check

6.6.1 Overview

Link Check detects the data transmission of redundancy protocol (STP/RSTP/DT-Ring)-enabled ports. Link check helps to detect the anomaly for timely processing When a fault occurs.

6.6.2 Web Configuration

Figure 50 shows the link check configuration.



Link Check

Port	Administration Status	Run Status
FE1	Enable	Normal Link
FE2	Enable	Receive Fault
FE3	Enable	Send Fault
FE4	Disable	Disable
FE5	Disable	Disable
FE6	Disable	Disable
FE7	Disable	Disable
FE8	Disable	Disable
FE9	Disable	Disable
FE10	Disable	Disable
FE11	Disable	Disable
FE12	Disable	Disable
FE13	Disable	Disable
FE14	Disable	Disable
FE15	Disable	Disable
FE16	Disable	Disable
FX17	Disable	Disable
FX18	Disable	Disable
FX19	Disable	Disable
FX20	Disable	Disable

Figure 50 Link Check Configuration

Administration Status

Options: Enable/Disable

Default: Enable

Description: The function can be enabled only on a redundant protocol-enabled port.

Caution:

If the peer device does not support the function, the function shall be disabled on the connected port of the local device.

Run Status

Options: Normal Link/Receive Fault/Disable/Send Fault

Description: If Link Check is enabled on a ring port and the port sends and receives data normally, Normal Link is displayed. If the peer end does not receive the detection packets from the device, Send Fault is displayed. If the device does not receive detection packets from the peer end, Receive Fault is displayed. If Link Check is not enabled on a port, Disable is displayed.

6.7 Static Multicast

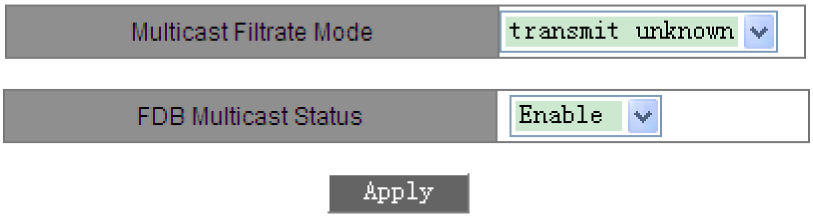
6.7.1 Overview

You can configure the static multicast address table. You can add an entry to the table in <multicast MAC address, VLAN ID, multicast member port> format. When receiving multicast packets, the; switch searches the table for the corresponding member port to forward the packets.

The device supports up to 256 multicast entries.

6.7.2 Web Configuration

1. Enable static multicast, as shown in Figure 51.



Multicast Filtrate Mode: transmit unknown

FDB Multicast Status: Enable

Figure 51 Enabling Static Multicast

Multicast Filtrate Mode

Options: transmit unknown/drop unknown

Default: transmit unknown

Function: Configure the processing mode for unknown multicast packets.

Description: Unknown multicast packets are packets not manually added or learned through IGMP Snooping and GMRP.

Transmit unknown indicates unknown multicast packets are broadcasted in the corresponding VLANs; drop unknown indicates unknown multicast packets are discarded.

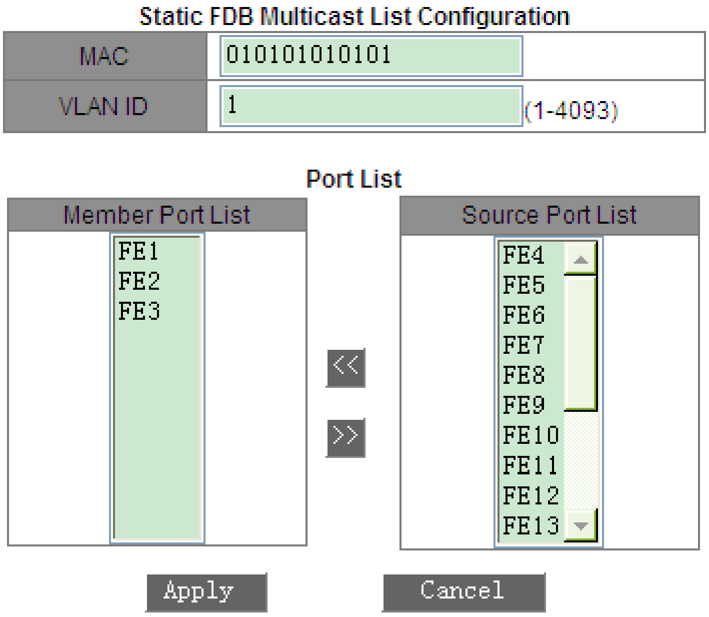
FDB Multicast Status

Options: Enable/Disable

Default: Disable

Function: Enable or disable static multicast. Static multicast and IGMP Snooping cannot be enabled at the same time.

2. Add a static multicast entry, as shown in Figure 52.



Static FDB Multicast List Configuration

MAC	010101010101
VLAN ID	1 (1-4093)

Port List

Member Port List	Source Port List
FE1 FE2 FE3	FE4 FE5 FE6 FE7 FE8 FE9 FE10 FE11 FE12 FE13

Figure 52 Adding a Static Multicast Entry

MAC

Portfolio: HHHHHHHHHHHH (H is a hexadecimal number.)

Function: Configure the multicast group address. The lowest bit of the highest byte is 1.

VLAN ID

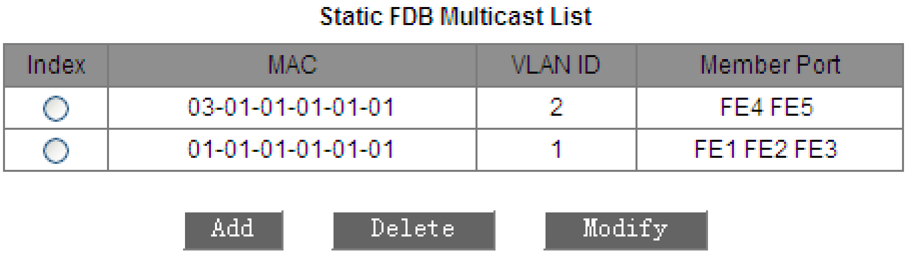
Options: All existing VLANs

Function: Set the VLAN ID of the entry. Only the member ports of the VLAN can forward the multicast packets.

Member Port List

Select member ports for the multicast address. If hosts connected to a port need to receive the packets from a multicast address, you can configure the port as the member port of the multicast address.

3. View, modify, or delete a static multicast entry, as shown in Figure 53.



Static FDB Multicast List

Index	MAC	VLAN ID	Member Port
○	03-01-01-01-01-01	2	FE4 FE5
○	01-01-01-01-01-01	1	FE1 FE2 FE3

Figure 53 Operations on a Static Multicast Entry

The static multicast address list contains the MAC address, VLAN ID, and member port. To delete an entry, select the entry and click <Delete>. To modify an entry, select the entry and click <Modify>.

6.8 IGMP Snooping

6.8.1 Overview

Internet Group Management Protocol Snooping (IGMP Snooping) is a multicast protocol at the data link layer. It is used for managing and controlling multicast groups. IGMP Snooping-enabled switches analyze received IGMP packets, establish mapping between ports and MAC multicast addresses, and forward multicast packets according to the mapping.

6.8.2 Concepts

- Querier: periodically sends IGMP general query packets to query the status of the members in the multicast group, maintaining the multicast group information. When multiple queriers exist on a network, they automatically elect the one with the smallest IP address to be the querier. Only the elected querier periodically sends IGMP general query packets. The other queriers only receive and forward IGMP query packets.
- Router port: receives general query packets (on an IGMP-enabled switch) from the querier. Upon receiving an IGMP report, a switch establishes a multicast entry and adds the port that receives the IGMP report to the

member port list. If a router port exists, it is also added to the member port list. Then the switch forwards the IGMP report to other devices through the router port, so that the other devices establish the same multicast entry.

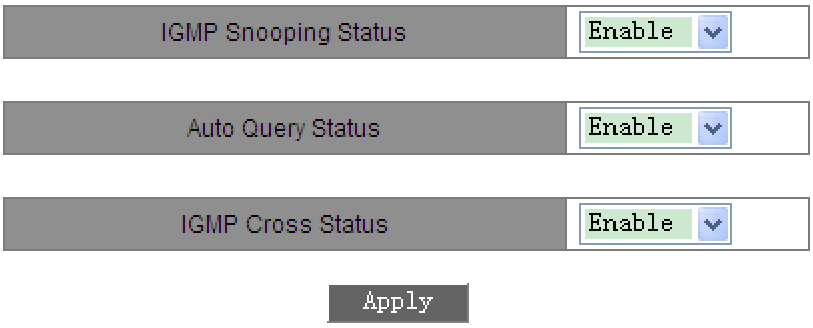
6.8.3 Principle

IGMP Snooping manages and maintains multicast group members by exchanging related packets among IGMP-enabled devices. The related packets are as follows:

- General query packet: The querier periodically sends general query packets (destination IP address: 224.0.0.1) to confirm whether or not the multicast group has member ports. After receiving the query packet, a non-querier device forwards the packet to all its connected ports.
- Specific query packet: If a device wants to leave a multicast group, it sends an IGMP leave packet. After receiving the leave packet, the querier sends a specific query packet (destination IP address: IP address of the multicast group) to confirm whether the group contains other member ports.
- Membership report packet: If a device wants to receive the data of a multicast group, the device sends an IGMP report packet (destination IP address: IP address of the multicast group) immediately to respond to the IGMP query packet of the group.
- Leave packet: If a device wants to leave a multicast group, the device will send an IGMP leave packet (destination IP address: 224.0.0.2).

6.8.4 Web Configuration

1. Enable IGMP Snooping and enable or disable auto query, as shown in Figure 54.



IGMP Snooping Status: Enable

Auto Query Status: Enable

IGMP Cross Status: Enable

Figure 54 Enabling IGMP Snooping

IGMP Snooping Status

Options: Enable/Disable

Default: Disable

Function: Enable or disable IGMP Snooping. IGMP Snooping and static multicast/GMRP cannot be enabled at the same time.

Auto Query Status

Options: Enable/Disable

Default: Disable

Function: Enable or disable auto query for querier election.

Description: The auto query function can be enabled only if IGMP Snooping is enabled.

CAUTION

Caution:

The auto query function on a network shall be enabled on at least one switch.

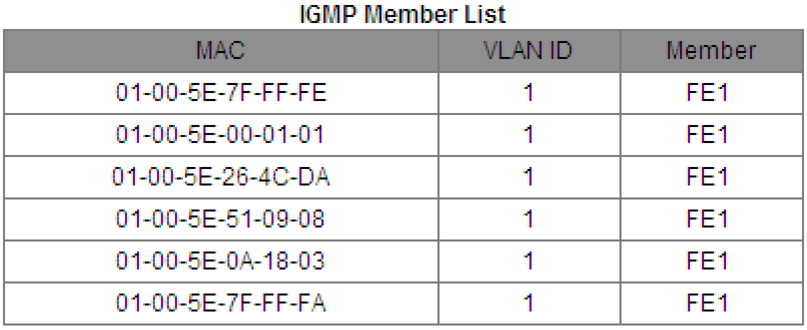
IGMP Cross Status

Options: Enable/Disable

Default: Disable

Function: If the function is enabled, report and leave packets can be forwarded by the DT ring ports.

2. View the multicast member list, as shown in Figure 55.



IGMP Member List

MAC	VLAN ID	Member
01-00-5E-7F-FF-FE	1	FE1
01-00-5E-00-01-01	1	FE1
01-00-5E-26-4C-DA	1	FE1
01-00-5E-51-09-08	1	FE1
01-00-5E-0A-18-03	1	FE1
01-00-5E-7F-FF-FA	1	FE1

Figure 55 IGMP Snooping Member List

IGMP Member List

Combination: {MAC address, VLAN ID, member port}

In the FDB multicast table dynamically learned through IGMP Snooping, the VLAN ID is the VLAN ID of member ports.

6.8.5 Typical Configuration Example

As shown in Figure 56, IGMP Snooping is enabled on Switch 1, Switch 2, and Switch 3. Auto query is enabled on Switch 2 and Switch 3.The IP address of Switch 2 is 192.168.1.2 and that of Switch 3 is 192.168.0.2.Therefore, Switch 3 is elected as the querier.

1.Enable IGMP Snooping on Switch 1.

2.Enable IGMP Snooping and auto query on Switch 2.

3.Enable IGMP Snooping and auto query on Switch 3.

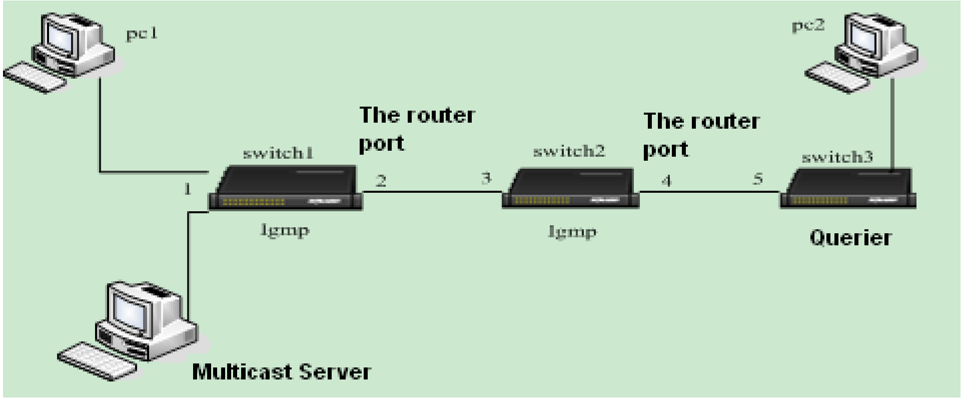


Figure 56 IGMP Snooping Configuration Example

➢ Switch 3 as the querier periodically sends general query packets. Port 4 of

Switch 2 receives the packets and is thus elected as the routing port. Switch 2 forwards the packets through port 3. Then port 2 of Switch 1 receives the packets and is thus elected as the routing port.

- When PC 1 is added to multicast group 225.1.1.1 and send IGMP report packets, port 1 and port 2 (routing port) of Switch 1 are added to multicast group 225.1.1.1. IGMP report packets are forwarded to Switch 2 through port 2. Then port 3 and port 4 of Switch 2 are also added to multicast group 225.1.1.1. Switch 2 forwards the report packets to Switch 3 through port 4. As a result, port 5 of Switch 3 is also added to multicast group 225.1.1.1.
- When receiving multicast data, Switch 1 forwards the data to PC 1 through port 1. As port 2 is also a multicast group member, it also forwards multicast data. As the process proceeds, multicast data finally reaches port 5 of Switch 3 because no further receiver is available. If PC 2 is also added to multicast group 225.1.1.1, multicast data is also forwarded to PC 2.

6.9 ACL

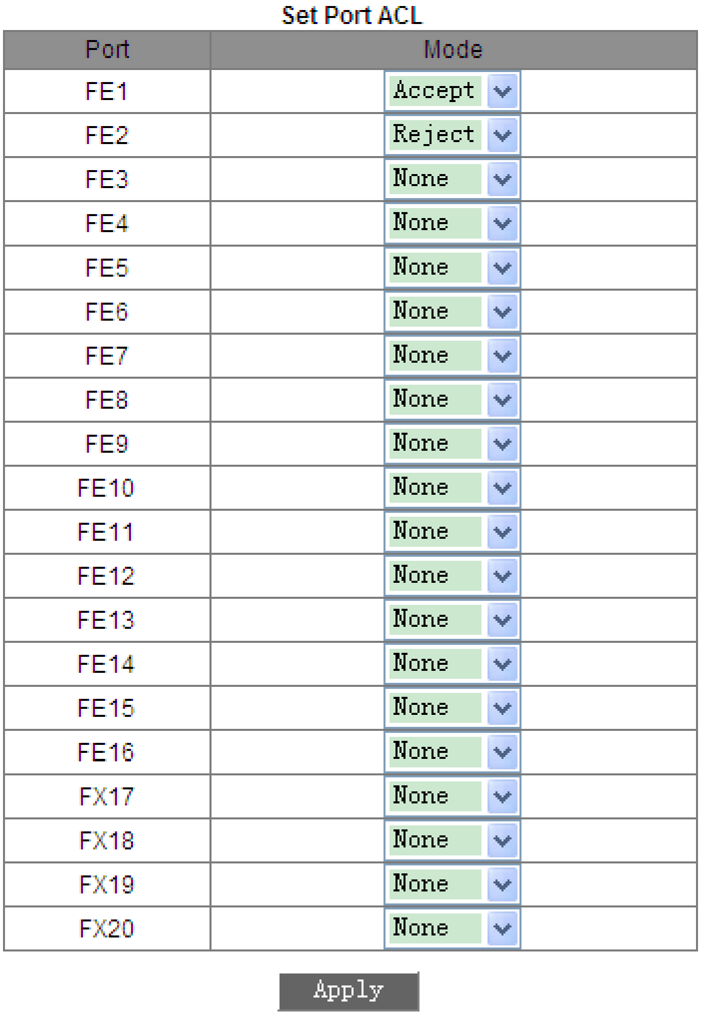
6.9.1 ACL (SICOM3016/3024/2024M)

6.9.1.1 Overview

With the Access Control List (ACL) function, the switch filters received packets according to the matched rules defined in the ACL, preventing illegitimate users’ access and saving network resources.

6.9.1.2 Web Configuration

Configure the ACL mode for ports, as shown in Figure 57.



Set Port ACL

Port	Mode
FE1	Accept
FE2	Reject
FE3	None
FE4	None
FE5	None
FE6	None
FE7	None
FE8	None
FE9	None
FE10	None
FE11	None
FE12	None
FE13	None
FE14	None
FE15	None
FE16	None
FX17	None
FX18	None
FX19	None
FX20	None

Figure 57 ACL Mode Configuration

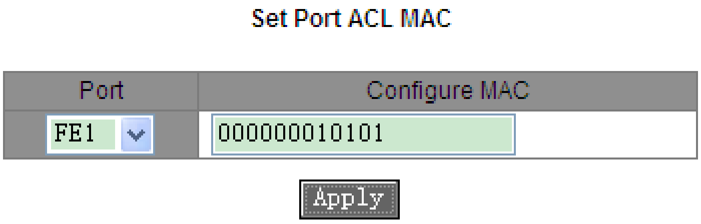
Mode

Options: None/Accept/Reject

Default: None

Function: Configure the ACL mode, that is, the processing mode towards matched packets.

2. Set parameters for the ACL entry, as shown in Figure 58.



Set Port ACL MAC

Port	Configure MAC
FE1	000000010101

Figure 58 Configuring an ACL Entry

Port

Options: all switch ports

Function: Configure the port on which the ACL entry takes effect.

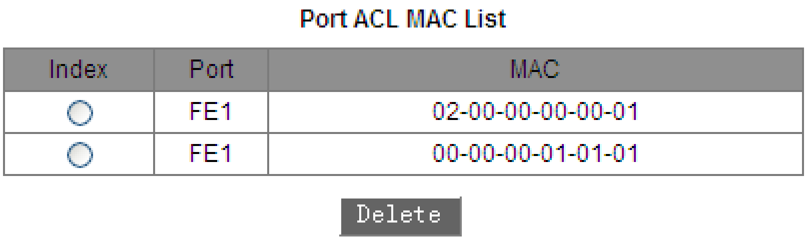
Configure MAC

Format: {HHHHHHHHHHHH} (H is a hexadecimal number.)

Function: Configure the source MAC address for the ACL entry. If the source MAC address of a packet is identical with the configured MAC address, the packet matches the entry.

Description: Each port supports a maximum of 24 ACL entries.

3. View the ACL.



Port ACL MAC List

Index	Port	MAC
○	FE1	02-00-00-00-00-01
○	FE1	00-00-00-01-01-01

Figure 59 ACL Entries

Select an ACL entry in Figure 59. You can delete the entry.

6.9.1.3 Typical Configuration Example

Port 1 accepts only the packets whose source MAC address is 00-00-00-01-01-01.

Configuration steps:

1. Select Accept for the ACL mode of port 1, as shown in Figure 57.
2. Set the source MAC address of ACL entry for port 1 to 00-00-00-01-01-01, as shown in Figure 58.

6.9.2 ACL (SICOM8000)

6.9.2.1 Overview

With the development of network technologies, security issues have become increasingly prominent, calling for access control mechanism. With the Access Control List (ACL) function, the switch matches packets with the list to implement access control.

6.9.2.2 Implementation

The series switches filter packets according to the matched ACL. Each entry consists several conditions in the logical AND relationship. ACL entries are independent of each other.

The switch compares a packet with ACL entries in the ascending order of entry IDs. Once a match is found, the action is taken and no further comparison is conducted, as shown in the following figure.

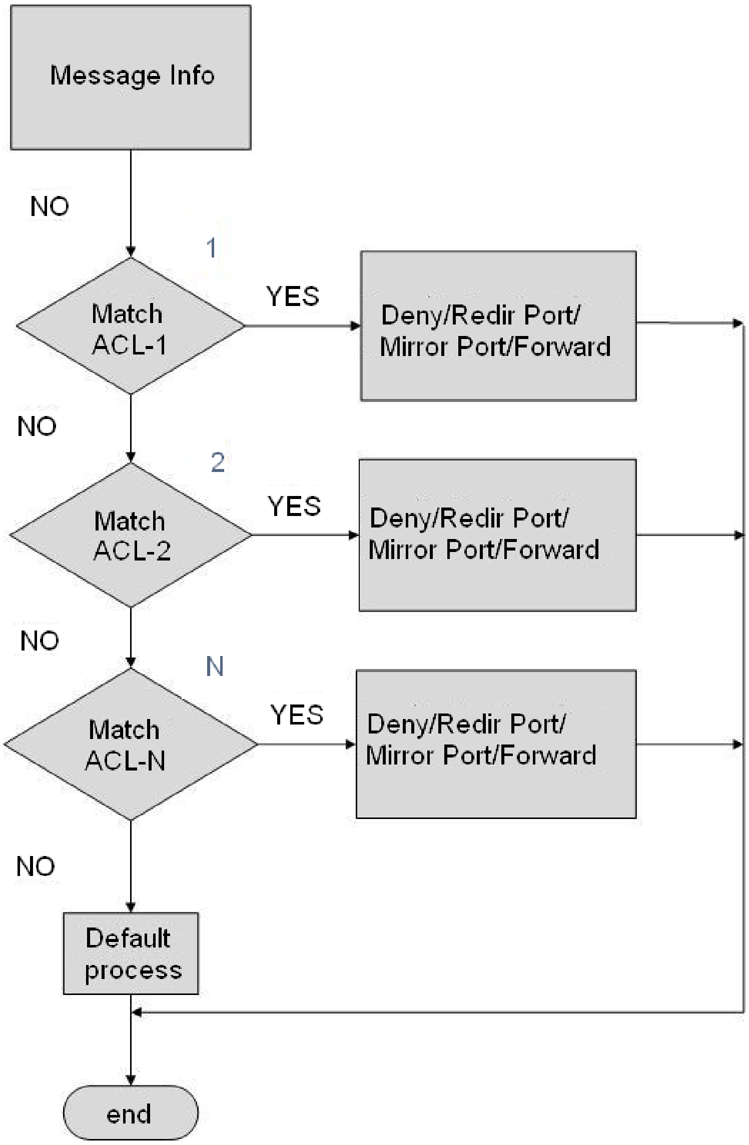

Message Info
NO
1
Match ACL-1
YES
Deny/Redir Port/ Mirror Port/Forward
NO
2
Match ACL-2
YES
Deny/Redir Port/ Mirror Port/Forward
NO
N
Match ACL-N
YES
Deny/Redir Port/ Mirror Port/Forward
NO
Default process
end

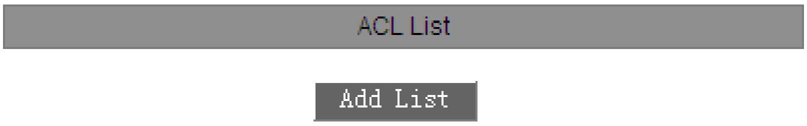
Figure 60 ACL Processing Flowchart

Note:

Default process indicates the processing mode towards packets matching no ACL entry.

6.9.2.3 Web Configuration

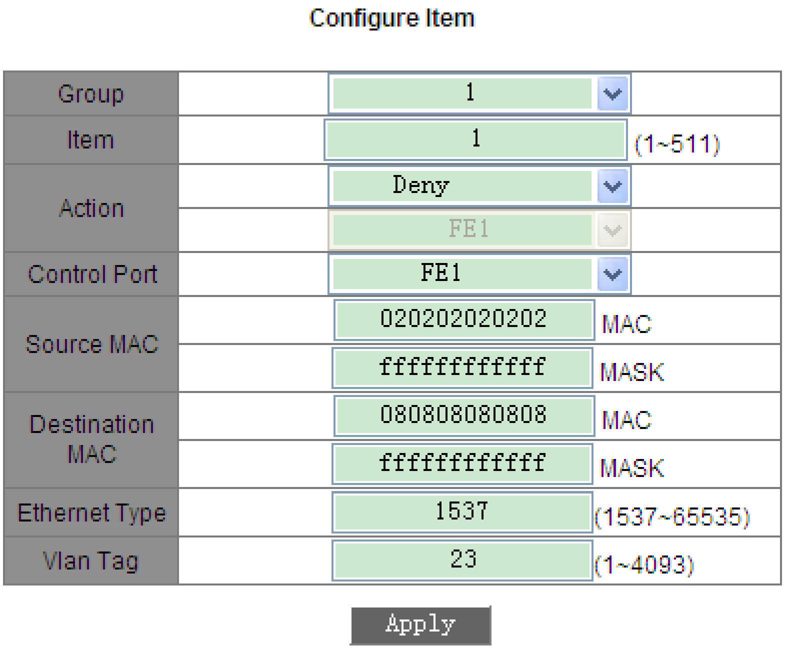
1. Add an ACL entry.



ACL List

Figure 61 Adding an ACL Entry

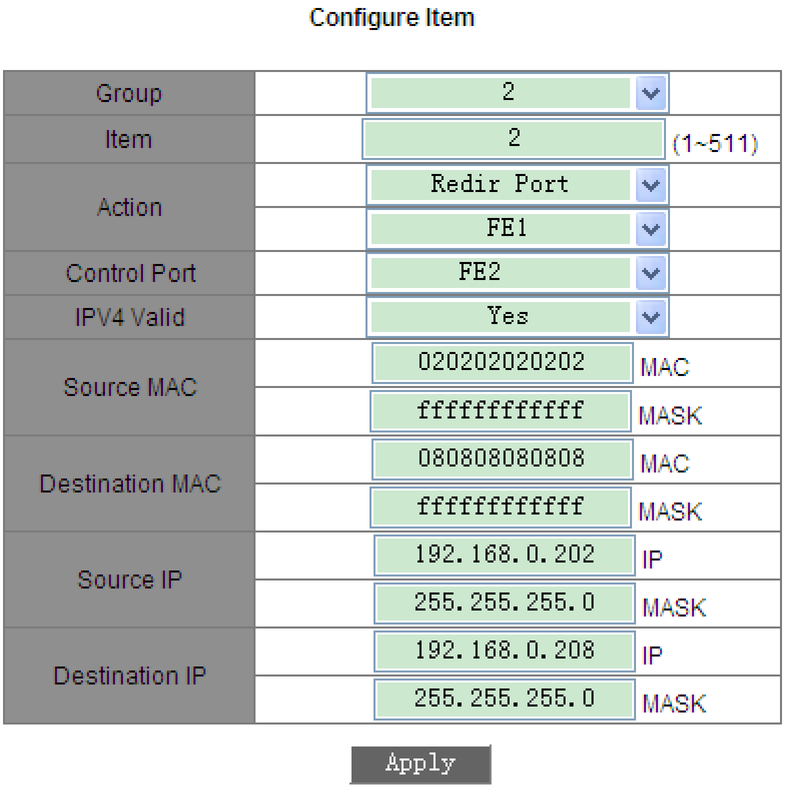
Click <Add List> in the preceding figure to add an ACL entry. Different group IDs correspond to different ACL parameters, as shown in the following figures.



