SICOM8010/3009/3009BA/3000BA Series

Industrial Ethernet Switches

Web Operation Manual

Kyland Technology Co., LTD.

Publication Date: Jul. 2012

Version: V2.0

Customer Service Hotline: (+8610) 88796676

FAX: (+8610) 88796678

Website: http://www.kyland.cn

E-mail: support@kyland.biz

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 1
1 Product Introduction 5
1.1 Overview 5
1.2 Product Models 5
1.3 Software Features 7
2 Switch Access 8
2.1 View Types 8
2.2 Switch Access by Console Port 9
2.3 Switch Access by Telnet 13
2.4 Switch Access by Web 14
3 Device Management 17
4 Device Status 18
4.1 Basic Information 18
4.2 Port Status 18
4.3 Port Statistics 20
4.4 System Operating Information 20
5 Basic Configuration 21
5.1 IP Address 21
5.2 Device Information Configuration 22
5.3 Port Configuration 23
5.4 Change Password 25
5.5 Software Update 26
5.5.1 Software Update by FTP 26
5.6 Configuration Upload & Download 31
6 Device Advanced Configuration 33
6.1 Port Rate Configuration 33
6.1.1 Overview 33

6.1.2 Web Configuration 33
6.1.3 Typical Configuration Example 35
6.2 VLAN Configuration 35
6.2.1 Overview 35
6.2.2 Principle 35
6.2.3 Port-based VLAN 36
6.2.4 Web Configuration 38
6.2.5 Typical Configuration Example 41
6.3 PVLAN Configuration 43
6.3.1 Overview 43
6.3.2 Web Configuration 44
6.3.3 Typical Configuration Example 45
6.4 Port Mirroring 46
6.4.1 Overview 46
6.4.2 Explanation 47
6.4.3 Web Configuration 47
6.4.4 Typical Configuration Example 48
6.5 Link Check 49
6.5.1 Overview 49
6.5.2 Web Configuration 49
6.6 Port Trunk 50
6.6.1 Overview 50
6.6.2 Implementation 50
6.6.3 Explanation 51
6.6.4 Web Configuration 52
6.6.5 Typical Configuration Example 54
6.7 Static Multicast Address Table 54
6.7.1 Overview 54
6.7.2 Web Configuration 55

6.8 IGMP Snooping....56
6.8.1 Overview....56
6.8.2 Basic Concepts....57
6.8.3 Principles....57
6.8.4 Web Configuration....58
6.8.5 Typical Configuration Example....59
6.9 ARP Configuration....60
6.9.1 Overview....60
6.9.2 Description....61
6.9.3 Web Configuration....61
6.10 RSTP Configuration....63
6.10.1 Overview....63
6.10.2 Basic Concepts....64
6.10.3 BPDU....64
6.10.4 Implementation....65
6.10.5 Web Configuration....67
6.10.6 Typical Configuration Example....70
6.11 RSTP Transparent Transmission....72
6.11.1 Overview....72
6.11.2 Web Configuration....73
6.11.3 Typical Configuration Example....74
6.12 DT-Ring Configuration....74
6.12.1 Overview....74
6.12.2 Basic Concepts....74
6.12.3 Implementation....75
6.12.4 Web Configuration....78
6.12.5 Typical Configuration Example....81
6.13 QoS Configuration....82
6.13.1 Overview....82

6.13.2 Principle 83
6.13.3 Web Configuration 84
6.13.4 Typical Configuration Example 87
6.14 MAC Aging Time 88
6.14.1 Overview 88
6.14.2 Web Configuration 88
6.15 LLDP 89
6.15.1 Overview 89
6.15.2 Web Configuration 89
6.16 MOTD 90
6.16.1 Overview 90
6.16.2 Web Configuration 90
6.16.3 Typical Configuration Example 91
6.17 SNTP 92
6.17.1 Overview 92
6.17.2 Web Configuration 93
6.18 Alarm 95
6.18.1 Overview 95
6.18.2 Web Configuration 95
6.19 SNMPv2 98
6.19.1 Overview 98
6.19.2 Implementation 98
6.19.3 Description 99
6.19.4 MIB 99
6.19.5 Web Configuration 100
6.19.6 Typical Configuration Example 103
6.20 SNMPv3 104
6.20.1 Overview 104
6.20.2 Implementation 104

6.20.3 Web Configuration 104
6.20.4 Typical Configuration Example 109
6.21 RMON 110
6.21.1 Overview 110
6.21.2 RMON Group 110
6.21.3 Web Configuration 112
6.22 SSH 117
6.22.1 Overview 117
6.22.2 Key 117
6.22.3 Implementation 118
6.22.4 Web Configuration 118
6.22.5 Typical Configuration Example 123
6.23 AAA Configuration 131
6.23.1 Overview 131
6.23.2 Implementation 131
6.23.3 Web Configuration 132
6.24 TACACS+ Configuration 133
6.24.1 Overview 133
6.24.2 Web Configuration 134
6.24.3 Typical Configuration Example 136
Appendix: Acronyms 138

Preface

This manual mainly introduces the access methods and software features of SICOM8010/3009/3009BA/3000BA series industrial Ethernet switches, and details Web configuration methods.

Content Structure

The manual contains the following contents:

Main Content	**Description**
1.Product introduction	➢Overview ➢Product models ➢Software features
2.Switch access	➢View types ➢Switch access by console port ➢Switch access by Telnet ➢Switch access by Web
3.Device management	➢Restart ➢Logout
4.Device status	➢Basic information ➢Port status ➢Port statistics ➢System running information
5.Device basic configuration	➢IP address ➢Device basic information configuration ➢Port configuration ➢Password change ➢Software update (FTP) ➢Configuration upload/download
6.Device advanced configuration	➢Port rate configuration

	➢VLAN configuration ➢PVLAN configuration ➢Port mirroring ➢Link check ➢Port trunk configuration ➢Static multicast address list ➢IGMP snooping ➢ARP configuration ➢RSTP configuration ➢RSTP transparent transmission ➢DT-Ring configuration ➢QoS configuration ➢MAC aging time ➢LLDP ➢MOTD ➢SNTP ➢Alarm ➢SNMPv2 and SNMPv3 ➢RMON ➢SSH ➢AAA configuration ➢TACACS+ configuration

Conventions in the manual

1. Text format conventions

Format	Explanation
< >	The content in < > is a button name. For example, click <Apply>.
[ ]	The content in [ ] is a window name or a menu name. For example,

	click [File].
{ }	The content in { } is a group. For example, {IP address, MAC address} means that IP address and MAC address are a group 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 submenu [All programs], then click the submenu [Accessories].
/	Select one from two or more options that are separated by "/". For example "Add/Subtract" means addition or subtraction.
~	It means a range. For example, "1~255" means a range from 1 to 255

2. CLI conventions

Format	Explanation
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	Explanation
Caution	The matters need attention during the operation and configuration, and it is a supplement to the operation content
Note	Necessary explanations to operation contents
Warning	The matters that call for special attention. Incorrect operation might cause data loss or damage to devices

Product Documents

The documents of SICOM8010/3009/3009BA/3000BA series industrial Ethernet switches include:

Name of Document	Content Introduction
SICOM8010 Series Industrial Ethernet Switches Hardware Installation Manual	Introduces hardware structure, hardware specifications, mounting and dismounting methods of SICOM8010.
SICOM3009 Series Industrial Ethernet Switches Hardware Installation Manual	Introduces hardware structure, hardware specifications, mounting and dismounting methods of SICOM3009.
SICOM3009BA Series Industrial Ethernet Switches Hardware Installation Manual	Introduces hardware structure, hardware specifications, mounting and dismounting methods of SICOM3009BA.
SICOM3000BA Series Industrial Ethernet Switches Hardware Installation Manual	Introduces hardware structure, hardware specifications, mounting and dismounting methods of SICOM3000BA.
SICOM8010/3009/3009BA/3000BA Series Industrial Ethernet Switches Web Operation Manual	Introduces 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.cn

1 Product Introduction

1.1 Overview

SICOM8010/3009/3009BA/3000BA includes a series of green DIN-rail industrial Ethernet switches applied in the wind power, distribution network automation, power, and intelligent transportation industries. SICOM3000BA and SICOM3009BA employ the intrinsic safety design and provide bare board models that can be embedded in other devices for integration.SICOM8010 supports PoE and meets IP40 protection class. The Reset button allows one-touch recovery.

1.2 Product Models

The series switches include four models (SICOM8010, SICOM3009, SICOM3009BA, and SICOM3000BA) with extensive port types to suit customers' different needs, as listed in Table 1.

Table 1 Product Models

Model	**Gigabit**		**100M**			**Device Form**
	SFP Slot	**M12 Port**	**SC/ST/FC Port**	**RJ45 Port**	**M12 Port**	
SICOM8010-2GE-M12-8T-M12	--	2	--	--	8	Integrated device
SICOM8010-2GE-M12-8T-4P-M12	--	2	--	--	8 (4 with PSE)	Integrated device
SICOM8010-2GE-M12-8T-8P-M12	--	2	--	--	8 (PSE)	Integrated device
SICOM8010-8T-M12	--	--	--	--	8	Integrated device
SICOM8010-8T-4P-M12	--	--	--	--	8 (4 with	Integrated

					PSE)	device
SICOM8010-8T-8P-M12	--	--	--	--	8 (PSE)	Integrated device
SICOM3009-3S/M-6T	--	--	3	6	--	Integrated device
SICOM3009-2S/M-6T	--	--	2	6	--	Integrated device
SICOM3009BA-EM-C-3S/M-6T	--	--	3	6	--	Bare board (conformal coating)
SICOM3009BA-EM-C-2S/M-6T	--	--	2	6	--	Bare board (conformal coating)
SICOM3000BA-3GX-6T	3	--	--	6	--	Integrated device
SICOM3000BA-2GX-6T	2	--	--	6	--	Integrated device
SICOM3000BA-C-3GX-6T	3	--	--	6	--	Integrated device (conformal coating)
SICOM3000BA-C-2GX-6T	2	--	--	6	--	Integrated device (conformal coating)
SICOM3000BA-EM-C-3GX-6T	3	--	--	6	--	Bare board (conformal coating)

SICOM3000BA-EM-C-2GX-6T	2	--	--	6	--	Bare board (conformal coating)

1.3 Software Features

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

- Redundancy protocols: RSTP/STP, DT-Ring
- Multicast protocols: IGMP Snooping, static multicast
- Switching attributes: VLAN, PVLAN, QoS, ARP
- Bandwidth management: port trunk, and port rate limiting
- Synchronization protocol: SNTP
- Security: TACACS+, SSH, SSL, AAA
- Device management: FTP/TFTP software update, configuration upload/download
- Device diagnosis: port mirroring, LLDP, link check
- Alarming: port alarm, AC/DC alarm, ring 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, as listed in Table 2.

Table 2 View Switching

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 operation ➢Restart the switch ➢Save current configuration ➢Display current configuration	➢Input "**configure terminal**" to enter the configuration view from the management view ➢Input "**exit**" to return to the user view

		➢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 Switch Access by Console Port

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

1.Run the Hyper Terminal in Windows desktop. Click [Start]→ [All Programs] → [Accessories] → [Communications] → [Hyper Terminal], as shown in Figure 1.

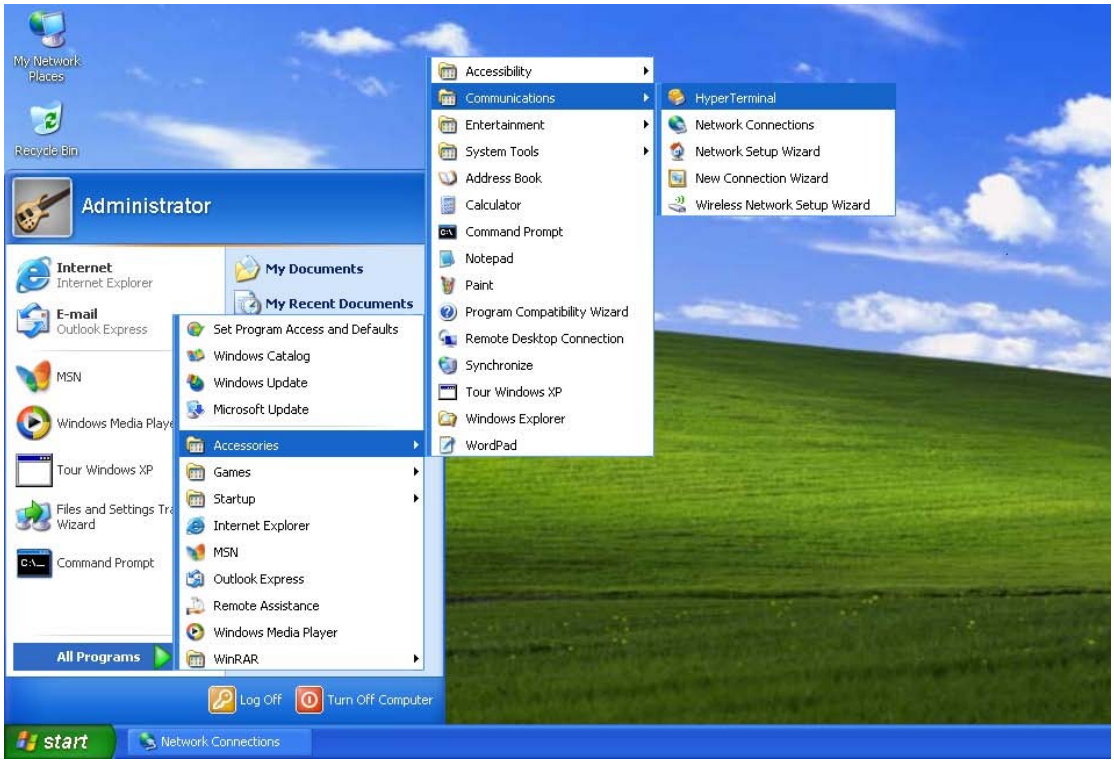

Figure 1 Starting the Hyper Terminal

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

Figure 2 Creating a New Connection

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

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] to view the communication port.

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

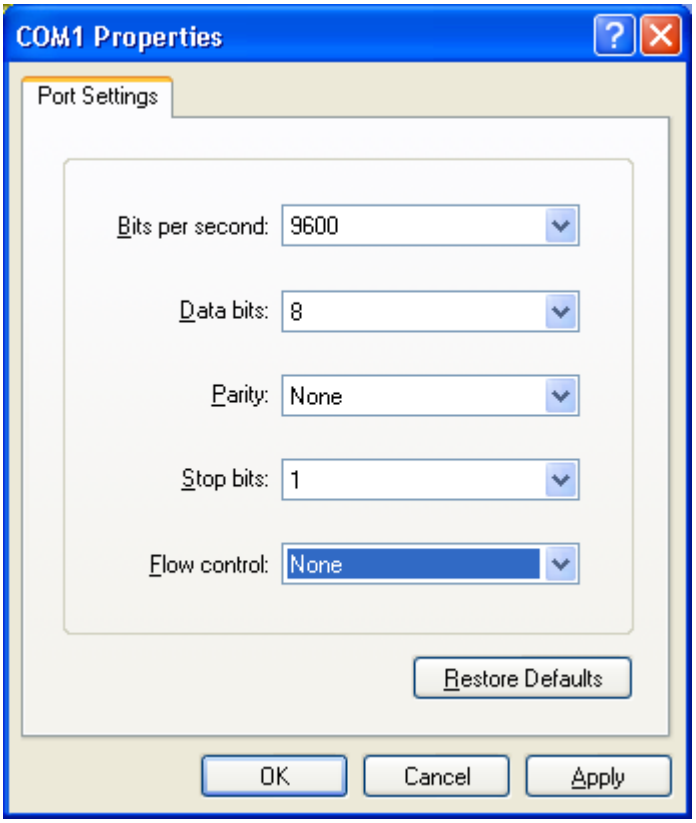

Figure 4 Setting Port Parameters

5.Click <OK>. The switch CLI is displayed. Input password "admin" and press <Enter> to enter the user view, as shown in Figure 5.

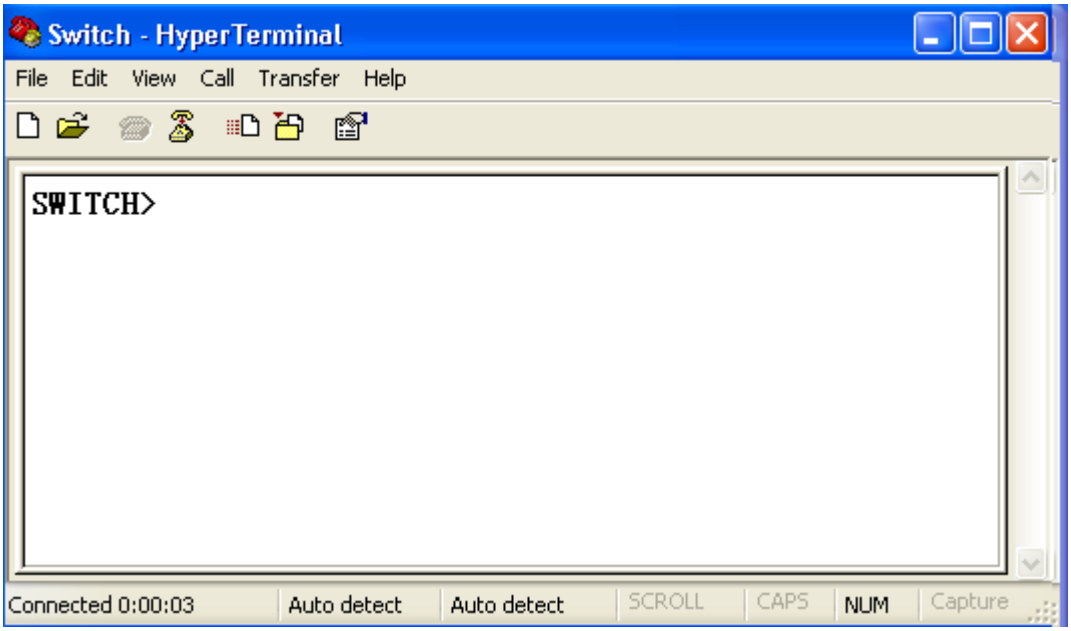

Figure 5 CLI

2.3 Switch Access by 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.

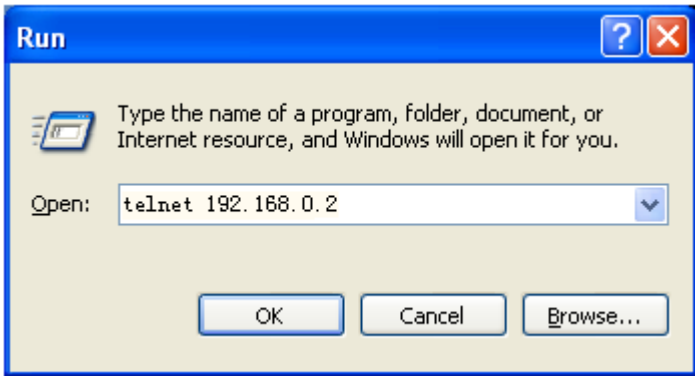

Figure 6 Telnet Access

Note:

To confirm the switch IP address, please refer to "5.1 IP Address" to learn how to obtain the IP address.

2.In the Telnet interface, input "admin" in User, and "123" in Password. Click <Enter > to log in to the switch, as shown in Figure 7.

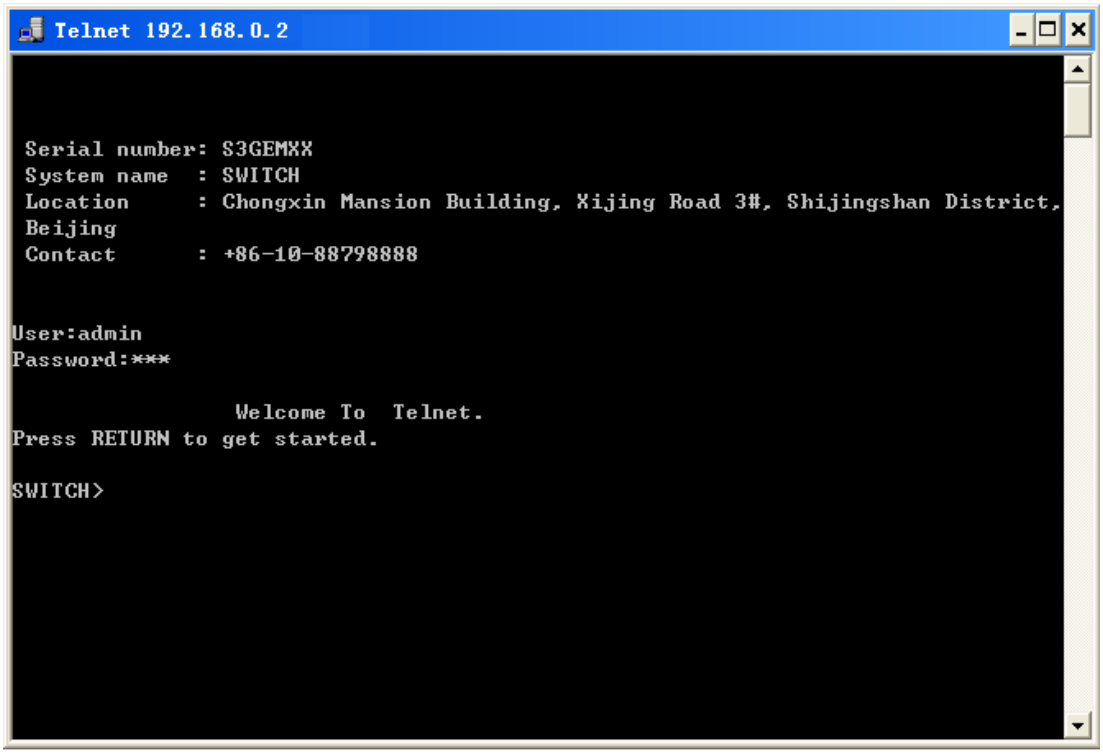

Figure 7 Telnet Interface

2.4 Switch Access by 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 <Sign in>.

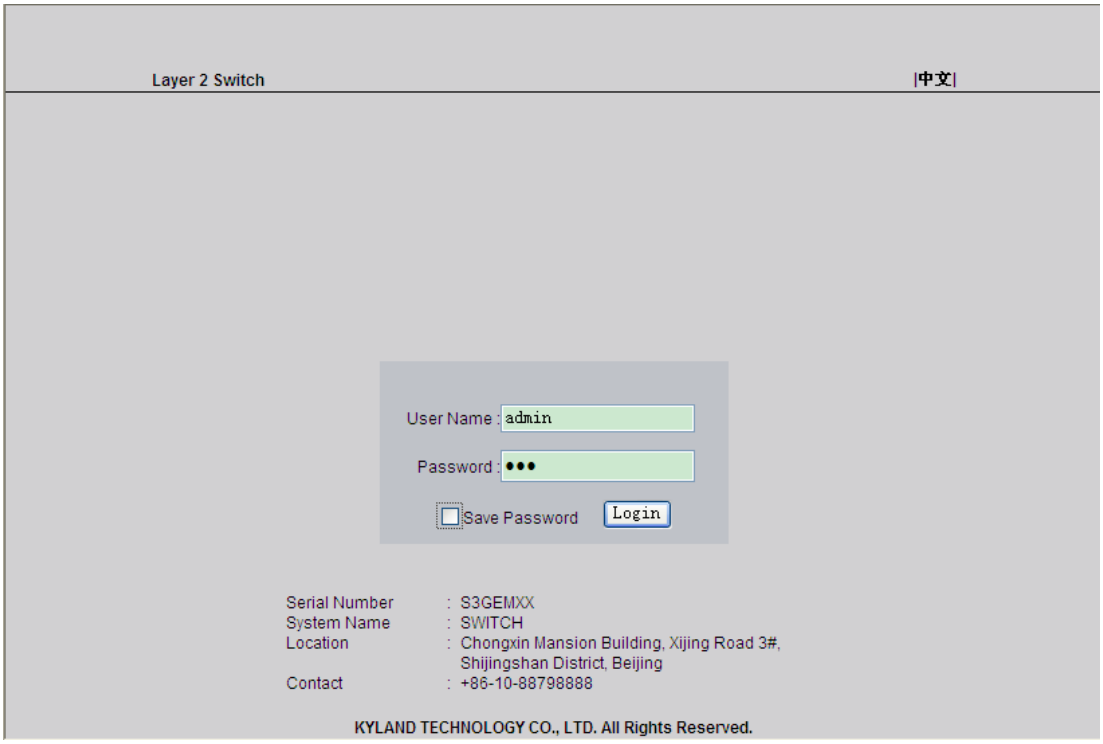

Figure 8 Web Login

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

Note:

To confirm the switch IP address, please refer to "5.1 IP Address" to learn how to obtain the IP address.

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

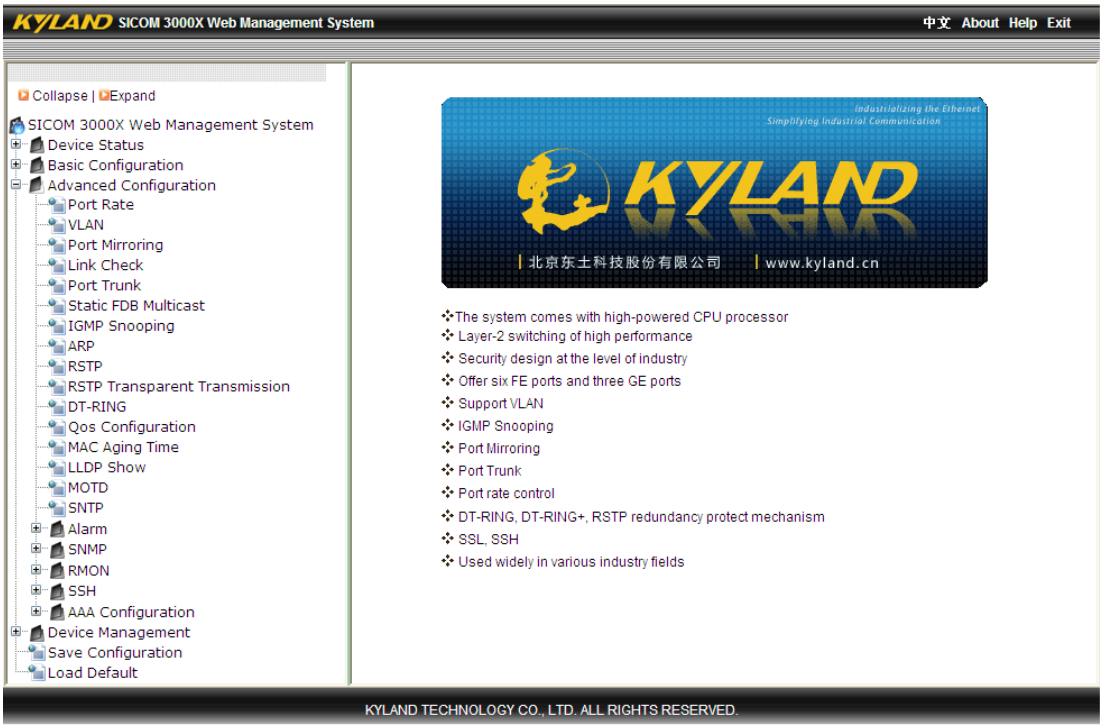

Figure 9 Web Interface

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:

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.

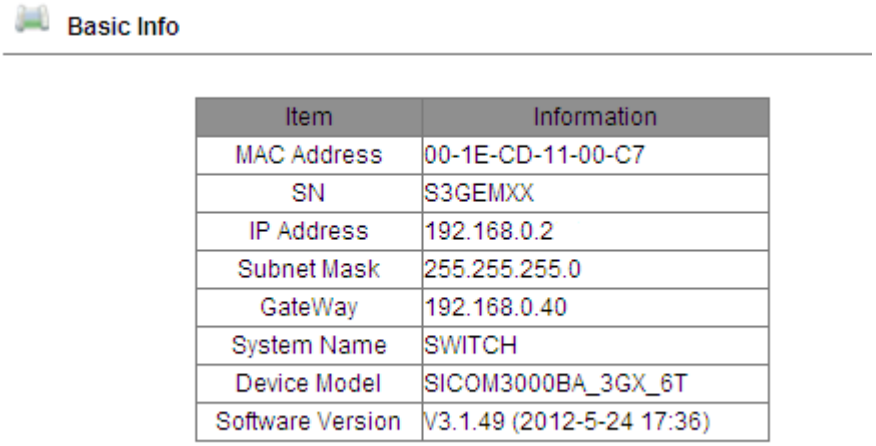

Figure 10 Switch Basic Information

4.2 Port Status

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

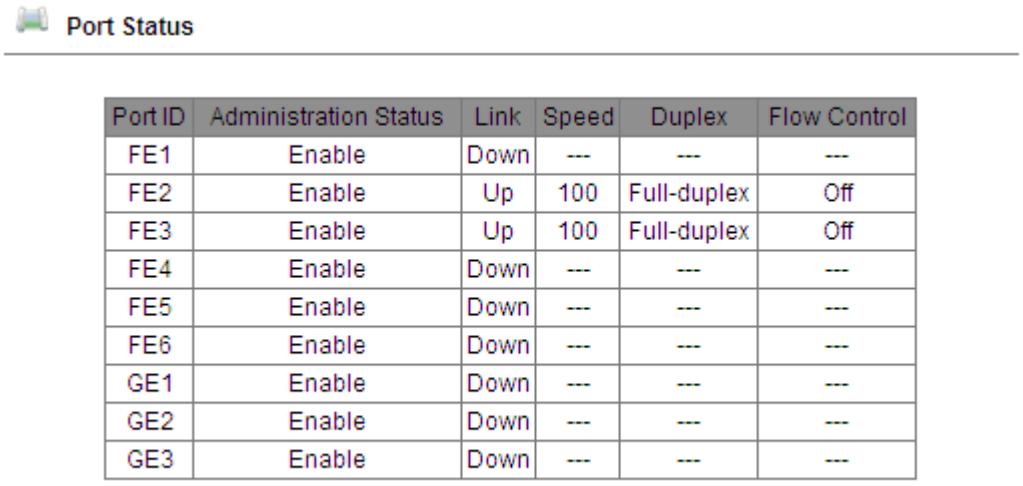

Figure 11 Port Status

Port

Display port number printed on the switch front panel.

