SICOM3024GS(V2.0) Series
Industrial Ethernet Switches
Web Operation Manual

Publication Date: Dec. 2021

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: services@kyland.com.cn

Contents

Perface

This manual mainly introduces the access methods and software features of SICOM3024GS(V2.0) industrial Ethernet switch, and details Web configuration methods.

Content Structures

The manual contains the following contents:

Main Content	Explanation
1. Product Introduction	➢ Overview ➢ Software Features
2. Switch Access	➢ View Types ➢ Switch Access by Console Port ➢ Switch Access by Telnet ➢ Switch Access by Web
3. User	➢ User Management ➢ Auth Type
4.System	➢ Basic information ➢ Config Management ➢ Clock management ➢ Software update（HTTP, FTP,TFTP） ➢ Soft Application Active ➢ Language Update ➢ Restart ➢ About
5. Service	➢ SSL Configuration ➢ SNMP v1/v2c/v3 ➢ SSH Configuration ➢ TACACS+ Configuration ➢ RADIUS Configuration ➢ DNS

	➢ RMON
6. Alarm	
7. Function Management	➢ Port Configuration ➢ VLAN ➢ IP Configuration ➢ Port Aggregation ➢ Redundancy ➢ DT-Ring ➢ ARP Configuration ➢ ACL Configuration ➢ MAC Address Configuration ➢ POE ➢ IGMP snooping ➢ DHCP Configuration ➢ IEEE802.1X Configuration ➢ GMRP ➢ PIM# ➢ NAT# ➢ IGMP# ➢ Route# ➢ GMRP ➢ Static Route ➢ QoS Configuration ➢ VRRP#
8. Diagnosis	➢ Log ➢ Port Mirror ➢ LLDP ➢ Trace Route ➢ Ping

	➢ IP Source Guard ➢ DDM

NOTE:

The SICOM3024GS-L2G series does not support this marking function.

Conventions in the manual

1. 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.

2. CLI conventions

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

3. Symbol conventions

Symbol	**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 SICOM3024GS(V2.0) series industrial Ethernet switches include:

Name of Document	Content Introduction
SICOM3024GS(V2.0) Series Industrial Ethernet Switches Hardware Installation Manual	Describes the hardware structure, hardware specifications, mounting and dismounting methods.
SICOM3024GS(V2.0) Series Industrial Ethernet Switches Web Operation Manual	Describes the switch software functions, Web configuration methods, and steps of all functions.

Document Obtainment

Product documents can be obtained by:

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

1 Product Introduction

1.1 Overview

SICOM3024GS(V2.0) include a series of high-performance industrial Ethernet switches developed by Kyland particularly for rail transportation industry. The series devices meet the requirements stipulated in the EN50155, EN50121 and other industrial standards. The switches support MSTP/RSTP, DT-Ring, IEC62439-6 redundancy protocols, guaranteeing the reliable operation of the system.

1.2 Software Features

SICOM3024GS(V2.0) provides abundant software features, satisfying customers' various requirements.

- Redundancy protocols: DT-Ring DRP, STP/RSTP, VRRP and MSTP.
- Multicast protocols: IGMP Snooping, GMRP， PIM-SM、PIM-DM.
- Switching attributes: VLAN, PVLAN, GVRP, QoS, and ARP.
- Bandwidth management: port static aggregation, LACP, port rate limiting, and port storm suppression.
- Security: user management, access management, SSH, SSL, TACACS+, RADIUS, IEEE802.1X, ACL, IP Source Guard and Port Isolate.
- Synchronization protocols: SNTP, NTP.
- Device management: software update, configuration file upload/download, and log record and upload.
- Device diagnosis: port mirror, LLDP.
- Alarm function: power alarm, port alarm, ring alarm, and IP/MAC address conflict alarm.
- Network management: management by CLI, Telnet, Web and Kyvision network management software, DHCP, and SNMP v1/v2c/v3 network monitoring.
- Network related: NAT, DNS.
- ……

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 #	Privileged mode	View recently used commands. View software version. View response information for ping operation. Upload/Download configuration file. Restore Default configuration. Reboot switch. Save current configuration. Display current configuration. Update software.	Input “**configure terminal**” to switch from privileged mode to configuration mode. Input “**exit**” to return to the general mode.
SWITCH（config）#	Configuration mode	Configure all switch functions.	Input "**exit**" or "**end**" to return to the Privileged mode.

When the switch is configured through the CLI, "?" can be used to get command help. In the help information, there are different parameter description formats. For example, <1, 255>

means a number range; <xx:xx:xx:xx:xx:xx> means a MAC address; <word31> means the string range is 1~31. 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 M12-A-4P-M console cable.

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

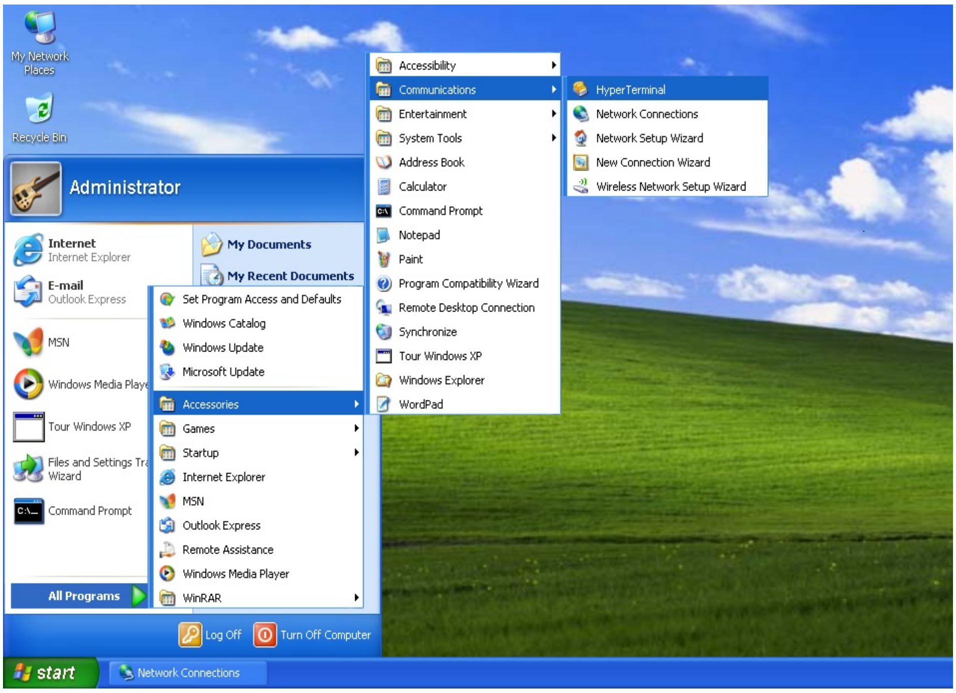


Figure 1 Starting the Hyper Terminal

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.

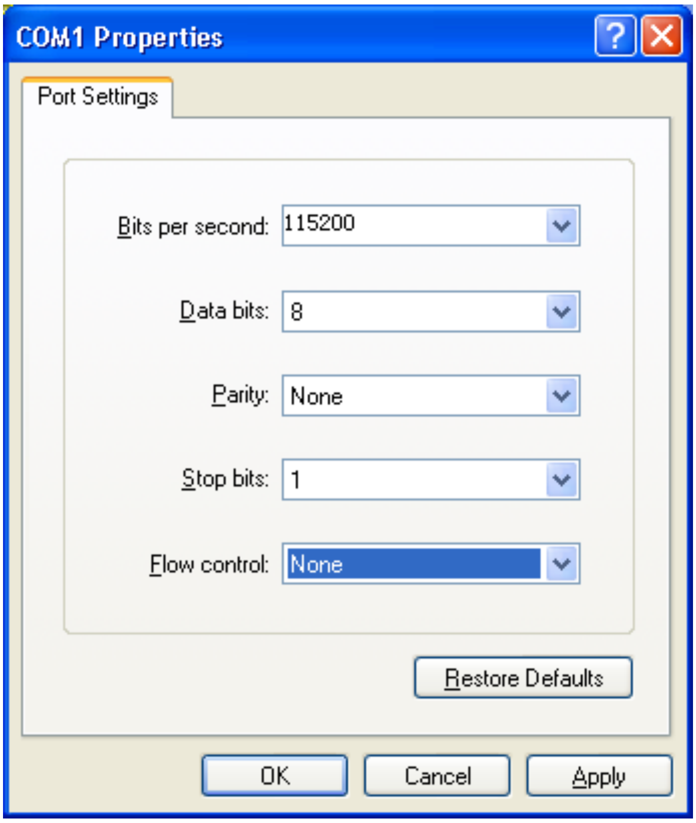


Figure 4 Setting Port Parameters

6. Click <OK> button to enter the switch CLI. Input default user "admin", and password"123" to enter the privileged mode. You can also input other created users and password, as shown in Figure 5.

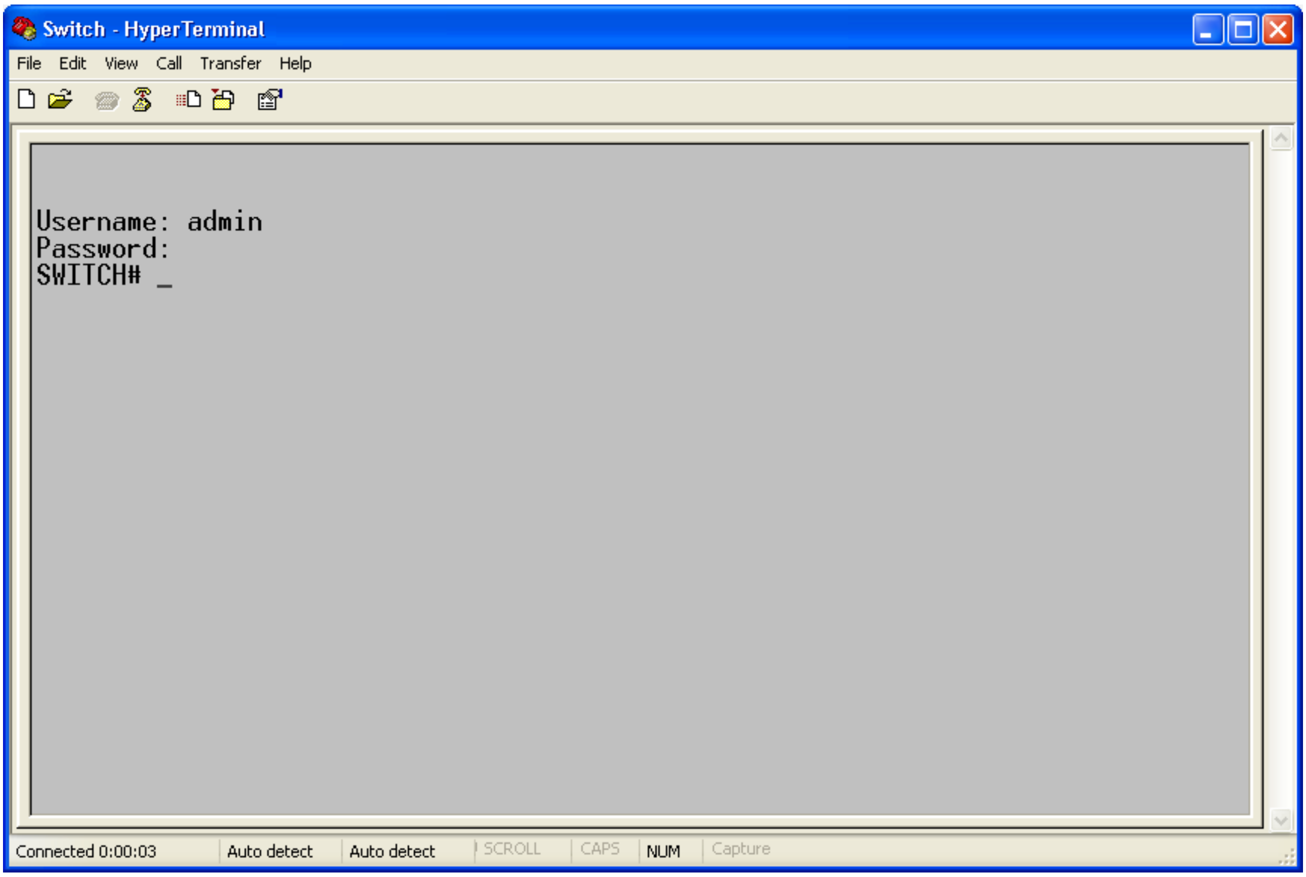


Figure 5 CLI

2.3 Switch Access by Telnet

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

1. Enter "**telnet** *IP address*" in the Run dialog box, as shown in Figure 6. The default IP address of a Kyland switch is 192.168.0.2.

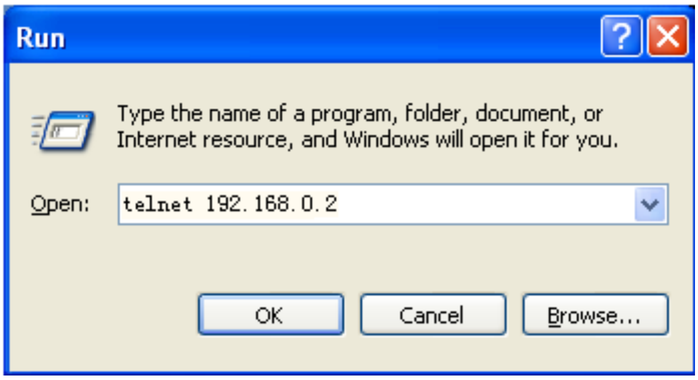


Figure 6 Telnet Access

Note:

To confirm the switch IP address, please refer to "7.3 IP Configuration" 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 7.

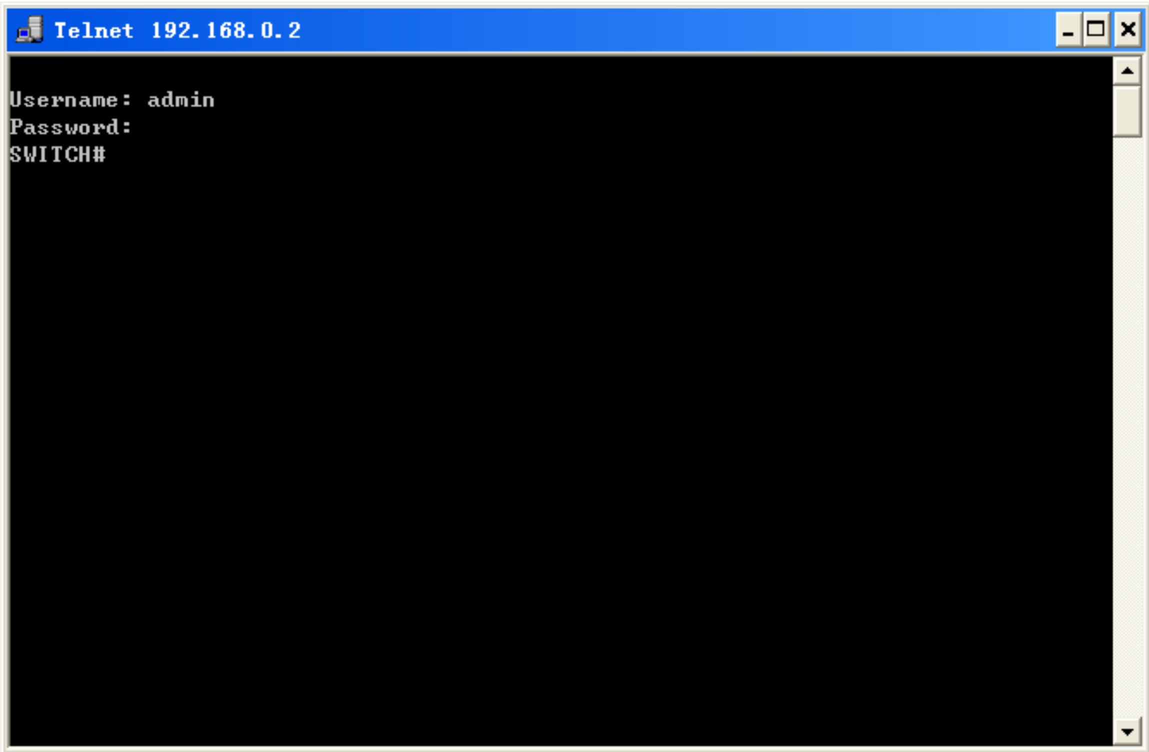


Figure 7 Telnet Interface

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 8. Input the default user name "admin", password "123", and the Verification. Click <Login>. You can also input other created users and password.

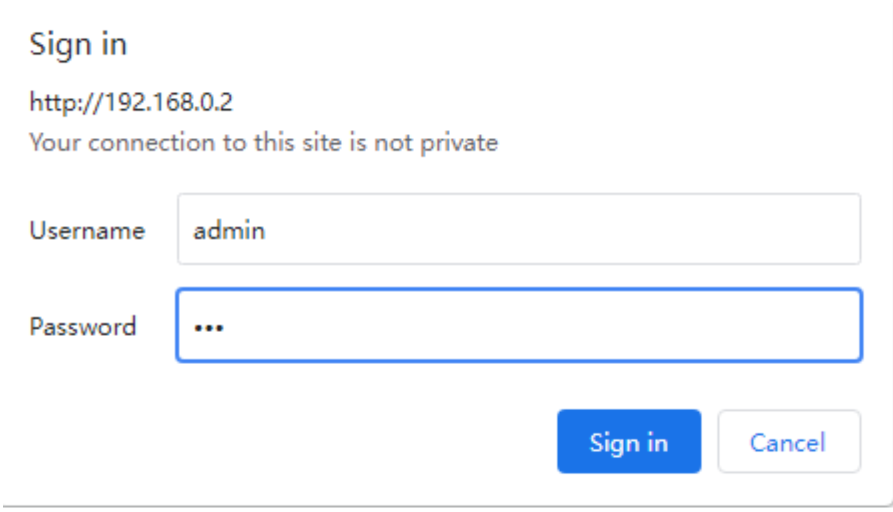


Figure 8 Web Login

Enter the main interface. In the upper right corner, you can switch to the English or Chinese Web operation interface. The English login interface is displayed by default.

Note：

To confirm the switch IP address, please refer to “7.3 IP Configuration” to learn how to obtain IP address.

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

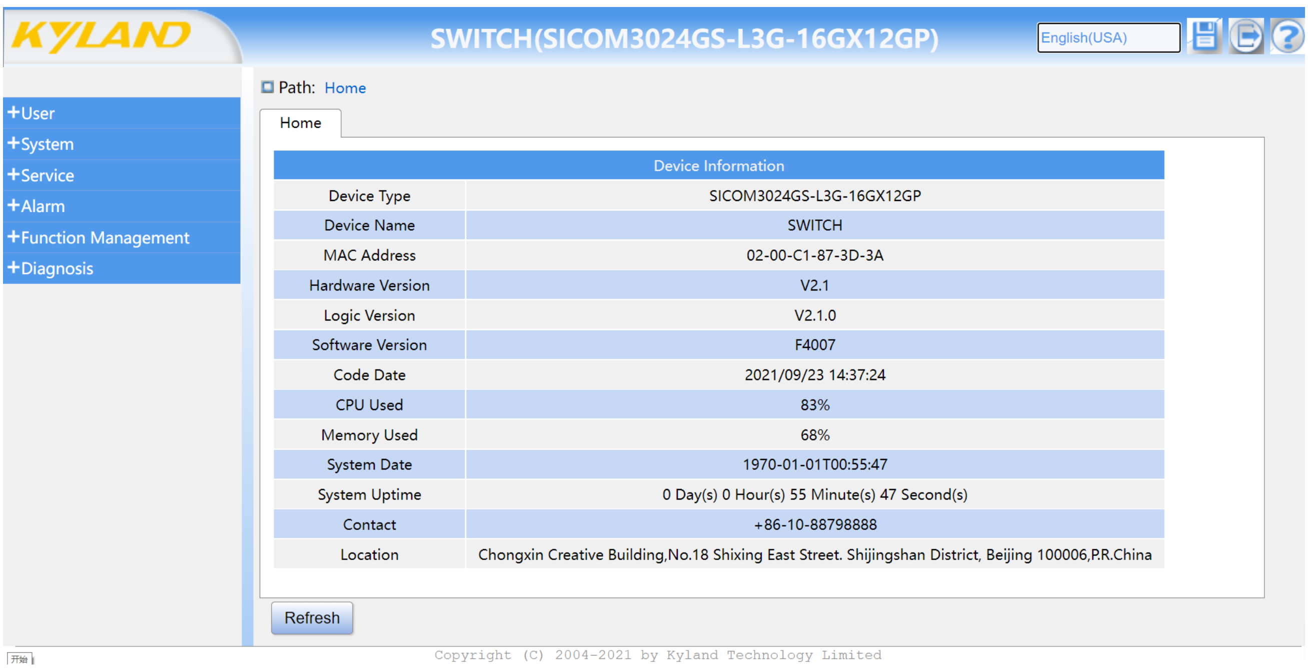


Figure 9 Web Interface

You can expand or collapse the navigation tree by clicking menu on the navigation tree. You can click Home to link to Figure 9, and click  to exit the Web interface.

3 User

3.1 User management

3.1.1 Introduce

To solve the security problem caused by illegal user access switch, the switch provides the function of user hierarchical management, based on different user identity, set different permissions to meet the diversify of user permissions control.

3.1.2 Web Configuration

1. Create a new user, as shown below.

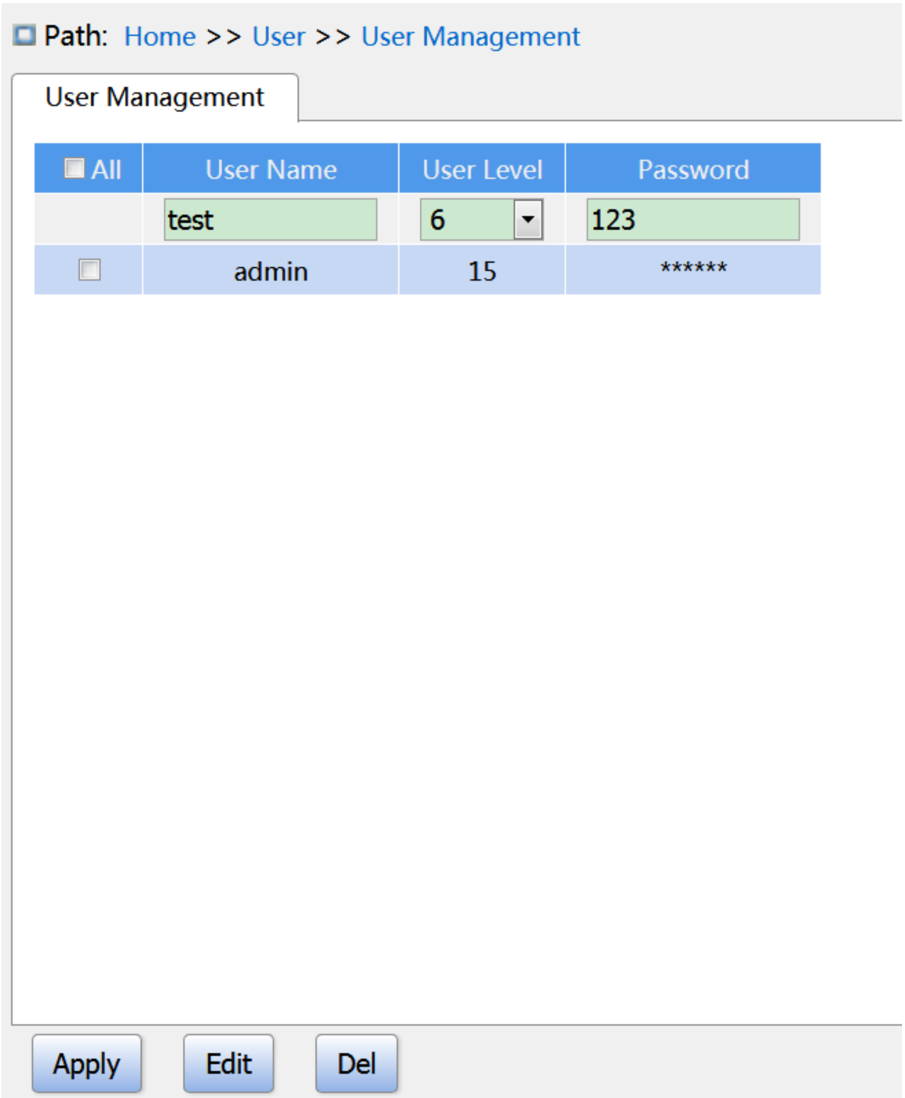


Figure 10 Create a new user

Add a new user in the user name formula bar, configure different user levels, and max 20 users can be created.

User name

Configuration range：1~31 characters

Function：configure user name.

User level

Configuration range：0~15

Function：Configure the user's permission level. Users with different permission levels have different access permissions.

Password

Configuration range：0~31 characters

Function：configure user login password.

2. Edit user configuration, as shown below.

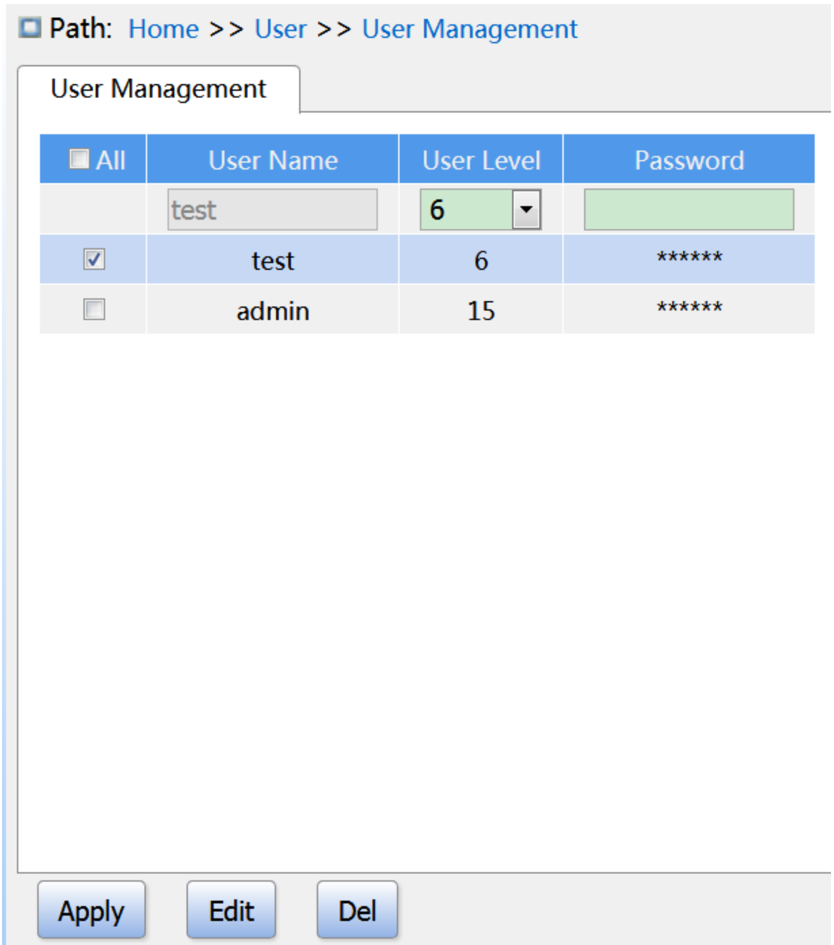


Figure 11 Edit user configuration

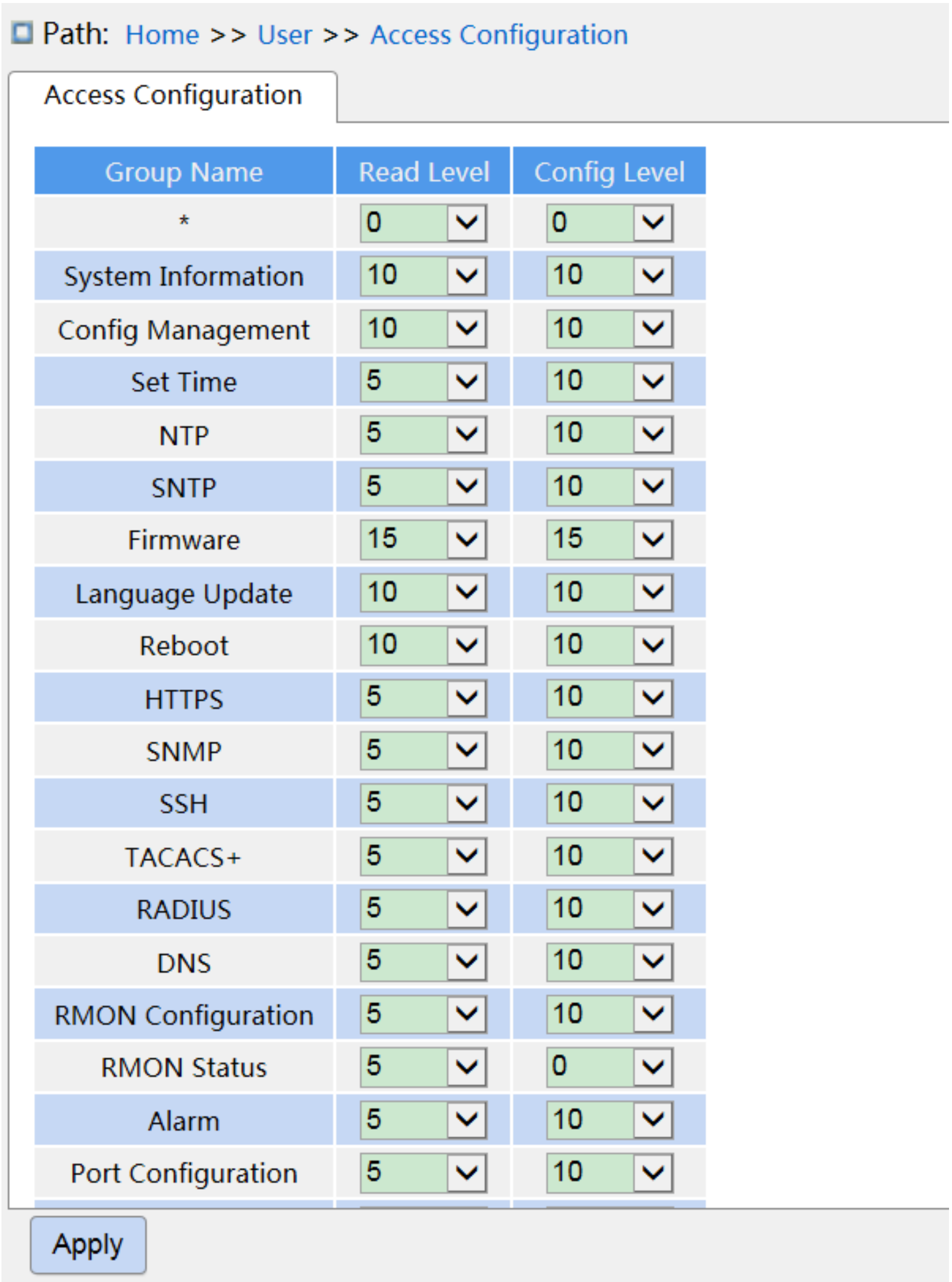
Check the user who needs to be edited, click <Edit> button to midify the password and permission levels of user.

Click <Del> button to delete the current user.

Note:

- The default user admin can't be deleted:

3. Configure groups privilege level, as shown below.



Group Name	Read Level	Config Level
*	0	0
System Information	10	10
Config Management	10	10
Set Time	5	10
NTP	5	10
SNTP	5	10
Firmware	15	15
Language Update	10	10
Reboot	10	10
HTTPS	5	10
SNMP	5	10
SSH	5	10
TACACS+	5	10
RADIUS	5	10
DNS	5	10
RMON Configuration	5	10
RMON Status	5	0
Alarm	5	10
Port Configuration	5	10

Figure 12 Configure groups privilege level

Group Name

Configuration options: All functional groups

Function: Select the switch function group for the operation

Read Level

Configuration options: 0-15

Default configuration: 5

Function: Configure the level at which the current function group can be viewed by the user. Different levels of function groups have different permission level requirements for user viewing.

Config Level

Configuration options: 0-15

Default configuration: 10

Function: Configure the level at which the current function group can be operated by the user. Different levels of function groups have different permission level requirements for user operations.

Note：

When the user privilege level is same or greater than a group privilege level, the user can access or configure the group. The access or configure right is based on the user privilege level.

3.2 Auth Type

Configure access mode to switch, authentication mode and authentication order, as shown below.

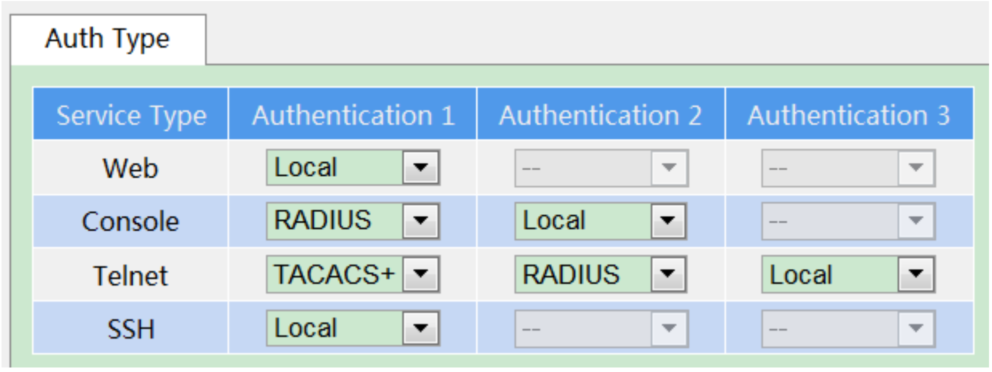


Figure 13 Authentication Login Configuration

Service Type

Configuration options: Web/Console/Telnet/SSH

Function: Select access mode to switch.

Authentication1/ Authentication2/ Authentication3

Configuration options: --/local/tacacs/radius

Default configuration: local

Function: The methods from left to right are Authentication1, Authentication2, and Authentication3. 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: **--** means authentication is disabled and login is not possible. **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:

If tacacs/radius is selected for Authentication1 and Authentication 2, it is recommended to configure Authentication 3 as local. This will enable the management client to login switch vis the local user if none of the configured remote authentication servers are alive.

---

4 System

4.1 Basic Information

System information includes Device Type, Device Name, MAC Address, Hardware Version, Logic Version, Software Version, Code Date, CPU Used, Memory Used, System Date, ystem Uptime, Contact and Location, as shown below.