Configure Item

Group	1	
Item	1	(1~511)
Action	Deny FE1	
Control Port	FE1	
Source MAC	020202020202	MAC
	ffffffffffff	MASK
Destination MAC	080808080808	MAC
	ffffffffffff	MASK
Ethernet Type	1537	(1537~65535)
Vlan Tag	23	(1~4093)

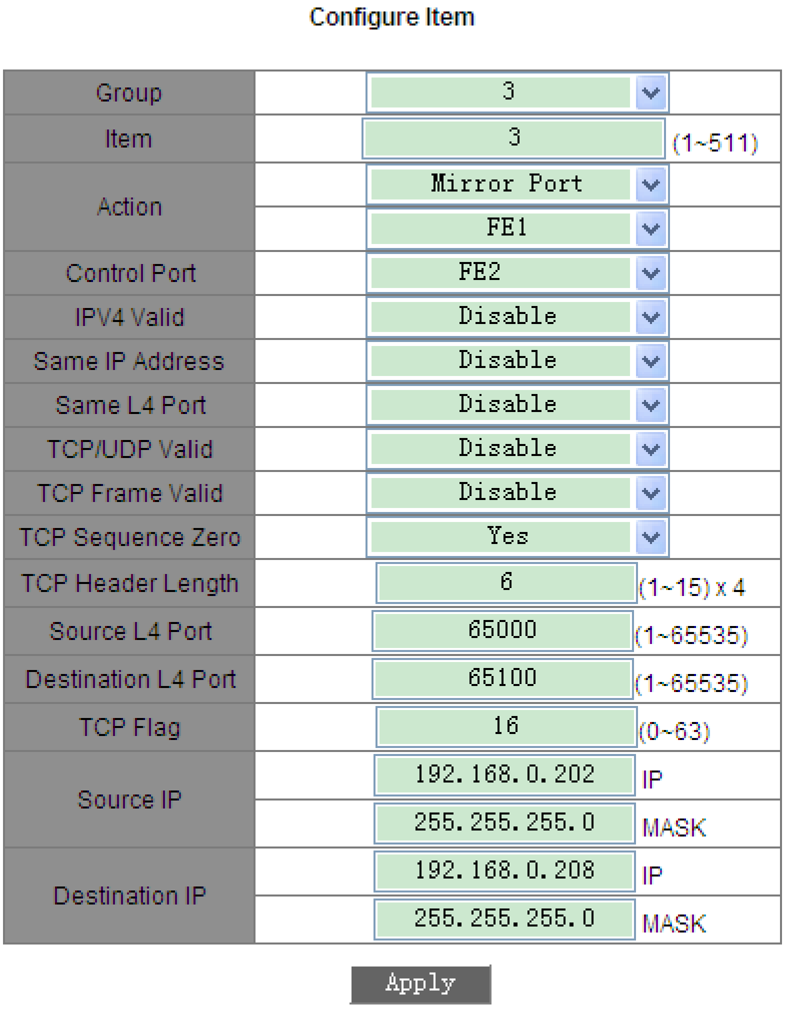
Figure 62 Setting ACL Entry Parameters - Group 1



Configure Item

Group	2	
Item	2	(1~511)
Action	Redir Port	
	FE1	
Control Port	FE2	
IPV4 Valid	Yes	
Source MAC	020202020202	MAC
	ffffffffffff	MASK
Destination MAC	080808080808	MAC
	ffffffffffff	MASK
Source IP	192.168.0.202	IP
	255.255.255.0	MASK
Destination IP	192.168.0.208	IP
	255.255.255.0	MASK

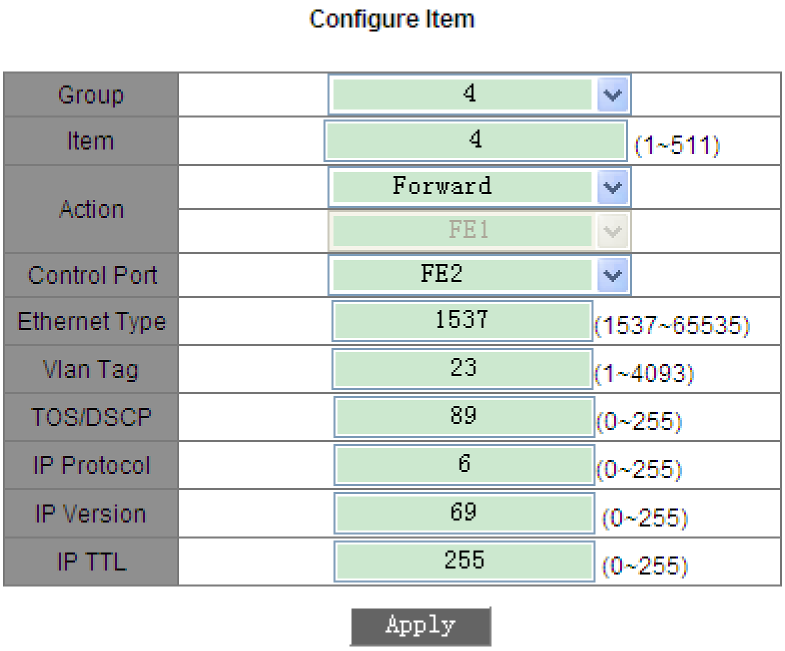
Figure 63 Setting ACL Entry Parameters - Group 2



Configure Item

Group	3	
Item	3	(1~511)
Action	Mirror Port FE1	
Control Port	FE2	
IPV4 Valid	Disable	
Same IP Address	Disable	
Same L4 Port	Disable	
TCP/UDP Valid	Disable	
TCP Frame Valid	Disable	
TCP Sequence Zero	Yes	
TCP Header Length	6	(1~15) x 4
Source L4 Port	65000	(1~65535)
Destination L4 Port	65100	(1~65535)
TCP Flag	16	(0~63)
Source IP	192.168.0.202 255.255.255.0	IP MASK
Destination IP	192.168.0.208 255.255.255.0	IP MASK

Figure 64 Setting ACL Entry Parameters - Group 3



Configure Item

Group	4	
Item	4	(1~511)
Action	Forward FE1	
Control Port	FE2	
Ethernet Type	1537	(1537~65535)
Vlan Tag	23	(1~4093)
TOS/DSCP	89	(0~255)
IP Protocol	6	(0~255)
IP Version	69	(0~255)
IP TTL	255	(0~255)

Figure 65 Setting ACL Entry Parameters - Group 4

Group

Options: 1~4

Default: 1

Function: Configure the group number of the ACL entry.

Description: Different group IDs correspond to different ACL parameters.

Item

Range: 1~511

Function: Set the ID of the ACL entry. You can configure a maximum of 511 ACL entries. When multiple ACL entries are configured, they are compared with packets in the ascending order of IDs.

Action

Options: Deny/Redir Port/Mirror Port/Forward

Default: Deny

Function: Configure the action towards a packet that matches the ACL entry.

Deny: Packets matching the entry will be denied.

Redir Port: Packets matching the entry will be forwarded to the specified port. You need to specify the port in the drop-down list.

Mirror Port: Packets matching the entry will be forwarded to both the destination port and the specified port in the drop-down list.

Control Port

Options: All /Any specified port

Function: Select the port on which the ACL takes effect.

Source MAC

Portfolio: {MAC address, MAC subnet mask}

Format: {HHHHHHHHHHHH, HHHHHHHHHHHH} (H is a hexadecimal number.)

Function: Configure the source MAC address and subnet mask. If the source MAC address and subnet mask of a packet is identical with the value of this parameter, then the condition is met.

Destination MAC

Portfolio: {MAC address, MAC subnet mask}

Format: {HHHHHHHHHHHH, HHHHHHHHHHHH} (H is a hexadecimal number.)

Function: Configure the destination MAC address and subnet mask. If the destination MAC address and subnet mask of a packet is identical with the value of this parameter, then the condition is met.

Ethernet Type

Range: 1537~65535

Function: Configure the Ethernet type. If the Ethernet type field of a packet is identical with the value of this parameter, the condition is met.

Vlan Tag

Range: 1~4093

Function: Configure the VLAN ID. If the corresponding field of a packet is identical with the value of this parameter, the condition is met.

IPV4 Valid

Options: Disable/Yes/No

Default: Disable

Function: Check whether the received packet is a valid IPv4 packet.

Disable indicates the rule is not used.

Yes indicates the condition is met if the received packet is a valid IPv4 packet.

No indicates the condition is met if the received packet is not a valid IPv4 packet.

Source IP

Portfolio: {IP address, IP subnet mask}

Format: {A.B.C.D, A.B.C.D}

Function: Configure the source IP address and subnet mask. If the source IP address and subnet mask of a packet is identical with the value of this parameter, then the condition is met.

Destination IP

Portfolio: {IP address, IP subnet mask}

Format: {A.B.C.D, A.B.C.D}

Function: Configure the destination IP address and subnet mask. If the destination IP address and subnet mask of a packet is identical with the value of this parameter, then the condition is met.

Same IP Address

Options: Disable/Yes/No

Default: Disable

Function: Check whether the source IP address of a packet is identical with its destination IP address.

Disable indicates the rule is not used.

No indicates the condition is met if the source IP address of a packet is different from its destination IP address.

Yes indicates the condition is met if the source IP address of a packet is identical with its destination IP address.

Same L4 Port

Options: Disable/Yes/No

Default: Disable

Function: Check whether the source Layer-4 port number of a packet is identical with its destination Layer-4 port number.

Disable indicates the rule is not used.

No indicates the condition is met if the source Layer-4 port number of a packet is different from its destination Layer-4 port number.

Yes indicates the condition is met if the source Layer-4 port number of a packet is identical with its destination Layer-4 port number.

TCP/UDP Valid

Options: Disable/Yes/No

Default: Disable

Function: Check whether the received packet is a TCP/UDP packet.

Disable indicates the rule is not used.

Yes indicates the condition is met if the received packet is a valid TCP/UDP packet.

No indicates the condition is met if the received packet is not a valid TCP/UDP packet.

TCP Frame Valid

Options: Disable/Yes/No

Default: Disable

Function: Check whether the received packet is a valid TCP frame.

Disable indicates the rule is not used.

Yes indicates the condition is met if the received packet is a valid TCP frame.

No indicates the condition is met if the received packet is not a valid TCP frame.

TCP Sequence Zero

Options: Disable/Yes/No

Default: Disable

Function: Check whether the TCP Sequence field of a packet is 0.

Disable indicates the rule is not used.

No indicates the condition is met if the TCP Sequence field of a packet is not 0.

Yes indicates the condition is met if the TCP Sequence field of a packet is 0.

TCP Header Length

Range: 1~15

Function: Configure the TCP header length. If the corresponding field of a packet is smaller than the value of this parameter, then the condition is met.

Source L4 Port

Range: 1~65535

Function: Configure the source port number for Layer-4 protocol packets. If the corresponding field of a packet is identical with the value, then the condition is met.

Destination L4 Port

Range: 1~65535

Function: Configure the destination port number for Layer-4 protocol packets. If the corresponding field of a packet is identical with the value, then the condition is met.

TCP Flag

Range: 0~63

Function: Configure the TCP flag. If the corresponding field of a packet is identical with the value of this parameter, then the condition is met.

TOS/DSCP

Range: 0~255

Function: Configure the service type. If the corresponding field of a packet is identical with the value of this parameter, then the condition is met.

IP Protocol

Range: 0~255

Function: Configure the IP protocol value. If the corresponding field of a packet is identical with the value of this parameter, then the condition is met.

IP Version

Range: 0~255

Function: Configure the value of the IP protocol version plus the header length. If the corresponding field of a packet is identical with the value of this parameter, then the condition is met.

IP TTL

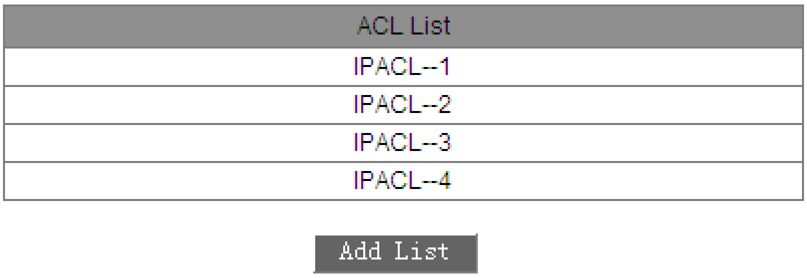
Range: 0~255

Function: Configure the TTL field. If the corresponding field of a packet is identical with the value of this parameter, then the condition is met.

Note:

You do not need to set all these parameters. If only one parameter is required, keep all the other parameters empty. At least one parameter shall be configured.

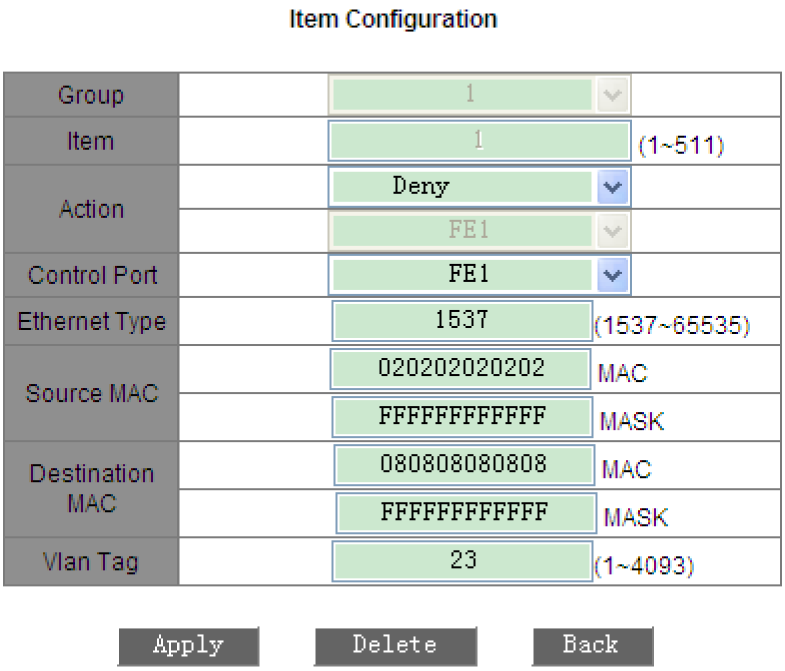
3. View the ACL.



ACL List
IPACL--1
IPACL--2
IPACL--3
IPACL--4

Figure 66 ACL Entries

Click an ACL entry in the preceding figure. You can modify or delete the ACL entry, as shown in the following figure.



Item Configuration

Group	1	
Item	1	(1~511)
Action	Deny FE1	
Control Port	FE1	
Ethernet Type	1537	(1537~65535)
Source MAC	020202020202	MAC
	FFFFFFFFFFFF	MASK
Destination MAC	080808080808	MAC
	FFFFFFFFFFFF	MASK
Vlan Tag	23	(1~4093)

Figure 67 Modifying/Deleting an ACL Entry

After modifying parameters, you need to click <Apply> to make the modification take effect. You can click <Delete> to delete the ACL entry.

6.9.2.4 Typical Configuration Example

Connect port 2 of the switch. Configure the port to receive packets only from source MAC address 02-02-02-02-02-02 and forward the packets through port 1.

Configuration steps (as shown in Figure 62 or Figure 63):

1. Set group ID to 1 or 2.
2. Set the action to Redir Port and select port 1 in the drop-down list.
3. Select FE2 in Control Port.
4. Set the source MAC address to 020202020202 and subnet mask to FFFFFFFFFFFF.
5. Keep all the other parameters empty.

6.10 ARP

6.10.1 Overview

The Address Resolution Protocol (ARP) resolves the mapping between IP addresses and MAC addresses by the address request and response mechanism. The switch can learn the mapping between IP addresses and MAC addresses of other hosts on the same network segment. It also supports static ARP entries for specifying mapping between IP addresses and MAC addresses. Dynamic ARP entries periodically age out, ensuring consistency between ARP entries and actual applications.

The series switches provides not only Layer 2 switching function, but also the ARP function for resolving the IP addresses of other hosts on the same network segment, enabling the communication between the NMS and managed hosts.

6.10.2 Description

ARP entries fall into dynamic and static ones.

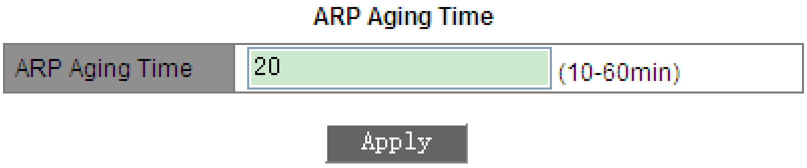
Dynamic entries are generated and maintained based on the exchange of ARP packets. Dynamic entries can expire, be updated by a new ARP packet, or be overwritten by a static ARP entry.

Static entries are manually configured and maintained. They never expire or are overwritten by dynamic ARP entries.

The switch supports up to 512 ARP entries (256 static ones at most).When the number of ARP entries is larger than 512, new entries automatically overwrite old dynamic entries.

6.10.3 Web Configuration

1. Configure ARP aging time, as shown in Figure 68.



ARP Aging Time

ARP Aging Time	20 (10-60min)

Figure 68 Configuring Aging Time

ARP Aging Time

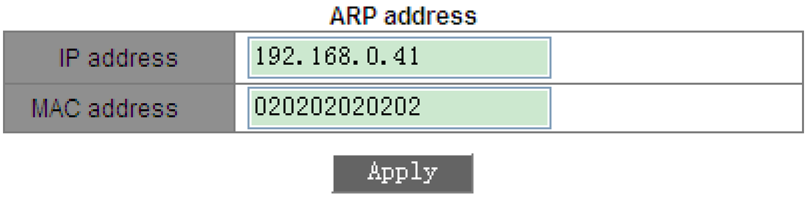
Range: 10~60 minutes

Default: 20 minutes

Function: Configure ARP aging time.

Description: ARP aging time is the duration from when a dynamic ARP entry is added to the table to when the entry is deleted from the table.

2. Add a static ARP entry, as shown in Figure 69.



ARP address

IP address	192.168.0.41
MAC address	020202020202

Figure 69 Adding a Static ARP Entry

ARP address

Portfolio: {IP address, MAC address}

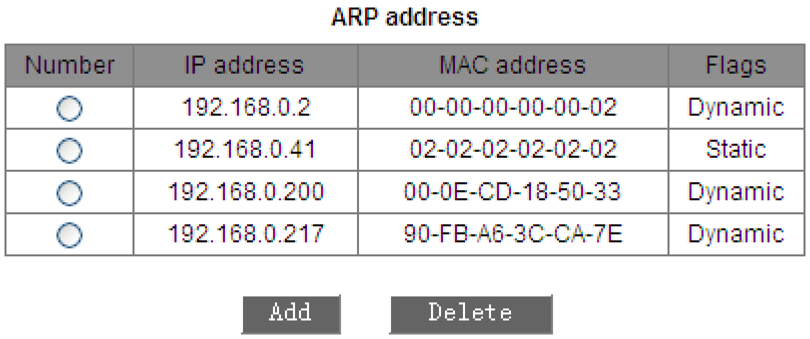
Format: {A.B.C.D, HHHHHHHHHHHH} (H is a hexadecimal number.)

Function: Configure static ARP entry.

Caution:

- The IP address of a static ARP entry must be on the same network segment with the IP address of the switch.
- If the IP address of a static entry is the IP address of the switch, the system automatically maps the IP address to the MAC address of the switch.
- In general, the switch automatically learns ARP entries. Manual configuration is not required.

3. View or delete an ARP entry, as shown in Figure 70.



ARP address

Number	IP address	MAC address	Flags
○	192.168.0.2	00-00-00-00-00-02	Dynamic
○	192.168.0.41	02-02-02-02-02-02	Static
○	192.168.0.200	00-0E-CD-18-50-33	Dynamic
○	192.168.0.217	90-FB-A6-3C-CA-7E	Dynamic

Figure 70 ARP Address Table

ARP Address

Portfolio: {IP address, MAC address, flag}

Function: Display ARP entries, including static and dynamic ones.

Operation: Select a static entry in the Number column. Click <Delete>. You can delete the entry.

Caution:

You cannot delete dynamic ARP entries.

6.11 SNMP

6.11.1 Overview

The Simple Network Management Protocol (SNMP) is a framework using TCP/IP to manage network devices. With the SNMP function, the administrator can query device information, modify parameter settings, monitor device status, and discover network faults.

6.11.2 Implementation

SNMP adopts the management station/agent mode. Therefore, SNMP involves two types of NEs: NMS and agent.

➢ The Network Management Station (NMS) is a station running

SNMP-enabled network management software client. It is the core for the network management of an SNMP network.

- Agent is a process in the managed network devices. It receives and processes request packets from the NMS. When an alarm occurs, the agent proactively reports it to the NMS.

The NMS is the manager of an SNMP network, while agent is the managed device of the SNMP network. The NMS and agents exchange management packets through SNMP. SNMP involves the following basic operations:

- Get-Request
- Get-Response
- Get-Next-Request
- Set-Request
- Trap

The NMS sends Get-Request, Get-Next-Request, and Set-Request packets to agents to query, configure, and manage variables. After receiving these requests, agents reply with Get-Response packets. When an alarm occurs, an agent proactively reports it to the NMS with a trap message.

6.11.3 Description

This series switches support SNMPv2. SNMPv2 is compatible with SNMPv1.

SNMPv1 uses community name for authentication. A community name acts as a password, limiting NMS's access to agents. If the switch does not acknowledge the community name carried by an SNMP packet, the packet is discarded.

SNMPv2 also uses community name for authentication. It is compatible with SNMPv1, and extends the functions of SNMPv1.

To enable the communication between the NMS and agent, their SNMP versions must match. Different SNMP versions can be configured on an agent, so that it can use different versions to communicate with different NMSs.

6.11.4 MIB

Any managed resource is called managed object. The Management Information Base (MIB) stores managed objects. It defines the hierarchical relationships of managed objects and attributes of objects, such as names, access permissions, and data types. Each agent has its own MIB. The NMS can read/write MIBs based on permissions. Figure 71 shows the relationships among the NMS, agent, and MIB.

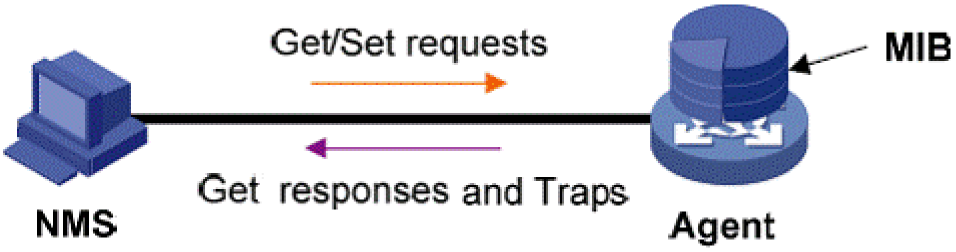


Figure 71 Relationship among NMS, Agent, and MIB

MIB defines a tree structure. The tree nodes are managed objects. Each node has a unique Object Identifier (OID), which indicates the location of the node in the MIB structure. As shown in Figure 72, the OID of object A is 1.2.1.1.

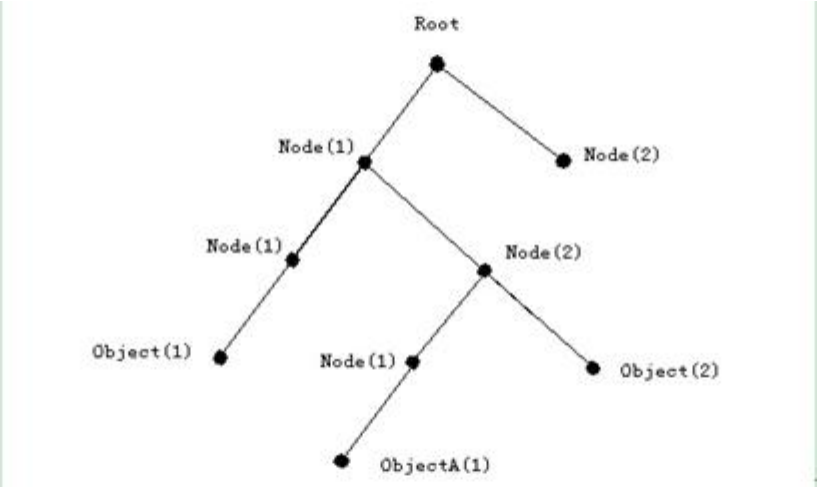
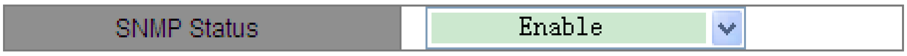


Figure 72 MIB Structure

6.11.5 Web Configuration

1. Enable SNMP, as shown in Figure 73.



SNMP Status	Enable

Figure 73 Enabling SNMP

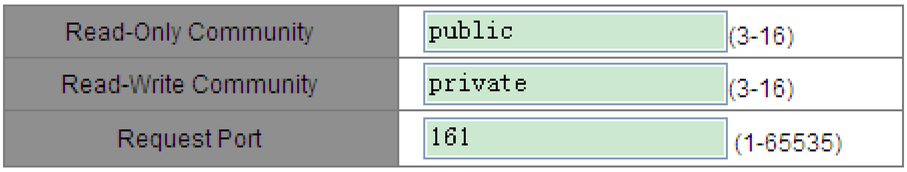
SNMP Status

Options: Enable/Disable

Default: Enable

Function: Enable or disable SNMP.

2. Configure access rights, as shown in Figure 74.



Read-Only Community	public (3-16)
Read-Write Community	private (3-16)
Request Port	161 (1-65535)

Figure 74 Access Rights Configuration

Read-Only Community

Range: 3~16 characters

Default: public

Function: Configure the name of read-only community.

Description: The MIB information of the switch can be read only if the community name carried by an SNMP packet is identical with that configured on the switch.

Read-Write Community

Range: 3~16 characters

Default: private

Function: Configure the name of read-write community.

Description: The MIB information of the switch can be read and written only if the community name carried by an SNMP packet is identical with that configured on the switch.

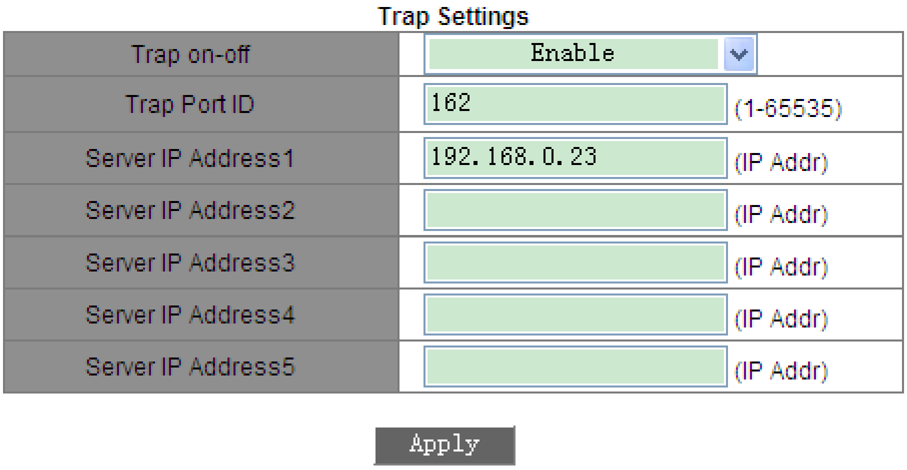
Request Port

Range: 1~65535

Default: 161

Function: Configure the number of the port for receiving SNMP requests.

3. Set trap parameters, as shown in Figure 75.



Trap Settings

Trap on-off	Enable	
Trap Port ID	162	(1-65535)
Server IP Address1	192.168.0.23	(IP Addr)
Server IP Address2		(IP Addr)
Server IP Address3		(IP Addr)
Server IP Address4		(IP Addr)
Server IP Address5		(IP Addr)

Figure 75 Trap Configuration

Trap on-off

Options: Enable/Disable

Default: Enable

Function: Enable or disable trap sending.

Trap Port ID

Options: 1~65535

Default: 162

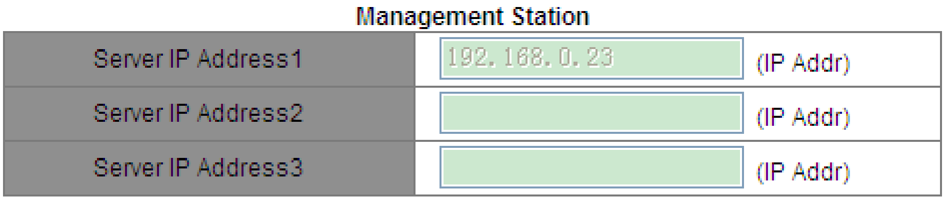
Function: Configure the number of port for sending trap messages.

Server IP Address

Format: A.B.C.D

Function: Configure the address of the server for receiving trap messages. You can configure a maximum of five servers.

4. View the IP address of the management server, as shown in Figure 76.



Management Station

Server IP Address1	192.168.0.23	(IP Addr)
Server IP Address2		(IP Addr)
Server IP Address3		(IP Addr)

Figure 76 IP Address of Management Server

The IP address of the management server does not need to be configured manually. The switch automatically displays it only if the NMS is running on the server and reads and writes the MIB node information of the device.

6.11.6 Typical Configuration Example

SNMP management server is connected to the switch through Ethernet. The IP address of the management server is 192.168.0.23, and the switch is 192.168.0.2.The NMS monitors and manages the Agent through SNMPv2, and reads and writes the MIB node information of the Agent. When the Agent is faulty, it proactively sends trap messages to the NMS, as shown in Figure 77.

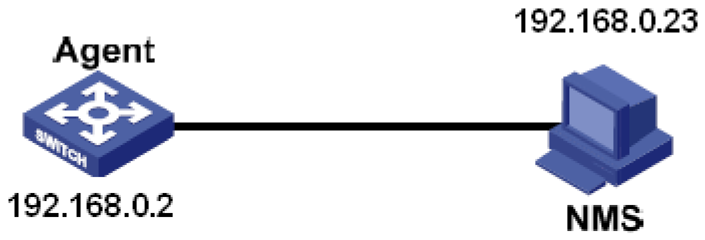


Figure 77 SNMP Configuration Example

Configuration on the Agent:

1. Enable SNMP, as shown in Figure 73.
2. Configure access rights. Set read-only community name to public, read-write community name to private, and request port to 161, as shown in Figure 74.
3. Enable trap sending, set trap port number to 162, and IP address of server to 192.168.0.23, as shown in Figure 75.

To monitor and manage the status of the Agent, run the management software, for example, Kyvision, on the NMS.

For operations on Kyvision, refer to the *Kyvision Operation Manual*.

6.12 DT-Ring

6.12.1 Overview

DT-Ring and DT-Ring+ are Kyland-proprietary redundancy protocols. They enable a network to recover within 50ms when a link fails, ensuring stable and reliable communication.

DT-Ring fall into two types: port-based ring (DT-Ring-Port) and VLAN-based ring (DT-Ring-VLAN).

- DT-Ring-Port: specifies a port to forward or block packets.
- DT-Ring-VLAN: specifies a port to forward or block the packets of a specific VLAN. This allows multiple VLANs on a tangent port, that is, one port is part of different redundant rings based on different VLANs.