Port types:

FE: 10/100Base-TX RJ45 port

FX: 100Base-FX port

GE: 10/100/1000Base-TX RJ45 port

GX: Gigabit SFP port

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.

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.

Note:

For details about duplex and flow control, refer to "5.3 Port Configuration".

4.3 Port Statistics

The Port Statistics interface displays the number of bytes and packets that each port sends, and the number of bytes and packets that each port receives, CRC errors, and the number of packets whose lengths are less than 64 bytes, as shown in Figure 12.

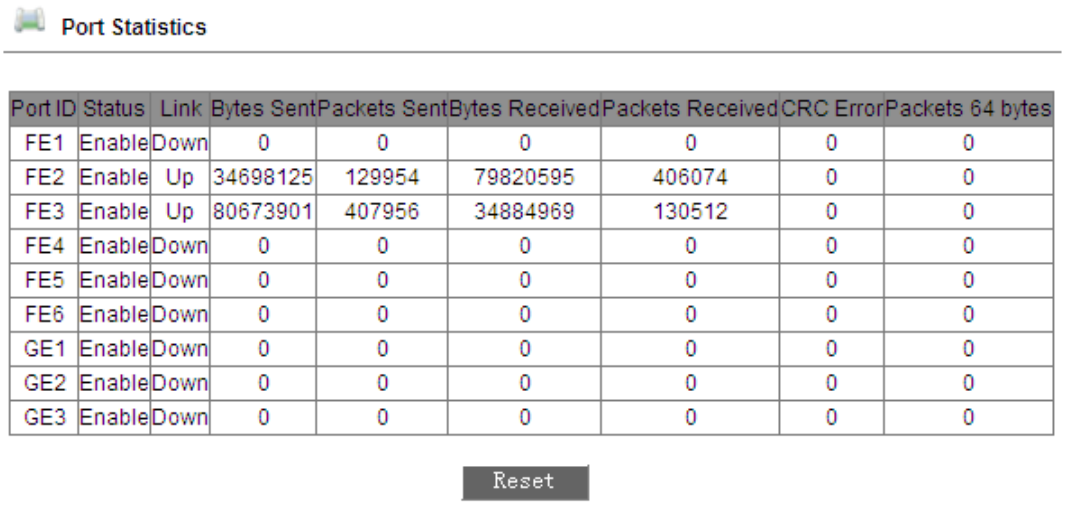

Figure 12 Port Statistics

4.4 System Operating Information

The device operating time and CPU usage can be automatically displayed, as shown in Figure 13.

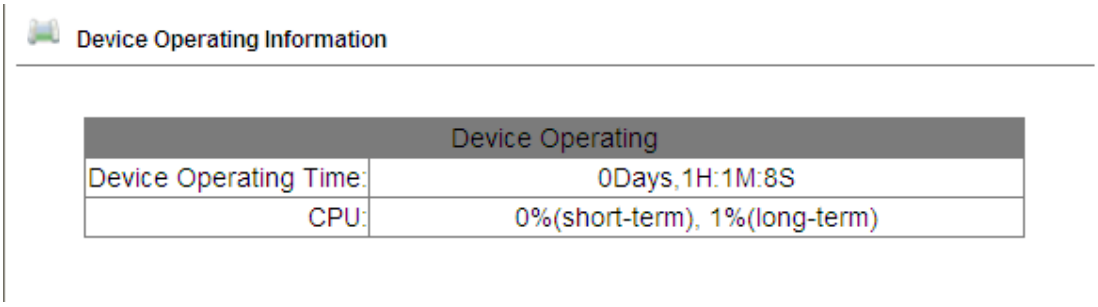

Figure 13 System Operating Information

5 Basic Configuration

5.1 IP Address

1.Display switch IP address by using console port

Use console port to log into switch command line interface. Enter the "**show interface**" command in the user view to check the switch IP address. As shown in Figure 14, the IP address is circled in red.

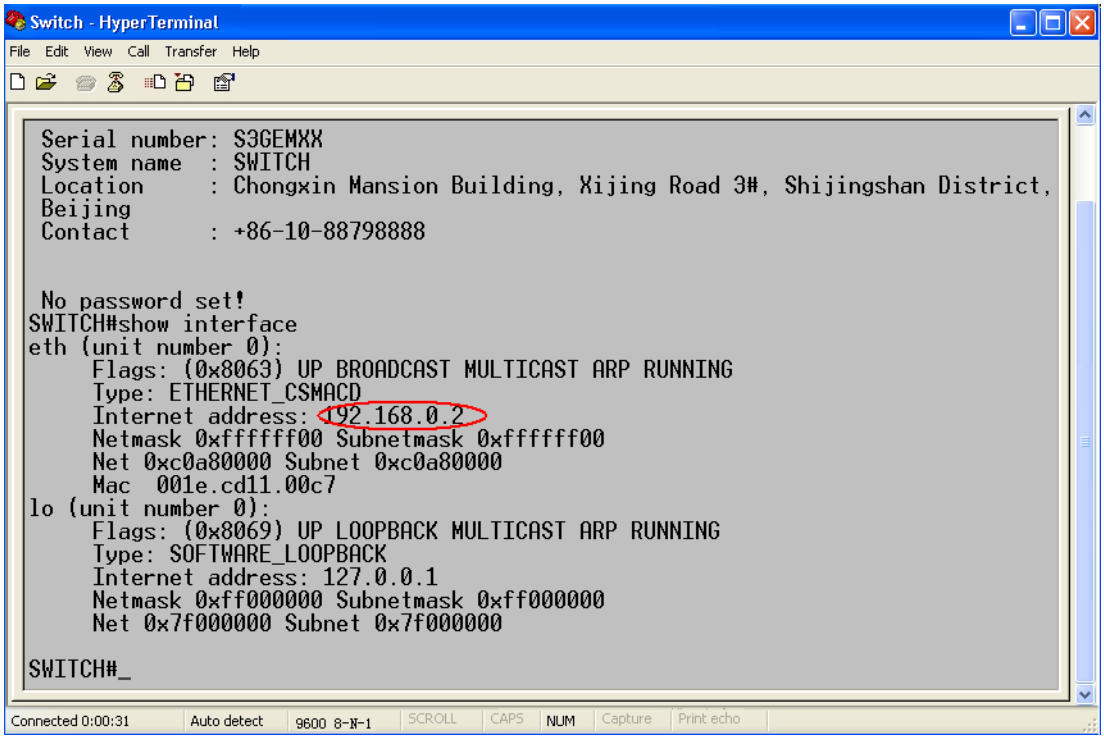

Figure 14 Viewing IP Address

2.IP address configuration

Switch IP address and gateway can be configured manually, as shown in Figure 15.

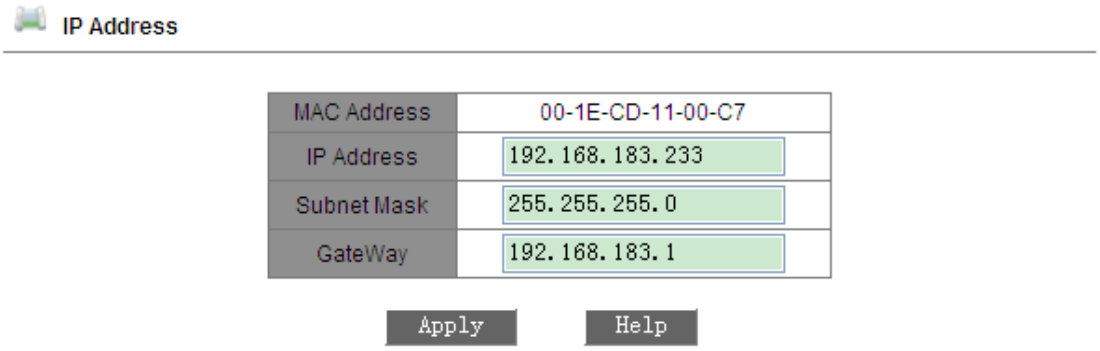

Figure 15 IP Address

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 Device Information Configuration

Device information includes the project name, switch name, location, and contact, as shown in Figure 16.

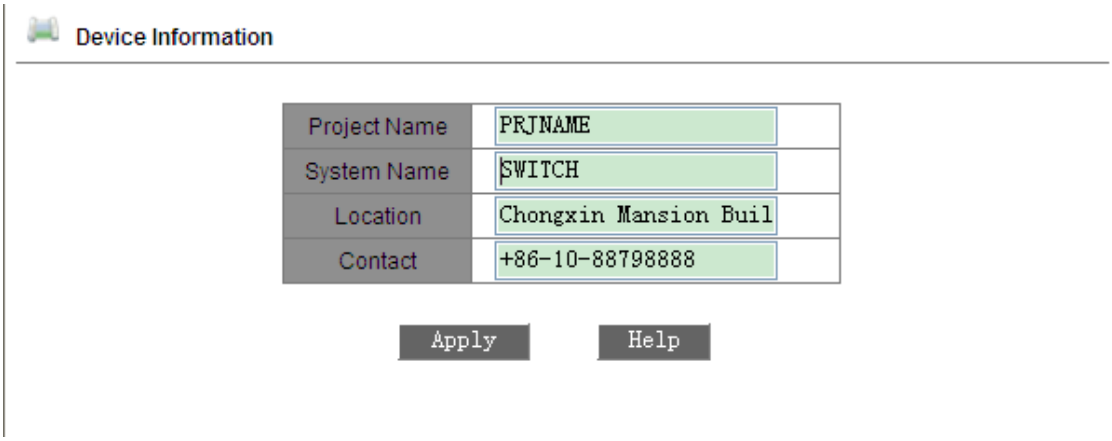

Figure 16 Device Information

Project Name

Range: 1~64 characters

Switch Name

Range: 1~32 characters

Location

Options: character/Chinese character

Range: 1~255 characters (One Chinese character occupies two characters.)

Contact

Options: character/Chinese character

Range: 1~32 characters (One Chinese character occupies two characters.)

5.3 Port Configuration

In port configuration, you can configure port status, port speed, flow control, and other information, as shown in Figure 17.

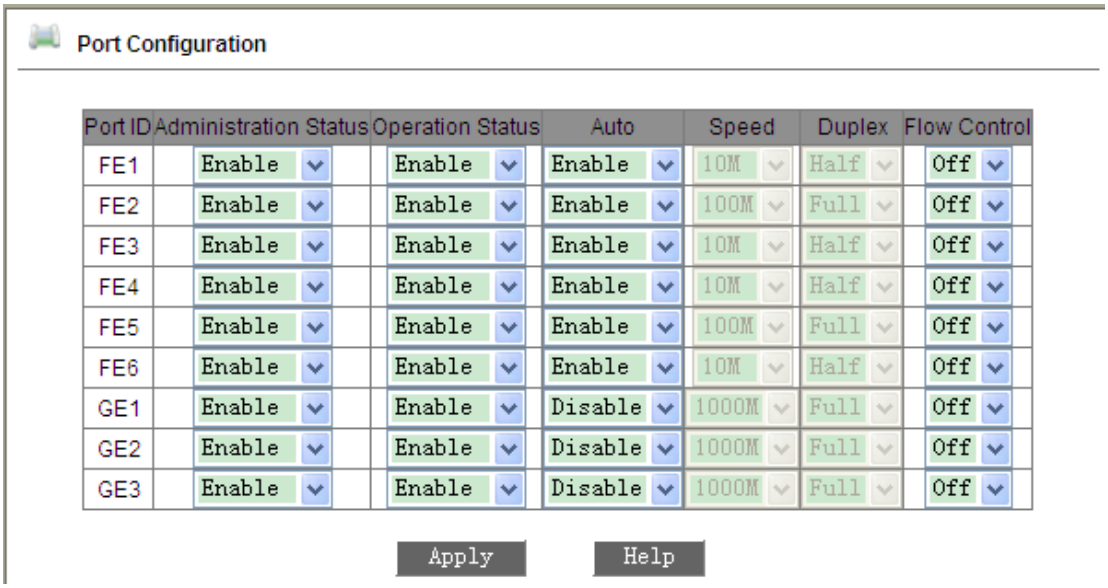

Figure 17 Port Configuration

Administration Status

Options: Enable/Disable

Default: Enable

Function: Enable means that the port is open and permits data transmission; Disable means that the port is blocked without data transmission. This option can directly affect the hardware status of the port and trigger port alarms.

Operation Status

Options: Enable/Disable

Default: Enable

Function: configure the port operation state.

Description: The port is disabled by protocols.

Auto

Options: Enable/Disable

Default: Enable

Function: Configure the auto-negotiation status of ports.

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

Speed

Options: 10M/100M/1000M

Function: forced port speed

Description: When Auto is disabled, the port speed can be configured.

Duplex

Options: Half/Full

Function: Configure the duplex mode of ports.

Description: When Auto is disabled, the port duplex mode can be configured.

Caution:

- 10/100Base-TX ports can be configured to auto-negotiation, 10M&full duplex, 10M&half duplex, 100M&full duplex, and 100M&half duplex.
- 100Base-FX ports are forced to 100M&full duplex.
- 1000M electrical ports can be configured to auto-negotiation.
- 1000M fiber ports can be configured 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/duplex mode 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.

5.4 Change Password

You can change the password for user name "admin", as shown in Figure 18.

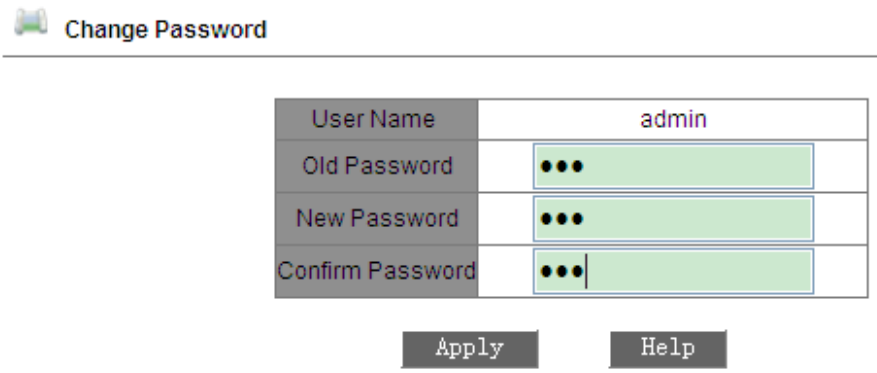

Figure 18 Changing the Password

5.5 Software Update

The switch provides better performance after software update. 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 is not changed, you can update only the system software version.

The software version update requires an FTP/TFTP server.

5.5.1 Software Update by 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 19. Create a user name and password, for example, user name "admin" and password "123". Click <OK>.

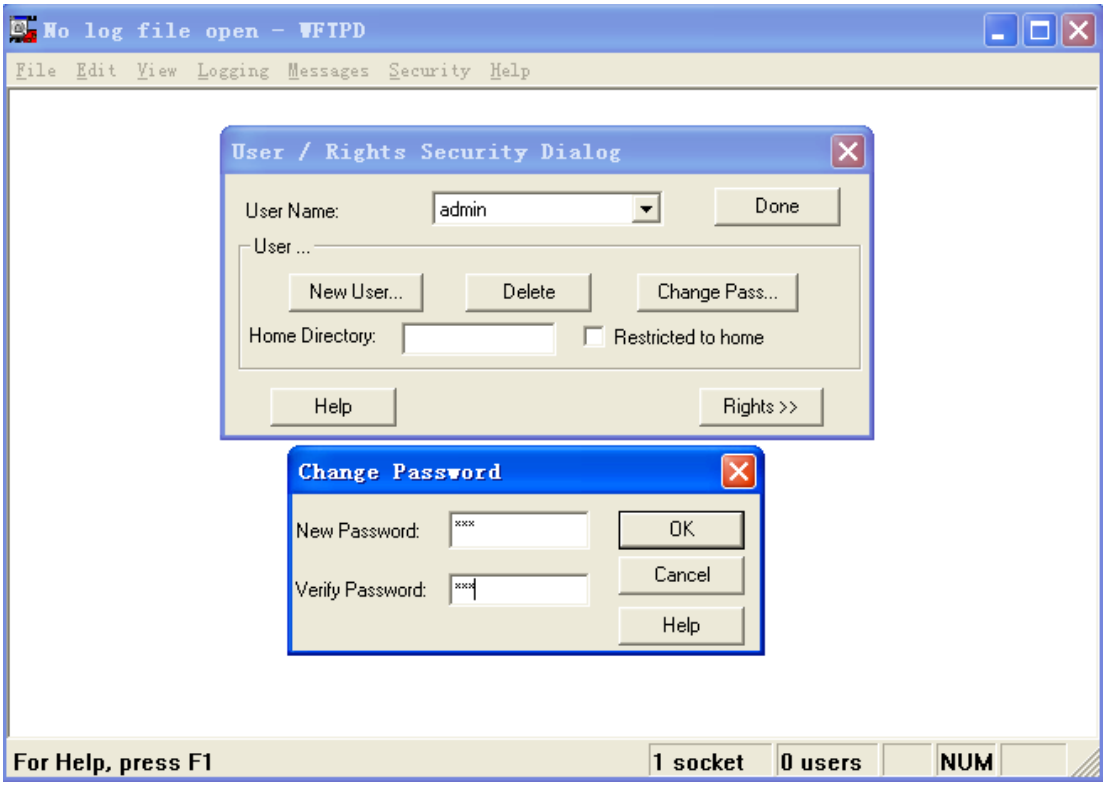

Figure 19 Creating a New FTP User

2.Input the storage path of the update file in "Home Directory", as shown in Figure 20. Click <Done>.

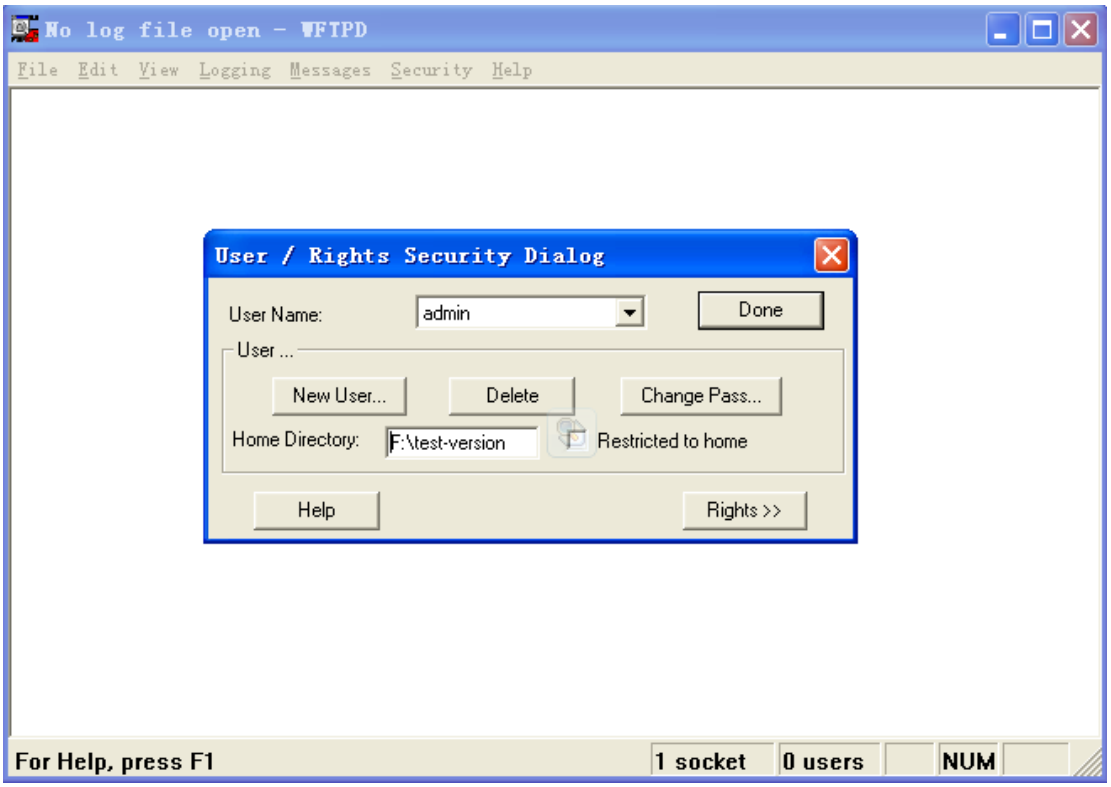

Figure 20 File Storage Path

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

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

Table 3 lists the parameter descriptions.

Table 3 Parameters for BootROM Update by FTP

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

4.Figure 21 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>.

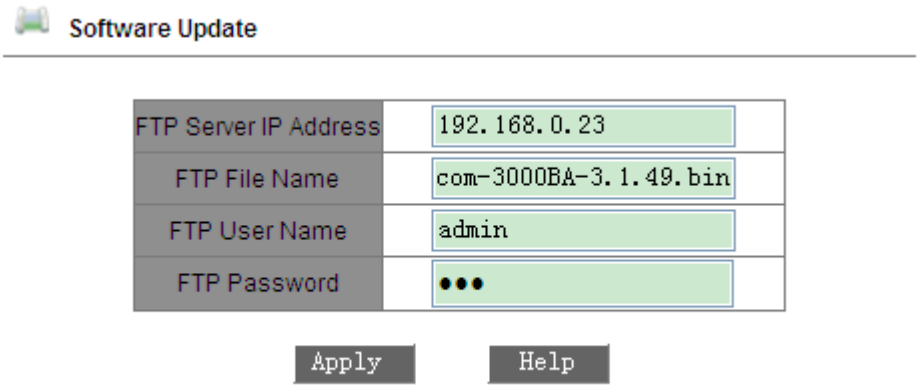

Figure 21 Software Update by FTP

Warning:

The file name must contain an extension. Otherwise, the update may fail.

5.Make sure the normal communication of FTP server and switch, as shown in Figure 22.

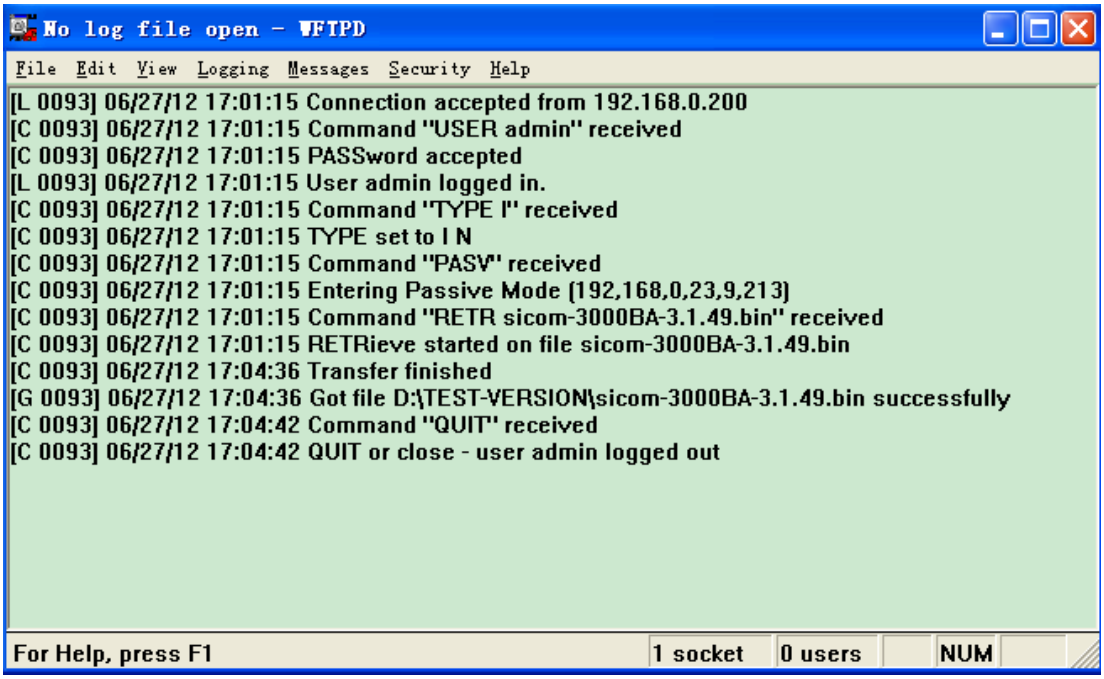

Figure 22 Normal Communication Between FTP Server and Switch

Caution:

To display update log information as shown in Figure 22, you need to click [Logging] → [Log Options] in WFTPD and select Enable Logging and the log information to be displayed.

6.Wait for the update to complete, as shown in Figure 23.

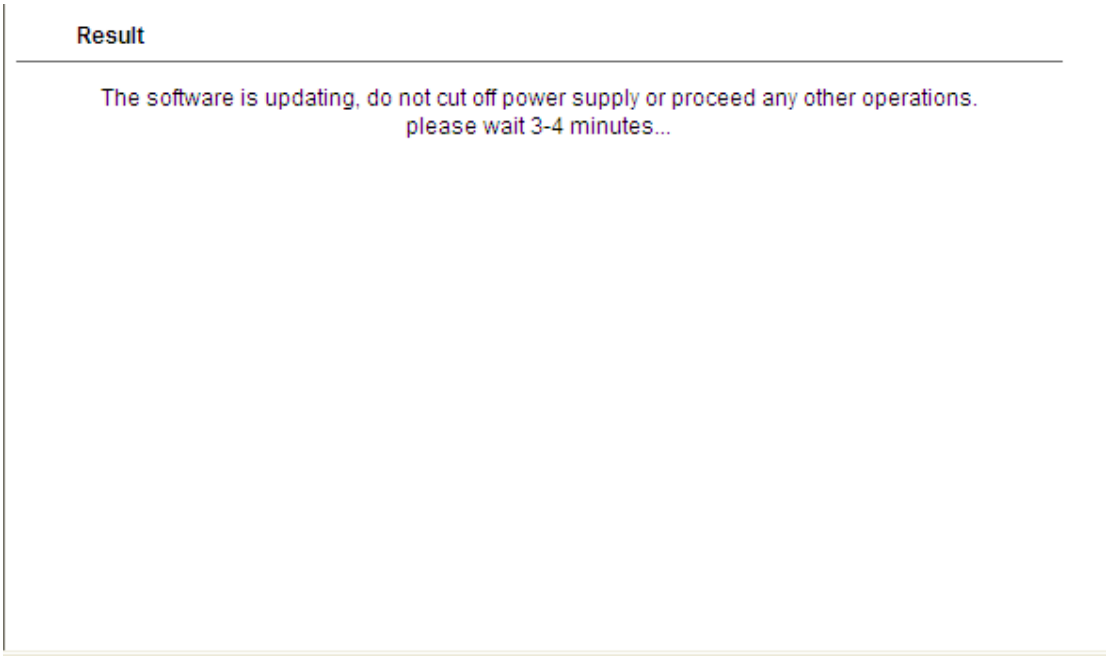

Figure 23 Waiting for the Update to Complete

7.When update completes as shown in Figure 24, please reboot the device and open the Basic Information to check if update succeeded and the new version is active.

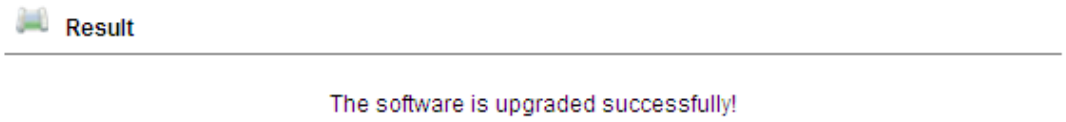

Figure 24 Successful Software Update by FTP

Warning:

- In the software update process, keep the FTP server software running.
- When update completes, reboot the device to activate the new version.
- If update fails, do not reboot the device to avoid the loss of software file and

the switch cannot be started normally.

5.6 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 by FTP/TFTP protocol.

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 25 and Figure 26.

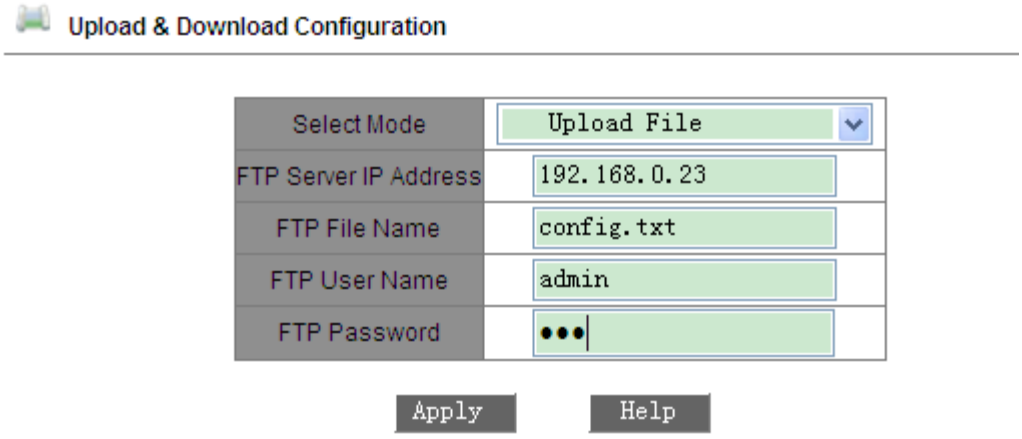

Figure 25 Configuration File Upload

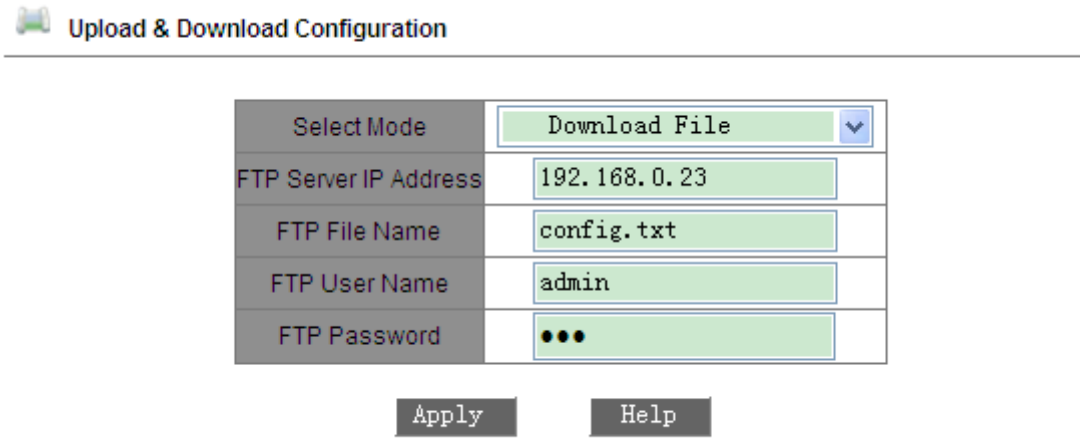

Figure 26 Configuration File Download

Caution:

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

6 Device Advanced Configuration

6.1 Port Rate Configuration

6.1.1 Overview

Port rate configuration is to limit the number of port-received/transmitted packets and drop the data that is over the limitation. Ingresses limit the rate of the selected packets, while egresses limit the rate of all packets.