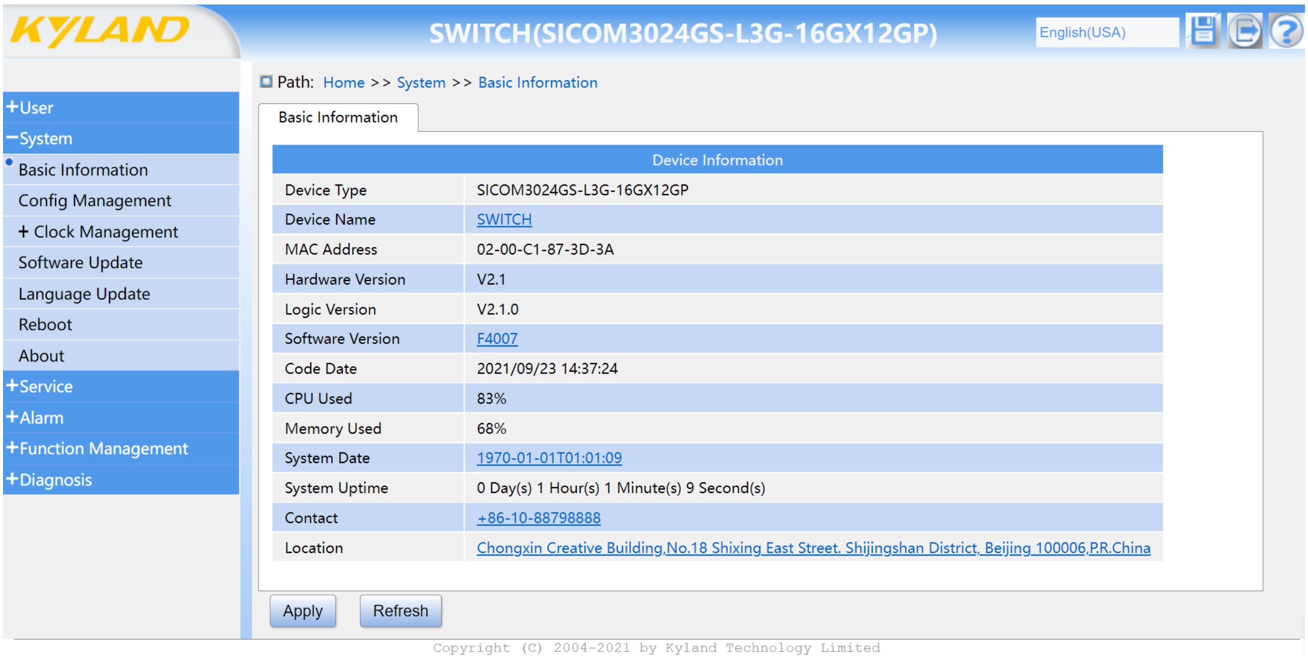


Figure 14 Basic Infomation

4.2 Config Management

1. Save the current configuration information, as shown in the following figure.

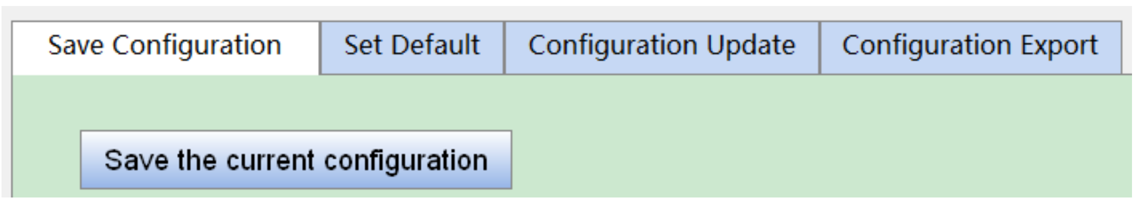


Figure 15 Save the current configuration

2. Restore the factory configuration, as shown below.

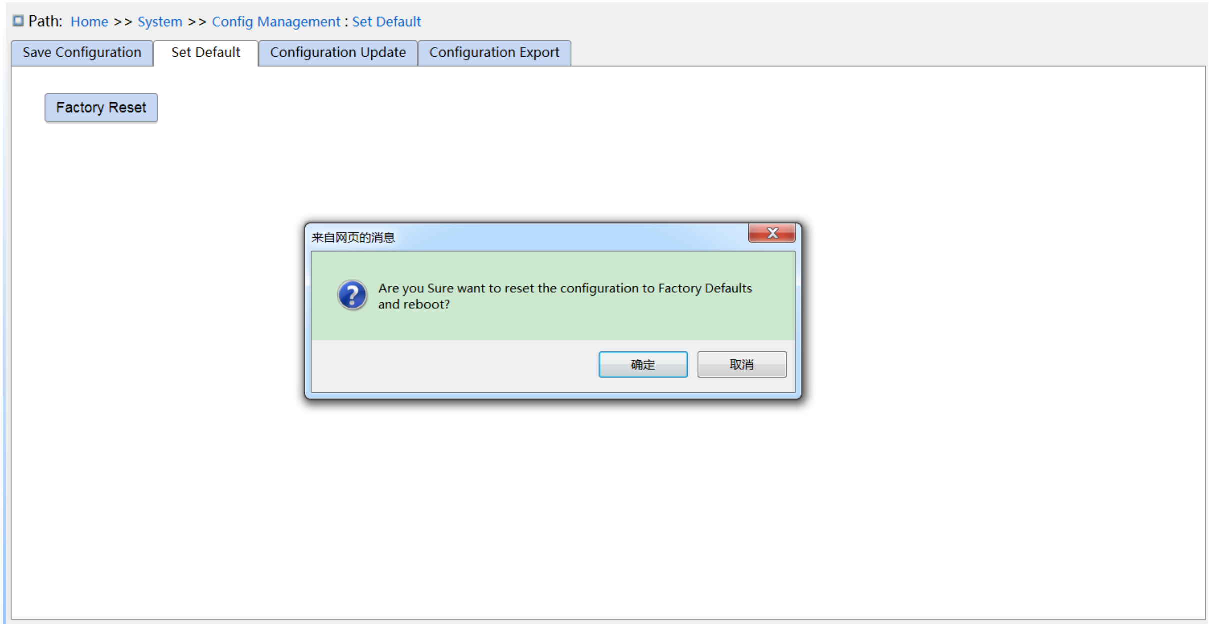


Figure 16 Restore the factory configuration

3. Configuration Export. Download the file from the switch to the local / server, as shown in Figure 17 - Figure 19.

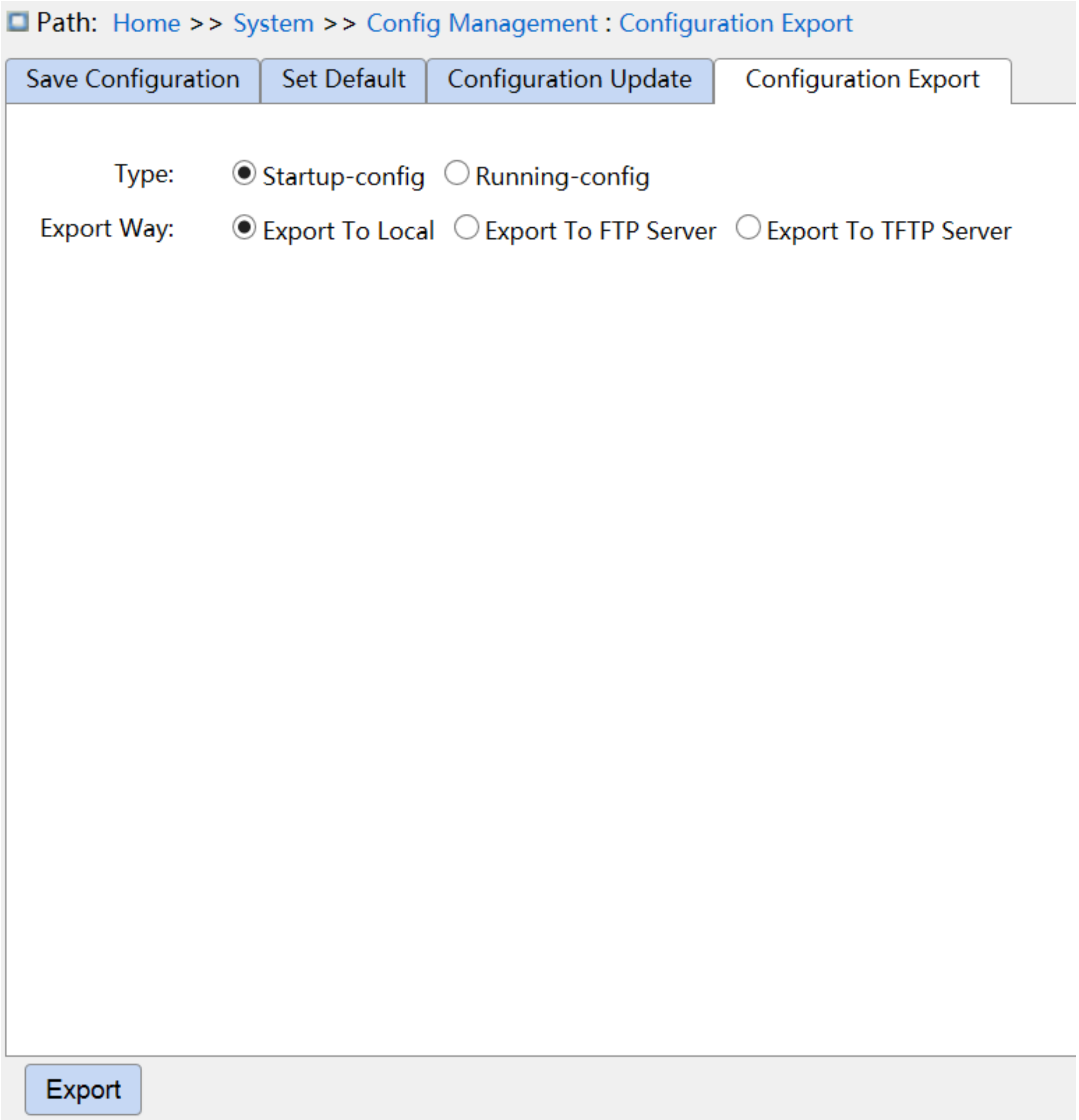


Figure 17 Export Configuration File-HTTP

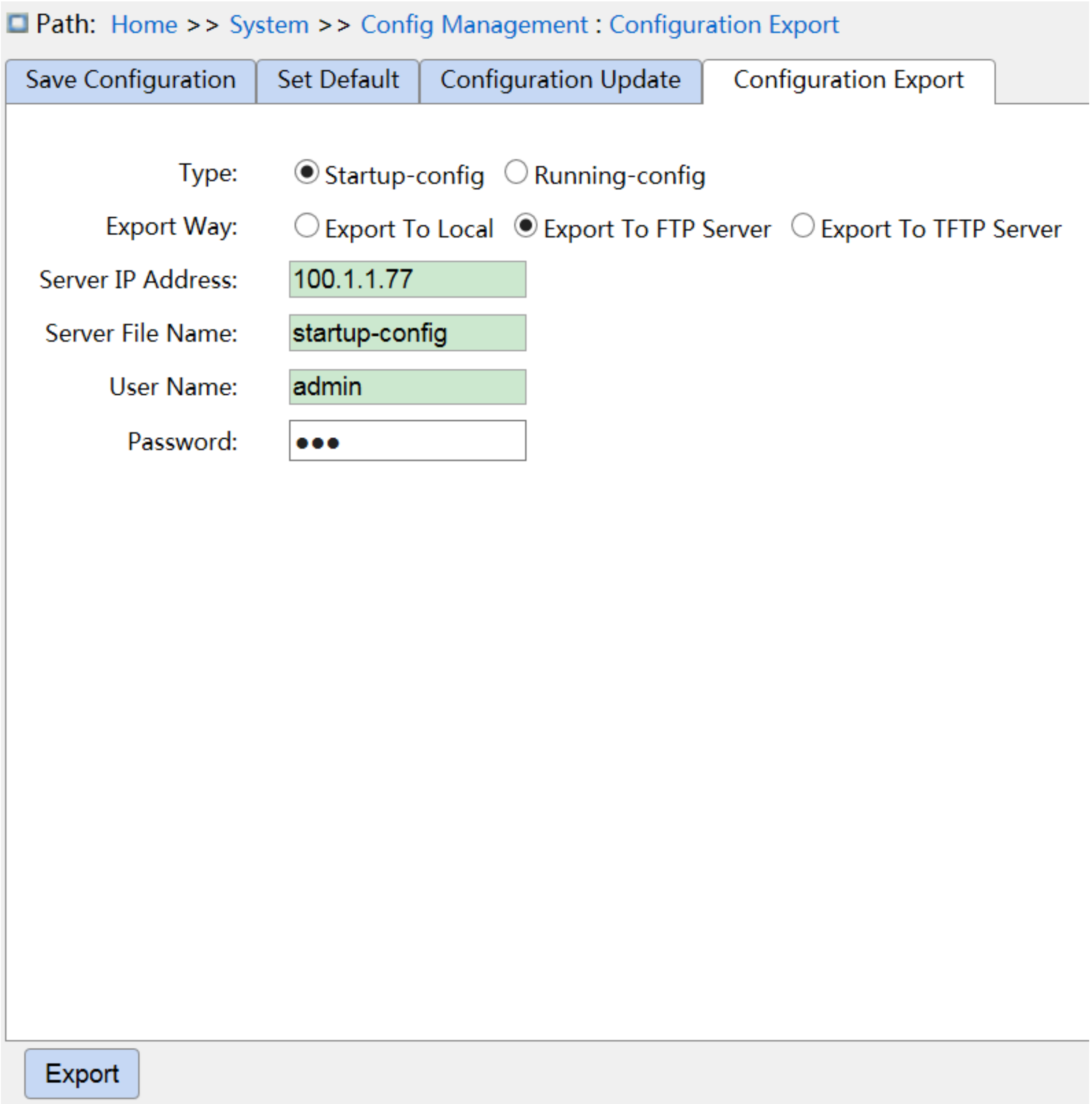


Figure 18 Export Configuration File –FTP

Server IP address

Format: A.B.C.D

Description: Configure the IP address of the FTP server.

Server file name

Configuration range: 1~63 characters

Description: Configure the configuration file name stored on FTP server.

{ User name, Password }

Configuration range: { 1~63 characters, 1~63 characters }

Description: Input the user name and password created on FTP server.

Caution:

- Transmission file by FTP, you need to configure FTP user name, password, and FTP server IP address.
- In the file transmission process, keeps the FTP server running.

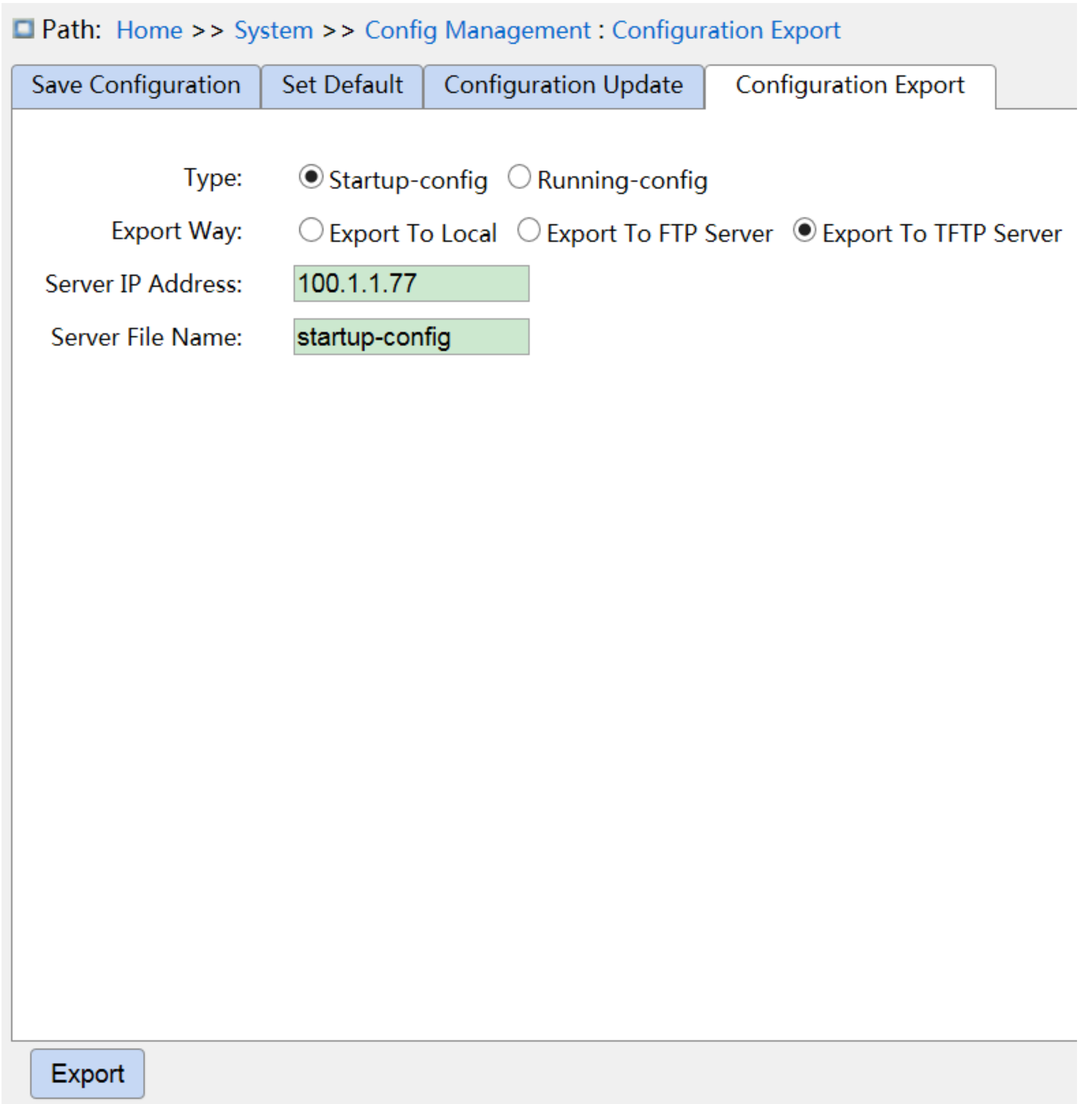


Figure 19 Export Configuration File-TFTP

You can save a file in the switch to the local /server. **running-config** is the current running configuration file of the switch, and **startup-config** is the switch startup file. Select a file and click < Export> to save the file to the local/server.

4. Configuration Update. Download the configuration file from local /server to switch as a

new startup file for the switch, as shown in Figure 20 -Figure 22.

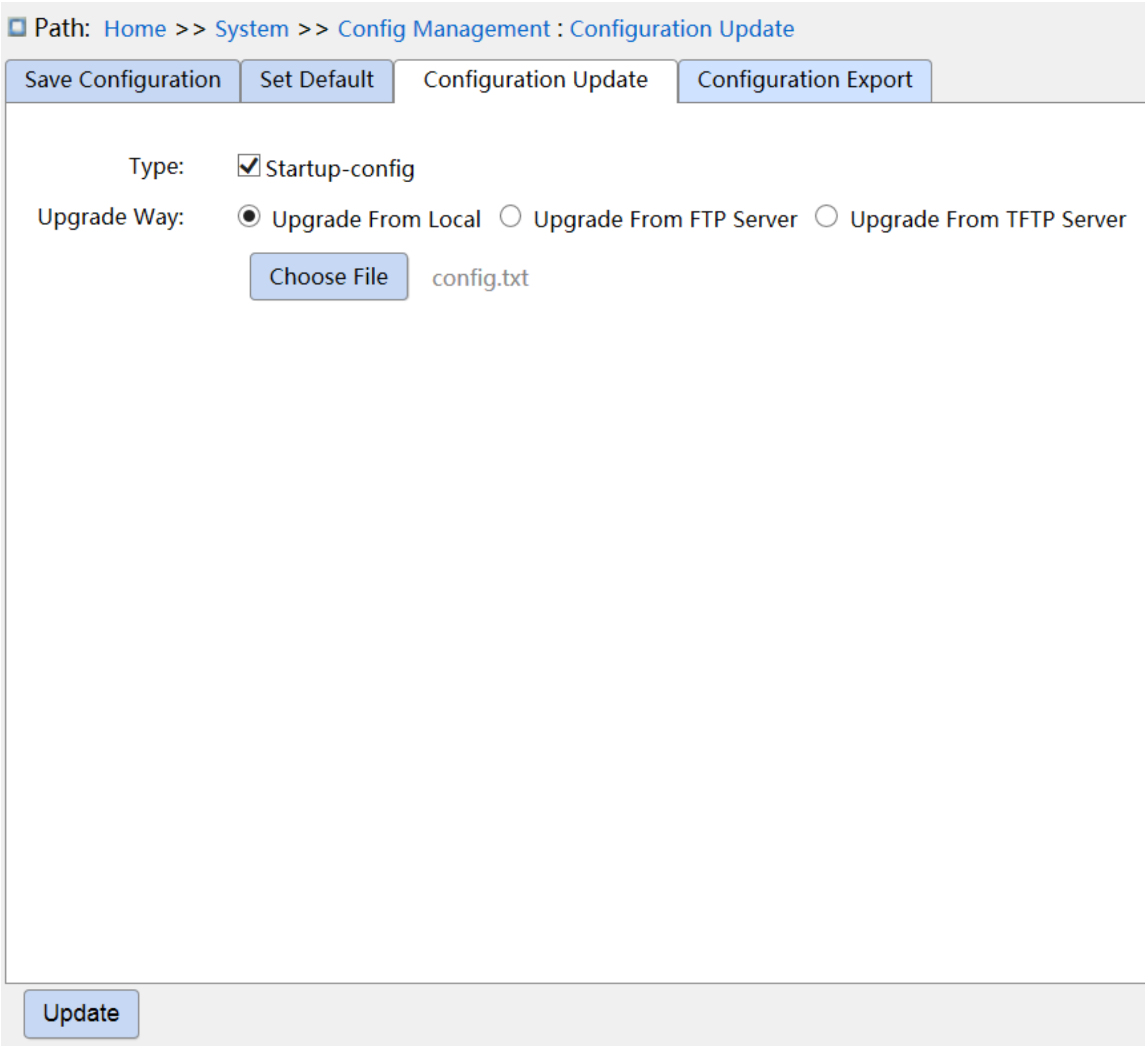


Figure 20 Download Configuration File-HTTP

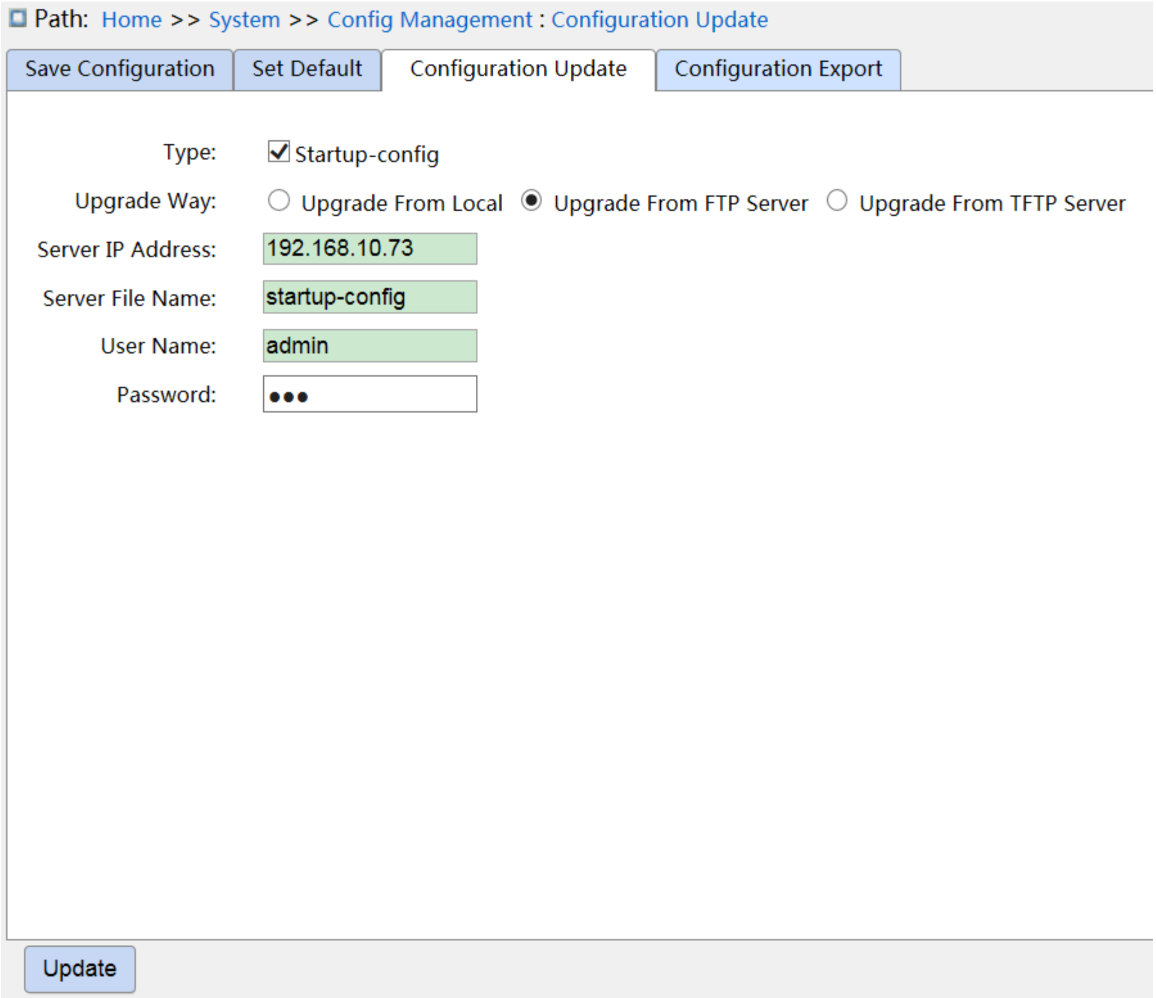


Figure 21 Download Configuration File-FTP

Server IP address

Configuration Format: A.B.C.D

Description: Configure the IP address of the FTP server.

Server file name

Configuration range: 1~63 characters

Description: Configure the firmware update file name stored on FTP server.

{ User name, Password }

Configuration range: { 1~63 characters, 1~63 characters }

Description: Input the user name and password created on FTP server.

Caution:

➢When using FTP to transfer files, you need to configure the FTP user name, password, and FTP server IP address and file name..

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

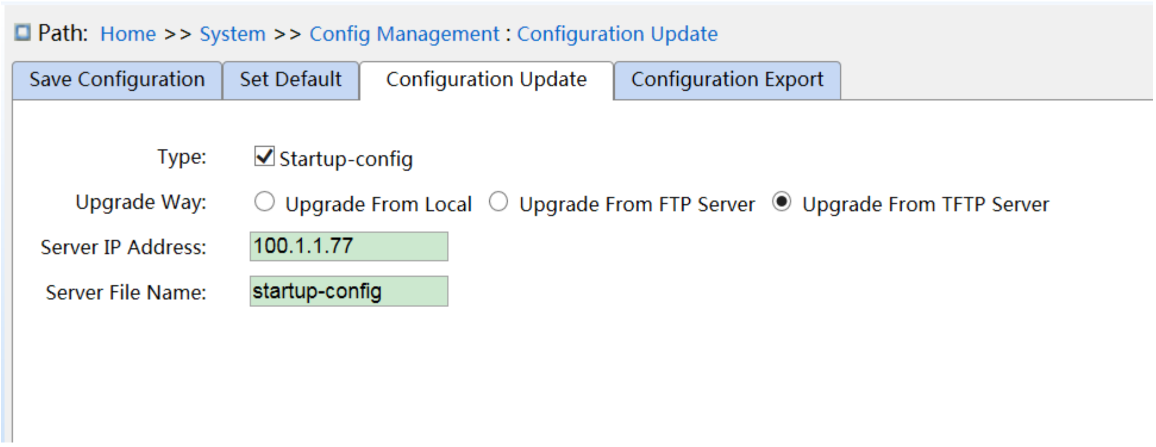


Figure 22 Download Configuration File-TFTP

You can download the configuration file from local /server to switch as a new startup file for the switch. The new startup file will replace the original **startup-config** file. Click <Update> to download the configuration file from local /server to switch.

4.3 Clock management

1. Set DST, as shown below.

In order to make full use of daylight and save energy in summer, you can use DST（DST: Daylight Saving Time）. DST configuration is divided into recurring and non-recurring configuration.

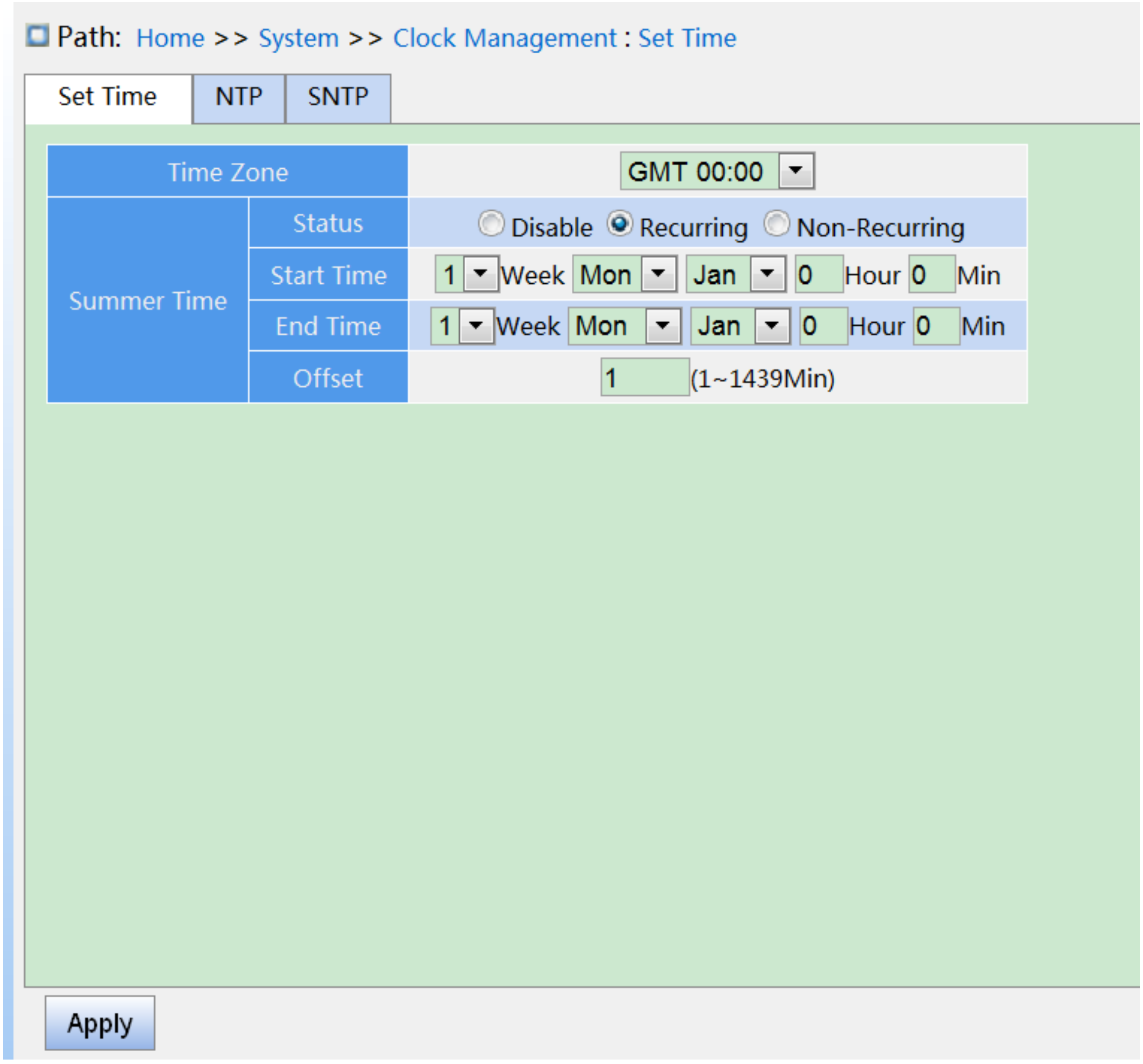


Figure 23 recurring configuration

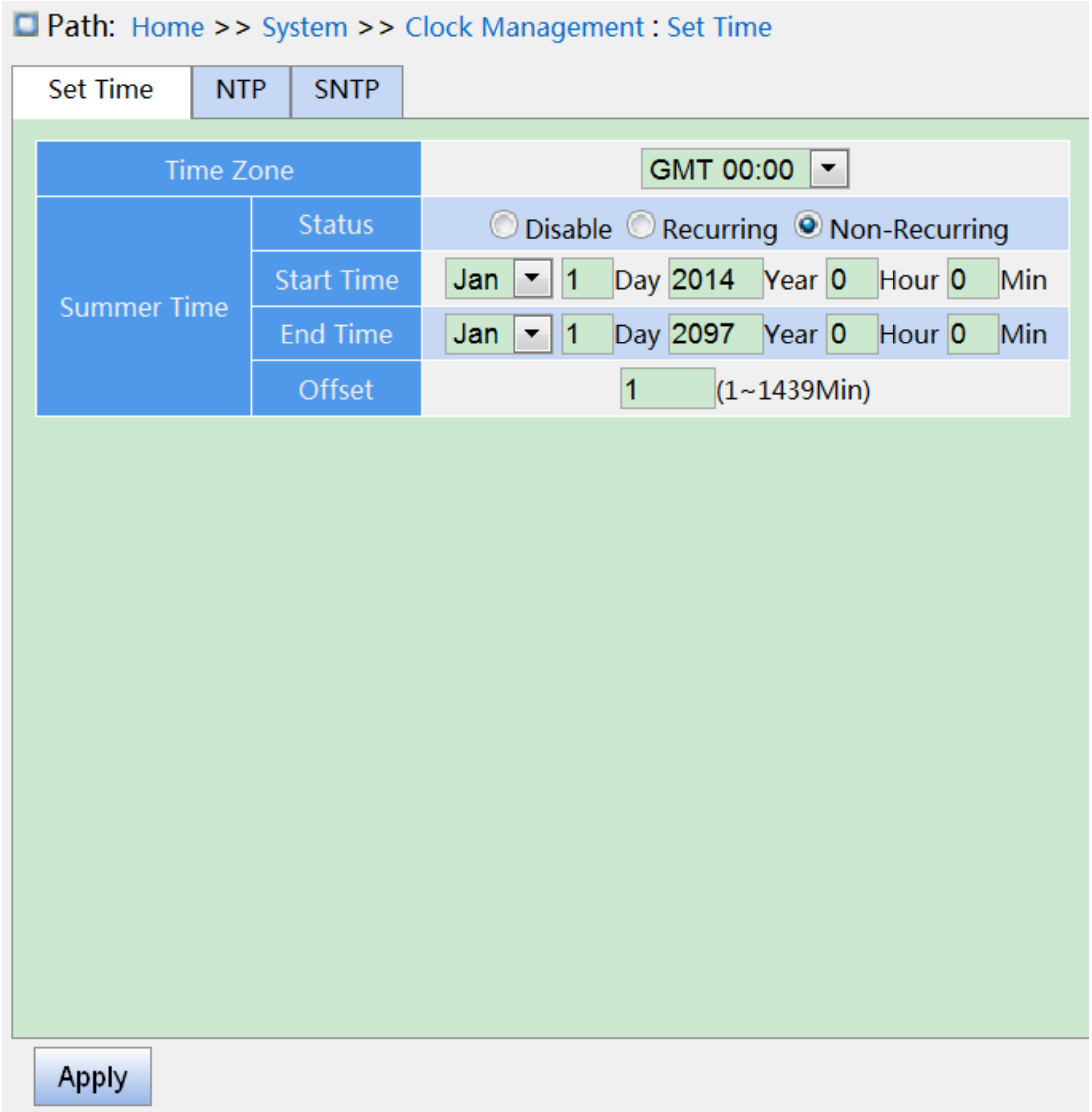


Figure 24 Non-recurring configuration

Time zone

Function：select local time zone.

DST status

Configuration options：disable/recurring/non-recurring

Default configuration：disable

Function：Whether enable daylight saving time, after enable, select DST mode, recurring mode by year.

Start time/end time

Function：after enabling DST, set the time range of DST. Non-recurring mode configure year, month, day, hour and minute to appoint the operation range of DST, as shown Figure 23 set DST between 00:00 on 1 January in 2014 and 23:59 on 1 July in 2097. Recurring mode configure month, week, date, hour and minute to appoint the operation range of DST per year, as Figure 22 set DST between 00:00 on the first Monday in January and 23:59 on the first Monday in July per year.

Offset

Configuration range：1~1439min

Default configiruation：1min

Function：configurate DST offset, that is start time of DST, and advanced time.

Caution：

- The start time and end time should be different:
- The start time is non-DST time, the end time is DST time.

Example：the DST time from 10:00:00 on April 1 to 9:00:00 on October 1, so the DST offset is 60 min。

Non-DST time runs to 10: 00: 00 on April 1 and jumps directly to 11: 00: 00 DST to begin DST. When DST runs to 9: 00: 00 on October 1, it returns to 8: 00: 00 non-DST.

2. NTP configuration

NTP (network time protocol) is used to synchronize time between the distributed time server and the client. NTP can synchronize the clock of all devices with clock in the network, so that the clock of all devices in the network is same. So that the device can provide a variety of applications based on the same time. For the local system running NTP, it can receive synchronization from other clock sources or synchronize other clocks as clock sources.

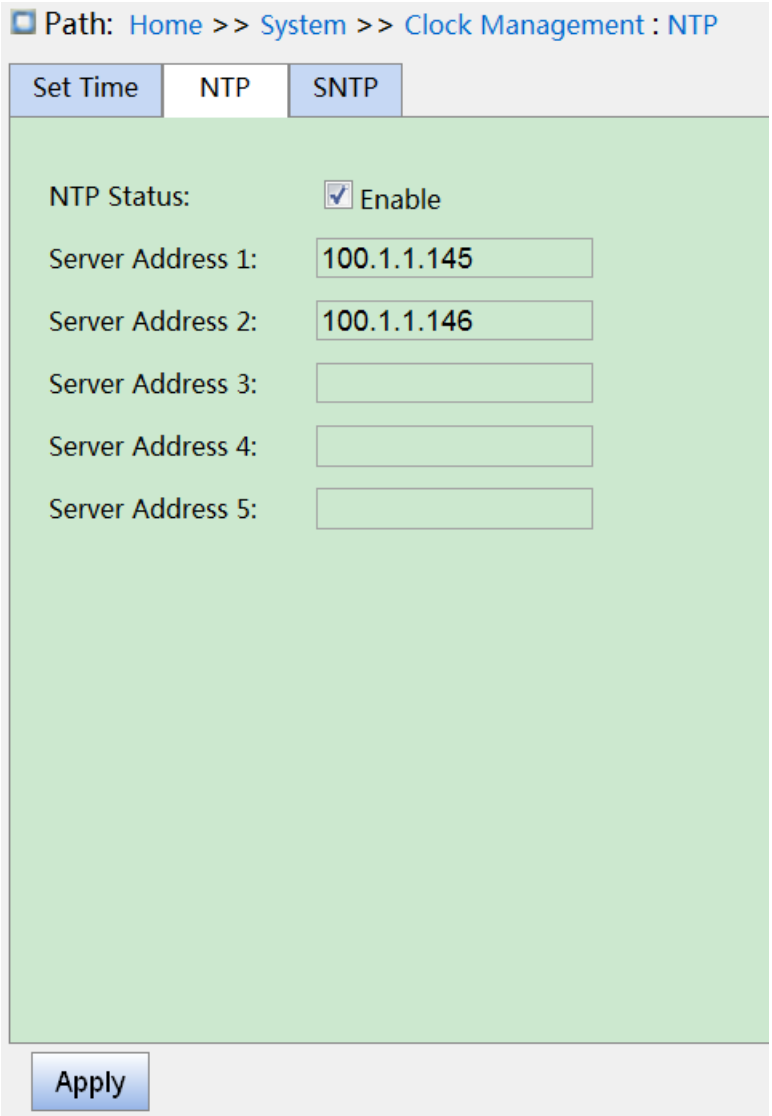


Figure 25 NTP configuration

NTP status

Configuration options：enable/disable

Default configuration：disable

Function：Whether enable global NTP services.

Caution：

- NTP and SNTP protocol mutually exclusive. Because NTP and SNTP use the same UDP port , both cannot be enabled at the same time；
- When NTP services are disable, NTP services can be configured and saved, that is, the enable or disable NTP services does not affect the configuration of NTP services.

Server address 1/ server address 2/ server address 3/ server address 4/ server address 5

Configuration format：A.B.C.D

Function：Configure the IP address of the NTP server, and the client will calibrate time according to NTP server’s message.

3. SNTP configuration

SNTP（Simple Network Time Protocol）protocol calibrates time by requesting and responding between the server and the client. The switch as a client calibrate the time according to the server's message.

Caution:

- When the switch enables SNTP, the SNTP server should be active.
- The time information in SNTP protocol is standard time information of the 0 time zone.

