SICOM3024P V3.2 Series
Industrial Ethernet Switch
Web Operation Manual

Publication Date:Dec. 2024

Version: V1.1

KYLAND

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.

Website: http://www.kyland.com

FAX: +86-10-88796678

Email: support@kyland.com

Contents

Preface

This manual mainly introduces the access methods and software features of SICOM3024P V3.2 series industrial Ethernet switches, and details Web configuration methods.

Content Structure

The manual contains the following contents:

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

	➢ PVLAN ➢ Port mirroring ➢ Port trunk ➢ Link check ➢ Static multicast ➢ IGMP Snooping ➢ ACL ➢ ARP ➢ SNMP ➢ DT-Ring ➢ RSTP/STP ➢ RSTP/STP transparent transmission ➢ DRP# ➢ QoS ➢ MAC address aging time ➢ LLDP ➢ SNTP ➢PTP ➢ Port isolate configuration# ➢ Alarm ➢ Port traffic alarm ➢ GMRP configuration and query ➢ RMON ➢ Log query* ➢ Unicast address configuration and query ➢ DHCP# ➢DHCP ➢IEEE802.1x ➢RADIUS

	➢AAA

Conventions in the manual

1. Text format conventions

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

2. CLI conventions

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

3. Symbol conventions

Symbol	Description
Caution	The matters need attention during the operation and configuration, and they are supplement to the operation description.
Note	Necessary explanations to the operation description.

 Warning	The matters call for special attention. Incorrect operation might cause data loss or damage to devices.

Product Documents

The documents of SICOM3024P V3.2 series industrial Ethernet switches include:

Document	Content
SICOM3024P V3.2 Industrial Ethernet Switches Hardware Installation Manual	Describes the hardware structure, hardware specifications, mounting and dismounting methods of SICOM3024P V3.2.
SICOM3024P V3.2 Series Industrial Ethernet Switch Web Operation Manual	Describes the switch software functions, Web configuration methods, and steps of all functions.

Document Obtainment

Product documents can be obtained by:

➢Kyland website: www.kyland.com

1 Product Introduction

1.1 Overview

The series switches are applied in the power, rail transit, coal mining, and many other industries, and can work properly in rugged environment. They support RSTP, DT-Ring, and IEC62439-6 redundancy protocols, guaranteeing the reliable operation of the system. The series switches employ the internal modular design for flexible expansion. They comply with IEC61850-3 and IEEE1613 standards.

1.2 Product Models

This series switches include:

SICOM3024P_V3.2 (V3.2 indicates the hardware version)

1.3 Software Features

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

- Redundancy protocols: RSTP/STP, DT-Ring and IEC62439-6
- Multicast protocols: IGMP Snooping, GMRP, and static multicast
- Switching attributes: VLAN, PVLAN, QoS, and ARP
- Bandwidth management: port trunk, port rate limiting
- Security: ACL, port isolate
- Synchronization protocol: SNTP and PTP
- Device management: FTP software update, configuration upload/download
- Device diagnosis: port mirroring, LLDP, link check
- Alarm function: port alarm, power alarm, ring alarm, IP/MAC address conflict alarm, temperature alarm, and port traffic alarm
- Network management: management by CLI, Telnet, Web and Kyvision network management software, and SNMP network monitoring

2 Switch Access

You can access the switch by:

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

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

2.1 View Types

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

Table 1 View Types

View Prompt	View Type	View Function	Command for View Switching
SWITCH>	General mode	View recently used commands. View software version. View response information for ping operation.	Input "**enable**" to enter the Privileged mode.
SWITCH #	Privileged mode	Upload/Download configuration file. Restore default configuration. View response information for ping operation. Restart the switch. Save current configuration. Display current configuration. Update software.	Input "**configure terminal**" to enter the Configuration mode from the Privileged mode. Input "**exit**" to return to the General mode.
SWITCH(config) #	Configuration mode	Configure switch functions.	Input "**exit**" or "**end**" to return to the Privileged mode.

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

2.2 Access through Console Port

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

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

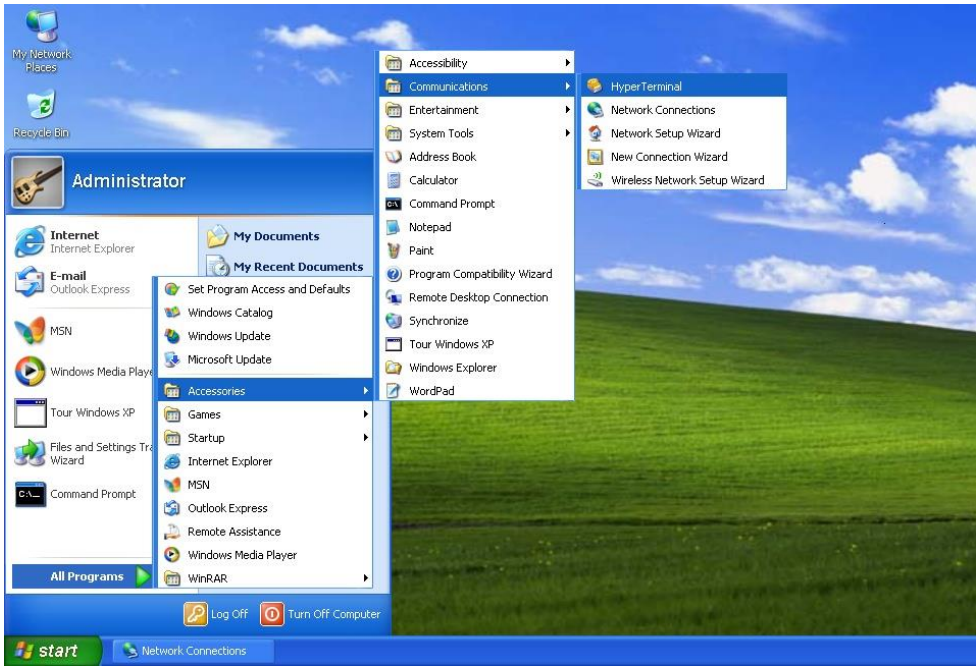


Figure 1 Starting the Hyper Terminal

3. Create a new connection "Switch", as shown in the following figure.

Figure 2 Creating a New Connection

4. Connect the communication port in use, as shown in the following figure.

Figure 3 Selecting the Communication Port

Note:

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

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

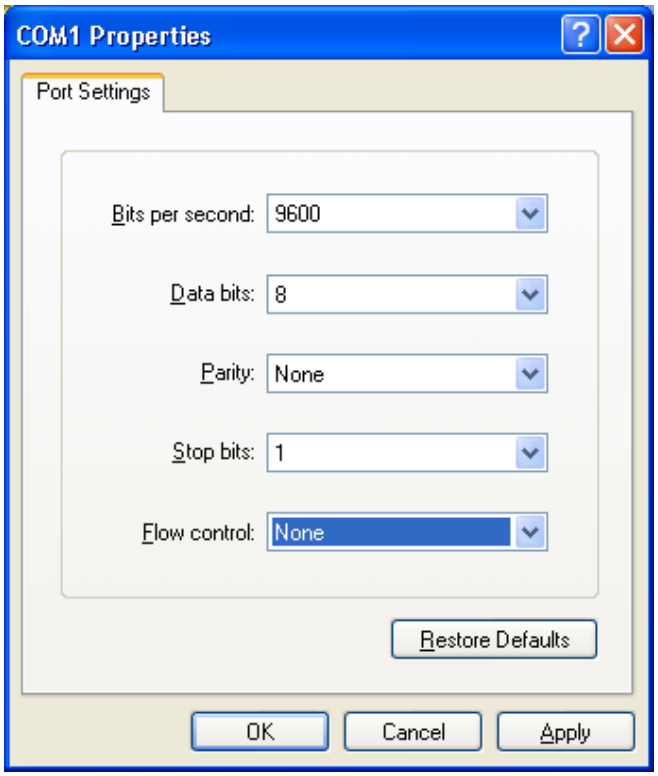


Figure 4 Setting Port Parameters

6. Click <OK>. The switch CLI is displayed. Input password "admin" and press <Enter> to enter the General mode, as shown in the following figure.

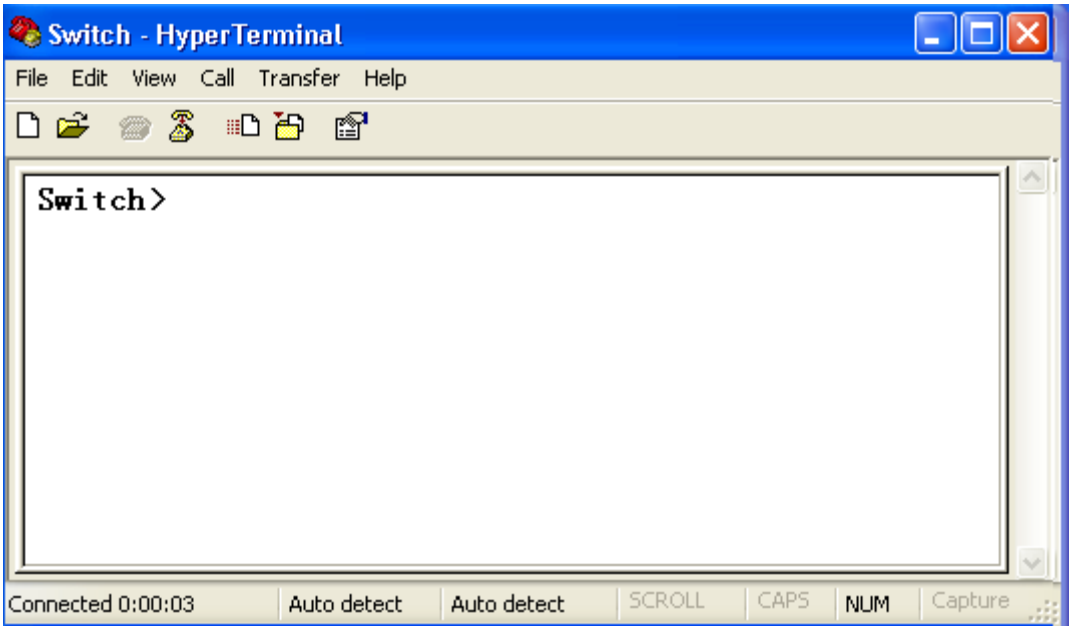


Figure 5 CLI

2.3 Access through Telnet

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

PC and the switch.

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

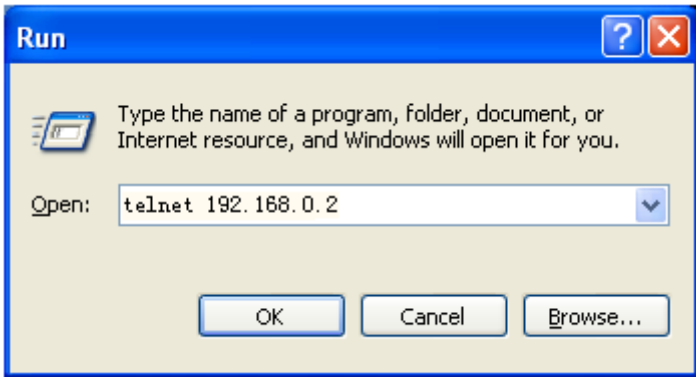


Figure 6 Telnet Access

Note:

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

2. In the Telnet interface, input "admin" in User, and "123" in Password. Press <Enter> to log in to the switch, as shown in the following figure.

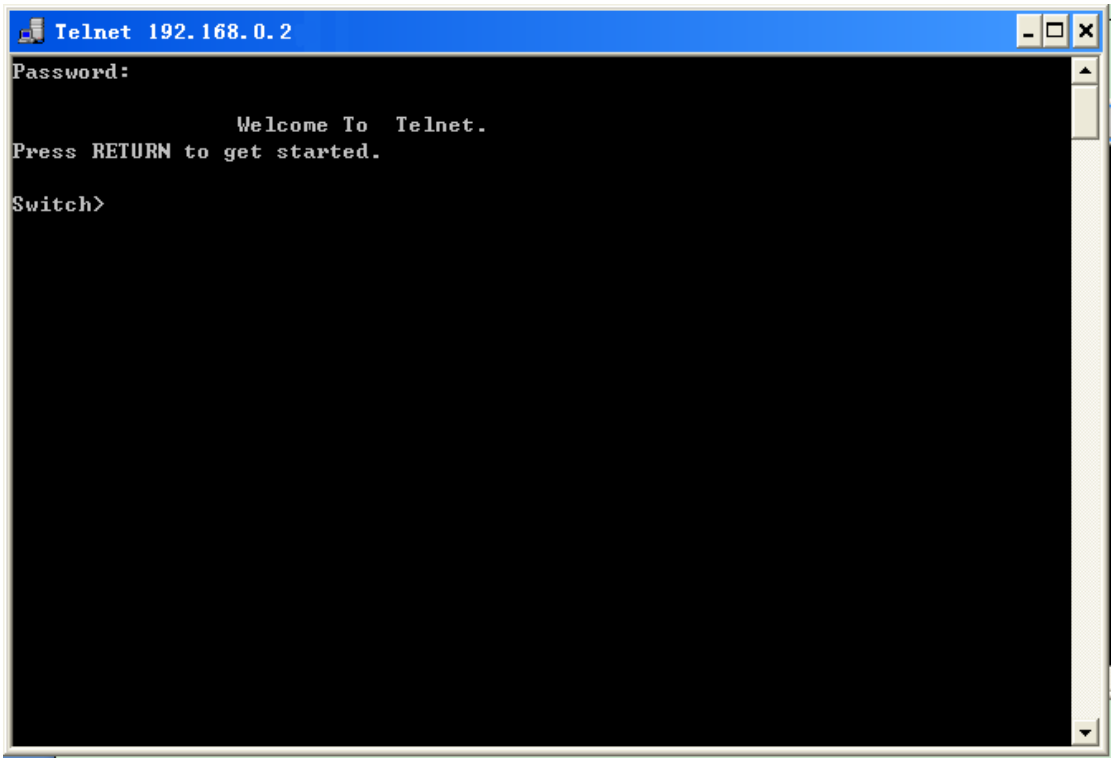


Figure 7 Telnet Interface

2.4 Access through Web

The precondition of accessing switch by Web is the normal communication between the PC and the 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 the following figure. Input the default user name "admin" and password "123". Click <Login>.

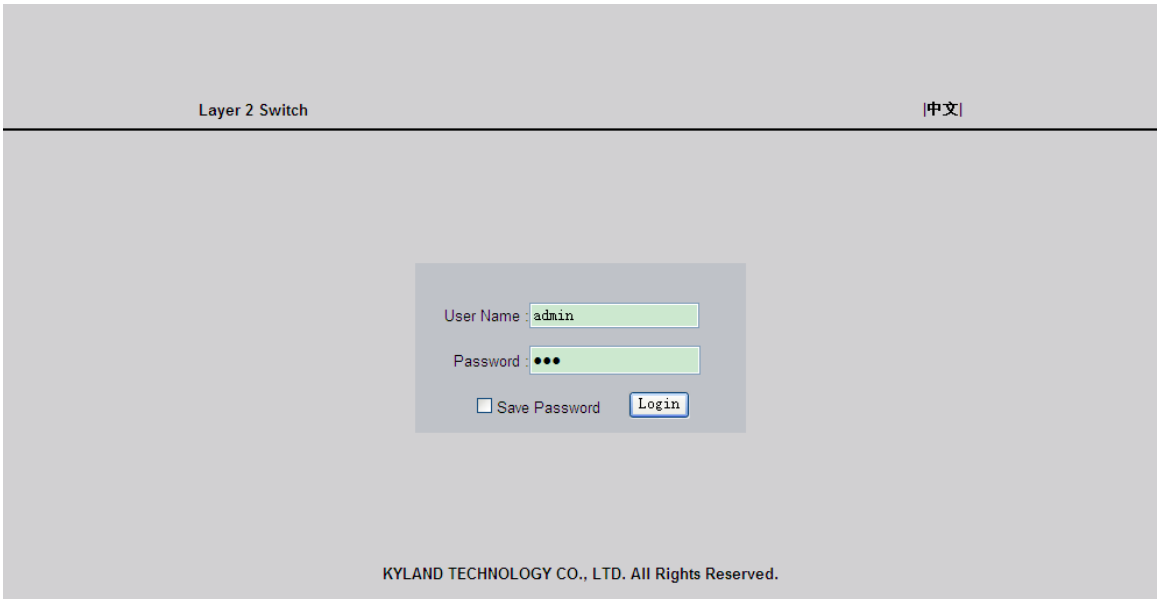


Figure 8 Web Login

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

Note:

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

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

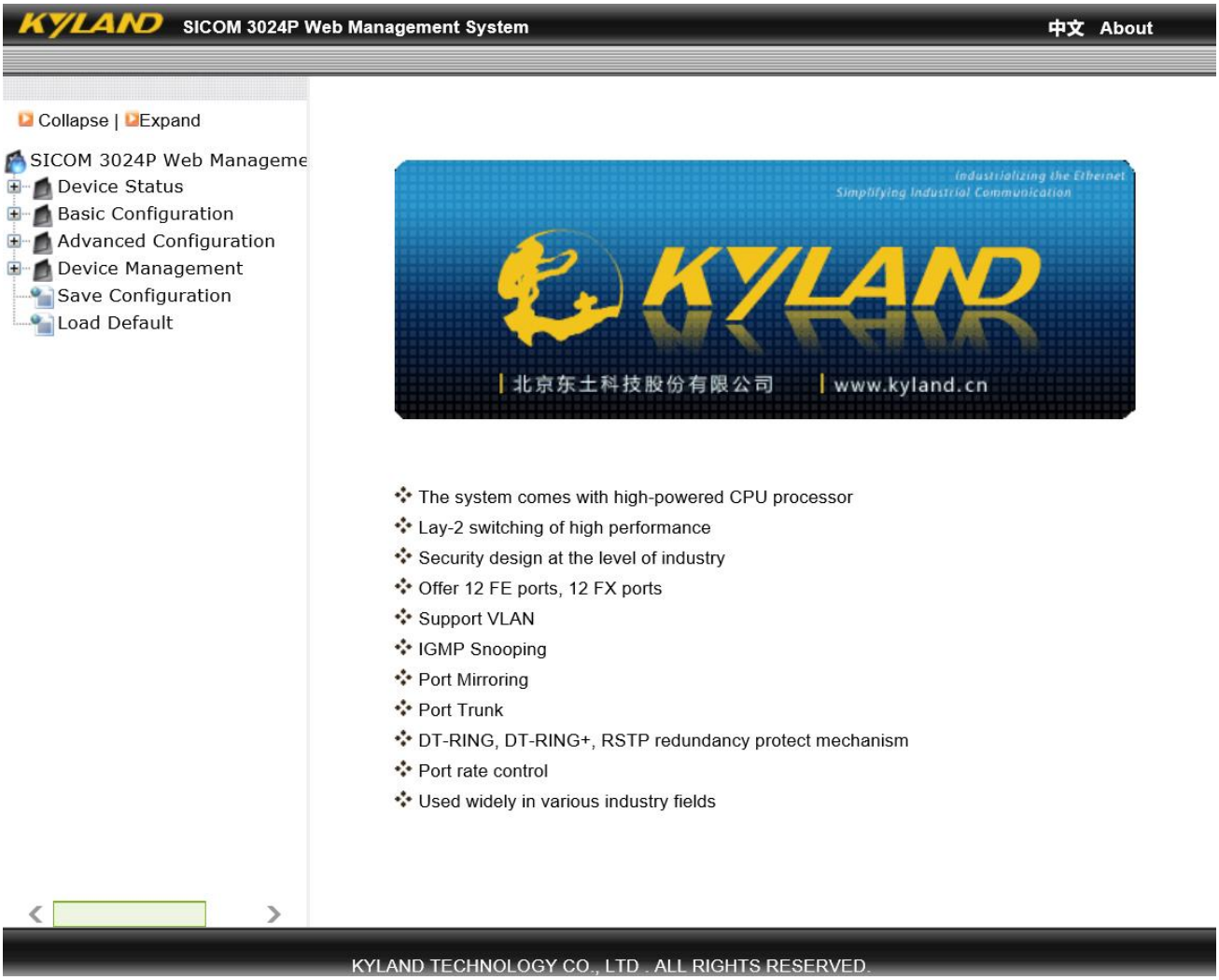


Figure 9 Web Interface

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 Configuration] or [Load Default] in the top menu. In the upper right corner, you can click <中文> to switch to the Chinese 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 version information, as shown in the following figure.

Item	Information
MAC Address	00-1E-CD-2E-C5-C9
SN	S3MOTA210200200
IP Address	192.168.0.2
Subnet Mask	255.255.255.0
GateWay	192.168.0.1
System Name	SWITCH
Device Model	SICOM3024P-12SFP12T-HV-HV
Software Version	ID:1 R4002 (2021-2-8 15:28)
FW Version	V3.0.2 (2017-8-9 15:40)

Figure 10 Basic Information

4.2 Port Status

Port status page displays the port number, administration status, link status, speed, duplex, and flow control, as shown in the following figure.

Port ID	Administration Status	Operation Status	Link	Speed	Duplex	Flow Control	RX	TX
S1/FE1	Enable	Enable	Down	---	---	---	---	---
S1/FE2	Enable	Enable	Down	---	---	---	---	---
S1/FE3	Enable	Enable	Down	---	---	---	---	---
S1/FE4	Enable	Enable	Up	100M	Full-duplex	Off	Enable	Enable
S1/FE5	Enable	Enable	Down	---	---	---	---	---
S1/FE6	Enable	Enable	Down	---	---	---	---	---
S1/FE7	Enable	Enable	Down	---	---	---	---	---
S1/FE8	Enable	Enable	Down	---	---	---	---	---
S4/GE1	Enable	Enable	Down	---	---	---	---	---
S4/GE2	Enable	Enable	Down	---	---	---	---	---
S4/GE3	Enable	Enable	Down	---	---	---	---	---
S4/GE4	Enable	Enable	Down	---	---	---	---	---

Figure 11 Port Status

Port ID

Display the type and ID of ports.

Port ID is in Sα/β format.

α indicates the number of the slot where the board resides.

β indicates the port type and ID of the board/panel where the port resides.

FE/FX/GE/GX indicate port types.

FE: 10/100Base-TX RJ45 port

FX: 100Base-FX port

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

GX: Gigabit SFP slot

Administration Status

Display the administration status of ports.

Enable: The port is available and permits data transmission.

Disable: The port is locked without data transmission.

Operation Status

Display the operation status of ports.

Link

Display the link status of ports.

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

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

Speed

Display the communication speed of Linkup ports.

Duplex

Display the duplex mode of Linkup ports.

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

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

Flow Control

Display the flow control status of Linkup ports.

RX

Options: Enable/Disable

Enable: The port can receive data.

Disable: The port cannot receive data.

TX

Options: Enable/Disable

Enable: The port can transmit data.

Disable: The port cannot transmit data.

Note:

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

4.3 Port Statistics

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

Port ID	State	Link	Bytes Sent	Packets Sent	Bytes Received	Packets Received	CRC Error	Packets 64 bytes
S1/FE1	Enable	Down	0	0	0	0	0	0
S1/FE2	Enable	Down	0	0	0	0	0	0
S1/FE3	Enable	Down	0	0	0	0	0	0
S1/FE4	Enable	Up	1670419	7399	14367882	171176	0	0
S1/FE5	Enable	Down	0	0	0	0	0	0
S1/FE6	Enable	Down	0	0	0	0	0	0
S1/FE7	Enable	Down	0	0	0	0	0	0
S1/FE8	Enable	Down	0	0	0	0	0	0
S4/GE1	Enable	Down	0	0	0	0	0	0
S4/GX2	Enable	Down	0	0	0	0	0	0
S4/GE3	Enable	Down	0	0	0	0	0	0
S4/GE4	Enable	Down	0	0	0	0	0	0

Reset

Figure 12 Port Statistics

You can click <Reset> to restart statistics collection.

4.4 Pluggable module information

4.4.1 Optical module hardware information

Optical module hardware information statistics optical module port, supplier name, model number, version, serial number, transmission distance (transmission media) and digital diagnostic functions, as shown in figure 13;

Port ID	VendorName	VendorPn	VendorRev	VendorSn	TransLen(MediaType)	DDMI
S3/FX2	Yuguang	Yuguang	1.0	SK6A234359	2000m(MMF_62P5UM_OM1), 2000m(MMF_50UM_OM2)	Int_Calibrate
S3/FX3	Yuguang	Yuguang	1.0	SK6A234382	2000m(MMF_62P5UM_OM1), 2000m(MMF_50UM_OM2)	Int_Calibrate
S3/FX4	Yuguang	Yuguang	1.0	SHAJ401272	2000m(MMF_62P5UM_OM1), 2000m(MMF_50UM_OM2)	Int_Calibrate

Figure 13 Optical module hardware information

4.4.2 Receiving & Transmitting optical power information

Receiving & Transmitting optical power statistics the current value of the receiving optical power and the transmitting optical power corresponding to the port of the inserted

optical module, as shown in figure 14;

Port	RX_POWER Current Value (dBm)	TX_POWER Current Value (dBm)
S3/FX2	-40.0	-17.4
S3/FX3	-40.0	-16.7

Figure 14 Receiving & Transmitting optical power information

4.5 System Operating Information

System operating information includes the device runtime, CPU usage, Memory usage, device temperature, and device time (local time), as shown in the following figures.

Device Operating	
Device Operating Time:	1Days,0H:35M:50S
CPU Usage:	2%(30 seconds), 1%(5 minutes)
Memory Usage:	68%
Device Temperature:	+33C
Device Time:	2015.01.20 20:20:21 Tuesday

Figure 15 System Operating Information

5 Basic Configuration

5.1 IP Address

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

Log in to the switch CLI through the console port. Run the "**show interface**" command in the Privileged mode to view the switch IP address. As shown in the following figure, the IP address is circled in red.

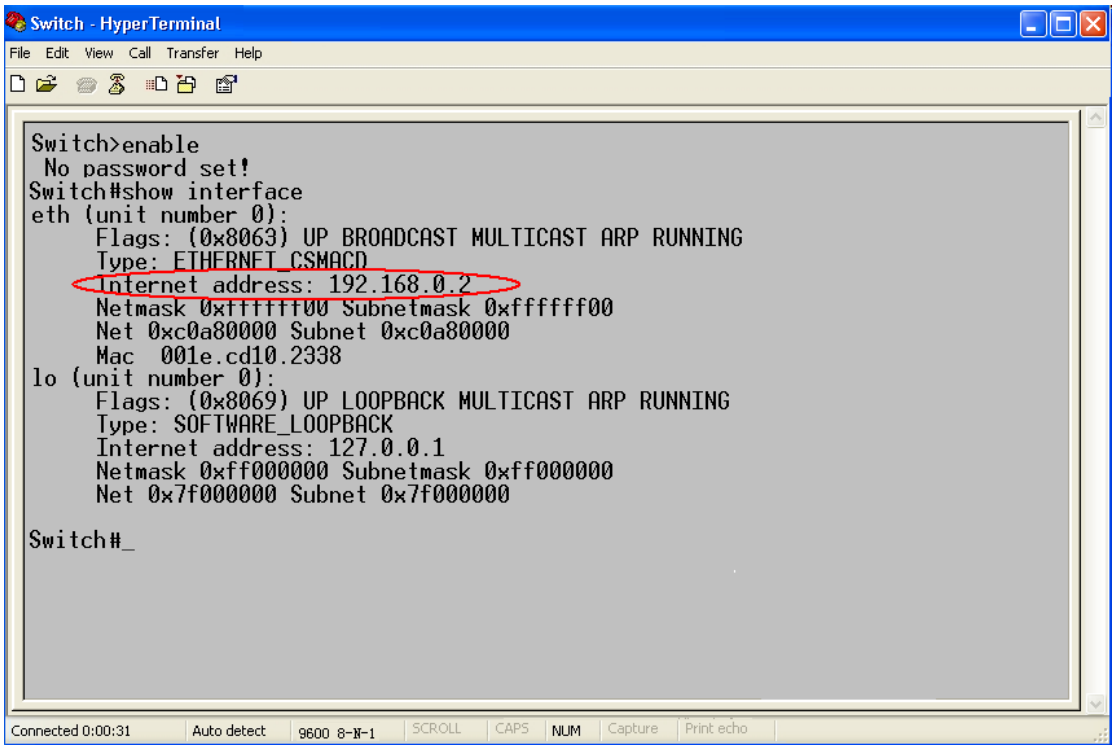


Figure 16 Viewing IP Address

2. Set the IP address.

Switch IP address and gateway can be configured manually, as shown in the following figure.

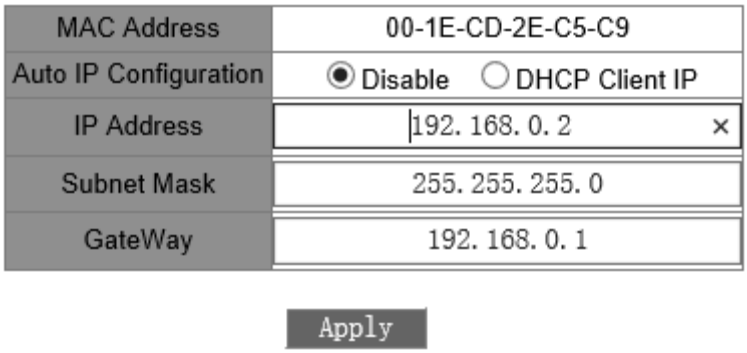


Figure 17 IP Address

Caution:

- IP address and gateway must be in the same network segment; otherwise, the IP address cannot be modified.
- For this series switches, the change in IP address will take effect immediately after modification without the need of reboot.

5.2 Basic Information

Basic information includes the project name, system name, time zone, location, contact, and system time, as shown in the following figures.

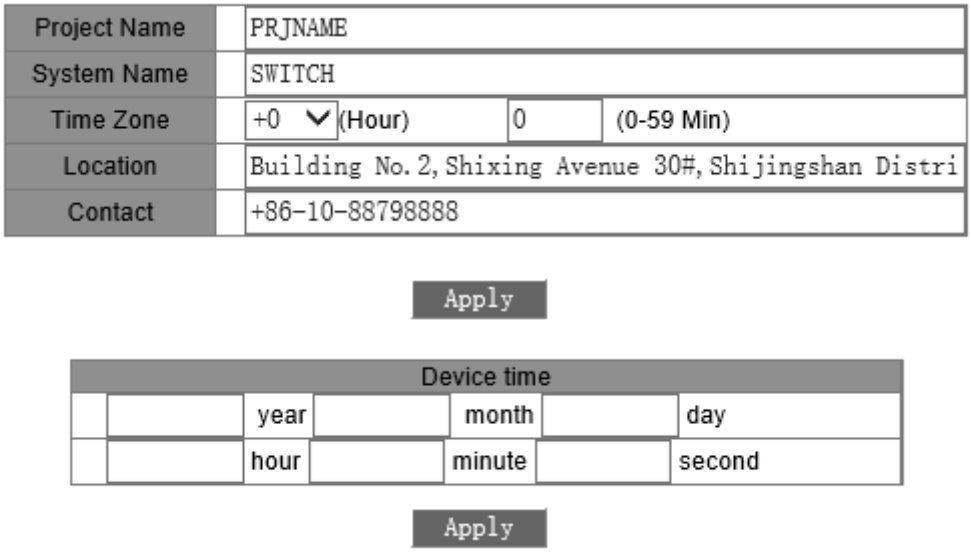


Figure 18 Device Information

Project Name

Range: 1~64 characters

System Name

Range: 1~32 characters

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 hour

0~59 min

Default: 0 hour 0 min

Function: Select the local time zone.

Location

Value: English/Chinese characters

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

Contact

Value: English/Chinese characters

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

Device time

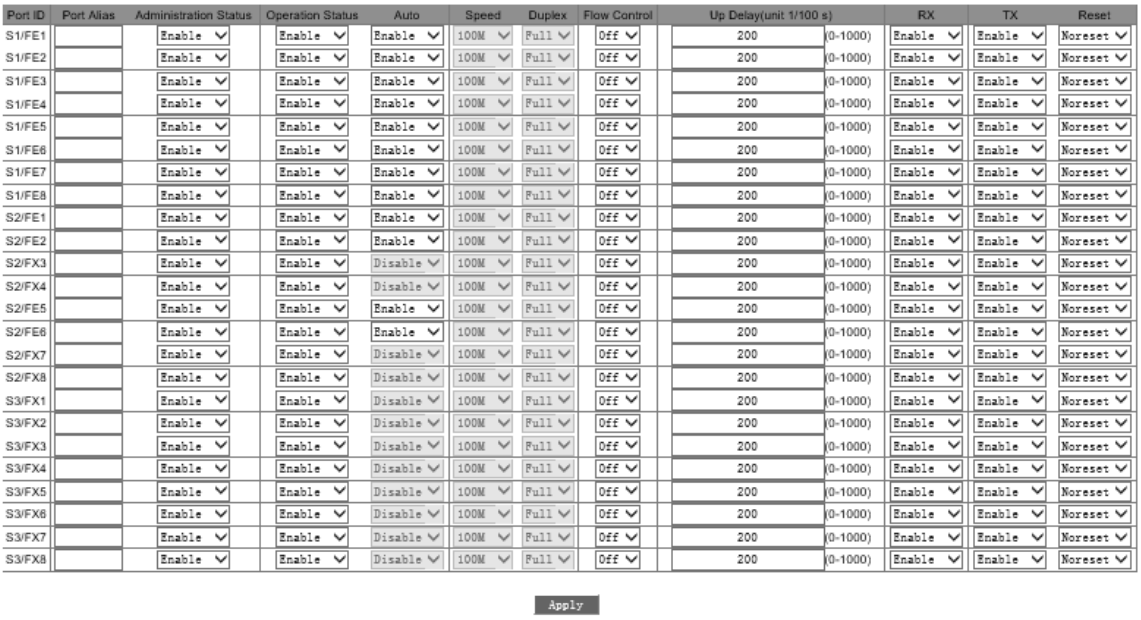
Portfolio: {YYYY, MM, DD, HH, MM, SS}

Range: YYYY (year) ranges from 2000 to 2099, MM (month) from 1 to 12, DD (day) from 1 to 31, HH (hour) from 0 to 23, and MM (minute) and SS (second) from 0 to 59.

Function: Set the system date and time. The switch can continue timekeeping after powered off.

5.3 Port Configuration

In port configuration, you can configure port status, port speed, flow control, and other information, as shown in the following figure.



Port ID	Port Alias	Administration Status	Operation Status	Auto	Speed	Duplex	Flow Control	Up Delay(unit 1/100 s)		RX	TX	Reset
S1/FE1		Enable	Enable	Enable	100M	Full	Off	200	(0-1000)	Enable	Enable	Noreset
S1/FE2		Enable	Enable	Enable	100M	Full	Off	200	(0-1000)	Enable	Enable	Noreset
S1/FE3		Enable	Enable	Enable	100M	Full	Off	200	(0-1000)	Enable	Enable	Noreset
S1/FE4		Enable	Enable	Enable	100M	Full	Off	200	(0-1000)	Enable	Enable	Noreset
S1/FE5		Enable	Enable	Enable	100M	Full	Off	200	(0-1000)	Enable	Enable	Noreset
S1/FE6		Enable	Enable	Enable	100M	Full	Off	200	(0-1000)	Enable	Enable	Noreset
S1/FE7		Enable	Enable	Enable	100M	Full	Off	200	(0-1000)	Enable	Enable	Noreset
S1/FE8		Enable	Enable	Enable	100M	Full	Off	200	(0-1000)	Enable	Enable	Noreset
S2/FE1		Enable	Enable	Enable	100M	Full	Off	200	(0-1000)	Enable	Enable	Noreset
S2/FE2		Enable	Enable	Enable	100M	Full	Off	200	(0-1000)	Enable	Enable	Noreset
S2/FX3		Enable	Enable	Disable	100M	Full	Off	200	(0-1000)	Enable	Enable	Noreset
S2/FX4		Enable	Enable	Disable	100M	Full	Off	200	(0-1000)	Enable	Enable	Noreset
S2/FE5		Enable	Enable	Enable	100M	Full	Off	200	(0-1000)	Enable	Enable	Noreset
S2/FE6		Enable	Enable	Enable	100M	Full	Off	200	(0-1000)	Enable	Enable	Noreset
S2/FX7		Enable	Enable	Disable	100M	Full	Off	200	(0-1000)	Enable	Enable	Noreset
S2/FX8		Enable	Enable	Disable	100M	Full	Off	200	(0-1000)	Enable	Enable	Noreset
S3/FX1		Enable	Enable	Disable	100M	Full	Off	200	(0-1000)	Enable	Enable	Noreset
S3/FX2		Enable	Enable	Disable	100M	Full	Off	200	(0-1000)	Enable	Enable	Noreset
S3/FX3		Enable	Enable	Disable	100M	Full	Off	200	(0-1000)	Enable	Enable	Noreset
S3/FX4		Enable	Enable	Disable	100M	Full	Off	200	(0-1000)	Enable	Enable	Noreset
S3/FX5		Enable	Enable	Disable	100M	Full	Off	200	(0-1000)	Enable	Enable	Noreset
S3/FX6		Enable	Enable	Disable	100M	Full	Off	200	(0-1000)	Enable	Enable	Noreset
S3/FX7		Enable	Enable	Disable	100M	Full	Off	200	(0-1000)	Enable	Enable	Noreset
S3/FX8		Enable	Enable	Disable	100M	Full	Off	200	(0-1000)	Enable	Enable	Noreset

Apply

Figure 19 Port Configuration

Administration Status

Options: Enable/Disable

Default: Enable

Function: Allow data transmission on port or not.

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

Operation Status

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

Auto

Options: Enable/Disable

Default: Enable

Function: Configure the auto-negotiation status of ports.

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

Caution:

- 10/100/1000Base-T(X) ports are set to enable forcibly.
- 100Base-FX ports are set to Disable forcibly.

Speed

Options: 10M/100M/1000M

Function: Configure the speed of ports forcibly.

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

Duplex

Options: Half/Full

Function: Configure the duplex mode of ports.

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

Caution:

- 10/100Base-T(X) ports can be set to auto-negotiation, 10M&full duplex, 10M&half duplex, 100M&full duplex, or 100M&half duplex.
- 100Base-FX ports are set to 100M&full duplex forcibly.
- 10/100/1000Base-T(X) ports are set to auto-negotiation forcibly.
- 1000M fiber ports can be set to auto-negotiation and 1000M&full duplex.

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

RX

Options: Enable/Disable

Default: Enable

Function: Allow the port to receive data or not.

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

TX

Options: Enable/Disable

Default: Enable

Function: Allow the port to receive data or not.

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

Reset

Options: Reset/Noreset

Default: Noreset

Function: Reset the port or not.

5.4 User management

In order to solve the security risks caused by illegal users access to switches, this series of switches manage users by level and formulate different levels based on different user permissions, to meet the diversified requirements of user permission control. Support 4

levels as shown in Table 2;

Table 2 User level description

User level	**Permission description**
Guess user	The permission is the lowest, access only some of the features in the switch, but can't modify the configuration. The following functions are not accessible to guest user: software upgrade, user management, file transfer services, restart, save configuration, and restore factory configuration.
System user	Some permissions are limited, some functions in the switch can be accessed and the configuration can be modified. The following functions are not accessible to system user: software upgrade, user management, file transfer services, restart, and restore factory configuration. Note: System user can modify the current user's login password.
Management user	Permissions are limited，only software upgrade, user management and other operations, but cannot view the log.
Audit user	Only view, configure log.

5.4.1 User management

1、User management configuration

On the user management configuration interface, the user name, service type, user level, authentication mode, password/secret key can be configured, as shown in below figure.

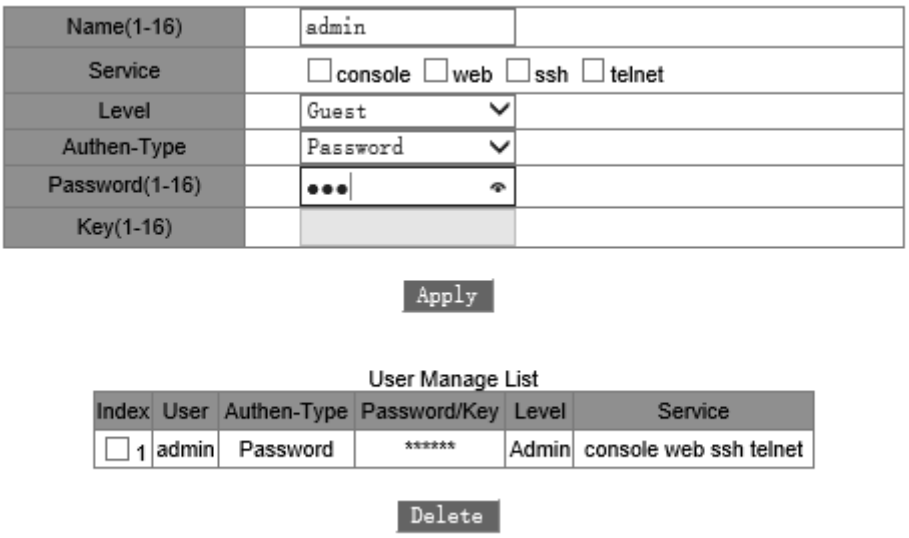


Figure 20 User management

User name

Configuration range: 1~16 character

User type

Configuration option: console/web/ssh/telnet

Function: Select the method of current user access the switch, one or more access methods can be selected.

User level

Configuration option: Guess/Audit/System/Management

Default configuration: Guess

Function: Select the level of the current user, with different levels have different operational permissions to the switch.

Authentication mode

Configuration option: password/secret key

Default configuration: password

Function: Select the authentication mode when the current user accesses the switch. The following password option need to be configured when selecting the password,; the following key option need to be configured when selecting the key.

Password

Configuration range: 1~32 character

Function: Configure the password used when the current user access the switch.

Key

Function: Select the key name that the current user uses to access the switch through the ssh.

Note:

- console/telnet/web do not support key authentication mode currently, so service type is console/telnet/web, do not select key authentication mode;
- ssh supports both password and key authentication mode;
- Up to 9 users can be configured.
- Default user admin can't be deleted. This user's default type (console, telnet, ssh, web) and suer level can't be modified; default password (123) can be modified.

2、Delete user information

Click to select the serial number in the user management list, and click the < Delete> button to delete the user.

5.4.2 SSH Key configuration

Click the navigation tree [the basic device configuration]→[User management configuration]→[SSH key configuration] menu enter into SSH key configuration interface, as shown in figure 21:

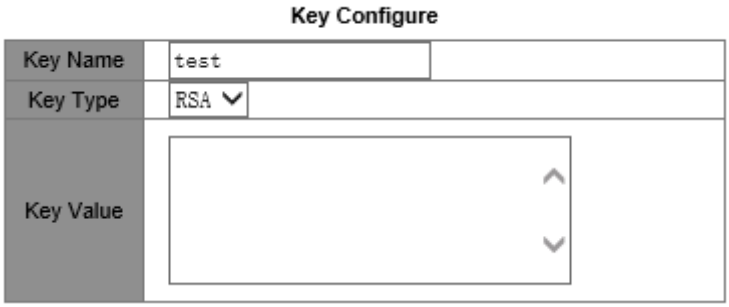


Figure 21 SSH key configuration

Key name

Configuration range: 1~16 character

Key type

Force configuration: RSA

The series product only supports RSA key algorithms.

Key value

Configuration format: {Algorithm name, public key, key information}

Algorithm name: ssh-rsa | ssh-dsa

Public key: Based on 64-bit code, length less than 2048 bytes

Key information: more information of key

Function: Configure the client's public key, usually generated by the Puttygen software and copied to the server's key value, and the private key is saved in the client.

5.5 Software Update

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

The software version update requires an FTP server.

5.5.1 HTTP upgrade

Select to upgrade by HTTP, select local version file, and then click Upgrade, restart the device after completing the upgrade.