The rate of the following packets is limited at the ingress.

- Multicast packets: packets manually added or learned through IGMP Snooping and GMRP
- Flooded unicast packets: packets not added manually or learned from source MAC addresses
- Broadcast storm: packets with the destination MAC address as FF:FF:FF:FF:FF:FF.

6.1.2 Web Configuration

1. Add port rate configuration, as shown in Figure 27.

Port Rate

The restricted speed is disabled when it is set to 0.
Set Packet Type for Rate Control

Type for Rate Control	InRate
Limit all frames	○
Limit just multicast and flooded unicast frames (including broadcast frames)	○
Limit just multicast frames (including broadcast)	◉
Limit just broadcast frames	○

Port ID	InRate	OutRate
FE1	70 Kbps	80 Kbps
FE2	0 Kbps	0 Kbps
FE3	0 Kbps	0 Kbps
FE4	0 Kbps	0 Kbps
FE5	0 Kbps	0 Kbps
FE6	0 Kbps	0 Kbps
GE1	0 Kbps	0 Kbps
GE2	0 Kbps	0 Kbps
GE3	0 Kbps	0 Kbps

Apply Help

Figure 27 Port Rate Configuration

Packet Type

Options: Limit all frames, Limit just multicast and flooded unicast frames, Limit just multicast frames, or Limit just broadcast frames

Function: Set packet type for ingress rate control.

InRate

Range: 62~250000Kbps

Function: limit the ingress rate of port-received packets and the packets that exceed the limitation will be dropped

Description: The ingress rate of Fast Ethernet port is in the range of 62~100000Kbps

The ingress rate of Gigabit Ethernet port is in the range of 64~200000Kbps

Egress Rate

Range: 62~250000Kbps

Function: limit the egress rate of port-transmitted packets.

Description: The egress rate of Fast Ethernet port is in the range of 62~100000Kbps.

The egress rate of Gigabit Ethernet port is in the range of 62~250000Kbps.

Caution:

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

6.1.3 Typical Configuration Example

Limit the ingress rate of multicast and broadcast packets received by port 1 to 70Kbps and set the egress rate of port 1 to 80Kbps.

Configuration steps: select packet types: multicast and broadcast packets, set the ingress rate to 70Kbps and the egress rate to 80Kbps, as shown in Figure 27.

6.2 VLAN Configuration

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 4 shows the structure of an 802.1Q frame.

Table 4 802.1Q 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 Tag packet; if not, it is an Untag packet. The packets in switch all carry an 802.1Q tag.

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

Table 5 Different Processing Modes for Packets

<table>
<tr><th colspan="2">Processing Received Packets</th><th colspan="2">Processing Packets to Be Forwarded</th></tr>
<tr><th>Untagged packets</th><th>Tagged packets</th><th>Port Type</th><th>Packet Processing</th></tr>
<tr><td rowspan="2">Add PVID tags to untagged packets.</td><td rowspan="2">➢ If the VLAN ID in a packet is in the list of VLANs allowed through, accept the packet.
➢ If the VLAN ID in a packet is not in the list of VLANs</td><td>Untag</td><td>Forward the packet after removing the tag.</td></tr>
<tr><td>Tag</td><td>Keep the tag and forward the packet.</td></tr>
</table>

	allowed through, discard the packet.		

6.2.4 Web Configuration

1.Create a VLAN.

Click <Add> to create a VLAN, as shown in Figure 28. Select the ports to be added to the VLAN and set port parameters, as shown in Figure 29.

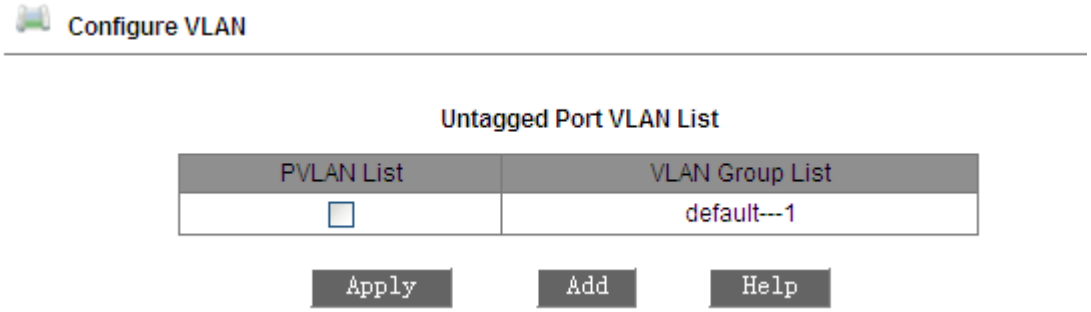

Figure 28 Creating a VLAN

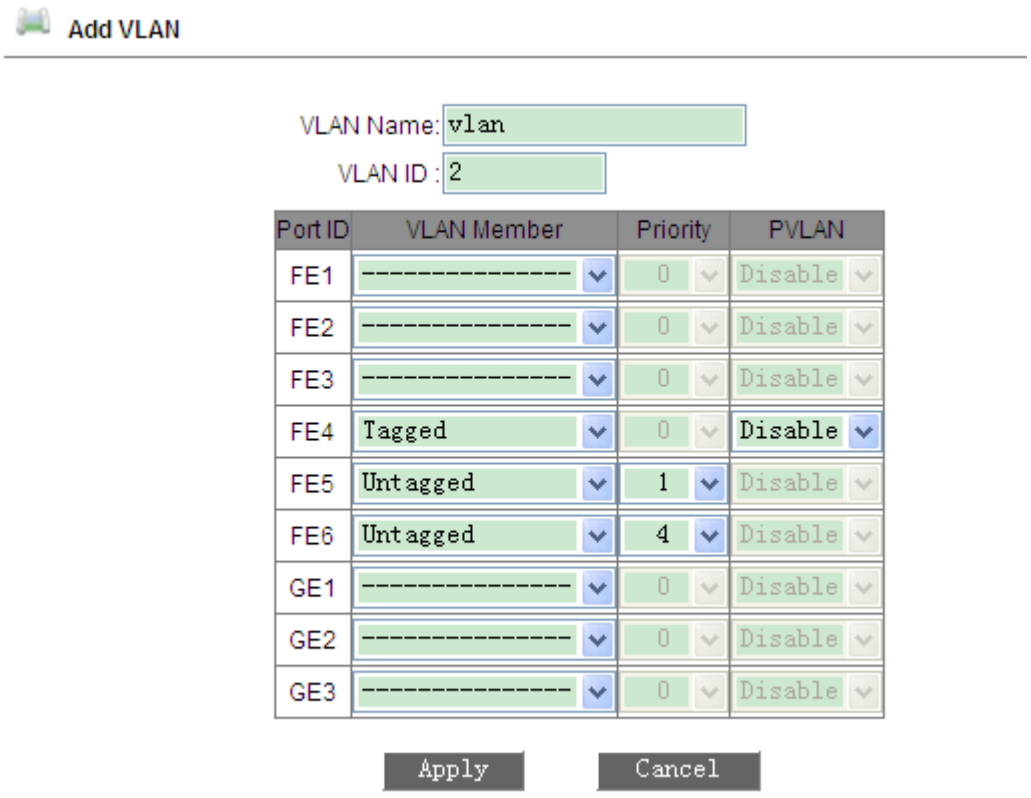

Figure 29 VLAN Configuration

VLAN Name

Range: 1~31 characters

Function: set VLAN name

VLAN ID

Range: a number in the range of 2~4093

Function: Configure VLAN ID

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

VLAN Member

Options: Tagged/Untagged

Function: select the port type in VLAN

Priority

Range: 0~7

Default: 0

Function: set the port default priority. When adding an 802.1Q Tag into an untagged packet, the PRI field is this priority value.

PVLAN

Options: Enable/Disable

Default: Disable

Function: For Tag port, enable PVLAN or not. More information about PVLAN will be provided in a later section.

Caution:

An Untag port can be added to only one VLAN and its VLAN ID is the port PVID. By default, it is VLAN 1, but a tag port can be added to multiple VLANs.

2. Display VLAN list, as shown inFigure 30.

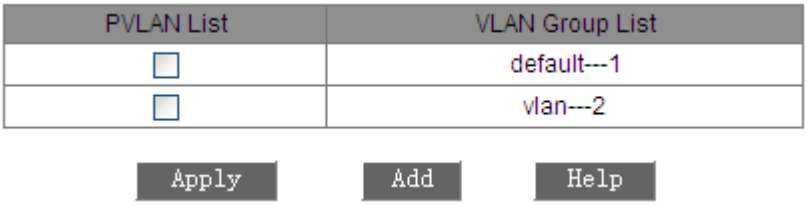

Figure 30 Viewing VLAN List

PVLAN List

Options: Select/Deselect

Function: Enable or disable the PVLAN function. For details, see section 0 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 29.

.

3. Display the VLAN list of Untag ports and it is the port PVID, as shown in Figure 31.

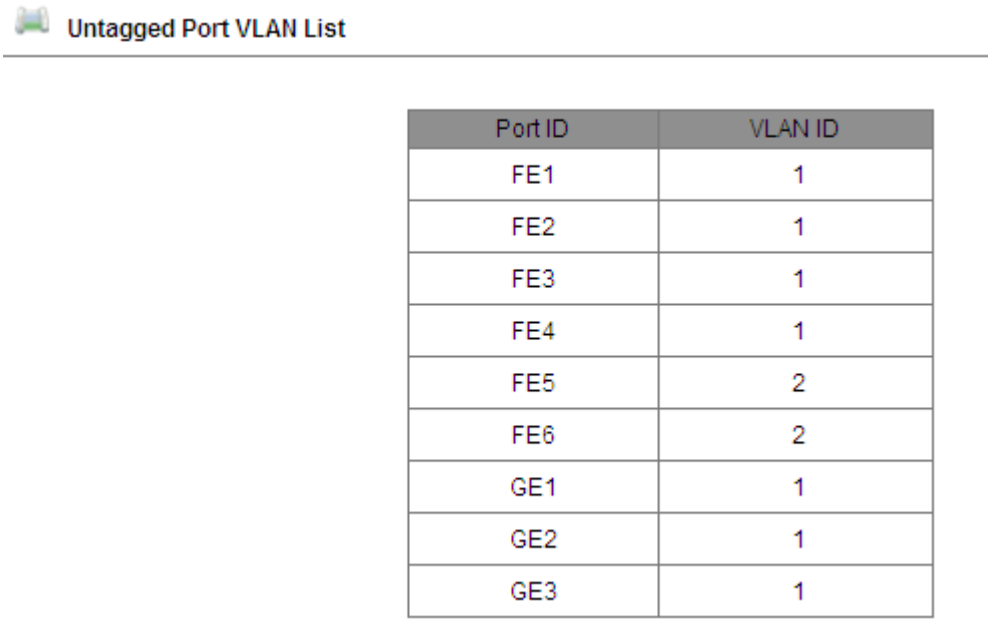

Figure 31 Port PVID List

Caution:

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

4. Modify/Delete VLAN.

Click a VLAN in Figure 30 to enter the corresponding screen in which the VLAN can be deleted or modified. Click <Delete> to delete the selected VLAN, as shown in Figure 32.

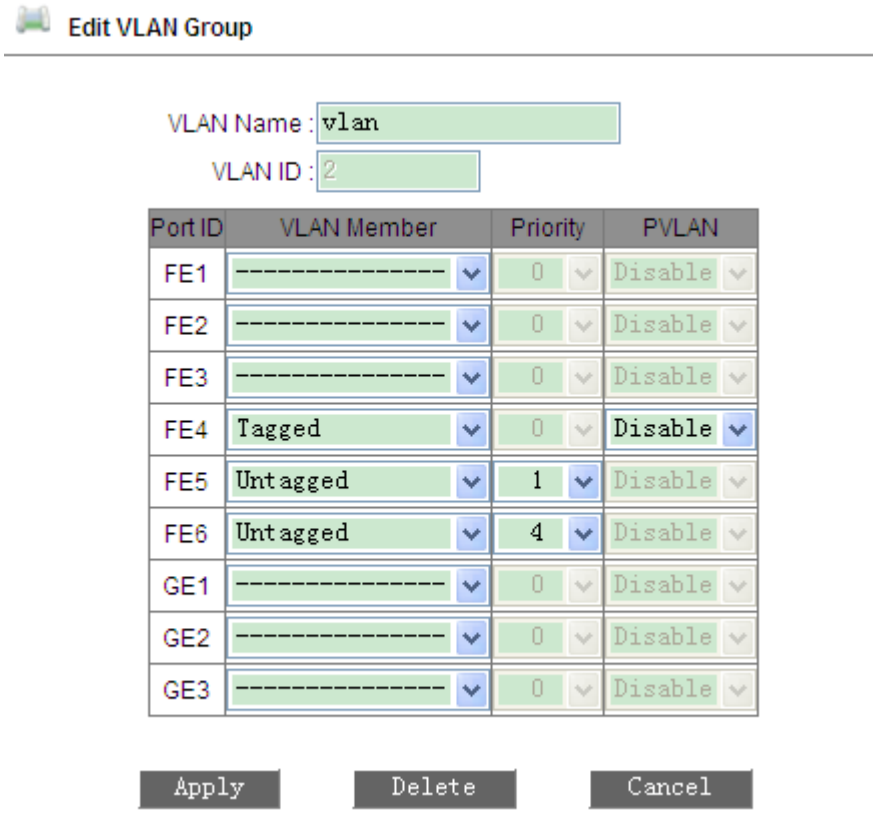

Figure 32 Modifying/Deleting a VLAN

6.2.5 Typical Configuration Example

As shown in Figure 33, 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 6 shows specific configuration.

Table 6 VLAN Configuration

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

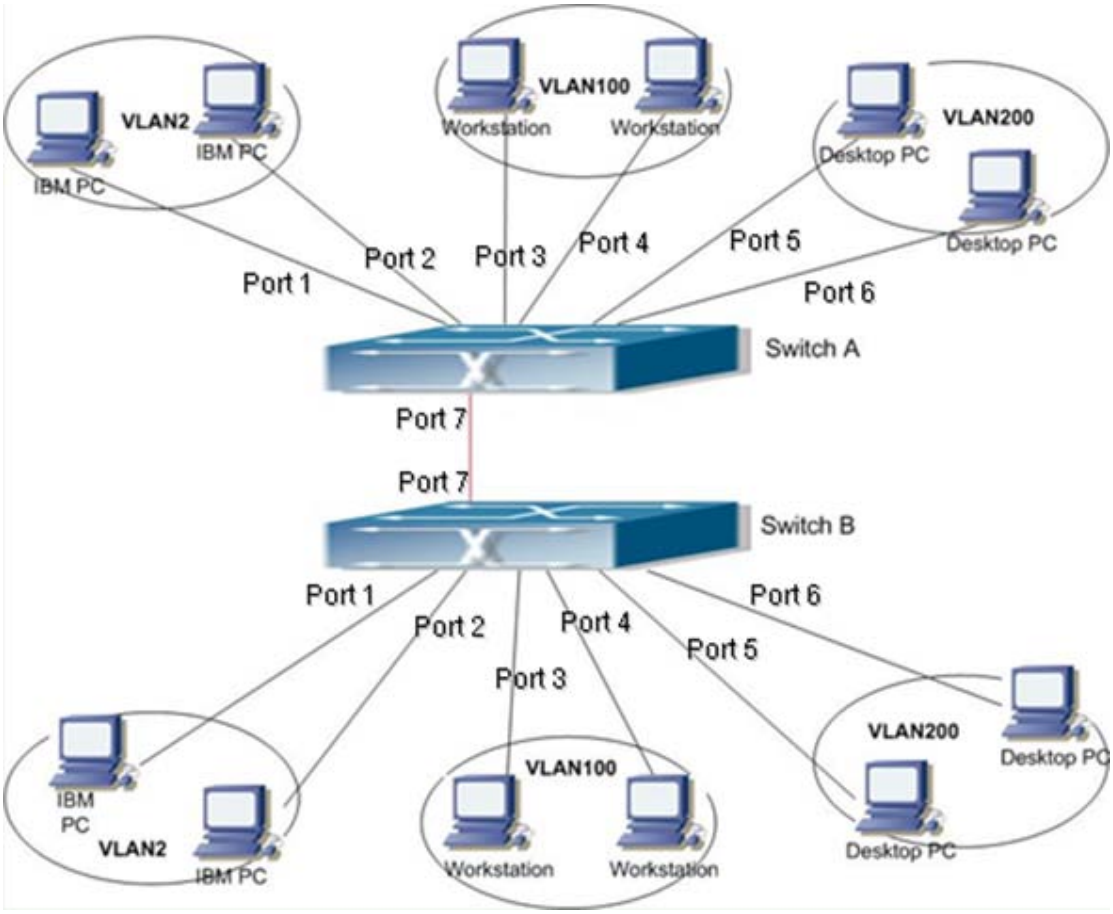

Figure 33 VLAN Application

Configurations on Switch A and Switch B:

1. Create VLAN 2, add port 1 and port 2 into VLAN 2 as Untag ports, and add port 7 into VLAN 2 as Tag port, as shown in Figure 29.
2. Create VLAN 100, add port 3 and port 4 into VLAN 100 as Untag ports, and add port 7 into VLAN 100 as Tag port, as shown in Figure 29.

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 29.

6.3 PVLAN Configuration

6.3.1 Overview

PVLAN (Private VLAN) 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.

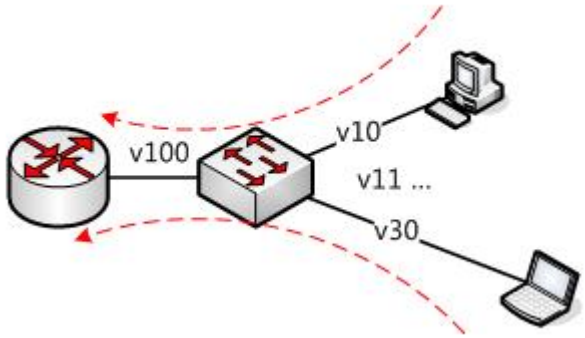

Figure 34 PVLAN Application

As shown in Figure 34, 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 to each other, such as VLAN 10 cannot communicate with VLAN 30.

Caution:

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 function on port, as shown in Figure 35.

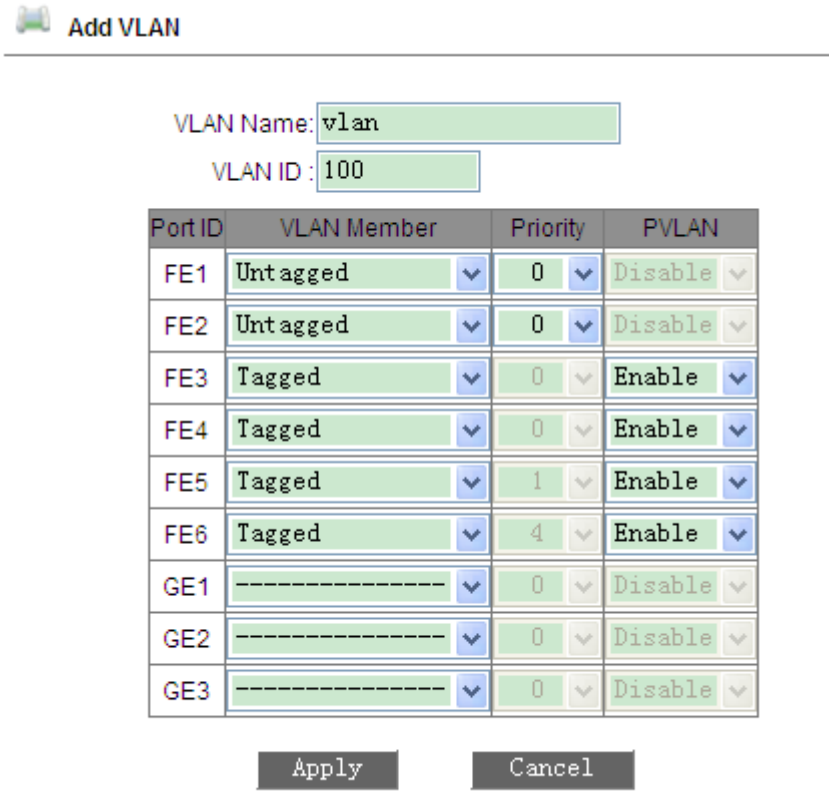

Figure 35 Enabling PVLAN

In VLAN configuration interface, Tag ports can enable PVLAN function.

If the VLAN is a shared domain, the uplink port should be set to untagged, and the downlink port should be set to tagged.

If the VLAN is an isolation domain, the downlink port should be set to untagged, and the uplink port should be set to tagged.

2. Select VLAN members for PVLAN, as shown in Figure 36.

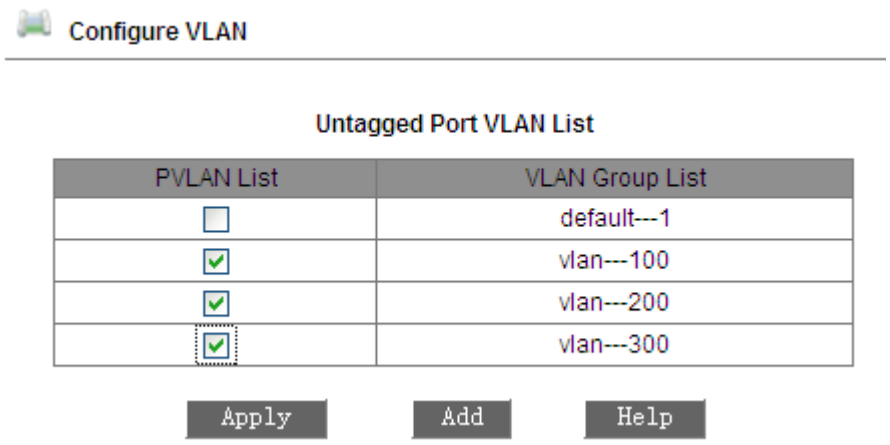

Figure 36 PVLAN Member Configuration

PVLAN List

Options: Select or Deselect

Default: Deselect

Function: Select members for PVLAN.

6.3.3 Typical Configuration Example

Figure 37 shows 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.

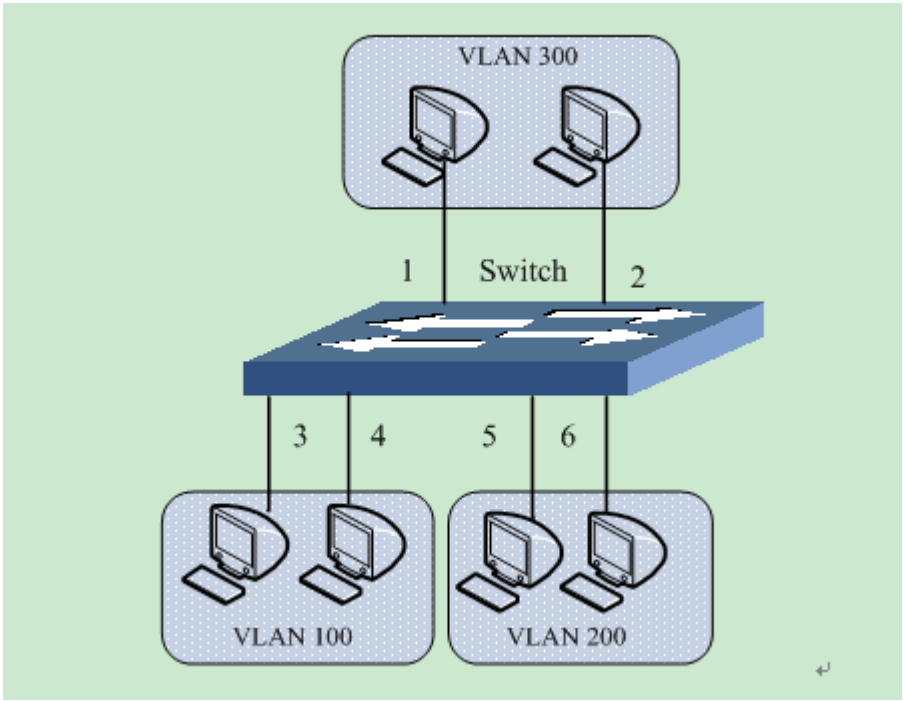

Figure 37 PVLAN Configuration Example

Switch Configuration:

1. Configure the shared domain, VLAN 300, as shown in Figure 35.

   Port 1 and port 2 are set to Untagged and are assigned to the shared domain of VLAN 300;

   Port 3 and port 4 are set to Tagged and are assigned to the shared domain of VLAN 300, and enable PVLAN;

   Port 5 and port 6 are set to Tagged and are assigned to the shared domain of VLAN 300, and enable PVLAN;

2. Configure VLAN 100, the isolation domain, as shown in Figure 35.

   Port 1 and port 2 are set to Tagged and are assigned to the isolation domain of VLAN 100, and enable PVLAN;

   Port 3 and port 4 are set to Untag ports and are assigned to the isolation domain of VLAN 100.

3. Configure VLAN 200, the isolation domain, as shown in Figure 35.

   Port 1 and port 2 are set to Tagged and are assigned to the isolation domain of VLAN 200, and enable PVLAN;

   Port 5 and port 6 are set to Untagged and are assigned to the isolation domain of VLAN 200.

4. Set VLAN300, VLAN100 and VLAN200 to PVLAN members, as shown in Figure 35.

6.4 Port Mirroring

6.4.1 Overview

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

6.4.2 Explanation

A switch supports only one mirroring destination port, but there is no such restriction on mirroring source ports and it supports one or multiple source ports.

Multiple source ports can be in the same VLAN, or in different VLANs. Mirroring source port and destination port can be in the same VLAN or in different VLANs.

Source port and destination port cannot be the same port.

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 38.

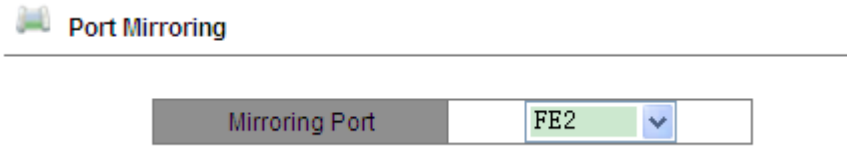

Figure 38 Selecting a Mirroring Port

Monitoring Port

Options: Disable/A switch port

Default: Disable

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

2. Select mirroring source ports and the mirroring mode, as shown in Figure 39.

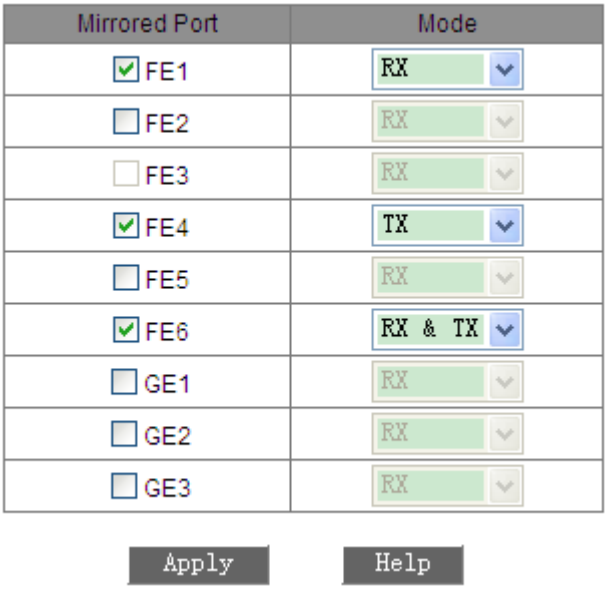

Figure 39 Mirroring Source Port

Mode

Options: RX/TX/RX&TX

Function: Select the data to be mirrored.

TX mirrors only the transmitted packets of the source port.

RX mirrors only the received packets of the source port.

TX&RX mirrors all packets of the source port.

6.4.4 Typical Configuration Example

As shown in Figure 40, the mirroring destination port is port 2 and the mirroring source port is port 1. All packets on port 1 are mirrored to port 2.

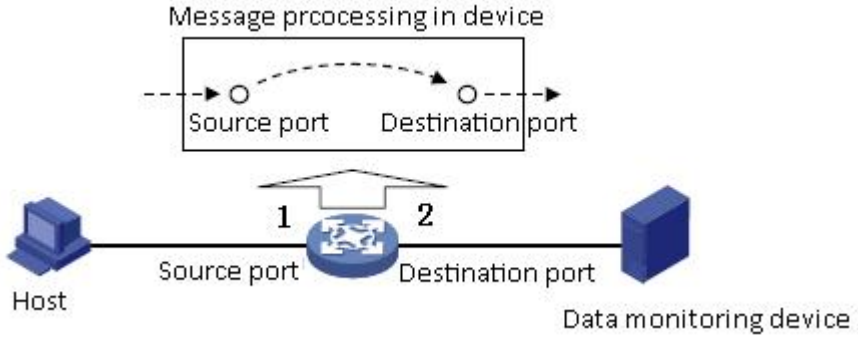

Figure 40 Port Mirroring Example

Configuration process:

1.Set port 2 to the mirroring destination port, as shown in Figure 38.