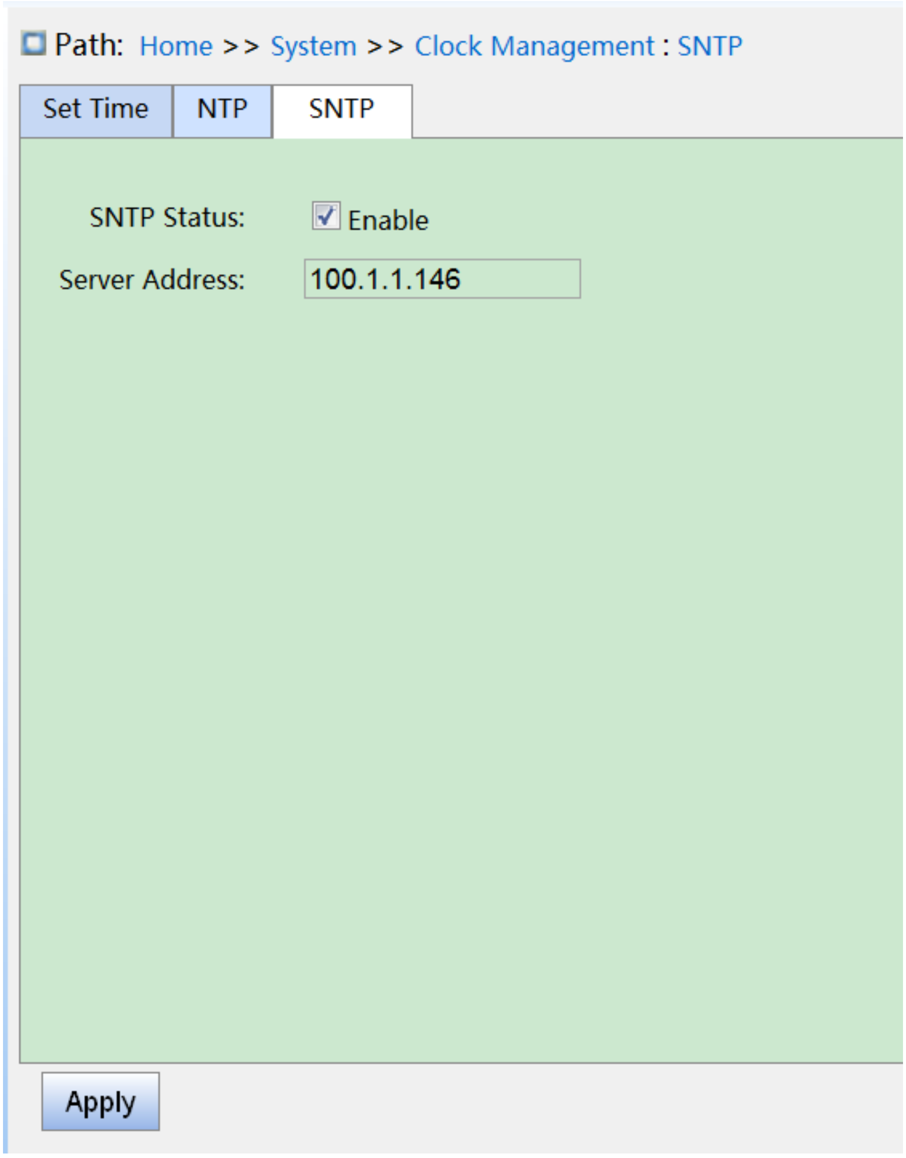


Figure 26 SNTP configuration

SNTP status

Configuration options：enable/disable

Default configuration：diable

Function：Whether enable SNTP.

Server address

Configuration format：A.B.C.D

Function：Configure the IP address of the SNTP server, and the client will calibrate time according to the servier's message.

4. Check if the switch time is synchronized with server time.

Click on the navigation tree [system] → [basic information] to view system time information, as shown below.

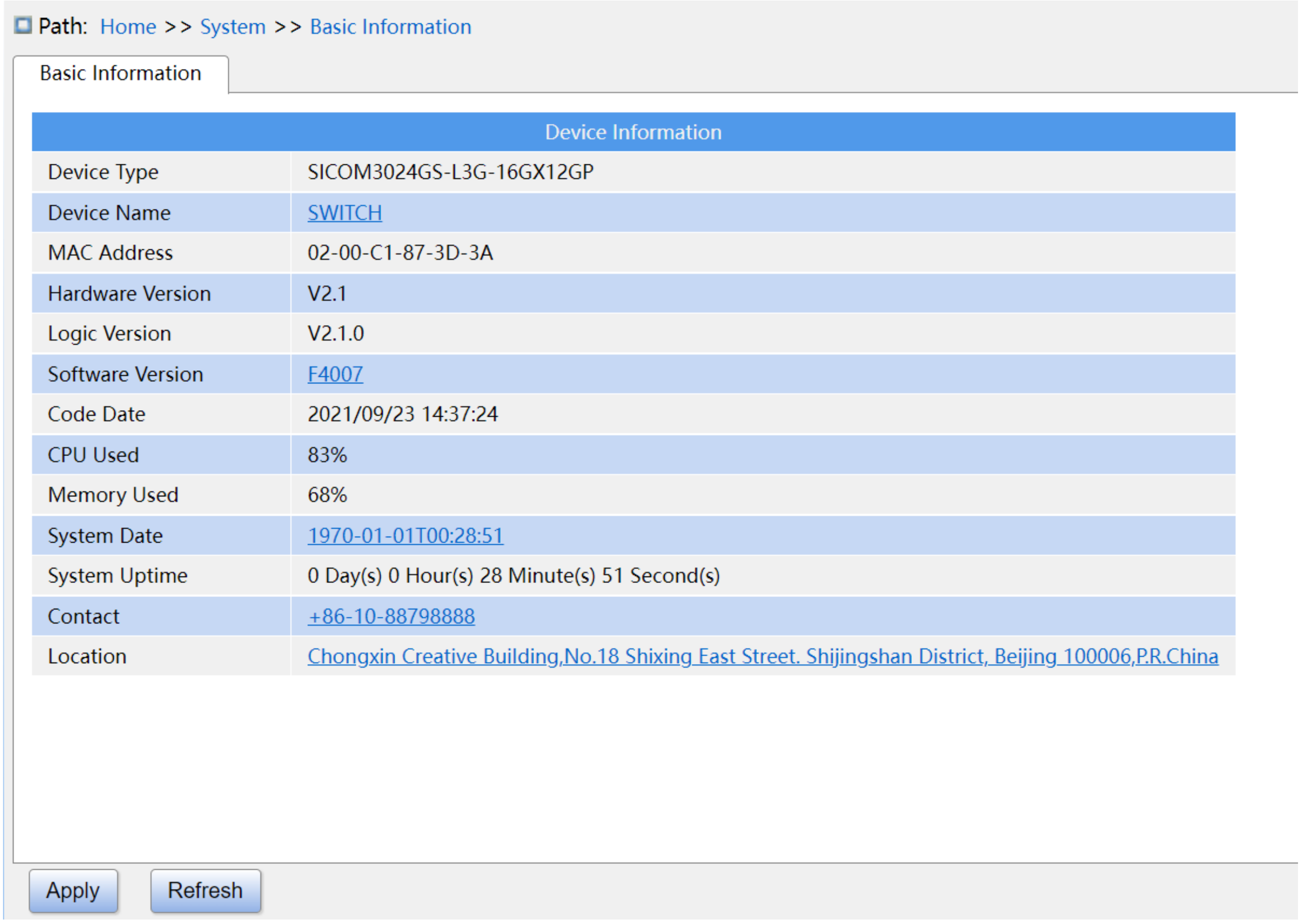


Figure 27 view clock informaton

View switch time information according to server time, time zone and DST configuration.

4.4 Software update

Switches can achieve better performance by upgrading software versions. This series of switch upgrades include boot version upgrade and software version upgrade, first upgrade the boot version then upgrade the software version, only the software version is upgraded when the boot version remains the same. The software version can be upgraded through the Local/FTP/TFTP protocol.

4.4.1 Local update

1. Local upgrade software, as shown below.

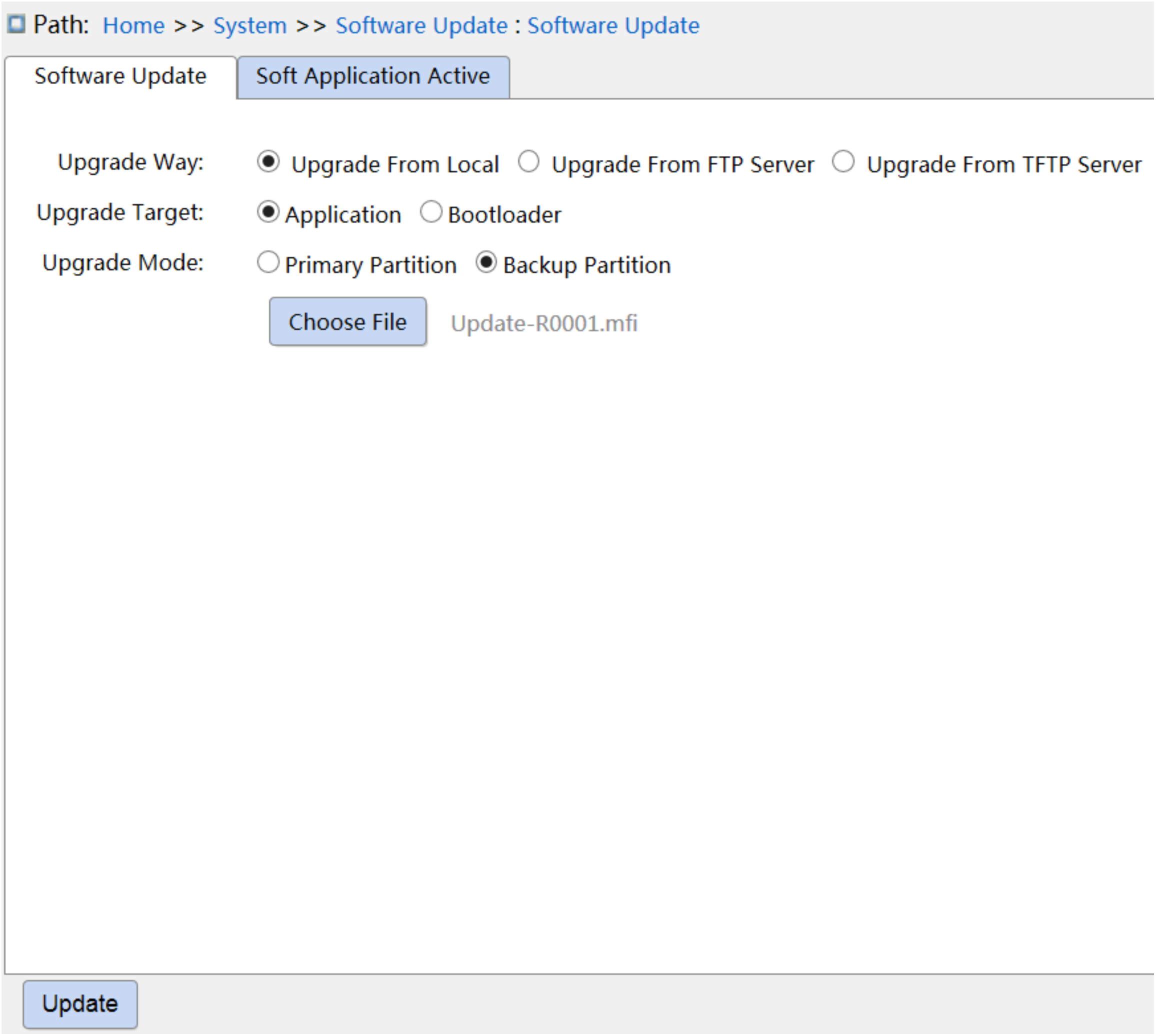


Figure 28 upgrade software-Local

Upgrade way

Configuration options：upgrade from local/upgrade from FTP server/ Upgrade From TFTP Server

Function：select upgrade way.

Upgrade target

Configuration options：software version/Boot version

Function：select upgrade target.

Upgrade mode

Configuration options：primary partition/backup partition

Description：two versions of software can be downloaded, the two versions can be the same or different.

2. After upgrading successfully, as shown in figure 28, activate the software version and

restart the device, then check if the software version is the upgraded version in the system information.

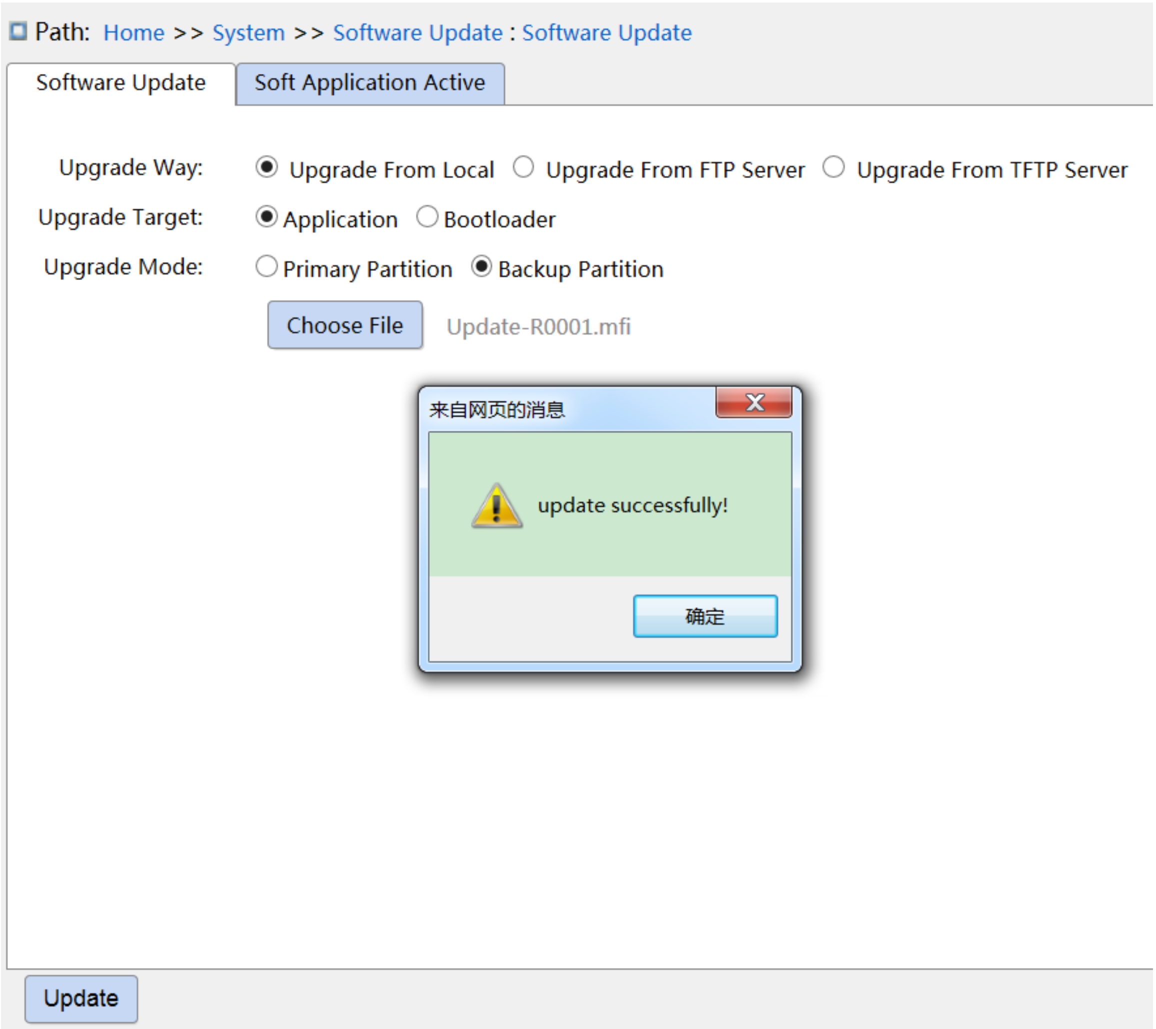


Figure 29 upgrade successfully

Warning:

- After the software upgrade is successful, you must activate the software version and restart the device before the software version can take effect;
- Cannot restart switch after upgrade failure, avoid version file loss and device can not start normally.

4.4.2 FTP upgrade

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 30. Create a user name and password, for example, user name "admin" and password "123". Click <OK>.

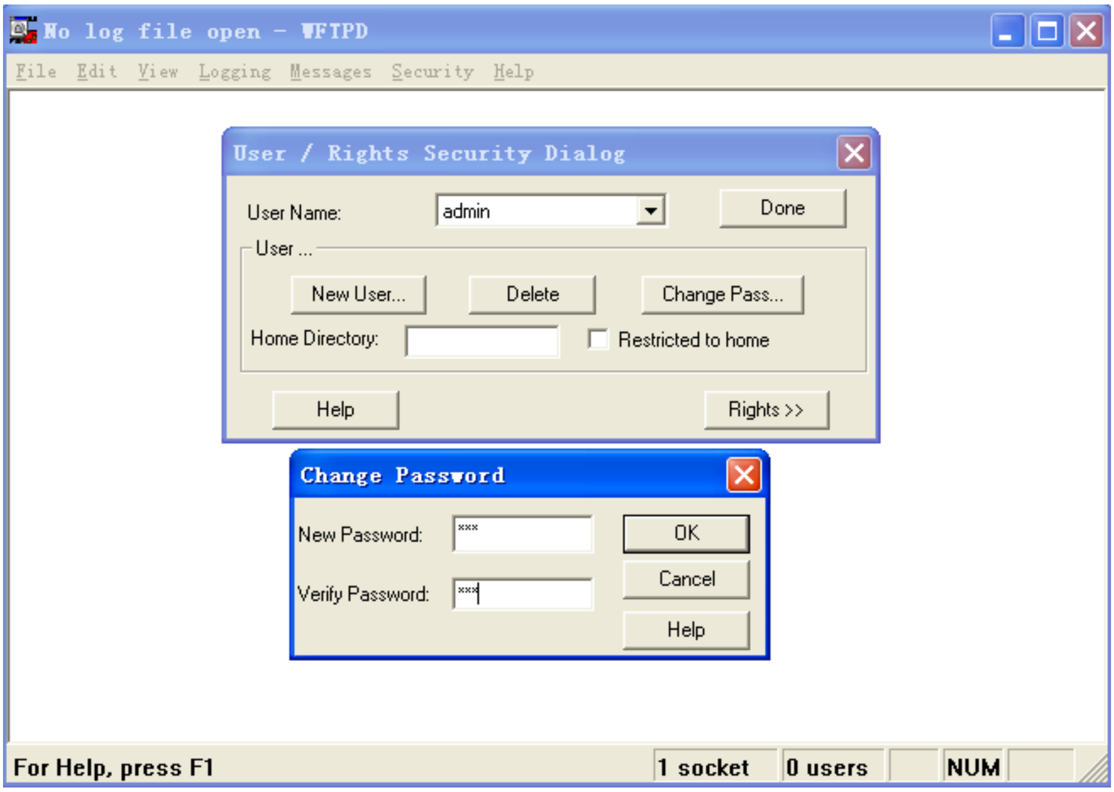


Figure 30 Creating a New FTP User

2. Input the storage path of the update file in "Home Directory", as shown in Figure 31. Click <Done>.

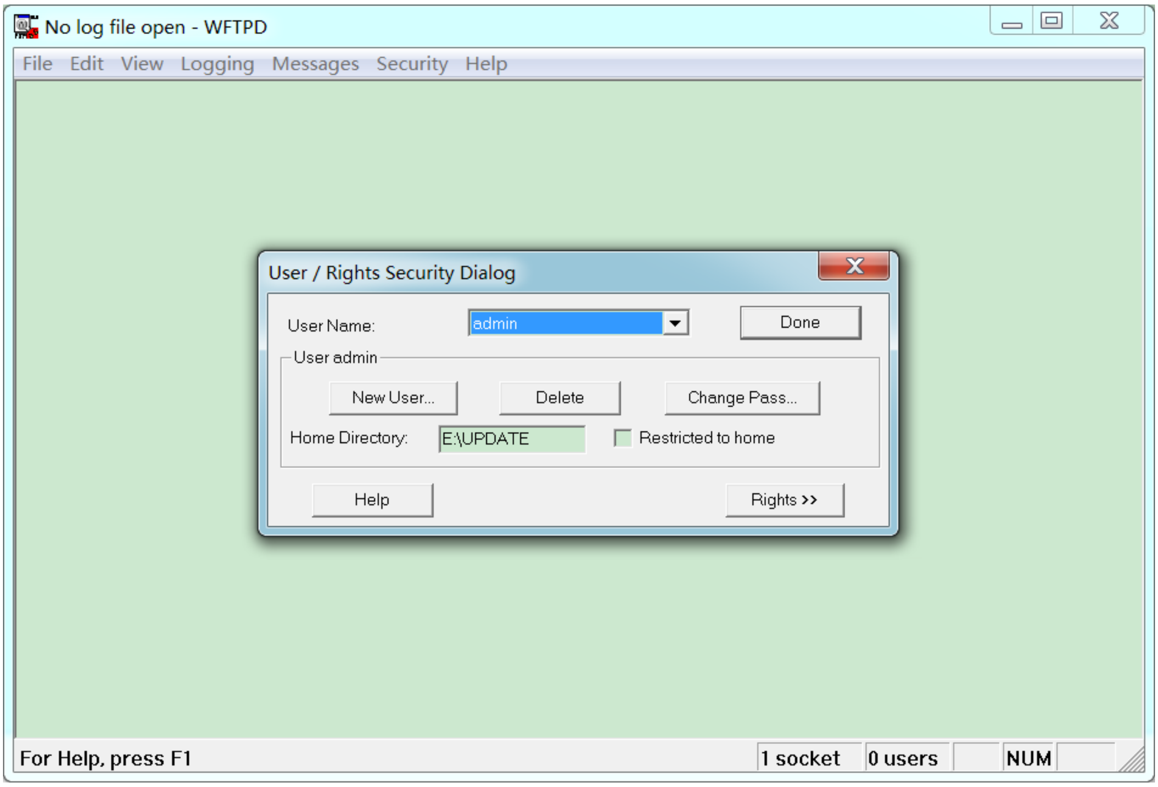


Figure 31 File Location

3. Click [System] → [Software Update] in the navigation tree to enter the software update page, as shown in Figure 32. Enter the IP address of FTP server, FTP user name, password, and file name on the server. Click <Update>.

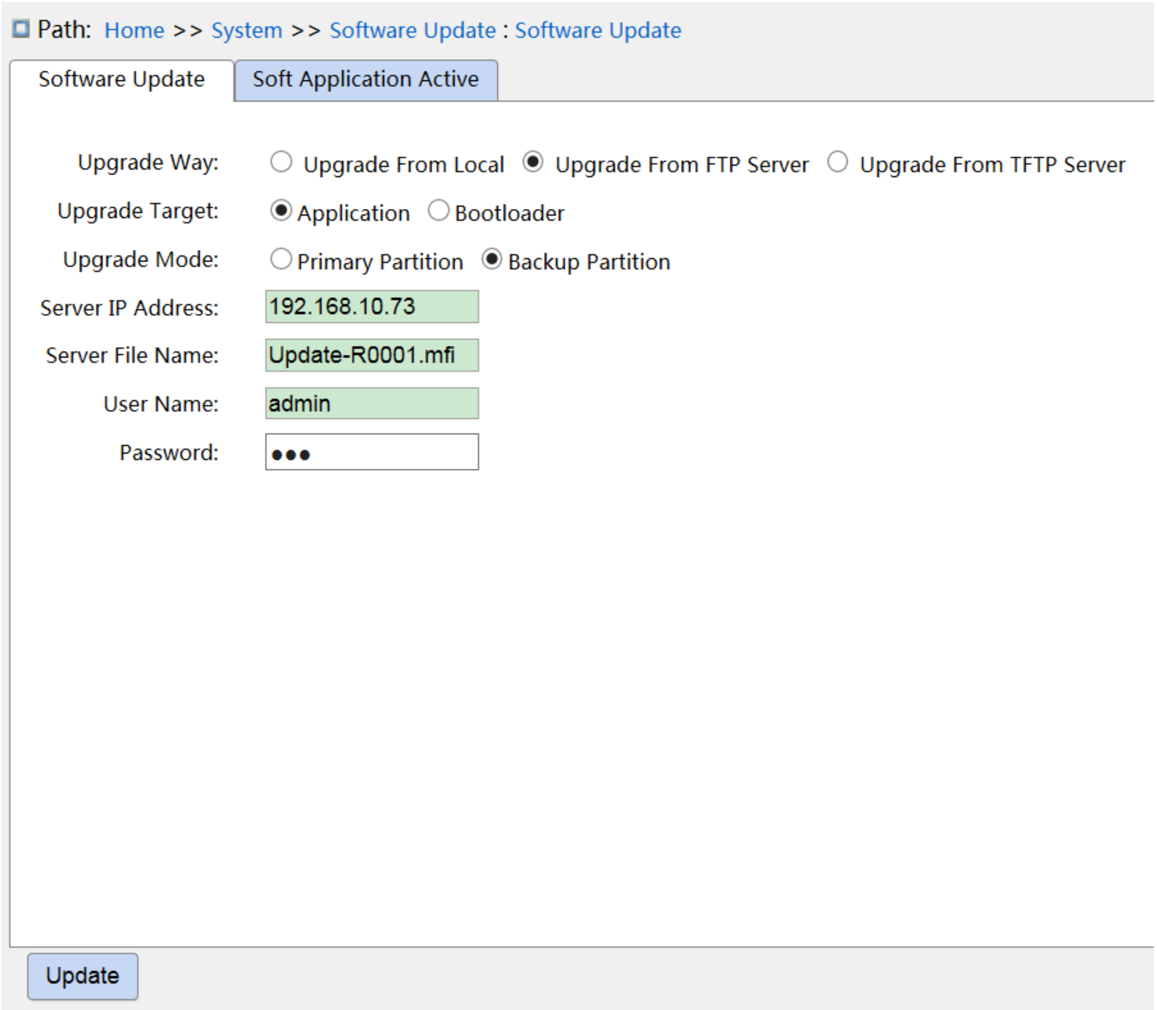


Figure 32 Software Update by FTP

Upgrade Way

Configuration options:Upgrade From Local / Upgrade From FTP Server/ Upgrade From TFTP Server

Explanation: Select upgrade mode

UpgradeTarget

Configuration options: Appication/Bootloader

Function: Select the upgrade target.

Upgrade Mode

Configuration options:Primary Partition/Backup Partition

Description: Two firmware versions can be downloaded to the switch, and they can be the same or different.

Warning:

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

4. Make sure the normal communication between the FTP server and the switch, as shown below.

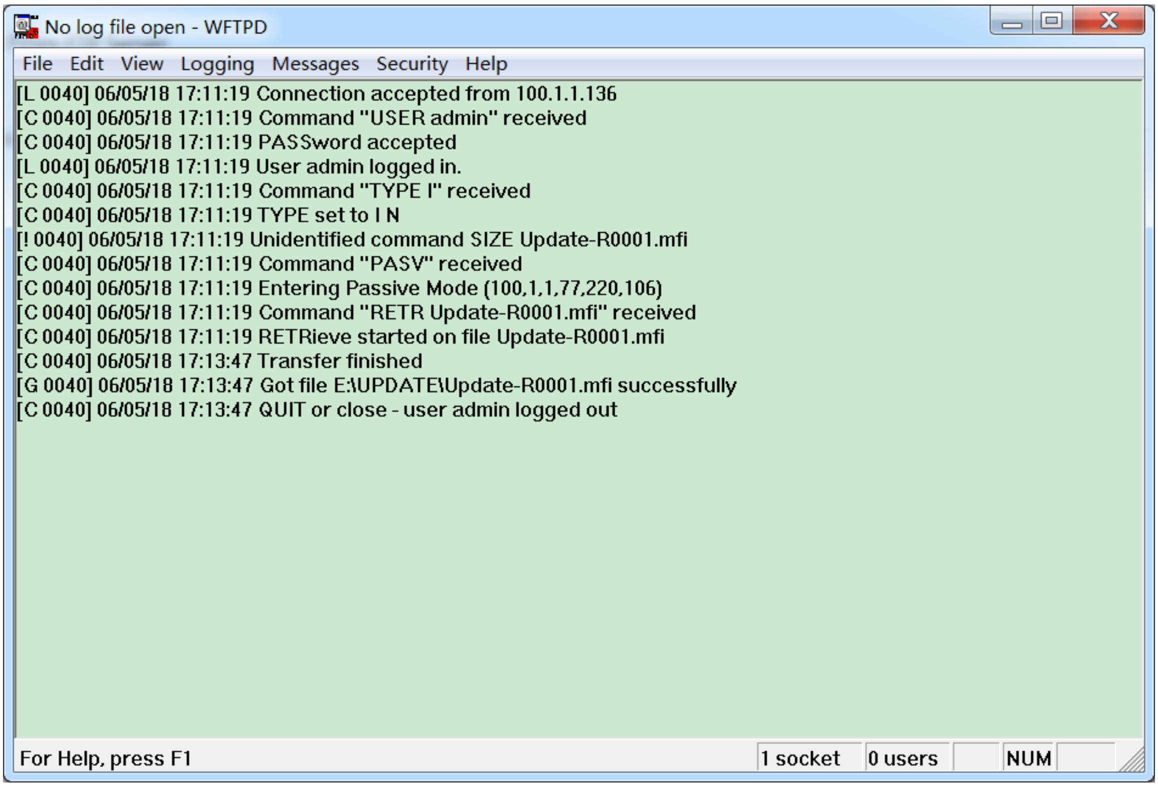


Figure 33 Normal Communication between FTP Server and Switch

Caution:

To display update log information as shown in Figure 33, you need to click [Logging] → [Log Options] in WFTPD and select Enable Logging and the log information to be displayed.

5. Wait for the update to complete, as shown in Figure 34;

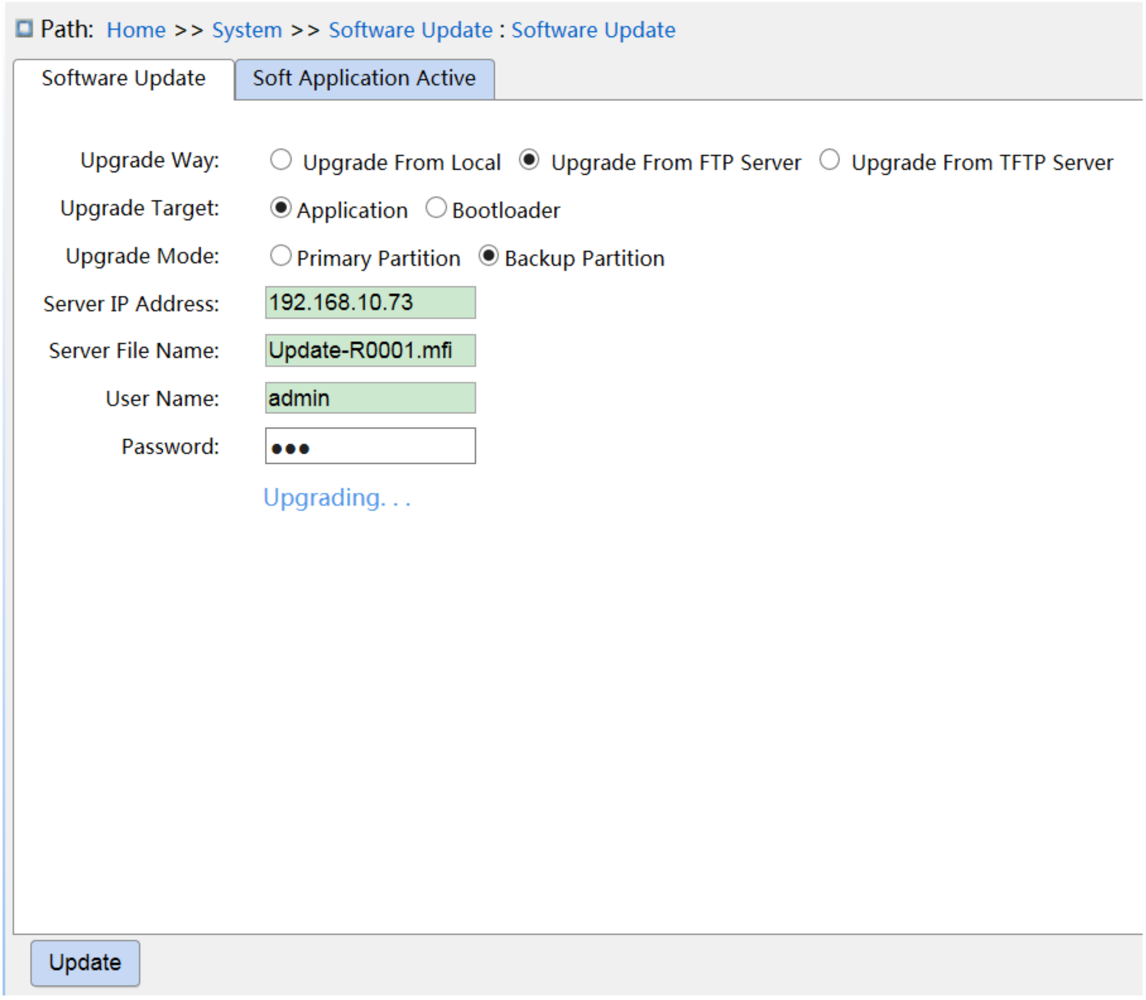


Figure 34 Waiting for the Update to Complete

6. 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 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.

