SICOM6000A Industrial Ethernet Switch
Web Operation Manual

Publication Date: Jul. 2018

Version: V1.0

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 SICOM6000A industrial Ethernet switch, and details Web configuration methods.

Content Structure

The manual contains the following contents:

Main Content	Explanation
1. Product introduction	➤ Overview ➤ Product models ➤ Software features
2. Switch access	➤ View types ➤ Switch access by console port ➤ Switch access by Telnet ➤ Switch access by Web
3. Device information	Switch basic information
4. Switch maintenance	➤ Reboot ➤ Software update (by FTP, TFTP)
5. Device basic configuration	➤ Basic configuration (Basic configuration, clock configuration) ➤ User management configuration ➤ Port configuration (physical port configuration, port information) ➤ VLAN configuration ➤ PVLAN configuration ➤ Port mirroring ➤ Port storm suppression ➤ Port isolate ➤ Port channel ➤ Telnet server configuration ➤ SSH server configuration

	➢ SSL configuration
	➢ File transmission (TFTP service, FTP service)
	➢ MAC address table configuration
	➢ Basic configuration debug
6. Device advanced configuration	➢ ARP configuration
	➢ Layer-3 interface configuration
	➢ SNMP v2c, SNMP v3
	➢ DT-Ring
	➢ DRP configuration
	➢ STP/RSTP
	➢ MSTP
	➢ Alarm
	➢ Port traffic alarming
	➢ Log configuration
	➢ Static route configuration
	➢ RIP configuration
	➢ OSPF configuration
	➢ DHCP server configuration
	➢ QoS configuration
	➢ IEC61850 configuration
	➢ IGMP Snooping
	➢ GMRP
	➢ Static multicast configuration
	➢ LLDP
	➢ VRRP
	➢ SNTP configuration
	➢ NTP configuration
	➢ TACACS+ configuration

	➢ RADIUS configuration
	➢ IEEE802.1x configuration
	➢ Authentication login configuration
	➢ Link check
	➢ Loop Detect Configuration
	➢ CRC Protect Configuration

Conventions in the manual

1. CLI conventions

Format	Description
Bold	The keywords of a command line are in **bold**.
Italic	Command arguments are in *italic*.
[ ]	Items (keywords or arguments) in [ ] are optional.
{x|y|……}	Alternative items are grouped in { } and separated by vertical bars. One is selected.
[x|y|……]	Optional alternative items are grouped in [ ] and separated by vertical bars. One or none is selected.
<x|y|……>	Alternative items are grouped in < > and separated by vertical bars. A minimum of one or a maximum of all can be selected.
//	A line starting with the // sign is comments.

2. Text format conventions

Format	Explanation
< >	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 IP address and MAC address is 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.

3. Symbol conventions

Symbol	Explanation
⚠ **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 SICOM6000A industrial Ethernet switch include:

Name of Document	Content Introduction
SICOM6000A Series Industrial Ethernet Switches Hardware Installation Manual	Describes the hardware structure, hardware specifications, mounting and dismounting methods.
SICOM6000A 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:

➢ CD shipped with the device

➢ Kyland website: www.kyland.com

1. Product Introduction

1.1 Overview

SICOM6000A includes a series of high-performance managed industrial Ethernet switches applied in the rail transportation industry. SICOM6000A conforms to EN50155, EN50121 and other industrial standards. The switch is a layer 3 switch that supports the layer 3 routing protocol, and MSTP, RSTP, DT-Ring, IEC62439-6 redundancy protocols, guaranteeing the reliable operation of the system.

1.2 Software Features

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

➢ Redundancy protocols: STP/RSTP, MSTP, DT-Ring, VRRP, and IEC62439-6

➢ Routing protocols: OSPFv2, static routing protocol, RIP

➢ Multicast protocols: IGMP Snooping, GMRP, and static multicast

➢ Switching attributes: VLAN, PVLAN, QoS, and ARP

➢ Bandwidth management: port channel, port rate limiting, and port storm suppression

➢ Synchronization protocols: SNTP, NTP

➢ Security: IEEE802.1x, TACACS+, RADIUS, SSH, SSL, MAC address binding, port isolation, and user management

➢ Device management: FTP/TFTP software update, FTP/TFTP file transmission, log record and upload

➢ Device diagnosis: port mirroring, LLDP, link check, loop detect, and CRC protect

➢ Alarm function: port alarm, power alarm, ring alarm, high-temperature alarm, low-temperature alarm, and port traffic alarm

➢ Network management: management by CLI, Telnet, Web and Kyvision network management software, DHCP, and SNMP v1/v2c/v3 and IEC61850 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 system date and time. ➢ Show software version.	Input "**enable**" to enter the privileged mode.
Switch#	Privileged mode	➢ Configure system clock and date. ➢ Transmit file and update software. ➢ Delete switch file. ➢ Configure CLI language. ➢ View switch configuration and system information. ➢ Restore default configuration. ➢ Save current configuration.	➢ Input "**config**" to switch from privileged mode to configuration mode. ➢ Input "**exit**" to return to the general mode.

		➢ Reboot switch.	
Switch (config) #	Configuration mode	Configure all switch functions.	Input "**exit**" to return to 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 Switch Access by 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 9-pin serial port of a PC to the console port of the switch with the DB9-M12 console cable.

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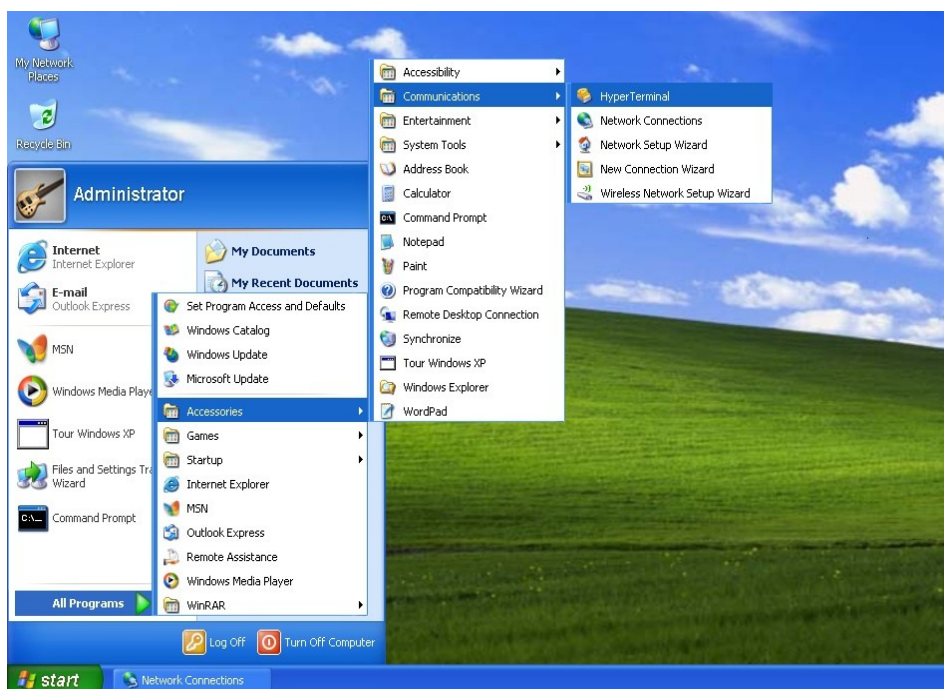
Figure 1 Starting the Hyper Terminal

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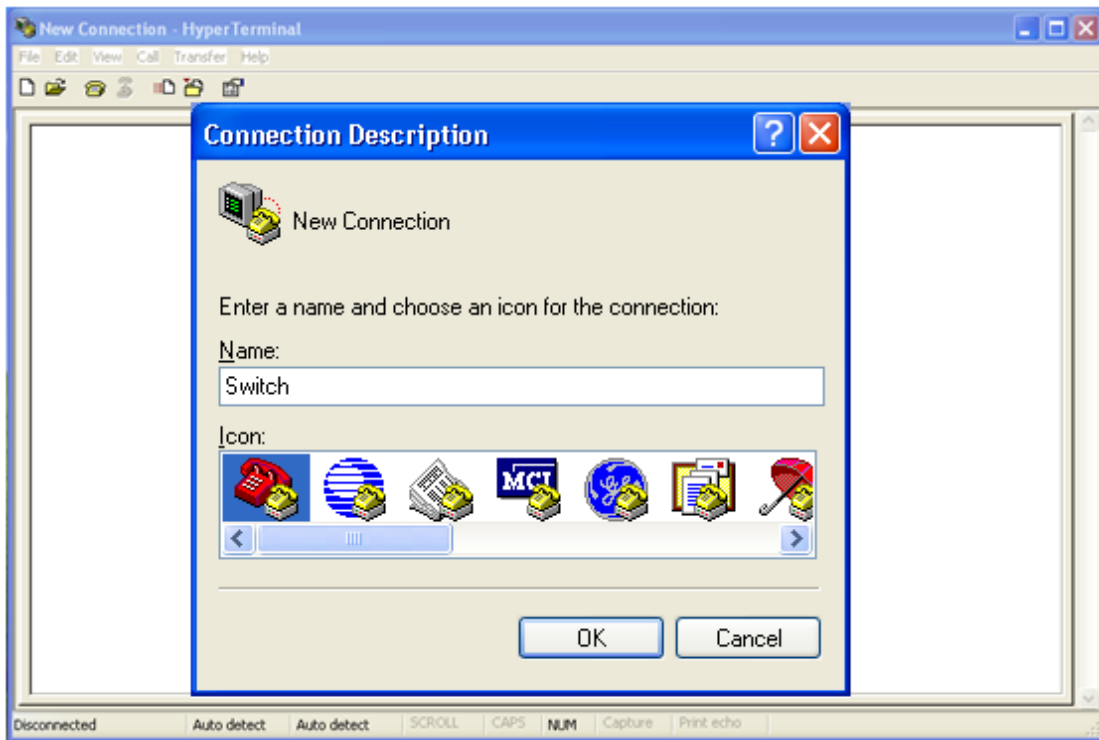
Figure 2 Creating a New Connection

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

Figure 3 Selecting the Communication Port

Note:

To confirm the communication port in use, right-click [My Computer] and click [Property] →

[Hardware] → [Device Manager] → [Port].

5. Set port parameters (Bits per second: 115200, Data bits: 8, Parity: None, Stop bits: 1, and Flow control: None), as shown in Figure 4.
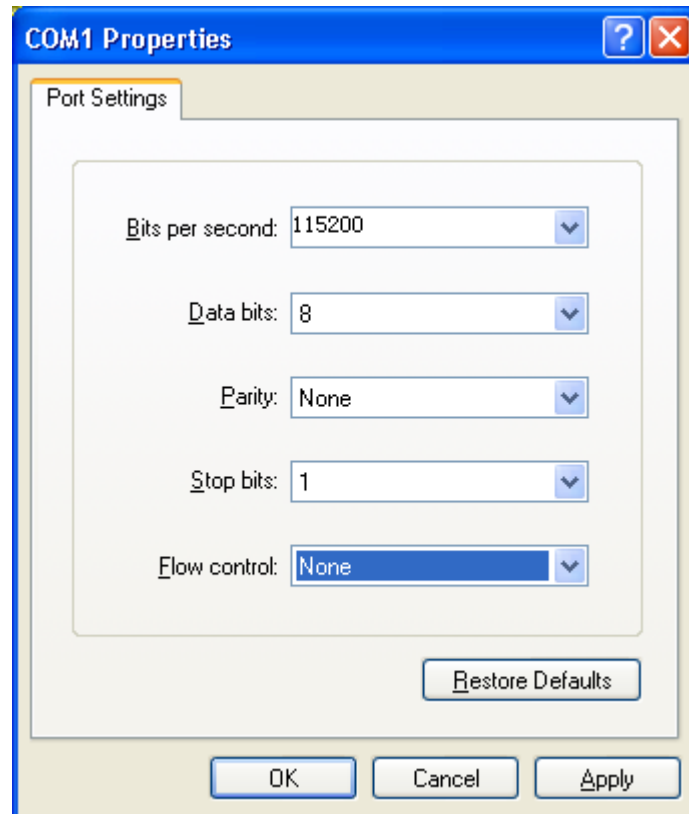
Figure 4 Setting Port Parameters

6. Click <OK> button to enter the switch CLI. Input password "admin" and press <Enter> to enter the General mode, as shown in Figure 5.
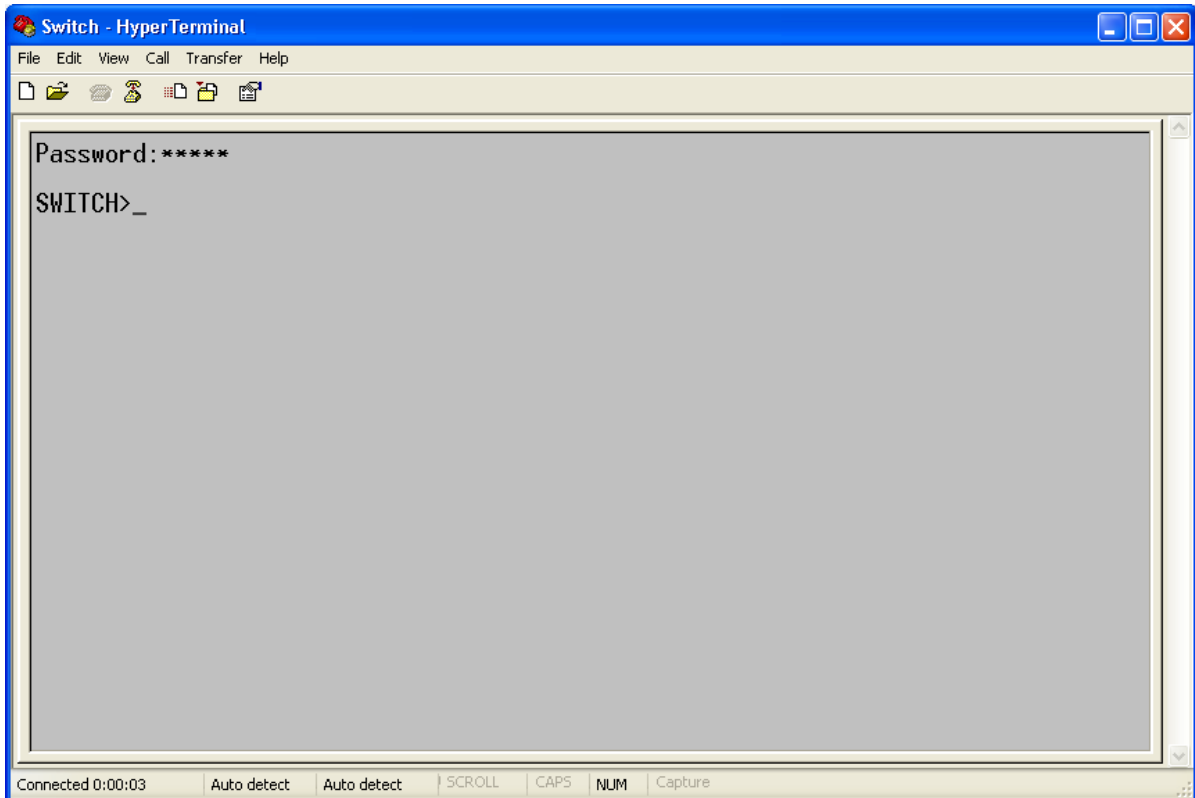
Figure 5 CLI

7. Input command "enable", default user "admin", and password"123" to enter the privileged

mode. You can also input other created users and password, as shown in Figure 6.
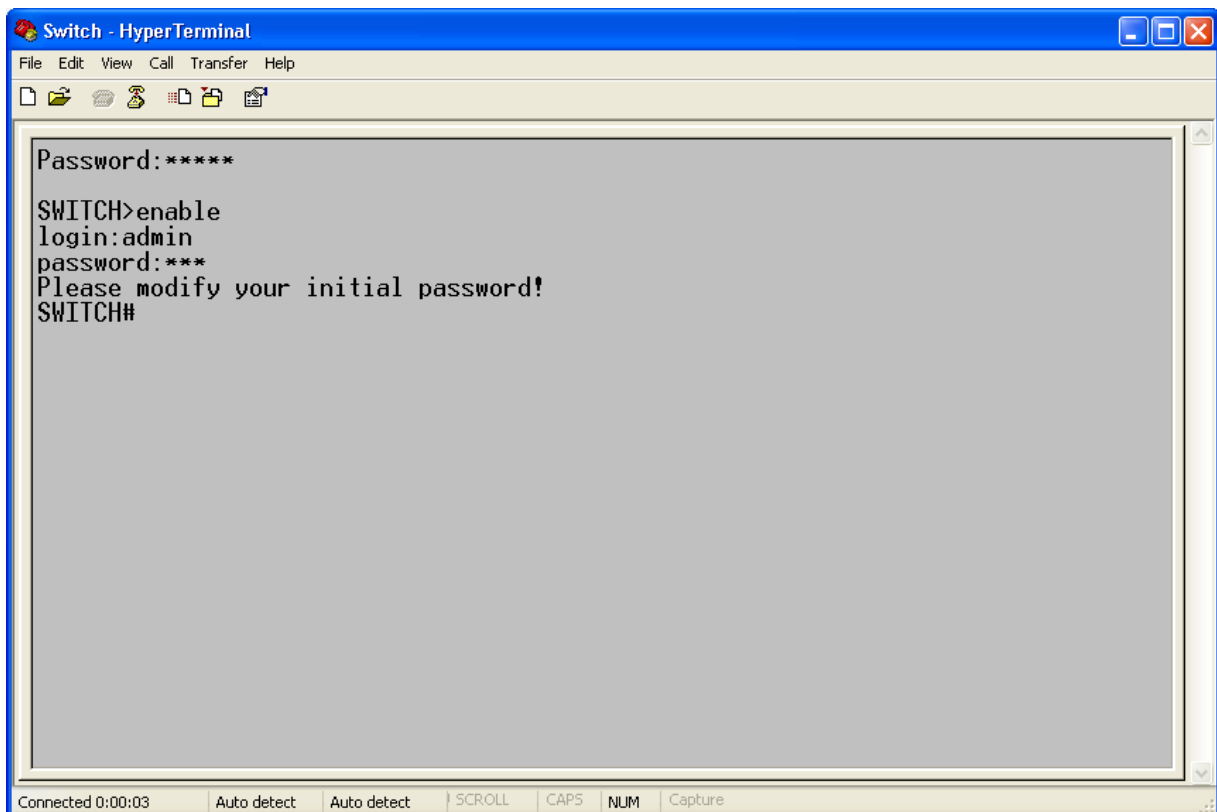
Figure 6 Privileged mode

2.3 Switch Access by Telnet

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

1. Enter "**telnet** *IP address*" in the Run dialog box, as shown in Figure 7. The default IP address of a Kyland switch is 192.168.0.2.
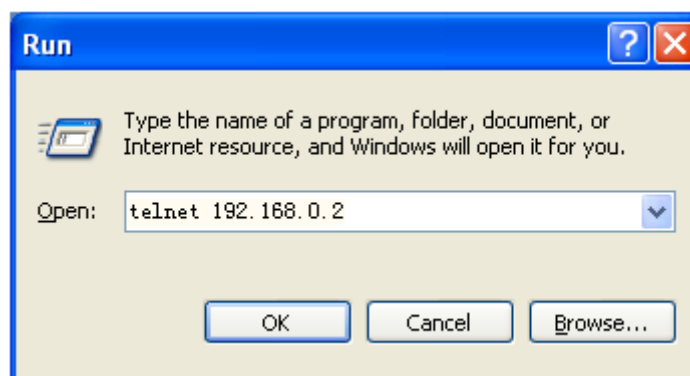
Figure 7 Telnet Access

	Note:
NOTE	To confirm the switch IP address, please refer to "6.2.1 Switch IP Address" to learn how to obtain IP address.

2. In the Telnet interface, input user "admin", and password "123" to log in to the switch. You can also input other created users and password, as shown in Figure 8.
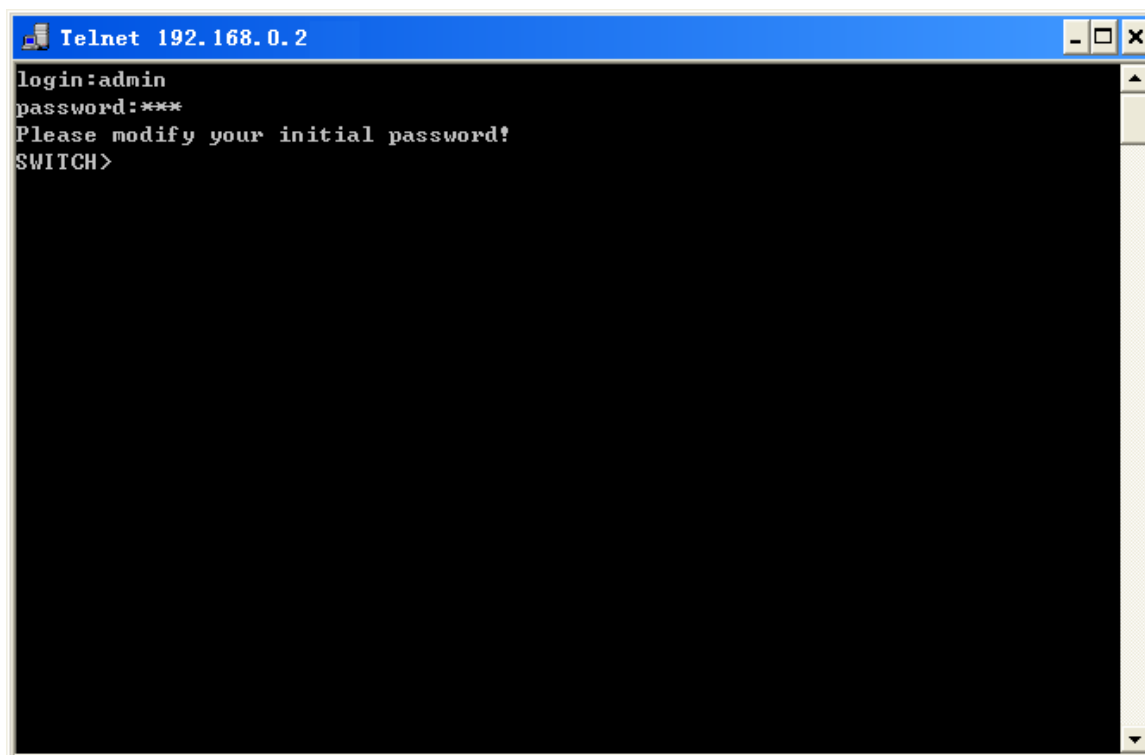
Figure 8 Telnet Interface

2.4 Switch Access by Web

The precondition for accessing a 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 Figure 9. Input the default user name "admin", password "123", and the Verification. Click

<Login>. You can also input other created users and password.
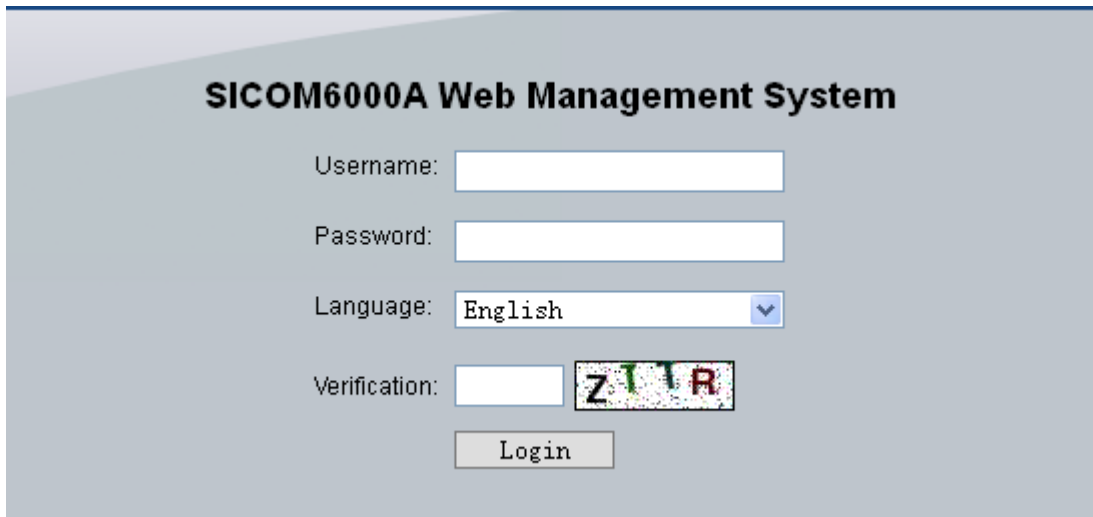
Figure 9 Web Login

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

Chinese login interface.

> **Note:**
>
> To confirm the switch IP address, please refer to "6.2.1 Switch IP Address" to learn how to
>
> obtain IP address.

2. The prompt of modifying the initial password is displayed, click <OK> button.

3. After you log in successfully, there is a navigation tree on the left of the interface, as

shown in Figure 10.
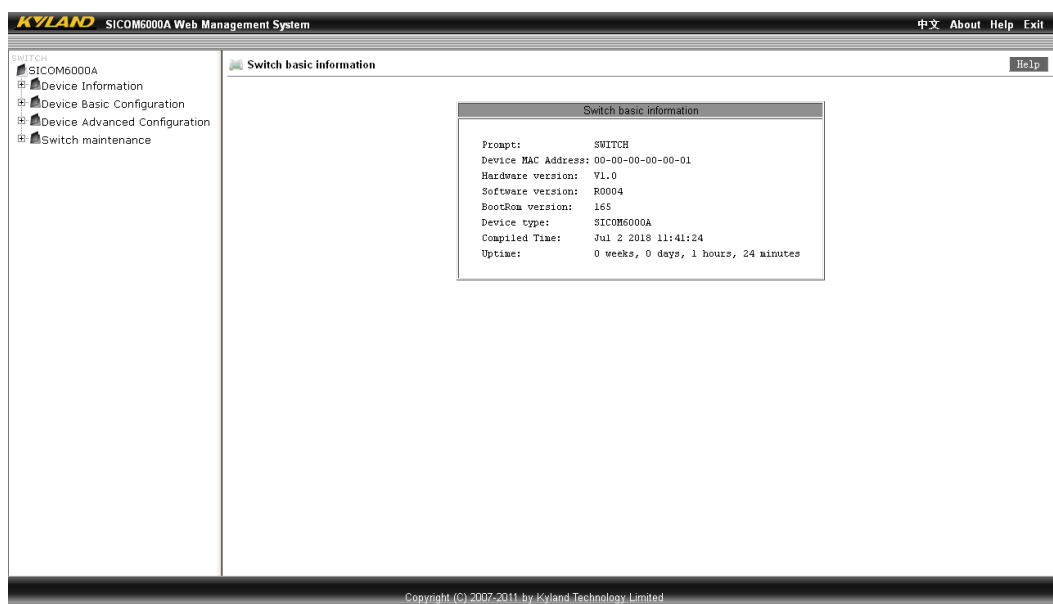
Figure 10 Web Interface

In the top right corner, you can click <中文> to change language to Chinese or <Exit> to exit the Web interface.

3. Device Information

3.1 Switch Basic Information

The switch basic information includes the prompt, MAC address, hardware version, software version, BootROM version, device type, compilation date, and runtime. Click [Device Information] → [Switch basic information] in the navigation tree to show the switch basic information, as shown in Figure 11.

```
                    Switch basic information

    Prompt:              SWITCH
    Device MAC Address: 00-00-00-00-00-01
    Hardware version:    V1.0
    Software version:    R0004
    BootRom version:     165
    Device type:         SICOM6000A
    Compiled Time:       Jul 2 2018 11:41:24
    Uptime:              0 weeks, 0 days, 1 hours, 24 minutes
```

Figure 11 Switch Basic Information

4. Switch Maintenance

In the navigation tree, you can click [Save current running-config] to save the current configuration or [Reboot with the default configuration] to enter the page shown in Figure 12. Then you can click <Yes> to restore the default configuration.

Reboot
| Save current configuration before reboot? | ⊙ Yes ○ No |

Apply

Figure 12 Restoring Default Configuration

4.1 Reboot

To reboot the device, click [Switch maintenance] → [Reboot] in the navigation tree to enter the reboot interface, as shown in Figure 13.

Reboot
| Save current configuration before reboot? | ⊙ Yes ○ No |

Apply

Figure 13 Reboot

Before rebooting, please confirm whether to save current configuration. If you select "Yes", the switch runs the current configuration after reboot. If you select "No", the switch runs the previous saved configuration. If no configuration has been saved, the switch will restore the default configuration after reboot.

4.2 Software Update

Software updates may help the switch to improve its performance. The series switches need to update only one software version file. It contains not only the system software version, but also the BootROM software version.

The software version update needs the assistance of FTP/TFTP server.

4.2.1 Software Update by FTP

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

1. Click [Security] → [Users/Rights]. The "Users/Rights Security Dialog" dialog box is displayed. Click <New User> to create a new FTP user, as shown in Figure 14. Create a user name and password, for example, user name "admin" and password "123". Click <OK>.
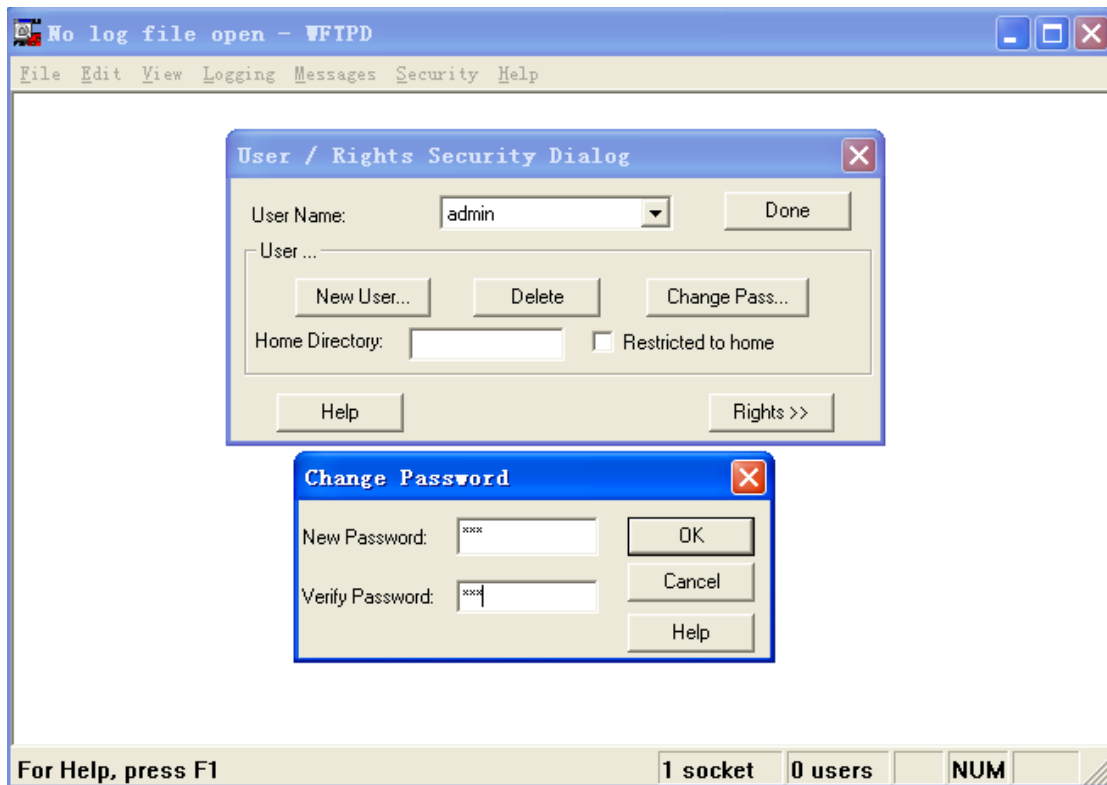
Figure 14 Creating a New FTP User

2. Input the storage path of the update file in "Home Directory", as shown in Figure 15. Click <Done>.
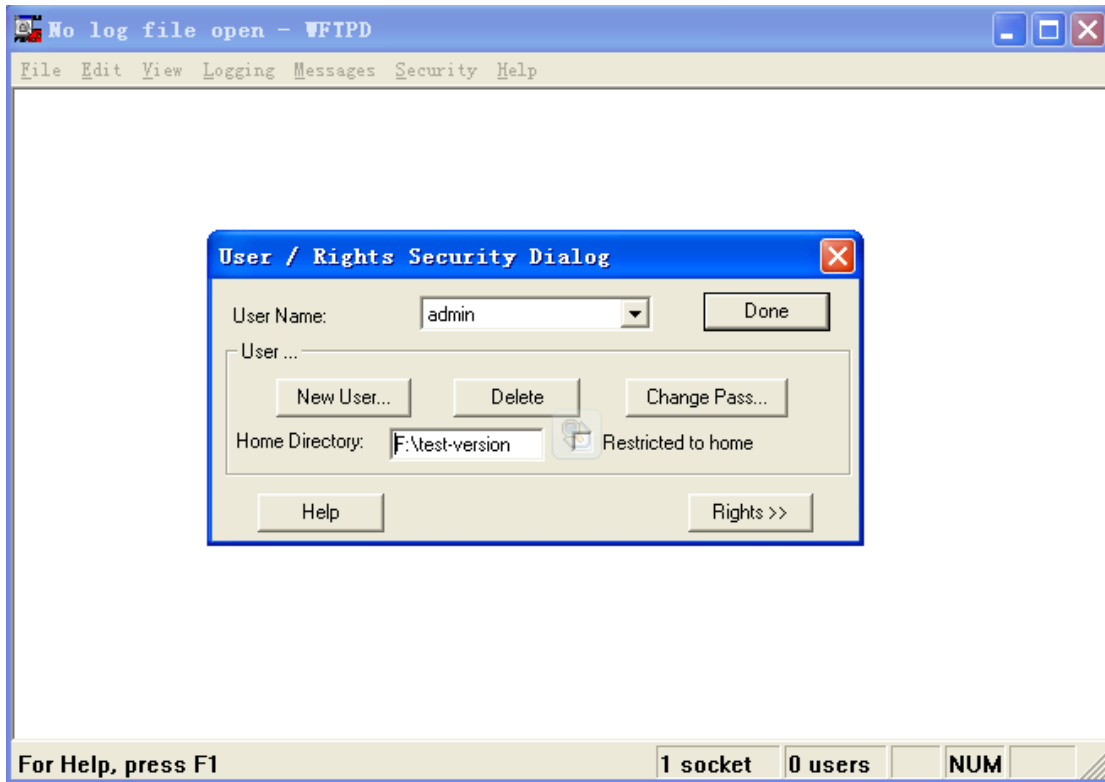
Figure 15 File Location

3. Click [Switch maintenance] → [FTP software update] in the navigation tree to enter the FTP software update page, as shown in Figure 16. Enter the IP address of FTP server, FTP user name, password, and file name on the server. Click <Update>.

Figure 16 Software Update by FTP

Transmission type

Options: **binary/ascii**

Default: **binary**

Function: Select the file transmission standard.

Explanation: **ascii** means using ASCII standard to transmit file; **binary** means using binary standard to transmit file.

ForceUpdate

Options: YES/NO

Default: NO

Function: Select the handling method when the software version does not match the switch hardware.

Explanation: NO means to cancel software update if software and hardware do not match. YES means to continue software update even if software and hardware do not match. However, it might result in system anomaly, or even boot failure.

	Warning:
	➢ The file name must contain an extension. Otherwise, the update may fail.
	➢ Software version file is not a text file, and it must adopt the binary standard for transmission.
	➢ To guarantee normal running, please select NO for ForceUpdate. That is, do not update software if the software and hardware version do not match

4. Make sure the normal communication between the FTP server and the switch, as shown in Figure 17.
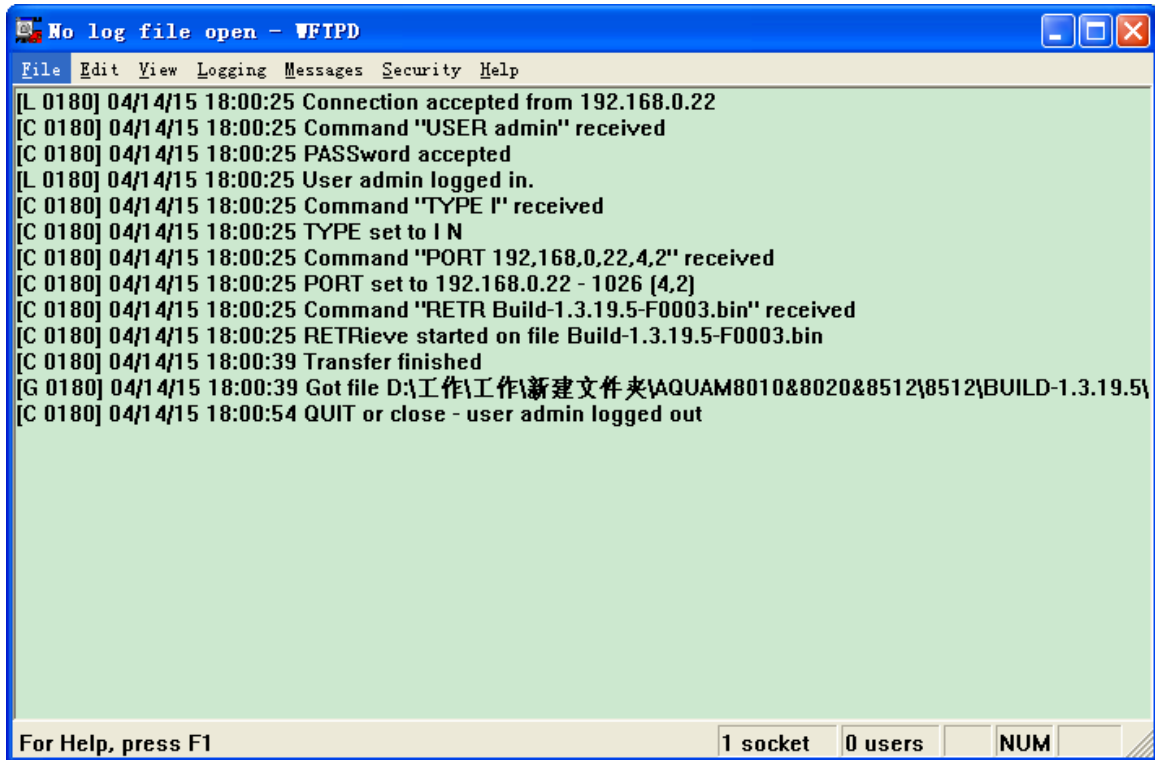
Figure 17 Normal Communication between FTP Server and Switch

⚠️ CAUTION	**Caution:** To display update log information as shown in Figure 17, you need to click [Logging] → [Log Options] in WFTPD and select Enable Logging and the log information to be displayed.

5. When the update is completed, please reboot the device and open the Switch Basic Information page to check whether the update succeeded and the new version is active.

⚡ WARNING	**Warning:** ➢ In the software update process, keeps the FTP server software running. ➢ When update completes, reboot the device to activate the new version. ➢ If update fails, do not reboot the device to avoid the loss of software file and startup anomaly.

4.2.2 Software Update by TFTP

Install TFTP server. The following uses TFTPD software as an example to introduce TFTP server configuration.

Figure 18 TFTP Server Configuration

1. In "Current Directory", select the storage path of update file on server. Enter the server IP address in "Server interface".

2. Click [Switch maintenance] → [TFTP software update] in the navigation tree to enter the TFTP software update page, as shown in Figure 19. Enter the IP address of the TFTP server and file name on server. Click <Update>, and wait for update to complete.

Figure 19 Software Update by TFTP

Transmission type

Options: **binary/ascii**

Default: **binary**

Function: Select the file transmission standard.

Explanation: **ascii** means using ASCII standard to transmit file; **binary** means using binary

21

standard to transmit file.

ForceUpdate

Options: YES/NO

Default: NO

Function: Select the handling method when the software version does not match the switch

hardware.

Explanation: NO means to cancel software update if software and hardware do not match.

YES means to continue software update even if software and hardware do not match.

However, it might result in system anomaly, or even boot failure.

	Warning:
⚠️ WARNING	➢ The file name must contain an extension. Otherwise, the update may fail.
	➢ Software version file is not a text file, and it must adopt the binary standard for transmission.
	➢ To guarantee normal running, please select NO for ForceUpdate. That is, do not update software if the software and hardware version do not match

3. Make sure the normal communication between the TFTP server and the switch, as shown
in Figure 20.
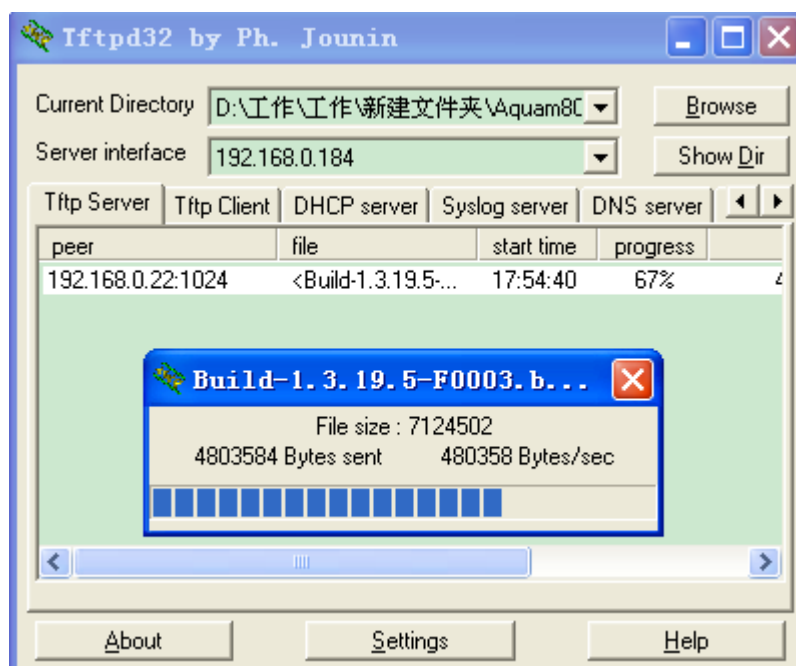
Figure 20 Normal Communication between TFTP Server and Switch

4. When the update is completed, please reboot the device and open the Switch Basic Information page to check whether the update succeeded and the new version is active.

	Warning:
	➢ In the software update process, keeps the TFTP server software running.
	➢ When update completes, reboot the device to activate the new version.
	➢ If update fails, do not reboot the device to avoid the loss of software file and startup anomaly.

5. Device Basic Configuration

5.1 Switch Basic Configuration

Switch basic configuration includes hostname, mapping between host and IP address, and switch clock.

5.1.1 Basic Configuration

1. Setting Hostname

Click [Device Basic Configuration] → [Switch Basic Configuration] → [Basic Config] to enter switch basic configuration page, as shown in Figure 21.

Set Hostname

Hostname(1-30 character)	SWITCH

Reset   Apply

Figure 21 Setting Hostname

Hostname

Range: 1-30 characters

Default: SWITCH

Function: Set the prompt in switch CLI.

Method: Click <Apply> to activate the new hostname. Click <Reset> to cancel the current setting and use the previous hostname.

2. Setting mapping between hostname and IP address, as shown in Figure 22.

Mapping hostname and IP

Hostname(1-15 character)	kyland
IP address	192.168.1.23

Add   Del

Hostname	IP Address
Switch	192.168.1.144
kyland	192.168.1.23

{Host name, IP address}

Format: {1-15 characters, A.B.C.D}

Function: According to the mapping, use hostname to access the corresponding device.

Method: Input valid hostname and IP address. Then click <Add> to set a mapping entry of hostname and IP address or <Del> to delete the mapping entry.

Example: After setting the mapping between hostname "Switch" and IP address "192.168.0.4" successfully, you can ping the switch by using the **ping host Switch** command instead of **ping 192.168.0.4**.

5.1.2 Setting the Clock

You can set the system date and time. The series switches support Real-Time Clock (RTC). Even if they are powered off, they continue timing.

To make full use of time and save energy, Daylight Saving Time (DST) can be used in summer. To be specific, adjust clock forward one hour in summer.

Click [Device Basic Configuration] →[Switch Basic Configuration]→[Clock configuration] to enter clock configuration page, as shown in Figure 23.

Figure 23 Clock Configuration

HH:MM:SS

Range: The value of HH ranges from 0 to 23, and that of MM and SS ranges from 0 to 59.

YYYY.MM.DD

Range: The value of YYYY ranges from 1970 to 2099, that of MM from 1 to 12, and that of DD from 1 to 31.

Description: The range of DD varies with month. For example, the range of DD for March is from 1 to 31, and that for April is from 1 to 30. You can configure it according to the actual situation.

Timezone

Function: Select the local timezone.

Daylight Saving Time status

Options: Enable/Disable

Default: Disable

Function: Enable or disable DST. After DST is enabled, clock will be adjusted forward one hour in summer.

Daylight Saving Time

Configure the time segment for DST.

⚠️ CAUTION	**Caution:** ➢ Start time should be different from end time. ➢ Start time indicates non-DST time. End time indicates DST time.

For example, run DST from 10:00:00 April 1st to 9:00:00 October 1st.

Non-DST time will run until 10:00:00 April 1st. Then the clock jumps to 11:00:00 to start DST. DST runs until 9:00:00 October 1st. Then the clock jumps back to 8:00:00 to run non-DST time.

5.2 User Management Configuration

To avoid security problems caused by illegitimate users, the series switches provide hierarchical user management. The switch provides different operation rights based on user levels, satisfying diversified access control requirements. Three user levels are available, as

shown in Table 2.

Table 2 User Level

User Level	Description
Guest	The lowest level, guest users can only view switch configuration, but cannot perform configuration or modification. Guest users cannot access the following functions: software update, user management, file transmission, reboot, save current configuration, and load default.
System	Medium level, system users have certain access and configuration rights. System users cannot access the following functions: software update, user management, file transmission, reboot, and load default. Note: System user can modify password of the current user.
Admin	Highest level, admin users have the rights to perform all functions.

5.2.1 Web Configuration

1. Configure users

Click [Device Basic Configuration] →[User Configuration]→[User Configuration] to enter user configuration page, as shown in Figure 24.

Figure 24 User Configuration

Name

Range: 1~16 characters

Service

Options: console/telnet/ssh/web

Function: Select switch access mode for the current user. One or multiple access modes can be selected.

Level

Option: Guest/System/Admin

Default: Guest

Option: Select user level, users of different levels have different operation rights.

Authen-Type

Option: Password/Key/Password or Key

Default: Password

Function: Selected the authentication type to be used when the current user accesses the switch. When selecting **Password**, you must configure the **Password** option. When selecting Key, you must configure the **Key name** option.

Password

Range: 1~32 characters

Function: Configure the password to be used when the current user accesses the switch.

Key name

Function: Select the key name to be used when current user accesses the switch in ssh mode.

Note:

➤ Currently, console/telnet/web does not support the key-based authentication mode. Therefore, when the service type is console/telnet/web, does not select key-based authentication as the authentication type.

➤ ssh supports two authentication modes, that is, password-based authentication and key-based authentication.

➤ The switch supports a maximum of nine users.

➤ Default user admin cannot be deleted. The default service (console, telnet, ssh, web) and level (administration level) of this user cannot be modified, but the default password (123)

can be modified.

➢ For the switch access mode of console/telnet/web, please see the "1 错误!表格结果无效。"

section.

➢ For the switch access mode of ssh, please see the "5.11 SSH Server Configuration" section.

2. Modify and delete user information

Click the user entry under user configuration list in Figure 24. You can modify and delete the user configuration, as shown in Figure 25.

Figure 25 Modify and Delete User Information

3. Configure SSH Key

Click [Device Basic Configuration] → [User Configuration]→[SSH Key Configuration] to enter SSH key configuration page, as shown in Figure 26.

Figure 26 SSH Key Configuration

Key Name

Range: 1~16 characters

Key Type

Mandatory configuration: RSA

This series switches only support RSA key algorithm.

Key Value

Format: {algorithm name, public key, key info}

Algorithm name: ssh-rsa | ssh-dsa

Public key: it is based on 64 codes and the length is less than 2048 bytes

Key info: more info for the key

Function: Configure the public key corresponding to the client. Generally, the public key is generated by Puttygen software and is copied to the key value of the server, the private key is saved in the client.

4. Modify the password of current user

Click [Device Basic Configuration] →[User Configuration]→[Modify Password] to enter password modification page, as shown in Figure 27.

Figure 27 Modify

New password/Repeat password

Range: 1~32 characters

5. Configure timeouts for switch access modes

Click [Device Basic Configuration] →[User Configuration]→[Timeouts Configuration] to enter password modification page, as shown in Figure 28.

Figure 28 Timeouts Configuration

Time

Range: 0~44640 min

Default: 5 min for console/ssh/telnet; 10 min for web

Function: Configure the login user timeout and disconnection time. The time starts counting when a user finishes all configurations, and the system will automatically exit the access mode when the time ends. When the time is set to 0, the user timeout and disconnection function is disabled. In this case, the server will not judge whether the user login times out and therefore the user will not exit the current login mode.

5.3 Port Configuration

5.3.1 Physical Port Configuration

5.3.1.1 Introduction

In physical port configuration, you can configure the cable type, management status, rate/mode, and other information.

5.3.1.2 Web Configuration

Click [Device Basic Configuration] → [Port configuration] → [Ethernet port configuration] → [Physical port configuration] to enter the port configuration page, as shown in Figure 29.
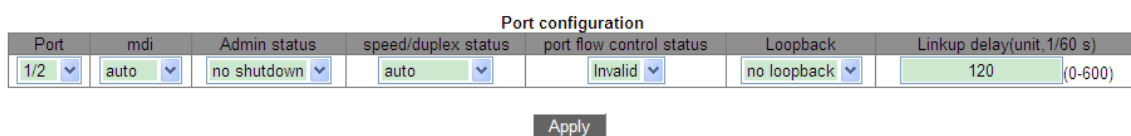
Figure 29 Physical Port Configuration

Port

Options: all switch ports

Description: X/Y is the port name format; X is 1 for this switch, and Y is the port number on the panel.

mdi

Options: auto/normal/across

Default: auto

Function: Configure the cable type for the Ethernet port.

Description: auto means auto-recognition of cable type; across means the port supports only cross-over cable; normal means the port supports only straight-through cable.

Caution:

The auto option is recommended.

Admin Status

Options: shutdown/no shutdown

Default: no shutdown

Function: Allow data transmission on port or not.

Description: no shutdown indicates the port is enabled and permits data transmission; shutdown indicates the port is disabled and disallows data transmission. This option directly affects the hardware status of the port and triggers port alarms.

Speed/duplex status

Options: auto, 10M/Half, 10M/Full, 100M/Half, 100M/Full, 1000M/Half, 1000M/Full

Default: auto

Function: Configure the port speed and duplex mode.

Description: Port speed and duplex mode support auto-negotiation and forced configuration. If it is set to "auto", the port speed and duplex mode will be automatically negotiated according to port connecting status. When the port duplex mode changes from auto-negotiation to forced full duplex or half duplex, the port speed will also be changed to forced mode. It is recommended to set the parameter to auto to avoid the connection problem caused by unmatched port configuration on both ends of link. If you set the port to forced speed or duplex, please ensure the speed or duplex mode configurations on both ends of the connection are the same.

Caution:

➢ The speed/duplex mode of a 10/100Base-TX port can be set to auto, 10M/Half, 10M/Full,

100M/Half, or 100M/Full.

➢ The speed/duplex mode of a 10/100/1000Base-TX port can be set to auto, 10M/Half,

10M/Full, 100M/Half, 100M/Full, 1000M/Half, or 1000M/Full.

port flow control status

Options: Invalid/Valid

Default: Invalid

Function: Enable/Disable the port 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.

Linkup delay

Range: 0~600 (unit: 1/60 s)

Default: 0

Function: Configuration the port linkup delay, please ensure the linkup delay configurations on both ends of the connection are the same.

You can view port information based on Ethernet port configuration and communication conditions, as shown in Figure 30.

Port list

Port	Type	mdi	Status	Admin status	Speed	Mode	Flow control	Loopback	Linkup delay(unit,1/60 s)
1/1	FE	auto	down	no shutdown	auto	auto	Invalid	no loopback	0
1/2	FE	auto	down	no shutdown	auto	auto	Invalid	no loopback	120
1/3	FE	auto	up	no shutdown	auto	auto	Invalid	no loopback	0
1/4	FE	auto	down	no shutdown	auto	auto	Invalid	no loopback	0
1/5	FE	auto	down	no shutdown	auto	auto	Invalid	no loopback	0
1/6	FE	auto	down	no shutdown	auto	auto	Invalid	no loopback	0
1/7	FE	auto	down	no shutdown	auto	auto	Invalid	no loopback	0
1/8	FE	auto	down	no shutdown	auto	auto	Invalid	no loopback	0
1/9	GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	0
1/10	GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	0
1/11	GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	0
1/12	GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	0

Figure 30 Port List

5.3.2 Port Information

Click [Device Basic Configuration] → [Port configuration] → [Port debug and maintenance] → [Show port information] to enter the port information page. It contains the port connecting status, port type, input/output packet statistics, and other information, as shown in Figure 31.

Please select port   1/8 ⌄

Refresh

```
                        Information Display
Ethernet1/8 is up, line protocol is up
Ethernet1/8 is layer 2 port, alias name is (null), index is 8
Hardware is Fast-Ethernet,  address is 00-1E-CD-0F-01-0A
PVID is 1
MTU 10240 bytes, BW 100000 Kbit
Encapsulation ARPA, Loopback  not set
Auto-duplex:  Negotiation  full-duplex,   Auto-speed:  Negotiation
100M bits
FlowControl is off,  MDI type is auto

Input and output rate statistics:
5 minute input rate 2576 bytes/sec, 29 packets/sec
5 minute output rate 1238 bytes/sec, 1 packets/sec
The last 5 second input rate 7450 bytes/sec, 78 packets/sec
The last 5 second output rate 71659 bytes/sec, 86 packets/sec

Input packets statistics:
177281 input packets, 19390123 bytes, 0 no buffer
8590 unicast packets, 7791 multicast packets, 160900 broadcast packets
0 input errors, 0 CRC, 0 frame alignment, 0 overrun, 0 ignored,
0 abort, 0 length error , 0 pause frame

Output packets statistics:
15501 output packets, 14575608 bytes, 0 underruns
14684 unicast packets, 815 multicast packets, 2 broadcast packets
0 output errors, 0 collisions , 0 pause frame

Input and output packets by length:
(64)         bytes:     91383, (65~127)    bytes:     75519,
(128~255)    bytes:      4359,  (256~511)   bytes:     1502,
(512~1023)   bytes:      7828, (1024~10240) bytes:     12191
```

Figure 31 Port Information

5.4 VLAN Configuration

5.4.1 Introduction

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.

5.4.2 Principle

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

Table 3 802.1Q Frame Structure

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

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

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

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

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

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

Note:

➢ VLAN 1 is the default VLAN and cannot be manually created and deleted.

➢ Reserved VLANs are reserved to realize specific functions by the system and cannot be manually created and deleted.

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

5.4.3 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. Port Mode

➢ Access: In access mode, the port must be untag and added to one VLAN; the port cannot be tag and added to any VLAN.

➢ Trunk: In trunk mode, the port must be untag and added to the PVID VLAN; the port can be tag/untag and added to any other VLAN.

3. PVID

Each port has a PVID. When receiving an untagged packet, a port adds a tag to the packet according to the PVID. The default PVID of all ports is 1.

The PVID of an Access port is the ID of VLAN that the port belongs to, and it cannot be configured.

The PVID of a Trunk port can be configured as one of the VLAN IDs allowed through the port.

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

Table 4 Different Processing Modes for Packets

Processing Received Packets		Processing Packets to Be Forwarded	
Untagged packets	Tagged packets	Port Type	Packet Processing
Add PVID tags to packets.	➢ 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	Untag	Forward the packet after removing the tag.
		Tag	Keep the tag and forward the packet.

	VLANs allowed through, discard the packet.		

5.4.4 Web Configuration

1. Create or delete a VLAN.

Click [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Create/Remove VLAN] → [VLAN ID allocation] to enter the VLAN configuration page, as shown in Figure 32.

VLAN ID configuration

VLAN ID(1-4093)	2

Add   Remove

Figure 32 Creating/Deleting a VLAN

VLAN ID

Range: 2~4093. The default VLAN ID is 1.

Function: Use different VLAN IDs to distinguish VLANs.

Description: The series switches support a maximum of 4093 VLANs.

Method: Click <Add> to create a VLAN; click <Remove> to delete the specified VLAN.

2. Configure a VLAN name.

Click [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Create/Remove VLAN] → [VLAN ID attribution configuration] to enter the VLAN name configuration page, as shown in Figure 33.

Modify switch VLAN ID attribution

VLAN ID	2
VLAN Name(1-11 character)	VLAN2
VLAN Type	universal

Apply

Figure 33 VLAN Configuration

VLAN ID

Range: all created VLANs

Function: Input the ID of the VLAN whose name is to be modified.

VLAN Name

Range: 1~11 characters

Function: Input the name of the VLAN with the specified ID.

VLAN Type

Options: universal

Default: universal

After setting is completed, the "VLAN ID Information" page lists the attribute information of all created VLANs, as shown in Figure 34.

VLAN ID information

VLAN ID	VLAN Name	VLAN Type
1	default	universal
2	VLAN2	universal
100	VLAN100	universal
200	VLAN200	universal

Figure 34 VLAN List

3. Configure port mode

Click [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Port type configuration] → [Set port mode (Trunk/Access)] to enter the port type configuration page, as shown in Figure 35.