2.Set port 1 to the mirroring source port and the port mirroring mode is set to RX&TX, as shown in Figure 39.

6.5 Link Check

6.5.1 Overview

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

6.5.2 Web Configuration

Figure 41 shows the link check configuration.

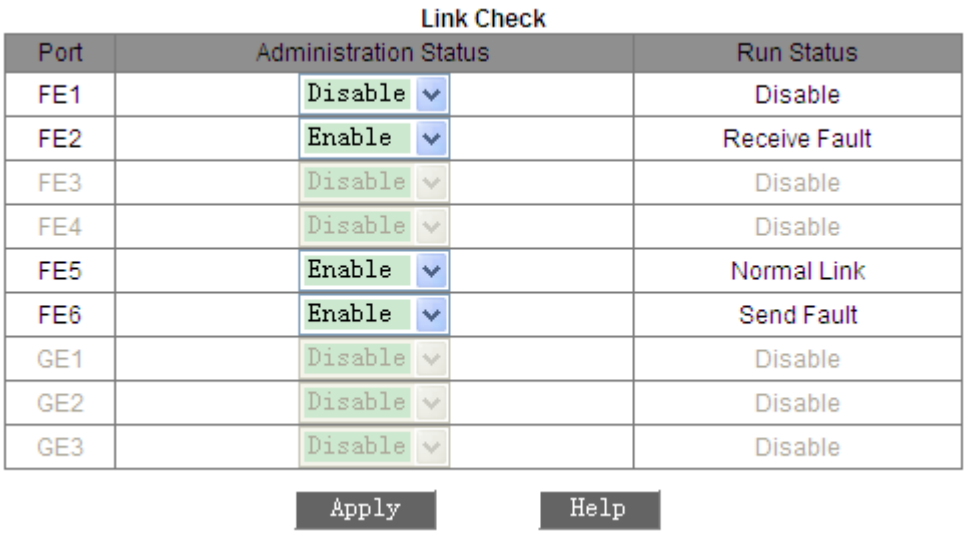

Figure 41 Link Check Configuration

Administration Status

Options: Enable/Disable

Default: Enable

Description: only the redundancy protocol-enabled port can enable this

function

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.

Caution:

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

6.6 Port Trunk

6.6.1 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.

6.6.2 Implementation

As shown in Figure 42, three ports in Switch A aggregate to a trunk group and the bandwidth of the trunk group is the total bandwidth of three ports.

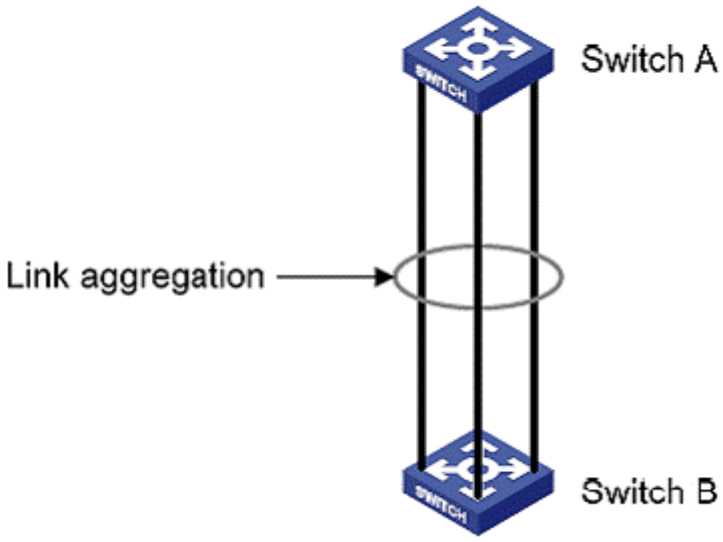

Figure 42 Port Trunk

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.

6.6.3 Explanation

Port trunk and the following port operations are mutually exclusive:

- Port trunk is mutually exlusive 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.

- Add a trunk member port to a static multicast entry.
- Configure a port added to a static entry as a trunk member port.

Caution:

- Gigabit ports of the series switches do not support port trunk.
- A port can be added to only one trunk group.
- Ports added to one trunk group must belong to one VLAN and have the same attributes.

6.6.4 Web Configuration

1. Add Port Trunk, as shown in Figure 43. Click <Add>.

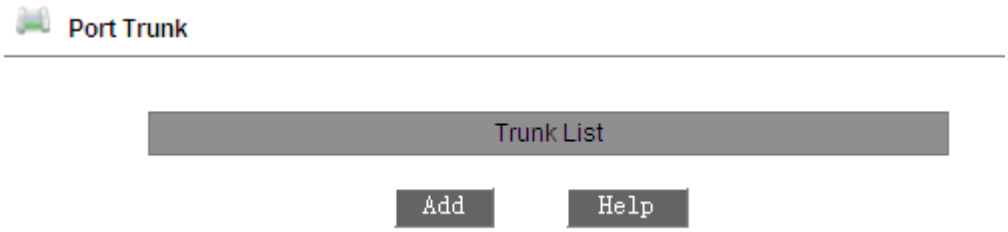

Figure 43 Configuring Port Trunk

2. Configure Port Trunk, as shown in Figure 44.

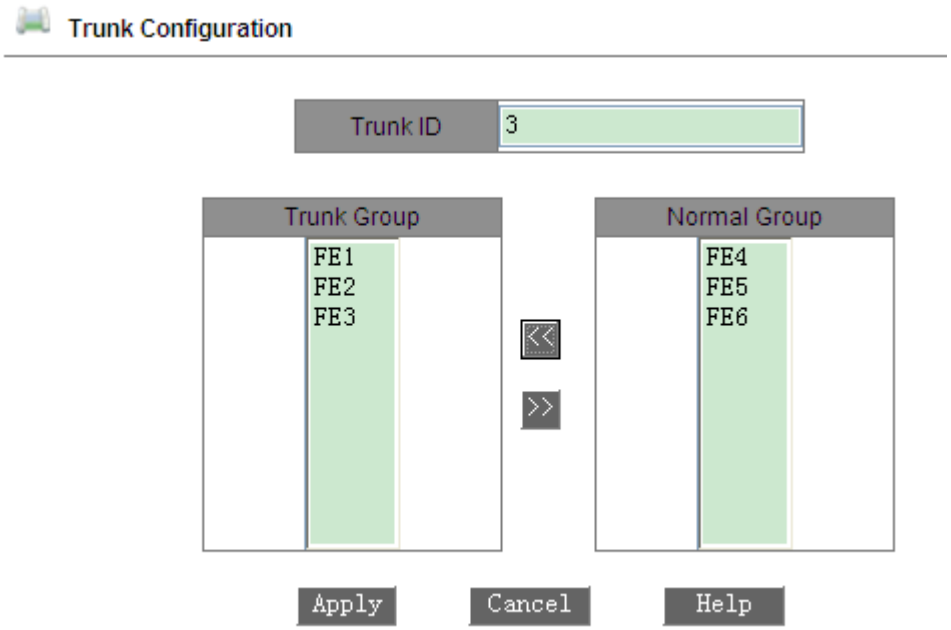

Figure 44 Port Trunk Configuration

Trunk ID

Configuration range: 1 to 16

Function: Set the trunk group ID.

Description: The series switches support max 16 trunk groups and each trunk group supports max four member ports.

3. View trunk group list, as shown in Figure 45.

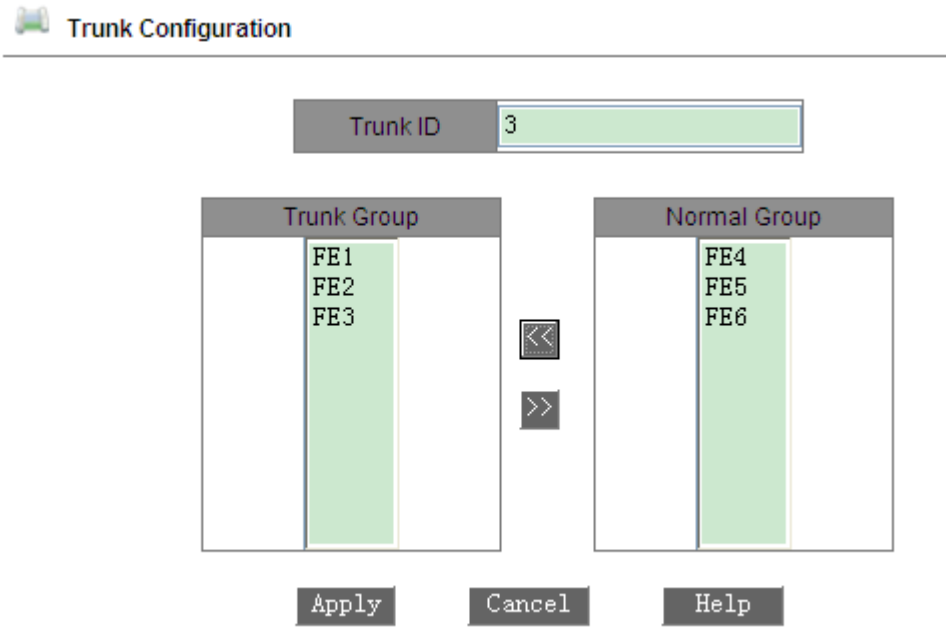

Figure 45 Trunk Group List

Click a trunk group in Figure 45. You can view the members of the group, modify group settings, or delete the group, as shown in Figure 46.

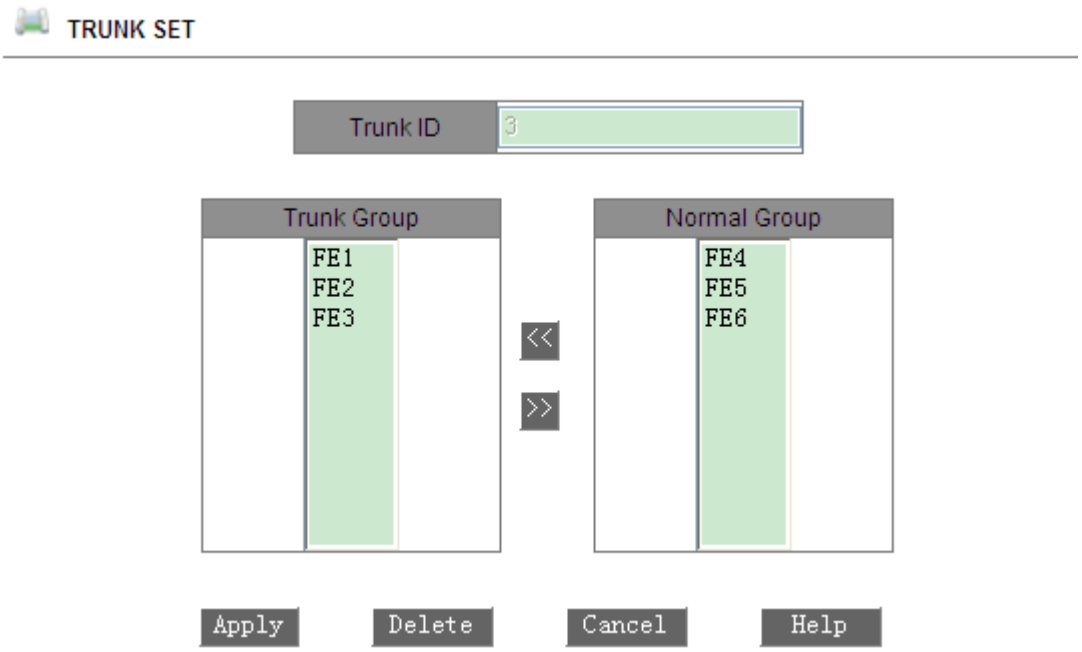

Figure 46 Details about the Trunk Group

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.

6.6.5 Typical Configuration Example

As shown in Figure 42, port 1, port 2, and port 3 of Switch A are connected to those of Switch B respectively, forming trunk group 3 to achieve load balancing among ports.

Configuration on switches:

1. Add trunk group 3 on Switch A and add port 1, port 2, and port 3 to the group, as shown in Figure 44.
2. Add trunk group 3 on Switch B and add port 1, port 2, and port 3 to the group, as shown in Figure 44.

6.7 Static Multicast Address Table

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, 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 47.

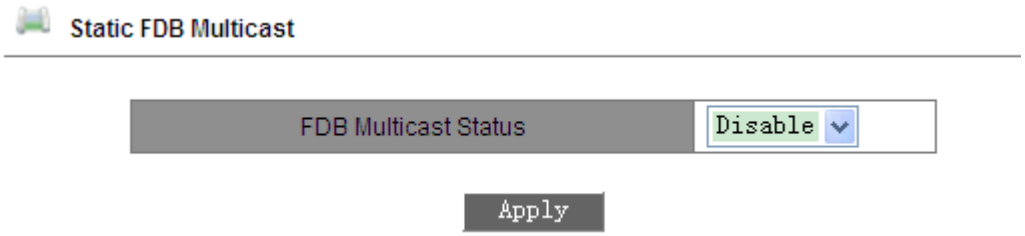

Figure 47 Enabling Static Multicast

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 48.

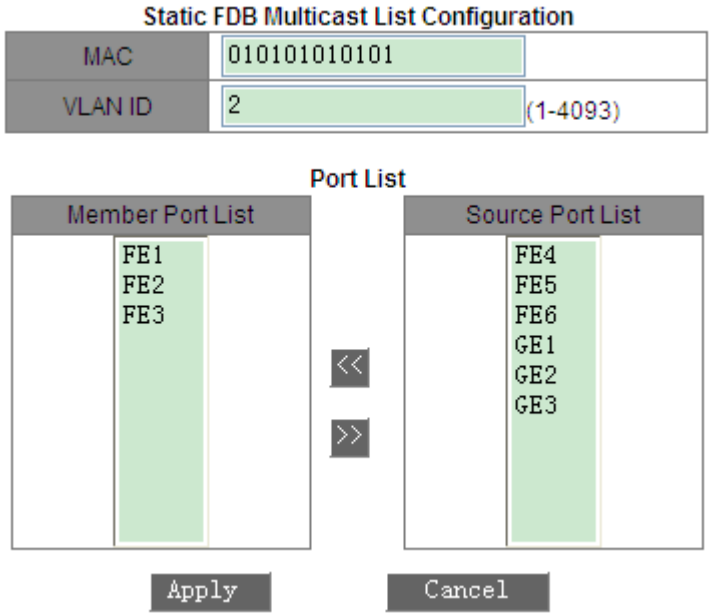

Figure 48 Adding a Static Multicast Entry

MAC

Combination: 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 49.

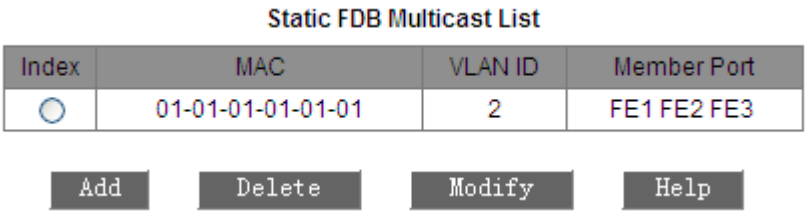

Figure 49 Operations on a Static Multicast Entry

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 Basic 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 Principles

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 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 50.

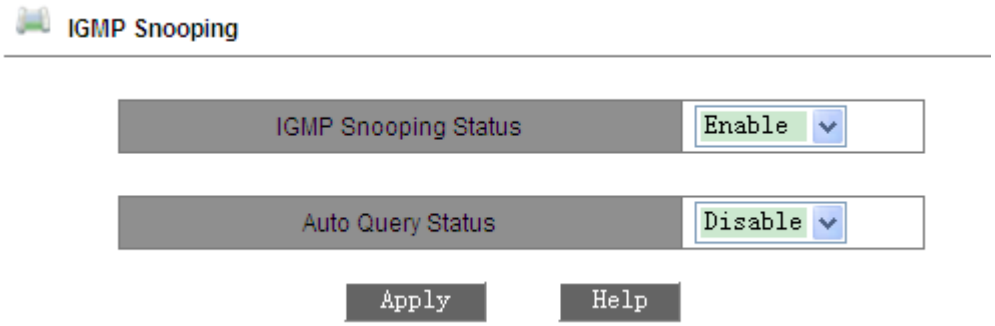

Figure 50 Enabling IGMP Snooping

IGMP Snooping Status

Options: Enable/Disable

Default: Disable

Function: Enable or disable IGMP Snooping. IGMP Snooping and static multicast 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:

On a network, the auto query function shall be enabled on one switch at least.

2. View the multicast member list, as shown in Figure 51.

IGMP Member List

MAC	VLAN ID	Member
01-00-5E-7F-FF-FE	1	FE6
01-00-5E-00-01-01	1	FE6
01-00-5E-51-09-08	1	FE4 FE6
01-00-5E-7F-FF-FA	1	FE4 FE6
01-00-5E-0A-18-03	1	FE4 FE6

Figure 51 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 52, 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.

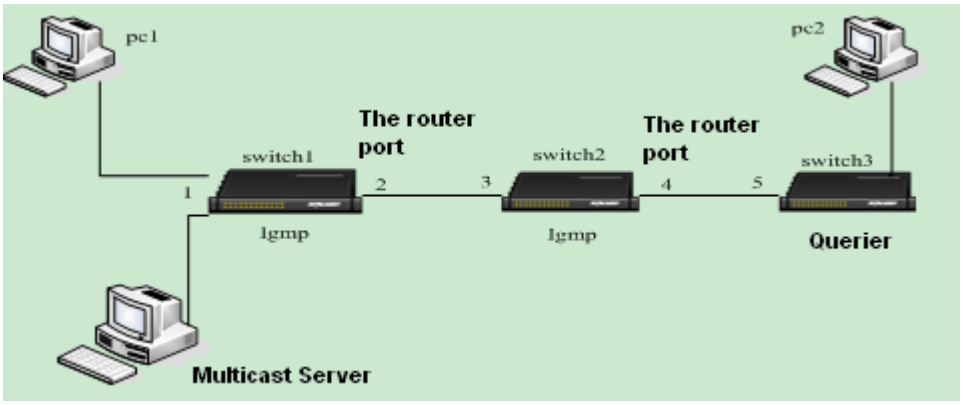

Figure 52 IGMP Snooping Configuration Example

- As the querier, Switch 3 periodically sends general query packets. Port 4 of Switch 2 receives the packets and is thus elected as the routing port. Meanwhile, 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. Meanwhile, 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 ARP Configuration

6.9.1 Overview

The Address Resolution Protocol 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.

This series switches provide 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.

6.9.2 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 age out, be updated by a new ARP packet, or be overwritten by a static ARP entry.

Static entries are manually configured and maintained. They never age out 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 ones.

6.9.3 Web Configuration

1. Configure ARP aging time, as shown in Figure 53.

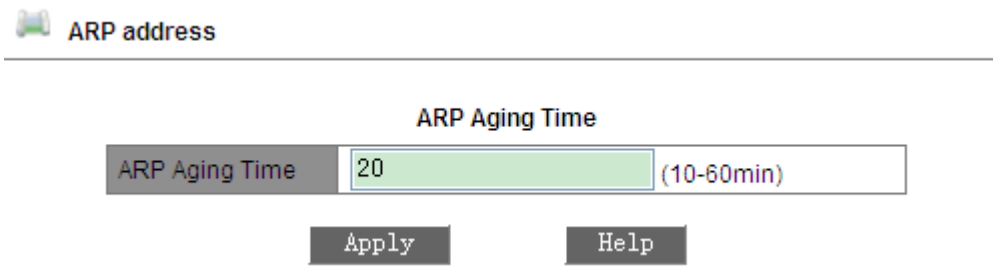

Figure 53 Configuring Aging Time

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 54.

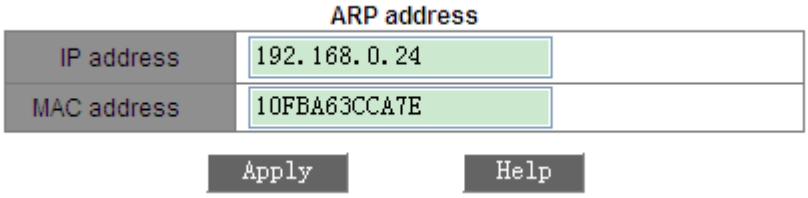

Figure 54 Adding a Static ARP Entry

ARP address

Combination: {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 55.

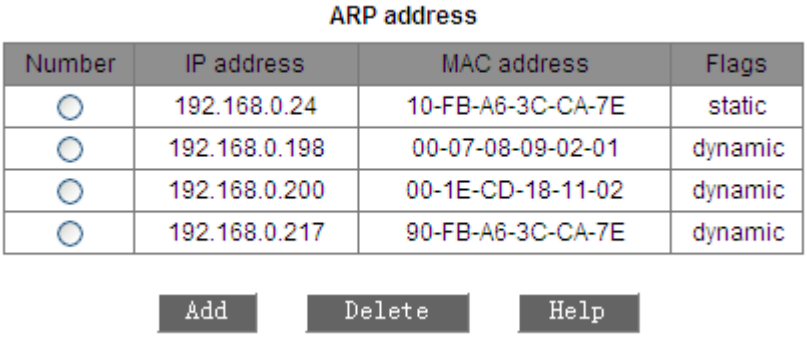

Figure 55 ARP Address

ARP Address

Combination: {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.

6.10 RSTP Configuration

6.10.1 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 in no time.

6.10.2 Basic 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.

6.10.3 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 7 shows the data structure of a BPDU.

Table 7 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).

6.10.4 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, the port does not perform any operation.
   - If the priority of the received BPDU is higher, 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, 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, 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, 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.

6.10.5 Web Configuration

1. Enable STP/RSTP, as shown in Figure 56.

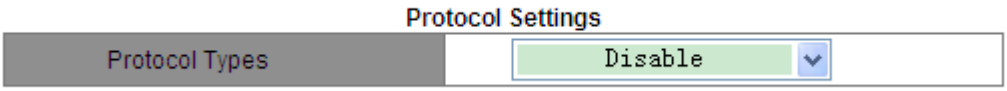

Figure 56 Enabling RSTP/STP

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 57.

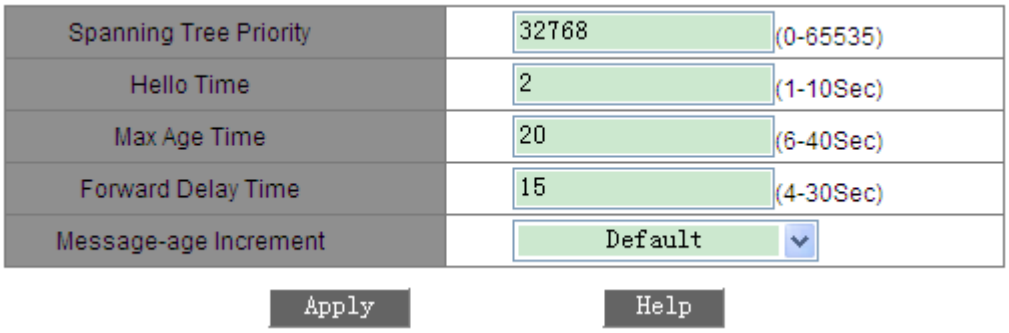

Figure 57 Setting Time Parameters of the Network Bridge

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: 6~40s

Default: 20s

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

Forward Delay Time

Range: 4~30s

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 58.

Port Settings

Port	Protocol Status	Port Priority(0~255)	Path Cost(1~200000000)	Cost Count
FE1	Enable	128	2000000	Yes
FE2	Enable	128	2000000	No
FE3	Enable	128	2000000	Yes
FE4	Enable	128	2000000	No
FE5	Disable	128	2000000	Yes
FE6	Disable	128	2000000	Yes
GE1	Disable	128	20000	Yes
GE2	Disable	128	20000	Yes
GE3	Disable	128	20000	Yes

Apply Help

Figure 58 Port Settings

Protocol Status

Options: Enable/Disable

Default: Disable

Function: Enable or disable STP on ports.

Caution:

- Port mirroring and STP are mutually exclusive. STP cannot be enabled on a mirroring or mirrored port. An STP-enabled port cannot be configured as a mirroring or mirrored port.
- Port Trunk and STP are mutually exclusive. STP cannot be enabled on a port added to a trunk group. An STP-enabled port cannot be added to a trunk group.

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 this 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.

6.10.6 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 59.

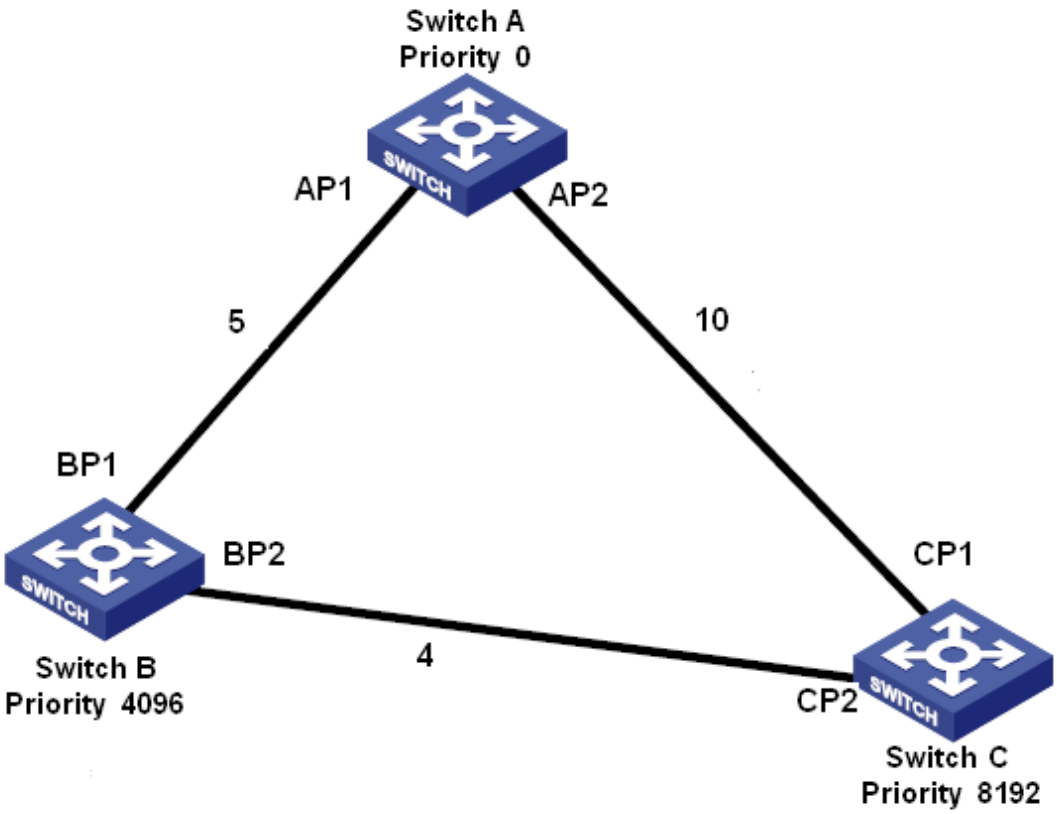

Figure 59 RSTP Configuration Example

Configuration on Switch A:

1. Set priority to 0 and time parameters to default values, as shown in Figure 57.
2. Set the path cost of port 1 to 5 and that of port 2 to 10, as shown in Figure 58.

Configuration on Switch B:

1.Set priority to 4096 and time parameters to default values, as shown in Figure 57.

2.Set the path cost of port 1 to 5 and that of port 2 to 4, as shown in Figure 58.

Configuration on Switch C:

1.Set priority to 8192 and time parameters to default values, as shown in Figure 57.

2.Set the path cost of port 1 to 10 and that of port 2 to 4, as shown in Figure

58.

- 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.

6.11 RSTP Transparent Transmission

6.11.1 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 the problem, Kyland develops the RSTP transparent transmission function. The function enables the switch to keep other redundant protocols while transparently transmit 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 60, 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.

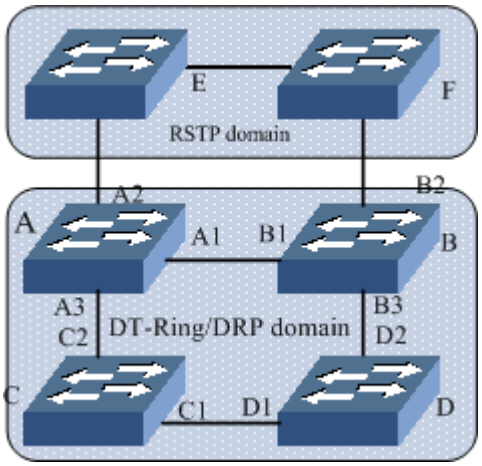

Figure 60 RSTP Transparent Transmission

6.11.2 Web Configuration

Configure RSTP transparent transmission on ports, as shown in Figure 61.