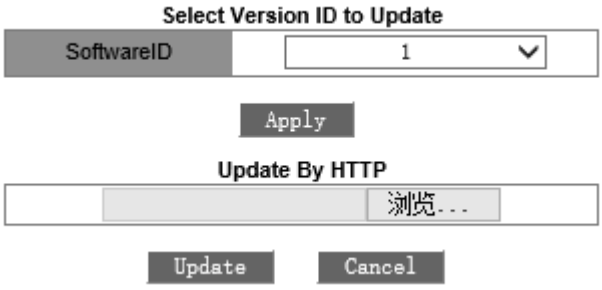


Figure 22 HTTP upgrade

5.5.2 Software Update through FTP

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

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

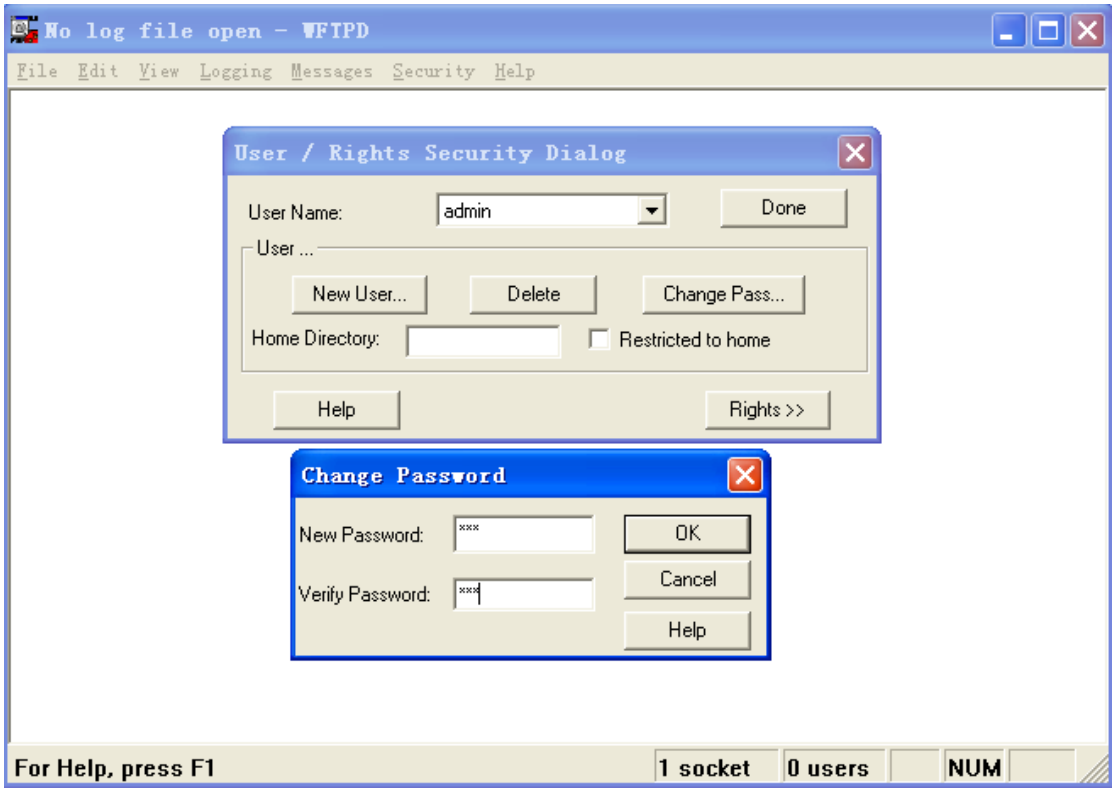


Figure 23 Creating a New FTP User

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

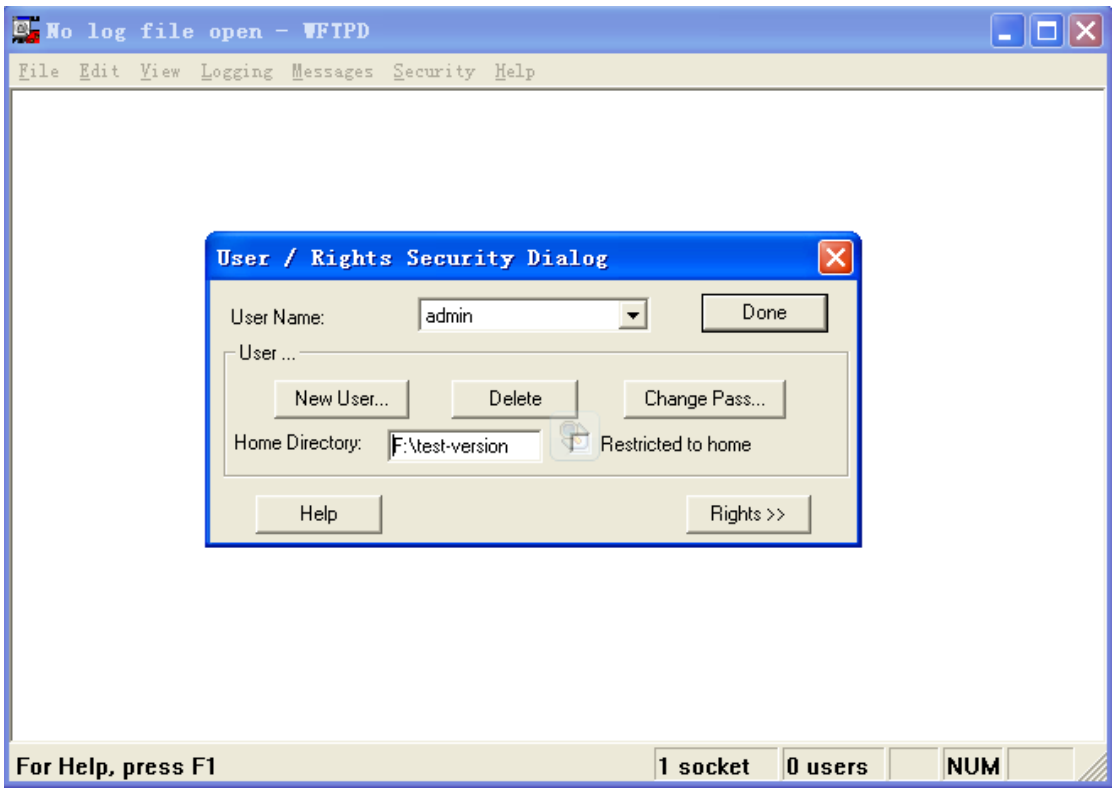


Figure 24 File Location

3. To update the BootROM software, input the following command in the Privileged mode.

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

The following table lists the parameter descriptions.

Table 3 Parameters for BootROM Update by FTP

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

4. The following figure 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>.

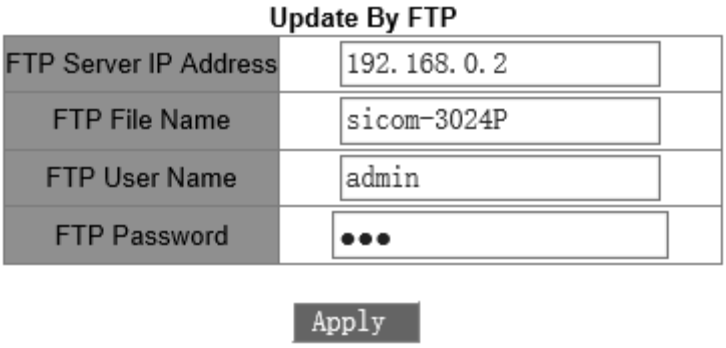


Figure 25 Software Update through FTP

Warning:

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

5. Ensure normal communication between the FTP server and the switch, as shown in the following figure.

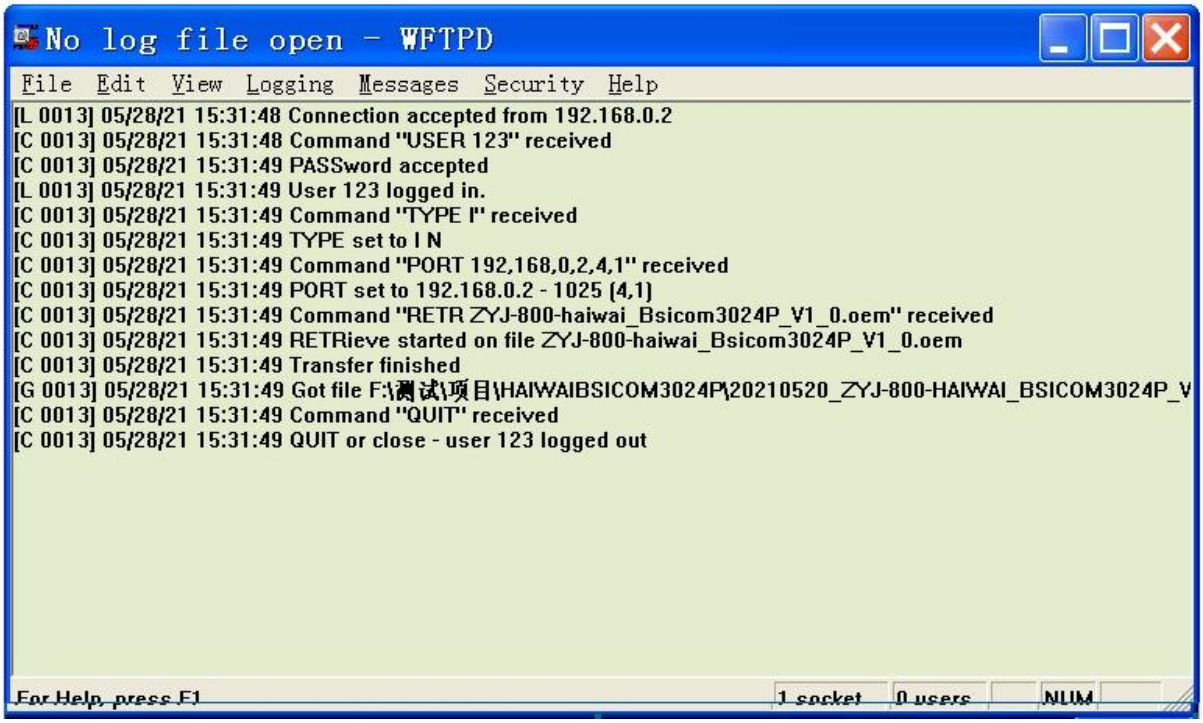


Figure 26 Normal Communication between the FTP Server and the Switch

Caution:

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

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

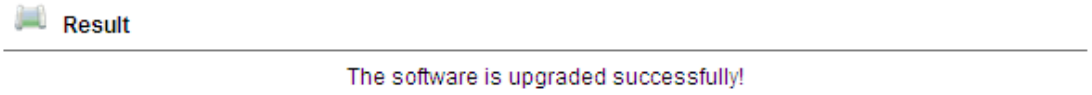


Figure 27 Successful Software Update through FTP

Warning:

- In the software update process, keeps the FTP server software running.
- When update completes, reboot the device to make the new version take effect.
- If update fails, do not reboot the device to avoid the loss of software file and startup anomaly.

5.6 Software Version Query

Two software versions can be downloaded to the switch, but only one can be in active state at a time.

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

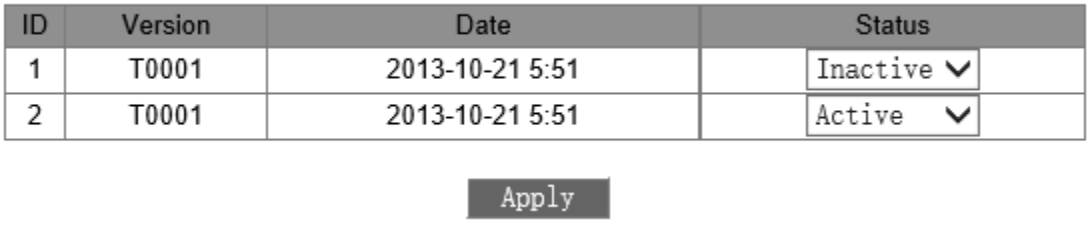


Figure 28 Software Version Query

5.7 Configuration Upload/Download

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

from the server to switch through FTP.

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

Caution:

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

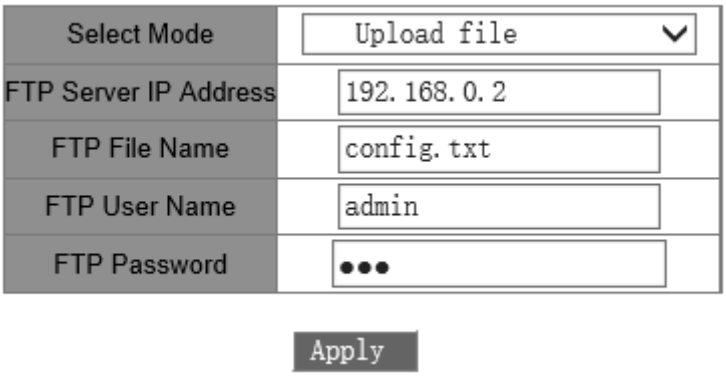


Figure 29 Configuration File Upload

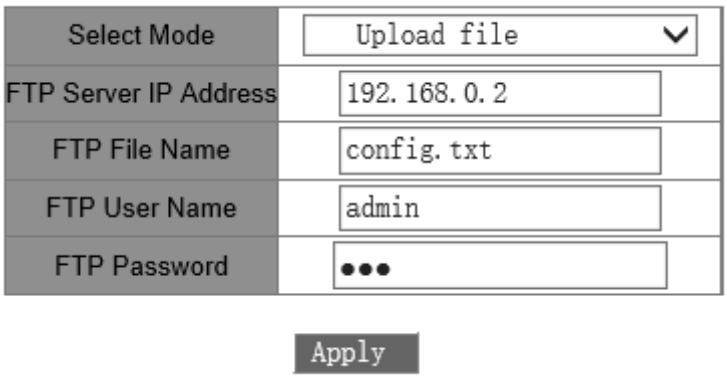


Figure 30 Configuration File Download

5.8 Logout timeout time

Logout timeout time configuration interface, the automatic logout time can be configured, as shown in Figure 31

Figure 31 Device logout time configuration

Logout time

Configuration range: 0~300 minutes

Function: The device logs out automatically after exceeding the set time.

Note: When the logout timeout set as 0, the device does not log out automatically.

5.9 Password enhanced configuration

Password enhanced configuration interface, whether enabling password enhanced can be configured, as shown in Figure 32:

Figure 32 Enable password enhanced configuration

Password enhanced

Configuration option: Enable/disable

Default configuration: Disable

Function: After enabling the password enhanced, log in to the device next time, if the password does not meet the requirements, should update to meet the required password to log in to the device.

The enhanced password requirement is as shown in Figure 33:

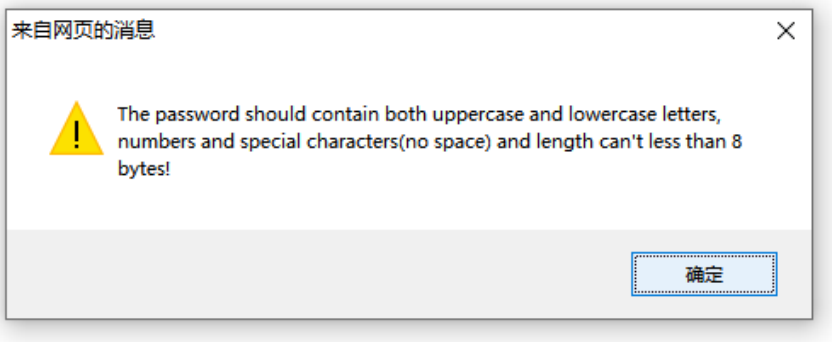


Figure 33 The enhanced password requirement

Change password interface is shown in Figure 34, enter the old password and new password and confirm the new password, click “Apply” to change the password successfully.

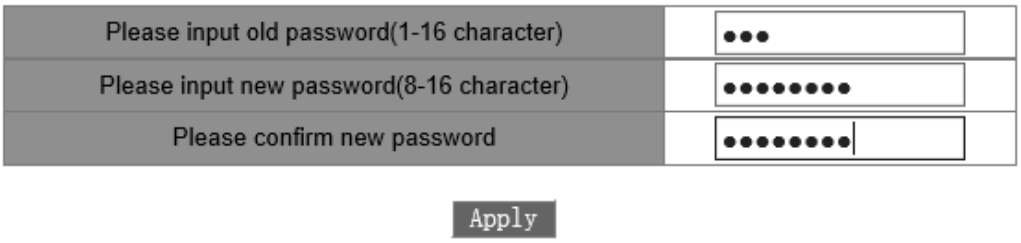


Figure 34 The enhanced password requirement

6 dvanced Configuration

6.1 Port Rate Limiting

6.1.1 Overview

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

The following packets are controlled at the ingress.

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

6.1.2 Web Configuration

1. Select the packet types for rate control, as shown in the following figure.

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

Set Packet Type for Rate Control

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

Figure 35 Packet Types for Rate Control

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

2. Configure port rate control, as shown in the following figure.

Port ID	Service		Broadcast		OutRate	
S1/FE1	0	Kbps	0	Kbps	0	Kbps
S1/FE2	0	Kbps	0	Kbps	0	Kbps
S1/FE3	0	Kbps	0	Kbps	0	Kbps
S1/FE4	0	Kbps	0	Kbps	0	Kbps
S1/FE5	0	Kbps	0	Kbps	0	Kbps
S1/FE6	0	Kbps	0	Kbps	0	Kbps
S1/FE7	0	Kbps	0	Kbps	0	Kbps
S1/FE8	0	Kbps	0	Kbps	0	Kbps
S2/FE1	0	Kbps	0	Kbps	0	Kbps
S2/FE2	0	Kbps	0	Kbps	0	Kbps
S2/FX3	0	Kbps	0	Kbps	0	Kbps
S2/FX4	0	Kbps	0	Kbps	0	Kbps
S2/FE5	0	Kbps	0	Kbps	0	Kbps
S2/FE6	0	Kbps	0	Kbps	0	Kbps
S2/FX7	0	Kbps	0	Kbps	0	Kbps
S2/FX8	0	Kbps	0	Kbps	0	Kbps
S3/FX1	0	Kbps	0	Kbps	0	Kbps
S3/FX2	0	Kbps	0	Kbps	0	Kbps
S3/FX3	0	Kbps	0	Kbps	0	Kbps
S3/FX4	0	Kbps	0	Kbps	0	Kbps
S3/FX5	0	Kbps	0	Kbps	0	Kbps
S3/FX6	0	Kbps	0	Kbps	0	Kbps
S3/FX7	0	Kbps	0	Kbps	0	Kbps
S3/FX8	0	Kbps	0	Kbps	0	Kbps

Apply

Figure 36 Port Rate Control

Service/Broadcast

Range: 64~1000000Kbps

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

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

The ingress rate for a 1000M port ranges from 64 to 1000000Kbps.

OutRate

Range: 64~1000000Kbps

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

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

The ingress rate for a 1000M port ranges from 64 to 1000000Kbps.

Caution:

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

6.1.3 Typical Configuration Example

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

Configuration steps:

1. Select unicast and multicast packets in the Service column, and broadcast packets in the Broadcast column, as shown in Figure 35.
2. On port 2, set the service rate threshold to 70Kbps, broadcast rate threshold to 80Kbps, and outgoing rate to 90Kbps, as shown in Figure 36.

6.2 VLAN

6.2.1 Overview

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

VLAN partition is not restricted by physical location. Each VLAN is regarded as a logical network. If a host in one VLAN needs to send data packets to a host in another VLAN, a

router or layer-3 device must be involved.

6.2.2 Principle

To enable network devices to distinguish packets from different VLANs, fields for identifying VLANs need to be added to packets. At present, the most commonly used protocol for VLAN identification is IEEE802.1Q. The following table 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/or deleted.
- Reserved VLANs are reserved to realize specific functions by the system and cannot be manually created and/or deleted.

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

6.2.3 Port-based VLAN

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

1.Port Type

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

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

2.PVID

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

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

The following table 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 allowed through, discard the packet.</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>

6.2.4 Web Configuration

1. Configure the VLAN transparent transmission mode, as shown in the following figure.

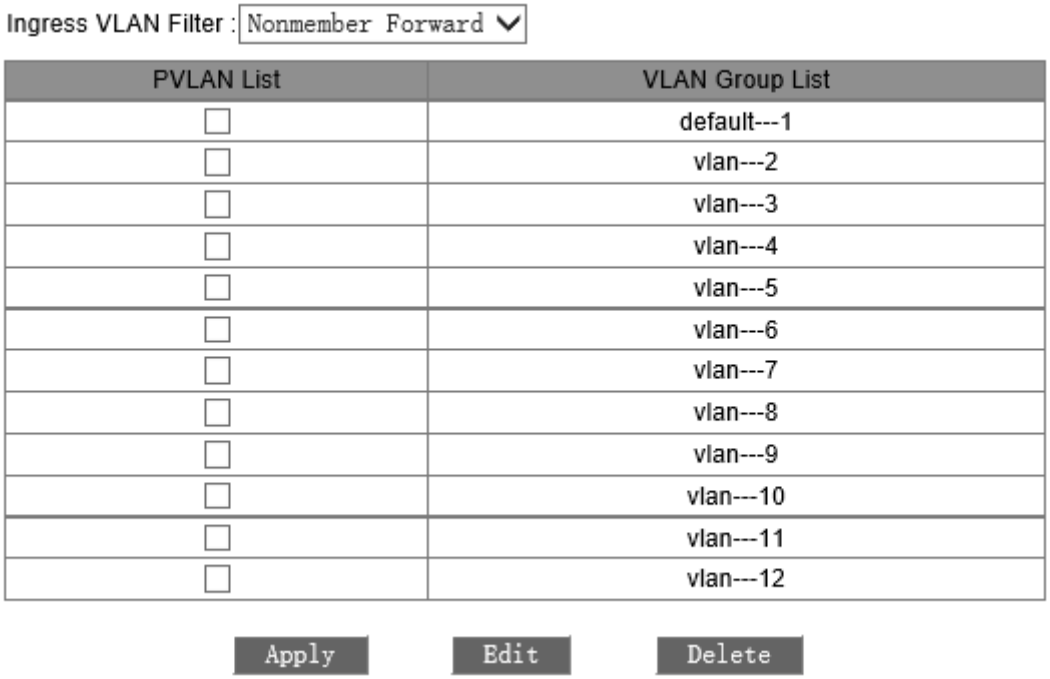


Figure 37 Configuring VLAN Transparent Transmission Mode

Ingress VLAN Filter

Options: Nonmember Drop/Nonmember Forward

Default: Nonmember Drop

Function: Configure the VLAN transparent transmission mode.

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

2. Create a VLAN.

Click <Add> in Figure 37 to create a VLAN. As shown in the following figure, select the ports to be added to the VLAN and set port parameters.

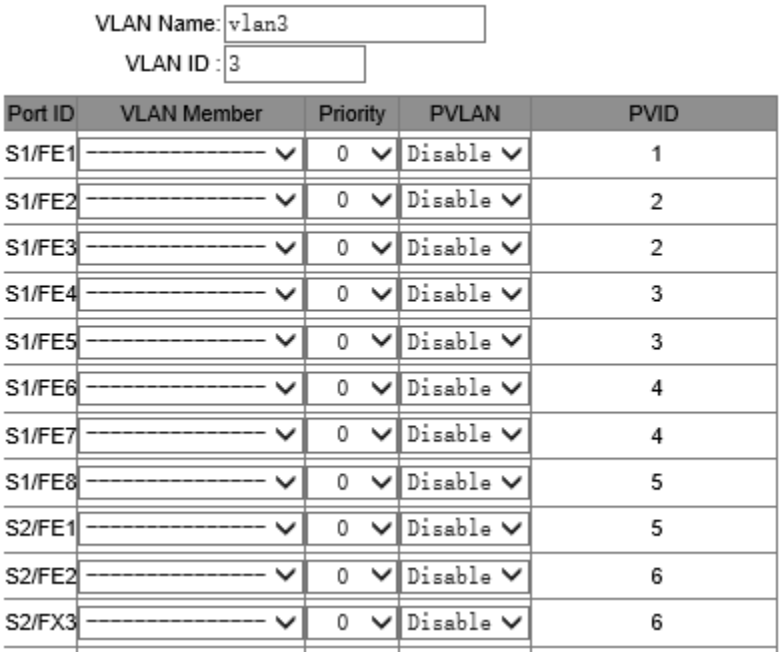


Figure 38 VLAN Configuration

VLAN Name

Range: 1~31 characters

Function: Set the VLAN name.

VLAN ID

Range: 2~4093

Function: Configure the VLAN ID.

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

VLAN Member

Options: Tagged/Untagged

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

Priority

Range: 0~7

Default: 0

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

PVLAN

Options: Enable/Disable

Default: Disable

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

Caution:

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

3. View the VLAN list, as shown in the following figure.

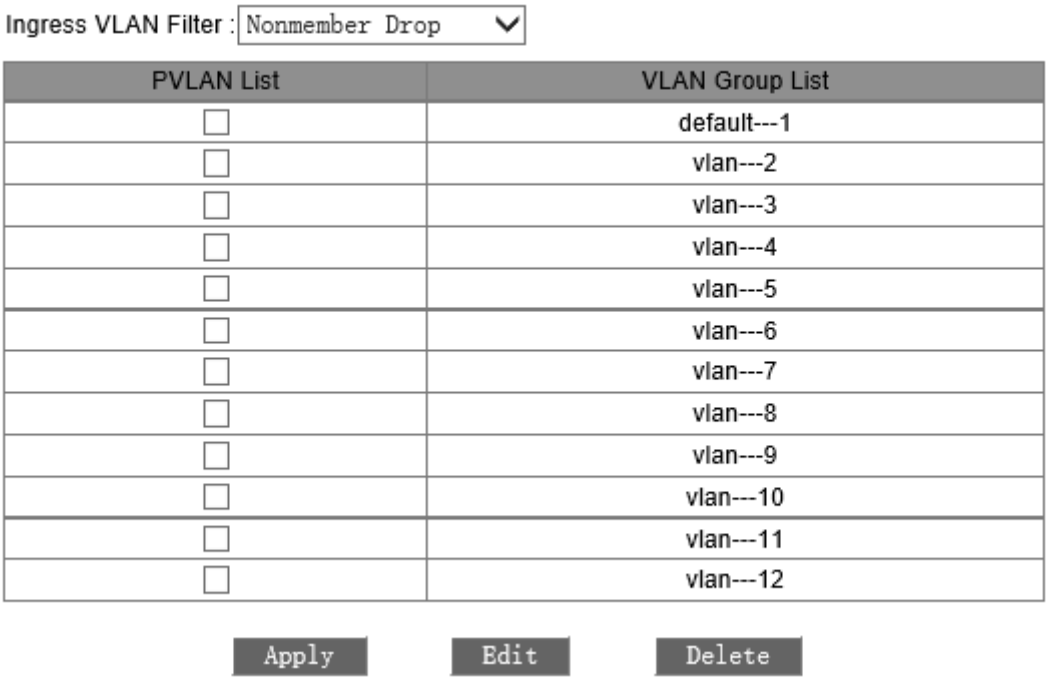


Figure 39 Viewing VLAN List

PVLAN List

Options: select/deselect

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

4. View the PVIDs of ports.

Click <Untagged Port VLAN List> in Figure 39. The following page is displayed.

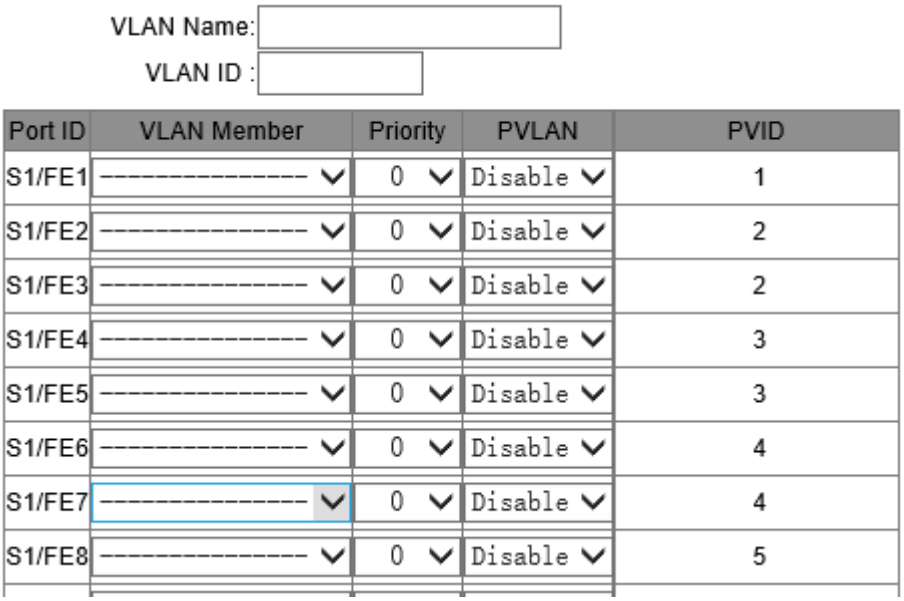


Figure 40 Port PVID List

Caution:

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

5. Modify/Delete VLAN.

Click a VLAN list in Figure 39. You can modify or delete a created VLAN. Click <Delete> at the bottom. You can delete a VLAN directly, as shown in the following figure.

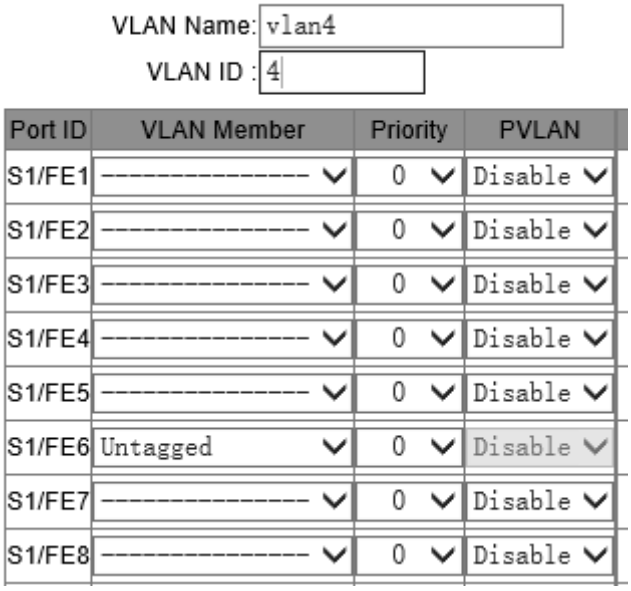


Figure 41 Modifying/Deleting a Created VLAN

6.2.5 Typical Configuration Example

As shown in the following figure, 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. The following table shows specific configuration.

Table 6 VLAN Configuration

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

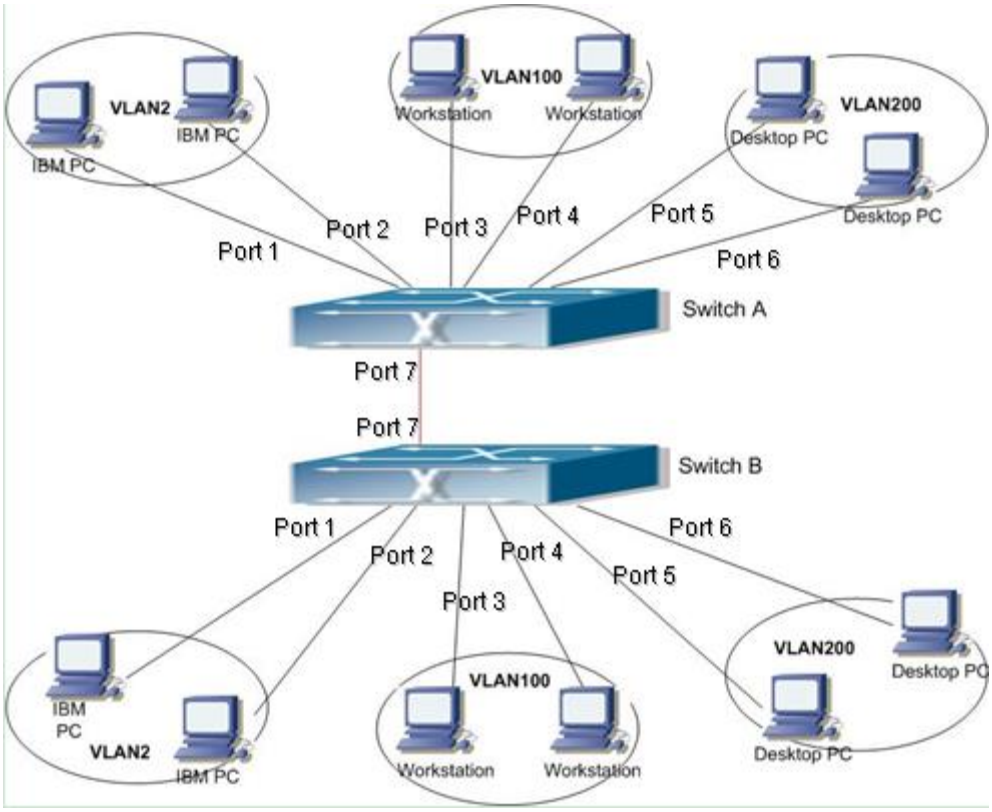


Figure 42 VLAN Application

Configurations on Switch A and Switch B:

1. Create VLAN 2, add port 1 and port 2 to VLAN 2 as Untag ports, and add port 7 into VLAN 2 as Tag port, as shown in Figure 38.
2. Create VLAN 100, add port 3 and port 4 to VLAN 100 as Untag ports, and add port 7 into VLAN 100 as Tag port, as shown in Figure 38.
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 38.

6.3 Port Mirroring

6.3.1 Overview

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

6.3.2 Description

A switch supports only one mirroring destination port but multiple source ports.

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

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

Caution:

- A mirroring source or destination port cannot be added to a Trunk group, while the port added to a Trunk group cannot be set to a mirroring destination or source port.
- A mirroring source or destination port cannot be set to a redundant port, while a redundant port cannot be set to a mirroring source or destination port.

6.3.3 Web Configuration

1. Select the mirroring destination port, as shown in the following figure.

Figure 43 Selecting a Mirroring Port

Mirroring Port

Options: Disable/a switch port

Default: Disable

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

2. Select mirroring source ports and the mirroring mode, as shown in the following figure.

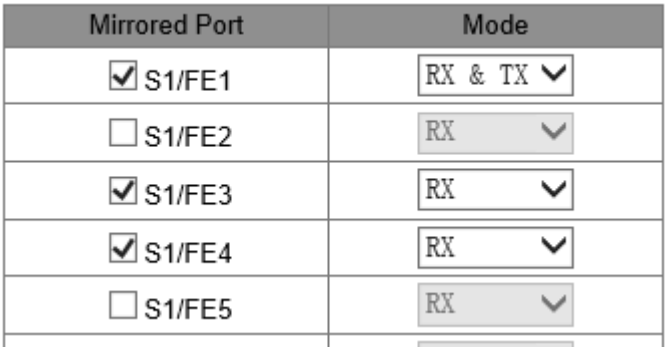


Figure 44 Mirroring Source Port

Mode

Options: RX/TX/RX & TX

Function: Select the data to be mirrored.

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

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

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

6.3.4 Typical Configuration Example

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

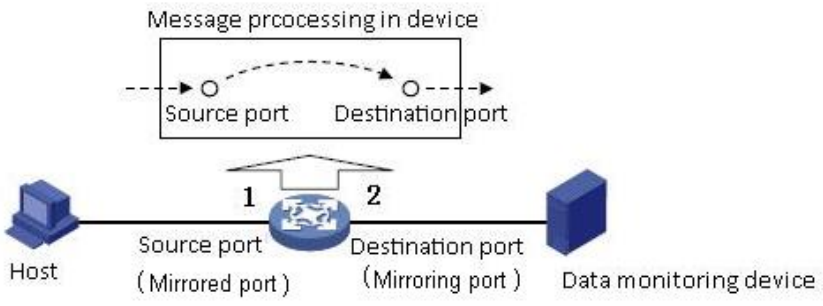


Figure 45 Port Mirroring Example

Configuration steps:

1. Set port 2 to the mirroring destination port, as shown in Figure 43.
2. Set port 1 to the mirroring source port and the port mirroring mode to TX&RX, as shown in Figure 44.

6.4 Port Trunk

6.4.1 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 can not only share the load, but also become a dynamic backup for each other to enhance connection reliability.

6.4.2 Implementation

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

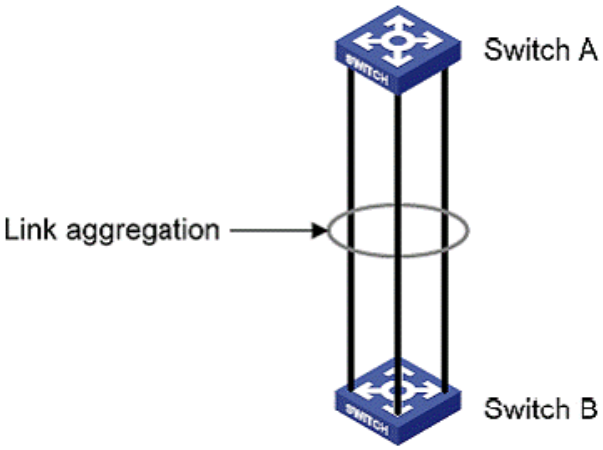


Figure 46 Port Trunk

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.

6.4.3 Description

Port trunk and the following port configurations cannot be used together:

- 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 mirroring: A port added to a trunk group cannot be configured as a mirroring destination or source port, while a mirroring destination or source port cannot be added to a trunk group.
- DHCP Snooping: A port added to a trunk group cannot be configured as a DHCP Snooping Trust-Port, while a DHCP Snooping Trust-Port cannot be added to a trunk group.

In addition, the following operations are not recommended.

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

Caution:

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

6.4.4 Web Configuration

1. Add Port Trunk.

Click <Add> to add a trunk group, as shown in the following figure.

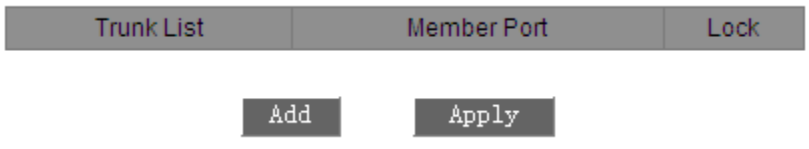


Figure 47 Adding a Trunk Group

2. Configure the trunk group, as shown in the following figure.

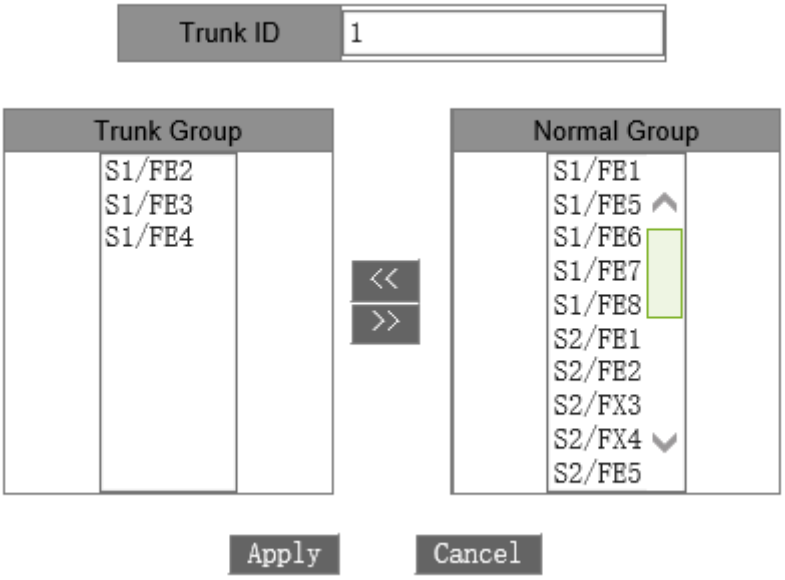


Figure 48 Configuring the Trunk Group

Trunk ID

Range: 1~14

Function: Set the trunk group ID.

Description: The series switches support a maximum of 14 trunk groups. Each group can contain a maximum of 4 ports.

3. View trunk group list, as shown in the following figure.

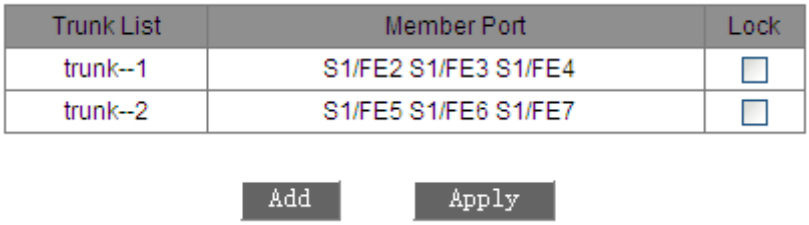


Figure 49 Trunk Group List

Lock

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

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

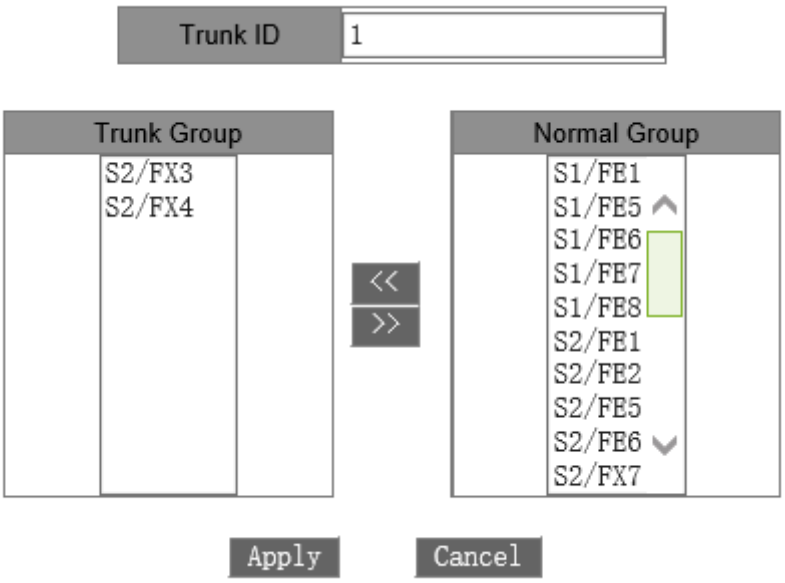


Figure 50 Modifying/Deleting a Trunk Group

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

6.4.5 Typical Configuration Example

As shown in Figure 46, port 2, port 3, and port 4 of Switch A are connected to ports of Switch B respectively, forming trunk group 1 to achieve load balancing among ports.

Configuration steps:

1.Create trunk group 1 on Switch A and add port 2, port 3, and port 4 to the group, as shown in Figure 48.

2.Create trunk group 1 on Switch B and add port 2, port 3, and port 4 to the group, as shown in Figure 48.

6.5 Link Check

6.5.1 Overview

Link check adopts periodic interaction of protocol packets to judge the link connectivity and display communication status of redundancy protocol-enabled ports. In case of a fault, the problem can be found and handled in time.

The port for which link status check is enabled sends link-check packets periodically (every 1s) to check the link status. If the port does not receive a link-check packet from the peer end within the receive timeout period (5s), it indicates that the link is abnormal and the port displays receive fault state. If the port receives a link-check packet from the peer end and the packet shows that the link-check packet is received from local within the receive timeout period (5s), the port displays the normal link state. If the port receives a link-check packet from the peer end but the packet shows that the link-check packet is not received from local within the receive timeout period (5s), the port displays send fault state.

The port for which link status check is disabled works in passive mode. That is, it does not send a link-check packet in active mode. However, after receiving a link-check packet from the peer end, this port returns a link-check packet immediately to inform the peer end that it has received the link-check packet.

Note：

- The function is valid only for a redundant protocol-enabled port
- When the DRP ring/backup port, DT-Ring ring/backup port, RSTP port for which link check is enabled is abnormal (for example, receiving is abnormal, sending is abnormal), the redundant protocol will block this port.

6.5.2 Web Configuration

The following figure shows the link check configuration.

Link Check

Port	Administration Status	Run Status
S1/FE1	Enable	Normal Link
S1/FE2	Enable	Send Fault
S1/FE3	Enable	Receive Fault
S1/FE4	Disable	Disable
S1/FE5	Disable	Disable
S1/FE6	Disable	Disable
S1/FE7	Disable	Disable
S1/FE8	Disable	Disable
S4/GE1	Disable	Disable
S4/GE2	Disable	Disable
S4/GE3	Disable	Disable
S4/GE4	Disable	Disable

Apply

Figure 51 Link Check Configuration

Administration Status

Options: Enable/Disable

Default: Enable

Description: Enable/Disable link check on port.

Caution:

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

Run Status

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

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

6.6 Static Multicast

6.6.1 Overview

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

The device supports up to 256 multicast entries.

6.6.2 Web Configuration

1. Enable static multicast, as shown in the following figure.

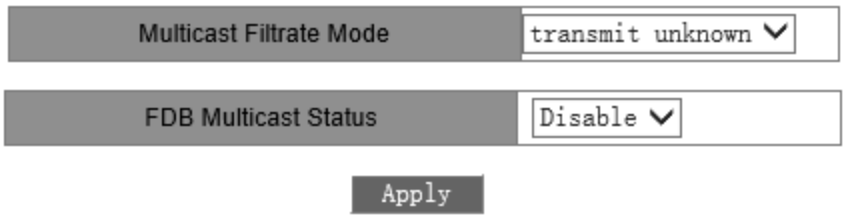


Figure 52 Enabling Static Multicast

Multicast Filtrate Mode

Options: transmit unknown/drop unknown

Default: transmit unknown

Function: Configure the processing mode for unknown multicast packets.

Description: Unknown multicast packets are packets neither manually added nor learned through IGMP Snooping or GMRP.

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

FDB Multicast Status

Options: Enable/Disable

Default: Disable

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

2. Add a static multicast entry, as shown in the following figure.

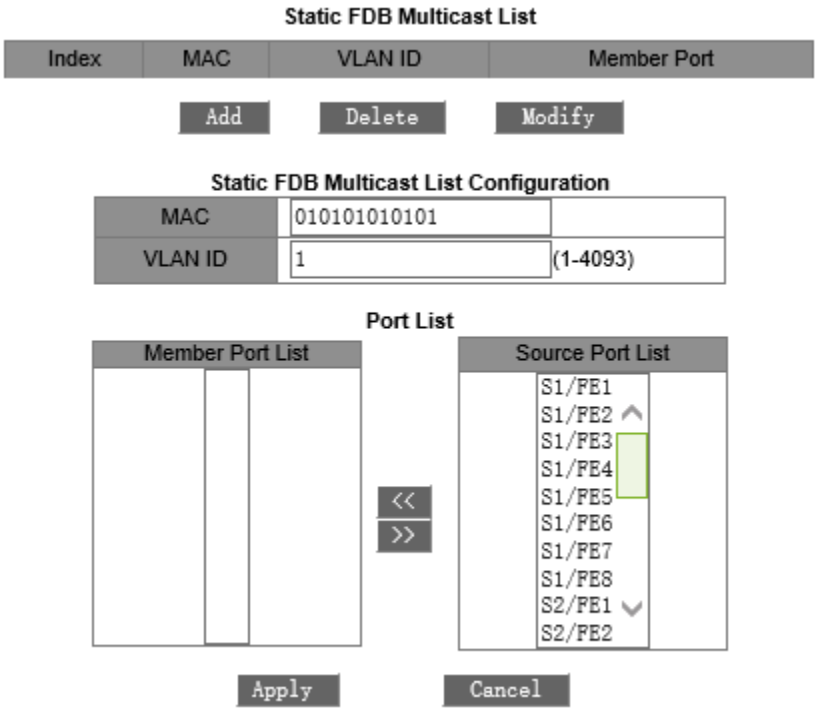


Figure 53 Adding a Static Multicast Entry

MAC

Portfolio: HHHHHHHHHHHH (H is a hexadecimal number.)

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

VLAN ID

Options: all existing VLANs

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

Member Port List

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

3. View, modify, or delete a static multicast entry, as shown in the following figure.

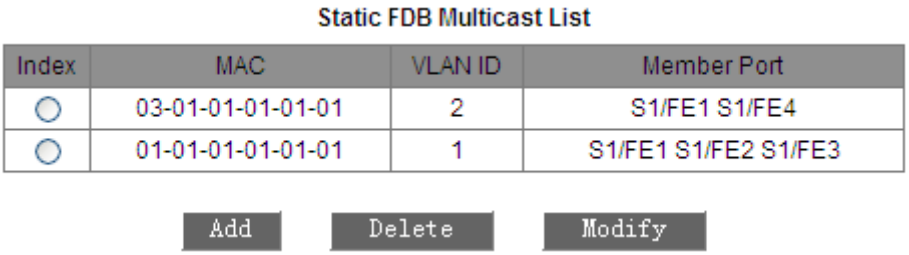


Figure 54 Operations on a Static Multicast Entry

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>.

6.7 IGMP Snooping

6.7.1 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.