Port mode configuration

Port	Type
1/1	access

Apply

Figure 35 Port Type Configuration

Port

Options: all switch ports

Type

Options: access/trunk

Default: access

Function: Select the mode for the specified port. Each port supports only one mode.

After setting is completed, the "Port mode configuration" page lists all port types, as shown in Figure 36.

Port mode configuration

Port	Type
1/1	access
1/2	access
1/3	access
1/4	access
1/5	access
1/6	access
1/7	trunk
1/8	access
1/9	access
1/10	access
1/11	access
1/12	access

Figure 36 Port Type Information

4. Allocate ports to the created VLANs.

Click [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Allocate ports for VLAN] → [Allocate ports for VLAN] to enter the Access port VLAN configuration page, as shown in Figure 37.

Allocate ports for VLAN

VLAN ID	2
Ethernet port	1/1
Tag Type	Untag

Add Port   Delete Port

Note:TR : Trunk mode, TG : Tag, S-CH : Serial Card, H-CH : HSR/PRP Card, T-CH : TMS Card

VLAN ID	Name	Type	Media	Port ID
1	default	Static	ENET	1/7(TR) 1/8 1/9 1/10 1/11 1/12
2	VLAN2	Static	ENET	1/1 1/2 1/7(TR|TG)
100	VLAN100	Static	ENET	1/3 1/4 1/7(TR|TG)
200	VLAN200	Static	ENET	1/5 1/6 1/7(TR|TG)

Figure 37 Allocating Access Ports to VLANs

Tag Type

Option: Tag/Untag

Function: Select the type of the port to be added to the VLAN.

Caution:

➢ In access mode, the port must be untag and added to one VLAN.

➢ In trunk mode, the port must be untag and added to the PVID VLAN; the port can be

tag/untag and added to any other VLAN.

5. Configure the PVID for a Trunk port.

Click [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Trunk

port configuration] → [VLAN setting for trunk port] to enter the Trunk port VLAN configuration

page, as shown in Figure 38.

Figure 38 Trunk Port PVID Configuration

Trunk Port

Options: all Trunk ports

Trunk Native VLAN (pvid)

Options: all created VLANs

Default: 1

Function: Configure the PVID for a Trunk port.

Description: No matter whether a port does not exist in a VLAN or exists in a VLAN in the form of Untag/tag, after the PVID is specified, this port will be added to the VLAN in the form of Untag.

Method: Click <Default> to restore the PVID of selected Trunk port to 1.

6. Configure VLANs for a Trunk port, as shown in Figure 39.

Figure 39 Configuring VLANs for a Trunk Port

Trunk Port

Options: all Trunk ports

Tag Type

Option: Tag/Untag

Function: Select the type of the trunk port to be added to the VLAN.

Trunk Allow VLAN List

Options: all created VLANs

Default: all created VLANs

Function: Configure VLANs for the selected Trunk port.

After setting is completed, the VLAN information of all Trunk ports is displayed, as shown in Figure 40.

Trunk Port	Native VLAN	Allow VLAN List(Tag)	Allow VLAN List(Untag)
1/7	1	2;100;200	1
1/9	2	1	2;100

<center>Figure 40 VLAN Configuration of Trunk Ports</center>

7. Configure VLAN ingress rule for a port.

Click [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Enable/Disable VLAN ingress rule] → [Enable/Disable VLAN ingress rule] to enter the VLAN ingress rule configuration page, as shown in Figure 41.

Enable/Disable VLAN ingress rule

Port	1/1 ∨
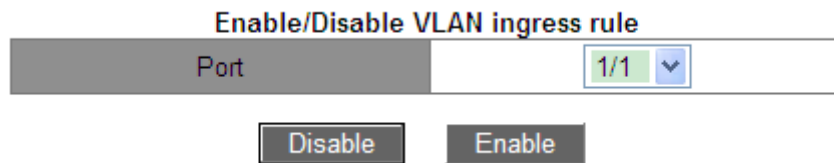
Disable   Enable

<center>Figure 41 Configuring VLAN Ingress Rule</center>

Options: Enable/Disable

Default: Enable

Function: Enable or disable the VLAN ingress rule for a port.

Description: If this function is enabled, the port checks the VLAN ID of a packet against its allowed VLAN list upon receiving the packet. If a match is found, the port forwards the packet; otherwise, the packet is discarded. If this function is disabled, the port forwards all packets without checking their VLAN IDs.

After setting is completed, all VLAN ingress rules information is displayed, as shown in Figure 42.

Port	Type	Ingress Rule
1/1	FE	Disable
1/2	FE	Enable
1/3	FE	Enable
1/4	FE	Enable
1/5	FE	Enable
1/6	FE	Enable
1/7	FE	Enable
1/8	FE	Disable
1/9	FE	Enable
1/10	FE	Enable
1/11	FE	Enable
1/12	FE	Enable

Figure 42 VLAN Ingress Rule Information

8. Configure VLAN-aware

Click [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] →

[VLAN-aware] → [VLAN-aware] to enter the VLAN ingress rule configuration page, as shown

in Figure 43.

VLAN-aware Configuration

VLAN-aware	Aware ∨

Apply   Cancel
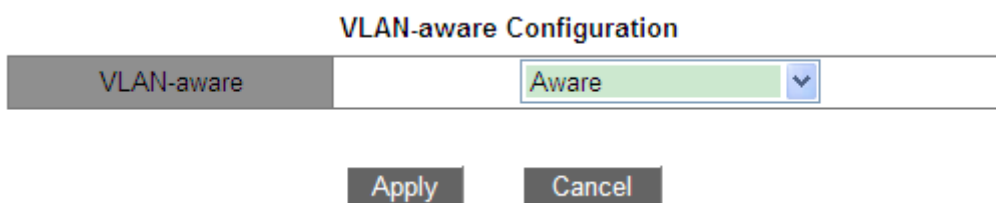
Figure 43 VLAN-aware Configuration

Option: Aware/Unaware

Default: Aware

Function: When Aware is selected, the device identifies and judges the VLAN according to

the IEEE802.1Q protocol and forwards packets properly. When Unaware is selected, the

device does not judge the VLAN ID of an unknown unicast packet and forwards the packet to

any port (broadcast); the device does not judge the VLAN ID of a known unicast packet and

forwards the packet to a relevant port according to the MAC address table.

9. View the information about all created VLANs.

Click [Device Basic Configuration] → [VLAN configuration] → [VLAN debug and

maintenance] → [Show VLAN] to enter the VLAN information page, as shown in Figure 44.

VLAN ID	Name	Type	Media	Portid
1	default	Static	ENET	1/7(TR) 1/8 1/9(TR|TG) 1/10 1/11 1/12
2	VLAN2	Static	ENET	1/1 1/2 1/7(TR|TG) 1/9(TR)
100	VLAN100	Static	ENET	1/3 1/4 1/7(TR|TG) 1/9(TR)
200	VLAN200	Static	ENET	1/5 1/6 1/7(TR|TG)

Figure 44 VLAN Information

5.4.5 Typical Configuration Example

As shown in Figure 45, the entire LAN is divided into 3 VLANs: VLAN2, VLAN100, and VLAN200. It is required that the devices in the same VLAN can communicate with each other, but different VLANs are isolated. The terminal PCs cannot distinguish tagged packets, so the ports connecting Switch A and Switch B with PCs are set to access 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 trunk port, permitting the packets of VLAN 2, VLAN 100, and VLAN 200 to pass through. Table 5 shows specific configuration.

Table 5 VLAN Configuration

VLAN	Configuration
VLAN2	Set port 1/1 and port 1/2 of Switch A and B to untag ports, and port 1/7 to tag port.
VLAN100	Set port 1/3 and port 1/4 of Switch A and B to untag ports, and port 1/7 to tag port.
VLAN200	Set port 1/5 and port 1/6 of Switch A and B to untag ports, and port 1/7 to tag port.
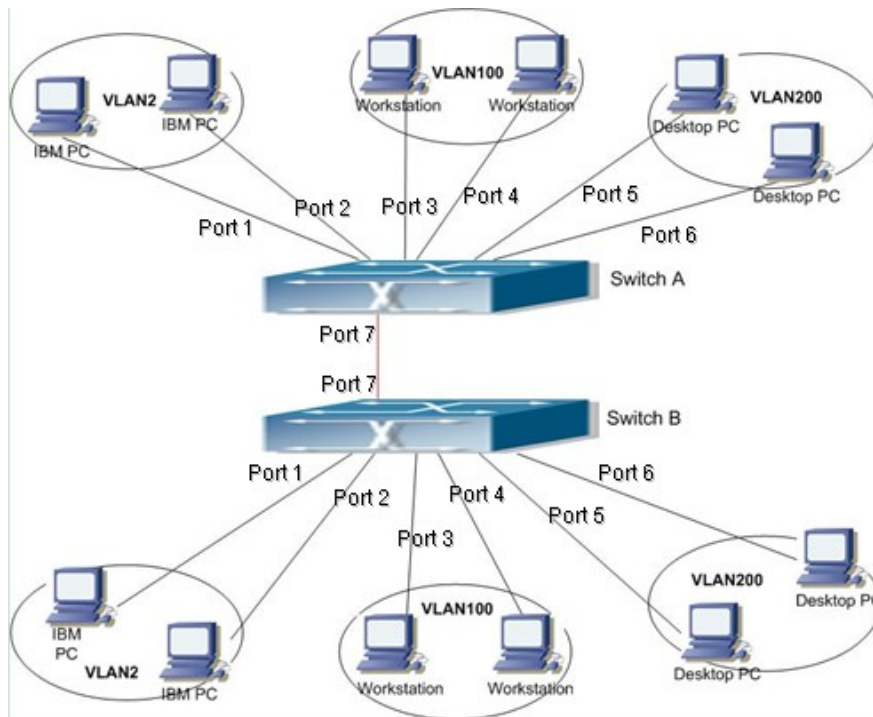
Figure 45 VLAN Application

Configurations on Switch A and Switch B:

1. Create VLAN2, VLAN100, and VLAN200, as shown in Figure 32.

2. Configure ports 1/1, 1/2, 1/3, 1/4, 1/5, 1/6 as Access ports, and port 1/7 as Trunk port, as shown in Figure 35.

3. Add ports 1/1 and 1/2 to VLAN2 as untag ports; ports 1/3 and 1/4 to VLAN100 as untag ports; ports 1/5 and 1/6 to VLAN200 as untag ports; port 1/7 to VLAN2, VLAN100, VLAN200 as tag port, as shown in Figure 37.

5.5 PVLAN Configuration

5.5.1 Introduction

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

The upper VLAN is a shared domain VLAN in which ports are uplink ports. The lower VLANs are isolation domains in which ports are downlink ports. Downlink ports can be assigned to different isolation domains and they can communicate with uplink port at the same time. Isolation domains cannot communicate to each other.
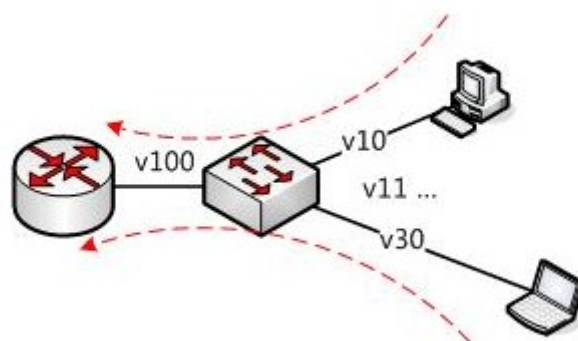
Figure 46 PVLAN Application

As shown in Figure 46, the shared domain is VLAN100 and the isolation domains are VLAN 10 and VLAN 30; the devices in the isolation domains can communicate with the device in the share domain, such as VLAN 10 can communicate with VLAN 100; VLAN 30 can also communicate with VLAN 100, but the devices in different isolation domains cannot communicate with each other, such as VLAN 10 cannot communicate with VLAN 30.

5.5.2 Explanation

PVLAN function can be implemented through special configuration on ports.

➢ The PVID of uplink ports are the same as shares domain VLAN ID; the PVID of downlink ports are the same as their own isolation domain VLAN ID.

➢ The uplink ports are set to untag and are assigned to the shares domain VLAN and all isolation domains; the downlink ports are set to untag and are assigned to the shared domain VLAN and own isolation domain.

5.5.3 Typical Configuration Example

Figure 47 shows PVLAN application. VLAN300 is a shared domain and port 1 and port 2 are uplink ports; VLAN100 and VLAN200 are isolation domains and ports 3, 4, 5, and 6 are downlink ports.
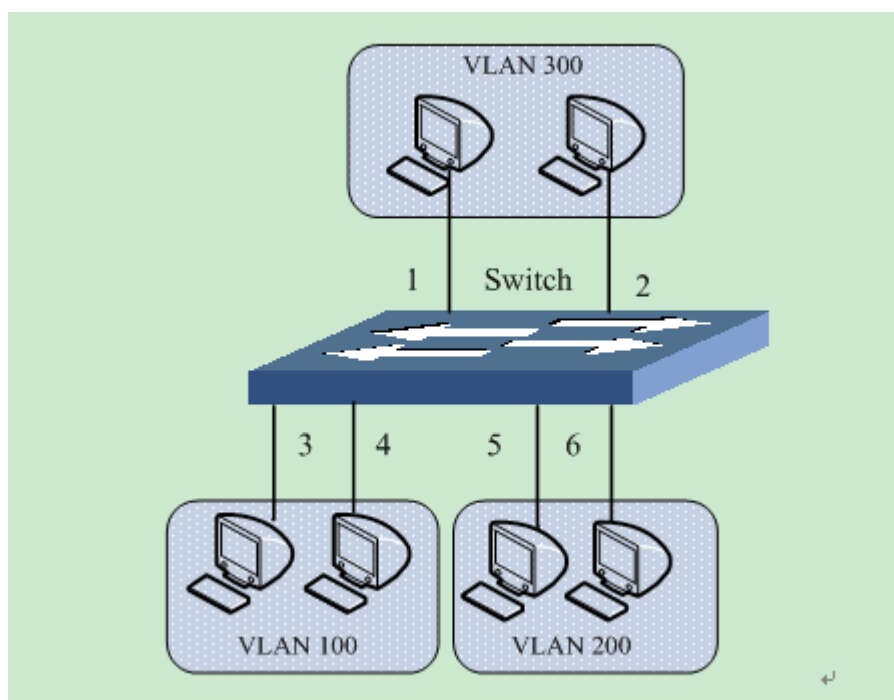
Figure 47 PVLAN Configuration Example

Switch configuration:

1. Create VLAN300, VLAN 100, and VLAN 200, as shown in Figure 32.

2. Configure ports 1, 2, 3, 4, 5, 6 as trunk ports, as shown in Figure 35.

3. Add ports 1~6 to VLAN300 as untag ports; ports 1~4 to VLAN100 as untag ports; ports 1, 2, 5, 6 to VLAN200 as untag ports, as shown in Figure 37.

4. Configure the PVID of ports 1 and 2 to 300; the PVID of ports 3 and 4 to 100; the PVID of ports 5 and 6 to 200, as shown in Figure 38.

5.6 Port Mirroring

5.6.1 Introduction

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.

5.6.2 Explanation

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:**
>
> ➢ Mirroring destination port and port channel are mutually exclusive. The mirroring destination port cannot be added to a port channel, and the port in a port channel cannot be set to a mirroring destination port.
>
> ➢ Mirroring destination port and redundant port are mutually exclusive. The mirroring destination port cannot be set to a redundant port, and a redundant port cannot be set to a mirroring destination port.
>
> ➢ Redundant port in this document refers to DT-Ring ring port, DT-Ring backup port, DRP ring port, DRP backup port, RSTP port, and MSTP port.

5.6.3 Web Configuration

1. Select the mirroring source port and mirroring mode.

Click [Device Basic Configuration] → [Port mirroring configuration] → [Mirror configuration] to enter the mirroring source port configuration page, as shown in Figure 48.

Port mirroring configuration

Session	1
Mirror direction	rx
Source port	1/1

Reset   Apply   Del

Figure 48 Mirroring Source Port Configuration

Session

Option: 1~7

Default: 1

Function: Select a mirroring group.

Mirror Direction

Options: rx/tx/both

Default: both

Function: Select the data to be mirrored in the mirroring source port.

Description: rx indicates only the received packets are mirrored in the source port.

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

Both indicates both transmitted and received packets are mirrored in the source port.

Source port

Options: all switch ports

Function: Select the mirroring source port. You can select multiple source ports.

2. Select the mirroring destination port, as shown in Figure 49.

Figure 49 Mirroring Destination Port Configuration

Session

Option: 1~7

Default: 1

Function: Select a mirroring group.

Destination port

Options: all ports other than the source port

Function: Select the mirroring destination port.

Description: Set a port to a mirroring destination port. There is only one mirroring destination port. The mirroring destination port cannot be a member of a port channel. It is better that the throughput of the destination port is larger than or equal to the total throughputs of its source ports.

5.6.4 Typical Configuration Example

As shown in Figure 50, 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.
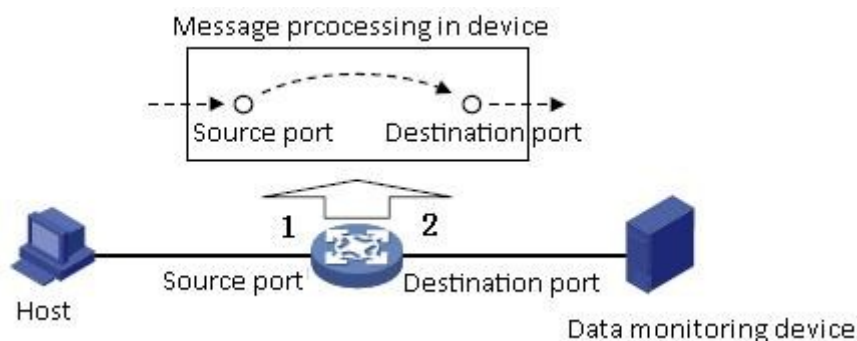
Figure 50 Port Mirroring Example

Configuration process:

1. Set port 2 to the mirroring destination port, as shown in Figure 49.

2. Set port 1 to the mirroring source port and the port mirroring mode to both, as shown in

Figure 48.

5.7 Port Storm Control

5.7.1 Introduction

Port storm control is to limit the port-received broadcast/multicast/unknown unicast packets.

When the rate of broadcast/multicast/unknown unicast packets received on the port exceeds

the configured threshold, the system will discard excess broadcast/multicast/unknown

unicast packets to keep the broadcast/multicast/unknown unicast traffic within the allowable

range, ensuring normal network operation.

5.7.2 Web Configuration

1. Configure the port storm control threshold.

Click [Device Basic Configuration] → [Port Storm Suppression configuration] → [Port Storm

Suppression configuration] to enter the configuration page, as shown in Figure 51.

Figure 51 Port Storm Control Threshold Configuration

Port name

Options: all switch ports

Function: Select the ports that need rate limiting.

Rate Unit:

Options: bps/kbps/percent

Function: Select the unit of the threshold.

Rate Value:

Range: 1~1000000kbps/1~1000000000bps/1~100 Percent

Default: 0, when the value is 0, port storm control is disabled.

Function: Configure the threshold for port rate limiting and the packets that exceed the threshold will be dropped. The value range depends on the actual port speed. For details, see Table 6.

Description: The threshold of Fast Ethernet port is in the range of 1~100000kbps/1~100000000bps; the threshold of Gigabit Ethernet port is in the range of 1~1000000kbps/1~1000000000bps. Percent corresponds to the port bandwidth, for example, if the rate limiting value of a 100M port is 60%, the port begins to discard data after receiving 60M data traffic.

Table 6 Value Range of Port Rate Threshold

Port Rate	Threshold Unit	Step	Value Range
10M	bps	512	512~10000000
	kbps	Not recommended	Not recommended
100M	bps	5120	5120~100000000
	kbps	5	5~100000
1000M	bps	51200	51200~1000000000

	kbps	50	50~1000000

2. Select the type of packets to be controlled, as shown in Figure 52.

Figure 52 Configuring the Packets to Be Controlled

Port name

Options: all ports on which port storm control is enabled

Suppression Type

Options: Multicast/broadcast/dlf

Function: Select the type of packets to be controlled.

Function

Options: Enable/Disable

Default: Disable

Function: Enable or disable the control on the type of packets.

Note:

On each port, only one threshold can be configured. The threshold takes effect on the

configured packet type.

5.7.3 Typical Configuration Example

Enable the unknown multicast storm control on port 1/1 with the bandwidth threshold of 1000kbps.

Configuration process:

1. Select port 1/1 and set rate unit to kbps and rate value to 1000kbps, as shown in Figure 51.

2. Set packet type to multicast, as shown in Figure 52.

5.8 Port Isolation

5.8.1 Introduction

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. User only needs to add port to 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.
>
> ➢ One device supports a maximum of 14 isolation groups, and there is no limit to the number of Ethernet ports in each group.
>
> ➢ 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.
>
> ➢ Isolated port and port channel are mutually exclusive. The port of isolation group cannot be added to a port channel, and the port in a port channel cannot be added to an isolation group.
>
> ➢ It is not recommended that ports in an isolation group are configured as redundant ports at the same time, and redundant ports cannot be added to an isolation group.

5.8.2 Web Configuration

Enable the port isolation, as shown in Figure 53.

Figure 53 Port Isolation Configuration

Port isolate

Options: Enable/Disable

Default: Disable

Function: Enable or disable the port isolate.

> **Caution:**
>
> One port is added to only one isolation group.

5.8.3 Typical Configuration Example

Connect PC1, PC2, and PC3 to the Ethernet port 1, 2, and 3 of the switch, and connect port 4 to the external network. Ports 1, 2, 3, and 4 are in the VLAN 1. PC1, PC2, and PC3 cannot communicate with each other, but they can access the external network, as shown in Figure 54.
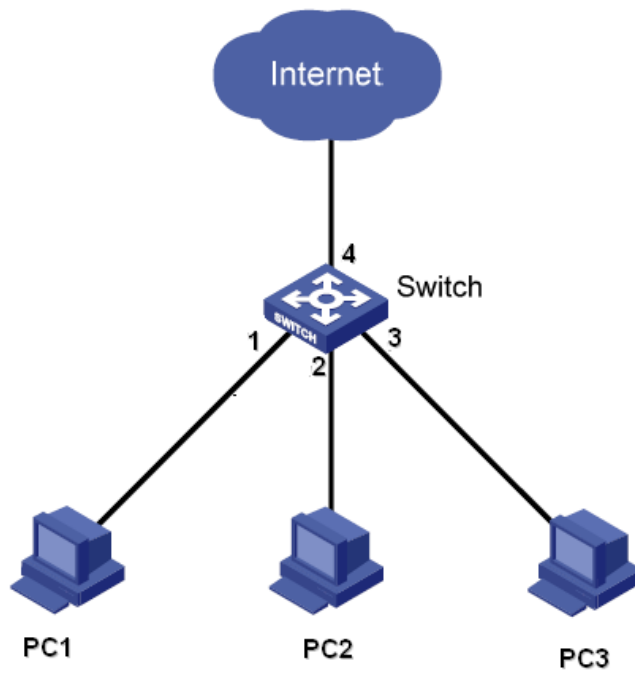
Figure 54 Port Isolation configuration Instance

Add port 1, 2, and 3 to the isolation group to isolate PC1, PC2, and PC3, as shown in Figure 53.

5.9 Port Channel

5.9.1 Introduction

Port channel is to bind a group of physical ports that have the same configuration to a logical port to increase bandwidth and improve transmission speed. The member ports in a same group share traffic and serve as dynamic backups for each other, improving connection reliability.

Port group is a physical port group on the configuration layer. Only the physical ports that join in port group can participate in link aggregation and become a member of port channel. When physical ports in a port group meet certain conditions, they can conduct port aggregation and form a port channel and become an independent logical port, thereby increasing network bandwidth and providing link backup.

5.9.2 Implementation

As shown in Figure 55, three ports on Switch A and Switch B aggregate to form a port

channel. The bandwidth of the port channel is the total bandwidth of these three ports.
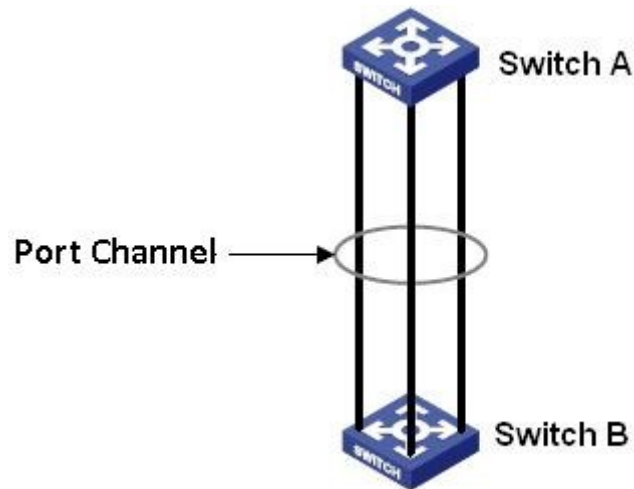
Figure 55 Port Channel

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

5.9.3 Explanation

The series switches support a maximum of 8 port groups and each group contains a maximum of 8 member ports.

Caution:

➢ A port can be added to only one port group.

➢ Port channel and isolated port are mutually exclusive. The port in a port channel cannot be added to an isolation group; the port of isolation group cannot be added to a port channel.

➢ Port channel and mirroring destination port are mutually exclusive. The port in a port channel cannot be configured as a mirroring destination port; the mirroring destination port cannot be added to a port channel.

➢ Port channel and redundant port are mutually exclusive. The port in a port channel cannot be configured as a redundant port, and a redundant port cannot be added to a port channel.

5.9.4 Web Configuration

1. Configure load sharing mode of port channel.

Click [Device Basic Configuration] → [Port channel configuration] → [LACP port group configuration] to enter the configuration page, as shown in Figure 56.

Load balance mode configuration

Load balance mode	mac-only ▾

Apply
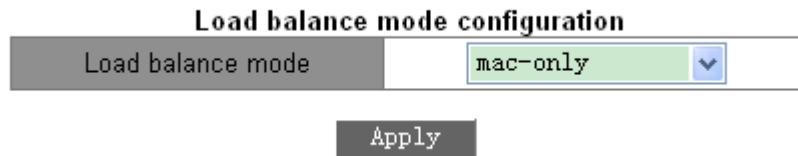
Figure 56 Load Sharing Mode Configuration

Load balance mode

Options: mac-only/ip-only/mac-ip/ip-l4/mac-ip-l4

Default: mac-only

Function: Set the load sharing mode of port channel.

Description: mac-only indicates MAC address-based load sharing.

ip-only indicates IP address-based load sharing.

mac-ip indicates load sharing based on MAC address and IP address.

ip-l4 indicates load sharing based on IP address and TCP/UDP port number.

mac-ip-14 indicates load sharing based on MAC address, IP address, and TCP/UDP port number.

Explanation: If load sharing mode needs to be changed after a port channel is formed, the change will take effect after the next aggregation.

2. Create or delete a port group, as shown in Figure 57.

LACP port group configuration

LACP group number(1-8)	
Operation type	Add port group ▾

Apply
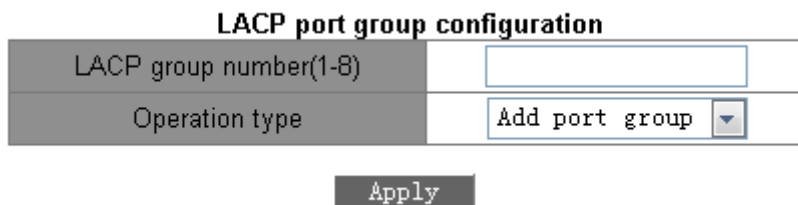
Figure 57 Port Channel Configuration

LACP group number

Range: 1~8

Function: Set the port group number with a maximum of 8 port groups.

Operation type

Options: add port group/remove port group

Default: add port group

Function: Create or delete a port group.

After setting is completed, the "port group table" page lists all created port groups and load sharing modes, as shown in Figure 58.

port group table

port group	load balance
3	mac-only
2	mac-only
1	mac-only

Figure 58 Port Group List

3. Configure a port group member.

Click [Device Basic Configuration] → [Port channel configuration] → [LACP port configuration] to enter the configuration page, as shown in Figure 59.

LACP Port configuration

LACP group number(1-8)	2
Port	1/1
Operation type	Add port to group

Apply

Figure 59 Port Group Member Configuration

LACP group number

Options: all created port group numbers

Port

Options: all switch ports

Function: Select the port to be added to or deleted from a port group.

Description: The member ports in a same port group have the same port attributes.

Operation type

Options: Add port to group/Remove port from group

Default: Add port to group

Function: Add a port to or remove a port from a port group.

5.9.5 Typical Configuration Example

As shown in Figure 55, add three ports (port 1, 2, and 3) of Switch A to port group 1 and three ports (port 1, 2, and 3) of switch B to port group 2. Use network cables to connect these ports to form a port channel, realizing load sharing among ports. (It is assumed that the three ports on Switch A and B have the same attributes respectively.)

Configuration on switches:

1. Add port group 1 on Switch A, as shown in Figure 57.

2. Add port 1, 2, and 3 to port group 1, as shown in Figure 58.

3. Add port group 2 on Switch B, as shown in Figure 57.

4. Add port 1, 2, and 3 to port group 2, as shown in Figure 58.

5.10 Telnet Server Configuration

5.10.1 Introduction

Telnet is a protocol for accessing remote terminals. You can log in to a remote host by using the IP address or host name through Telnet.   Telnet can transmit your commands to the remote host and return the output of the remote to your display through TCP.

Telnet adopts the client/server mode. The local system is the client, while the remote host is the server. This series switches can serve as a Telnet server or client.

When a switch serves as a Telnet server, you can log in to the switch by using the Telnet client software in the Windows or other OSs. When the switch serves as a Telnet server, it can establish TCP connections with a maximum of 5 Telnet clients.

When the switch serves as a Telnet client, you can use Telnet commands in the general view to log in to other remote hosts. When serving as a Telnet client, the switch can establish TCP connection with only one remote host. To establish TCP connection with another host, the switch must disconnect the connected host first.

5.10.2 Web Configuration

1. Enable the Telnet server function.

Click [Device Basic Configuration] → [Telnet server configuration] → [Telnet server user configuration] to enter telnet server configuration page, as shown in Figure 60.

Telnet Server Configuration

Telnet server State	Open ▾

Apply

Figure 60 Telnet Server Configuration

Telnet server state

Configuration items: open/close

Default: open

Function: Enable or disable the Telnet server function.

Description: Open means that Telnet clients can log in to the switch. Close means that Telnet clients cannot log in to the switch.

> **Note:**
>
> The switch can work as a Telnet client to log in to a remote host regardless of whether the function is enabled.

2. Configure security IP address for Telnet client login.

Click [Device Basic Configuration] → [Telnet server configuration] → [Telnet security IP] to enter security IP address configuration page, as shown in Figure 61.

Telnet server Security IP

Security IP address	192.168.1.32

Add   Del

Figure 61 Telnet Server Security IP

Security IP address

Format: A.B.C.D

Function: Configure security IP address for Telnet client login when the switch works as a Telnet server.

Description: If the security IP is not set, there is not restriction on Telnet client's IP address. After the security IP addresses are set, only the client with a security IP address can log in to and configure the switch by Telnet.

A switch allows a maximum of 32 security IP addresses. By default, no security IP address is configured.

After setting is completed, the "Telnet server Security IP list" displays Telnet client IP addresses that can log in to the switch, as shown in Figure 62.

Telnet server Security IP list
192.168.1.30
192.168.1.31
192.168.1.32
192.168.1.33
192.168.1.34
192.168.1.35

Figure 62 Security IP Address List

5.11 SSH Server Configuration

5.11.1 Introduction

SSH (Secure Shell) is a network protocol for secure remote login. It encrypts all transmitted data to prevent information disclosure. When data is encrypted by SSH, users can only use command lines to configure switches.

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

5.11.2 Secret Key

The unencrypted message is called plaintext, and the encrypted message is called cipher text. Encryption or decryption is under the control of the secret key. A secret key is a specific character string and is the only parameter to control the transformation between plain text

and cipher text, working as a Key. Encryption can change plain text to cipher text, while decryption can change cipher text to plain text.

The key-based security authentication needs secret keys, and each end of the communication has a pair of secret keys, private key and public key. Public key is used to encrypt data, and the legal owner of private key can use the private key to decrypt the date to guarantee the data security.

5.11.3 Implementation

In order to realize the SSH secure connection in the communication process, the server and the client experience the following five stages:

Version negotiation stage: currently, SSH consists of two versions: SSH1 and SSH2. The two parties negotiate a version to use.

Key and algorithm negotiation stage: SSH supports multiple types of encryption algorithms. The two parties negotiate an algorithm to use.

Authentication state: the SSH client sends an authentication request to the server and the server authenticates the client.

Session request stage: the client sends a session request to the server after passing the authentication.

Session stage: the client and the server start communication after passing the session request.

5.11.4 Web Configuration

➢ SSH server configuration steps:

Click [Device Basic Configuration] → [SSH Server Configuration] → [SSH server configuration] to enter the SSH server configuration page.

1. Disable SSH status.

2. Click <Destroy> to destroy the old key pair, as shown in Figure 63.
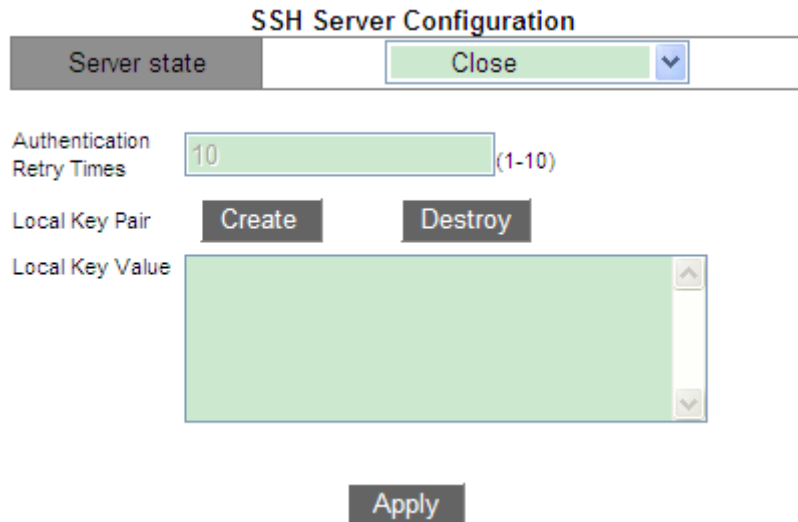
Figure 63 Destroy the Old Key Pair

3. Click <Create> to create a new key pair.

4. Enable SSH protocol and configure the SSH server, as shown in Figure 64.
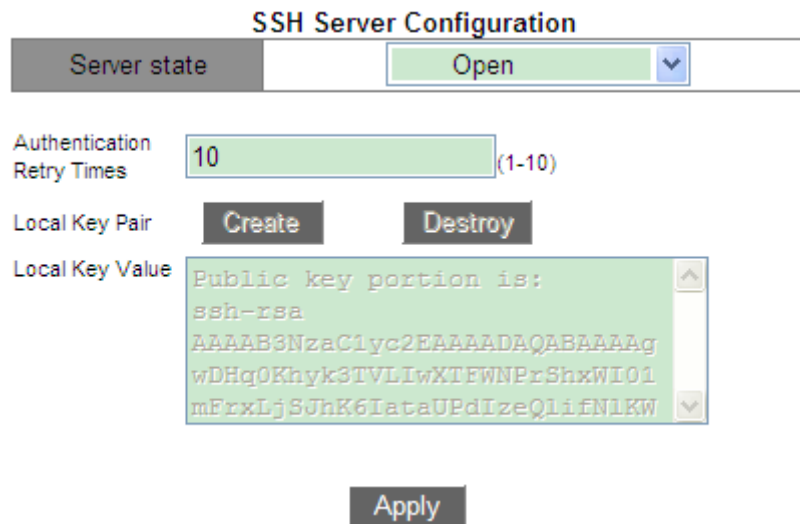
Figure 64 SSH Server Configuration

Server state

Option: Open/Close

Default: Close

Function: Enable/Disable SSH protocol. If it is enabled, the switch works as the SSH server.

Authentication Retry Times

Configuration range: 1~10

Default: 10

Function: set the number of attempts to log into SSH server.

Local Key Pair

Configuration options: Create/Destroy

Function: create or destroy the local key pair of the SSH server. Please create a local key pair before enabling SSH server; destroy the old key pair before creating a new key pair.

Local Key Value

Function: show the local key value. Click <Create> to automatically generate the key value.

➢ Configure security IP address for SSH client login.

Click [Device Basic Configuration] → [SSH Server Configuration] → [SSH security IP] to enter security IP address configuration page, as shown in Figure 65.
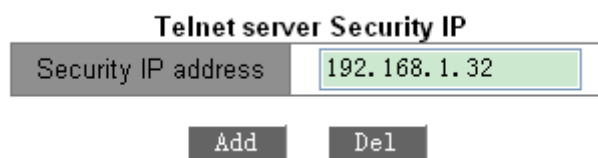
SSH Server Security IP

Security IP Address	192.168.0.184

Add   Del

SSH Server Security IP List
192.168.0.23

Figure 65 SSH Sever Security IP Configuration

Security IP Address

Format: A.B.C.D

Function: Configure security IP address for SSH client login when the switch works as a SSH server. If the security IP is not set, there is not restriction on SSH client's IP address. After the security IP addresses are set, only the client with a security IP address can log in to and configure the switch by SSH.

Explanation: A switch allows a maximum of 6 security IP addresses. By default, no security IP address is configured.

5.11.5 Typical Configuration Example

The Host works as the SSH client to establish a local connection with switch, as shown in

Figure 66.
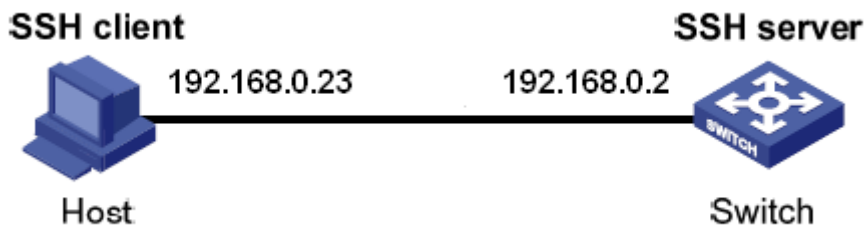
Figure 66 SSH Configuration Example

➢ SSH user chooses the authentication type of "password".

1. Destroy the old key pair of the server, create a new key pair and start SSH server, see Figure 63, Figure 64.

2. Set SSH user name to 333, service to SSH, authen-type to password, password to 333, see Figure 24.

3. Establish the connection with the SSH server. First, run the PuTTY.exe software, as shown in Figure 67; input the IP address of the SSH server "192. 168.0.2" in the space of Host Name (or IP address).
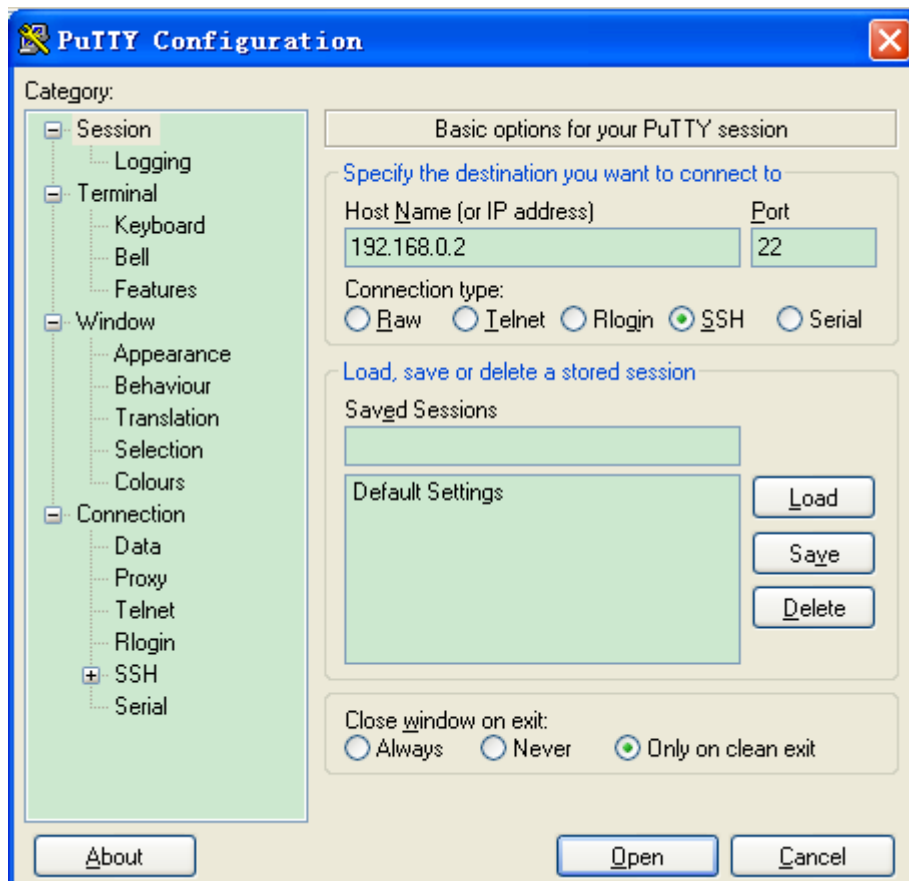
Figure 67 SSH Client Configuration

4. Click <Open> button and following warning message appears shown in Figure 68, click

the <是(Y)> button.
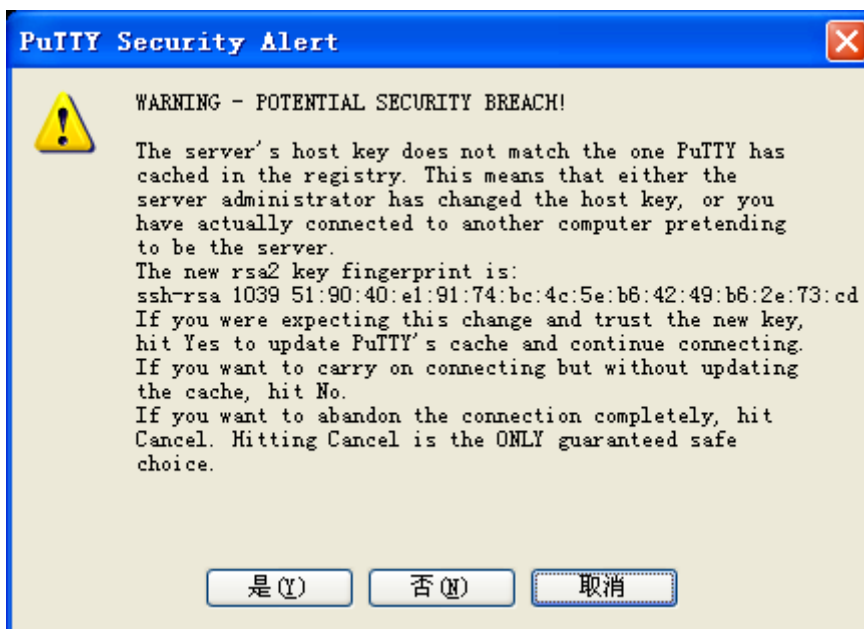
Figure 68 Warning Message

5. Input the user name "333" and the password "333" to enter the switch configuration

interface, as shown in Figure 69.

Figure 69 Login Interface of the SSH Password Authentication

➢ SSH user chooses the authentication type of "Key".

1. Destroy the old key pair of the server, create a new key pair and start SSH server, see Figure 63, Figure 64.

2. Configure SSH client, see Figure 26, run PuTTYGen.exe in the client, click <Generate> button to generate the client key pair, as shown in Figure 70.
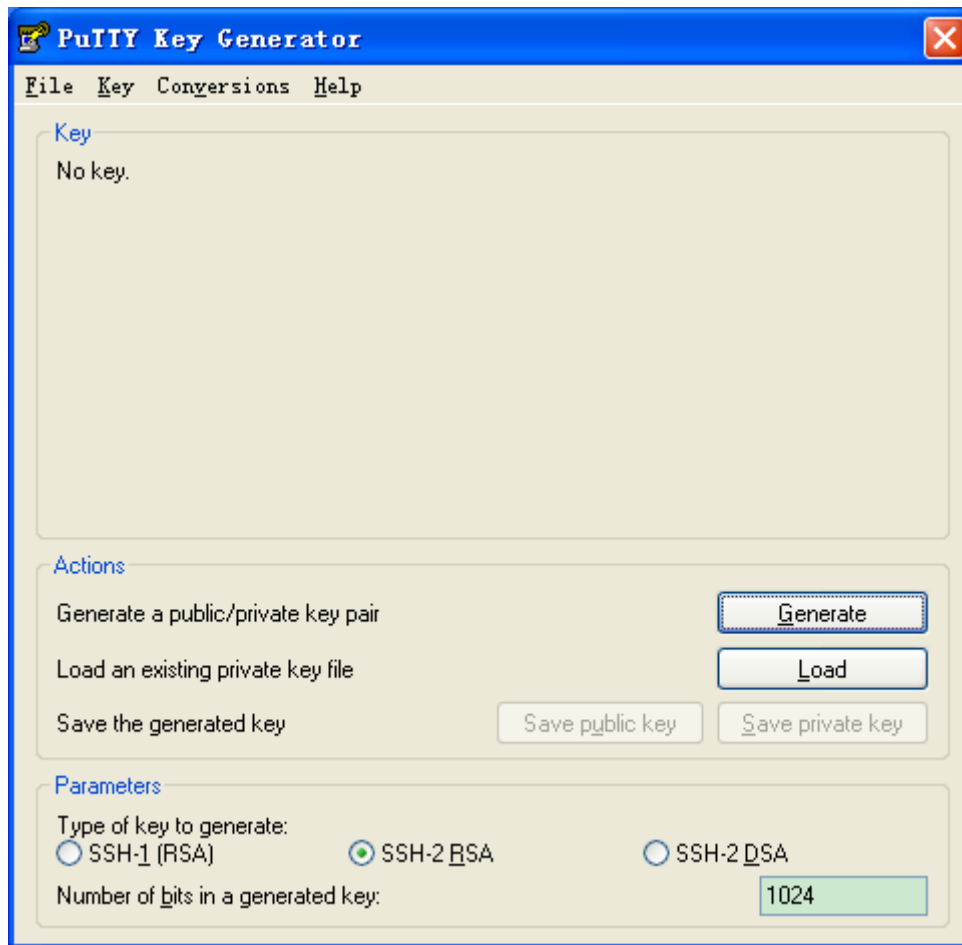
Figure 70 Generate the Client Key

3. In the generation process, please move the mouse in the screen, otherwise, the progress bar does not move forward and the generation stops, as shown in Figure 71.
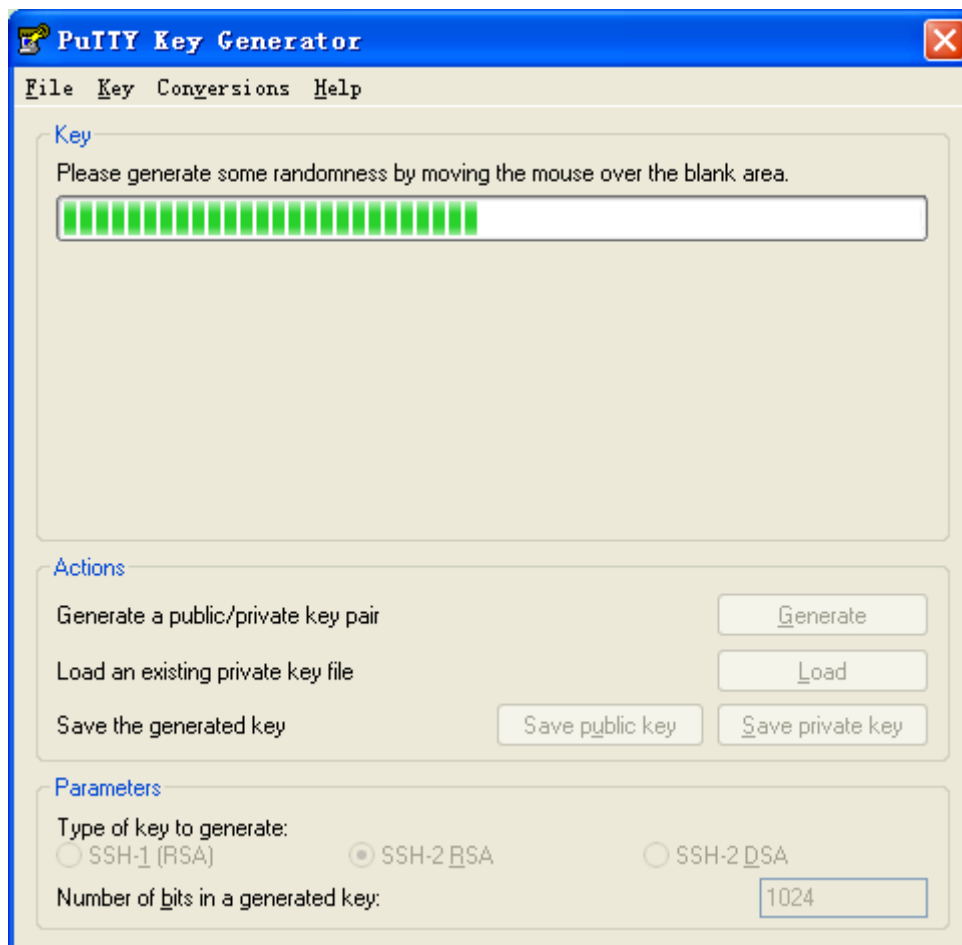
Figure 71 Key Generation

4. As Figure 72 shows, click <Save private key> to save the private key as 444.ppk, and copy the public key to the space of Key Value in the SSH Key Configuration interface and input the key name 444, as shown in Figure 26.
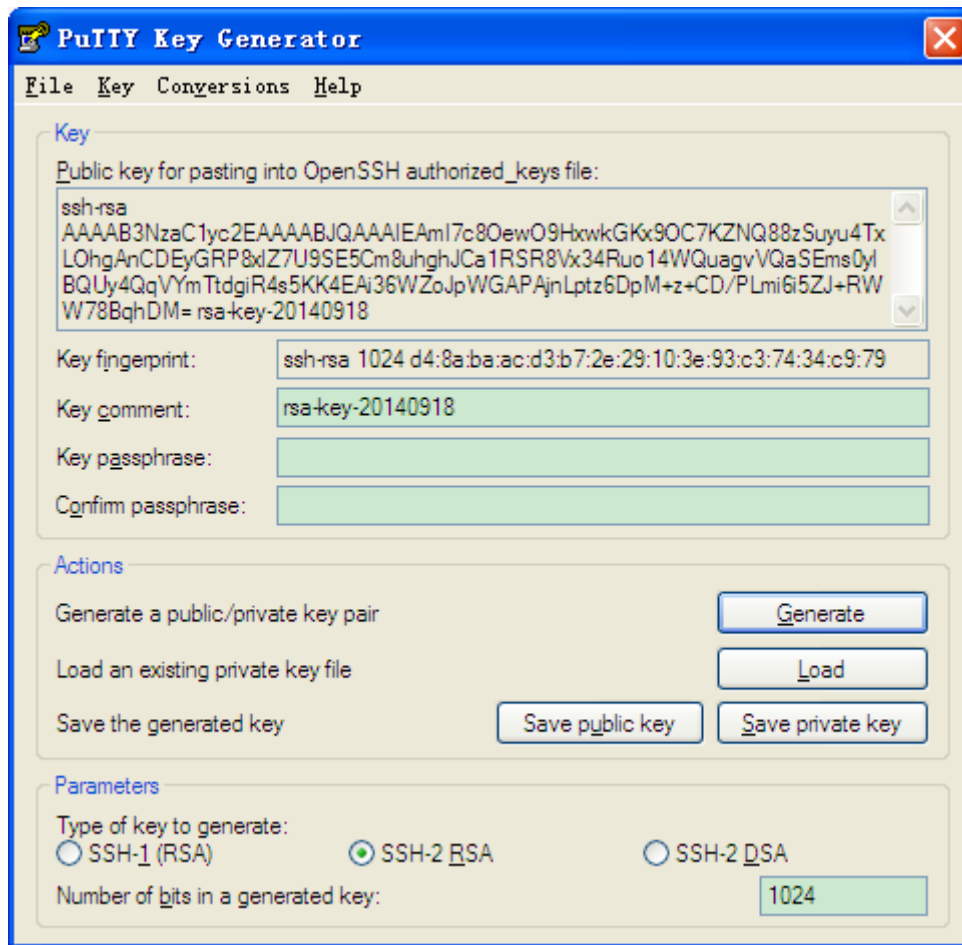
Figure 72 Generate the Key Value

5. Set SSH user name to 444, service to SSH, authen-type to key, key name to 444, see Figure 24

6. Establish a connection with the SSH server. First, run the PuTTY.exe software, as shown in Figure 73; input the IP address of the SSH server "192.168.0.2" in the space of Host Name (or IP address).
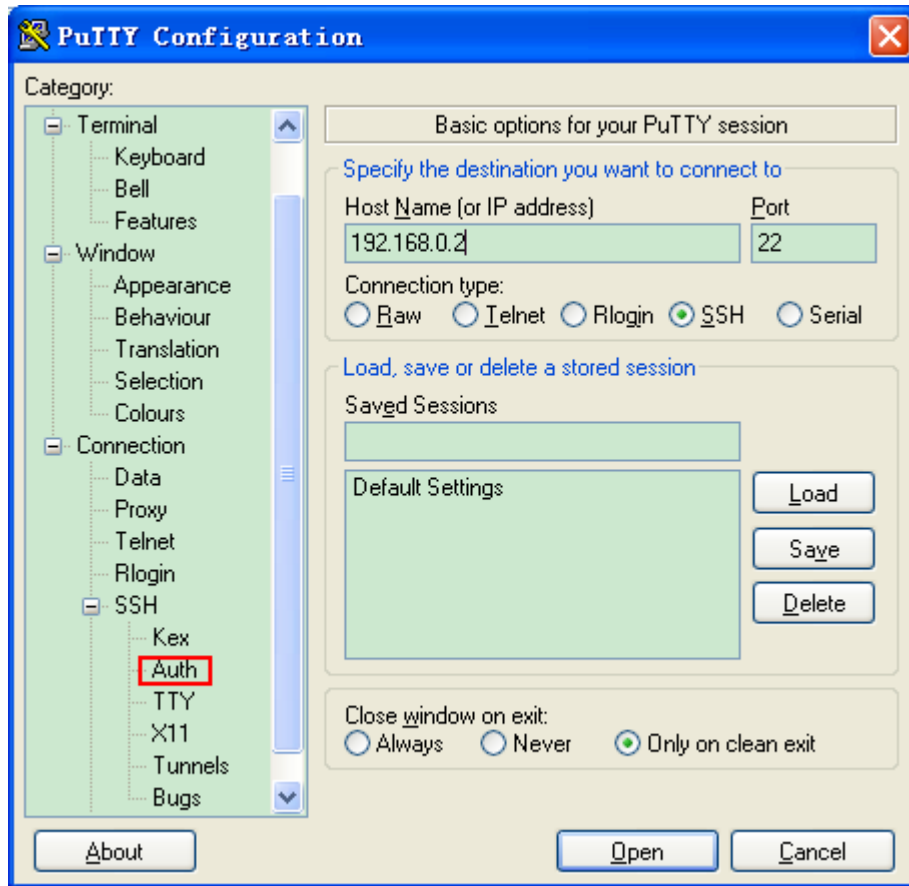
Figure 73 SSH Client Configuration of the "key" Authentication

7. Click [SSH] →[Auth] in the left side of the Figure 73, and the screen shown in Figure 74 appears, click <Browse> and choose the private file saved in the step 4.
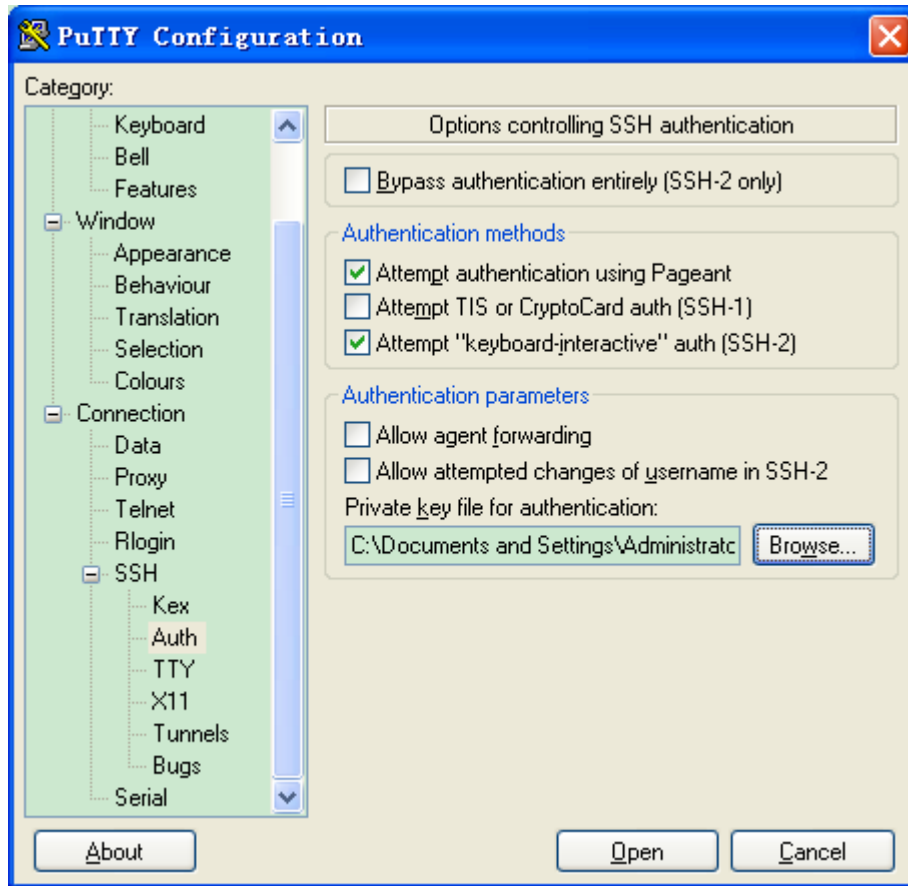
Figure 74 Choose the Key File

8. Click <Open> button; input the user name to enter the switch configuration interface, as shown in Figure 75.
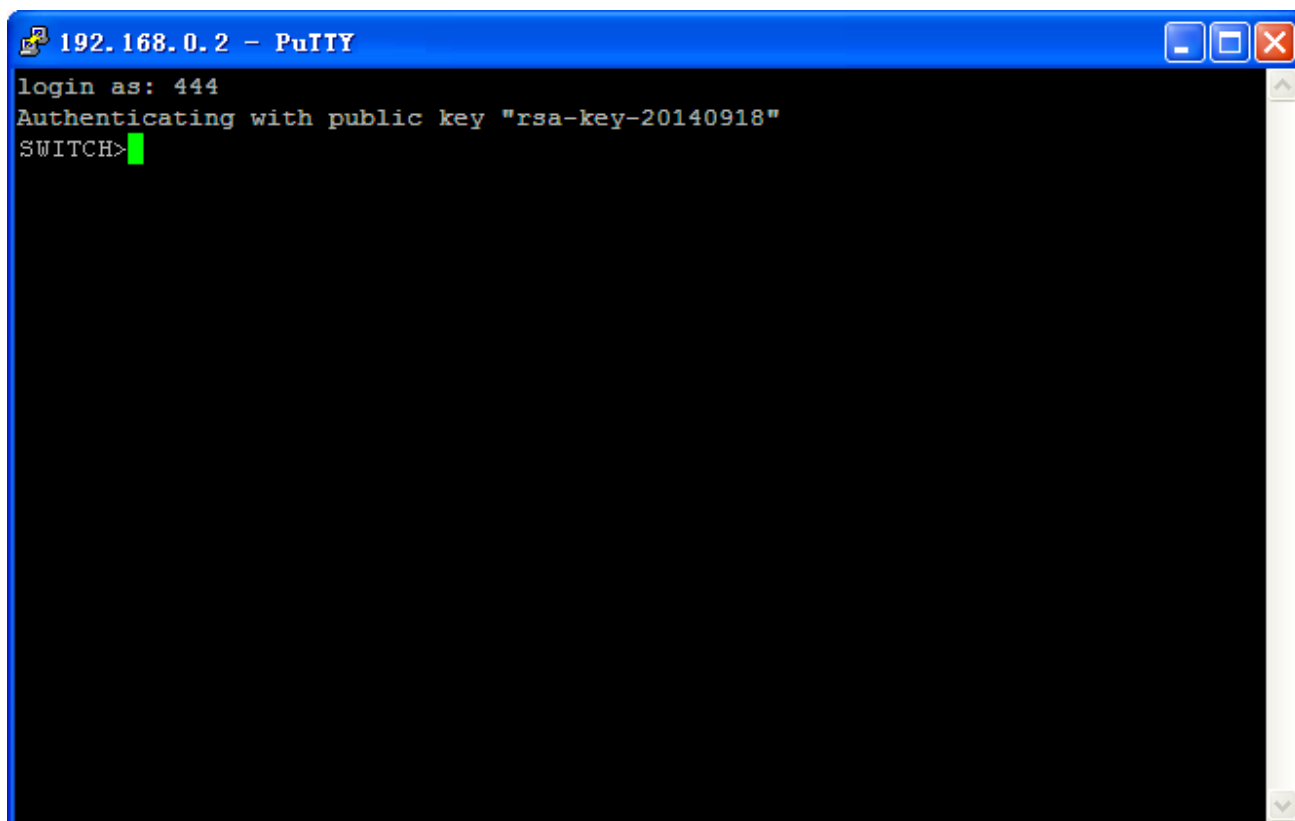
Figure 75 Login Interface of the SSH Public Key Authentication

5.12 SSL Configuration

5.12.1 Introduce

SSL (Secure Socket Layer) is a security protocol and provides the security link for the TCP-based application layer protocol, such as HTTPS. SSL encrypts the network connection at the transport layer and uses the symmetric encryption algorithm to guarantee the data security, and uses the secret key authentication code to ensure the information reliability. This protocol is widely used in Web browser, receiving and sending emails, network fax, real time communication, and so on, providing an encryption protocol for the security transmission in the network.