DT-Ring-Port and DT-Ring-VLAN cannot be used together.

6.12.2 Concepts

- Master station: One ring has only one master station. The master station sends DT-Ring packets and detects the current status of the ring.
- Master port: On the master station, the first port whose link status changes to up is called the master port. It is in forwarding state.
- Slave port: On the master station, the port whose link status changes to up later is called the slave port. When the ring is closed, the slave port is in blocking state. When a ring is open due to a link or port failure, the status of the slave port changes to forwarding.
- Slave station: A ring can include multiple slave stations. Slave stations listen to and forward DT-Ring packets and report fault information to the master station.
- Backup port: The port for communication between DT rings is called the backup port.
- Master Backup Port: When there are multiple backup ports in a ring, the master backup port is the backup port corresponding to a large device MAC address and it is in a Forwarding state
- Slave Backup Port: When there are multiple backup ports in a ring, all the other ports (except the master backup port) are slave backup ports and they

are in blocking state.

- Forwarding state: port can forward and receive data
- Blocking state: port can receive and forward only DT-Ring packets, but cannot receive or forward any other data packets.

6.12.3 Implementation

1. DT-Ring implementation

The master port on the master station periodically sends DT-Ring packets to detect ring status. If the slave port of the master station receives the packets, the ring is closed; otherwise, the ring is open.

When a ring is closed, the master port of the master station is in a forwarding state, the slave port in a blocking state, and all ring ports of slave stations are in a forwarding state.

A ring may be open in the following cases:

- The master port of the master station fails. The statuses of the slave port on the master station and all ring ports of slave stations change to forwarding.
- The slave port of the master station fails. The statuses of the master port on the master station and all ring ports of slave stations change to forwarding.
- Another port or link fails. The statuses of the two ports of the master station and all up ports of slave stations change to forwarding.

DT-Ring configurations should meet the following conditions:

- All switches in the same ring must have the same domain number.
- Each ring can only have one master station and multiple slave stations.
- Only two ports can be configured on each switch for a ring.
- For two connected rings, backup ports can be configured only in one ring.
- Multiple backup ports can be configured in one ring.
- On a switch, only one backup port can be configured for one ring.
- DT-Ring-Port and DT-Ring-VLAN cannot be configured on one switch at the same time.

Figure 78 shows the working process of switch A, B, C, D.

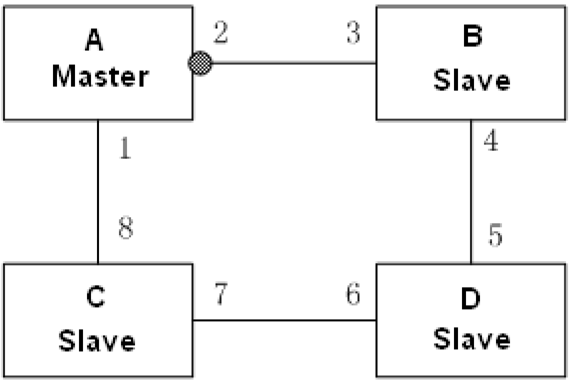


Figure 78 DT-Ring Topology

1. Configure Switch A as the master station, and others as slave stations.
2. Because Ring port 1 on the master station links up first, it is in a Forwarding state, and ring port 2 is in a Blocking state. The two ring ports of each slave are in a Forwarding state.
3. When link CD (connecting Switch C to Switch D) fails, as shown in Figure 79, port 2 switches to a Forwarding state, and port 6 and port 7 are in a Blocking state.

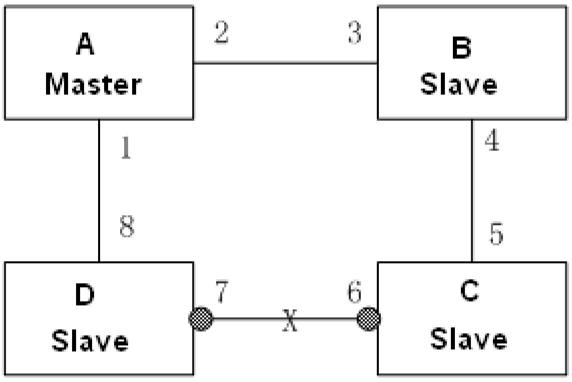


Figure 79 DT-Ring Link Fault

Caution:

The change in link state affects the roles and status of ring ports.

2. DT-Ring+ implementation

DT-Ring+ can provide backup for two DT rings, as shown in Figure 80. One backup port is configured respectively on Switch C and Switch D. Which port is the master backup port depends on the MAC addresses of the two ports. If the master backup port or its link fails, the slave backup port will forward packets, preventing loops and ensuring normal communication between redundant rings.

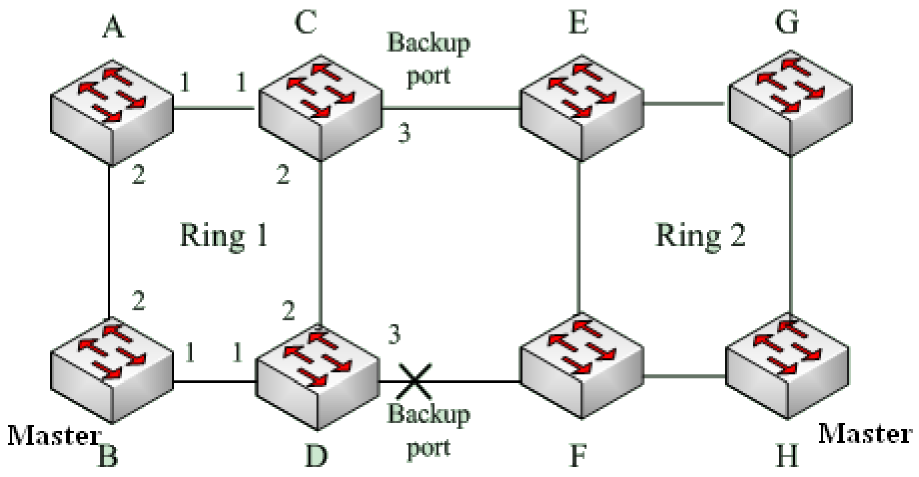


Figure 80 DT-Ring+ Topology

Caution:

Link status change affects the status of backup ports.

3. DT-Ring-VLAN implementation

DT-Ring-VLAN allows the packets of different VLANs to be forwarded in different paths. Each forwarding path for a VLAN forms a DT-Ring-VLAN. Different DT-Ring-VLANs can have different master stations. As shown in Figure 81, two DT-Ring-VLANs are configured.

Ring links of DT-Ring-VLAN10: AB-BC-CD-DE-EA

Ring links of DT-Ring-VLAN20: FB-BC-CD-DE-EF

The two rings are tangent at link BC, CD, and DE. Switch C and Switch D share the same ports in the two rings, but use different logical links based on VLAN.

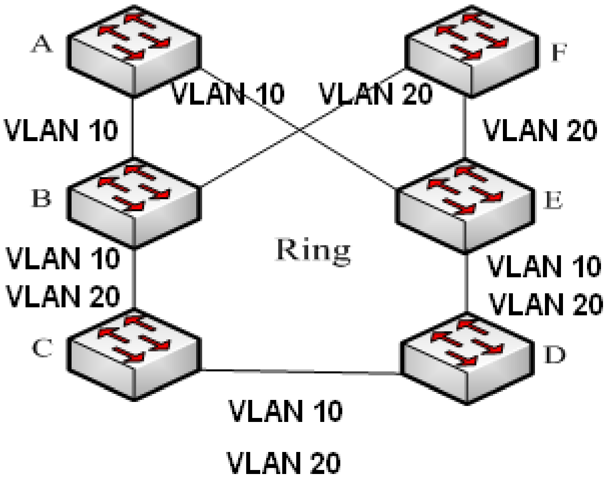
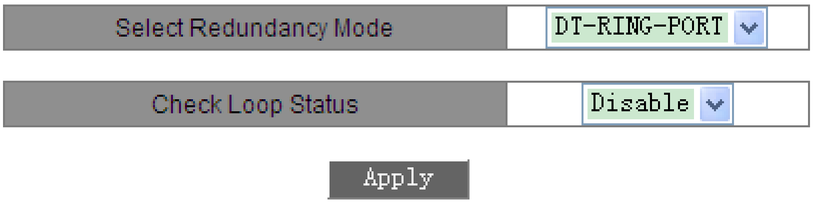


Figure 81 DT-Ring-VLAN

6.12.4 Web Configuration

1. Configure redundant ring mode and ring status detection, as shown in Figure 82.



Select Redundancy Mode: DT-RING-PORT

Check Loop Status: Disable

Figure 82 Redundant Ring Mode Configuration

Select Redundancy Mode

Options: DT-RING-PORT/DT-RING-VLAN

Default: DT-RING-PORT

Function: Select the redundancy mode.

Check Loop Status

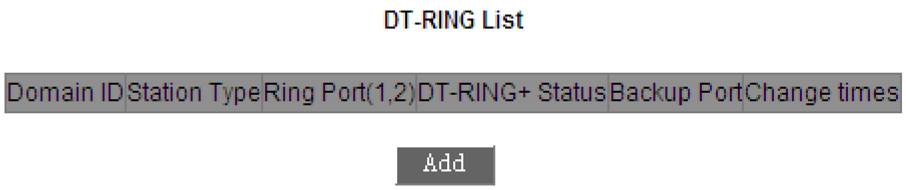
Options: Disable/Enable

Default: Disable

Function: Enable or disable ring status detection.

Description: After ring status detection is enabled, the switch automatically detects ring status. When a non-ring port receives DT-Ring packets, the port will be locked. Therefore, use the function with caution.

2. Create a DT ring, as shown in Figure 83.



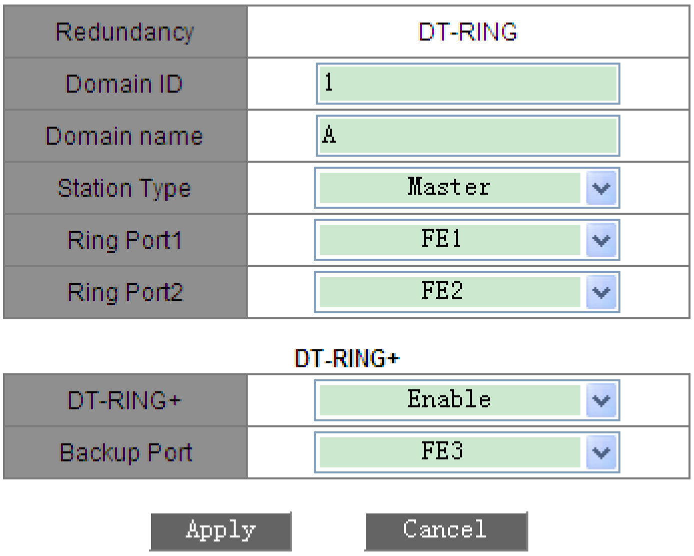
DT-RING List

Domain ID	Station Type	Ring Port(1,2)	DT-RING+ Status	Backup Port	Change times

Figure 83 Creating a DT Ring

Click <Add> and configure the DT ring.

3. Configure DT-Ring-Port and DT-Ring-VLAN, as shown in Figure 84 and Figure 85.

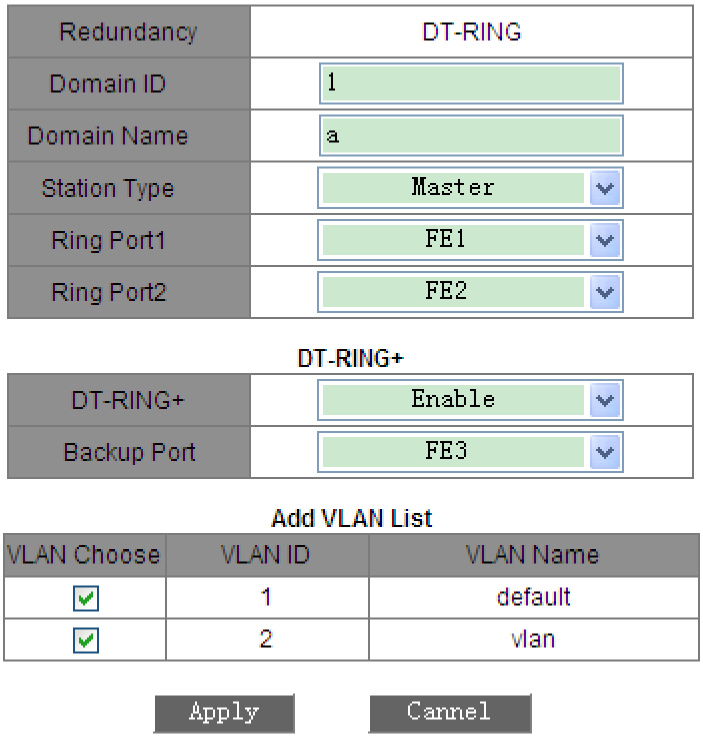


Redundancy	DT-RING
Domain ID	1
Domain name	A
Station Type	Master
Ring Port1	FE1
Ring Port2	FE2

DT-RING+

DT-RING+	Enable
Backup Port	FE3

Figure 84 DT-Ring-Port Configuration



Redundancy	DT-RING
Domain ID	1
Domain Name	a
Station Type	Master
Ring Port1	FE1
Ring Port2	FE2

DT-RING+

DT-RING+	Enable
Backup Port	FE3

Add VLAN List

VLAN Choose	VLAN ID	VLAN Name
☑	1	default
☑	2	vlan

Figure 85 DT-Ring-VLAN Configuration

Redundancy

Forced configuration: DT-Ring

Domain ID

Configuration rang: 1~32

Function: The domain ID is used to distinguish different rings. One switch supports a maximum of 16 port-based rings or 8 VLAN-based rings.

Domain name

Range: 1~31 characters

Function: Configure the domain name.

Station Type

Options: Master/Slave

Default: Master

Function: Select the switch role in a ring.

Ring port 1/Ring port 2

Options: all switch ports

Function: Select two ring ports.

DT-Ring+

Options: Enable/Disable

Default: Disable

Function: Enable/disable DT-Ring+.

Backup port

Options: all switch ports

Function: Set a port to backup port.

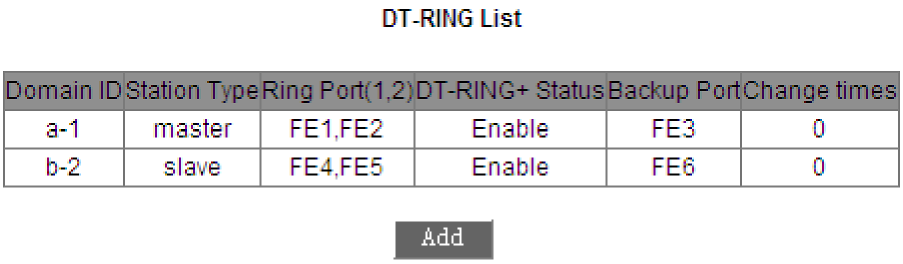
Explanation: Enable DT-Ring+ before setting backup port.

Add VLAN list

Options: all created VLANs

Function: Select the VLANs for the ring port.

After parameters are set, the DT-Ring List shows all created rings, as shown in Figure 86.



DT-RING List

Domain ID	Station Type	Ring Port(1,2)	DT-RING+ Status	Backup Port	Change times
a-1	master	FE1,FE2	Enable	FE3	0
b-2	slave	FE4,FE5	Enable	FE6	0

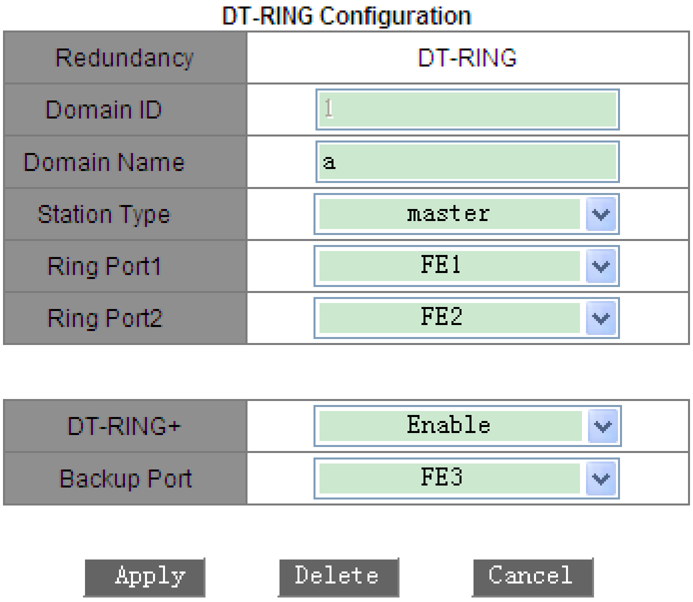
Figure 86 DT-Ring List

Caution:

- A ring port or backup port cannot be added to a trunk group. A port added to a trunk group cannot be configured as a ring port or backup port.
- A ring port or backup port can be configured as a mirroring source or destination port. A mirroring source or destination port cannot be configured as a ring port or backup port.
- STP cannot be enabled on a ring port or a backup port. An STP-enabled port cannot be configured as a ring port or backup port.

4. View and modify DT-Ring configuration.

Click a DT-Ring entry in Figure 86 to show its ring configuration and modify it, as shown in Figure 87.



DT-RING Configuration

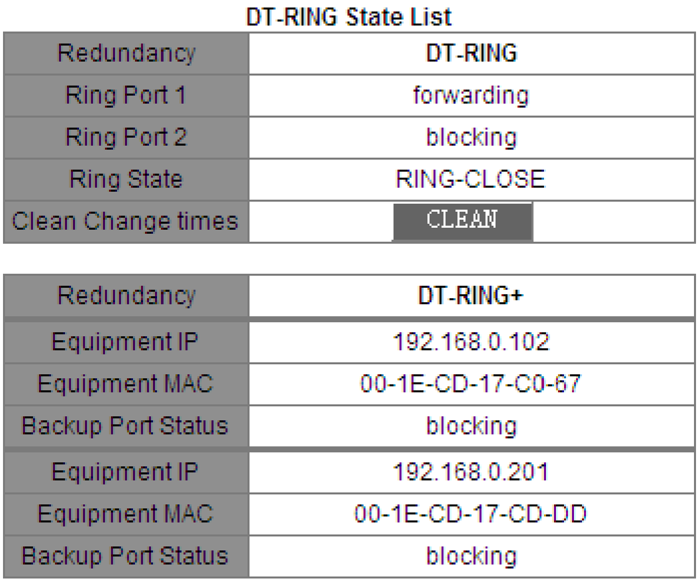
Redundancy	DT-RING
Domain ID	1
Domain Name	a
Station Type	master
Ring Port1	FE1
Ring Port2	FE2

DT-RING+	Enable
Backup Port	FE3

Figure 87 DT-Ring Configuration

Click <Apply> for changes to take effect after modification. Click <Delete> to delete the DT-Ring configuration entry.

5. View DT-Ring and port status, as shown in Figure 88.



DT-RING State List

Redundancy	DT-RING
Ring Port 1	forwarding
Ring Port 2	blocking
Ring State	RING-CLOSE
Clean Change times	CLEAN

Redundancy	DT-RING+
Equipment IP	192.168.0.102
Equipment MAC	00-1E-CD-17-C0-67
Backup Port Status	blocking
Equipment IP	192.168.0.201
Equipment MAC	00-1E-CD-17-CD-DD
Backup Port Status	blocking

Figure 88 DT-Ring State

6.12.5 Typical Configuration Example

As shown in Figure 80, Switch A, B, C, and D form Ring 1; Switch E, F, G, and H form ring 2. Links CE and DF are the backup links between Ring 1 and Ring 2.

Configuration on Switch A:

1. Domain ID: 1; Domain name: Ring; Ring port: port 1 and port2; Station type: Slave; DT-Ring+: Disable; do not set backup ports, as shown in Figure 84.

Configuration on Switch B:

2. Domain ID: 1; Domain name: Ring; Ring port: port 1 and port 2; Station type: Master; DT-Ring+: Disable; do not set backup ports, as shown in Figure 84.

Configuration on Switch C and Switch D:

3. Domain ID: 1; Domain name: Ring; Ring port: port 1 and port2; Station type: Slave; DT-Ring+: Enable; Backup port: port 3, as shown in Figure 84.

Configuration on Switch E, Switch F, and Switch G:

4. Domain ID: 2; Domain name: Ring; Ring port: port 1 and port2; Station type: Slave; DT-Ring+: Disable; do not set backup ports, as shown in Figure 84.

Configuration on Switch H:

5. Domain ID: 2; Domain name: Ring; Ring port: port 1 and port2; Station type: Master; DT-Ring+: Disable; do not set backup ports, as shown in Figure 84.

6.13 RSTP/STP

6.13.1 Overview

Standardized in IEEE802.1D, the Spanning Tree Protocol (STP) is a LAN protocol used for preventing broadcast storms caused by link loops and providing link backup. STP-enabled devices exchange packets and block certain ports to prune "loops" into "trees", preventing proliferation and endless loops. The drawback of STP is that a port must wait for twice the forwarding delay to move to the forwarding state.

To overcome the drawback, IEEE creates 802.1w standard to supplement 802.1D.IEEE802.1w defines the Rapid Spanning Tree Protocol (RSTP). Compared with STP, RSTP achieves much more rapid convergence by adding alternate port and backup port for the root port and designated port respectively. When the root port is invalid, the alternate port can enter the forwarding state quickly.

6.13.2 Concepts

- Root bridge: serves as the root for a tree. A network has only one root bridge. The root bridge changes with network topology. The root bridge periodically sends BPDU to the other devices, which forward the BPDU to ensure topology stability.
- Root port: indicates the best port for transmission from the non-root bridges to the root bridge. The best port is the port with the smallest cost to the root bridge. A non-root bridge communicates with the root bridge through the root port. A non-root bridge has only one root port. The root bridge has no root port.
- Designated port: indicates the port for forwarding BPDU to other devices or LANs. All ports on the root bridge are designated ports.
- Alternate port: indicates the backup port of the root port. If the root port fails, the alternate port becomes the new root port.
- Backup port: indicates the backup port of the designated port. When a designated port fails, the backup port becomes the new designated port and forwards data.

6.13.3 BPDU

To prevent loops, all the bridges of a LAN calculate a spanning tree. The calculation process involves transmitting BPDUs among devices to determine the network topology. Table 6 shows the data structure of a BPDU.

Table 6 BPDU

…	Root bridge ID	Root path cost	Designated bridge ID	Designated port ID	Message age	Max age	Hello time	Forward delay	…
…	8 bytes	4 bytes	8 bytes	2 bytes	2 bytes	2 bytes	2 bytes	2 bytes	…

Root bridge ID: priority of the root bridge (2 bytes)+MAC address of the root bridge (6 bytes).

Root path cost: cost of the path to the root bridge.

Designated bridge ID: priority of the designated bridge (2 bytes)+MAC address of the designated bridge (6 bytes).

Designated port ID: port priority+port number.

Message age: duration that a BPDU can be spread in a network.

Max age: maximum duration that a BPDU can be saved on a device. When Message age is larger than Max age, the BPDU is discarded.

Hello time: interval for sending BPDUs.

Forward delay: status change delay (discarding--learning--forwarding).

6.13.4 Implementation

The process for all bridges calculating the spanning tree with BPDUs is as follows:

1. In the initial phase, each port of all devices generates the BPDU with itself as the root bridge; both root bridge ID and designated bridge ID are the ID of the local device; the root path cost is 0; the designated port is the local port.
2. Best BPDU selection: All devices send their own BPDUs and receive BPDUs from other devices. Upon receiving a BPDU, each port compares the received BPDU with its own.

➢ If the priority of its own BPDU is higher, then the port does not perform any operation.

- If the priority of the received BPDU is higher, then the port replaces the local BPDU with the received one.

Devices compare the BPDUs of all ports and figure out the best BPDU. Principles for comparing BPDUs are as follows:

- The BPDU with a smaller root bridge ID has a higher priority.
- If the root bridge IDs of two BPDUs are the same, their root path costs are compared. If the root path cost in a BPDU plus the path cost of the local port is smaller, then the priority of the BPDU is higher.
- If the root path costs of two BPDUs are also the same, the designated bridge IDs, designated port IDs, and IDs of the port receiving the BPDUs are further compared in order. The BPDU with a smaller ID has a higher priority. The BPDU with a smaller root bridge ID has a higher priority.
- If the root bridge IDs of two BPDUs are the same, their root path costs are compared. If the root path cost in a BPDU plus the path cost of the local port is smaller, the priority of the BPDU is higher.
- If the root path costs of two BPDUs are also the same, the designated bridge IDs, designated port IDs, and IDs of the port receiving the BPDUs are further compared in order. The BPDU with a smaller ID has a higher priority.

3. Selection of the root bridge: The root bridge of the spanning tree is the bridge with the smallest bridge ID.
4. Selection of the root bridge: A non-root-bridge device select the port receiving the best BPDU as the root port.
5. BPDU calculation of the designated port: Based on the BPDU of the root port and the path cost of the root port, a device calculated a designated port BPDU for each port as follows:

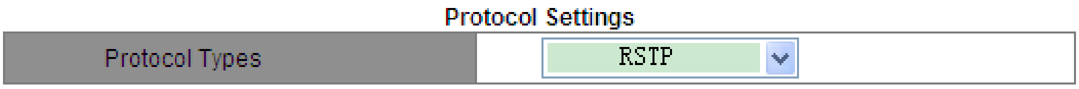
- Replace the root bridge ID with the root bridge ID of the BPDU of the root port.

- ➢ Replace the root path cost with the root path cost of the root port BPDU plus the path cost of the root port.
- ➢ Replace designated bridge ID with the ID of the local device.
- ➢ Replace the designated port ID with the ID of the local port.

6. Selection of the designated port: If the calculated BPDU is better, then the device selects the port as the designated port, replaces the port BPDU with the calculated BPDU, and sends the calculated BPDU. If the port BPDU is better, then the device does not update the port BPDU and blocks the port. Blocked ports can receive and forward only RSTP packets, but not other packets.

6.13.5 Web Configuration

1. Enable STP/RSTP, as shown in Figure 89.



Protocol Settings

Protocol Types	RSTP

Figure 89 Enabling RSTP/STP

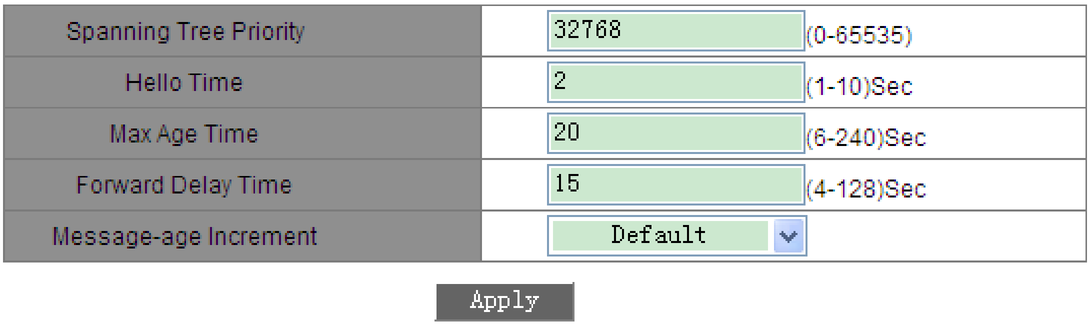
Protocol Types

Options: Disable/RSTP/STP

Default: Disable

Function: Disable or enable RSTP or STP.

2. Set the time parameters of the network bridge, as shown in Figure 90.



Spanning Tree Priority	32768	(0-65535)
Hello Time	2	(1-10)Sec
Max Age Time	20	(6-240)Sec
Forward Delay Time	15	(4-128)Sec
Message-age Increment	Default	

Figure 90 Setting Time Parameters of the Network Bridge

Spanning Tree Priority

Range: 0~65535. The step is 4096.

Default: 32768

Function: Configure the priority of the network bridge.

Description: The priority is used for selecting the root bridge. The smaller the value, the higher the priority.

Hello time

Range: 1~10s

Default: 2s

Function: Configure the interval for sending BPDU.

Max Age Time

Range: 6~240s

Default: 20s

Description: If the value of message age in the BPDU is larger than the specified value, then the BPDU is discarded.

Forward Delay Time

Range: 4~128s

Default: 15s

Function: Configure status change time from Discarding to Learning or from Learning to Forwarding.

Message-age Increment

Options: Compulsion/Default

Default: Default

Function: Configure the value to be added to message age when a BPDU passes through a network bridge.

Description: In compulsion mode, the value is 1.