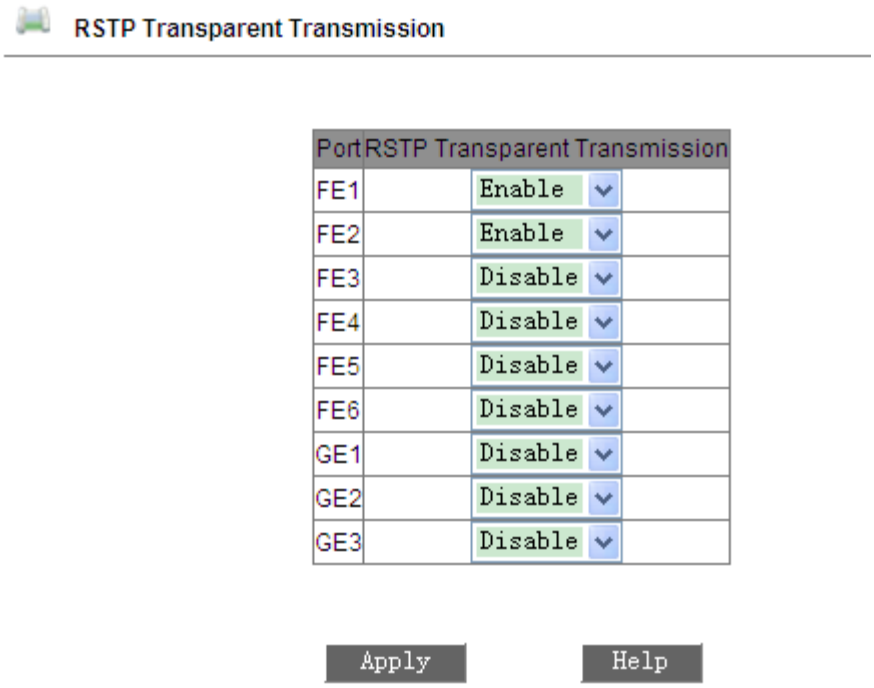

Figure 61 RSTP Transparent Transmission Configuration

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.

6.11.3 Typical Configuration Example

As shown in Figure 60, 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 56 and Figure 58.
- Enable RSTP transparent transmission on ports A1, A2, A3, B1, B2, B3, C1, C2, D1, and D2, as shown in Figure 61.

6.12 DT-Ring Configuration

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.

6.12.2 Basic Concepts

- Master station: One ring has only one master station. The master station forwards 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 a ring has two backup ports, the backup port with the larger MAC address is the master backup port. It is in forwarding state.
- Slave backup port: When a ring has two backup ports, the backup port with the smaller MAC address is the slave backup port. It is in blocking state.
- Forwarding state: If a port is in forwarding state, the port can both receive and forward data.
- Blocking state: If a port is in blocking state, the port can receive and forward only DT-Ring packets, but not other packets.

6.12.3 Implementation

1. Implementation of DT-Ring

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 forwarding state, the slave port in blocking state, and all ring ports of slave stations are in 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 have only 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.

As shown in Figure 62, the working process of Switch A, B, C, and D is as follows:

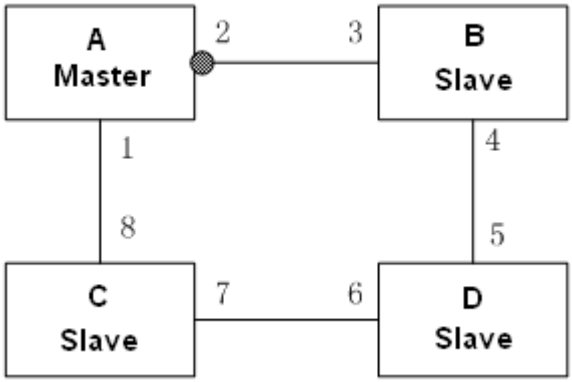

Figure 62 DT-Ring Topology

1) Configure Switch A as the master station and the other switches as salve stations.
2) Port 1, the first port whose link status changes to up on the master station is in forwarding state. Port 2 is in blocking state. The ring ports of the slave station are in forwarding state.
3) When link CD fails, the status of port 2 changes to forwarding, and the

status of port 6 and port 7 change to blocking, as shown in Figure 63.

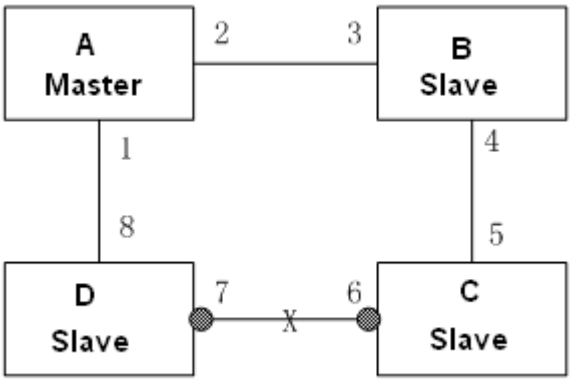

Figure 63 DT-Ring Link Fault

Caution:

Link status change affects the role and status of ring ports.

2. Implementation of DT-Ring+

DT-Ring+ can provide backup for two DT rings, as shown in Figure 64. 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.

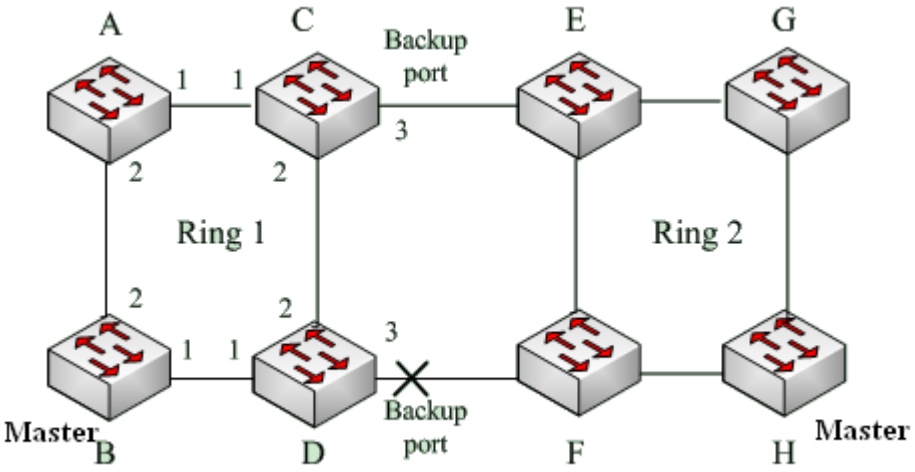

Figure 64 DT-Ring+ Topology

Caution:

Link status change affects the status of backup ports.

6.12.4 Web Configuration

1. Configure ring status detection, as shown in Figure 65.

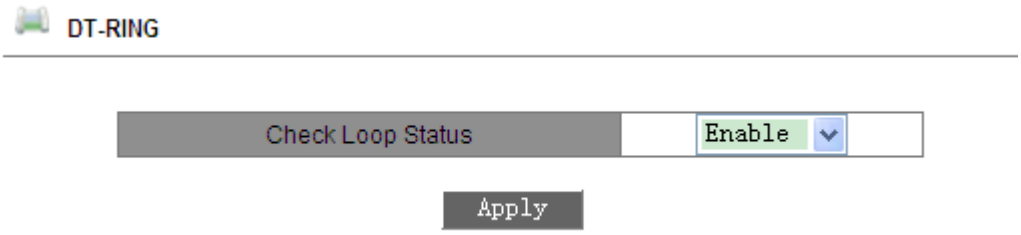

Figure 65 Configuring Ring Status Detection

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 and configure a DT ring, as shown in Figure 66. Click <Add>. The DT-RING configuration page is displayed, as shown in Figure 67.

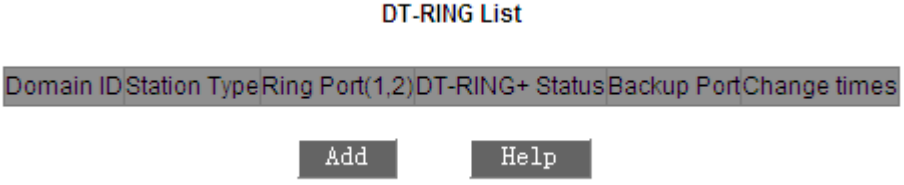

Figure 66 Creating a DT Ring

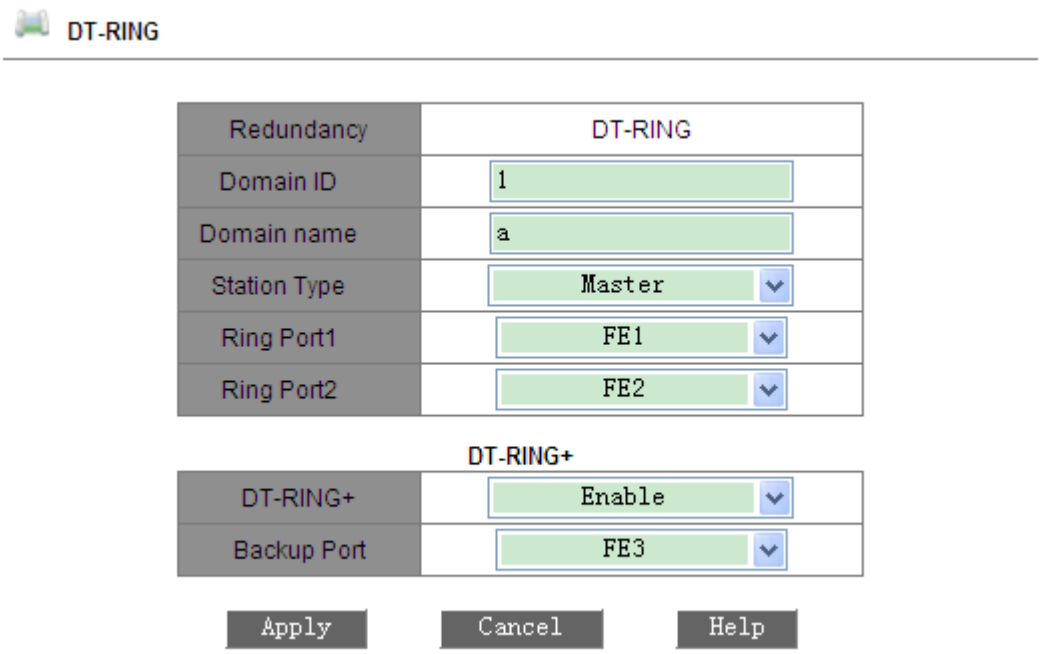

Figure 67 DT-Ring Configuration

Redundancy

Forcible configuration: DT-RING

Domain ID

Range: 1~32

Function: The domain ID is used to differentiate rings.

Domain name

Range: 1~31 characters

Function: Configure the domain name.

Station Type

Options: Master/Slave

Default: Master

Function: Select the role of the switch in the current ring.

Ring Port1/Ring Port2

Options: All ports of the switch

Function: Select two ring ports.

Caution:

Port trunk and ring are mutually exclusive. The ports added to a trunk group cannot be configured as a ring port, and a ring port cannot be added to a trunk group.

DT-Ring+

Options: Enable/Disable

Default: Disable

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

Backup Port

Options: All ports of the switch

Function: Select one port as the backup port.

Description: You can configure a backup port only after the DT-Ring+ function is enabled.

After the configurations are completed, created rings are listed in the DT-RING List, as shown in Figure 68.

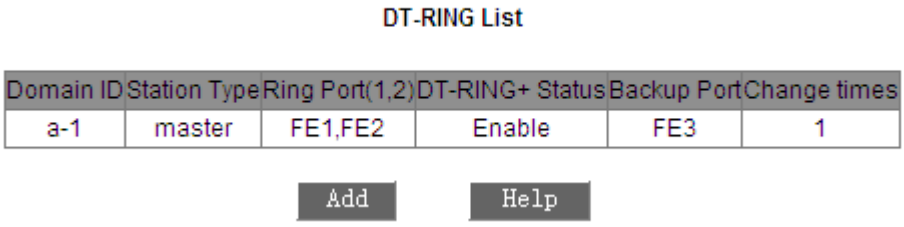

Figure 68 DT Ring List

3. View and modify DT-Ring configuration.

Click the DT-Ring options in Figure 68. You can view and modify the configurations of the ring, as shown in Figure 69.

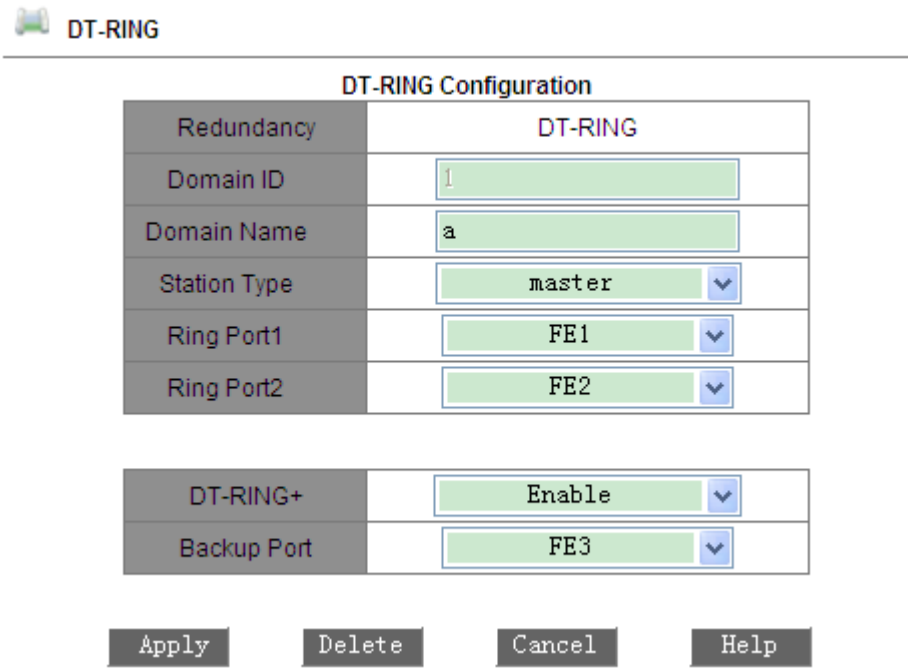

Figure 69 Viewing and Modifying DT Ring Configuration

After modification is completed, click <Apply> to make the modification take effect. You can delete the DT-Ring configuration entry by clicking <Delete>.

4. View the status of DT-Ring and ports, as shown in Figure 70.

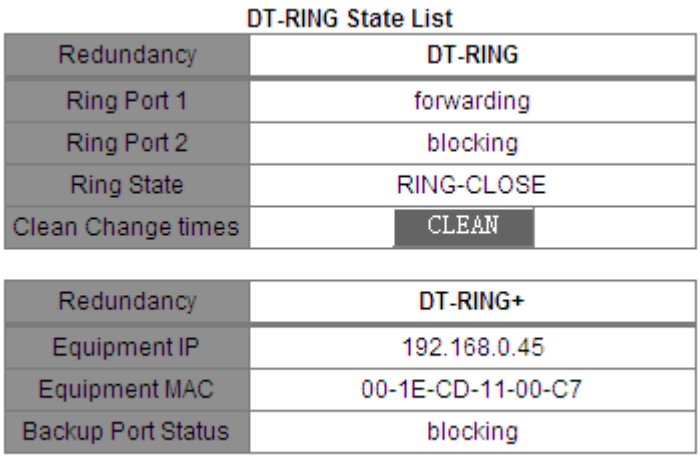

Figure 70 Viewing DT Ring State

6.12.5 Typical Configuration Example

As shown in Figure 64, A, B, C, and D form Ring 1; E, F, G, and H form Ring 2; CE and DF are the backup links of Ring 1 and Ring 2.

Configuration on switch A:

1. Domain ID: 1; Domain name: Ring; Station Type: Slave; Ring Port 1 and 2; DT-Ring+: Disable; Backup Port: none, as shown in Figure 67.

Configuration on switch B:

2. Domain ID: 1; Domain name: Ring; Station Type: Master; Ring Port 1 and 2; DT-Ring+: Disable; Backup Port: none, as shown in Figure 67.

Configuration on switch C and switch D:

3. Domain ID: 1; Domain name: Ring; Station Type: Slave; Ring Port 1 and 2; DT-Ring+: Enable; Backup Port: 3, as shown in Figure 67.

Configuration on switch E and switch F:

4. Domain ID: 2; Domain name: Ring; Station Type: Slave; Ring Port 1 and 2; DT-Ring+: Disable; Backup Port: none, as shown in Figure 67.

Configuration on switch G:

5. Domain ID: 2; Domain name: Ring; Station Type: Slave; Ring Port 1 and 2; DT-Ring+: Disable; Backup Port: none, as shown in Figure 67.

Configuration on switch H:

6. Domain ID: 2; Domain name: Ring; Station Type: Master; Ring Port 1 and 2; DT-Ring+: Disable; Backup Port: none, as shown in Figure 67.

6.13 QoS Configuration

6.13.1 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.

6.13.2 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 two queue mapping modes for priority identification: TOS/DIFF and 802.1p.

- 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 STRICT Priority

Scheduling (STRICT).

- 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.
- STRICT 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.

6.13.3 Web Configuration

1. Configure QoS Mode, as shown in Figure 71.

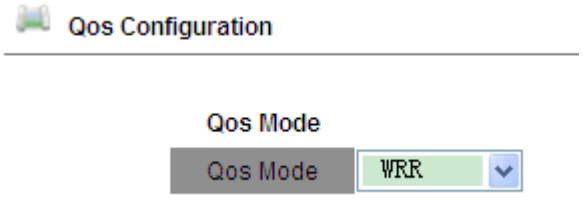

Figure 71 QoS Mode

Options: Disable/WRR/STRICT

Default: STRICT

Function: Configure the bandwidth allocation mode of a port.

Description: If STRICT is selected, the data of high-priority queues is processed preferentially. If WRR is adopted, different queues have varied weight configurations. The switch employs fixed weight ratio, that is, 8:4:2:1 for queues 3, 2, 1, and 0.

2. Configure QoS port priority mapping mode, as shown in Figure 72.

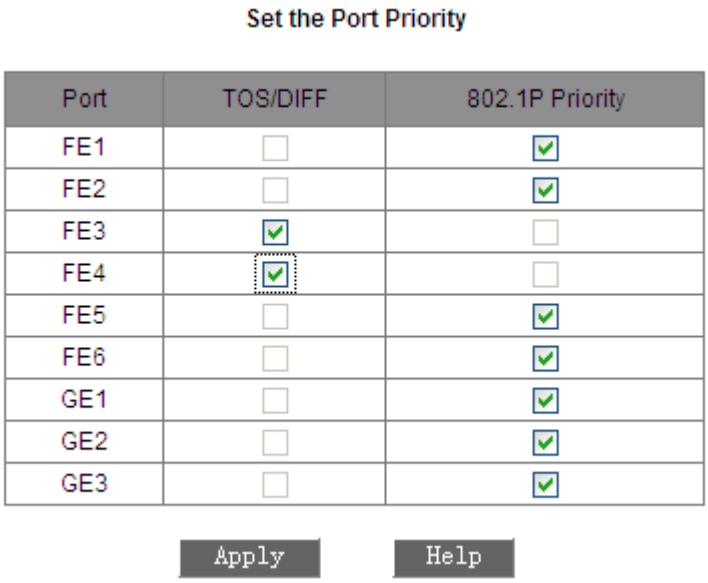

Figure 72 Setting QoS Port Priority Mapping Mode

Set the Port Priority

Options: TOS/DIFF or 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.

3. Configure 802.1p priority-queue mapping, as shown in Figure 73.

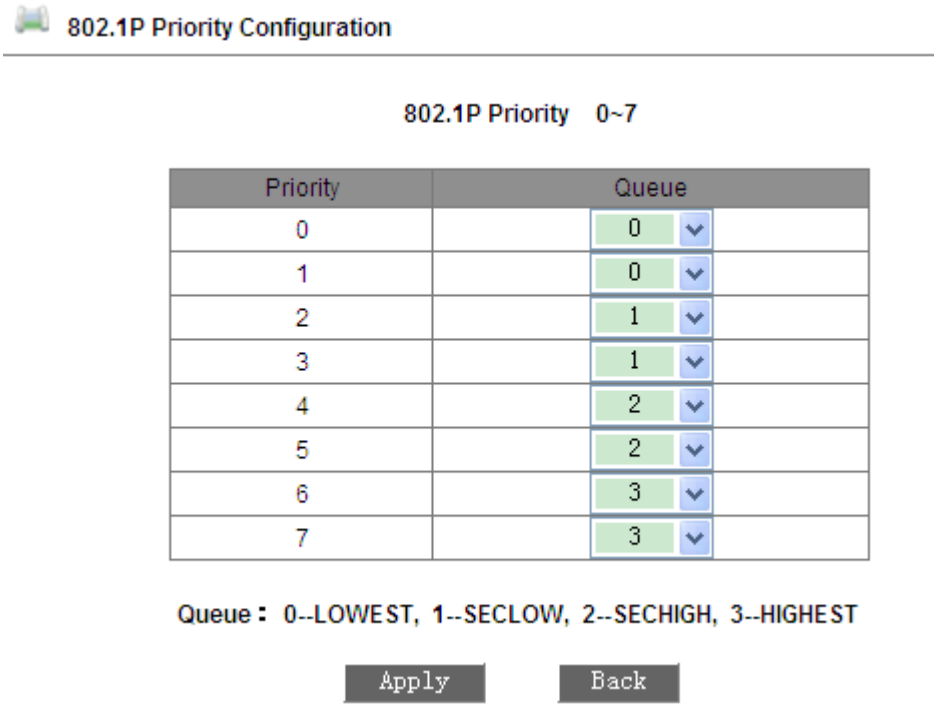

Figure 73 802.1p Priority-Queue Mapping

802.1p Priority Configuration

Combination: {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.

4. Configure DSCP priority-queue mapping, as shown in Figure 74.

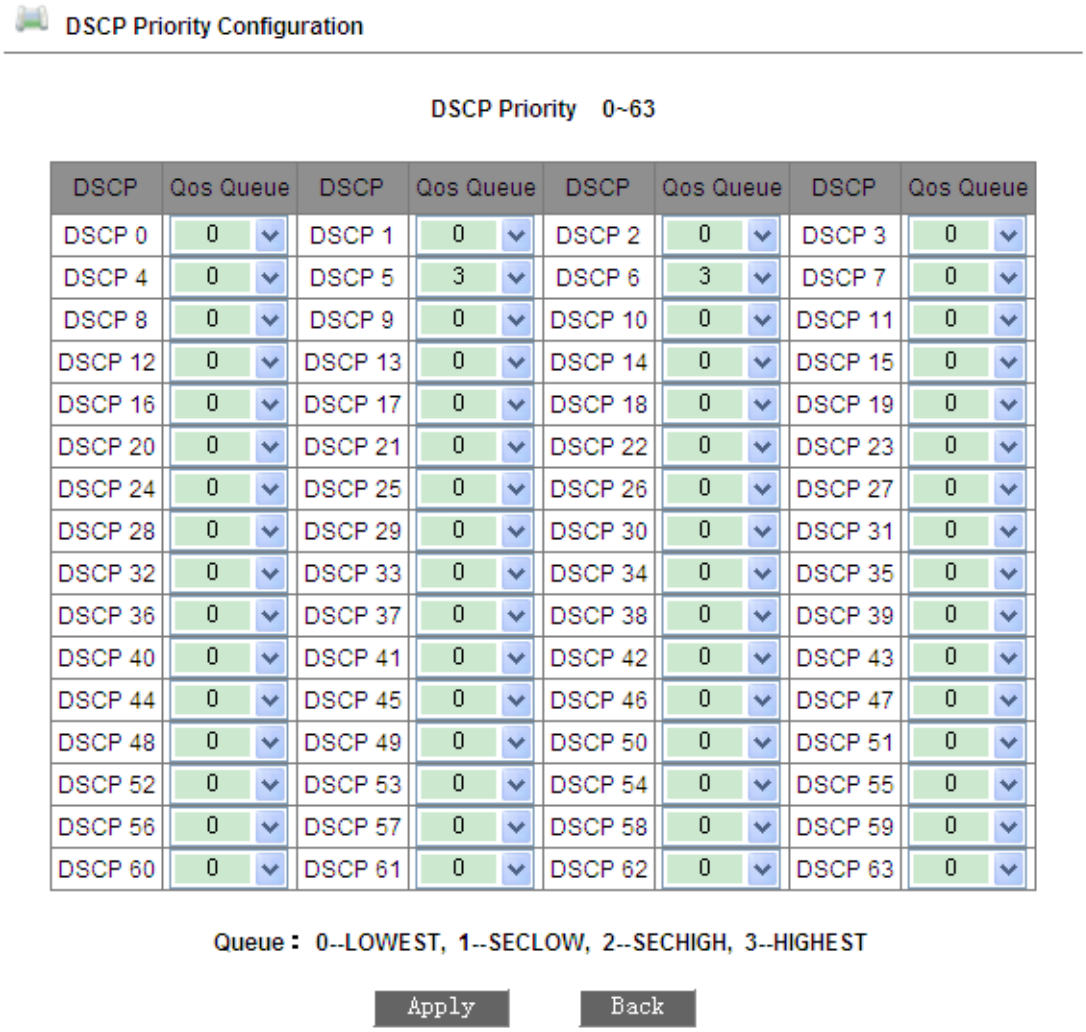

Figure 74 DSCP Priority-Queue Mapping

DSCP Priority Configuration

Combination: {DSCP, QoS Queue}

Range: {0~63, 0~3}

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

Function: Configure the mapping between DSCP priority and queue.

6.13.4 Typical Configuration Example

As shown in Figure 75, port 1 to port 4 forward packets to port 5. The 802.1p priority carried by packets from port 1 is 3, which is mapped to queue 1. The 802.1p priority carried by packets from port 2 is 4, which is mapped to queue 2. The DSCP priority carried by packets from port 3 is 5, which is mapped to queue 3. 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. Configure 802.1p for the incoming packets of port 1 and port 2, and TOS/DIFF for the incoming packets of port 3 and port 4, as shown in Figure 72.
2. Configure WRR for the outgoing packets of port 5, as shown in Figure 71.
3. Configure 802.1p priority 3 and 4 to map to queue 1 and queue 2 respectively, as shown in Figure 73.
4. Configure 802.1p priority 3 and 4 to map to queue 3, as shown in Figure 74.

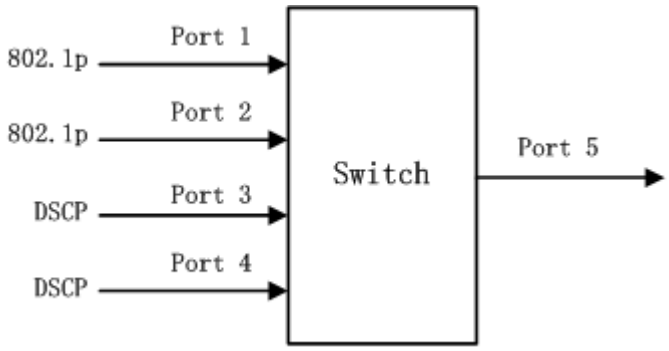

Figure 75 QoS Configuration Example

Packets received through port 3 and port 4 are put into queue 3; packets received through port 1 are put into queue 1; packets received through port 2 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 3 and port 4 are put into queue 3 and forwarded according to the FIFO mechanism. The total bandwidth ratio of port 3 and port 4 is 8/(2+4+8).

6.14 MAC Aging Time

6.14.1 Overview

Ports of the switch 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, 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.

6.14.2 Web Configuration

Configure MAC address aging time, as shown in Figure 76.

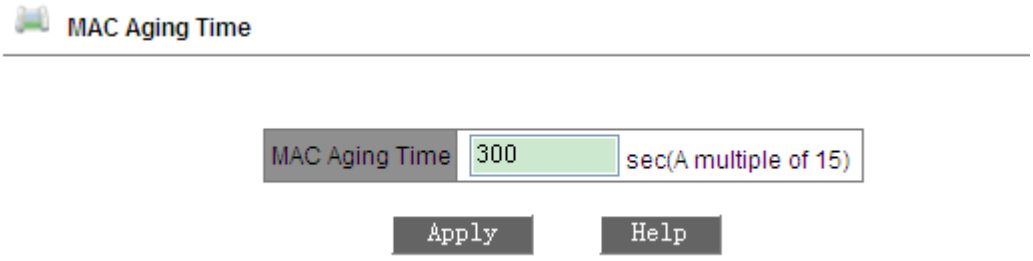

Figure 76 MAC Address Aging Time

MAC Aging Time

Range: 15~3600 seconds

Default: 300 seconds

Description: The value must be a multiple of 15.You can adjust the aging time as required.

6.15 LLDP

6.15.1 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 these information to MIB for query and link status check by the NMS.

6.15.2 Web Configuration

View LLDP connection information, as shown in Figure 77.

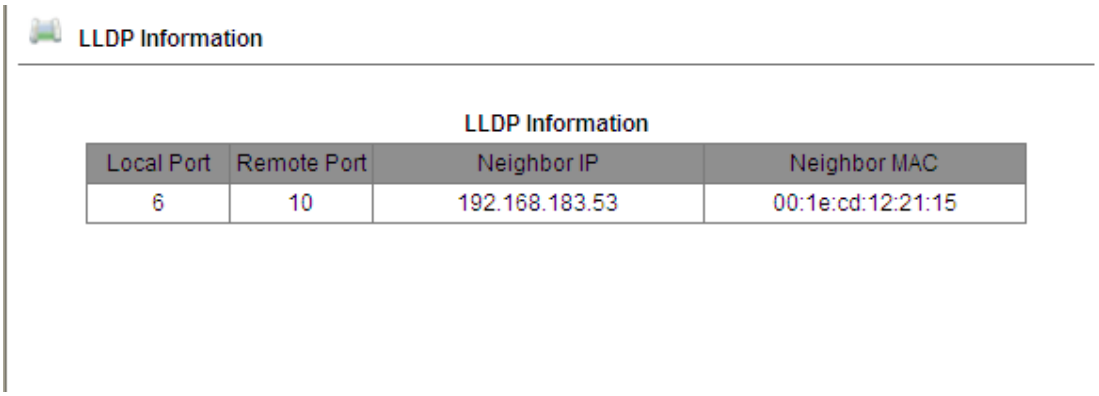

Figure 77 LLDP Information

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 and enabled by default.

6.16 MOTD

6.16.1 Overview

Message Of The Day (MOTD) is used to configure the login page information, such as the welcome message, SN, address, and contact.