Once a switch enables SSL, users must use the secure link https, such as https://192.168.0.2, to access the switch.

5.12.2 Web Configuration

1. Enable HTTPS protocol

74

Click [Device Basic Configuration] → [SSH configuration] → [SSH Configuration] to enter the SSL configuration page, as shown in Figure 76.
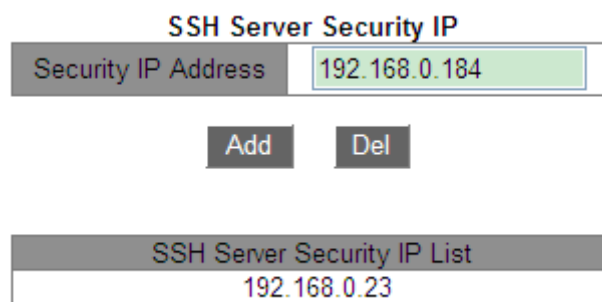
SSL Configuration

Server state	Enable ▾

Apply

Certificate	mgCM+YoP6kt4Zkj2z5IRfm7WrycKsnpnOR+tGeqAjkCe Z6/36o9191RvPnN1VJ/i xQv2df0KFeMr00IkDdTNAdIWqFkSsZTAY2QAdgenb7MB 1joejquYzO2DQIO7+wpH irObpESxAZLySCmPPg==

Private key	rHuDo6bgpjUAAXM+v3fcpsfZSNO6V7kCIQCtbVjanpUw vZkMI9by02oUk9taki3b PzPfAfNPYAbCJQIhAJXNQDWyqwn/1GmR11cqY2y9nZ1+ 5w3yHGatLrcDnQHxAiEA vnlEGo8K85u+KwIOimM48ZG8oTk7iFdkqLJR1utT3aU=

Add

Figure 76 Enable HTTPS Protocol

Server state

Option: Enable/Disable

Default: Disable

Function: Enable or disable the SSL protocol.

Explanation: After enabling SSL, users must use the secure link https://*ip address* to access the switch.

Certificate/Private key

Function: Input correct certificate and private key, then click <Add> button to import them to switch.

⚠ **Caution:**
CAUTION
The default certificate and private key provided by the company have already been imported to the switch. Users can enable SSL protocol directly and access the switch in HTTPS mode.

2. Input the username and password to successfully log into switch through HTTPS.

5.13 File Transmission Service

File transmission service enables mutual file backup between the server and the client. When a file on the server (or client) is changed, you can obtain the backup file from the client (or server) through FTP or TFTP.

The switch can serve as the client or server to upload and download files through FTP or TFTP.

5.13.1 TFTP Service

1. The switch works as the TFTP client.

➢ First, install TFTP server, as shown in Figure 77. In Current Directory, browse the file storage path in use. Input the server IP address in Server interface.
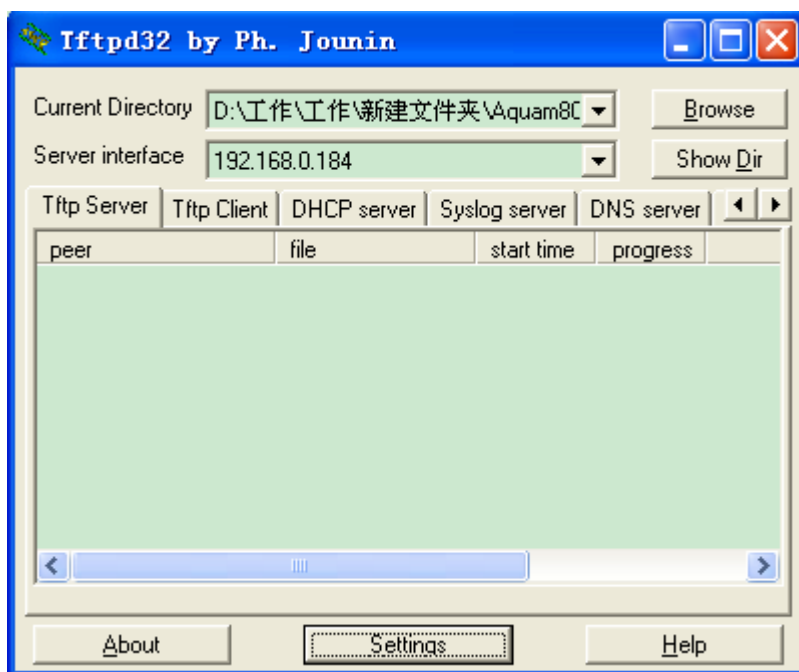
Figure 77 TFTP Server Configuration

➢ Click [Device Basic Configuration] → [File transmit] → [TFTP Service] → [TFTP client service] to enter TFTP client configuration page, as shown in Figure 78.

TFTP client service

Server IP address	192.168.0.184
Local file name(1-100 character)	config.txt
Server file name(1-100 character)	startup-config
Transmission type	binary ⌄

Upload to PC   Download to Device

Figure 78 TFTP Client Service

Server IP address

Format: A.B.C.D

Description: Input the server IP address.

Local file name

Range: 1~100 characters

Description: Input the file name of the switch.

Server file name

Range: 1~100 characters

Description: Input the file name of the server.

Transmission type:

Configuration items: binary/ascii

Default: binary

Function: Select the file transmission standard.

Explanation: ascii means using ASCII standard to transmit file; binary means using binary standard to transmit file.

Method: Click <Upload to PC> to upload the file from switch to server or <Download to Device> to download file from server to switch.

➢   When file transmission succeeds, the following information appears on the Web interface, as shown in Figure 79 and Figure 80.

```
                    Information Display
Begin to send file, please wait...

File transfer complete.
Close tftp client.
```

Figure 79 Successful File Upload through TFTP

```
                    Information Display
Begin to receive file, please wait...

File transfer complete.
Recv total 2087 bytes
Write "config.txt" to file system 0.0 %
Write "config.txt" to file system 100.0 %
Close tftp client.
```

Figure 80 Successful File Download through TFTP

Caution:

➢ In the file transmission process, keeps the TFTP server running.

➢ Software version file is not a text file, and it must adopt the binary standard for transmission

2. The switch works as the TFTP server.

Click [Device Basic Configuration] → [File transmit] → [TFTP Service] → [TFTP server service] to enter the TFTP server configuration page, as shown in Figure 81.

```
              TFTP server service
  Server state                    |  Open    ▼ |
  TFTP Timeout(5-3600 second)     |  20        |
  TFTP Retransmit times(1-20)     |  5         |

              [ Apply ]
```

Figure 81 TFTP Server Service

Server state

Configuration items: Close/Open

Default: Close

Function: Enable/Disable the TFTP server function.

TFTP Timeout

Range: 5~3600s

Default: 20s

Function: Configure the timeout of TFTP server connection.

TFTP Retransmit times

Range: 1~20

Default: 5

Function: Configure the retransmission times of TFTP server during timeout.

➢ Install TFTP client software, as shown in Figure 82. Input switch IP address in Host; select

the client file storage path in Local File; input the file name saved in switch in Remote File;

click <Get> to download file from switch to client; click <Put> to upload client file to switch.
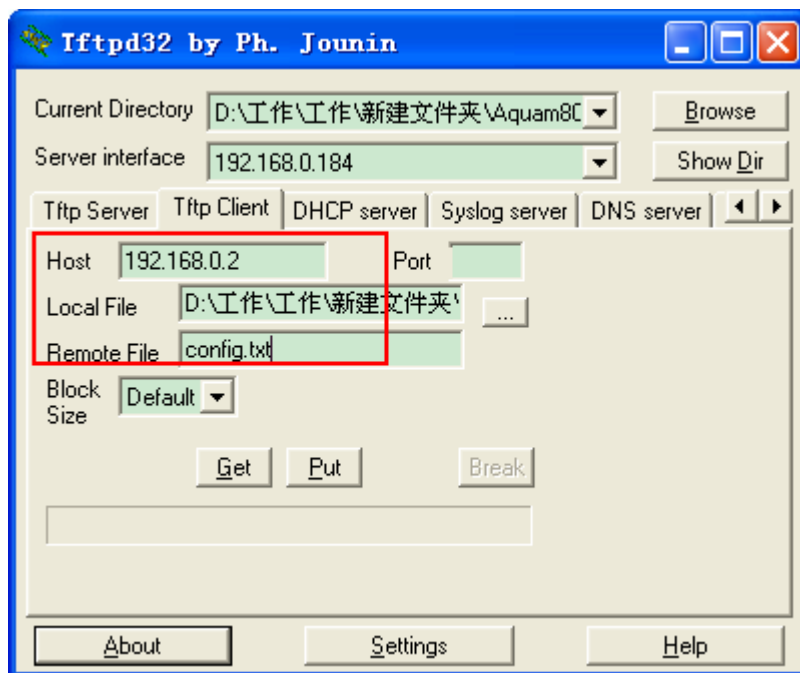
Figure 82 TFTP Client Configuration

> **Caution:**
>
> During file transmission, keep TFTP client software running.

5.13.2 FTP Service

1. The switch works as the FTP client.

➢ First, install FTP server. Click [Security] → [users/rights] to open the dialog box. Click

<new user> to create a new FTP user, as shown in Figure 83. Input username and

password, for example, username: admin; password: 123. Click <OK>.
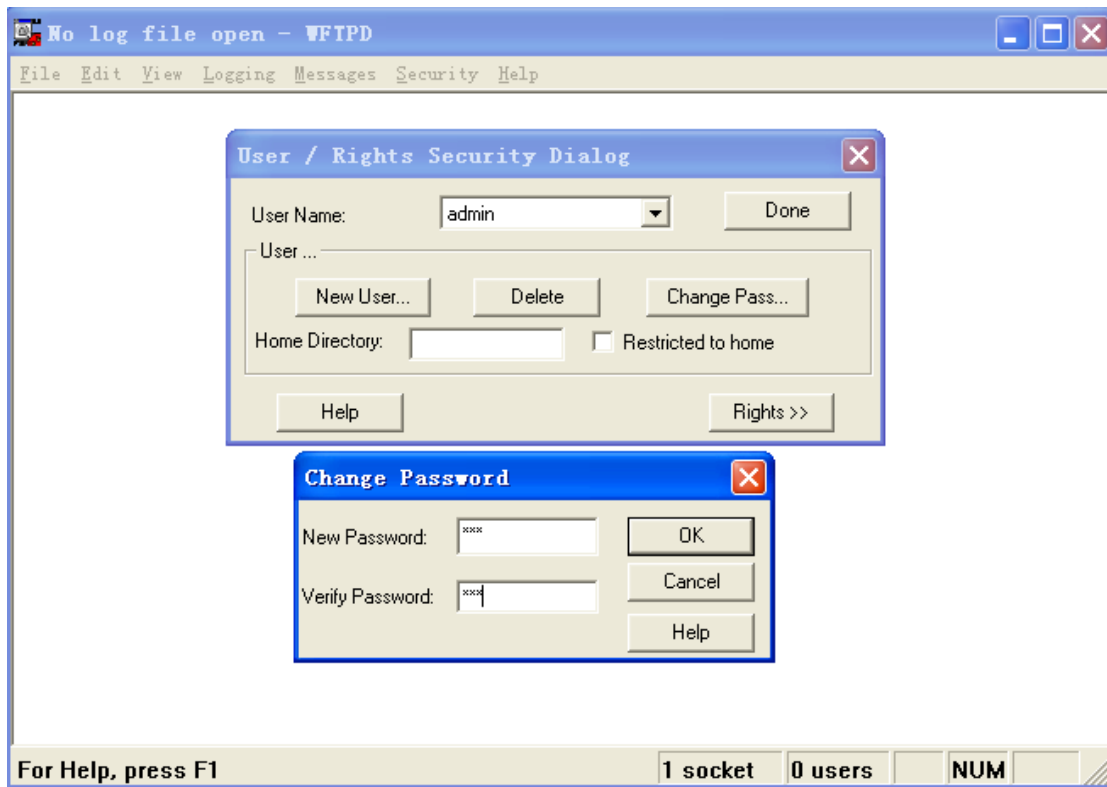
Figure 83 Creating a New FTP User

➢ Input the file storage path in server in Home Directory, as shown in Figure 84. Click <Done>.

Figure 84 File Storage Path

➢ Click [Device Basic Configuration] → [File transmit] → [FTP Service] → [FTP client service] to enter FTP client configuration page, as shown in Figure 85.

Figure 85 FTP Client Service

Server IP address

Format: A.B.C.D

Description: indicates the server IP address.

{User name, Password}

Range: {1~100 characters, 1~100 characters}

Description: indicates the username and password created on FTP server.

Local file name:

Range: 1~100 characters

Description: indicates the file name in switch.

Server file name

Range: 1~100 characters

Description: indicates the file name in server.

Transmission type:

Configuration items: binary/ascii

Default: binary

Function: Select the file transmission standard.

Explanation: ascii means using ASCII standard to transmit file; binary means using binary standard to transmit file.

Method: Click <Upload to PC> to upload the file from switch to server. Click <Download to Device> to download file from server to switch.

➢ When file transmission succeeds, the following information appears on the Web interface, as shown in Figure 86 and Figure 87.

Figure 86 Successful File Upload through FTP

Figure 87 Successful File Download through FTP

⚠ CAUTION

Caution:

➢ In the file transmission process, keep FTP server software running.

➢ Software version file is not a text file, and it must adopt the binary standard for transmission.

---

2. The switch works as an FTP server.

➢ Click [Device Basic Configuration] → [File transmit] → [FTP Service] → [FTP server service] to enter FTP server configuration page, as shown in Figure 88.

FTP Server Service

FTP server State	Close ▼
FTP Timeout(5-3600 second)	600

Apply

Figure 88 TFTP Server Service

FTP Server state

Options: Close/open

Default: close

Function: Enable or disable the FTP server function.

FTP Timeout

Range: 5~3600s

Default: 600s

Function: Configure the timeout of FTP server connection.

Description:

If no data is transmitted between the FTP server and client within the timeout, the connection between them is disconnected.

➢ Configure the username and password used for logging in to the FTP server, as shown in Figure 89.

FTP user name and password setting

User name(1-100 character)	admin
Password(1-100 character)	123
State	Plain text ▼

Add   Del

Figure 89 FTP Server User Name and Password Configuration

{Username, Password}

Range: {1~16 characters, 1~8 characters}

Default: {admin, 123}

Function: Configure the username and password used for logging in to the FTP server.

Description: When the switch works as an FTP server, it can be connected to multiple FTP

clients at the same time.

State

Options: Plain text/Encrypted text

Default: Plain text

Function: Select the password display mode.

➢ Click [Start] → [Run] in the Windows OS. The Run dialog box is displayed. Input "cmd" and press Enter. The following page is displayed.
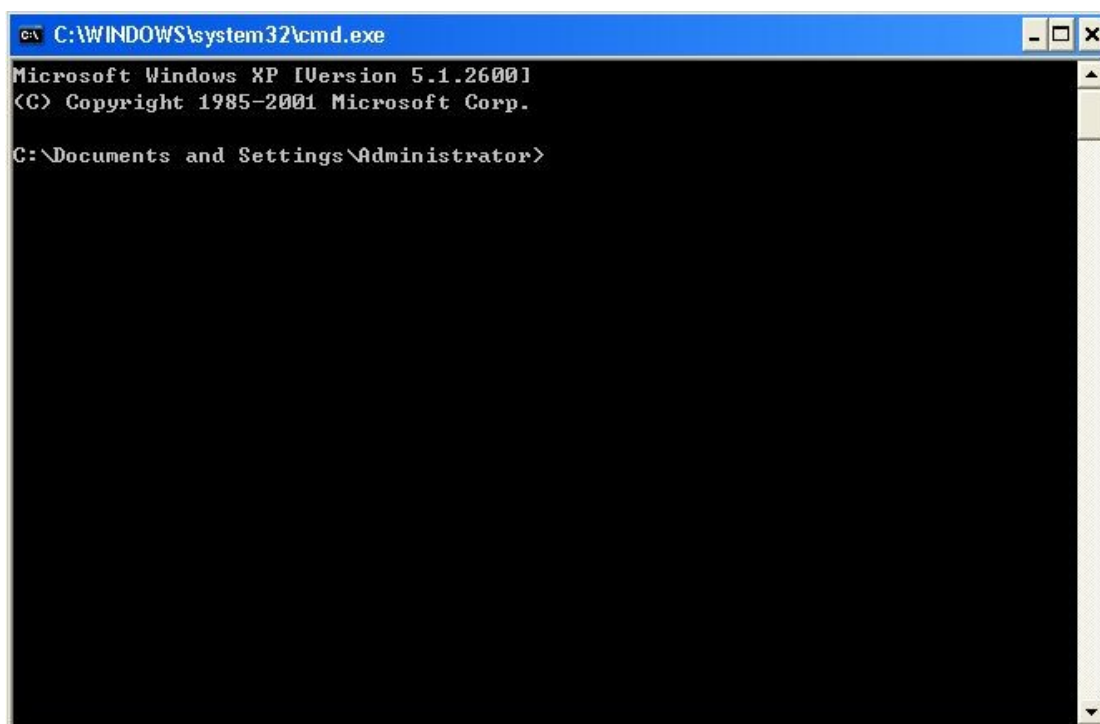
Figure 90 CLI

➢ The file transmission path can be changed. Log in to the FTP server, as shown in Figure 91.
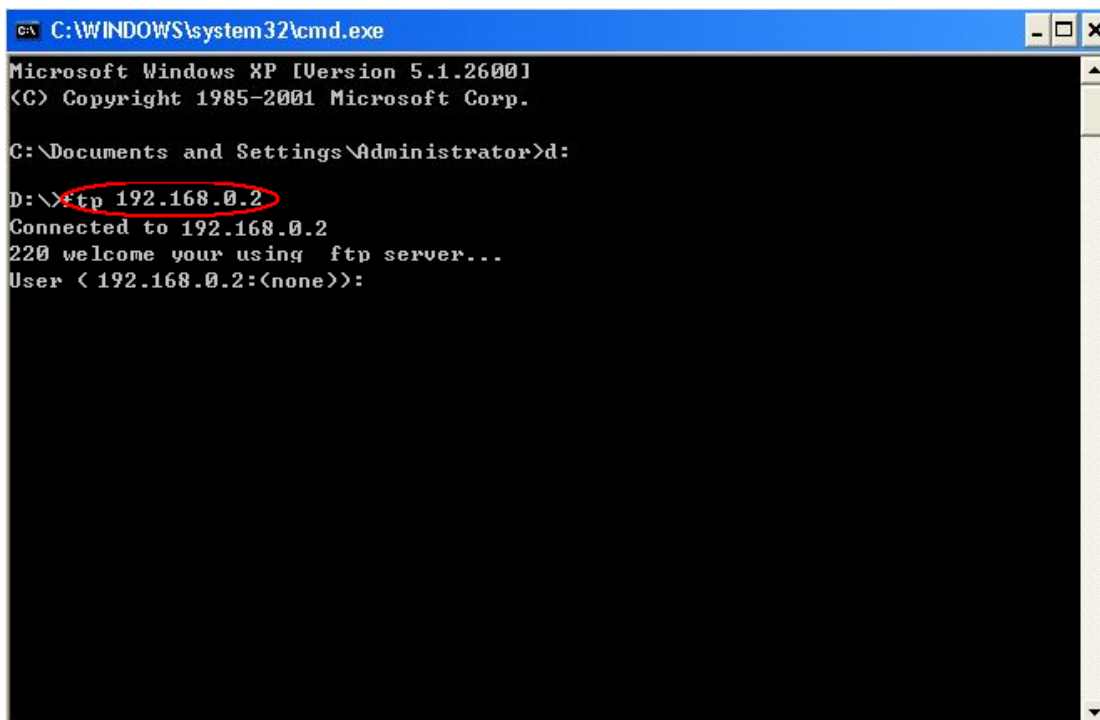
Figure 91 FTP Server Connection

➢ Use the configured user name "admin" and password "123" to log in to the FTP server, as

shown in Figure 92.
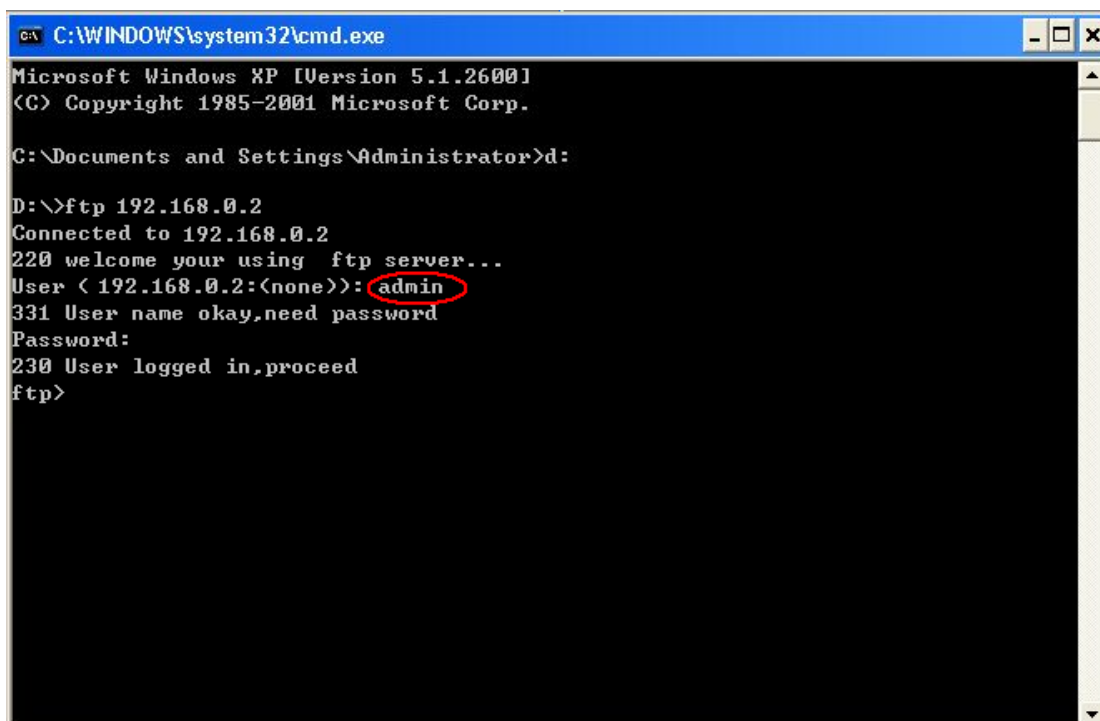
Figure 92 Logging in to the FTP Server

➢ Use the "get" command to download the file to the designated path on client, as shown in

Figure 93. Input the "get" command and press Enter. Input the name of file on switch to be

downloaded in Remote file and the file name saved in client in Local file.
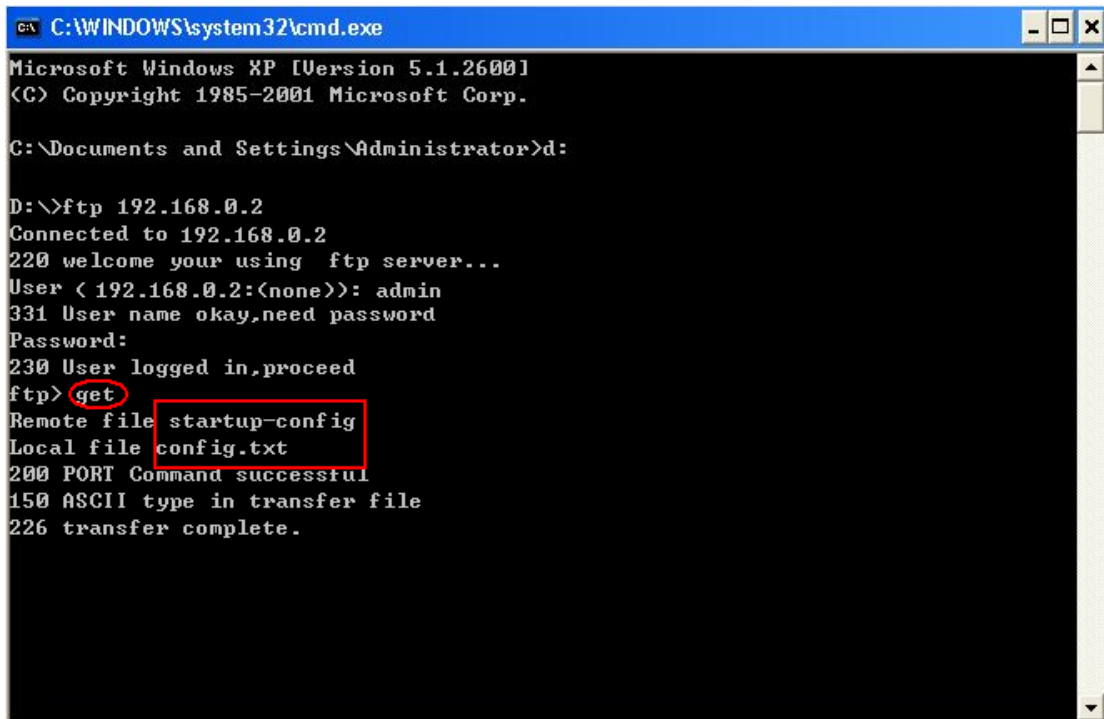
Figure 93 Downloading File from Switch to Client

➢ Use the "put" command to upload the file in the designated path in the client to the server, as shown in Figure 94. Run the "put" command and press Enter. Input the file name in switch in Remote file and the name of file in the client to be uploaded in Local File.
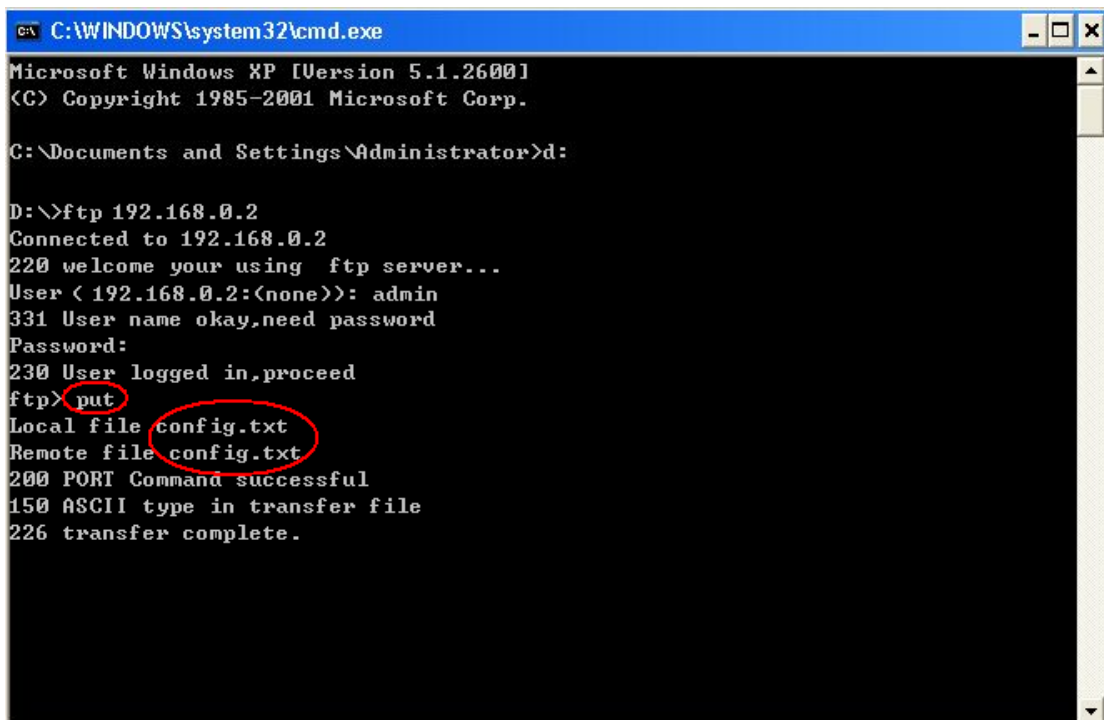
Figure 94 Uploading File from Client to Switch

5.14 MAC Address Configuration

5.14.1 Introduction

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.

A static MAC address is configured by a user. It has the highest priority (not overridden by dynamic MAC addresses) and is permanently valid.

Dynamic MAC addresses are learned by the switch in data forwarding. They 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.

Aging time starts from when a dynamic MAC address is added to the MAC address table. If no port receives a frame with the MAC address within one to two times the aging time, the switch deletes the entry of the MAC address from the dynamic forwarding address table. Static MAC addresses do not involve the concept of aging time.

The switch supports a maximum of 1024 static unicast entries.

5.14.2 Web Configuration

1. Configure MAC binding

Click [Device Basic Configuration] → [MAC address table configuration] → [MAC bind Configuration] to enter MAC binding configuration page, as shown in Figure 95.

MAC bind Configuration

MAC bind state	Enable ⌄

Apply
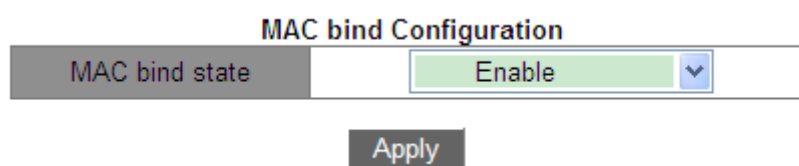
Figure 95 MAC Bind Configuration

MAC bind state

Option: Enable/Disable

Default: Disable

Function: Enable or disable MAC binding function. When enable is selected, for a packet whose source MAC address and VLAN ID are consistent with the MAC address and VLAN ID of a static unicast MAC address entry, the switch checks whether the inlet port is consistent with the port of this static unicast MAC address entry. If yes, the switch receives and forwards the packet. If no, the switch discards the packet. When disable is selected, the preceding check is not performed.

2. Add a static unicast MAC address.

Click [Device Basic Configuration] → [MAC address configuration] → [Unicast address configuration] to enter unicast MAC address configuration page, as shown in Figure 96.

Unicast MAC operation

MAC address(HH-HH-HH-HH-HH-HH)	EC-DE-12-34-56-78
VLAN ID	1
Configuration type	static
Port list	1/2

Add

Figure 96 Adding a Static FDB Entry

MAC address

Format: HH-HH-HH-HH-HH-HH (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

Default: VLAN1

Configuration type

Options: static/blackhole

Default: static

Function: Select the type of the MAC address entry.

Description: Static means establishing mapping between the designated MAC address and port number or VLAN ID.

Blackhole is to drop the packet whose source MAC address or destination MAC address is the designated MAC address.

Port list

Options: all switch ports

Function: Select ports to forward the packets with this destination MAC address. The selected ports must be in the specified VLAN.

3. Delete a unicast address.

Click [Device Basic Configuration] → [MAC address configuration] → [Delete unicast address] to enter the configuration page, as shown in Figure 97.

Delete unicast address

☐ Delete by VLAN ID	1
☑ Delete by Address Type	Static
☐ Delete by MAC(00-00-00-00-00-00)	
☐ Delete by port	1/1

Remove

Figure 97 Deleting a Unicast MAC Address

Select the criterion for deleting the unicast address. If multiple criteria are selected, their relationship is logical "And".

4. Configure MAC address aging time.

Click [Device Basic Configuration] → [MAC address configuration] → [MAC address aging time setting] to enter the aging time configuration page, as shown in Figure 98.

MAC address aging time setting (0 to disable the aging function)

aging time(10-100000 seconds or 0)	300

Apply

Figure 98 MAC Address Aging Time Configuration

Aging time

Range: 10~100000s

Default: 300s

Function: Set the aging time for the dynamic MAC address entry.

Description: When aging time is set to 0, aging is prohibited. In this case, the address dynamically learned does not age with time.

5. Query unicast MAC addresses.

Click [Device Basic Configuration] → [MAC address configuration] → [MAC address query] to enter the unicast MAC address query page, as shown in Figure 99.

Figure 99 Unicast MAC Address Query

Select the criterion for unicast MAC address query. If multiple criteria are selected, their relationship is logical "And". For example: If you query the unicast address of port Ethernet 1/1, the following page is displayed.

Figure 100 Unicast MAC Address List

6. View unicast address entries.

Click [Device Basic Configuration] → [MAC address configuration] → [Show mac-address table] to enter the unicast MAC address query page. All dynamic and static entries are displayed, as shown in Figure 101.

Figure 101 Unicast Address Query

5.15 Basic Configuration Maintenance and Debugging Information

When configuring the switch, you may need to check the correctness of various configurations to ensure normal running; or when certain anomalies occur, you may need to locate the fault. In these cases, you can perform the following operations to view system configurations and running status.

1. Ping operation.

Click [Device Basic Configuration] → [Basic configuration debug] → [Ping and Traceroute] to enter ping operation page, as shown in Figure 102.

Figure 102 Ping Operation

IP address

Format: A.B.C.D

Description: Input the IP address of the remote device.

Hostname

Range: 1~30 characters

Function: If the mapping between the remote host and IP address has been set, just input the remote host name and conduct Ping operation.

Description: The switch sends ICMP request packets to the remote device to detect the communication between the switch and remote device.

2. Configure Traceroute operation, as shown in Figure 103.

Traceroute

IP address	192.168.1.2
Hostname	wm
Hops	10
Timeout	100

Reset   Apply

Figure 103 Traceroute Operation

IP address

Format: A.B.C.D

Description: Input the IP address of the remote device.

Hostname

Range: 1~30 characters

Function: If the mapping between the remote host and IP address has been set, you need to input only the remote host name to conduct Traceroute operation.

Hops

Options: 1~255

Function: Test the number of gateways that the packets pass through from the sending device to the destination device.

Timeout

Options: 100~10000ms

Function: Configure the timeout. If the sending device does not receive the response packet from the receiving device within this time, it is considered that the communication fails.

3. View system date and time.

This series switches support RTC. Even the power is cut off, timekeeping continues.

Click [Device Basic Configuration] → [Basic configuration debug] → [show clock] to enter

clock information page, as shown in Figure 104.

Figure 104 Clock Information

4. View the file information in Flash.

Click [Device Basic Configuration] → [Basic configuration debug] → [show flash] to enter

flash information page, as shown in Figure 105.

Figure 105 Flash Information

5. View configuration information, that is, the parameters after modification.

Click [Device Basic Configuration] → [Basic configuration debug] → [show running-config] to

enter operation configuration page, as shown in Figure 106.

Figure 106 Configuration Information

6. View port information.

Click [Device Basic Configuration] → [Basic configuration debug] → [show switchport interface] to enter port information page, as shown in Figure 107.

Figure 107 Port Information

Type

94

Description: the VLAN type.

Mode

Description: the port mode.

Port VID

Description: the port PVID

Trunk allowed Vlan With TAG

Description: Indicates VLANs for the selected Trunk port as tag.

Trunk allowed Vlan With UNTAG

Description: Indicates VLANs for the selected trunk port as untag.

7. View the TCP connection status.

Click [Device Basic Configuration] → [Basic configuration debug] → [show tcp] to enter TCP

connection information page, as shown in Figure 108.

```
                              Information Display
LocalAddress     LocalPort   ForeignAddress   ForeignPort    State
2.1.1.1          80          2.1.1.23         1486           ESTABLISH
2.1.1.1          80          2.1.1.23         1485           TIMEWAIT
2.1.1.1          80          2.1.1.23         1484           TIMEWAIT
2.1.1.1          80          2.1.1.23         1483           TIMEWAIT
2.1.1.1          80          2.1.1.23         1482           TIMEWAIT
2.1.1.1          80          2.1.1.23         1481           TIMEWAIT
2.1.1.1          80          2.1.1.23         1480           TIMEWAIT
2.1.1.1          80          2.1.1.23         1479           TIMEWAIT
2.1.1.1          80          2.1.1.23         1478           TIMEWAIT
0.0.0.0          80          0.0.0.0          0              LISTEN
0.0.0.0          23          0.0.0.0          0              LISTEN
```

Figure 108 TCP Connection

Local Address

Description: indicates the local address of TCP connection.

Local Port

Description: indicates the local port number of TCP connection.

Foreign Address

Description: indicates the address in the other end of TCP connection.

Foreign Port

Description: indicates the port number in the other end of TCP connection.

State

Description: indicates the current status of TCP connection.

8. View the UDP connection status.

Click [Device Basic Configuration] → [Basic configuration debug] → [show udp] to enter UDP connection information page, as shown in Figure 109.

```
                              Information Display
LocalAddress      LocalPort   ForeignAddress      ForeignPort      State
0.0.0.0           0           0.0.0.0             0                (null)
```

Figure 109 UDP Connection Information

Local Address

Description: indicates the local address of UDP connection.

Local Port

Description: indicates the local port number of UDP connection.

Foreign Address

Description: indicates the IP address in the other end of UDP connection.

Foreign Port

Description: indicates the port number in the other end of UDP connection.

State

Description: indicates the current status of UDP connection.

9. View the information of login users.

Click [Device Basic Configuration] → [Basic configuration debug] → [show login] to enter login user information page, as shown in Figure 110.

```
                              Information Display
No.  Name             Level    Login    Authen    IP Address         Time(min)
---- ---------------- -------- -------- -------- ------------------ ---------
1    444              guest    ssh      local    192.168.0.184      0
2    333              guest    ssh      local    192.168.0.184      2
3    222              system   telnet   local    192.168.0.184      2
4    111              guest    telnet   local    192.168.0.184      3
5    admin            admin    web      local    192.168.0.184      3
6    111              guest    console  local    ----               3
```

Figure 110 Login Users

6. Device Advanced Configuration

6.1 ARP Configuration

6.1.1 Introduction

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

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

6.1.2 Explanation

ARP entries fall into dynamic and static ones.

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

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

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

6.1.3 Proxy ARP

If an ARP request is sent from a host to another host which is in the same network segment but on a different physical network, the gateway in direct connection with the source host and with proxy ARP function can respond to this request message. This process is called

proxy ARP.

The proxy ARP process is as follows:

1. A source host sends an ARP request to another host on a different physical network.

2. The proxy ARP function on this VLAN interface has been enabled on the gateway in direct connection with the source host. If a normal route to the destination host exists, the gateway replies its own MAC address for the destination host.

3. The IP packets sent from the source host to the destination host are sent to the device with proxy ARP enabled.

4. The gateway carries out normal IP routing and forwarding for packets.

5. The IP packets to be sent to the destination host finally reach the destination host via network.

> **Caution:**
>
>   No proxy is performed for the ARP requests matching default routing.

6.1.4 Web Configuration

1. Add or delete a static ARP entry.

Click [Device Advanced Configuration] → [ARP configuration] → [ARP configuration] to enter the ARP configuration page, as shown in Figure 111.

<div align="center">

ARP configuration

IP address(0.0.0.0)	192.168.0.23
MAC address(HH-HH-HH-HH-HH-HH)	00-00-00-00-00-01
Operation type	Add
L3 interface	Vlan1
Ethernet port	1/8

Apply

</div>

Figure 111 Configuring a Static ARP Entry

IP address

Format: A.B.C.D

Function: Configure the IP address of the static ARP entry.

MAC address

Format: HH-HH-HH-HH-HH-HH (H is a hexadecimal number)

Function: Configure the MAC address of the static ARP entry.

Operation type

Options: Add/Del

Default: Add

Function: Add or delete an ARP entry.

L3 interface

Options: all created Layer-3 VLAN interfaces

Default: VLAN1

Function: Select the Layer-3 VLAN interface for the current ARP entry.

Ethernet Port

Options: all ports in the designated VLAN

Function: Select the egress corresponding to the current ARP entry.

	Caution:
⚠️ CAUTION	➢ The IP address bound to a static ARP entry cannot be the IP address of the switch.
	➢ Different IP addresses can be bound to one MAC address.
	➢ In a VLAN, an ARP entry can correspond to only one forwarding port.
	➢ Generally, the switch automatically learns ARP entries without administrator intervention.

2. View ARP addresses entry.

Click [Device Advanced Configuration] → [ARP configuration] → [Show ARP] to enter the ARP configuration page, as shown in Figure 112.

ARP list

IP address	MAC address	L3 interface	Ethernet port	Type
192.168.0.21	12-2a-bd-c3-44-55	Vlan1	1/8	dynamic
192.168.0.120	78-2b-cb-60-3c-e3	Vlan1	1/8	dynamic
192.168.0.23	00-00-00-00-00-01	Vlan1	1/8	static
192.168.0.18	00-72-75-78-88-5b	Vlan1	1/8	dynamic
192.168.0.19	d0-67-e5-2d-95-a5	Vlan1	1/8	dynamic
192.168.0.199	70-71-bc-95-cc-22	Vlan1	1/8	dynamic
192.168.0.86	80-c1-6e-e0-5b-9a	Vlan1	1/8	dynamic
192.168.0.192	78-2b-cb-2c-6b-87	Vlan1	1/8	dynamic
192.168.0.2	00-1e-cd-00-e6-5f	Vlan1	1/8	dynamic
192.168.0.212	00-71-bc-95-cc-4d	Vlan1	1/8	dynamic
192.168.0.99	c8-9c-dc-a8-c4-ac	Vlan1	1/8	dynamic
192.168.0.184	44-37-e6-88-6e-90	Vlan1	1/8	dynamic
192.168.0.44	08-00-3e-32-53-29	Vlan1	1/8	dynamic

Refresh

Figure 112 ARP List

ARP list

Portfolio: {IP address, MAC address, L3 interface, Ethernet port, Type}

Function: View ARP entries.

Description: ARP list shows all ARP entries corresponding to LinkUp ports, including static entries and dynamic entries.

3. Clear ARP cache.

Click [Device Advanced Configuration] → [ARP configuration] → [Clear ARP cache] to clear ARP cache, as shown in Figure 113.

Clear ARP cache

Apply

Figure 113 Clearing ARP Cache

Click <Apply> to clear dynamic ARP entries in cache.

4. Enable proxy ARP

Click [Device Advanced Configuration] → [ARP configuration] → [Proxy ARP configuration] to configure proxy ARP, as shown in Figure 114

Enable Proxy ARP

VLAN interface	Vlan2 ˅

Apply   Default
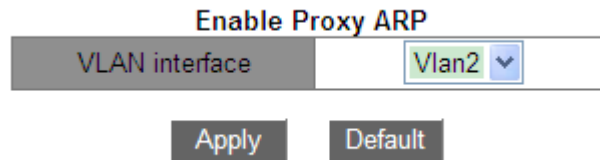
Figure 114 Configure Proxy ARP

VLAN interface

Function: Select the 3-layer VLAN interface to be enabled proxy ARP.

6.1.5 Typical Configuration Example

As shown in Figure 115, PC1, PC2 and PC3 are hosts in the same network segment, belonging to different subnets VLAN1, VLAN2 and VLAN4 respectively.
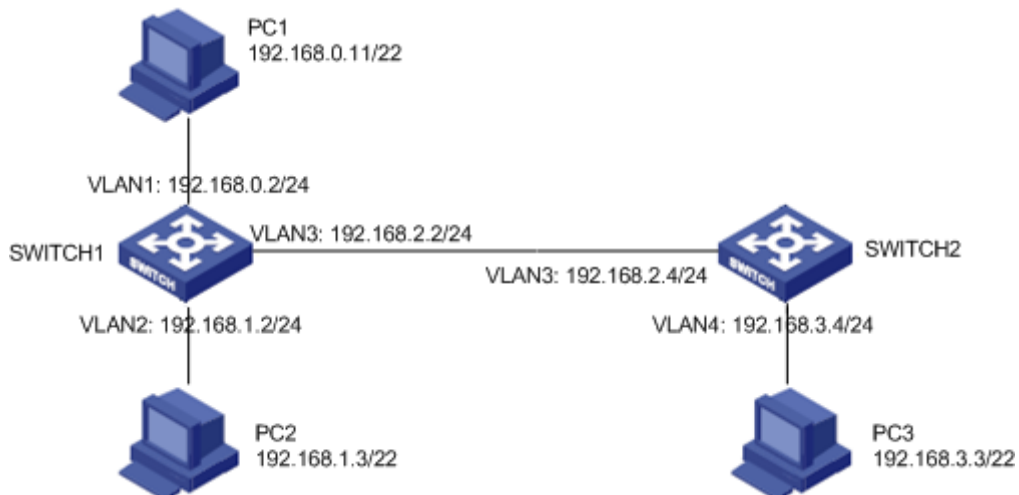
Figure 115 Proxy ARP Configuration Example

PC1 broadcasts ARP requests, requesting for the MAC addresses of PC2 and PC3.

➢ When the proxy ARP function at interface VLAN1 of SWITCH1 is not enabled, as they are in different VLANs, the ARP request cannot reach PC2 or PC3 and communication between the two parties is not possible.

➢ When the proxy ARP function at interface VLAN1 of SWITCH1 is enabled, after receiving the ARP request through interface VLAN1, SWITCH1 checks the routing table and locates the routes to PC2 and PC3, and then uses the MAC address of interface VLAN1 to send ARP response messages (with source IP addresses being the IP addresses of PC2 and PC3). After receiving the response message, PC1 establishes the ARP entry for

sending subsequent IP packets toward PC2 and PC3 to interface VLAN1 of SWITCH1 which then carries out forwarding.

6.2 Layer-3 interface configuration

6.2.1 Switch IP Address

Log in to the CLI of the switch through the console port. Run the **enable** command in the general view to enter the privileged view. Run the **show interface vlan 1** command to view the IP address of the switch, as shown in the red circle of Figure 116.
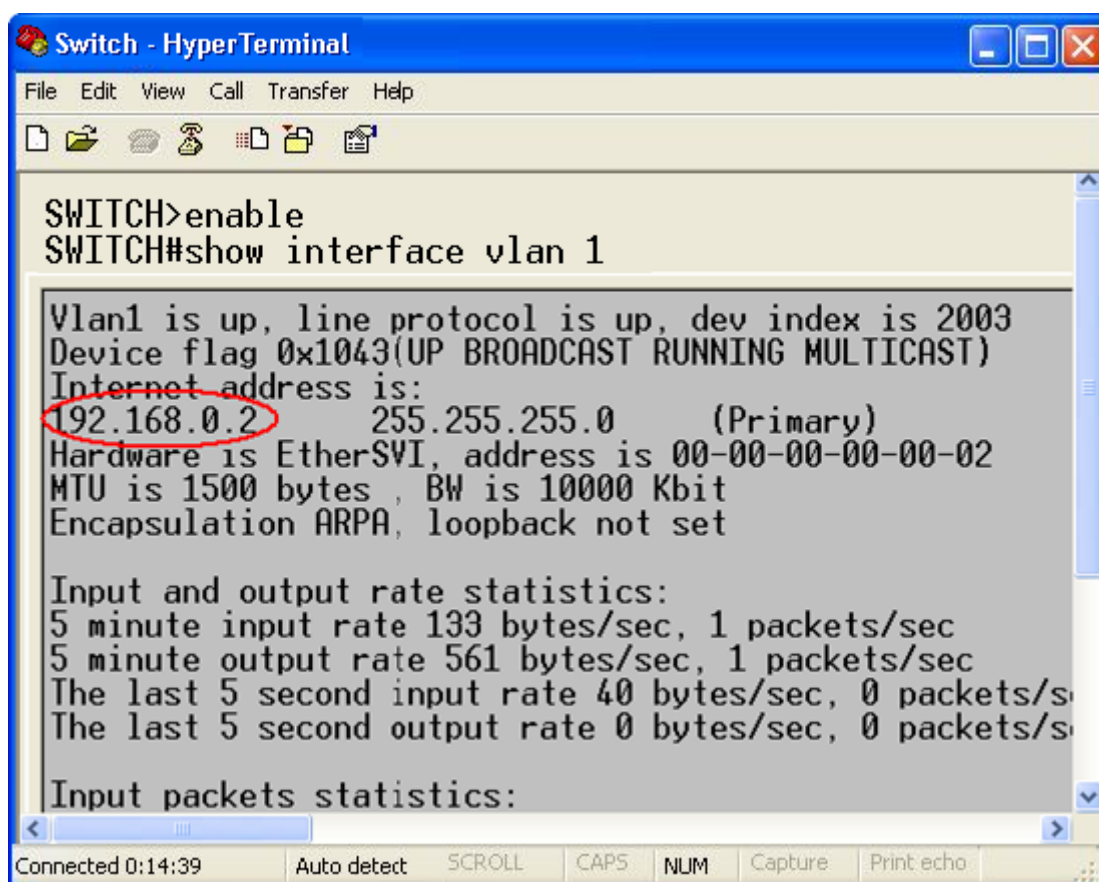
Figure 116 Displaying IP Address

6.2.2 IP Address Configuration

1. Create Layer-3 VLAN interface.

Hosts in different VLANs cannot communicate with each other. Their communication packets need to be forwarded by a router or Layer 3 switch through a VLAN interface.

This series switches support VLAN interfaces, which are virtual Layer 3 interfaces used for inter-VLAN communication. You can create one VLAN interface for each VLAN. The interface is used for forwarding Layer 3 packets of the ports in the VLAN.

Click [Device Advanced Configuration] → [L3 interface configuration] → [Add interface VLAN] to enter the configuration page, as shown in Figure 117.

Add interface VLAN

Interface vlan ID(1-4093)	2

Reset   Add   Del

L3 Interfacelist
Vlan1
Vlan2
Vlan3
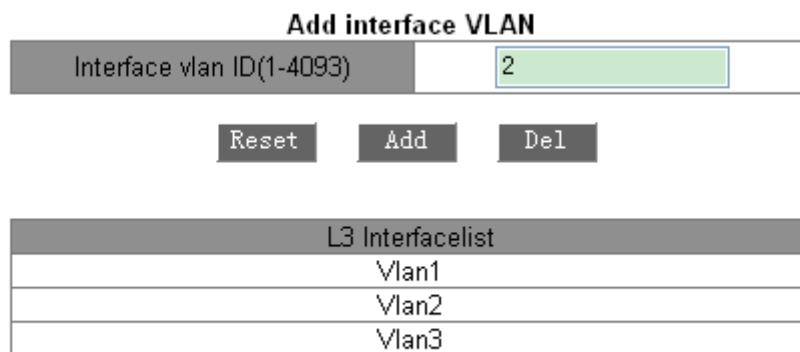
Figure 117 Creating a VLAN Interface

Interface vlan ID

Options: all created VLAN numbers

Default: 1

Function: Create a Layer-3 VLAN interface.

> **Note:**
> ➢ The switch supports a maximum of 16 Layer-3 VLAN interfaces.
> ➢ Before creating a VLAN interface, please ensure the existence of the corresponding VLAN. If the VLAN does not exist, its VLAN interface cannot be created.
> ➢ You cannot delete the VLAN interface whose corresponding IP address is used to access the switch by Web.

2. IP address obtainment

Switch IP address can be manually configured or automatically obtained.

Click [Device Advanced Configuration] → [L3 interface configuration] → [L3 port IP address mode configuration] to enter the IP address configuration page, as shown in Figure 118.

Figure 118 Obtaining the IP Address

Port

Options: all created Layer-3 VLAN interfaces

Default: VLAN1

IP Mode

Options: bootp-client/dhcp-client/Specify IP address

Default: Specify IP address

Function: Select the mode for obtaining an IP address.

Description: Specify IP address is to configure IP address manually; bootp-client/dhcp-client is that the switch automatically obtains an IP address through DHCP/BOOTP. There should be a DHCP/BOOTP server in the network to assign IP addresses to clients.　About DHCP/BootP server configuration, please refer to "6.14 DHCP Configuration".

3. Manually configure IP address.

Click [Device Advanced Configuration] → [L3 interface configuration] → [Allocate IP address for L3 port] to allocate IP address, as shown in Figure 119.

Figure 119 IP Address Configuration

IP Address

Configuration format: A.B.C.D

Function: Configure the IP address for the specified Layer-3 VLAN interface.

Subnet mask

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 as 255.255.255.0.

Status

Options: no shutdown/ shutdown

Default: no shutdown

Function: Configure the status of the Layer-3 VLAN interface.

Description: no shutdown: opens the Layer-3 VLAN interface. Shutdown: closes the Layer-3 VLAN interface.

Click <Add> to configure IP address for the VLAN interface; click <Del> to delete the current IP address, you should remove secondary IP first before deleting the primary IP address; click <Update> to modify the primary IP address of the VLAN interface.

Note:

➢ Each Layer-3 VLAN interface supports a maximum of 32 IP addresses.

➢ IP addresses of the same network segment or different network segments can be configured for each VLAN interface.

➢ IP addresses of different network segments should be configured for different VLAN interfaces.

6.3 SNMP v2c

6.3.1 Introduction

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.

6.3.2 Implementation

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

➢ The Network Management Station (NMS) is a station running SNMP-enabled network management software client. It is the core for the network management of an SNMP network.

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

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

➢ Get-Request

➢ Get-Response

➢ Get-Next-Request

➢ Set-Request

➢ Trap

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

6.3.3 Explanation

This series switches support SNMP v2c. SNMP v2c is compatible with SNMPv1.

SNMP v1 uses community name for authentication. A community name acts as a password, limiting NMS's access to agents. If the community name carried by an SNMP packet is not acknowledged by the switch, the request fails and an error message is returned.

SNMP v2c also uses community name for authentication. It is compatible with SNMP v1, and

extends the functions of SNMP v1.