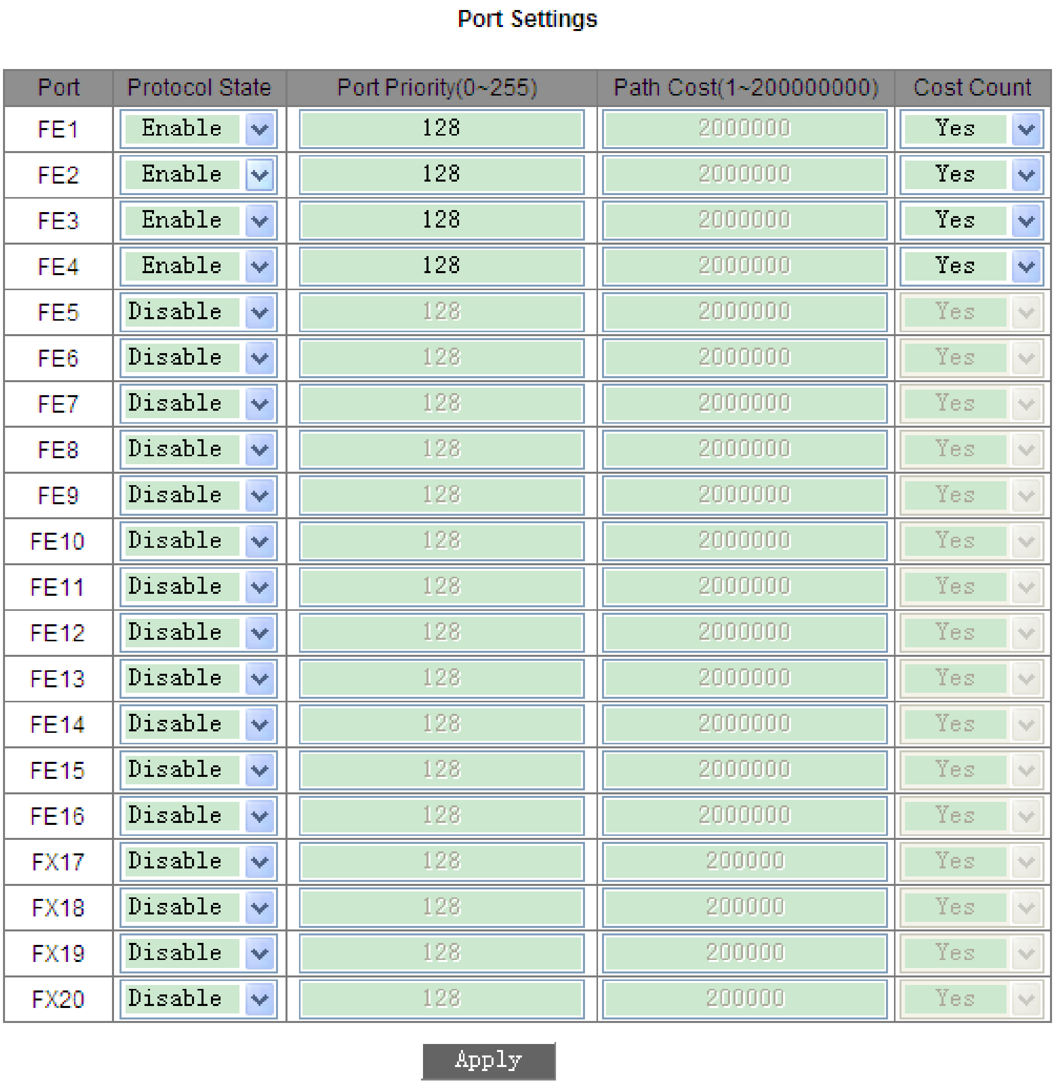
In default mode, the value is max(max age time/16, 1).

Forward Delay Time, Max Age Time, and Hello Time shall meet the following requirements:

2 x (Forward Delay Time – 1.0 seconds) >= Max Age Time;

Max Age Time >= 2 x (Hello Time + 1.0 seconds).

3. Enable RSTP on ports, as shown in Figure 91.



Port Settings

Port	Protocol State	Port Priority(0~255)	Path Cost(1~200000000)	Cost Count
FE1	Enable	128	2000000	Yes
FE2	Enable	128	2000000	Yes
FE3	Enable	128	2000000	Yes
FE4	Enable	128	2000000	Yes
FE5	Disable	128	2000000	Yes
FE6	Disable	128	2000000	Yes
FE7	Disable	128	2000000	Yes
FE8	Disable	128	2000000	Yes
FE9	Disable	128	2000000	Yes
FE10	Disable	128	2000000	Yes
FE11	Disable	128	2000000	Yes
FE12	Disable	128	2000000	Yes
FE13	Disable	128	2000000	Yes
FE14	Disable	128	2000000	Yes
FE15	Disable	128	2000000	Yes
FE16	Disable	128	2000000	Yes
FX17	Disable	128	200000	Yes
FX18	Disable	128	200000	Yes
FX19	Disable	128	200000	Yes
FX20	Disable	128	200000	Yes

Figure 91 Port Settings

Protocol Status

Options: Enable/Disable

Default: Disable

Function: Enable or disable STP on ports.

Caution:

➢ An STP-enabled port cannot be configured as a mirroring source or destination port. STP cannot be enabled on a mirroring source or destination port.

- An STP-enabled port cannot be added to a trunk group. STP cannot be enabled on a port added to a trunk group.
- An STP-enabled port cannot be configured as a ring port or backup port. STP cannot be enabled on a ring port or a backup port.

Port Priority

Range: 0~255. The step is 16.

Default: 128

Function: Configure the port priority, which determines the roles of ports.

Path Cost

Range: 1~200000000

Default: 2000000 (10M port), 200000 (100M port), 20000 (1000M port)

Description: The path cost of a port is used to calculate the best path. The value of the parameter depends on the bandwidth. The larger the value, the lower the cost. You can change the role of a port by changing the value of the path cost parameter. To configure the value manually, select No for Cost Count.

Cost Count

Range: Yes/No

Default: Yes

Description: Yes indicates the path cost of the port adopts the default value. No indicates you can configure the path cost.

6.13.6 Typical Configuration Example

The priority of Switch A, B, and C are 0, 4096, and 8192. Path costs of links are 4, 5, and 10, as shown in Figure 92.

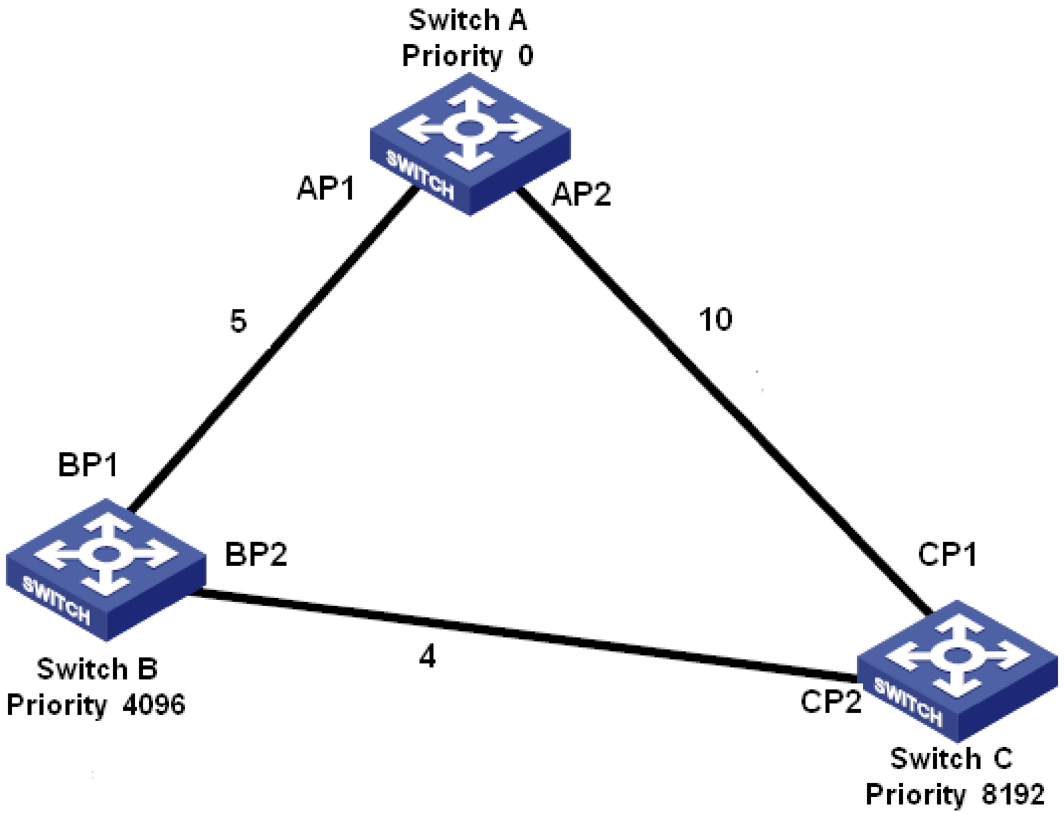


Figure 92 RSTP Configuration Example

Configuration on Switch A:

1. Set priority to 0 and time parameters to default values, as shown in Figure 90.
2. Set the path cost of port 1 to 5 and that of port 2 to 10, as shown in Figure 91.

Configuration on Switch B:

1. Set priority to 4096 and time parameters to default values, as shown in Figure 90.
2. Set the path cost of port 1 to 5 and that of port 2 to 4, as shown in Figure 91.

Configuration on Switch C:

1. Set priority to 8192 and time parameters to default values, as shown in Figure 90.
2. Set the path cost of port 1 to 10 and that of port 2 to 4, as shown in Figure 91.

- The priority of Switch A is 0 and the root ID is the smallest. Therefore, Switch A is the root bridge.
- The path cost from AP1 to BP1 is 5 and that from AP2 to BP2 is 14. Therefore, BP1 is the root port.
- The path cost from AP1 to CP2 is 9 and that from AP2 to CP1 is 10. Therefore, CP2 is the root port and BP2 is the designated port.

6.14 RSTP/STP Transparent Transmission

6.14.1 Overview

RSTP is compliant with IEEE standard. DT-Ring is the private redundant protection protocol of Kyland, but cannot coexist with RSTP on the same network. To solve this problem, Kyland developed the RSTP transparent transmission function. The function enables the switch to keep other redundant protocols while transparently transmitting RSTP packets, meeting industrial communication requirements.

Switches running other redundant protocols can receive and forward RSTP packets only if the RSTP transparent transmission function is enabled. RSTP transparent transmission-enabled switches can be regarded as a transparent link.

As shown in Figure 93, Switch A, Switch B, Switch C, and Switch D form a DT-Ring network. The transparent transmission function is enabled on these four switches, so that Switch E and Switch F can receive RSTP packets from each other.

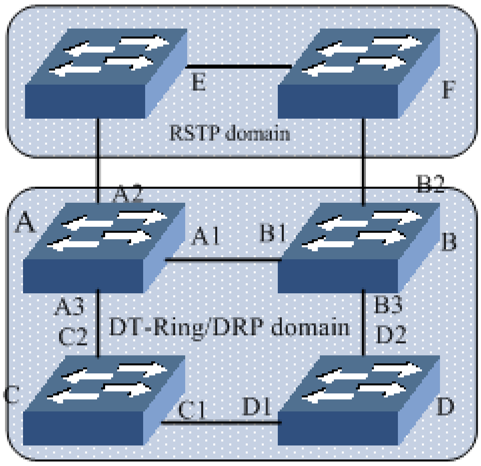
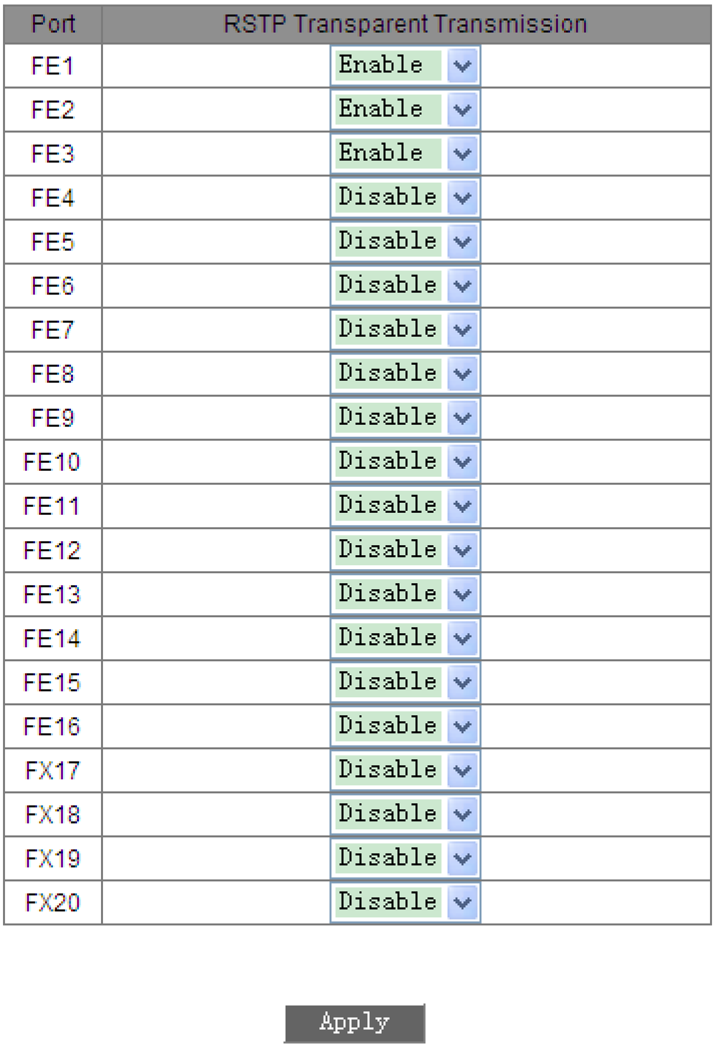


Figure 93 RSTP Transparent Transmission

6.14.2 Web Configuration

Configure RSTP transparent transmission on ports, as shown in Figure 94.



Port	RSTP Transparent Transmission
FE1	Enable
FE2	Enable
FE3	Enable
FE4	Disable
FE5	Disable
FE6	Disable
FE7	Disable
FE8	Disable
FE9	Disable
FE10	Disable
FE11	Disable
FE12	Disable
FE13	Disable
FE14	Disable
FE15	Disable
FE16	Disable
FX17	Disable
FX18	Disable
FX19	Disable
FX20	Disable

Figure 94 RSTP Transparent Transmission Configuration

RSTP Transparent Transmission

Options: Enable/Disable

Default: Disable

Function: Enable or disable RSTP transparent transmission on ports.

Caution:

RSTP transparent transmission cannot be enabled on RSTP-enabled ports.

6.14.3 Typical Configuration Example

As shown in Figure 93, Switch A, Switch B, Switch C, and Switch D form a DT ring, and Switch E and Switch F form an RSTP ring. In the RSTP ring, the entire DT ring serves as a transparent link to forward RSTP packets of Switch E and Switch F.

- Configure Switch A, Switch B, Switch C, and Switch D as a DT ring. For details, see DT-Ring Configuration.
- Enable RSTP on the involved ports of Switch E and Switch F, as shown in Figure 89 and Figure 91.
- Enable RSTP transparent transmission on ports A1, A2, A3, B1, B2, B3, C1, C2, D1, and D2, as shown in Figure 94.

6.15 QoS

6.15.1 Overview

Quality of Service (QoS) enables differentiated services based on different requirements under limited bandwidths by means of traffic control and resource allocation on IP networks. QoS tries to satisfy the transmission of different services to reduce network congestion and minimize congestion's impact on the services of high priority.

QoS mainly involves service identification, congestion management, and congestion avoidance.

Service identification: Objects are identified based on certain match rules. For example, the objects can be priority tags carried by packets, priority mapped by ports and VLANs, or priority information mapped by quintuples. Service identification is the precondition for QoS.

Congestion management: This is mandatory for solving resource competition. Congestion management caches packets in queues and determines the sequence of packet forwarding based on a certain scheduling algorithm, achieving preferential forwarding for key services.

Congestion avoidance: Excessive congestion may result in damage on network resources. Congestion avoidance monitors the use of network resources. When detecting increasing congestion, the function adopts proactive packet discarding and tunes traffic volume to solve the overload.

6.15.2 Principle

Each port of the switch has four cache queues, from 0 to 3 in priority ascending order.

You can configure the mapping between priority and queues. When a frame reaches the port, the switch determines the queue for the frame according to the information in the frame header. The switch supports three queue mapping modes for priority identification: highest priority, TOS/DIFF, and 802.1p.

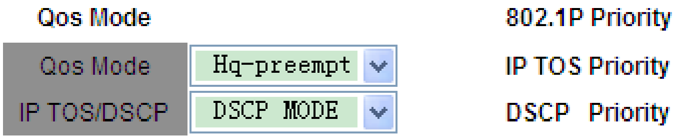
- If the highest priority is configured on a port, then packets to be forwarded are put in queue 3.
- The TOS/DIFF value depends on the TOS/DSCP in packets. You can configure the mapping between priority and queues.
- When a packet is tagged, the 802.1p value depends on the priority of 802.1Q in the packet. When a packet is untagged, the 802.1p value depends on the default priority of the port. You can configure the mapping between the 802.1p priority and queues.

When forwarding data, a port uses a scheduling mode to schedule the data of four queues and the bandwidth of each queue. The switch supports two scheduling modes: Weighted Round Robin (WRR) and preempt mode.

- ➢ WRR schedules data flows based on weight ratio. Queues obtain their bandwidths based on their weight ratio. WRR prioritizes high-weight ratio queues. More bandwidths are allocated to queues with higher weight ratio.
- ➢ Hq-preempt mode forwards high-priority packets preferentially. It is mainly used for transmitting sensitive signals. If a frame enters the high-priority queue, the switch stops scheduling the low-priority queues and starts to process the data of the high-priority queue. When the high-priority queue contains no data, the switch starts to process the data of the queue with lower priority.

6.15.3 Web Configuration

1. Configure the QoS mode, as shown in Figure 95.



Qos Mode: Hq-preempt

IP TOS/DSCP: DSCP MODE

Figure 95 QoS Mode

QoS Mode

Options: Disable/WRR/Hq-preempt

Default: Hq-preempt

Function: Configure the scheduling mode of a port.

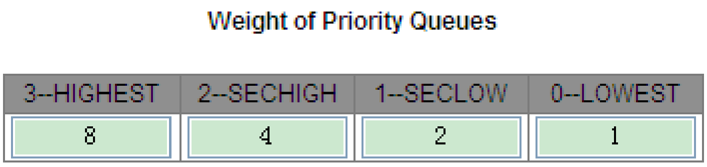
IP TOS/DSCP

Options: DSCP MODE/IP TOS MODE

Default: DSCP MODE

Function: DSCP and IP TOS share the same field. DSCP mode indicates the DSCP priority-queue mapping mode and IP TOS mode indicates the IP TOS priority-queue mapping mode.

2. Configure the queue weight ratio, as shown in Figure 96.



Weight of Priority Queues

3--HIGHEST	2--SECHIGH	1--SECLOW	0--LOWEST
8	4	2	1

Figure 96 Configuring Queue Weight Ratio

{3-HIGHEST, 2-SECHIGH, 1-SECLOW, 0-LOWEST}

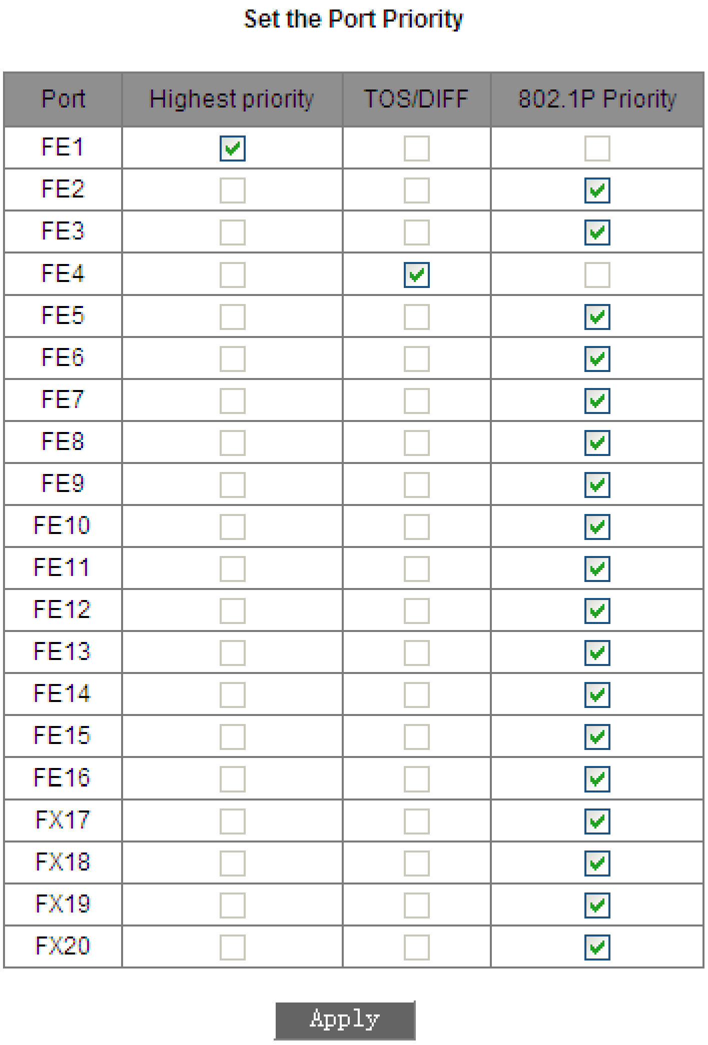
Range: {1~55, 1~55, 1~55, 1~55}

Default: {8, 4, 2, 1}

Function: Configure the queue weight ratio by obeying the following rules:

Weight of queue 3 ≥ 2 × Weight of queue 2, Weight of queue 2 ≥ 2 × Weight of queue 1, Weight of queue 1 ≥ 2 × Weight of queue 0

3. Configure QoS port priority mapping mode, as shown in Figure 97.



Set the Port Priority

Port	Highest priority	TOS/DIFF	802.1P Priority
FE1	☑	□	□
FE2	□	□	☑
FE3	□	□	☑
FE4	□	☑	□
FE5	□	□	☑
FE6	□	□	☑
FE7	□	□	☑
FE8	□	□	☑
FE9	□	□	☑
FE10	□	□	☑
FE11	□	□	☑
FE12	□	□	☑
FE13	□	□	☑
FE14	□	□	☑
FE15	□	□	☑
FE16	□	□	☑
FX17	□	□	☑
FX18	□	□	☑
FX19	□	□	☑
FX20	□	□	☑

Figure 97 Setting QoS Port Priority Mapping Mode

Set the Port Priority

Options: Highest priority/TOS/DIFF/802.1p Priority

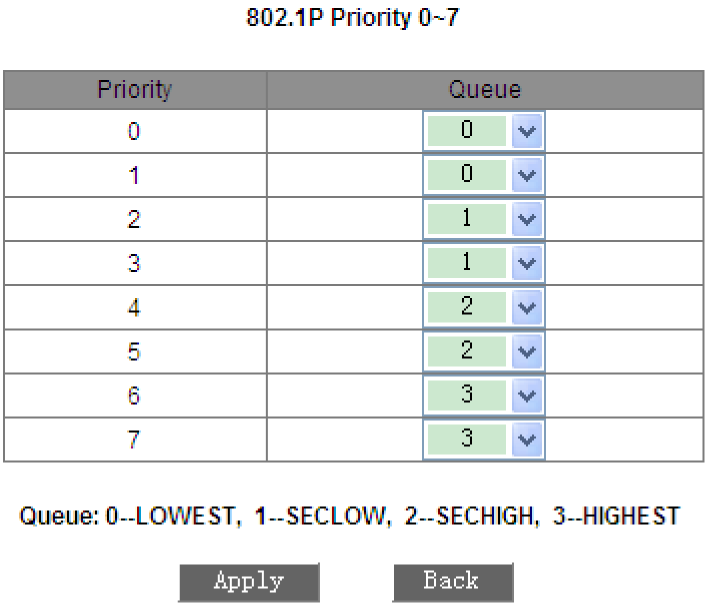
Default: 802.1p Priority

Function: Configure port priority mapping mode.

Description: Only one priority mapping mode can be selected for each port.

4. Configure 802.1p priority-queue mapping.

Click <802.1p Priority> in Figure 95 to configure the 802.1p priority-queue mapping, as shown in Figure 98.



802.1P Priority 0~7

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

Queue: 0--LOWEST, 1--SECLOW, 2--SECHIGH, 3--HIGHEST

Figure 98 802.1p Priority-Queue Mapping

802.1p Priority Configuration

Portfolio: {Priority, Queue}

Range: {0~7, 0~3}

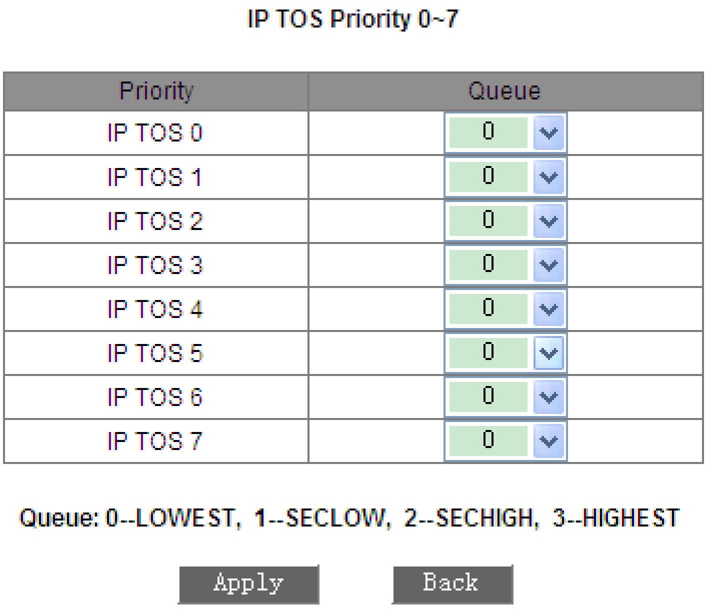
Default: Priority 0 and 1 are mapped to queue 0; priority 2 and 3 are mapped to queue 1.

Priority 4 and 5 are mapped to queue 2; priority 6 and 7 are mapped to queue 3.

Function: Configure the mapping between 802.1p priority and queue.

5. Configure IP TOS priority-queue mapping.

Click <IP TOS Priority> in Figure 95 to configure the DSCP priority-queue mapping, as shown in Figure 99.



IP TOS Priority 0~7

Priority	Queue
IP TOS 0	0
IP TOS 1	0
IP TOS 2	0
IP TOS 3	0
IP TOS 4	0
IP TOS 5	0
IP TOS 6	0
IP TOS 7	0

Queue: 0--LOWEST, 1--SECLOW, 2--SECHIGH, 3--HIGHEST

Figure 99 IP TOS Priority-Queue Mapping

IP TOS Priority Configuration

Portfolio: {Priority, Queue}

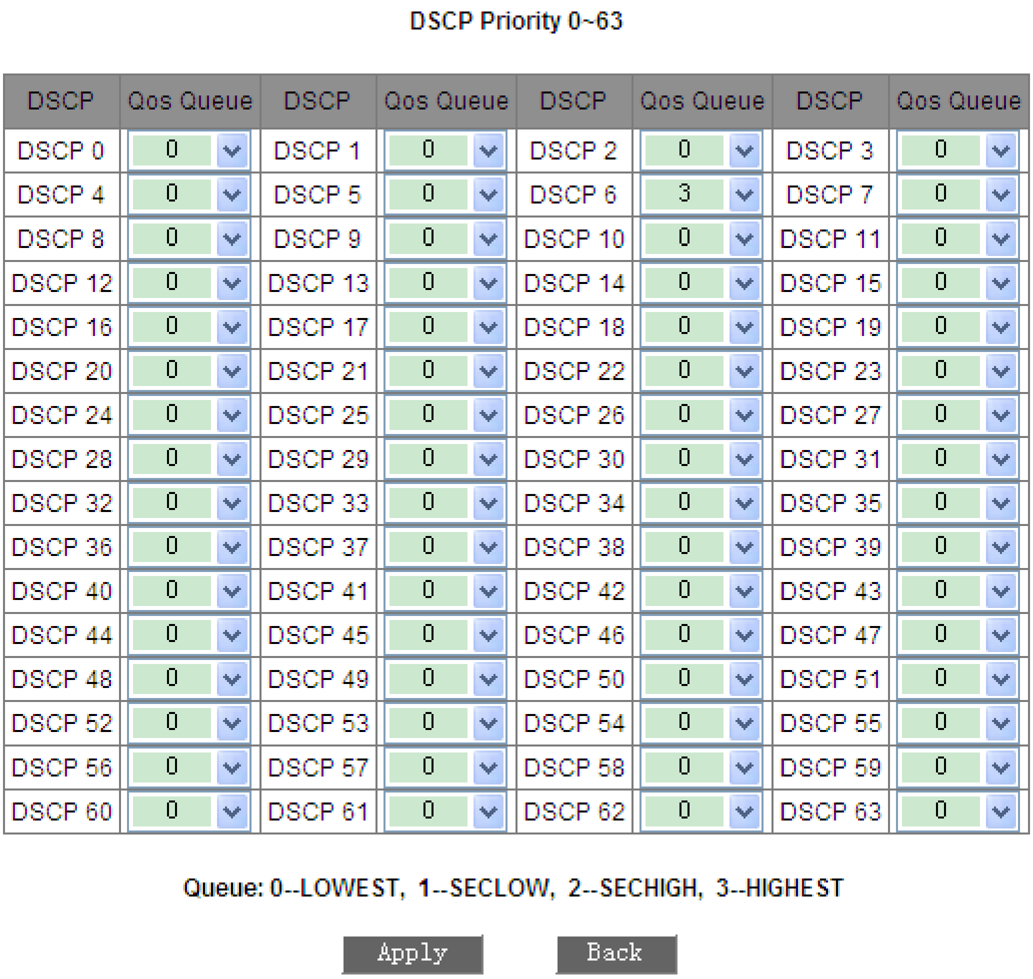
Range: {0~7, 0~3}

Default: Priority 0 to 7 is mapped to queue 0.

Function: Configure the mapping between IP TOS priority and queue.

6. Configure DSCP priority-queue mapping.

Click <DSCP Priority> in Figure 95 to configure the DSCP priority-queue mapping, as shown in Figure 100.