4.4.3 TFTP upgrade

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

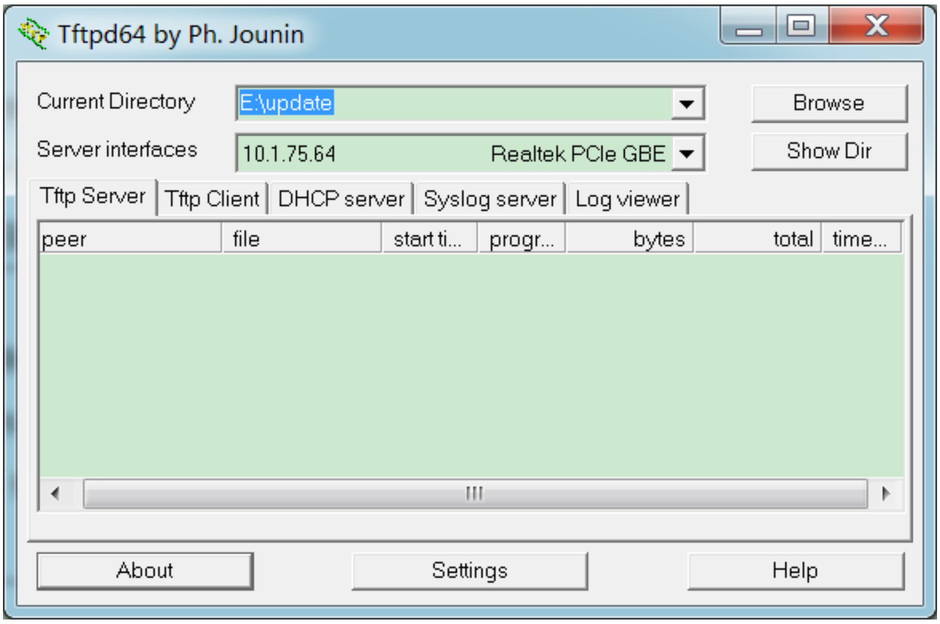


Figure 35 TFTP Server Configuration

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

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

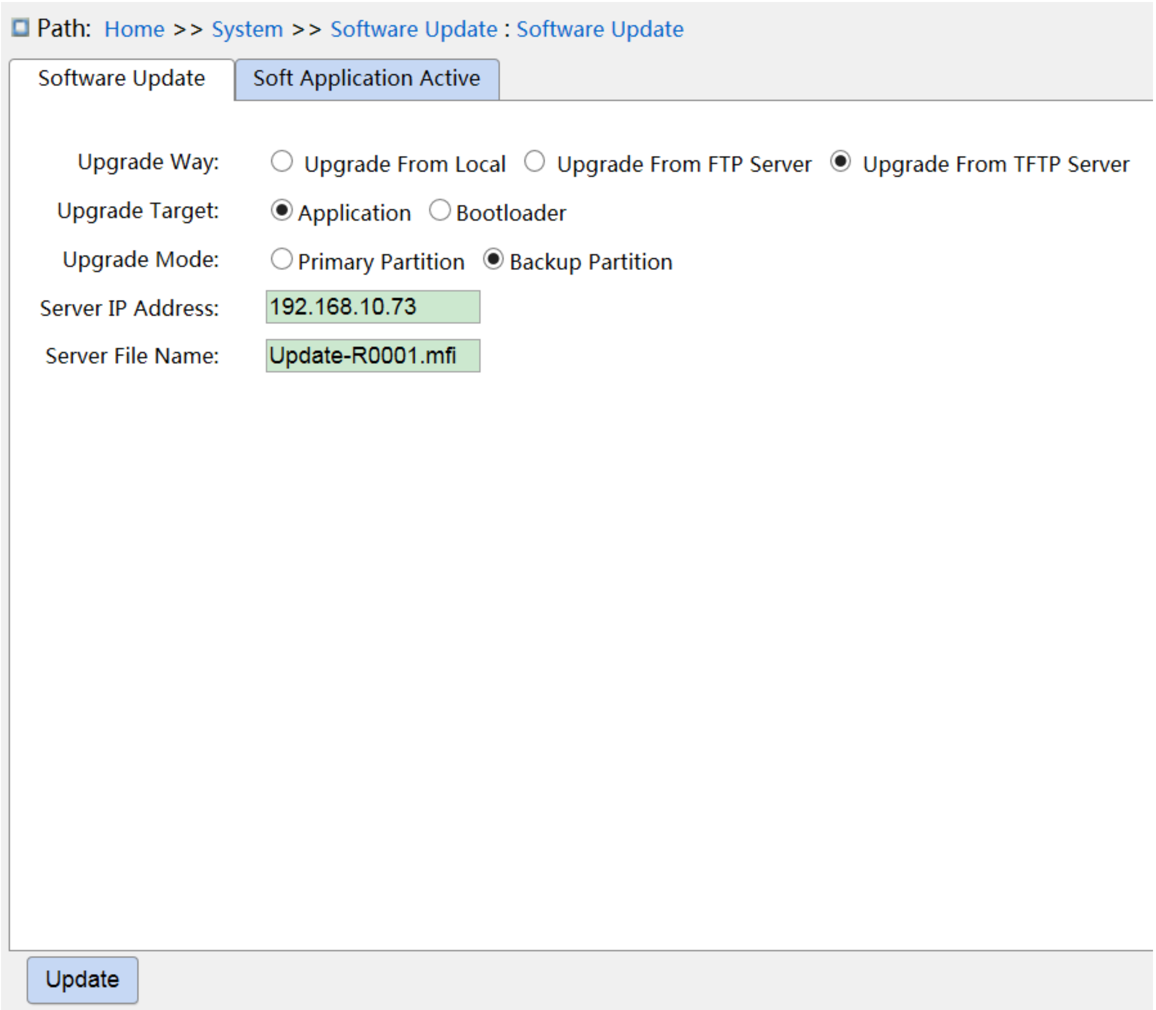


Figure 36 Software Update by TFTP

3. Make sure the normal communication between the TFTP server and the switch, as shown below.

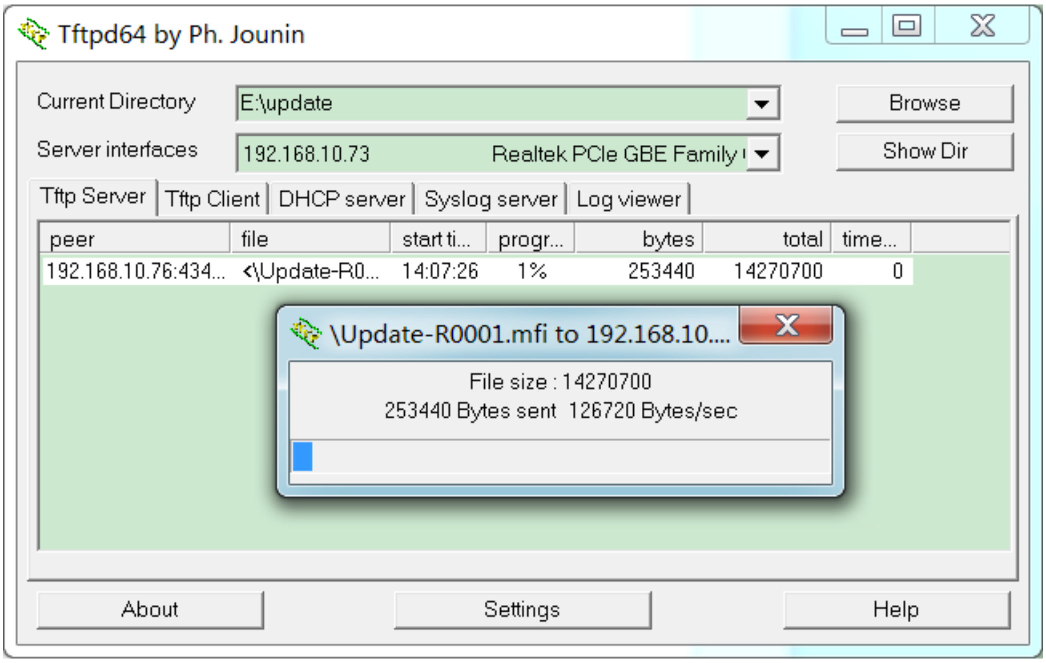


Figure 37 Normal Communication between TFTP Server and Switch

4. Wait for the update to complete, as shown below.

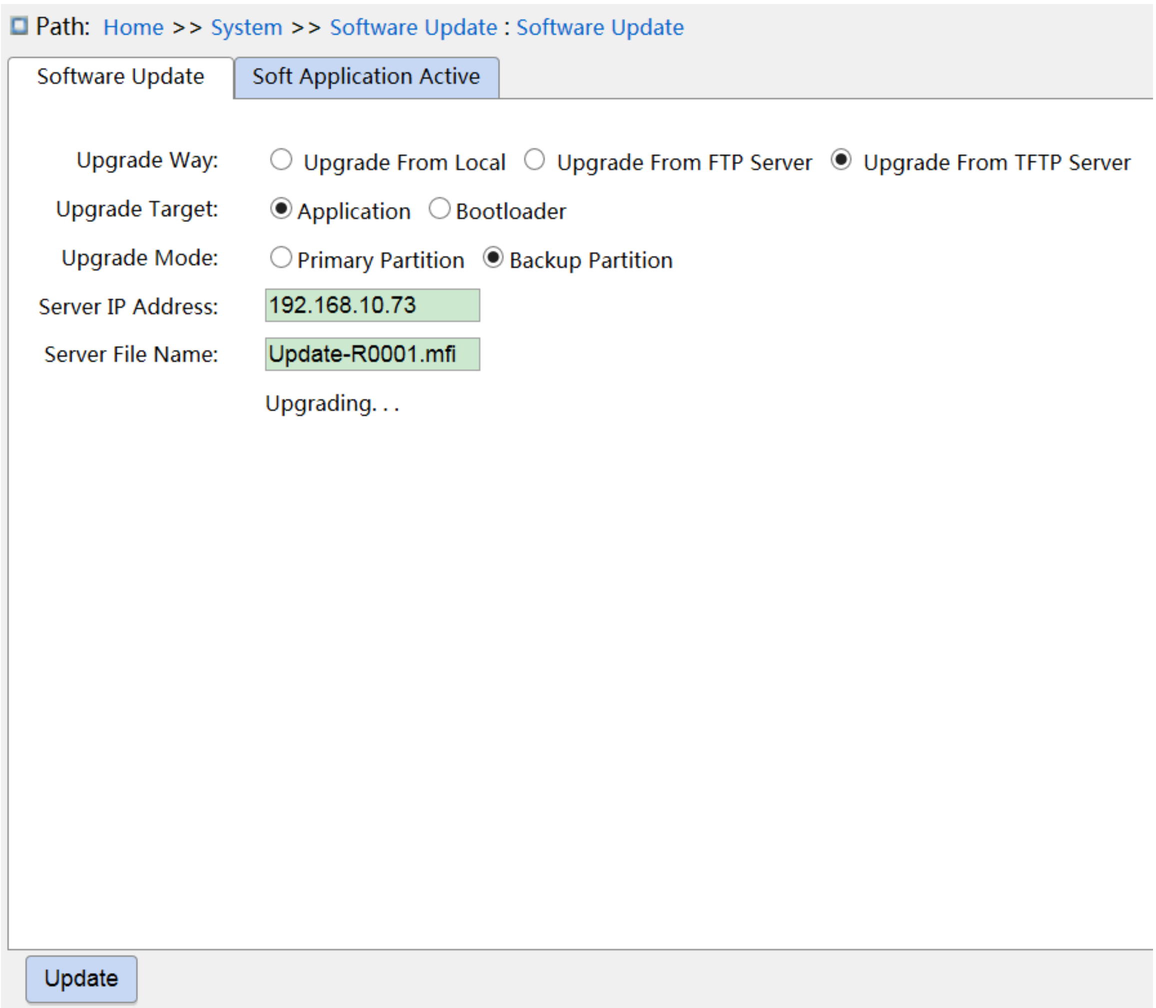


Figure 38 Waiting for Update to Complete

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:

➢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.

4.5 Soft Application Active

Activate the firmware application, as shown in Figure 39.

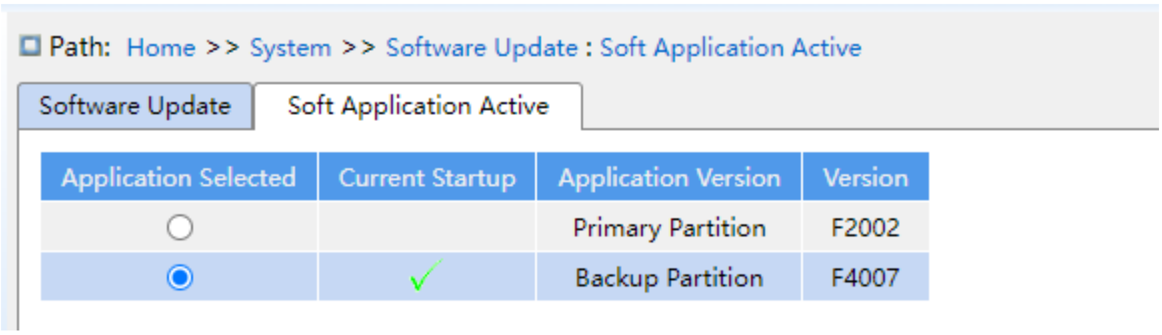


Figure 39 Activate the firmware application

Select one version and click <Apply> button, configuring the version to be active version that is the next startup version. Only one can be active version at a time.

Current Startup indicates the version is current running version.

4.6 Language Update

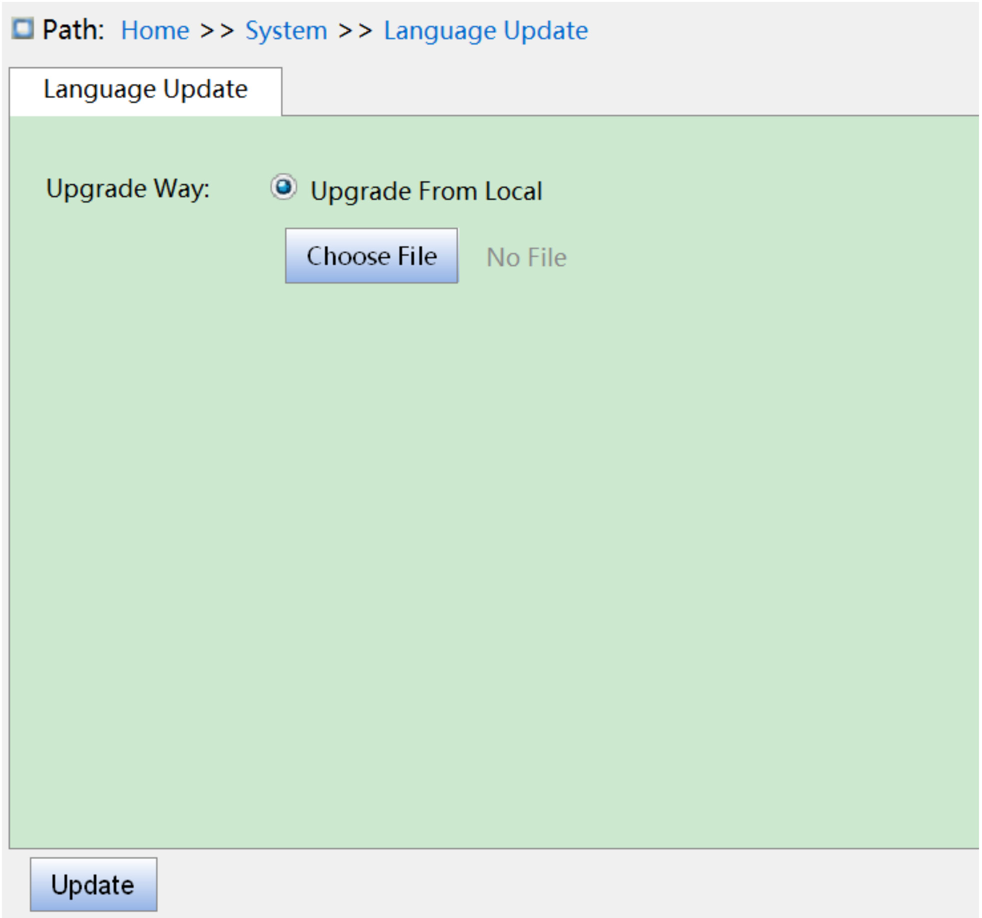


Figure 40 Update language

Upgrade way

Configuration options：upgrade from local

Function ：Download language packs to devices that support multiple language access.

4.7 Restart

Restart device，as shown below.

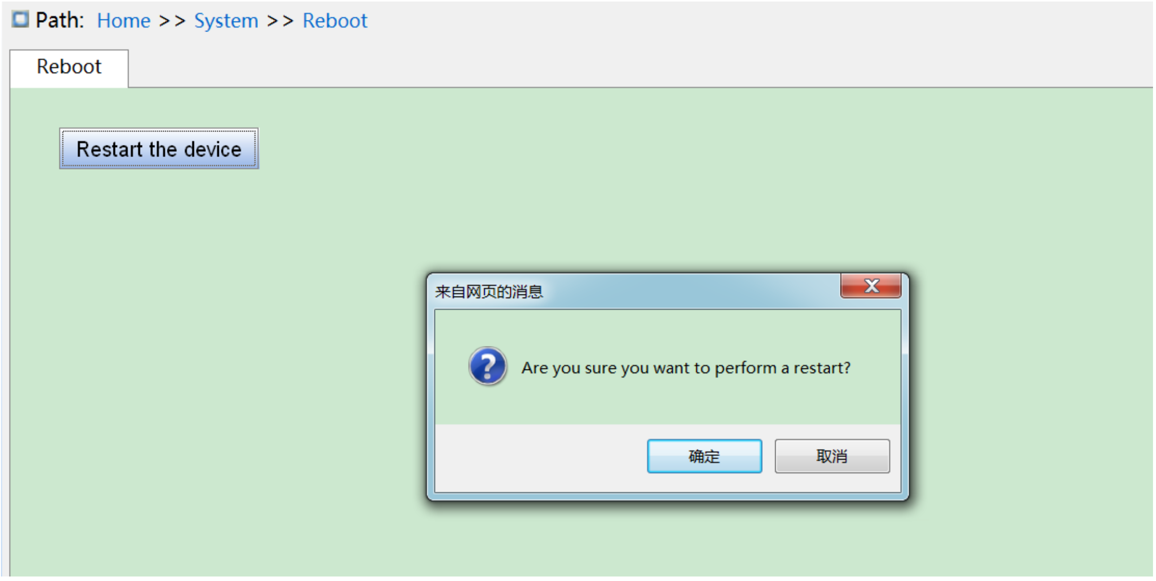


Figure 41 restart device

Before restarting the device, confirm whether save the current configuration, the switch configuration is the latest information after reboot, and if not, the switch configuration will be restored to the factory Default configuration after reboot.

4.8 Abort

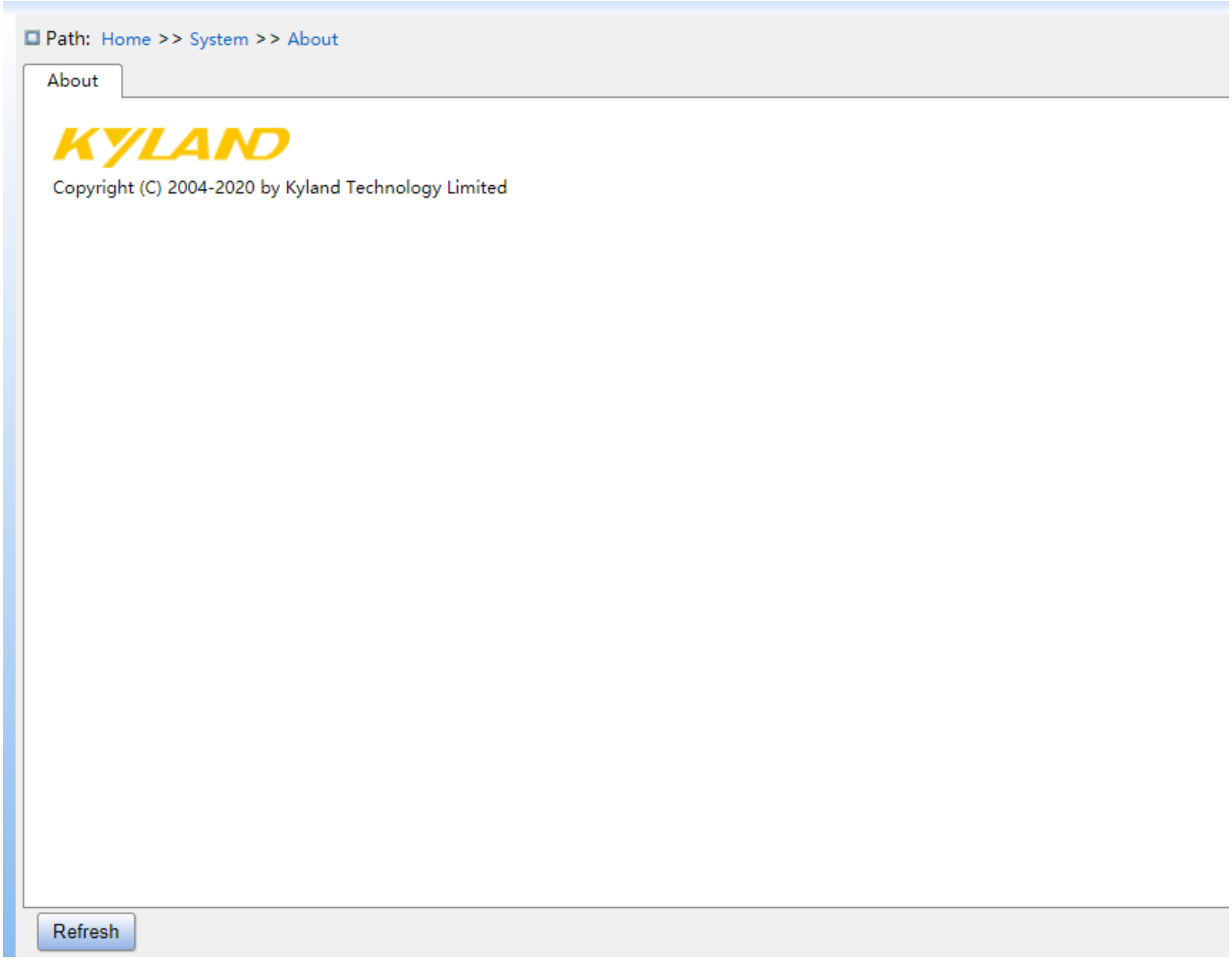


Figure 42 System related information

5 Service

5.1 SSL Configuration

5.1.1 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.

5.1.2 Web Configuration

1. Enable HTTPS, as shown below.

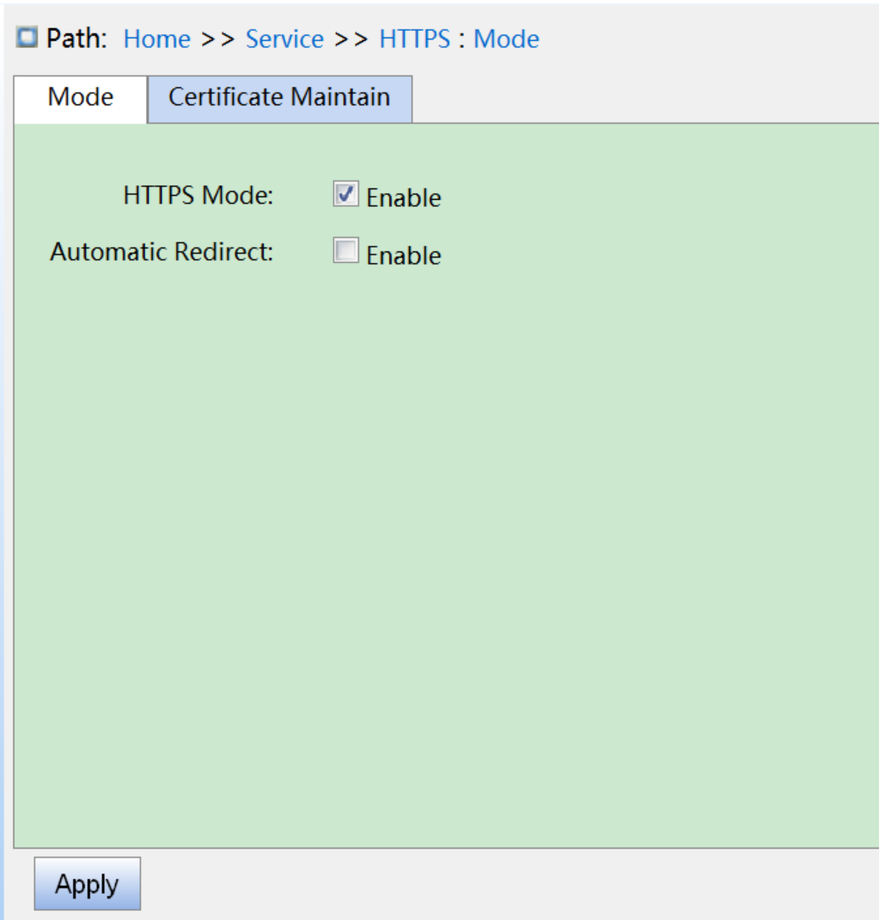


Figure 43 Enable HTTPS

HTTPS Mode

Configuration options: Enable /Disable

Default configuration：Disable

Function：enable or disable HTTPS, if enable，login in the switch Web infterface via http://*ip address* and secure link https://*ip address*.

Automatic redirection

Configuration options：Enable /Disable

Default configuration：Disable

Function：if enable, only secure link https://ip address is allowed to login switch web pages. If disable, the switch web page can be login via http and https. The automatic redirect parameter only can be configured when the https status is enable.

2. Certificate management, as shown below.

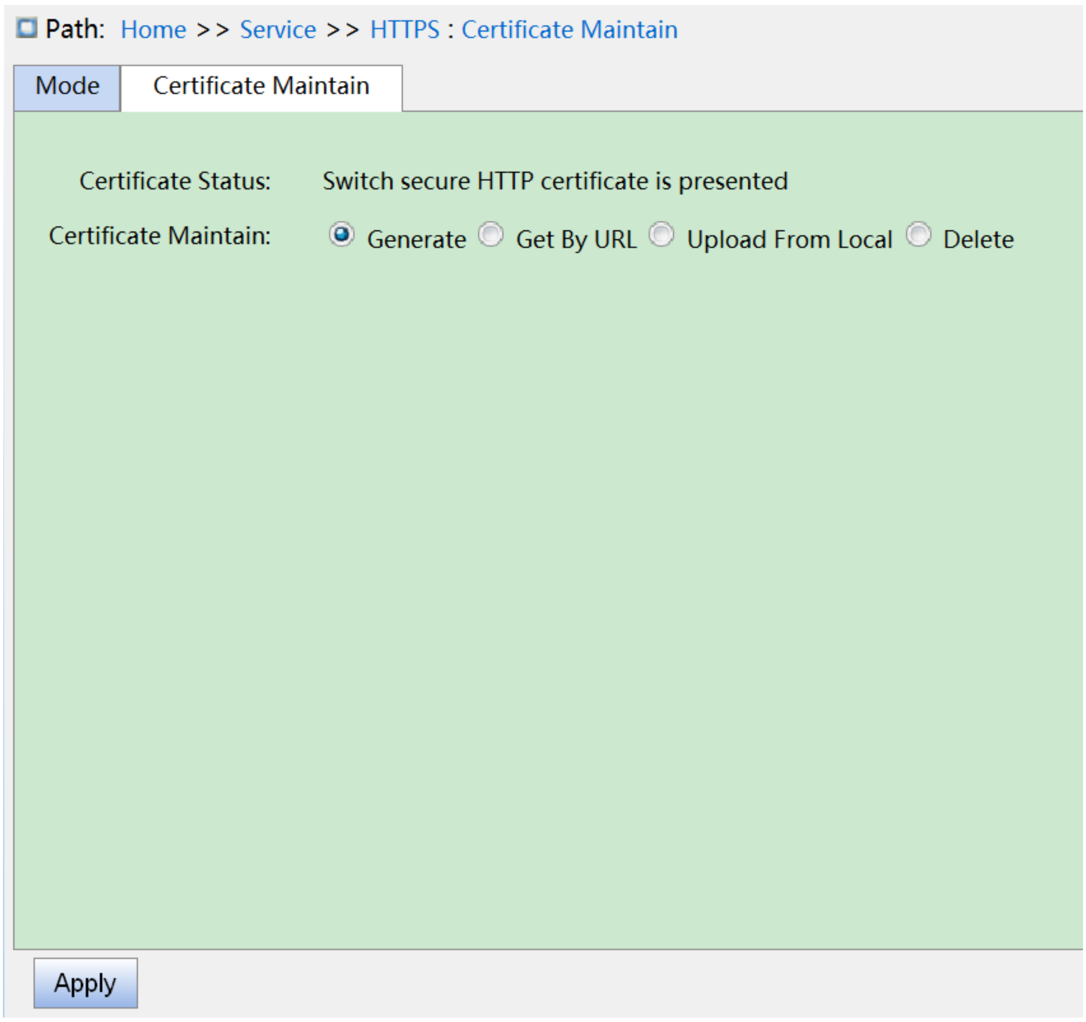


Figure 44 Generate certificate

Maintain

Configuration options：Generate/Get by URL/Upload from local/Delete

Function：select upload mode of certificate

Get certifictate by URL

URL

Function：set web path such as https://10.10.10.10:80/new_image_path/new_image.dat

Upload from local

Select file

Function: select HTTPS certificates file from local.

5.2 SNMP v1/SNMP v2c

5.2.1 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.

5.2.2 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.

5.2.3 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.

5.2.4 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 45 shows the relationships among the NMS, agent, and MIB.

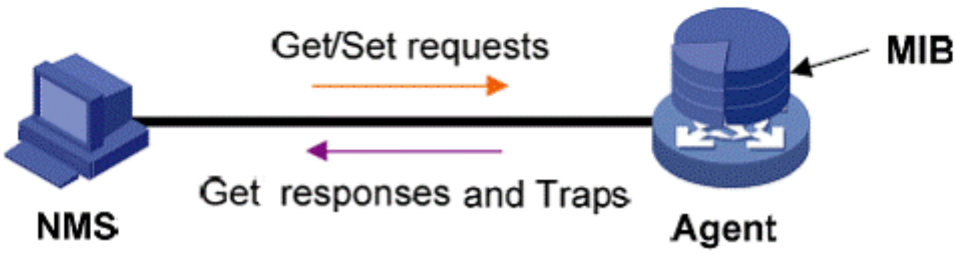


Figure 45 Relationship among NMS, Agent, and MIB

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 46, the OID of object A is 1.2.1.1.

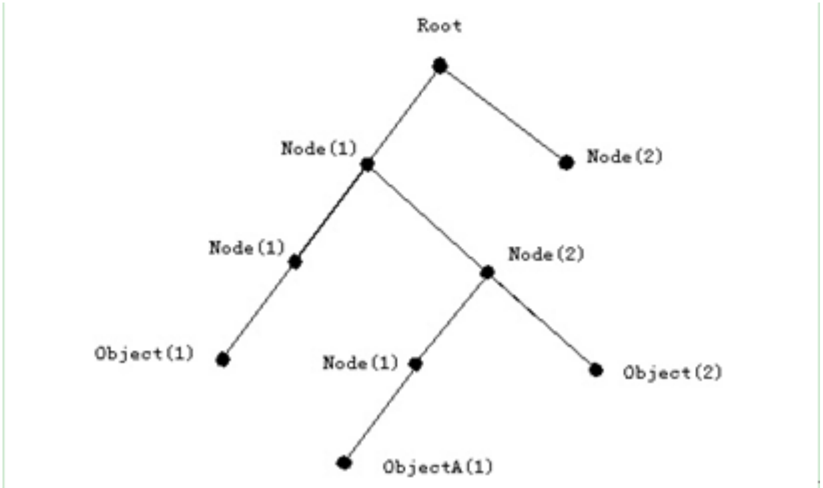


Figure 46 MIB Structure

5.2.5 Web Configuration

1. Enable SNMP, as shown below.

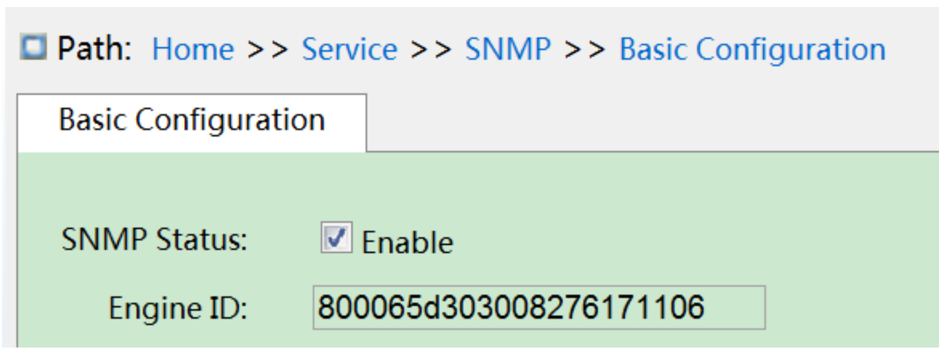


Figure 47 Enable SNMP

SNMP status

Configuration options：Enable/Disable

Default configuration：Enable

Function：Enable or disable SNMP.

Engine ID

Configuration range：hexadecimal number is even, can not be all 0 or F, the value range of even number is10~64.

Function：Configure SNMP v3 system engine ID, the user corresponding to the device ID in the user table will be clear when the eigine ID is modified.

2. Configure Community, as shown below.

Figure 48 Configure Community

Community

Configration range: 1~32 charactercs

Function: configure the community of switch.

Description: The MIB library information of the switch can only be accessed when the community name in the snmp message is consistent with the community string.

Note: up 16 community strings can be configured.

Access Prority

Configuration options: Read Only/Read And Write

Default configuration: Read Only.

Function: configure the access priority of MIB library.

Description: the MIB library information only can be ready with read-only permissions; the MIB library information can be read with read and write permissions.

3. Configure trap, as shown below.

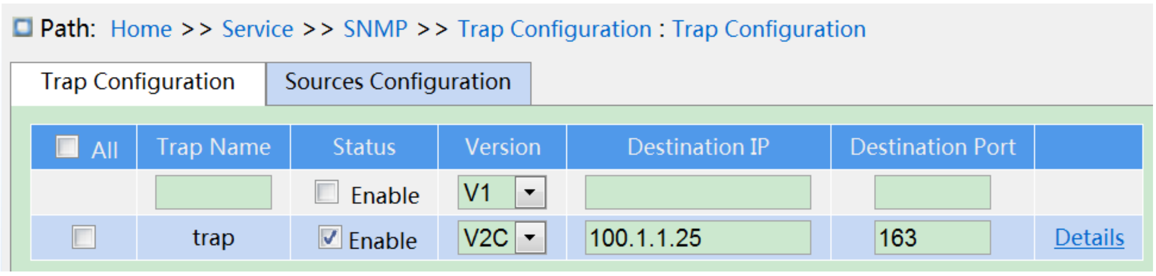


Figure 49 Configure trap

Trap name

Configuration range: 1~32 charactercs

Function: configure trap name.

status

Configuration options: enable/disable

Default configuration: diable

Function: enable or disable trap, the switch sends the corresponding trap message to the server if enable.

Version

Configuration options: SNMP v1/SNMP v2c/SNMP v3

Default configuration: SNMP v1

Function: configurate the trap meassage version number that the switch sends to the server.

Destination IP

Configuration format: A.B.C.D

Function: Configure the server address where the trap message is received.

Destination Port

Configuration range: 1~65535

Default configuration: 162

Function: Configure the port number that sends the trap message.

4. Click on the trap configuration item details to see the trap configuration details, as shown below.

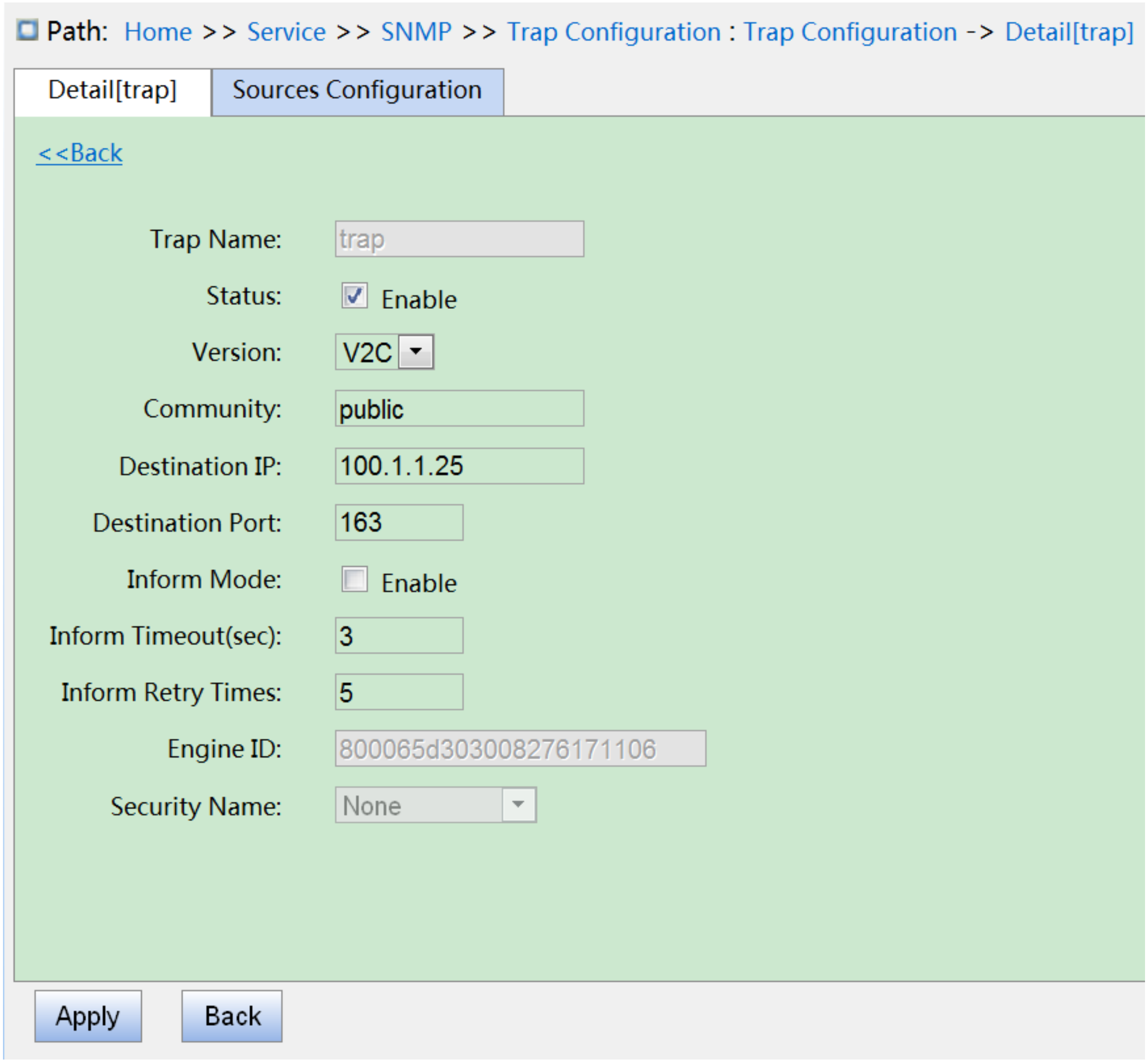


Figure 50 trap detail information

Community

Configuration range: 0~255 charactercs

Default configuration: public

Function: Configure the community name that is carried in the sending trap message.

Inform Mode

Configuration options: enable/disable

Default configuration: disable

Function: Whether the server sends a reply message to the switch after receiving the trap message.

Inform Timeout

Configuration range: 0~2147s

Default configuration: 3s

Function: Configure the trap message sending timeout; after the switch sends the trap message, if no response from the server within that time, resend the trap message.

Inform retry Times

Configuration range: 0~255

Default configuration: 5

Function: Configure the number of times the trap message is timed out. If the cumulative number of sending times exceeds the configuration value, the server still does not reply, then the trap message sends failed.

5. Configure trap event, as shown below.

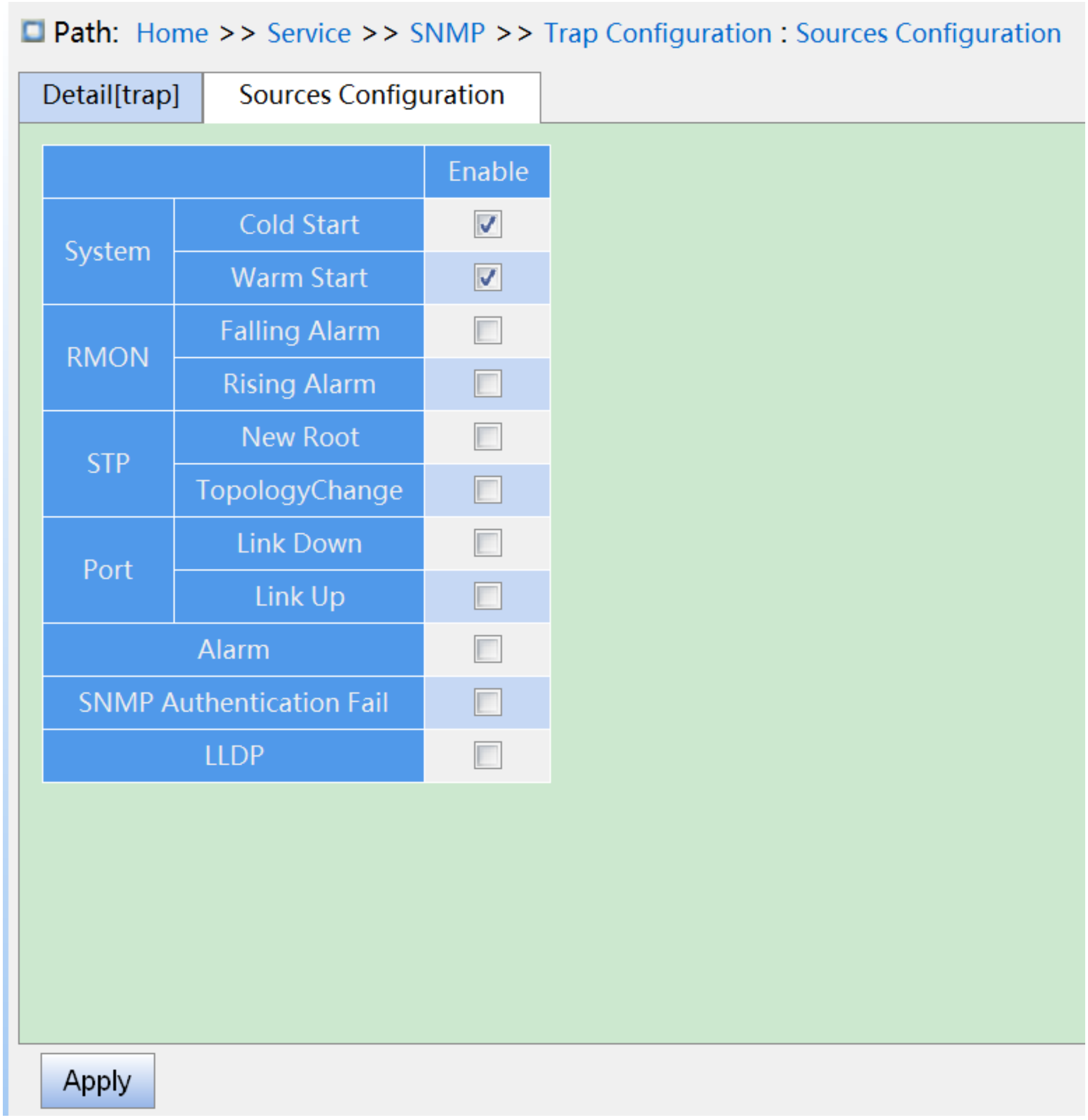


Figure 51 trap source configuration

System warm start/cold start

Configuration options: enable/disable

Default configuration: diable

Function: Whether to send trap message when the system is warm start / cold start.c

RMON falling alarm/rising alarm

Configuration options: enable/disable

Default configuration: diable

Function: Whether to send a trap message when the RMON generates afaulling alarm / rising alarm.