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

6.3.4 MIB Introduction

Any managed resource is called managed object. The Management Information Base (MIB) stores managed objects. It defines the hierarchical relationships of managed objects and attributes of objects, such as names, access permissions, and data types. Each agent has its own MIB. The NMS can read/write MIBs based on permissions. Figure 120 shows the relationships among the NMS, agent, and MIB.
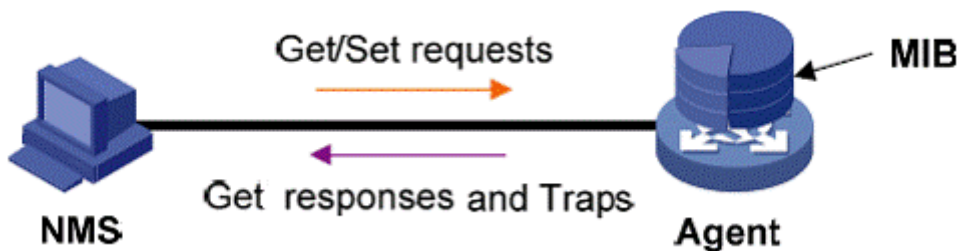
Figure 120 Relationship among NMS, Agent, and MIB

MIB defines a tree structure. The tree nodes are managed objects. Each node has a unique Object Identifier (OID), which indicates the location of the node in the MIB structure. As shown in Figure 121, the OID of object A is 1.2.1.1.
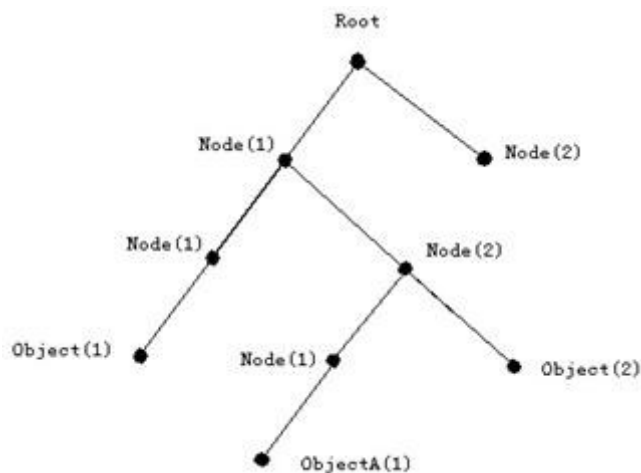
Figure 121 MIB Structure

6.3.5 Web Configuration

1. Configure SNMP v2c

Click [Device Advanced Configuration] → [SNMP Configuration] → [SNMP Base Configuration] to configure SNMP v2c, as shown in Figure 122.

Figure 122 SNMP v2c Configuration

Snmp Agent state

Options: Enable/Disable

Default: Disable

Function: Enable/Disable SNMP.

V1/ V2C/ V3 state

Options: Enable/Disable

Function: Choose a SNMP version.

Request Port

Range: 1~65535

Default: 161

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

Community

Range: 4~16 characters

Function: Configure switch community.

Description: The packet can access the switch MIB only when the community name carried in the SNMP packet is the same as this community string.

Explanation: A maximum of 5 community strings can be set.

Access Permission

Options: Read Only/Read And Write

Default: Read Only

Function: Configure the MIB access mode.

Description: Read only: only reads MIB information. Read and write: reads and writes MIB information.

2. Configure security IP addresses.

Click [Device Advanced Configuration] → [SNMP Configuration] → [IP Address of SNMP Manager] to enter security IP address configuration page, as shown in Figure 123.
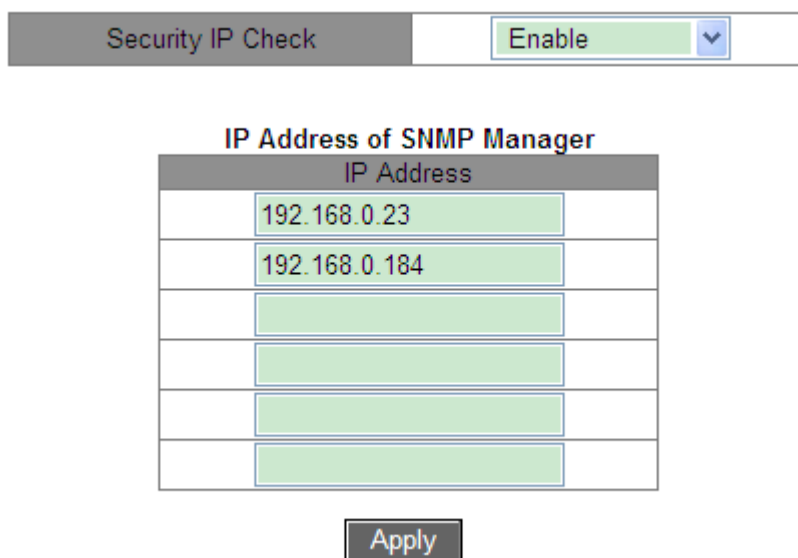
Figure 123 Security IP Address Configuration

Security IP Check

Option: Enable/Disable

Default: Disable

Function: Enable or disable security IP check. If security IP check is disabled, there is not restriction on NMS IP address, any NMS connected to the switch can access switch MIB information. After security IP check is enabled, you need to set security IP address, and only the NMS with a security IP address can access switch MIB information.

IP Address

Format: A.B.C.D

Function: Configure the security IP address of the NMS.

Description: Only the NMS whose IP address matches the security IP address can access switch MIB information. A switch allows a maximum of 6 security IP addresses of the NMS.

3. Configure Trap.

Click [Device Advanced Configuration] →[SNMP Configuration]→[TRAP Configuration] to configure trap, as shown in Figure 124.

TRAP Configuration

TRAP State	Open	
TRAP Port	162	(1-65535)

TRAP Configuration Table

All	Version	Destination IP Address	Security Level	Security Name	Context Name
	V3		NoAuthNoPriv		
☐	V1	192.168.0.23	---	---	---
☐	V2C	192.168.0.184	---	---	---

Apply   Edit   Delete

Figure 124 Enable Trap

TRAP State

Options: Open/Close

Default: Close

Function: allow switch to send Trap message or not.

TRAP Port

Options: 1~65535

Default: 162

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

Version

Option: V1/ V2C/ V3

Function: V1/V2C indicates that the switch sends trap messages of version 1/version 2C to the server. V3 indicates that the switch sends trap messages of version 3 to the server. If you select V1/ V2C, only destination IP address needs to be configured.

Destination IP Address

Format: A.B.C.D

Function: Configure the address of the server for receiving trap messages. You can configure a maximum of 8 servers, that is, 8 trap entries.

4. View SNMP statistics.

Click [Device Advanced Configuration] → [SNMP Configuration] → [SNMP Statistics] to enter SNMP statistics page, as shown in Figure 125.

SNMP Statistics	number
Incoming Snmp Packet	37
Version Error Snmp Packet	0
Received Snmp GetNext Packet	4
Received SET Request Packet	2
Outgoing Snmp Packet	20
Too_big Error Snmp Packet	0
Max-Length of Snmp Datagram	1500
Snmp Request for Inexistent MIB Object	0
Bad_value Error Snmp Packet	0
General_error Snmp Packet	0
Transmitting Response Packet	12
Transmitting TRAP Packet	8
Nms SET Request Packet	2
Communitry String Error Snmp Packet	0
Communitry String Priority Error	6
Coding Error Snmp Packet	0

Show

Figure 125 SNMP Statistics

6.3.6 Typical Configuration Example

SNMP management server is connected to the switch through Ethernet. The IP address of the management server is 192.168.0.23, and that of the switch is 192.168.0.2. The NMS monitors and manages the Agent through SNMP v2c, and reads and writes the MIB node information of the Agent. When the Agent is faulty, it proactively sends trap packets to the NMS, as shown in Figure 126.
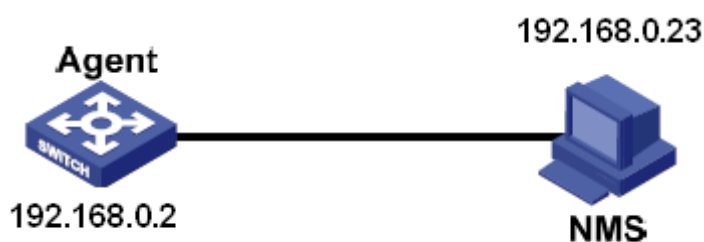
Figure 126 SNMP v2c Configuration Example

Configuration on Agent:

1. Enable SNMP and v2c state; configure access rights with Read only community "public" and Read and write community "private", as shown in Figure 122.

2. Set security IP address to 192.168.0.23, as shown in Figure 123.

3. Enable the trap state; set the trap version to V2C, destination IP address to 192.168.0.23, as shown in Figure 124.

If you want to monitor and manage Agent devices, run the corresponding management software in NMS, such as Kyvision developed by Kyland.

For details about operations of Kyvision, refer to the *Kyvision Operation Manual*.

6.4 SNMPv3

6.4.1 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.

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

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.

6.4.3 Web Configuration

1. Configure the user table

Click [Device Advanced Configuration] → [SNMP Configuration] → [V3 User Table] to enter the V3 user table configuration page, as shown in Figure 127.

V3 User Table

Number	State	User Name	Authentication protocol	Authentication password	Privacy protocol	Privacy password
1	active	1111	HMAC-MD5	••••	HMAC-DES	••••
2	active	2222	HMAC-SHA	••••	HMAC-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

Figure 127 SNMP v3 User Table Configuration

User Name

Range: 4~16 characters

Function: Create the user name.

Authentication protocol

Options: NONE/HMAC-MD5/HMAC-SHA

Default: NONE

Function: Select an authentication algorithm.

Authentication password

Range: 4~16 characters

Function: Create the authentication password.

Privacy protocol

Options: NONE/HMAC-DES

Default: NONE

Function: Select a packet encryption protocol.

Privacy password

Range: 4~16 characters

Function: Create the packet encryption password.

2. Configure the group table

Click [Device Advanced Configuration] → [SNMP Configuration] → [V3 Group Table] to enter

the V3 group table configuration page, as shown in Figure 128.

Number	GroupName	SecurityName	SecurityModel
1	group	1111	SNMP V3
2	group	2222	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

Figure 128 SNMP v3 Group Table Configuration

Group Name

Range: 4~16 characters

Function: Configure the name of the group table.

Security Name

Range: all existing user names, 4~16 characters

Function: Configure the security name. The security name must be identical with the user

name in the user table. Users with the same group name belong to the same group.

Security Model

Default: SNMP v3

Description: SNMP v3 indicates that User-based Security Model (USM) is adopted. Currently, the value must be SNMP v3.

3. Configure the context table

Click [Device Advanced Configuration] → [SNMP Configuration] → [V3 Context Table] to enter the V3 context table configuration page, as shown in Figure 129.

V3 Context Table

Number	ContextName
1	default empty context
2	context
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	

Apply

Figure 129 SNMP v3 Context Table Configuration

Context Name

Range: 4~16 characters

Function: Configure the context name.

Description: The first context name must be empty.

4. Configure the view table

Click [Device Advanced Configuration] → [SNMP Configuration] → [V3 View Table] to enter

the V3 view table configuration page, as shown in Figure 130.

V3 View Table

Index	View Name	Type	oid-tree	mask
1	view1	included ∨	1.3.6.1.2.1.1.1	0xfd,0xff,0xff,0xff
2	view2	excluded ∨	1.3.6.1.2.1.1.1	0xff,0xff,0xff,0xff
3	view-no	excluded ∨	1	0xff,0xff,0xff,0xff
4	view-all	included ∨	1	0xff,0xff,0xff,0xff
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

Figure 130 SNMP v3 View Table Configuration

View Name

Range: 4~16 characters

Function: Configure the view name.

Type

Options: included/excluded

Default: included

Function: Included indicates that the current view includes all nodes of the MIB tree.

Excluded indicates that the current view does not include any nodes of the MIB tree.

oid-tree

Function: MIB tree, indicated by the OID of the root node of the tree.

Mask

Function: Mask of the MIB tree. Oid-tree and mask together determine the MIB node information of the current view.

For example, in the Figure 130, the view name "view1" can only access the information of node 1.3.6.1.2.1.1.1, 1.3.6.1.2.1.2.1, 1.3.6.1.2.1.3.1, and 1.3.6.1.2.1.4.1… 1.3.6.1.2.1.n.1.

5. Configure the access table

Click [Device Advanced Configuration] → [SNMP Configuration] → [V3 Access Table] to enter the V3 access table configuration page, as shown in Figure 131.

V3 Access Table

Number	GroupName	Context Prefix	Context Match	SecurityModel	SecurityLevel	readView	writeView	notifyView
1	group	context	exact	SNMP V3	AuthNoPriv	view-all	view-no	view-all
2			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
3			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
4			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
5			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
6			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
7			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
8			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
9			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
10			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
11			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
12			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
13			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
14			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
15			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1
16			exact	SNMP V3	NoAuthNoPriv	view1	view1	view1

Apply

Figure 131 SNMP v3 Access Table Configuration

Group Name

Range: all existing group names, 4~16 characters

Function: Users in the group have the same access rights.

Context Prefix

Range: all existing context names, 4~16 characters

Function: Configure the context name. The group name and context name together determine the access rights of the group. Because the first context name must be empty in context table, context prefix can be empty.

Context Match

Options: exact/prefix

Default: exact

Function: Select the match mode of the context name. Exact indicates that the value of Context Prefix must be identical with the context name. Prefix indicates that the value of Context Prefix must be identical with the first 4 to 16 characters of the context name. In this case, context names with the same prefix have the same access rights.

Security Model

Default: SNMP V3

Description: SNMPv3 indicates that User-based Security Model (USM) is adopted. Currently, the value must be SNMP v3.

Security Level

Options: NoAuthNoPriv/AuthNoPriv/AuthPriv

Default: NoAuthNoPriv

Function: Select the access rights for MIB information.

Description: NoAuthNoPriv indicates that neither authentication nor packet encryption is required. AuthNoPriv indicates that authentication is required but not packet encryption. AuthPriv indicates that both authentication and packet encryption are required. When encryption is required, the user can access specified MIB information only if the encryption algorithm and password are identical with those configured in the user table.

read View

Options: all existing view names

Function: Select the name of read-only view.

write View

Options: all existing view names

Function: Select the name of write view.

notify View

Options: all existing view names

Function: Select the name of view that can send trap message.

6. Configure security IP addresses.

Click [Device Advanced Configuration] → [SNMP Configuration] → [IP Address of SNMP

Manager] to enter security IP address configuration page, as shown in Figure 132.
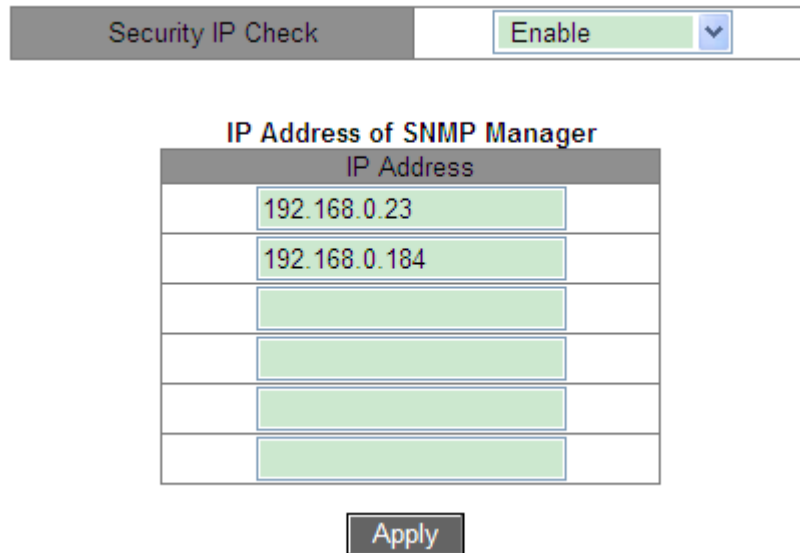
Figure 132 Security IP Address Configuration

Security IP Check

Option: Enable/Disable

Default: Disable

Function: Enable or disable security IP check. If security IP check is disabled, there is not

restriction on NMS IP address, any NMS connected to the switch can access switch MIB

information. After security IP check is enabled, you need to set security IP address, and only

the NMS with a security IP address can access switch MIB information.

IP Address

Format: A.B.C.D

Function: Configure the security IP address of the NMS.

Description: Only the NMS whose IP address matches the security IP address can access

switch MIB information. A switch allows a maximum of 6 security IP addresses of the NMS.

7. Configure Trap.

Click [Device Advanced Configuration] →[SNMP Configuration]→[TRAP Configuration] to

configure trap, as shown in Figure 133.

Figure 133 SNMP v3 Trap Configuration

TRAP State

Options: Open/Close

Default: Close

Function: Allow switch to send Trap message or not.

TRAP Port

Options: 1~65535

Default: 162

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

Version

Option: V1/V2C/V3

Function: V1/V2C indicates that the switch sends trap messages of version 1/version 2C to the server. V3 indicates that the switch sends trap messages of version 3 to the server.

Destination IP Address

Format: A.B.C.D

Function: Configure the address of the server for receiving trap messages. You can configure a maximum of 8 servers, that is, 8 trap entries.

{Security Level, Security Name, Context Name}

Options: {NoAuthNoPriv/AuthNoPriv/AuthPriv, 4~16 characters, 4~16 characters}

Function: These three parameters need to be configured only when V3 is selected. These

configurations must be consistent with those in the access table. The security level can be equal to or higher than that in the access table. For example, when the access right of user 1111 is set to AuthNoPriv, the switch can send trap messages to the server only if the security level of security name 1111 is AuthNoPriv or AuthPriv. The context name should be identical with Context Prefix in the access table.

6.4.4 Typical Configuration Example

SNMP management server is connected to the switch through Ethernet. The IP address of the management server is 192.168.0.23, and that of the switch is 192.168.0.2. User 1111 and user 2222 manage the Agent through SNMP v3. Security level is set to AuthNoPriv, and the switch can perform read-only operation on all node information of the Agent. When an alarm occurs, the Agent sends trap v3 messages to the NMS proactively, as shown in Figure 134.
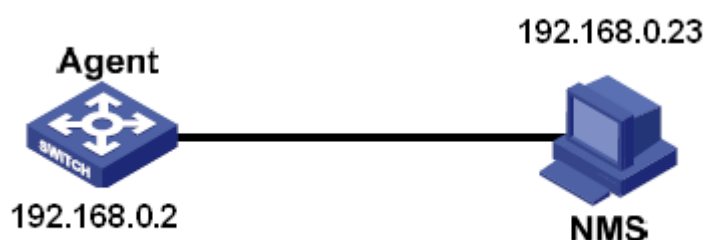
Figure 134 SNMP v3 Configuration Example

Configuration on the Agent:

1. Configure the SNMP v3 user table. Set a user name to 1111, authentication protocol to HMAC-MD5, authentication password to aaaa, privacy protocol to HMAC-DES, and privacy password to xxxx. Set another user name to 2222, authentication protocol to HMAC-SHA, authentication password to bbbb, privacy protocol to HMAC-DES, and privacy password to yyyy, as shown in Figure 127.

2. Create group and add user 1111 and user 2222 to the group, as shown in Figure 128.

3. Create a context name, that is, context, as shown in Figure 129.

4. Create view table view-all includes all nodes of MIB tree 1, view-no does not include any

node of MIB tree 1, as shown in Figure 130.

5. Configure the SNMP v3 access table. Set the group name to group, context name to context, context match to exact, security level to AuthNoPriv, readView to view-all, writeView to view-no, and notifyView to view-all, as shown in Figure 131.

6. Enable the trap function and set the port number to 162. Configure the trap entry. Set the trap version to V3, destination IP address to 192.168.0.23, security level to AuthPriv, security name to 1111, context name to context, as shown in Figure 133.

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

6.5 DT-Ring

6.5.1 Introduction

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.

6.5.2 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.

> **Note:**
> 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.

6.5.3 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 Figure 135.

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.
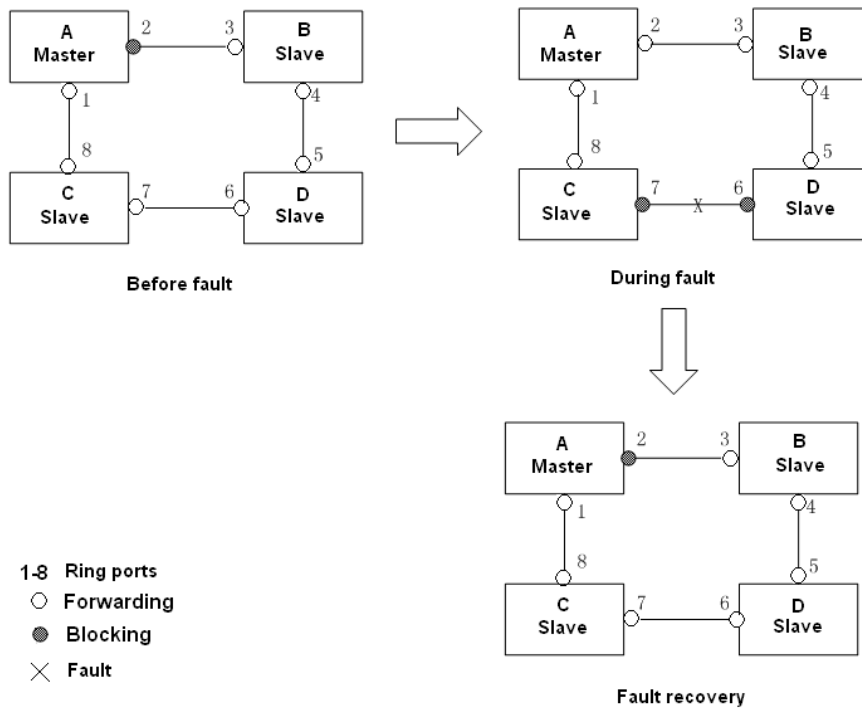
Figure 135 CD Link Fault

4. If link AC is faulty, as shown in Figure 136.

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, port 1 is still in blocking state and port 8 is in forwarding state. No switchover occurs.
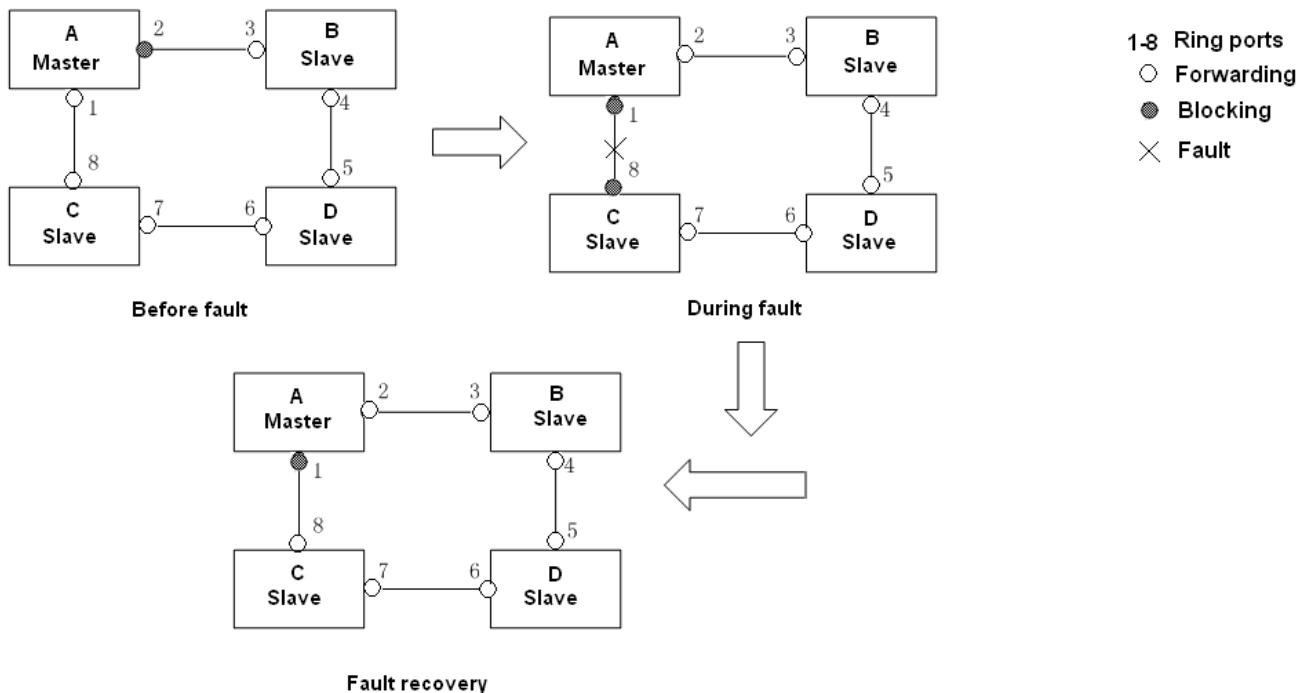
Figure 136 DT-Ring Link Fault

	Caution:
⚠️ 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 Figure 137, 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.
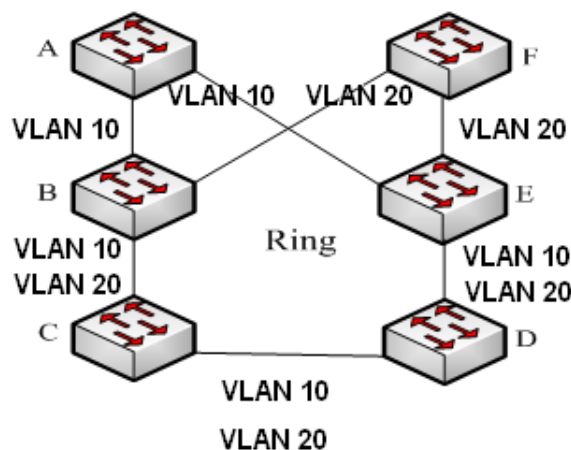
Figure 137 DT-Ring-VLAN

	Note:
📝 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 Figure 138. 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.
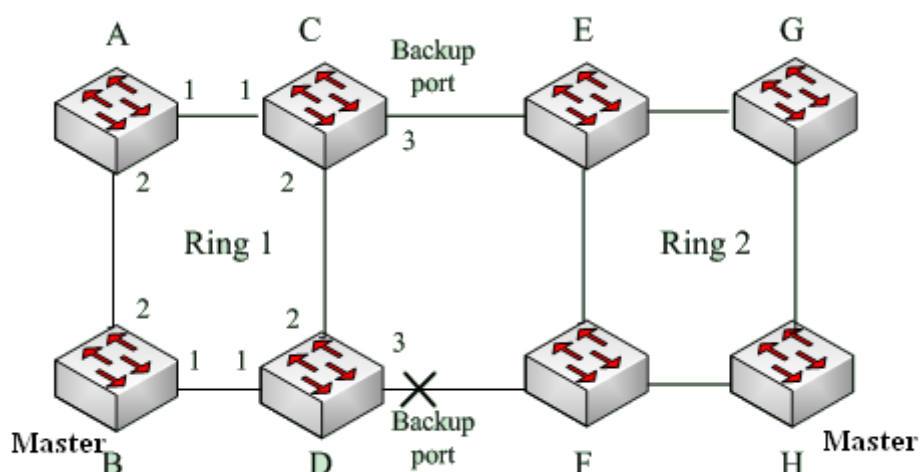
Figure 138 DT-Ring+ Topology

> **Caution:**
>
> Link status change affects the status of backup ports.

6.5.4 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.

6.5.5 Web Configuration

1. Configure redundant ring mode.

Click [Device Advanced Configuration] → [DT-Ring Configuration] → [DT-Ring Mode] to enter ring mode configuration page, as shown in Figure 139.

Redundancy Mode Set   DT-PORT ⌄

Apply
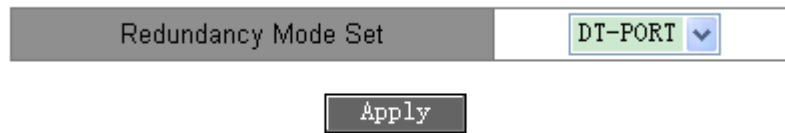
Figure 139 Redundant Ring Mode Configuration

Redundancy Mode Set

Options: Disable/DT-PORT/DT-VLAN

Default: Disable

Function: Enable/disable DT-Ring protocol and choose redundant ring mode.

> **Caution:**
> ➤ Port-based ring protocols include RSTP, DT-Ring-Port, and DRP-Port, and VLAN-based
>   ring protocols include MSTP, 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. Create DT-Ring.

Click [Device Advanced Configuration] → [DT-Ring Configuration] → [DT-Ring Configuration]
to create DT-Ring, as shown in Figure 140.

DT-Ring List

Add
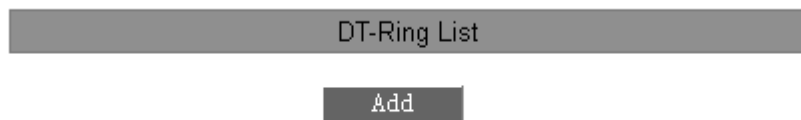
Figure 140 Creating DT-Ring

Click <Add> to create DT-Ring.

3. Configure DT-Ring and DT-VLAN-Ring, as shown in Figure 141 and Figure 142.

Redundancy	DT-Ring
Domain ID	1
Domain name	a
Station Type	Master
Ring Port1	1/1
Ring Port2	1/2

DT-Ring+

DT-Ring+	Enable
Backup Port	1/3

Apply   Back

Figure 141 DT-Ring Configuration

Redundancy	DT-Ring
Domain ID	1
Domain name	a
Station Type	Master
Ring Port1	1/1
Ring Port2	1/2

DT-Ring+

DT-Ring+	Enable
Backup Port	1/3

Add VLAN List

VLAN Choose	VLAN ID	VLAN Name
☑	1	default
☑	2	VLAN0002

Apply   Back

Figure 142 DT-VLAN-Ring Configuration

Redundancy

Forced configuration: DT-Ring

Domain ID

Configuration rang: 1~32

Function: The domain ID is used to distinguish different rings. One switch supports a maximum of 16 VLAN-based rings, the number of port-based rings depends on the number of switch ports.

Domain name

Range: 1~31 characters

Function: Configure the domain name.

Station Type

Options: Master/Slave

Default: Master

Function: Select the switch role in a ring.

Ring port 1/Ring port 2

Options: all switch ports

Function: Select two ring ports.

Caution:

➢ DT-Ring ring port or backup port and port channel are mutually exclusive. A DT-Ring ring port or backup port cannot be added to a port channel; a port in a port channel cannot be configured as a DT-Ring ring port or backup port.

➢ DT-Ring ring port or backup port and a mirroring destination port are mutually exclusive. A DT-Ring ring port or backup port cannot be configured as a mirroring destination port; a mirroring 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 cannot 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 cannot be configured as DT-Ring-Port ring port or backup port.

➢ It is not recommended that ports in an 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 an isolation group.

DT-Ring+

Options: Enable/Disable

Default: Disable

Function: Enable/disable DT-Ring+.

Backup port

Options: all switch ports

Function: Set a port to backup port.

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

Add VLAN list

Options: all created VLANs

Function: Select the VLANs for the ring port.

After setting is completed, DT-Ring List shows all created rings, as shown in Figure 143.

DT-Ring List
a-1
b-2

Add

Figure 143 DT-Ring List

4. View and modify DT-Ring configuration.

Click a DT-Ring entry in Figure 143 to show its ring configuration and modify it, as shown in Figure 144.

Redundancy	DT-Ring
Domain ID	1
Domain name	a
Station Type	Master
Ring Port1	1/1
Ring Port2	1/2

DT-Ring+

DT-Ring+	Enable
Backup Port	1/3

Apply   Delete   Back

Figure 144 DT-Ring Configuration

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

5. View DT-Ring and port status, as shown in Figure 145.

DT-Ring State List

Redundancy	DT-Ring
Ring Port1	forwarding
Ring Port2	blocking
Ring State	RING-CLOSE

Redundancy	DT-Ring+
Equipment IP	192.168.0.4
Equipment MAC	00-00-00-00-00-01
BackupPort Status	blocking

Figure 145 DT-Ring State

6.5.6 Typical Configuration Example

As shown in Figure 138, Switch A, B, C, and D form Ring 1; Switch E, F, G, and H form ring 2. Links CE and DF are the backup links between Ring 1 and Ring 2.

Configuration on Switch A:

1. Domain ID: 1; Domain name: Ring; Ring port: port 1 and port2; Station type: Slave;

DT-Ring+: Disable; do not set backup ports, as shown in Figure 141.

Configuration on Switch B:

2. Domain ID: 1; Domain name: Ring; Ring port: port 1 and port 2; Station type: Master;

DT-Ring+: Disable; do not set backup ports, as shown in Figure 141.

Configuration on Switch C and Switch D:

3. Domain ID: 1; Domain name: Ring; Ring port: port 1 and port2; Station type: Slave;

DT-Ring+: Enable; Backup port: port 3, as shown in Figure 141.

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

4. Domain ID: 2; Domain name: Ring; Ring port: port 1 and port2; Station type: Slave;

DT-Ring+: Disable; do not set backup ports, as shown in Figure 141.

Configuration on Switch H:

5. Domain ID: 2; Domain name: Ring; Ring port: port 1 and port2; Station type: Master;

DT-Ring+: Disable; do not set backup ports, as shown in Figure 141.

6.6 STP/RSTP

6.6.1 Introduction

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.

6.6.2 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.

6.6.3 BPDU

To prevent loops, all the bridges of a LAN calculate a spanning tree. The calculation process involves transmitting BPDUs among devices to determine the network topology. Table 7 shows the data structure of a BPDU.

Table 7 BPDU

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

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

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

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

designated bridge (6 bytes).

Designated port ID: port priority+port number.

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

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

Hello time: interval for sending BPDUs.

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

6.6.4 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.

6.6.5 Web Configuration

1. Enable RSTP.

Click [Device Advanced Configuration] → [RSTP configuration] → [RSTP configuration] to

enter RSTP configuration page, as shown in Figure 146.

Figure 146   Enabling RSTP/STP

Protocol Status

Options: Enable/Disable

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 MSTP, 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 Figure 147.

Bridge Priority	32768	(0-65535)
Hello Time(s)	2	(1-10)
Max Age Time(s)	20	(6-40)
Forward Delay Time(s)	15	(4-30)
Message-age Increment	Default	

Apply

Figure 147 Setting Time Parameters of the Network Bridge

Bridge Priority

Range: 0~65535. The step is 4096.

Default: 32768

Function: Configure the priority of the network bridge.

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

Hello Time

Range: 1~10s

Default: 2s

Function: Configure the interval for sending BPDU.

Max Age Time

Range: 6~40s

Default: 20s

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

Forward Delay Time

Range: 4~30s

Default: 15s

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

Message-age Increment

Options: Compulsion/Default

Default: Default

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

Description: In compulsion mode, the value is 1.

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

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

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

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

3. Enable RSTP on ports, as shown in Figure 148.

Port Configuration

Port	Type	Protocol Status	Port Priority(0~255)	Auto Cost Count	Path Cost(1~200000000)
1/1	FE	☑	128	☑	2000000
1/2	FE	☑	128	☐	2000000
1/3	FE	☑	128	☑	2000000
1/4	FE	☑	128	☐	2000000
1/5	FE	☐	128	☑	2000000
1/6	FE	☐	128	☑	2000000
1/7	FE	☐	128	☑	2000000
1/8	FE	☐	128	☑	2000000
1/9	FE	☐	128	☑	2000000
1/10	FE	☐	128	☑	2000000
1/11	FE	☐	128	☑	2000000
1/12	FE	☐	128	☑	2000000

Apply

Figure 148 Port Settings

Protocol Status

Options: Enable/Disable

Default: Disable

Function: Enable or disable STP/RSTP on ports.

Caution:

➢ RSTP port and port channel are mutually exclusive. A RSTP port cannot be added to a port channel; a port in a port channel cannot be configured as a RSTP port.

➢ RSTP port and a mirroring destination port are mutually exclusive. A RSTP port cannot be configured as a mirroring destination port; a mirroring destination port 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, a RSTP port cannot be configured as DRP-Port/DT-Ring-Port ring port, or DRP-Port/DT-Ring-Port backup port; DRP-Port/DT-Ring-Port ring port, and DRP-Port/DT-Ring-Port backup port cannot be configured as a RSTP port.

➢ It is not recommended that ports in an isolation group are configured as RSTP ports at the

same time, and RSTP ports cannot be added to a isolation group

Port Priority

Range: 0~255. The step is 16.

Default: 128

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

Path Cost

Range: 1~200000000

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

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

Auto 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 Figure 149.

Root Info

Root MAC	00:1e:cd:11:01:b1
Root Priority	0x8000
Root Path Cost	200000
Root Port	1/3
Max Age(s)	20
Hello Time(s)	2
Forward Delay(s)	15

Bridge Info

Bridge MAC	08:00:3e:32:53:22
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
1/1	0x80	200000	Root	Forwarding	Up
1/2	0x80	2000000	Alternate	Discarding	Up
1/3	0x80	200000	Disabled	Discarding	Down
1/4	0x80	2000000	Disabled	Discarding	Down

Figure 149 RSTP Status Information

6.6.6 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 Figure 150.
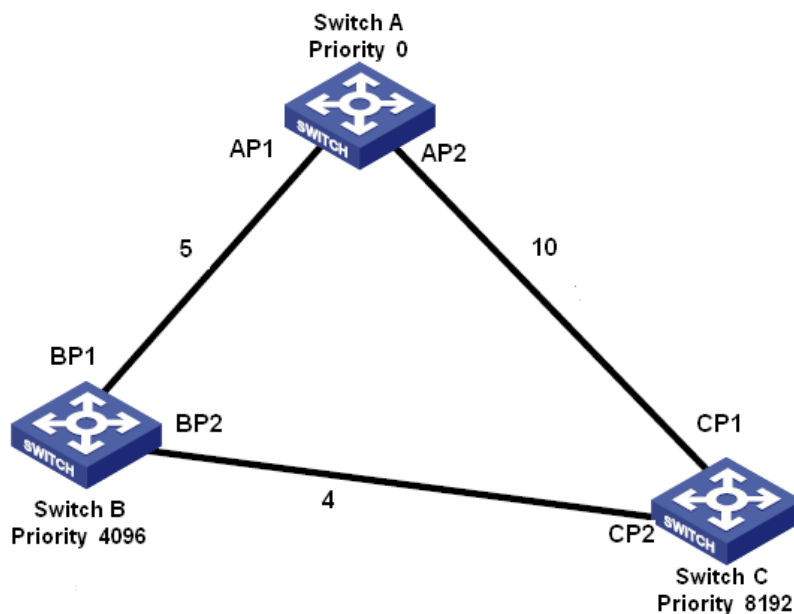
Figure 150 RSTP Configuration Example

Configuration on Switch A:

1. Set priority to 0 and time parameters to default values, as shown in Figure 147.

2. Set the path cost of port 1 to 5 and that of port 2 to 10, as shown in Figure 148.

Configuration on Switch B:

1. Set priority to 4096 and time parameters to default values, as shown in Figure 147.

2. Set the path cost of port 1 to 5 and that of port 2 to 4, as shown in Figure 148.

Configuration on Switch C:

1. Set priority to 8192 and time parameters to default values, as shown in Figure 147.

2. Set the path cost of port 1 to 10 and that of port 2 to 4, as shown in Figure 148.

➢ 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.

6.7 DRP

6.7.1 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.

6.7.2 Concepts

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.

Primary port: indicates the ring port (on the root) whose status is configured as forwarding forcibly by user when the ring is closed.

> **Caution:**
> ➢ If no primary port is configured on the root, 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.
> ➢ 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.

6.7.3 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 an 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. 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.

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 status. 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.

3. When link CD recovers, D is still the Root because its vector is larger than the vector of C.

➢ If no primary port is configured on D, port 7 is still in blocking state and port 8 is in forwarding state.

➢ If port 7 on D is configured as primary port, port 7 changes to forwarding state and port 8 is in blocking state.

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.
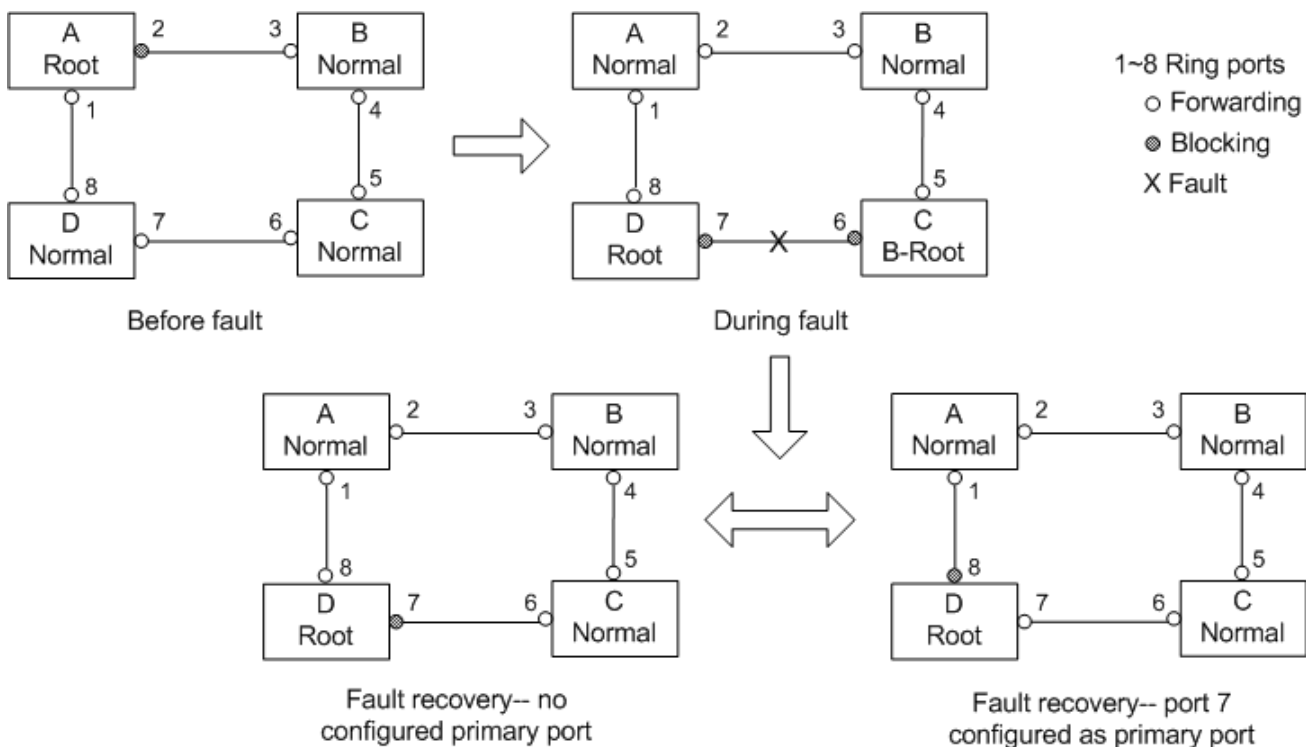
Figure151 DRP Link Fault

> **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 sets the mapping between VLAN and STG instance. One or multiple VLANs can be mapped to one STG instance.

STG instance: Each STG instance corresponds to one DRP-VLAN-Based ring. With DRP, STG instance records device roles and port status. After receiving a packet, the switch determines the mapped STG instance based on the VLAN attribute of the packet. The switch processes the packet according to the device roles and port status of the instance.

With the configuration of DRP-VLAN-Based ring, packets of different VLANs can be forwarded along different paths. As shown in Figure152, the mapping between STG instances and VLANs are the same among all devices.

STG1-based ring link: AB-BC-CD-DE-EA. Packets of VLAN10 and VLAN20 are forwarded along the link. A is the Root.

STG2-based ring link: FB-BC-CD-DE-EF. Packets of VLAN30 are forwarded along the link. F is the Root.

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.
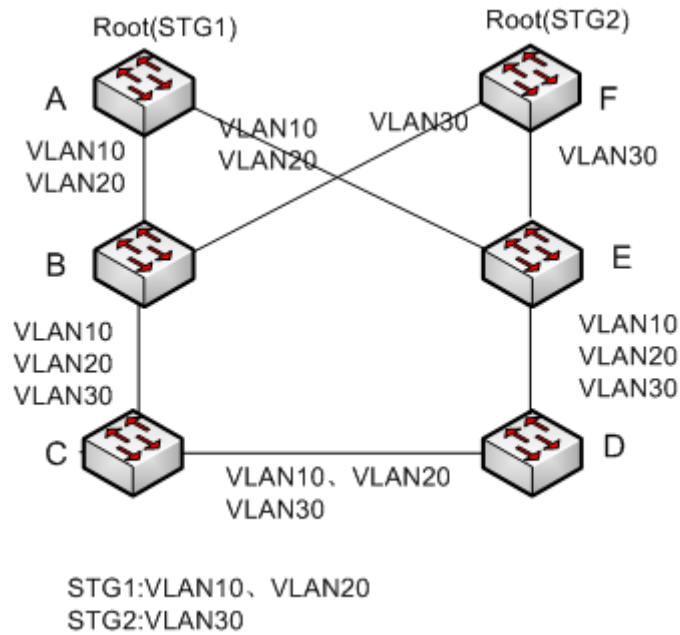
Figure152 DRP-VLAN-Based

> **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.
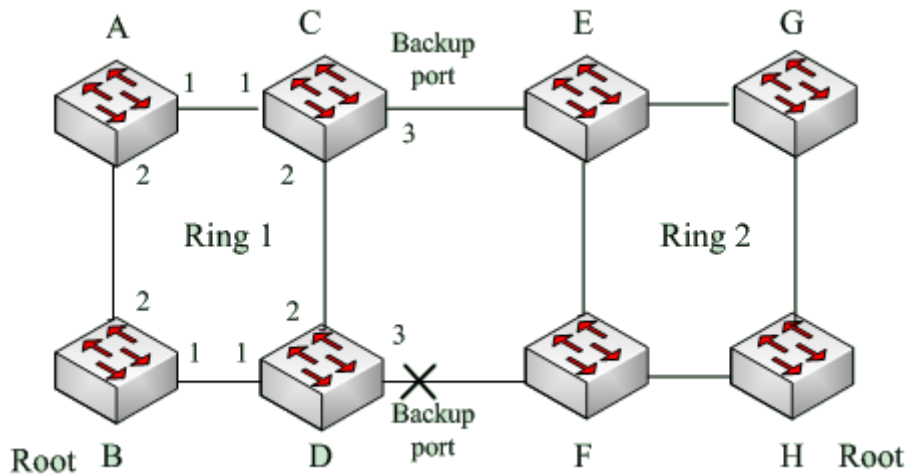
Figure153 DRP Backup

⚠ **CAUTION**	**Caution:**
	Link status change affects the status of backup ports.

6.8 DHP

6.8.1 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.
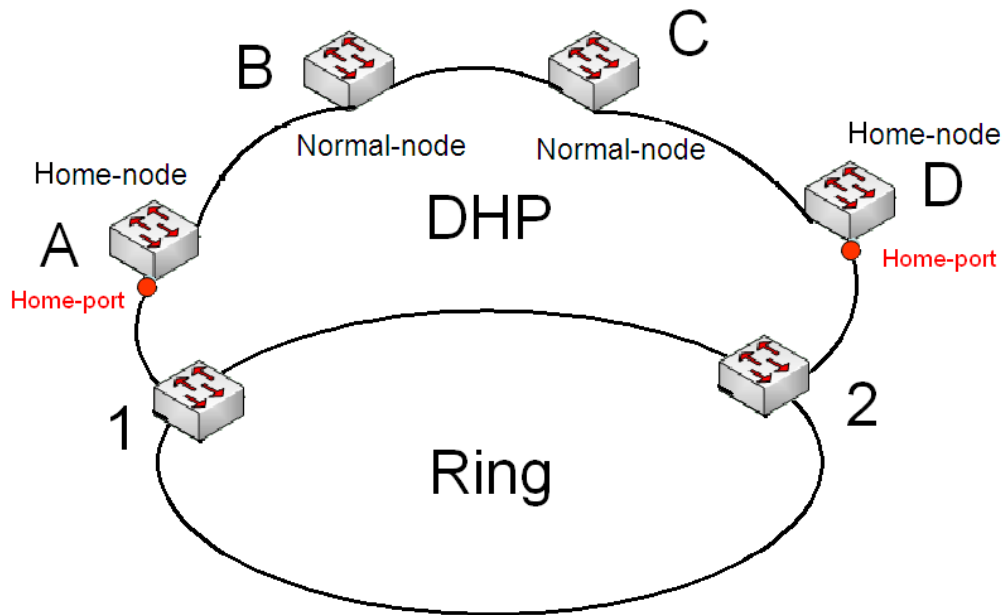
Figure154 DHP Application

6.8.2 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.

6.8.3 Implementation
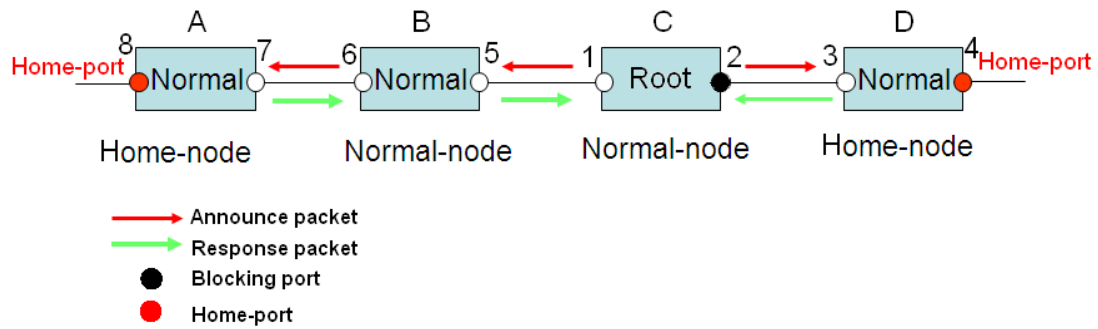
Figure155 DHP Configuration

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.

Figure156 DHP Fault Recovery
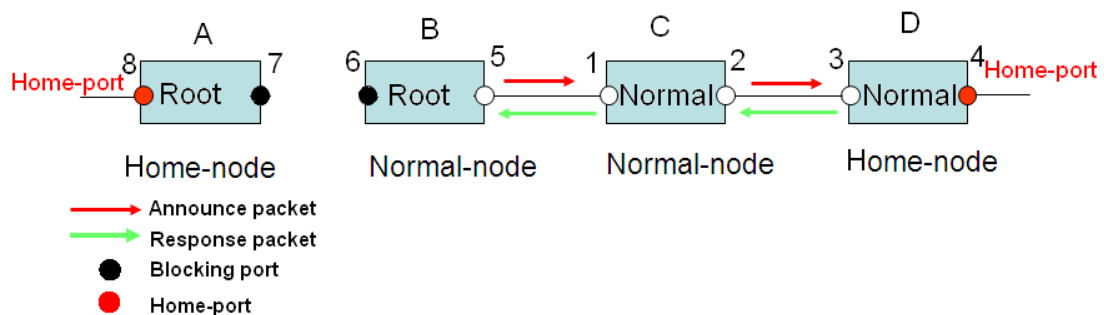
Figure156 DHP Fault Recovery

6.8.4 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.

6.8.5 Web Configuration

1. Configure the DRP mode.

Click [Device Advanced Configuration] → [DRP configuration] → [DRP Mode] to enter the DRP mode configuration page, as shown in the following figure.

Figure157 DRP Mode

DRP Mode

Options: Port Based/VLAN Based

Default: Port Based

Function: Configure the DRP mode.

Caution:

➢ Port-based ring protocols include RSTP, DT-Ring-Port, and DRP-Port, and VLAN-based ring protocols include MSTP, 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. Create a DRP-Port-Based entry.

Click [Device Advanced Configuration] → [DRP configuration] → [Port-Based DRP Configuration] to enter the DRP entry creating page, as shown in the following figure.

DRP list

| Add |

Figure158 Creating a DRP-Port-Based Entry

Click <Add> to create a DRP entry.

➢ Set parameters for the DRP-Port-Based entry, as shown in the following figure.

Redundancy	DRP
Domain ID	1
Domain name	a
Ring Port1	1/1
Ring Port2	1/2
DHP Mode	Home-node
DHP Home Port	Ring-Port-1
Crc Threshold	100
Role-Priority	128
Backup Port	---------
Primary-Port	Ring-Port-1

| Apply | | Back |

Figure159 Configuring a DRP-Port-Based Entry

Redundancy

Mandatory configuration: DRP

Domain ID

Range: 1~32

Description: Each ring has a unique domain ID. The number of port-based rings depends on the number of switch ports.

Domain name

Range: 1~31 characters

Function: Configure the domain name.

Ring Port 1/Ring Port 2

Options: all switch ports

Function: Select two ring ports.

DHP Mode

Options: Disable/Normal-node/Home-node

Default: Disable

Function: Disable DHP or configure the DHP mode.

DHP 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.

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.

Role-Priority

Range: 0~255

Default: 128

Function: Configure the priority of a switch.

Backup Port

Options: all switch ports

Function: Configure the backup port.

⚠ CAUTION	**Caution:** Do not configure a ring port as a backup port.

Primary-Port

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

Default: --

Function: Configure the primary port. When the ring is closed, the primary port on root is in forwarding state.

After you have completed setting the parameters, the created entry will be displayed in the DRP List, as shown in the following figure.

DRP list
a-1

Add

Figure160 DRP-Port-Based List

⚠ CAUTION	**Caution:** ➢ DRP ring port or backup port and port channel are mutually exclusive. A DRP ring port or backup port cannot be added to a port channel; a port in a port channel cannot be configured as a DRP ring port or backup port. ➢ DRP ring port or backup port and a mirroring destination port are mutually exclusive. A DRP ring port or backup port cannot be configured as a mirroring destination port; a mirroring 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 cannot 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 cannot be configured as DRP-Port

ring port or backup port.

➢ It is not recommended that ports in an isolation group are configured as DRP ports and

backup ports at the same time, and DRP ports and backup ports cannot be added to an

isolation group.

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

Click the DRP entry in Figure160. You can view and modify the parameter settings of the

entry, as shown in the following figure.

Redundancy	DRP
Domain ID	1
Domain name	a
Ring Port1	1/1
Ring Port2	1/2
DHP Mode	Home-node
DHP Home Port	Ring-Port-1
Crc Threshold	100
Role-Priority	128
Backup Port	---------
Primary-Port	---

Apply   Delete   Back

Figure161 Querying and Modifying 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.

Ring State List

Redundancy	DRP
Role State	ROOT
Ring Port1	BLOCK
Ring Port2	FORWARD
Backup Port	------
Ring State	RING-CLOSE

Figure162 DRP-Port-Based Status Query

3. Configure a DRP-VLAN-Based entry.

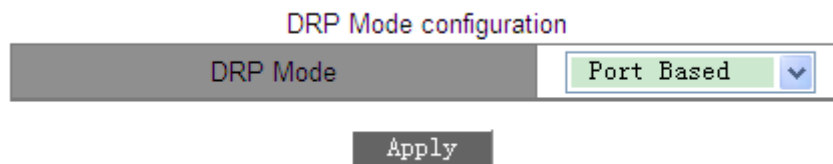Click [Device Advanced Configuration] → [DRP configuration] → [DRP Mode] to enter the DRP mode configuration page. Select VLAN Based.

➢ DRP instance configuration

Click [Device Advanced Configuration] → [DRP configuration] → [VLAN-Based DRP Configuration] → [STG Instance Configuration] to enter the DRP instance configuration page, as shown in the following figure.

DRP STG Instance Configuration

STG Instance No.(16-31)	18

Add   Delete

STG Instance
16   17

Figure163 DRP Instance Configuration

STG Instance No. (16-31)

Range: 16~31

Function: Configure the DRP instance ID.

➢ VLAN configuration in a DRP instance

Click [Device Advanced Configuration] → [DRP configuration] → [VLAN-Based DRP Configuration] → [STG Instance Protocol VLAN Configuration] to enter the DRP instance VLAN configuration page, as shown in the following figure.

Figure164 VLAN Configuration for a DRP Instance

DRP STG Instance VLAN Configuration

Portfolio: {STG instance ID, VLAN ID}

Range: {16~31, 1~4093}

Function: Configure the VLAN ID for the DRP instance.

Description: One instance can correspond to multiple VLAN IDs, but one VLAN ID can correspond to only one instance.

➢ View the information about DRP instances.

Click [Device Advanced Configuration] → [DRP configuration] → [VLAN-Based DRP Configuration] → [STG Instance Information] to enter the DRP instance information page, as shown in the following figure.

Figure165 DRP Instance Information

➢ DRP-VLAN-Based configuration

Click [Device Advanced Configuration] → [DRP configuration] → [VLAN-Based DRP Configuration] to enter the DRP-VLAN-Based creating page, as shown in the following figure.
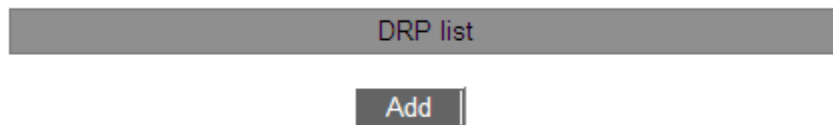
Figure166 Creating a DRP-VLAN-Based Entry

Click <Add> to create a DRP entry. Set parameters for the entry, as shown in the following figure.

Figure167 Configuring a DRP-VLAN-Based Entry

Redundancy

Mandatory configuration: DRP

Domain ID

Range: 1~32

Function: Each ring has a unique domain ID. One switch supports a maximum of 8 VLAN-based rings.

Domain name

Range: 1~31 characters

Function: Configure the domain name.