DSCP Priority 0~63

DSCP	Qos Queue	DSCP	Qos Queue	DSCP	Qos Queue	DSCP	Qos Queue
DSCP 0	0	DSCP 1	0	DSCP 2	0	DSCP 3	0
DSCP 4	0	DSCP 5	0	DSCP 6	3	DSCP 7	0
DSCP 8	0	DSCP 9	0	DSCP 10	0	DSCP 11	0
DSCP 12	0	DSCP 13	0	DSCP 14	0	DSCP 15	0
DSCP 16	0	DSCP 17	0	DSCP 18	0	DSCP 19	0
DSCP 20	0	DSCP 21	0	DSCP 22	0	DSCP 23	0
DSCP 24	0	DSCP 25	0	DSCP 26	0	DSCP 27	0
DSCP 28	0	DSCP 29	0	DSCP 30	0	DSCP 31	0
DSCP 32	0	DSCP 33	0	DSCP 34	0	DSCP 35	0
DSCP 36	0	DSCP 37	0	DSCP 38	0	DSCP 39	0
DSCP 40	0	DSCP 41	0	DSCP 42	0	DSCP 43	0
DSCP 44	0	DSCP 45	0	DSCP 46	0	DSCP 47	0
DSCP 48	0	DSCP 49	0	DSCP 50	0	DSCP 51	0
DSCP 52	0	DSCP 53	0	DSCP 54	0	DSCP 55	0
DSCP 56	0	DSCP 57	0	DSCP 58	0	DSCP 59	0
DSCP 60	0	DSCP 61	0	DSCP 62	0	DSCP 63	0

Queue: 0--LOWEST, 1--SECLOW, 2--SECHIGH, 3--HIGHEST

Figure 100 DSCP Priority-Queue Mapping

DSCP Priority Configuration

Portfolio: {DSCP, Qos Queue}

Range: {0~63, 0~3}

Default: Priority 0 to 63 is mapped to queue 0.

Function: Configure the mapping between DSCP priority and queue.

6.15.4 Typical Configuration Example

As shown in Figure 101, port 1 to port 4 forward packets to port 5. The highest priority mode is configured on port 1. Packets from port 1 are mapped to queue 1. The 802.1p priority carried by packets from port 2 is 2, which is mapped to queue 1. The 802.1p priority carried by packets from port 3 is 4, which is mapped to queue 2. The DSCP priority carried by packets from port 4 is 6, which is mapped to queue 3. Port 5 adopts the WRR scheduling mode.

Configuration steps:

1. Select WRR for QoS mode and DSCP for IP TOS/DSCP. Keep default settings for WRR queue weight ratio, as shown in Figure 95 and Figure 96.
2. Configure highest priority-queue mapping on port 1, 802.1p on port 2 and port 3, and TOS/DIFF on port 4, as shown in Figure 97.
3. Configure 802.1p priority 2 and 4 to map to queue 1 and queue 2 respectively, as shown in Figure 98.
4. Configure DSCP priority 6 to map to queue 3, as shown in Figure 100.

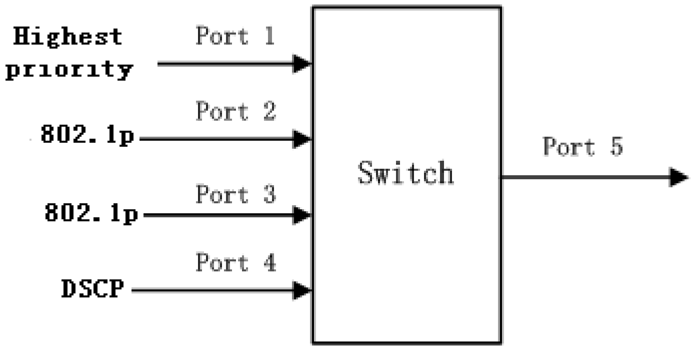


Figure 101 QoS Configuration Example

Packets received through port 1 and port 4 are put into queue 3; packets received through port 2 are put into queue 1; packets received through port 3 are put into queue 2. According to the mapping between queues and weights, the weight of queue 1 is 2, the weight of queue 2 is 4, and the weight of queue 3 is 8. As a result, the packets in queue 1 enjoy 2/(2+4+8) bandwidth, those in queue 2 enjoy 4/(2+4+8) bandwidth, and those in queue 3 enjoy 8/(2+4+8) bandwidth. Packets received through port 1 and port 4 are put into queue 3 and forwarded according to the FIFO mechanism. The total bandwidth ratio of port 1 and port 4 is 8/(2+4+8).

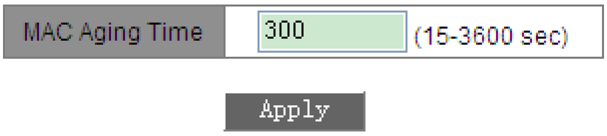
6.16 MAC Address Aging Time

6.16.1 Overview

Switch ports can learn addresses automatically. The switch adds the source addresses (source MAC address, switch port number) of received frames to the address table. Aging time starts from when a dynamic MAC address is added to the MAC address table. If no port receives a frame with the MAC address within one to two times the aging time, then the switch deletes the entry of the MAC address from the dynamic forwarding address table. Static MAC address table does not involve the concept of aging time.

6.16.2 Web Configuration

Configure MAC address aging time, as shown in Figure 102.



MAC Aging Time 300 (15-3600 sec)

Figure 102 MAC Address Aging Time

MAC Aging Time

Range: 15~3600 seconds

Default: 300 seconds

Description: You can adjust the aging time as required.

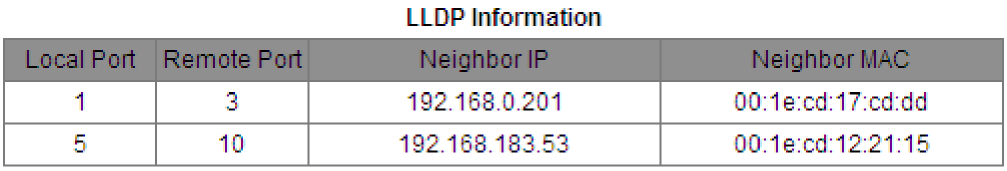
6.17 LLDP

6.17.1 Overview

The Link Layer Discovery Protocol (LLDP) provides a standard link layer discovery mechanism. It encapsulates device information such as the capability, management address, device identifier, and interface identifier in a Link Layer Discovery Protocol Data Unit (LLDPDU), and advertises the LLDPDU to its directly connected neighbors. Upon receiving the LLDPDU, the neighbors save this information to MIB for query and link status check by the NMS.

6.17.2 Web Configuration

View LLDP connection information, as shown in Figure 103.



LLDP Information

Local Port	Remote Port	Neighbor IP	Neighbor MAC
1	3	192.168.0.201	00:1e:cd:17:cd:dd
5	10	192.168.183.53	00:1e:cd:12:21:15

Figure 103 LLDP Information

In LLDP information, you can view the information about neighboring devices, including port number of the neighboring device connected to the local switch, IP address and MAC address of the neighboring device.

Caution:

To display LLDP information, LLDP must be enabled on the two connected devices. LLDP is a link-layer detection protocol enabled by default.

6.18 SNTP

6.18.1 Overview

The Simple Network Time Protocol (SNTP) synchronizes time between server and client by means of requests and responses. As a client, the switch synchronizes time from the server according to packets of the server. In this case, a maximum of four SNTP servers can be configured, but only one can be active at a time. The switch can also serve as the SNTP server to provide time synchronization for clients.

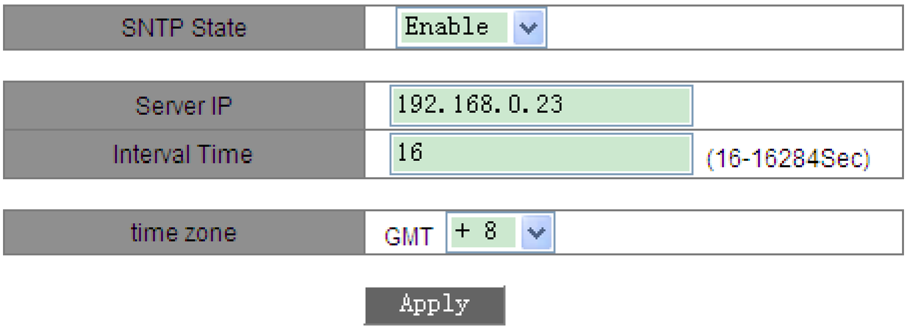
The SNTP client sends a request to each server one by one through unicast. The server that responds first is in an active state. The other servers are in an inactive state.

Caution:

To synchronize time by SNTP, there must be an active SNTP server.

6.18.2 Web Configuration

1. Enable SNTP. Select the server and set related parameters, as shown in Figure 104.



SNTP State: Enable

Server IP: 192.168.0.23

Interval Time: 16 (16-16284Sec)

time zone: GMT + 8

Figure 104 SNTP Configuration

SNTP State

Options: Enable/Disable

Default: Disable

Function: Enable/Disable SNTP.

Server IP

Format: A.B.C.D

Function: Set the IP address of the SNTP server. The client synchronizes time from the server based on the packets sent by the server.

Interval Time

Options: 16~16284s

Function: Configure the interval for sending synchronization requests from the SNTP client to the server.

Time Zone

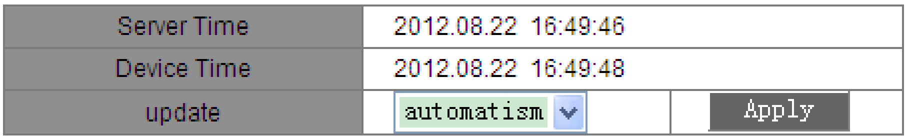
Options: 0, +1, +2, +3, +4, +5, +6, +7, +8, +9, +10, +11, +12, +13, -1, -2, -3, -4,

-5, -6, -7, -8, -9, -10, -11, -12

Default: 0

Function: Select the local time zone.

2. Select the synchronization mode between the client and the server, as shown in Figure 105.



Server Time	2012.08.22 16:49:46	
Device Time	2012.08.22 16:49:48	
update	automatism	Apply

Figure 105 Time Synchronization Mode

Server Time

Function: Display the latest time obtained from the server.

Device Time

Function: Display the time of the device.

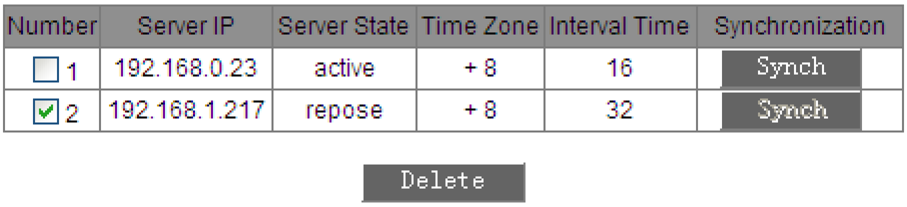
Update

Options: automatism/manual

Default: automatism

Function: Select the time synchronization mode between the device and the server.

3. View SNTP configuration. You can select an SNTP server and click <Delete> to delete it, as shown in Figure 106.



Number	Server IP	Server State	Time Zone	Interval Time	Synchronization
□ 1	192.168.0.23	active	+ 8	16	Synch
☑ 2	192.168.1.217	repose	+ 8	32	Synch

Figure 106 SNTP Configuration

Server State

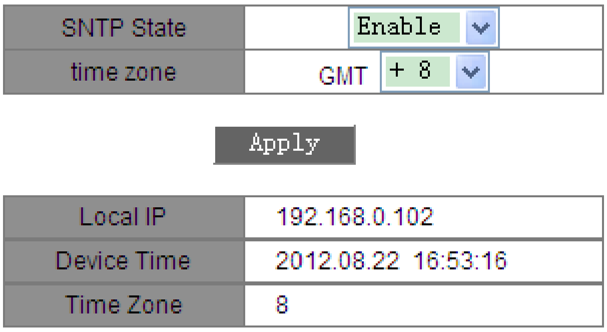
Options: active/repose

Description: The active server provides SNTP time for the client. Only one server can be in active state at a time.

Synchronization

To synchronize time manually, click <Synch>.

4. Configure the switch as the SNTP server, as shown in Figure 107.



SNTP State	Enable
time zone	GMT + 8

Local IP	192.168.0.102
Device Time	2012.08.22 16:53:16
Time Zone	8

Figure 107 Configuring the Switch as the SNTP Server

SNTP State

Options: Enable/Disable

Default: Disable

Function: Enable or disable the SNTP server function.

Time zone

Options: 0, +1, +2, +3, +4, +5, +6, +7, +8, +9, +10, +11, +12, +13, -1, -2, -3, -4, -5, -6, -7, -8, -9, -10, -11, and -12

Default: +8

Function: Select the server time zone.

6.19 MSTP

6.19.1 Overview

Although RSTP achieves rapid convergence, it also has the following defect similar to STP: all bridges in the LAN share one spanning tree and packets of all VLANs are forwarded along the spanning tree. As shown in Figure 108 below, certain configurations may block the link between switch A and switch C. Because switch B and switch D are not in VLAN 1, they cannot forward the packets of VLAN 1. As a result, the VLAN 1 port of switch A cannot communicate with that of switch C.

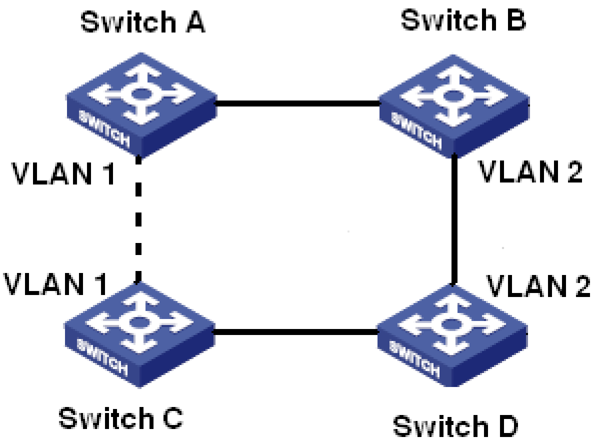


Figure 108 RSTP Defect

Multiple Spanning Tree Protocol (MSTP) resolves this issue. It achieves both rapid convergence and separate forwarding paths for the traffic of different VLANs, providing a better load sharing mechanism for redundant links.

MSTP maps one or multiple VLANs into one instance. Switches with the same configuration form a region. Each region contains multiple mutually independent spanning trees. The region serves as a switch node. It participates in the calculation with other regions based on the spanning tree algorithm, calculating an overall spanning tree. Based on this algorithm, the network in Figure 108 forms the topology shown in Figure 109. Both switch A and switch C are in Region1. No link is blocked because the region contains no loops. This is the same with Region2. Region1 and Region2 are similar to switch nodes. These two "switches" form a loop. Therefore, a link should be blocked.

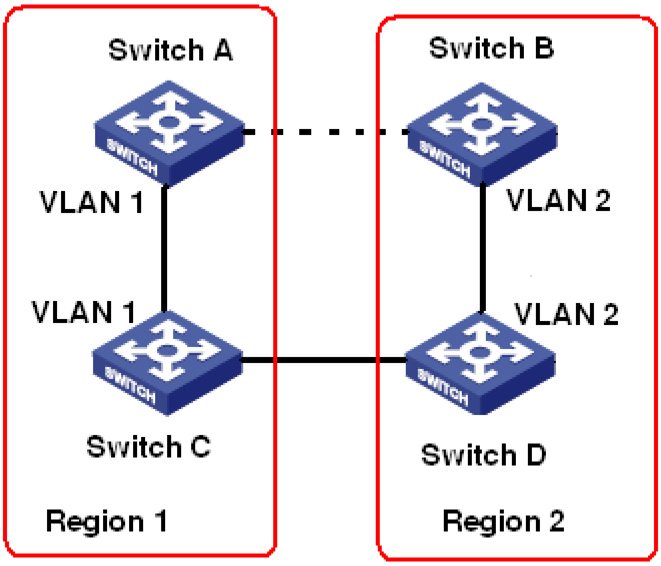


Figure 109 MSTP Topology

6.19.2 Concepts

Learn MSTP concepts based on Figure 110 to Figure 113.

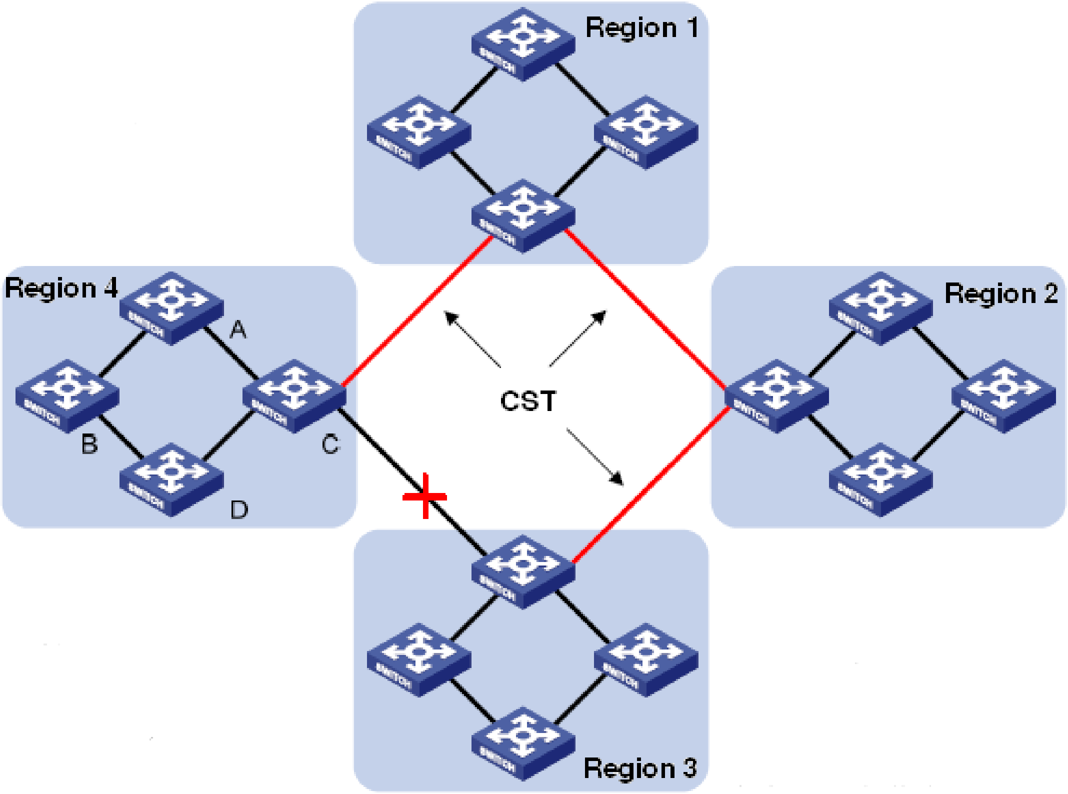


Figure 110 MSTP Concepts

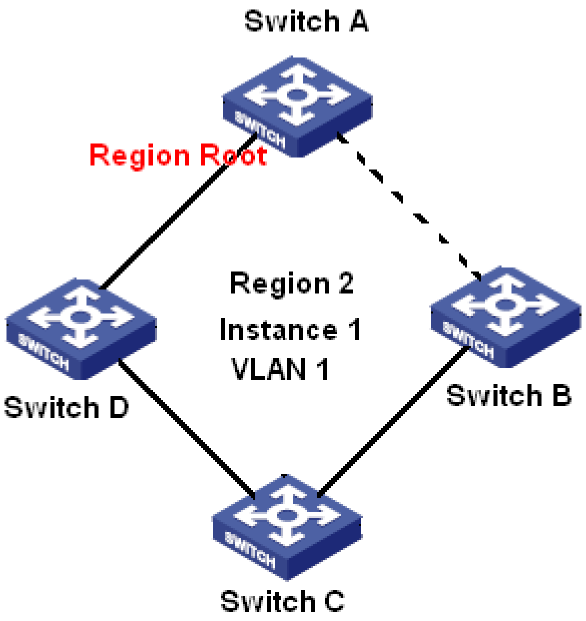


Figure 111 VLAN 1 Mapped to Instance 1

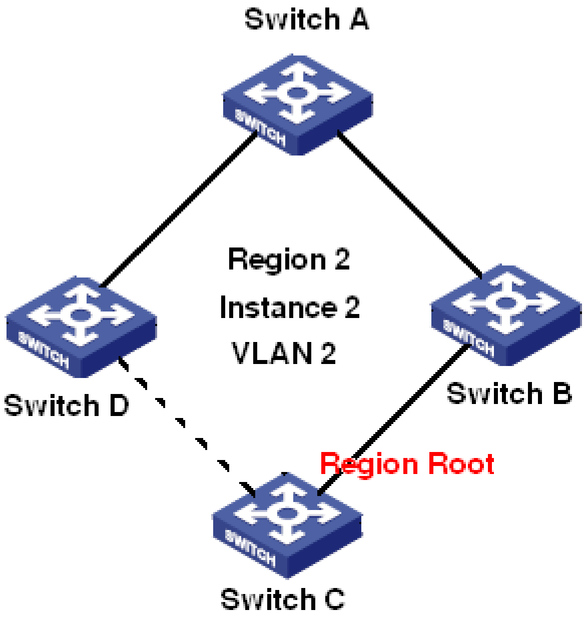


Figure 112 VLAN 2 Mapped to Instance 2

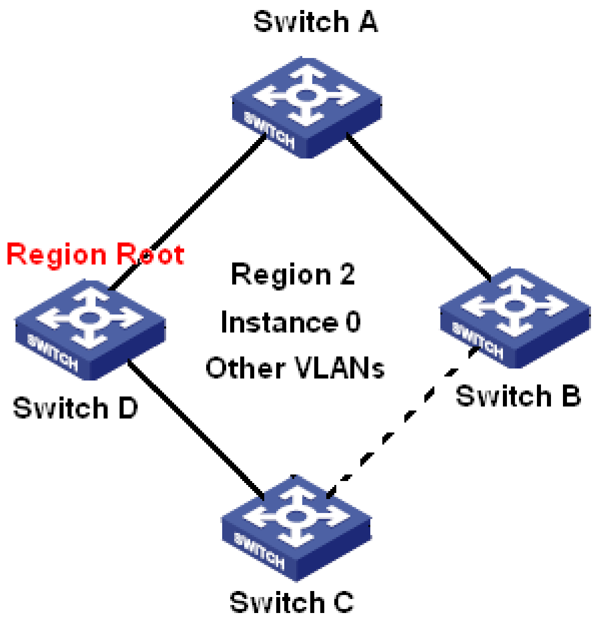


Figure 113 Other VLANs Mapped to Instance 0

- Instance: a collection of multiple VLANs. One VLAN (as shown in Figure 111 and Figure 112) or multiple VLANs with the same topology (as shown in Figure 113) can be mapped to one instance; that is, one VLAN can form a spanning tree and multiple VLANs can share one spanning tree. Different instances are mapped to different spanning trees. Instance 0 is the spanning tree for the devices of all regions, while the other instances are the spanning trees for the devices of a specific region.
- Multiple Spanning Tree Regions (MST regions): Switches with the same MSTP region name, revision level, and VLAN-to-instance mapping are in the same MST region. As shown in Figure 110, Region1, Region2, Region3, and Region4 are four different MST regions.
- VLAN mapping table: consists of the mapping between VLANs and spanning trees. In Figure 110, VLAN mapping table of region 2 is the mapping between VLAN 1 and instance 1, as shown in Figure 111; VLAN 2 is mapped to instance 2, as shown in Figure 112. The other VLANs are mapped to instance 0, as shown in Figure 113.
- Common and Internal Spanning Tree (CIST): indicates instance 0, that is, the spanning tree covering all the devices on a switching network. As shown

in Figure 110, the CIST comprises IST and CST.

- Internal Spanning Tree (IST): indicates the CIST segment in the MST region, that is, instance 0 of each region, as shown in Figure 113.
- Common Spanning Tree (CST): indicates the spanning tree connecting all MST regions in a switching network. If each MST region is a device node, the CST is the spanning tree calculated based on STP/RSTP by these device nodes. As shown in Figure 110, the red lines indicate the spanning tree.
- MSTI (Multiple Spanning Tree Instance): one MST region can form multiple spanning trees and they are independent of each other. Each spanning tree is a MSTI, as shown in Figure 111 and Figure 112. IST is also a special MSTI.
- Common root: indicates the root bridge of the CIST. The switch with the smallest root bridge ID in a network is the common root.
- Regional root: In an MST region, spanning trees have different topologies, and their regional roots can also be different. As shown in Figure 111, Figure 112, and Figure 113, the three instances have different regional roots.

  The root bridge of the MSTI is calculated based on STP/RSTP in the current MST region.

  The root bridge of the IST is the device that is connected to another MST region and selected based on the priority information received.
- Boundary port: indicates the port that connects an MST region to another MST region, STP running region, or RSTP running region.
- Port state: A port can be in either of the following states based on whether it is learning MAC addresses and forwarding traffic.
- Forwarding state: indicates that a port learns MAC addresses and forwards traffic.

  Learning state: indicates that a port learns MAC addresses but does not forward traffic.

Discarding state: indicates that a port neither learns MAC addresses nor forwards traffic.

- Root port: indicates the best port from a non-root bridge to the root bridge, that is, the port with the smallest cost to the root bridge. A non-root bridge communicates with the root bridge through the root port. A non-root bridge has only one root port. The root bridge has no root port.

  The root port can be in forwarding, learning, or discarding state.
- Designated port: indicates the port for forwarding BPDU to other devices or LANs. All ports on the root bridge are designated ports.

  The designated port can be in forwarding, learning, or discarding state.
- Master port: indicates the port that connects an MST region to the common root. The port is in the shortest path to the common root. From the CST, the master port is the root port of a region (as a node). The master port is a special boundary port. It is the root port for the CIST and master port for other instances.

  The master port can be in forwarding, learning, or discarding state.
- Alternate port: indicates the backup port of the root port or master port. When the root port or master port fails, the alternate port becomes the new root port or master port.

  The master port can only be in a discarding state.
- Backup port: indicates the backup port of the designated port. When a designated port fails, the backup port becomes the designated port and forwards data without any delay.

  The backup port can only be in a discarding state.

6.19.3 Implementation

MSTP divides a network into multiple MST regions. CST is calculated between regions. Multiple spanning trees are calculated in a region. Each spanning tree is an MSTI. Instance 0 is the IST, and other instances are MSTIs.

1. CIST calculation

- A device sends and receives BPDU packets. Based on the comparison of MSTP configuration messages, the device with the highest priority is selected as the common root of the CIST.
- An IST is calculated in each MST region.
- Each MST region is considered as a single device and CST is calculated between regions.
- CST and IST constitute the CIST of the entire network.

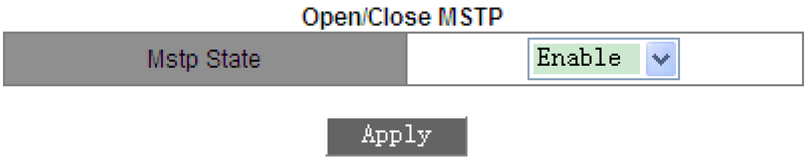
2. MSTI calculation

In an MST region, MSTP generates different spanning trees for VLANs based on the mapping between VLANs and spanning trees. Each spanning tree is calculated independently. The calculation process is similar to that in STP.

In an MST region, VLAN packets are forwarded along corresponding MSTIs. Between MST regions, VLAN packets are forwarded along the CST.

6.19.4 Web Configuration

1. Enable MSTP, as shown in Figure 114.



Open/Close MSTP

Mstp State	Enable

Figure 114 Enabling MSTP

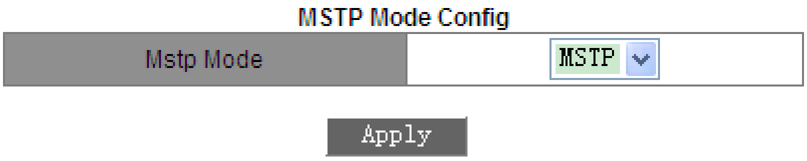
Mstp status

Options: Enable/Disable

Default: Disable

Function: Enable/Disable MSTP.

2. Configure MSTP operation mode, as shown in Figure 115.



MSTP Mode Config

Mstp Mode	MSTP

Figure 115 Configuring MSTP Operation Mode

Mstp Mode

Options: MSTP/STP

Default: MSTP

Function: Configure the mode of switch running spanning tree.

Description: In STP mode, all switch ports can send only STP BPDU packets. In MSTP mode, all switch ports send out MSTP BPDU packets, but if the switch is connected to an STP-enabled device, then the port will automatically change to STP mode.

3. Force port to work in MSTP mode, as shown in Figure 116.

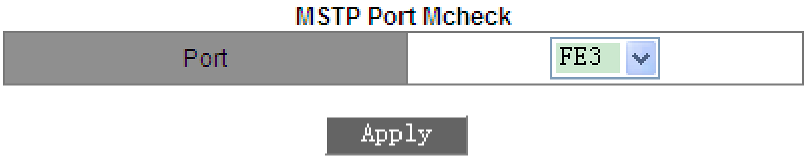


Figure 116 Forcing Port to Work in MSTP Mode

Port

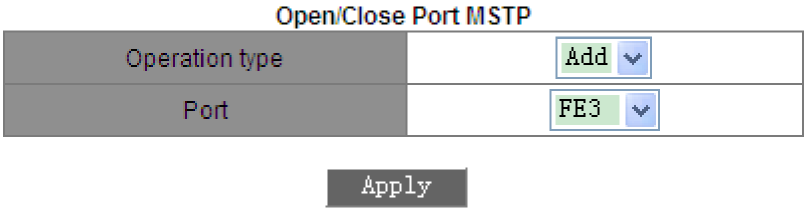
Options: all switch ports

Function: When an MSTP-enabled port is connected to an STP-enabled device, the connected port will automatically change to STP mode. If the STP-enabled device is removed, the port will not automatically go back to MSTP mode. If you want the switch to go back to MSTP mode in such a condition, configure this function for the port. Then if the port receives an STP message again, the port will automatically change to STP mode again.