STP new root/ topology change

Configuration options: enable/disable

Default configuration: diable

Function: Whether to send the trap message when the state of STP changes.

Port link up/down

Configuration options: enable/disable

Default configuration: diable

Function: Whether to send trap message of port up/down when port status changes.

Alarm

Configuration options: enable/disable

Default configuration: diable

Function: When there is alarm information, whether to send trap message.

SNMP authentication fail

Configuration options: enable/disable

Default configuration: diable

Function: If snmp authentication fails, whether to send trap message.

LLDP

Configuration options: enable/disable

Default configuration: diable

Function: Whether to send LLDP trap message when the neighbor status changes.

5.2.6 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 52.

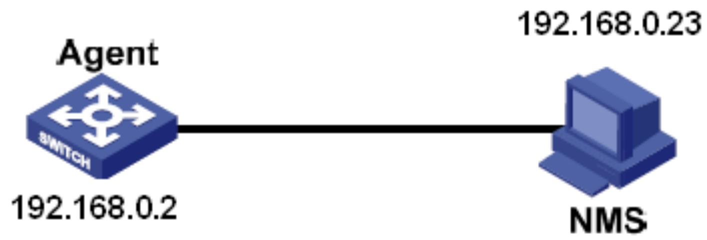


Figure 52 SNMP v2c Configuration Example

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 47、Figure 48.
2. Configure global trap mode, as shown in Figure 49.
3. Create trap entry 111, enable trap mode; set the trap version to SNMP v2c, destination IP address to 192.168.0.23. Select system, interface, authentication, and switch all trap events, and adopt default settings for the other parameters, as shown in Figure 50、Figure 51.

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*.

5.3 SNMPv3

5.3.1 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.

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.

5.3.2 Implementation

SNMP v3 provides four configuration tables. Each table can contain 16 entries. These tables determine whether specific users can access MIB information.

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

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

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

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

5.3.3 Web Configuration

1. Enable SNMP, as shown below.

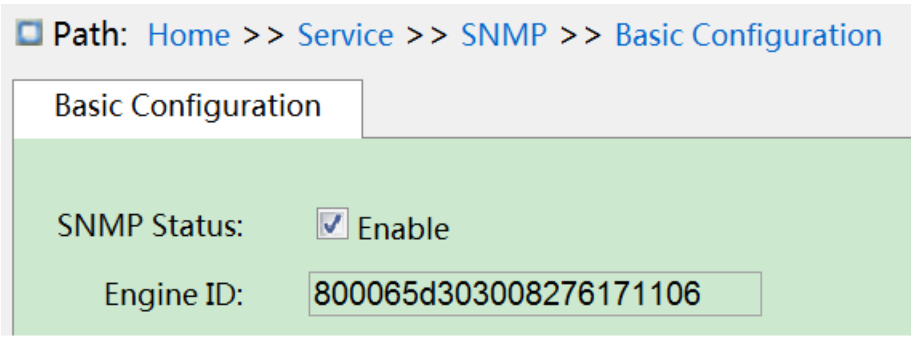


Figure 53 enable SNMP

SNMP Status

Configuration options: enable/disable

Default configuration: diable

Function: enable or disable SNMP.

Engine ID

Configuration range: hexadecimal number is even, can not be all 0 or F, the value range of even number is 10~64.

Function: Configure SNMP v3 system engine ID, the user corresponding to the device ID in the user table will be clear when the eigine ID is modified.

2. Configure trap, as shown below.

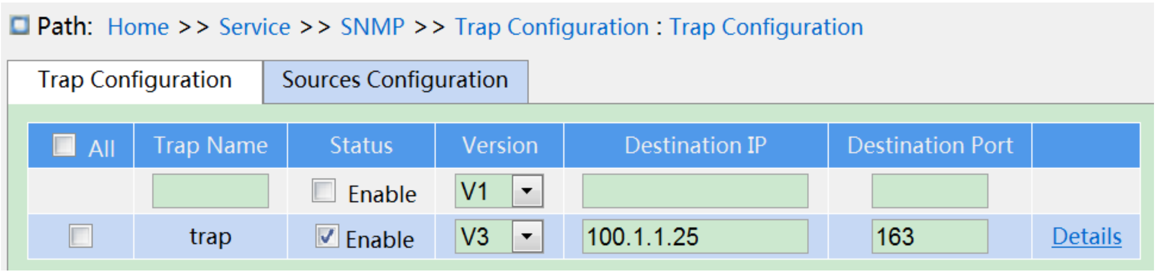


Figure 54 Configure Trap

Trap name

Configuration range: 1~32 charactercs

Function: configure trap name.

Status

Configuration options: enable/disable

Default configuration: diable

Function: enable or disable trap, the switch sends the corresponding trap message to the server if enable.

Version

Configuration options: SNMP v1/SNMP v2c/SNMP v3

Default configuration: SNMP v1

Function: configurate the trap meassage version number that the switch sends to the server.

Destination IP

Configuration format: A.B.C.D

Function: Configure the server address where the trap message is received.

Destination port

Configuration range: 1~65535

Default configuration: 162

Function: Configure the port number that sends the trap message.

3. Click on the trap configuration item details to see the trap configuration details, as shown

below.

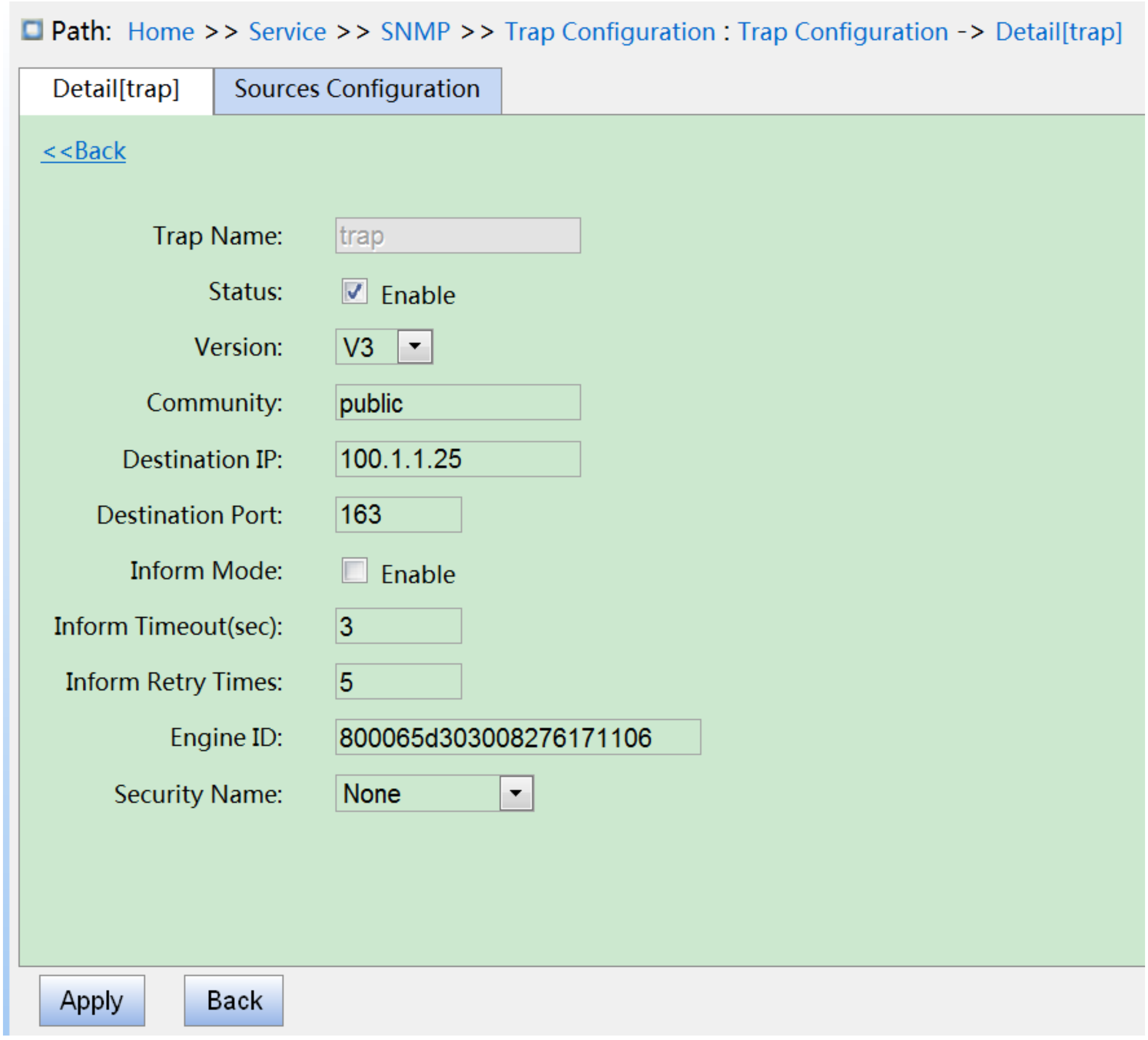


Figure 55 trap detail information

Community

Configuration range: 0~255 charactercs

Default configuration: public

Function: Configure the community name that is carried in the sending trap message.

Inform Mode

Configuration options: enable/disable

Default configuration: disable

Function: Whether the server sends a reply message to the switch after receiving the trap message.

Inform Timeout

Configuration range: 0~2147s

Default configuration: 3s

Function: Configure the trap message sending timeout; after the switch sends the trap message, if no response from the server within that time, resend the trap message.

Inform Retry Times

Configuration range: 0~255

Default configuration: 5

Function: Configure the number of times the trap message is timed out. If the cumulative number of sending times exceeds the configuration value, the server still does not reply, then the trap message sends failed.

Engine ID

Configuration range: hexadecimal number is even, can not be all 0 or F, the value range of even number is 10~64.

Function: Configure the security engine ID value which is carried in the SNMP v3 trap message.

4. Configure trap event, as shown below.

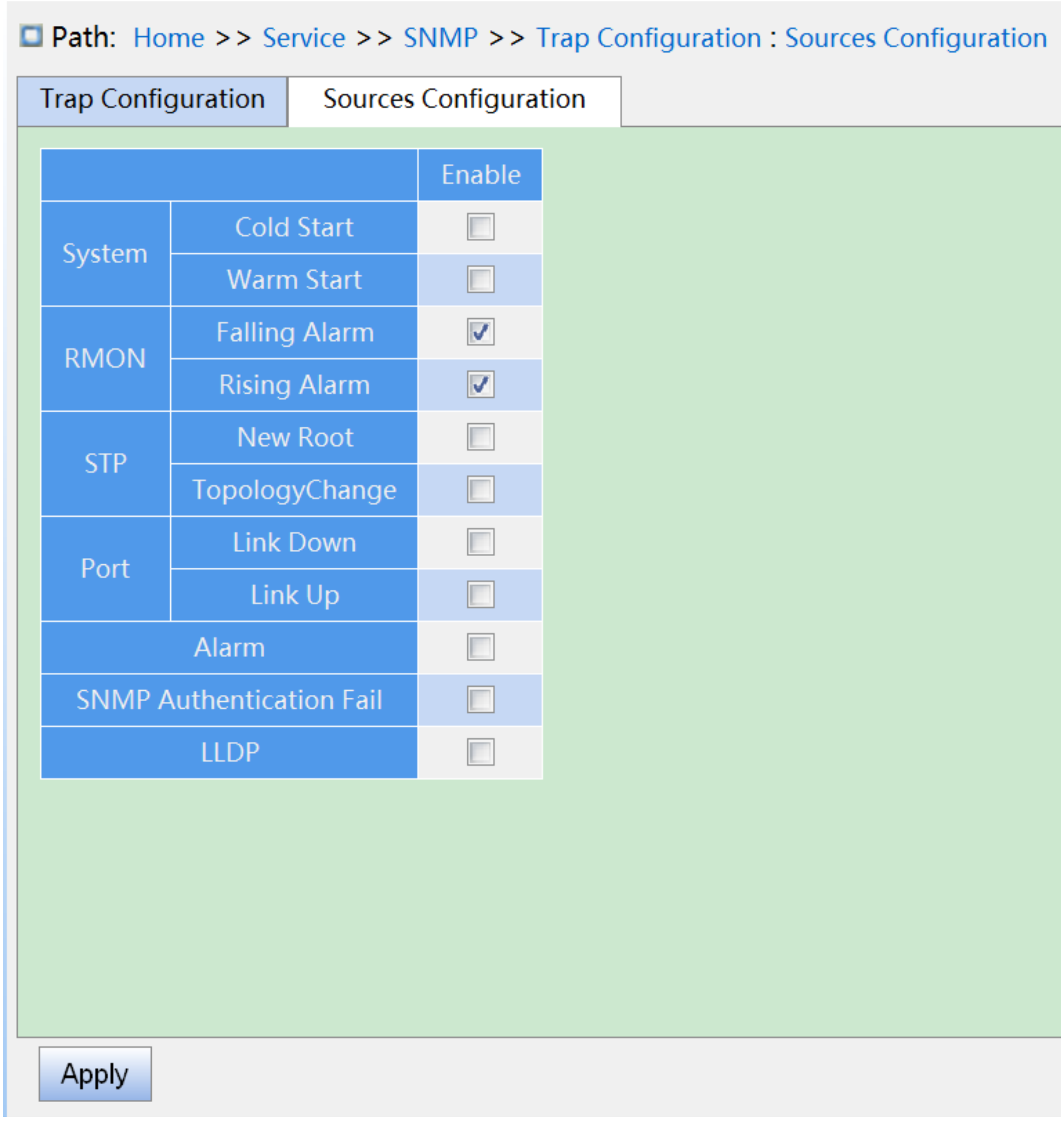


Figure 56 trap source configuration

System warm start/cold start

Configuration options: enable/disable

Default configuration: diable

Function: Whether to send trap message when the system is warm start / cold start.c

RMON falling alarm/rising alarm

Configuration options: enable/disable

Default configuration: diable

Function: Whether to send a trap message when the RMON generates afaulling alarm / rising alarm.

STP new root/ topology change

Configuration options: enable/disable

Default configuration: diable

Function: Whether to send the trap message when the state of STP changes.

Port link up/down

Configuration options: enable/disable

Default configuration: diable

Function: Whether to send trap message of port up/down when port status changes.

Alarm

Configuration options: enable/disable

Default configuration: diable

Function: When there is alarm information, whether to send trap message.

SNMP authentication fail

Configuration options: enable/disable

Default configuration: diable

Function: If snmp authentication fails, whether to send trap message.

LLDP

Configuration options: enable/disable

Default configuration: diable

Function: Whether to send LLDP trap message when the neighbor status changes.

5. Configure user name table, as shown below.

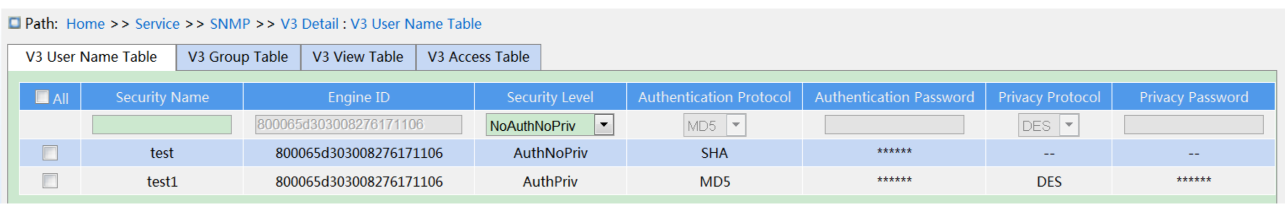


Figure 57 configure SNMPv3 user name table

Security Name

Configuration range: 1~32 characters

Function: Create user name.

Engine ID

Configuration range：hexadecimal number is even, can not be all 0 or F, the value range of even number is10~64.

Function: Configure the security engine ID value which is carried in the SNMP v3 trap message.

Security Level

Configuration options: NoAuthNoPriv/AuthNoPriv/AuthPriv

Function: Configure the security level of the current user.

Description: NoAuthNoPriv requires neither authentication nor encryption, AuthNoPriv need to authenticate but not to encrypt, AuthPriv requires both authentication and encryption.

Authentication Protocol

Configuration options: MD5/SHA

Function: Select an authentication protocol. When selecting authnopriv/authpriv at the security level, you need to configure the authentication protocol and authentication password.

Authentication Password

Configuration range: 8~40 characters（MD5 protocol）8~32 characters（SHA protocol）

Function: Create authentication password.

Privacy Protocol

Configuration options: DES/AES

Function: Select a privacy protocol. The privacy protocol and password need to be configured when selecting Auth, Priv at the security level.

Privacy Password

Configuration range: 8~32 characters

Function: Create privacy password.

Up 16 users can be configured.

5. Configure group table, as shown below.

Figure 58 Configure SNMPv3 group table

Group name

Configuration range: 1~32 characters

Function: configure the name of group table, the users with the same group name belong to the same group.

Security model

Default configuration: SNMP v3

Function: Select the security model of current group （that is SNMP version number）, SNMPv3 use USM（security model based on user）technology, This option force on the SNMP V3 model currently.

Security name

Configuration range: Created user name, 1~32 characters

Function: configure security name, the security name should match the user name in the user table. Users with the same group name belong to the same group.

Up 32 group tables can be configured.

6. Configure view table, as shown below.

Figure 59 Configure SNMPv3 view table

View Name

Configuration range: 1~32 characters

Function: Configurate view name.

View Type

Configuration options: included/excluded

Function: Included indicates that the current view includse all the nodes of the MIB subtree, excluded indicates that the current view does not include any nodes of the MIB subtree.

OID subnode

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

Up 16 view tables can be configured.

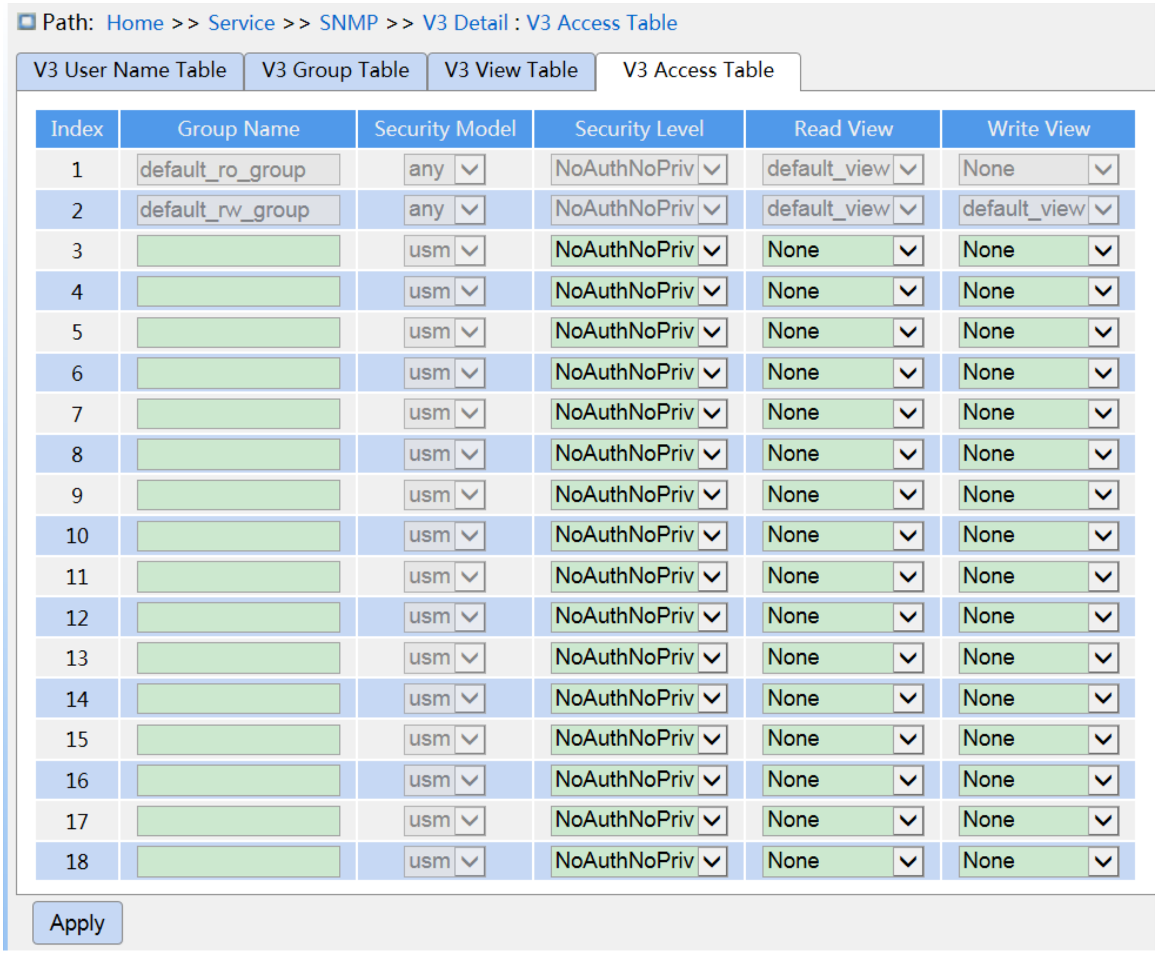
NOTE

Note:

The view table by default in the switch default_view include all nodes of a subtree.

---

7. Configure access table, as shown below.



Path: Home >> Service >> SNMP >> V3 Detail : V3 Access Table

V3 User Name Table | V3 Group Table | V3 View Table | V3 Access Table

Index	Group Name	Security Model	Security Level	Read View	Write View
1	default_ro_group	any	NoAuthNoPriv	default_view	None
2	default_rw_group	any	NoAuthNoPriv	default_view	default_view
3		usm	NoAuthNoPriv	None	None
4		usm	NoAuthNoPriv	None	None
5		usm	NoAuthNoPriv	None	None
6		usm	NoAuthNoPriv	None	None
7		usm	NoAuthNoPriv	None	None
8		usm	NoAuthNoPriv	None	None
9		usm	NoAuthNoPriv	None	None
10		usm	NoAuthNoPriv	None	None
11		usm	NoAuthNoPriv	None	None
12		usm	NoAuthNoPriv	None	None
13		usm	NoAuthNoPriv	None	None
14		usm	NoAuthNoPriv	None	None
15		usm	NoAuthNoPriv	None	None
16		usm	NoAuthNoPriv	None	None
17		usm	NoAuthNoPriv	None	None
18		usm	NoAuthNoPriv	None	None

Apply

Figure 60 Configure SNMPv3 access table

Group Name

Configuration range: Created group name, 1~32 characters

Description: All users in a group have the same access authority.

Security Model

Default configuration: any/v1/v2/usm

Function: Select the security model for the current group access switch（that is SNMP version number）, SNMPv3 use USM（security model based on user）technology. Any refers to use any security model. Group name, security model configuration should be consistent with group name and security model in group table.

Security level

Configuration options: NoAuthNoPriv/AuthNoPriv/AuthPriv

Function: Configure the security level of current group.

Description: NoAuthNoPriv requires neither authentication nor encryption, AuthNoPriv need to authenticate but not to encrypt, AuthPriv requires both authentication and encryption. When encryption is needed, the authentication / encryption protocol, the authentication / encryption password on the NMS side should be consistent with the configuration of the user table, then the node information of the switch can be accessed successfully.

The security level of NoAuthNoPriv、AuthNoPriv、AuthPriv increment in turn, a low level of security allows it can be accessed by a high level of security. If a group is configured the security level as AuthNoPriv, users with a security level as AuthNoPriv and AuthPriv in this group can successfully access the switch if both the authentication / encryption protocol and the authentication / encryption password are correct, but users with a security level as NoAuth/ NoPriv cannot access the switch.

Read View

Configuration options: default_view/None/Created view name

Function: Select read only view name.

Write View

Configuration options: default_view/None/Created view name

Function: Select read and write view name.

Up 16 access tables can be configured.

Note:

The default access tables in the switch {default_ro_group, any, NoAuth,NoPriv, default_view, None}、{default_rw_group, any, NoAuth,NoPriv, default_view, default_view}.

5.3.4 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 61.

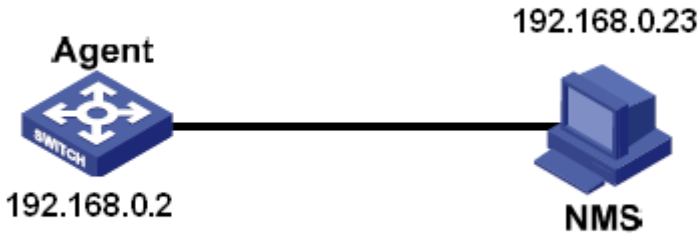


Figure 61 SNMP v3 Configuration Example

Configuration on the Agent:

1. Enable SNMP and v3 state, as shown in Figure 53.

2. Configure the SNMP v3 user table

Set a user name to 1111, security level to Auth,Priv, authentication protocol to MD5, authentication password to aaaaaaaa, privacy protocol to DES, and privacy password to xxxxxxxx.

Set another user name to 2222, security level to Auth,Priv, authentication protocol to SHA, authentication password to bbbbbbbb, privacy protocol to AES, and privacy password to yyyyyyyy, as shown in Figure 57.

3. Create group, set security model to usm, and add user 1111 and user 2222 to the group, as shown in Figure 58.

4. Configure the SNMP v3 access table

Set the group name to group, security model to usm, security level to Auth,NoPriv, read view to default_view, and write view to None, as shown in Figure 60.

5. Enable the global trap mode, as shown in Figure 54.

6. Create trap entry 222, enable trap mode; set the trap version to SNMP v3, destination IP address to 192.168.0.23. Select system, interface, authentication, and switch all trap events, and adopt default settings for the other parameters.

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

5.4 SSH Configuration

5.4.1 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.

5.4.2 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.

5.4.3 Web Configuration

1. Enable SSH protocol, as shown below.

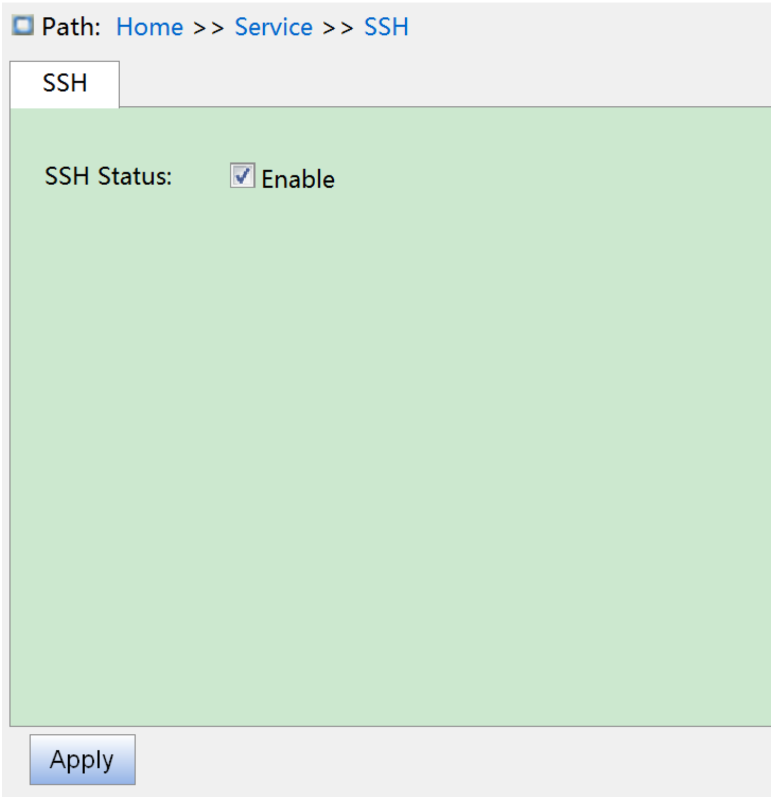


Figure 62 Enable SSH Protocol

SSH Status

Configuration options: Enabled/Disabled

Default configuration: Enabled

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

5.4.4 Typical Configuration Example

The Host works as the SSH client to establish a local connection with switch, as shown in Figure 63；

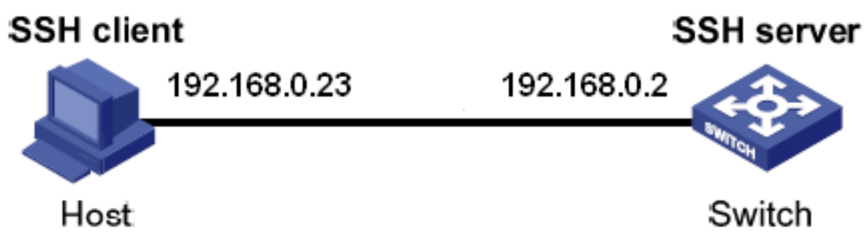


Figure 63 SSH Configuration Example

1. Enable SSH protocol, as shown in Figure 62;

2. Establish the connection with the SSH server. First, run the PuTTY.exe software, as shown in Figure 64; input the IP address of the SSH server "192. 168.0.2" in the space of Host Name (or IP address).

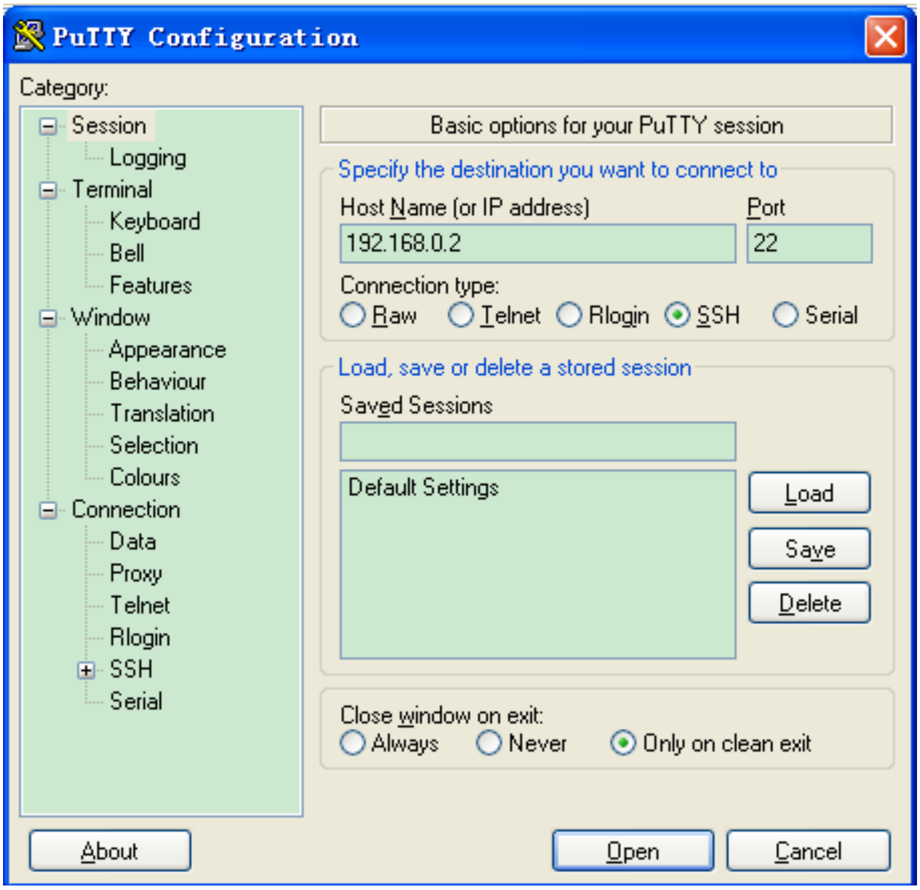


Figure 64 SSH Client Configuration

3. Click <Open> button and following warning message appears shown in Figure 65, click the <是(Y)> button.

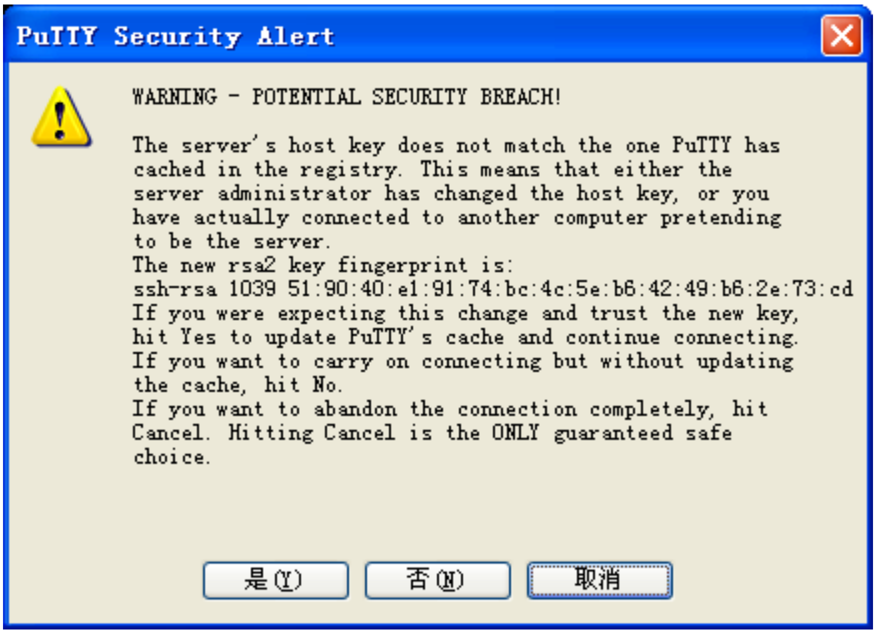


Figure 65 Warning Message

4. Input the user name "admin" and the password "123" to enter the switch configuration interface, as shown in Figure 66.

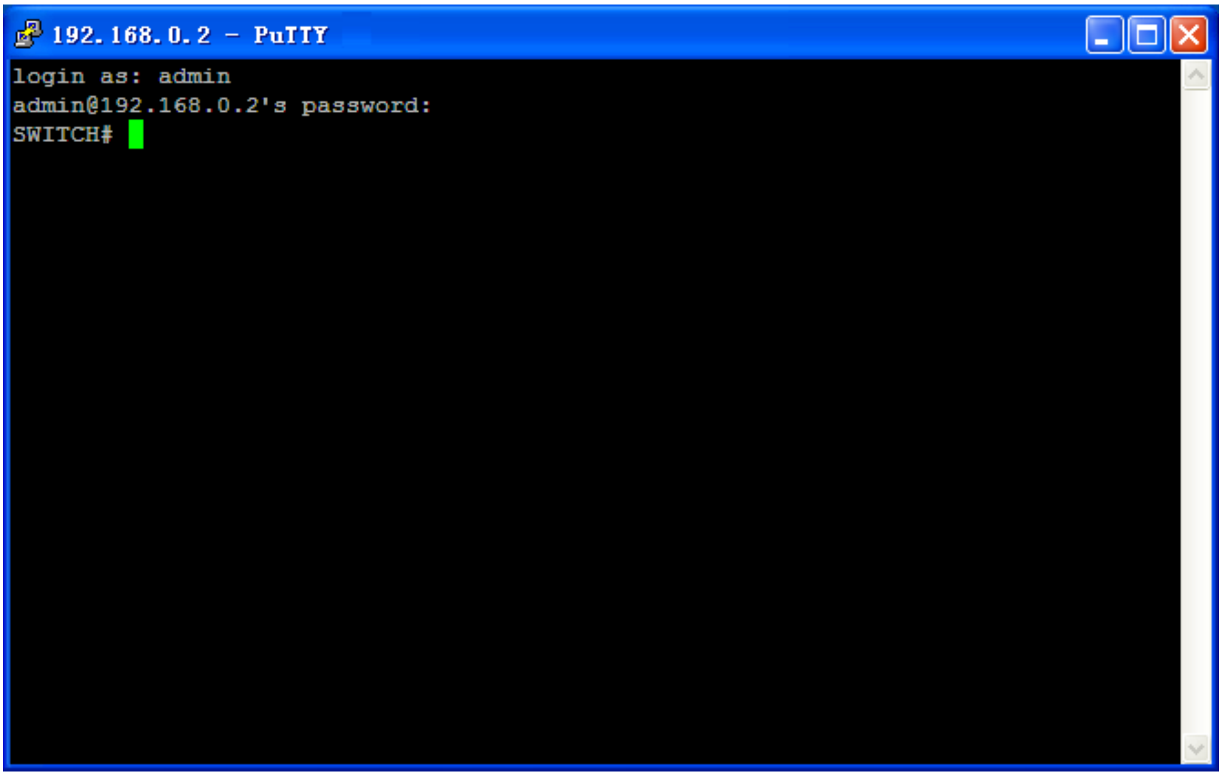


Figure 66 Login Interface of the SSH Authentication

5.5 TACACS+ Configuration

5.5.1 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 67 shows the structure.