Ring Port 1/Ring Port 2

Options: all switch ports

Function: Select two ring ports.

DHP Mode

Options: Disable/Normal-node/Home-node

Default: Disable

Function: Disable DHP or configure the DHP mode.

DHP 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.

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.

Role-Priority

Range: 0~255

Default: 128

Function: Configure the priority of a switch.

Caution:

➢ DRP ring port or backup port and port channel are mutually exclusive. A DRP ring port or backup port cannot be added to a port channel; a port in a port channel cannot be configured as a DRP ring port or backup port.

➢ DRP ring port or backup port and a mirroring destination are mutually exclusive. A DRP ring port or backup port cannot be configured as a mirroring destination port; a mirroring

destination port cannot be configured as a DRP ring port or backup port.

➢ It is not recommended that ports in an isolation group are configured as DRP ports and backup ports at the same time, and DRP ports and backup ports cannot be added to an isolation group.

Backup Port

Options: all switch ports

Function: Configure the backup port.

> **Caution:**
>
> Do not configure a ring port as a backup port.

STG Instance

Options: created DRP instances

Function: Configure the instance for the ring.

Description: The blocking port in the ring will block the data packets of all VLANs that correspond to the instance.

Protocol VLAN (1~4093)

Range: 1~4093

Description: The VLAN ID must be one of those that correspond to the STG instance.

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

Primary-Port

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

Default: --

Function: Configure the primary port. When the ring is closed, the primary port on root is in forwarding state.

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

Figure168 DRP-VLAN-Port List

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

Figure169 Viewing and Modifying a DRP-VLAN-Based Entry

After modification is completed, click <Apply> for the modification to 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.

163

Figure170 DRP-VLAN-Based Entry Query

6.8.6 Typical Configuration Example

As shown in Figure153, 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 Figure159.

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 Figure159.

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 Figure159.

6.9 MSTP Configuration

6.9.1 Introduction

Although RSTP achieves rapid convergence, it also has the following defect just as the STP: all bridges in the LAN share one spanning tree and packets of all VLANs are forwarded along the spanning tree. As shown in Figure 171, certain configurations may block the link between switch A and switch C. Because switch B and switch D are not in VLAN 1, they cannot forward the packets of VLAN 1. As a result, the VLAN 1 port of switch A cannot communicate with that of switch C.
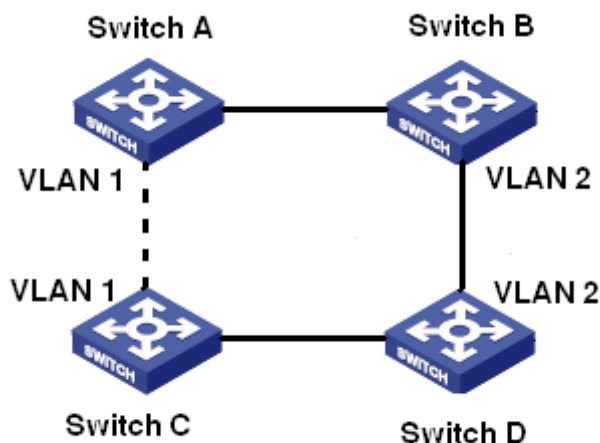
Figure 171 RSTP Disadvantage

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

MSTP maps one or multiple VLANs into one instance. Switches with the same configuration form a region. Each region contains multiple mutually independent spanning trees. The region serves as a switch node. It participates in the calculation with other regions based on the spanning tree algorithm, calculating an overall spanning tree. Based on this algorithm, the network in Figure 171 forms the topology shown in Figure 172. Both switch A and switch C are in Region1. No link is blocked because the region contains no loops. This is the same with Region2. Region1 and Region2 are similar to switch nodes. These two "switches" form a loop. Therefore, a link should be blocked.
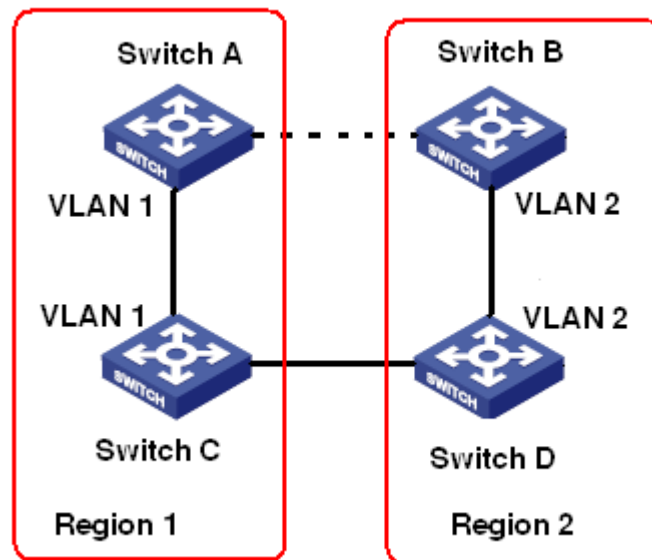
Figure 172 MSTP Topology

6.9.2 Basic Concepts

Learn MSTP concepts based on Figure 173 to Figure 176.
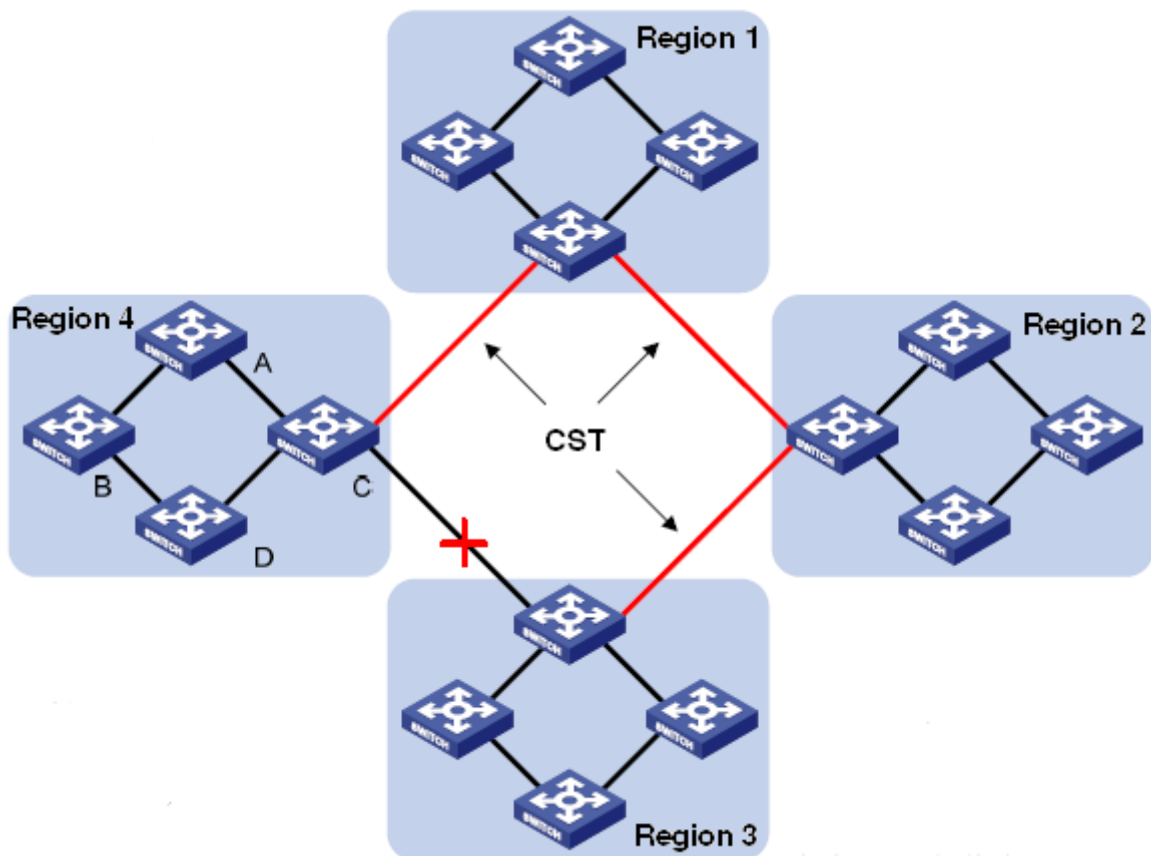
Figure 173 MSTP Concepts
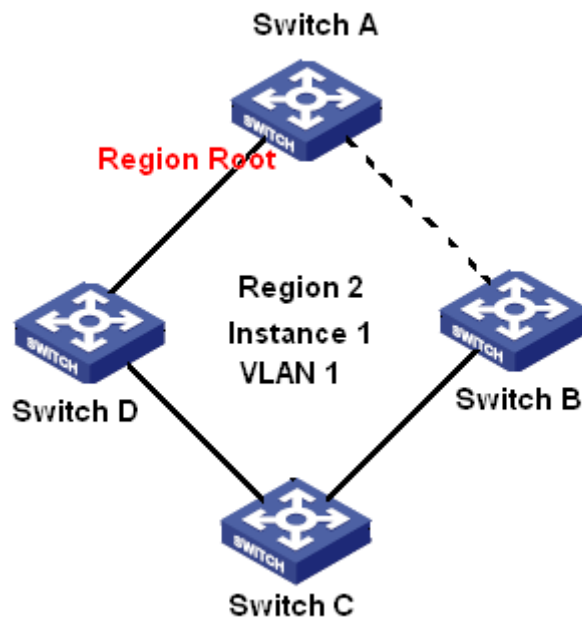
Figure 174 VLAN 1 Mapping to Instance 1
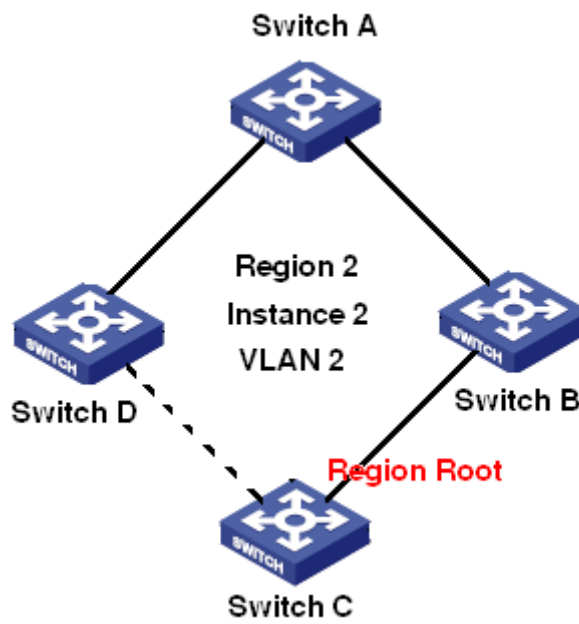
Figure 175 VLAN2 Mapping to Instance 2
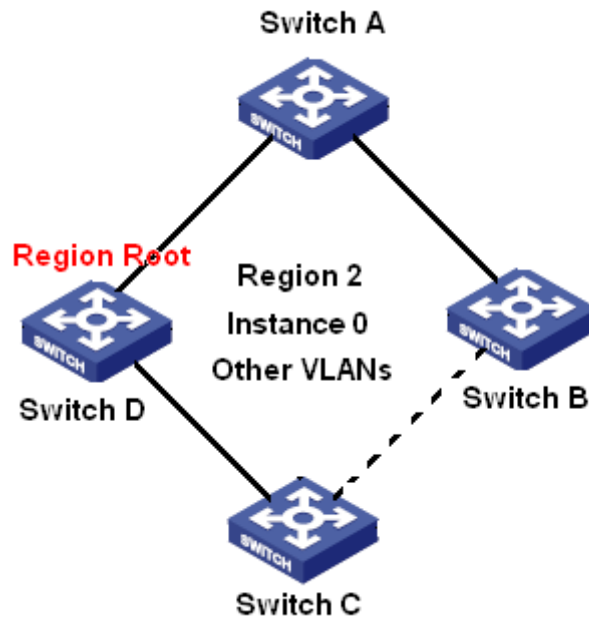
Figure 176 Other VLAN Mapping to Instance 0

Instance: a collection of multiple VLANs. One VLAN (as shown in Figure 174 and Figure 175) or multiple VLANs with the same topology (as shown in Figure 176) can be mapped to one instance; that is, one VLAN can form a spanning tree and multiple VLANs can share one spanning tree. Different instances are mapped to different spanning trees. Instance 0 is the spanning tree for the devices of all regions, while the other instances are the spanning trees for the devices of a specific region.

Multiple Spanning Tree Region (MST region): Switches with the same MSTP region name, revision level, and VLAN-to-instance mapping are in the same MST region. As shown in Figure 173, Region1, Region2, Region3, and Region4 are four different MST regions.

VLAN mapping table: consists of the mapping between VLANs and spanning trees. In Figure 173, VLAN mapping table of region 2 is the mapping between VLAN 1 and instance 1, as shown in Figure 174; VLAN 2 is mapped to instance 2, as shown in Figure 175. The other VLANs are mapped to instance 0, as shown in Figure 176.

Common and Internal Spanning Tree (CIST): indicates instance 0, that is, the spanning tree covering all the devices on a switching network. As shown in Figure 173, the CIST comprises IST and CST.

Internal Spanning Tree (IST): indicates the CIST segment in the MST region, that is,

instance 0 of each region, as shown in Figure 176.

Common Spanning Tree (CST): indicates the spanning tree connecting all MST regions in a switching network. If each MST region is a device node, the CST is the spanning tree calculated based on STP/RSTP by these device nodes. As shown in Figure 173, the red lines indicate the spanning tree.

MSTI (Multiple Spanning Tree Instance): one MST region can form multiple spanning trees and they are independent of each other. Each spanning tree is a MSTI, as shown in Figure 174 and Figure 175. IST is also a special MSTI.

Common root: indicates the root bridge of the CIST. The switch with the smallest root bridge ID in a network is the common root.

In an MST region, spanning trees have different topologies, and their regional roots can also be different. As shown in Figure 174, Figure 175, and Figure 176, the three instances have different regional roots. The root bridge of the MSTI is calculated based on STP/RSTP in the current MST region. The root bridge of the IST is the device that is connected to another MST region and selected based on the priority information received.

Boundary port: indicates the port that connects an MST region to another MST region, STP running region, or RSTP running region.

Port state: A port can be in either of the following states based on whether it is learning MAC addresses and forwarding traffic.

Forwarding state: indicates that a port learns MAC addresses and forwards traffic.

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

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

Root port: indicates the best port from a non-root bridge to the root bridge, that is, the port with the smallest cost to the root bridge. A non-root bridge communicates with the root bridge through the root port. A non-root bridge has only one root port. The root bridge has no root port. The root port can be in forwarding, learning, or discarding state.

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

or discarding state.

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

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

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

6.9.3 MSTP Implementation

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

1. CIST calculation

➢ A device sends and receives BPDU packets. Based on the comparison of MSTP configuration messages, the device with the highest priority is selected as the common root of the CIST.

➢ An IST is calculated in each MST region.

➢ Each MST region is considered as a single device and CST is calculated between regions.

➢ CST and IST constitute the CIST of the entire network.

2. MSTI calculation

In an MST region, MSTP generates different spanning trees for VLANs based on the mapping between VLANs and spanning trees. Each spanning tree is calculated

independently. The calculation process is similar to that in STP.

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

regions, VLAN packets are forwarded along the CST.

6.9.4 Web Configuration

1. Enable MSTP protocol.

Click [Device Advanced Configuration] → [MSTP configuration] → [Enable MSTP] to enter

MSTP protocol configuration page, as shown in Figure 177.
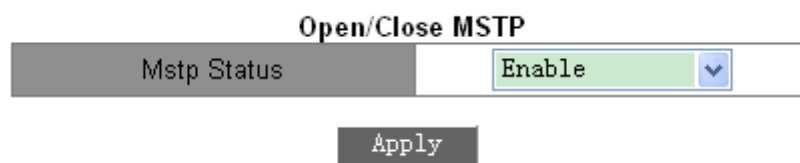
Figure 177 Enabling MSTP

Mstp status

Options: Enable/Disable

Default: Disable

Function: Enable/Disable MSTP.

	Caution:
⚠️ CAUTION	➢ Port-based ring protocols include RSTP, DT-Ring-Port, and DRP-Port, and VLAN-based ring protocols include MSTP, 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. Force port to work in MSTP mode, as shown in Figure 178.
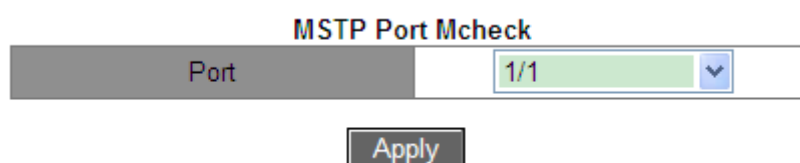
Figure 178 Forcing Port to Work in MSTP Mode

Port

Options: all switch ports

Function: When MSTP-enabled port is connected to STP-enable device, this port will be automatically changed to work in STP mode. If the STP-enable device is removed, this port won't automatically go back to work in MSTP mode. If wish switch to go back to work in MSTP mode in this condition, please set this function for port. Once port receives STP message again, the port will automatically change to work in STP mode again.

⚠ CAUTION	**Caution:** This configuration will take effect only when switch run in MSTP mode; otherwise, it is useless.

3. Configure MSTP state of port.

Click [Device Advanced Configuration] → [MSTP configuration] → [Enable Port MSTP] to enter MSTP protocol configuration page, as shown in Figure 179.
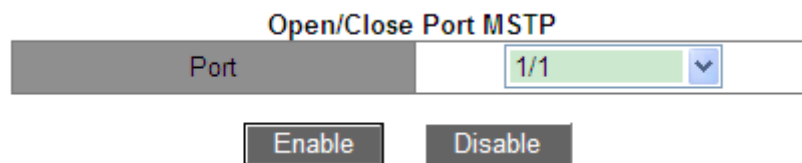
Figure 179 Configuring MSTP on Port

Port

Options: all switch ports

Default: If global MSTP protocol has been enabled, MSTP status of all ports is open.

Function: Enable/Disable MSTP on port.

4. Configure MST region parameter.

Click [Device Advanced Configuration] → [MSTP configuration] → [MSTP Region Config] to enter MST region parameter configuration page, as shown in Figure 180.

Figure 180 Configuring MST Region Parameters

MSTP Region Name config

Range: 1-32 characters

Default: device MAC address

Function: Configure the name of MST region.

MSTP Revision level config

Options: 0~65535

Default: 0

Function: Configure the revision parameter of MSTP region.

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

5. Configure VLAN mapping table, as shown in Figure 181.

Figure 181 Configuring VLAN Mapping Table

{MSTP Instance ID, VLAN list}

Range: {0~16, 1~4094}

Default: {0, 1~4094}

Function: Configure the VLAN mapping table in MST region.

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

⚠ CAUTION	**Caution:** <Del> cannot delete the VLAN list of instance 0.

After setting is completed, the "Instance List" will show the mapping between VLAN and instance.

6. Configure the bridge priority of the switch in designated instance.

Click [Device Advanced Configuration] → [MSTP configuration] → [MSTP Instance Config] to enter MSTP instance parameter configuration page, as shown in Figure 182.

MSTP MST Priority

MSTP Instance ID	0
MSTP Bridge Priority	32768

Apply   Default

Figure 182 Configuring Bridge Priority in Designated Instance

MSTP Instance ID

Options: all created instances

MSTP Bridge Priority

Range: 0~61440 with the step length of 4096

Default: 32768

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

Description: The bridge priority determines whether the switch can be elected to regional root of spanning tree instance. The smaller value is, the higher priority is. By setting a lower priority, a certain device can be designated to root bridge of spanning tree. The

MSTP-enabled device can be configured with different priorities in different spanning tree instance.

7. Configure port priority and path cost in the designated instance, as shown in Figure 183.

Figure 183 Setting Port Priority and Path Cost in Designated Instance

MSTP Instance ID

Options: all created instances

Port

Options: all switch ports

Priority

Range: 0~240 with step length of 16

Default: 128

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

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

MSTP Port Path cost

Range: 1~200000000

Default: as listed in Table 9 and Table 10.

Table 9 Default Path Cost of Common Port

Port Type	Default Path Cost	Recommended Range
10Mbps	2000000	2000000~20000000

| 100Mbps | 200000 | 200000~2000000 |
| 1Gbps | 20000 | 20000~200000 |

Table 10 Default Path Cost of Aggregation Port

Port Type	Number of Aggregation Ports (in Allowed Aggregation Range)	Recommended Range
10Mbps	N	2000000/N
100Mbps	N	200000/N
1Gbps	N	20000/N

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

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

8. Configure MSTP time parameter.

Click [Device Advanced Configuration] → [MSTP configuration] → [MSTP Time Config] to enter MSTP time parameter configuration page, as shown in Figure 184.
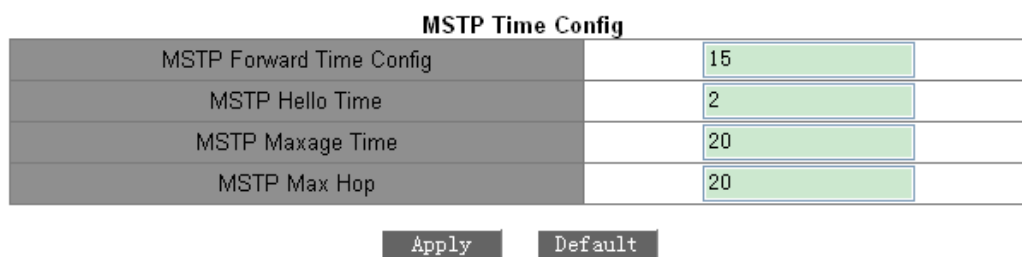
Figure 184 Configuring MSTP Time Parameters

MSTP Forward Time Config

Options: 4~30s

Default: 15s

Function: Configure the time interval for port state transition (Discarding – Learning or

Learning – Forwarding).

MSTP Hello Time

Range: 1~10s

Default: 2s

Function: Configure the time interval for sending BPDUs.

MSTP Max Age Time

Range: 6~40s

Default: 20s

Function: Set the maximum age of BPDU packets.

> **Caution:**
> ➢ The values of Forward Delay Time, Hello Time and Max Age Time should meet the following requirements: 2 * (Forward Delay Time–1.0 seconds) >= Max Age Time; Max Age Time >= 2 * (Hello Time + 1.0 seconds)
> ➢ The default setting is recommended.

MSTP Max Hop

Range: 1~40

Default: 20

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

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

> **Caution:**
> ➢ Only the maximum hop configuration of root bridge in MST region is valid. Non-root bridge device adopts the maximum hop configuration of root bridge.
> ➢ The default setting is recommended.

9. Configure rapid state transition feature of MSTP.

Click [Device Advanced Configuration] → [MSTP configuration] → [MSTP Fast Transfer Config] to enter the configuration page, as shown in Figure 185.

MSTP Fast Transfer Config

Port	1/1
MSTP Port Link Type	AUTO
Set/Cancel Edge Port	Ordinary port

Apply   Default

Figure 185 Configuring Rapid State Transition

MSTP Port Link Type

Options: AUTO/Force True/Force False

Default: AUTO

Function: Set the link type of the port. If the port is connected to a point-to-point link, the port state can be transited rapidly

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

Set/Cancel Edge Port

Options: Edge port/Ordinary port

Default: Ordinary port

Function: Configure the port as Edge port or ordinary port.

Description: When the port is directly connected to end devices, but not connected to other devices or shared segments, this port is an edge port. An edge port can rapidly transit from blocking to forwarding without delay. Once the edge port receives a BPDU message, this port will change to ordinary port again.

10. View MSTP configuration.

Click [Device Advanced Configuration] → [MSTP configuration] → [MSTP Information] to show the MSTP configuration, as shown in Figure 186.

```
                        Information Display
                  -- MSTP Bridge Config Info --
Bridge MAC   :   00:1e:cd:0f:01:01
Bridge Times :   Max Age 20, Hello Time 2, Forward Delay 15
Force Version:   3
######################### Instance 0 #############################
Self Bridge Id    : 32768 -  00:1e:cd:0f:01:01
Root Id           : this switch
Ext.RootPathCost  : 0
Region Root Id    : this switch
Int.RootPathCost  : 0
Root Port ID      : 0
Current port list in Instance 0:
Ethernet1/8 (Total 1)
   PortName      ID      ExtRPC    IntRPC  State Role     DsgBridge      DsgPort
-------------- ------- --------- --------- --- ---- ------------------ -------
   Ethernet1/8 128.008        0         0 FWD DSGN 32768.001ecd0f0101 128.008
```

Figure 186 MSTP Configuration

6.9.5 Typical Configuration Example

As shown in Figure 187, Switch A, B, C, and D belong to the same MST region. The VLANs marked in red indicate the VLAN packets can be transmitted through the links. After configurations are completed, VLAN packets can be forwarded along different spanning tree instances. VLAN 10 packets are forwarded along instance 1 and the root bridge of instance 1 is Switch A; VLAN 30 packets are forwarded along instance 3 and the root bridge of instance 3 is Switch B. VLAN 40 packets are forwarded along instance 4 and the root bridge of instance 4 is Switch C. VLAN 20 packets are forwarded along instance 0 and the root bridge of instance 0 is Switch B.
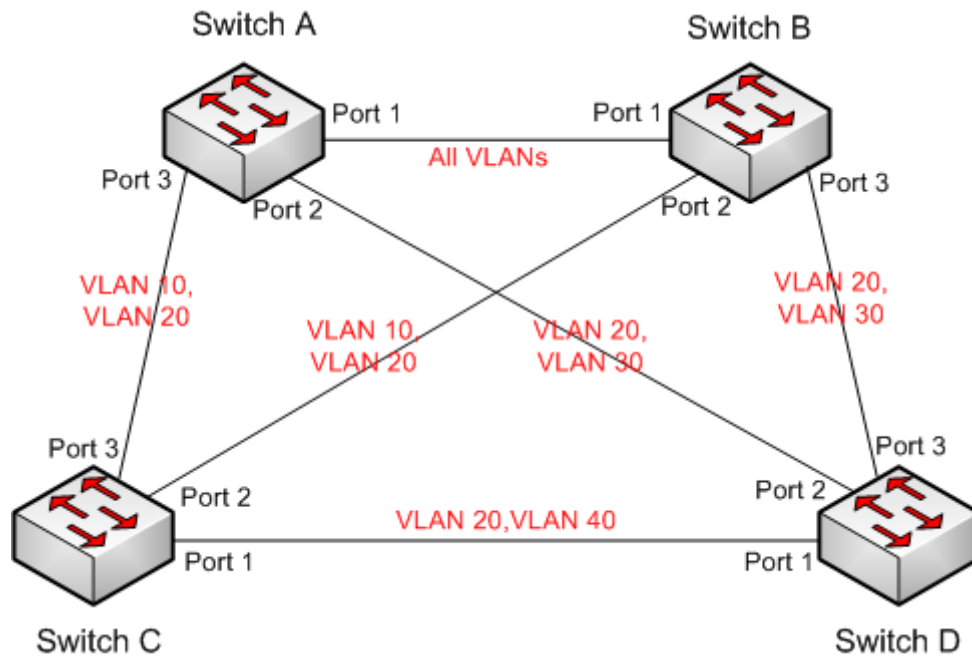
Figure 187 MSTP Typical Configuration Example

Configuration on Switch A:

1. Create VLAN 10, 20, and 30 on Switch A; set the ports to Trunk ports and allow the packets of corresponding VLANs to pass through.

2. Enable global MSTP protocol, as shown in Figure 177.

3. Set the name of MST region to Region and the revision parameter to 0, as shown in Figure 180.

4. Create instance 1, 3, and 4 and map VLAN 10, 30, and 40 to instance 1, 3, and 4 respectively, as shown in Figure 181.

5. Set the switch bridge priority in instance 1 to 4096, and keep default priority in other instances, as shown in Figure 182.

Configuration on Switch B:

6. Create VLAN 10, 20, and 30 on Switch B; set the ports to Trunk ports and allow the packets of corresponding VLANs to pass through.

7. Enable global MSTP protocol, as shown in Figure 177.

8. Set the name of MST region to Region and the revision parameter to 0, as shown in Figure 180.

9. Create instance 1, 3, and 4 and map VLAN 10, 30, and 40 to instance 1, 3, and 4

respectively, as shown in Figure 181.

10. Set switch bridge priority in instance 3 and instance 0 to 4096, and keep default priority in other instances, as shown in Figure 182.

Configuration on Switch C:

11. Create VLAN 10, 20 and 40 on Switch C; set the ports to Trunk ports and allow the packets of corresponding VLANs to pass through.

12. Enable global MSTP protocol, as shown in Figure 177.

13. Set the name of MST region to Region and the revision parameter to 0, as shown in Figure 180.

14. Create instance 1, 3, and 4 and map VLAN 10, 30, and 40 to instance 1, 3, and 4 respectively, as shown in Figure 181.

14. Set the switch bridge priority in instance 4 to 4096, and keep default priority in other instances, as shown in Figure 182.

Configuration on Switch D:

16. Create VLAN 20, 30 and 40 on Switch D; set the ports to Trunk ports and allow the packets of corresponding VLANs to pass through.

17. Enable global MSTP protocol, as shown in Figure 177.

18. Set the name of MST region to Region and the revision parameter to 0, as shown in Figure 180.

19. Create instance 1, 3, and 4 and map VLAN 10, 30, and 40 to instance 1, 3, and 4 respectively, as shown in Figure 181.

When MSTP calculation is completed, the MSTI of each VLAN is as follows:
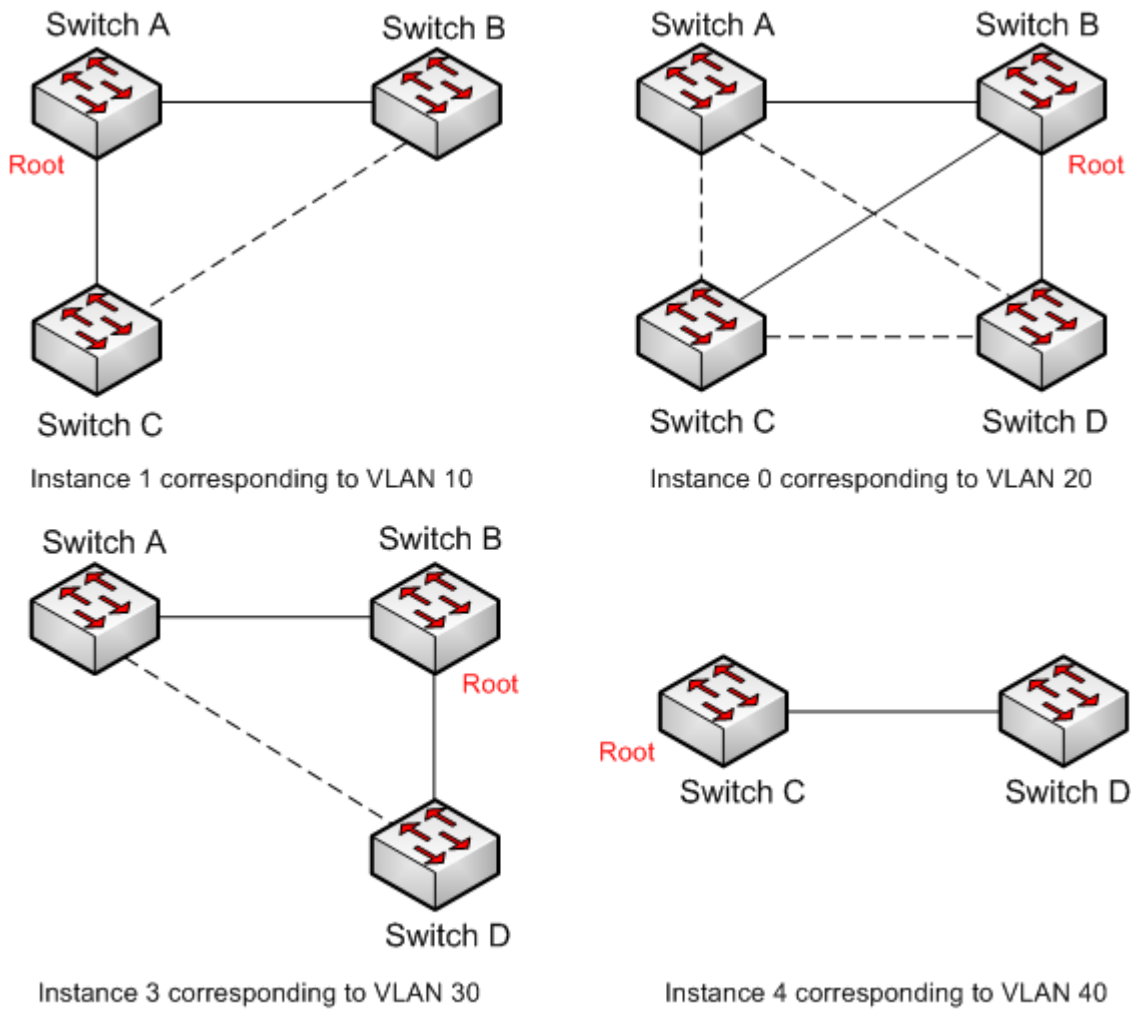
Figure 188 Spanning Tree Instance of each VLAN

6.10 Alarm

6.10.1 Introduction

This series switches support the following types of alarms:

➢ Port alarm: If this function is enabled, an alarm is triggered when the port is in link down state.

➢ Power alarm: It is applicable to dual power supply products. If this function is enabled, an alarm is triggered when the power is cut off or abnormal.

➢ Ring alarm: If this function is enabled, an alarm is triggered when the ring is open.

➢ High-temperature alarm: If this function is enabled, an alarm is triggered when the switch

temperature exceeds the high-temperature threshold.

The range of the general high-temperature threshold (T-high) is from 85℃ to 94℃ with the default setting of 85℃.

The range of the dangerous high-temperature threshold (T-Max) is from 95℃ to 100℃ with the default setting of 95℃.

General high-temperature alarm is triggered when the switch temperature (T-cur) is higher than the T-high threshold and lower than the T-Max threshold (T-high <T-cur<T-max).

Dangerous high-temperature alarm is triggered when the switch temperature is equal to or higher than the T-Max threshold (T-cur>=T-max).

➢ Low-temperature alarm: If this function is enabled, alarm is triggered when the switch temperature exceeds the low-temperature threshold.

The range of the low temperature threshold (T-low) is from -40℃ to 10℃ with the default setting of -40℃.

Low-temperature alarm is triggered when the switch temperature (T-cur) is lower than T-low threshold (T-cur<T-low).

When the alarm function is enabled, alarm modes include logging, front alarm LED blinking, alarm terminal block triggering, and SNMP trap packet sending.

Caution:

Only the master station of a DT ring and the root of a DRP support the ring alarm function.

6.10.2 Web Configuration

1. Configure and display port alarm.

➢ Click [Device Advanced Configuration] → [Alarm] → [Alarm Configuration] to enter port alarm configuration page, as shown in Figure 189.

Set Port Alarm

Port	1/1
Alarm Administrative State	Disable

Apply   Cancel

Port	Alarm Administrative State	Port	Alarm Administrative State
1/1	Enable	1/2	Disable
1/3	Disable	1/4	Disable
1/5	Disable	1/6	Disable
1/7	Disable	1/8	Enable
1/9	Disable	1/10	Disable
1/11	Disable	1/12	Disable

Figure 189 Port Alarm Configuration

Port

Options: all switch ports

Alarm Administrative State

Options: Disable/Enable

Default: Disable

Function: Enable/Disable port alarm.

➢ Click [Device Advanced Configuration] → [Alarm] → [Alarm Show] to display port alarm, as shown in Figure 190.

Port Alarm Status

Port	Alarm Administrative State	Port	Alarm Administrative State
1/1	LinkDown	1/8	LinkUp

Figure 190 Port Alarm

Alarm Administrative State

Options: LinkDown/LinkUp

Function: View the connection status of port on which port alarm function is enabled.

Description: LinkUp means the port is in connection state and supports normal communication. LinkDown means the port is disconnected or in abnormal connection (communication failure).

2. Configure and display DT-Ring alarm.

➢ Click [Device Advanced Configuration] → [Alarm] → [Alarm Configuration] to enter DT-Ring alarm configuration page, as shown in Figure 191.

Set Ring Alarm

Ring ID	Alarm Administrative State
1	Disable ▾
2	Disable ▾

Apply   Cancel

Ring ID	Alarm Administrative State
1	Enable
2	Enable
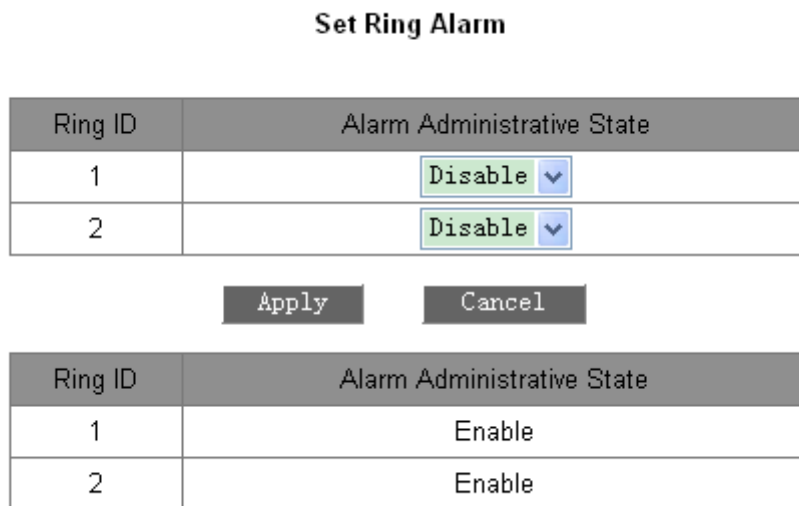
Figure 191 DT-Ring Alarm Configuration

Alarm Administrative State

Options: Disable/Enable

Default: Disable

Function: Enable/Disable DT-Ring alarm.

➢ Click [Device Advanced Configuration] → [Alarm] → [Alarm Show] to show DT-Ring alarm, as shown in Figure 192.

Ring Alarm Status

Ring ID	Alarm Administrative State
1	No Alarm
2	Alarm
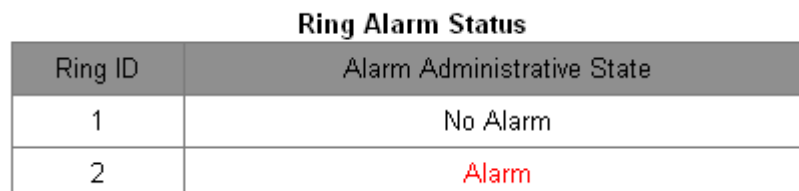
Figure 192 DT-Ring Alarm

Alarm Administrative State

Options: Alarm/No alarm

Function: View the status of rings on which the DT-Ring alarm function is enabled.

Description: No alarm means DT-Ring is closed. Alarm means DT-Ring is open or in abnormal state.

3. Configure and display DRP alarm.

➤ Click [Device Advanced Configuration] → [Alarm] → [Alarm about DRP] to enter DRP alarm configuration page, as shown in Figure 193.

Set DRP Alarm

Ring ID(1-32)	1
Admin State	Enable

Apply   Cancel

Figure 193 DRP Alarm Configuration

Ring ID

Options: All created DRP ring ID.

Admin State

Options: Disable/Enable

Default: Disable

Function: Enable/Disable DRP alarm.

➤ Show DRP alarm, as shown in Figure 194.

Ring ID	Admin State	Current State
1	Enable	Normal
2	Enable	Alarm

Figure 194 DRP Alarm

Current State

Options: Alarm/Normal

Function: View the status of rings on which the DRP alarm function is enabled.

Description: Normal means DRP is closed. Alarm means DRP is open or in abnormal state.

4. Configure and display power and temperature alarm.

➤ Click [Device Advanced Configuration] → [Alarm] → [Alarm Configuration] to enter power

and temperature alarm configuration page, as shown in Figure 195.

Set Other Alarm

AlarmType	Power Alarm
Alarm Administrative State	Disable

Apply   Cancel

Alarm Type	Alarm Administrative State
Power Alarm	Disable
High-Temperature Alarm	Enable
Low-Temperature Alarm	Enable

Figure 195 Power and Temperature Alarm Configuration

Alarm type

Options: Power Alarm/High-Temperature Alarm/Low-Temperature Alarm

Function: Select the alarm type.

Alarm administrative state

Options: Disable/Enable

Default: Disable power alarm and enable High-Temperature and Low-Temperature alarm.

Function: Enable/Disable this type of alarms.

➤ Click [Device Advanced Configuration] → [Alarm] → [Alarm Show] to view power and

temperature alarms, as shown in Figure 196.

Other Alarm Status

Alarm Type	Alarm Administrative State
Power Alarm	Abnormal
High-Temperature Alarm	No Alarm
Low-Temperature Alarm	No Alarm

Figure 196 Alarm Status

187

Power Alarm administrative state

Options: Normal/Abnormal

Function: View power alarm status.

Description:

Abnormal: For redundant power products, one of the power modules fails or works abnormally and an alarm is triggered.

Normal: For single power products, the power module supplies power normally; for redundant power product, two power modules both supply power normally.

High-Temperature alarm administrative state

Options: No Alarm/Alarm

Function: View the working temperature of the switch.

Description: Alarm means switch temperature exceeds the high-temperature threshold and triggers alarm. No Alarm means the working temperature of switch is normal.

Low-Temperature alarm administrative state

Options: No Alarm/Alarm

Function: View the working temperature of the switch.

Description: Alarm means the switch temperature exceeds the low-temperature threshold and triggers an alarm. No Alarm means the working temperature of switch is normal.

6.11 Port Traffic Alarming

6.11.1 Introduction

With the port traffic alarming function, the switch generates an alarm if the traffic rate of a port exceeds the specified threshold or a CRC error occurs. Alarm modes include logging, front alarm LED blinking, alarm terminal block triggering, and SNMP trap packet sending.

Caution:

➢ The traffic alarming function is based on a port. Such an alarm is generated only if the function is enabled on a port.

➢ The traffic alarming function is direction-specific. Incoming and outgoing traffic corresponds

to different alarms.

➢ If a CRC error occurs, an alarm is generated.

6.11.2 Web Configuration

1. Configure port traffic alarming.

Click [Device Advanced Configuration] → [Alarm] → [Alarm about PortRate/CRC] to enter

the port traffic alarming configuration page, as shown in Figure 197.

Set Port Alarm

Port	1/1	
Alarm Type	input rate alarm	
Admin State	Enable	
Threshold	1000	kbps

Apply   Cancel

Figure 197 Configuring Port Traffic Alarming

Alarm Type

Options: input rate alarm/output rate alarm/CRC

Function: Configure the alarm type for the port traffic alarming function.

Admin State

Options: Enable/Disable

Function: Configure the status of the alarm type.

Threshold

Range: 1 to 1000000000bps or 1 to 1000000kbps.

Function: Configure the threshold for the port traffic rate.

2. View port traffic alarm information, as shown in Figure 198.

Port	input rate alarm			output rate alarm			CRC	
	Admin State	Threshold	Current State	Admin State	Threshold	Current State	Admin State	Current State
1/1	Enable	1000kbps	Normal	Enable	100bps	Normal	Disable	Normal
1/2	Disable		Normal	Disable		Normal	Disable	Normal
1/3	Disable		Normal	Disable		Normal	Disable	Normal
1/4	Disable		Normal	Disable		Normal	Disable	Normal
1/5	Disable		Normal	Disable		Normal	Disable	Normal
1/6	Disable		Normal	Disable		Normal	Disable	Normal
1/7	Disable		Normal	Disable		Normal	Disable	Normal
1/8	Enable	10bps	Alarm	Enable	10kbps	Alarm	Disable	Normal
1/9	Disable		Normal	Disable		Normal	Disable	Normal
1/10	Disable		Normal	Disable		Normal	Disable	Normal
1/11	Disable		Normal	Disable		Normal	Disable	Normal
1/12	Disable		Normal	Disable		Normal	Disable	Normal

Figure 198 Port Traffic Alarm Information

6.12 Log Configuration

6.12.1 Introduction

The log function mainly records system status, fault, debugging, anomaly, and other information. With appropriate configuration, the switch can upload logs into a Syslog-supported server in real time.

Logs fall into 4 levels based on their importance and the importance from Critical, Warning, Information, to Debugging in descending order. The smaller the value, the more urgent the information is.

Table 11 Information Levels

Information Level	Value	Description
Critical	2	Serious system problem
Warning	4	Warning information
Information	6	Notification that needs to be recorded
Debugging	7	Information generated in the debugging process

6.12.2 Web Configuration

1. Configure the log function

Click [Device Advanced Configuration] → [Log Configuration] → [Log Configuration] to enter

the log configuration page, as shown in Figure 199.

Log Configuration

IP Address of remote logging server	192.168.0.23
Facility	Local0
Level	Warning

Reset   Apply

Figure 199 Log Configuration

IP Address of remote logging server

Configure the IP address of the server that log information is uploaded to.

Facility

Options: Local0-Local7

Default: Local0

Description: Facility is used to identify different log sources on the log server.

Level

Options: Critical/Warning/Information/Debugging

Default: Warning

Function: Select the level of the recorded log information.

Description: Log information can be filtered according to levels. The filtering rule is that the

output of the information whose value is bigger than that of the selected information level is

forbidden. For example, if the selected information level is Warning and its corresponding

value is 4, the system only output the Critical information with the value of 2 and the Warning

information with the value of 4.

You can install Syslog Server software, for example, Tftp32, on a PC to build a "Syslog

Server".

Log information can be displayed in real time on the Syslog Server, as shown in Figure 200.
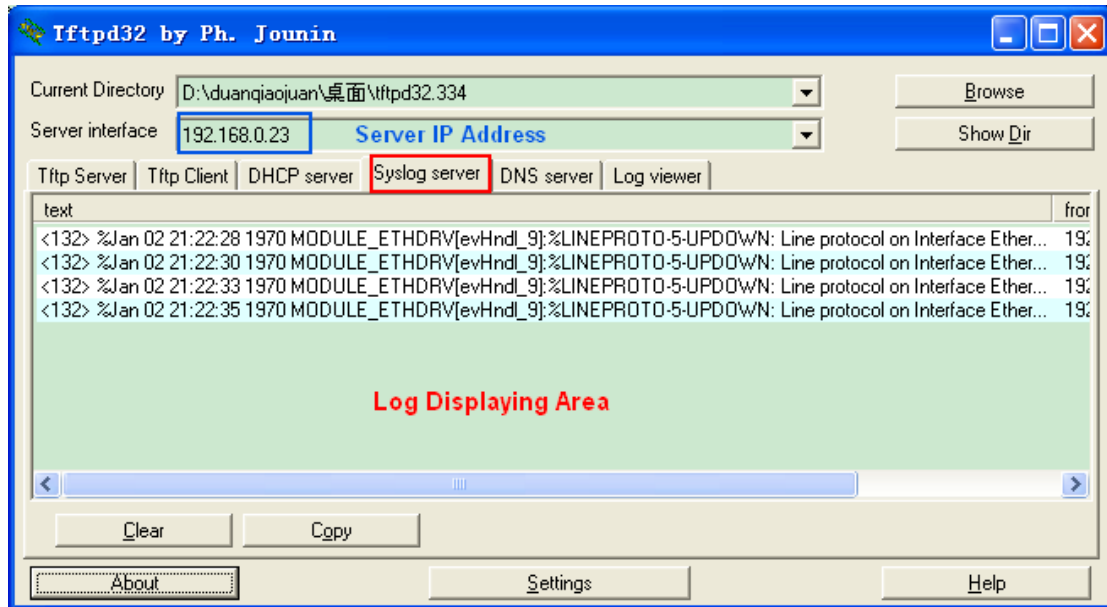
Figure 200 Uploading Log Information in Real Time

2. View log configuration

Click [Device Advanced Configuration] → [Log Configuration] → [Show Log] to view log, as shown in Figure 201.
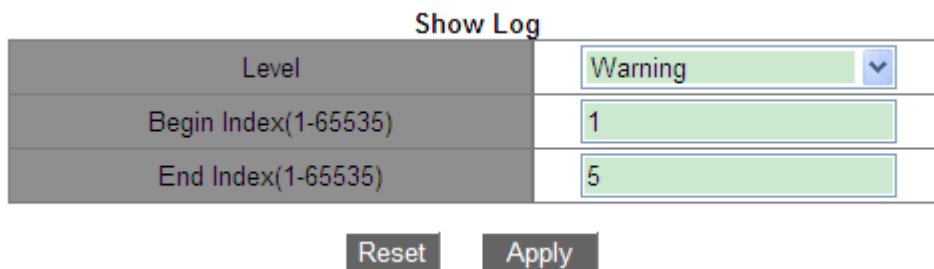
Figure 201 Log Settings

Level

Options: Warning/Critical

Default: Warning

Function: Select the lowest level of log information to be displayed.

Begin Index/End Index

Range: 1~65535

Function: View the specified log information in buffer and one line indicates one record.

Figure 202 shows the specified log information in buffer.

Figure 202 Log Information

Caution:

Only the Critical and Warning log information are saved in Buffer without Information and

Debugging log information.

3. Log uploading

Click [Device Advanced Configuration] → [Log Configuration] → [Log Transmit] to enter the

log uploading page, as shown in Figure 203.

Figure 203 Upload logs

FTP Server

Format: A.B.C.D

Function: Set the IP address of FTP server.

User Name

Function: Configure FTP user name.

Password

Function: Configure FTP user password.

File Name

Range: 1~32 characters

Function: set the file name saved in server.

> ⚠ **Caution:**
>
> CAUTION FTP server must remain in online state when logs are uploading.

4. Clear log information in Buffer

Click [Device Advanced Configuration] → [Log Configuration] → [Clear Log] to clear log, as shown in Figure 204.

Clear Log

`Clear`

Figure 204 Clearing Logs

6.13 Route configuration

To access a remote host on the Internet, a host must select an appropriate route by way of routers or Layer-3 switches. During the process of path selection, each Layer-3 switch selects the path to the next Layer-3 switch according to the destination address of the received packet, until the last Layer-3 switch sends the packet to the destination host. The path that each Layer-3 switch selects is called a route. Routes fall into the following types:

Direct route: indicates a route discovered by a link layer protocol.

Static route: indicates a route configured by the network administrator manually.

Dynamic route: indicates a route discovered by a routing protocol.

6.13.1 Static Route Configuration

6.13.1.1 Introduction

Static routes are manually configured. If a network's topology is simple, you only need to configure static routes for the network to work properly. Static routes are easy to configure and stable. They can be used to achieve load balancing and route backup, preventing illegitimate route changes. The disadvantage of using static routes is that they cannot adapt to network topology changes. If a fault or a topological change occurs in the network, the relevant routes will be unreachable and the network breaks. When this happens, the network administrator must modify the static routes manually.

6.13.1.2 Routing Table

Each Layer-3 switch maintains a routing table that records all the routes used by the switch. Each entry in the table specifies which VLAN interface a packet destined for a certain subnet or host should go out to reach the next router or the directly connected destination.

A route entry includes the following items:

Destination: indicates the destination IP address or network.

Network mask: specifies, in company with the destination address, the network where the destination host or Layer-3 switch resides. A logical AND operation between the destination address and the network mask yields the address of the destination network. For example, if the destination address is 129.102.8.10 and the mask 255.255.0.0, the address of the destination network is 129.102.0.0. A network mask is made up of a certain number of consecutive 1s. It can be expressed in dotted decimal format or by the number of the 1s.

Egress: specifies the interface through which a matching IP packet is to be forwarded.

IP address of the next Layer-3 switch (next hop): indicates the new Layer-3 switch that the IP packet will pass by.

Priority: Routes to the same destination but having different next hops may have different priorities and be found by various routing protocols or manually configured. The optimal route is the one with the highest priority.

6.13.1.3 Default Route

To prevent too many entries in a routing table, you can configure a default route. The default route is a static route. If a data packet fails to find a match in the routing table, it is forwarded according to the default route. In a routing table, the default route is the route with both the destination and mask being 0.0.0.0. If a packet does not match any entry in the routing table and no default route is configured, the switch discards the packet and returns an ICMP packet indicating that the destination address or network is unreachable.

6.13.1.4 Web Configuration

1. Configure a static route.

Click [Device Advanced Configuration] → [Route configuration] → [Static route configuration] → [Static route configuration] to enter the static route configuration page, as shown in Figure 205.

Static route configuration

Destination IP address	1.1.5.0
Destination network mask	255.255.255.0
Gateway	1.1.4.3
Priority(1-255,optional)	2

Add   Del

Figure 205 Static Routing Configuration

Destination IP address

Format: A.B.C.D

Function: Set the IP address of the destination host or network.

Destination network mask

Function: Set the subnet mask for the network where the destination host or Layer-3 switch resides.

Gateway

Format: A.B.C.D

Function: Set the next-hop IP address.

Priority

Range: 1~255

Default: 1

Function: Set the priority of the current route. The route with the smallest value for priority is selected as the best route for packet forwarding.

To delete a route entry, you need to set all the parameters to be consistent with those of the route; otherwise, the route cannot be deleted due to match failure.

After a route is configured, it is displayed in the list of static routes, as shown in Figure 206.

Static ip route list

Destination IP address	Destination network mask	Gateway	Priority
1.1.1.0	255.255.255.0	1.1.2.3	1
1.1.5.0	255.255.255.0	1.1.4.3	2

Figure 206 List of Static Routes

6.13.1.5 Typical Configuration Example

As shown in Figure 207, the network masks of all Layer-3 switches and PCs on the network are 255.255.255.0. It is required to configure static routes to enable any of the hosts to communicate with each other.
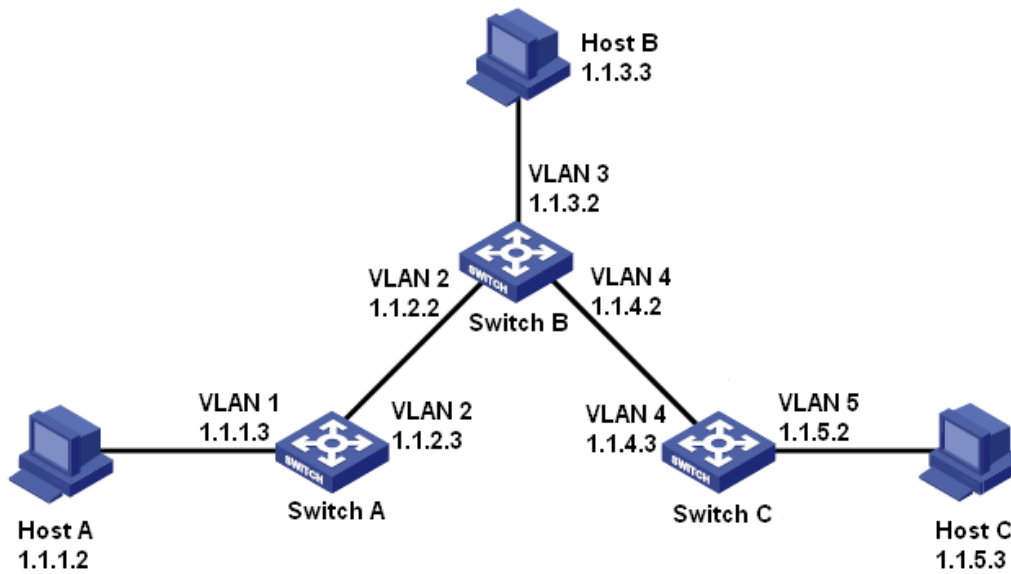
Figure 207 Example for Configuring Static Routes

Configuration on Switch A:

1. Set IP addresses for VLAN interfaces.

2. Configure a static route with the following parameters:

Destination IP address: 1.1.3.0; destination network mask: 255.255.255.0; default gateway:

1.1.2.2; priority: 1, as shown in Figure 205.

Destination IP address: 1.1.5.0; destination network mask: 255.255.255.0; default gateway:

1.1.2.2; priority: 1, as shown in Figure 205.

Configuration on Switch B:

3. Set IP addresses for VLAN interfaces.

4. Configure a static route with the following parameters:

Destination IP address: 1.1.1.0; destination network mask: 255.255.255.0; default gateway:

1.1.2.3; priority: 1, as shown in Figure 205.

Destination IP address: 1.1.5.0; destination network mask: 255.255.255.0; default gateway:

1.1.4.3; priority: 1, as shown in Figure 205.

Configuration on Switch C:

5. Set IP addresses for VLAN interfaces.

6. Configure a static route with the following parameters:

Destination IP address: 0.0.0.0; destination network mask: 0.0.0.0; default gateway: 1.1.4.2; priority: 1, as shown in Figure 205.

7. Configure the default gateways for host A, host B, and host C as 1.1.1.3, 1.1.3.2, and 1.1.5.2 respectively.

6.13.2 RIP Configuration

6.13.2.1 Introduction

> **Note:**
>
> Routers in this chapter refer to Layer-3 switches.

Routing Information Protocol (RIP) is a distance vector interior gateway protocol, using UDP packets for exchanging information through port 520. Each L3 switch that runs RIP has a routing database. The routing database contains routing entries to all reachable destinations of this L3 switch based on which a routing table is established. When a L3 switch running RIP sends route update packets to its neighboring devices, this packet carries the entire routing table established by this L3 switch based on routing database. Therefore, on a large-scale network, each L3 switch needs to transmit and handle a large amount of routing data, which thereby compromises the network performance. RIP allows the routing information discovered by other routing protocols to be introduced to the routing table.