6.16.2 Web Configuration

1. Enable MOTD, as shown in Figure 78.

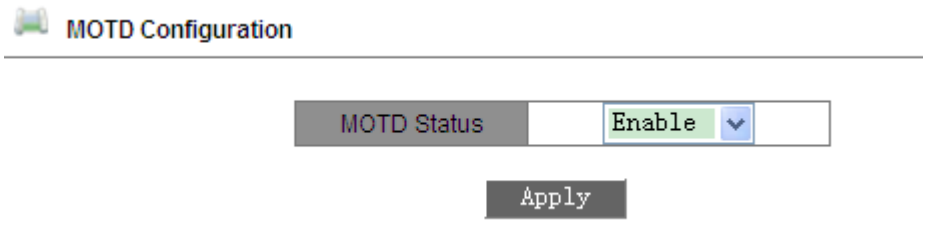

Figure 78 Enabling MOTD

MOTD Status

Options: Enable/Disable

Default: Enable

Function: Enable or disable MOTD.

2. Configure customized information, as shown in Figure 79.

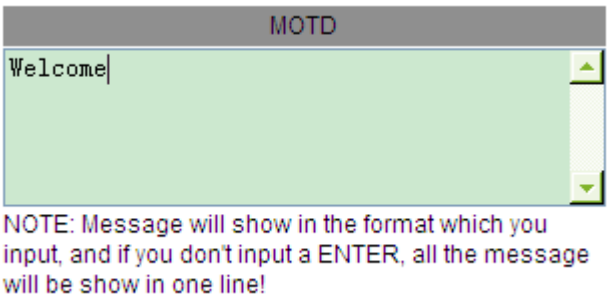

Figure 79 Configuring Customized Information

MOTD

Range: 1~255 bytes

Function: Configure customized information. The information will be displayed in the user login page.

3. Select the information to be displayed, as shown in Figure 80.

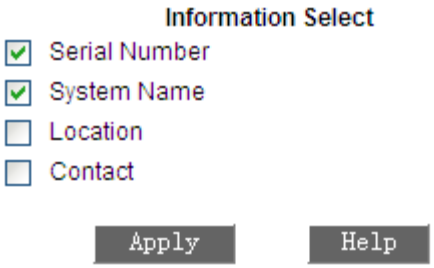

Figure 80 Selecting the Information to Be Displayed

Select the information to be displayed on the user login page.

6.16.3 Typical Configuration Example

Configure user login information, including "Welcome", SN, and system name.

Configuration on switches:

1. Enable MOTD, as shown in Figure 78.
2. Configure customized information "Welcome", as shown in Figure 79.
3. Select SN and system name, as shown in Figure 80.
4. After configuration is completed, the user login page will display the selected information, as shown in Figure 81.

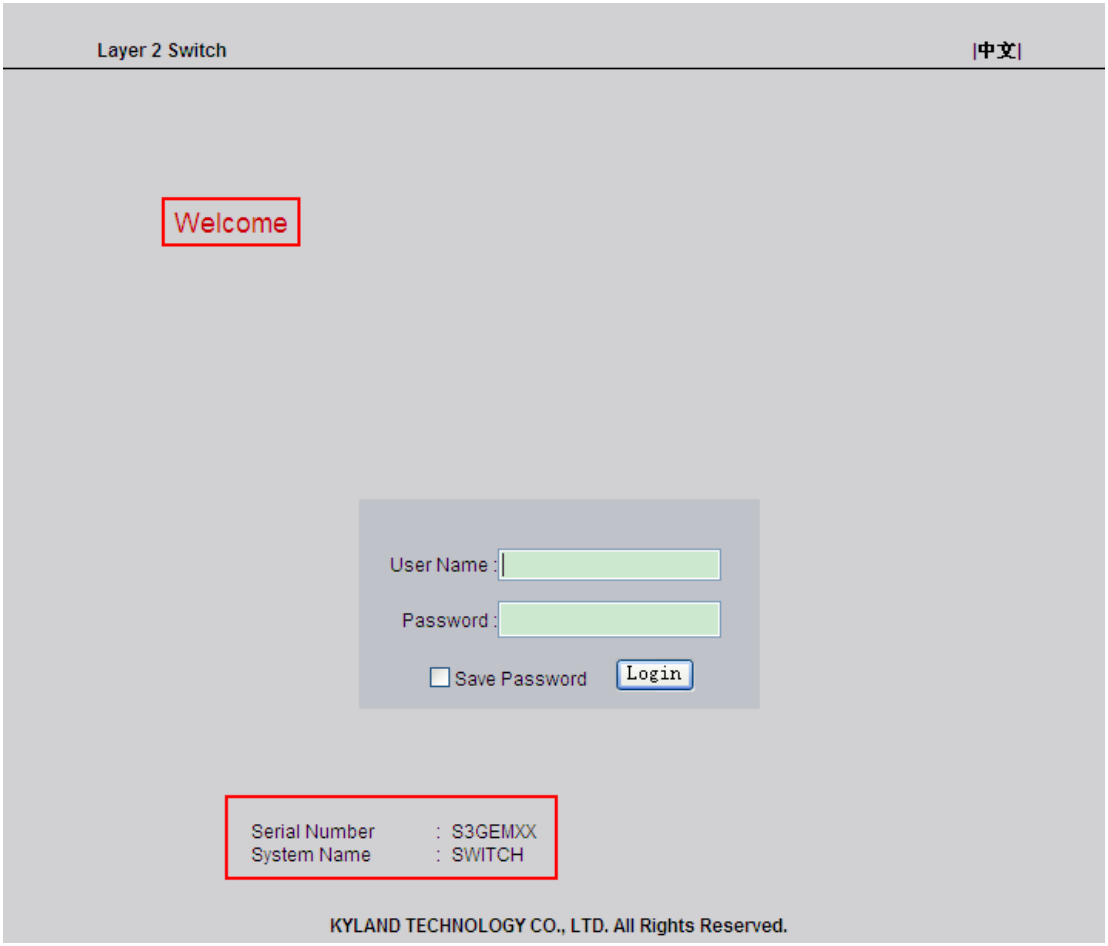

Figure 81 User Login Page

6.17 SNTP

6.17.1 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. Multiple SNTP servers can be configured for one switch, but only one can be active at a time.

The SNTP client sends a request to each server one by one through unicast. The server that first gives a response is in active state. The other servers are in non-active state.

Caution:

- The switch cannot serve as the SNTP server.
- To synchronize time by SNTP, there must be an active SNTP server.

6.17.2 Web Configuration

1. Enable SNTP. Select the server and set other parameters, as shown in Figure 82.

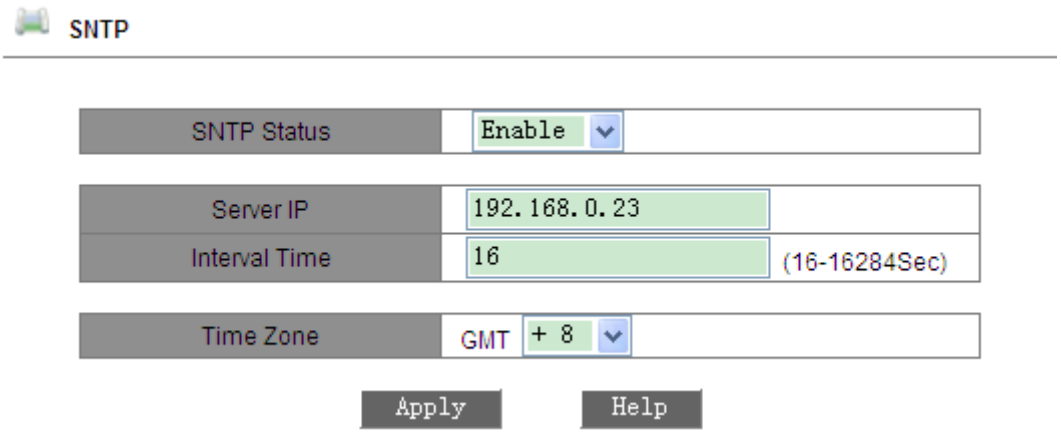

Figure 82 SNTP Configuration

SNTP Status

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 83.

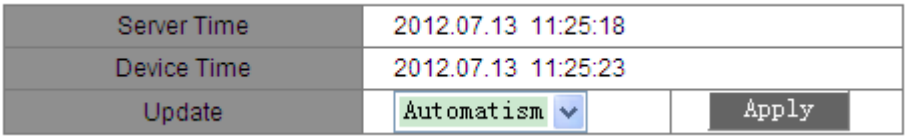

Figure 83 Time Synchronization Mode

Server Time

Format: yyyy.mm.dd, hh.mm.ss

Default: 0000.00.00 00.00.00

Function: Display the time obtained from the server.

Device Time

Format: yyyy.mm.dd hh.mm.ss

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, as shown in Figure 84.

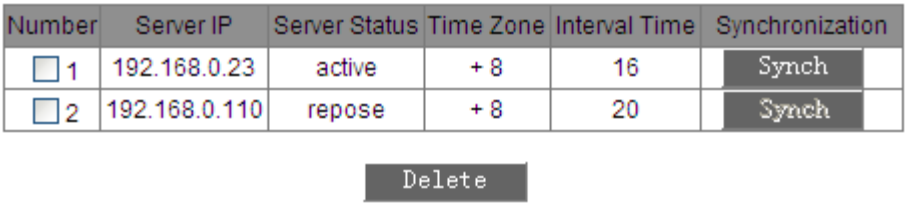

Figure 84 SNTP Configuration

Number

Select the number of the server configuration to be deleted.

Server Status

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>.

6.18 Alarm

6.18.1 Overview

This series switches support the following types of alarms:

- AC/DC alarm: If the function will be enabled, an alarm is generated for DC power supply.
- Port alarm: If the function is enabled, an alarm will be generated for the port in link down state.
- Ring alarm: If the function is enabled, an alarm will be generated for an open ring.

Caution:

- The AC/DC alarm function is available only on SICOM3000BA-EM-C-3GX-6T and SICOM3009BA-EM-C-3S/M-6T.
- Only the master station of a DT ring supports the ring alarm function.

6.18.2 Web Configuration

1. Set alarm parameters, as shown in Figure 85.

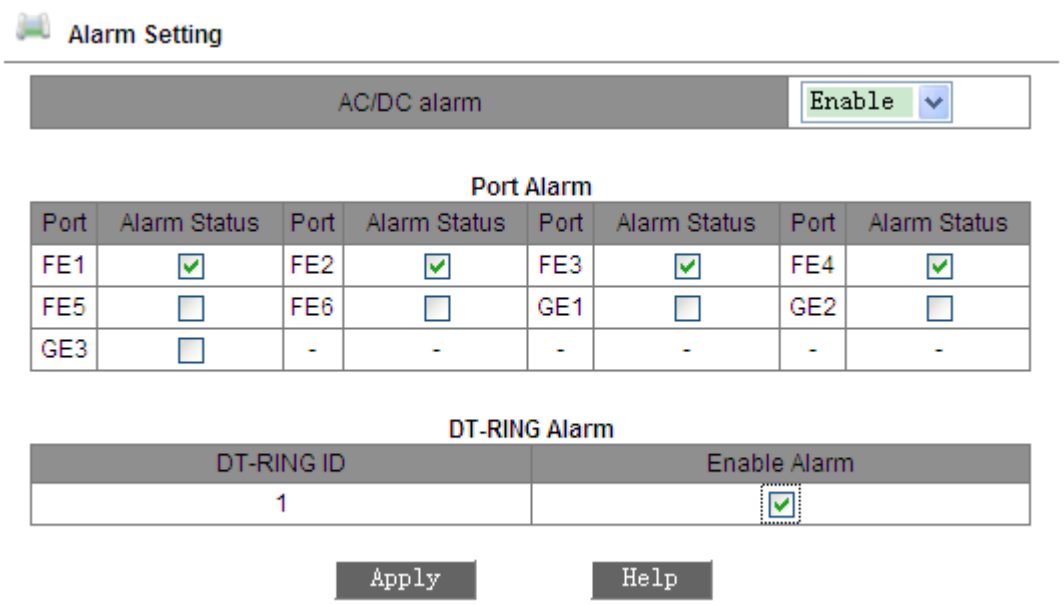

Figure 85 Alarm Setting

AC/DC alarm

Options: Enable/Disable

Default: Enable

Function: Enable or disable AC/DC alarm.

Port alarm

Options: Select/Deselect

Default: Deselect

Function: Enable or disable port alarm.

Ring alarm

Options: Select/Deselect

Default: Deselect

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

2. Enable port alarm and ring alarm. The alarm information includes both types of alarms, as shown in Figure 86.

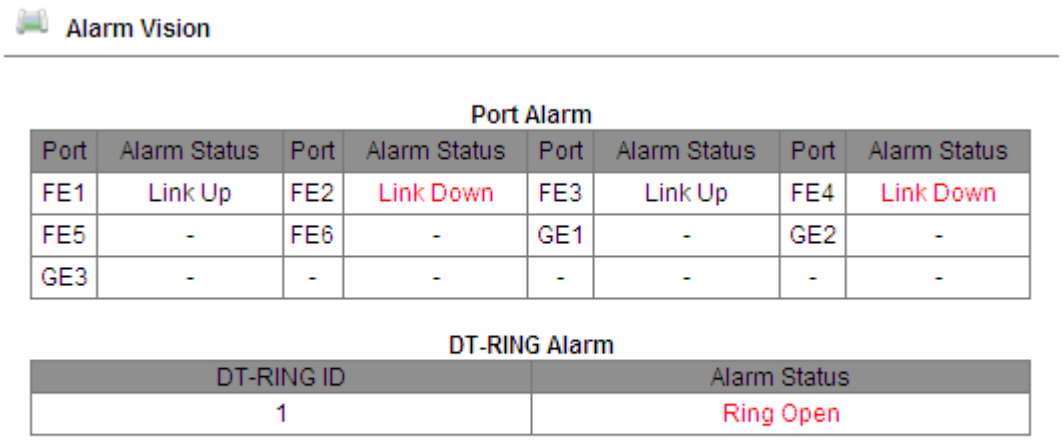

Figure 86 Alarm Information

Port Alarm Status

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.

Ring Alarm Status

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.

3. Enable AC/DC alarm. The alarm information contains current information, as shown in Figure 87.

Figure 87 AC/DC Alarm Information

AC/DC Current Information

Options: Alternating Current/Direct Current

Description: When AC power supply is adopted, Alternating Current is displayed in green. When DC power supply is adopted, Direct Current is displayed in red.

Caution:

To use the AC/DC alarm function, you need to provide the external mechanism.

6.19 SNMPv2

6.19.1 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.

6.19.2 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.

6.19.3 Description

This series switches support SNMPv2 and SNMPv3. 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 community name carried by an SNMP packet is not acknowledged by the switch, the packet is discarded.

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

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

6.19.4 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 88 shows the relationships among the NMS, agent, and MIB.

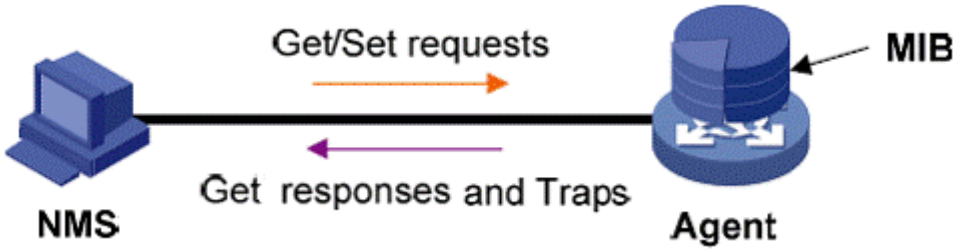

Figure 88 Relationship among NMS, Agent, and MIB

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 89, the OID of object A is 1.2.1.1.

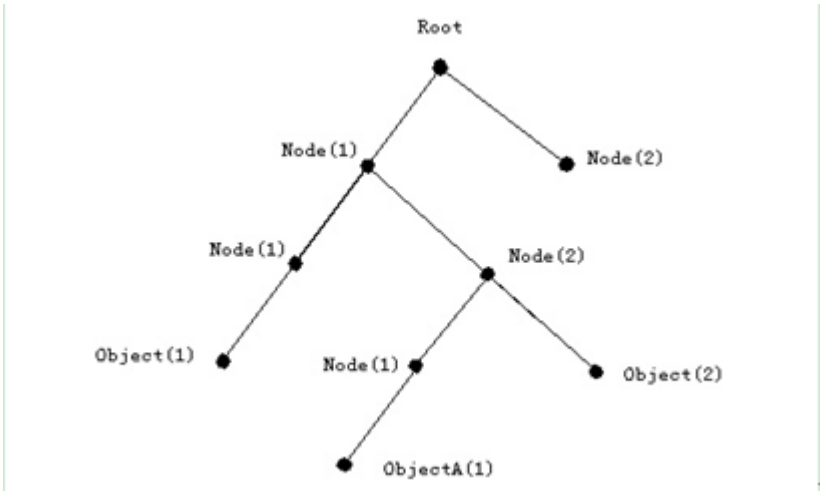

Figure 89 MIB Structure

6.19.5 Web Configuration

1. Enable SNMP, as shown in Figure 90.

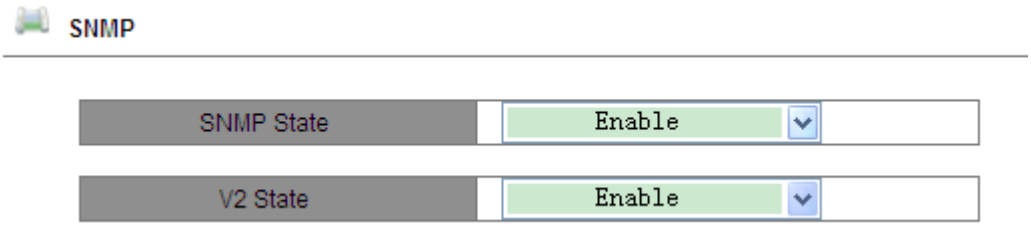

Figure 90 Enabling SNMP and Selecting SNMP Version

SNMP State

Options: Enable/Disable

Default: Enable

Function: Enable or disable SNMP.

V2 State

Options: Enable/Disable

Default: Disable

Description: SNMPv2 is compatible with SNMPv1.

2. Configure access rights, as shown in Figure 91.

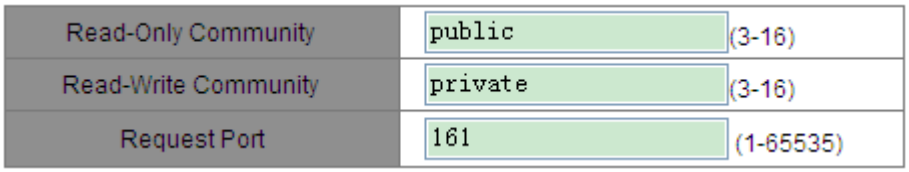

Figure 91 Access Rights Configuration

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 92.

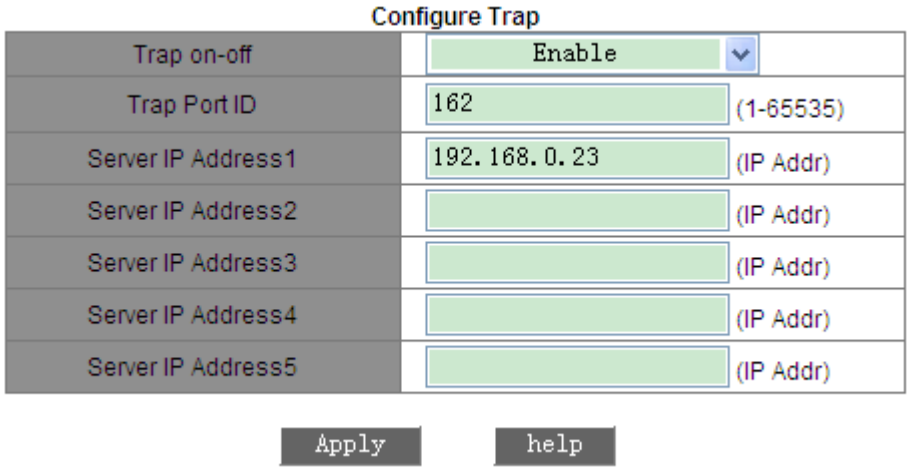

Figure 92 Trap Configuration

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 93.

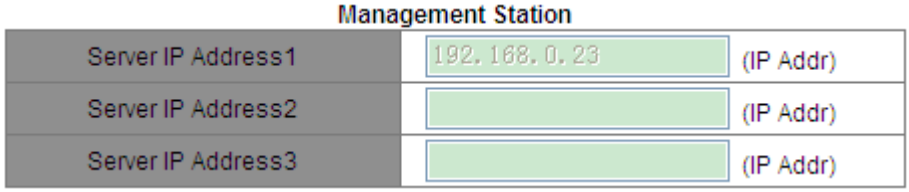

Figure 93 IP Address of Management Server

The IP address of 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.

6.19.6 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 that of 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 94.

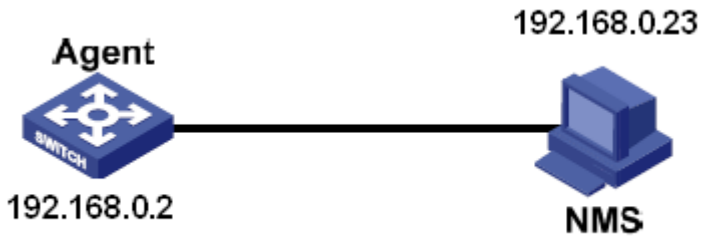

Figure 94 SNMPv2 Configuration Example

Configuration on the Agent:

1. Enable SNMP and v2 state, as shown in Figure 90.
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 91.
3. Enable trap sending, set trap port number to 162, and IP address of server to 192.168.0.23, as shown in Figure 92.

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

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

6.20 SNMPv3

6.20.1 Overview

SNMPv3 provides a User-Based Security Model (USM) authentication mechanism. You can configure authentication and encryption functions. Authentication is used for verifying the validity of packet sender, preventing illegitimate users' access. Encryption is used for encrypt packets transmitted between the NMS and the Agent, avoiding interception. The authentication and encryption functions can improve the security of communication between the SNMP NMS and the SNMP Agent.

6.20.2 Implementation

SNMPv3 provides four configuration tables. Each table can contain 16 entries. These tables determine whether specific users can access MIB information.

You can create multiple users in the user table. Each user uses different security policies for authentication and encryption.

You can define MIB access rights in the access table by group name, context name, security model, and security level.

The group table is the collection of multiple users. In the group table, access rights are defined based on user groups. All the users of a group have the rights of the group.

The context table identifies the strings that can be read by users, irrespective of security models.

6.20.3 Web Configuration

1. Configure the user table, as shown in Figure 95.

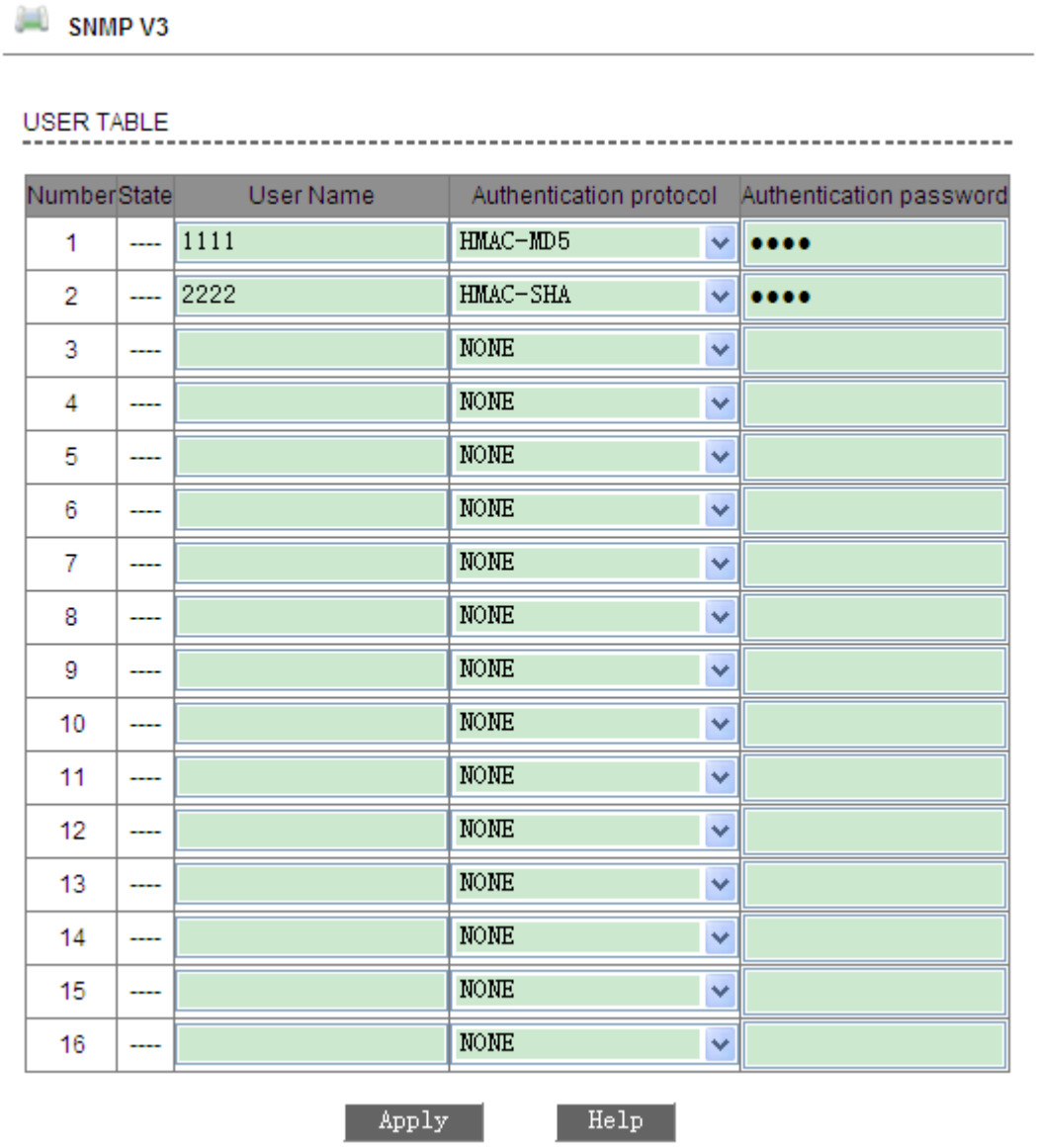

Figure 95 SNMPv3 User Table Configuration

User Name

Range: 4~16 characters

Function: Create the user name.

Authentication protocol

Options: NONE/HMAC-MD5/HMAC-SHA

Default: NONE

Function: Select an authentication algorithm.

Authentication password

Range: 4~16 characters

Function: Create password for a user.

2. Configure the access table, as shown in Figure 96.

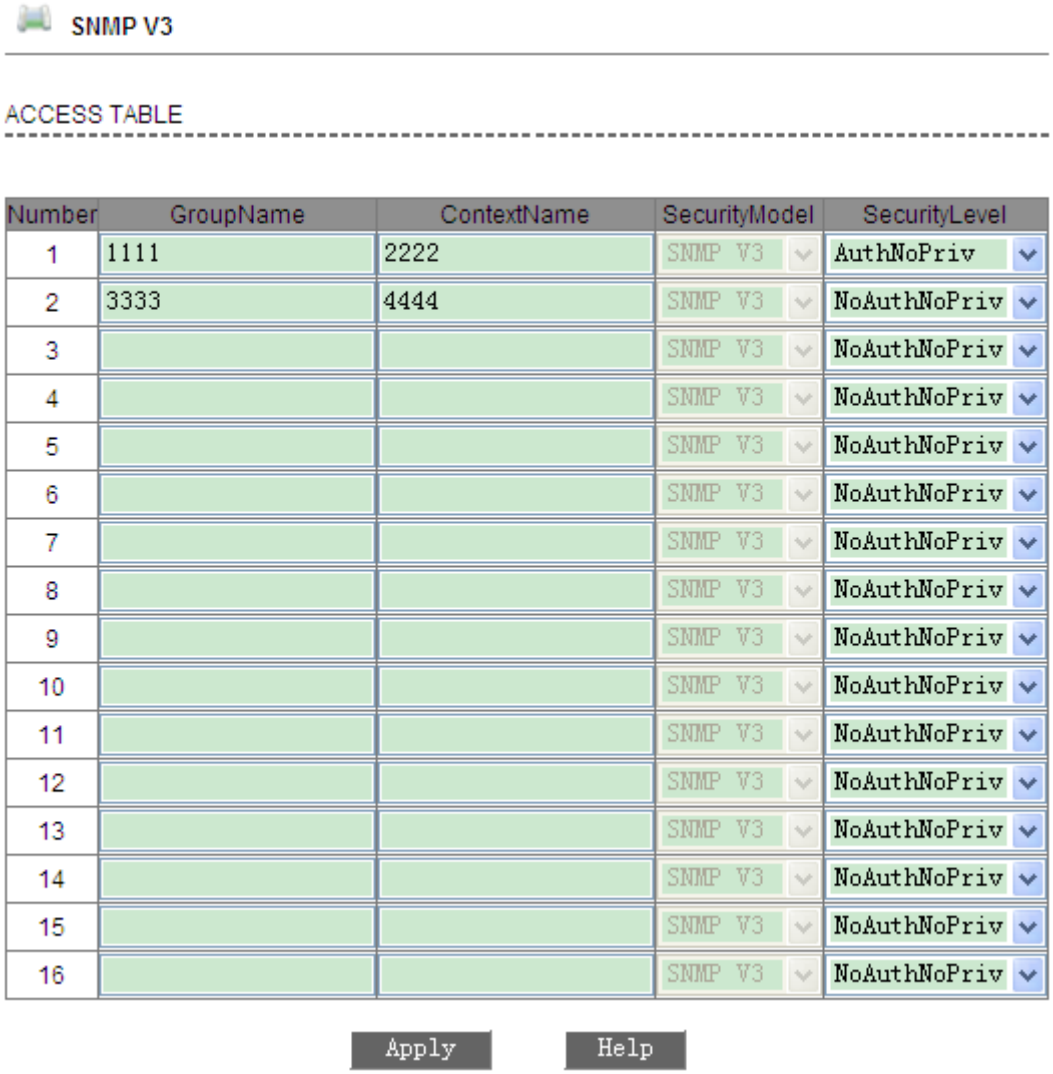

Figure 96 SNMPv3 Access Table

Group Name

Range: 4~16 characters

Function: Configure the name of the group table.