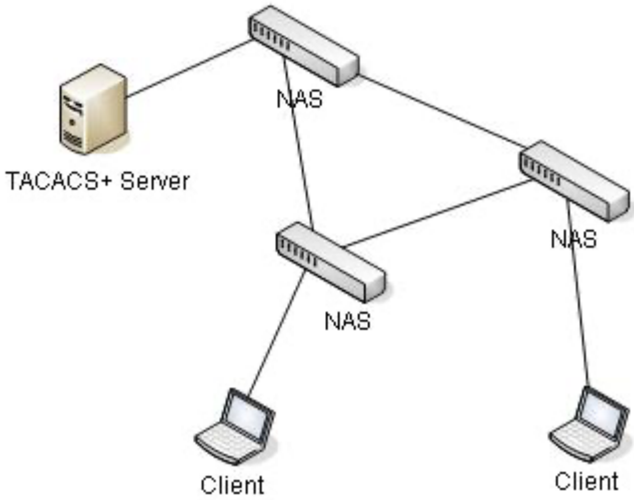


Figure 67 TACACS+ Structure

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.

5.5.2 Web Configuration

1. Configure the TACACS+ server, as shown below.

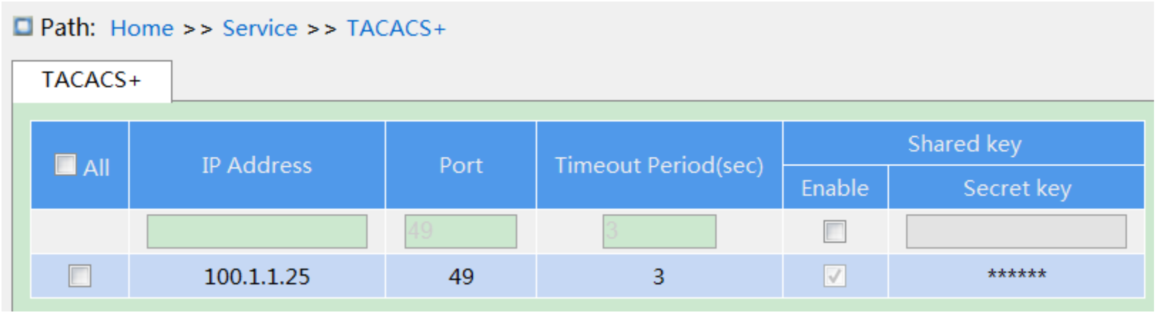


Figure 68 TACACS+ Server Configuration

IP Address

Function: Configure the IP address or hostname of TACACS+ server. A maximum of 5 TACACS+ server can be configured.

Port

Configuration range: 0~65535

Default configuration: 49

Function: Set TCP port of the TACACS+ server for authentication.

Timeout Period(sec)

Configuration range: 1~1000s

Function: Set the overtime for response from the TACACS+ server. After sending a TACACS+ request packet, if the device still receives no response from the TACACS+ server after the specified time, authentication fails, and the device will consider the TACACS+ server is invalid.

Share Key

Configuration range: 0~63 characters

Function: 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.

5.5.3 Typical Configuration Example

As shown in Figure 69, 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.

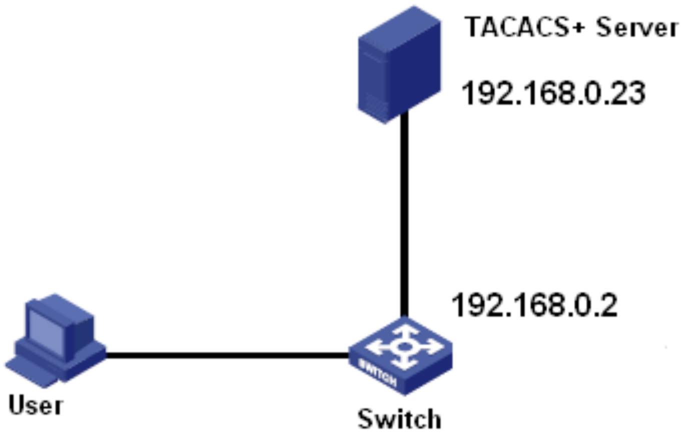


Figure 69 TACACS+ Authentication Example

1. TACACS+ server configuration. Set the server IP address to 192.168.0.23 and key to aaa, as shown in Figure 68.
2. When logging in to the switch through Web, select "Local", while logging in to the switch through telnet, select "Tacacs+", as shown in Figure 13.
3. Configure username and password "bbb", encrypt key “aaa” on TACACS+ server.
4. When logging in to the switch through Web, input the username "admin" and password "123" to pass the local authentication.
5. When logging in to the switch through Telnet, input the username and password "bbb" to pass the TACACS+ authentication.

5.6 RADIUS Configuration

5.6.1 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 70 shows the structure.

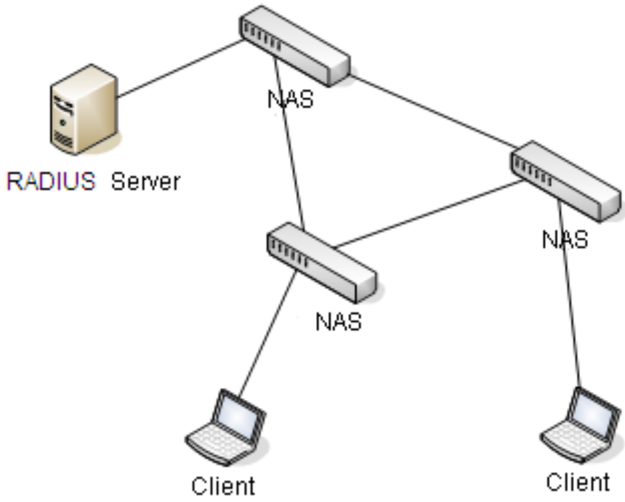
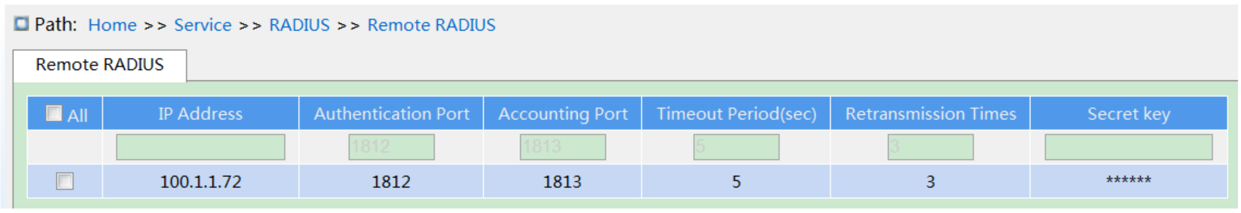


Figure 70 RADIUS Structure

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.

5.6.2 Web Configuration

1. Configure the RADIUS server, as shown below.


Path: Home >> Service >> RADIUS >> Remote RADIUS

Remote RADIUS

All	IP Address	Authentication Port	Accounting Port	Timeout Period(sec)	Retransmission Times	Secret key
		1812	1813	5	3	
	100.1.1.72	1812	1813	5	3	******

Figure 71 Configure the RADIUS Server

IP Address

Function: Configure the IP address or hostname of RADIUS server. A maximum of 5 RADIUS server can be configured.

Authentication Port

Configuration range: 0~65535

Default configuration: 1812

Function: Set UDP port of the RADIUS server for authentication.

Accounting Port

Configuration range: 0~65535

Default configuration: 1813

Function: Set UDP port of the RADIUS server for accounting. Since RADIUS uses different UDP ports for receiving and sending authentication and accounting messages, different port numbers must be configured for authentication and accounting.

Timeout Peroid(sec)

Configuration range: 1~1000s

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.

Retransmission Times

Configuration range: 1~1000

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, authentication fails, and the device will consider the RADIUS server is invalid.

Secret Key

Configuration range: 0~63 characters

Function: Set the key to improve the communication security between client and RADIUS 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 RADIUS server.

Note:

The priority of “Timeout Peroid”, “Retransmission Times”, and “Secret Key” in RADIUS server configuration is higher than those in global configuration.

2. RADIUS Global Configuration, as shown below.

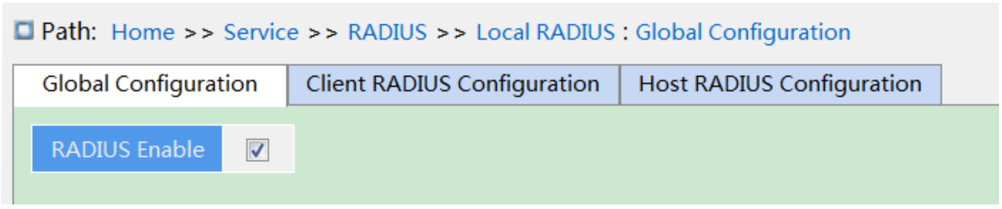


Figure 72 global configuration

RADIUS Enable

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether enable local RADIUS to be used by other devices as RADIUS servers.

3. Client RADIUS Configuration, as shown below.

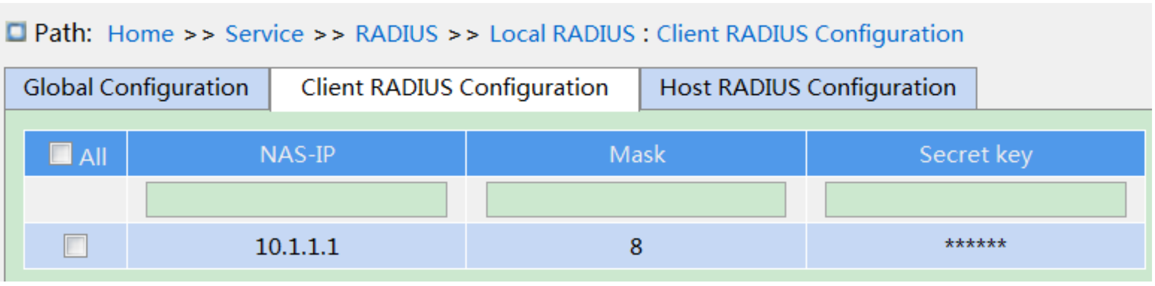


Figure 73 Client RADIUS configuration

NAS-IP

Function: Configure IP address or IP address segment of RADIUS client.

Mask

Configuration range: 1-32

Function: Configure network segment of RADIUS client, the IP address of the same network segment only configure one segment.

Secret key

Configuration range: 1~63 characters

Function: Configure the shared key the device and the radius client to verify the validity of the message. Only if the key is the same, then accept and respond the message each other, so the shared key configured on the device must be same with the key value on the RADIUS client.

4. Host RADIUS Configuration, as shown below.

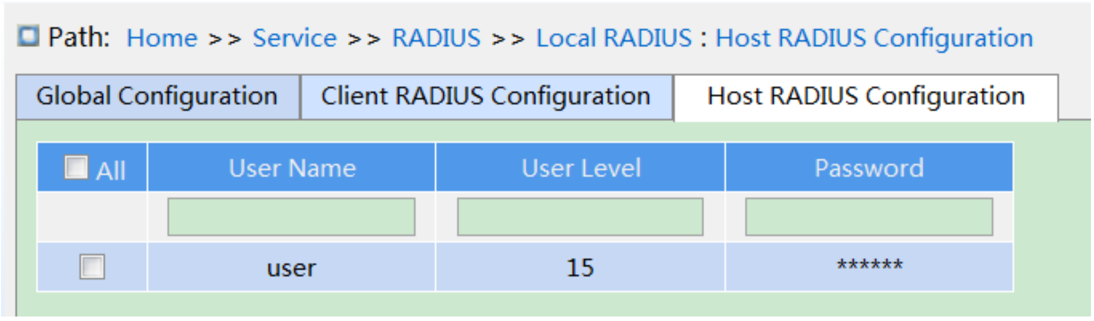


Figure 74 Host RADIUS configuration

User Name

Configuration range: 1-31 characters

Function: Configure RADIUS user name.

User Level

Configuration range:1~15

Function: Configure the user authority level. Users with different anthority levels have different access authority.

Password

Configuration range: 1-31 characters

Function: Configure the login password of user.

5.6.3 Typical Configuration Example

As shown in Figure 75, 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 aaa.

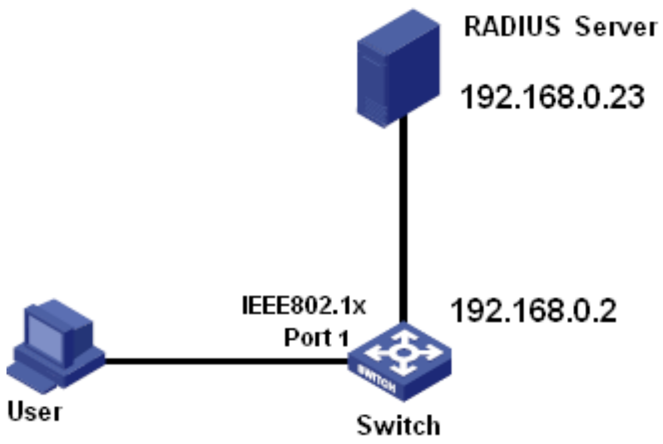


Figure 75 RADIUS Authentication Example

1. Set the IP address of the authentication server to 192.168.0.23 and password to aaa, as shown in Figure 71.
2. IEEE802.1x settings: enable IEEE802.1X globally. Set authentication type to radius, admin state of port 1 to port-based 802.1X, keep default settings for the other parameters.
3. Set both the user name and password on the RADIUS Server to ccc, encrypt key to aaa.
4. 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.

5.7 DNS

5.7.1 Introduction

DNS（Domain Name System）is a distributed database for TCP/IP applications that provides conversion between domain names and IP addresses. Through the domain name system, the user can use the domain name which is easy to remember and meaningful, and the domain name can be converted to the correct IP address by the DNS server in the network.

Domain name resolution is divided into static domain name resolution and dynamic domain name resolution. In the process of domain name resolution, first use static domain name resolution (search the static domain name resolution table), if the static domain name resolution is not successful, then use dynamic domain name resolution.

Static domain name resolution is to manually establish the corresponding relationship between domain name and IP address. When the user uses the domain name for some applications (such as telnet application), the system searches the static domain name resolution table and obtains the IP address for the specified domain name.

5.7.2 Web Configuration

1. Enable DNS proxy, configure domain name.

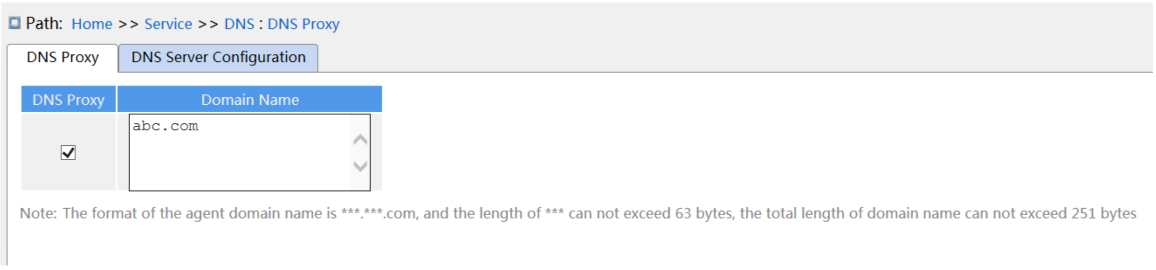


Figure 76 Configure DNS

DNS Proxy

Configuration options: Disable/enable

Default configuration: Disable

Function: Disable or enable DNS proxy.

Domain Name

Configuration range: The format of domain is ***.***.com，and the length of *** is less than 63 characters, the total length is less than 251 characters.

Default configuration: None

Function: After the client request the domain name to server directly and resolve the address failure, add the domain name suffix resolves to the DNS server again.

2. DNS Server Configuration

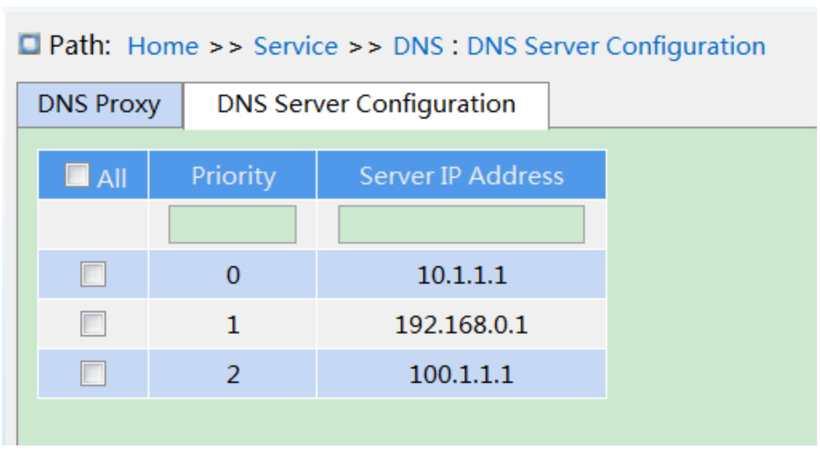


Figure 77 Configure the DNS server

Priority

Configuration range: 0, 1, 2

Default configuration: None

Function: the proxy device resolves the address to the specified DNS server in priority order until the resolution is successful.

Server IP Address

Configuration format: A.B.C.D

Function: Manually configure the DNS server IP address.

5.7.3 Typcial Configuration Example

As shown in Figure 75, sometimes the DNS client can not or must not be directly configured as the DNS server address. At this time, the DNS address of the client can be set directly to the DNS proxy address by setting the dns proxy on the switch. After configuring the domain name suffix list, the DNS proxy will automatically add the configured suffix to the domain name when sending the DNS resolution request again after a request fails.

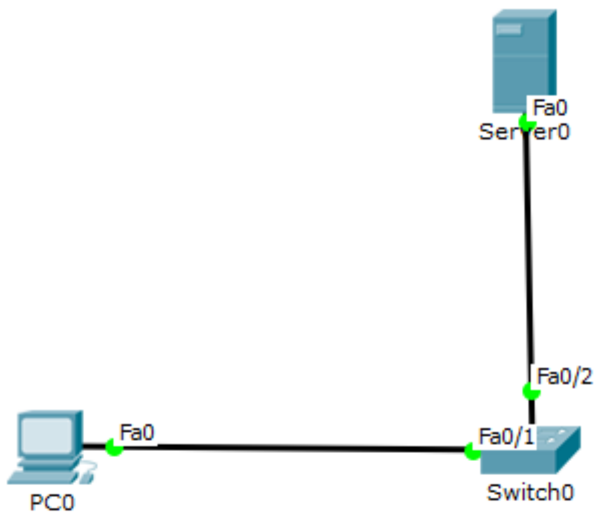


Figure 78 DNS proxy configuration example

1. Configure DNS Server IP address as 192.168.0.254/24。

2. Configure PC IP address as 192.168.1.2/24，DNS Server as 192.168.1.1；

3. Configure Switch0 interface Fa1/1 as access mode to join VLAN 1，configure L3 interface

IP as 192.168.1.1/24，interface Fa1/2 as access mode to join VLAN 2，configure L3 interface IP as 192.168.0.1/24；

4. Enable DNS proxy in Switch0, configure DNS Server IP as 192.168.0.254，configure domain suffix as abc.com，Thus the switch proxy DNS server can be implemented for DNS domain name resolution.

5.8 RMON

5.8.1 Introduce

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

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

5.8.2 RMON Groups

RMON (RFC2819) defines multiple RMON groups. The series devices support statistics group, history group, event group, and alarm group in public MIB.

- Statistics group

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

- History group

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

- Event group

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

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

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

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

None: indicates no action.

- Alarm group

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

CAUTION

Caution:

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

5.8.3 Web Configuration

1. Configure statistics table, as shown below.

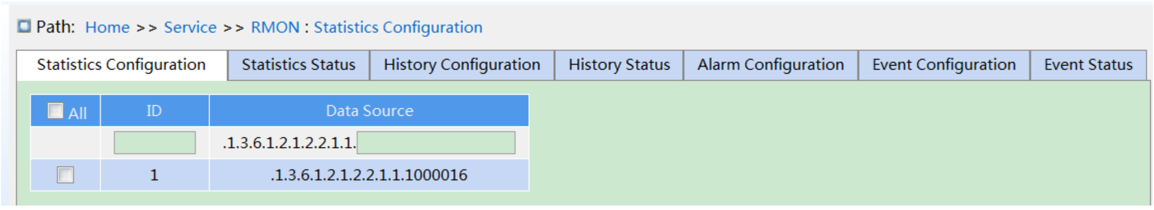


Figure 79 Configure RMON Statistics Table

ID

Configuration range: 1~65535

Function: Configure the number of the statistics entry. Statistics group supports up to 128 entries.

Data Source

Configuration range: 10000portid

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

2. View statistics group status, as shown below.

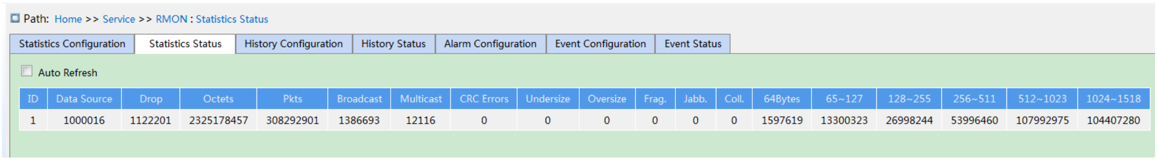


Figure 80 Overview statistics group status

Drop: the number of packets dropped by the port.

Octets: the number of bytes received by the port.

Pkts: the number of packets received by the port.

Broadcast: the number of broadcast packets received by the port.

Multicast: the number of multicast packets received by the port.

CRC Errors: the number of CRC error packets with a length of between 64 and 9600 bytes received by the port.

Undersize: the number of packets with less than 64 bytes received by the port.

Oversize: the number of packets with more than 9600 bytes received by the port.

Frag.: the number of CRC error packets with less than 64 bytes received by the port.

Jabb.: the number of CRC error packets with more than 9600 bytes received by the port.

Coll.: the number of collisions received by the port under half duplex mode.

64 Bytes: the number of packets with a length of 64 bytes received by the port.

65~127: the number of packets with a length of between 65 and 127 bytes received by the port.

128~255: the number of packets with a length of between 128 and 255 bytes received by the port.

256~511: the number of packets with a length of between 256 and 511 bytes received by the port.

512~1023: the number of packets with a length of between 512 and 1023 bytes received by the port.

1024~1588: the number of packets with a length of between 1024 and 1588 bytes received by the port.

Note:

The oversize depends on the parameter "Maximum Frame Size" in Port Configuration, as shown in 7.1 Port Configuration. In above example, the oversize is 9600 bytes.

3. Configure history table, as shown below.

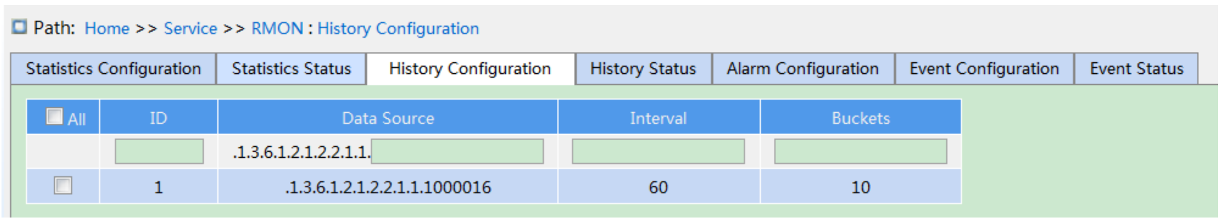


Figure 81 Configure History Table

ID

Configuration range: 1~65535

Function: Configure the number of the history entry. History group supports up to 256 entries.

Data Source

Configuration options: 100000portid

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

Interval

Configuration range: 1~3600s

Default configuration: 1800s

Function: Configure the sampling period of the port.

Buckets

Configuration range: 1~65535

Default configuration: 50

Function: Configures the number of latest sampling values of port information stored in RMON.

4. View history group status, as shown below.

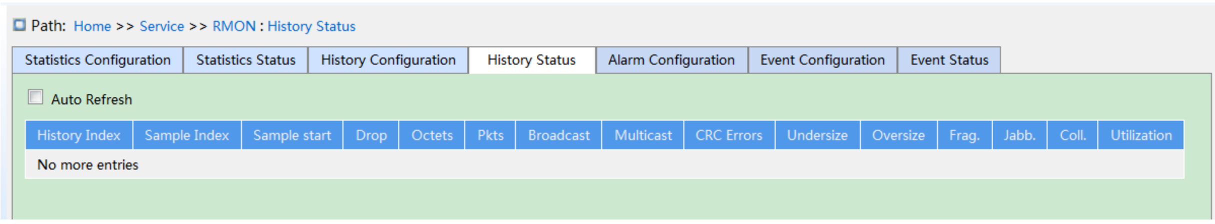


Figure 82 Overview History Group Status

5. Configure event table, as shown below.

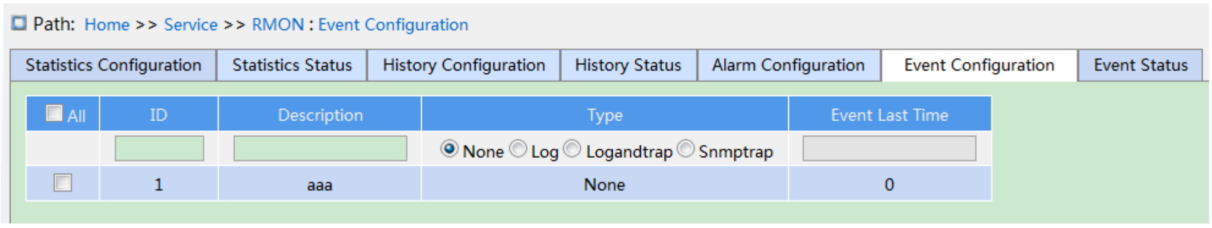


Figure 83 Configure Event Table

ID

Configuration range: 1~65535

Function: Configure the index number of the event entry. Event group supports up to 128 entries.

Description

Configuration range: 0~127 characters

Function: Describe the event.

Type

Configuration options: none/log/snmptrap/logandtrap

Default configuration: none

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

Event Last Time

Function: Displays the value of sysUpTime when the event is used last time.

6. View event group status, as shown below.

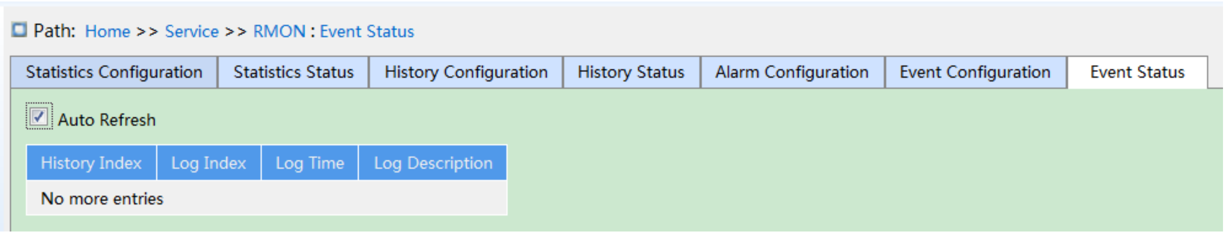


Figure 84 Overview Event Group Status

7. Configure alarm table, as shown below.

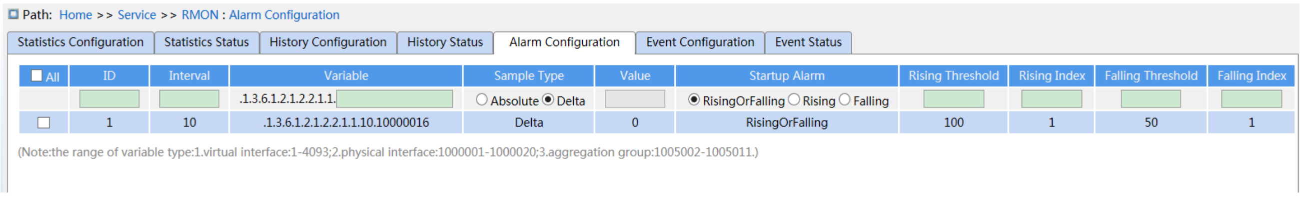


Figure 85 Configure Alarm Table

ID

Configuration range: 1~65535

Function: Configure the number of the alarm entry. Alarm group supports up to 256 entries.

Interval

Configuration range: 1~2147483647s

Configuration Deault: 30s

Function: Configure the sampling period.

Variable

Configuration Format: A.10000portid

Configuration range: A：10~21

Function: Select the port MIB information to be monitored.

InOctets: A=10, the number of bytes received by the port.

InUcastPkts: A=11, the number of unicast packets received by the port.

InNUcastPkts: A=12, the number of broadcast and multicast packets received by the port.

InDiscards: A=13, the number of packets dropped by the port.

InErrors: A=14, the number of error packets received by the port.

InUnknownProtos: A=15, the number of unknown packets received by the port.

OutOctets: A=16, the number of bytes sent by the port.

OutUcastPkts: A=17, the number of unicast packets sent by the port.

OutNUcastPkts: A=18, the number of broadcast and multicast packets sent by the port.

OutDiscards: A=19, the number of discarded packets sent by the port.

OutErrors: A=20, the number of error packets sent by the port.

OutQLen: A=21, The length of packets in port outlet queue.

Sample Type

Configuration options: Absolute/Delta

Default configuration: Delta

Function: choose the method of comparing the sampling value and threshold.

Description: Absolute: directly compare each sampling value to threshold; Delta: the sampling value minus the previous sampling value, then use the difference to compare with threshold.

Startup Alarm

Configuration options: Rising/Falling/RisingOrFalling

Default configuration: RisingOrFalling

Function: choose the alarm type.

Rising Threshold

Configuration range: 1~2147483647

Function: Set a rising threshold. When the sampling value exceeds the rising threshold and the alarm type is RisingAlarm or RisOrFallAlarm, the alarm will be triggered and the rising event index will be activated.

Rising Index

Configuration range: 1~65535

Function: Set the index of a rising event. It is the handing method of a rising alarm.

Falling Threshold

Configuration range: 1~2147483647

Function: Set a falling threshold. When the sampling value is lower than the falling threshold and the alarm type is FallingAlarm or RisOrFallAlarm, the alarm will be triggered and the falling event index will be activated.

Falling Index

Configuration range: 1~65535

Function: Set the index of a falling event. It is the handling method of a falling alarm.

6 Alarm

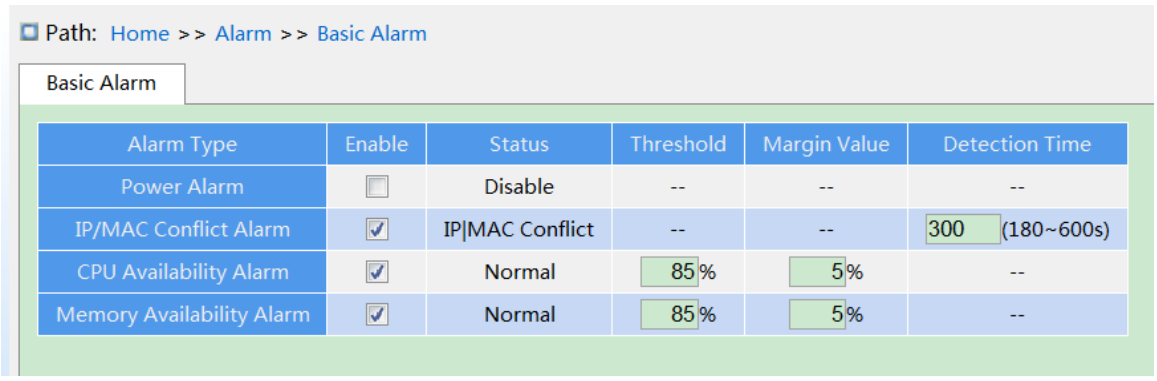
6.1 Introduction

This series switches support the following types of alarms:

- Power alarm: If the function is enabled, then an alarm will be generated for a single power input.
- IP/MAC conflict alarm: If the function is enabled, then an alarm will be triggered for an IP/MAC conflict.
- Memory / CPU usage alarm: If this function is enabled, an alarm is generated when the CPU / memory usage exceeds the specified threshold.
- Port alarm: If this function is enabled, an alarm is triggered when the port is in link down state.
- Port traffic alarm: If this function is enabled, an alarm is generated when the incoming / outgoing traffic rate of a port exceeds the specified threshold.
- CRC error / packet loss alarm: If this function is enabled, an alarm is generated when the number of CRC error / packet loss of a port exceeds the specified threshold.
- Ring alarm: If this function is enabled, an alarm is triggered when the ring is open.

6.2 Web Configuration

1. Basic alarm configuration and display, as shown below.



Alarm Type	Enable	Status	Threshold	Margin Value	Detection Time
Power Alarm	☐	Disable	--	--	--
IP/MAC Conflict Alarm	☑	IP|MAC Conflict	--	--	300 (180~600s)
CPU Availability Alarm	☑	Normal	85 %	5 %	--
Memory Availability Alarm	☑	Normal	85 %	5 %	--

Figure 86 Basic Alarm

Power Alarm

Configuration options: Enable/Disable

Default configuration: Disable

Function: Enable/Disable Power Alarm.

Status

Configuration options: Normal/Alarm

Function: View power alarm status.

Alarm: 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.

IP, MAC Conflict

Configuration options: Enable/Disable

Default configuration: Enable

Function: Enable/Disable IP/MAC conflict alarm.

Status

Configuration options: Conflict / No Conflict

Description: When an IP/MAC conflict occurs, Conflictis displayed; otherwise, No Conflictis displayed.

Check Time

Configuration range: 180~600s

Default configuration: 300s

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

CPU/Memory Availability Alarm

Configuration options: Enable/Disable

Default configuration: Enable

Function: Enable/Disable CPU/Memory Availability Alarm.

Threshold (%)

Configuration range: 50~100

Default configuration: 85

Function: Set the CPU/memory usage threshold. When the CPU/memory usage of the switch is higher than the threshold, an alarm is generated.

Margin Value (%)

Configuration range: 1~20

Default configuration: 5

Function: Set the CPU/memory usage margin value.

Description: If the CPU/memory usage fluctuates around the threshold, alarms may be generated and cleared repeatedly. To prevent this phenomenon, you can specify a margin value (5% by default). The alarm will be cleared only if the CPU/memory usage is lower than the threshold by the margin value or more. For example, the memory usage threshold is set to 60% and the margin value is set to 5%. If the memory usage of the switch is lower than or equal to 60%, no alarm is generated. If the memory usage is higher than 60%, an alarm will be generated. The alarm will be cleared only if the memory usage is equal to or lower than 55%.