6.7.2 Concepts

Querier: periodically sends IGMP general query packets to query the status of the members in the multicast group, maintaining the multicast group information. When multiple queriers exist on a network, they automatically elect the one with the smallest IP address to be the querier. Only the elected querier periodically sends IGMP general query packets. The other queriers only receive and forward IGMP query packets.

Router port: receives general query packets (on an IGMP-enabled switch) from the querier. Upon receiving an IGMP report, a switch establishes a multicast entry and adds the port that receives the IGMP report to the member port list. If a router port exists, it is also added to the member port list. Then the switch forwards the IGMP report to other devices through the router port, so that the other devices establish the same multicast entry.

6.7.3 Principle

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

General query packet: The querier periodically sends general query packets (destination IP address: 224.0.0.1) to confirm whether or not the multicast group has member ports. After receiving the query packet, a non-querier device forwards the packet to all its connected ports.

Specific query packet: If a device wants to leave a multicast group, it sends an IGMP leave packet. After receiving the leave packet, the querier sends a specific query packet (destination IP address: IP address of the multicast group) to confirm whether the group contains other member ports.

Membership report packet: If a device wants to receive the data of a multicast group, the device sends an IGMP report packet (destination IP address: IP address of the multicast group) immediately to respond to the IGMP query packet of the group.

Leave packet: If a device wants to leave a multicast group, the device will send an IGMP leave packet (destination IP address: 224.0.0.2).

6.7.4 Web Configuration

1. Enable IGMP Snooping, as shown in the following figure.

Figure 55 Enabling IGMP Snooping

IGMP Snooping Status

Options: Enable/Disable

Default: Disable

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

cannot be enabled at the same time.

Auto Query Status

Options: Enable/Disable

Default: Disable

Function: Enable or disable auto query for querier election.

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

Caution:

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

IGMP Cross Status

Options: Enable/Disable

Default: Disable

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

2. View the multicast member list, as shown in the following figure.

IGMP Member List

MAC	VLAN ID	Member
01-00-5E-7F-FF-FA	1	S1/FE1
01-00-5E-0A-18-03	1	S1/FE1
01-00-5E-51-09-08	1	S1/FE1

Figure 56 IGMP Snooping Member List

IGMP Member List

Combination: {MAC, VLAN ID, Member}

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

6.7.5 Typical Configuration Example

As shown in the following figure, 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.

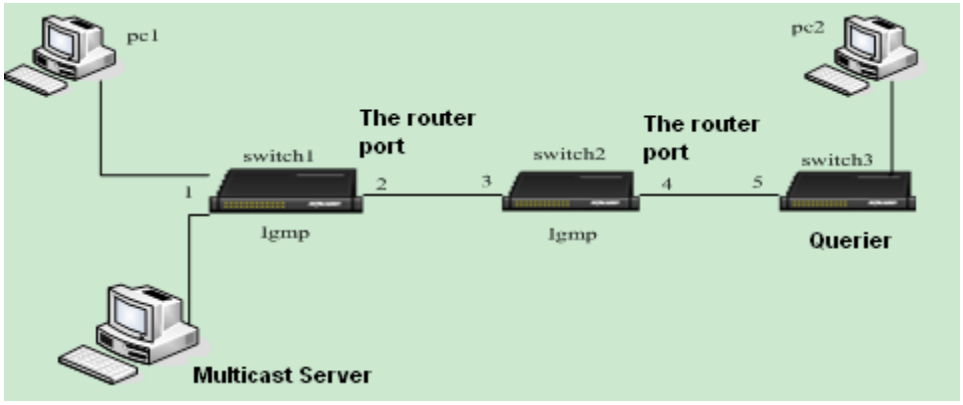


Figure 57 IGMP Snooping Configuration Example

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

6.8 ACL

6.8.1 Overview

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

6.8.2 Implementation

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

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

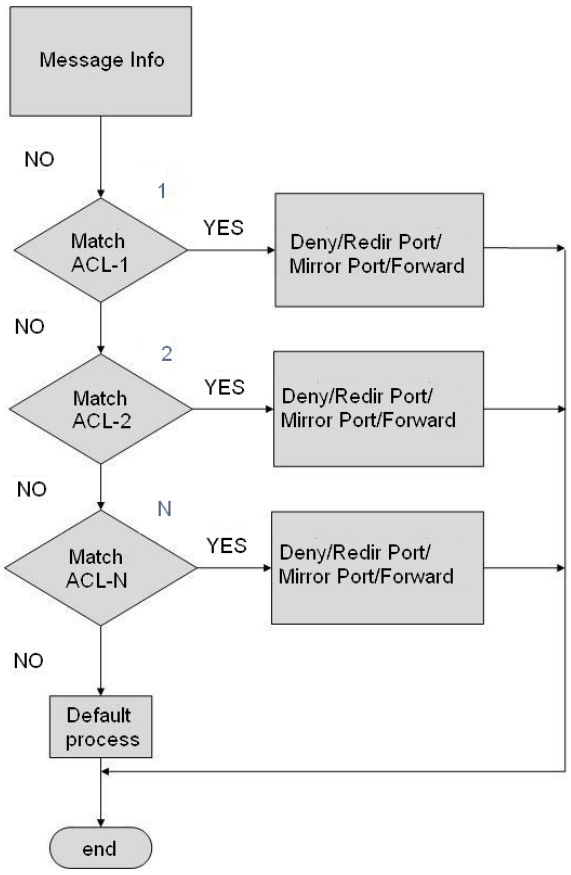


Figure 58 ACL Processing Flowchart

Note:

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

6.8.3 Web Configuration

1. Add an ACL entry.

Click <Add List> to add an ACL entry, as shown in the following figure.

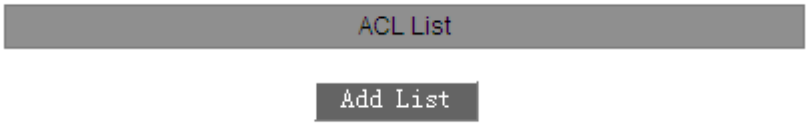


Figure 59 Adding an ACL Entry

2. Set parameters for the ACL entry, as shown in the following figure.

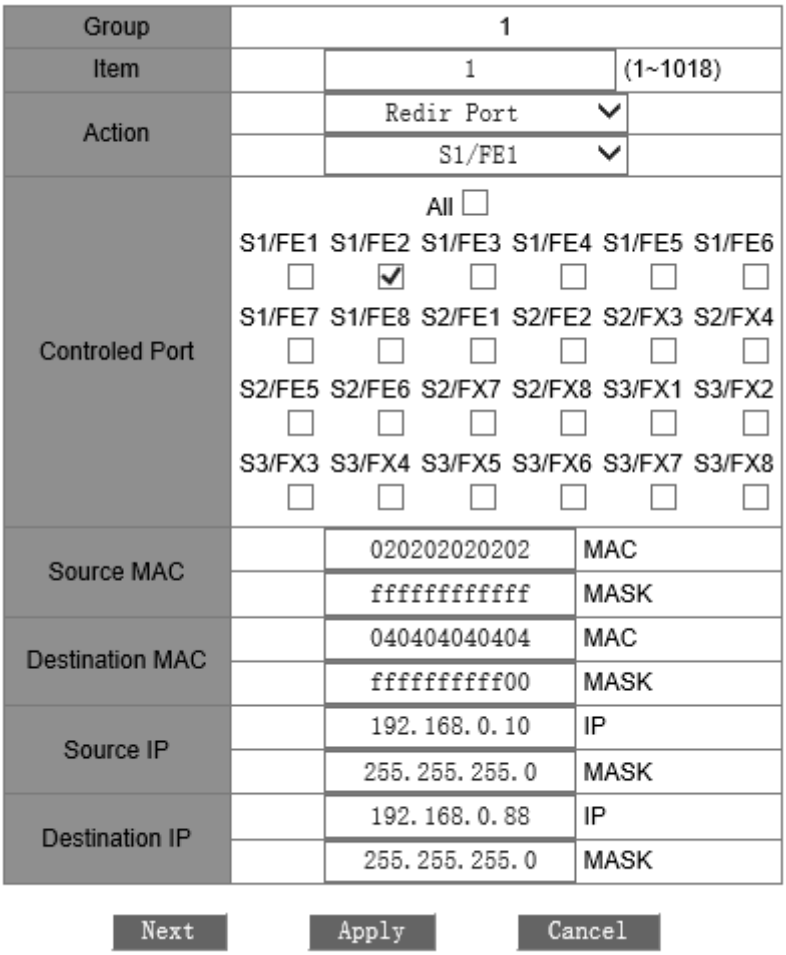


Figure 60 Setting ACL Entry Parameters 1

The switch provides a number of ACL entry parameters. You need to click <Next> to finish setting all of them, as shown in the following figures.

Configure Item

Ethernet Type		1539			(1537~65535)
TOS/DSCP		7			(0~255)
IP Protocol		6			(0~255)
IP TTL		2			(0~3)
Max ICMP		1000			(0~1023)
TCP Flag		60			(0~63)
ICMP Type Code		5000			(0~65535)
Vlan ID		2			(1~4093)
Vlan ID Range 0		5	~	16	(1~4093)
Vlan ID Range 1			~		(1~4093)
Vlan ID Range 2			~		(1~4093)
Vlan ID Range 3			~		(1~4093)

Back Next Apply Cancel

Figure 61 Setting ACL Entry Parameters 2

Configure Item

Source L4 Port		65535			(1~65535)
Src Port Range 0			~		(1~65535)
Src Port Range 1			~		(1~65535)
Src Port Range 2			~		(1~65535)
Src Port Range 3			~		(1~65535)
Destination L4 Port		21			(1~65535)
Dst Port Range 0			~		(1~65535)
Dst Port Range 1			~		(1~65535)
Dst Port Range 2			~		(1~65535)
Dst Port Range 3			~		(1~65535)
L2 Format		None			
L3 Format		None			
L4 Format		None			
Same IP		Disable			
Same L4 Port		Disable			
TCP Sequence Zero		Disable			

Back Next Apply Cancel

Figure 62 Setting ACL Entry Parameters 3

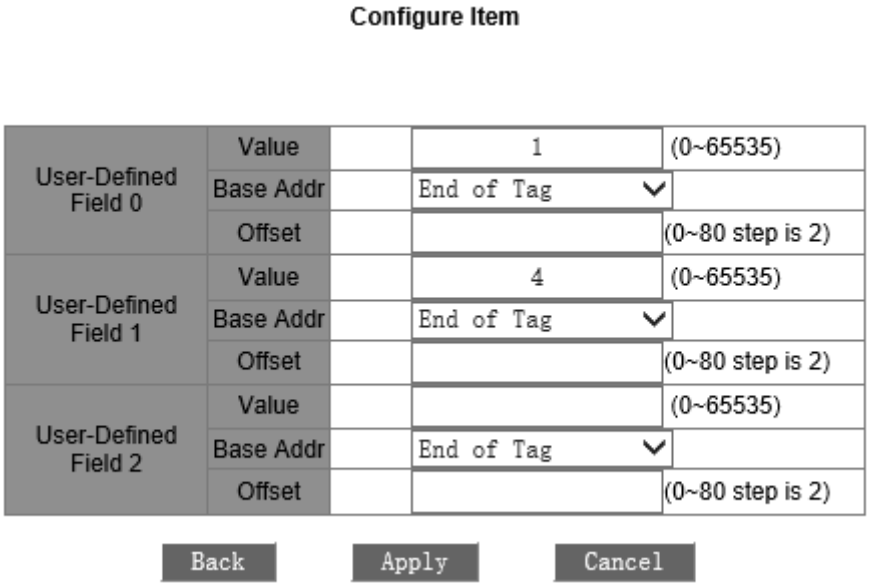


Figure 63 Setting ACL Entry Parameters 4

Group

Forcible configuration: 1

Item

Range: 1~1018

Function: Set the ID of the ACL entry. You can configure a maximum of 1023 ACL entries. When multiple ACL entries are configured, they are compared with packets in the ascending order of IDs.

Action

Options: Deny/Redir Port/Mirror Port/Forward

Default: Deny

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

Deny: Packets matching the entry will be denied.

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

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

Forward: Packets matching the entry will be forwarded to the destination port.

Control Port

Options: all/one or multiple ports

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

Source MAC

Portfolio: {MAC, MASK}

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

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

Destination MAC

Portfolio: {MAC, MASK}

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

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

Source IP

Portfolio: {IP, MASK}

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

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

Destination IP

Portfolio: {IP, MASK}

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

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

Ethernet Type

Range: 1537~65535

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

TOS/DSCP

Range: 0~255

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

IP Protocol

Range: 0~255

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

IP TTL

Range: 0~3

Function: Configure the TTL field. If the value is set to 0, the TTL of a matched packet must be 0; if the value is set to 1, the TTL of a matched packet must be 1; if the value is set to 2, the TTL of a matched packet range from 2 to 254; if the value is set to 3, the TTL of a matched packet must be 255. If the corresponding field of a packet meets these rules, then the condition is met.

Max ICMP

Range: 0~1023

Function: Configure the Max ICMP value. The value indicates the data length of ICMP packets. If the data length of an ICMP packet is larger than the value, then the condition is met.

TCP Flag

Range: 0~63

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

ICMP Type Code

Range: 0~65535

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

Vlan ID

Range: 1~4093

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

Vlan ID Range (0~3)

Portfolio: {X~Y} (X and Y (X≤Y) range from 1 to 4093. X and Y indicate the lower and upper limits of Vlan IDs respectively.)

Function: Configure the range of VLAN IDs of packets. The condition is met when the VLAN ID of a packet is within the specified range.

Source L4 Port

Range: 1~65535

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

Src Port Range (0~3)

Portfolio: {X~Y} (X and Y (X≤Y) range from 1 to 65535. X and Y indicate the lower and upper limits of Layer-4 source port numbers respectively.)

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

Destination L4 Port

Range: 1~65535

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

Dst Port Range (0~3)

Portfolio: {X~Y} (X and Y (X≤Y) range from 1 to 65535. X and Y indicate the lower and upper limits of Layer-4 destination port numbers respectively.)

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

L2 Format

Options: None/L2_Others/Ethernet_II/IEEE_802_2_SNAP

Default: None

Function: Configure Layer-2 Ethernet frame format. None indicates this rule is not used; L2_Others indicates all of the other Ethernet frame formats except Ethernet_II and

IEEE_802_2_SNAP. When the Ethernet frame format of a packet is consistent with the specified value, then the condition is met.

L3 Format

Options: None/L3_Others/IPV4_without_frag/IPV6_without_exten

Default: None

Function: Configure the Layer-3 Internet protocol. None indicates this rule is not used; L3_Others indicates all the Layer-3 Internet protocols except IPV4_without_frag and IPV6_without_exten. When the Layer-3 Internet protocol of a packet is consistent with the specified value, then the condition is met.

L4 Format

Options: None/L4_Others/TCP/UDP/ (ICMP/IGMP)

Default: None

Function: Configure the Layer-4 protocol type. None indicates this rule is not used; L4_Others indicates all the protocols except TCP, UDP, ICMP, and IGMP. When the Layer-4 protocol type of a packet is consistent with the specified value, then the condition is met.

Same IP

Options: Disable/False/True

Default: Disable

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

Disable indicates the rule is not used.

False indicates the condition is met if the source IP address of a packet is different from its destination IP address.

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

Same L4 Port

Options: Disable/False/True

Default: Disable

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

Disable indicates the rule is not used.

False indicates the condition is met if the source Layer-4 port number of a packet is different from its destination Layer-4 port number.

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

TCP Sequence Zero

Options: Disable/False/True

Default: Disable

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

Disable indicates the rule is not used.

False indicates the condition is met if the TCP Sequence field of a packet is not 0.

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

User-Defined Field (0~2)

Portfolio: {Value, Base Addr, Offset}

Range or Options:

Value: 1~65535

Base Addr: End of Tag (Default)/End of EthType/End of IP Header

Offset: 0~80, the step is 2

Function: Define a field as an ACL condition. Value indicates the value to be matched; Base Addr indicates the reference point of a packet; End of Tag indicates the end of the Tag field is the reference point; End of EthType indicates the end of the EthType field is the reference point; End of IP Header indicates the end of the IP header field is the reference point; Offset indicates the offset of the value compared with the reference point. If the *Offset* of a packet compared with *Base Addr* is *Value*, then the condition is met.

Note:

It is not necessary to set all these parameters, but at least one parameter needs to be set. If only one parameter is required, then leave all the other parameters empty.

3. View the ACL.

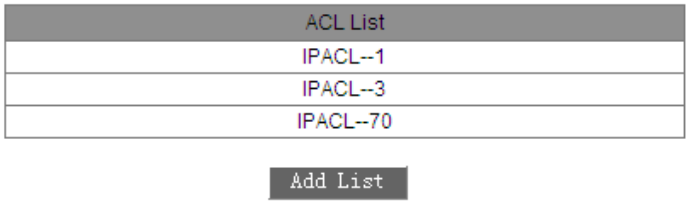


Figure 64 ACL Entries

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

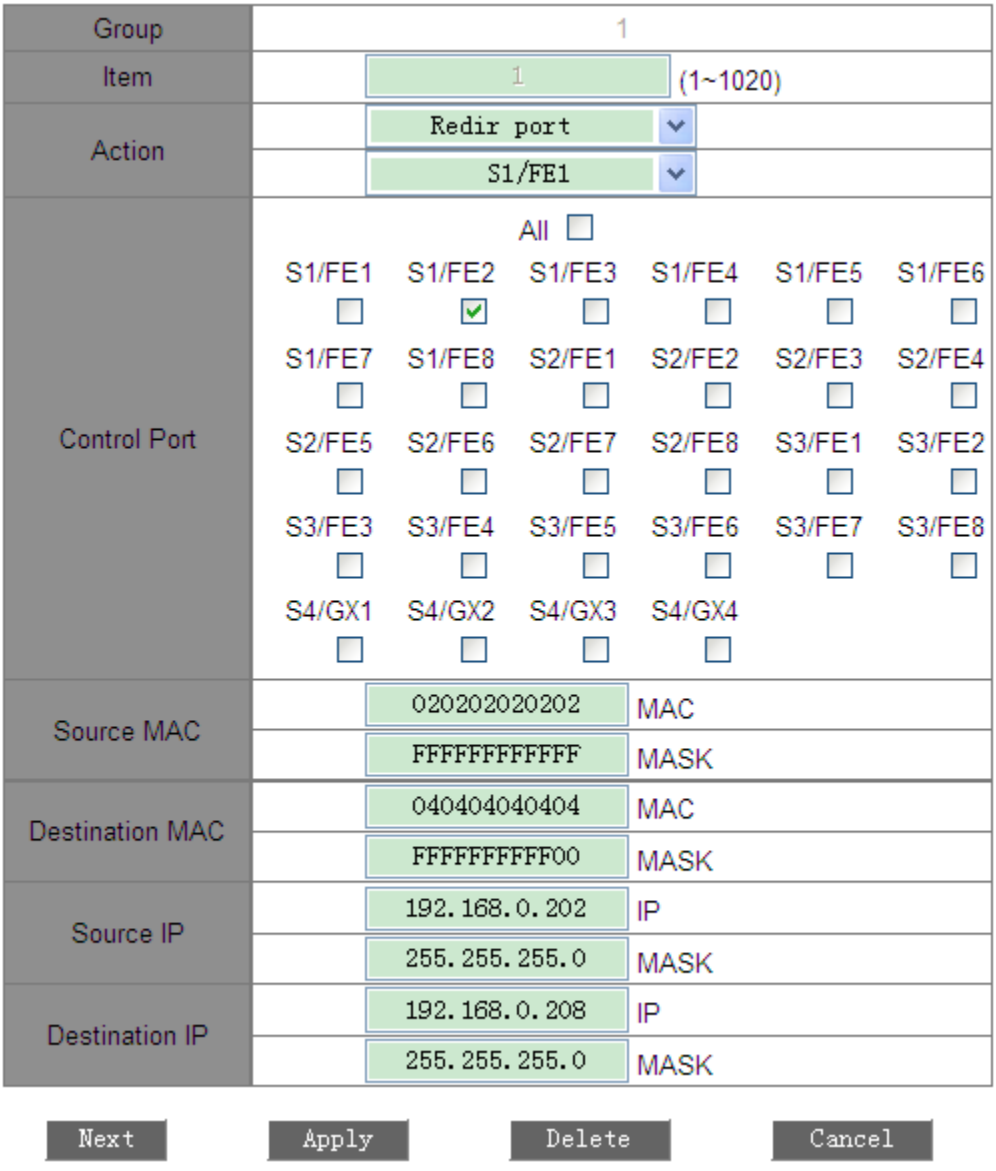


Figure 65 Modifying/Deleting an ACL Entry

Click <Apply> for changes to take effect after modification. Click <Delete> to delete the ACL entry.

6.8.4 Typical Configuration Example

The following uses SICOM3024P V3.2 as an example to describe the configuration steps for an ACL entry.

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

Configuration steps:

1. Set the action to Redir Port and select port 1 in the drop-down list, as shown in Figure 60.
2. Select FE2 in Control Port, as shown in Figure 60.
3. Set the source MAC address to 020202020202 and subnet mask to FFFFFFFFFFFF, as shown in Figure 60.
4. Keep all the other parameters empty.

6.9 ARP

6.9.1 Overview

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

The series switches 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 expire, be updated by a new ARP packet, or be overwritten by a static ARP entry.

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

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

6.9.3 Web Configuration

1. Configure ARP aging time, as shown in the following figure.

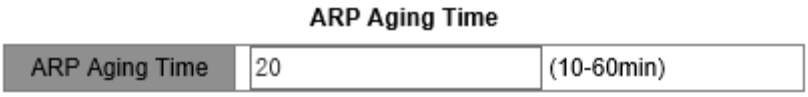


Figure 66 Configuring Aging Time

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 the following figure.

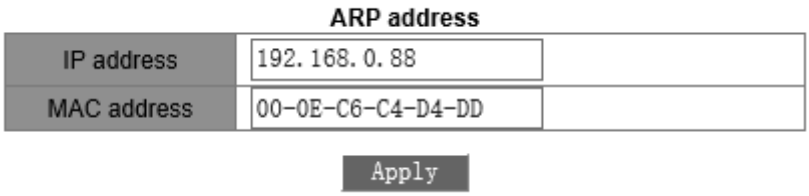


Figure 67 Adding a Static ARP Entry

ARP address

Portfolio: {IP address, MAC address}

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

Function: Configure a 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 the following figure.

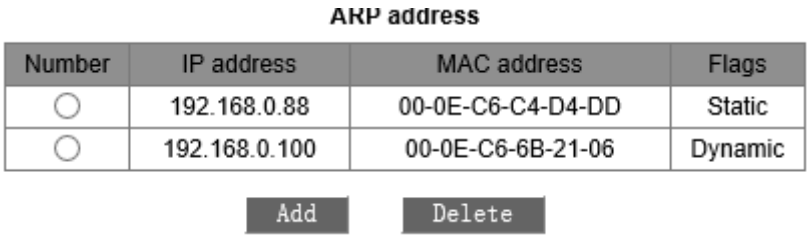


Figure 68 ARP Address Table

ARP address

Portfolio: {IP address, MAC address, Flags}

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

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

Caution:

You cannot delete dynamic ARP entries.

6.10 SNMP

6.10.1 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.

6.10.2 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 the 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.

6.10.3 Description

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

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

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

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

6.10.4 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. The following figure shows the relationships among the NMS, agent, and MIB.

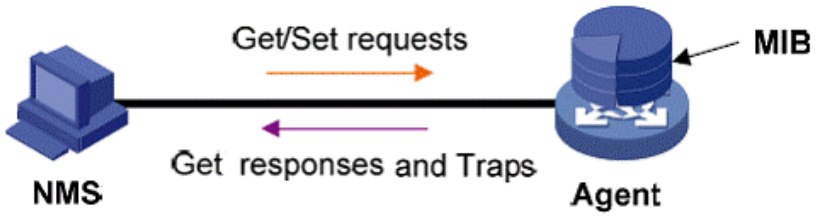


Figure 69 Relationship among NMS, Agent, and MIB

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 the following figure, the OID of object A is 1.2.1.1.

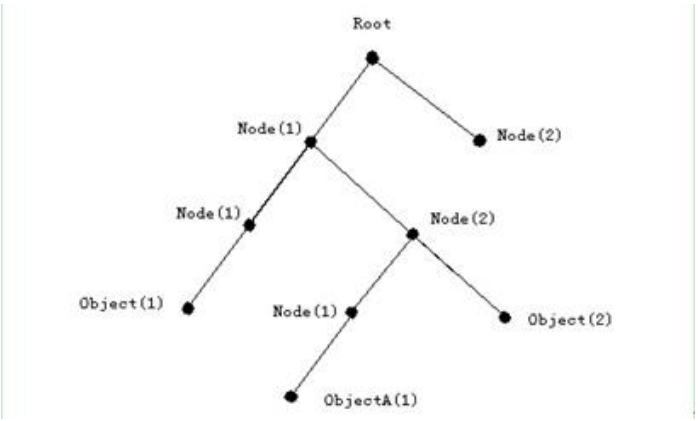


Figure 70 MIB Tree Structure

6.10.5 Web Configuration

1. Enable SNMP, as shown in the following figure.

Figure 71 Enabling SNMP

SNMP Status

Options: Enable/Disable

Default: Enable

Function: Enable or disable SNMP.

2. Configure access rights, as shown in the following figure.

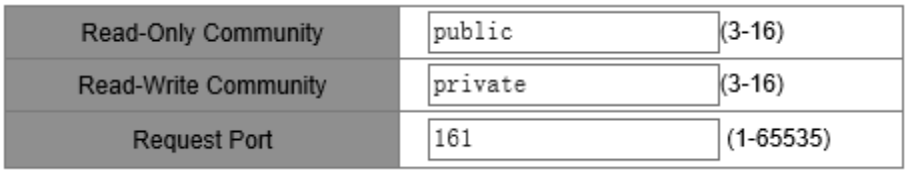


Figure 72 Access Rights Configuration

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 the following figure.

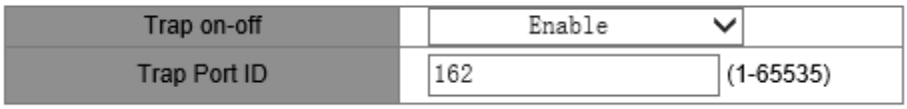


Figure 73 Trap Configuration

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 the following figure.

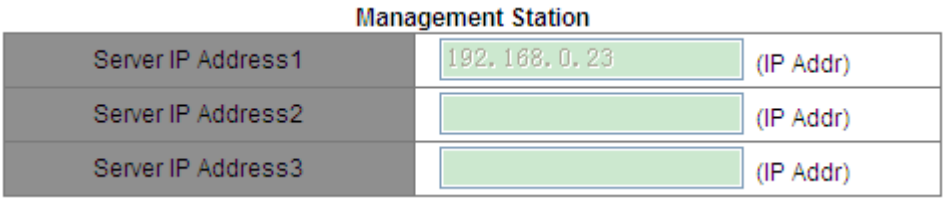


Figure 74 IP Address of Management Server

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

6.10.6 Typical Configuration Example

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

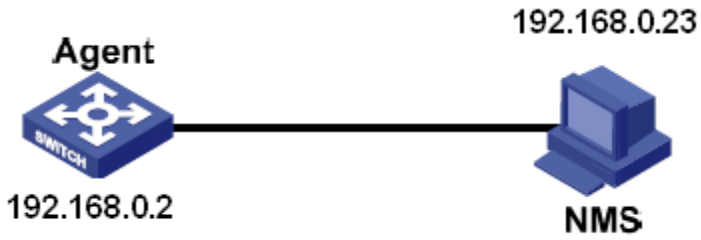


Figure 75 SNMP Configuration Example

Configuration on the Agent:

1. Enable SNMP, as shown in Figure 71.
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 72.
3. Enable trap sending, set trap port number to 162, and IP address of server to 192.168.0.23, as shown in Figure 73.

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

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

6.10.7 SNMPv3 Introduce

SNMP v3 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.

6.10.8 Implementation

SNMP v3 provides five 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.

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 view table refers to the MIB view information, which specifies the MIB information that can be accessed by users. The MIB view may contain all nodes of a certain MIB subtree (that is, users are allowed to access all nodes of the MIB subtree) or contain none of the nodes of a certain MIB subtree (that is, users are not allowed to access any node of the MIB subtree).

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

6.10.9 SNMPV3 Web page configuration

1、Configurate user table

Click the navigation tree [Device advanced configuration] →[SNMP configuration]→[V3 user table configuration] menu, enter into SNMP v3 user table configuration interface, as shown in figure 76;

Number	State	User Name	Authentication protocol	Authentication password	Privacy protocol	Privacy password
1	----	test1	HMAC-MD5	••••••	CBC-DES	••••••
2	----	test2	HMAC-SHA	••••••	CBC-DES	••••••
3	----		NONE		NONE	
4	----		NONE		NONE	
5	----		NONE		NONE	
6	----		NONE		NONE	
7	----		NONE		NONE	
8	----		NONE		NONE	
9	----		NONE		NONE	
10	----		NONE		NONE	
11	----		NONE		NONE	
12	----		NONE		NONE	
13	----		NONE		NONE	
14	----		NONE		NONE	
15	----		NONE		NONE	
16	----		NONE		NONE	

Apply Help

Figure 76 SNMP v3 user table configuration

User Name

Configuration range: 4~16 character

Function: User name that created.

Authentication Encryption Protocol

Configuration option: NONE/HMAC-MD5/HMAC-SHA

Default configuration: NONE

Function: Select one authentication encryption protocol.

Authentication Encryption Password

Configuration range: 4~16 character

Function: Create authentication encryption password.

Message Encryption Protocol

Configuration option: NONE/HMAC-DES

Default configuration: NONE

Function: Select one message encryption protocol.

Message Encryption Password

Configuration range: 4~16 character

Function: Create message encryption password.

2、Configure group table

Click the navigation tree [Device advanced configuration] →[SNMP configuration]→[V3 group table] menu, enter in SNMP v3 group table configuration interface, as shown in Figure 77;

GROUP TABLE

Number	GroupName	SecurityName	SecurityModel
1	Group1	test1	SNMP V3
2	Group2	test2	SNMP V3
3			SNMP V3
4			SNMP V3
5			SNMP V3
6			SNMP V3
7			SNMP V3
8			SNMP V3
9			SNMP V3
10			SNMP V3
11			SNMP V3
12			SNMP V3
13			SNMP V3
14			SNMP V3
15			SNMP V3
16			SNMP V3

Apply Help

Figure 77 SNMP v3 group table configuration

Group Name

Configuration range: 4~16 character

Function: Configurate group table name.

Security Name

Configuration range: Created user name, 4~16 character

Function: Configure the security name, which should be same with the user name in the user table. Users with the same group name belong to the same group.

Security Mode

Default configuration: SNMPv3

Description: SNMPv3 means to use USM (User-Based Security Model) technology, which is currently forced to SNMPv3 mode.

3、Configure the context table

Click the navigation tree[Device advanced configuration]→[SNMP configuration]→[V3 context table configuration] menu, enter into SNMP v3 context table configuration interface, as shown in Figure 78;

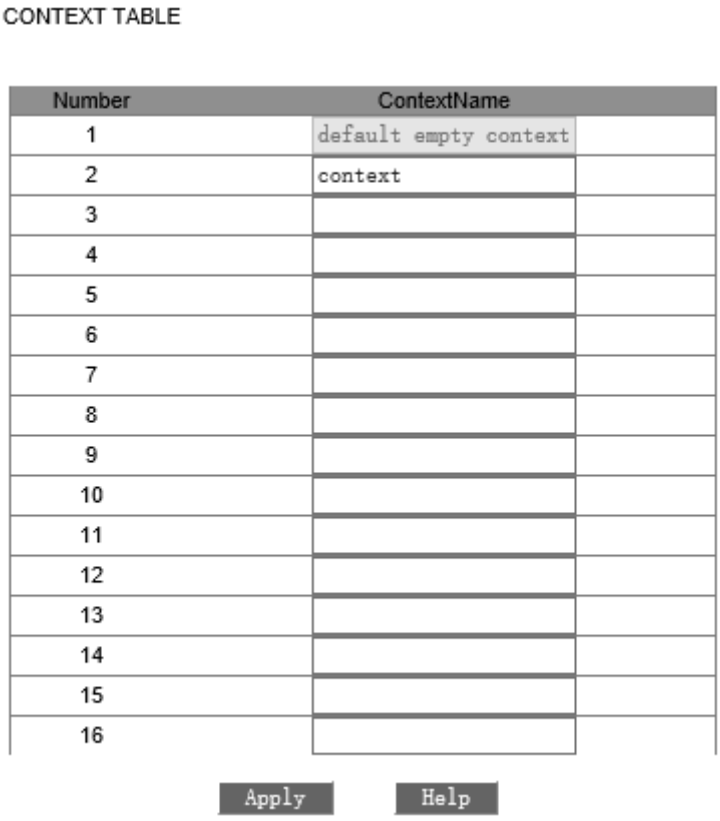


Figure 78 SNMP v3 context table configuration

Context Name

Configuration range: 4~16 character

Function: Configurate context name.

Description: The first context name is forced to empty.

4、Configurate view table

Click the navigation tree [Device advanced configuration]→[SNMP configuration]→[V3 view table configuration] menu, enter into SNMP v3 view table configuration interface, as shown in Figure 79;

VIEW TABLE

Index	View Name	Type	oid-tree	mask
1	all-of-mib	included	1	0xff, 0xff, 0xff, 0xff
2	view1	included	1. 3. 6. 1. 2. 1. 1	0xff, 0xff, 0xff, 0xff
3	view2	included	1. 3. 6. 1. 2. 1. 2	0xff, 0xff, 0xff, 0xff
4		included		
5		included		
6		included		
7		included		
8		included		
9		included		
10		included		
11		included		
12		included		
13		included		
14		included		
15		included		
16		included		

Apply Help

Figure 79 SNMPv3 view table configuration

View Name

Configuration range: 4~16 character

Function: Configurate view name.

Type

Configuration option: included/excluded

Default configuration: included

Function: included means that the current view includes any node of the MIB subtree; excluded means that the current view does not include any nodes of the MIB subtree.

oid-tree

Function: MIB subtree, use OID of subtree root node to indicate.

Subtree Mask

Function: MIB subtree mask。Oid-tree and mask jointly determine the MIB node information of the current view.

For example：in figure79, view name view1 only access 1.3.6.1.2.1.1.1、1.3.6.1.2.1.2.1、1.3.6.1.2.1.3.1、1.3.6.1.2.1.4.1……1.3.6.1.2.1.n.1 node information

5、Configure access table

Click the navigation tree [Device advanced configuration]→[SNMP configuration]→[V3 access table configuration] menu, enter into SNMP v3 access configuration interface, as shown in Figure 80;

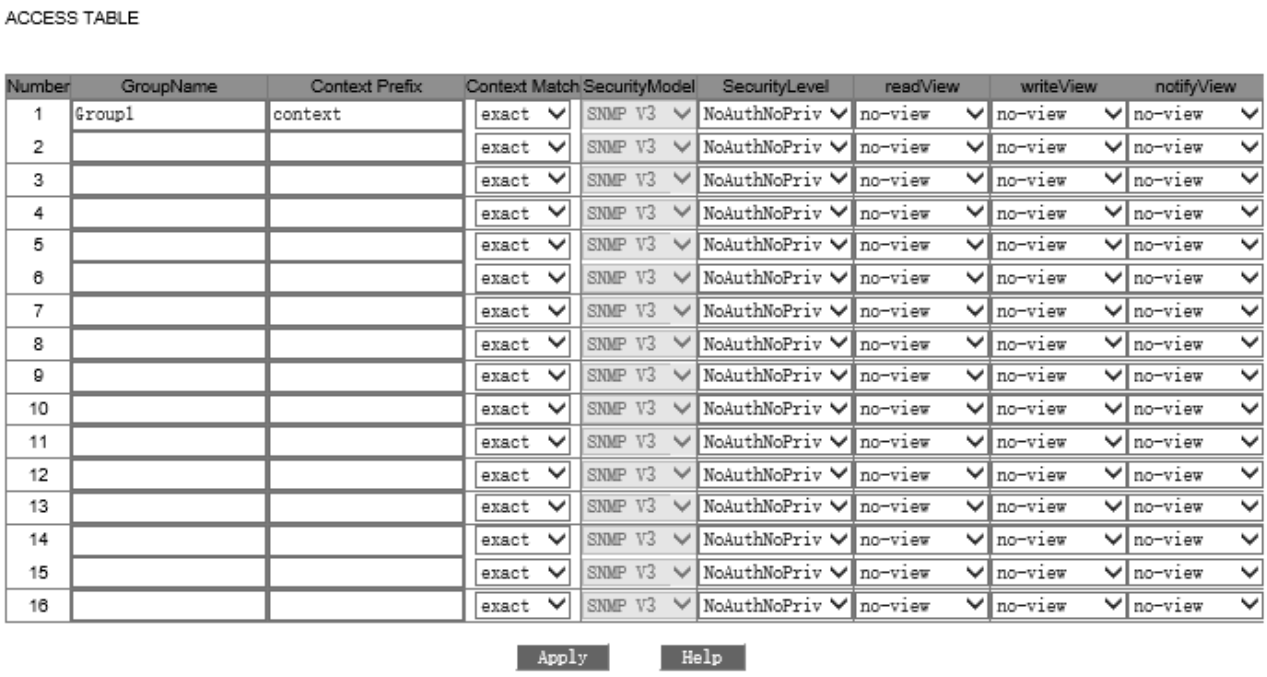


Figure 80 SNMPv3 access configuration

Group Name

Configuration range: Created group name, 4~16 character

Function: All users in the group have the same access permission.

Context Name

Configuration range: Created context name, 4~16 character

Function: Configure context name, The group name and the context name jointly determine a group of access permission. The first context name in the context table is forced to empty, so the context name can be empty.

Context Matching mode

Configuration option: exact/prefix

Default configuration: exact

Function: Select context name matching mode. Exact means all match, which means that the context name should be consistent with the context name in the context table; prefix means prefix matches, which means that context name is configured to the first 4~16 character of the context name in the context table, the same context name with the same prefix has the same access permission.

Security Mode

Default configuration: SNMP V3

Description: SNMPv3 means to use USM (User-Based Security Model) technology, which is currently forced to SNMPv3 mode.

Security Level

Configuration option: NoAuthNoPriv/AuthNoPriv/AuthPriv

Default configuration: NoAuthNoPriv

Function: Select access permission to access MIB information.

Description: NoAuthNoPriv neither authentication nor message encryption is required; AuthNoPriv authentication encryption but not message encryption; AuthPriv both authentication and message encryption are required. When encryption is required, the encryption algorithm and encryption password in the network management software should be consistent with the configuration in the user table to successfully access the corresponding node information of the switch.

Read View

Configuration option: Created view name

Function: Select read only view name.

Write View

Configuration option: Created view name

Function: Select write view name.

Announce View

Configuration option: Created view name

Function: Select the view name that can send trap messages.

6、Configure Trap

Click the navigation tree [Device advanced configuration]→[SNMP configuration]→[TRAP configuration] menu, enter into Trap configuration interface, as shown in Figure 81;

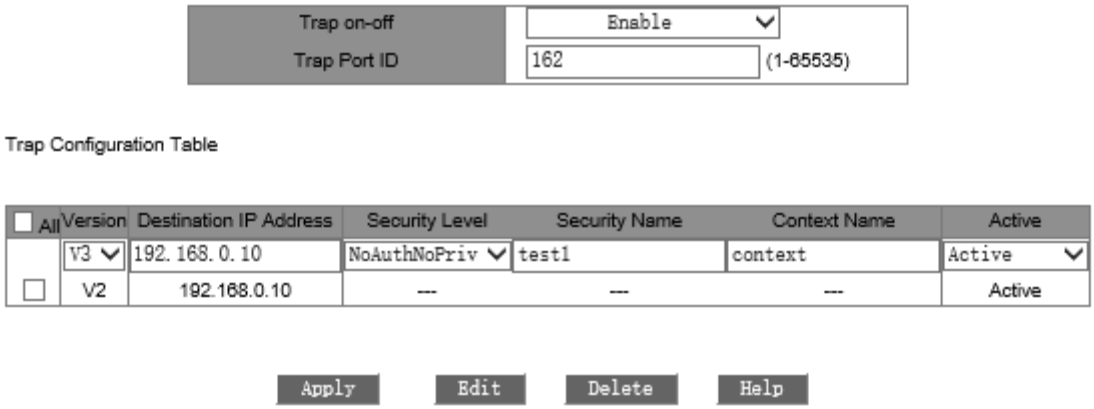


Figure 81 SNMP v3 Trap configuration

TRAP Switch

Configuration option: Open/Close

Default configuration: Close

Function: Whether to allow switch send trap message.

TRAP Port Number

Configuration range: 1~65535

Default configuration: 162

Function: Port number that sends the trap message message.

Version

Configuration option: V1/V2C/V3

Function: V1/V2C means that the switch sends the trap message with v1/v2c version to the server; V3 means that the switch sends the trap message with V3 version to the server.

Destinate IP address

Configuration format: A.B.C.D

Function: Configure the server address to receive trap messages, supporting up to 8 trap server addresses, that is up to 8 trap table items.

{Security Level, Security name, Context name }

Configuration option: {NoAuthNoPriv/AuthNoPriv/AuthPriv, 4~16 character, 4~16 character }

Function: The three items must only be configured when sending trap message with V3 version. This configuration should be consistent with the corresponding configuration in the access table, where the security level can be equal to or higher than security level in the access table. For example, access permission of user 1111 is AuthNoPriv, the trap message can be sent to server when security level of security name 1111 is AuthNoPriv or AuthPriv. The context name matches consistent with the Context Prefix in the access table.

6.10.10 SNMPV3 Typical Configuration Example

The SNMP management station is connected to the switch via Ethernet, management station IP address is 192.168.0.23, switch IP address is 192.168.0.2. User 1111 and user 2222 monitor and manage Agent via SNMPv3, security level is AuthNoPriv, so they can do read only operation for all node information in Agent; Agent actively sends trap V3 message to NMS when alarm occur. as shown in Figure 82;

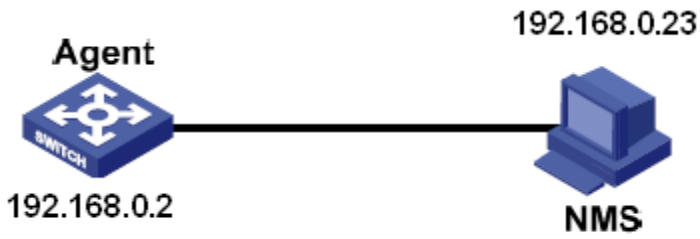


Figure 82 SNMPv3 configuration example

Configuration on the Agent：

1. Set a username to 1111, Authentication Encryption: HMAC-MD5, authentication encryption Password: aaaa,Message Encryption Protocol:HMAC-DES， Message

Encryption Password :xxxx;Set a username to 2222, Authentication Encryption:HMAC-SHA, authentication encryption Password: bbbb,Message Encryption Protocol:HMAC-DES，Message Encryption Password :yyyy, as shown in figure 76；

2. Create group, Include usersand 1111 and user 2222 to the group, as shown in figure 77；

3. Create Context, Context name: context, as shown in figure 78；

4. Create view view-all includes all nodes, view-no does not include any nodes, as shown in figure 79；

5.Configure SNMPv3 access table, group name: group, context name: context, context matching method: all match, security level: AuthNoPriv, read view: view-all, write view: view-no, notification view: view-all, as shown in the figure 80；

6. Create trap entry 162, enable trap mode; set the trap version to SNMP v3, destination IP address to 192.168.0.23. security leve：AuthPriv ，Security name ：1111，Context name: context, as shown in figure 81；

If you want to monitor and manage Agent devices, run the corresponding management software in NMS.

6.11 DT-Ring

6.11.1 Overview

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

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

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

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

6.11.2 Concepts

- Master: One ring has only one master. The master sends DT-Ring protocol packets and detects the status of the ring. When the ring is closed, the two ring ports on the master are in forwarding and blocking state respectively.
- Primary port: indicates the ring port (on the master) whose status is configured as forwarding forcibly by user when the ring is closed.

Note:

If no primary port is configured on the master, the first port whose link status changes to up when the ring is closed is in forwarding state. The other ring port is in blocking state.

- Slave: A ring can include multiple slaves. Slaves listen to and forward DT-Ring protocol packets and report fault information to the master.
- Backup port: The port for communication between DT rings is called the backup port.
- Master backup port: When a ring has multiple 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 multiple backup ports, all the backup ports except the master backup port are slave backup ports. They are in blocking state.
- Forwarding state: If a port is in forwarding state, the port can both receive and send data.
- Blocking state: If a port is in blocking state, the port can receive and forward only DT-Ring protocol packets, but not other packets.

6.11.3 Implementation

DT-Ring-Port Implementation

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

Working process of switch A, Switch B, Switch C, and Switch D:

1. Configure Switch A as the master and the other switches as slaves.
2. Ring port 1 on the master is in forwarding state while ring port 2 is in blocking state. Both

two ports on the slave are in forwarding state.

3. If link CD is faulty, as shown in the following figure:

a) When link CD is faulty, port 6 and port 7 on the slave are in blocking state. Port 2 on the master changes to forwarding state, ensuring normal link communication.

b) When the fault is rectified, port 6 and port 7 on the slave are in forwarding state. Port 2 on the master changes to blocking state. Link switchover occurs and links restore to the state before CD is faulty.

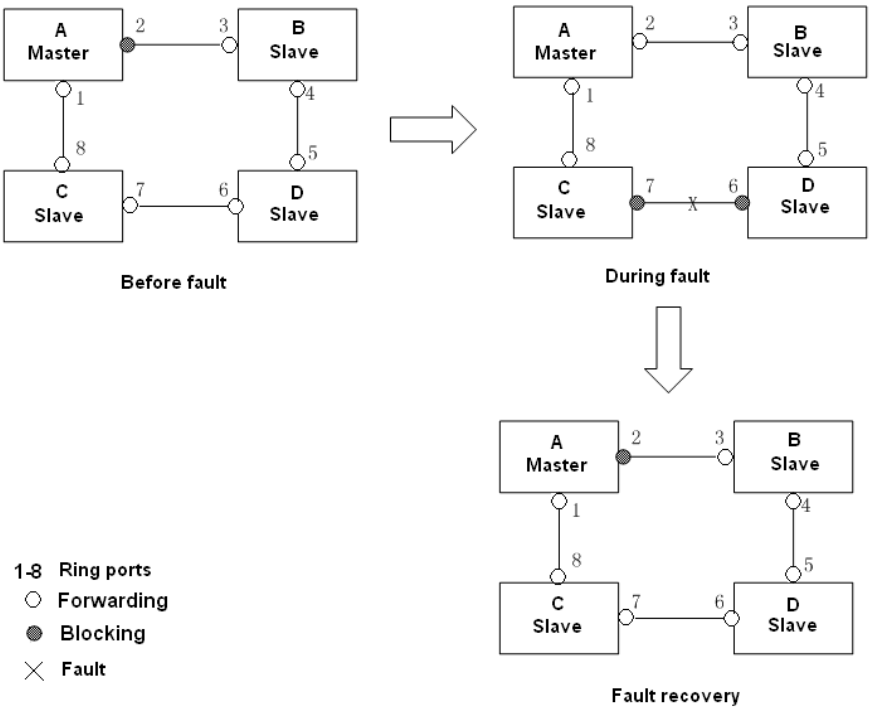


Figure 83 CD Link Fault

Note:

If port 1 on master A is configured as the primary port, the fault and fault recovery processes are identical with those described above.