Caution:

This configuration will take effect only when the switch runs in MSTP mode; otherwise, it is invalid.

4. Configure the MSTP state of port, as shown in Figure 117.



Open/Close Port MSTP

Operation type	Add
Port	FE3

Figure 117 Configuring MSTP on Port

Operation type

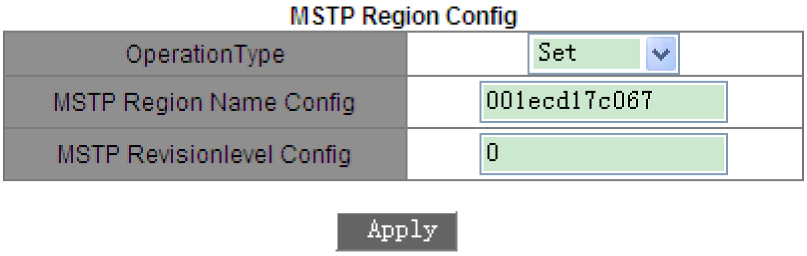
Options: Add/Del

Default: Add

Function: Enable/Disable MSTP on a port.

Description: Add is to enable MSTP on the port; Del is to disable MSTP on the port. If MSTP is enabled globally, MSTP is enabled on all ports by default.

5. Set MST region parameters, as shown in Figure 118.



MSTP Region Config

OperationType	Set
MSTP Region Name Config	001ecd17c067
MSTP Revisionlevel Config	0

Figure 118 Configuring MST Region Parameters

Operation Type

Options: Set/Default

Function: Select the operation type of MST region parameters.

MSTP Region Name Config

Range: 1~32 characters

Default: device MAC address

Function: Configure the name of MST region.

MSTP Revision level Config

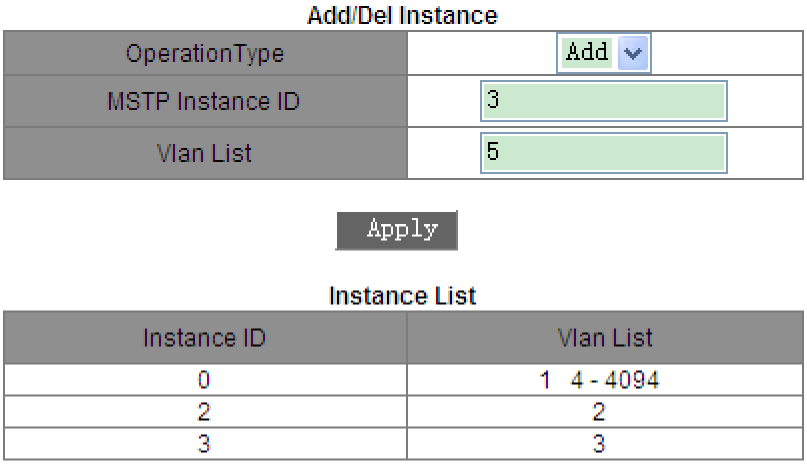
Options: 0~65535

Default: 0

Function: Configure the revision parameter of MSTP region.

Description: Revision parameter, MST region name, and VLAN mapping table codetermines the MST region that the device belongs to. When all configurations are the same, the devices are in same MST region.

6. Configure VLAN mapping table, as shown in Figure 119.



Add/Del Instance

OperationType	Add
MSTP Instance ID	3
Vlan List	5

Instance List

Instance ID	Vlan List
0	1 4 - 4094
2	2
3	3

Figure 119 Configuring VLAN Mapping Table

Operation Type

Options: Add/Del

Function: Configure the operation type of VLAN mapping table.

Portfolio: <MSTP Instance ID, VLAN list>

Range: <0~16, 1~4094>

Default: <0, 1~4094>

Function: Configure the VLAN mapping table in MST region.

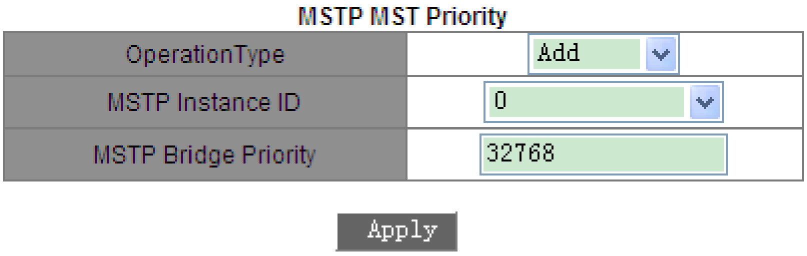
Description: By default, all VLANs map to instance 0. One VLAN maps to only one spanning tree instance. If a VLAN with an existing mapping is mapped to another instance, the previous mapping is cancelled. If the mapping between the designated VLAN and instance is deleted, this VLAN will be mapped to instance 0.

Caution:

<Del> cannot delete the VLAN list of instance 0.

The "Instance List" will show the mapping between VLAN and instance once the setting have been completed.

7. Configure the bridge priority of the switch in designated instance, as shown in Figure 120.



MSTP MST Priority

OperationType	Add
MSTP Instance ID	0
MSTP Bridge Priority	32768

Figure 120 Configuring Bridge Priority in Designated Instance

Operation Type

Options: Add/Default

Function: Select the operation type of the bridge priority for the switch in a designated instance.

MSTP Instance ID

Options: all created instances

MSTP Bridge Priority

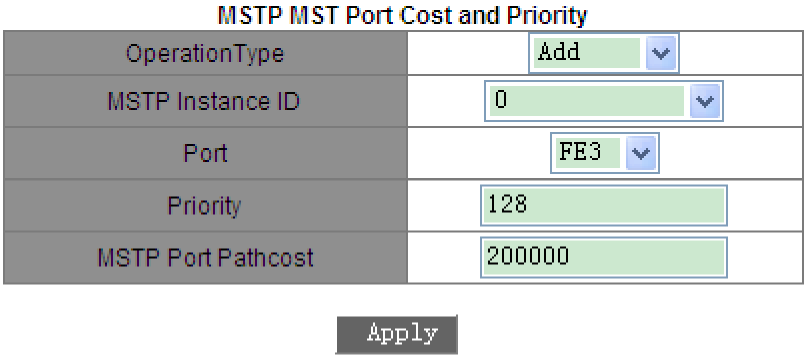
Range: 0~61440 with the step of 4096

Default: 32768

Function: Configure the bridge priority of the switch in designated instance.

Description: The bridge priority determines whether the switch can be elected to regional root of spanning tree instance. The smaller the value is, the higher the priority. By setting a lower priority, a specific device can be designated as root bridge of the spanning tree. The MSTP-enabled device can be configured with different priorities in different spanning tree instance.

8. Configure port priority and path cost in the designated instance, as shown in Figure 121.



MSTP MST Port Cost and Priority

OperationType	Add
MSTP Instance ID	0
Port	FE3
Priority	128
MSTP Port Pathcost	200000

Figure 121 Setting Port Priority and Path Cost in Designated Instance

Operation Type

Options: Add/Default

Function: Select the operation type of the priority and path cost of the port in a designated instance.

MSTP Instance ID

Options: all created instances

Port

Options: all switch ports

Priority

Range: 0~240 with step of 16

Default: 128

Function: Configure the priority of the port in the designated instance.

Description: Port priority determines whether it will be elected to root port. In the same condition, the port with lower priority will be elected to root port. The MSTP-enabled ports can be configured with different priorities and play different port roles in different spanning tree instances.

MSTP Port Path cost

Range: 1~200000000

Default: listed in Table 7 and Table 8.

Table 7 Default Path Cost of Common Port

Port Type	Default Path Cost	Recommended Range
10Mbps	2000000	2000000~20000000
100Mbps	200000	200000~2000000
1Gbps	20000	20000~200000

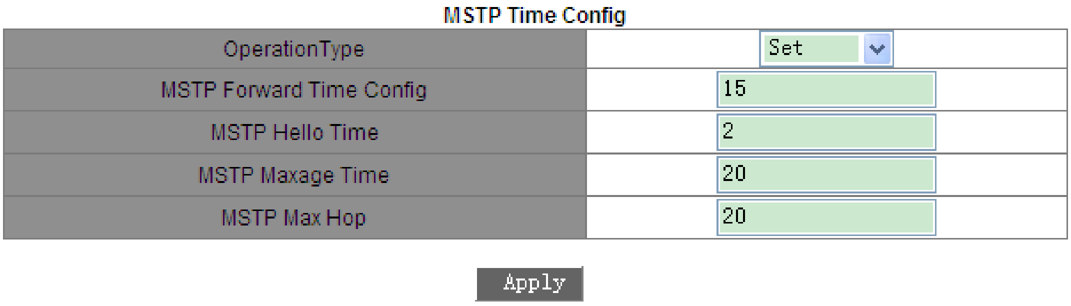
Table 8 Default Path Cost of Aggregation Port

Port Type	Number of Aggregation Ports	Recommended
10Mbps	N	2000000/N
100Mbps	N	200000/N
1Gbps	N	20000/N

Function: Configure the path cost of the port in the designated instance.

Description: Port path cost is used to calculate the optimum path. This parameter depends on bandwidth. The bigger the bandwidth is, the lower the cost. Changing port path costs can change the transmission path between the device and root bridge, thereby changing port role. The MSTP-enabled port can be configured with different path costs in different spanning tree instances.

9. Set MSTP time parameters, as shown in Figure 122.



MSTP Time Config

OperationType	Set
MSTP Forward Time Config	15
MSTP Hello Time	2
MSTP Maxage Time	20
MSTP Max Hop	20

Figure 122 Setting MSTP Time Parameters

Operation Type

Options: Set/Default

Function: Select the operation type of MSTP time parameters.

MSTP Forward Time Config

Options: 4~30s

Default: 15s

Function: Configure the time interval for port state transition (Discarding — Learning or Learning — Forwarding).

MSTP Hello Time

Range: 1~10s

Default: 2s

Function: Configure the time interval for sending BPDUs.

MSTP Max Age Time

Range: 6~40s

Default: 20s

Function: Set the maximum age of BPDU packets.

Caution:

- The values of Forward Delay Time, Hello Time, and Max Age Time should meet the following requirements:

  2 x (Forward Delay Time - 1.0 seconds) >= Max Age Time

  Max Age Time >= 2 x (Hello Time + 1.0 seconds)

- The default settings are recommended.

MSTP Max Hop

Range: 1~40

Default: 20

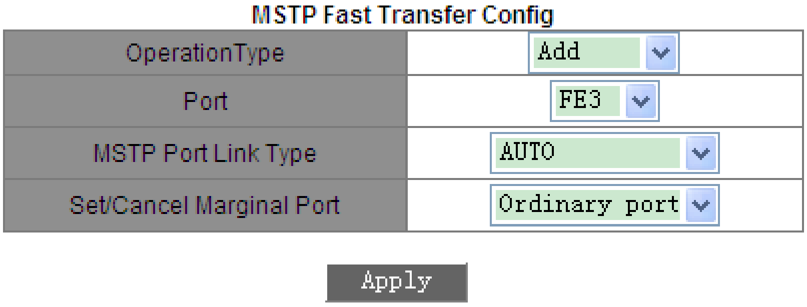
Function: Configure the maximum hops of MST region. The maximum hops of MST region limit the scale of MST region; the maximum number of hops of regional root is the maximum number of hops of MST region.

Description: Starting from the root bridge of spanning tree in MST region, the hop number deducts 1 when the BPDU passes through a device in the region. Device drops the BPDU with the hop number of 0.

Caution:

- Only the maximum hop configuration of the root bridge in MST region is valid. Non-root bridge device adopts the maximum hop configuration of the root bridge.
- The default settings are recommended.

10. Configure MSTP fast transfer, as shown in Figure 123.



MSTP Fast Transfer Config

OperationType	Add
Port	FE3
MSTP Port Link Type	AUTO
Set/Cancel Marginal Port	Ordinary port

Figure 123 Configuring MSTP Fast Transfer

Operation Type

Options: Add/Default

Function: Select the operation type of MSTP fast transfer.

Port

Options: all switch ports

MSTP Port Link Type

Options: AUTO/Force True/Force False

Default: AUTO

Function: Set the link type of the port. If the port is connected to a point-to-point link, then fast state transfer is available on the port.

Description: **AUTO** means the switch will automatically detect link type according to port duplex state. When the port works in full duplex mode, MSTP protocol will automatically assume that the link connected to the port is a point-to-point link. When the port works in half-duplex mode, MSTP protocol will automatically assume that the link connected to the port is a shared link. **Force True** means the link connected to the local port is a point-to-point link.

Force False means the link connected to the local port is a shared link.

Set/Cancel Marginal Port

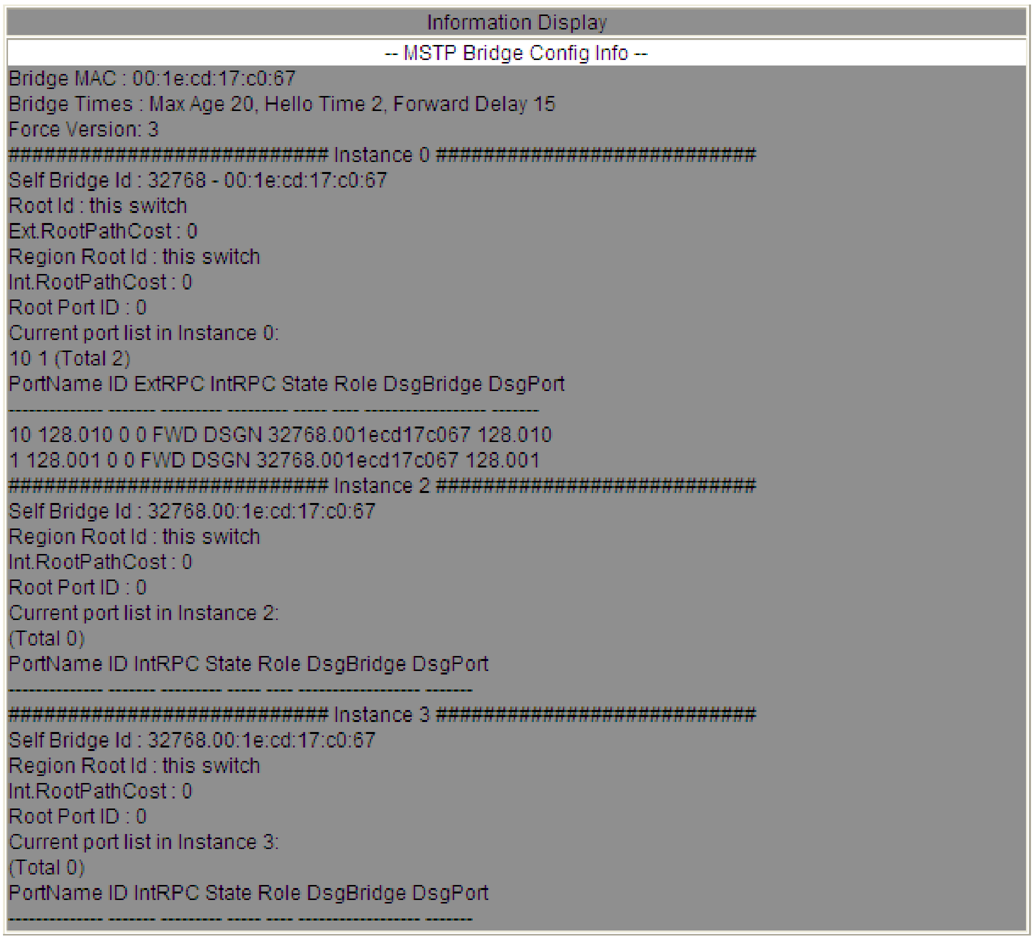
Options: Marginal port/Ordinary port

Default: Ordinary port

Function: Configure the port as marginal or ordinary port.

Description: When the port is directly connected to terminals, but not connected to other devices or shared network segments, this port is a marginal port. A marginal port can transfer from blocking to forwarding without delay. Once the marginal port receives a BPDU, the port will change back to ordinary port.

11. View MSTP configuration, as shown in Figure 124.



Information Display

-- MSTP Bridge Config Info --

```
Bridge MAC : 00:1e:cd:17:c0:67
Bridge Times : Max Age 20, Hello Time 2, Forward Delay 15
Force Version: 3
############################## Instance 0 ##############################
Self Bridge Id : 32768 - 00:1e:cd:17:c0:67
Root Id : this switch
Ext.RootPathCost : 0
Region Root Id : this switch
Int.RootPathCost : 0
Root Port ID : 0
Current port list in Instance 0:
10 1 (Total 2)
PortName ID ExtRPC IntRPC State Role DsgBridge DsgPort
-------------- ------- --------- --------- ----- ---- ------------------ -------
10 128.010 0 0 FWD DSGN 32768.001ecd17c067 128.010
1 128.001 0 0 FWD DSGN 32768.001ecd17c067 128.001
############################## Instance 2 ##############################
Self Bridge Id : 32768.00:1e:cd:17:c0:67
Region Root Id : this switch
Int.RootPathCost : 0
Root Port ID : 0
Current port list in Instance 2:
(Total 0)
PortName ID IntRPC State Role DsgBridge DsgPort
-------------- ------- --------- ----- ---- ------------------ -------
############################## Instance 3 ##############################
Self Bridge Id : 32768.00:1e:cd:17:c0:67
Region Root Id : this switch
Int.RootPathCost : 0
Root Port ID : 0
Current port list in Instance 3:
(Total 0)
PortName ID IntRPC State Role DsgBridge DsgPort
-------------- ------- --------- ----- ---- ------------------ -------
```

Figure 124 MSTP Configuration

6.19.5 Typical Configuration Example

As shown in Figure 125, Switch A, B, C, and D belong to the same MST region. The VLANs marked in red indicate the VLAN packets can be transmitted through the links. After configurations are completed, VLAN packets can be forwarded along different spanning tree instances. VLAN 10 packets are forwarded along instance 1 and the root bridge of instance 1 is Switch A; VLAN 30 packets are forwarded along instance 3 and the root bridge of instance 3 is Switch B. VLAN 40 packets are forwarded along instance 4 and the root bridge of instance 4 is Switch C. VLAN 20 packets are forwarded along instance 0 and the root bridge of instance 0 is Switch B.

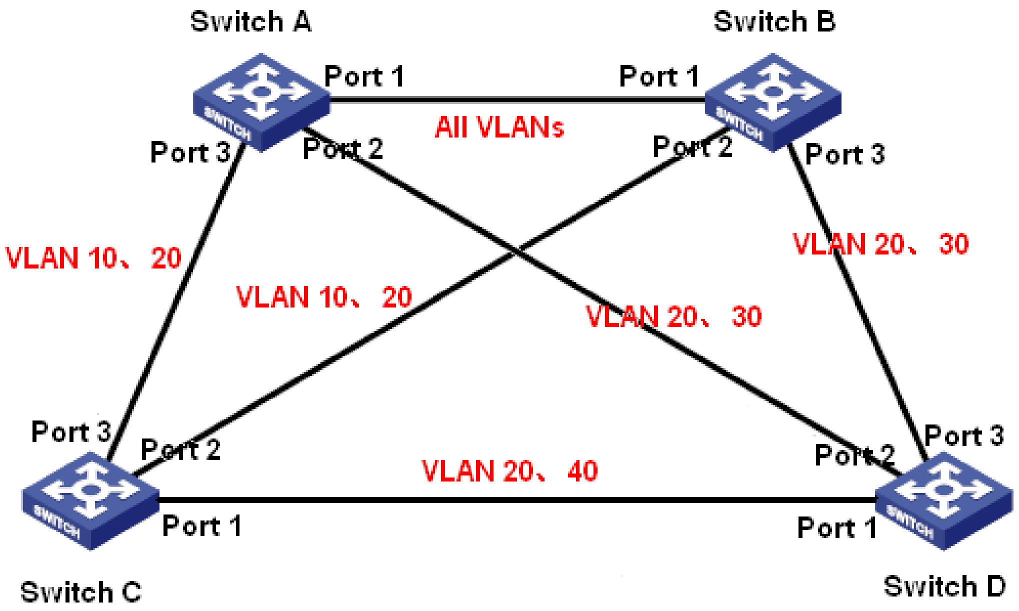


Figure 125 MSTP Typical Configuration Example

Configuration on Switch A:

1. Create VLAN 10, 20, and 30 on Switch A. Configure the ports to allow the packets of respective VLANs to pass through.
2. Enable global MSTP protocol, as shown in Figure 114.
3. Set the name of MST region to Region and the revision parameter to 0, as shown in Figure 118.
4. Create instance 1, 3, and 4 and map VLAN 10, 30, and 40 to instance 1, 3,

and 4 respectively, as shown in Figure 119.

5. Set the switch bridge priority in instance 1 to 4096, and keep default priority in other instances, as shown in Figure 120.

Configuration on Switch B:

6. Create VLAN 10, 20, and 30 on Switch B. Configure the ports to allow the packets of respective VLANs to pass through.
7. Enable global MSTP protocol, as shown in Figure 114.
8. Set the name of MST region to Region and the revision parameter to 0, as shown in Figure 118.
9. Create instance 1, 3, and 4 and map VLAN 10, 30, and 40 to instance 1, 3, and 4 respectively, as shown in Figure 119.
10. Set switch bridge priority in instance 3 and instance 0 to 4096, and keep default priority in other instances, as shown in Figure 120.

Configuration on Switch C:

11. Create VLAN 10, 20 and 40 on Switch C. Configure the ports to allow the packets of respective VLANs to pass through.
12. Enable global MSTP protocol, as shown in Figure 114.
13. Set the name of MST region to Region and the revision parameter to 0, as shown in Figure 118.
14. Create instance 1, 3, and 4 and map VLAN 10, 30, and 40 to instance 1, 3, and 4 respectively, as shown in Figure 119.
15. Set the switch bridge priority in instance 4 to 4096, and keep default priority in other instances, as shown in Figure 120.

Configuration on Switch D:

16. Create VLAN 20, 30 and 40 on Switch D. Configure the ports to allow the packets of respective VLANs to pass through.
17. Enable global MSTP protocol, as shown in Figure 114.
18. Set the name of MST region to Region and the revision parameter to 0, as shown in Figure 118.

19.Create instance 1, 3, and 4 and map VLAN 10, 30, and 40 to instance 1, 3, and 4 respectively, as shown in Figure 119.

When MSTP calculation is completed, the MSTI of each VLAN is as follows:

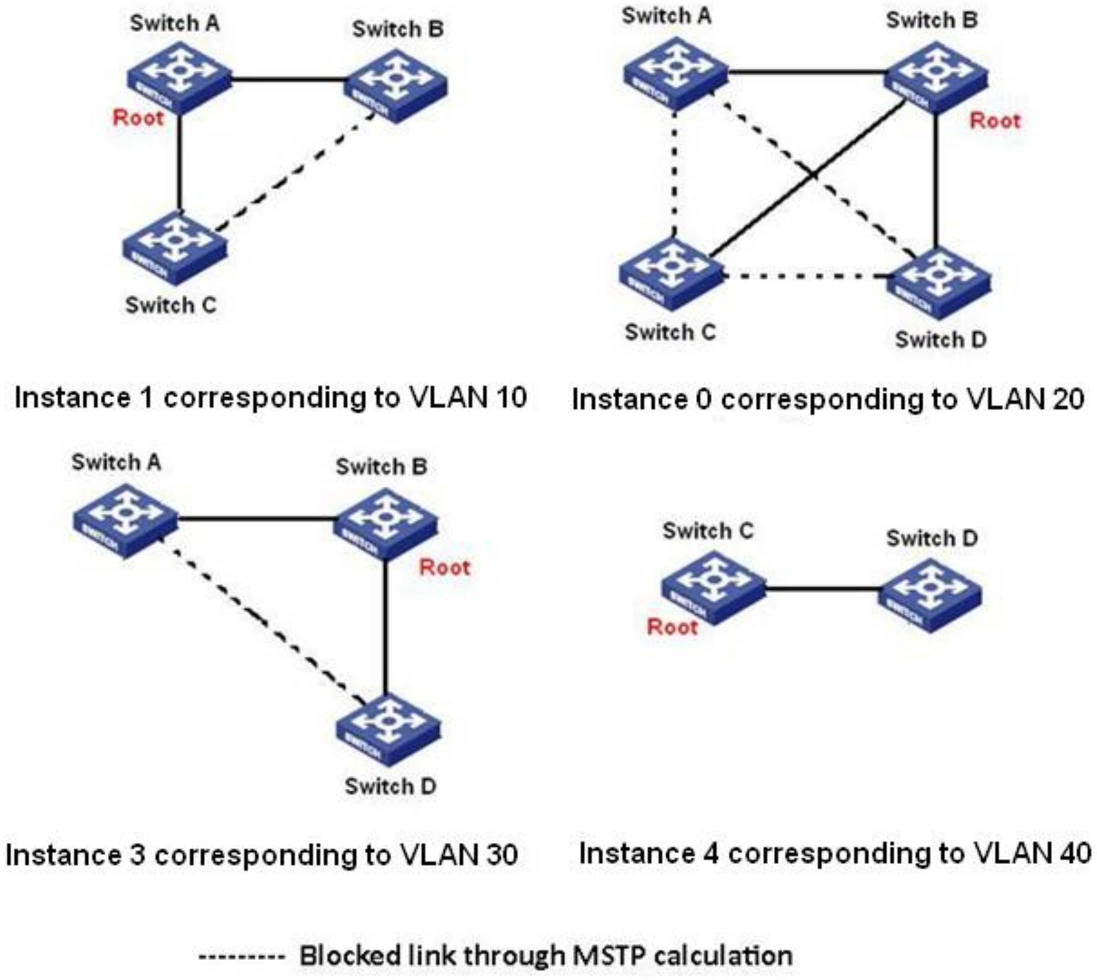

Switch A
Switch B
Root
Switch C
Instance 1 corresponding to VLAN 10
Switch A
Switch B
Root
Switch C
Switch D
Instance 0 corresponding to VLAN 20
Switch A
Switch B
Root
Switch D
Instance 3 corresponding to VLAN 30
Switch C
Switch D
Root
Instance 4 corresponding to VLAN 40
--------- Blocked link through MSTP calculation

Figure 126 Spanning Tree Instance of each VLAN

6.20 Alarm

6.20.1 Overview

This series switches support the following types of alarms:

- IP/MAC conflict alarm: If the function is enabled, then an alarm will be generated for an IP/MAC conflict.
- Port alarm: If this function is enabled, then an alarm is triggered when the port is in link down state.

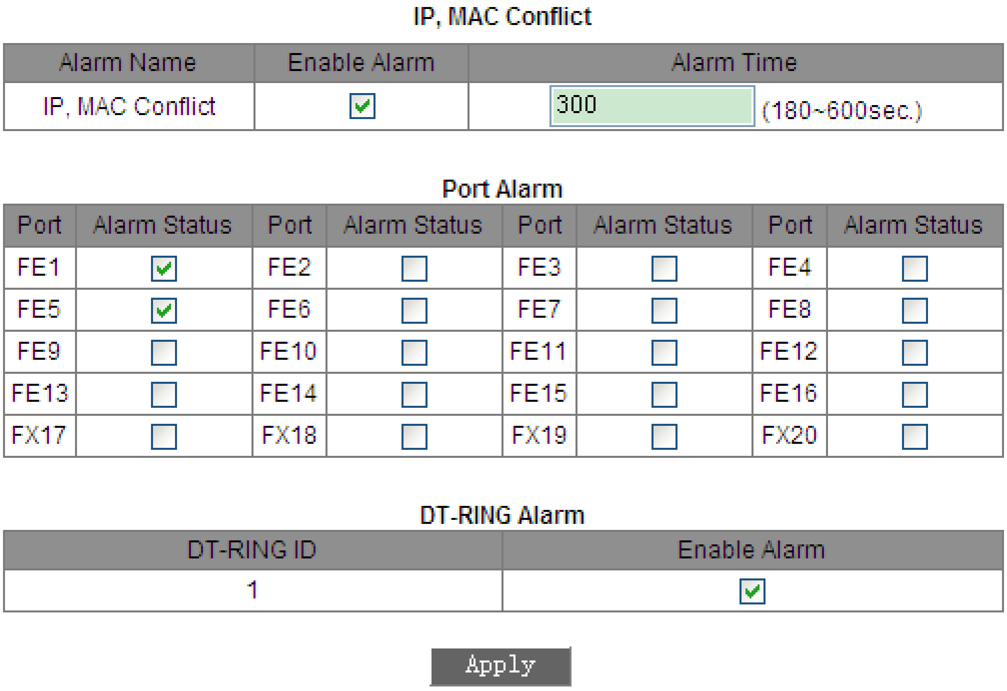
- ➢ Ring alarm: If this function is enabled, then an alarm is triggered when the ring is open.
- ➢ Power alarm: If the function is enabled, then an alarm will be generated for a single power input.

Caution:

Only the master station of a DT ring supports the ring alarm function.

6.20.2 Web Configuration

1. Set alarm parameters, as shown in Figure 127,Figure 128 and Figure 129.



IP, MAC Conflict

Alarm Name	Enable Alarm	Alarm Time
IP, MAC Conflict	☑	300 (180~600sec.)