2. Configure and display port alarm, as shown below.

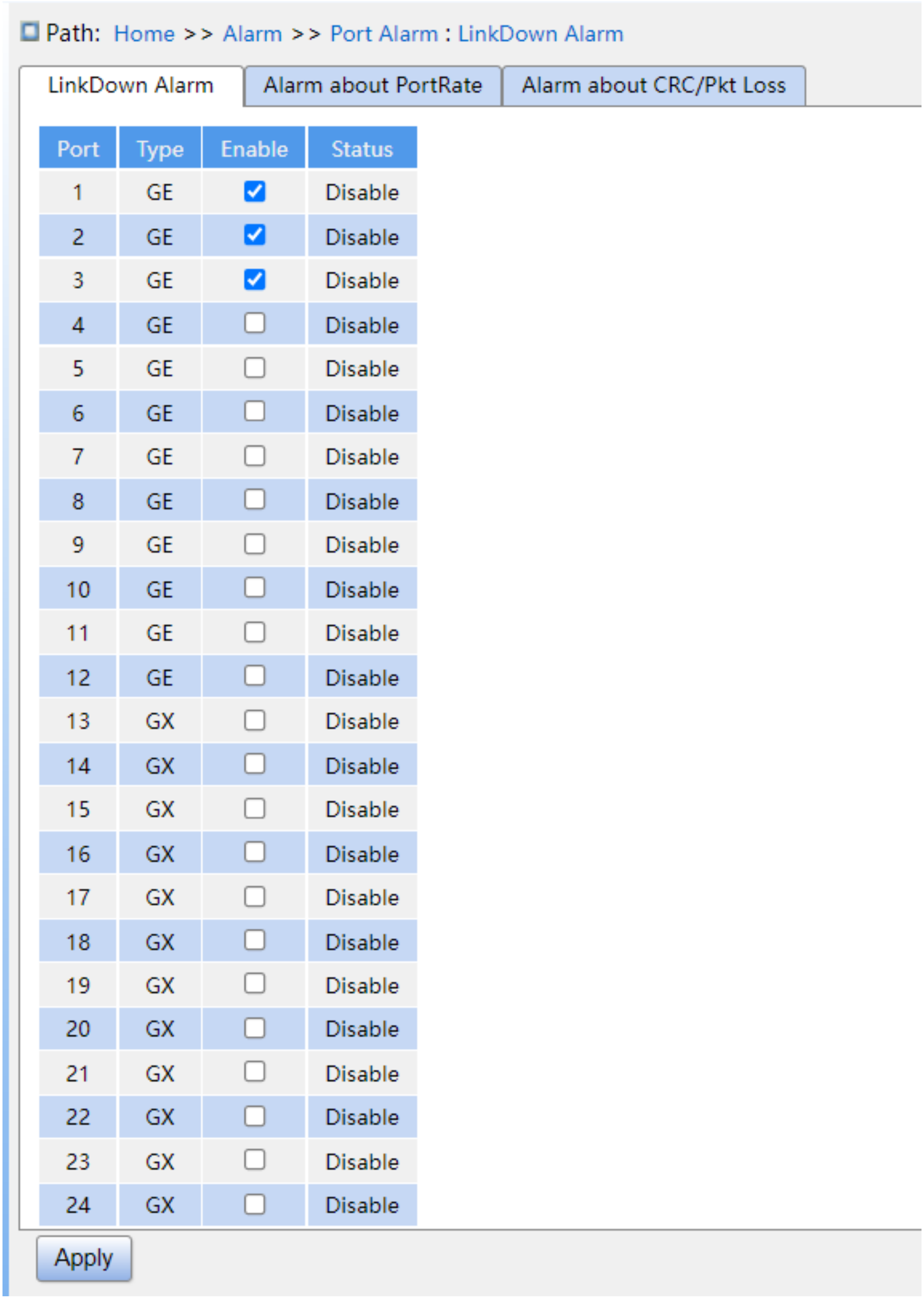


Figure 87 Port Alarm

Port Alarm Configuration

Configuration options: Disable/Enable

Default configuration: Disable

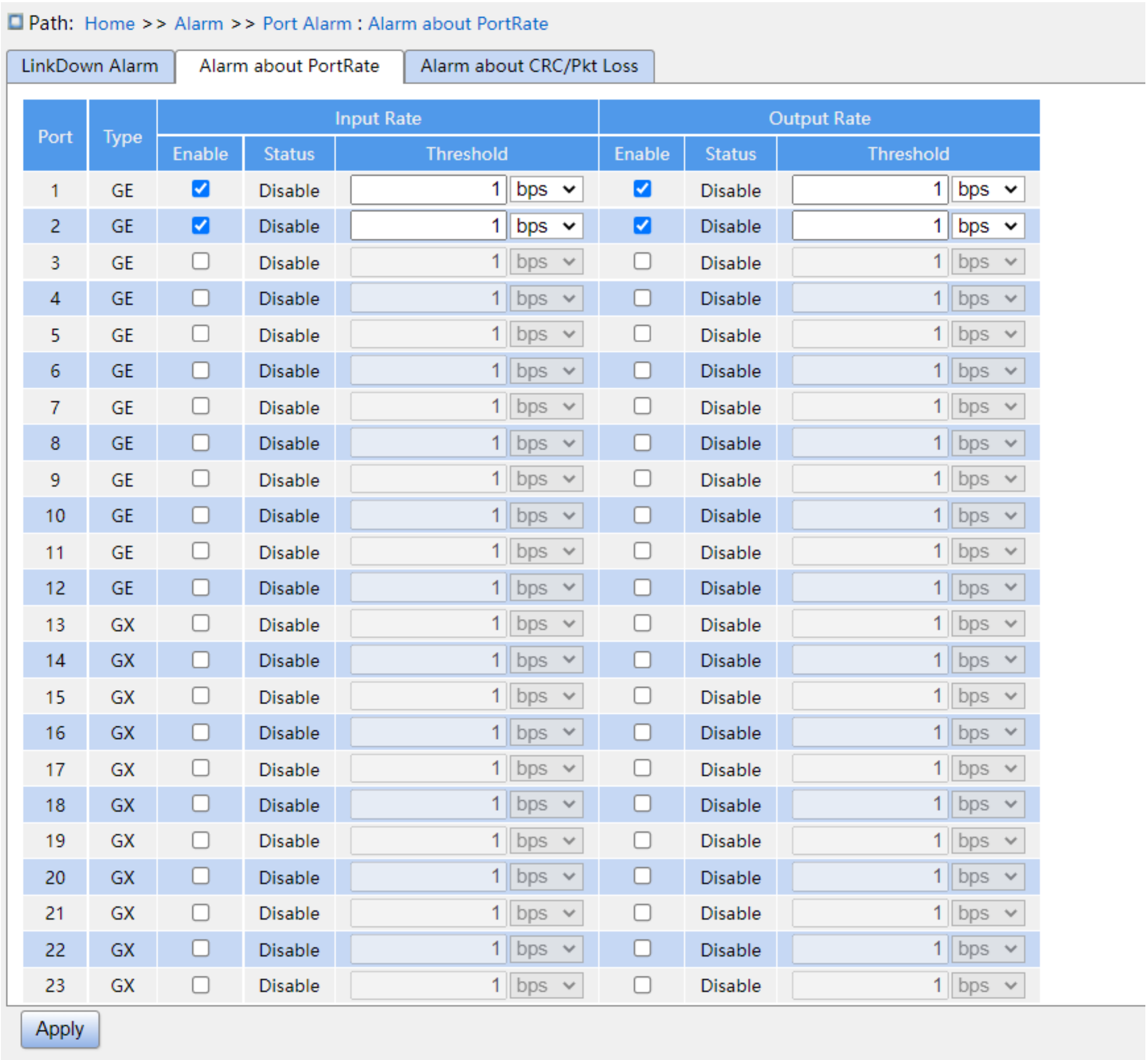
Function: Enable/Disable port alarm.

Status

Configuration options: Link Up/Link Down

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

3. Configure and display port traffic alarm, as shown below.



Port	Type	Input Rate			Output Rate		
		Enable	Status	Threshold	Enable	Status	Threshold
1	GE	☑	Disable	1 bps	☑	Disable	1 bps
2	GE	☑	Disable	1 bps	☑	Disable	1 bps
3	GE	☐	Disable	1 bps	☐	Disable	1 bps
4	GE	☐	Disable	1 bps	☐	Disable	1 bps
5	GE	☐	Disable	1 bps	☐	Disable	1 bps
6	GE	☐	Disable	1 bps	☐	Disable	1 bps
7	GE	☐	Disable	1 bps	☐	Disable	1 bps
8	GE	☐	Disable	1 bps	☐	Disable	1 bps
9	GE	☐	Disable	1 bps	☐	Disable	1 bps
10	GE	☐	Disable	1 bps	☐	Disable	1 bps
11	GE	☐	Disable	1 bps	☐	Disable	1 bps
12	GE	☐	Disable	1 bps	☐	Disable	1 bps
13	GX	☐	Disable	1 bps	☐	Disable	1 bps
14	GX	☐	Disable	1 bps	☐	Disable	1 bps
15	GX	☐	Disable	1 bps	☐	Disable	1 bps
16	GX	☐	Disable	1 bps	☐	Disable	1 bps
17	GX	☐	Disable	1 bps	☐	Disable	1 bps
18	GX	☐	Disable	1 bps	☐	Disable	1 bps
19	GX	☐	Disable	1 bps	☐	Disable	1 bps
20	GX	☐	Disable	1 bps	☐	Disable	1 bps
21	GX	☐	Disable	1 bps	☐	Disable	1 bps
22	GX	☐	Disable	1 bps	☐	Disable	1 bps
23	GX	☐	Disable	1 bps	☐	Disable	1 bps

Figure 88 Port Traffic Alarm Configuration

input rate alarm/output rate alarm

Configuration options: Enable/Disable

Default configuration: Disable

Function: Enable/Disable port traffic alarm.

Threshold

Configuration range: 1 to 1000000000bps or 1 to 1000000kbps.

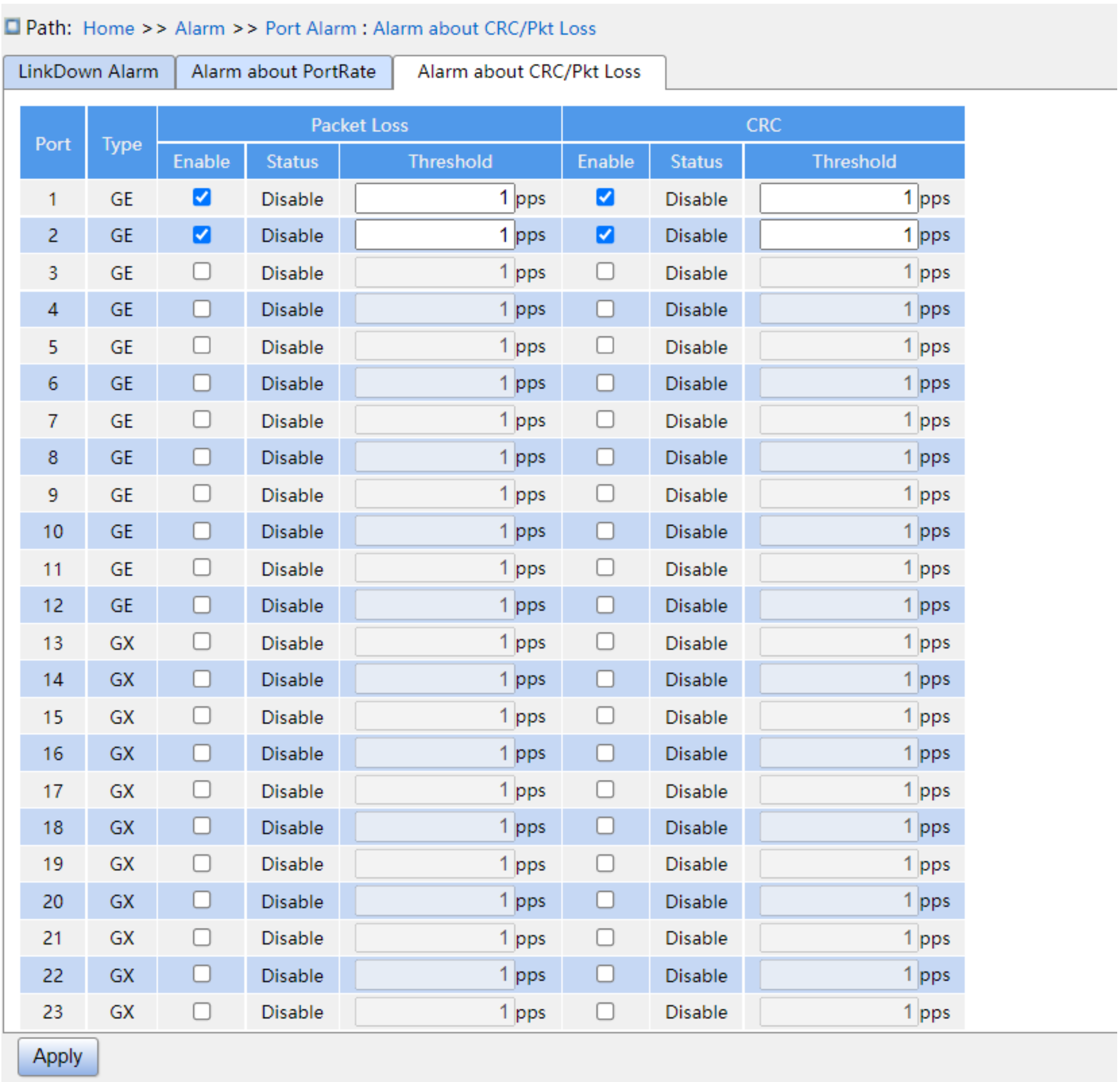
Function: Configure the threshold for the port traffic.

Alarm Status

Configuration options: Disable/Alarm/ Normal

Function: View the port traffic status. Alarm means the incoming / outgoing traffic rate exceeds the threshold and triggers alarm.

4. Configure and display CRC error / packet loss alarm, as shown below.



Port	Type	Packet Loss			CRC		
		Enable	Status	Threshold	Enable	Status	Threshold
1	GE	☑	Disable	1 pps	☑	Disable	1 pps
2	GE	☑	Disable	1 pps	☑	Disable	1 pps
3	GE	☐	Disable	1 pps	☐	Disable	1 pps
4	GE	☐	Disable	1 pps	☐	Disable	1 pps
5	GE	☐	Disable	1 pps	☐	Disable	1 pps
6	GE	☐	Disable	1 pps	☐	Disable	1 pps
7	GE	☐	Disable	1 pps	☐	Disable	1 pps
8	GE	☐	Disable	1 pps	☐	Disable	1 pps
9	GE	☐	Disable	1 pps	☐	Disable	1 pps
10	GE	☐	Disable	1 pps	☐	Disable	1 pps
11	GE	☐	Disable	1 pps	☐	Disable	1 pps
12	GE	☐	Disable	1 pps	☐	Disable	1 pps
13	GX	☐	Disable	1 pps	☐	Disable	1 pps
14	GX	☐	Disable	1 pps	☐	Disable	1 pps
15	GX	☐	Disable	1 pps	☐	Disable	1 pps
16	GX	☐	Disable	1 pps	☐	Disable	1 pps
17	GX	☐	Disable	1 pps	☐	Disable	1 pps
18	GX	☐	Disable	1 pps	☐	Disable	1 pps
19	GX	☐	Disable	1 pps	☐	Disable	1 pps
20	GX	☐	Disable	1 pps	☐	Disable	1 pps
21	GX	☐	Disable	1 pps	☐	Disable	1 pps
22	GX	☐	Disable	1 pps	☐	Disable	1 pps
23	GX	☐	Disable	1 pps	☐	Disable	1 pps

Figure 89 CRC Error/ Pkt Loss Alarm Configuration

CRC/Pkt Loss Alarm

Configuration options: Enable/Disable

Default configuration: Disable

Function: Enable/Disable CRC/ Pkt loss alarm.

Threshold

Configuration range: 1 to 1000000pps.

Function: Configure the threshold for the port CRC/ Pkt loss alarm.

Alarm Status

Configuration options: Disable/Alarm/ Normal

Function: View the port CRC/ Pkt loss status. Alarm means the port CRC/ Pkt loss exceeds the threshold and triggers alarm.

5. Configure and display Ring alarm, as shown below.

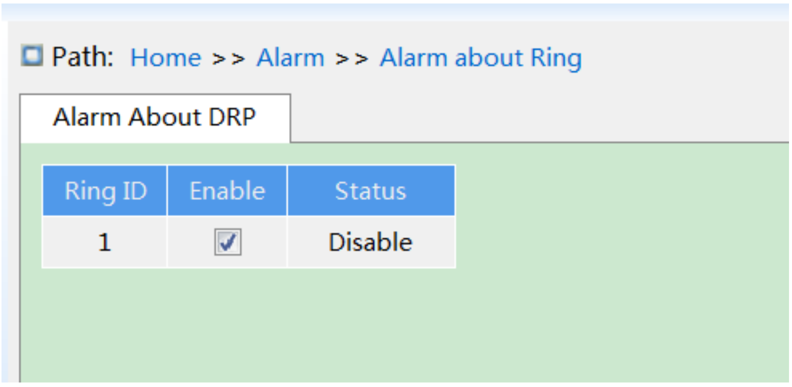


Figure 90 Ring Alarm Configuration

Alarm About DRP

Configuration options: Disable/Enable

Default configuration: Disable

Function: Enable/Disable DRP alarm.

Alarm Status

Configuration options: Disable/Alarm/---

Function: View the DRP status. --- means DRP is closed. Alarm means DRP is open or in abnormal state.

6、Alarm configuration and display of receiving optical power software,as shown below;

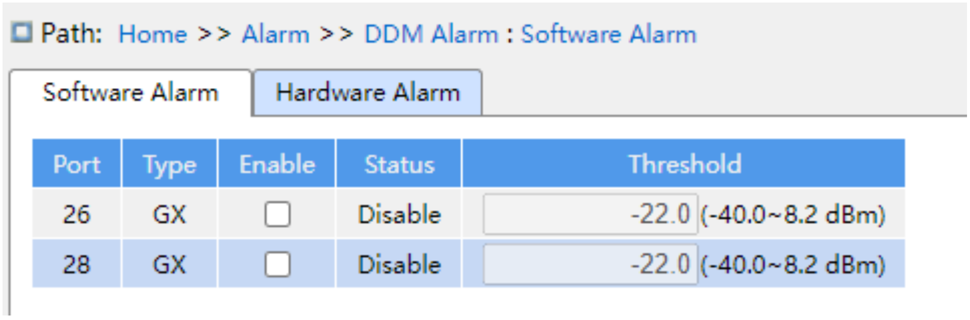


Figure 91 Software Alarm

Software Alarm

Configuration options: Disable/Enable

Default configuration: Disable

Function: Enable/Disable received optical power alarm of port.

Threshold

Configuration range:-40~8.2 dBm

Default configuration: -22.0dBm

Function: Configure the received optical power alarm threshold.

Status

Display options:Alarm/ Disable

Description: After the received optical power alarm is enabled, when the received optical power monitoring value of the SFP optical module is lower than the alarm threshold, an alarm is displayed; when the received optical power monitoring value of the SFP optical module is not lower than the alarm threshold, the display is normal.

7、Pluggable module hardware alarm configuration, as shown below;

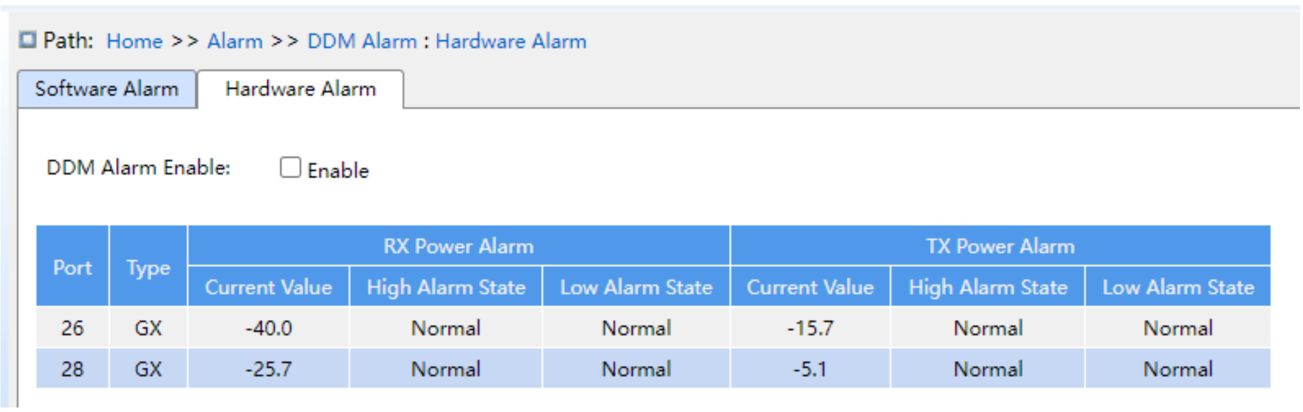


Figure 92 Pluggable module alarm configuration

Hardware Alarm

Configuration options: Disable/Enable

Default configuration: Disable

Function: Enable/Disable SFP the optical power alarm of the SFP optical module. When the current value of optical power is lower than the lower threshold, an optical power lower limit alarm is generated; when the current value of optical power is higher than the upper limit alarm, an optical power upper limit alarm is generated.

Caution:

The upper and lower thresholds of the optical power are determined by hardware and cannot be configured.

7 Function Management

7.1 Port Configuration

1. Configure port status, port rate, flow control etc. information, as shown below.

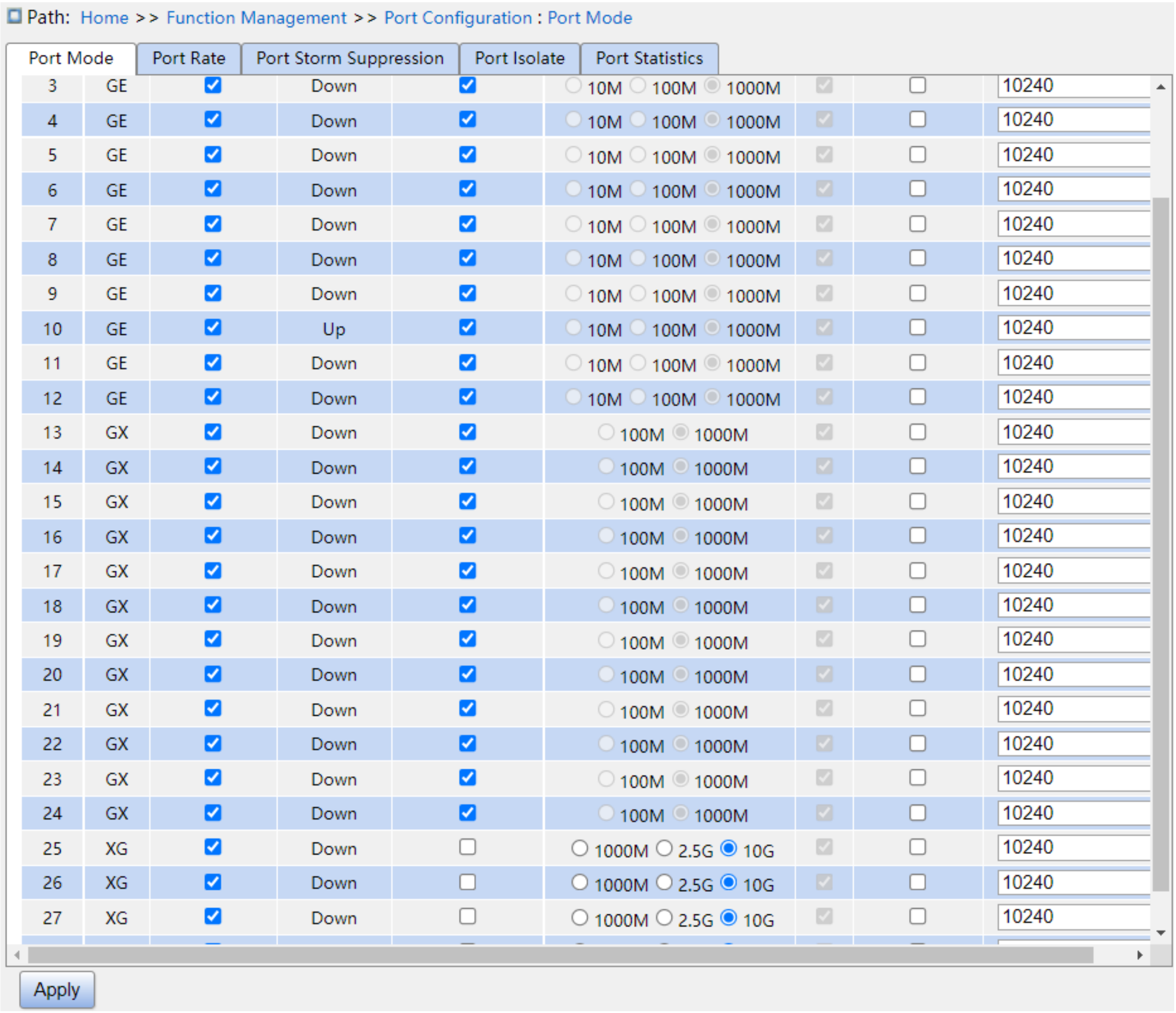


Figure 93 Configure port mode

Administration Status

Configuration options: Enable/disable

Default configuration: Enable

Function: Whether the port is allowed to transfer data.

Description: Open port to transfer data if enable, close port and no data is transferred if disable. This option directly affects the hardware status of the port and triggers port alarm information.

Link Status

Displays the connection status of the current port.

Up means port is LinkUp status and communication is normal.

Down means port is LinkDown status and communication is abnormal.

Auto Negotiate

Configuration options: Enable/disable

Default configuration: Enable

Description: Configure port rate and duplex mode. Port rate and duplex mode can be auto negotiation or can be forced. Port rate and duplex mode automatically negotiated according to the connection status of both ports when configured to automatic negotiation mode. It is recommended that the user configure the speed and duplex mode of the port to automatic negotiation so to avoid connection problems caused by the mismatch of the port configuration as far as possible. If the user configures the port to forced rate / duplex mode, make sure the both ends connection rate / duplex mode configuration are same.

Caution:

- The Gigabit electoric port can be configured as auto negotiation, 10M full duplex, 10M half-duplex, 10M full duplex, 100M and 1000M full duplex.
- The 10 Gigabit optical port can be configured as 1000m full duplex, 2.5G full duplex and 10g full duplex.

Speed

Configuration options: 100M/1000M or 10M/100M/1000M or 1000M/2.5G/10G

Function: Configure auto negotiation speed of port.

Description: When configuring port mode to automatic negotiation, the speed of port is determined through auto negotiation with the opposite end by default. The negotiated speed can be any of the port speed range. By configuring speed, the port can negotiate only part rate, thus controlling rate negotiation.

Caution:

Duplex capability and rate capability configuration can only be configured when auto-negotiation mode is off.

Full

Configuration options: Enable/disable

Function: Configure port auto negotiation duplex mode.

Description: full duplex means that the port can receive data while sending data; half duplex port can only send or receive data at any one time. When the port mode is configured to automatic negotiation, the port duplex mode is determined by negotiation with the end-to-end by default. The negotiated duplex mode can be either full duplex or half-duplex. By configuring the duplex, the port can negotiate only one duplex mode, thus controlling the duplex mode negotiation.

Flow Control

Configuration options: Enable/disable

Default configuration: Disable

Function: Enable or disable flow control.

Description: after enable port flow control, when the port receives more traffic than the maximum value the port cache can hold, the port will inform the sending end to slow down the sending speed to prevent packet loss according to the algorithm or protocol. For half duplex mode and full duplex mode, flow control is implemented in different ways. In full duplex mode, the receiving end informs the sending end to stop sending the message by sending a special data frame (pause frame), after receiving the pause frame, the sending end will stop sending the message according to the waiting time in the frame. The half-duplex mode supports backpressure flow control, and the receiving end can intentionally create a collision or carrier signal, once the sending end detects the collision or carrier signal then adopts Backoff to delay the data transmission.

Maximum Frame Size

Configuration options: 1518~10240 bytes

Default configuration: 10240 bytes

Function: configure the allowed maximum frame size of the port, and the frame above that size will be discarded.

2、Port Rate, as shown below.

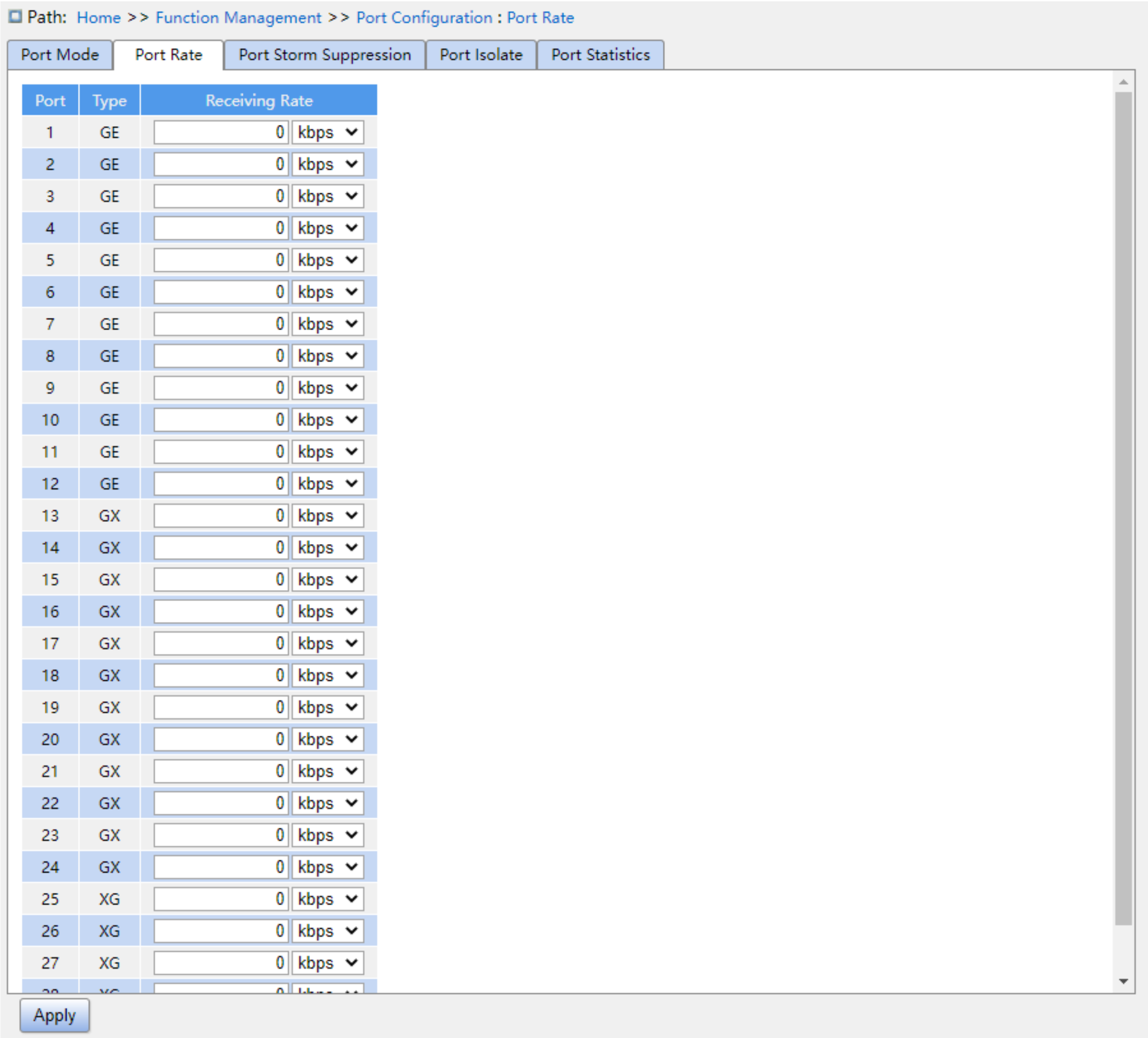


Figure 94 Port Rate

Receiving Rate

Configure options: 10~13128147kbps/10~13128147fps/1~13128kfps/1~13128mbps

Default configuration: 0，value is 0 means disable limit rate.

Function: configure port rate limit threshold. Message data above the threshold will be discarded.

3. Port Storm Suppression configuration, as shown below.

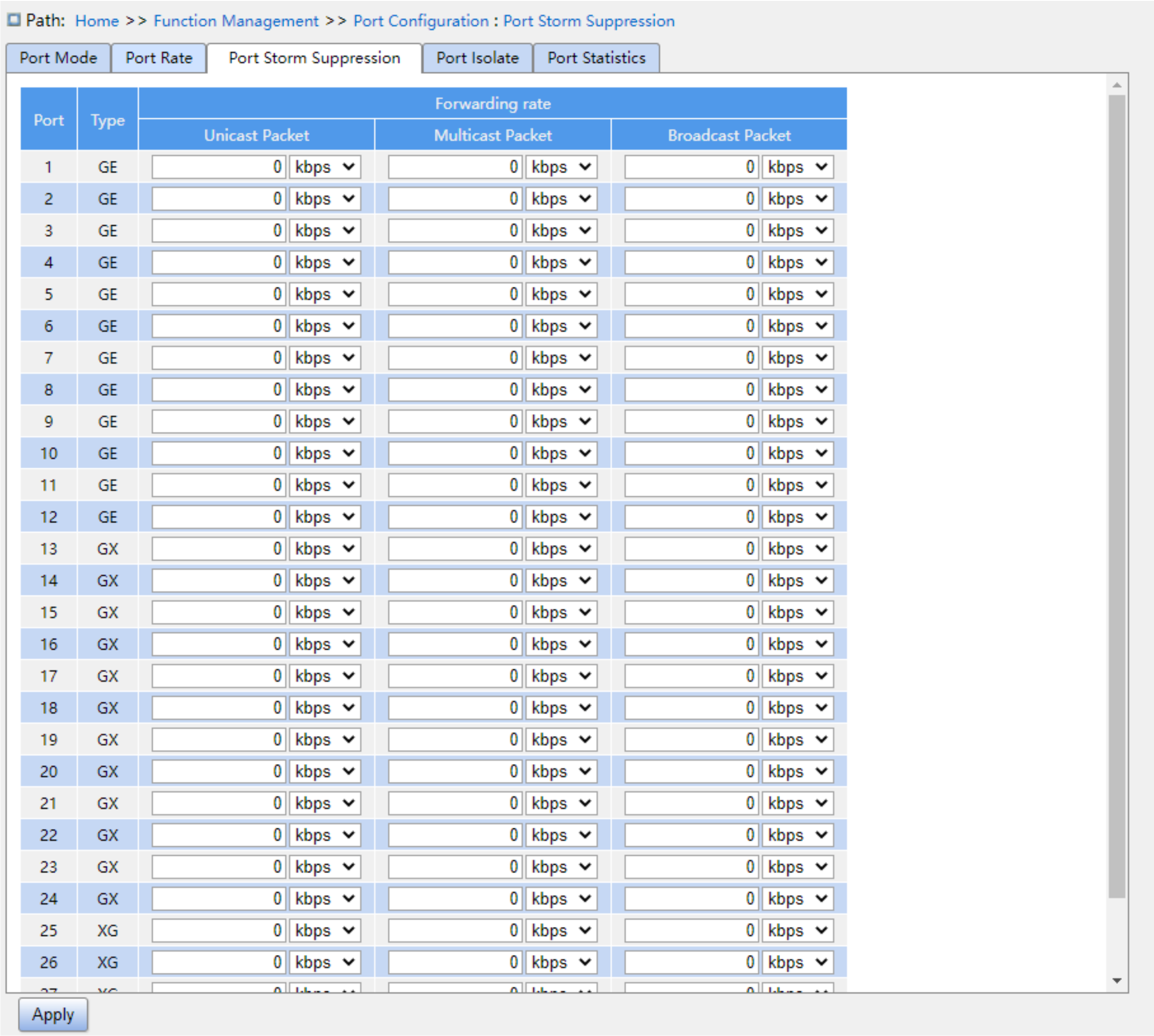


Figure 95 Port Storm Suppression

Forwarding Rate

Configuration options: Unicast Packet/Multicast Packet/Broadcast Packet

Configuration range: 10~13128147kbps/10~13128147fps/1~13128kfps/1~13128mbps

Default configuration: 0 (disable storm suppression).

Function: configure port forwarding rate threshold, this type of packet data above the threshold will be discarded.

4、Port Isolate configuration, as shown below.

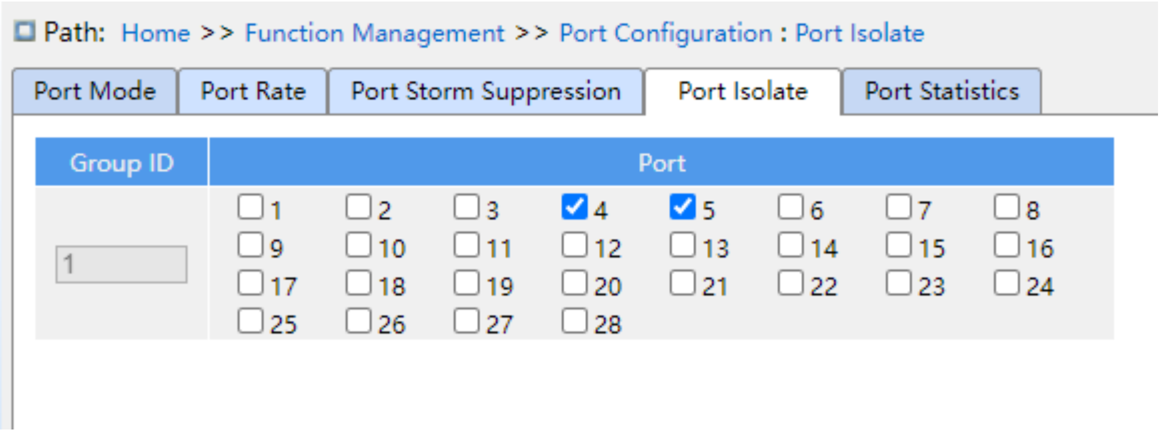


Figure 96 Port Isolate

Enable Port Isolate

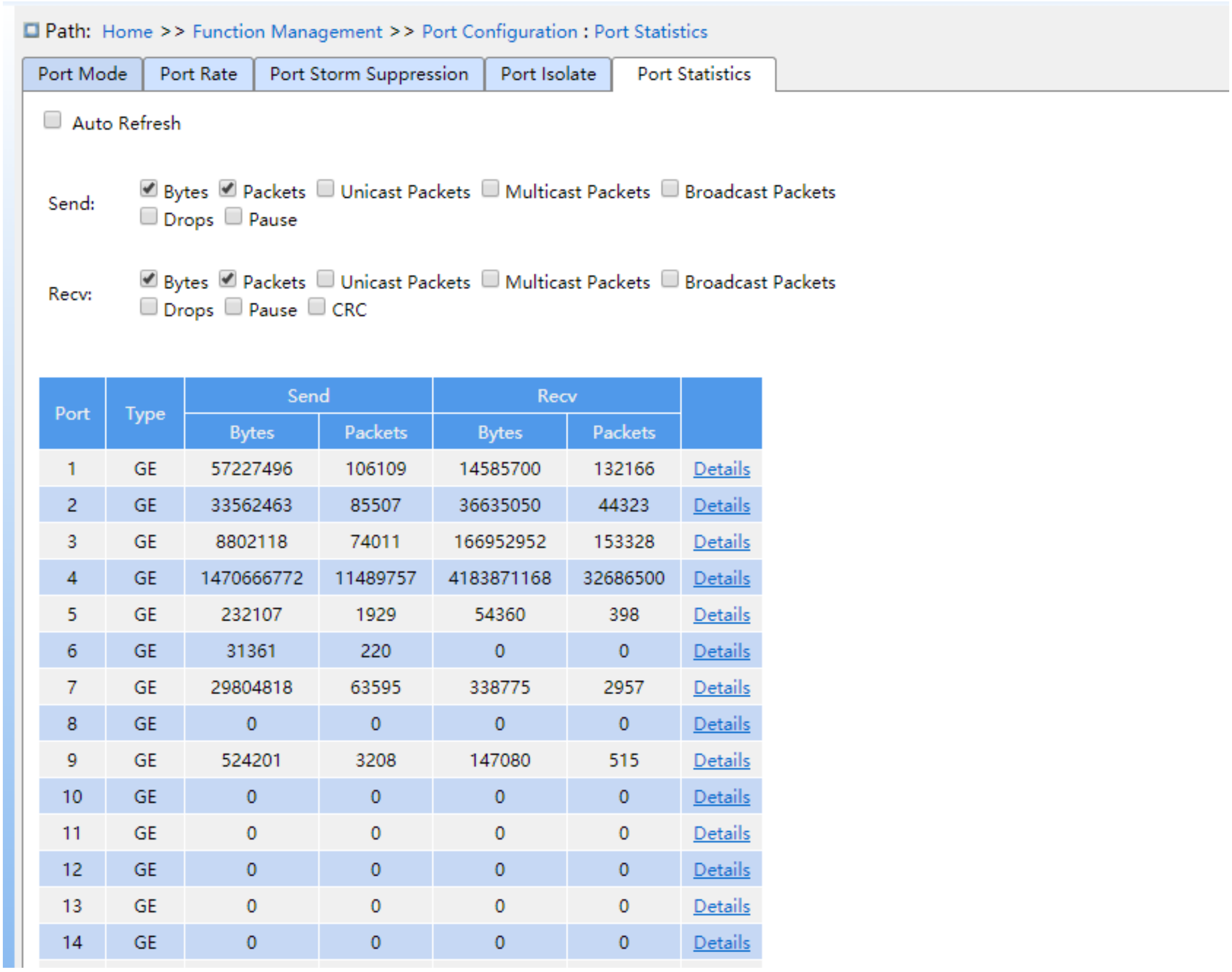
Configuration options: Enable/disable

Default configuration: Disable

Function: Enable or disable port isolate.