4. If link AC is faulty, as shown in the following figure:

a) When link AC is faulty, port 1 is in blocking state and port 2 changes to forwarding state, ensuring normal link communication.

b) After the fault is rectified,

➢ If no primary port is configured on master A, port 1 is still in blocking state and port 8 is in

forwarding state. No switchover occurs.

- If port 1 on master A is configured as primary port. When the ring is closed, primary port must be in forwarding state. Therefore, port 1 changes to forwarding state. Port 8 is in forwarding state and port 2 is in blocking state. Link switchover occurs.

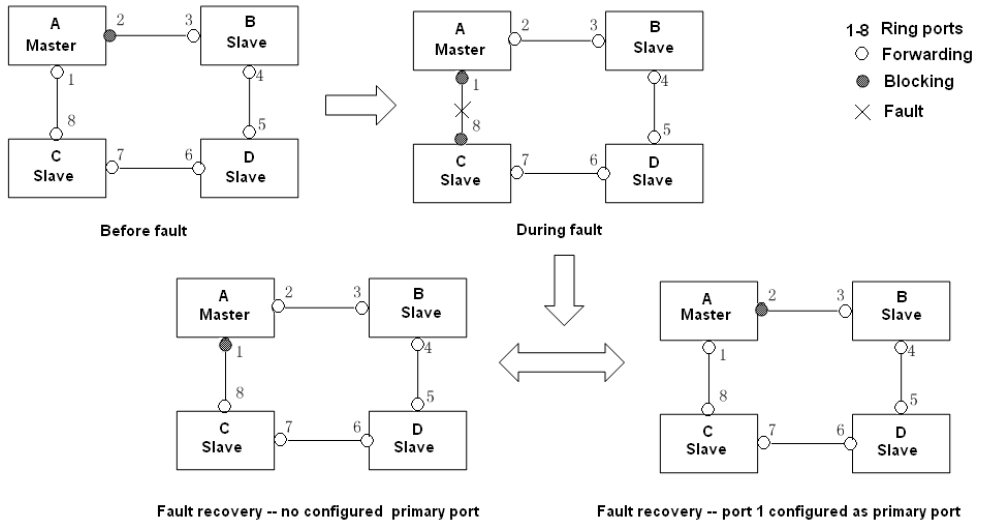


Figure 84 DT-Ring Link Fault

Caution:

Link status change affects the status of ring ports.

DT-Ring-VLAN Implementation

DT-Ring-VLAN allows the packets of different VLANs to be forwarded in different paths. Each forwarding path for a VLAN forms a DT-Ring-VLAN. Different DT-VLAN-Rings can have different masters. As shown in the following figure, two DT-Ring-VLANs are configured.

Ring links of DT-Ring-VLAN 10: AB-BC-CD-DE-EA.

Ring links of DT-Ring-VLAN 20: FB-BC-CD-DE-EF.

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

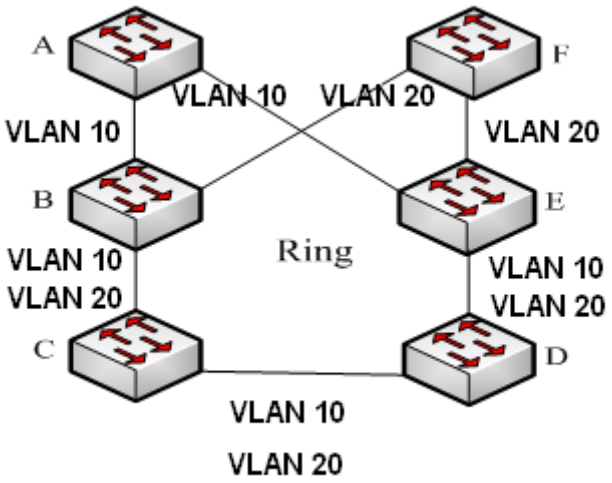


Figure 85 DT-Ring-VLAN

Note:

In each DT-Ring-VLAN logical ring, the implementation is identical with that of DT-Ring-Port.

DT-Ring+ Implementation

DT-Ring+ can provide backup for two DT rings, as shown in the following figure. 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.

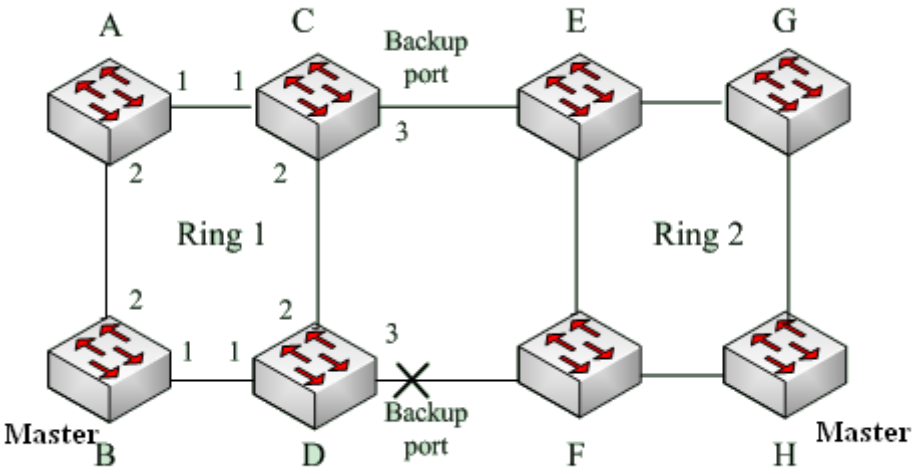


Figure 86 DT-Ring+ Topology

Caution:

Link status change affects the status of backup ports.

6.11.4 Explanation

DT-Ring configurations should meet the following conditions:

- All switches in the same ring must have the same domain number.
- Each ring can only have one master and multiple slaves.
- 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.
- A maximum of two backup ports can be configured in one ring.
- On a switch, only one backup port can be configured for one ring.
- DT-Ring-Port and DT-Ring-VLAN cannot be configured on one switch at the same time.

6.11.5 Web Configuration

1. Configure redundant ring mode, as shown in the following figure.

Figure 87 Redundant Ring Mode Configuration

Select Redundancy Mode

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

Default: DT-RING-PORT

Function: Select the redundancy mode.

Caution:

- Port-based ring protocols include RSTP, DT-Ring-Port, and DRP-Port, and VLAN-based ring protocols include DT-Ring-VLAN and DRP-VLAN.
- VLAN-based ring protocols are mutually exclusive, and only type of VLAN-based ring protocol can be configured for one device.
- Port-based ring protocol and VLAN-based ring protocol are mutually exclusive, and only one

ring protocol mode can be selected for one device.

Check Loop Status

Options: Disable/Enable

Default: Disable

Function: Enable or disable ring status detection.

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

2. Create a DT ring, as shown in the following figure.

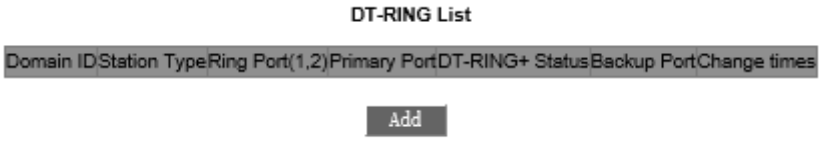


Figure 88 Creating a DT Ring

Click <Add> and configure the DT ring.

3. Configure DT-Ring and DT-VLAN-Ring, as shown in the following figures.

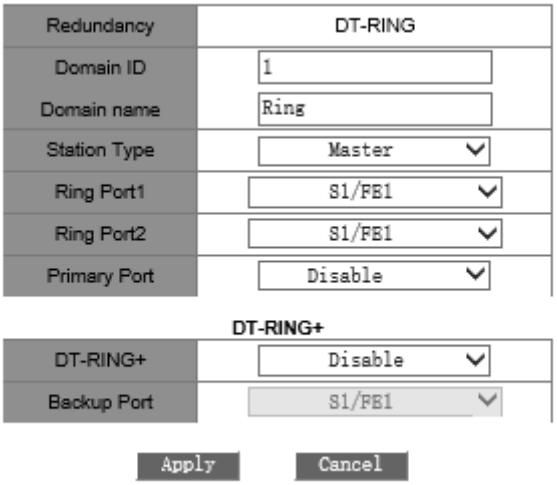


Figure 89 DT-Ring Configuration

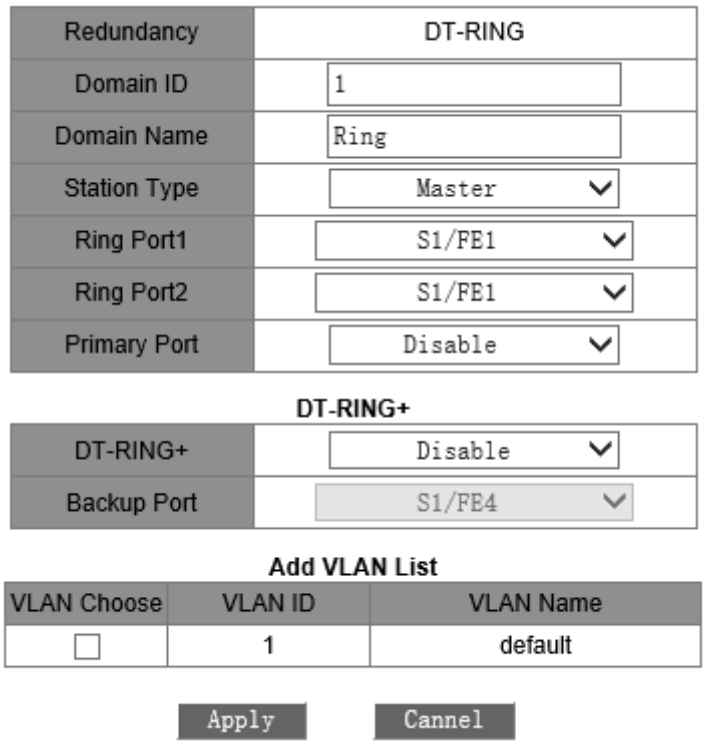


Figure 90 DT-VLAN-Ring Configuration

Redundancy

Forced configuration: DT-RING

Domain ID

Configuration rang: 1~32

Function: Differentiate rings. A maximum of 16 port-based rings or 8 VLAN-based rings can be configured on one switch.

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 switch ports

Function: Select two ring ports.

Caution:

- A DT-Ring ring port or backup port cannot be added to a trunk group. A port added to a trunk group cannot be configured as a DT-Ring ring port or backup port.
- A DT-Ring ring port or backup port can be configured as a mirroring source or destination port. A mirroring source or destination port cannot be configured as a DT-Ring ring port or backup port.
- Ring ports between port-based ring protocols RSTP, DT-Ring-Port, and DRP-Port are mutually exclusive, that is, the ring port and backup port of DT-Ring-Port must not be configured as RSTP port, DRP-Port ring port, or DRP-Port backup port; RSTP port, DRP-Port ring port, and DRP-Port backup port must not be configured as DT-Ring-Port ring port or backup port.
- It is not recommended that ports in isolation group are configured as DT-Ring ports and backup ports at the same time, and DT-Ring ports and backup ports cannot be added to the isolation group at the same time.

Primary Port

Options: Disable/All switch ports

Default: Disable

Function: Configure the primary port.

Description: When the ring is closed, the primary port is in forwarding state.

Caution:

- The primary port takes effect only when the ring is closed.
- The primary port must be one of the two ring ports on the master.

DT-RING+

Options: Enable/Disable

Default: Disable

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

Backup Port

Options: All switch ports

Function: Select one port as the backup port.

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

Add VLAN List

Options: All created VLANs

Function: Select the VLANs managed by current DT-Ring-VLAN ring.

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

Figure 91 DT-Ring List

4. View and modify DT-Ring configuration.

Click the DT-Ring options in the preceding figure. You can view and modify the configurations of the ring, as shown in the following figure.

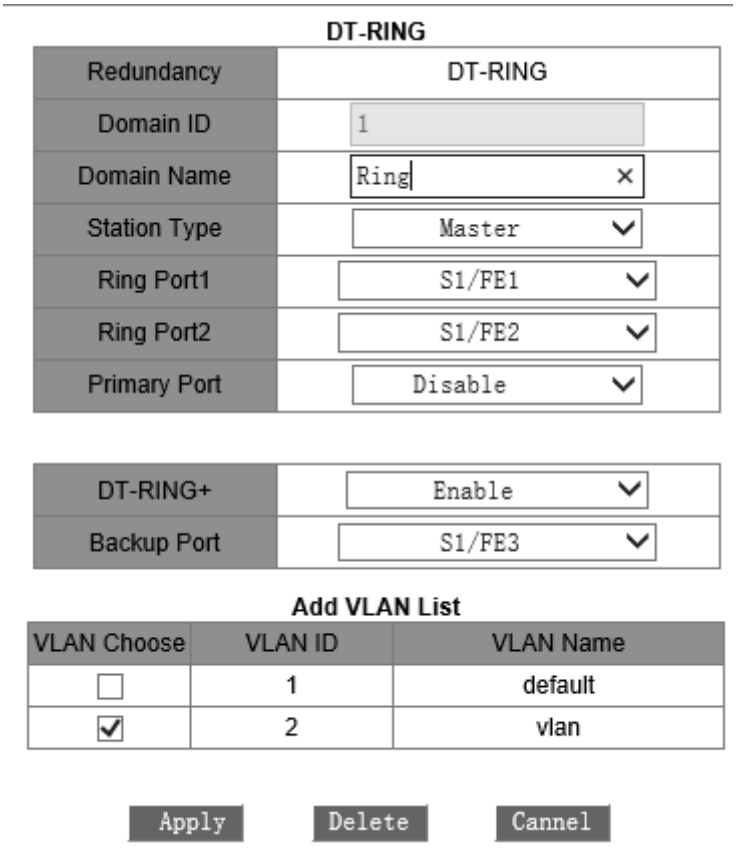


Figure 92 DT-Ring Configuration

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

5. View DT-Ring and port status, as shown in the following figure.

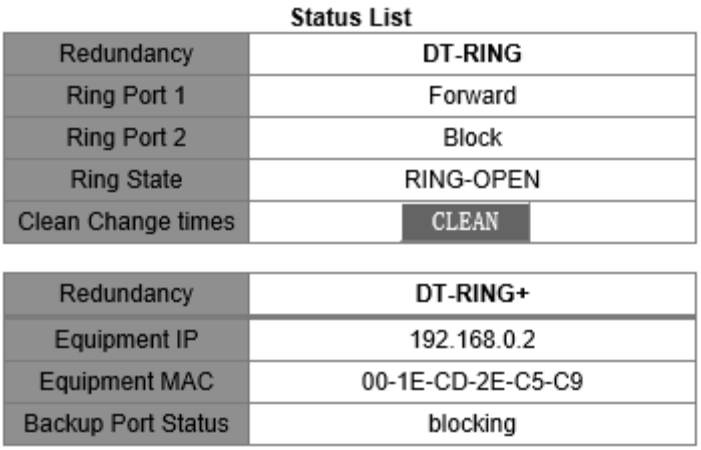


Figure 93 DT-Ring State

6.11.6 Typical Configuration Example

As shown in Figure 86, Switch A, B, C, and D form Ring 1; Switch E, F, G, and H form ring 2. Links CE and DF are the backup links between Ring 1 and Ring 2.

Configuration on Switch A:

1. Domain ID: 1; Domain name: Ring; Ring port: port 1 and port 2; Station type: Slave; DT-Ring+: Disable; do not set backup ports, as shown in Figure 89.

Configuration on Switch B:

2. Domain ID: 1; Domain name: Ring; Ring port: port 1 and port 2, no primary port; Station type: Master; DT-Ring+: Disable; do not set backup ports, as shown in Figure 89.

Configuration on Switch C and Switch D:

3. Domain ID: 1; Domain name: Ring; Ring port: port 1 and port 2; Station type: Slave; DT-Ring+: Enable; Backup port: port 3, as shown in Figure 89.

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

4. Domain ID: 2; Domain name: Ring; Ring port: port 1 and port 2; Station type: Slave; DT-Ring+: Disable; do not set backup ports, as shown in Figure 89.

Configuration on Switch H:

5. Domain ID: 2; Domain name: Ring; Ring port: port 1 and port 2, no primary port; Station type: Master; DT-Ring+: Disable; do not set backup ports, as shown in Figure 89.

6.12 RSTP/STP

6.12.1 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 transfer to the forwarding state.

To overcome the drawback, IEEE creates 802.1w standard to supplement 802.1D.IEEE802.1w defines the Rapid Spanning Tree Protocol (RSTP). Compared with STP, RSTP achieves much more rapid convergence by adding alternate port and backup port for

the root port and designated port respectively. When the root port is invalid, the alternate port can enter the forwarding state quickly.

6.12.2 Concepts

Root bridge: serves as the root for a tree. A network has only one root bridge. The root bridge changes with network topology. The root bridge periodically sends BPDU to the other devices, which forward the BPDU to ensure topology stability.

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

Designated port: indicates the port for forwarding BPDU to other devices or LANs. All ports on the root bridge are designated ports.

Alternate port: indicates the backup port of the root port. If the root port fails, the alternate port becomes the new root port.

Backup port: indicates the backup port of the designated port. When a designated port fails, the backup port becomes the new designated port and forwards data.

6.12.3 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. The following table 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).

6.12.4 Implementation

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

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

- If the priority of its own BPDU is higher, then the port does not perform any operation.
- If the priority of the received BPDU is higher, then the port replaces the local BPDU with the received one.

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

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

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 port: A non-root-bridge device selects 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 calculates a designated port BPDU for each port as follows:

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

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

6.12.5 Web Configuration

1. Enable STP/RSTP, as shown in the following figure.

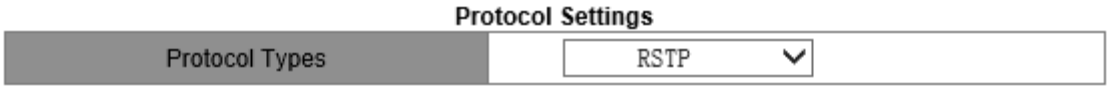


Figure 94 Enabling RSTP/STP

Protocol Types

Options: Disable/RSTP/STP

Default: Disable

Function: Disable or enable RSTP or STP.

Caution:

- Port-based ring protocols include RSTP, DT-Ring-Port, and DRP-Port, and VLAN-based ring protocols include DT-Ring-VLAN and DRP-VLAN.
- Port-based ring protocol and VLAN-based ring protocol are mutually exclusive, and only one

ring protocol mode can be selected for one device.

2. Set the time parameters of the network bridge, as shown in the following figure.

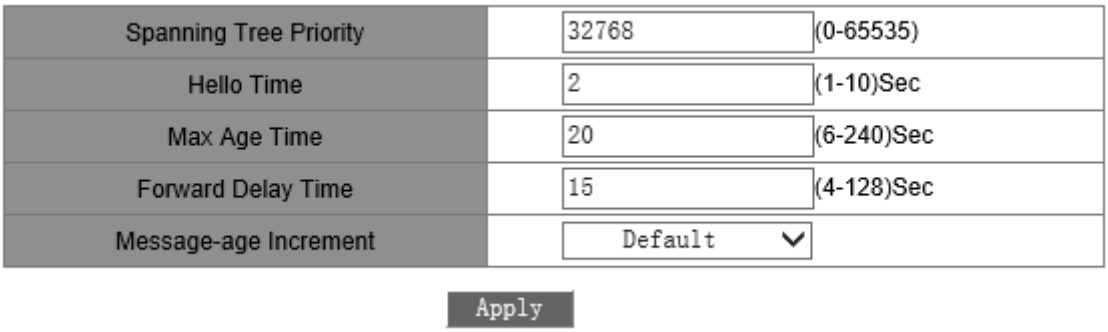


Figure 95 Setting Time Parameters of the Network Bridge

Spanning Tree Priority

Range: 0~65535. The step is 4096.

Default: 32768

Function: Configure the priority of the network bridge.

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

Hello Time

Range: 1~10s

Default: 2s

Function: Configure the interval for sending BPDU.

Max Age Time

Range: 6~240s

Default: 20s

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

Forward Delay Time

Range: 4~128s

Default: 15s

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

Forwarding.

Message-age Increment

Options: Compulsion/Default

Default: Default

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

Description: In compulsion mode, the value is 1.

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

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

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

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

3. Enable RSTP on ports, as shown in the following figure.

Port Settings

Port	Protocol State	Port Priority(0~255)	Path Cost(1~200000000)	Cost Count
S1/FE1	Enable	128	2000000	Yes
S1/FE2	Enable	128	2000000	No
S1/FE3	Enable	128	2000000	Yes
S1/FE4	Disable	128	2000000	Yes
S1/FE5	Disable	128	2000000	Yes
S1/FE6	Disable	128	2000000	Yes

Figure 96 Port Settings

Protocol State

Options: Enable/Disable

Default: Disable

Function: Enable or disable STP on ports.

Caution:

- A RSTP port cannot be configured as a mirroring source or destination port. A mirroring source or destination port cannot be configured as a RSTP port.
- A RSTP port cannot be added to a trunk group. A port added to a trunk group cannot be configured as a RSTP port.
- Ring ports between port-based ring protocols RSTP, DT-Ring-Port, and DRP-Port are mutually exclusive, that is, RSTP port must not be configured as DT-Ring-Port/ DRP-Port

ring port, or DT-Ring-Port/ DRP-Port backup port; DT-Ring-Port/ DRP-Port ring port, and DT-Ring-Port/ DRP-Port backup port must not be configured as RSTP port.

- It is not recommended that ports in isolation group are configured as RSTP ports at the same time, and RSTP ports cannot be added to the isolation group at the same time.

Port Priority

Range: 0~255. The step is 16.

Default: 128

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

Path Cost

Range: 1~200000000

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

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

Cost Count

Range: Yes/No

Default: Yes

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

4. View the RSTP status, as shown in the following figure.

Root Info

Root MAC	00:1e:cd:2e:c5:c9
Root Priority	0x8000
Root Path Cost	0
Root Port	None
Max Age(s)	20
Hello Time(s)	2
Forward Delay(s)	15

Bridge Info

Bridge MAC	00:1e:cd:2e:c5:c9
Bridge Priority	0x8000
Bridge Version	2
Max Age(s)	20
Hello Time(s)	2
Forward Delay(s)	15

Port Info

Port	Priority	Path Cost	Role	State	Link State
S1/FE1	0x80	200000	Designated	Forwarding	Up
S1/FE2	0x80	2000000	Disabled	Discarding	Down
S1/FE3	0x80	2000000	Disabled	Discarding	Down

Figure 97 RSTP Status Information

6.12.6 Typical Configuration Example

The priorities of Switch A, B, and C are 0, 4096, and 8192. Path costs of links are 4, 5, and 10, as shown in the following figure.

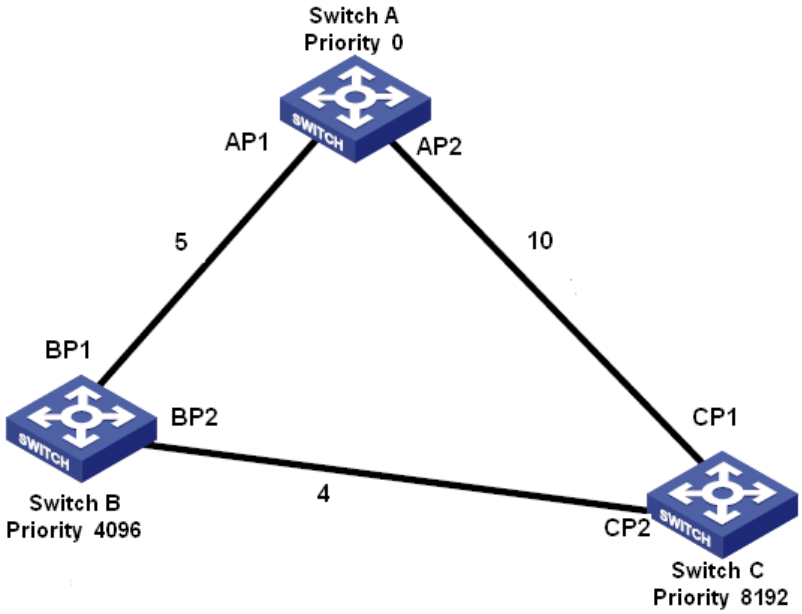


Figure 98 RSTP Configuration Example

Configuration on Switch A:

1. Set priority to 0 and time parameters to default values, as shown in Figure 95.
2. Set the path cost of port 1 to 5 and that of port 2 to 10, as shown in Figure 96.

Configuration on Switch B:

1. Set priority to 4096 and time parameters to default values, as shown in Figure 95.
2. Set the path cost of port 1 to 5 and that of port 2 to 4, as shown in Figure 96.

Configuration on Switch C:

1. Set priority to 8192 and time parameters to default values, as shown in Figure 95.
2. Set the path cost of port 1 to 10 and that of port 2 to 4, as shown in Figure 96.

- The priority of Switch A is 0 and its 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.

6.13 RSTP/STP Transparent Transmission

6.13.1 Overview

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

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

As shown in the following figure, switch A, Switch B, Switch C, and Switch D form a DT ring. The transparent transmission function is enabled on these four switches, so that Switch E and Switch F can receive RSTP packets from each other.

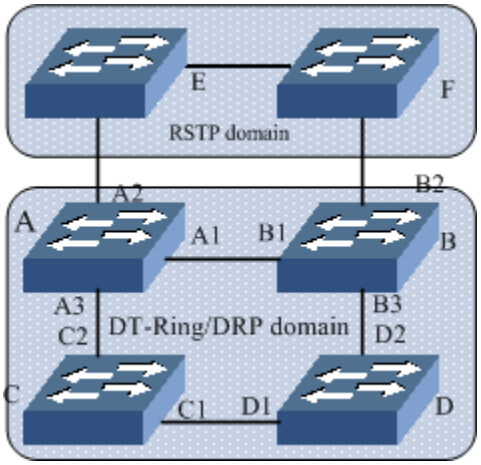


Figure 99 RSTP Transparent Transmission

6.13.2 Web Configuration

Configure RSTP transparent transmission on ports, as shown in the following figure.

Port	RSTP Transparent Transmission
S1/FE1	Disable
S1/FE2	Disable
S1/FE3	Disable
S1/FE4	Disable
S1/FE5	Disable
S1/FE6	Disable
S1/FE7	Disable
S1/FE8	Disable
S2/FE1	Disable
S2/FE2	Disable
S2/FX3	Disable
S2/FX4	Disable
S2/FE5	Disable
S2/FE6	Disable
S2/FX7	Disable
S2/FX8	Disable
S3/FX1	Disable
S3/FX2	Disable
S3/FX3	Disable
S3/FX4	Disable
S3/FX5	Disable
S3/FX6	Disable
S3/FX7	Disable
S3/FX8	Disable

Apply

Figure 100 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 an RSTP-enabled port.

6.13.3 Typical Configuration Example

As shown in Figure 99, 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

section 6.11 DT-Ring.

- Enable RSTP on the involved ports of Switch E and Switch F, as shown in Figure 94 and Figure 96.
- Enable RSTP transparent transmission on ports A1, A2, A3, B1, B2, B3, C1, C2, D1, and D2, as shown in Figure 100.

6.14 DRP

6.14.1 Overview

Kyland develops the Distributed Redundancy Protocol (DRP) for data transmission on ring-topology networks. It can prevent broadcast storms for ring networks. When a link or node is faulty, the backup link can take over services in real time to ensure continuous data transmission.

Compliant with the IEC 62439-6 standard, DRP uses the master election mechanism with no fixed master. DRP provides the following features:

- Network scale-independent recovery time

DRP achieves network scale-independent recovery time by optimizing the ring detection packet forwarding mechanism. DRP enables networks to recover within 20ms, with the introduction of real-time reporting interruption, improving reliability for real-time data transmission. This feature enables switches to provide higher reliability for the applications in the power, rail transit, and many other industries that require real-time control.

- Diversified link detection functions

To improve network stability, DRP provides diversified link detection functions for typical network faults, including fast disconnection detection, optical fiber unidirectional link detection, link quality inspection, and equipment health check, ensuring proper data transmission.

- Applicable to multiple network topologies

Besides rapid recovery for simple ring networks, DRP also supports complex ring topologies, such as intersecting rings and tangent rings. Additionally, DRP supports VLAN-based multiple instances, thereby suiting various network applications with flexible networking.

➢ Powerful diagnosis and maintenance functions

DRP provides powerful status query and alarm mechanisms for network diagnosis and maintenance, as well as mechanism for preventing unintended operation and incorrect configurations that may lead to ring network storms.

6.14.2 Concept

1. DRP Modes

DRP involves two modes: DRP-Port-Based and DRP-VLAN-Based.

DRP-Port-Based: forwards or blocks packets based on specific ports.

DRP-VLAN-Based: forwards or blocks packets based on VLANs. If a port is in blocking state, only the data packets of the specified VLAN are blocked. Therefore, multiple VLANs can be configured on tangent ring ports. A port can belong to different DRP rings according to VLAN configurations.

2. DRP Port Statuses

Forwarding state: If a port is in forwarding state, it can receive and forward data packets.

Blocking state: If a port is in blocking state, it can receive and forward DRP packets, but not other data packets.

Caution:

A port in blocking state on the Root can proactively send DRP packets.

3. DRP Roles

DRP determines the roles of switches by forwarding Announce packets, preventing redundancy rings to form loops.

INIT: indicates the device on which DRP is enabled and the two ring ports are in Link down state.

Root: indicates the device on which DRP is enabled and at least one ring port is in Link up state. In a ring, the Root is elected according to the vectors of Announce packets. It may change with the network topology. The Root sends its own Announce packets to other devices periodically. Statuses of ring ports: One ring port is in forwarding state and the other is in blocking state. Upon receiving the Announce packet of another device, the Root

compares the vector of the packet with that of its own Announce packet. If the vector of the received packet is larger, the Root changes its role to Normal or B-Root according to the link status and CRC degradation of ports.

B-Root: indicates the device on which DRP is enabled, meeting at least one of the following conditions: one ring port is in Link up state while the other is in Link down, CRC degradation, the priority is not less than 200. The B-Root compares and forwards Announce packets. If the vector of a received Announce packet is smaller than that of its own announce packet, the B-Root changes its role to Root; otherwise, it forwards the received packet and does not change its own role. Statuses of ring ports: One ring port is in forwarding state.

Normal: indicates the device on which DRP is enabled and both ring ports are in Link up state without CRC degradation and the priority is more than 200. The Normal only forwards Announce packets, but does not check the content of packets. Statuses of ring ports: Both ring ports are in forwarding state.

Note:

CRC degradation: indicates that the number of CRC packets exceed the threshold in 15 minutes.

6.14.3 Implementation

Each switch maintains its own vector of Announce packet. The switch with the larger vector will be elected as the Root.

The vector of Announce packet contains the following information for role assignment.

Table 8 Vector of Announce Packet

Link status	CRC degradation		Role priority	IP address of the device	MAC address of the device
	CRC degradation status	CRC degradation rate			

Link status: The value is set to 1 if one ring port is in Link down state and set to 0 if both ring ports are in Link up state.

CRC degradation status: If CRC degradation occurs on one port, the value is set to 1. If CRC degradation does not occur on the two ring ports, the value is set to 0.

CRC degradation rate: The ratio of the number of CRC packets and the threshold in 15 minutes.

Role priority: The value can be set on the Web UI.

The parameters in Table 8 are compared in the following procedure:

1. The value of link status is checked first. The device with a larger link status value is considered to have a larger vector.
2. If the two compared devices have the same link status value, the values of CRC degradation status are compared. The device with a larger CRC degradation status value is considered to have a larger vector. If the CRC degradation status value of all compared devices is 1, the device with a larger CRC degradation rate value is considered to have a larger vector.
3. If the two compared devices have the same link status value and CRC degradation value, the values of role priority, IP addresses, and MAC addresses are compared sequentially. The device with a larger value is considered to have a larger vector.
4. The device with the larger vector is elected as the Root.

Note:

Only when CRC degradation status value is 1, the CRC degradation rate value participates in vector comparison. Otherwise, the vectors are compared regardless of CRC degradation rate value.

➢ Implementation of DRP-Port-Based mode

The roles of switches are as follows:

1. Upon startup, all switches are in INIT state. When the state of one port changes to Link up, the switch becomes the Root and sends Announce packets to the other switches in the ring for election.
2. The switch with the largest vector of Announce packet is elected as the Root. The ring port that links up first on the Root is in forwarding state and the other ring port is in blocking state. Among the other switches in the ring, the switch with one ring port in Link down or CRC degradation state is the B-Root. The switch with both ring ports in Link up state and no CRC degradation is the Normal.

The fault recovery procedure is as follows:

1. In the initial topology, A is the Root; port 1 is in forwarding state and port 2 in blocking state. B, C, and D are Normal(s), and their ring ports are in forwarding state, as shown in the following figure.

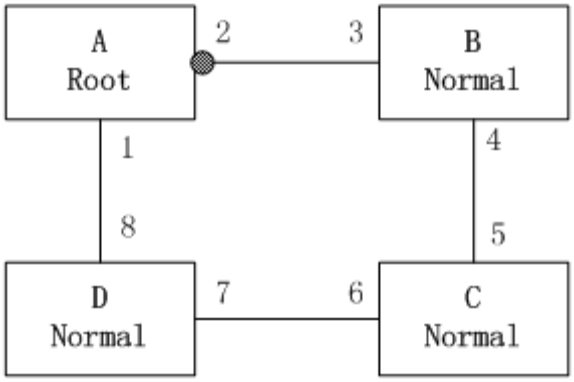


figure 101 DRP Topology

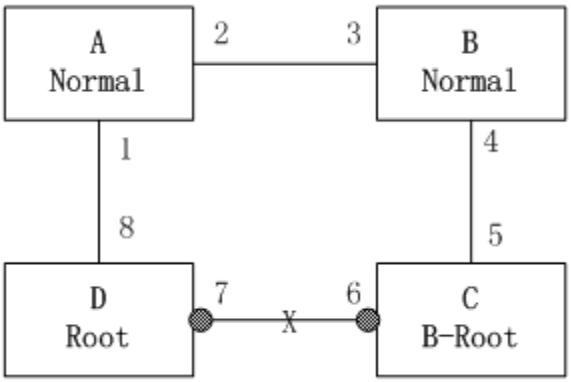


Figure 102 Link Fault

2. When link CD is faulty, DRP changes the statuses of port 6 and port 7 to blocking. As a result, C and D become the Roots. Because A, C, and D are Roots at the moment, they all send Announce packets. The vectors of C and D are larger than that of A because port 7 and port 6 are in Link down state. In this case, if the vector of D is larger than that of C, D is elected as the Root and C becomes the B-Root. When receiving the Announce packet of D, A finds that the vector of D is larger than its own vector and both its ring ports are in Link up state. Therefore, A becomes a Normal and changes the status of port 2 to forwarding, as shown in the preceding figure.

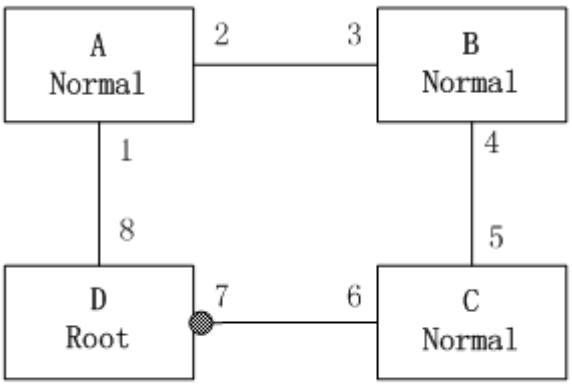


Figure 103 Link Recovery

3. When link CD recovers, D is still the Root because its vector is larger than the vector of C. Because D is the Root, port 7 is in blocking state. In this case, port 6 is in Link up state, so DRP changes the state of port 6 to forwarding. As a result, C becomes a Normal. Therefore, the roles of switches do not change for link recovery.

Note:

On a DRP ring network, the roles of switches change upon a link fault, but do not change when the link recovers. This mechanism improves network security and reliability of data transmission.

➢ Implementation of DRP-VLAN-Based mode

DRP-VLAN-Based ring allows the packets of different VLANs to be forwarded in different paths. Each forwarding path for a VLAN forms a DRP-VLAN-Based. Different DRP-VLAN-Based ring can have different roots. As shown in the following figure, two DRP-VLAN-Based rings are configured.

Ring links of DRP-VLAN10/20-Based: AB-BC-CD-DE-EA.

Ring links of DRP-VLAN30-Based: FB-BC-CD-DE-EF.

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

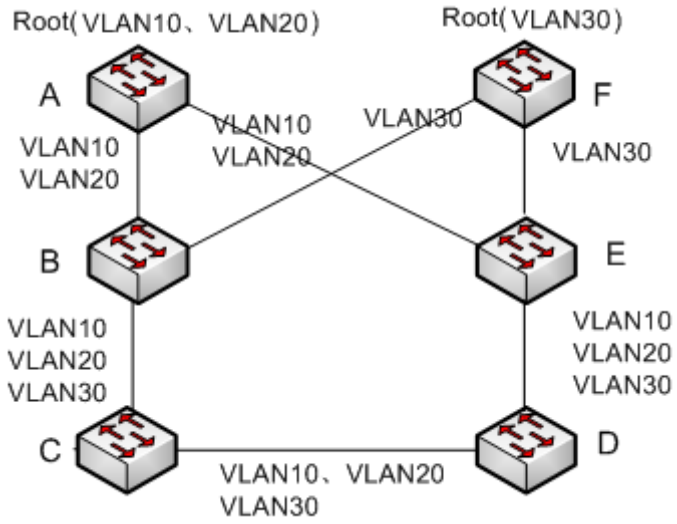


Figure 104 DRP-VLAN-Based

Note:

The port status and role assignment of each DRP-VLAN-Based ring are the same as those of DRP-Port-Based ring.

➢ DRP Backup

DRP can also provide backup for two DRP rings, preventing loops and ensuring normal communication between rings.

Backup port: indicates the communication port between DRP rings. Multiple backup ports can be configured, but must be in the same ring. The first backup port that links up is the master backup port, which is in forwarding state. All the other backup ports are slave. They are in blocking state.

As shown in the following figure, one backup port can be configured on each switch. The master backup port is in forwarding state and the other backup ports are in blocking state. If the master backup port or its link is faulty, a slave backup port will be selected to forward data.

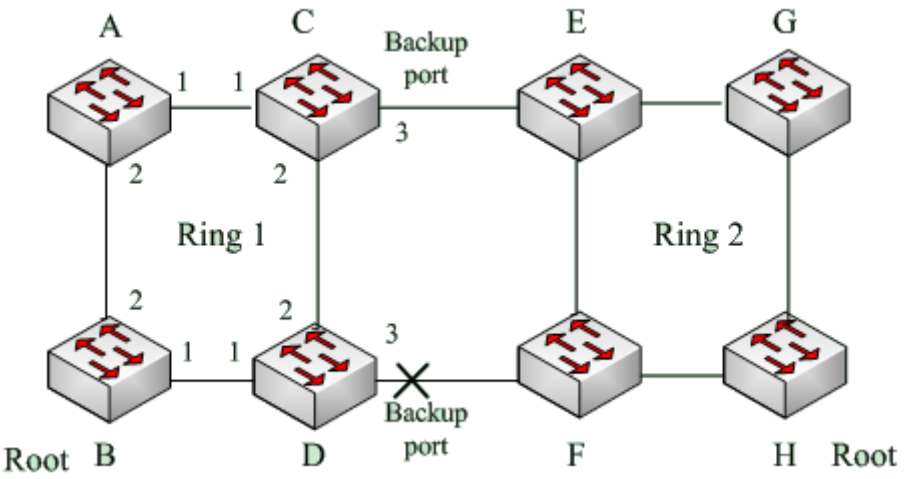


Figure 105 DRP Backup

Caution:

Link status change affects the status of backup ports.

6.15 DHP

6.15.1 Overview

As shown in the following figure, A, B, C, and D are mounted to a ring. Dual Homing Protocol (DHP) achieves the following functions if it is enabled on A, B, C, and D:

- A, B, C, and D can communicate with each other, without affecting the proper running of devices in the ring.
- If the link between A and B is faulty, A can still communicate with B, C, and D by way of Device 1 and Device 2.

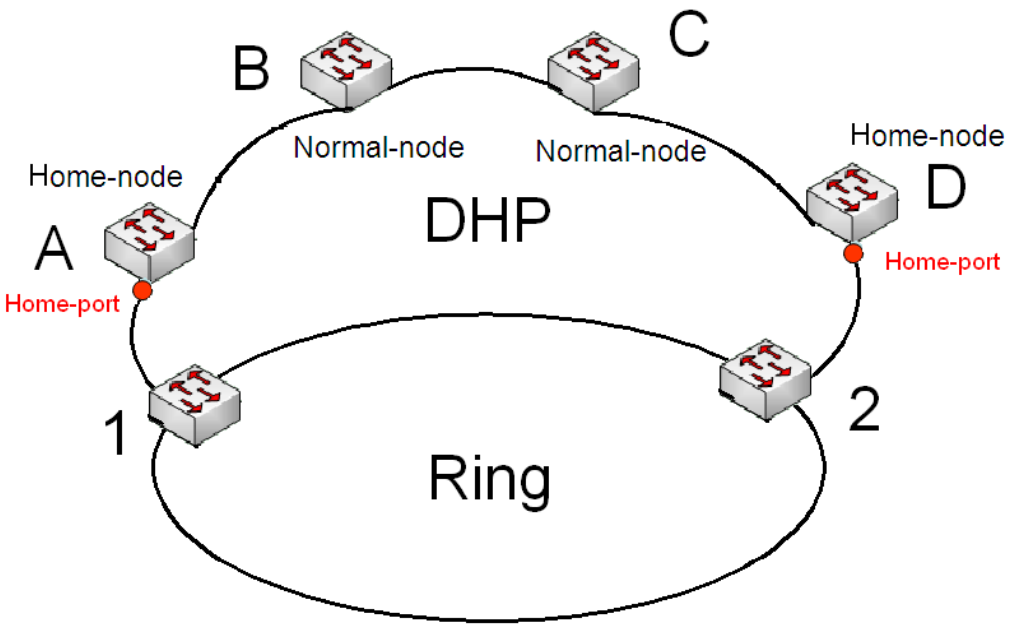


Figure 106 DHP Application

6.15.2 Concepts

The implementation of DHP is based on DRP. The role election and assignment mechanism of DHP is the same as that of DRP. DHP provides link backup through the configuration of Home-node, Normal-node, and Home-port.

Home-node: indicates the devices at both ends of the DHP link and terminates DRP packets.

Home-port: indicates the port connecting a Home node to the external network. A Home-port provides the following functions:

- Sending response packets to the Root upon receiving Announce packets from the Root. The Root identifies the ring status as closed if it receives response packets. If the Root does not receive response packets, it identifies the ring status as open.
- Blocking the DRP packets of external networks and isolating the DHP link from external networks.
- Sending entry clearing packets to connected devices on external networks upon a topology change of the DHP link.

Normal-node: indicates the devices in the DHP link, excluding the devices at both ends. Normal-nodes transmit the response packets of Home-nodes.

6.15.3 Implementation

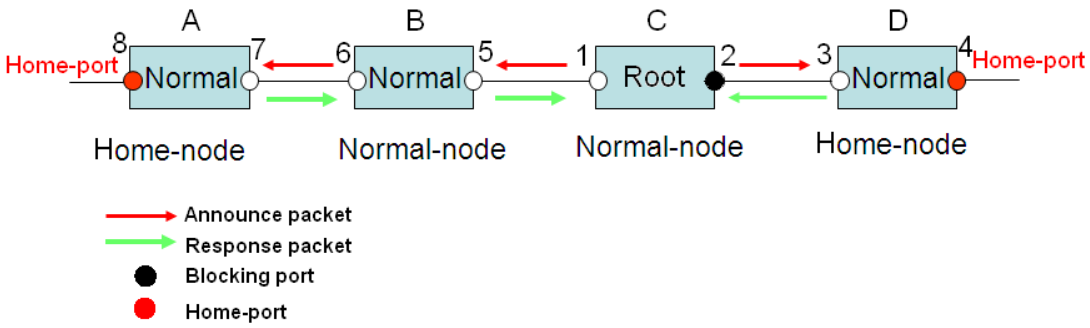


Figure 107 DHP Configuration

As shown in the preceding figure, the configurations of A, B, C, and D in figure 6 are as follows:

- DRP configuration: C is the Root; port 2 is in blocking state; A, B, and D are Normal; all the other ring ports are in forwarding state.
- DHP configuration: A and D are Home-nodes; port 8 and port 4 are Home-ports; B and C are Normal-nodes.

Implementation:

1. C, the Root, sends Announce packets through its two ring ports. Home-port 8 and Home-port 4 terminate the received Announce packets and send response packets to C. C identifies the ring status as closed. Port 2 is in blocking state.

2. When the link between A and B is blocked, the topology involves two links: A and B-C-D.

- A is elected as the Root. Port 7 is in blocking state.
- In link B-C-D, B is elected as the Root. Port 6 is in blocking state. C becomes the Normal. Port 2 is forwarding state. A can communicate with B, C, and D by way of Device 1 and Device 2, as shown in the following figure.