Description: Currently, each group can contain only one user. Therefore, the group name must be identical with the user name in the user table.

Context Name

Range: 4~16 characters

Function: Configure the context name.

Security Model

Options: SNMPv3

Description: SNMPv3 indicates that USM is adopted.

Security Level

Options: NoAuthNoPriv/AuthNoPriv

Default: NoAuthNoPriv

Function: Select whether authentication and encryption are required.

Description: NoAuthNoPriv indicates no authentication or encryption. AuthNoPriv indicates authentication without encryption.

3. Configure the context table, as shown in Figure 97.

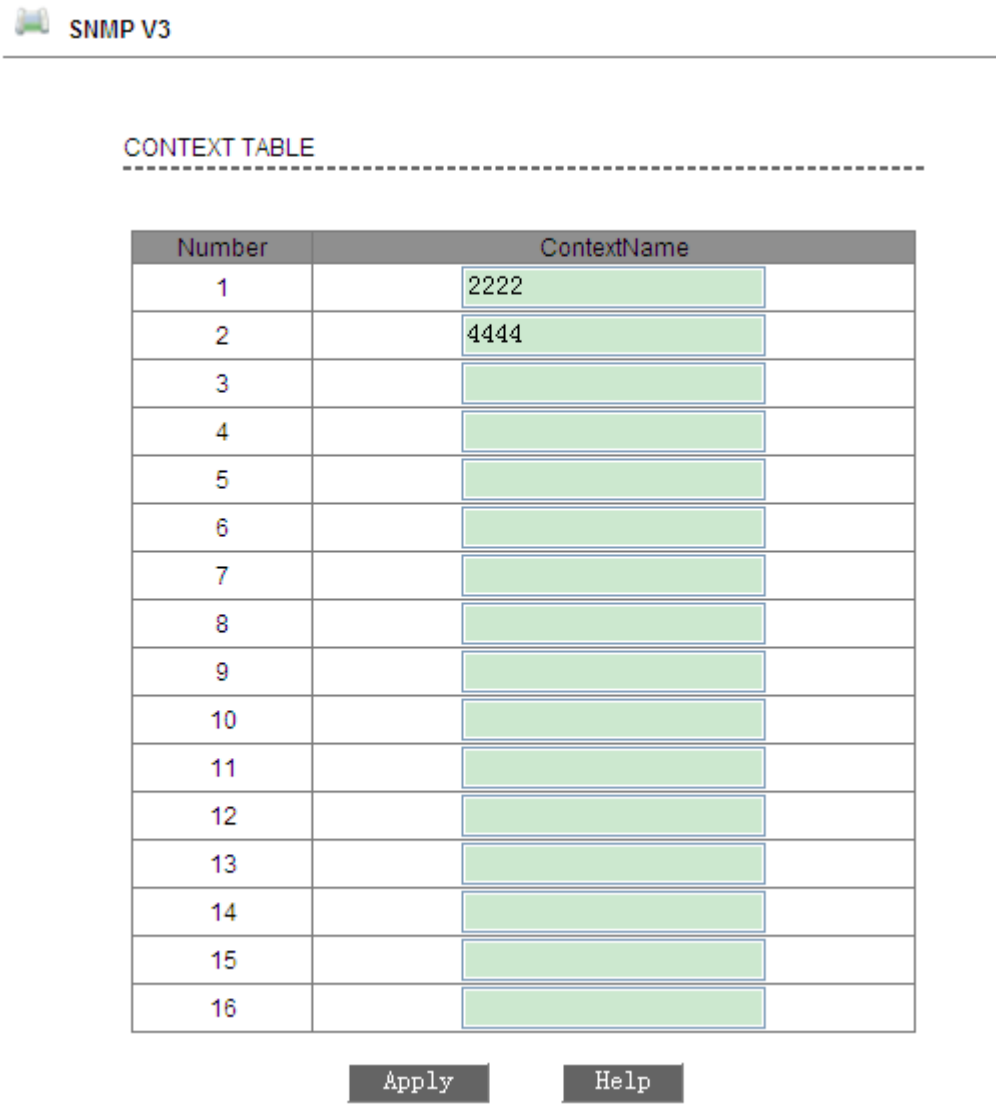

Figure 97 SNMPv3 Context Table Configuration

Context Name

Range: 4~16 characters

Function: Define the objects that can be accessed by SNMP. The configuration must be identical with that in the access table.

4. Configure the group table, as shown in Figure 98.

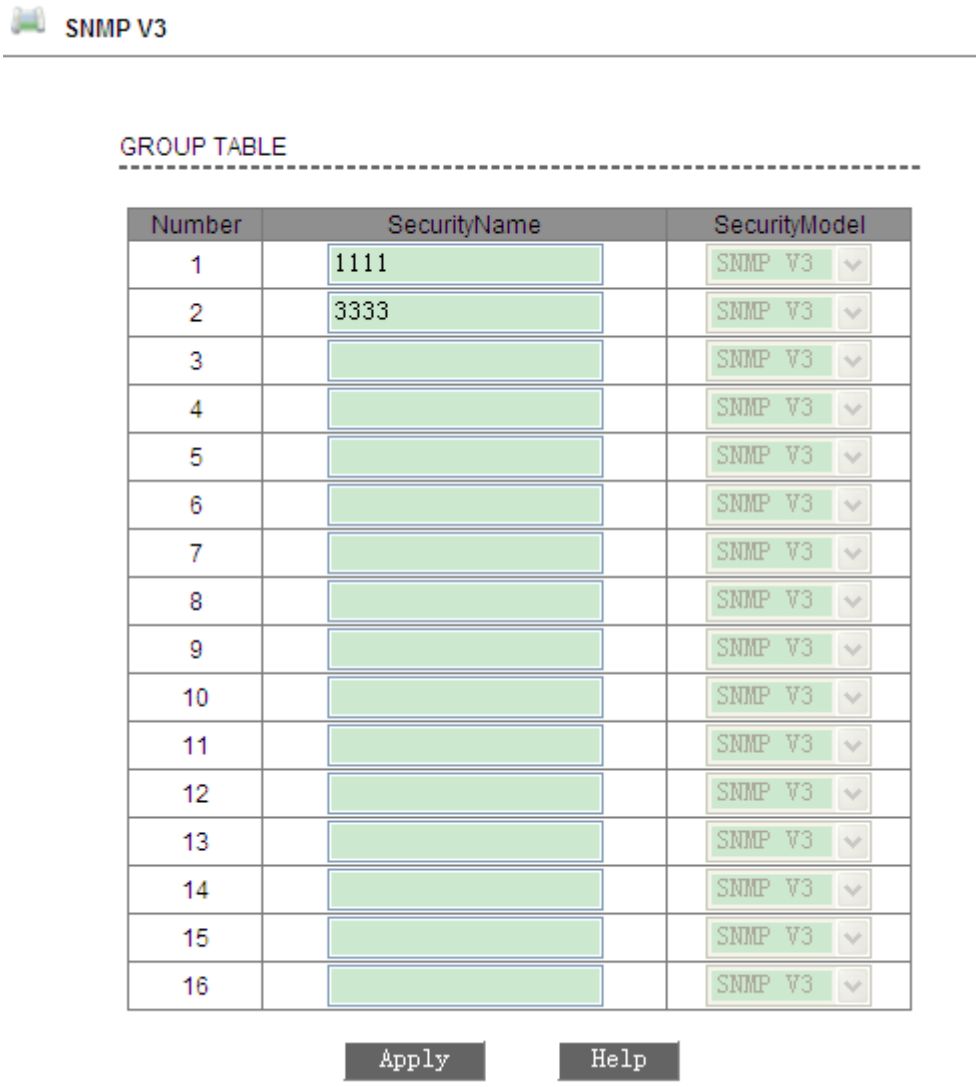

Figure 98 SNMPv3 Group Table Configuration

Security Name

Range: 4~16 characters

Function: Configure the name of the group name. Currently, each group can contain only one user. Therefore, the security name must be identical with the user name in the user table.

Security Model

Options: SNMPv3/SNMPv2

Default: SNMPv3

Description: SNMPv3 indicates USM is adopted. Currently, the value must be SNMPv3.

6.20.4 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 that of the switch is 192.168.0.2.User 1111 monitors and manages the Agent through SNMPv3. The authentication protocol is HMAC-MD5, and the security level is AuthNoPriv, as shown in Figure 99.

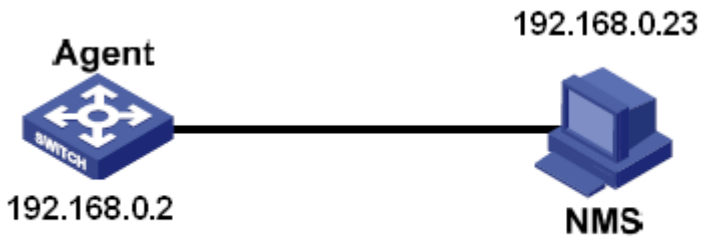

Figure 99 SNMPv3 Configuration Example

Configuration on the Agent:

1. Configure the SNMPv3 user table. Set user name to 1111, authentication protocol to HMAC-MD5, and authentication password to aaaa, as shown in Figure 95.
2. Configure the SNMPv3 access table. Set group name to 1111, context name to 2222, and security level to AuthNoPriv, as shown in Figure 96.
3. Configure the SNMPv3 context table. Set the context name to 2222, as shown in Figure 97.
4. Configure the SNMPv3 group table. Set the security name to 1111, as shown in Figure 98.

To monitor and manage the status of the Agent, you need to run the

management software, for example, Kyvision, on the NMS.

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

6.21 RMON

6.21.1 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 traffic of ports.

RMON mainly provides statistics and alarm functions. Statistics function is that Agents can periodically collect statistics on various traffic of 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.

6.21.2 RMON Group

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

The statistics group is that the system collects statistics on all kinds 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.

- 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, the alarm event is triggered only for the first time. That means the rising alarm and falling alarm are generated alternately.

- 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.

6.21.3 Web Configuration

1. Configure the statistics table, as shown in Figure 100.

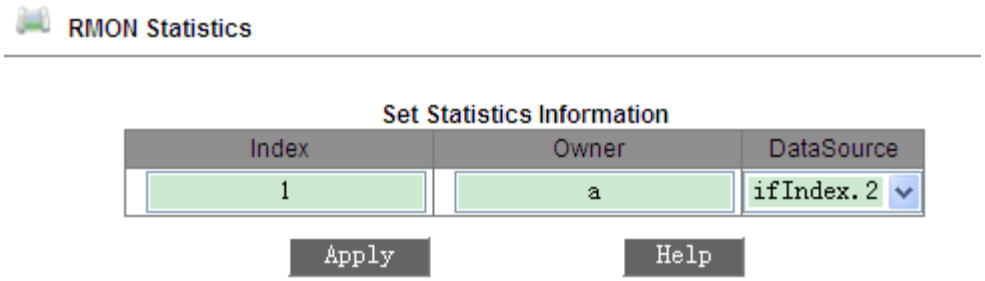

Figure 100 RMON Statistics Table

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 101.

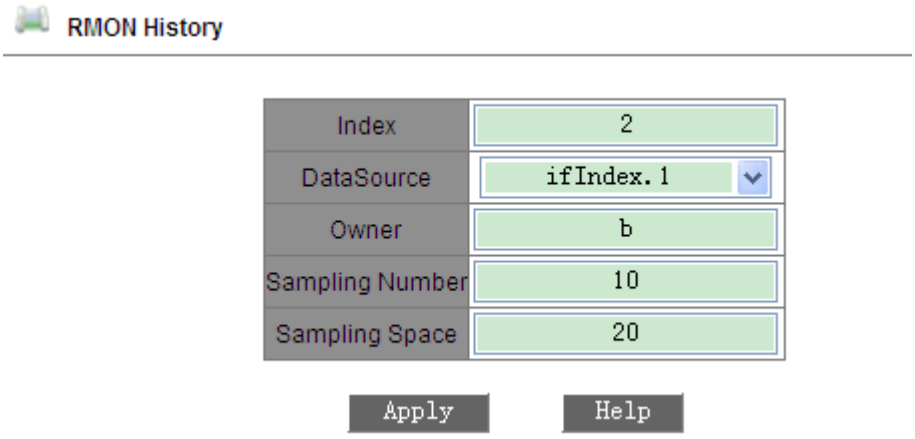

Figure 101 RMON History Table

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 102.

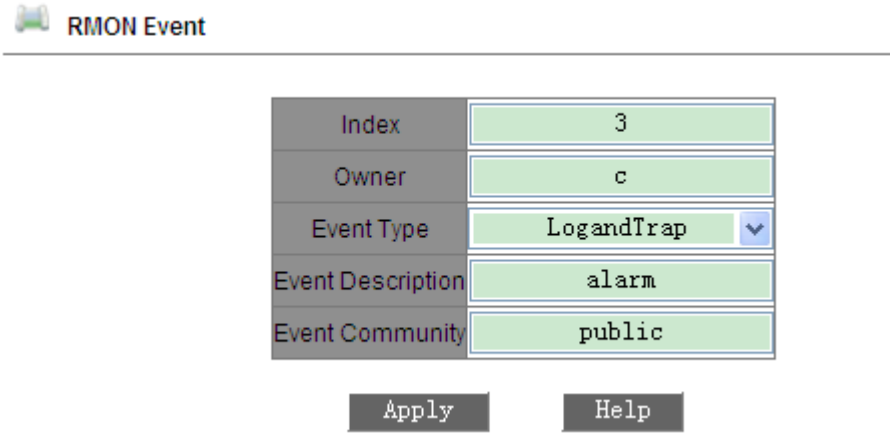

Figure 102 RMON Event Table

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: 1~32 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 103 and Figure 104.

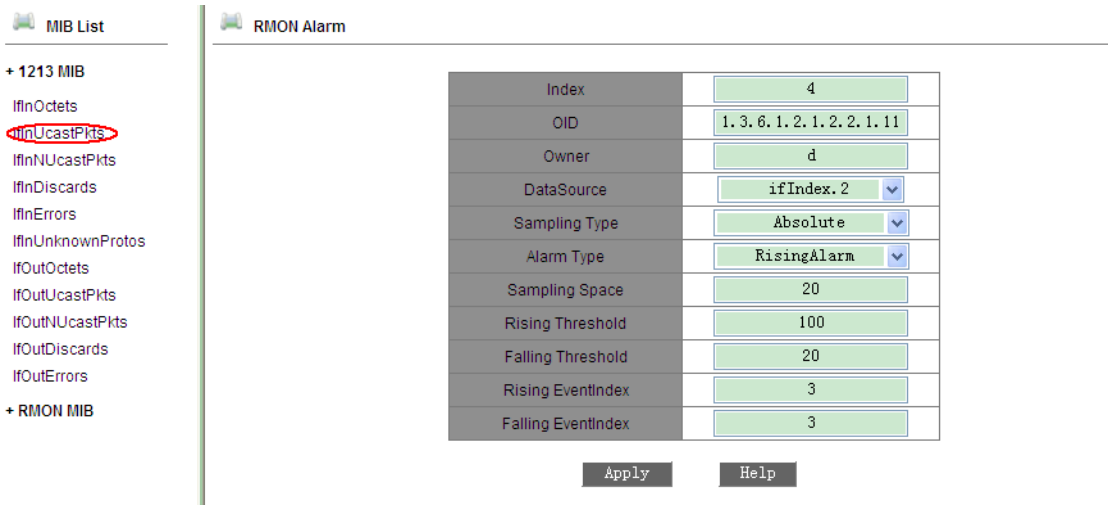

Figure 103 RMON Alarm Table - 1213 MIB Node

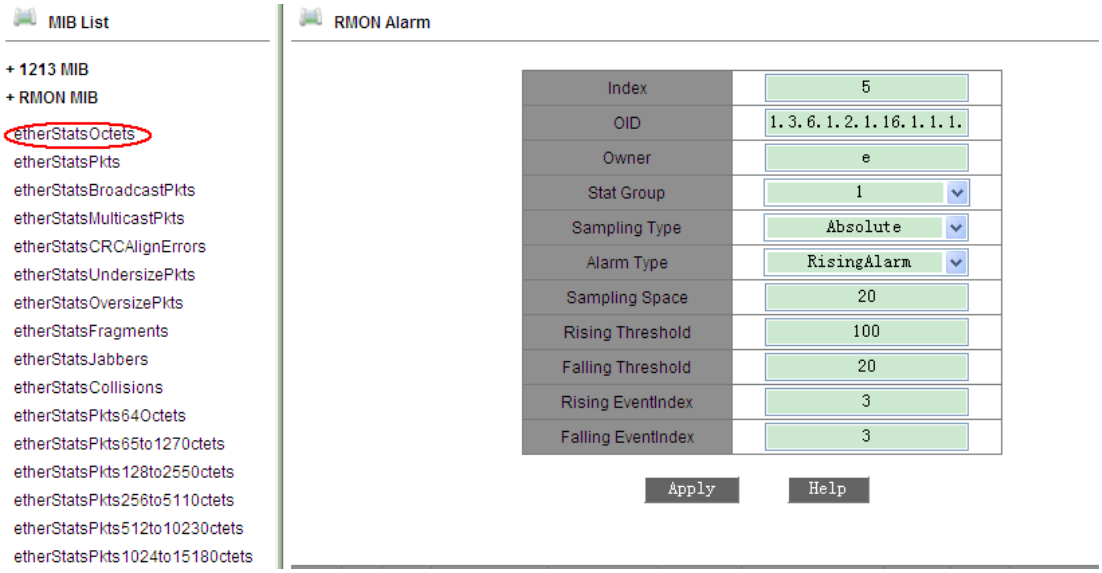

Figure 104 RMON Alarm Table - RMON MIB Node

MIB List

Select the MIB whose statistics are to be collected, for example, number of incoming unicast packets on ports. After you double-click the node, the OID is added automatically.

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: Configure the comparison method for the sampling value and threshold.

Description: If Absolute is selected, each sampling value is compared with the threshold directly. If Delta is selected, the current sampling value is first deducted by the last sampling value and the deduction result is compared with the threshold.

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.

6.22 SSH

6.22.1 Overview

Secure Shell (SSH) is a network protocol for secure remote login. SSH encrypts transmitted data to prevent information disclosure. In this case, you can configure the switch through the CLI.

The switch supports the SSH server function and allows the connection of multiple SSH users that log in to the switch remotely through SSH, but only one user can connect to the switch at a time.

6.22.2 Key

Unencrypted packet is called plain text while encrypted packet is called cipher text. Both encryption and decryption require the key. A key is a specific string and is the only parameter for transformation between plain text and cipher text. Encryption changes plain text to cipher text, while decryption changes cipher text to plain text.

Key-based security authentication needs keys, and each end of the communication has a pair of keys: private one and public one. The public key is used to encrypt data, and a legitimate user can use the private key to decrypt the data to guarantee confidentiality.

6.22.3 Implementation

To implement SSH connection during communication, the server and the client go through the following phases:

- Version negotiation phase: SSH has two versions: SSH1 and SSH2. Two communication parties negotiate the version to be used.
- Key and algorithm negotiation phase: SSH supports multiple encryption algorithms. Two communication parties negotiate the algorithm to be used.
- Authentication phase: The SSH client initiates an authentication request to the server. Then the server authenticates the client.
- Session request phase: After passing the authentication, the client sends a session request to the server.
- Session phase: After the session request is accepted, the server and the client start communication.

6.22.4 Web Configuration

- Configuration steps of SSH server:

1. Select Disable for SSH Sate.
2. Click <Destroy> to delete the old key pair, as shown in Figure 105.

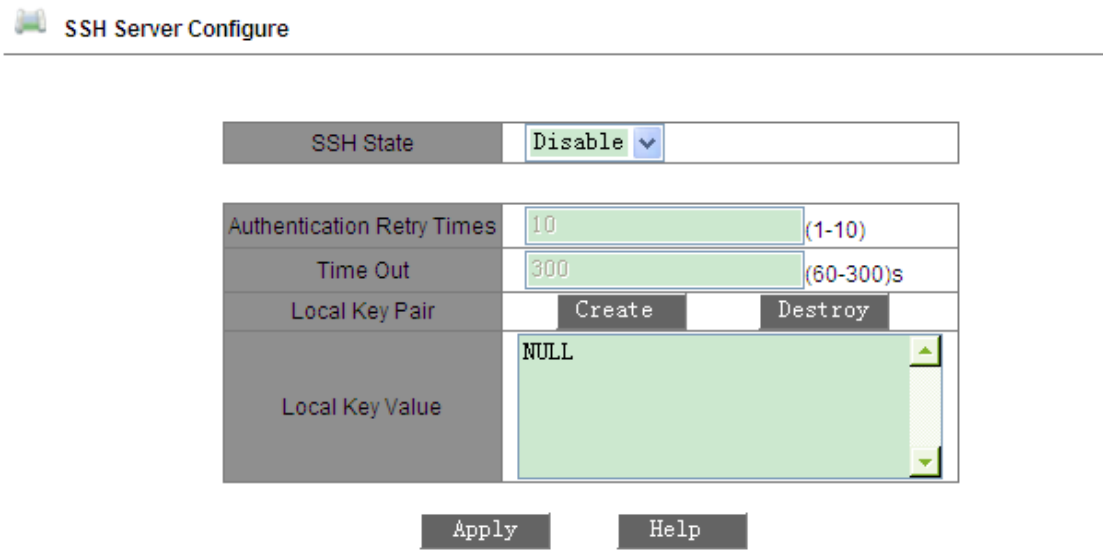

Figure 105 Destroying the Old Key Pair

3. Click <Create> to generate the new key pair, as shown in Figure 106.

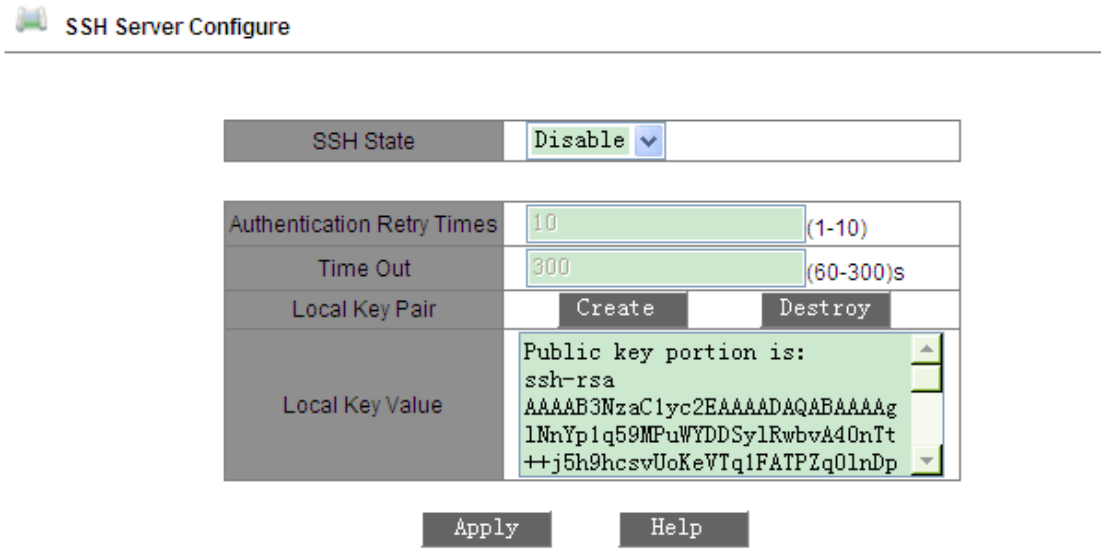

Figure 106 Creating a New Key Pair

4. Enable SSH. Set server parameters, as shown in Figure 107.

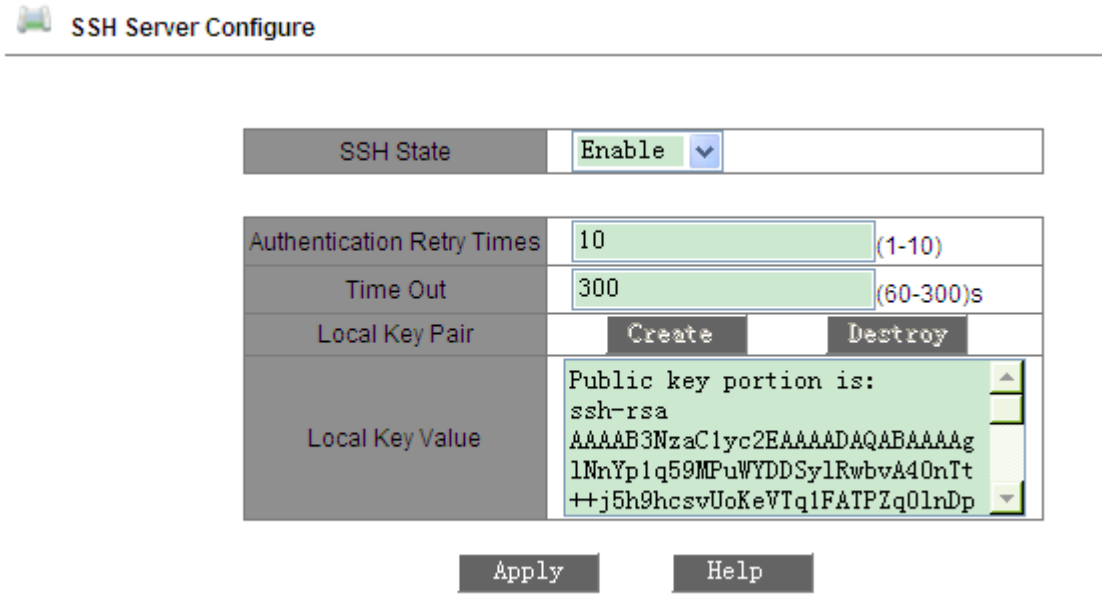

Figure 107 SSH Server Configuration

SSH State

Options: Enable/Disable

Default: Enable

Function: Enable or disable SSH. If SSH is enabled, the device serves as the

SSH server.

Authentication Retry Times

Range: 1~10

Default: 10

Function: Set the number of attempts to log in to the SSH server.

Time Out

Options: 60~300

Default: 300

Description: Set the SSH connection validity during no data transmission. If the time expires, the client is disconnected automatically.

Local Key Pair

Options: Create/Destroy

Function: Create or destroy the local key pair of the SSH server. The local key pair must be generated before the SSH server is enabled and the old key pair must be destroyed before a new one is created.

Local Key Value

Display the local key value. Click <Create>. The key value is created automatically.

- Configuration steps of SSH key:

1. Configure the SSH key, as shown in Figure 108.

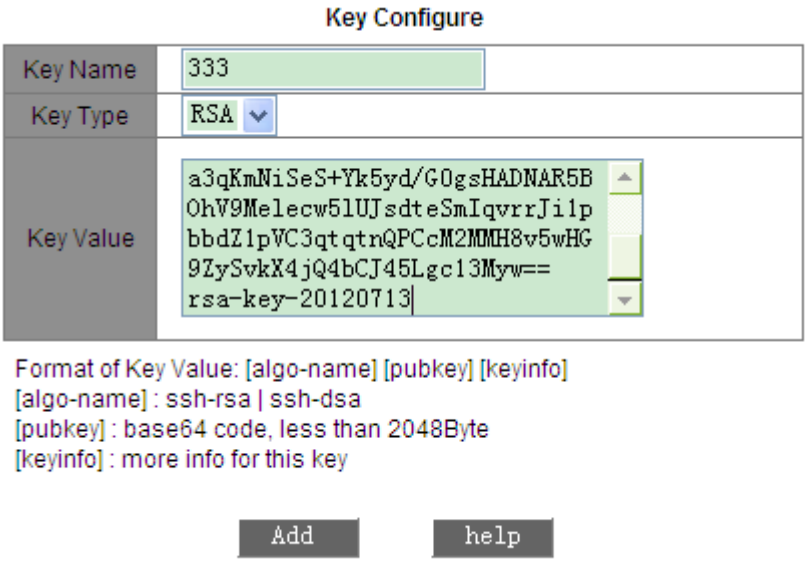

Figure 108 SSH Key Configuration

Key Name

Range: 3~20 characters

Function: Configure the key name. A maximum of three keys can be configured.

Key Type

Forcible configuration: RSA

Description: The product supports only the RSA algorithm.

Key Value

Format: {Algorithm name, public key, key information}

Algorithm name: ssh-rsa | ssh-dsa

Public key: 64 bit code-based, less than 2048 bytes.

Key information: more information about the key.

Function: Configure the public key for the client.

Description: The public key is usually generated by Puttygen and copied to the key value of the server. The private key is saved in the client.

2. View the public key list. You can delete a selected key entry, as shown in Figure 109.

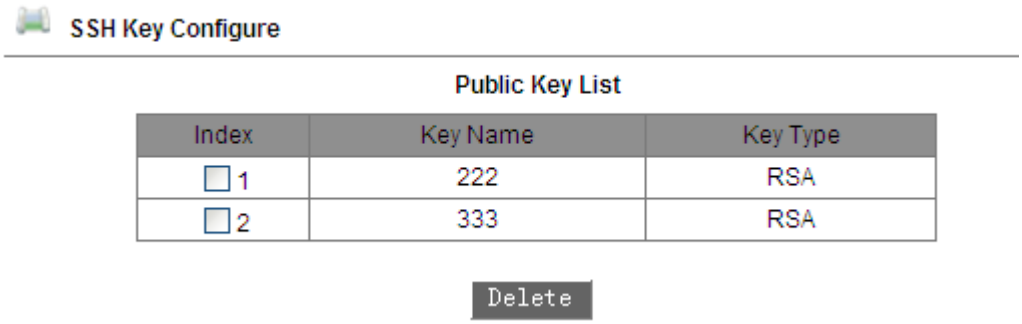

Figure 109 Public Key List

➢ Configuration steps of SSH user:

1. Configure the SSH user, as shown in Figure 110.

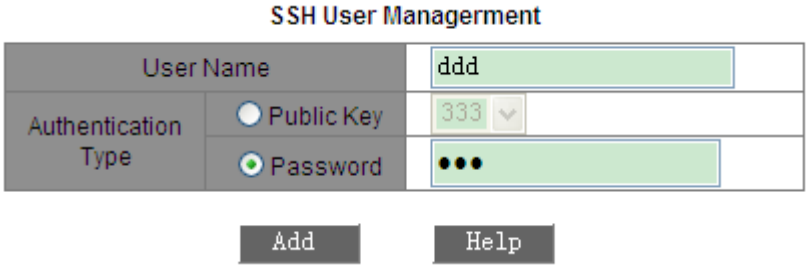

Figure 110 SSH User Configuration

User Name

Range: 3~20 characters

Function: Create the user name. You can configure a maximum of four users.