RIP has two versions, RIP-1 and RIP-2. RIP-1 supports message advertisement via broadcast only, does not support subnet mask and authentication. Some fields in the RIP-1 message must be zero. These fields are called zero fields which should be check when receiving RIP-1 message. If such a field contains a non-zero value, the RIP-1 message will not be processed. RIP-2 is improved based on RIP-1. In RIP-2, protocol packets are sent in multicast mode and the destination address is 224.0.0.9. In addition, RIP-2 has a subnet mask domain and an RIP verification domain (simple plaintext password and MD5 password verification supported) added, and supports variable length subnet masks (VLSMs). RIP-2 retains part of the all-zero domains in RIP-1 and therefore it is unnecessary to check all-zero

domains. By default, layer-3 switch transmits RIP-2 message in multicast mode, receives RIP-1 and RIP-2 message.

RIP uses a hop count to measure the distance to a destination. The hop count from a router to a directly connected network is 0. The hop count from a router to a directly connected router is 1. To limit convergence time, the range of RIP metric value is from 0 to 15. A metric value of 16 (or greater) is considered infinite, which means the destination network is unreachable. That is why RIP is suitable for small-sized networks.

6.13.2.2 Routing loops prevention

On a network running RIP, when an RIP route becomes unreachable, the RIP L3 switch will not send a route update packet immediately until the route update interval (30s) elapses. If a neighboring L3 switch sends a packet carrying its own routing table information to the L3 switch before a route update packet is received, infinite counting will occur. That is, the metric for selecting a route to the unreachable L3 switch increases incrementally. This affects the routing time and route aggregation time remarkably.

To avoid infinite counting, RIP provides the split horizon and triggered update mechanisms to solve the problem of routing loop. Split horizon aims to avoid sending routes to a gateway from which the routes are learned. It contains simple split horizon and split horizon with poisoned reverse. Simple split horizon involves deleting routes that are to be sent to a neighboring gateway from which these routes are learned. Split horizon with poisoned reverse involves deleting the preceding routes from the route update packet and setting the metric of these routes to 16. In the triggered update mechanism, whenever a gateway changes the metric of a route, a route update packet will be broadcast immediately without considering the status of the 30-second update timer.

6.13.2.3 Operation

1. After RIP is enabled, the router sends request messages to neighboring routers. Neighboring routers return response messages including information about their routing tables.

2. After receiving such information, the router updates its local routing table, and sends triggered update messages to its neighbors. All routers on the network do the same to keep the lastest routing information.

3. By default, the local routing table will be sent to neighboring routers at 30-second intervals. After receiving the packet carrying this routing table, the neighboring routers running RIP will maintain their own local routes, select an optimal route, and send an update message to their respective neighbors so that the updated route will be globally effective. Moreover, RIP employs the expiration mechanism for handling expired routes. Specifically, if an L3 switch does not receive route update information from a neighbor within the specified time interval (invalid timer value), all routes from this neighbor will be considered an invalid route and the route enters the suppression state. This route has a validity period (holddown timer value) in the routing table. If no update information is received from this neighbor within this period, these routes will be deleted from the routing table.

6.13.2.4 Web Configuration

The basic configuration of operating RIP in layer-3 switch is simple. Generally, you need to enable RIP, and enable port to transmit and receive RIP packet, that means transmitting and receiving RIP packet according to RIP default configuration(By default, layer-3 switch transmits RIP-2, receives RIP-1 and RIP-2).

1. Enable RIP

Click [Device Advanced Configuration] → [Route configuration]→[RIP configuration]→[Enable RIP]→[Enable RIP] to enable RIP, as shown in Figure 208.
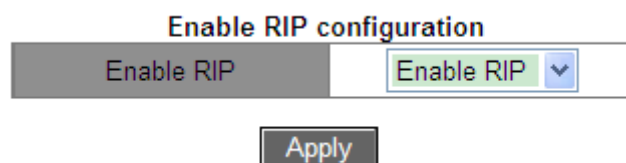
Figure 208 Enable RIP

Enable RIP

Option: Enable RIP/Disable RIP

Default: Disable RIP

Function: Enable/Disable RIP.

2. Enable RIP on interface

Click [Device Advanced Configuration] → [Route configuration]→[RIP configuration]→[Enable RIP]→[Enable port to receive/transmit RIP packet] to enable RIP on interface, as shown in Figure 209.
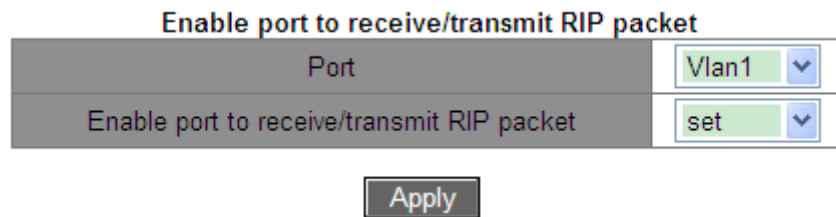
Figure 209 Enable RIP on Interface

Enable port to receive/transmit RIP packet

Options: set/cancel

Default: set

Function: Enable/Disable RIP on interface.

3. Configure imported route

Click [Device Advanced Configuration] →[Route configuration]→[RIP configuration]→[RIP parameter configuration]→[Enable imported route] to enter imported route configuration page, as shown in Figure 210.
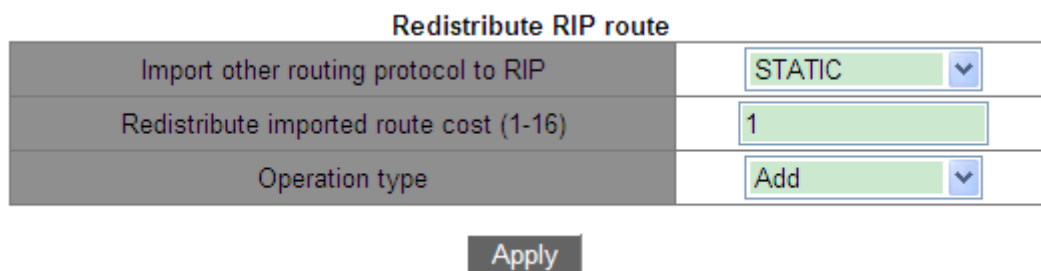
Figure 210 Imported Route Configuration

Import other routing protocol to RIP

Options: STATIC/OSPF

Function: Import other routing protocol to RIP. Only active routes can be imported.

Redistribute imported route cost

Range: 1~16

Function: Redistribute the metric value of the imported route. This parameter is optional. If the parameter is not configured, it will be redistributed according to default metric value.

Operation type

Options: Add/Del

Function: Add/Cancel importing other routing protocol to RIP. By default, no other routing protocol is imported to RIP.

4. Configure the additional routing metric

Click [Device Advanced Configuration] →[Route configuration]→[RIP configuration]→[RIP parameter configuration]→[Metricin/out configuration] to enter the additional routing metric configuration page, as shown in Figure 211.

Metricin/out configuration

Port	Vlan1
In(1-15)	1
Out(0-15)	0

Apply   Default

Figure 211 Additional Routing Metric Configuration

In

Range: 1~15

Default: 1

Function: Configure the inbound additional routing metric. The inbound additional metric is added to the metric of a received route before the route is added into the routing table, and the route's metric is changed. If the sum of the additional metric and the original metric is greater than 16, the metric of the route will be 16.

Out

Range: 0~15

Default: 0

Function: Configure the outbound additional routing metric. The outbound additional metric is added to the metric of a sent route, and the route's metric in the routing table is not

changed.

5. Configure RIP port

Click [Device Advanced Configuration] →[Route configuration]→[RIP configuration]→[RIP parameter configuration]→[RIP port configuration] to enter RIP port configuration page, as shown in Figure 212.

Figure 212 RIP Port Configuration

Receiving RIP version

Options: version 1/version 2/version 1 and 2

Default: version 1 and 2

Function: Set the version of RIP message received by interface. Version 1 means RIP-1 message received by interface, version 2 means RIP-2, and version 1 and 2 means RIP-1 and RIP-2.

Sending RIP version

Options: version 1/version 2 (BC)/version 2 (MC)

Default: version 2 (MC)

Function: Set the version of RIP message transmitted by interface. Version 1 means RIP-1 message transmitted by interface, version 2 (BC) means RIP-2 message transmitted by interface in broadcast mode, version 2 (MC) means RIP-2 message transmitted by interface in multicast mode.

Receive packet

Options: Yes/No

Default: Yes

Function: Allow interface to receive RIP message or not.

Send packet

Options: Yes/No

Default: Yes

Function: Allow interface to transmit RIP message or not.

Split-horizon status

Options: permit/forbid

Default: permit

Function: Permit/Forbid horizontal split. Horizontal split is to avoid routing loops, means avoid routes learned from an interface are transmitted from this interface again.

RIP authentication key

Range: 1~16 characters

Function: Set the key of RIP authentication.

RIP authentication type

Options: text /Cisco MD5/MD5/cancel

Default: text

Function: Set the type of RIP authentication. text means text authentication; MD5 means general MD5 authentication; Cisco MD5 means Cisco MD5 authentication; cancel means restoring the default authentication: text authentication. RIP-1 does not support authentication.

6. Configure RIP mode

Click [Device Advanced Configuration] →[Route configuration]→[RIP configuration]→[RIP parameter configuration]→[RIP mode configuration] to enter RIP mode configuration page, as shown in Figure 213.

Route mode configuration

Set receiving/sending RIP version for all ports	version 1
Auto-summary	cancel
Rip priority	120
Set default route cost for imported route(1-16)	1
Rip checkzero	set checkzero
Rip broadcast	set

Apply

Figure 213 RIP Mode Configuration

Set receiving/sending RIP version for all ports

Options: version 1/version 2/cancel

Default: Transmitting RIP-2 message, receiving RIP 1 and RIP 2 message.

Function: Configure the version of RIP message transmitted and received by all routing

interfaces. version 1 means RIP-1 message transmitted and received by all routing

interfaces, version 2 means RIP-2, cancel means restoring the default configuration.

Auto-summary

Options: cancel/set

Default: cancel

Function: Set/Cancel route aggregation. Route aggregation means that subnets in a natural

network are summarized into a natural network that is sent to other networks. This feature

can reduce the amount of routing information in routing table and the amount of switching

information. RIP-1 does not support subnet mask, if forwarding subnet route might cause

ambiguity, so RIP-1 always enable routing aggregation function. For RIP-2, when you want

to broadcast subnet routes, disable routing aggregation function.

Rip priority

Range: 0~255

Default: 120

Function: Specify the priority of RIP. The smaller the value, the higher the priority. The priority

will decide routes in core routing table will adopt which kind of routing algorithm to obtain the

best routing.

Set default route cost for imported route

Range: 1~16

Default: 1

Function: Configure default metric value of the imported route.

Rip checkzero

Options: set checkzero/cancel checkzero

Default: set checkzero

Function: Check RIP-1 message zero field or not. Some fields in the RIP-1 message must be zero. These fields are called zero fields. You can enable zero field check on received RIP-1 message. If such a field contains a non-zero value, the RIP-1 message will not be processed. Because there is not zero field in RIP-2 message, this function doesn't work to RIP-2.

Rip broadcast

Options: set/cancel

Default: set

Function: set is to permit all interfaces in layer-3 switch to transmit RIP broadcast packets or multicast packets; cancel is to forbid all interfaces in layer-3 switch transmitting RIP broadcast packets or multicast packets, only transmitting RIP data packets between neighbor layer-3 switches.

7. Configure RIP timers

Click [Device Advanced Configuration] →[Route configuration]→[RIP configuration]→[RIP parameter configuration]→[RIP timer configuration] to enter RIP timers configuration page, as shown in Figure 214.

Figure 214 RIP Timers Configuration

Update timer

Range: 1～2147483647

Default: 30

Function: Configure the interval between routing updates.

Invalid timer

Range: 1～2147483647

Default: 180

Function: Configure the time range of declaring RIP routing invalid. If an L3 switch does not receive route update information from a neighbor within the specified time interval (invalid timer value), all routes from this neighbor will be considered an invalid route and the route enters the suppression state. Invalid timer >Update timer.

Holddown timer

Range: 1～2147483647

Default: 120

Function: Configure how long a RIP route stays in the suppressed state. If no update information is received from this neighbor within this period (holddown timer value), these routes will be deleted from the routing table. Holddown timer >Update timer.

6.13.2.5 Typical Configuration Example

As shown in Figure 215, Switch B is connected to Switch A through interface VLAN 2 and to Switch C through interface VLAN 4, three switches all operate RIP routing protocol. The network masks of all switches on the network are 255.255.255.0.
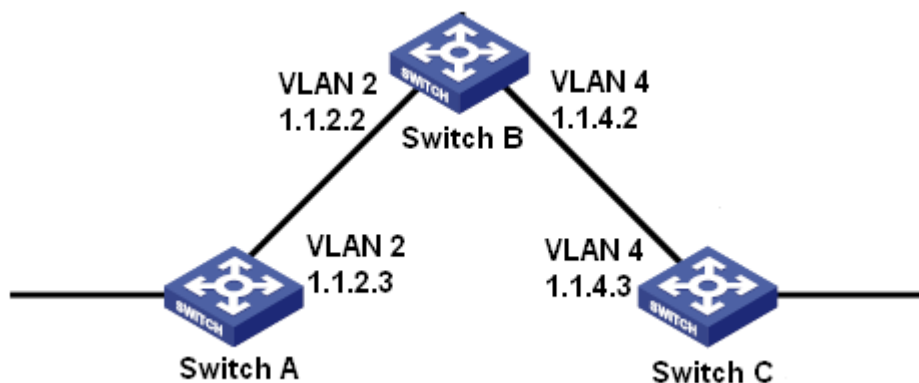
Figure 215 RIP Configuration Example

Configuration on Switch A:

1. Set IP address for VLAN 2 interface.

2. Enable RIP protocol, as shown in Figure 208.

3. Enable VLAN 2 interface to transmit/ receive RIP message, as shown in Figure 209.

Configuration on Switch B:

1. Set IP addresses for VLAN 2 and VLAN 4 interfaces.

2. Enable RIP protocol, as shown in Figure 208.

3. Enable VLAN 2 and VLAN 4 interfaces to transmit/ receive RIP message, as shown in

Figure 209.

Configuration on Switch C:

1. Set IP address for VLAN 4 interface.

2. Enable RIP protocol, as shown in Figure 208.

3. Enable VLAN 4 interface to transmit/ receive RIP message, as shown in Figure 209.

6.13.3 OSPF Configuration

6.13.3.1 Introduction

Open Shortest Path First (OSPF) is a link state interior gateway protocol. Layer-3 switches

exchange link state information to compose a link state database (LSDB). Then each switch

uses the shortest path first (SPF) algorithm based on the LSDB to generate a routing table.

This series switches support OSPF version 2.

> **Note:**
>
> Routers in this chapter refer to Layer-3 switches.

6.13.3.2 Basic Concepts

1. AS

An Autonomous System (AS) comprises a group of routers that run the same routing protocol.

2. Router ID

Router ID (RID): An OSPF-enabled router must have its own router ID, which is the unique identifier of the router in the AS. RID can be either configured manually or generated automatically. The automatically generated RID is the primary IP address of the VLAN interface with the smallest ID on the switch.

3. OSPF packets

Hello: Periodically sent to find and maintain neighbors, containing the values of some timers, information about the DR, BDR, and known neighbors.

Database description (DD): Describes the digest of each Link State Advertisement (LSA) in the LSDB, exchanged between two routers for data synchronization.

Link state request (LSR): After exchanging the DD packets, the two routers know which LSAs of the neighbor are missing from their LSDBs. They then send an LSR packet to each other, requesting the missing LSAs. The LSA packet contains the digest of the missing LSAs.

Link state update (LSU): Transmits the LSAs to be updated to the neighbor. Each LSU packet may contain multiple LSAs.

Link state acknowledgment (LSAck): Acknowledges received LSU packets. It contains the headers of received LSAs (an LSAck packet can acknowledge multiple LSAs).

4. Neighbor and adjacency

Neighbor: When an OSPF router starts, it sends a hello packet via the OSPF interface, and the router that receives the hello packet checks parameters carried in the packet. If

parameters of the two routers match, they become neighbors.

Adjacency: Two OSPF neighbors establish an adjacency relationship to synchronize their LSDBs. Therefore, any two neighbors without exchanging route information do not establish an adjacency.

5. LSA types

LSAs can be exchanged only between adjacent routers. Various types of LSAs describe the OSPF network topology. All LSAs are saved in the LSDB. The information in the LSDB is used to compute the best route by the SPF algorithm.

Router LSA (Type 1): originated by each router in the OSPF network and flooded throughout the generated area. The LSA describes the link state and cost of the router.

Network LSA (Type 2): originated by the designated router (DR) and flooded throughout the generated area. This LSA contains the link state of all routers on the network segment.

Network Summary LSA (Type 3): originated by Area Border Routers (ABRs) and advertised to the other areas. The LSA describes the routing information in the area.

ASBR Summary LSA (Type 4): originated by ABRs and advertised to related areas. Type 4 LSAs describe routes to Autonomous System Boundary Router (ASBR).

AS External LSA (Type5): originated by ASBRs, and flooded throughout the AS (except stub areas). Each type 5 LSA describes a route to another AS.

6.13.3.3 Area and Router

1. Area partition

OSPF splits an AS into multiple areas, which are identified by area IDs. Areas classify routers on the network into different logical groups, as shown in Figure 216. Routing information summary is exchanged among areas.

Area 0, the backbone area, is the core area of the entire OSPF network. All non-backbone areas must be directly connected to the backbone area. The routing information of non-backbone areas must be forwarded by the backbone area.

To reduce the size of the topology database, OSPF can divide certain areas into stub areas.

Type 4 and Type 5 LSAs are not allowed to enter stub areas. To ensure that the routes to the other areas in the AS or to other ASs are still reachable, the ABR generates a default route and advertises it to other routers in the area.
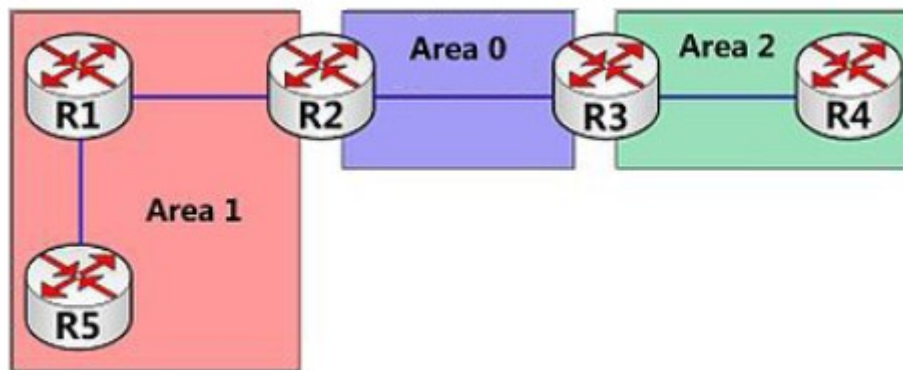
Figure 216 Area Partition

Area partition is based on interfaces. Therefore, a router with multiple interfaces may belong to multiple areas, but each interface belongs to only one area. All routers in the same area maintain the same LSDB. If a router belongs to multiple areas, it maintains an LSDB for each area. Network partition has the following advantages:

➢ The routers in each area maintain only the LSDB of the area, but not the entire OSPF network.

➢ If network topology is confined to an area, it does not affect the entire OSPF network, lowering the frequency of SPF computing.

➢ Confining the transmission of LSAs to one area can reduce OSPF data.

2. Router types

Based on the position of a Layer-3 switch in the AS, the role of the switch can be internal router, ABR, backbone router, or ASBR, as shown in Figure 217.
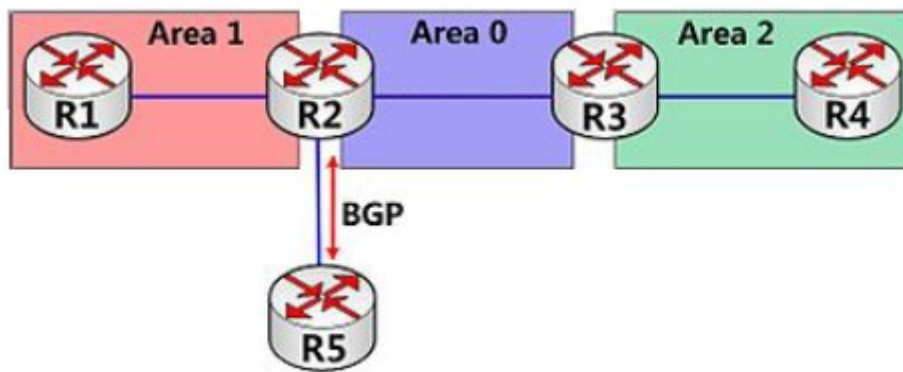
Figure 217 OSPF Router Types

Internal router: All interfaces on an internal router belong to one OSPF area. For example, R1 and R4 in Figure 217.

ABR: An ABR connects one or multiple areas to the backbone area. On an ABR, at least one interface must belong to the backbone area. For example, R2 and R3 in Figure 217.

Backbone router: At least one interface of a backbone router must reside in the backbone area. All ABRs and internal routers in area 0 are backbone routers. For example, R2 and R3 in Figure 217.

ASBR: A router exchanging routing information with another AS is an ASBR. For example, R2 in Figure 217.

One router can be of multiple types. For example, R2 in Figure 217 is a backbone router, ABR, and ASBR.

3. Virtual link

If non-backbone areas cannot communicate with the backbone area due to certain limitations, OSPF virtual links can be configured to build logical connections among them.
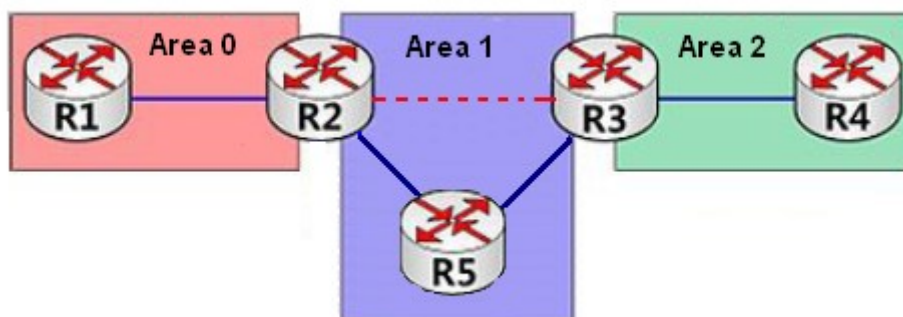
Figure 218 Virtual Link

A virtual link is a logical connection established between two ABRs through a non-backbone area and is configured on both ABRs to take effect. The non-backbone area is called a transit area. For example, the red dotted line in Figure 218 is a virtual link and Area 1 is the transit area for the virtual link.

4. Route types

OSPF prioritize routes into four levels: intra-area routes, inter-area routes, Type 1 external routes, and Type 2 external routes, in descending order. The intra-area and inter-area routes describe the network topology of the AS. The external routes describe routes to external ASs.

6.13.3.4 DR and BDR

On NBMA networks, any two routers exchange routing information with each other. As a result, many unnecessary LSAs are generated. The Designated Router (DR) was introduced to solve this problem. All the other routers establish an adjacent relationship and exchange routing information with the DR. The DR advertises network link state to other routers. To prevent single-point failures caused by a failed DR, OSPF defines the Backup Designated Router (BDR). BDRs also establish the adjacent relationship with other routers. BDR is the backup of DR. When the DR fails, the BRD becomes DR. Since the adjacent relationships with other routers have been established, the DR failure imposes tiny impact on the network.
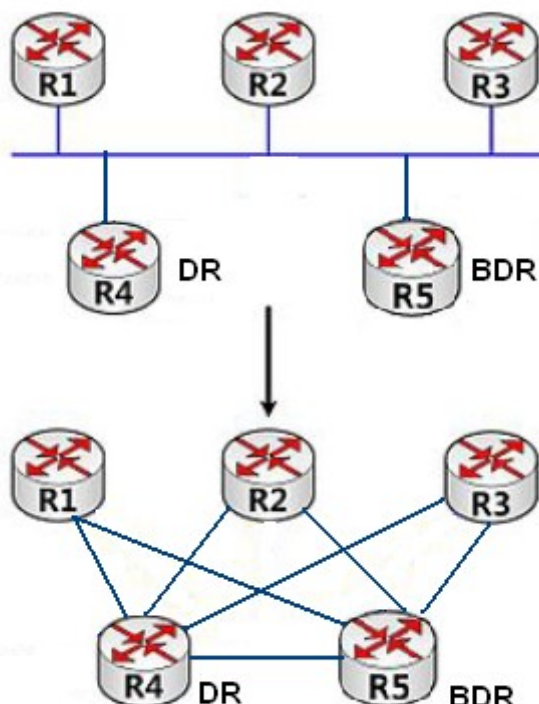
Figure 219 DR and DBR

As shown in Figure 219, the first figure shows Ethernet physical connections, and the second figure show the established adjacent relationship. After DR/BDR is adopted, five routers require only seven adjacent relationships.

The rules for DR/BDR election are as follows:

➢ A router with router priority 0 cannot become the DR or BDR.

➢ A router with the highest priority on a network segment is elected as the DR, and the one with the second highest priority is the BDR.

➢ If multiple routers have the same priority, the router with the larger RID is selected as the DR.

➢ When the DR fails, the BDR becomes DR and another route is elected as a BDR.

➢ The DR concept is based on interface. A router may be a DR in terms of one interface and a BDR or common router in terms of another interface.

➢ If a router with the highest priority is added to the network after DR/BDR election, the router will not replace the existing DR or BDR to become the new DR or BDR.

6.13.3.5 Web Configuration

1. Enable OSPF.

Click [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF process configuration] → [OSPF Enable/Disable] to enter the OSPF enable page, as shown in Figure 220.
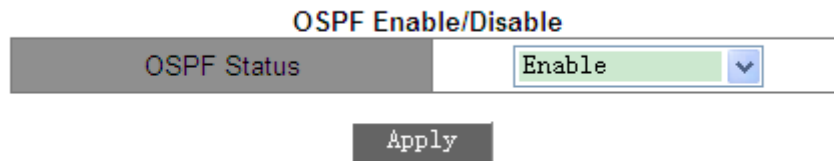
Figure 220 Enabling OSPF

OSPF Status

Options: Enable/Disable

Default: Disable

Function: Enable or disable OSPF.

2. Set an RID.

Click [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF process configuration] → [Router-ID configuration] to enter the RID configuration page, as shown in Figure 221.
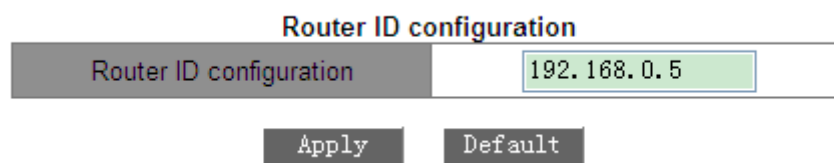
Figure 221 Setting the RID

Router ID configuration (IP address)

Format: A.B.C.D

Default: primary IP address of the VLAN interface with the smallest VLAN ID on the switch.

Function: Set the RIDs of OSPF-enabled switches. Each OSPF-enabled switch has a unique RID in the AS.

⚠ CAUTION	**Caution:** The change of an RID takes effect only after OSPF is re-enabled.

3. Set an OSPF network range.

Click [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] →
[OSPF process configuration] → [OSPF network range configuration] to enter the OSPF
network range configuration page, as shown in Figure 222.

OSPF network range configuration

Network	192.168.0.0
Network mask	255.255.255.0
Area ID (0-4294967295)	0
Advertise	Yes

Add   Remove

Figure 222 Setting OSPF Network Range

Network

Format: A.B.C.D

Function: Set the network IP address.

Network mask

Function: Set the subnet mask of the network.

Description: The network mask and IP address determine a network range.

Area ID

Range: 0~4294967295

Function: Configure the area for the network range.

Description: If a network range is added to an area, all the internal routes of the network
range are not advertised to other areas.

Advertise

Options: Yes/No

Default: Yes

Function: Configure whether to advertise the digest information of the routes in the network range.

4. Set the area for the VLAN interface.

Click [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF process configuration] → [OSPF area configuration for port (must)] to enter the VLAN interface area configuration page, as shown in Figure 223.

Figure 223 Setting the Area for the VLAN Interface

Area ID

Range: 0~4294967295

Function: Set the area for the VLAN interface.

Description: If a VLAN interface is added to an OSPF area, OSPF is enabled on the VLAN interface.

5. Set OSPF authentication parameters

Click [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF TX-parameter configuration] → [OSPF authentication parameter configuration] to enter the OSPF authentication configuration page, as shown in Figure 224.

Figure 224 Setting OSPF Authentication Parameters

Authentication mode

Options: SIMPLE/MD5

Function: Configure the authentication mode for OSPF packet receiving on a specified interface.

Description: SIMPLE indicates plain-text authentication. MD5 indicates encrypted authentication.

SIMPLE Authentication key

Range: 1~8 characters

Function: Set the key for SIMPLE authentication.

Description: The setting of this parameter takes effect only if SIMPLE is selected as the authentication mode.

MD5 Authentication key

Range: 1~16 characters

Function: Set the key for MD5 authentication.

Description: The setting of this parameter takes effect only if MD5 is selected as the authentication mode.

MD5 Key ID

Range: 1~255

Function: Set the MD5 authentication key ID.

⚠ **Caution:**
To send and receive OSPF properly, identical authentication parameters must be configured on both ends.

6. Configure the OSPF Rx/Tx mode for the VLAN interface.

Click [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF TX-parameter configuration] → [Passive interface configuration] to enter the OSPF Rx/Tx mode configuration page, as shown in Figure 225.
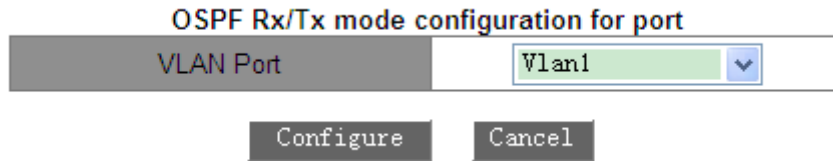
Figure 225 Configuring the OSPF Rx/Tx Mode for the VLAN Interface

VLAN Port

Options: VLAN interfaces on which OSPF is to be enabled.

Function: Configure the specified VLAN interface to only receive (but not send) OSPF packets.

Description: By default, all OSPF-enabled interfaces can send and receive OSPF packets.

7. Set OSPF packet sending timer parameters.

Click [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF TX-parameter configuration] → [OSPF packet sending timer configuration] to enter the packet sending timer configuration page, as shown in Figure 226.
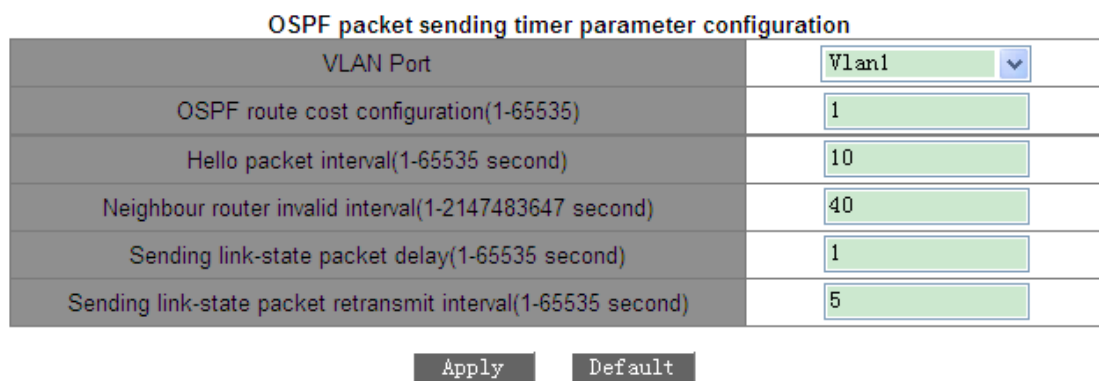
Figure 226 Setting Parameters for the OSPF Packet Sending Timer

OSPF route cost configuration

Range: 1~65535s

Default: 1s

Function: Configure the OSPF route cost for the specified interface.

Hello packet interval

Range: 1~65535s

Default: 10s

Function: Configure the interval for sending hello packets on the specified interface.

Description: The switch periodically sends hello packets to adjacent devices to discover and maintain adjacent relationships and elect the DR and BDR.

Neighbour router invalid interval

Range: 1~2147483647 s

Default: 40s

Function: Configure the interval for the expiration of routes to adjacent switches. The value must be larger than or equal to four times the hello packet interval.

Description: If the switch does not receive hello packets from an adjacent device within the interval, the adjacent device is considered as unreachable and invalid.

Sending link-state packet delay

Range: 1~65535s

Default: 1s

Function: Configure LSA sending delay on the specified interface.

Sending link-state packet retransmit interval

Range: 1~65535s

Default: 5s

Function: Set the interval for retransmitting LSAs to adjacent switches on a specified interface.

Description: After sending an LSA to an adjacent device, the switch keeps the LSA until it receives the confirmation from the adjacent device. If the switch does not receive the confirmation within the interval, it retransmits the LSA.

> **Caution:**
>
> To ensure the normal running of OSPF, the timer parameters must be identical between OSPF neighbors.

8. Set parameters for OSPF routes importing.

Click [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] →

[Imported route parameter configuration] → [Imported route parameter configuration] to enter the OSPF routes importing configuration page, as shown in Figure 227.

Imported route parameter configuration	
Imported route parameter configuration	2
Default imported route tag(0-4294967295)	2147483648
Default imported route metric (1-16777214)	1
Imported route interval(1-65535)	1
Maximum imported route(1-65535)	100

Apply   Default

Figure 227 Setting Parameters for Router Importing

Imported route parameter configuration

Options: 1/2

Default: 2

Function: Set the default type of imported routes.

Description: 1 indicates Type 1 external routes, and 2 indicates Type 2 external routes. The cost from a router to the destination of the Type 1 external route is the cost from the router to the corresponding ASBR plus the cost from the ASBR to the destination of the external route. The cost from the internal router to the destination of the Type 2 external route is the cost from the ASBR to the destination of the Type 2 external route.

Default imported route tag

Range: 0~4294967295

Default: 2147483648

Function: Set the default tag of imported routes.

Default imported route cost

Range: 1~16777214

Default: 1

Function: Set the default cost of imported routes.

Imported route interval

Range: 1~65535s

Default: 1s

Function: Set the interval for importing external routes. OSPF periodically imports external route information and flood the information in the entire AS.

Maximum imported route

Range: 1~65535

Default: 100

Function: Set the maximum number of routes that can be imported by OSPF at one time.

9. Configure other protocol routes importing.

Click [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [Imported route parameter configuration] → [Import external routing information] to enter the external routes importing configuration page, as shown in Figure 228.

Import external routing information

Imported type	Static
Type	2
Tag(0-4294967295)	3
Metric Value(1-16777214)	20

Add   Remove

Figure 228 Configuring Other Protocol Routes Importing

Imported type

Options: Static/RIP/Connected/BGP

Function: Configure the routing protocol.

Description: Static indicates importing static routes; RIP indicates importing RIP routes; connected indicates importing directly connected routes; BGP indicates importing BGP routes.

Type

Options: 1/2

Function: Configure the type of imported routes.

Description: 1 indicates Type 1 external routes, and 2 indicates Type 2 external routes.

Tag

Range: 0~4294967295

Function: Configure the tag of imported routes.

Metric Value

Range: 1~16777214

Function: Configure the metric value of imported routes.

10. Setting Priorities for Routing Protocols

Click [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [Other parameter configuration] → [OSPF priority configuration] to enter the routing protocol priority configuration page, as shown in Figure 229.
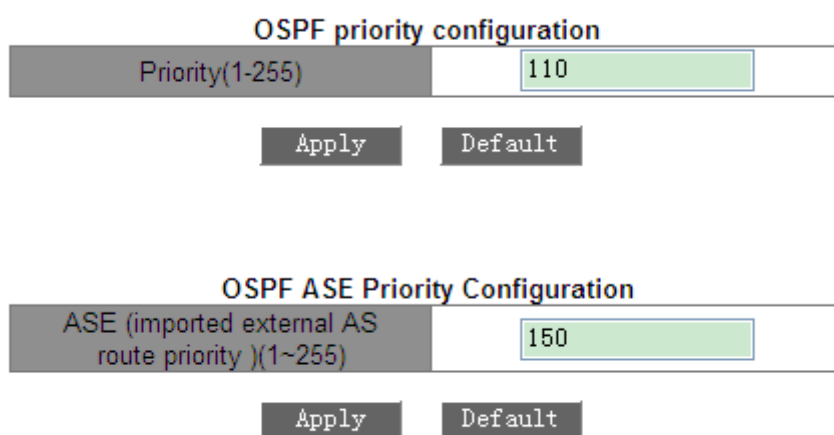
Figure 229 Setting Priorities for Routing Protocol

Priority

Range: 1~255

Default: 110

Function: Set the priority of OSPF.

ASE (imported external AS route priority)

Range: 1~255

Default: 150

Function: Set the priority of imported routes.

Description: Since multiple routing protocols may be enabled on Layer-3 switches, route sharing and selection become important. Therefore, a priority is set for each routing protocol.

If the same route is discovered by multiple routing protocols, the protocol with the highest priority (smallest number) is valid.

11. Configuring a stub area.

Click [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [Other parameter configuration] → [OSPF STUB area and default route cost] to enter the stub area configuration page, as shown in Figure 230.

OSPF STUB area and default route cost

Default Route Cost(1-65535)	60
Area ID(1-4294967295)	1

Add   Remove
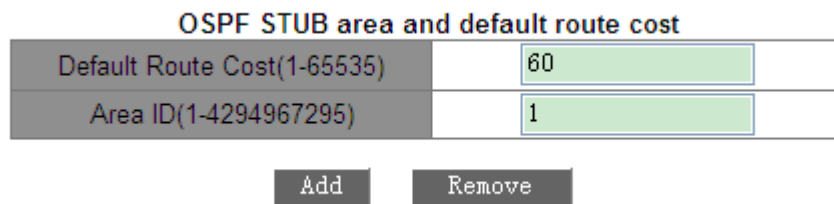
Figure 230 Configuring Stub Areas

Default Route Cost

Range: 1~65535

Function: Set the default route cost for the stub area.

Area ID

Range: 1~4294967295

Function: Configure a specified area as the stub area.

⚠️ **Caution:**
CAUTION
The backbone area, that is, Area 0, cannot be configured as the stub area.

---

12. Configure an OSPF virtual link.

Click [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [Other parameter configuration] → [OSPF virtual link configuration] to enter the OSPF virtual link configuration page, as shown in Figure 231.

OSPF virtual link configuration

Route ID(A.B.C.D)	11.1.1.1
Transmit Area ID(1-4294967295)	2
Hello packet interval (1-65535 秒)	10
Neighbour router invalid interval(1-2147483647 秒)	40
Sending link-state packet delay (1-65535 秒)	1
Sending link-state packet retransmit interval (1-65535 秒)	5

Add   Remove

Figure 231 Configuring OSPF Virtual Links

Route ID

Format: A.B.C.D

Function: Set the RID for the peer end of the virtual link.

Transit Area ID

Range: 1~4294967295

Function: Specify the transit area for the virtual link.

Hello packet interval

Range: 1~65535s

Default: 10s

Function: Configure the interval for sending hello packets on the specified interface.

Description: The switch periodically sends hello packets to neighbors to discover and maintain neighboring relationships and elect the DR and BDR.

Neighbour router invalid interval

Range: 1~2147483647 s

Default: 40s

Function: Configure the interval for the expiration of routes to adjacent switches. The value must be larger than or equal to four times the hello packet interval.

Description: If the switch does not receive hello packets from an adjacent device within the interval, the adjacent device is considered as unreachable and invalid.

Sending link-state packet delay

Range: 1~65535s

Default: 1s

Function: Configure LSA sending delay on the specified interface.

Sending link-state packet retransmit interval

Range: 1~65535s

Default: 5s

Function: Set the interval for retransmitting LSAs to adjacent switches on a specified interface.

Description: After sending an LSA to an adjacent device, the switch keeps the LSA until it receives the confirmation from the adjacent device. If the switch does not receive the confirmation within the interval, it retransmits the LSA.

> **Caution:**
> The parameter settings must be consistent between both ends of a virtual link.

13. Set the priority of a VLAN interface

Click [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [Other parameter configuration] → [Port DR priority configuration] to enter the VLAN interface priority configuration page, as shown in Figure 232.

Figure 232 Setting Priority for the VLAN Interface

Priority

Range: 0~255

Default: 1

Function: Set the priority of the OSPF-enabled VLAN interface.

Description: During DR and BDR selection, the switch with the largest value for this parameter is selected as the DR.

14. View OSPF information.

Click [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF debug] → [show ip ospf] to enter the OSPF information page, as shown in Figure 233.

OSPF information

my router ID	1.1.1.1
preference	110
ase preference	200
export metric	1
export tag	2147483648

Figure 233 OSPF Information

15. View OSPF external route information.

Click [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF debug] → [show ip ospf ase] to enter the OSPF external route information page, as shown in Figure 234.

OSPF Imported External AS Route Information

Destination	AdvRouter	NextHop	Age	SeqNumber	Type	Cost
7.7.7.0	2.2.2.2	2.2.2.3	1145	-2147483506	DTYPE_ASBR	1

Figure 234 External Route Information

16. View OSPF statistics.

Click [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF debug] → [show ip ospf cumulative] to enter the OSPF statistics page, as shown in Figure 235.

OSPF information

my router ID	1.1.1.1
preference	110
ase preference	200
export metric	1
export tag	2147483648

Figure 235 OSPF Statistics

17. View OSPF database information

Click [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF debug] → [show ip ospf database] to enter the OSPF database information page, as shown in Figure 236.

OSPF database information

AREA 0

Router LSAs

LS ID(Router ID)	ADV rtr	Age	Sequence	Cost	Checksum				
2.2.2.2	2.2.2.2	331	0x800001ea	1	49246	Type : Transit net	Cost : 1	DR : 2.2.2.2	Address: 2.2.2.2
						Type : Virtual link	Cost : 1	RouterID : 3.3.3.3	Address: 3.3.3.1
1.1.1.1	1.1.1.1	340	0x80000228	0	59435	Type : Transit net	Cost : 1	DR : 2.2.2.2	Address: 2.2.2.1
3.3.3.3	3.3.3.3	330	0x80000231	2	36454	Type : Virtual link	Cost : 1	RouterID : 2.2.2.2	Address: 3.3.3.2

Network LSAs

LS ID(DR's IP)	ADV rtr	Age	Sequence	Cost	Checksum
2.2.2.2	2.2.2.2	336	0x800000c0	1	64898

Summary Network LSAs

LS ID(Net's IP)	ADV rtr	Age	Sequence	Cost	Checksum
20.1.1.0	1.1.1.1	521	0x80000178	65535	26468
5.5.5.0	3.3.3.3	333	0x80000006	4	33976
4.4.4.255	3.3.3.3	416	0x8000021e	3	26814
3.3.3.0	3.3.3.3	333	0x80000119	3	39318
3.3.3.0	2.2.2.2	336	0x800001ef	2	2643

ASBR Summary LSAs

LS ID(Net's IP)	ADV rtr	Age	Sequence	Cost	Checksum

AREA 4

Router LSAs

LS ID(Router ID)	ADV rtr	Age	Sequence	Cost	Checksum				
1.1.1.1	1.1.1.1	746	0x8000010e	0	13044	Type : Stub net	Cost : 1	Network : 20.1.1.0	NetMask: 255.255.255.0

Network LSAs

LS ID(Router ID)	ADV rtr	Age	Sequence	Cost	Checksum

Summary Network LSAs

LS ID(Net's IP)	ADV rtr	Age	Sequence	Cost	Checksum
5.5.5.0	1.1.1.1	319	0x80000001	65535	56937
2.2.2.255	1.1.1.1	319	0x80000007	65535	8493
4.4.4.255	1.1.1.1	319	0x80000001	65535	63571
3.3.3.0	1.1.1.1	319	0x80000003	65535	3903

ASBR Summary LSAs

LS ID(ASBR's Rtr ID)	ADV rtr	Age	Sequence	Cost	Checksum
2.2.2.2	1.1.1.1	335	0x80000001	65535	2886

AS External LSAs

LS ID(ASBR's Rtr ID)	ADV rtr	Age	Sequence	Cost	Checksum	ls_type	metric	ase_type	forward	tag

Figure 236 OSPF Database Information

18. View OSPF neighbor information.

Click [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF debug] → [show ip ospf neighbor] to enter the OSPF neighbor information page, as shown in Figure 237.

OSPF Neighbor

interface p :20.1.1.1						
neighbor: area	router id	router IP	state	priority	DR	BDR
interface ip :2.2.2.1						
neighbor: area	router id	router IP	state	priority	DR	BDR
0	2.2.2.2	2.2.2.2	NFULL	1	2.2.2.2	2.2.2.1

Figure 237 OSPF Neighbor Information

19. View OSPF routing information.

Click [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF debug] → [show ip ospf routing] to enter the OSPF routing information page, as shown in Figure 238.

OSPF routes information

AS internal routes

Destination	Area	Cost	Dest Type	Next Hop	ADV rtr
20.1.1.0	4	1	DTYPE_NET	20.1.1.1	1.1.1.1
2.2.2.0	0	1	DTYPE_NET	2.2.2.1	2.2.2.2
3.3.3.0	0	2	DTYPE_NET	2.2.2.2	2.2.2.2
5.5.5.0	0	4	DTYPE_NET	2.2.2.2	3.3.3.3
4.4.4.0	0	3	DTYPE_NET	2.2.2.2	3.3.3.3

AS external routes

Destination	AdvRouter	NextHop	Age	SeqNumber	Dest Type	Cost
7.7.7.0	2.2.2.2	2.2.2.3	1245	0x8000008e	DTYPE_ASBR	1

Figure 238 OSPF Route Information

20. View route entries.

Click [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [show ip route] to enter the routing information page, as shown in Figure 239.

```
                              Information Display
Total route items is 6, the matched route items is 6
Codes: C - connected, S - static, R - RIP derived, O - OSPF derived
       A - OSPF ASE, B - BGP derived, D - DVMRP derived

    Destination      Mask             Nexthop        Interface       Preference
C   2.2.2.0          255.255.255.0    0.0.0.0        Vlan2           0
O   3.3.3.0          255.255.255.0    2.2.2.2        Vlan2           110
O   4.4.4.0          255.255.255.0    2.2.2.2        Vlan2           110
O   5.5.5.0          255.255.255.0    2.2.2.2        Vlan2           110
A   7.7.7.0          255.255.255.0    2.2.2.3        Vlan2           200
C   20.1.1.0         255.255.255.0    0.0.0.0        Vlan1           0
```

Figure 239 Routing Table

6.13.3.6 Typical Configuration Example

It is required to enable OSPF on all the switches and divide the entire AS into three areas. Area 2 is not directly connected to Area 0. A virtual link is required between R2 and R3. As the transit area, Area 1 connects Area 2 to Area 0. R2 and R3 serve as ABRs to forward the information about inter-area routes.
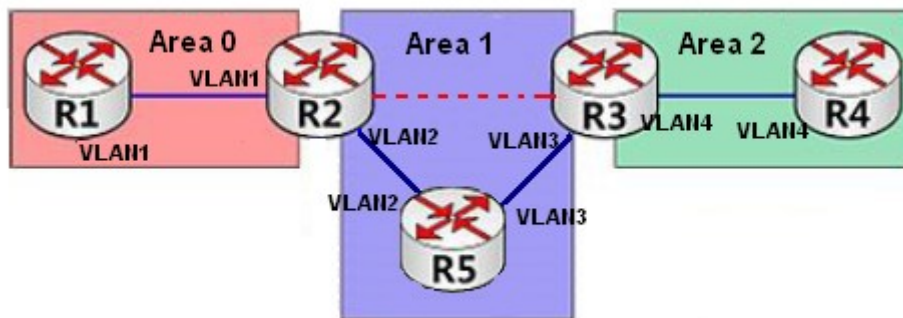
Figure 240 OSPF Typical Configuration Example

Configuration on R1:

1. Set the IP address of interface VLAN1 to 192.168.1.1 and subnet mask to 255.255.255.0.

2. Set the RID to 192.168.1.1, as shown in Figure 221.

3. Enable OSPF, as shown in Figure 220.

4. Configure the network range. Set the Network IP address to 192.168.1.0, Network mask to 255.255.255.0, Area ID to 0, and Advertise to Yes, as shown in Figure 222.

5. Add interface VLAN1 to Area 0, as shown in Figure 223.

Configuration on R2:

1. Set the IP address of interface VLAN1 to 192.168.1.2 and subnet mask to 255.255.255.0, and those of interface VLAN2 to 192.168.2.1 and 255.255.255.0.

2. Set the RID to 192.168.1.2, as shown in Figure 221.

3. Enable OSPF, as shown in Figure 220.

4. Configure network range. Set the Network IP address to 192.168.1.0, Network mask to 255.255.255.0, Area ID to 0, and Advertise to Yes. Set the Network IP address to 192.168.2.0, Network mask to 255.255.255.0, Area ID to 1, and Advertise to Yes, as shown in Figure 222.

5. Add VLAN1 to Area 0 and VLAN2 to Area 1, as shown in Figure 223.

6. Configure a virtual link. Set the ID of the Layer-3 switch to 192.168.3.2, Transit Area ID to 1, and adopt default settings for the other parameters, as shown in Figure 231.

Configuration on R3:

1. Set the IP address of interface VLAN3 to 192.168.3.2 and subnet mask to 255.255.255.0, and those of interface VLAN4 to 192.168.4.1 and 255.255.255.0.

2. Set the RID to 192.168.3.2, as shown in Figure 221.

3. Enable OSPF, as shown in Figure 220.

4. Configure network range. Set the Network IP address to 192.168.3.0, Network mask to 255.255.255.0, Area ID to 1, and Advertise to Yes. Set the Network IP address to 192.168.4.0, Network mask to 255.255.255.0, Area ID to 2, and Advertise to Yes, as shown in Figure 222.

4. Add VLAN3 to Area 1 and VLAN4 to Area 2, as shown in Figure 223.

5. Configure a virtual link. Set the ID of the Layer-3 switch to 192.168.1.2, Transit Area ID to 1, and adopt default settings for the other parameters, as shown in Figure 231.

Configuration on R4:

1. Set the IP address of interface VLAN4 to 192.168.4.2 and subnet mask to 255.255.255.0.

2. Set the RID to 192.168.4.2, as shown in Figure 221.

3. Enable OSPF, as shown in Figure 220.

4. Configure the network range. Set the Network IP address to 192.168.4.0, Network mask

to 255.255.255.0, Area ID to 2, and Advertise to Yes, as shown in Figure 222.

5. Add interface VLAN4 to Area 2, as shown in Figure 223.

Configuration on R5:

1. Set the IP address of interface VLAN2 to 192.168.2.2 and subnet mask to 255.255.255.0, and those of interface VLAN3 to 192.168.3.1 and 255.255.255.0.

2. Set the RID to 192.168.2.2, as shown in Figure 221.

3. Enable OSPF, as shown in Figure 220.

4. Configure network range. Set the Network IP address to 192.168.2.0, Network mask to 255.255.255.0, Area ID to 1, and Advertise to Yes. Set the Network IP address to 192.168.3.0, Network mask to 255.255.255.0, Area ID to 1, and Advertise to Yes, as shown in Figure 222.

5. Add VLAN2 to Area 1 and VLAN3 to Area 1, as shown in Figure 223.

6.14 DHCP Configuration

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 241.
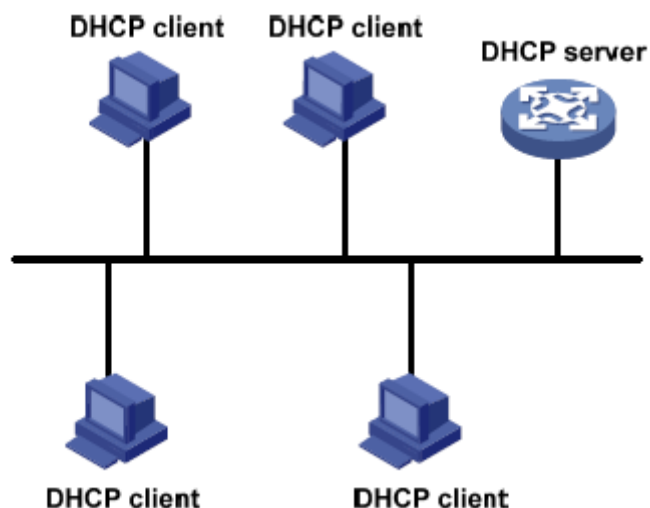
Figure 241 DHCP Typical Application

	Caution:
⚠️ 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.

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.

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.

6.14.1 DHCP Server Configuration

6.14.1.1 Introduction

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.

6.14.1.2 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.

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.

6.14.1.3 Web Configuration

1. Enable DHCP server

Click [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Enable DHCP] to enable DHCP server, as shown in Figure 242.
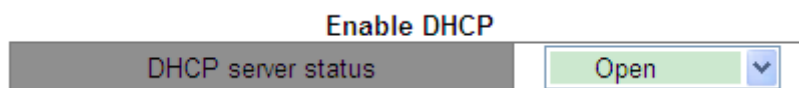
Figure 242 Enable DHCP Server

DHCP server status

Option: Open/Close

Default: Close

Function: select the current switch to the DHCP server to allocate an IP address to a client or

not.

2. Statically allocate IP Address

Click [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Address pool configuration] to create DHCP address pool, as shown in Figure 243.

Figure 243 Create Address Pool

DHCP pool name

Range: 1~32 characters

Function: configure the name of the IP address pool. Create/delete an address pool by selecting "Add pool/Del pool".

DHCP pool domain name

Range: 1~255 characters

Function: Configure the domain name of the IP address pool. When allocating an IP address to a client, send the domain name suffix to the client too.

Address lease timeout

Range: 0 day 0 Hour 0 Minute ~ 365 day 23 Hour 59 Minute

Description: The lease timeout of static allocation is infinite. The configuration of this parameter is invalid for static allocation.

Note:

➢ Static allocation of IP address can be regarded as obtaining IP address from a special

address pool that contains only one specific IP address. Therefore, a DHCP address pool

must be created before the statically allocated IP address.

➢ Only one type of IP address allocation mechanism can be configured for each DHCP

address pool.

Click [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Manual address pool configuration] to enter static allocation configuration page, as shown in Figure 244.

Figure 244 Statically Allocate IP Address

DHCP pool name

Function: select a created pool name.

Hardware address

Format: HH-HH-HH-HH-HH-HH (H is a hexadecimal number)

Function: Configure the MAC address of the client statically bounded.

Client IP

Format: A.B.C.D

Function: Configure the IP address of the client statically bounded.

Description: Static IP address allocation is implemented by bounding the MAC address and IP address of the client. When the client with this MAC address requests for IP address, the DHCP server finds the IP address corresponding to the MAC address of the client and allocates the IP address to the client. The priority of this allocation mode is higher than that of dynamic IP address allocation, and the tenancy term is permanent.

Client network mask

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.

User name

Range: 1~255 characters

Function: Configure client user name.

3. Dynamically Allocate IP Address

Click [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Address pool configuration] to enter dynamic allocation configuration page, as shown in Figure 245.

Figure 245 Dynamically Allocate IP Address

DHCP pool name

Range: 1~32 characters

Function: configure the name of the IP address pool. Create/delete an address pool by selecting "Add pool/Del pool".

DHCP pool domain name

Range: 1~255 characters

Function: Configure the domain name of the IP address pool. When allocating an IP address to a client, send the domain name suffix to the client too.

Address range of allocating {IP, MASK}

Fuction: Configure the range of the IP address pool, and the address range is determined by the subnet mask. 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.

> **Note:**
>
> Only one address segment can be configured in each address pool.

DHCP client node type

Option: --/Broadcast node/Peer-to-peer node/Mixed node/Hybrid node

Default: --

Function: Configure the client NetBIOS node type allocated by DHCP server. When the DHCP client uses the NetBIOS protocol for communication on the network, a mapping must be established between the host name and IP address. Different node types obtain the mapping in different modes.

Description: The broadcast node obtains the mapping in broadcast mode. The peer-to-peer node obtains the mapping by sending a unicast packet to communicate with the WINS server. The mixed node obtains the mapping by sending a broadcast packet the first time. If the mixed node fails to obtain the mapping the first time, it obtains the mapping by sending a unicast packet to communicate with the WINS server the second time. The hybrid node obtains the mapping by sending a unicast packet to communicate with the WINS server the first time. If the hybrid node fails to obtain the mapping the first time, it obtains the mapping by sending a broadcast packet the second time.

Address lease timeout

Range: 0 day 0 Hour 0 Minute ~ 365 day 23 Hour 59 Minute

Description: Configure lease timeout of dynamic allocation. 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.

4. Configure DHCP client's gateway

Click [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Client's default gateway configuration] to enter DHCP client's gateway configuration page, as shown in Figure 246.

Figure 246 DHCP Client's Gateway Configuration

DHCP pool name

Function: select a created pool name.

Gateway 1~Gateway 8

Function: Configure the client gateway address allocated by DHCP server.

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 8 gateways. Gateway 1 has the highest priority, and gateway 8 has the lowest priority.

5. Configure DHCP client DNS server

Click [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Client DNS server configuration] to enter DHCP client DNS server configuration page, as shown in Figure 247.

Figure 247 DHCP Client DNS Server Configuration

DHCP pool name

Function: select a created pool name.

DNS server 1~DNS server 8

Function: Configure the client DNS server address allocated by DHCP server.

Explanation: 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 (Domain Name System). 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 8 DNS servers. DNS server 1 has the highest priority, and DNS server 8 has the lowest priority.

6. Configure DHCP client WINS server

Click [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Client WINS server configuration] to enter DHCP client WINS server configuration page, as shown in Figure 248.