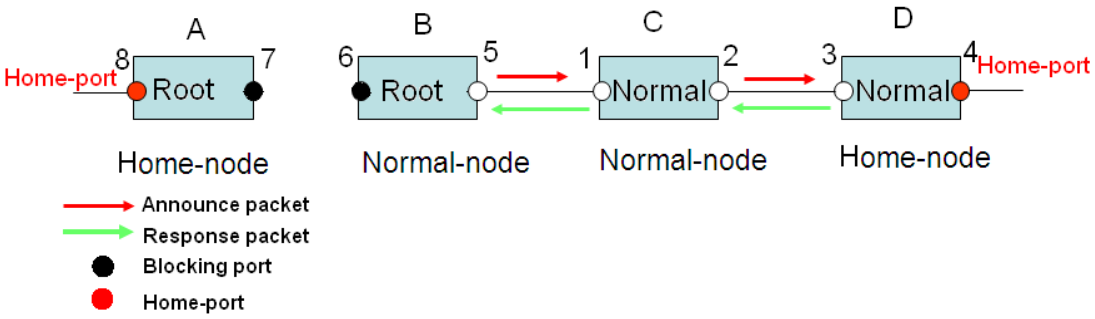


Figure 108 DHP Fault Recovery

6.15.4 Description

DRP configurations meet the following requirements:

- All switches in the same ring must have the same domain number.
- One ring contains only one Root, but can contain multiple B-Roots or Normal(s).
- 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.

6.15.5 Web Configuration

1. Configure the DRP mode, as shown in the following figure.

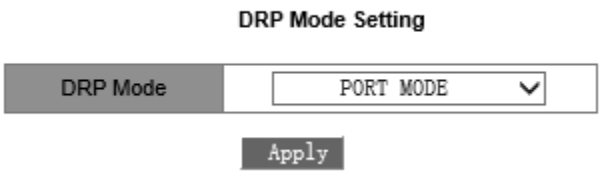


Figure 109 DRP Mode configuration

DRP Mode

Options: PORT MODE/VLAN MODE

Default: PORT MODE

Function: Configure the DRP mode.

Caution:

➢Port-based ring protocols include RSTP, DT-Ring-Port, and DRP-Port, and VLAN-based ring

protocols include DT-Ring-VLAN and DRP-VLAN.

- VLAN-based ring protocols are mutually exclusive, and only type of VLAN-based ring protocol can be configured for one device.
- Port-based ring protocol and VLAN-based ring protocol are mutually exclusive, and only one ring protocol mode can be selected for one device.

2. Configure DRP-Port-Based ring, as shown in the following figure.

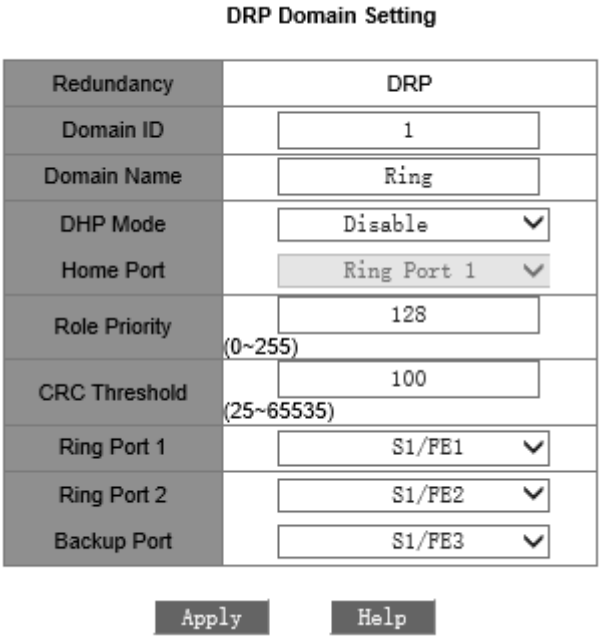


Figure 110 DRP-Port-Based Configuration

Redundancy

Mandatory configuration: DRP

Domain ID

Range: 1~32

Function: Each ring has a unique domain ID. On one switch, a maximum of 16 DRP-Port-Based rings can be configured.

Domain Name

Range: 1~31 characters

Function: Configure the domain name.

DHP Mode

Options: Disable/Normal Node/Home Node

Default: Disable

Function: Enable or disable DHP or configure the DHP mode.

Caution:

DHP is available only in DRP-Port-Based mode.

Home Port

Options: Ring Port 1/Ring Port 2/Ring Port 1-2

Function: Configure the Home-port for a DHP Home-node.

Description: If there is only one device in DHP link, the both ring ports of the Home-node must be configured as the Home-port.

Role Priority

Range: 0~255

Default: 128

Function: Configure the priority of a switch.

CRC Threshold

Range: 25~65535

Default: 100

Function: Configure the CRC threshold.

Description: This parameter is used in root election. The system counts the number of received CRCs. If the number of CRCs of one ring port exceeds the threshold, the system considers the port to have CRC degradation. As a result, the CRC degradation value is set to 1 in the vector of the Announce packet of the port.

Ring Port 1/Ring Port 2

Options: all switch ports

Function: Select two ring ports.

Backup Port

Options: all switch ports

Function: Configure the backup port.

Caution:

Do not configure a ring port as a backup port.

After the configurations are completed, created rings are listed in the DRP List, as shown in the following figure.

DRP List

Domain ID	Role Status	Ring Port(1,2)	Backup Port	Ring Status
1-Ring	INIT	S1/FE4,S1/FE5	S1/F	-----

Figure 111 DRP-Port-Based List

Caution:

- A DRP ring port or backup port cannot be added to a trunk group. A port added to a trunk group cannot be configured as a DRP ring port or backup port.
- A DRP ring port or backup port can be configured as a mirroring source or destination port. A mirroring source or destination port cannot be configured as a DRP ring port or backup port.
- Ring ports between port-based ring protocols RSTP, DT-Ring-Port, and DRP-Port are mutually exclusive, that is, the ring port and backup port of DRP-Port must not be configured as RSTP port, DT-Ring-Port ring port, or DT-Ring-Port backup port; RSTP port, DT-Ring-Port ring port, and DT-Ring-Port backup port must not be configured as DRP-Port ring port or backup port.
- It is not recommended that ports in isolation group are configured as DRP ring ports and backup ports at the same time, and DRP ring ports and backup ports cannot be added to the isolation group at the same time.

- View the parameter settings of a DRP-Port-Based.

Click the DRP entry in Figure 111. You can view and modify the parameter settings of the entry, as shown in the following figure.

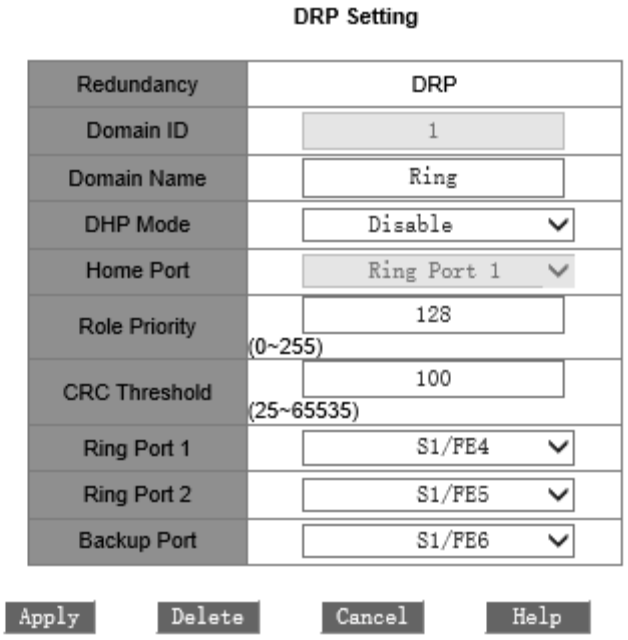


Figure 112 Quering and Modify a DRP-Port-Based entry

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

- View the roles and port status of a DRP ring, as shown in the following figure.

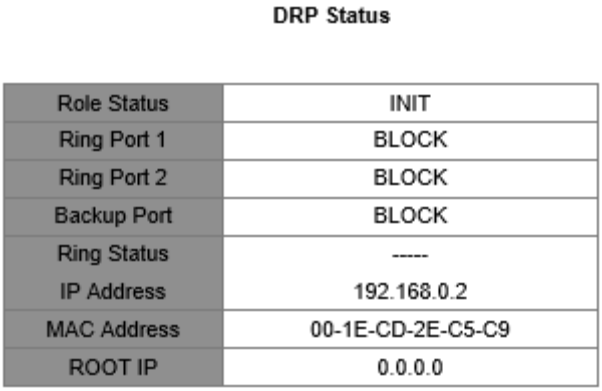


Figure 113 DRP-Port-Based Status Query

3. Configure DRP-Port-Based ring, as shown in the following figure. ring, as shown in the following figure.

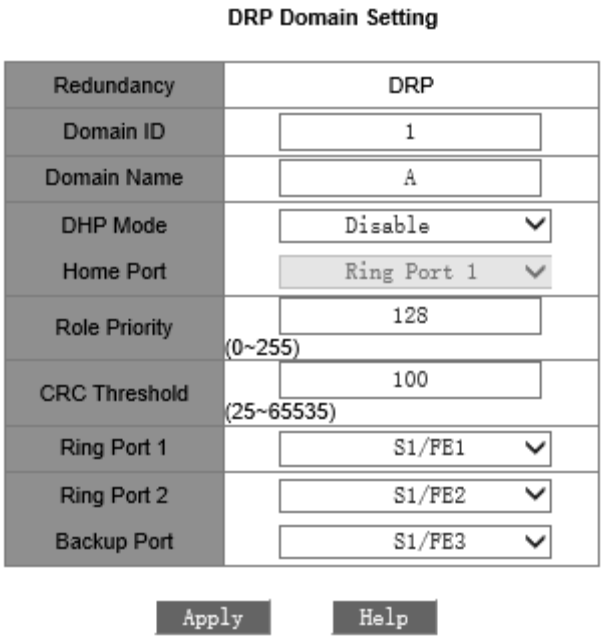


Figure 114 DRP-VLAN-Based Configuration

Redundancy

Mandatory configuration: DRP

Domain ID

Range: 1~32

Function: Each ring has a unique domain ID. On one switch, a maximum of 8

DRP-VLAN-Based rings can be configured.

Domain Name

Range: 1~31 characters

Function: Configure the domain name.

Role Priority

Range: 0~255

Default: 128

Function: Configure the priority of a switch.

CRC Threshold

Range: 25~65535

Default: 100

Function: Configure the CRC threshold.

Description: This parameter is used in root election. The system counts the number of received CRCs. If the number of CRCs of one ring port exceeds the threshold, the system considers the port to have CRC degradation. As a result, the CRC degradation value is set to 1 in the vector of the Announce packet of the port.

Ring Port 1/Ring Port 2

Options: all switch ports

Function: Select two ring ports.

Backup Port

Options: all switch ports

Function: Configure the backup port.

Caution:

- A DRP ring port or backup port cannot be added to a trunk group. A port added to a trunk group cannot be configured as a DRP ring port or backup port.
- A DRP ring port or backup port can be configured as a mirroring source or destination port. A mirroring source or destination port cannot be configured as a DRP ring port or backup port.
- It is not recommended that ports in isolation group are configured as DRP ring ports and backup ports at the same time, and DRP ring ports and backup ports cannot be added to the isolation group at the same time.

Backup Port

Options: all switch ports

Function: Configure the backup port.

Caution:

Do not configure a ring port as a backup port.

Protocol VLAN

Range: 1~4093

Description: The VLAN ID must be one of service VLAN.

Function: DRP packets with the VLAN ID serve as the basis for the diagnosis and maintenance of the DRP-VLAN-Based ring.

Service VLAN

Options: All created VLANs

Function: Select the VLANs managed by current DRP-VLAN-Based ring.

After the configurations are completed, created rings are listed in the DRP List, as shown in the following figure.

DRP List

Domain ID	Role Status	Ring Port(1,2)	Backup Port	Ring Status
1-A	ROOT	S1/FE1,S1/FE2	S1/F	Ring-Open

Figure 115 DRP-VLAN-Based List

- View the parameter settings of a DRP-VLAN-Based

Click the DRP entry in Figure 115. You can view and modify the parameter settings of the entry, as shown in the following figure.

DRP Domain Setting

Redundancy	DRP
Domain ID	1
Domain Name	A
DHP Mode	Disable
Home Port	Ring Port 1
Role Priority	128 (0~255)
CRC Threshold	100 (25~65535)
Ring Port 1	S1/FE1
Ring Port 2	S1/FE2
Backup Port	S1/FE3
Protocol Vlan	2 (1~4093)
Service Vlan	3 (e.g. 1,2,3,6-8)

Apply Help

Figure 116 Quering and Modify a DRP-VLAN-Based entry

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

View the roles and port status of a DRP ring, as shown in the following figure.

Role Status	ROOT
Ring Port 1	FORWARD
Ring Port 2	BLOCK
Backup Port	BLOCK
Ring Status	Ring-Close
IP Address	192.168.0.222
MAC Address	08-00-3E-32-53-22

Figure 117 DRP-VLAN-Based Status Query

6.15.6 Typical Configuration Example

As shown in Figure 105, 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 and switch B:

1. Set Domain ID to 1 and Domain name to Ring. Select ring port 1 and ring port 2. Keep default values for role priority and backup port, as shown in Figure 110.

Configuration on switch C and switch D:

2. Set Domain ID to 1, Domain name to Ring, and Backup port to 3. Select ring port 1 and ring port 2. Keep the default value for role priority, as shown in Figure 110.

Configuration on switch E, F, G, and H:

3. Set Domain ID to 2 and Domain name to Ring. Select ring port 1 and ring port 2. Keep default values for role priority and backup port, as shown in Figure 110.

6.16 QoS

6.16.1 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.

6.16.2 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 five queue mapping modes for priority identification: highest priority, port-based, DIFF, TOS/DIFF, and 802.1p

- If the highest priority is configured on a port, then packets to be forwarded are put in queue 3.
- If port-based queue mapping mode is configured on a port, received packets are queued according to the default priority of the port. The mapping between the default priority and queues is consistent with that between 802.1p priority and queues.
- The DIFF value relies on the DSCP in packets while 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), Hq-preempt mode, and STRICT mode.

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

6.16.3 Web Configuration

1. Configure the QoS mode, as shown in the following figure.

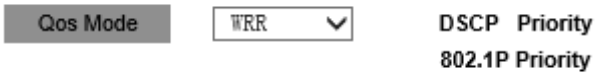


Figure 118 QoS Mode

Qos Mode

Options: Disable/WRR/STRICT

Default: STRICT

Function: Configure the scheduling mode of a port.

2. Configure the queue weight ratio, as shown in the following figure.

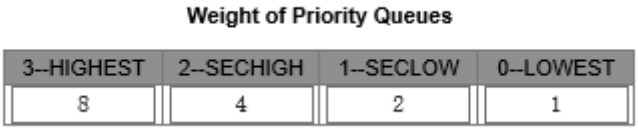


Figure 119 Configuring Queue Weight Ratio

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

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

Default: {8, 4, 2, 1}

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

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

3. Configure QoS port priority mapping mode, as shown in the following figure.

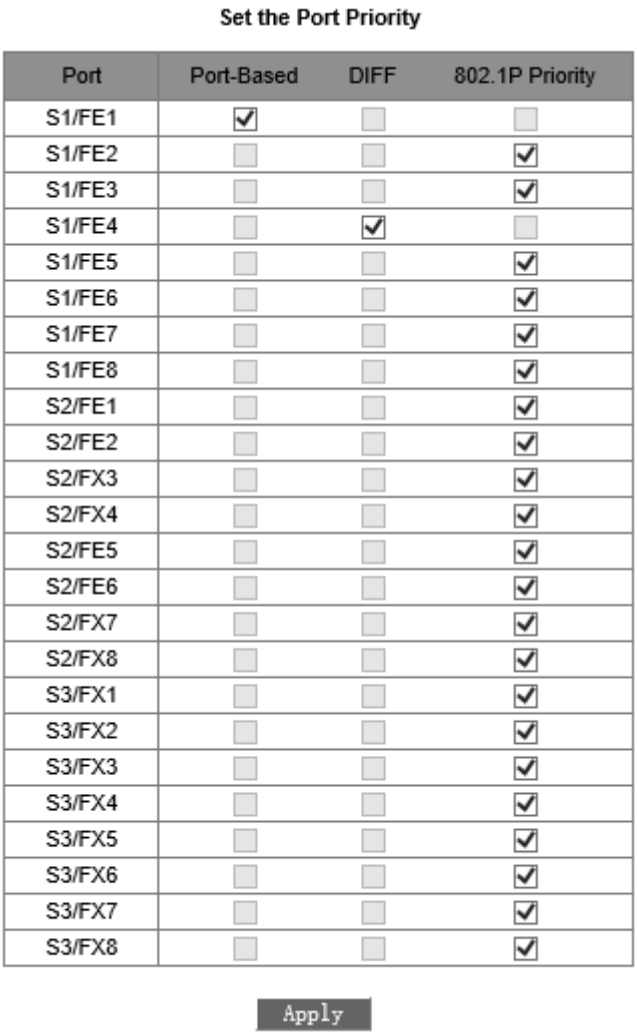


Figure 120 Setting QoS Port Priority Mapping Mode

Set the Port Priority

Options: Port-Based/DIFF/802.1P Priority

Default: 802.1P Priority

Function: Configure port priority mapping mode.

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

4. Configure port-based/ 802.1p priority-queue mapping.

The queue mapping of the port-based mode is consistent with that of 802.1p priority mode. If you want to configure either of the two modes, set parameters in the 802.1p priority mapping table, as shown in the following figure.

Click <802.1p Priority> in Figure 118. The following page is displayed.

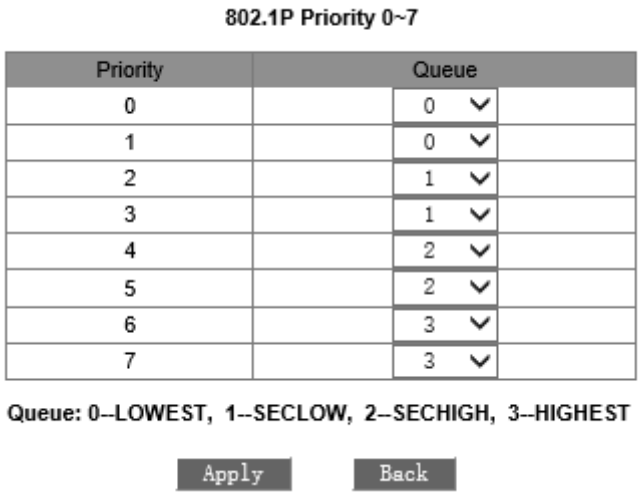


Figure 121 802.1p Priority-Queue Mapping

802.1P Priority

Portfolio: {Priority, Queue}

Range: {0~7, 0~3}

Default: Priority 0 and 1 are mapped to queue 0; priority 2 and 3 are mapped to queue 1. Priority 4 and 5 are mapped to queue 2; priority 6 and 7 are mapped to queue 3.

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

5. Configure DSCP priority-queue mapping.

Click <DSCP Priority> in Figure 118 to configure the DSCP priority-queue mapping, as shown in the following figure.

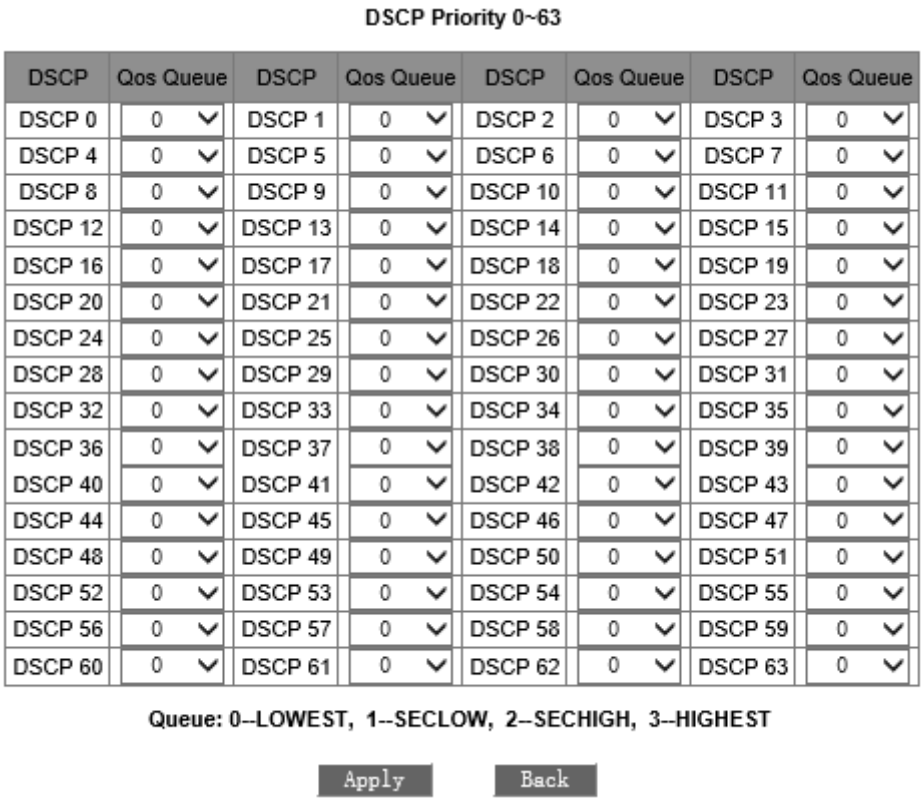


Figure 122 DSCP Priority-Queue Mapping

DSCP Priority

Portfolio: {DSCP, Qos Queue}

Range: {0~63, 0~3}

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

Function: Configure the mapping between DSCP priority and queue.

6.16.4 Typical Configuration Example

The following uses SICOM3024P V3.2 as an example to describe QoS configuration.

As shown in the following figure, port 1, port 2, port 3, and port 4 forward packets to port 5. The port-based mode is configured on port 1. The default priority of port 1 is 6. Packets from port 1 are mapped to queue 3. The 802.1p priority carried by packets from port 2 is 2, which is mapped to queue 1. The 802.1p priority carried by packets from port 3 is 4, which is mapped to queue 2. The DSCP priority carried by packets from port 4 is 6, which is mapped to queue 3. Port 5 adopts the WRR scheduling mode.

Configuration steps:

1. Select WRR for QoS mode and keep the default values for the WRR queue weight ratio, as shown in Figure 118 and Figure 119.
2. Configure highest priority-queue mapping on port 1, 802.1p on port 2 and port 3, and DIFF on port 4, as shown in Figure 120.
3. Configure 802.1p priority 6, 2, and 4 to map to queue 3, 1, and 2 respectively, as shown in Figure 121.
4. Configure DSCP priority 6 to map to queue 3, as shown in Figure 122.

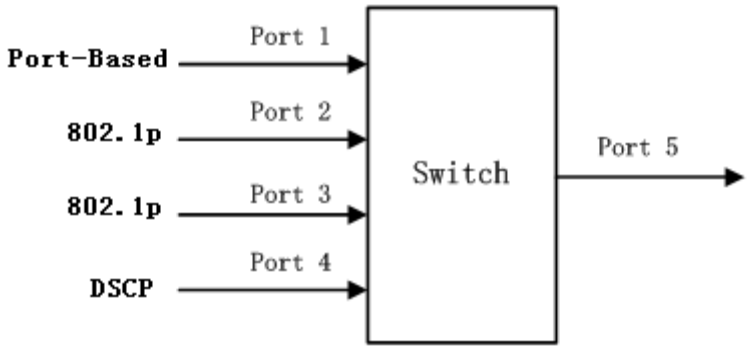


Figure 123 QoS Configuration Example

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

6.17 MAC Address Aging Time

6.17.1 Overview

Switch ports can learn addresses automatically. The switch adds the source addresses (source MAC address, switch port number) of received frames to the address table. Aging time starts from when a dynamic MAC address is added to the MAC address table. If no port receives a frame with the MAC address within one to two times the aging time, then the

switch deletes the entry of the MAC address from the dynamic forwarding address table. Static MAC address table does not involve the concept of aging time.

6.17.2 Web Configuration

Configure MAC address aging time, as shown in the following figure.

Figure 124 MAC Address Aging Time

MAC Aging Time

Range: 15~3600 seconds

Default: 300 seconds

Description: You can adjust the aging time as required.

6.18 LLDP

6.18.1 Overview

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

6.18.2 Web Configuration

1. Enable LLDP protocol, as shown in the following figure.

Figure 125 Enable LLDP

LLDP

Options: Enable/Disable

Default: Enable

Function: Enable/Disable LLDP protocol.

Explanation: If LLDP is enabled, the switch will send LLDP messages to its neighbor devices, meanwhile, receive and process the LLDP messages from the neighbor devices. If LLDP is disabled, the switch neither sends nor processes LLDP messages.

2. View LLDP connection information, as shown in the following figure.

LLDP Information

Local Port	Remote Port	Neighbor IP	Neighbor MAC
1/1	0/1	192.168.0.109	00:00:ee:ee:02:05

Figure 126 LLDP Information

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

Caution:

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

6.19 SNTP

6.19.1 Overview

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

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

Caution:

- To synchronize time by SNTP, there must be an active SNTP server.
- All the time information carried in the SNTP protocol is standard time information of time zone 0.

6.19.2 Web Configuration

1. Enable SNTP. Select the server and set related parameters, as shown in the following figure.

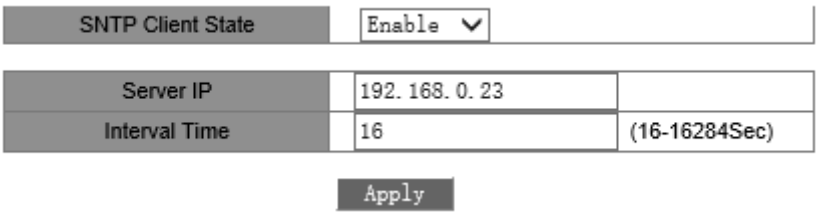


Figure 127 SNTP Configuration

SNTP Client State

Options: Enable/Disable

Default: Disable

Function: Enable/Disable SNTP.

Server IP

Format: A.B.C.D

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

Interval Time

Range: 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 the following figure.

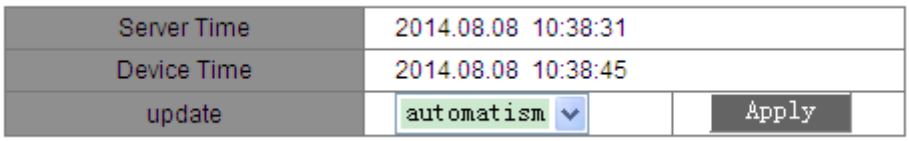


Figure 128 Time Synchronization Mode

Server Time

Function: Display the device latest time obtained from the server.

Device Time

Function: Display the local 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 the following figure. You can click the check box of an SNTP server and click <Delete> to delete it.

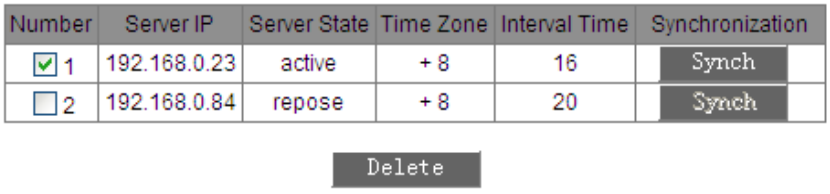


Figure 129 SNTP Configuration

Server State

Options: active/repose

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

Synchronization

To synchronize time manually, click <Synch>.

4. Configure the switch as the SNTP server, as shown in the following figure.

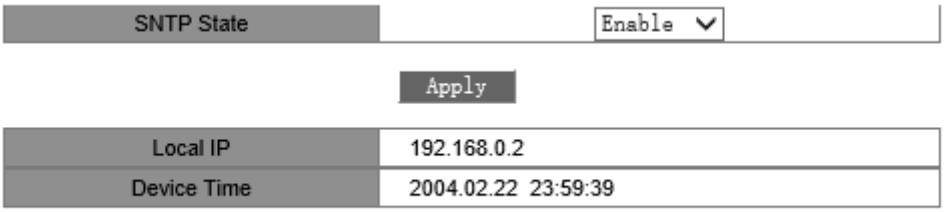


Figure 130 Configuring the Switch as the SNTP Server

SNTP State

Options: Enable/Disable

Default: Disable

Function: Enable or disable the SNTP server function.

time zone

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

Default: +8

Function: Select the server time zone.

6.20 PTP Configuration

6.20.1 Introduction

The Precision Time Protocol (PTP) synchronizes independent clocks on distributed nodes of the measurement and control system with high precision and accuracy. The protocol synchronizes both phase and frequency with precision up to ±100ns.

6.20.2 Concepts

1. PTP domain

A network on which PTP is applied is a PTP domain. A PTP domain has only one master clock. All the other devices synchronize time from it.

2. PTP port

A PTP-enabled port is called PTP port

3. Clock node

The nodes in a PTP domain are clock nodes. PTP defines the following clock nodes:

➢Ordinary Clock(OC)

In a PTP domain, the OC node has only one port participating in clock synchronization. The port synchronizes time from uplink clock node or to downlink clock node.

➢Boundary Clock (BC)

In a PTP domain, the BC node has one or multiple PTP ports participating in clock synchronization. If only one PTP port participates in clock synchronization, the port synchronizes time from uplink clock node or to downlink clock node. If multiple PTP ports take part in clock synchronization, one of these ports synchronizes time from uplink clock node and the other ports synchronize time to downlink clock nodes. When the BC serves as the clock source, it can deliver time to downlink clock nodes through multiple PTP ports.

➢Transparent Clock (TC)

The TC node does not need to keep time with other clock nodes. It has multiple PTP ports. These ports only forward PTP packets and verify forwarding delay, but do not perform clock synchronization. Transparent transmission clocks fall into the following types:

End-to-End Transparent Clock (E2ETC): directly forwards non-PTP packets and participates in delay calculation of the entire link.

Peer-to-Peer Transparent Clock (P2PTC): directly forwards Sync, Follow_Up, and Announce packets, terminates other PTP packets, and participates in delay calculation of each segment of a link.

4. Relationship between a pair of synchronous clock nodes:

The node sending synchronization clock information is the master mode, while the nodes receiving the information are slave nodes.

The clock of the master node is master clock, while the clock of a slave node is slave clock.

The port sending synchronization clock information is the master port, while the ports receiving the information are slave ports.

6.20.3 Synchronization Principle

1. Selection of the grandmaster clock

All clock nodes select the grandmaster clock in the PTP domain by exchanging Announce packets with clock stratum and clock ID information. Then the master/slave relationship

between nodes and master/slave ports on the nodes are determined. With this process, a spanning tree with the grandmaster clock as the root is established throughout the PTP domain. Then the master clock periodically sends Announce packets to slave clocks. If a slave clock does not receive Announce packets from the master clock within a period, the master clock is considered invalid and new selection is started.

Announce packets contain the following information for grandmaster clock selection: grandmaster priority 1, clock stratum, clock accuracy, grandmaster priority 2, and clock ID. The information is compared in the following procedure: the clock with lowest grandmaster priority 1 is elected as the grandmaster clock; if clocks have the same value for grandmaster priority 1, the clock with lowest clock stratum is elected as the grandmaster clock; similarly, if clocks have the same values for grandmaster priority 1, clock stratum, clock accuracy, grandmaster priority 2, the clock with lowest clock ID is elected as the grandmaster clock.

2. Synchronization principle

Master and slave clocks exchange synchronization packets, record sending and receiving time of packets, and calculate the total delay between master and slave clocks based on time difference. If the network path is symmetric, the unidirectional delay is half the total delay. A slave clock adjusts local time according to the time difference between master and slave clocks and unidirectional delay, implementing time synchronization from the master clock.

PTP supports two delay measurement mechanisms:

Request-response mechanism: used for the end-to-end delay measurement of an entire link.

Peer-to-peer mechanism: used for point-to-point delay measurement. Compared with the request_response mechanism, the peer-to-peer mechanism measures the delay of each segment of a link.

6.20.4 Web Configuration

1. Enable PTP on the port.as shown in Figure 131.

Port Status Configuration

Port	Status	Pdelay Correction		Master-allow	Limit Class		Limit Accuracy	
1/1	Disable	0	(-65535~65535ns)	Enable	0	(0~255)	0	(0~255)
1/1	Disable	0		Enable	0		0	
1/2	Disable	0		Enable	0		0	
1/3	Disable	0		Enable	0		0	
1/4	Disable	0		Enable	0		0	
1/5	Disable	0		Enable	0		0	
1/6	Disable	0		Enable	0		0	
1/7	Disable	0		Enable	0		0	
1/8	Disable	0		Enable	0		0	
2/1	Disable	0		Enable	0		0	
2/2	Disable	0		Enable	0		0	
2/3	Disable	0		Enable	0		0	
2/4	Disable	0		Enable	0		0	
2/5	Disable	0		Enable	0		0	
2/6	Disable	0		Enable	0		0	
2/7	Disable	0		Enable	0		0	
2/8	Disable	0		Enable	0		0	
3/1	Disable	0		Enable	0		0	
3/2	Disable	0		Enable	0		0	
3/3	Disable	0		Enable	0		0	
3/4	Disable	0		Enable	0		0	
3/5	Disable	0		Enable	0		0	

Figure 131 Enabling PTP on Port

Status

Options: Enable/Disable

Default: Disable

Function: Enable/disable the port PTP function.

Pdelay Correction

Range: -65535~65535 ns

Default: 0 ns

Function: Configure PTP link delay compensation.

Description: When there is a fixed offset between the master and slave clocks, the parameter needs to be configured on the slave clock to synchronize phase.

Master-allow

Options: Enable/Disable

Default: Enable

Function: This parameter determines whether the current port is allowed to be used as the master port for releasing synchronization clock. When **Enable** is selected, the clock node can synchronize other network clocks through this port. When **Disable** is selected, the clock node cannot synchronize other network clocks through this port. This prevents other network

clock information from being affected by the clock node.

Limit Class

Range: 0~255

Default: 0

Function: To prevent the current system clock information from being affected by external clock sources, configure the clock stratum limit value to limit the clock stratum in the Announce packet received by this port. If the clock stratum in the Announce packet received by this port is superior to the limit value (that is, the clock stratum value is smaller than the limit value), modify the clock stratum in the packet to be consistent with the limit value. Otherwise, the clock stratum in the packet is not processed. When the limit value is 0, the clock stratum in the Announce packet is not limited.

Limit Accuracy

Range: 0~255

Default: 0

Function: To prevent the current system clock information from being affected by external clock sources, configure the clock accuracy limit value to limit the clock accuracy in the Announce packet received by this port. If the clock accuracy in the Announce packet received by this port is superior to the limit value (that is, the clock accuracy value is smaller than the limit value), modify the clock accuracy in the packet to be consistent with the limit value. Otherwise, the clock accuracy in the packet is not processed. When the limit value is 0, the clock accuracy in the Announce packet is not limited.

2. Set PTP parameters, as shown in Figure 132.

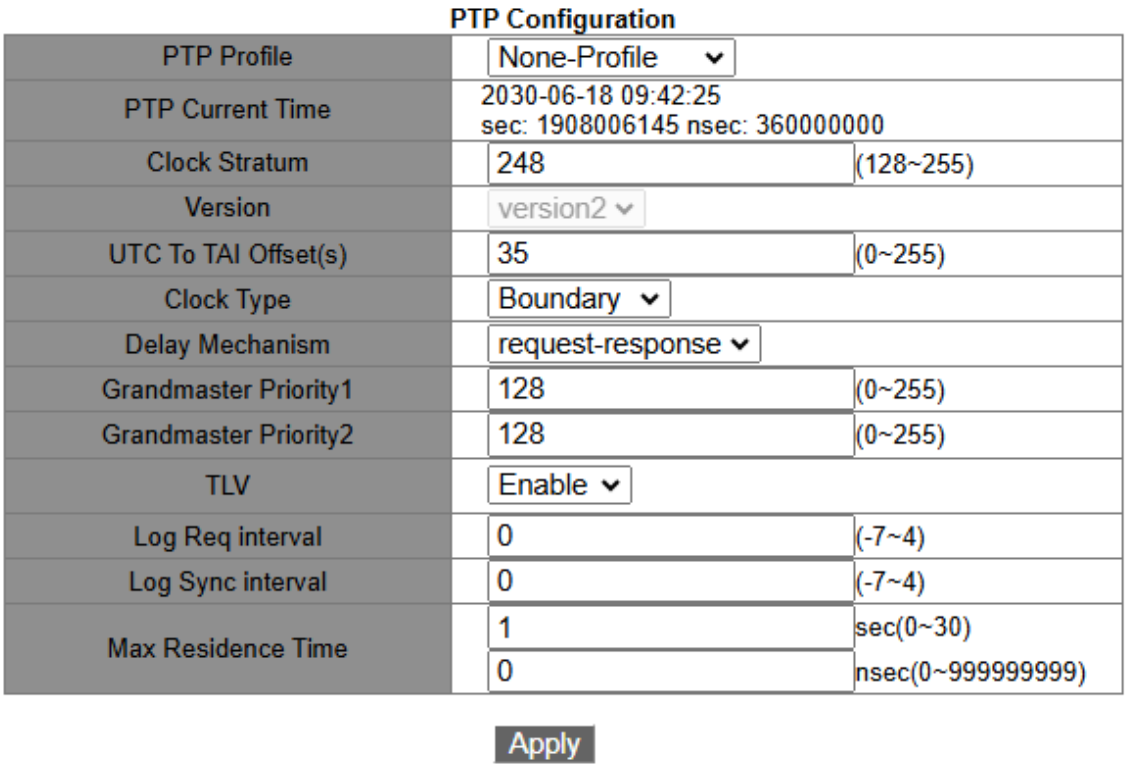


Figure 132 PTP Setting

PTP Profile

Options: Power-Profile/None-Power-Profile

Default: None-Power-Profile

Function: Configure PTP Profile. PTP Profile indicates the set of PTP application features.

Description: Power-Profile is the set of PTP features that enable the switch to apply to power industry. For example, "delay mechanism" is forcibly configured as peer-to-peer, and "TLV" is forcibly enabled.

PTP Current Time

Function: View switch PTP clock information. The PTP time is shown in TAI time.

Clock Stratum

Range: 128~255

Default: 248

Function: Select the clock stratum.

Description: When clocks have the same value for grandmaster priority 1, the clock with lowest clock stratum is elected as the grandmaster clock. If a clock obtains time from GPS

clock, the clock stratum can be automatically configured as 6, 7, 52 or 187 to improve the possibility of being elected as the grandmaster clock.

Explanation: Clock stratum can be configured as 255 when the clock type is Slave-only. Otherwise, the clock stratum cannot be configured as 255.

Note：

When the GPS is in the fix state, the clock stratum is 6 (clock accuracy is 0x21); when the GPS is in the lock state, the clock stratum is 6 (clock accuracy is 0x20); when GPS failures occur, the clock stratum is 7 (clock accuracy is 0x23); when the hold over time runs out after GPS failure, the clock stratum is 52 or 187 (clock accuracy is 0x30).

Version

Options: version2

Default: version2

Function: Select the version of PTP.

UTC To TAI Offset

Range: 0~255 s

Default: 35 s

Function: Configure UTC-To-TAI Offset. The value can be overwritten by UTCOffSet value obtained from GPS or Announce packets of master clock. The relationship among UTC, TAI, and Offset is: UTC=TAI-Offset.

Clock Type

Options: Boundary/E2E/P2P/Slave-only

Default: Boundary

Function: Select the type of PTP clock.

Description: Slave-only indicates that the OC clock can only be a slave clock.

Delay Mechanism

Options: request-response/peer-to-peer

Default: request-response

Function: Configure PTP delay measurement mechanism.

Caution：

- The clock node having multiple domains must be configured to boundary clock type.
- The delay mechanism of BC/OC clock node can be set to request-response or peer-to-peer mode.
- If the type of TC clock node is E2ETC, the delay measurement mechanism must be set to request-response mode.
- If the type of TC clock node is P2PTC, the delay measurement mechanism must be set to peer-to-peer mode.
- The delay measurement mechanism of all devices in the same PTP domain should be the same, so the types of all TC clock nodes in a PTP domain should be the same.

Grandmaster priority1/Grandmaster priority2

Range: 0~255

Default: 128

Function: Configure Grandmaster priority1 and Grandmaster priority2.

Description: Grandmaster priority1 and Grandmaster priority2 are used to select the grandmaster clock. The clock with lowest grandmaster priority is elected as the grandmaster clock.

TLV

Options: Enable/Disable

Default: Enable

Function: Enabling TLV means Announce packets carry TLV field. Disabling TLV means Announce packets do not carry TLV field.

Log Req interval

Range: -7~4

Default: 0

Function: The interval between Delay Request message transmissions from the PTP clock.

Log Req interval

Range: -7~4

Default: 0

Function: Control the interval between the transmission of synchronization messages; these messages are the primary time synchronization messages in PTP.

Max Residence Time

Range:sec(0~30)/ nsec(0~999999999)

Function: Residence time of PTP messages on this device.

3. Set TLV parameters, as shown in Figure 133.

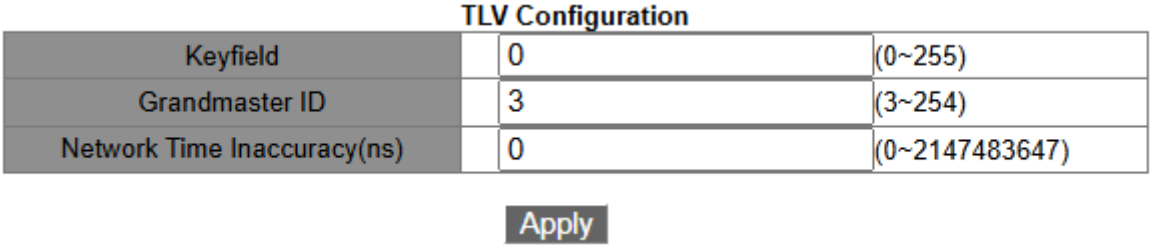


Figure 133 TLV parameters configuration

Keyfield

Range: 0~255

Default: 0

Function: Configure grandmaster clock Keyfield. If the type of TLV field carried by Announce packets is ALTERNATE_TIME_OFFSET_INDICATOR, the parameter needs to be configured.

Grandmaster ID

Range: 3~254

Default: 3

Function: Configure grandmaster ID. If the type of TLV field carried by Announce packets is ORGANIZATION_EXTENSION, the parameter needs to be configured.

Network Time Inaccuracy

Range: 0~2147483647 ns

Default: 0 ns

Function: Configure PTP network time inaccuracy. If the type of TLV field carried by Announce packets is ORGANIZATION_EXTENSION, the parameter needs to be configured as time inaccuracy accumulated in the worst network path.

4. Configure PTP Domain,as shown in Figure 134.

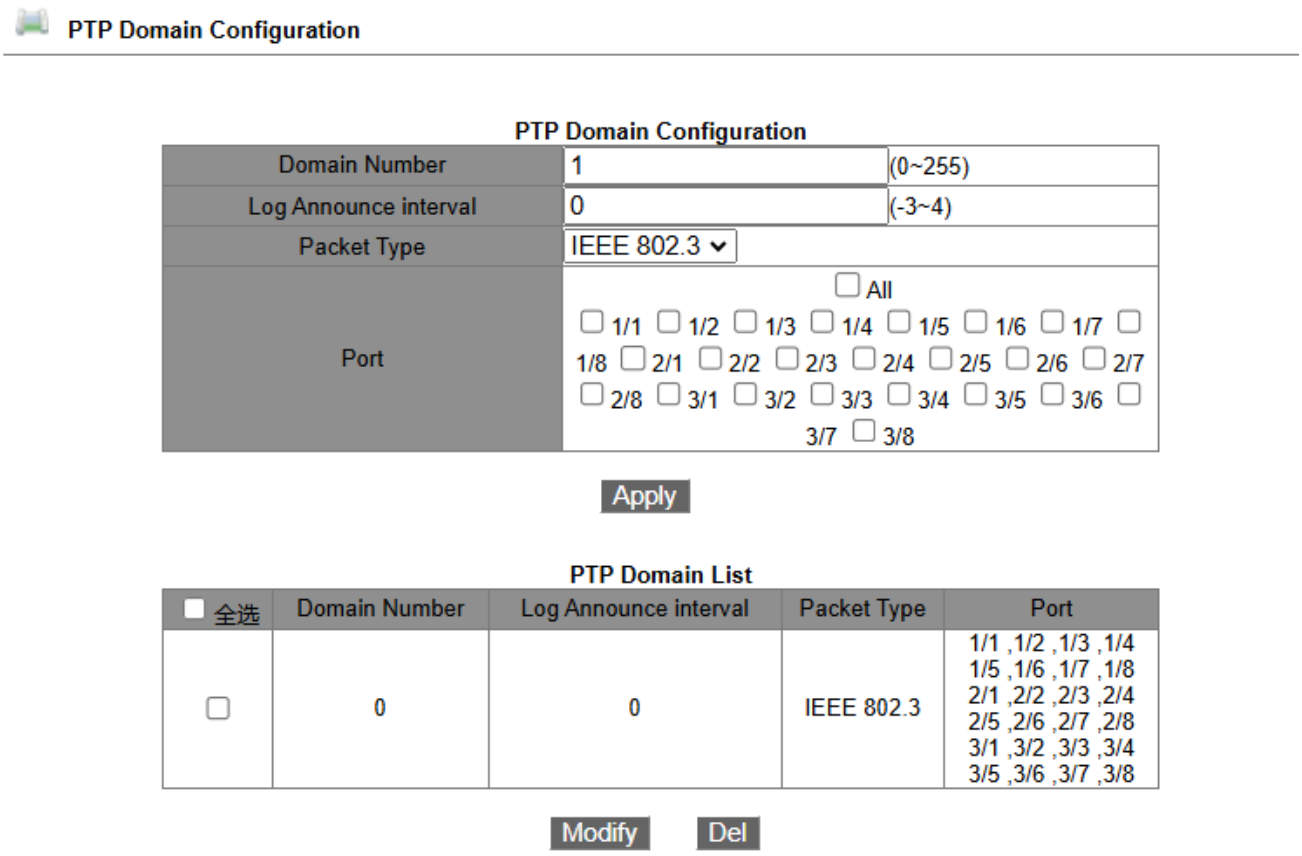


Figure 134 PTP Domain Configuration

Domain Number

Range: 0~255

Default: 0

Function: Configure the domain ID of PTP.

Log Announce interval

Range: -3~4

Default: 0

Function: Configure the exponent of Announce interval.

Description: Each node sends Announce packets at the interval of 2^n s (n is the exponent).

Packey Type

Options: IEEE802.3/IPv4 UDP

Default: IEEE802.3

Function: Select the type of packets carrying PTP information.

Port

Function: Select the port of the device in the current PTP domain.