Authentication Type

Options: Public Key/Password

Default: Password

Function: Configure the authentication type of the user. If you select Password, enter 3 to 8 characters. If you select Public Key, select a key from the public key list.

2. View the SSH user list. You can delete a selected user, as shown in Figure 111.

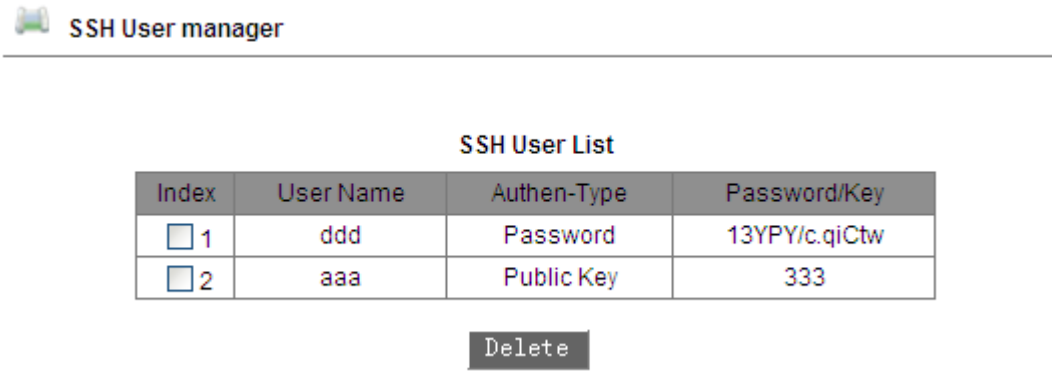

Figure 111 SSH User List

6.22.5 Typical Configuration Example

Establish an SSH connection between the host (SSH client) and the switch, as shown in Figure 112.

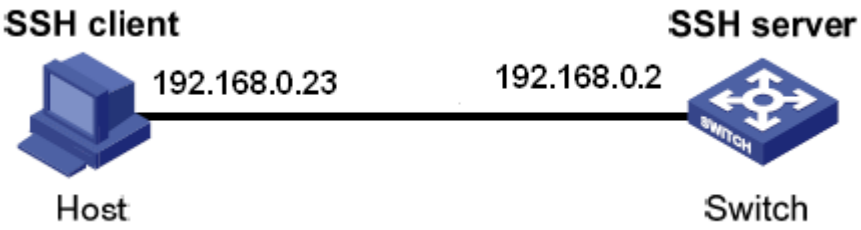

Figure 112 SSH Configuration Example

- An SSH user adopts password authentication.

1. Destroy the old key pair, create the new key pair, and start the SSH server, as shown in Figure 105, Figure 106, and Figure 107.
2. Set the SSH user name to ddd, select the password authentication mode, and set password to 444, as shown in Figure 110.
3. Establish the connection between the host and the SSH server. Open PuTTY.exe. Enter the IP address of SSH server, namely, 192.168.0.2, and set port number to 22, as shown in Figure 113.

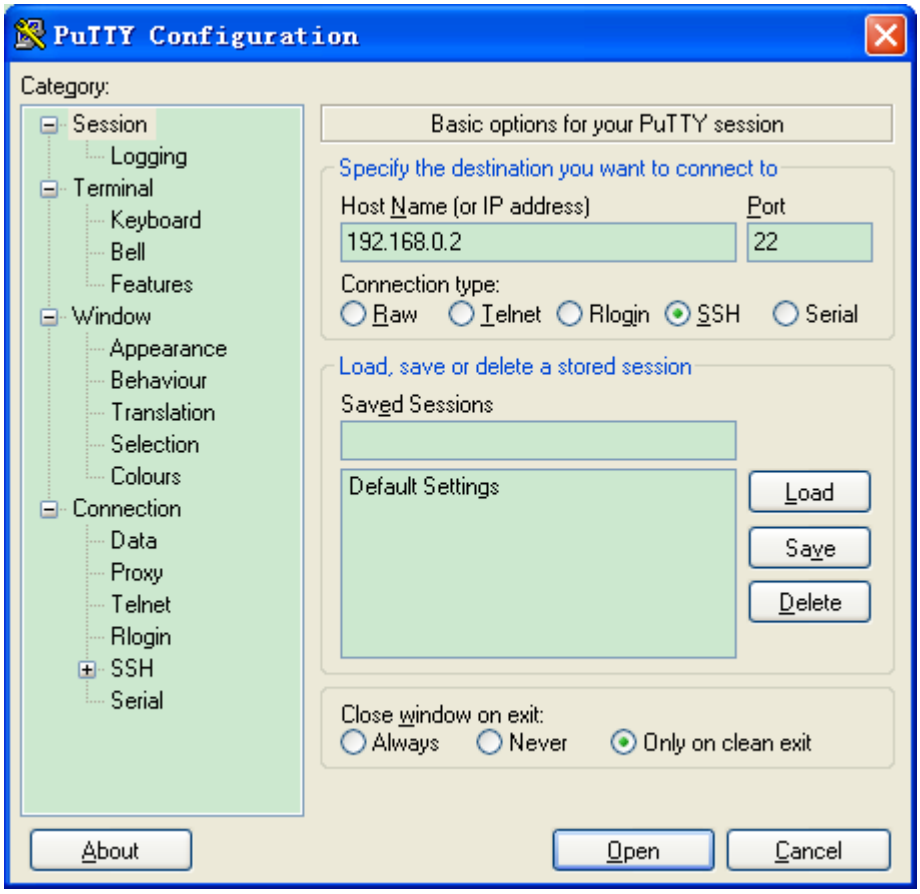

Figure 113 SSH Client Configuration

4. Click <Open>. The following page is displayed. Click <Yes>.

Figure 114 Alarm Information

5. Enter user name "ddd" and password "444". The switch configuration page is displayed, as shown in Figure 115.

Figure 115 SSH Login Interface (Password Authentication)

➢ An SSH user adopts key authentication.

1. Destroy the old key pair, create the new key pair, and start the SSH server, as shown in Figure 105, Figure 106, and Figure 107.
2. Configure the SSH client, as shown in Figure 108. Run PuTTYGen.exe on the client. Click <Generate> to generate a key pair, as shown in Figure 116.

Figure 116 Gererating a Key Pair

3. During the process of generating a key pair, move your mouse in the window, as shown in Figure 117. Otherwise, the progress bar does not continue and the generation is stopped.

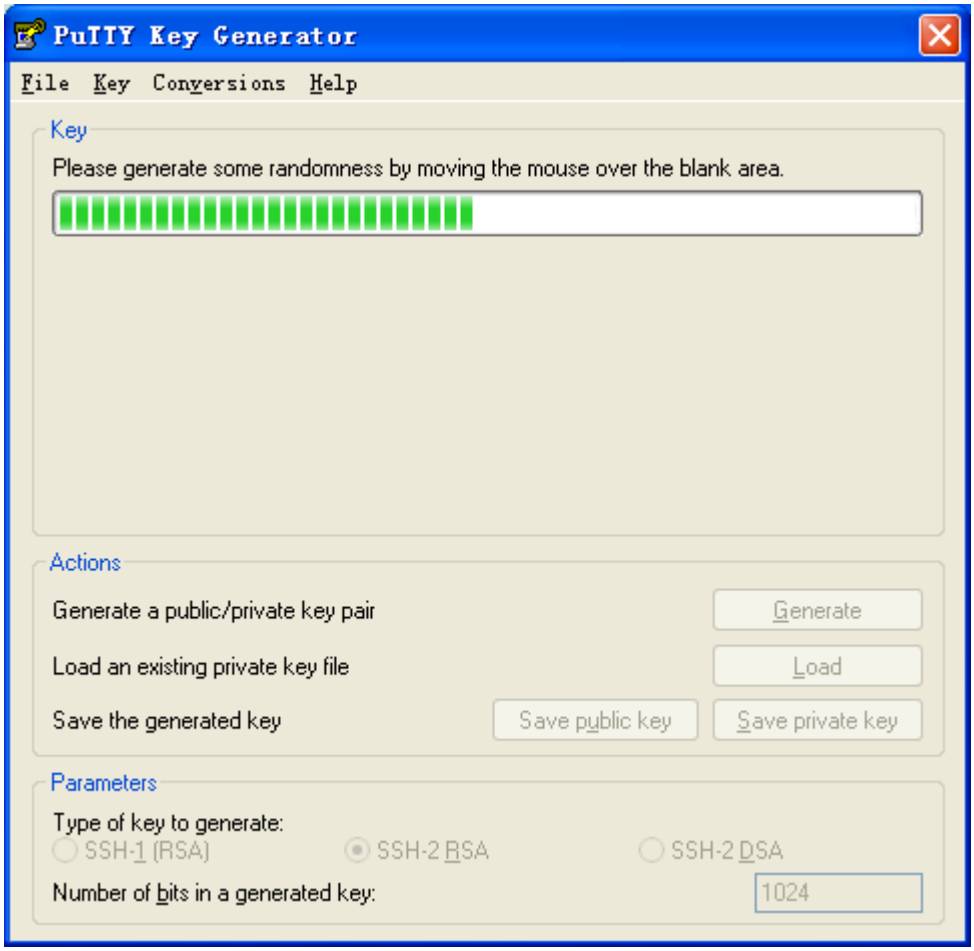

Figure 117 Generation Process

4. As shown in Figure 118, the key is created. Click <Save private key>. Copy the public key to the key value in SSH key configuration and enter the key name, as shown in Figure 108.

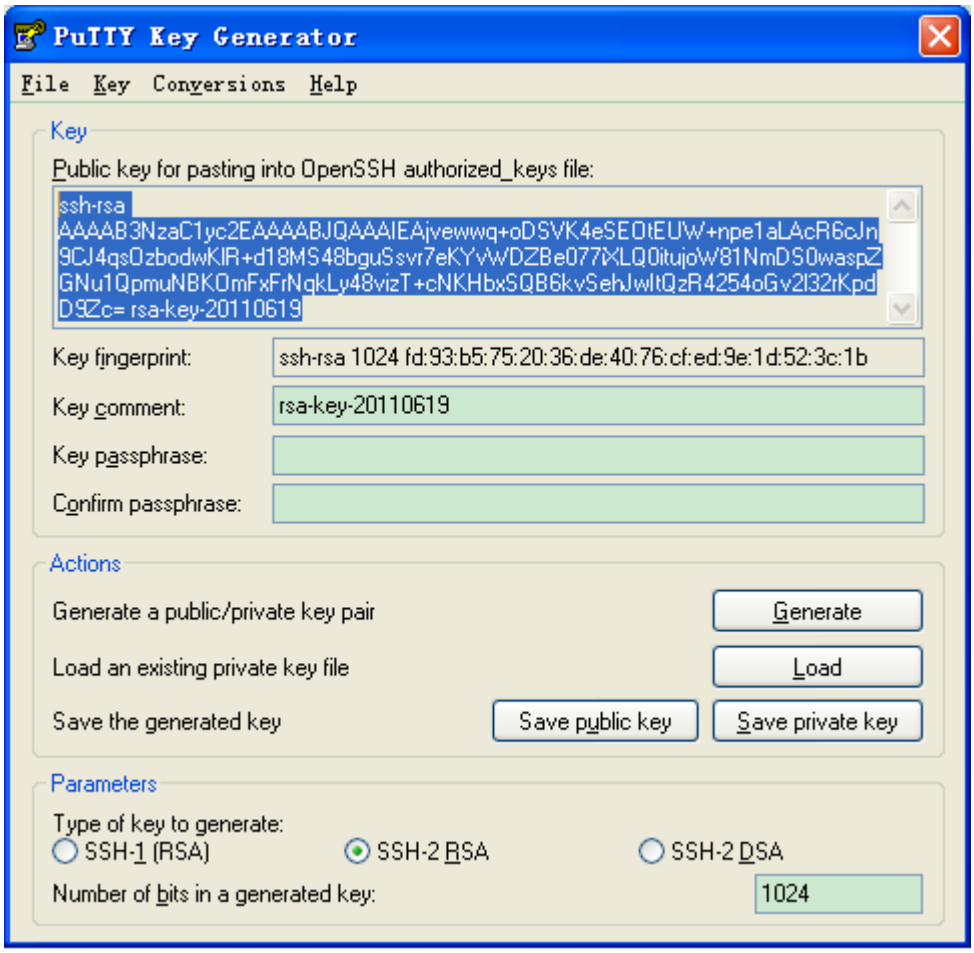

Figure 118 Key Value

5. Set the SSH user name to ddd, and select key authentication and key name, as shown in Figure 110.
6. Establish the connection between the host and the SSH server. Open PuTTY.exe. Enter the IP address of SSH server, namely, 192.168.0.2, and set port number to 22, as shown in Figure 119.

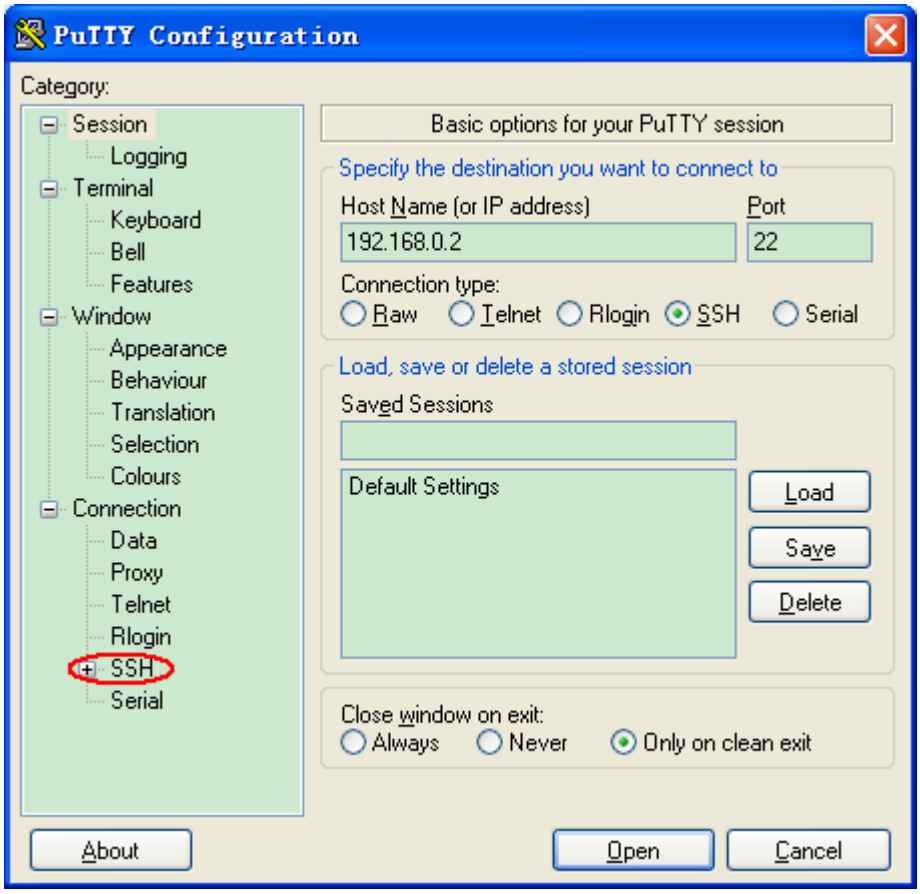

Figure 119 SSH Client Configuration (Key Authentication)

7. In the left column of Figure 119, click [SSH] → [Auth]. The following page is displayed. Click <Browse>. Select the private key saved in step 4.

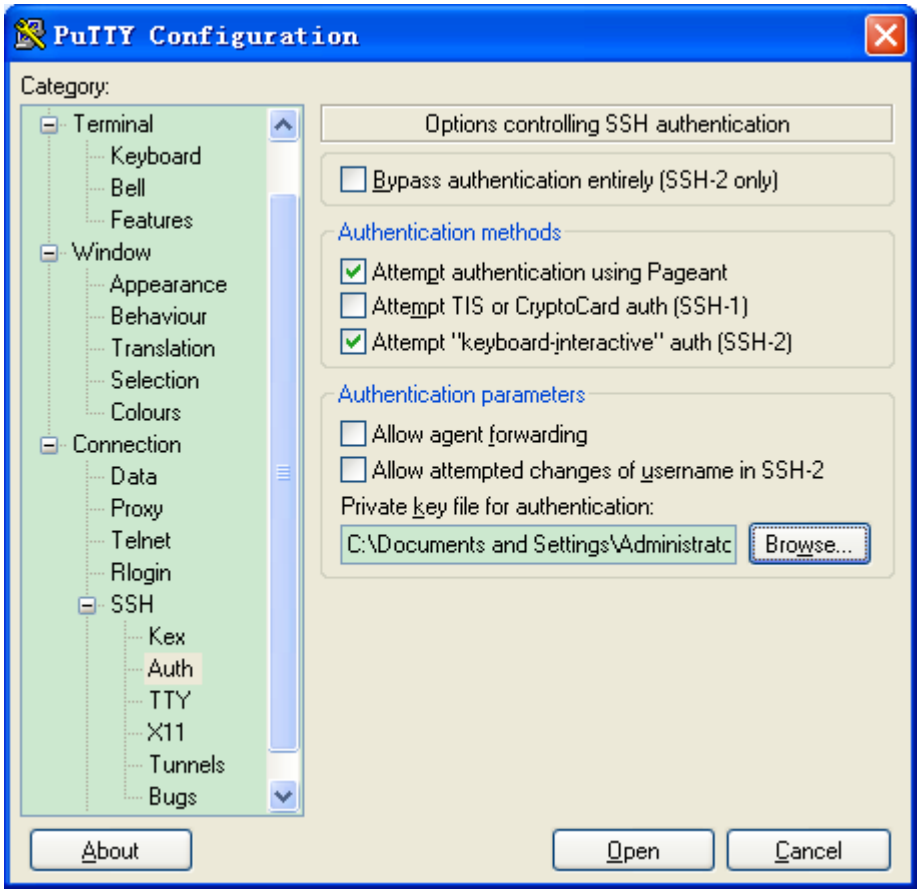

Figure 120 Selecting the Key File

8. Click <Open>. Enter the user name. The switch configuration interface is displayed, as shown in Figure 121.

Figure 121 Login Interface (SSH Key Authentication)

6.23 AAA Configuration

6.23.1 Overview

Authentication, Authorization, Accounting (AAA) is a management mechanism for network security, providing authentication, authorization, and accounting functions.

Authentication: authenticates the identity of the remote accessing user and check the legitimacy of the user.

Authorization: grants different rights to users and limits services available to users.

Accounting: records all operations performed by users when they use network services, including service type, start time, and data flow. It is not only an accounting method, but also the supervision of network security.

6.23.2 Implementation

First, authentication usually uses user name and password to verify user rights. The principle of authentication is that each user has a unique standard for obtaining rights. The AAA server checks the standard with user standards in the database one by one. If a match is found, the user passes the authentication; if not, the server refuses the network connection request.

Then a user obtains operation rights through authorization. For example, a user may execute certain commands for operations after logging into system. In this case, the authorization process will detect whether the user has rights to execute these commands. To be simple, the authorization process checks the activity type or quality, and resources or services allocated to the user. Authorization is performed along with authentication. Once a user passes authentication, the user is granted corresponding rights. Accounting calculates

the number of resources consumed in the user connection process. These resources contain the connecting time or the transmitted and received data in the user connection process. The accounting process can be executed according to statistics logs in the connection process and the user information, and the authorization control, bill and trend analysis, resource utilization, and capacity planning.

Currently, the network connection server interface coordinating with AAA server is the TACACS+ protocol.

6.23.3 Web Configuration

1. Configure authentication method order, as shown in Figure 122.

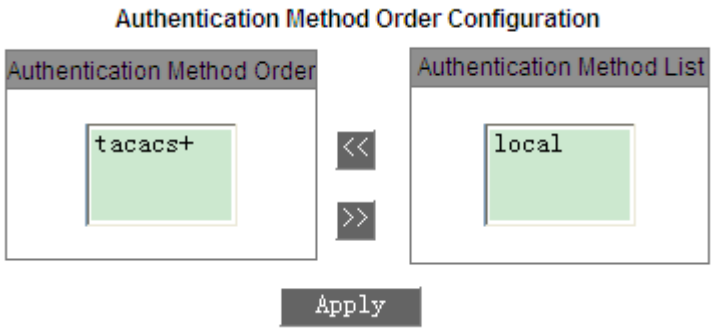

Figure 122 Configuring Authentication Method

Authentication Method Order Configuration

Options: local/tacacs+/local, tacacs+/tacacs+, local

Default: local

Function: Select the order of login authentication.

Description: Local indicates local authentication, in which the user name and password created on the device are used. tacacs+ indicates tacacs+ authentication, in which the user name and password configured on the tacacs+ server are used. Local, tacacs+ indicates that local authentication is first adopted and tacacs+ authentication is used only after local authentication fails. tacacs+, local indicates that tacacs+ authentication is first adopted and

local authentication is used only after local authentication fails.

2. Configure the login mode for TACACS+ authentication, as shown in Figure 123.

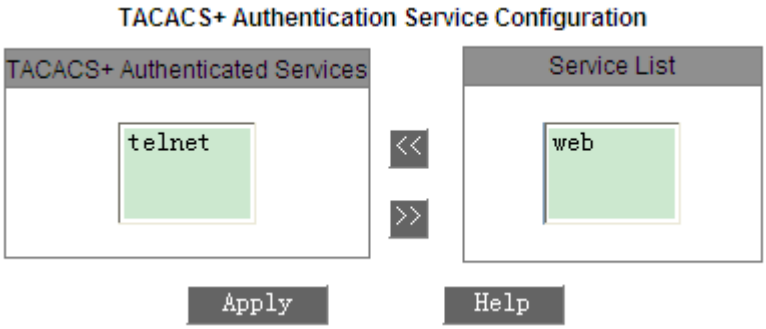

Figure 123 Configuring TACACS+ Authentication Service

TACACS+ Authenticated Services

Options: telnet/web

Function: Select the login mode for TACACS+ authentication.

6.24 TACACS+ Configuration

6.24.1 Overview

Terminal Access Controller Access Control System (TACACS+) is a TCP-based application. It adopts the client/server mode to implement the communication between Network Access Server (NAS) and TACACS+ server. The client runs on the NAS and user information is managed centrally on the server. The NAS is the server for users but client for the server. Figure 124 shows the structure.

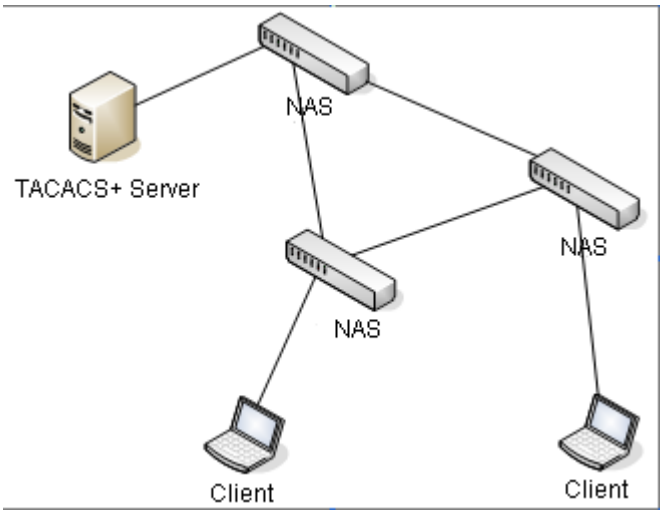

Figure 124 TACACS+ Network Structure

The protocol authenticates, authorizes, and charges terminal users that need to log in to the device for operations. The device serves as the TACACS+ client, and sends the user name and password to the TACACS+ server for authentication. The server receives TCP connection requests from users, responds to authentication requests, and checks the legitimacy of users. If a user passes the authentication, it can log in to the device for operations.

6.24.2 Web Configuration

1. Enable TACACS+, as shown in Figure 125.

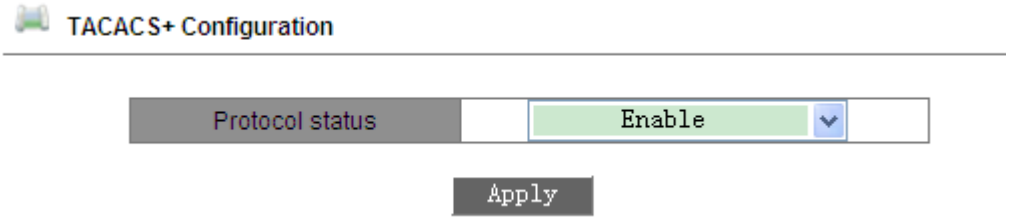

Figure 125 Enabling TACACS+

Protocol status

Options: Enable/Disable

Default: Disable

Function: Enable/Disable TACACS+.

2. Set TACACS+ server parameters, as shown in Figure 126.

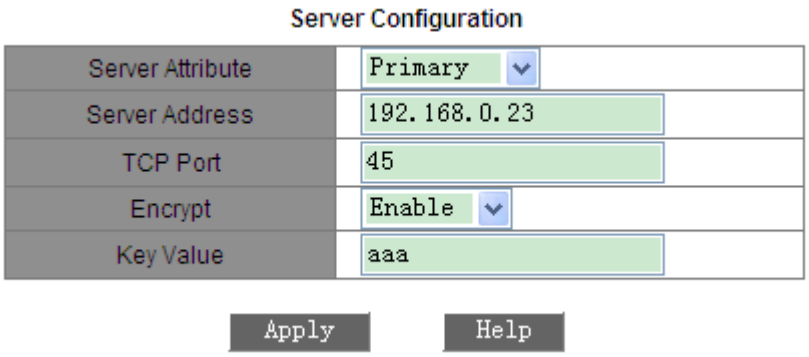

Figure 126 TACACS+ Server Configuration

Server Attribute

Options: Primary/Secondary

Default: Primary

Function: Select the server type.

Server Address

Function: Enter the IP address of the server.

TCP Port

Range: 1~65535

Default: 49

Function: Set the port for receiving NAS authentication requests.

Encrypt

Options: Enable/Disable

Default: Enable

Function: Enable or disable packet encryption. After encryption is enabled, you need to enter the key value.

Key Value

Range: 1~32 characters

Function: Configure the key value.

Description: The key value is used to ensure the security of communication between the client and TACACS+ server. The two parties use the shared key to verify the validity of packets. They can respond to each other's packets only

if their keys are identical. Therefore, you must ensure the key configured on the device is identical with that on the TACACS+.

3. View TACACS+ server list, as shown in Figure 127.

Server List

Index	Attribute	Server Address	TCP Port	Encrypt
1	Primary	192.168.0.23	45	Enable
2	Secondary	192.168.0.46	49	Disable

Delete Modify

Figure 127 Server List

View TACACS+ server list. You can delete or modify selected servers.

6.24.3 Typical Configuration Example

As shown in Figure 128, the TACACS+ server authenticates and authorizes users through the switch. The IP address of the server is 192.168.0.23. The key for packet exchange between the switch and the server is aaa.

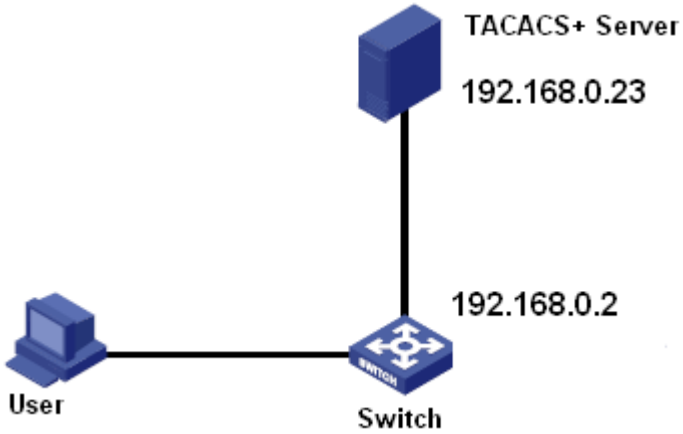

Figure 128 TACACS+ Authentication Example

1. Enable TACACS+, as shown in Figure 125.
2. Set the IP address of the server to 192.168.0.23, enable packet encryption, and set the key value to aaa, as shown in Figure 126.
3. Adopt local authentication for Web login and TACACS+ authentication for Telnet login, as shown in Figure 122 and Figure 123.

4. Configure user name and password "bbb" on the TACACS+ server.
5. For Web login, enter user name "admin" and password "123" to access the switch through local authentication.
6. For Telnet login, enter user name and password "bbb" to access the switch through TACACS+ authentication.

Appendix: Acronyms

Acronym	Full Spelling
AAA	Authentication, Authorization, Accounting
ARP	Address Resolution Protocol
BPDU	Bridge Protocol Data Unit
CLI	Command Line Interface
CRC	Cyclic Redundancy Check
DSCP	Differentiated Services CodePoint
FTP	File Transfer Protocol
IGMP	Internet Group Management Protocol
IGMP Snooping	Internet Group Management Protocol Snooping
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MIB	Management Information Base
MOTD	Message Of The Day
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
TACACS+	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network

WRR	Weighted Round Robin