Figure 248 DHCP Client WINS Server Configuration

DHCP pool name

Function: select a created pool name.

WINS server 1~WINS server 8

Function: Configure the client WINS server address allocated by the DHCP server.

Explanation: For the client running a Microsoft Windows operating system (OS), the Windows Internet Naming Service (WINS) server provides the service of resolving a host name into an IP address for the host that uses the NetBIOS protocol for communication. Therefore, most Windows OS-based clients require WINS configuration. To enable the DHCP client to resolve a host name into an IP address, specify the WINS server address when the DHCP server allocates an IP address to the client. DHCP address pool can configure max 8 WINS servers. WINS server 1 has the highest priority, and WINS server 8 has the lowest priority.

7. Configure DHCP client TFTP server address and bootfile name

Click [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [DHCP file server address configuration] to enter DHCP client TFTP server address and bootfile name configuration page, as shown in Figure 249.

DHCP file server address configuration

DHCP pool name	pool-2
DHCP client bootfile name(1-128 character)	boot.img
File server 1	192.168.0.204
File server 2(optional)	
File server 3(optional)	
File server 4(optional)	
File server 5(optional)	
File server 6(optional)	
File server 7(optional)	
File server 8(optional)	

Apply

Figure 249 DHCP Client TFTP Server Address and Bootfile Name Configuration

DHCP pool name

Function: select a created pool name.

DHCP client bootfile name

Range: 1~128 characters

Function: Configure the client startup file name allocated by the DHCP server. During startup of a diskless device, the startup file must be downloaded from the server and then imported.

File server 1~File server 8

Function: Configure the client TFTP server address allocated by the DHCP server. DHCP address pool can configure max 8 file servers. File server 1 has the highest priority, and File server 8 has the lowest priority.

8. Configure DHCP network parameter

Click [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [DHCP network parameter configuration] to enter DHCP network parameter configuration page, as shown in Figure 250.

Figure 250 DHCP Network Parameter Configuration

DHCP pool name

Function: select a created pool name.

Code

Range: 0~254

Function: Configure the DHCP option. The DHCP retains the message format of BootP for compatibility with BootP. The newly added function of BootP is implemented through the **Option** field. The DHCP transmits control information and network configuration parameters through the **Option** field, implementing IP address allocation and providing the client with richer configuration information. For example, Option72 is an option of the WWW server, which is used to specify the WWW server address to be allocated to the client.

Note:

➢ For details about DHCP options, see RFC2132.

➢ The Web page provides configuration of common options (for example, gateway address, DNS server address, and WINS server address). Network parameter codes cannot be configured as these common options.

Network parameter value type

Options: ascii/hex/ip address

Function: Configure the network parameter value type. ascii is an ascii character string, and its configuration range is 1 to 255 characters. Hex is a hexadecimal number, and its configuration length must be an even number in the range of 1 to 510.

Network parameter value

Function: Configure a corresponding network parameter value based on the network parameter value type.

Operation type

Option: Set/cancel network parameter.

Function: Set/cancel the network parameter value of the current option.

9. Query DHCP address pool configuration

Click [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Query address pool configuration] to query DHCP address pool configuration, as shown in Figure 251.

Figure 251 Query DHCP Address Pool Configuration

DHCP pool name

Function: select a created pool name.

10. Configure the range of IP addresses are not allocated dynamically in the DHCP address pool

Click [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Excluded address configuration] to enter excluded address configuration page, as shown in Figure 252.

Figure 252 Configure the Range of IP Addresses are not Allocated Dynamically

Starting address/Ending address

Function: Configure the range of IP addresses are not allocated dynamically in the DHCP address pool. When allocating IP addresses, the DHCP server must eliminate the occupied IP address (for example, IP addresses of the gateway and DNS server). Otherwise, the same IP address may be allocated to two clients, causing IP address conflict.

Operation type

Options: Add address not for allocating dynamically/Remove address not for allocating dynamically

Function: Add/Remove the range of IP addresses are not allocated dynamically in the DHCP address pool.

11. View DHCP packet statistics

Click [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [DHCP packet statistics] to view DHCP packet statistics, as shown in Figure 253.

DHCP packet statistics

Address pool	2
Proxy database	0
Dynamical allocated address	1
Manual binded address	-1
Address conflict	0
Binding exceeding lease time	2
Errors	546

Received DHCP packet statistics

Received	3395
DHCPDISCOVER	1226
DHCPREQUEST	1724
DHCPDECLINE	24
DHCPRELEASE	7
DHCPINFORM	412

Transmitted DHCP packet statistics

Transmitted	2580
DHCPOFFER	1162
DHCPACK	562
DHCPNAK	570
DHCPRELAY	0
DHCPFORWARD	0

Clear   Show

Figure 253 View DHCP Packet Statistics

You can click <Show> button to update DHCP data packet statistics in real time, and you can click <Clear> button to clear the received/transmitted DHCP data packet statistics.

12. Delete DHCP server statistics log

Click [Device Advanced Configuration] → [DHCP configuration] → [DHCP debugging] → [Delete DHCP server statistics log] to delete DHCP server statistics log, as shown in Figure 254.

Delete DHCP server statistics log

Apply

Figure 254 Delete DHCP Server Statistics Log

Click <Apply> button to clear received/transmitted DHCP packet statistics.

13. Show IP-MAC binding information

Click [Device Advanced Configuration] → [DHCP configuration] → [DHCP debugging] → [Show IP-MAC binding] to show IP-MAC binding information, as shown in Figure 255.

```
                          Information Display
IP address            Hardware adress          Lease expiration
Type
192.168.0.23          44-37-E6-88-6E-90        Infinite
Manual
192.168.0.6           00-1E-CD-19-00-02        Infinite
Manual
Total dhcp binding items: 2, the matched: 2
```

Figure 255 Show IP-MAC Binding Information

6.14.1.4 Typical Configuration Example

As Figure 256 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 two ways. The excluded IP address range is 192.168.0.1~192.168.0.9 when DHCP server dynamically allocates IP address.
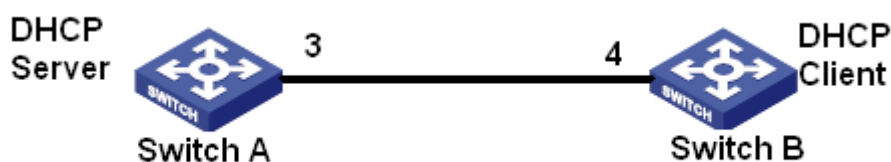
Figure 256 DHCP Typical Configuration Example

Statically allocate IP address

➤ Switch A configuration:

1. Enable DHCP server status, as shown in Figure 242.

2. Create a DHCP IP pool: pool-1, as shown in Figure 243.

3. Bind the MAC address of switch B: 00-1e-cd-19-00-02 to the IP address: 192.168.0.6, set mask as 255.255.255.0, as shown in Figure 244.

➤ Switch B configuration:

1. Set the mode for obtaining an IP addresses bootp-client or dhcp-client, as shown in Figure 118.

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 257.

L3 interface IP configuration

Interface	IP address	Subnet mask	Status
Vlan1	0.0.0.0	0.0.0.0	no shutdown

Add   Del

Vlan1		
IP address	Subnet mask	Type
192.168.0.6	255.255.255.0	(Primary)

Figure 257 DHCP Client Obtain IP Address-1

Dynamically allocate IP address

➢ Switch A configuration:

1. Enable DHCP server status, as shown in Figure 242.

2. Create a DHCP IP pool: pool-2, set domain name to domain.com, address range for allocating to 192.168.0.3(IP) and 255.255.255.0(MASK), and lease timeout to 20 days, as shown in Figure 245.

3. Configure excluded IP address range as 192.168.0.1~192.168.0.9, as shown in Figure 252.

➢ Switch B configuration:

1. Set the mode for obtaining an IP addresses bootp-client or dhcp-client, as shown in Figure 118.

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 in Figure 258.

L3 interface IP configuration

Interface	IP address	Subnet mask	Status
Vlan1	0.0.0.0	0.0.0.0	no shutdown

Add   Del

Vlan1		
IP address	Subnet mask	Type
192.168.0.10	255.255.255.0	(Primary)

Figure 258 DHCP Client Obtain IP Address-2

6.15 QoS Configuration

6.15.1 Introduction

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

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

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

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

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

6.15.2 QoS CAR

QoS committed access rate (CAR) is a type of rate limiting policy. This policy quotes the ACL rule for stream identification, limits the port rate for matched packet, and discards the stream going beyond the range (width and burst value) stipulated by the QoS policy in the packet.

6.15.3 QoS Remark

QoS Remark quotes the ACL rule for stream identification and specifies priority (DSCP or COS value) for the matched package again.

6.15.4 Principle

Each port of this series switches supports 8 cache queues, from 0 to 7 in priority ascending order.

You can configure the mapping between priority and queues. When a frame reaches the port, the switch determines the queue for the frame according to the information in the frame header. The switch supports two queue mapping modes for priority identification: CoS and DSCP.

➢ The CoS value depends on the priority of 802.1Q Tag in the packet. The mapping between CoS value and Queue can be configured.

➢ DSCP value depends on TOD/DSCP part of the packet. The mapping between DSCP value and queue can be configured.

When forwarding data, a port uses a scheduling mode to schedule the data in 8 queues and the bandwidth of each queue. This series switches support two scheduling modes: WRR (Weighted Round Robin) and priority-queue.

➢ WRR schedules data flows based on weight ratio. Queues obtain their bandwidths based on their weight ratio. WRR prioritizes high-weight ratio queues. More bandwidths are allocated to queues with higher weight ratio.

➢ Priority-queue scheduling mode can stringently guarantee the top forwarding priority to the packet with highest priority and mainly used in the sensitive signal transmission. Once a frame enters a high priority queue, the system stops the data scheduling of the low priority queue and handles the data in high priority queue. Only when the high priority queue is empty can it start processing the data in the lower priority queue in turn.

6.15.5 Web Configuration

1. Enable QoS function.

Click [Device Advanced Configuration] → [QoS configuration] → [Enable QoS] → [Enable/Disable QoS] to enable QoS, as shown in Figure 259.
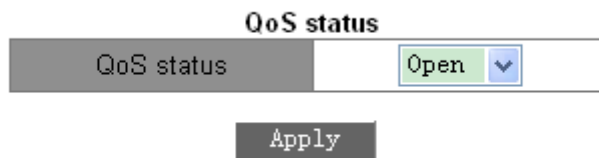
Figure 259 Enable QoS

QoS Status

Options: Open/close

Default: Close

Function: Enable/Disable the global QoS function.

2. Add/Remove class-map

Click [Device Advanced Configuration] → [QoS configuration] → [Class-map configuration] → [Add/Remove calss-map] to add/remove class-map, as shown in Figure 260.
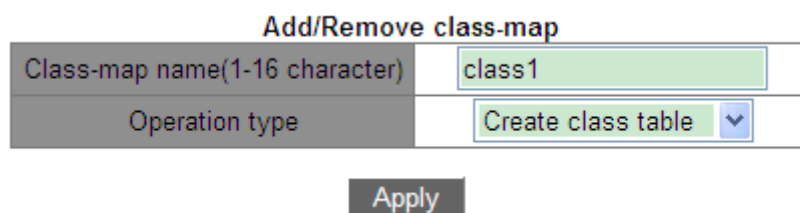
Figure 260 Add/Remove Class-map

Class-map name

Range: 1~16 characters

Function: Configure class-map name.

Operation type

Options: Create class table/ Remove class table

Function: Create/Remove class table

3. Configure match action of the class-map

Click [Device Advanced Configuration] → [QoS configuration] → [Class-map configuration]

→ [Class-map configuration] to enter class-map configuration page, as shown in Figure 261.

Class-map configuration

Class-map name	class1 ∨
Match action	access-group 1st ∨
Match value 1	1024
Operation type	Set ∨

Apply

Figure 261 Match action of the class-map configuration

Class-map name

Options: All created class-maps

Match action

Default: access-group 1st

Function: Configure match action of the class-map.

Match value 1

Default: 1024

Function: Match the specified ACL entry. The ACL 1024 entry exists on the switch by default, and this entry matches all packets.

Operation type

Options: Set/Del

Function: Set/Delete match action of the class-map.

4. Add/Remove policy-map

Click [Device Advanced Configuration] → [QoS configuration] → [Policy-map configuration]

→ [Add/Remove policy-map] to add/remove policy-map, as shown in Figure 262.

Operation

| Policy-map name (1-16 character) | policy1 |
| Operation type | Add policy table ∨ |

Apply

Figure 262 Add/Remove Policy-map

Policy-map name

Range: 1~16 characters

Function: Configure policy-map name.

Operation type

Options: Create policy table/ Remove policy table

Function: Create/Remove policy table

5. Configuration policy-map bandwidth

Click [Device Advanced Configuration] → [QoS configuration] → [Policy-map configuration] → [Policy-map bandwidth configuration] to enter policy-map bandwidth configuration page, as shown in Figure 263.

Figure 263 Policy-map Bandwidth Configuration

Policy-map name

Options: All created policy-maps.

Class-map name

Options: All created class-maps

Rate

Range: 1~10000000 kbit/s

Function: Configure rate value.

Normal burst

Range: 1~1000000 kbyte

Function: Configure normal burst value.

Exceed action

Options: Drop

Function: Execute the packet dropping policy for the part exceeding the rate limit value in the packet meeting match action in the class-map.

Operation type

Options: Set/Del

Function: Set/Delete policy-map bandwidth configuration

6. Configure priority remarking of the policy-map

Click [Device Advanced Configuration] → [QoS configuration] → [Policy-map configuration] → [Policy-map priority configuration] to enter policy-map priority configuration page, as shown in Figure 264.

Figure 264 Priority Remarking Configuration

Policy-map name

Options: All created policy-maps.

Class-map name

Options: All created class-maps.

Priority type

Options: DSCP value/COS value

Function: Select the priority type that needs to be remarked.

Priority value

Options: 0~63 (DSCP value) /0~7 (COS value)

Function: Configure the re-marking value of the priority.

Description: Execute the re-marking policy for the priority value in the packet meeting match action in the class-map.

Operation type

Options: Set/Del

Function: Set/Delete priority remarking of the policy-map.

7. Apply policy-map to port

Click [Device Advanced Configuration] → [QoS configuration] → [Apply QoS to the port] → [Apply policy-map to port] to apply policy-map to port, as shown in Figure 265.

Apply policy-map to port	
Port	1/1
Policy-map name	a
Port direction	Input
Operation	Set

Reset　Apply

Figure 265 Apply Policy-map to Port

Policy-map name

Options: All created policy-maps.

Port direction

Options: Input

Function: Apply this policy table in the inlet direction of the port to implement rate limiting or priority re-marking for the packet received through the port.

Operation type

Options: Set/Del

Function: Set/Delete application policy-map to port.

> **Caution:**
> ➢ Apply only one policy-map to a port.
> ➢ Port trust mode configuration and application policy-map to port are mutually exclusive.

8. Configure port trust mode.

Click [Device Advanced Configuration] → [QoS Configuration] → [Apply QoS to port] → [Port trust mode configuration] to enter port trust mode configuration page, as shown in Figure 266.

Port trust mode configuration

Port	1/3
⦿ Port trust status	dscp
○ Port priority(0-7)	

Reset   Apply   Default
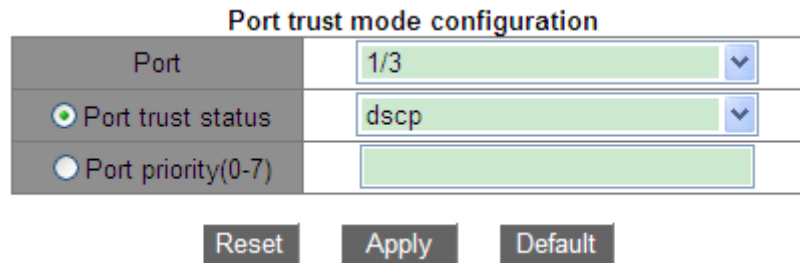
Figure 266 Port Trust Mode Configuration

Port

Options: all switch ports

Port trust status

Options: cos/cos pass through dscp/dscp/dscp pass through cos

Default: If the port-received packet is an IP packet, the default is dscp; if it is not an IP packet but is a tagged packet, the default is cos. If it is not an IP packet but an untagged packet, the port does not have a default trust mode, and will save the packet in queue 0.

Function: Configure the trust status of switch ports.

Description: **cos** and **cos pass through dscp** both mean port trust CoS value. The queue to save the port-received packet is determined by the CoS value and queue mapping. If the packet does not have a CoS value, it is mapped to queue according to the CoS value of 0. The differences between **cos** and **cos pass through dscp** are that **cos** will change the packet's DSCP value to the one in the mapping between CoS and DSCP during packet forwarding, but **cos pass through dscp** does not change the packet's DSCP value during packet forwarding.

dscp and **dscp pass through cos** both mean port trust DSCP value. The queue to save the port-received packet is determined by the DSCP value and queue mapping. If the packet does not have a DSCP value, it is mapped to queue according to the DSCP value of 0. The differences between **dscp** and **dscp pass through cos** are that **dscp** will change the

packet's CoS value to the one in the mapping between DSCP and CoS during packet forwarding, but **dscp pass through cos** does not change the packet's CoS value during packet forwarding.

Port priority

Options: 0~7

Default: 0

Function: Assign a priority to the physical port. The packets received from the port are queued according to the assigned priority, but not the priority carried by the packets. The packets received from port of priority 0 are put in queue 0 and those received from port of priority 1 are put in queue 1. The rest can be done in the same manner.

9. Configure port default CoS value.

Click [Device Advanced Configuration] → [QoS Configuration] → [Apply QoS to port] → [Port default CoS configuration] to enter port default CoS configuration page, as shown in Figure 267.

Port default CoS configuration

Port	1/3
Default CoS value(0-7)	5

Reset   Apply   Default

Figure 267 Port Default CoS Configuration

Port

Options: all switch ports

Default CoS value

Options: 0~7

Default: 0

Function: Configure the default CoS value of the port.

Explanation: When a packet is untagged, the priority in the tag added to the packet is the default CoS value of the port.

10. Configure port queue scheduling mode to priority-queue.

Click [Device Advanced Configuration] → [QoS Configuration] → [Egress-queue

configuration] → [Port Egress-queue work mode configuration] to enter priority-queue scheduling mode configuration page, as shown in Figure 268.

Port name	Egress-queue Work Mode
1/5	WRR

Reset   Apply

Figure 268 Egress-queue Mode Configuration

Egress-queue Work Mode

Options: PQ/WRR

Default: PQ

Function: Configure the egress-queue mode of the selected port.

11. Configure the weight WRR of the port queue.

Click [Device Advanced Configuration] → [QoS Configuration] → [Egress-queue configuration] → [Port Egress-queue wrr weight configuration] to enter weight WRR configuration page, as shown in Figure 269.

Port Egress-queue wrr weight configuration

Profileindex	2
Weight for queue0(1-16)	4
Weight for queue1(1-16)	5
Weight for queue2(1-16)	1
Weight for queue3(1-16)	3
Weight for queue4(1-16)	2
Weight for queue5(1-16)	3
Weight for queue6(1-16)	6
Weight for queue7(1-16)	6

Reset   Apply

Figure 269 Weight Configuration

Profileindex

Options: 1~6

Default: 1

Function: Configure a group of weight values.

Explanation: The switch supports a maximum of 6 groups of weight values.

{Weight for queue0, Weight for queue1, Weight for queue2, Weight for queue3, Weight for queue4, Weight for queue5, Weight for queue6, Weight for queue7}

Options: {0~15, 0~15, 0~15, 0~15, 0~15, 0~15, 0~15}

Default: {1, 2, 3, 4, 5, 6, 7, 8}

Function: Configure weight values. Absolute weight value is meaningless. WRR allocates bandwidth according to 8 weight value ratios.

Description: If the weight value of one queue is 0, this queue has the highest priority and its packets will be forwarded with top priority. If the weight value of multiple queues is 0, the top forwarding priority is given to the data with the weight value of 0 and in the high priority queue, and the second priority is given to the data with the weight value of 0 and in the low priority queue. When all data with the weight value of 0 is forwarded, the switch starts forwarding data in other queues according to weight ratio.

12. Set the port queue scheduling mode to WRR and bind the weight ratio to port, as shown in Figure 270.

Figure 270 WRR Scheduling Mode Configuration

Port name

Options: all switch port

Function: Select the port to set its scheduling mode to WRR.

Profileindex

Options: 1~6

Function: Select the WRR weight ratio of the port.

13. Configure the mapping between CoS value and queue.

Click [Device Advanced Configuration] → [QoS Configuration] → [Egress-queue configuration] → [Mapping CoS values to egress queue] to enter CoS and queue mapping configuration page, as shown in Figure 271.

Mapping CoS values to egress queue

CoS0 value(0-7)	0
CoS1 value(0-7)	1
CoS2 value(0-7)	1
CoS3 value(0-7)	3
CoS4 value(0-7)	4
CoS5 value(0-7)	5
CoS6 value(0-7)	6
CoS7 value(0-7)	7

Reset   Apply   Default

Figure 271 Configuring Mapping between CoS Value and Queue

{CoS0~CoS7 value, Queue-ID }

Default: CoS value 0 is mapped to queue 0; CoS value 1 is mapped to queue 1;

CoS value 2 is mapped to queue 2; CoS value 3 is mapped to queue 3;

CoS value 4 is mapped to queue 4; CoS value 5 is mapped to queue 5;

CoS value 6 is mapped to queue 6; CoS value 7 is mapped to queue 7.

Function: Configure the mapping between CoS value and queue. The left column is CoS value, and the right column is queue ID.

Explanation: Each CoS value can be mapped to only one queue. Multiple CoS values can be mapped to one queue.

14. Configure the mapping between DSCP value and queue.

Click [Device Advanced Configuration] → [QoS Configuration] → [Egress-queue configuration] → [Mapping DSCP values to egress queue] to enter DSCP and queue mapping configuration page, as shown in Figure 272.

Mapping DSCP values to egress queue

Operation type	Set
DSCP1<0-63>	4
DSCP2<0-63>	5
DSCP3<0-63>	6
DSCP4<0-63>	14
DSCP5<0-63>	54
DSCP6<0-63>	57
DSCP7<0-63>	42
DSCP8<0-63>	58
Queue value<0-7>	1

Apply

Figure 272 Configuring Mapping between DSCP Value and Queue

Operation type

Options: Set/Del

Default: Set

Function: Configure the mapping between DSCP and Queue.

Description: Set is to establish the new mapping between DSCP value and queue. Del is to restore the default mapping between DSCP value and queue.

{DSCP, Queue value}

Options: {0~63, 0~7}

Default:

DSCP value 0~7 is mapped to queue 0; DSCP value 8~15 is mapped to queue 1;

DSCP value 16~23 is mapped to queue 2; DSCP value 24~31 is mapped to queue 3;

DSCP value 32~39 is mapped to queue 4; DSCP value 40~47 is mapped to queue 5;

DSCP value 48~55 is mapped to queue 6; DSCP value 56~63 is mapped to queue 7.

Function: Configure the mapping between DSCP value and queue.

Explanation: Each DSCP value can be mapped to only one queue. Multiple DSCP values can be mapped to one queue.

15. Configure mapping between CoS value and DSCP value.

Click [Device Advanced Configuration] → [QoS Configuration] → [QoS mapping configuration] → [CoS-to-DSCP mapping] to enter CoS to DSCP mapping configuration page, as shown in Figure 273.

Figure 273 Configuring Mapping between CoS and DSCP

Operation type

Configuration type: Set/Del

Default: Set

Function: Configure mapping between CoS and DSCP.

Description: Set is to establish the new mapping between CoS and DSCP. Del is to restore the default mapping between CoS and DSCP.

DSCP value

Options: 0~63

Default:

CoS value 0 is mapped to DSCP value 0; CoS value 1 is mapped to DSCP value 8;

CoS value 2 is mapped to DSCP value 16; CoS value 3 is mapped to DSCP value 24;

CoS value 4 is mapped to DSCP value 32; CoS value 5 is mapped to DSCP value 40;

CoS value 6 is mapped to DSCP value 48; CoS value 7 is mapped to DSCP value 56.

Function: Configure the mapping between CoS and DSCP. When the port trust mode is CoS, packet DSCP value can be changed according to this mapping.

Explanation: Multiple CoS values can be mapped to one DSCP value.

16. Configure mapping between DSCP value and CoS value.

Click [Device Advanced Configuration] → [QoS Configuration] → [QoS mapping configuration] → [DSCP-to-QoS mapping] to enter DSCP to CoS mapping configuration

page, as shown in Figure 274.

Figure 274 Configuring Mapping between DSCP and CoS

Operation type

Configuration type: Set/Del

Default: Set

Function: Configure mapping between DSCP and CoS.

Description: Set is to establish the new mapping between DSCP and CoS. Del is to restore

the default mapping between DSCP and CoS.

{DSCP value, COS value}

Options: {0~63, 0~7}

Default: DSCP value 0~7 is mapped to CoS value 0;

DSCP value 8~15 is mapped to CoS value 1;

DSCP value 16~23 is mapped to CoS value 2;

DSCP value 24~31 is mapped to CoS value 3;

DSCP value 32~39 is mapped to CoS value 4;

DSCP value 40~47 is mapped to CoS value 5;

DSCP value 48~55 is mapped to CoS value 6;

DSCP value 56~63 is mapped to CoS value 7.

Function: Configure the mapping between DSCP and CoS. When the port trust mode is DSCP, the packet CoS value can be changed according to this mapping.

Explanation: A maximum of 8 DSCP values can be mapped to one CoS value.

17. Configure mapping between DSCP value and DSCP value.

Click [Device Advanced Configuration] → [QoS Configuration] → [QoS mapping configuration] → [DSCP-to-DSCP mutation mapping] to enter DSCP to DSCP mapping configuration page, as shown in Figure 275.

Figure 275 Configuring Mapping between DSCP and DSCP

Operation type

Configuration type: Set/Del

Default: Set

Function: Configure the mapping between DSCP and DSCP.

Description: Set is to establish the mapping between DSCP and DSCP. Del is to delete the mapping between DSCP and DSCP. This series switches support a maximum of 28 DSCP mutation mappings.

DSCP mutation name

Range: 1~16 characters

Function: Set a name for DSCP mutation.

{Out-DSCP value, In-DSCP value}

Options: {0~63, 0~63}

Function: Configure the mapping between DSCP and DSCP. To change the packet DSCP value, use this mapping when the egress forwards the packet.

Explanation: A maximum of 8 DSCP values can be mapped to one DSCP value.

> **Caution:**
>
> The queue to save packets is determined by the initial mapping between DSCP value and queue.

18. Apply DSCP mutation mapping on port.

Click [Device Advanced Configuration] → [QoS Configuration] → [Apply QoS to port] → [Apply DSCP mutation mapping] to enter the configuration page, as shown in Figure 276.

Figure 276 Application of DSCP Mutation Mapping on Port

Port name

Options: all switch ports

Function: Select the port for using DSCP mutation mapping.

DSCP mutation name

Options: Name of DSCP to DSCP mapping

Function: Configure port-used DSCP mutation mapping.

Operation

Options: Set/Del

Function: Add/Delete port-used DSCP mutation mapping.

6.15.6 Typical Configuration Example

As shown in Figure 277, port 1, 2, 3, and 4 forward packet to port 5. Among them, the DSCP value of port 1 received packet is 6, trust mode is DSCP pass CoS, and the packets entering port 1 are mapped to queue 3; CoS value of port 2 received packet is 2, trust mode is CoS pass DSCP, and the packets entering port 2 are mapped to queue 1; CoS value of port 3 received packet is 2, DSCP value of that is 32, trust mode is DSCP, and packets entering port 3 are mapped to queue 2; DSCP value of port 4 received packet is 26, CoS value of that is 3, trust mode is CoS, and the packets entering port 4 are mapped to queue 3; port 5 adopts WRR scheduling mode.

Configuration process:

1. Enable QoS, as shown in Figure 259.

2. Set the trust mode of port 1 to DSCP pass CoS, port 2 to CoS pass DSCP, port 3 to DSCP, and port 4 to CoS, as shown in Figure 266.

3. The CoS-to-DSCP mapping and DSCP-to-CoS mapping both use default mapping, which means the CoS value of port 3 forwarding packets is changed to 4, while DSCP value of port 4 forwarding packets is changed to 24.

4. Map the CoS value 2 to queue 1 and the CoS value 3 to queue 3, as shown in Figure 271.

5. Map the DSCP value 6 to queue 3 and the DSCP value 32 to queue 2, as shown in Figure 272.

6. Configure port 5 queue scheduling mode to WRR, see Figure 268; use default queue weight ratio, as shown in Figure 270.
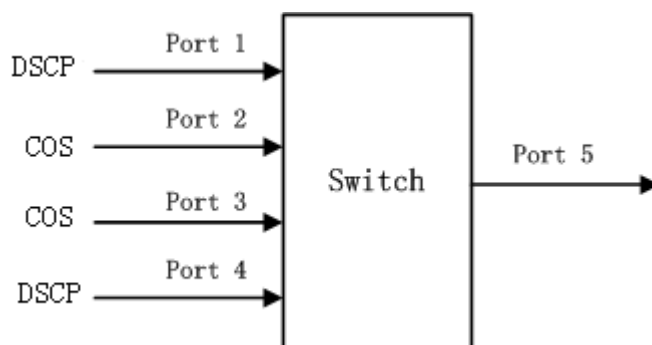
Figure 277 QoS Configuration Example

Port 1 and port 4 packets enter queue 3, port 2 packets enter queue 1, and port 3 packets

enter queue 2. According to the mapping between queue and weight, the weight of queue 1 is 2, and that of queue 2 is 3, and that of queue 3 is 4, so the bandwidth proportion allocated to the packets in ingress queue 1 is 2/ (2+3+4), that allocated to the packets in ingress queue 2 is 3/ (2+3+4), and that allocated to the packets in ingress queue 3 is 4/ (2+3+4). Among them, port 1 and port 4 packets both enter queue 3, so they are forwarded according to the rule of First In, First out (FIFO), but the total bandwidth proportion of port 1 and port 4 must be 4/ (2+3+4).

6.16 IEC61850 Configuration

6.16.1 Introduction

Currently, switches are transparent for other functional entities in substation networks. Tools other than IEC61850 are needed to monitor switches, such as EMS, Web, CLI, and OPC, causing inconsistency and inconveniency of network configuration and management.

To solve these problems, we create modeling for switches according to the IEC61850 standard and introduce switches to the substation automation systems as Intelligent Electronic Devices (IEDs), achieving a unified view of substation automation monitoring, facilitating integration and management solution planning, and saving construction and maintenance costs.

> **Caution:**
>
> The default modeling file **switch.cid** provided by the company has already been imported into the switch. If a customer wants to import other modeling files, please refer to "5.13 File Transmission Service" section.

6.16.2 Web Configuration

1. Enable IEC61850

Click [Device Advanced Configuration] → [IEC61850 Configuration] → [IEC61850 Configuration] to enter IE61850 configuration page, as shown in Figure 278.

Figure 278 IEC61850 Configuration

IEC61850 Function

Options: Enable/Disable

Default: Disable

Function: Enable or disable the IEC61850 function.

2. Configure IEC 61850
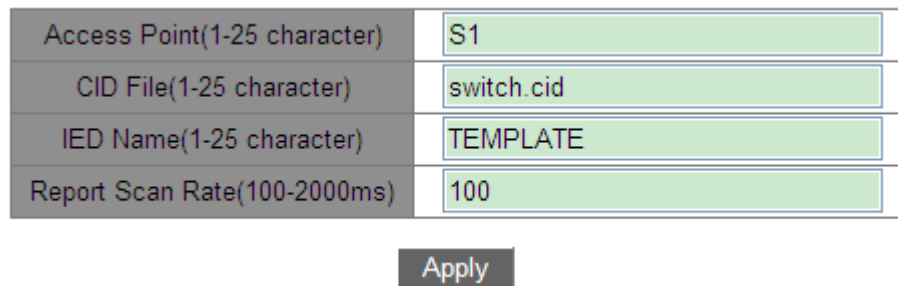
Figure 279 IEC61850 Configuration

Access Point

Range: 1~25 characters

Default: S1

Function: Configure name of access point corresponding to the IED in CID file.

CID File

Range: 1~25 characters

Default: switch.cid

Function: Configure name of the valid CID modeling file when IEC61850 function starts.

IED Name

Range: 1~25 characters

Default: TEMPLATE

Function: Configure logical device name corresponding to the IED in CID file.

Report Scan Rate

Range: 100~2000ms

Default: 100ms

Function: Configure interval of scanning device node information.

> **Caution:**
>
> Access Point and IED name configurations must be consistent with the Access Point and IED name in the specified modeling file. Otherwise, the IEC61850 function cannot be enabled.

6.17 IGMP Snooping

6.17.1 Introduction

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.

6.17.2 Basic Concepts

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

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

6.17.3 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 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).

6.17.4 Web Configuration

1. Enable IGMP Snooping.

Click [Device Advanced Configuration] → [Multicast protocol configuration] → [IGMP Snooping configuration] → [Enable IGMP Snooping] to enter the IGMP Snooping global configuration page, as shown in Figure 280.

Figure 280 Enabling IGMP Snooping

IGMP Snooping

Options: Open/Close

Default: Close

Function: Enable or disable the global IGMP Snooping protocol. IGMP Snooping and GMRP cannot be enabled at the same time.

2. Configure IGMP Snooping parameters.

Click [Device Advanced Configuration] → [Multicast protocol configuration] → [IGMP Snooping configuration] → [IGMP Snooping configuration] to enter the IGMP Snooping configuration page, as shown in Figure 281.

IGMP Snooping Configuration

VLAN ID	Snooping State	Static IP
vlan 1	Open	192.168.0.2

Apply

Figure 281 IGMP Snooping Configuration

VLAN ID

Options: all created VLAN IDs

Snooping state

Options: Open/Close

Default: Open

Function: Enable or disable the VLAN IGMP Snooping function. The precondition of this function is to enable global IGMP Snooping function.

Static IP

Format: A.B.C.D

Default: 192.168.0.2

Function: Configure the source IP address of sending packets.

3. Configure IGMP query parameters, as shown in Figure 282.

IGMP query Configuration

VLAN ID	Query State	Static IP	Robustness(2-10)	Query Interval(1-65535)	Max Response(10-25)
vlan 1	Open	192.168.0.2	2	125	10

Apply

Figure 282 IGMP Query Configuration

VLAN ID

Options: All created VLAN IDs

Function: Select the VLAN ID to enable IGMP query function.

Query State

Options: Open/ Close

Default: Close

Function: Enable or disable the IGMP query function for the selected VLAN. The precondition of this function is to enable global IGMP Snooping function.

Description: If there are multiple queriers in network, they will automatically select the one with the smallest IP address to be the querier. If there is only one device which enables IGMP query function, it will be the querier.

Caution:

Query and Snooping function are mutually exclusive in a VLAN. That means if query is open, snooping must be closed in one VLAN; if snooping is open, query must be closed.

Static IP

Format: A.B.C.D

Default: 192.168.0.2

Function: Configure the source IP address of sending the query packet.

Robustness

Range: 2~10

Default: 2

Function: Specify the robustness parameter of the IGMP query function.

Description: The larger the parameter, the worse the network environment. User can set a suitable robustness parameter according to the actual network.

Query Interval

Range: 1~65535s

Default: 125s

Function: Configure the interval of sending query packet.

Max Response

Range: 10~25s

Default: 10s

Function: Configure the max response time of responding the query packet.

After setting is completed, "IGMP Configuration" lists IGMP configuration information, as shown in Figure 283.

IGMP Configuration

VLAN ID	Snooping State	Query State	Static IP	Robustness	Query Interval	Max Response
1	Close	Open	192.168.0.2	8	125	10
2	Open	Close	192.168.0.2	0	0	0

Figure 283 IGMP Configuration

4. Configure IGMP Snooping static multicast parameters.

Click [Device Advanced Configuration] → [Multicast protocol configuration] → [IGMP Snooping configuration] → [IGMP Snooping static multicast configuration] to enter the IGMP Snooping static configuration page, as shown in Figure 284.

IGMP Snooping static multicast configuration

VLAN ID	1
Operation type	Add
Multicast group member port	1/1
Multicast address	225.0.0.0

Apply

Figure 284 IGMP Snooping Static Multicast Group Configuration

VLAN ID

Options: all created VLAN IDs

Operation type

Options: Add/Del

Default: Add

Function: Add/Delete a member port of multicast group.

Multicast group member port

Options: all switch ports

Function: Select the member port to be added to or deleted from the multicast group. If a port is connected to a host and the host receives data of a certain multicast group, this port can be configured to join a static multicast group and becomes the static member port.

Multicast address

Range: 224.0.1.0~239.255.255.255

Function: Input the multicast group address.

Description: When the newly added static multicast address is dynamically learned, this static multicast address will cover the dynamic multicast address.

5. View multicast entries.

Click [Device Advanced Configuration] → [Multicast protocol configuration] → [IGMP Snooping configuration] → [Show IGMP Snooping information] to display multicast entries, as shown in Figure 285.

Show IGMP Snooping information

VLAN ID	1

Apply
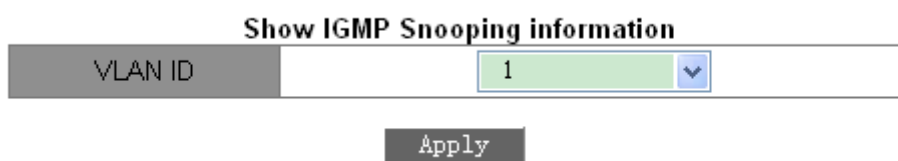
Figure 285 Multicast Member List

View the multicast entries in the selected VLAN.

6.17.5 Typical Application Example

As shown in Figure 286, enable IGMP Snooping function in Switch 1, Switch 2, and Switch 3. Enable auto query 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, so Switch 3 is elected to querier.

1. Enable IGMP Snooping.

2. Enable IGMP Snooping and auto-query.

3. Enable IGMP Snooping and auto-query.
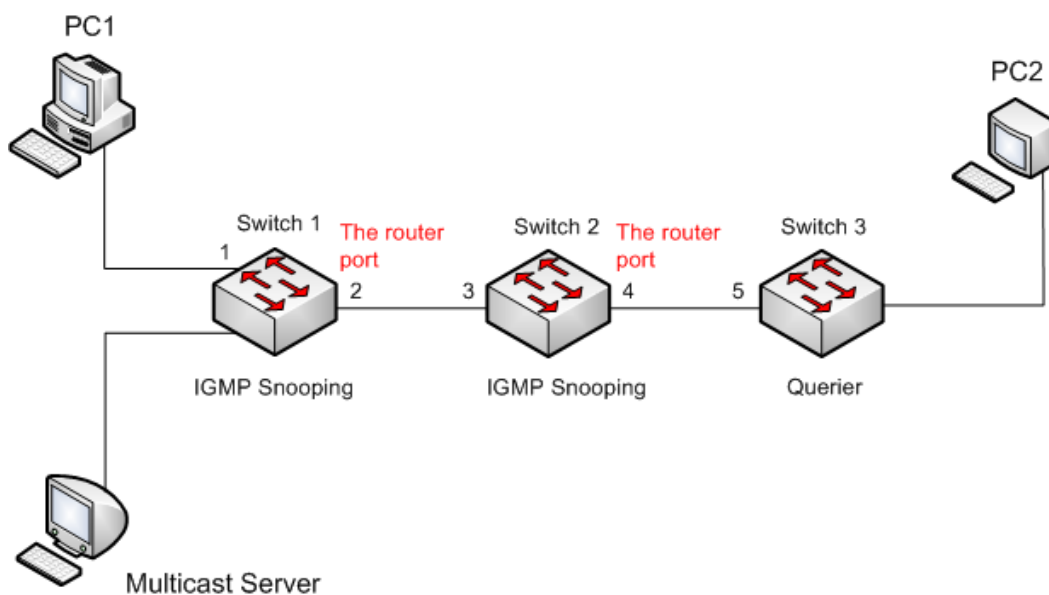
Figure 286 IGMP Snooping Application Example

➢ Because Switch 3 is elected as the querier, it periodically sends out a general query message.

➢ Port 4 of Switch 2 receives query message. It becomes router port. Meanwhile, Switch 2 forwards query message from port 3. Then port 2 of Switch 1 is elected to router port once it receives query message from Switch 2.

➢ When PC 1 joins in multicast group 225.1.1.1, it will send out IGMP report message, so port 1 and router port 2 of Switch 1 will also join in multicast group 225.1.1.1. Then, the IGMP report message will be forwarded to Switch 2 by router port 2, so port 3 and port 4 of Switch 2 will also join in 225.1.1.1, and then the IGMP report message will be forwarded to Switch 3 by router port 4, so port 5 of Switch 3 will join in 225.1.1.1 as well.

➢ When multicast server's multicast data reaches Switch 1, the data will be forwarded to PC1 by port 1; because router port 2 is also a multicast group member, so the multicast data will be forwarded by router port. In this way, when the data reaches port 5 of Switch 3, it will stop forwarding because there is no receiver any more, but if PC2 also joins in group 255.1.1.1, the multicast data will be forwarded to PC2.

6.18 GMRP

6.18.1 GARP Introduction

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

With GARP, the configuration information of a GARP member will spread 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. Leave messages fall into two types: LeaveEmpty and LeaveIn. A LeaveIn message is sent to cancel a registered attribute, while a LeaveEmpty message is sent to cancel an attribute that is not registered yet.

➢ 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 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 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, 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.

6.18.2 GMRP Protocol

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 spread 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, the GMRP-enabled port broadcasts the information to all the ports in the same VLAN.

6.18.3 Explanation

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 proxy 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.

6.18.4 Web Configuration

1. Enable the global GMRP protocol.

Click [Device Advanced Configuration] → [Multicast protocol configuration] → [GMRP configuration] → [GMRP configuration] to enter GMRP configuration page, as shown in Figure 287.
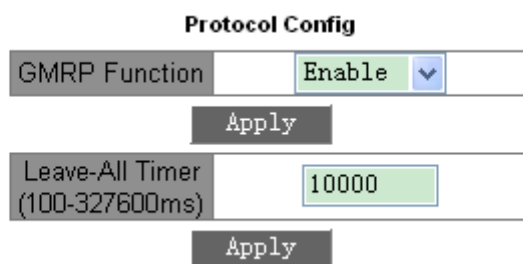
Figure 287 GMRP Global Configuration

GMRP function

Options: Enable/Disable

Default: Disable

Function: Enable/Disable the global GMRP function. The function cannot be used together with the IGMP Snooping function.

Leave-All timer

Range: 100ms~327600ms

Default: 10000ms

Function: The time interval for sending LeaveAll packets. The value must be a multiple of 100.

Explanation: if different devices' LeaveAll timers expire at the same time, they will send multiple LeaveAll messages at the same time, which increases message quantity. In order to

avoid the expiration of LeaveAll timers of different devices at the same time, the actual

running time of LeaveAll timer is a random value that is longer than the time of one LeaveAll

timer, and less than 1.5 times of LeaveAll timer.

2. Configure GMPR function on port, as shown in Figure 288.

Port Config

Port name	GMRP Function	GMRP Agent Function	Hold Timer (100-327600ms)	Join Timer (100-327600ms)	Leave Timer (100-327600ms)
1/1	Enable	Enable	100	500	3000

Apply

Figure 288 Port GMRP Configuration

Port name

Options: all switch ports

GMRP Function

Options: Enable/Disable

Default: Disable

Function: Enable GMRP function on port or not

GMRP Agent Function

Options: Enable/Disable

Default: Disable

Function: Enable GMRP agent function on port or not

Caution:

➢ Agent port cannot propagate agent entry.

➢ The premise of enabling GMRP agent function on port is to enable GMRP function on port.

Hold Timer

Range: 100ms~327600ms

Default: 100ms

Description: This value must be a multiple of 100. It is better to set same time of Hold timers

on all GMRP-enabled ports

Join Timer

Range: 100ms~327600ms

Default: 500ms

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

Leave Timer

Range: 100ms~327600ms

Default: 3000ms

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

3. Add a GMRP agent entry.

Click [Device Advanced Configuration] → [Multicast protocol configuration] → [GMRP configuration] → [GMRP agent configuration] to enter GMRP agent configuration page, as shown in Figure 289.


Figure 289 GMRP Agent Entry Configuration

Operation

Options: Add/Del

Default: Add

Function: Add or delete the entry.

Port name

Options: all configured agent ports

MAC address

Format: HH-HH-HH-HH-HH-HH (H is a hexadecimal number)

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

VLAN

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.

4. View GMRP agent entry.

Click [Device Advanced Configuration] → [Multicast protocol configuration] → [GMRP configuration] → [Show GMRP agent configuration] to show GMRP agent entries, as shown in Figure 290.

```
                          Information Display
Index    MAC-Address              VLAN    Port(s)
-------  -----------------------  ------  --------------
1        01-00-00-00-00-02        1       Ethernet1/1
2        01-00-00-00-00-03        1       Ethernet1/1
```

Figure 290 GMRP Agent Entry

5. The multicast members of this agent entry on the connected neighbor device are displayed, as shown in Figure 291.

It should meet following conditions:

➢   GMRP function is enabled on the inter-connected devices.

➢   The two ports that connect the devices must be propagation ports, and the propagation port in local device must be in VLAN ID of agent entry.

GMRP Dynamic Multicast List

Index	Multicast MAC	VLAN ID	Member Port
1	01-00-00-00-00-03	1	FE15
2	01-00-00-00-00-02	1	FE15

Figure 291 GMRP Dynamic Multicast Table

GMRP dynamic multicast

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

Function: View GMRP dynamic multicast entries.

6.18.5 Typical Configuration Example

As shown in Figure 292, Switch A and Switch B are connected by 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.
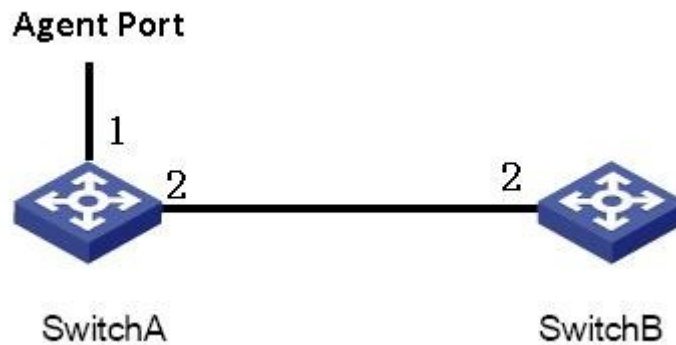
Figure 292 GMRP Networking

Configuration on Switch A:

1. Enable global GMRP function in switch A; set LeaveAll timer to the default value, as shown in Figure 287.

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 288.

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 289.

Configuration on Switch B:

4. Enable global GMRP function in switch B; set LeaveAll timer to the default value, as shown in Figure 287.

5. Enable GMPR function in port 2; set the timers to default values, as shown in Figure 288.

Table 12 lists the dynamically learned GMRP multicast entries in Switch B.

Table 12 Dynamic Multicast Entries

Attribute of Port 2 on Switch A	Attribute of Port 2 on Switch B	Multicast Entries Received on Switch B
Access VID=1	Access VID=1	MAC: 01-00-00-00-00-01 VLAN ID: 1

		Member port: 2
Access VID=2	Access VID= 2	MAC: 01-00-00-00-00-02 VLAN ID: 2 Member port: 2
Access VID= 1	Access VID= 2	MAC: 01-00-00-00-00-01 VLAN ID: 2 Member port: 2

6.19 Unregistered Multicast Action Configuration

6.19.1 Introduction

Unregistered multicast packets refer to the multicast packets without corresponding forwarding entries on the switch. When receiving an unregistered multicast packet, the switch broadcasts the packet within the VLAN (all ports except the inlet port). This will occupy large network bandwidth, affecting the forwarding rate. In this case, the function of discarding unregistered multicast packets can be enabled. If this function is enabled, after receiving an unregistered multicast packet, the switch discards it rather than forwards it.

6.19.2 Web Configuration

1. Configure unregistered multicast action

Click [Device Advanced Configuration] → [Multicast protocol configuration] → [Unregistered multicast action configuration] to enter unregistered multicast action configuration page, as shown in Figure 293.
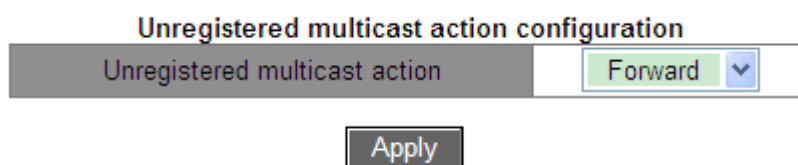
Unregistered multicast action configuration

Unregistered multicast action	Forward ∨

Apply

Figure 293 Unregistered Multicast Action Configuration

Unregistered multicast action

Options: Forward/Discard

Default: Forward

Function: Configure unregistered multicast action.

2. Configure multicast stream monitor port, as shown in Figure 294.

Configure Multicast Stream Monitor Port

Port	1/1
Multicast Stream Monitor Port State	Enable

Apply   Cancel

Figure 294 Multicast Stream Monitor Port Configuration

Multicast Stream Monitor Port

Options: Disable/Enable

Default: Disable

Function: Configure multicast stream monitor port. This monitor port forwards the multicast service streams (including the registered multicast service stream and unregistered multicast service stream) received by other ports within the same VLAN. This function is mainly used for multicast monitoring.

> **Note:**
> ➢ When the unregistered multicast action is configured as discard, the multicast stream monitor port cannot be configured.
> ➢ If a multicast monitor port is available, the unregistered multicast stream is forwarded to only the multicast monitor port. If no multicast monitor port is available, the unregistered multicast stream is forwarded to all ports in the VLAN.
> ➢ The multicast monitor port does not have the capability of the multicast protocol; therefore, it cannot be configured as a multicast member port.

6.20 Static Multicast Configuration

6.20.1 Introduction

Multicast address table can be statically configured. An entry is added into the multicast

address table in the form of {VLAN ID, Multicast MAC address, Multicast member port}, and a multicast message will be forwarded to the corresponding member port according to the entry

6.20.2 Web Configuration

1. Add a static multicast entry

Click [Device Advanced Configuration] → [Multicast protocol configuration] → [Static Multicast Configuration] to enter static multicast configuration page, as shown in Figure 295.

Static Multicast Configuration

VLAN	1
MAC Address (HH-HH-HH-HH-HH-HH)	01-01-01-01-01-01
Port	☑ 1/1 ☑ 1/2 ☑ 1/3 ☐ 1/4 ☐ 1/5 ☐ 1/6 ☐ 1/7 ☐ 1/8 ☐ 1/9 ☐ 1/10 ☐ 1/11 ☐ 1/12

Add   Delete

Figure 295 Add Static Multicast Address Entry

VLAN

Options: All existing VLAN IDs

Function: set the VLAN ID of the static multicast entry. Only VLAN member ports can forward this multicast message.

MAC Address

Format: HH-HH-HH-HH-HH-HH (H is a hexadecimal number)

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

Port

Function: choose the member ports of the multicast address. If a host connected to a port would like to receive a certain multicast group data, statically add this port into the multicast group and become a static member port.

Click <Add> button to add the static multicast entry; click <Delete> button to delete the static multicast entry.

2. View static multicast entries, as shown in Figure 296.

VLAN	MAC Address	Port
2	03-01-01-01-01-01	1/1 1/4
1	01-01-01-01-01-01	1/1 1/2 1/3
1	01-00-00-00-00-01	1/1 1/2

Figure 296 View Static Multicast Entries

6.21 LLDP

6.21.1 Introduction

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

6.21.2 Web Configuration

1. Enable LLDP.

Click [Device Advanced Configuration] → [LLDP configuration] → [LLDP configuration] to enter LLDP configuration page, as shown in Figure 297.

LLDP configuration	Enable ▼

Apply

Figure 297 Enabling LLDP

LLDP configuration

Options: Enable/Disable

Default: Disable

Function: Enable LLDP.

2. Enable TLV management address function, as shown in Figure 298.
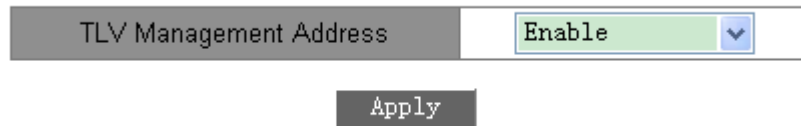
Figure 298 Enabling TLV Management Address

TLV Management Address

Options: Enable/Disable

Default: Disable

Function: Send the interface IP address (that is, the primary IP address of the first VLAN interface where this port resides) to the connected device when this function is disabled. If no IP address is configured for the VLAN interface where this port resides, the interface IP address is 127.0.0.1. Send the interface IP address and all IP addresses that have been configured for the current device to the connected device when this function is enabled. A maximum of 64 TLV management addresses can be sent out.

> ⚠ **Caution:**
> **CAUTION**
> When TLV management address function is enabled on the local device and the connecting neighbor device can analyze the TLV function, it can correctly display all configured IP addresses of the local switch.

3. View LLDP information.

Click [Device Advanced Configuration] → [LLDP configuration] → [Show lldp] to display LLDP information, as shown in Figure 299~Figure 302.

Figure 299 LLDP Information-1 When TLV Management Address Is Enabled

The preceding figure shows the condition that no IP address is configured for the first VLAN

interface where port 3/4 resides.

```
                            Information Display
 Local Port                    : Port_1/2
 Remote Port                   : Port_1/4
 Remote IP                     : 192.168.1.225
                                 192.168.0.225
                                 192.168.2.225
 Remote MAC                    : 00:1E:CD:14:26:F0
 Remote System Name            : Aquam8512
 Remote System Description     : SWITCH
```

Figure 300 LLDP Information-2 When TLV Management Address Is Enabled

The preceding figure shows the condition that the primary IP address of the first VLAN interface where port 3/4 resides is 192.168.1.225.

When the TLV management address is enabled, the LLDP display information includes the connected local port on the switch and the remote port on the neighbor device, interface IP address, all IP addresses configured, MAC address, and system information of the neighbor device.

```
                            Information Display
 Local Port                    : Port_1/2
 Remote Port                   : Port_1/4
 Remote IP                     : 127.0.0.1
 Remote MAC                    : 00:1E:CD:14:26:F0
 Remote System Name            : Aquam8512
 Remote System Description     : SWITCH
```

Figure 301 LLDP Information-1 When TLV Management Address Is Disabled

The preceding figure shows the condition that no IP address is configured for the first VLAN interface where port 3/4 resides.

```
                            Information Display
 Local Port                    : Port_1/2
 Remote Port                   : Port_1/4
 Remote IP                     : 192.168.1.225
 Remote MAC                    : 00:1E:CD:14:26:F0
 Remote System Name            : Aquam8512
 Remote System Description     : SWITCH
```

Figure 302 LLDP Information-2 When TLV Management Address Is Disabled

The preceding figure shows the condition that the primary IP address of the first VLAN interface where port 3/4 resides is 192.168.1.225.

When the TLV management address is disabled, the LLDP display information includes the

connected local port on the switch and the remote port on the neighbor device, interface IP address, MAC address, and system information of the neighbor device.

Caution:

The precondition for displaying LLDP information is that the LLDP-enabled devices are connected to each other.

6.22 VRRP

Note:

Routers in this chapter refer to Layer-3 switches.

6.22.1 Introduction

Virtual Router Redundancy Protocol (VRRP) adds multiple routers that can act as network gateways to a VRRP group, which forms a virtual router. Routers in the VRRP group elect a master through the VRRP election mechanism and the other routers in the group become backups. When the master fails, the backups elect a new master to undertake the responsibility of the failed master. This ensures uninterrupted data communication without configuration changes.
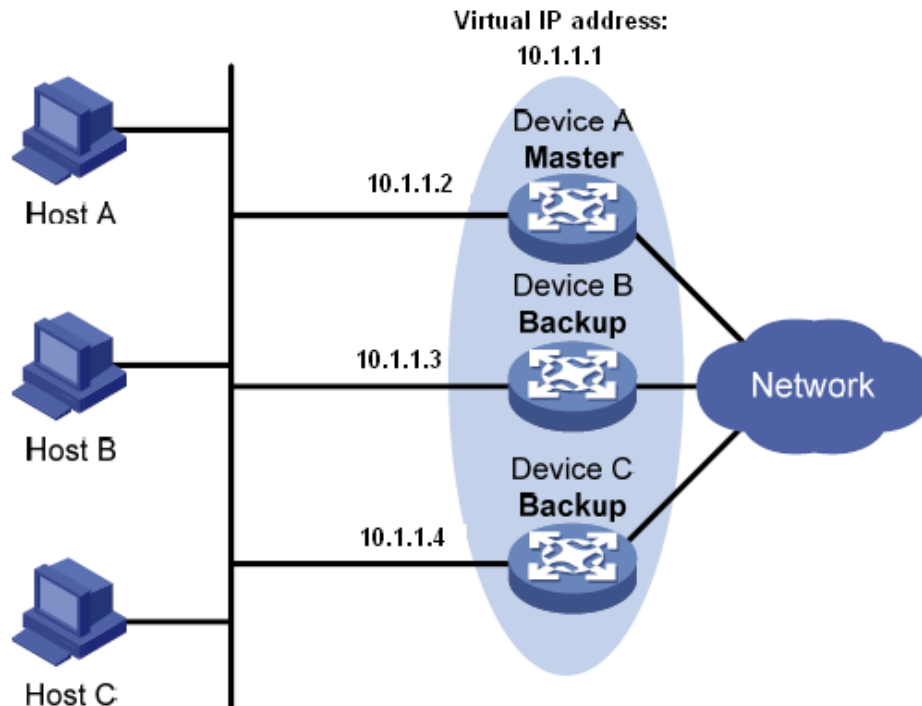
Figure 303 VRRP

As shown in Figure 303, Device A, Device B, and Device C form a virtual router with an IP address. Hosts can communicate with external networks through the virtual router only if the IP address of the virtual router is configured as the next hop of the default route on the hosts. A virtual router consists of one master and multiple backup switches. The master acts as the gateway. When it fails, one the backup routers will undertake the responsibility of the failed master to act as the gateway.