Note:

➢Domain 0 is the default PTP domain of the system, which cannot be deleted.

➢The packet type configurations of all devices in the same PTP domain must be consistent.

➢One port can be added to only one domain.

6.21 Port Isolate

6.21.1 Overview

To implement isolation of packets on layer 2, you can add ports to different VLANs. However, this method will cause a waste of limited VLAN resources. By adopting the port isolation feature, you can isolate ports in the same VLAN from each other. The user only needs to add the port to the isolation group, and the isolation of data in layer 2 among ports of the isolation group would be realized because the ports in the isolation group would not forward packets to other ports of the isolation group. The port isolation function provides users with a more secure and flexible networking solution.

Note:

➢Ports of the isolation group can only be ports from the same switch.

➢Following the configuration of the isolation group, only the packets among the ports of the isolation group could not exchange with each other, the communication between the ports within the isolation group and the ports outside the isolation group would not affected.

6.21.2 Web Configuration

Enable the port isolation, as shown in Figure 135.

Port	Isolate Enable
S1/FE1	☑
S1/FE2	☑
S1/FE3	☑
S1/FE4	☐
S1/FE5	☐
S1/FE6	☐
S1/FE7	☐
S1/FE8	☐
S2/FE1	☐

Figure 135 Port Isolation Configuration

Isolate Enable

Options: Enable/Disable

Default: Disable

Function: Enable or disable the port isolate.

Note:

The device support only one isolation group, which means that the ports with its port isolation being enabled could not exchange information with each other while the communication between the ports with its port isolation being enabled and the ports with its port isolation not being enabled would not be affected.

6.21.3 Typical Configuration Example

Networking Requirements:

Connect PC1, PC2 and PC3 to the Ethernet port 1, 2 and 3 of the switch, and connect port 4 to the external network. PC1, PC2 and PC3 cannot communication with each other, but they can access the external network, as shown in Figure 136.

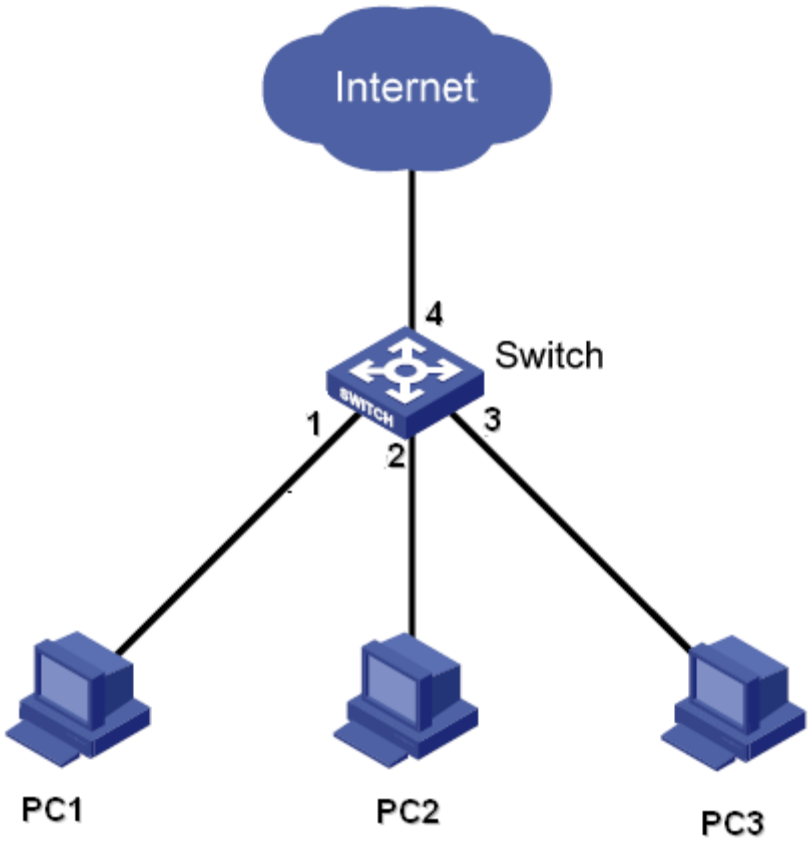


Figure 136 port isolation configuration instance

Specific configuration:

Add port 1, 2 and 3 to the isolation group to isolate PC1, PC2 and PC3, as shown in Figure 135.

6.22 Alarm

6.22.1 Introduce

The series device supports the following types of alarms:

IP/MAC conflict alarm: If enable, the alarm occurs when the IP/MAC address conflict;

Memory utilization alarm: If enable, the alarm occurs when the memory utilization is too high;

CPU utilization alarm: If enable, the alarm occurs when CPU utilization is too high;

Powe alarm: If enable, the alarm occurs when single power input;

Temperature alarm: If enable, the alarm occurs when the switch temperature is below the lower threshold or above the upper threshold;

Port alarm: If enable, the alarm occurs when port Link down;

Ring alarm: If enable, the alarm occurs when the ring is disconnected;

Configuration change alarm: If enable, the alarm occurs when configuration changes;

Login and Logout alarm: If enable, the alarm occurs when users log in and log out

Note:

- Only XJ-Ring master station and DRP ring Root support alarm function;
- Support IP/MAC conflict alarm, memory utilization alarm, CPU utilization alarm, power alarm, temperature alarm, port alarm, ring alarm, configuration change alarm and login/logout alarm

6.22.2 Web page configuration

1、Alarm configuration, as shown in Figure 137;

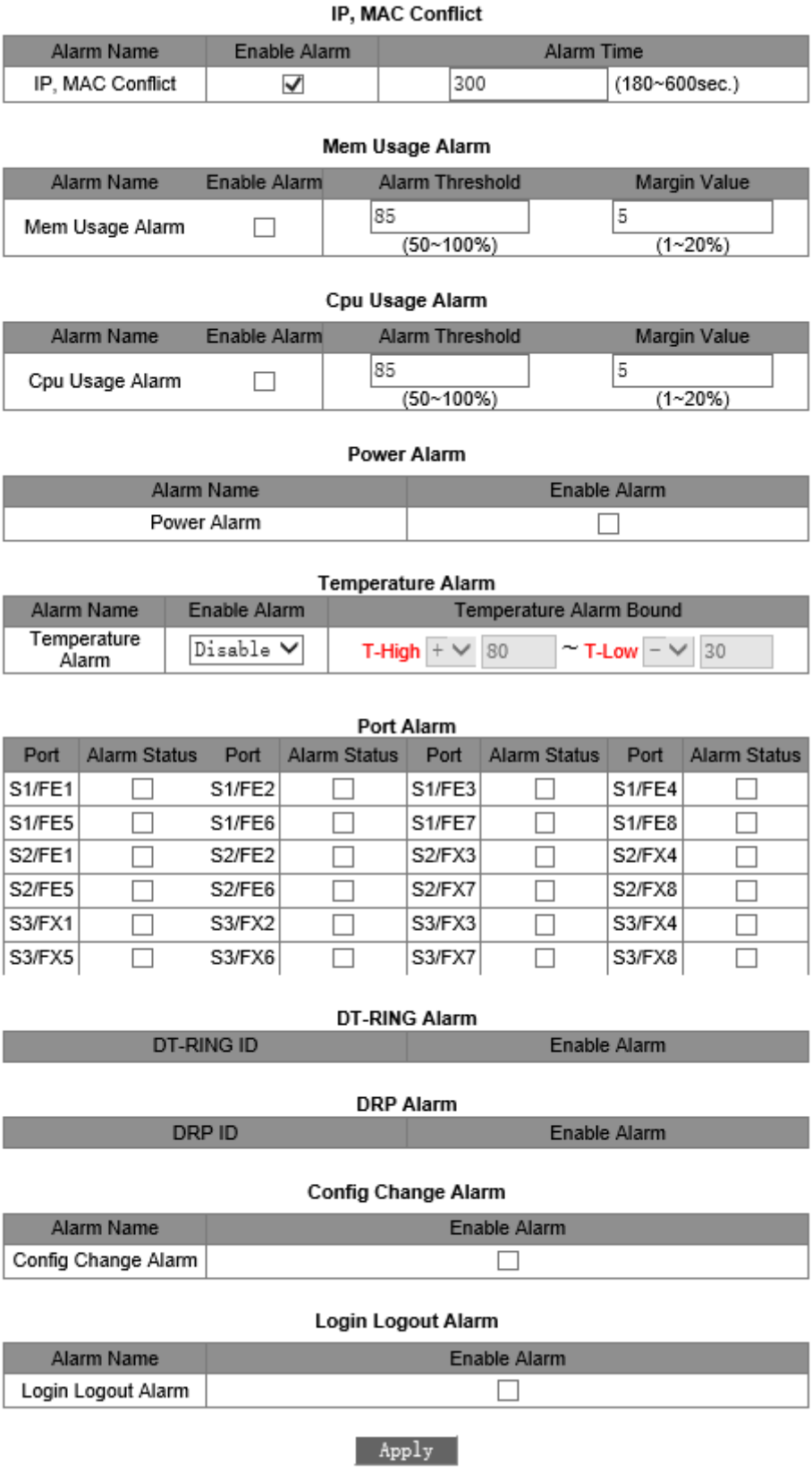


Figure 137 Alarm configuration

IP、MAC conflict alarm

Configuration option: Enable/disable

Default configuration: Enable

Function: Whether enable address conflict alarm.

Test time

Configuration range: 180~600s

Default: 300s

Function: Configure the time interval to detect address conflicts.

Memory utilization alarm

Configuration range: {Enable/disable，50%~100%}

Default configuration: {disable, 85%}

Function: Whether enable memory utilization alarm。

CPU utilization alarm

Configuration range: {Enable/disable，50%~100%}

Default configuration: {disable, 85%}

Function: Whether enable CPU utilization alarm。

Power alarm

Configuration option: Enable/disable

Default configuration: Disable

Function: Whether enable power alarm.

Temperature alarm {alarm enable, Upper threshold value ~ Lower threshold value}

Configuration range: {Enable/disable，+150℃~-55℃}

Default configuration: {Disable, +80℃~-30℃}

Function: Whether enable temperature alarm, and configure temperature upper and lower threshold value.

Port alarm

Configuration option: Enable/disable

Default configuration: Disable

Function: Whether enable port alarm.

Ring alarm/DRP alarm

Configuration option: Enable/disable

Default configuration: Disable

Function: Whether enable ring alarm.

Configuration change alarm

Configuration option: Enable/disable

Default configuration: Disable

Function: Whether enable configuration change alarm.

Login and logout alarm

Configuration option: Enable/disable

Default configuration: Disable

Function: Whether enable login and logout alarm.

2、After enabling alarm, alarm display as shown in Figure 138;

Basic Vision

Alarm Title	Alarm Status
power	WARN
temperature	NONE
IP Alarm	Normal
MAC Alarm	Normal

Port Alarm

Port	Alarm Status	Port	Alarm Status	Port	Alarm Status	Port	Alarm Status
S1/FE1	Link Up	S1/FE2	Link Up	S1/FE3	Link Down	S1/FE4	-
S1/FE5	-	S1/FE6	-	S1/FE7	-	S1/FE8	-
S2/FE1	-	S2/FE2	-	S2/FE3	-	S2/FE4	-
S2/FE5	-	S2/FE6	-	S2/FE7	-	S2/FE8	-
S3/FE1	-	S3/FE2	-	S3/FE3	-	S3/FE4	-
S3/FE5	-	S3/FE6	-	S3/FE7	-	S3/FE8	-
S4/GX1	-	S4/GX2	-	S4/GX3	-	S4/GX4	-

DT-RING Alarm

DT-RING ID	Alarm Status
2	Ring Open
1	Ring Close

DRP Alarm

DRP ID	Alarm Status
1	Normal
2	Alarm

Figure 138 Alarm display

Memory utilization:

Display option: Normal/Alarm

Description: After enabling memory utilization alarm, the alarm occurs when the memory utilization is high.

CPU utilization:

Display option: Normal/Alarm

Description: After enabling CPU utilization alarm, the alarm occurs when CPU utilization is high.

Power alarm

Display option: Normal/Alarm

Description: After enabling power alarm, the display is normal when dual power input,

the alarm occurs when single power input.

Temperature alarm

Display option: Normal/upper limit alarm/lower limit alarm

Description: The upper limit alarm is displayed when the switch temperature is above or equal to the upper threshold; the lower limit alarm is displayed when the switch temperature is below or equal to the lower threshold; otherwise, the display is normal.

IP/MAC conflict alarm

Display option: Normal/Alarm

Description: The alarm occurs when the address conflict, otherwise, the display is normal.

Port alarm

Display option: Link Up/Link Down

Description: After enabling port alarm, Link Up is shown when port connection is normal, Link Down is shown when port is disconnected or the connection is abnormal.

Ring alarm

XJ-Ring display option: Ring Open/Ring Close

DRP display option: Alarm/Normal

Description: After enabling ring alarm, Ring Open is shown or the alarm occurs when ring is open, Ring Close is displayed or the alarm occurs when ring is close or ring is normal.

Configuration change alarm：

Display option: Normal/Alarm

Description: After enabling configuration change alarm, the alarm is displayed when memory utilization is high.

Login and logout alarm

Display option: Normal/Alarm

Description: After enabling login and logout alarm, the alarm is displayed when user log in or log out.

6.23 Port Traffic Alarm

6.23.1 Overview

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

Caution:

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

6.23.2 Web Configuration

1. Configure port traffic alarm, as shown in the following figure.

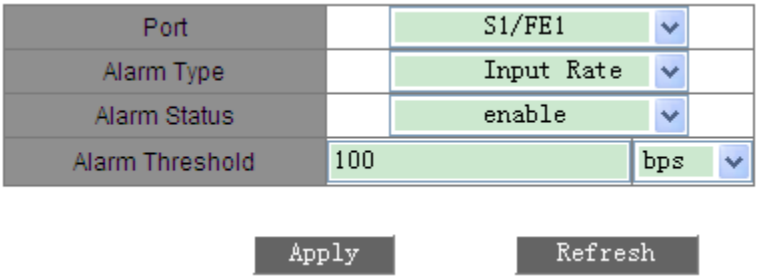


Figure 139 Configuring Port Traffic Alarm

Port

Options: all switch ports

Function: Select the ports for traffic alarm.

Alarm Type

Options: Input Rate/Output Rate/CRC Error

Function: Configure the port traffic alarm type.

Alarm Status

Options: enable/disable

Default: disable

Function: Enable or disable the alarm type.

Alarm Threshold

Range: 1~1000000000bps or 1~1000000kbps

Function: Configure the port traffic alarm threshold.

2. View port traffic alarm information, as shown in the following figure.

Port	Input Rate		Alarm Status	Output Rate		Alarm Status	Error CRC	Alarm Status
S1/FE1	enable	100bps	alarm	enable	1000bps	alarm	enable	alarm
S1/FE2	enable	100kbps	normal	enable	100bps	normal	enable	normal
S1/FE3	disable	-	-	disable	-	-	disable	-
S1/FE4	disable	-	-	disable	-	-	disable	-
S1/FE5	disable	-	-	disable	-	-	disable	-
S1/FE6	disable	-	-	disable	-	-	disable	-
S1/FE7	disable	-	-	disable	-	-	disable	-
S1/FE8	disable	-	-	disable	-	-	disable	-
S4/GE1	disable	-	-	disable	-	-	disable	-
S4/GE2	disable	-	-	disable	-	-	disable	-
S4/GE3	disable	-	-	disable	-	-	disable	-
S4/GE4	disable	-	-	disable	-	-	disable	-

Figure 140 Port Traffic Alarm Information

6.24 GMRP Configuration and Query

6.24.1 GARP

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

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

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

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

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

Note:

An application entity indicates a GARP-enabled port.

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

Hold Timer: When receiving a registration message, a GARP entity does not send a Join message immediately, but starts a Hold timer. When the timer expires, the entity sends all the registration messages received within the preceding period in one Join message, reducing packet sending for better network stability.

Join Timer: To ensure that Join messages are received by other application entities, a GARP application entity starts a Join timer after sending a Join message. If receiving no JoinIn message before Join timer expires, the entity sends the Join message again. If receiving a JoinIn message before the timer expires, the entity does not send the second Join message.

Leave Timer: When a GARP application entity wants to cancel the information about an attribute, the entity sends a Leave message. The entity receiving the message starts Leave timer. If receiving no Join message before the timer expires, then the entity receiving the message cancels the information about the attribute.

LeaveAll Timer: As a GARP application entity starts, it starts LeaveAll timer. When the timer expires, the entity sends a LeaveAll message, so that the other GARP application entities re-register all the attributes. Then the entity starts LeaveAll timer again for the new cycle.

6.24.2 GMRP

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

network.

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

6.24.3 Description

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

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

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

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

6.24.4 Web Configuration

1. Enable the global GMRP protocol, as shown in the following figure.

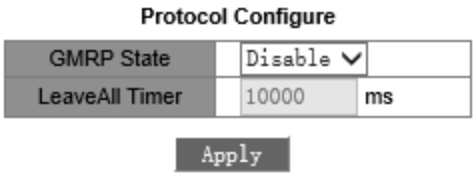


Figure 141 GMRP Global Configuration

GMRP State

Options: Enable/Disable

Default: Disable

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

LeaveAll Timer

Range: 100ms~327600ms

Default: 10000ms

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

100.

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

2. Configure GMPR function on each port, as shown in the following figure.

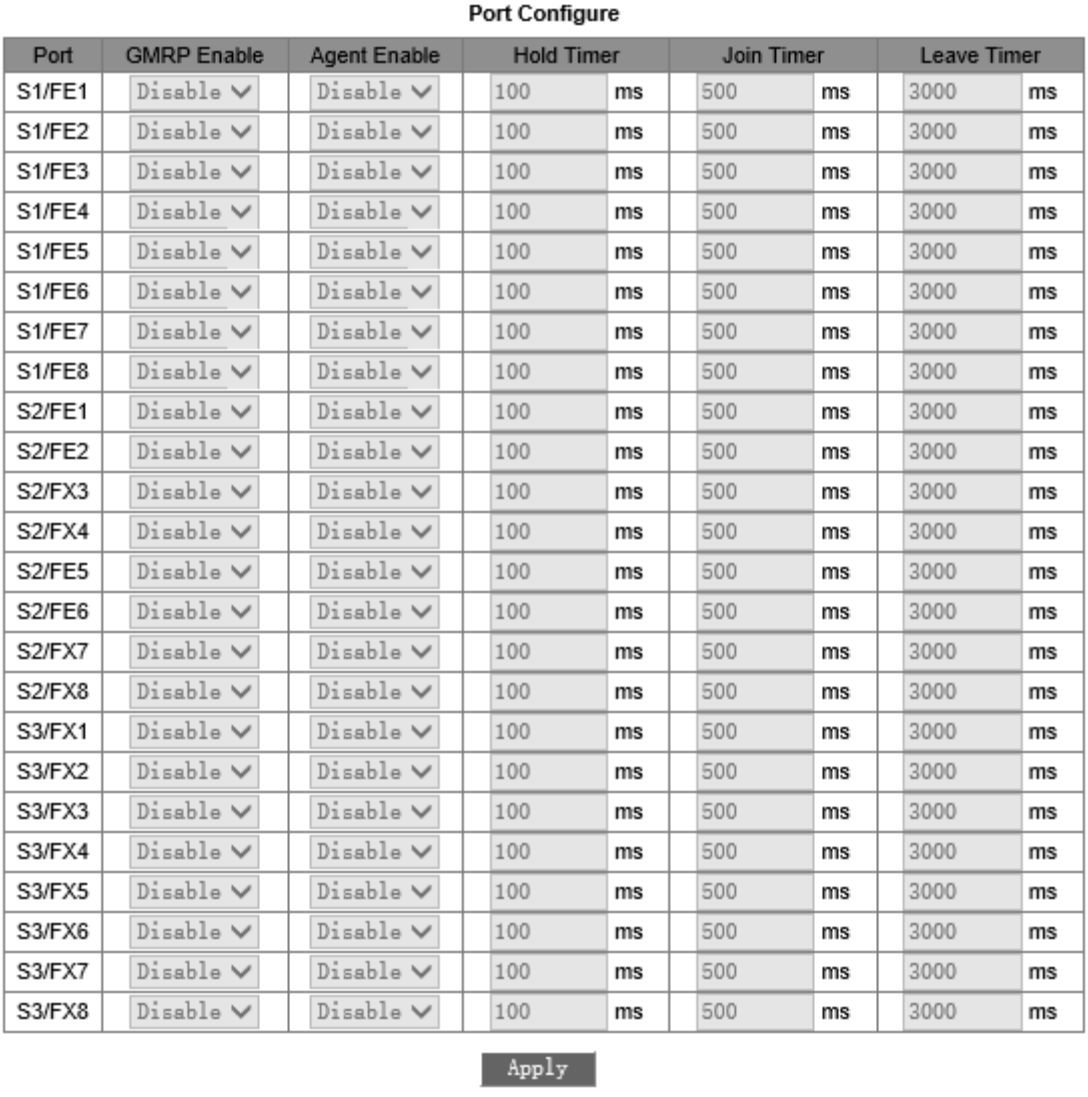


Figure 142 Port GMRP Configuration

GMRP Enable

Options: Enable/Disable

Default: Disable

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

Agent Enable

Options: Enable/Disable

Default: Disable

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

Caution:

- Agent port cannot propagate agent entry.
- To enable the GMRP agent function on a port, you need to enable the GMRP function first.

Hold Timer

Range: 100ms~327600ms

Default: 100ms

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

Join Timer

Range: 100ms~327600ms

Default: 500ms

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

Leave Timer

Range: 100ms~327600ms

Default: 3000ms

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

3. Add a GMRP agent entry, as shown in the following figure.

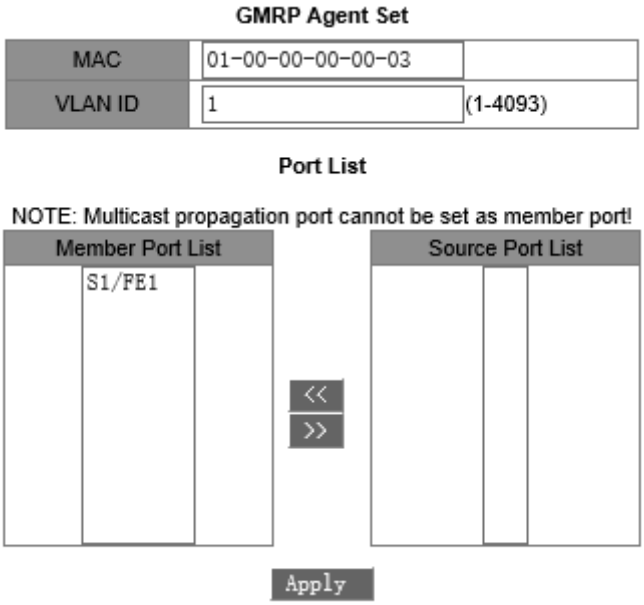


Figure 143 GMRP Agent Entry Configuration

MAC

Format: HHHHHHHHHHHH (H is a hexadecimal number.)

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

VLAN ID

Options: all created VLAN numbers

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

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

Member Port List

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

Source Port List

Options: all GMRP agent-enabled ports

4. View, modify, or delete a GMRP agent entry, as shown in the following figure.

GMRP Agent List

Index	MAC	VLAN ID	Member Port
1	01-00-00-00-00-01	1	S1/FE1
2	01-00-00-00-00-02	2	S1/FE1

Add Delete Modify

Figure 144 GMRP Agent Entry Operations

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

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

The following conditions shall be met.

- GMRP is enabled on the inter-connected devices.
- The two ports that connect the devices must be propagation ports, and the VLAN ID of the propagation port on the local device must be identical with that in the agent entry.

GMRP Dynamic Multicast List

Index	Multicast MAC	VLAN ID	Member Port
1	01-00-00-00-00-01	1	S0/FE1

Figure 145 GMRP Dynamic Multicast Table

GMRP Dynamic Multicast List

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

Function: View GMRP dynamic multicast entries.

6.24.5 Typical Configuration Example

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

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

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

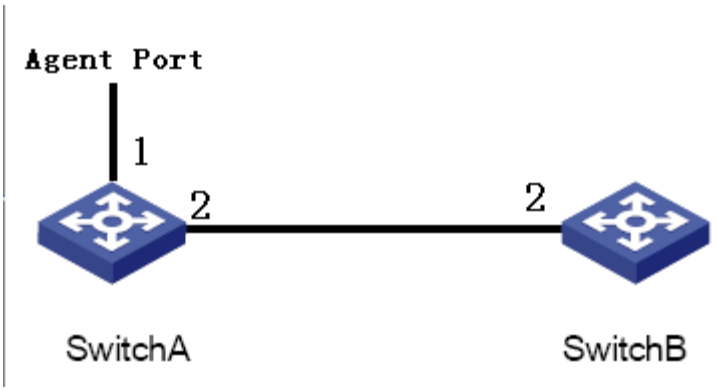


Figure 146 GMRP Networking

Configuration on Switch A:

1. Enable global GMRP function in switch A; set LeaveAll timer to the default value, as shown in Figure 141.
2. Enable GMRP function and agent function in port 1; enable only GMRP function in port 2; set the timers to default values, as shown in Figure 142.
3. Configure agent multicast entry. Set <MAC address, VLAN ID, Member port> to <01-00-00-00-00-01, 1, 1> and <01-00-00-00-00-02, 2, 1>, as shown in Figure 143.

Configuration on Switch B:

1. Enable global GMRP function in switch B; set LeaveAll timer to the default value, as shown in Figure 141.
2. Enable GMPR function on port 2; set the timers to default values, as shown in Figure 142.

The following table lists the dynamically learned GMRP multicast entries on Switch B.

Table 9 Dynamic Multicast Entries

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

		VLAN ID: 2 Member port: 2

6.25 RMON

6.25.1 Overview

Based on SNMP architecture, Remote Network Monitoring (RMON) allows network management devices to proactively monitor and manage the managed devices. An RMON network usually involves the Network Management Station and Agents. The NMS manages Agents and Agents can collect statistics on various types of traffic on these ports.

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

6.25.2 RMON Groups

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

- Statistics group

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

- History group

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

- Event group

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

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

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

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

None: indicates no action.

- Alarm group

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

Caution:

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

6.25.3 Web Configuration

1. Configure the statistics table, as shown in the following figure.

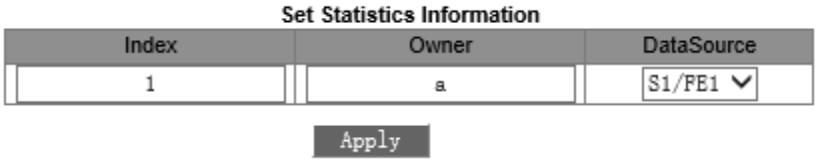


Figure 147 RMON Statistics

Index

Range: 1~65535

Function: Configure the number of the statistics entry.

Owner

Range: 1~32 characters

Function: Configure the name of the statistics entry.

Data Source

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

2. Configure the history table, as shown in the following figure.

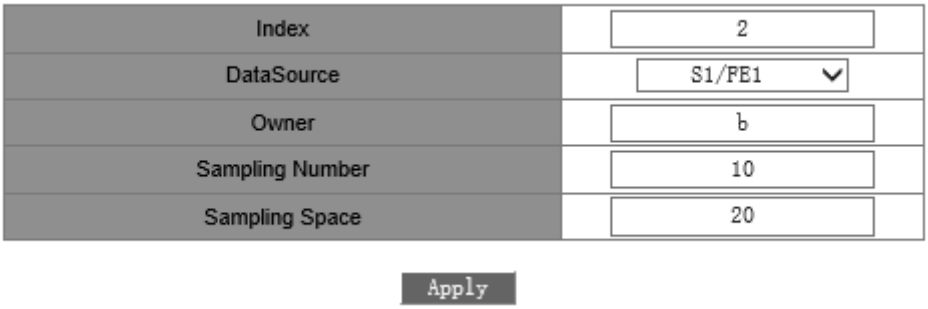


Figure 148 RMON History Table

Index

Range: 1~65535

Function: Configure the number of the history entry.

Data Source

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 the following figure.

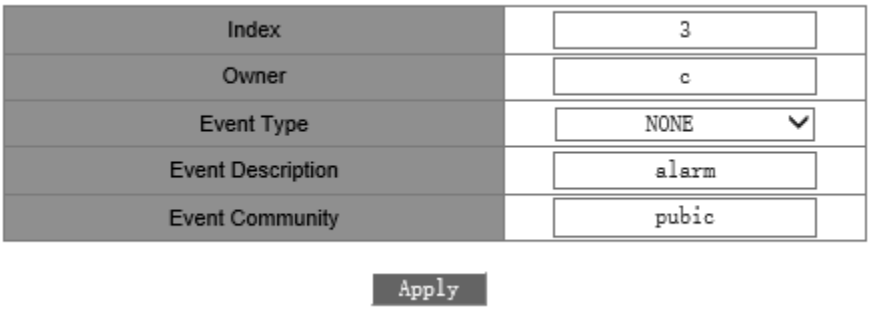


Figure 149 RMON Event Table

Index

Range: 1~65535

Function: Configure the index number of the event entry.

Owner

Range: 1~32 characters

Function: Configure the name of the event entry.

Event Type

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

Default: NONE

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

Event Description

Range: 1~127 characters

Function: Describe the event.

Event Community

Range: 1~127 characters

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

4. Configure the alarm table, as shown in the following figures.

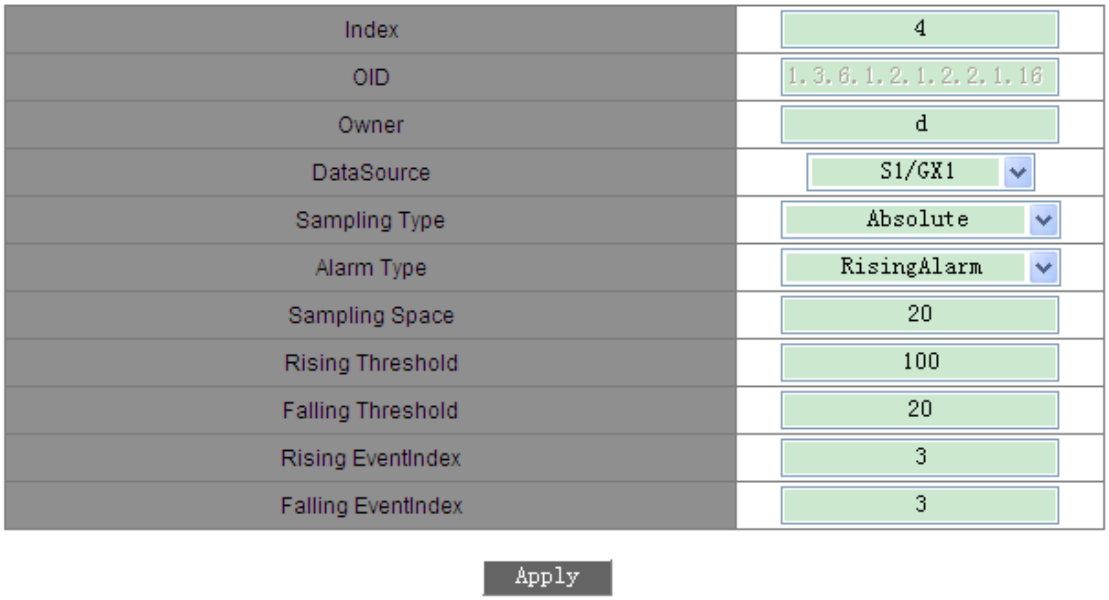


Figure 150 RMON Alarm Table

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

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

Sampling Type

Options: Absolute/Delta

Default: Absolute

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

Alarm Type

Options: RisingAlarm/FallingAlarm/RisOrFallAlarm

Default: RisingAlarm

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

Sampling Space

Range: 1~65535

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

Rising Threshold

Range: 0~65535

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

Falling Threshold

Range: 0~65535

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

Rising Event Index

Range: 0~65535

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

Falling Event Index

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

6.26 Log Query

6.26.1 Overview

The log function records the switch running information, facilitating the administrator in reading and managing log packets and locating faults.

Running log covers:

- Power alarm, temperature alarm, IP/MAC conflict alarm, port alarm, DT-Ring alarm, and port traffic alarm
- Broadcast storm
- Software system restart

6.26.2 Description

The running log contains a maximum of 1024 entries. When more than 1024 entries are configured, new entries overwrite the old entries.

6.26.3 Web Configuration

1. Enable the log function, as shown in the following figure.

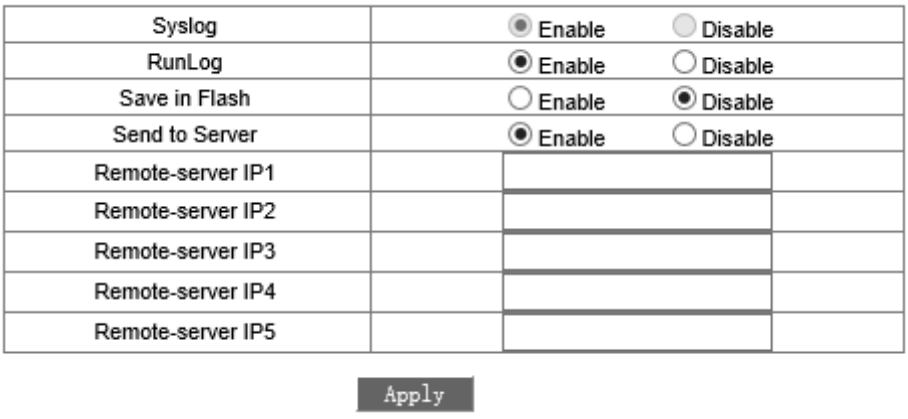


Figure 151 Log Status Configuration

Enable Runlog

Options: Enable/Disable

Default: Enable

Function: Enable or disable the running log function. If the function is enabled, running information will be recorded.

2. Configure running log upload, as shown in the following figure.

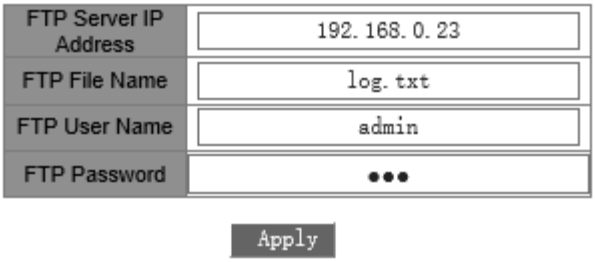


Figure 152 Running Log Upload

FTP Server IP Address

Format: A.B.C.D

Function: Set the IP address of the FTP server.

FTP File Name

Range: 1~20 characters

Function: Set the name of the log file saved on the server.

FTP User Name

Range: 1~20 characters

Function: Set the FTP user name.

FTP Password

Range: 1~20 characters

Function: Set the FTP password.

Caution:

The FTP server software needs to be running during log upload.

3. View the running log, as shown in the following figure.

Performance log

Index	LogType	Time	Description
10	Ring Open/Close	THU SEP 13 15:24:42 2012	Ring alarm: entity id:1 state:Ring open
9	PortLink Alarm	THU SEP 13 15:24:42 2012	Port alarm: entity id:1/2 port:1/2 state:Link down
8	Ring Open/Close	THU SEP 13 15:24:07 2012	Ring alarm: entity id:1 state:Ring close
7	PortLink Alarm	THU SEP 13 15:24:07 2012	Port alarm: entity id:1/2 port:1/2 state:Link up
6	Output rate	THU SEP 13 15:23:44 2012	Output alarm: entity id:1 state:Alarm
5	Input rate	THU SEP 13 15:23:43 2012	Input alarm: entity id:1 state:Alarm
4	PortLink Alarm	THU SEP 13 15:23:39 2012	Port alarm: entity id:1/1 port:1/1 state:Link up
3	Output rate	THU SEP 13 15:22:58 2012	Output alarm: entity id:2 state:Normal
2	PortLink Alarm	THU SEP 13 15:22:55 2012	Port alarm: entity id:1/2 port:1/2 state:Link down
1	PowerAlarm	THU SEP 13 15:21:49 2012	Power alarm: entity id:2 state:Power down
0	Output rate	THU SEP 13 15:21:28 2012	Output alarm: entity id:2 state:Alarm

Figure 153 Running Log Query

Performance log

Portfolio: {Index, LogType, Time, Description}

Function: Display the current running log.

6.27 Unicast Address Configuration and Query

6.27.1 Overview

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

A MAC address can be either static or dynamic.

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

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

The switch supports a maximum of 256 static unicast entries.

6.27.2 Web Configuration

1. Add a static MAC address entry, as shown in the following figure.

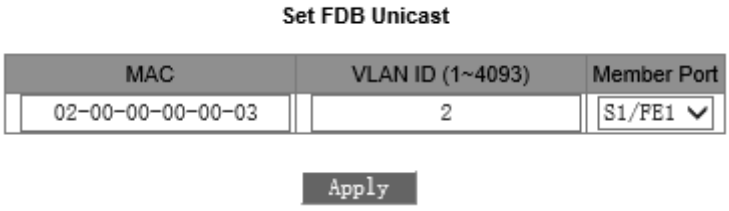


Figure 154 Adding a Static FDB Unicast Entry

MAC

Format: HHHHHHHHHHHH (H is a hexadecimal number.)

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

VLAN ID

Options: all created VLAN IDs

Member Port

Options: all switch ports

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

2. View the static unicast address list, as shown in the following figure.

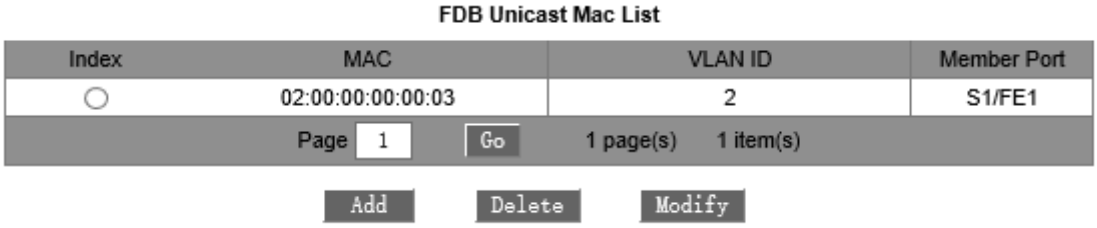


Figure 155 Viewing Static FDB Table

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

3. View the dynamic unicast address list, as shown in the following figure.

Dynamic Unicast Mac List

Index	MAC	VLAN ID	Member Port
1	ac:16:2d:03:a7:22	1	S1/FE2
2	70:71:bc:95:cc:22	1	S1/FE2
3	d0:67:e5:29:82:6e	1	S1/FE2
4	d4:be:d9:b9:47:ce	1	S1/FE2
5	c8:9c:dc:57:3e:96	1	S1/FE2
6	00:00:00:98:00:54	1	S1/FE2
7	40:16:9f:f0:b0:0e	1	S1/FE2
8	d0:67:e5:19:71:e2	1	S1/FE2
9	80:c1:6e:e0:5b:9a	1	S1/FE2
10	d0:27:88:70:5b:cd	1	S1/FE2
11	d4:be:d9:b9:46:fb	1	S1/FE2
12	d4:be:d9:b9:46:bb	1	S1/FE2
13	44:87:fc:40:02:be	1	S1/FE2
14	c8:3a:35:d3:cc:2a	1	S1/FE2
15	d0:27:88:45:ff:25	1	S1/FE2
16	00:1e:cd:17:83:6d	1	S1/FE2

Clear

Figure 156 Dynamic Unicast FDB Table

6.28 IEC61850

6.28.1 Introduce

At present, the switch is made transparent by the substation function main body in the substation network. Monitoring requires tools outside of IEC61850 (protocols) like EMS, WEB, CLI, OPC etc. Lead to knowledge points, configuration points scattered, not unified, inconvenient.

To solve these problems, building model according to the IEC61850 statute, and the switch is incorporated into the intelligent electronics device (IED, intelligent electronic device) as a substation automation system (IEC61850). Unified automatic monitoring view of substation to facilitate user integrated management plan planning, save construction cost and maintenance cost.

6.28.2 Web page configuration

1、Enable IEC 61850 function

Whether enable IEC 61850 can be configured in the IEC61850 configuration page, as shown in Figure 157;

Figure 157 IEC61850 configuration

IEC 61850 function

Configuration option: Enable/disable

Default configuration: Disable

Function: Whether enable IEC 61850.

2、Download IEC 61850 file

The file type, file name, IP address of FTP server, user name, password can be configured in the download IEC 61850 file page, as shown in Figure 158;

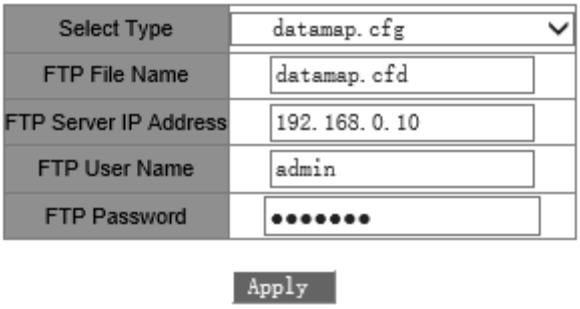


Figure 158 Download IEC 61850 file

File type selection

Configuration option: Mapping files / Initial files / OSI configuration files / Modeling files

Function: All four types of files are downloaded from the server to the device, then device can connect to the IEDScout software.

FTP server IP address

Configuration format: A.B.C.D

Function: Configure FTP server IP address.

File name

Configuration range: 1~20 character

Function: Configure the file name saved in the server.

User name

Configuration range: 1~20 character

Function: Configure FTP user name.

Password

Configuration range: 1~20 character

Function: Configure FTP password.

6.29 DHCP

With the continuous expansion of network scale and the growing of network complexity, under the conditions of the frequent movement of computers (such as laptops or wireless network) and the computers outnumbering the allocable IP addresses, the BOOTP protocol that is specially for the static host configuration has become increasingly unable to meet

actual needs. For fast access and exit network and improving the utilization ratio of IP address resources, we do need to develop an automatic mechanism based on BOOTP to assign IP addresses. DHCP (Dynamic Host Configuration Protocol) was introduced to solve these problems.

DHCP employs a client-server communication model. The client sends a configuration request to the server, and then the server replies configuration parameters such as an IP address to the client, achieving the dynamic configuration of IP addresses. The structure of a DHCP typical application is shown in Figure 159.

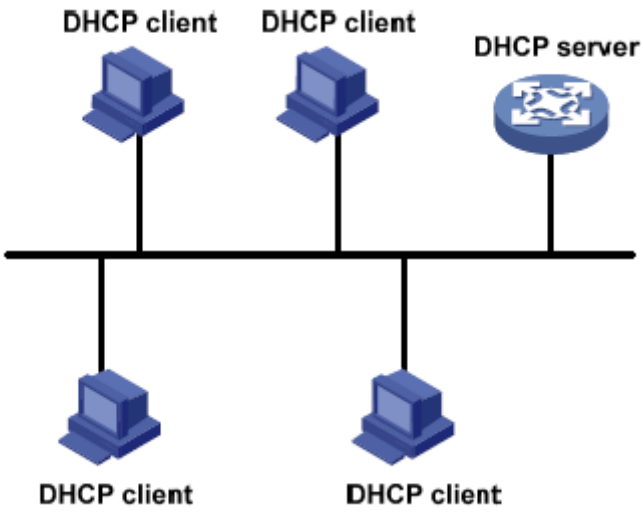


Figure 159 DHCP Typical Application

Caution:

In the process of dynamic obtainment of IP addresses, the messages are transmitted in the way of broadcast, so it is required that the DHCP client and the DHCP server are in a same segment. If they are in the different segments, the client can communicate with the server via a DHCP relay to get IP addresses and other configuration parameters. This series switches do not support DHCP relay, so the client and the server must be in a same segment.

DHCP supports two types of IP address allocation mechanisms.

Static allocation: the network administrator statically binds fixed IP addresses to few specific clients such as a WWW server and sends the binding IP addresses to clients by DHCP. This allocation mechanism contains port IP address binding and MAC address binding.

Dynamic allocation: DHCP server dynamically allocates an IP address to a client. This

allocation mechanism can allocate a permanent IP address or an IP address with a limited lease period to a client. When the lease expires, the client needs to reapply an IP address. The network administrator can choose a DHCP allocation mechanism for each client.

6.29.1 DHCP Server Configuration

6.29.1.1 Introduce

DHCP server is a provider of DHCP services. It uses DHCP messages to communicate with DHCP client to allocate a suitable IP address to the client and assign other network parameters to the client as required. In the following conditions, the DHCP server generally is used to allocate IP addresses.

- Large network scale. The workload of manual configuration is heavy and it is hard to manage the entire network.
- The hosts outnumber the assignable IP addresses, and it is unable to allocate a fixed IP address to each host.
- Only a few hosts in the network need fixed IP addresses.

6.29.1.2 DHCP Address Pool

The DHCP server selects an IP address from an address pool and allocates it together with other parameters to the client. The IP address allocation sequence is as follows:

1. The IP address statically bound to the client MAC address or the port ID connecting to the server.
2. The IP address that is recorded in the DHCP server that it was ever allocated to the client.
3. The IP address that is specified in the request message sent from the client.
4. The first allocable IP address found in an address pool.
5. If there is no available IP address, check the IP address whose lease expires and that had conflicts in order. If found, allocate the IP address. If not, no process.

6.29.1.3 Web Configuration

1. Enable DHCP server, as shown in Figure 160;

Figure 160 DHCP Server State

DHCP server status

Options: Enable/Disable

Default: Disable

Function: select the current switch to the DHCP server to allocate an IP address to a client or not. If a VLAN ID is selected during enabling, the DHCP server allocates an IP address to only the client sending a request in this VLAN. If all VLANs are selected, the DHCP server allocates IP addresses to all clients sending a request.

Explanation: During VLAN ID selection, you can select only one VLAN ID.

2. Select the DHCP server mode, as shown in Figure 161.

Figure 161 DHCP Server Mode

DHCP server mode

Options: Common-Mode/Port-Mode

Default: Port-Mode

Explanation: Common mode contains dynamic IP address allocation and static MAC address binding. Port mode means the port desired IP setting.

3. Port-Mode configuration

When select Port-mode in the DHCP server mode, allocate static binding IP addresses to ports, as shown in Figure 162.