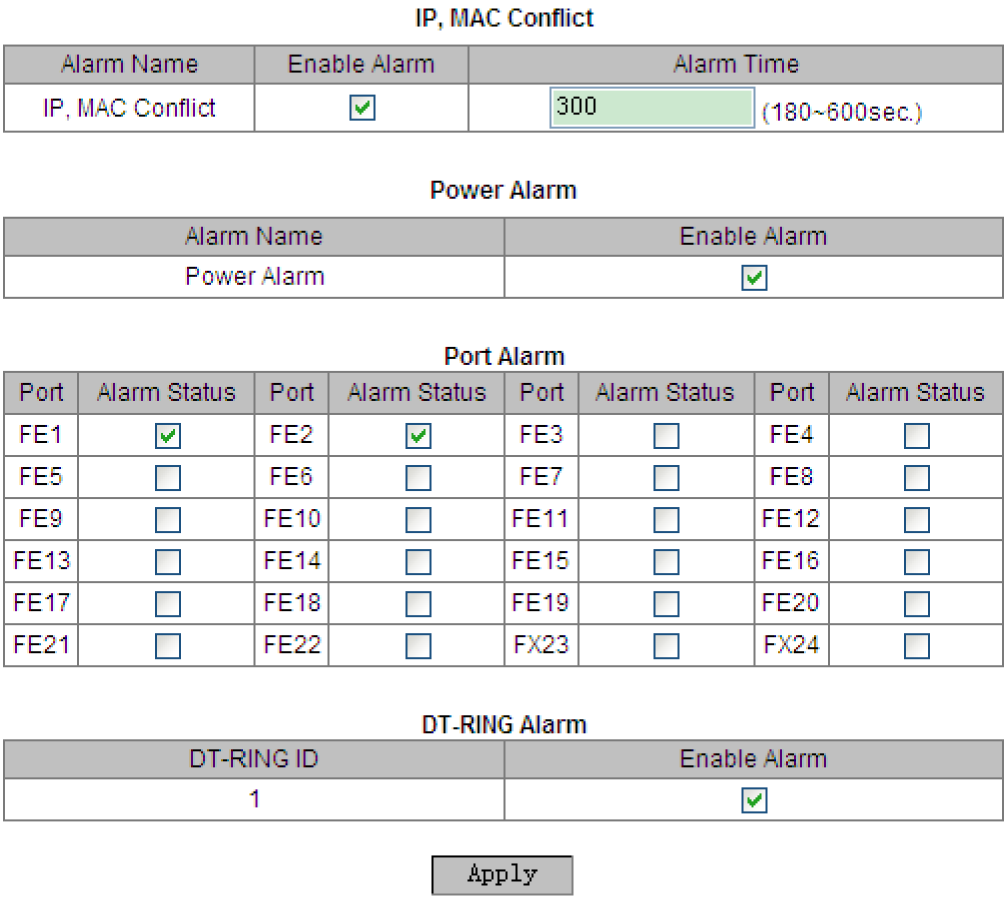
Port Alarm

Port	Alarm Status	Port	Alarm Status	Port	Alarm Status	Port	Alarm Status
FE1	☑	FE2	□	FE3	□	FE4	□
FE5	☑	FE6	□	FE7	□	FE8	□
FE9	□	FE10	□	FE11	□	FE12	□
FE13	□	FE14	□	FE15	□	FE16	□
FX17	□	FX18	□	FX19	□	FX20	□

DT-RING Alarm

DT-RING ID	Enable Alarm
1	☑

Figure 127 Alarm Setting (SICOM3016/8000)



IP, MAC Conflict

Alarm Name	Enable Alarm	Alarm Time
IP, MAC Conflict	☑	300 (180~600sec.)

Power Alarm

Alarm Name	Enable Alarm
Power Alarm	☑

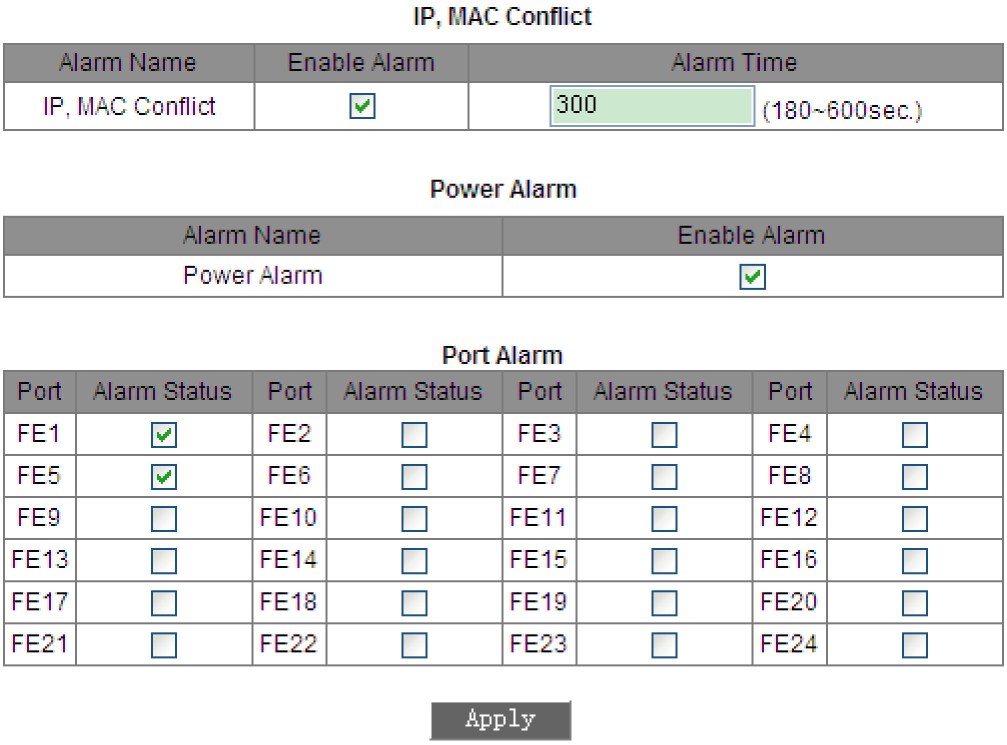
Port Alarm

Port	Alarm Status	Port	Alarm Status	Port	Alarm Status	Port	Alarm Status
FE1	☑	FE2	☑	FE3	☐	FE4	☐
FE5	☐	FE6	☐	FE7	☐	FE8	☐
FE9	☐	FE10	☐	FE11	☐	FE12	☐
FE13	☐	FE14	☐	FE15	☐	FE16	☐
FE17	☐	FE18	☐	FE19	☐	FE20	☐
FE21	☐	FE22	☐	FX23	☐	FX24	☐

DT-RING Alarm

DT-RING ID	Enable Alarm
1	☑

Figure 128 Alarm Setting (SICOM3024)



IP, MAC Conflict

Alarm Name	Enable Alarm	Alarm Time
IP, MAC Conflict	☑	300 (180~600sec.)

Power Alarm

Alarm Name	Enable Alarm
Power Alarm	☑

Port Alarm

Port	Alarm Status	Port	Alarm Status	Port	Alarm Status	Port	Alarm Status
FE1	☑	FE2	☐	FE3	☐	FE4	☐
FE5	☑	FE6	☐	FE7	☐	FE8	☐
FE9	☐	FE10	☐	FE11	☐	FE12	☐
FE13	☐	FE14	☐	FE15	☐	FE16	☐
FE17	☐	FE18	☐	FE19	☐	FE20	☐
FE21	☐	FE22	☐	FE23	☐	FE24	☐

Figure 129 Alarm Setting (SICOM2024M)

IP, MAC Conflict

Options: Select/Deselect

Default: Select

Function: Enable or disable IP/MAC conflict alarm.

Alarm Time

Range: 180~600s

Default: 300s

Function: Configure the interval for detecting IP/MAC conflicts.

Port Alarm

Options: Select/Deselect

Default: Deselect

Function: Enable or disable port alarm.

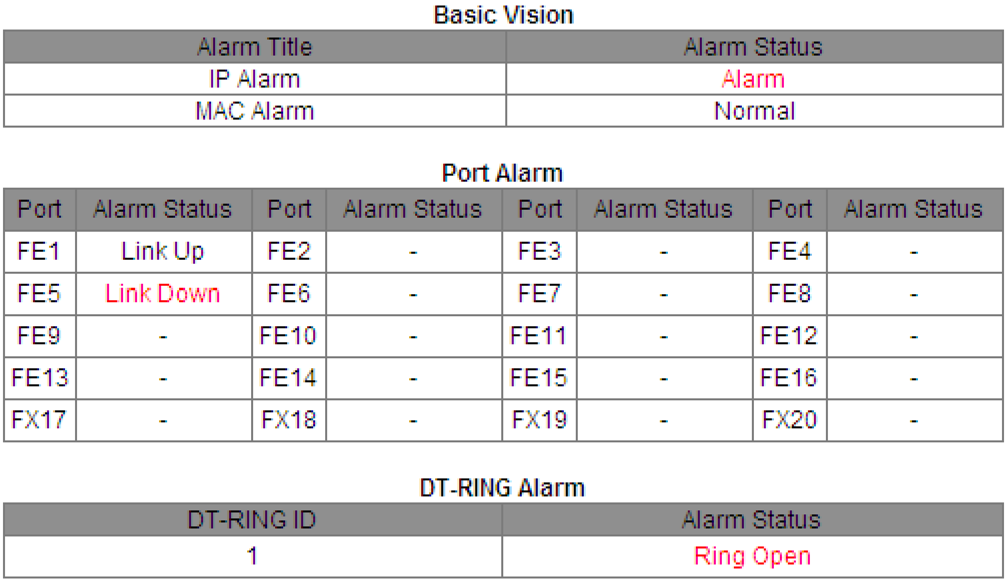
DT-RING Alarm

Options: Select/Deselect

Default: Deselect

Function: Enable or disable the DT-Ring alarm function.

2. After the alarm function is enabled, the alarm information is as follows:



Basic Vision

Alarm Title	Alarm Status
IP Alarm	Alarm
MAC Alarm	Normal

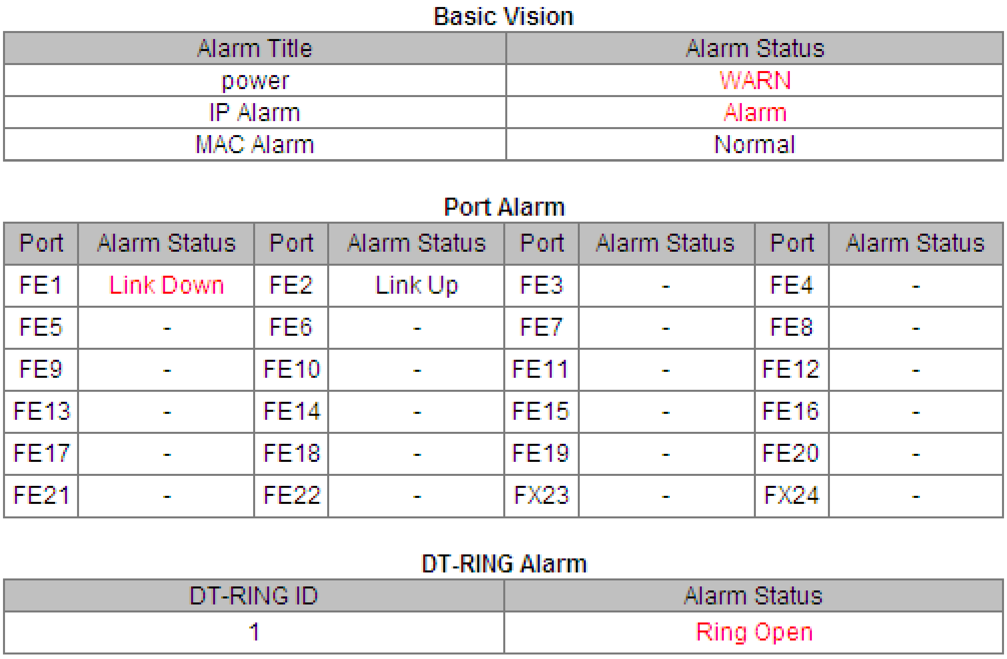
Port Alarm

Port	Alarm Status	Port	Alarm Status	Port	Alarm Status	Port	Alarm Status
FE1	Link Up	FE2	-	FE3	-	FE4	-
FE5	Link Down	FE6	-	FE7	-	FE8	-
FE9	-	FE10	-	FE11	-	FE12	-
FE13	-	FE14	-	FE15	-	FE16	-
FX17	-	FX18	-	FX19	-	FX20	-

DT-RING Alarm

DT-RING ID	Alarm Status
1	Ring Open

Figure 130 Alarm Information (SICOM3016/8000)



Basic Vision

Alarm Title	Alarm Status
power	WARN
IP Alarm	Alarm
MAC Alarm	Normal

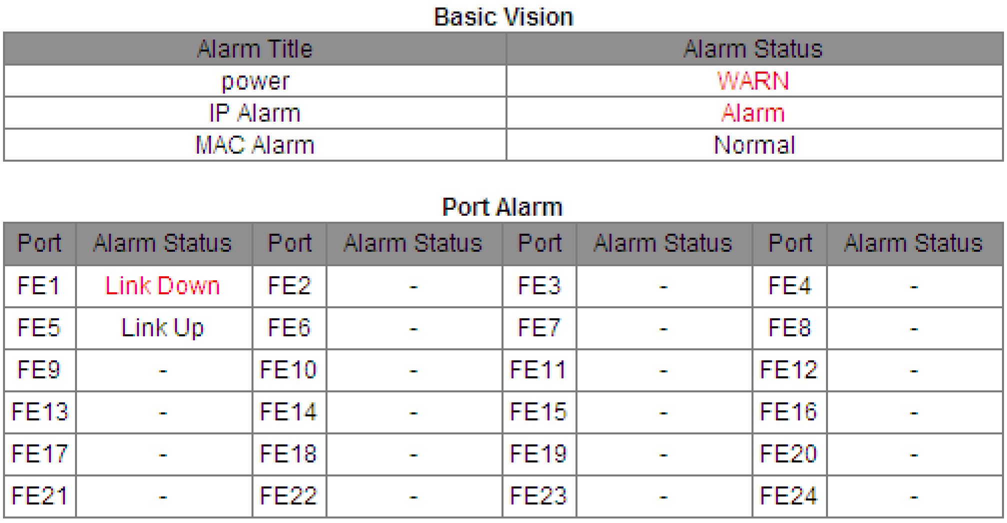
Port Alarm

Port	Alarm Status	Port	Alarm Status	Port	Alarm Status	Port	Alarm Status
FE1	Link Down	FE2	Link Up	FE3	-	FE4	-
FE5	-	FE6	-	FE7	-	FE8	-
FE9	-	FE10	-	FE11	-	FE12	-
FE13	-	FE14	-	FE15	-	FE16	-
FE17	-	FE18	-	FE19	-	FE20	-
FE21	-	FE22	-	FX23	-	FX24	-

DT-RING Alarm

DT-RING ID	Alarm Status
1	Ring Open

Figure 131 Alarm Information (SICOM3024)



Basic Vision

Alarm Title	Alarm Status
power	WARN
IP Alarm	Alarm
MAC Alarm	Normal

Port Alarm

Port	Alarm Status	Port	Alarm Status	Port	Alarm Status	Port	Alarm Status
FE1	Link Down	FE2	-	FE3	-	FE4	-
FE5	Link Up	FE6	-	FE7	-	FE8	-
FE9	-	FE10	-	FE11	-	FE12	-
FE13	-	FE14	-	FE15	-	FE16	-
FE17	-	FE18	-	FE19	-	FE20	-
FE21	-	FE22	-	FE23	-	FE24	-

Figure 132 Alarm Information (SICOM2024M)

Power Alarm

Options: Normal/WARN

Description: After the power alarm is enabled, Normal is displayed for dual power inputs while WARN is displayed for a single power input.

IP/MAC Conflict Alarm

Options: Normal/Alarm

Description: When an IP/MAC conflict occurs, Alarm is displayed; otherwise, Normal is displayed.

Port Alarm

Options: Link Up/Link Down

Description: After port alarm is enabled, Link Up is displayed for a port connected properly. Link Down is displayed for a port disconnected or connected abnormally.

DT-RING Alarm

Options: Ring Open/Ring Close

Description: After ring alarm is enabled, Ring Open is displayed for an open ring while Ring Close is displayed for a closed ring.

6.21 Port Traffic Alarm

6.21.1 Overview

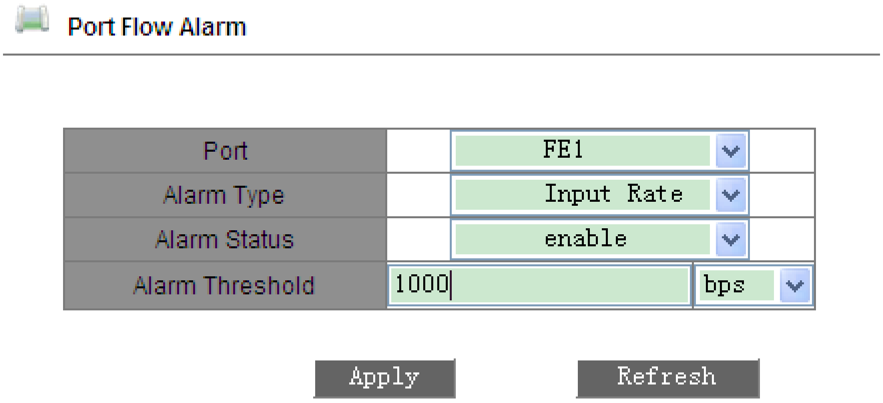
With the port traffic alarm function, the switch generates an alarm if the traffic rate of a port exceeds the specified threshold or a CRC error occurs.

Caution:

- ➢ The traffic alarm function is based on a port. An alarm is generated only if the function is enabled on a port.
- ➢ The traffic alarm function is direction-specific. Incoming and outgoing traffic corresponds to different alarms.
- ➢ If a CRC error occurs, then a CRC error alarm is generated.

6.21.2 Web Configuration

1. Configure port traffic alarm, as shown in Figure 133.



Port Flow Alarm

Port	FE1
Alarm Type	Input Rate
Alarm Status	enable
Alarm Threshold	1000 bps

Figure 133 Configuring Port Traffic Alarm

Port

Options: all switch ports

Function: Select the ports for traffic alarm.

Alarm Type

Options: Input Rate/Output Rate/CRC Error

Function: Configure the port traffic alarm type.

Alarm Status

Options: enable/disable

Default: disable

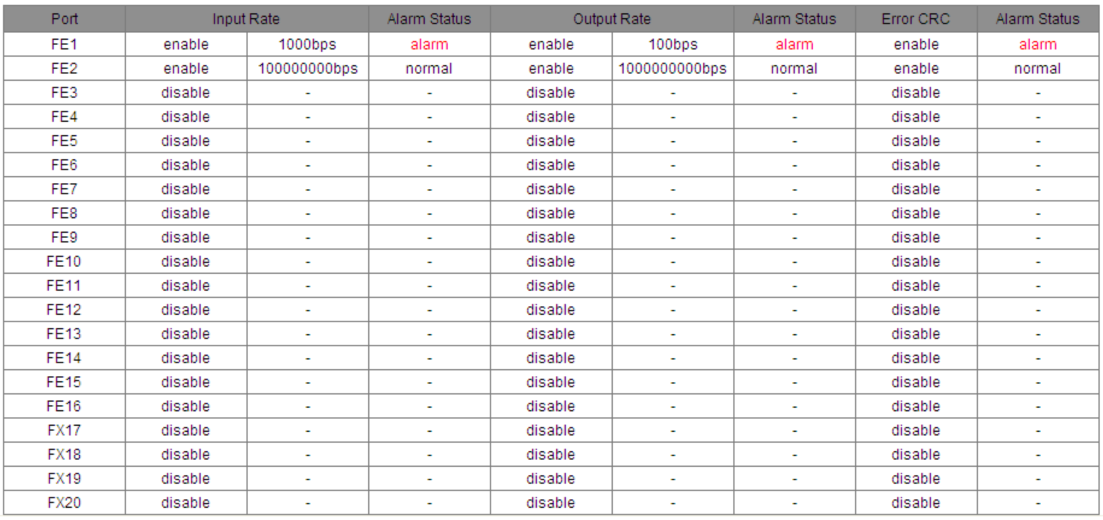
Function: Enable or disable the alarm type.

Alarm Threshold

Range: 1~1000000000bps or 1~1000000kbps

Function: Configure the port traffic alarm threshold.

2. View port traffic alarm information, as shown in Figure 134.



Port	Input Rate		Alarm Status	Output Rate		Alarm Status	Error CRC	Alarm Status
FE1	enable	1000bps	alarm	enable	100bps	alarm	enable	alarm
FE2	enable	100000000bps	normal	enable	1000000000bps	normal	enable	normal
FE3	disable	-	-	disable	-	-	disable	-
FE4	disable	-	-	disable	-	-	disable	-
FE5	disable	-	-	disable	-	-	disable	-
FE6	disable	-	-	disable	-	-	disable	-
FE7	disable	-	-	disable	-	-	disable	-
FE8	disable	-	-	disable	-	-	disable	-
FE9	disable	-	-	disable	-	-	disable	-
FE10	disable	-	-	disable	-	-	disable	-
FE11	disable	-	-	disable	-	-	disable	-
FE12	disable	-	-	disable	-	-	disable	-
FE13	disable	-	-	disable	-	-	disable	-
FE14	disable	-	-	disable	-	-	disable	-
FE15	disable	-	-	disable	-	-	disable	-
FE16	disable	-	-	disable	-	-	disable	-
FX17	disable	-	-	disable	-	-	disable	-
FX18	disable	-	-	disable	-	-	disable	-
FX19	disable	-	-	disable	-	-	disable	-
FX20	disable	-	-	disable	-	-	disable	-

Figure 134 Port Traffic Alarm Information

6.22 GMRP

6.22.1 GARP

The Generic Attribute Registration Protocol (GARP) is used for distributing, registering, and cancelling certain information (VLAN, multicast address) among switches on the same network.

With GARP, the configuration information of a GARP member will distribute the information to the entire switching network. A GARP member instructs the other GARP members to register or cancel its own configuration information by means of join/leave message respectively. The member also registers or cancels the configuration information of other members based on join/leave messages sent by other members.

GARP involves three types of messages: Join, Leave, and LeaveAll.

- When a GARP application entity wants to register its own information on other switches, the entity sends a Join message. Join messages fall into two types: JoinEmpty and JoinIn. A JoinIn message is sent to declare a registered attribute, while a JoinEmpty message is sent to declare an attribute that is not registered yet.
- When a GARP application entity wants to cancel its own information on

other switches, the entity sends a Leave message.

- After a GARP entity starts, it starts the LeaveAll timer. When the timer expires, the entity sends a LeaveAll message.

Note:

An application entity indicates a GARP-enabled port.

GARP timers include Hold timer, Join timer, Leave timer, and LeaveAll timer.

- **Hold Timer**: When receiving a registration message, a GARP entity does not send a Join message immediately, but starts a Hold timer. When the timer expires, the entity sends all the registration messages received within the preceding period in one Join message, reducing packet sending for better network stability.
- **Join Timer**: To ensure that Join messages are received by other application entities, a GARP application entity starts a Join timer after sending a Join message. If receiving no JoinIn message before Join timer expires, the entity sends the Join message again. If receiving a JoinIn message before the timer expires, the entity does not send the second Join message.
- **Leave Timer**: When a GARP application entity wants to cancel the information about an attribute, the entity sends a Leave message. The entity receiving the message starts Leave timer. If receiving no Join message before the timer expires, then entity receiving the message cancels the information about the attribute.
- **LeaveAll Timer**: As a GARP application entity starts, it starts LeaveAll timer. When the timer expires, the entity sends a LeaveAll message, so that the other GARP application entities re-register all the attributes. Then the entity starts LeaveAll timer again for the new cycle.

6.22.2 GMRP

The GARP Multicast Registration Protocol (GMRP) is a multicast registration protocol based on GARP. It is used for maintaining the multicast registration information of switches. All GMRP-enabled switches can receive multicast registration information from other switches, update local multicast registration information dynamically, and distribute local multicast registration information to other switches. This information exchange mechanism ensures the consistency of multicast information maintained by all GMRP-enabled switches on a network.

If a switch or terminal wants to join or leave a multicast group, then the GMRP-enabled port broadcasts the information to all the ports in the same VLAN.

6.22.3 Description

Agent port: indicates the port on which GMRP and the agent function are enabled.

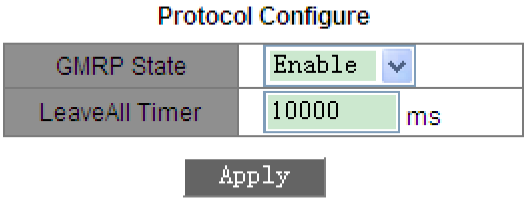
Propagation port: indicates the port on which only GMRP is enabled, but not the agent function.

Dynamically learned GMRP multicast entry and agent entry are forwarded by the propagation port to the propagation ports of the lower-level devices.

All GMRP timers on the same network must keep consistent to prevent mutual interference. The timers should comply with the following rules: Hold timer<Join timer, 2*Join timer<Leave timer, and Leave timer<LeaveAll timer.

6.22.4 Web Configuration

1. Enable the global GMRP protocol, as shown in Figure 135.



Protocol Configure

GMRP State	Enable
LeaveAll Timer	10000 ms

Figure 135 GMRP Global Configuration

GMRP State

Options: Enable/Disable

Default: Disable

Function: Enable or disable the global GMRP function. The function and IGMP Snooping cannot be used at the same time.

LeaveAll Timer

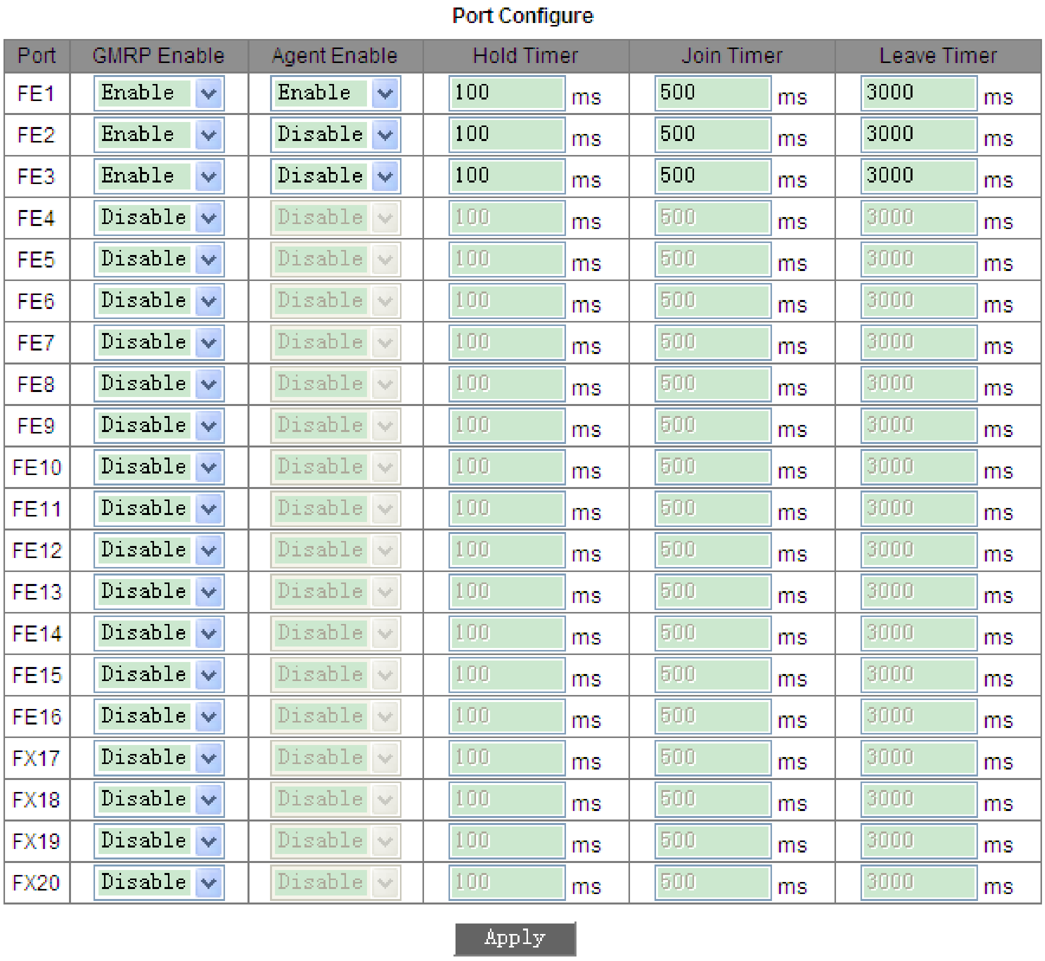
Range: 100ms~327600ms

Default: 10000ms

Function: Set the interval for sending LeaveAll messages. The value must be a multiple of 100.

Description: If the LeaveAll timers of different devices expire at the same time, multiple LeaveAll messages will be sent simultaneously, increasing unnecessary packets. To prevent this problem, the actual timeout of a LeaveAll timer is a random value between the specified value and 1.5 times the specified value.