> **Caution:**
> ➢ The IP address of the virtual router can be either an unused IP address on the segment where the VRRP group resides or the IP address of an interface on a router in the VRRP group.
> ➢ The router whose interface IP address is identical with that of the virtual router is the IP address owner.
> ➢ Each VRRP group contains only one IP address owner.

6.22.2 Master Election

VRRP selects the master by election.

1. A router with the highest priority in a VRRP group is elected to be the master. The master periodically sends VRRP advertisements to inform the other routers in the VRRP group that it operates properly.

	Note:
	VRRP priority is in the range of 0 to 255. The greater the number, the higher the priority. Priorities 1 to 254 are configurable. Priority 0 is reserved for special uses and priority 255 for the IP address owner.

2. Backup routers obtain the priorities of other routers in the group by exchanging VRRP packets.

➢ If the priority of the master in the advertisement is higher than its own priority, the router stays as the backup.

➢ If the priority of the master in the advertisement is lower than the router's own priority, the router takes over the master in preemptive mode and stays as the backup in non-preemptive mode.

➢ If receiving no VRRP advertisements within a certain period, the router considers that the master fails, and sends VRRP advertisements to start a new master election.

	Note:
	➢ Non-preemptive mode: When a router in the VRRP group becomes the master, it stays as the master as long as it operates normally, even if a backup is assigned a higher priority later.
	➢ Preemptive mode: When a backup finds its priority higher than that of the master, the backup sends VRRP advertisements to start a new master election in the VRRP group.

6.22.3 Monitoring a Specified Interface

If the uplink interface of a router in a VRRP group fails, usually the VRRP group cannot be

aware of the uplink interface failure. If the router is the master, hosts on the LAN are not able to access external networks. This problem can be solved by monitoring a specified uplink interface. If the uplink interface fails, the priority of the master is automatically decreased by a specified value and a higher-priority router in the VRRP group becomes the master.

6.22.4 Web Configuration

1. Create/Delete a VRRP group.

Click [Device Advanced Configuration] → [VRRP Configuration] → [Create/Remove VRRP] to enter the VRRP group configuration page, as shown in Figure 304.

Figure 304 Creating a VRRP Group

Virtual Router Identifier

Range: 1~255

Function: Set the ID of the VRRP group.

Note: This series switches support a maximum of 10 VRRP groups.

2. Set the IP address of the virtual router.

Click [Device Advanced Configuration] → [VRRP Configuration] → [VRRP Initialization] to enter the VRRP initialization page, as shown in Figure 305.

Figure 305 Setting the IP Address of the Virtual Router

Set Virtual IP

Format: A.B.C.D

Function: Set the IP address of the virtual router.

Note: The IP address of the virtual router must be on the same network segment with the interface IP address.

Set virtual router type

Options: Master/Backup

Description: Master indicates that the current device is the IP address owner of the virtual router. Backup indicates that the current device is not the IP address owner of the virtual router.

3. Configure the Layer-3 interface for VRRP, as shown in Figure 306.

Figure 306 Configuring the Layer-3 Interface for VRRP

Function: Configure the Layer-3 interface for the specified VRRP group.

4. Configure the working mode of the VRRP group.

Click [Device Advanced Configuration] → [VRRP Configuration] → [Set preempt mode] to enter the VRRP working mode configuration page, as shown in Figure 307.

Figure 307 Configuring the Working Mode of the VRRP Group

Set router priority

Range: 1~254

Default: 100 (for non-IP address owner)

Function: Set the priority of the router in the VRRP group.

Set preempt mode

Options: true/false

Default: true

Function: Set the working mode of the virtual router.

Description: True indicates the preemptive mode, and false indicates the non-preemptive mode.

5. Set the advertisement interval.

Click [Device Advanced Configuration] → [VRRP Configuration] → [Set advertisement interval and monitor interface] to enter the configuration page, as shown in Figure 308.

Set advertisement interval

| Virtual Router Identifier | 1 |
| Set advertisement interval (1~50, default 5) Unit:200ms | 5 |

Apply   Default

Figure 308 Setting the Advertisement Interval

Set advertisement interval

Range: 1~50 (Unit: 200ms)

Default: 5×200ms

Function: Set the interval for the master router to send VRRP advertisements.

6. Configure the monitored interface, as shown in Figure 309.

Set monitor interface

Virtual Router Identifier	1
Monitor interface	Vlan1
Priority decrement	30

Apply   Default

Figure 309 Configuring the Monitored Interface

Monitor Interface

Function: Select the VLAN interface to be monitored.

Priority decrement

Range: 1~253

Function: Set the value of the priority decrement.

	Caution:
⚠ CAUTION	➢ The IP address owner of the virtual router cannot be configured as the monitored interface.
	➢ The priority of the master router after decrement must be smaller than that of a backup router.

7. Set VRRP authentication parameters.

Click [Device Advanced Configuration] → [VRRP Configuration] → [VRRP Authentication] to enter the VRRP authentication configuration page, as shown in Figure 310.

Figure 310 Setting VRRP Authentication Parameters

Authentication text mode

Function: Enable the interface that requires simple authentication. The router sending a VRRP packet adds the authentication key to the packet. The router receiving the packet compares the authentication key in the packet with the local authentication key. If the two authentication keys are identical, the packet is considered legitimate and true. Otherwise, the packet is illegitimate.

Authentication string

Range: 1~8 characters

Function: Configure the authentication string.

8. Enable a VRRP group.

Click [Device Advanced Configuration] → [VRRP Configuration] → [VRRP Initialization] to

enter the VRRP initialization page, as shown in Figure 311.

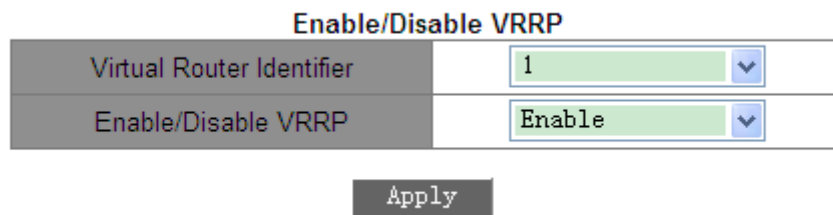Figure 311 Enabling VRRP

Function: Enable the VRRP group function.

6.22.5 Typical Configuration Example

As shown in Figure 312, Switch A and Switch B form a virtual router with IP address

192.168.2.4. Host A can communicate with Host B through the virtual router. When Switch A

operates properly, it is the master in the VRRP group. When Switch A or VLAN 3 fails, Switch
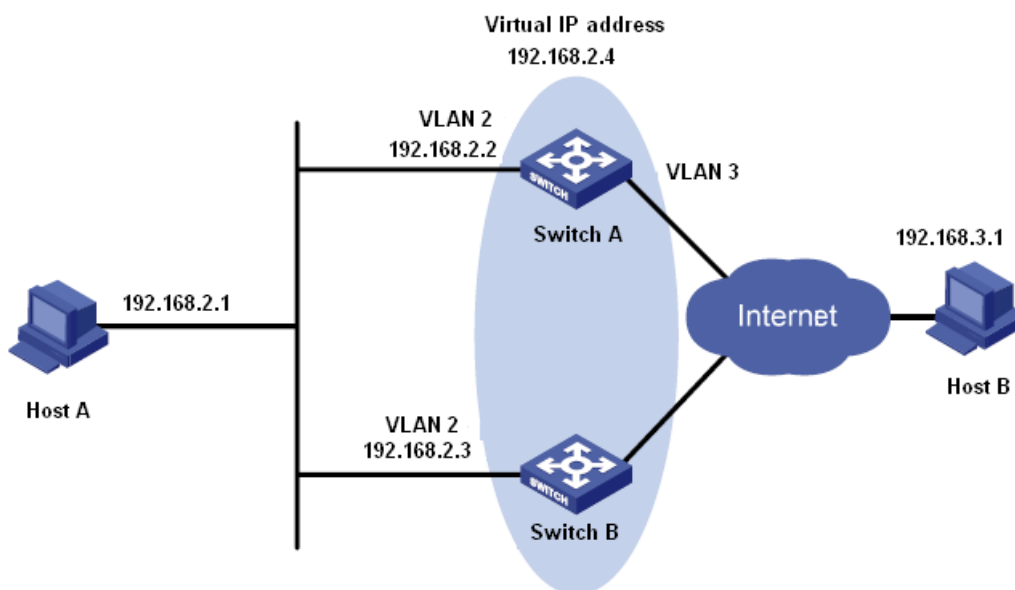
B becomes the master.

Figure 312 VRRP Typical Configuration Example

Configuration on Switch A:

1. Set the IP address of VLAN 2 to 192.168.2.2, and subnet mask to 255.255.255.0.

2. Create VRRP group 1, as shown in Figure 304.

3. Set the virtual IP address of VRRP group 1 to 192.168.2.4, and router type to Master, as shown in Figure 305.

4. Configure VLAN 2 as the Layer-3 interface for VRRP group 1, as shown in Figure 306.

5. Set the priority of Switch A in the VRRP group to 110, and preemptive mode to false, as shown in Figure 307.

6. Configure VLAN 3 as the monitored interface and set the priority decrement to 30, as shown in Figure 309.

7. Enable VRRP group 1, as shown in Figure 311.

Configuration on Switch B:

1. Set the IP address of VLAN 2 to 192.168.2.3, and subnet mask to 255.255.255.0.

2. Create VRRP group 1, as shown in Figure 304.

3. Set the virtual IP address of VRRP group 1 to 192.168.2.4, and router type to Backup, as shown in Figure 305.

4. Configure VLAN 2 as the Layer-3 interface for VRRP group 1, as shown in Figure 306.

5. Set the priority of Switch B in the VRRP group to 100, and preemptive mode to false, as shown in Figure 307.

6. Enable VRRP group 1, as shown in Figure 311.

6.23 SNTP Configuration

6.23.1 Introduction

The Simple Network Time Protocol (SNTP) synchronizes time between server and client by means of requests and responses. As a client, the switch synchronizes time from the server according to packets of the server. Multiple SNTP servers can be configured for one switch, but only one can be active at a time.

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

> **Caution:**
>
> ➢ 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.

6.23.2 Web Configuration

1. Enable SNTP protocol.

Click [Device Advanced Configuration] → [SNTP configuration] → [SNTP server configuration] to enter the SNTP configuration page, as shown in Figure 313.
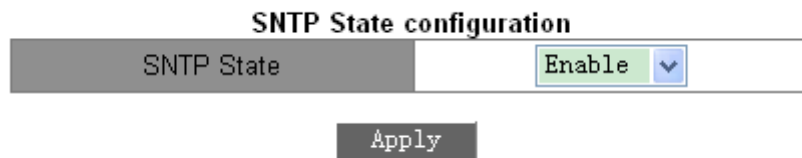
Figure 313 Enabling SNTP

SNTP State

Options: Enable/Disable

Default: Disable

Function: Enable/Disable SNTP.

> **Caution:**
>
> SNTP and NTP protocols are mutually exclusive. Because NTP and SNTP use the same UDP port number, they cannot be used at the same time.

---

2. Configure SNTP Server, as shown in Figure 314.

SNTP server and version configuration

Server address	192.168.0.23
Version(1-4)	1

Add   Del

Figure 314 SNTP Server Configuration

Server address

Format: A.B.C.D

Function: Configure the IP address of the SNTP server. Clients will synchronize time according to server packets.

Version

Options: 1~4

Function: Configure the version of SNTP.

⚠ CAUTION	**Caution:**
	There is no limit on the number of SNTP Servers, but to guarantee proper operation, no more than 5 servers are recommended in application.

3. Configure the time interval for sending synchronization requests, as shown in Figure 315.

Request interval from SNTP client to NTP/SNTP server

Interval(16-16284 second)	20

Apply   Default

Figure 315 Setting the Time Interval for Sending Synchronization Requests

Interval

Options: 16~16284s

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

4. Check whether the clock is synchronized from the server.

Click [Device Basic Configuration] → [Switch Basic Configuration] → [clock config] to enter the clock information page, as shown in Figure 316.

Figure 316 Synchronization Clock

Click <Show Clock>. The Information Display page displays the clock information after the synchronization from SNTP server.

5. View SNTP configuration information.

Click [Device Advanced Configuration] → [SNTP configuration] → [SNTP information] to view the SNTP configuration, as shown in Figure 317.

Figure 317 SNTP Configuration Page

Last receive displays the interval from the last synchronization time to the current time.

6.24 NTP Configuration

6.24.1 Introduction

The Network Time Protocol (NTP) synchronizes time between distributed servers and clients. NTP synchronizes the clocks of all network devices, ensuring time consistency among all devices. This enables devices to provide multiple applications based on the same time. NTP-enabled local system cannot only synchronize its clock from other clock sources, but also serve as the clock source for other devices.

As shown in Figure 318, the round-trip delay "(T4-T1)-(T3-T2)" and clock offset "((T2-T1) + (T3-T4))/2" can be calculated based on the exchange of NTP packets, thereby achieving high-precision clock synchronization among devices.
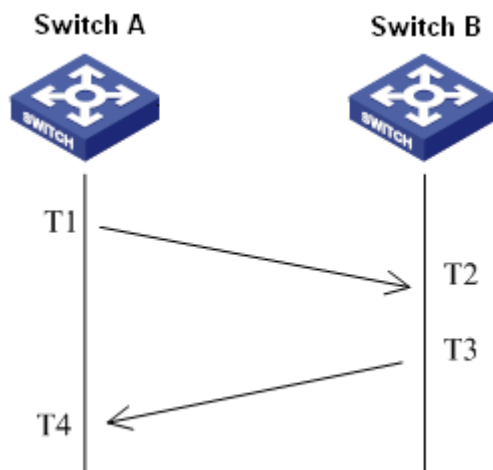
Figure 318 NTP

6.24.2 NTP Working Modes

NTP can adopt the following working modes for time synchronization. You can select the appropriate working mode as required.

Client/Server mode: In this mode, the client sends clock synchronization packets (client mode) to the server. After receiving the packets, the server automatically works in server mode and sends response packets (server mode). After receiving response packets, the client synchronizes from the optimal server clock.

Peer mode: In this mode, the active peer sends clock synchronization packets (active peer mode) to the passive peer. After receiving the packets, the passive peer automatically works in passive peer mode and sends response packets (passive peer mode). Based on the exchange of packets, the devices set up the peer mode. The active peer and passive peer can synchronize time from each other. If both peers have synchronized time from other devices, the peer with greater clock stratum synchronizes time from the peer with smaller clock stratum.

Broadcast mode: In this mode, the broadcast server periodically broadcasts clock

synchronization packets (broadcast mode). After receiving the packets, the broadcast client sends clock synchronization packets (client mode) to the server. After receiving the request packets, the server sends response packets (server mode). The server and the client accomplish clock synchronization by exchanging eight request and response packets.

Multicast mode: The multicast client periodically sends multicast synchronization request packets (client mode) to the multicast server. After receiving the packets, the server sends unicast response packets (server mode). Then the server and the client accomplish clock synchronization by exchanging unicast clock synchronization request and response packets.

6.24.3 Web Configuration

1. Enabling NRP.

Click [Device Advanced Configuration] → [NTP configuration] → [NTP Global Configuration] to enter the NTP global configuration page, as shown in Figure 319.
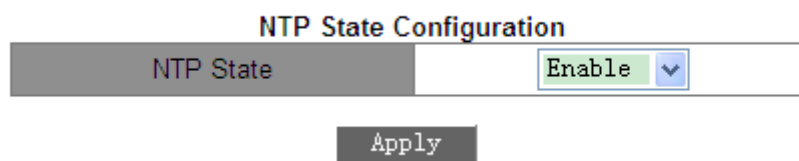
Figure 319 Enabling NTP

NTP State

Options: Enable/Disable

Default: Disable

Function: Enable or disable the global NTP service function.

⚠ CAUTION	**Caution:**
	➢ NTP and SNTP cannot be used simultaneously, because they use the same UDP port number.
	➢ You can also configure the NTP service and save the configuration when the NTP service is disabled. Whether the NTP service is enabled does not affect the configuration of the NTP service.

2. Configure NTP unicast, as shown in Figure 320.

NTP Unicast Configuration

NTP State	Server Mode ⌄
IP address	192.168.0.4
Min-Poll (interval<4,16>,in log2 unit seconds)	4
Max-Poll (interval<5,17>,in log2 unit seconds)	10
Packet Source Interface	Vlan1 ⌄

Apply   Delete

Figure 320 Configuring NTP Unicast

NTP State

Options: Server Mode/Peer Mode

Function: Select the NTP working mode.

Description: Server mode indicates that the NTP working mode is client/server mode; peer mode indicates that the NTP working mode is peer mode.

IP address

Format: A.B.C.D

Description: When the client/server mode is adopted, the IP address is that of the NTP server. When the peer mode is adopted, the IP address is that of the passive peer.

Min-Poll

Range: 4 to 16. Interval=2^n s ("n" is the value of this parameter)

Default: 4. In this case, the interval is 16s (2^4).

Function: Configure the minimum request interval for the NTP packet exchange between the local device and the server.

Max-Poll

Range: 5 to 17. Interval=2^n s ("n" is the value of this parameter)

Default: 10. In this case, the interval is 1024s (2^{10}).

Function: Configure the maximum request interval for the NTP packet exchange between the local device and the server.

Packet source interface

Function: Specify the port for sending NTP packets.

Description: When the client/server mode is adopted, the local device sends NTP packets to the server. The source IP address in the packets is the primary IP address of the port.

When the peer mode is adopted, the local device sends NTP packets to the peer. The source IP address in the packets is the primary IP address of the port.

> **Caution:**
>
> ➢ If the client/server mode is adopted, you only need to perform the preceding configuration on the client.
>
> ➢ The configured NTP server clock must be synchronized before provide time synchronization for other devices.
>
> ➢ If the peer mode is adopted, you only need to perform the preceding configuration on the active peer.
>
> ➢ Min-Poll ≤ Max-Poll.
>
> ➢ The Min-Poll values of NTP peers must be the same.

---

3. Configure the NTP multicast server.

Click [Device Advanced Configuration] → [NTP configuration] → [Multicast Server Configuration] to enter the multicast server configuration page, as shown in Figure 321.

Muticast Server Configuration

Muticast IP Address	224.0.1.1
Enable Muticast Interface	Vlan1

Apply   Delete

Figure 321 Configuring a Multicast Server

Multicast IP Address

Format: A.B.C.D

Function: Configure the multicast IP address. If no specified multicast IP address is available, 224.0.1.1 is adopted by default.

Enable Multicast Interface

Function: Specify the multicast port.

4. Configure the NTP multicast client.

Click [Device Advanced Configuration] → [NTP configuration] → [Multicast Client Configuration] to enter the multicast client configuration page, as shown in Figure 322.

Figure 322 Configuring a Unicast Client

Multicast IP Address

Format: A.B.C.D

Function: Configure the IP address used in multicast mode. If no specified multicast IP address is available, 224.0.1.1 is adopted by default.

Enable Multicast Interface

Function: Specify the multicast port.

Min-Poll

Range: 4 to 16. Interval=2^n s ("n" is the value of this parameter)

Default: 4. In this case, the interval is 16s (2^4).

Function: Configure the minimum request interval for the NTP packet exchange between the local device and the server.

Max-Poll

Range: 5 to 17. Interval=2^n s ("n" is the value of this parameter)

Default: 10. In this case, the interval is 1024s (2^{10}).

Function: Configure the maximum request interval for the NTP packet exchange between the local device and the server.

Max-TTL

Range: 1~255

Default: 64

Function: Configure the maximum TTL for multicast requests sent by the multicast client.

5. Configure the NTP broadcast server.

Click [Device Advanced Configuration] → [NTP configuration] → [Broadcast Server Configuration] to enter the broadcast server configuration page, as shown in Figure 323.

Figure 323 Configuring a Broadcast Server

Enable Broadcast Interface

Function: Specify the broadcast port.

6. Configure the NTP broadcast client.

Click [Device Advanced Configuration] → [NTP configuration] → [Broadcast Client Configuration] to enter the broadcast client configuration page, as shown in Figure 324.
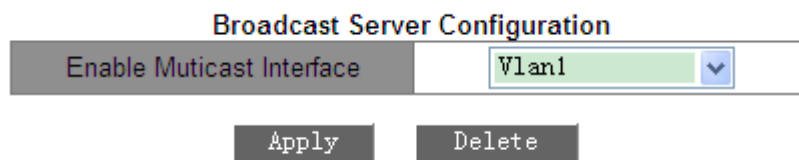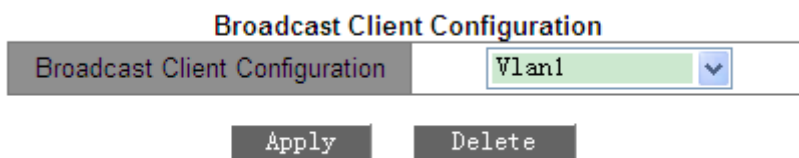

Figure 324 Configuring a Broadcast Client

Broadcast Client Configuration

Function: Specify the broadcast port.

7. Configure the reference clock.

Click [Device Advanced Configuration] → [NTP configuration] → [Reference Clock Configuration] to enter the reference clock configuration page, as shown in Figure 325.

Referance Clock Configuration	
Referance Clock IP Address	127.127.0.1
Referance Clock Level(1-15)	4

| Apply | Delete |

Figure 325 Configuring the Reference Clock

Reference Clock IP Address

Format: 127.127.t.u

Default: 127.127.0.1

Description: "t" in 127.127.0.1 indicates the reference clock type, while "u" indicates the instance ID. Only 127.127.0.1 is supported currently. That is, the system clock serves as the reference clock.

Reference Clock Level

Range: 1~15

Default: 4

Function: Configure the stratum of the reference clock.

Description: The clock stratum indicates the accuracy of a clock. The larger the number, the lower the accuracy. If the stratum is 16, the clock is not synchronized and thus cannot serve as the reference clock.

⚠ **Caution:**
CAUTION   Currently, only the switch itself can serve as the reference clock. Before configuring this item, you must confirm the time synchronization requirements of the system.

6.24.4 Typical Configuration Example

➢ Configuring the Peer Mode:

As shown in Figure 326, it is required to configure the local clock on Switch D as the

reference clock and set its stratum to 2. Switch A works in client mode and Switch D serves as the NTP server. Switch B works in peer mode and Switch A is its peer. Switch B is the active peer while Switch A is the passive peer.

Figure 326 Networking in Peer Mode

Configuration on Switch D:

1. Enable NTP, as shown in Figure 319.

2. Set the IP address of the reference clock to 127.127.0.1 and clock stratum to 2, as shown in Figure 325.

Configuration on Switch A:

3. Enable NTP, as shown in Figure 319.

4. Set the IP address of the NTP server to 192.5.5.8, Min-Poll to 4, Max-Poll to 10, and NTP Source to VLAN 1, as shown in Figure 320.

Configuration on Switch B:

5. Enable NTP, as shown in Figure 319.

6. Set the IP address of the NTP peer to 192.5.5.5, Min-Poll to 4, Max-Poll to 10, and NTP Source to VLAN 1, as shown in Figure 320.

➢ Configuring the Multicast Mode:

As shown in Figure 327, it is required to configure the local clock on Switch D as the reference clock and set the stratum to 2. Switch D works in multicast server mode. Multicast server mode is configured on VLAN 2 port. Switch A and Switch B work in multicast client mode. Multicast client mode is configured on VLAN 2.

Figure 327 Networking in Multicast Mode

Configuration on Switch D:

1. Enable NTP, as shown in Figure 319.

2. Set the IP address of the reference clock to 127.127.0.1 and clock stratum to 2, as shown in Figure 325.

3. Configure the multicast server: Set multicast IP address to 224.0.1.1 and port to VLAN 2, as shown in Figure 321.

Configurations on Switch A and Switch B:

4. Enable NTP, as shown in Figure 319.

5. Configure the multicast client: Set multicast IP address to 224.0.1.1, port to VLAN 2, Min-Poll to 4, Max-Poll to 10, and Max-TTL to 64, as shown in Figure 322.

➢ Configuring the Broadcast Mode:

As shown in Figure 328, it is required to configure the local clock on Switch D as the reference clock and set the stratum to 2. Switch D works in broadcast server mode. Broadcast server mode is configured on VLAN 2 port. Switch A and Switch B work in broadcast client mode. Broadcast client mode is configured on VLAN 2.
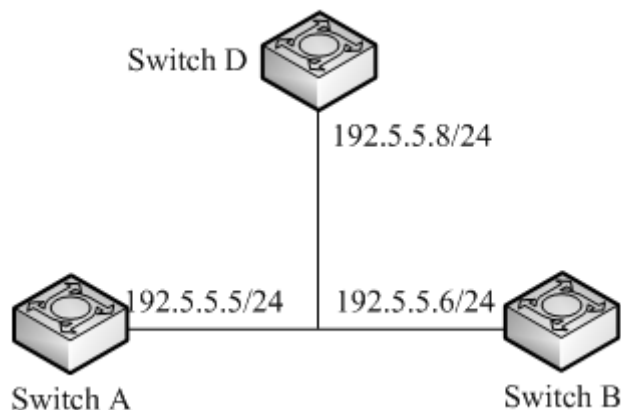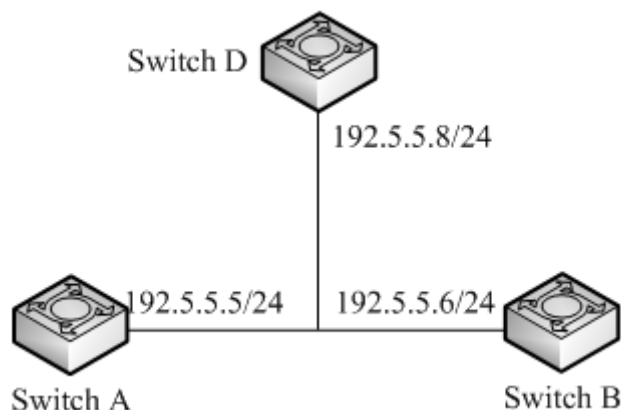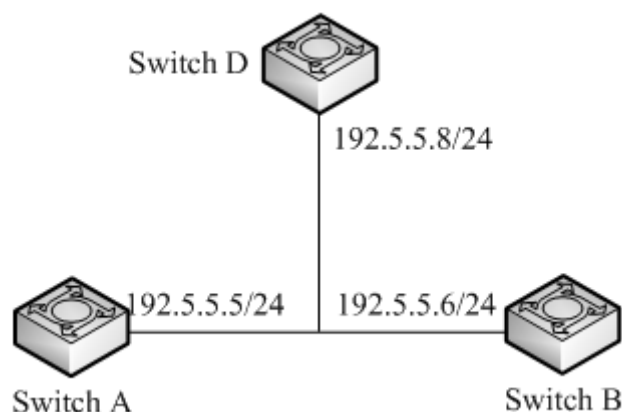
Figure 328 Networking in Broadcast Mode

Configuration on Switch D:

1. Enable NTP, as shown in Figure 319.

2. Set the IP address of the reference clock to 127.127.0.1 and clock stratum to 2, as shown in Figure 325.

3. Configure the broadcast server: Set broadcast port to VLAN 2, as shown in Figure 323.

Configurations on Switch A and Switch B:

4. Enable NTP, as shown in Figure 319.

5. Configure the broadcast client: Set broadcast port to VLAN 2, as shown in Figure 324.

6.25 TACACS+ Configuration

6.25.1 Introduction

Terminal Access Controller Access Control System (TACACS+) is a TCP-based application. It adopts the client/server mode to implement the communication between Network Access Server (NAS) and TACACS+ server. The client runs on the NAS and user information is managed centrally on the server. The NAS is the server for users but client for the server. Figure 329 shows the structure.
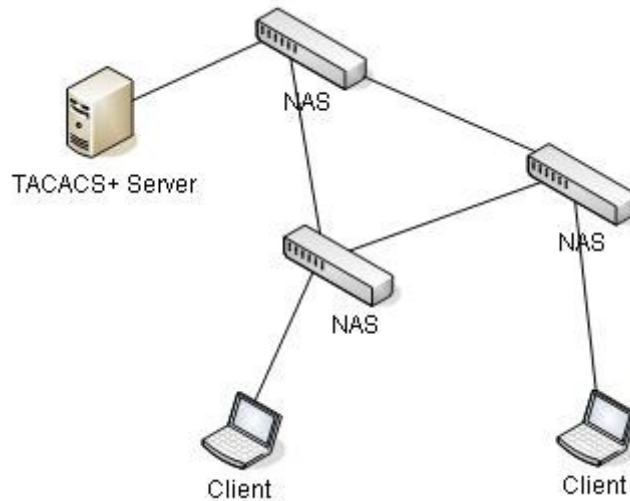
Figure 329 TACACS+ Structure

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

6.25.2 Web Configuration

1. Enable TACACS+.

Click [Device Advanced Configuration] → [TACACS-PLUS Configuration] → [TACACS-PLUS configuration] to enter the TACACS+ configuration page, as shown in Figure 330.

Figure 330 Enabling TACACS+

Tacacs-plus State

Options: Enable/Disable

Default: Disable

Function: Enable/Disable TACACS+.

2. Configure the TACACS+ server, as shown in Figure 331.

Server Configure				
Server	IP Address	TCP Port	Encrypt	Encrypt Key(1~32 ANSI characters)
Primary ⌄	192.168.0.23	45	Enable ⌄	aaa

Apply   Delete

Figure 331 TACACS+ Server Configuration

Server

Options: Primary/Secondary

Default: Primary

Function: Select the server type.

IP Address

Format: A.B.C.D

Function: Enter the server IP address.

TCP port

Range: 1~65535

Default: 49

Function: Set the number of ports that receive NAS authentication requests.

Encrypt

Options: Enable/Disable

Default: Disable

Function: Encrypt the packet or not. If it is enabled, the key is required.

Encrypt Key

Range: 1~32 characters

Description: Set the key to improve the communication security between client and TACACS+ server. The two parties share the key to verify the legitimacy of packets. Both parties can receive packets from each other only when the keys are the same. Therefore, make sure the configured key is the same as the key on the TACACS+ server.

After setting is completed, the following "Sever Configured" lists server configuration information, as shown in Figure 332.

Server Configured			
Primary Server	192.168.0.23	49	Encrypt
Secondary Server	192.168.0.32	45	Unencrypt

Figure 332 Server Configuration List

6.25.3 Typical Configuration Example

As shown in Figure 333, TACACS+ server can authenticate and authorize users by the switch. The server IP address is 192.168.0.23, and the shared key used when switch and server exchange packets is aaa.
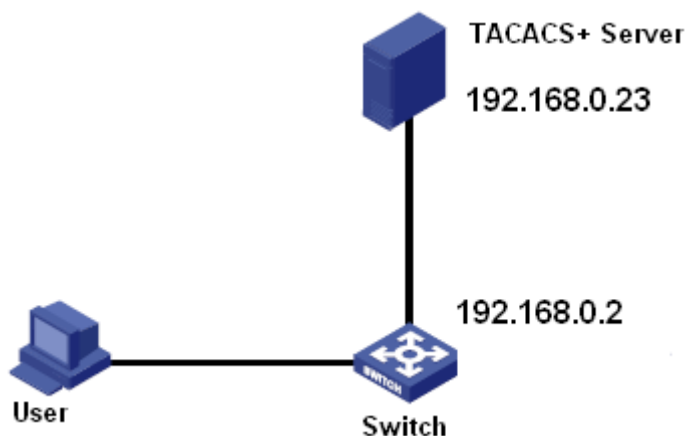
Figure 333 TACACS+ Authentication Example

1. Enable TACACS+, as shown in Figure 330.

2. TACACS+ server configuration. Set the server IP address to 192.168.0.23 and Encrypt key to aaa, and enable Encrypt, as shown in Figure 331.

3. When logging in to the switch through Web, select "Local", while logging in to the switch through telnet, select "Tacacs+", as shown in Figure 345.

4. Configure username and password "bbb"; encrypt key "aaa" on TACACS+ server.

5. When logging in to the switch through Web, input the username "admin" and password "123" to pass the local authentication.

6. When logging in to the switch through Telnet, input the username and password "bbb" to pass the TACACS+ authentication.

6.26 RADIUS Configuration

6.26.1 Introduction

RADIUS (Remote Authentication Dial-In User Service) is a distributed information exchange protocol. It defines UDP-based RADIUS frame format and information transmission mechanism, protecting networks from unauthorized access. RADIUS is usually used in networks that require high security and remote user access.

RADIUS adopts client/server mode to achieve communication between the NAS (Network Access Server) and the RADIUS server. The RADIUS client runs on the NAS. The RADIUS server provides centralized management for user information. The NAS is the server for users but client for the RADIUS server. Figure 334 shows the structure.
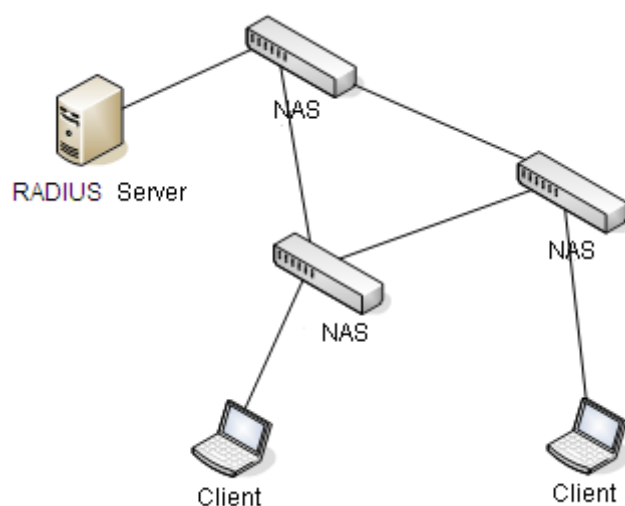
Figure 334 RADIUS Structure

The protocol authenticates terminal users that need to log in to the device for operation. Serving as the RADIUS client, the device sends user information to the RADIUS server for authentication and allows or disallows users to log in to the device according to authentication results.

6.26.2 Web Configuration

1. Configure RADIUS parameters

Click [Device Advanced Configuration] → [RADIUS configuration] → [RADIUS configuration]

to enter the RADIUS configuration page, as shown in Figure 335.

Protocol Configuration

Request Times	3
Timeout	3

Apply

Figure 335 RADIUS Parameter Configuration

Request Times

Range: 1~3

Default: 3

Function: Set the maximum retransmission attempts for RADIUS request packets. If the device still receives no response packets from the RADIUS server after maximum retransmission attempts, the device consider the authentication fails.

Timeout

Range: 1~3

Default: 3

Function: Set the overtime for response from the RADIUS server. After sending a RADIUS request packet, the device will retransmit a RADIUS request packet if it still receives no response from the RADIUS server after the specified time.

2. Configure RADIUS server, as shown in Figure 336.

Server Configuration

Server Type	Server IP	Port	Password
Authentication Primary Server ▾		1812	
Authentication Primary Server	192.168.0.23	1812	aaaa
Authentication Secondary Server	192.168.0.184	1812	bbbb

Apply   Remove

Figure 336 RADIUS Server Configuration

Server Type

Options: Authentication Primary Server/Authentication Secondary Server

Function: Configure the primary or secondary RADIUS server. If the primary server is unreachable, the will use the secondary server for authentication.

Server IP

Format: A.B.C.D

Function: Set the IP address of the RADIUS server.

Port

Range: 1~65535

Default: 1812

Function: Set UDP port of the RADIUS server.

Password

Range: 1~32 characters

Function: Configure the password of RADIUS server.

6.26.3 Typical Configuration Example

As shown in Figure 337, IEEE802.1x is enabled on port 1of the switch. Then users can log in to the switch through port 1 after passing the authentication on the RADIUS server. The IP address of the server is 192.168.0.23. The key for packet exchange between the switch and the server is aaaa.
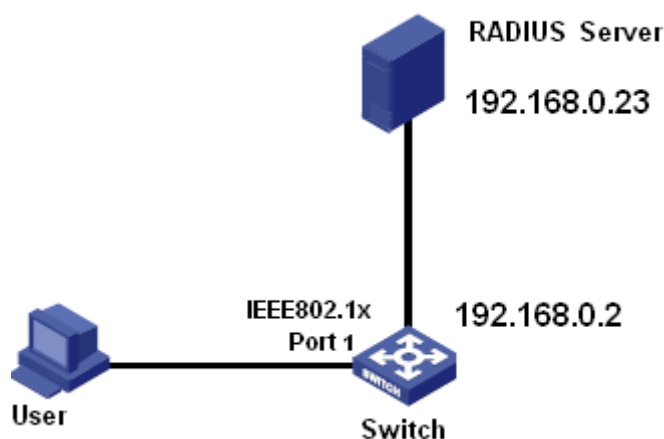

Figure 337 RADIUS Authentication Example

1. Set the IP address of the primary authentication server to 192.168.0.23 and password to aaaa, as shown in Figure 336.

2. IEEE802.1x settings: enable IEEE802.1x globally. Enable IEEE802.1x on port 1. Keep default settings for the other parameters. For details, see section "6.27 IEEE802.1x

Configuration".

3. Set dot1x to radius authentication, as shown in Figure 345.

4. Set both the user name and password on the RADIUS Server to ccc, encrypt key to aaaa.

5. Install and run 802.1x client software on a PC. Enter ccc for the user name and password.

Then the user can pass the authentication and access the switch through port 1.

6.27 IEEE802.1x Configuration

6.27.1 Introduction

To ensure WLAN security, IEEE802 LAN/WAN committee proposed the 802.1x protocol. As a common access control mechanism for LAN ports in Ethernet, 802.1x implements Ethernet authentication and security. 802.1x is a port-based network access control. Port-based network access control is to implement authentication and control on the ports of LAN access devices. If a user passes the authentication, it can access the resources in the LAN. If it cannot pass the authentication, it cannot access the resources in the LAN. 802.1x systems adopt the Client/Server structure. User authentication and authorization of port-based access control requires the following elements:

Client: usually indicates a user terminal. When a user wants to surf the Internet, it starts the client program and enters required user name and password. The client program will send a connection request.

Device: indicates the authentication switch in an Ethernet system. It uploads and delivers user authentication information, and enables or disables a port based on the authentication result.

Authentication server: indicates the entity that provides authentication service for devices. It checks whether users have the permissions to use network services according to the identifiers (user names and passwords) sent by clients, and enables or disables ports according to authentication results.

6.27.2 Web Configuration

1. Enable global IEEE802.1x protocol.

Click [Device Advanced Configuration] → [IEEE802.1x configuration] → [IEEE802.1x configuration] to enter the IEEE802.1x configuration page, as shown in Figure 338.

Figure 338 Enabling Global IEEE802.1x

IEEE802.1x State

Options: Enable/Disable

Default: Disable

Function: Enable/Disable global IEEE802.1x security function.

2. Configure the port on which IEEE802.1x is enabled, as shown in Figure 339.
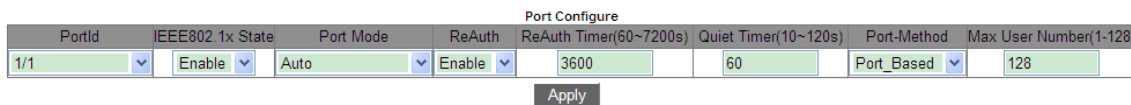
Figure 339 IEEE802.1x Port Configuration

PortId

Options: all switch ports

IEEE802.1x State

Options: Enable/Disable

Default: Disable

Function: Enable/Disable IEEE802.1x on port.

Description: When this function is enabled, users' communication through the port depends on IEEE802.1x port mode.

Port Mode

Options: Unauthorized-force/Auto/Authorized-force

Default: Auto

Function: Select the port authentication mode.

Description: **Unauthorized-force** means the port is always in unauthorized state and does not allow users to conduct authentication and the switch does not provide authentication services to clients that access the switch from this port. **Auto** means the initial state of port is unauthorized and the port does not allow users to access network resources. If a user passes authentication, the port will change to the authorized state and will allow users to access network resources. If a user fails to pass authentication, the port will change to the unauthorized state and will not allow users to access network resources. **Authorized-force** means port is always in an authorized state and allows users to access network resource without authentication.

ReAuth

Options: Enable/Disable

Default: Disable

Function: Configure whether regular re-authentication is required when authentication succeeds.

ReAuth Timer

Range: 60~7200s

Default: 3600s

Function: When authentication succeeds, set the time interval for re-authentication.

Quiet Timer

Range: 10~120s

Default: 60s

Function: If authentication fails, the silent period (QuietPeriod) starts. During the silent period, the server does not respond to authentication requests from the client. After the silent period ends, the server starts to accept authentication requests again.

Port-Method

Options: Port_ Based/ MAC_ Based

Default: Port_ Based

Function: Configure the access control mode of IEEE802.1x-enabled ports.

Description: MAC_Based indicates that users using the port need to be authenticated respectively. When a user is offline, only the user cannot use the network. Port_Based indicates that users are authenticated based on port. After the first user using the port passes authentication, all the other users using the port do not need to be authenticated. However, when the first user is offline, the port is disabled and all the other users using the port cannot use the network.

Max User Number

Range: 1~128

Default: 128

Function: Configure the maximum number of access users using the IEEE802.1x-enabled port.

Description: The configuration is only valid to ports with MAC-Based access control.

3. View IEEE802.1x configuration

Click [Device Advanced Configuration] → [IEEE802.1x configuration] → [IEEE802.1x information] to view the IEEE802.1x configuration, as shown in Figure 340.

```
                            Information Display

IEEE802.1X status        : enable
IEEE802.1X type          : chap
IEEE802.1X server-timeout : 100(s)

 interface  config   method      running  authentication mode  authentication result
 _____  _____  _____  _____  _____  _____
 1/1        enable   port-based  active   auto                 N/A
 1/2        disable  port-based  unactive auto                 N/A
 1/3        disable  port-based  unactive auto                 N/A
 1/4        disable  port-based  unactive auto                 N/A
 1/5        disable  port-based  unactive auto                 N/A
 1/6        disable  port-based  unactive auto                 N/A
 1/7        disable  port-based  unactive auto                 N/A
 1/8        disable  port-based  unactive auto                 N/A
 1/9        disable  port-based  unactive auto                 N/A
 1/10       disable  port-based  unactive auto                 N/A
 1/11       disable  port-based  unactive auto                 N/A
 1/12       disable  port-based  unactive auto                 N/A


******************** 1/1 ********************
IEEE802.1X config status          : enable
IEEE802.1X running status         : active
IEEE802.1X port method is         : port-based
IEEE802.1X port mode              : auto
IEEE802.1X authentication result  : N/A
IEEE802.1X reauthentication status : enable
IEEE802.1X reauthentication period : 3600(s)
IEEE802.1X quiet period           : 60(s)
IEEE802.1X max user number        : 128
```

Figure 340 View IEEE802.1x Configuration

4. Configure IEEE802.1x group

Click [Device Advanced Configuration] → [IEEE802.1x configuration] → [IEEE802.1x Group configuration] to enter IEEE802.1x group configuration page, as shown in Figure 341.

Group Configuration

All	Group Name	MAC (HH-HH-HH-HH-HH-HH)	All	Port
				☐ 1/1 ☐ 1/2 ☐ 1/3 ☐ 1/4 ☐ 1/5 ☐ 1/6 ☐ 1/7 ☐ 1/8 ☐ 1/9 ☐ 1/10 ☐ 1/11 ☐ 1/12
☐	111	00-00-11-22-33-44		1/1 1/2
☐	222	00-00-00-00-00-01,00-00-00-00-00-10		
☐	333			1/1 1/3

Apply   Edit   Delete

Figure 341 IEEE802.1x Group Configuration

Group Name

Range: 1~16 characters

Function: Configure group name.

MAC

Format: HH-HH-HH-HH-HH-HH (H is a hexadecimal number)

Function: Configure the MAC address for the group. Multiple MAC addresses can be added to one group, and MAC addresses are separated by single-byte commas.

Port

Function: Add ports for the group.

> **Note:**
> The user authentication group allows configuration of only the MAC address or port number.

5. Configure IEEE802.1x user information

Click [Device Advanced Configuration] → [IEEE802.1x configuration] → [IEEE802.1x User configuration] to enter IEEE802.1x user configuration page, as shown in Figure 342.

User Configuration

All	User name	Password	Group (Optional)
☐	ccc	******	
☐	aaa	******	111

Apply   Edit   Delete

Figure 342 IEEE802.1x User Configuration

User Name

Range: 1~16 characters

Function: Configure IEEE802.1x user name.

Password

Range: 1~16 characters

Function: Configure IEEE802.1x password.

Group

Function: Bind the user to a group.

Description: If the current user is bound to a user authentication group, only the user whose

MAC address and access port number both match the bound group can pass the

authentication and access the switch. It is also allowed that the current user is not bound to

any user authentication group. In this case, users can conduct authentication by using any

MAC address and port number.

6. View IEEE802.1x on-line user information

Click [Device Advanced Configuration] → [IEEE802.1x configuration] → [IEEE802.1x

On-line user] to view the IEEE802.1x on-line user information, as shown in Figure 343.

On-line user

All	User Name	MAC	Port	Authentication Mode	Time(min)
☐	ccc	44-37-e6-88-6e-90	Ethernet1/1	port-based	2

Disconnect

Figure 343 View IEEE802.1x On-line User Information

You can select one or multiple users and click <Disconnect>to disconnect the selected

user(s) from the switch.

6.27.3 Typical Configuration Example

As shown in Figure 344, Client is connected to port 1 of the switch. Enable IEEE802.1x on

port 1 and select Auto authentication mode. The username and password of the local

authentication are both ccc, and the username and password of the remote authentication

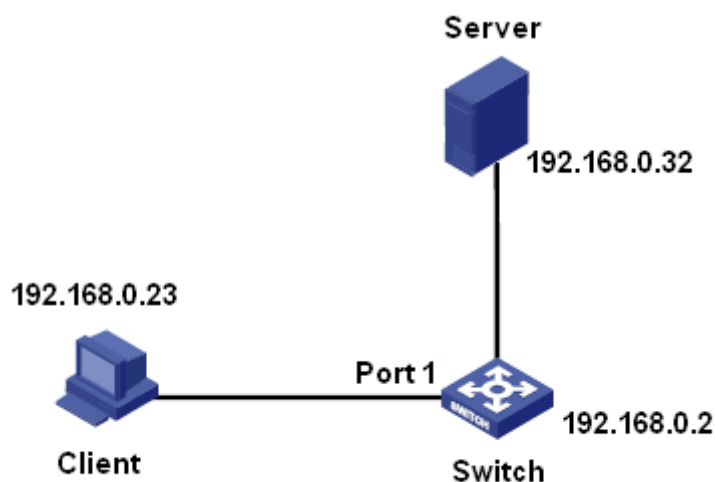are both ddd. Keep default values for other parameters.

Figure 344 IEEE802.1x Configuration Example

➢ Local authentication configuration

1. Enable global IEEE802.1x protocol, as shown in Figure 338.

2. Set dot1x to local authentication, as shown in Figure 345.

3. Set the username and password to ccc, as shown in Figure 342.

4. Enable IEEE802.1x on port 1, and set the authentication mode to Auto, as shown in Figure 339.

5. Install 802.1x authentication client software and start it. Input username and password "ccc" to pass the authentication. Then you can access the switch.

➢ Remote authentication configuration

You can refer to the typical configuration example in "6.26 RADIUS Configuration"

6.28 Authentication login configuration

Configure access mode to switch, authentication mode and authentication order.

Click [Device Advanced Configuration] → [Authentication login configuration] →

[Authentication login configuration] to enter the authentication login configuration page, as

shown in Figure 345.

Figure 345 Authentication Login Configuration

Login Method

Options: Telnet/Web/dot1x/SSH

Function: Select access mode to switch.

Authentication Method/Authentication Method 2/Authentication Method 3

Options: Local/Tacacs+/Radius

Default: Local

Function: Select the order of authentication. Authentication method 1 is first performed. If the authentication fails, authentication method 2 is conducted. If both authentications method 1 and authentication method 2 fail, authentication method 3 is conducted.

Description: **Local** means using username and password set in local to perform authentication. **Tacacs+** means using the username and password set in TACACS+ server for authentication. **Radius** means using the username and password set in RADIUS server for authentication.

> **Caution:**
> Only one authentication mode can be selected when dot1x is used to access the switch.

6.29 Link Check

6.29.1 Introduction

Link check adopts periodic interaction of protocol packets to judge the link connectivity and display the port communication status. 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 Rx 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 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 Tx fault state. If the link to the port is down, the port displays link down 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:**
>
> When the DRP ring/backup port for which link check is enabled is abnormal (for example, receiving is abnormal, sending is abnormal, or disconnected), the DRP ring protocol will block this ring/backup port.

6.29.2 Web Configuration

1. Enable link check function on port.

Click [Device Advanced Configuration] → [Diagnosis Configuration] → [Link Check] to enter link check configuration page, as shown in Figure 346.

Link Check

| Port | 1/1 |
| Link Check Administrative State | Enable |

Apply   Cancel

Figure 346 Enable Link Check on Port

Link Check Administrative State

Options: Disable/Enable

Default: Disable

Function: Enable/Disable link check on port.

⚠ CAUTION	**Caution:** If the peer device does not support the function, the function shall be disabled on the connected port of the local device.

2. Show link check state on port, as shown in Figure 347.

Port	Link Check State
1/1	Normal
1/2	Link Down
1/3	Disable
1/4	Disable
1/5	Disable
1/6	Disable
1/7	Disable
1/8	Rx Fault
1/9	Disable
1/10	Disable
1/11	Disable
1/12	Disable

Figure 347 Show Link Check State on Port

Link Check State

Options: Normal/Rx Fault/Disable/Tx Fault/Link Down

Description: If Link Check is enabled on a port and the port sends and receives data normally, Normal 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 port is link down, Link Down is displayed. If Link

Check is not enabled on a port, Disable is displayed.

6.30 Loop Detect Configuration

6.30.1 Overview

After loop detect is enabled for the port, loop detect packets would be sent out through the port to decide whether loops exist in the network connected to the port. The CPU send loop detect packets to the port periodically. If any port of the switch receives the loop detect packets, it is determined that the loops exist in the network. Shut down the port that is sending loop detect packets and the port would be linked up automatically after a while and continue detection. The time interval for sending loop detect packets and the port recover time can be configured in the software.

> **Note:**
>
> Loop detection and DT-Ring/DRP/RSTP/MSTP are mutually exclusive. A port enabled loop detection cannot be configured as a redandunt port; a redandunt port cannot be enabled loop detection.

6.30.2 Web Configuration

Configure the loop detect function of the port, as shown in Figure 348.

Port check interval (1-6000s)	2
Port recover time (0-6000s,0 is no recover)	30

Port	LoopDetect Enable	LoopDetect Status
1/1	☑	No
1/2	☑	No
1/3	☑	Yes
1/4	☐	-
1/5	☐	-
1/6	☐	-
1/7	☐	-
1/8	☐	-
1/9	☐	-
1/10	☐	-
1/11	☐	-
1/12	☐	-

Apply

Figure 348 Enable the Loop Detect Function of the Port

Port check interval

Range: 1~6000s

Default: 2s

Function: Configutr the time interval for sending loop detect packets.

Port recovery time

Range: 0~6000s

Default: 30s

Function: Configure the port recover time, 0 indicates the port cannot be linked up automatically.

Loop Detect Enable

Options: Enable/Disable

Default: Disable

Function: Enable or disable the loop detect function of the port.

Loop Detect Status

Options: Yes/No

Function: Loop detect status displays whether there are loops for the network in which the loop detect function of the port is enabled. Yes indicates there are loops while No indicated no loop exists.

6.30.3 Typical Configuration Example

Networking Requirements:

Port 3 of the switch is connected to the external network. When there are loops for the network, shut down port 3, as shown in Figure 349.
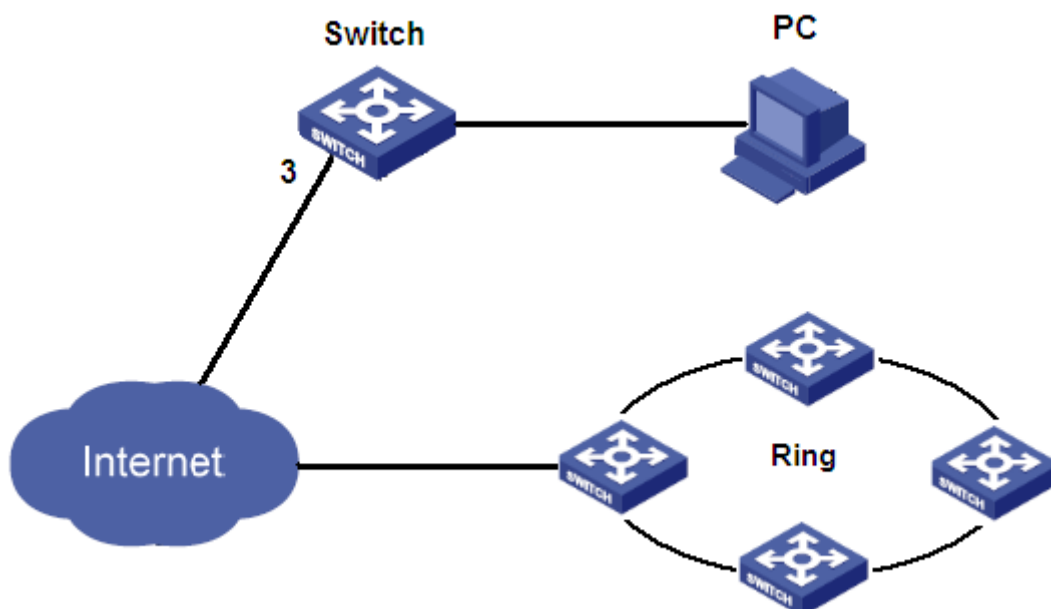
Figure 349 Loop Detect Instance

Specific configuration:

Enable the loop detect function of port 3, as shown in Figure 348.

6.31 Port CRC Protect

6.31.1 Overview

After the port CRC protect function is enabled, periodic detection of the CRC error packets can be realized. If the number of CRC error packets exceeds the expected threshold during the detection, shut down the port. Link up the port after a while and continue detection. The

time for detecting the CRC error packets and the port recover time can be configured in the software.

6.31.2 Web Configuration

Configure port CRC protect function, as shown in Figure350.

Port check interval (1-6000s)	5
Port recover time (0-6000m,0 is no recover)	5

Port	Port CRC Protect Enable	Port CRC Protect Status	CRC Threshold(1-10000)packets
1/1	☑	No	10
1/2	☑	No	100
1/3	☑	No	10
1/4	☐	-	10
1/5	☐	-	10
1/6	☐	-	10
1/7	☐	-	10
1/8	☐	-	10
1/9	☐	-	10
1/10	☐	-	10
1/11	☐	-	10
1/12	☐	-	10

Apply

Figure350 Enable the port CRC protect

Port check interval

Range: 1~6000s

Default: 5s

Function: Configure the time for detection of CRC error packets. If the number of CRC error packets exceeds the threshold, shut down the port.

Port recover time

Range: 1~6000 min

Default: 5m

Function: Configure the port recover time, 0 indicates the port cannot be linked up

automatically.

Port CRC Protect Enable

Options: Enable/Disable

Default: Disable

Function: Enable or disable the port CRC protect function. This detection mechanism only works for the port with its CRC protect function being enabled.

Port CRC Protect Status

Options: -- / Yes / No

Description: Yes: the port CRC protect function is enabled, and the port status is linkdown because of CRC error. No: the port CRC protect function is enabled, and the port status is linkup. --: the port CRC protect function is not enabled.

CRC Threshold

Range: 1~10000 packets

Default: 10 packets

Function: Configure the CRC threshold.

Appendix: Acronyms

Acronym	Full Spelling
ABR	Area Border Router
AS	Autonomous System
ASBR	Autonomous System Boundary Router
ARP	Address Resolution Protocol
BDR	Backup Designated Router
BootP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
CAR	Committed Access Rate
CIST	Common and Internal Spanning Tree
CLI	Command Line Interface
CoS	Class of Service
CST	Common Spanning Tree
DD	Database Description
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DR	Designated Router
DSCP	Differentiated Services CodePoint
DST	Daylight Saving Time
FTP	File Transfer Protocol
GARP	Generic Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
GVRP	GARP VLAN Registration Protocol
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IED	Intelligent Electronic Device

IGMP	Internet Group Management Protocol
IGMP Snooping	Internet Group Management Protocol Snooping
IST	Internal Spanning Tree
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
LSA	Link State Advertisement
LSAck	Link State Acknowledgment
LSDB	Link State Database
LSR	Link State Request
LSU	Link State Update
MIB	Management Information Base
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
NAS	Network Access Server
NetBIOS	Network Basic Input/Output System
NMS	Network Management Station
NTP	Network Time Protocol
OID	Object Identifier
OSPF	Open Shortest Path First
PVLAN	Private VLAN
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RID	Router ID
RIP	Routing Information Protocol
RMON	Remote Network Monitoring
RSTP	Rapid Spanning Tree Protocol
RTC	Real Time Clock
SNMP	Simple Network Management Protocol

SNTP	Simple Network Time Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
USM	User-Based Security Model
VLAN	Virtual Local Area Network
VRRP	Virtual Router Redundancy Protocol
WINS	Windows Internet Naming Service
WRR	Weighted Round Robin