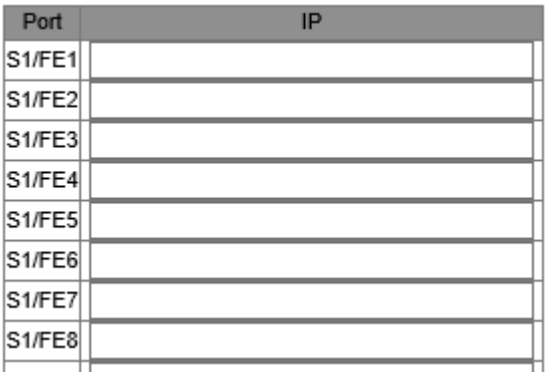


Figure 162 Port Desired IP Setting

Port desired IP setting is to statically configure an IP address to a port. When a port receives a request message from a client, the IP address bound to the port will be allocated to the client. This IP allocation mode has the highest priority and the lease period is 1000 days 23 hours and 59 minutes.

Caution:

The IP address bound to the port and the DHCP server must be in same segment.

When port mode is adopted for IP assignment, you need to configure the DHCP server, as shown in Figure 163.

Configuration Options		Configuration Information
DHCP server status		○ Enable All Vlans: ☑ Vlan-id: ◉ Disable
DHCP server mode		◉ Common-Mode ○ Port-Mode
DHCP server IP-pool name		pool
The domain name for the IP-Pool		domain
The starting IP address of the IP-Pool		
The ending IP address of the IP-Pool		
The subnet mask of the network-address		255. 255. 255. 0
The default lease time of the IP address		Infinite: ☐ 0 Days 1 Hours 0 Minutes
The maximum lease time of the IP address		1 Days 0 Hours 0 Minutes
The routers on the IP-Pool's subnet	IP Address 1:	
	IP Address 2:	
The dns-server for the IP-Pool's subnet	DNS1:	
	DNS2:	
Run		Run

Apply

Figure 163 Port Mode Server Configuration

DHCP server IP-pool name

Range: 1~15 characters

Function: configure the name of the IP address pool.

The domain name for the IP-Pool

Range: 1~60 characters

Function: configure the domain name of the IP address pool.

The subnet mask of the network-address

The subnet mask is a number with a length of 32 bits and consists of a string of 1 and a

string of 0. "1" corresponds to network number fields and subnet number fields, while "0" corresponds to host number fields. It is generally configured to 255.255.255.0.

Caution:

- After configuration, click <Run> button to allocate correct IP addresses to clients.
- After modifying configuration, click <Run> button again to allocate correct IP addresses to clients.

4. Common-Mode Configuration

When DHCP server mode is set to Common-Mode, it contains static MAC address binding and dynamic IP address allocation. In static MAC address binding, the system preferentially allocates the IP address bound to the MAC address; otherwise, dynamically allocate IP addresses in the address pool. The static MAC address binding configuration is shown in Figure 164 and Figure 165; dynamic IP address allocation configuration is shown in Figure 166.

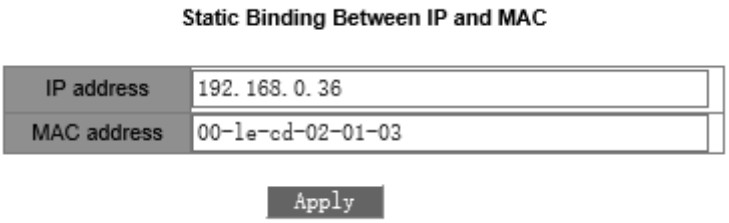


Figure 164 Static MAC Address Binding

Static MAC address binding is to bind the client MAC address to IP address. When the server receives an IP address request message whose source MAC address is the MAC address set here, the IP address bound to this MAC address will be allocated to the client. This kind of IP allocation mode requires server configuration as shown in Figure 166.

After configuration, the list of "Static Binding between IP and MAC" shows the statically-configured binding relationships of MAC addresses and IP addresses. Tick in the box of Index to delete the corresponding binding entry.

The list of Static Binding Between IP and MAC

Index	IP Address	MAC Address
☐	192.168.0.26	02-00-AA-BB-CC-05
☐	192.168.0.36	00-1E-CD-02-01-03

Delete

Figure 165 Static MAC Address Binding List

Configuration Options		Configuration Information
DHCP server status		○ Enable All Vlans: ☑ Vlan-id: ◉ Disable
DHCP server mode		◉ Common-Mode ○ Port-Mode
DHCP server IP-pool name		pool
The domain name for the IP-Pool		domain
The starting IP address of the IP-Pool		192. 168. 0. 100
The ending IP address of the IP-Pool		192. 168. 0. 200
The subnet mask of the network-address		255. 255. 255. 0
The default lease time of the IP address		Infinite: ☐ 0 Days 1 Hours 0 Minutes
The maximum lease time of the IP address		1 Days 0 Hours 0 Minutes
The routers on the IP-Pool's subnet	IP Address 1:	
	IP Address 2:	
The dns-server for the IP-Pool's subnet	DNS1:	
	DNS2:	
Run		Run

Apply

Figure 166 Common Mode Server Configuration

DHCP server IP-pool name

Range: 1-15 characters

Function: configure the name of the IP address pool

The domain name for the IP-Pool

Range: 1-60 characters

Function: configure the domain name of the IP address pool

The starting IP address of the IP-Pool/The ending IP address of the IP-Pool

Format: A.B.C.D (the starting IP address and the ending IP address must be in a same segment.

The subnet mask of the network-address

The subnet mask is a number with a length of 32 bits and consists of a string of 1 and a string of 0. "1" corresponds to network number fields and subnet number fields, while "0" corresponds to host number fields. It is generally configured to 255.255.255.0. In the dynamic address allocation, the range of the IP address pool need to be set and the address range is determined by the subnet mask.

The default lease time of the IP address

Range: 0 Days 0 Hours 1 Minutes – 1000 Days 23 Hours 59 Minutes/Infinite

Default: 0 Days 1 Hours 0 Minutes

Explanation: If the IP address request message sent from the client does not contain a valid lease time, the lease time of the IP address the server allocates to the client is the default value.

The maximum lease time of the IP address

Range: 0 Days 0 Hours 1 Minutes – 1000 Days 23 Hours 59 Minutes

Default: 1 Day 0 Hours 0 Minutes

Explanation: When the client sends an IP address request message to the server, the lease time of the message cannot be longer than the maximum lease time of the IP address. For different address pools, DHCP server can set different address lease time, but the addresses in the same DHCP address pool have the same lease time.

The routers on the IP-Pool's subnet

Explanation: when the DHCP client visits the host that is in the different segment, the data must be forwarded via gateways. When the DHCP server allocates IP addresses to clients, it can specify gateway addresses at the same time. DHCP address pool can configure max two gateway addresses.

The dns-server for the IP-Pool's subnet

When visiting the network host via a domain name, the domain name needs to be resolved to an IP address, which is realized by DNS. In order to let a DHCP client visit a network host via a domain name, when the DHCP server allocates IP addresses to clients, it can specify IP addresses of domain name servers at the same time. DHCP address pool can configure max two DNS addresses.

Caution:

- Configure the correct subnet based on the client's network topology.
- After configuration, click <Run> button to allocate correct IP addresses to clients.
- After modifying configuration, click <Run> button again to allocate correct IP addresses to clients.

6.29.1.4 Typical Configuration Example

As Figure 167 shows, switch A works as a DHCP server and switch B works as a DHCP client. The port 3 of Switch A connects with the port 4 of Switch B. The client sends out IP address request messages and the server can allocate an IP address to the client in three ways.

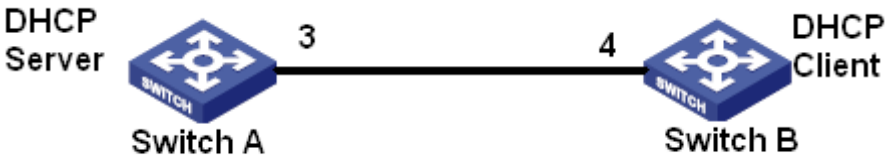


Figure 167 DHCP Typical Configuration example

Port IP binding

- Switch A configuration:

1. Enable DHCP server status, as shown in Figure 160.
2. Select Port-Mode in the DHCP server mode, as shown in Figure 161.
3. Set the "IP-pool name" to pool, set "the domain name for the IP- pool" to domain, set "the subnet mask" to 255.255.255.0, as shown in Figure 163.
4. Port 3 bind to the IP address of 192.168.0.6, as shown in Figure 162.
5. Click the <Run> button in the server configuration interface to run the server.

- Switch B configuration:

1. As DHCP Client, Switch B obtains automatically IP address.
2. The switch B obtains the IP address of 192.168.0.6 and the subnet mask of 255.255.255.0 from the DHCP server, as shown in Figure 168.

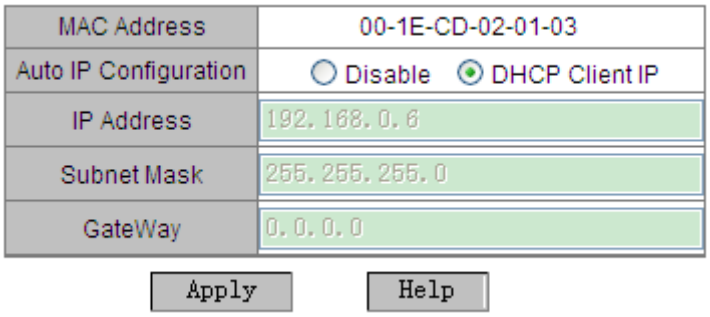


Figure 168 DHCP Client Obtain IP Address-1

Static MAC address binding method

➢ Switch A configuration:

1. Enable the DHCP server status, as shown in Figure 160.

2. Select Common-Mode in the DHCP server mode, as shown in Figure 161.

3. Set the “IP-pool name” to pool, set “the domain name for the IP- pool” to domain, set “the starting IP address of the IP-pool” to 192.168.0.3 and “the ending IP address of the IP-pool” to 192.168.0.201, set “the subnet mask” to 255.255.255.0 and the lease time uses the default value, as shown in Figure 166.

4. Bind the Switch B MAC address of 00-1E-CD-02-01-03 to the IP address of 192.168.0.36, as shown in Figure 164.

5. Click the <Run> button in the server configuration interface to run the server.

➢ Switch B configuration:

1. As DHCP Client, Switch B obtains automatically IP address..

2.The switch B obtains the IP address of 192.168.0.36 and the subnet mask of 255.255.255.0 from the DHCP server, as shown in Figure 169.

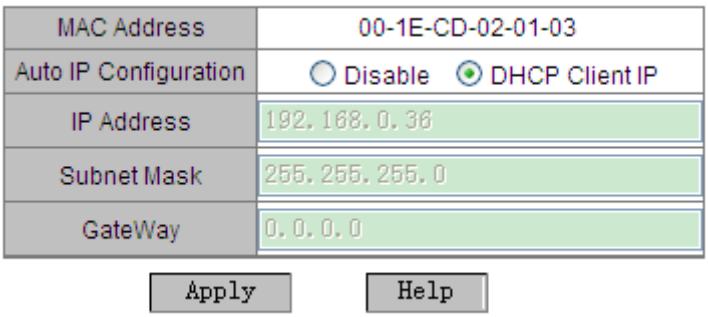


Figure 169 DHCP Client Obtain Address-2

Dynamic obtainment of IP address in address pool

➢ Switch A configuration:

1. Enable DHCP server status, as shown in Figure 160.

2. Select Common-Mode in the DHCP server mode, as shown in Figure 161.

3. Set the “IP-pool name” to pool, set “the domain name for the IP- pool” to domain, set “the starting IP address of the IP-pool” to 192.168.0.3 and “the ending IP address of the IP-pool” to 192.168.0.201, set “the subnet mask” to 255.255.255.0 and the lease time uses the default value, as shown in Figure 166.

4. Click the <Run> button in the server configuration screen to run the server.

➢ Switch B configuration：

1. As DHCP Client, Switch B obtains automatically IP address..

2. DHCP server searches the assignable IP addresses in the address pool in order and allocates the first found assignable IP address and other network parameters to Switch B. The subnet mask is 255.255.255.0, as shown Figure 170.

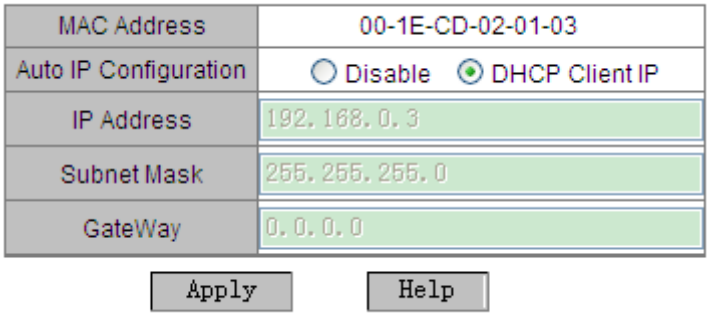


Figure 170 DHCP Client Obtain IP Address-3

6.29.2 DHCP Snooping

6.29.2.1 Introduce

DHCP Snooping is a monitoring function of DHCP services on layer 2 and is a security feature of DHCP, ensuring the security of the client further. The DHCP Snooping security mechanism can control that only the trusted port can forward the request message of the DHCP client to the legal server, meanwhile, it can control the source of the response message of the DHCP server, ensuring the client to obtain an IP address from the valid server and preventing the fake or invalid DHCP server from allocating IP addresses or other

configuration parameters to other hosts.

DHCP Snooping security mechanism divides port to trusted port and untrusted port.

Trusted port: it is the port that connects with the valid DHCP server directly or indirectly. Trusted port normally forwards the request messages of DHCP clients and the response messages of DHCP servers to guarantee that DHCP clients can obtain valid IP addresses.

Untrusted port: it is the port that connects with the invalid DHCP server. Untrusted port does not forward the request messages of DHCP clients and the response messages of DHCP servers to prevent DHCP clients from obtaining invalid IP addresses.

6.29.2.2 Web Configuration

1. Enable DHCP Snooping function, as shown in Figure 171.

Figure 171 DHCP Snooping State

DHCP Snooping Status

Options: Enable/Disable

Default: Disable

Function: Enable/Disable switch DHCP Snooping function.

Caution:

The switch working as DHCP server and client cannot enable DHCP Snooping function.

2. Configure trusted ports, as shown in Figure 172.

Port	Protocol Status
S1/FE1	Trust Untrust
S1/FE2	Trust Untrust
S1/FE3	Trust Untrust
S1/FE4	Trust Untrust
S1/FE5	Trust Untrust
S1/FE6	Trust Untrust
S1/FE7	Trust Untrust
S1/FE8	Trust Untrust

Figure 172 Trust Port Configuration

Protocol Status

Options: Trust/Untrust

Default: Untrust

Function: set the port to a trusted port or an untrusted port. The ports that connect with valid DHCP servers directly or indirectly are trusted ports.

Caution:

The trusted port configuration and Port Trunk is mutually exclusive. The port joining in a trunk group cannot be set to a trusted port. The trusted port cannot join in a trunk group.

6.29.2.3 Typical Configuration Example

As Figure 173 shows, the DHCP client requests an IP address from the DHCP server. An unauthorized DHCP server exists in the network. Set port 1 to a trusted port by DHCP Snooping to forward the request message of the DHCP client to the DHCP server and forward the response message of the DHCP server to the DHCP client. Set port 3 to an untrusted port that cannot forward the request message of the DHCP client and the response message of the unauthorized DHCP server, ensuring that the client can obtain a valid IP address from the valid DHCP server.

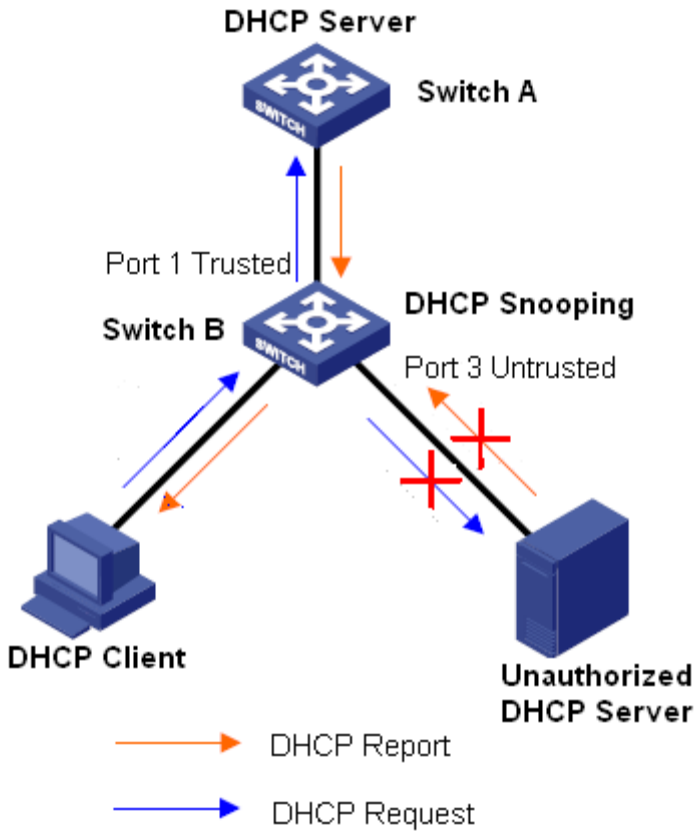


Figure 173 DHCP Snooping Typical Configuration Example

Switch B configuration:

➢ Enable DHCP Snooping function, as shown in Figure 171.

➢ Set the port 1 of switch B to a trusted port and set the port 3 to an untrusted port, as shown in Figure 172.

6.29.3 Option 82 Configuration

Option 82 (Relay Agent Information Entry) records the client information. When the Option 82 supported DHCP Snooping receives the request message from the DHCP client, it add the corresponding Option 82 field into the messages and then forward the message to the DHCP server. The server supporting Option 82 can flexibly allocate addresses according to the Option 82 message.

Once Option 82 is enabled, the Option 82 field needs to be added into the message. The Option 82 field of this series switches contains two sub-options: sub-option 1 (Circuit ID) and sub-option 2 (Remote ID). The formats of two sub-options are shown below:

➢ Sub-option 1 contains the VLAN ID and number of the port that receives the request

message from the DHCP client, as shown in Table 10.

Table 10 Sub-option 1 Field Format

Sub-option type (0x01)	Length (0x04)	VLAN ID	Port number
One byte	One byte	Two bytes	Two bytes

Sub-option type: the type of the sub-option 1 is 1.

Length: the number of bytes that VLAN ID and Port number occupy.

VLAN ID: On DHCP Snooping device, the VLAN ID of the port that receives the request message from the DHCP client.

Port number: On DHCP Snooping device, the number of the port that receives the request message from the DHCP client.

- The content of Sub-option 2 is the MAC address of the DHCP Snooping device that receives the request message from the DHCP client, as shown in Table 11, or the character string configured by users, as shown in Table 12.

Table 11 Sub-option 2 Field Format-MAC Address

Sub-option type (0x02)	Length (0x06)	MAC 地址
One byte	One byte	6 bytes

Table 12 Sub-option2 Field Format-Character String

Sub-option type (0x02)	Length (0x10)	Character string
One byte	One byte	16 bytes

Sub-option type: the type of the sub-option 2 is 2

Length: the number of bytes that sub-option2 content occupies. MAC address occupies 6 bytes and character string occupies 16 bytes.

MAC address: the content of sub-option2 is the MAC address of the DHCP Snooping device that receives the request message from the DHCP client.

Character string: the content of Sub-option2 is 1~16 characters set by users. (The character is indicated by ASCII code and each character occupies one byte). The length is fixed to 16. If the configured length of the character string is less than 16 bytes, fill in the missing

characters by 0.

6.29.3.1 DHCP Snooping Supports Option 82 Function

1. Introduction

If DHCP Snooping device supports Option 82 function, when the DHCP Snooping receives a DHCP request message, it will process the request message according to whether the message contains Option 82 and the client policy, and then forward the processed message to the DHCP server. The specific processing method is shown in Table 13.

Table 13 Processing Modes for Request Messages (DHCP Snooping)

Receive the request message from the DHCP client	**Configuration policy**	**DHCP Snooping device processing the request message**
The request message contains Option 82	Drop	Drop the request message
	Keep	Keep the message format unchanged and forward the message
	Replace	Replace the Option 82 field in the message with the Option 82 field of the Snooping device and forward the new message
The request message does not contain Option 82	Drop/Keep/Replace	Add the Option 82 field of the Snooping device into the message and forward it

When the DHCP Snooping device receives the response message from the DHCP server, if the message contains Option 82 field, remove the Option 82 field and forward the message to the client; if the message does not contain Option 82 field, process the response message according to the server policy, as shown in Table 14.

Table 14 Processing Modes for Response Messages (DHCP Snooping)

Receive the response message from the DHCP server	**Configuration policy**	**DHCP Snooping device processing the response message**
The response message contains Option 82 field	Drop/Keep	Remove the Option 82 field in the response message and forward the message

The response message does not contains Option 82 field	Drop	Drop the response message
	Keep	Keep the message format unchanged and forward the message

2. Web Configuration

DHCP Snooping Option 82 configuration is shown in Figure 174.

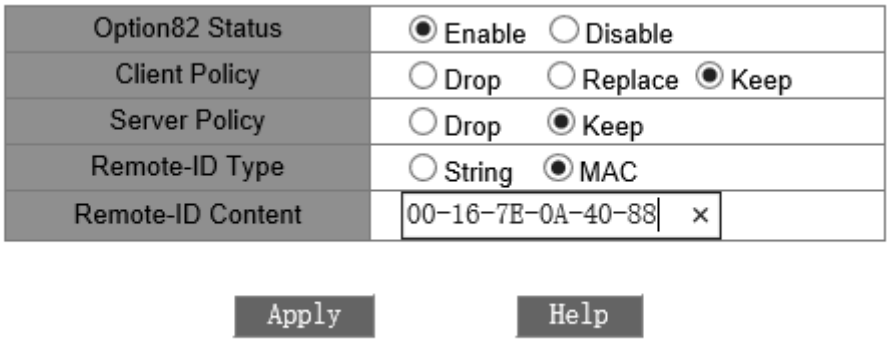


Figure 174 DHCP Snooping Option82 Configuration

Option82 Status

Options: Enable/Disable

Default: Disable

Function: Enable/Disable Option82 function on DHCP Snooping device.

Client Policy

Options: Drop/Replace/Keep

Default: Keep

Function: Configure client policy. The DHCP Snooping device processes the request message sent from the Client according to Client Policy, as shown in Table 13.

Server Policy

Options: Drop/Keep

Default: Keep

Function: Configure server policy. The DHCP Snooping device processes the response message sent from the server according to Server Policy, as shown in Table 14.

Remote-ID Type

Options: String/MAC

Default: MAC

Function: configure the content of Sub-option2.

Explanation: MAC means that the content of sub-option2 is the MAC address of the DHCP Snooping device that receives the request message from the client. String means the content of the sub-option2 is the character string defined by user.

Remote-ID Content

Options: MAC address/1~16 characters

Default: MAC address

Explanation: when the remote ID type is set to MAC, the Remote ID content is forced to the MAC address of the current Snooping device. When the remote ID type is set to String, the Remote ID content is configured by user. The configuration content is 1~16 characters (Each character occupies one byte)

6.29.3.2 DHCP Server Support Option 82 Function

1. Introduction

If the DHCP Server is set to support Option82 function, when the DHCP server receives the DHCP request message, it will provides different address allocation solution according to whether the message contains Option82 field and server configuration.

The DHCP server includes the following variables:

Class: each DHCP server can configure 32 classes. Each class contains three variables: start & end IP address and match always and relay information option.

Match the variable of relay information option to the Option 82 field. When the variable value is same as the Option82 field, it is assumed that they are matched, or else they are unmatched.

If match always is enabled, it is assumed that the value of relay information option always matches to the Option82 filed without the need of judgment. If the match always is disabled, it is needed to judge whether the value of relay information option matches to the Option82 filed.

According the configuration of the above variables, the server processes the request message as shown in .

Table 15.

Table 15 Processing Modes for Request Messages (Option82-enabled DHCP Server)

<table>
<tr><th>Receive the request message from the DHCP client</th><th colspan="2">Configuration Policy</th><th>DHCP server processing the request message</th></tr>
<tr><td rowspan="3">The request message contains Option82 field</td><td colspan="2">Enable match always</td><td>Add Option82 field into the response message, and allocate IP address and other parameters to the client</td></tr>
<tr><td rowspan="2">Disable Match-always</td><td>Configure the value of relay information option</td><td>➢ The value of relay information option is matched to the Option82 field: Add Option82 field into the response message, and allocate IP address and other parameters to the client
➢ The value of relay information option is not matched to the Option82 field: the server does not allocate IP address to the client</td></tr>
<tr><td>Do not configure the value of relay information option</td><td>The server does not allocate IP address to the client</td></tr>
<tr><td rowspan="2">The request message does not contain Option82 field</td><td colspan="2">Enable Match-always</td><td>The response message does not contain Option82 field, allocate IP address and other parameters to the client</td></tr>
<tr><td colspan="2">Disable Match-always</td><td>The server does not allocate IP address to the client</td></tr>
</table>

If the DHCP server does not support Option82 function, when the DHCP server receives the message that contains Option82 field, the response message does not contain Option82 field, and the server can allocate IP address and other parameters to the client. Under this

condition, the server processes the request message as shown in Table 16.

Table 16 Processing Modes for Request Messages (Option82-disabled DHCP Server)

Receive the request message from the DHCP client	**DHCP server processing the request message**
The request message contains Option82 field	The response message does not contain Option82 field, and the server allocate IP address and other parameter to the client
The request message does not contain Option82 field	

2 Web Configuration

- Enable Option82 function on DHCP server device, as shown in Figure 175.

Figure 175 DHCP Server Option82 Status

DHCP Server Option82 Enable

Options: Enable/Disable

Default: Disable

Function: Enable or disable the Option82 function on DHCP server device.

- Configure DHCP server Option82, as show in Figure 176.

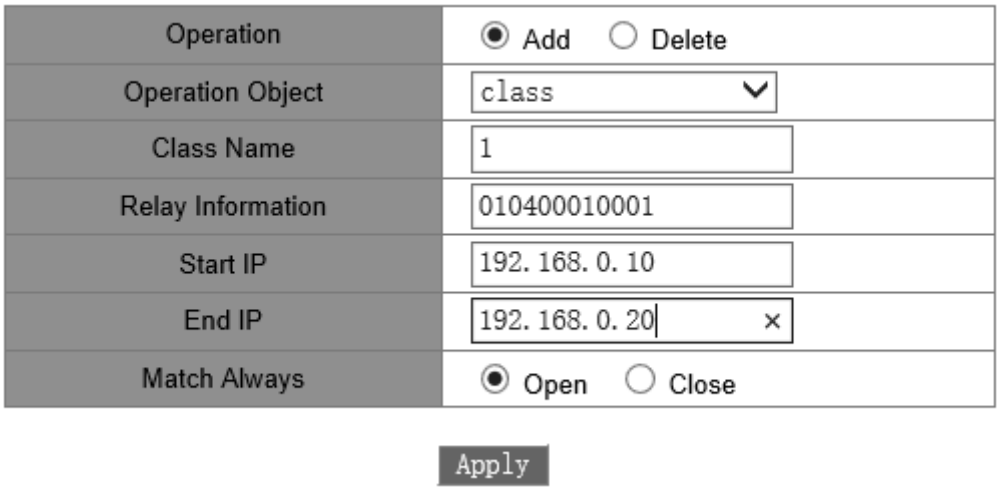


Figure 176 DHCP Server Option82 Configuration

Operation

Options: Add/Delete

Default: Add

Function: Add or delete a specified class.

Operation Object

Options: class/Relay Information/start & end ip/Match Always

Default: class

Description: When adding a class, you can configure the following parameters. When deleting a class, you only need to designate the class name. You can add multiple relay information to a designated class already created. Start & end IP/ match always is added to modify configuration of related parameters in a designated class already created. When deleting relay information, you can delete designated relay information in the current class.

Class Name

Range: 1~15 characters

Function: Configure name of the class.

Relay Information

Range: 12~60 hexadecimal number

Function: Configure relay information of the class.

Start IP/ End IP

Format: A.B.C.D

Function: Configure start/end IP address of the class. This range shall be selected from the address pool of the DHCP server.

Match Always

Options: Open/Close

Function: Open or close the match always option. If match always is enabled, it is assumed that the value of relay information option always matches to the Option82 filed without the need of judgment. If the match always is disabled, it is needed to judge whether the value of relay information option matches to the Option82 filed.

Caution:

During creation of multiple classes, the DHCP server allocates an IP address to a client based on the class information with matched relay information. If multiple classes have the matched relay information, the DHCP server allocates an IP address to a client based on the information of the class created firstly.

➢ Query DHCP server Option82 class, as shown in Figure 177.

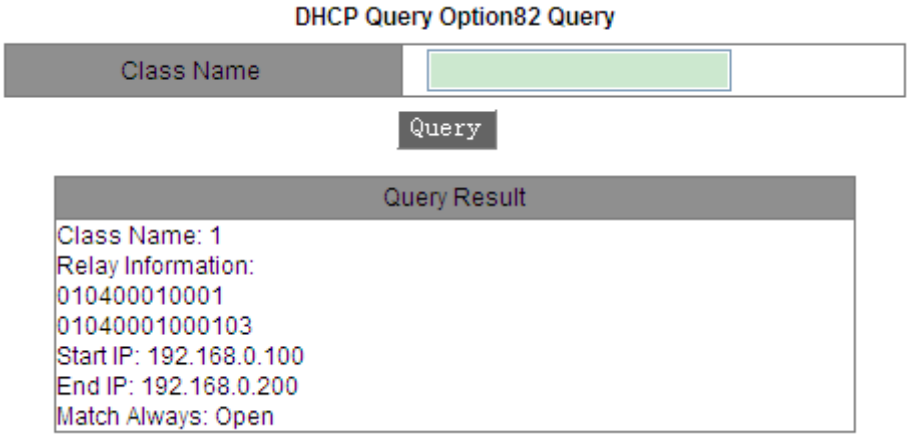


Figure 177 DHCP Server Option82 Class Query

6.30 IEEE802.1x

6.30.1 Introduce

IEEE802 LAN/WAN committee proposed the 802.1x protocol to solve the problem of wireless LAN network security. 802.1x protocol is applied in Ethernet as a common access control mechanism of LAN port, mainly solving the authentication and security problems in Ethernet. The 802.1x protocol is a port based network access control protocol. "Port based Network Access Control" means the authentication and control of the accessed device at the level of the port of the LAN access device. User devices connected to the port can access to resources in the LAN if authentication pass, and if not, can't access to resources in the LAN. The system with 802.1x is a typical client/server architecture, user authentication and authorization for port - based access control can only be completed with the following three elements:

Client: it is generally the user terminal device. When the user needs the Internet, activate the client program, enter the necessary user name and password, and the client program will send the connection request;

Device side: it is the authentication switch in the Ethernet system, the main role is to complete the upload and download of the user authentication information, and open or close the port according to the authentication results;

Authentication server: The entity that provides the authentication service to the device side determines whether the user has the permission to use the network service provided by the network system through verifying the identity (username and password) sent by the client, and send the open or keep close port status to the device side according to the authentication results.

6.30.2 Web page configuration

1、Enable global IEEE802.1x protocol

Configure whether enable IEEE802.1x in the IEEE802.1x interface, as shown in Figure 178;

Figure 178 IEEE802.1x protocol enable

IEEE802.1x status

Configuration option: Enable/disable

Default configuration: Disable

Function: Whether enable global IEEE802.1x security.

2、IEEE802.1x configuration method

IEEE802.1x configuration method, as shown in Figure 179:

Figure 179 IEEE802.1x configuration method

IEEE802.1x method

Configuration option: Local Mode / Remote Mode

Default configuration: Local mode

Function: Select method for IEEE802.1x to use

Authentication server timeout

Configuration range: 1~30s

Function: Configure the authentication server timeout

3、Configure the ports that enable the IEEE802.1x protocol, as shown in Figure 180;

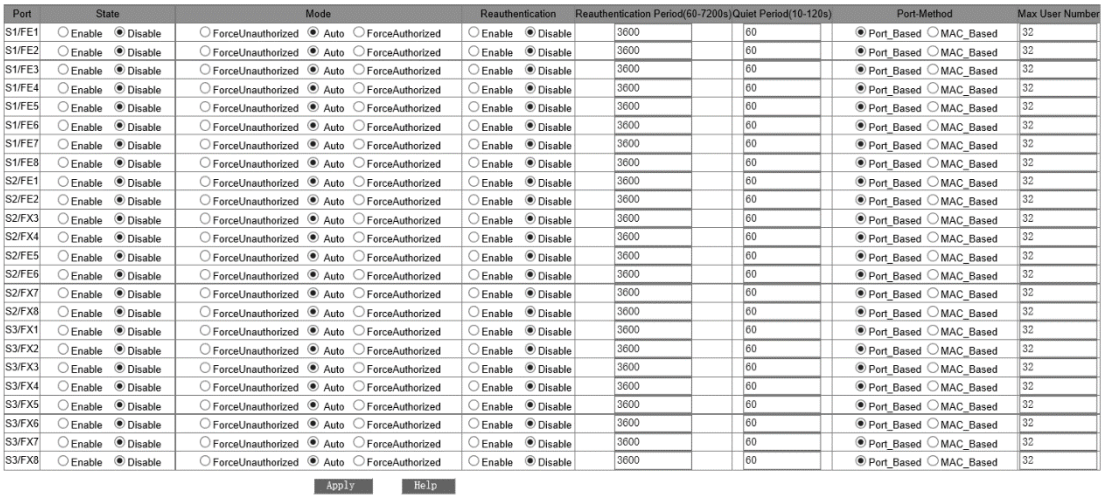


Figure 180 IEEE802.1x protocol port configuration

Port

Configuration option: All ports in switch

IEEE802.1x status

Configuration option: Enable/disable

Default configuration: Disable

Function: Whether enable the IEEE802.1X protocol of port.

Description: Port communication depends on the ieee802.1x authentication mode after enabling.

Authentication mode

Configuration option: Force unauthorized / Autorecognition / force authorized

Default configuration: Autorecognition

Function: Select authentication mode of port.

Description: Forced unauthorized mode means that the port is always unauthorized, does not allow user authentication, and the device side does not provide authentication services to clients accessed through the port. The automatic recognition mode means that the initial status of the port is unauthenticated, which does not allow users to access the network resources. If the authentication passes, the port switches to the authentication status to allow the user to access the network resources; If authentication fails, the port switches to an unauthenticated status, do not allow users to access the network resources. Forced authorization mode means that the port is always authorized, allow users to access network resources without authentication.

Reauthentication

Configuration option: Enable/disable

Default configuration: Disable

Function: Whether periodic reauthentication is required when the authentication is successful.

Reauthentication timer

Configuration range: 60~7200s

Default configuration: 3600s

Function: Time interval for reauthentication after authentication is successful.

Silence timer

Configuration range: 10~120s

Default configuration: 60s

Function: Enter into the silent cycle after the authentication fails, the server will accept the authentication request after silent cycle; the server does not respond to the authentication request of the client during the silent cycle.

Interface access control mode

Configuration option: Port based / MAC based

Default configuration: Port based

Function: Configure the access authentication mode of IEEE802.1x port.

Description: The access user is controlled based on the mac address, that is, all access users under the port require separate authentication, and when a user goes offline, only the user cannot use the network. The access user is controlled based on the port, that is, as long as the first user under the port is successfully authenticated, the port can be opened, and other access users can use the network resources without authentication, but when the first user goes off the line, the port is closed and other users will be refused to use the network.

Maximum Number of Users

Configuration range: 1~32

Default configuration: 32

Function: Configure the maximum number of access users to the ports that enable ieee802.1x.

Description: This configuration is only valid for ports based on MAC access control mode and invalid for ports based on port access control mode.

4、IEEE802.1x user configuration

IEEE802.1x user configuration interface, the corresponding user name and user password for each port can be configured, as shown in Figure 181;

Port	UserName	UserPassword
S1/FE1		
S1/FE2		
S1/FE3		
S1/FE4		
S1/FE5		
S1/FE6		
S1/FE7		
S1/FE8		
S2/FE1		
S2/FE2		
S2/FX3		
S2/FX4		
S2/FE5		
S2/FE6		
S2/FX7		
S2/FX8		
S3/FX1		
S3/FX2		
S3/FX3		
S3/FX4		
S3/FX5		
S3/FX6		
S3/FX7		
S3/FX8		

Figure 181 IEEE802.1x user information configuration

User name

Configuration range: 1~16 character

Function: Configure IEEE802.1x user name.

Password

Configuration range: 1~16 character

Function: Configure IEEE802.1x password.

6.30.3 Typical configuration example

As shown in Figure 182, client connect to port 1 of switch, enable IEEE802.1X protocol of port 1 and use Auto mode (Automatic authentication), local authentication user name and password are ccc, remote authentication user name and password are ddd, other

configuration keep default;

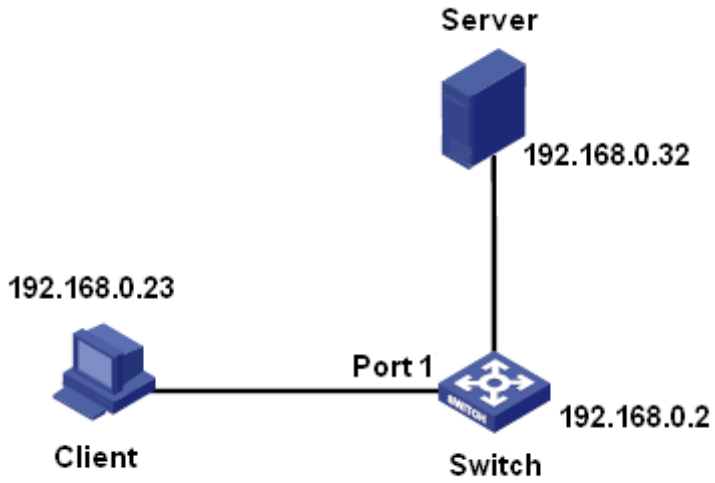


Figure 182 IEEE802.1x configuration example

➢Local authentication configuration:

➢Global enable IEEE802.1x protocol, as shown in figure 176;

➢Select local authentication for Dot1x authentication mode, as shown in figure 177;

➢Configure user name and password as ccc,

➢Enable IEEE802.1x protocol of port 1, select Auto authentication mode, as shown in figure 178;

➢Install and run the 802.1x authentication client software, enter the username and password ccc for authentication, and successfully access the switch after authentication is successful.

6.31 Radius

6.31.1 Introduce

RADIUS (Remote Authentication Dial-In User Service) is a distributed information interaction protocol that defines the UDP - based radius frame format and its message transfer mechanism that can protect the network from unauthorized access and is often used in various network environments that require both higher security and allow remote user to access.

The protocol uses C/S mode for communication between NAS (Network Access Server) and RADIUS server, the RADIUS client runs on the NAS, and the user information is

centrally managed on the radius server. The NAS is the server side for the user and the client side for the RADIUS server, and the structure schematic diagram is shown in Figure 183;

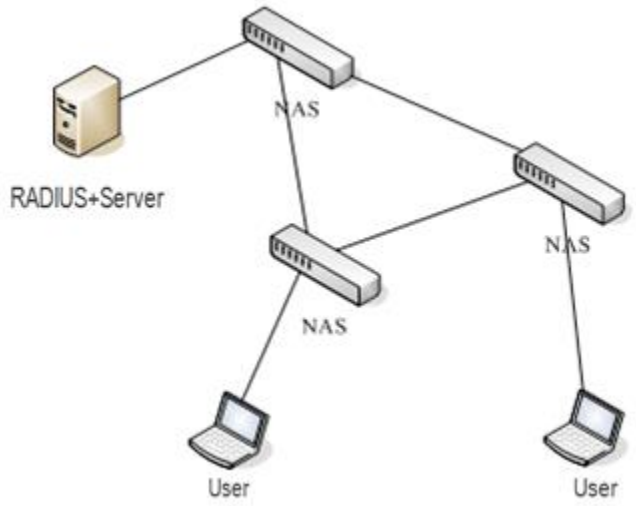


Figure 183 RADIUS structure schematic diagram

This protocol performs login authentication to end users who need to login to the device for operation. The device, as the client of the RADIUS, sends the authentication information sent by the user to the RADIUS server for authentication, and allows/ refuses the user to login to the device according to the authentication result of the RADIUS server.

6.31.2 Web page configuration

1、Configure RADIUS authentication parameters

The Radius authentication status, request times and timeout can be configured in the RAIDUS configuration interface, as shown in Figure 184;

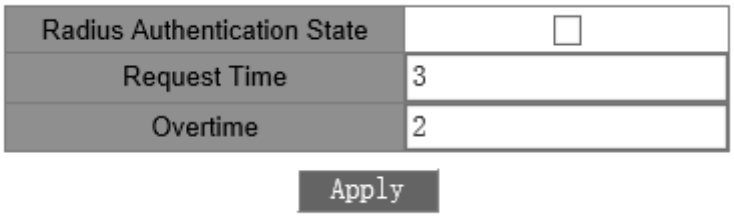


Figure 184 RADIUS authentication parameters configuration

Request times

Configuration range: 1~3

Default configuration: 3

Function: Configure the resending number of the RAIUDS request message timeout, and the authentication fails if the cumulative resending number exceeds the configuration value, and the RADIUS server still no response.

Timeout time

Configuration range: 1~3s

Default configuration: 2s

Function: Configure RADIUS server response timeout time; After the device sends the RADIUS request message, resend the RADIUS request message if no response from the RADIUS server.

2、RADIUS server configuration, as shown in Figure 185;

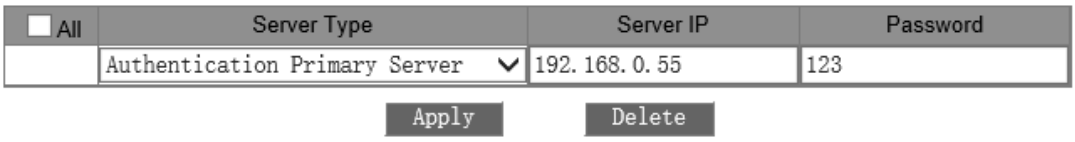


Figure 185 RADIUS server configuration

Server type

Configuration option: authentication master server / authentication slave server

Function: Configure RADIUS authentication master/slave server. When the master server is unreachable, the switch will authenticate from the slave server.

Server IP

Configuration format: A.B.C.D

Function: Configure RADIUS server IP address.

Password

Configuration range: 1~32 character

Function: Configure RADIUS server password.

6.31.3 Typical configuration example

As shown in Figure 186, enable IEEE802.1X protocol to Switch port1, user requires authentication via the RADIUS server to open port 1 and login to switch. Server IP address is

192.168.0.23，Shared key when the switch interacts with the server message is aaaa .

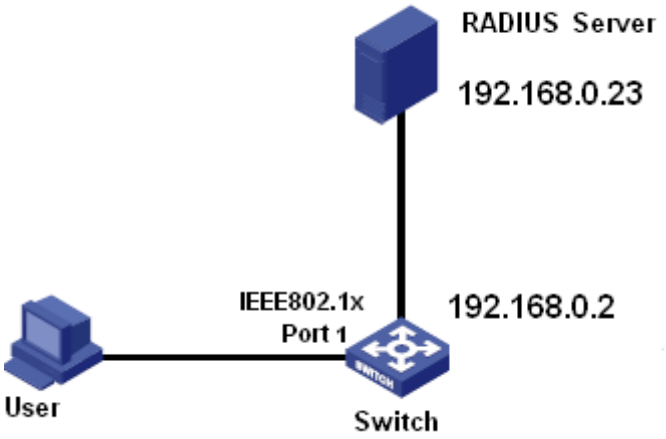


Figure 186 RADIUS authentication example

1、Configure authentication slave server IP address is 192.168.0.55, and password is aaaa，see the figure 183.

2、IEEE802.1x function configuration: global enable IEEE802.1x, enable IEEE802.1x of port 1, other configuration keep default, refer to“”section.

3、Select Radius authentication for Dot1x authentication method, see figure182;

4、Configure user name and password to ccc in the RADIUS Server, key is aaaa.

5、Install and run 802.1x authentication client software in the PC, enter the user name and password ccc, users can access the switch if passing authentication.

6.32 AAA

6.32.1 Introduce

AAA(Authentication、Authorization、Accounting) is a management mechanism of network security, which provides three security functions: authentication, authorization and accounting.

Authentication: Identify the remote access user and determine whether the visitor is a legitimate network user;

Authorization: Give different permissions to different users to limit the services that users can use;

Accounting: Record all operations in the user's network service, including the service

type, start time, data traffic, which is not only a accounting method, but also monitor the network security.

6.32.2 Realization

First, the authentication section provides the authentication to the user. The whole authentication is usually using the user input user name and password for permission audit, the authentication principle is that each user has an only permission obtainable standard. The AAA server checks the user's standard with each user in the database, passing the user authentication if met; if not, refuse the network connection.

Next, Users is also authorized permission to operate the corresponding task. For example, after logging on the system, the user may perform some commands to operate, at this moment the authorization process detects if the user has permission to perform these commands. In simple terms, the authorization process is a combination of force policies, including determining the type or quality of the activity, resources, or services the user is allowed. The authorization process takes place in the authentication context. Once the user is authenticated, they are also granted the permission accordingly. The last step is the account, which calculates the number of resources that users consume during the connection process. These resources include connection time or user traffic during the connection. The account process can be performed according to the connection process statistics log and user information, as well as authorization control, accounting, trend analysis, resource utilization, and capacity planning activities.

The network connection server interface currently cooperating with the AAA server is the TACACS+ protocol.

6.32.3 Web page configuration

1、sequence configuration of authentication method, as shown in Figure 187;

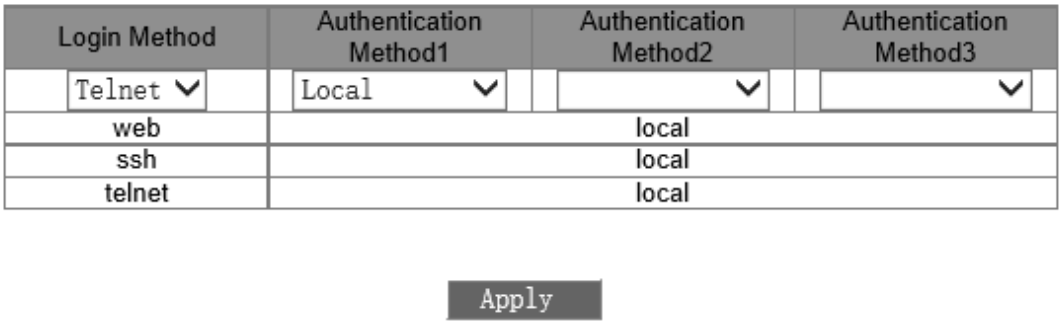


Figure 187 Configure authentication method

Login mode

Configuration option: Telnet/web/ssh

Default configuration: Telnet

Function: Select the login mode requiring authentication

Authentication method

Configuration option: local/tacacs-plus/radius

Default configuration: local

Function: Select login authentication method.