2. Configure GMPR function on each port, as shown in Figure 136.



Port Configure

Port	GMRP Enable	Agent Enable	Hold Timer	Join Timer	Leave Timer
FE1	Enable	Enable	100 ms	500 ms	3000 ms
FE2	Enable	Disable	100 ms	500 ms	3000 ms
FE3	Enable	Disable	100 ms	500 ms	3000 ms
FE4	Disable	Disable	100 ms	500 ms	3000 ms
FE5	Disable	Disable	100 ms	500 ms	3000 ms
FE6	Disable	Disable	100 ms	500 ms	3000 ms
FE7	Disable	Disable	100 ms	500 ms	3000 ms
FE8	Disable	Disable	100 ms	500 ms	3000 ms
FE9	Disable	Disable	100 ms	500 ms	3000 ms
FE10	Disable	Disable	100 ms	500 ms	3000 ms
FE11	Disable	Disable	100 ms	500 ms	3000 ms
FE12	Disable	Disable	100 ms	500 ms	3000 ms
FE13	Disable	Disable	100 ms	500 ms	3000 ms
FE14	Disable	Disable	100 ms	500 ms	3000 ms
FE15	Disable	Disable	100 ms	500 ms	3000 ms
FE16	Disable	Disable	100 ms	500 ms	3000 ms
FX17	Disable	Disable	100 ms	500 ms	3000 ms
FX18	Disable	Disable	100 ms	500 ms	3000 ms
FX19	Disable	Disable	100 ms	500 ms	3000 ms
FX20	Disable	Disable	100 ms	500 ms	3000 ms

Figure 136 Port GMRP Configuration

GMRP Enable

Options: Enable/Disable

Default: Disable

Function: Enable or disable the GMRP function on the port.

Agent Enable

Options: Enable/Disable

Default: Disable

Function: Enable or disable the GMRP agent function on the port.

Caution:

- Agent port cannot propagate agent entry.
- The premise of enabling GMRP agent function on port is enabling GMRP function on port.

Hold Timer

Range: 100ms~327600ms

Default: 100ms

Description: This value must be a multiple of 100. It is better to set the Hold timers on all GMRP-enabled ports to the same time.

Join Timer

Range: 100ms~327600ms

Default: 500ms

Description: This value must be a multiple of 100. It is better to set the Join timers on all GMRP-enabled ports to the same time.

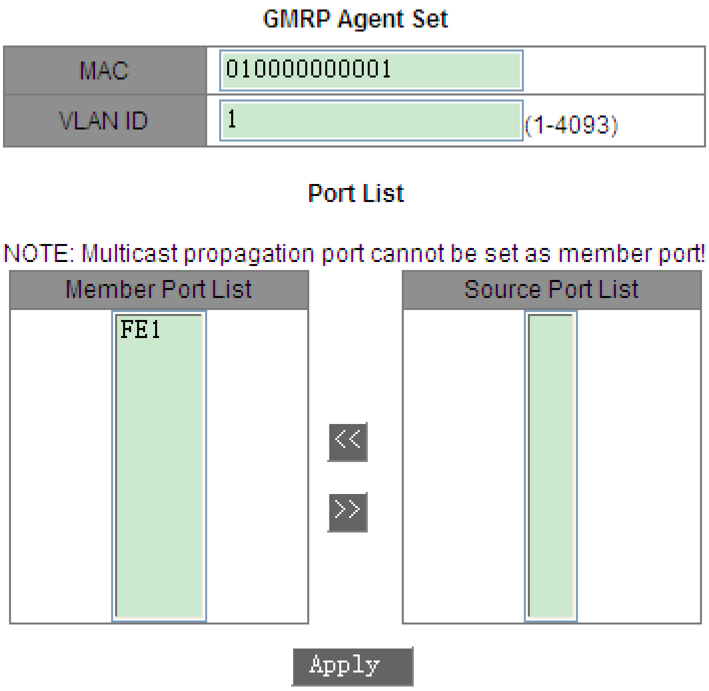
Leave Timer

Range: 100ms~327600ms

Default: 3000ms

Description: This value must be a multiple of 100. It is better to set the Leave timers on all GMRP-enabled ports to the same time.

3. Add a GMRP agent entry, as shown in Figure 137.



GMRP Agent Set

MAC	010000000001
VLAN ID	1 (1-4093)

Port List

NOTE: Multicast propagation port cannot be set as member port!

Member Port List	Source Port List
FE1	

Figure 137 GMRP Agent Entry Configuration

MAC

Format: HHHHHHHHHHHH (H is a hexadecimal number.)

Function: Configure the MAC address of multicast group. The lowest bit of the first byte is 1.

VLAN ID

Options: all created VLAN numbers

Function: Configure the VLAN ID for the GMRP agent entry.

Description: GMRP agent entry can only be forwarded from the propagation port with the VLAN ID same as this entry's VLAN ID.

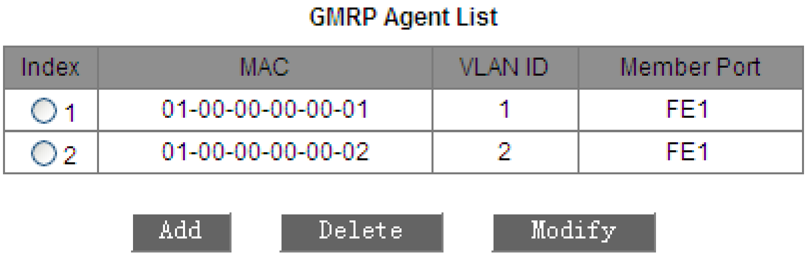
Member Port List

Select the member port for the agent entry. The port can only be selected from GMRP agent-enabled ports.

Source Port List

Options: all GMRP agent-enabled ports

4. View, modify, or delete a GMRP agent entry, as shown in Figure 138.



GMRP Agent List

Index	MAC	VLAN ID	Member Port
○ 1	01-00-00-00-00-01	1	FE1
○ 2	01-00-00-00-00-02	2	FE1

Figure 138 GMRP Agent Entry Operations

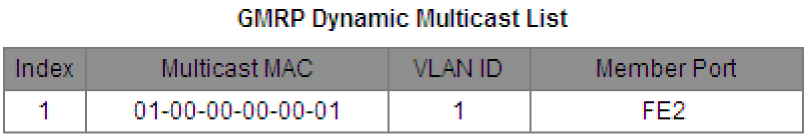
A GMRP agent entry consists of the MAC address, VLAN ID, and member port. To delete an entry, select the entry and click <Delete>. To modify an entry, select the entry and click <Modify>.

5. View the multicast members of this agent entry on the connected neighbor device as shown in Figure 139.

The following conditions shall be met.

- GMRP is enabled on the inter-connected devices.
- The two ports that connect the devices must be propagation ports, and the

VLAN ID of the propagation port on the local device must be identical with that in the agent entry.



GMRP Dynamic Multicast List

Index	Multicast MAC	VLAN ID	Member Port
1	01-00-00-00-00-01	1	FE2

Figure 139 GMRP Dynamic Multicast Table

GMRP Dynamic Multicast List

Portfolio: {Index, Multicast MAC, VLAN ID, Member Port}

Function: View GMRP dynamic multicast entries.

6.22.5 Typical Configuration Example

As shown in Figure 140, Switch A and Switch B are connected through port 2. Port 1 of Switch A is set to an agent port and generates two multicast entries:

- MAC address: 01-00-00-00-00-01, VLAN: 1
- MAC address: 01-00-00-00-00-02, VLAN: 2

After configuring different VLAN attributes on ports, observe the dynamic registration between switches and multicast information update.

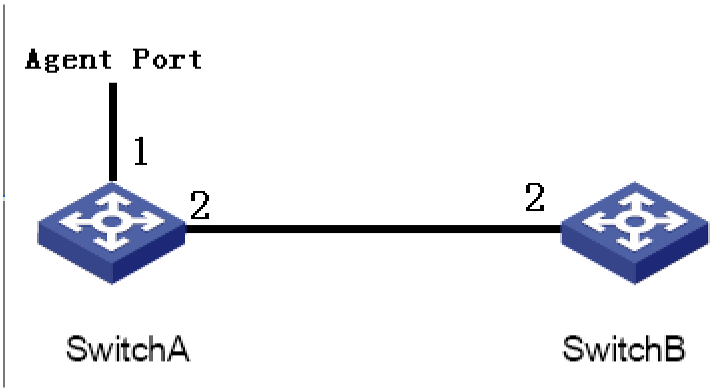


Figure 140 GMRP Networking

Configuration on Switch A:

1. Enable global GMRP function in switch A; set LeaveAll timer to the default value, as shown in Figure 135.
2. Enable GMRP function and agent function in port 1; enable only GMRP

function in port 2; set the timers to default values, as shown in Figure 136.

3. Configure agent multicast entry. Set <MAC address, VLAN ID, Member port> to <01-00-00-00-00-01, 1, 1> and <01-00-00-00-00-02, 2, 1>, as shown in Figure 137.

Configuration on Switch B:

1. Enable global GMRP function in switch B; set LeaveAll timer to the default value, as shown in Figure 135.
2. Enable GMPR function on port 2; set the timers to default values, as shown in Figure 136.

Table 9 lists the dynamically learned GMRP multicast entries on Switch B.

Table 9 Dynamic Multicast Entries

Attribute of Port 2 on Switch A	**Attribute of Port 2 on Switch B**	**Multicast Entries Received on Switch B**
Untag1	Untag1	MAC: 01-00-00-00-00-01 VLAN ID: 1 Member port: 2
Untag2	Untag2	MAC: 01-00-00-00-00-02 VLAN ID: 2 Member port: 2
Untag1	Untag2	MAC: 01-00-00-00-00-01 VLAN ID: 2 Member port: 2

6.23 RMON

6.23.1 Overview

Based on SNMP architecture, Remote Network Monitoring (RMON) allows network management devices to proactively monitor and manage the managed devices. An RMON network usually involves the Network

Management Station and Agents. The NMS manages Agents and Agents can collect statistics on various types of traffic on these ports.

RMON mainly provides statistics and alarm functions. With the tatistics function, Agents can periodically collect statistics on various types of traffic on these ports, such as the number of packets received from a certain network segment during a certain period. Alarm function is that Agents can monitor the values of specified MIB variables. When a value reaches the alarm threshold (such as the number of packets reaches the specified value), Agent can automatically record alarm events in RMON log, or send a Trap message to the management device.

6.23.2 RMON Groups

RMON (RFC2819) defines multiple RMON groups. The series devices support statistics group, history group, event group, and alarm group in public MIB. Each group supports up to 32 entries.

➢ Statistics group

With the statistics group, the system collects statistics on all types of traffic on ports and stores the statistics in the Ethernet statistics table for further query by the management device. The statistics includes the number of network collisions, CRC error packets, undersized or oversized packets, broadcast and multicast packets, received bytes, and received packets. After creating a statistics entry on a specified port successfully, the statistics group counts the number of packets on the port and the statistics is a continuously accumulated value.

➢ History group

History group requires the system to periodically sample all kinds of traffic on ports and saves the sampling values in the history record table for further query by the management device. The history group counts the statistics values of all kinds of data in the sampling interval.

- Event group

Event group is used to define event indexes and event handing methods. Events defined in the event group is used in the configuration item of alarm group. An event is triggered when the monitored device meets the alarm condition. Events are addressed in the following ways:

Log: logs the event and related information in the event log table.

Trap: sends a Trap message to the NMS and inform the NMS of the event.

Log-Trap: logs the event and sends a Trap message to the NMS.

None: indicates no action.

- Alarm group

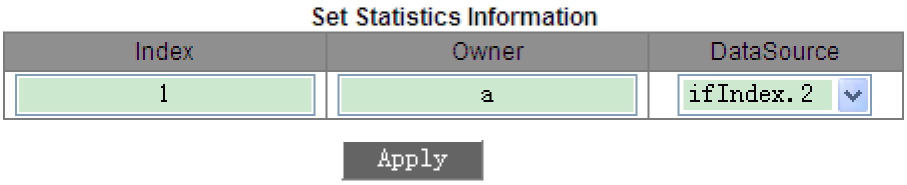
RMON alarm management can monitor the specified alarm variables. After alarm entries are defined, the system will acquire the values of monitored alarm variables in the defined period. When the value of an alarm variable is larger than or equal to the upper limit, a rising alarm event is triggered. When the value of an alarm variable is smaller than or equal to the lower limit, a falling alarm event is triggered. Alarms will be handled according to the event definition.

Caution:

If a sampled value of alarm variable exceeds the threshold multiple times in a same direction, then the alarm event is only triggered the first time. therefore the rising alarm and falling alarm are generated alternately.

6.23.3 Web Configuration

1. Configure the statistics table, as shown in Figure 141.



Set Statistics Information

Index	Owner	DataSource
1	a	ifIndex.2

Figure 141 RMON Statistics

Index

Range: 1~65535

Function: Configure the number of the statistics entry.

Owner

Range: 1~32 characters

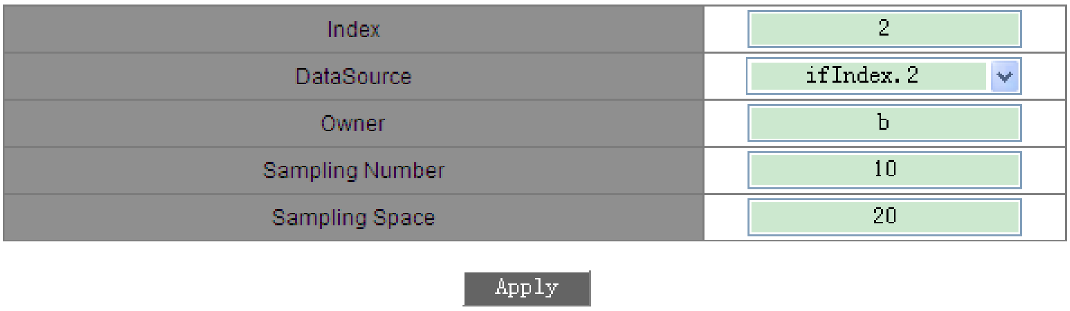
Function: Configure the name of the statistics entry.

Data Source

Options: ifIndex.portid

Function: Select the port whose statistics are to be collected.

2. Configure the history table, as shown in Figure 142.



Index	2
DataSource	ifIndex.2
Owner	b
Sampling Number	10
Sampling Space	20

Figure 142 RMON History Table

Index

Range: 1~65535

Function: Configure the number of the history entry.

Data Source

Options: ifIndex.portid

Function: Select the port whose information is to be sampled.

Owner

Range: 1~32 characters

Function: Configure the name of the history entry.

Sampling Number

Range: 1~65535

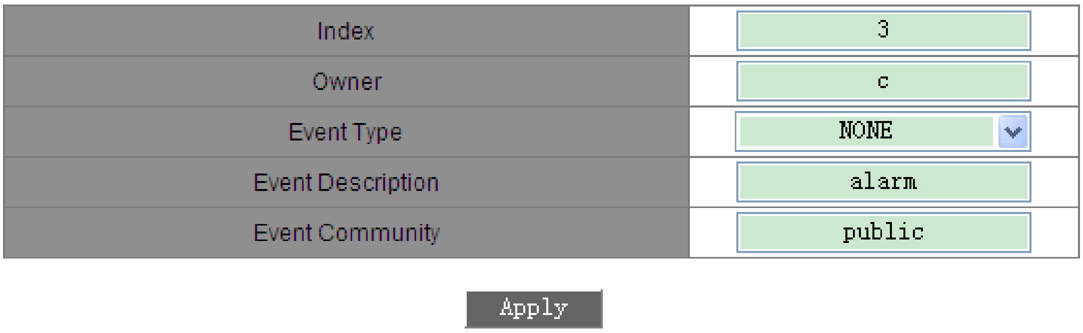
Function: Configure the sampling times of the port.

Sampling Space

Range: 1~3600s

Function: Configure the sampling period of the port.

3. Configure the event table, as shown in Figure 143.



Index	3
Owner	c
Event Type	NONE
Event Description	alarm
Event Community	public

Figure 143 RMON Event Table

Index

Range: 1~65535

Function: Configure the index number of the event entry.

Owner

Range: 1~32 characters

Function: Configure the name of the event entry.

Event Type

Options: NONE/LOG/Snmp-Trap/Log and Trap

Default: NONE

Function: Configure the event type for alarms, that is, the processing mode towards alarms.

Event Description

Range: 1~127 characters

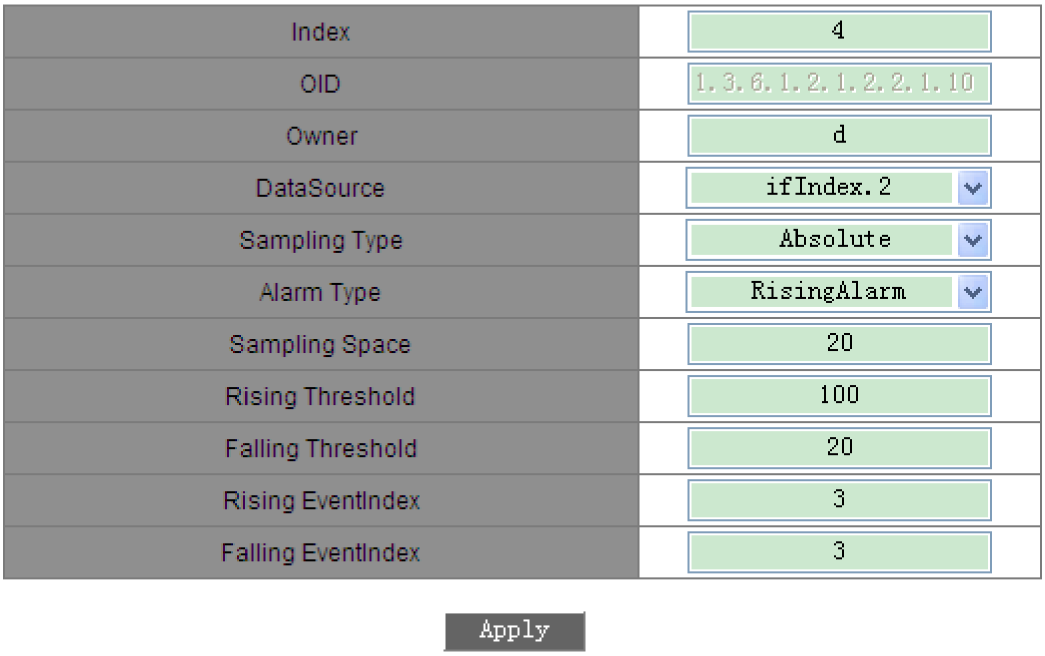
Function: Describe the event.

Event Community

Range: 1~127 characters

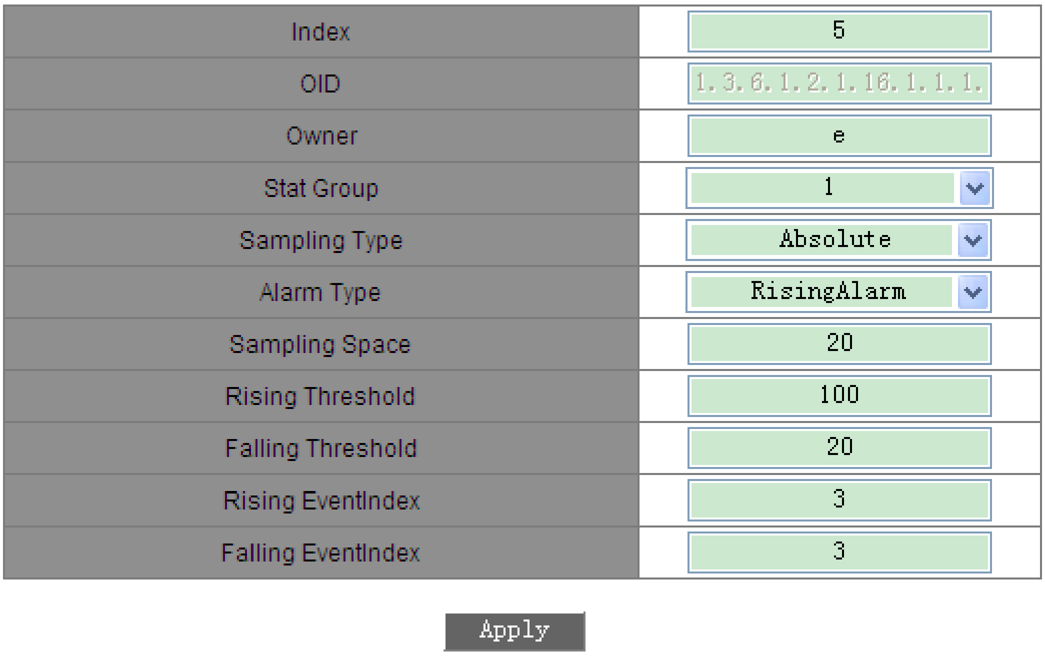
Function: Configure the community name for sending a trap event. The value shall be identical with that in SNMP.

4. Configure the alarm table, as shown in Figure 144 and Figure 145.



Index	4
OID	1.3.6.1.2.1.2.2.1.10
Owner	d
DataSource	ifIndex.2
Sampling Type	Absolute
Alarm Type	RisingAlarm
Sampling Space	20
Rising Threshold	100
Falling Threshold	20
Rising EventIndex	3
Falling EventIndex	3

Figure 144 RMON Alarm Table — 1213 MIB Node



Index	5
OID	1.3.6.1.2.1.16.1.1.1.
Owner	e
Stat Group	1
Sampling Type	Absolute
Alarm Type	RisingAlarm
Sampling Space	20
Rising Threshold	100
Falling Threshold	20
Rising EventIndex	3
Falling EventIndex	3

Figure 145 RMON Alarm Table — RMON MIB Node

Index

Range: 1~65535

Function: Configure the number of the alarm entry.

OID

Indicates the OID of the current MIB node.

Owner

Range: 1~32 characters

Function: Configure the name of the alarm entry.

Data Source

Options: ifIndex.portid

Function: Select the port whose information is to be monitored.

Stat Group

Options: Indexes of entries in the RMON statistics table.

Function: Select the statistics entry whose port is to be monitored.

Sampling Type

Options: Absolute/Delta

Default: Absolute

Function: Absolute indicates absolute value-based sampling. The value of the variable is directly extracted when the end of a sampling period approaches. Delta indicates change value-based sampling. The change value of the variable in the sampling period is extracted when the end of the period approaches.

Alarm Type

Options: RisingAlarm/FallingAlarm/RisOrFallAlarm

Default: RisingAlarm

Function: Select the alarm type, including the rising edge alarm, falling edge alarm, and both rising edge and falling edge alarms.

Sampling Space

Range: 1~65535

Function: Configure the sampling period. The value should be identical with that in the history table.

Rising Threshold

Range: 0~65535

Function: Configure the rising edge threshold. When the sampling value exceeds the threshold and the alarm type is set to RisingAlarm or RisOrFallAlarm, an alarm is generated and the rising event index is triggered.

Falling Threshold

Range: 0~65535

Function: Configure the falling edge threshold. When the sampling value is lower than the threshold and the alarm type is set to FallingAlarm or RisOrFallAlarm, an alarm is generated and the falling event index is triggered.

Rising Event Index

Range: 0~65535

Function: Configure the index of the rising event, that is, processing mode for rising edge alarms.

Falling Event Index

Range: 0~65535

Function: Configure the index of the falling event, that is, processing mode for falling edge alarms.

6.24 Unicast Address Configuration and Query

6.24.1 Overview

When forwarding a packet, the switch searches for the forwarding port in the MAC address table based on the destination MAC address of the packet.

A MAC address can be either static or dynamic.

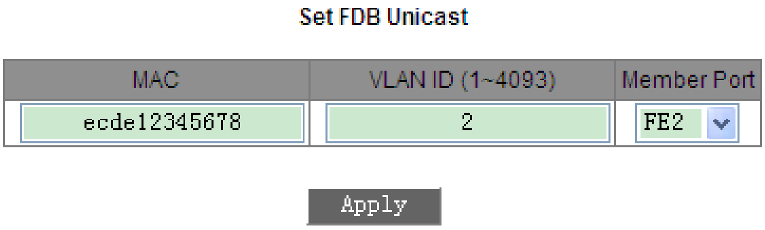
Static MAC addresses are configured. They have the highest priority (not overridden by dynamic MAC addresses) and are permanently valid.

Dynamic MAC addresses are learned by the switch in data forwarding, which are valid only for a certain period. The switch periodically updates its MAC address table. When receiving a data frame to be forwarded, the switch learns the source MAC address of the frame, establishes a mapping with the receiving port, and queries the forwarding port in the MAC address table based on the destination MAC address of the frame. If a match is found, the switch forwards the data frame from the corresponding port. If no match is found, the switch broadcasts the frame in its broadcast domain.

The switch supports a maximum of 256 static unicast entries.

6.24.2 Web Configuration

1. Add a static MAC address entry, as shown in Figure 146.



Set FDB Unicast

MAC	VLAN ID (1~4093)	Member Port
ecde12345678	2	FE2

Figure 146 Adding a Static FDB Unicast Entry

MAC

Format: HHHHHHHHHHHH (H is a hexadecimal number.)

Function: Configure the unicast MAC address. The lowest bit in the first byte is 0.

VLAN ID

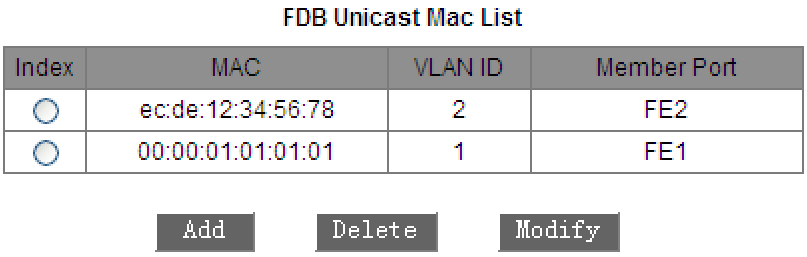
Options: all created VLAN IDs

Member Port

Options: all switch ports

Function: Select the port for forwarding packets destined for the MAC address. The port must be in the specified VLAN.

2. View the static unicast address list, as shown in Figure 147.



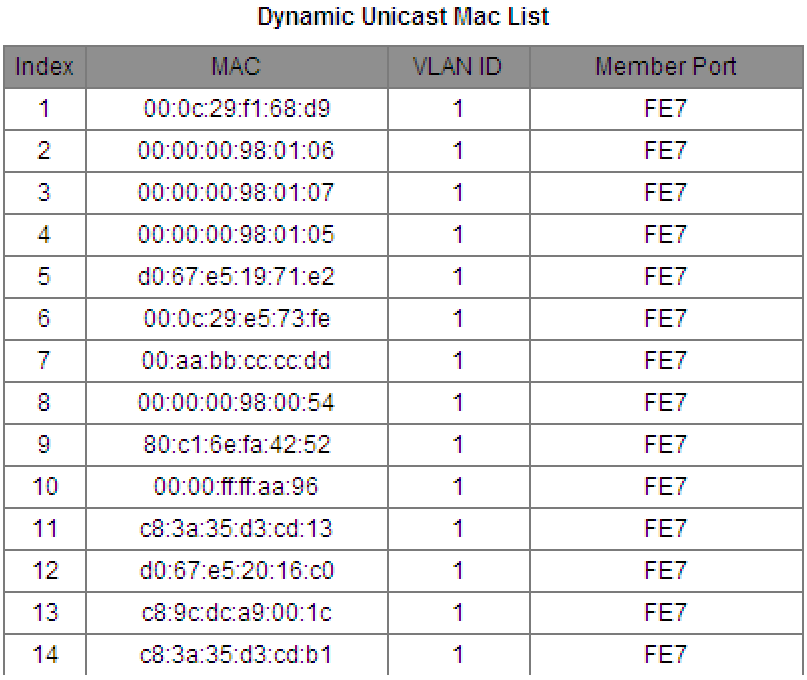
FDB Unicast Mac List

Index	MAC	VLAN ID	Member Port
○	ec:de:12:34:56:78	2	FE2
○	00:00:01:01:01:01	1	FE1

Figure 147 Viewing Static FDB Table

Select an entry. You can delete or modify the entry.

3. View the dynamic unicast address list, as shown in Figure 148.



Dynamic Unicast Mac List

Index	MAC	VLAN ID	Member Port
1	00:0c:29:f1:68:d9	1	FE7
2	00:00:00:98:01:06	1	FE7
3	00:00:00:98:01:07	1	FE7
4	00:00:00:98:01:05	1	FE7
5	d0:67:e5:19:71:e2	1	FE7
6	00:0c:29:e5:73:fe	1	FE7
7	00:aa:bb:cc:cc:dd	1	FE7
8	00:00:00:98:00:54	1	FE7
9	80:c1:6e:fa:42:52	1	FE7
10	00:00:ff:ff:aa:96	1	FE7
11	c8:3a:35:d3:cd:13	1	FE7
12	d0:67:e5:20:16:c0	1	FE7
13	c8:9c:dc:a9:00:1c	1	FE7
14	c8:3a:35:d3:cd:b1	1	FE7

Figure 148 Dynamic Unicast FDB Table

Appendix: Acronyms

Acronym	**Full Spelling**
ACL	Access Control List
ARP	Address Resolution Protocol
BPDU	Bridge Protocol Data Unit
CIST	Common and Internal Spanning Tree
CLI	Command Line Interface
CRC	Cyclic Redundancy Check
CST	Common Spanning Tree
DSCP	Differentiated Services Code Point
FTP	File Transfer Protocol
GARP	Generic Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
IGMP	Internet Group Management Protocol
IGMP Snooping	Internet Group Management Protocol Snooping
IST	Internal Spanning Tree
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MIB	Management Information Base
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
NMS	Network Management Station
OID	Object Identifier
QoS	Quality of Service
RMON	Remote Network Monitoring
RSTP	Rapid Spanning Tree Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol

STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
ToS	Type of Service
VLAN	Virtual Local Area Network
WRR	Weighted Round Robin