Description: local means local authentication, local authentication means use the username and user password created on the device to authenticate; tacacs-plus means tacacs-plus authentication, tacacs-plus authentication means use username and password configured on the tacacs-plus server to authenticate; Radius means radius authentication, radius authentication refer to 6.31Radius; One or more authentication methods can be selected for each login mode (like: authentication method 1: local, authentication method 2: tacacs-plus, authentication method 3: radius, the above authentication means first local authentication, if not pass, then tacacs-plus authentication, if not pass, using radius authentication); authentication mothod and sequence can be freely combined

2、802.1x configuration mode, as shown in Figure 188;

Figure 188 Configure 802.x configuration mode

802.1x configure authentication login mode

Configuration option: tacacs-plus/radiust

Function: Select 802.1x configuration mode authentication method.

6.33 Tacplus

6.33.1 Introduce

TACACS+(Terminal Access Controller Access Control System) is an application based on the TCP transmission protocol that uses the C/S mode to realize the communication between the NAS (Network Access Server) and the TACAC+ server. The client runs on the NAS and the server centrally manages the user information. NAS is a server side for the user and a client side for the server, and the structure diagram is shown in Figure 189;

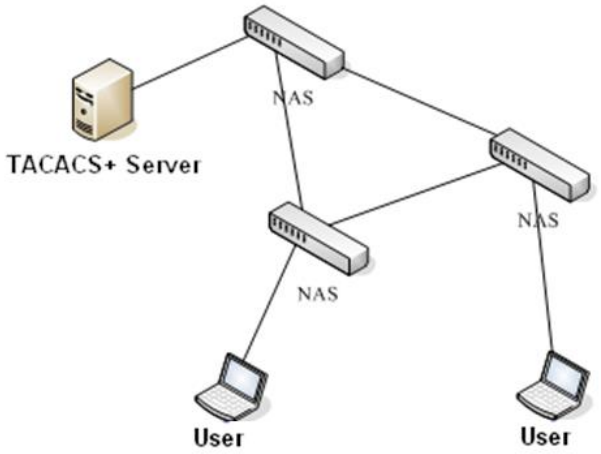


Figure 189 TACACS+ structure diagram

This protocol do authentication, authorization, and accounting to end users who need to login to the device for operation. As the client of TACACS+, the device sends the user name and password to the TACACS+ server for verification. The server accepts the customer's TCP connection and responds to the authentication request to verify whether the user is a

legal user, and the user can login to the device for operation.

6.33.2 Web page configuration

1、Enable TACACS+ protocol

TACACS+ configuration interface, as shown in Figure 190;

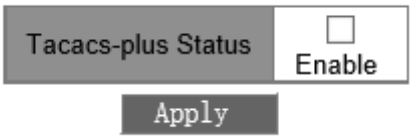


Figure 190 enable TACACS+ protocol

Tacacs-plus status

Configuration option: Enable/disable

Default configuration: Disable

Function: Whether enable TACACS protocol.

2、TACACS+ server configuration, as shown in figure 191;

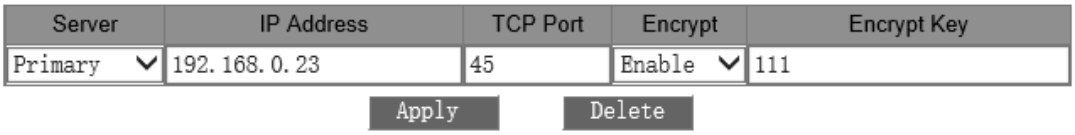


figure 191 TACACS+ server configuration

Server

Configuration option: Master server/slave server

Default configuration: Master server

Function: Select the currently configured server type.

IP address

Configuration format: A.B.C.D

Function: Input server IP address.

TCP port

Configuration range: 1~65535

Default configuration: 49

Function: The port number that receives the NAS authentication request.

Message encryption

Configuration option: Enable/disable

Default configuration: Disable

Function: Whether the message needs encryption, when the encryption enables, it needs to enter the encryption key value.

Key

Configuration range: 1~32 character

Description: Configure the key value improves the security of client communication with the TACACS+ server. Both parties verify the legitimacy of the message through the shared key of the device. Only when the key is consistent, both parties can receive the messages sent by each other and respond, so must ensure that the shared key configured on the device is exactly the same as the key value on the TACACS+ server.

Display the server configuration information under the TACACS+ server configuration bar,as shown in Figure 192;

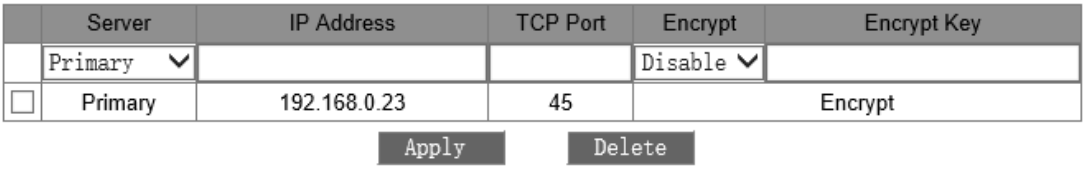


Figure 192 server configuration list

6.33.3 Typical configuration example

As shown in Figure 193, The TACACS+ server do authentication, authorization to the users through Switch. Server IP address is 192.168.0.23, shared key for switch message interaction with server is aaa.

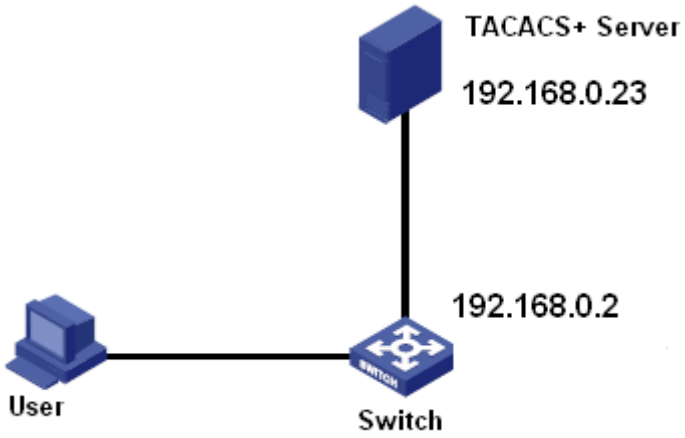


Figure 193 TACACS+ authentication example

➢Enable TACACS+ protocol, see Figure 190；

➢Server information configuration, IP address is 192.168.0.23, message encryption, and the key value is aaa, see figure 191；

➢Local authentication is used for web login; TACACS+ authentication is used for Telnet login, see the Figure 187；

➢Configure use name and password as bbb, on the TACACS+ server, key value is aaa;

➢Log in the switch through Web, and enter user name admin, password 123, then pass the authentication and access the switch successfully;

Log in switch through Telnet, enter user name and password bbb, then pass the TACACS+ authentication and access the switch successfully.

6.34 SSH

6.34.1 Introduce

SSH (Secure Shell) is a network protocol for secure remote login. SSH encrypts the transmitted data to prevent information leakage, and the user configure switch using the command line.

The series of devices supports SSH server, and multiple SSH user can be configured, but allows up to two SSH users to connect at the same time to login to the remote device via SSH.

6.34.2 Key

Unencrypted information is called plaintext, encrypted information is called ciphertext, and both encryption and decryption are performed under key control. The key is a specific set of strings that is the only parameter controlling the exchange of plaintext and ciphertext, acting as a "key." Encryption operations can turn plaintext to ciphertext, and decryption operations can restore it to plaintext.

Key-based security authentication requires a key, that is, a pair of keys exist at each end of the communication, namely a private key and a public key. The message can be encrypted with the public key and then decrypted by the legitimate person using the private key to ensure the confidentiality of the data.

6.34.3 Realization

In order to realize SSH secure connection during communication, there is five stages between server and client:

Version number negotiation stage: SSH currently includes SSH1 and SSH2, and the both parties determine the used version through version negotiation;

Key and algorithm negotiation stage: SSH supports various encryption algorithms, and the both parties negotiate the final used algorithm according to the supported algorithms;

Authentication stage: the SSH client sends an authentication request to the server, and the server authenticates the client;

Session request stage: After the authentication passes, the client sends the session request to the server;

Session phase: After the session request passes, the server interacts with the client.

6.34.4 Web page configuration

➢SSH server configuration:

SSH status, repeat authentication times, idle timeout, generate / destroy local key pair can be configured on the SSH server configuration interface, as shown in Figure 194;

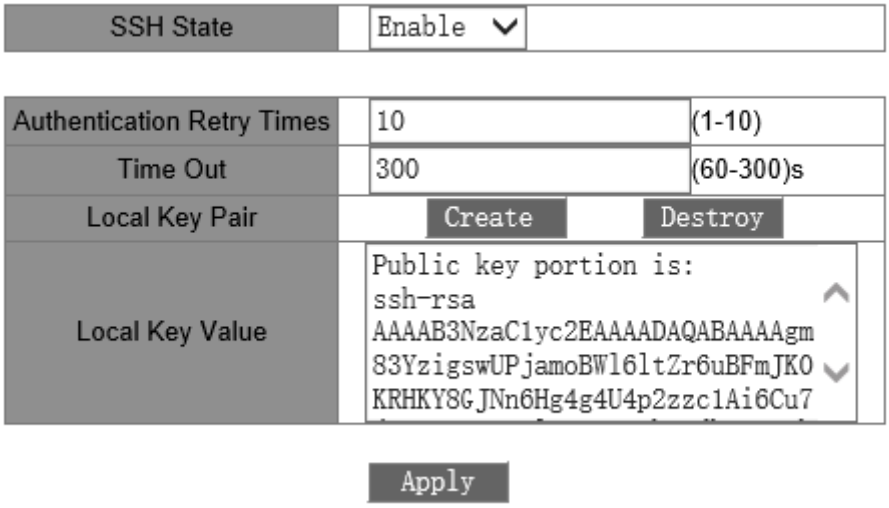


Figure 194 SSH serve configuration

➢Disable SSH status:

➢Click < Destroy > button to destroy old key pair, as shown in Figure 195;

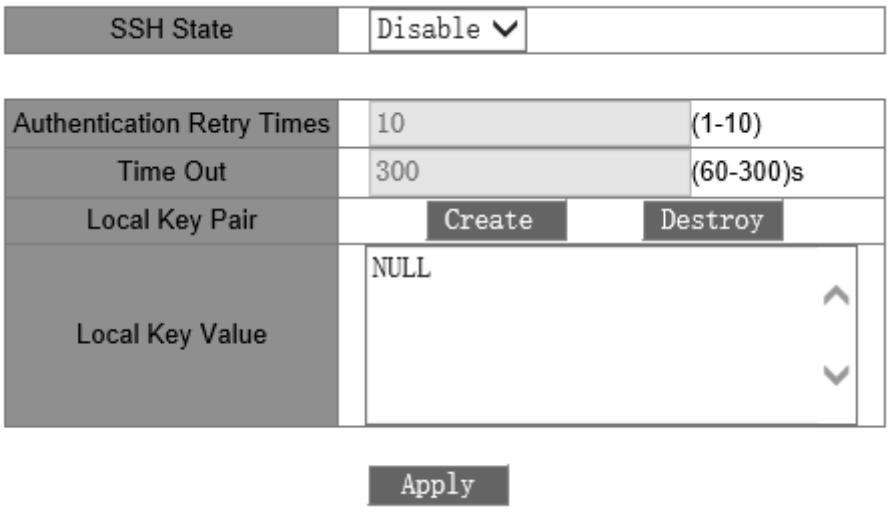


Figure 195 Destroy old key pair

3、Click <Generate> button to generate new key pair;

4、Enable SSH protocol, and configure SSH server, as shown in Figure 196;

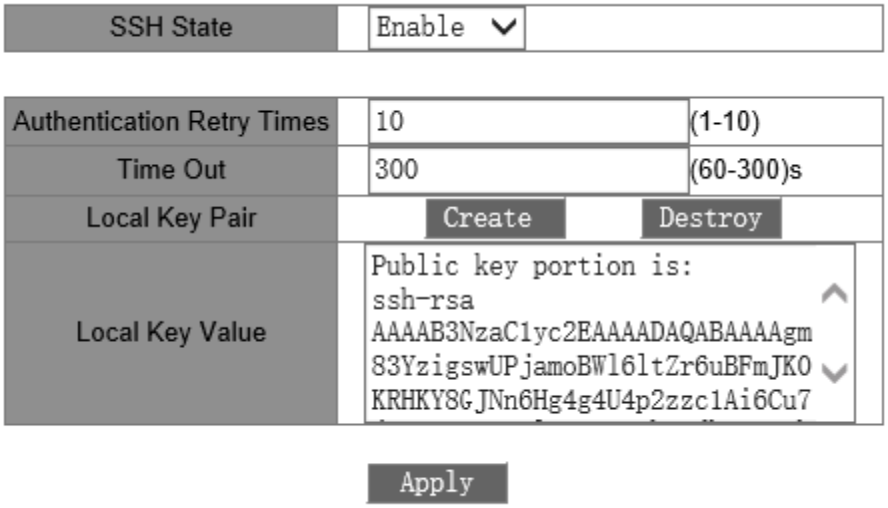


Figure 196 SSH server configuration

SSH status

Configuration option: Enable/disable

Default configuration: Disable

Function: Whether enable SSH protocol, if enable SSH, the device as SSH server.

Repeat authentication times

Configuration range: 1~10

Default configuration: 10

Function: The number of tries to log in to the SSH server.

Local key pair

Configuration option: Generate/Destroy

Function: Generate or destroy the local key pair of the SSH server, generate the local key pair before enabling the SSH server, and destroy the old key pair before generating the new key pair.

Local key value

Display the local key value and automatically generate key value after clicking the < Generate> button.

➢SSH secure IP address configuration

The SSH secure IP address can be added/ deleted on the SSH secure IP address

configuration interface, as shown in Figure 197;

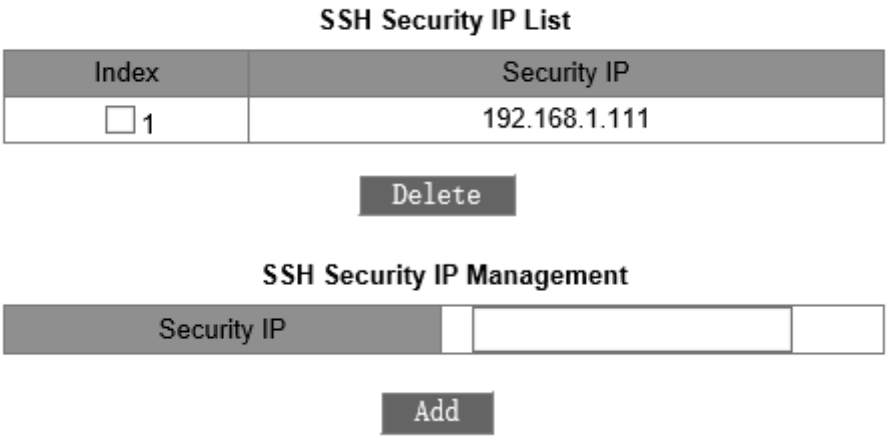


Figure 197 SSH secure IP address configuration

Secure IP address

Configuration format: A.B.C.D

Function: Configure the SSH client IP address that allows to log in switch; the SSH client IP address of the login switch is not restricted; when no secure IP address is configured, the secure IP address can access the switch only with the secure IP address through the SSH protocol.

Description: By default, no secure IP addresses are configured.

6.34.5 Typical configuration example

Host as SSH client establish local connection with Switch, as shown in Figure 198;

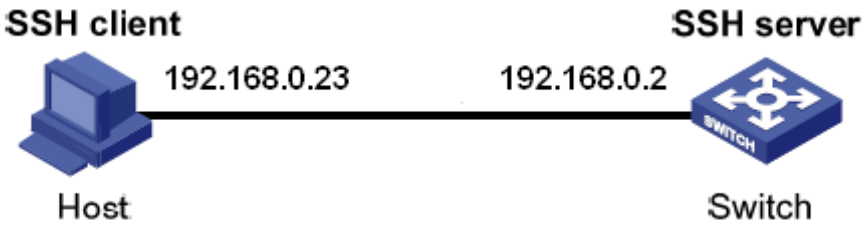


Figure 198 SSH configuration example

- SSH users adopt the password authentication mode;

1、Destroy the old server key pair, generate a new key pair, and start the SSH server, see the Figure 195,Figure 196；

2、Configure SSH user name: 333, service type: ssh, authentication type: password, password:333, see the Figure 20;

3、 Establish connection with SSH server, open PuTTY.exe software as shown in Figure 199，enter SSH server IP address in the Host Name (or IP address)：192.168.0.2；

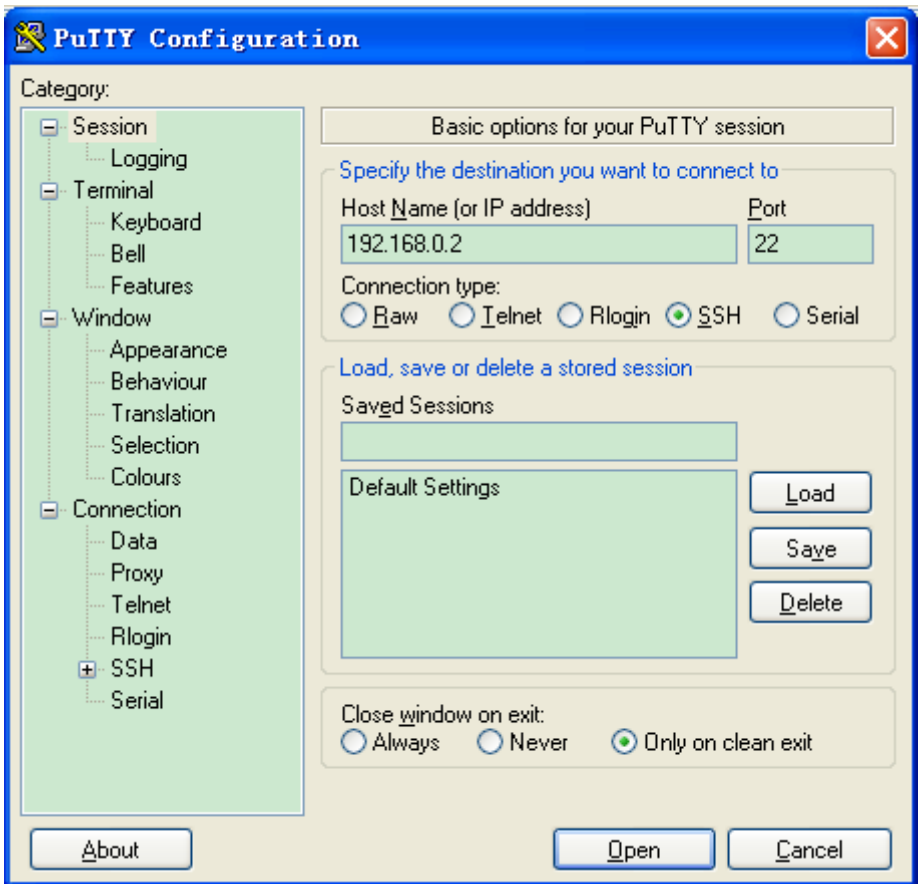


Figure 199 SSH client configuration

4、Click <Open> button, pop up alarm information as shown in Figure 200, click<Y> button;

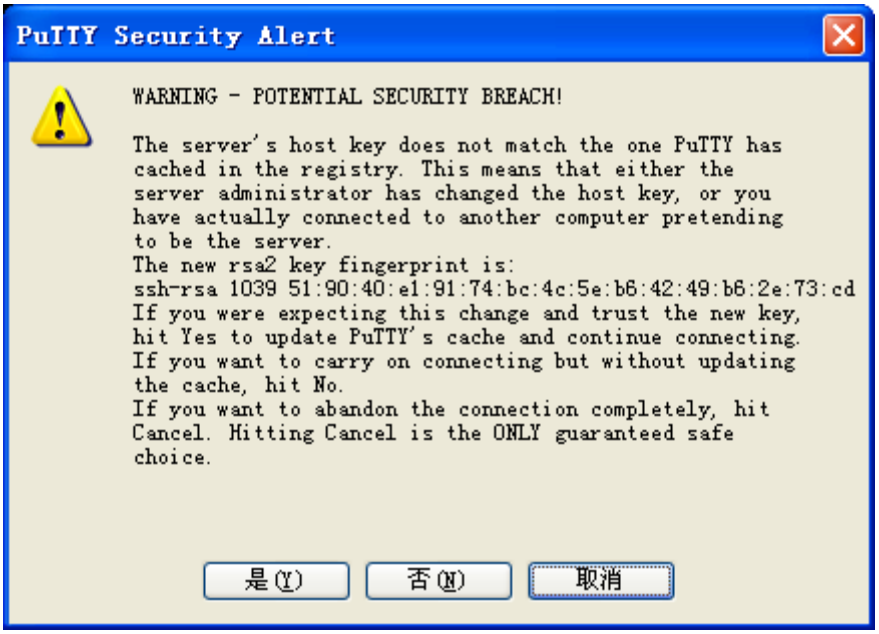


Figure 200 Alarm information

5、Follow prompted to enter user name: 333, enter into switch configuration page, as shown in Figure 201.

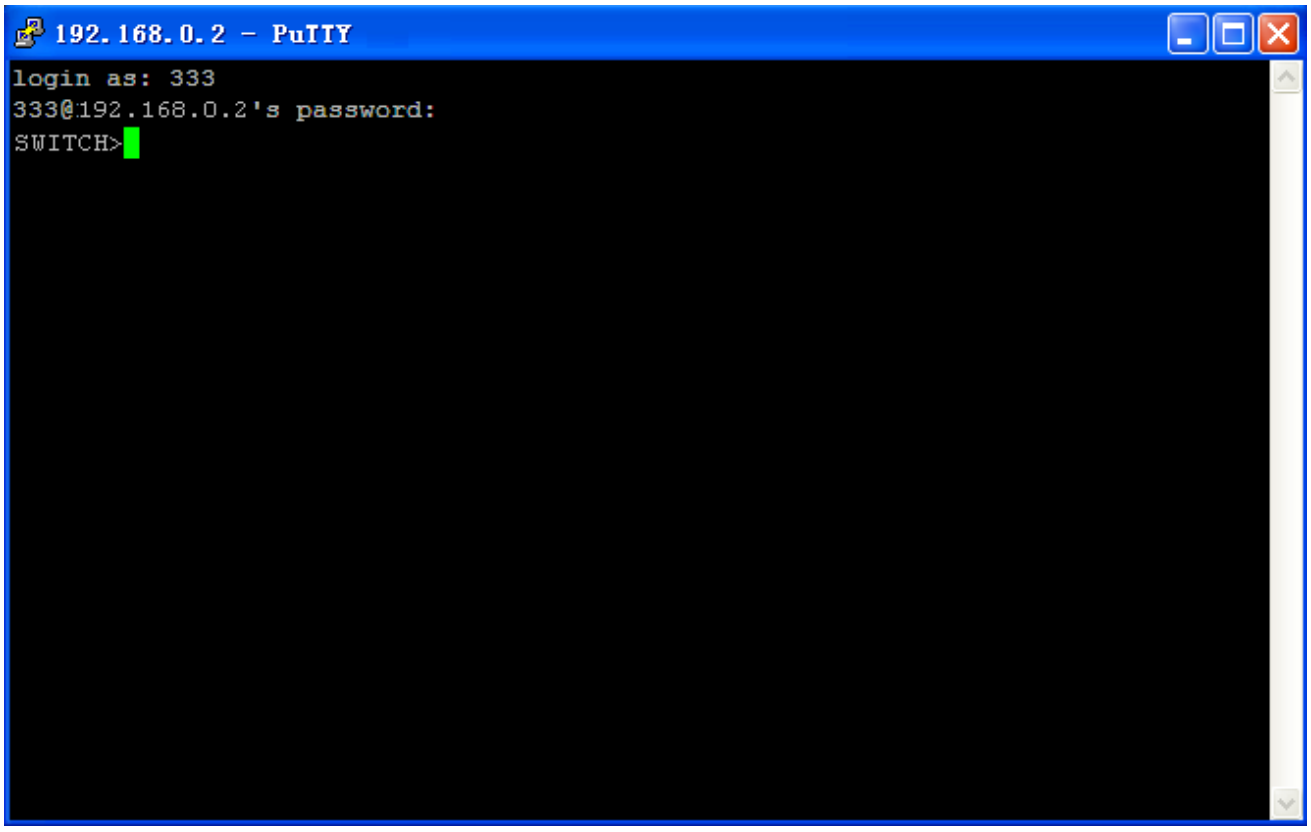


Figure 201 SSH password authentication mode login interface

- SSH user adopts the key authentication method;

1、Destroy the old server key pair, generate a new key pair, and start the SSH server, see the Figure 195,Figure 196；

2、Configure SSH client, see the Figure 194；run puttygen.exe in the client, click the<Generate> button to generate the client key pair, as shown in Figure 202;

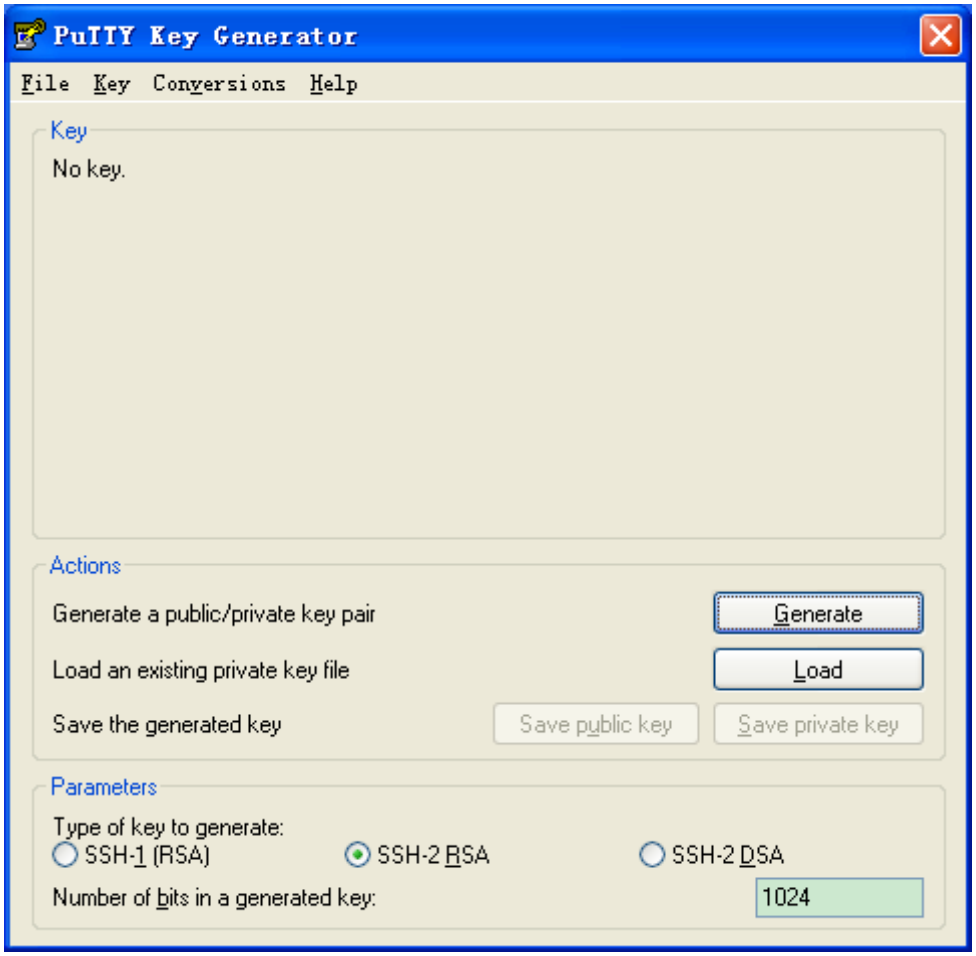


Figure 202 Generate client key

➢Move the mouse in the window during the process of generating the client key pair, otherwise the process bar is motionless and the key stops generating, as shown in Figure 203;

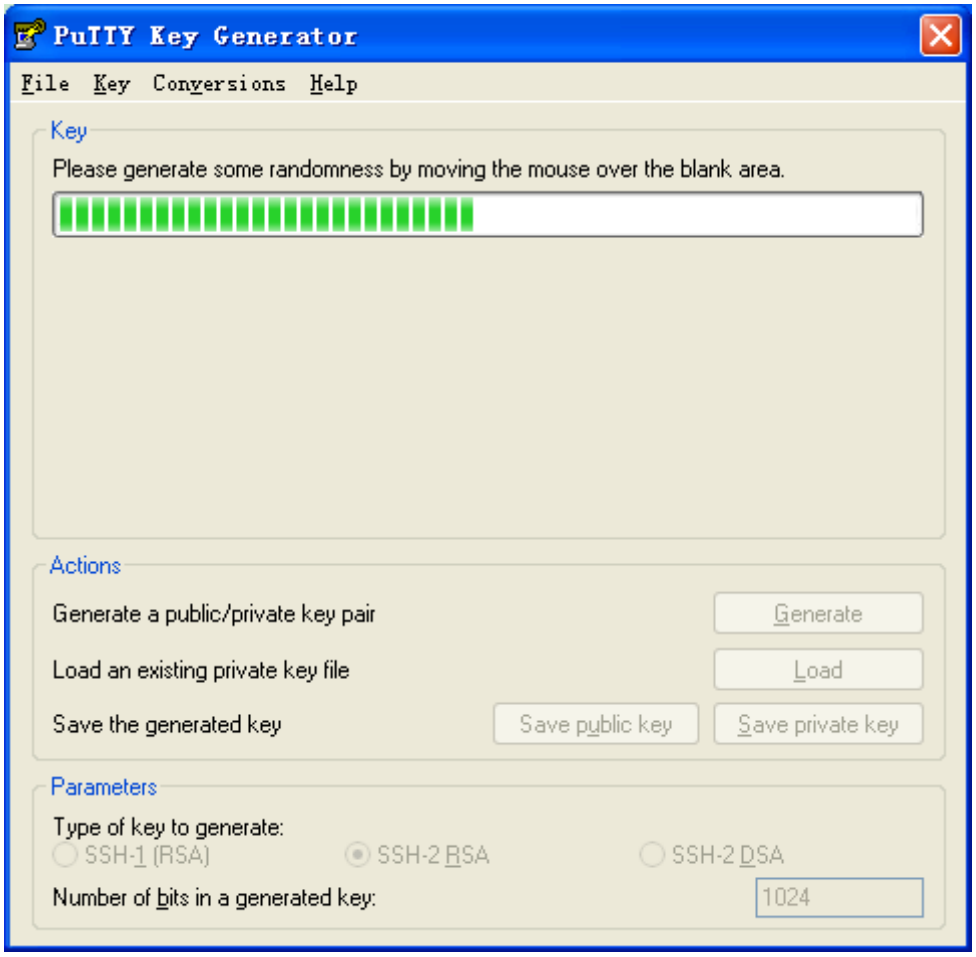


Figure 203 Key generation process

4、Generating key as shown in Figure 204, click <Save private key> button to store private key to 444.ppk file, the public key is copied to the key value of the SSH key configuration and entered the key name 444.

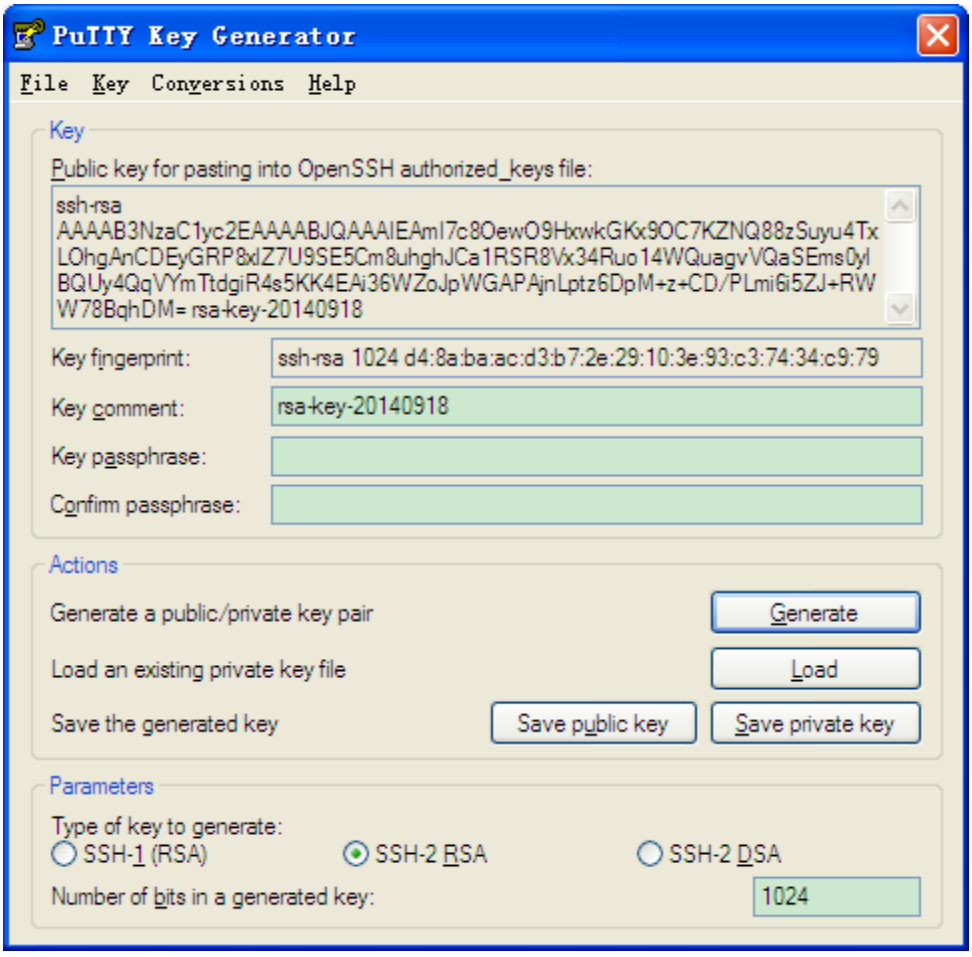


Figure 204 Generate key value

5、Configure SSH user name: 444, service type: ssh, authentication type: key, key: 444,

6、 Establish connection with SSH server, open PuTTY.exe software as shown in Figure 205, enter SSH server IP address in the Host Name (or IP address):192.168.0.2.

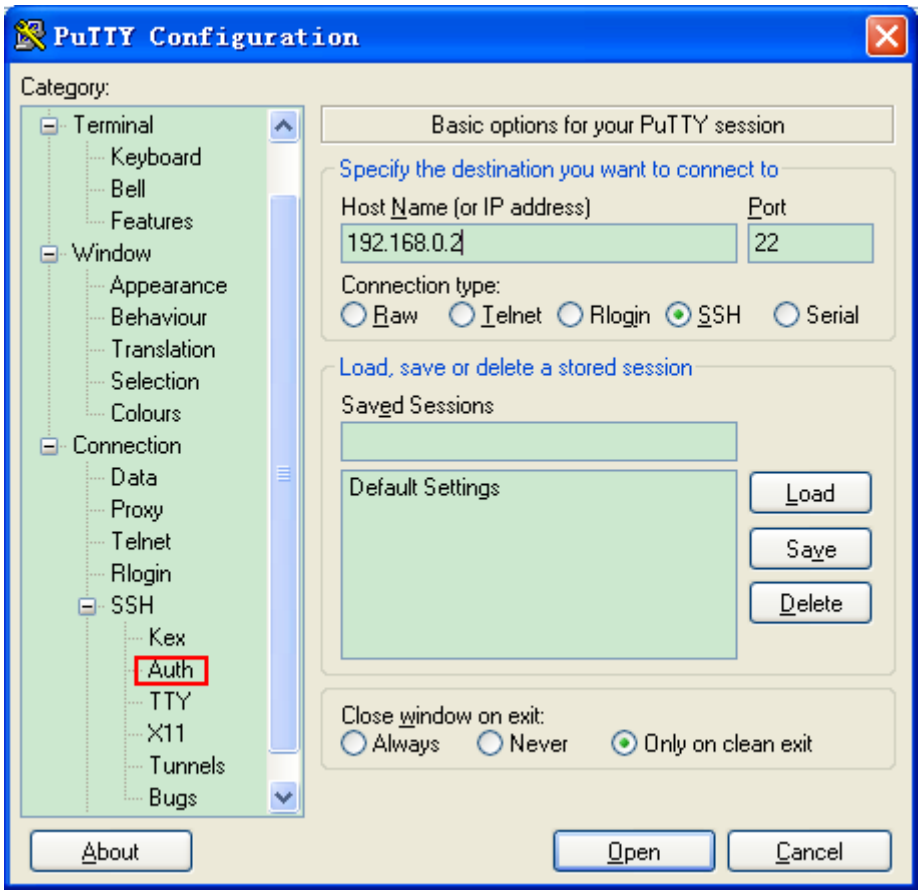


Figure 205 SSH client configuration when selecting key authentication method

7、Click the left of Figure 205 [SSH]→[Auth]，the interface as shown in the Figure 206, click <Browse> button, select stored private key file in the step 4,

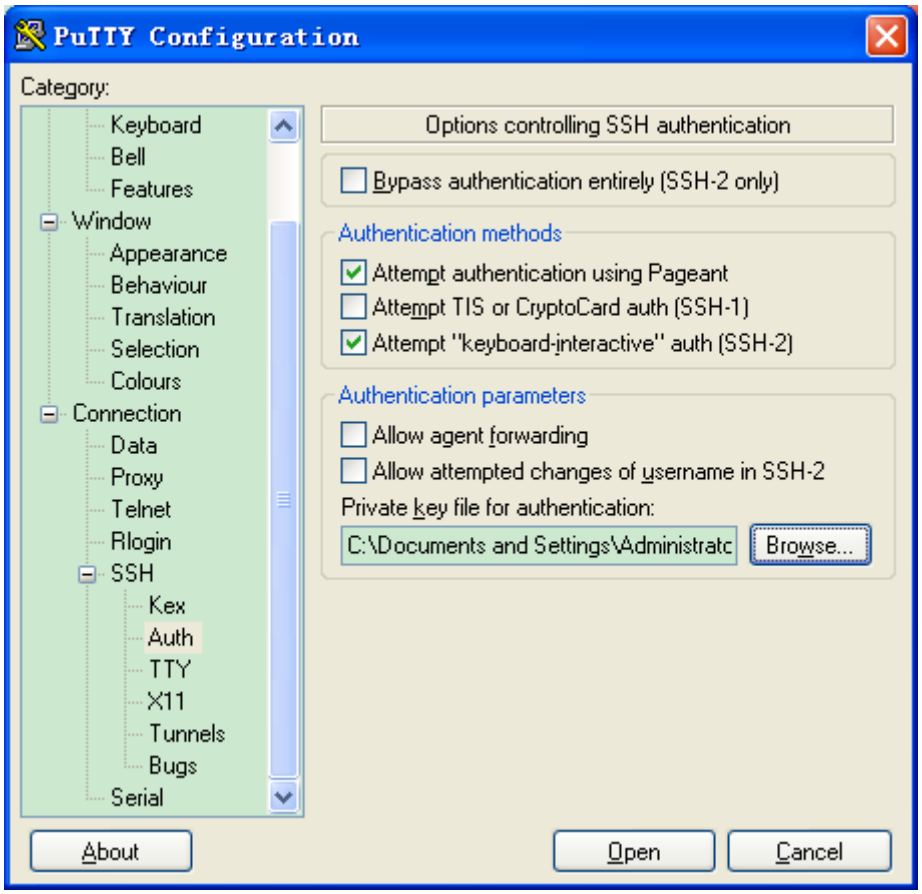


Figure 206 Select key file

8、Click <Open> button, following the prompts to enter the user name to enter the configuration interface of the switch, as shown in Figure 207;

Figure 207 SSH key authentication method login interface

6.35 Access management

6.35.1 Web page configuration

Whether enable access management, whether enable web/ftp/telnet access method, access management ID, Vlan ID, start IP address, end IP address, service type and delete access management method can be configure in the access management page, as shown in Figure 208;

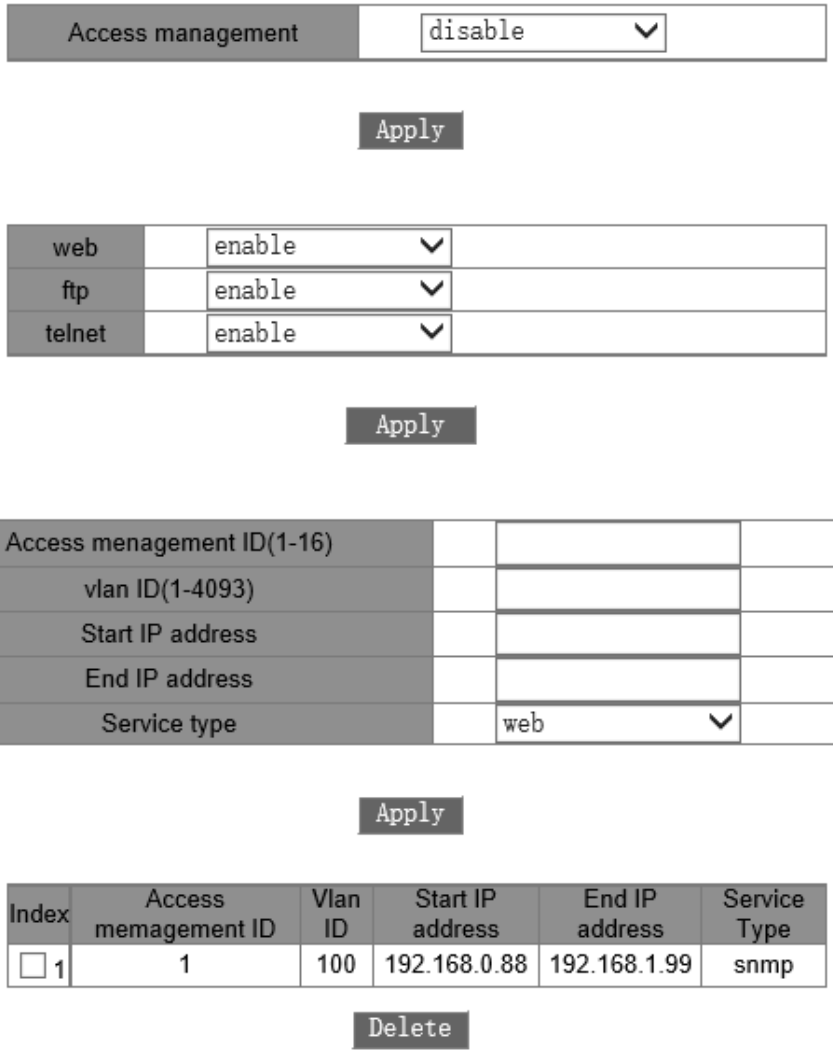


Figure 208 Access management configuration page

Access management status

Configuration option: Enable/Disable

Default configuration: Disable

Function: Whether enable access management, if enable, the device will manage the device access.

Web/ftp/telnet access status

Configuration range: Enable/Disable

Default configuration: Enable

Function: After web/ftp/telnet three methods of access the device are enabled, access the device through the enabled method (such as: web is enable, telnet is disable, so the

device can be accessed through web, but can't be accessed through telnet)

Access management ID

Configuration range: 1~16

Function: used to sign access management condition of device.

Vlan ID

Configuration range: 1~4093

Function: Configure the VLAN that require access management

Start IP address

Configuration format: A.B.C.D

Function: Configure the range of IP address that allows to log in switch; the start IP address cannot be empty; after the start IP address is configured, only the IP address after the start IP address can access the corresponding VLAN .

End IP address

Configuration format: A.B.C.D

Function: Configure the range of IP address that allows to log in switch; after the end IP address is configured, only the IP address between the start IP address and the end IP address can access the corresponding VLAN.

Service type

Configuration option:
web/snmp/"telnet/ssh"/web+snmp/"web+telnet/ssh"/"snmp+telnet/ssh"/all

Function: Configure the service type that requires access management.

6.35.2 Delete access management mode

Select the serial number before the access management ID, and click Delete to delete the corresponding access management items, as shown in Figure 209:

Index	Access memagement ID	Vlan ID	Start IP address	End IP address	Service Type
☑ 1	1	100	192.168.0.88	192.168.1.99	snmp

Delete

Figure 209 Delete access management configuration

6.36 MAC Learning

Configure whether enable MAC learning for each port in MAC leaning page, as shown in Figure 210;

MAC learn configuration

Port	Statue
S1/FE1	enable
S1/FE2	enable
S1/FE3	enable
S1/FE4	enable
S1/FE5	enable
S1/FE6	enable
S1/FE7	enable
S1/FE8	enable
S2/FE1	enable
S2/FE2	enable
S2/FX3	enable
S2/FX4	enable
S2/FE5	enable
S2/FE6	enable
S2/FX7	enable
S2/FX8	enable
S3/FX1	enable
S3/FX2	enable
S3/FX3	enable
S3/FX4	enable
S3/FX5	enable
S3/FX6	enable
S3/FX7	enable
S3/FX8	enable

Apply

Figure 210 MAC learning configuration

MAC leaning configuration

Configuration option: Enable/Disable

Default configuration: Enable

Function: Configure whether learning MAC address for each port.

Appendix: Acronyms

Acronym	Full Spelling
ACL	Access Control List
ARP	Address Resolution Protocol
BPDU	Bridge Protocol Data Unit
CLI	Command Line Interface
CRC	Cyclic Redundancy Check
DHCP	Dynamic Host Configuration Protocol
DHP	Dual Homing Protocol
DRP	Distributed Redundancy Protocol
DSCP	Differentiated Services Code Point
FTP	File Transfer Protocol
GARP	Generic Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
IGMP	Internet Group Management Protocol
IGMP Snooping	Internet Group Management Protocol Snooping
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
MAC	Media Access Control
MIB	Management Information Base
NMS	Network Management Station
OID	Object Identifier
PVLAN	Private VLAN
QoS	Quality of Service
RMON	Remote Network Monitoring
RSTP	Rapid Spanning Tree Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol

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