Note: there is only one port isolation group.

5. Port Statistics, as shown below.



Port	Type	Send		Recv		
		Bytes	Packets	Bytes	Packets	
1	GE	57227496	106109	14585700	132166	Details
2	GE	33562463	85507	36635050	44323	Details
3	GE	8802118	74011	166952952	153328	Details
4	GE	1470666772	11489757	4183871168	32686500	Details
5	GE	232107	1929	54360	398	Details
6	GE	31361	220	0	0	Details
7	GE	29804818	63595	338775	2957	Details
8	GE	0	0	0	0	Details
9	GE	524201	3208	147080	515	Details
10	GE	0	0	0	0	Details
11	GE	0	0	0	0	Details
12	GE	0	0	0	0	Details
13	GE	0	0	0	0	Details
14	GE	0	0	0	0	Details

Figure 97 Port Statistics

Bytes

Count the number of received/sent bytes.

Packets

Count the number of received/sent packets.

Unicast Packets

Count the number of received/sent unicast packets.

Multicast Packets

Count the number of received/sent multicast packets.

Broadcast Packets

Count the number of received/sent broadcast packets.

Drops

Count the number of messages dropped because receiving / sending conflicts.

Pause

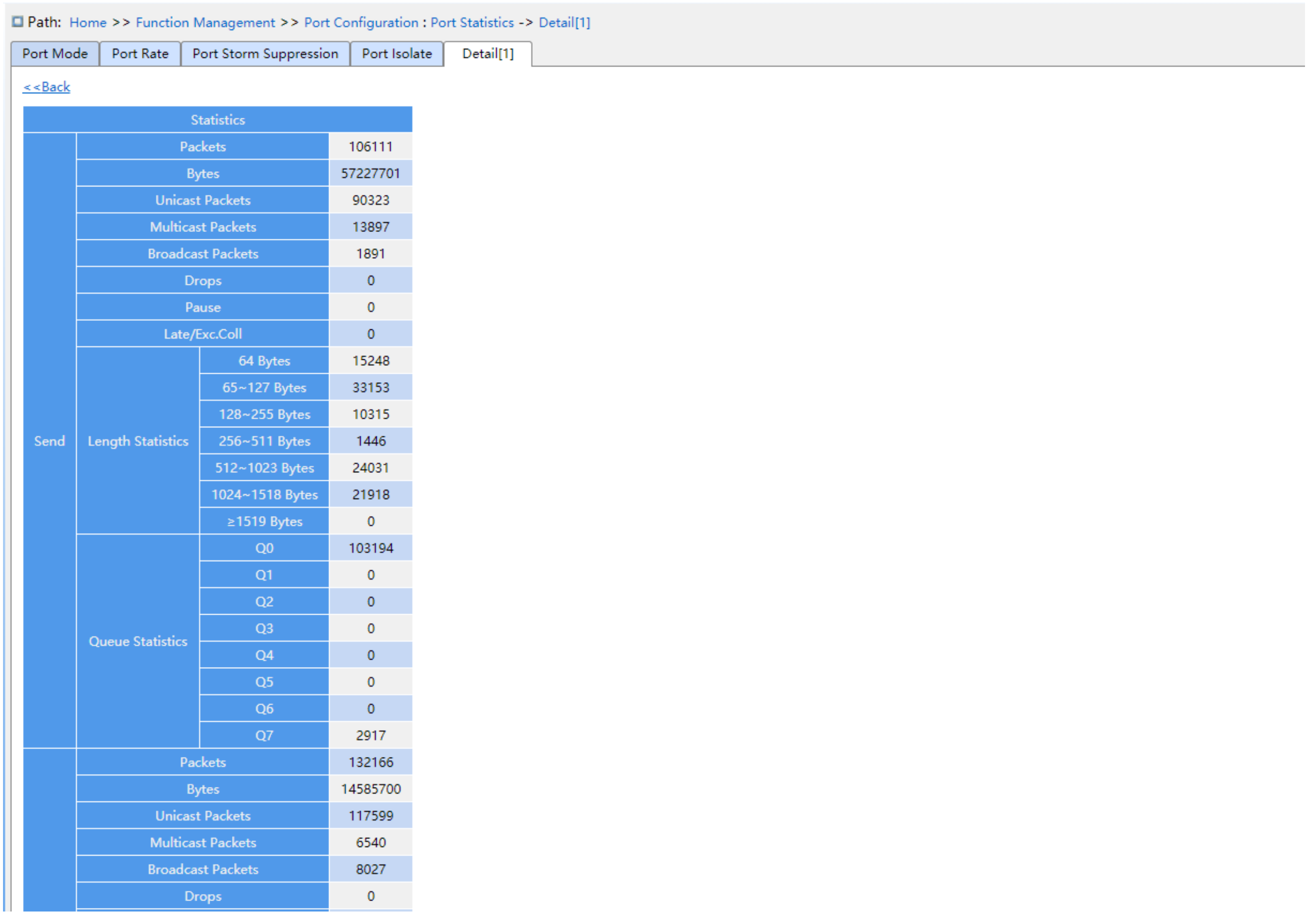
Count the number of received/sent Pause frames.

CRC

Count the number of received/sent CRC messages.

Click the port number corresponding details to enter the corresponding port detailed information statistics interface.

3. Port detail information statistics, as shown below.


Path: Home >> Function Management >> Port Configuration : Port Statistics -> Detail[1]

Port Mode | Port Rate | Port Storm Suppression | Port Isolate | Detail[1]

<<Back

Statistics			
Send	Packets		106111
	Bytes		57227701
	Unicast Packets		90323
	Multicast Packets		13897
	Broadcast Packets		1891
	Drops		0
	Pause		0
	Late/Exc.Coll		0
	Length Statistics	64 Bytes	15248
		65~127 Bytes	33153
		128~255 Bytes	10315
		256~511 Bytes	1446
		512~1023 Bytes	24031
		1024~1518 Bytes	21918
		≥1519 Bytes	0
	Queue Statistics	Q0	103194
		Q1	0
		Q2	0
		Q3	0
		Q4	0
		Q5	0
		Q6	0
		Q7	2917
	Packets		132166
	Bytes		14585700
	Unicast Packets		117599
	Multicast Packets		6540
	Broadcast Packets		8027
	Drops		0

Figure 98 Port detail information statistics

7.2 VLAN

7.2.1 VLAN Configuration

7.2.1.1 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.

7.2.1.2 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 2 shows the structure of an 802.1Q frame.

Table 2 802.1Q Frame Structure

DA	SA	802.1Q header				Length/type	Data	FCS
		TPID	PRI	CFI	VID			

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

TPID: 16 bits. It is used to identify a data frame carrying a VLAN tag. The value is 0x8100. The value of TPID specified in the 802.1Q protocol is 0x8100.

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

CFI: 1 bit, specifies whether an MAC address is encapsulated in the standard format in different transmission media. The value 0 indicates that an MAC address is encapsulated in the standard format and the value 1 indicates that an MAC address is encapsulated in non-standard format.

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.

7.2.1.3 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 Mode

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

Access: In access mode, the port can be added to only one VLAN. By default, all switch ports are access ports and belong to VLAN1. Packets forwarded by an access port do not have VLAN tags. Access ports are usually used to connect to terminals that do not support 802.1Q.

Trunk：In trunk mode, the port can be added to many VLAN. When sending PVID packets, the Trunk port can be set whether to carry the tag. It carries the tag when sending other packets. Trunk ports are usually used to connect network transmission devices.

Hybrid：In hybrid mode, the port can be added to many VLAN. You can set the type of packets to be received by a Hybrid port and whether the tag is carried when the Hybrid port sends packets. The Hybrid port can be used to connect network devices and user devices. The difference between a Hybrid port and a Trunk port is as follows: The Hybrid port does not carry the tag when sending packets from multiple VLANs and the Trunk port does not carry the tag only when sending PVID packets.

2. PVID

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

Caution:

- When configuring the PVID of a port, select one of the VLAN IDs allowed through the port; otherwise, the port may fail to forward packets.
- When the PVID tag is added to untagged packets, you can refer to PCP and DEI settings in

Figure 267 for the default PRI and CFI values of a port.

Table 3 shows how the switch processes received and forwarded packets according to the port mode, and PVID.

Table 3 Different Processing Modes for Packets

<table>
<tr><th colspan="2">Processing Received Packets</th><th colspan="2">Processing Packets to Be Forwarded</th></tr>
<tr><th>Untagged packets</th><th>Tagged packets</th><th>Port Mode</th><th>Packet Processing</th></tr>
<tr><td rowspan="3">Add PVID tags to packets:
➢ If the PVID is in the list of VLANs allowed through, accept the packet.
➢ If the PVID is not in the list of VLANs allowed through, discard the packet.</td><td rowspan="3">➢ If the VLAN ID in a packet is in the list of VLANs allowed through, accept the packet.
➢ If the VLAN ID in a packet is not in the list of VLANs allowed through, discard the packet.</td><td>Access</td><td>Forward the packet after removing the tag.</td></tr>
<tr><td>Trunk</td><td>Forward the packet according to the "Egress Tagging" configuration:
➢ Untag Port VLAN: If the VLAN ID in a packet is the same as PVID, and in the list of VLANs allowed through, forward the packet after removing the tag. If the VLAN ID in a packet is different from PVID, and in the list of VLANs allowed through, keep the tag and forward the packet.
➢ Tag All: If the VLAN ID in a packet is in the list of VLANs allowed through, keep the tag and forward the packet.</td></tr>
<tr><td>Hybrid</td><td>Forward the packet according to the "Egress Tagging" configuration:
➢ Untag Port VLAN: the same as above.
➢ Tag All: the same as above.
➢ Untag All: If the VLAN ID in a packet is in the list of VLANs allowed</td></tr>
</table>

			through, forward the packet after removing the tag.

7.2.1.4 Web Configuration

1. Configurate port link mode, as shown below.

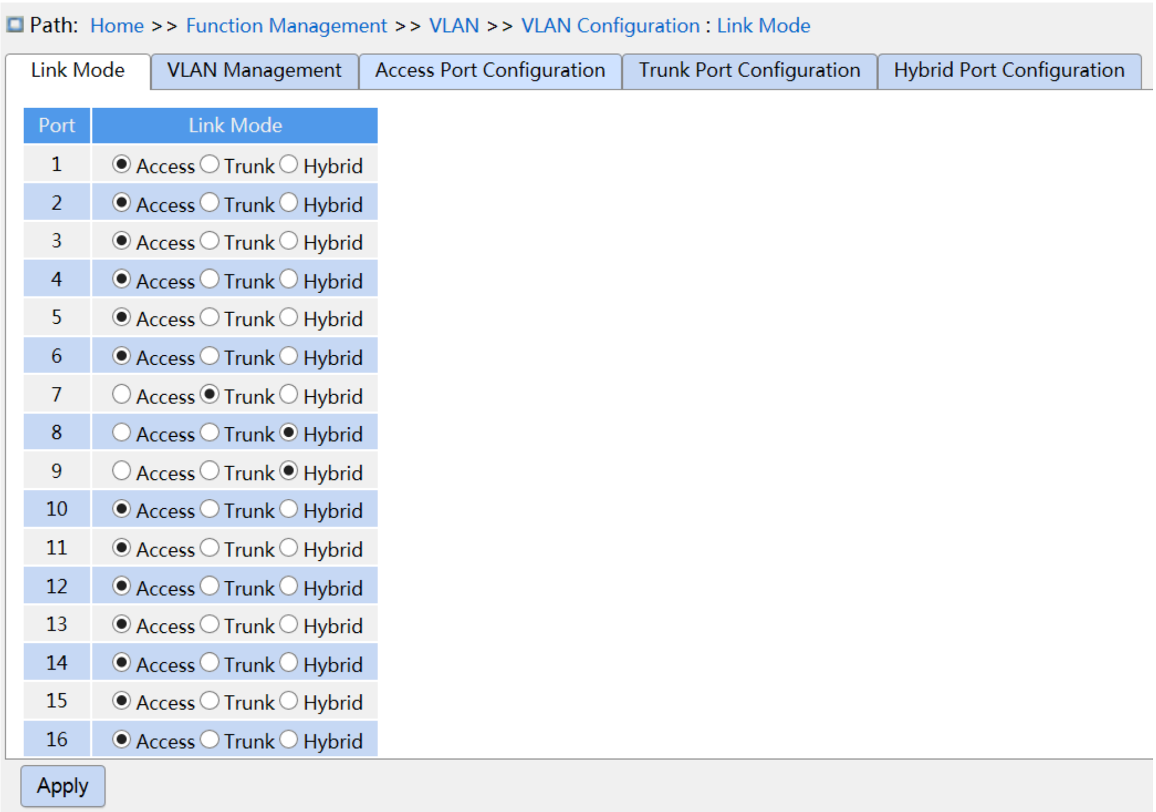


Figure 99 configurate port link mode

Link Mode

Configuration options: Access、Trunk、Hybrid

Default configuration: Access

Function: Configure the specified port link mode.

2. VLAN Management, as shown below.

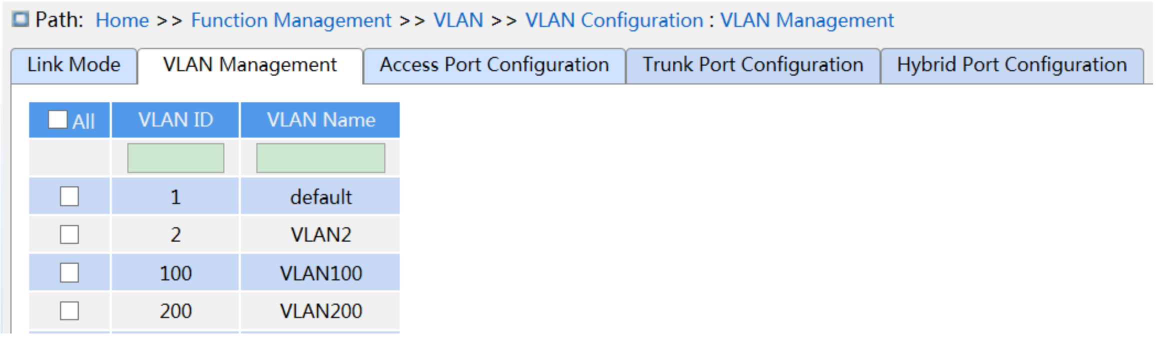


Figure 100 VLAN Management

VLAN ID

Configuration range: 1-4094

Default configuration: 1

Function: Create VLAN。

VLAN Name

Configuration range: 1-32 characters, include capital letters, lowercase letters, numbers, and underscores.

Function: configure VLAN name.

3. Access Port Configuration, as shown below.

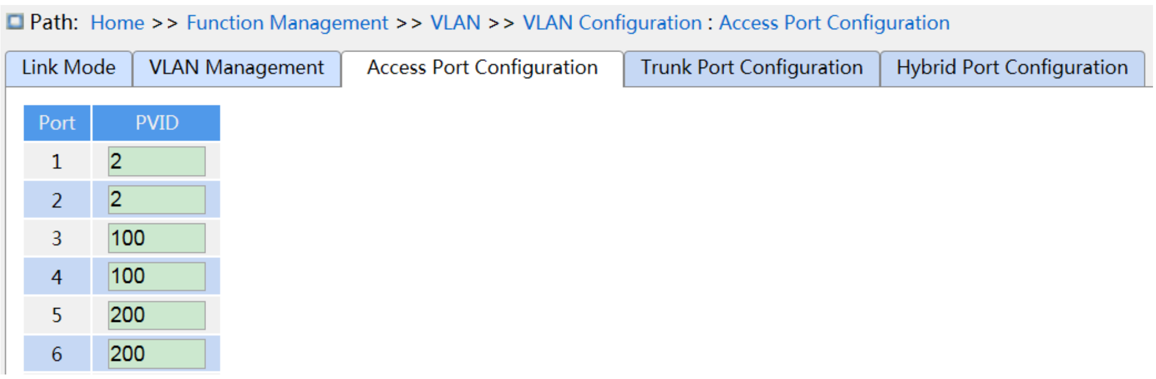


Figure 101 Configure Access Port

PVID

Configuration range: 1-4094

Default configuration: 1

Function: configure the default VLAN for the Access port.

Caution:

- The VLAN need to be created before configuring VLAN ID of Access port, the Trunk, Hybrid port are similar.

4. Trunk Port Configuration, as shown below.

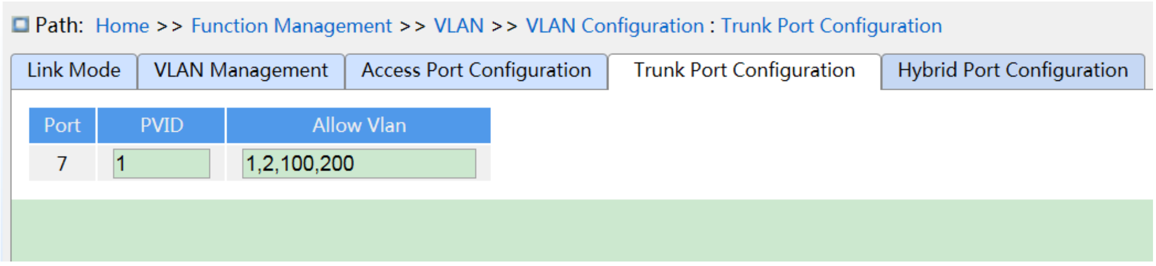


Figure 102 Trunk Port Configuration

PVID

Configuration range: 1-4094

Default configuration: 1

Function: Configure default VLAN of Trunk port.

Allowed VLAN

Configuration range: 1-4094, separated by half-angle comma ',' and a hyphen '-'（M-N，M must be less than N）, for example: 2, 33, 34-77.

Default configuration: 1

Function: Configure allowed VLAN of Trunk port.

5. Hybrid Port Configuration, as shown below.

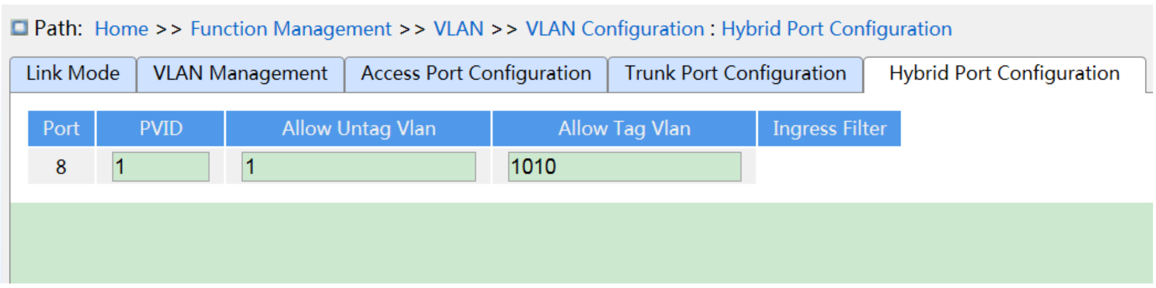


Figure 103 Hybrid Port Configuration

PVID

Configuration range: 1-4093

Default configuration: 1

Function: Configure default VLAN of Hybrid port.

Allowed Untag VLAN

Configuration range: 1-4093, separated by half-angle comma ',' and a hyphen '-'（M-N， M must be less than N）, for example: 2,33,34-77.

Default configuration: 1

Function: Configure allowed Untag VLAN of Hybrid port.

Allowed Tag VLAN

Configuration range: 1-4093, separated by half-angle comma ',' and a hyphen '-'（M-N，M must be less than N）, for example: 2,33,34-77.

Default configuration: None

Function: Configure allowed Tag VLAN of Hybrid port.

7.2.1.5 Typical Configuration Example

As shown in Figure 104, 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 4 shows specific configuration.

Table 4 VLAN Configuration

VLAN	**Configuration**
VLAN2	Set port 1 and port 2 of Switch A and B to access ports, and port 7 to trunk port.
VLAN100	Set port 3 and port 4 of Switch A and B to access ports, and port 7 to trunk port.
VLAN200	Set port 5 and port 6 of Switch A and B to access ports, and port 7 to trunk port.

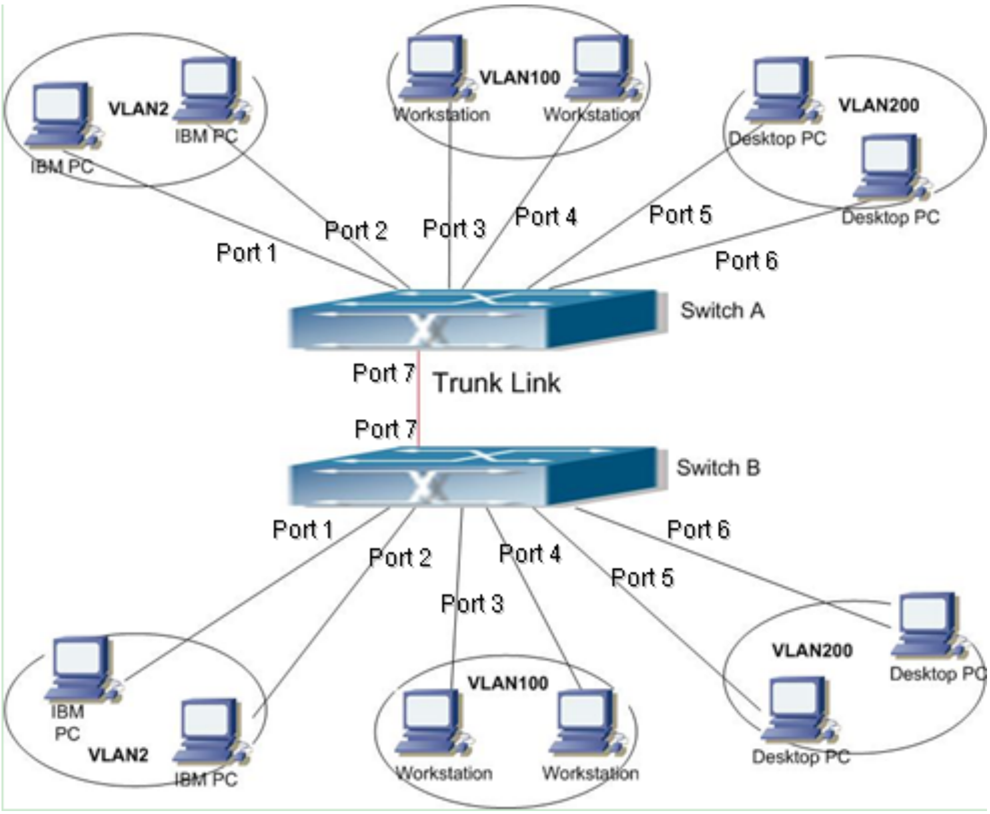


Figure 104 VLAN Application

Configurations on Switch A and Switch B:

1. Configure allowed access VLANs to 1,2,100,200, as shown in Figure 101.

2. Configure ports 1, 2 as access ports, port VLAN as 2. Configure ports 3, 4 as access ports, port VLAN as 100. Configure ports 5, 6 as access ports, port VLAN as 200. Configure port 7 as trunk port, port VLAN as 1, allowed VLANs as 1,2,100,200, as shown in Figure 102.

3. Keep all the other parameters default.

7.2.2 GVRP

7.2.2.1 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.

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

NOTE

Note：

An application entity indicates a GARP-enabled port.

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

Hold Timer: when a GARP-enabled switch receives a registration message, it starts s Hold timer rather than sending out the Join message immediately. When the Hold timer times out, it will put all registration information received during this time in a same Join message and send it out, reducing the message quantity for network stability.

Join Timer: in order to guarantee that the Join message can be reliably transmitted to other switches, the GARP-enabled switch will wait for a time interval of a Join timer after sending the first Join message. If the switch does not receive a Join In message during this time, it will send out a Join message again, otherwise, it won't send the second message.

Leave Timer: when a GARP-enabled switch wishes other switches to cancel its attribute information, it sends out a Leave message. Other GARP-enabled switches that receive this message will enable a Leave timer. If they do not receive a Join message until the timer times out, they will cancel this attribute information.

LeaveAll Timer: When a switch enables GARP, it starts a LeaveAll timer at the same time. When the timer times out, the switch will send a LeaveAll message to other GARP-Enabled switches and let them re-register their all attribute information, and then restart the LeaveAll timer to begin a new cycle.

7.2.2.2 GVRP Introduction

GVRP (GARP VLAN Registration Protocol) is a GARP application and is based on the GARP working mechanism to maintain the VLAN dynamic registration information of the device and propagate the information to other devices.

The GVRP-enabled device can receive VLAN registration information from other devices and dynamically update the local VLAN registration information, and the device can propagate the local VLAN registration information to other devices, reaching the consistency of VLAN information in all devices in the same LAN. The VLAN registration information propagated by GVRP contains not only the manually configured local static registration information, but also the dynamic registration information from other devices.

CAUTION

Caution:

GVRP port and port channel are mutually exclusive. The port in a port channel cannot be configured as a GVRP port; the GVRP port cannot be added to a port channel.

7.2.2.3 Web Configuration

1. Golbal enable GVRP protocol, and configure timer, as shown below.

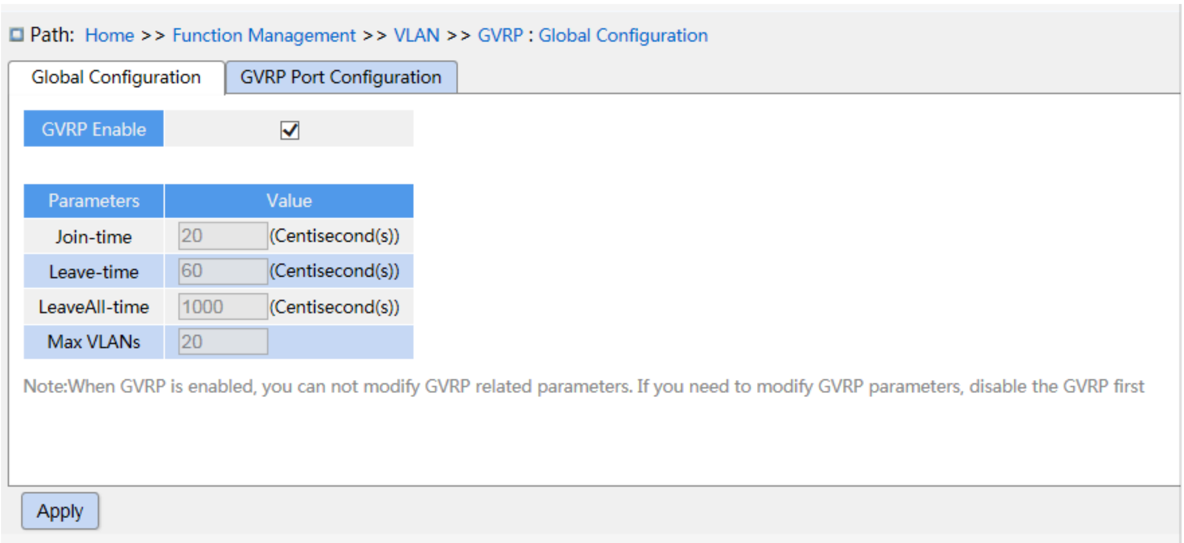


Figure 105 GVRP Global Configuration

GVRP enable

Configuration options: Enable/disable

Default configuration: Disable

Function: Enable or disable GVRP.

Join timer

Configuration options: 1-20（centisecond）

Default configuration: 20（centisecond）

Function: Configure Join timer value.

Leave timer

Configuration options: 60-300（centisecond）

Default configuration: 60（centisecond）

Function: Configure Leave timer value.

LeaveAll timer

Configuration options: 1000-5000（centisecond）

Default configuration: 1000（centisecond）

Function: Configure leave all timer value.

Description: if the LeaveAll timer for different devices times out at the same time, multiple LeaveAll messages are sent simultaneously to increase the number of unnecessary messages, in order to avoid the LeaveAll timer timeout on different devices at the same time, The value of the actual Leave all timer is a random value which is greater than the leave all timer value, less than 1.5 times the leave all timer value.

Max VLANs

Configuration range: 1~4094

Default configuration: 20

Function: Configure the registered dynamically max VLANs of GVRP port.

CAUTION

Caution:

- Disable GVRP before configuring GVRP timer and Max VLANs.

2. GVRP Port Configuration, as shown below.

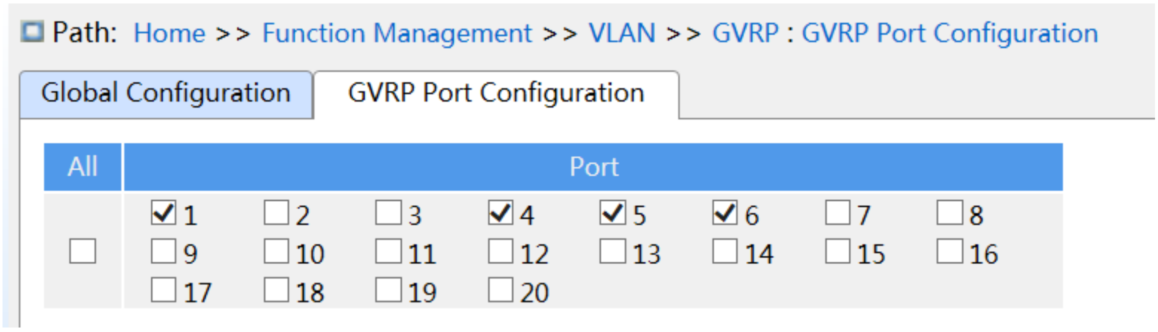


Figure 106 GVRP Port Configuration

Port

Configuration options: Enable/disable

Default configuration: Disable

Function: enable or disable GVRP of port.

Caution:

- The GVRP port should be configured as a trunk port;
- The GVRP port diffuses the VLAN property of other GVRP ports with the UP status.

7.2.2.4 Typical Configuration Example

As Figure 107 shows, GVRP needs to be enabled on devices so that VLAN information is dynamically registered and updated between device A and device B.

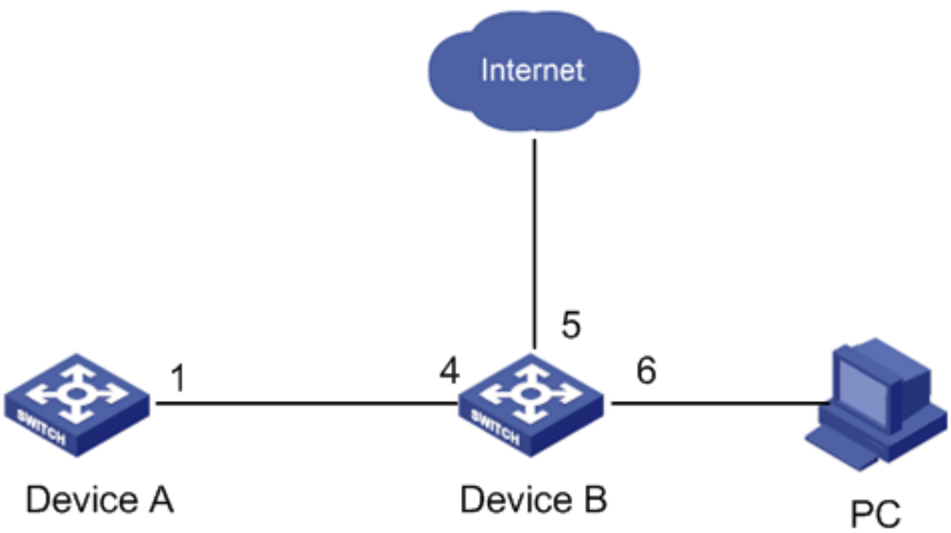


Figure 107 GVRP Configuration Example

Device A configuration are as follows:

1. Configure port 1 to trunk port, allowed VLANs to 1.
2. Enable global GVRP, as shown in Figure 105.
3. Enable GVRP on port 1, as shown in Figure 106.

Device B configuration are as follows:

1. Configure port 4 to trunk port, allowed VLANs to 1; configure port 5 to access port, allowed VLANs to 5; configure port 6 to trunk port, allowed VLANs to 1, 6.
2. Enable global GVRP, as shown in Figure 105.
3. Enable GVRP on port 4, 5, 6, as shown in Figure 106.

Port 1 of Switch A can register the same VLAN information as that of port 5 and 6 of Switch B。

7.2.3 PVLAN Configuration

7.2.3.1 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.

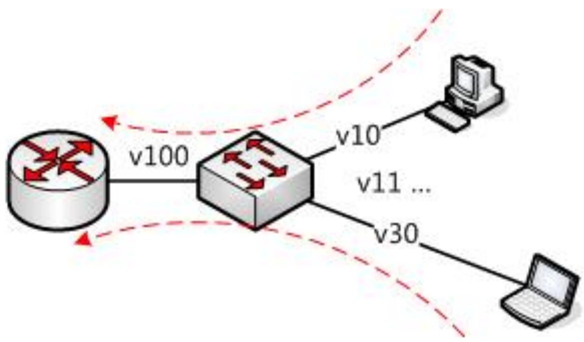


Figure 108 PVLAN Application

As shown in Figure 108, 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.

7.2.3.2 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 hybrid and are assigned to the shares domain VLAN and all isolation domains; the downlink ports are set to hybrid and are assigned to the shared domain VLAN and own isolation domain.
- The packets sent by PVLAN member ports are Untag.

7.2.3.3 Web Configuration

1. Uplink Port Configuration, as shown in below.

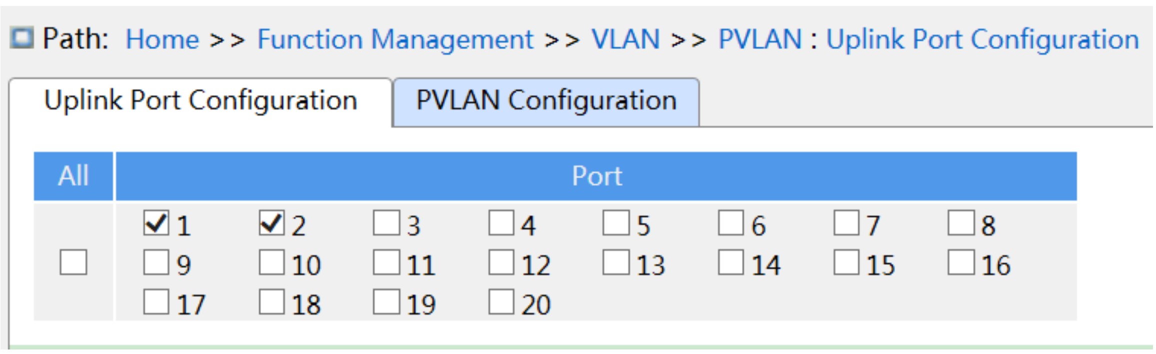


Figure 109 Configure Uplink Port

Port

Configuration options: Enable/disable

Default configuration: Disable

Function: configure port as uplink port

2. PVLAN Configuration, as shown below.

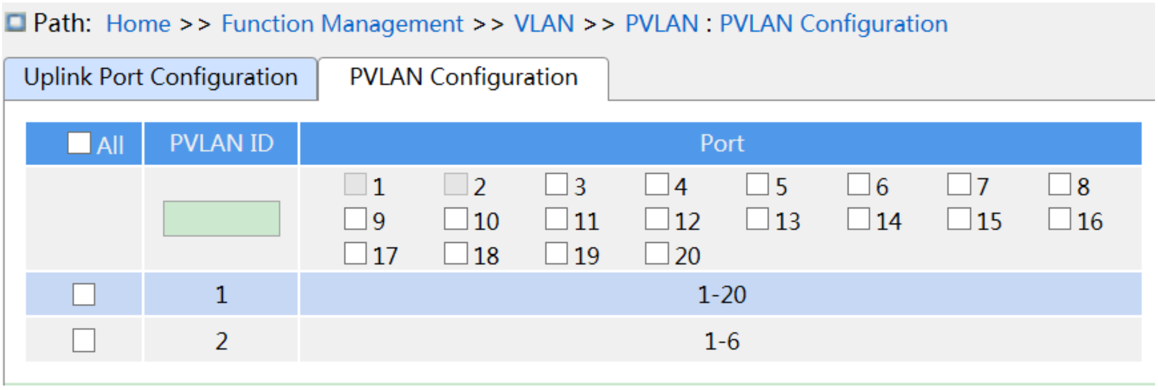


Figure 110 Configure PVLAN

PVLAN ID

Configuration options: 1-4094

Default configuration: 1

Function: configure the PVLAN ID of port.

Port

Configuration options: Enable/disable

Default configuration: 1-28

Function: specify PVLAN port.

7.2.3.4 Typical Configuration Example

Figure 111 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.

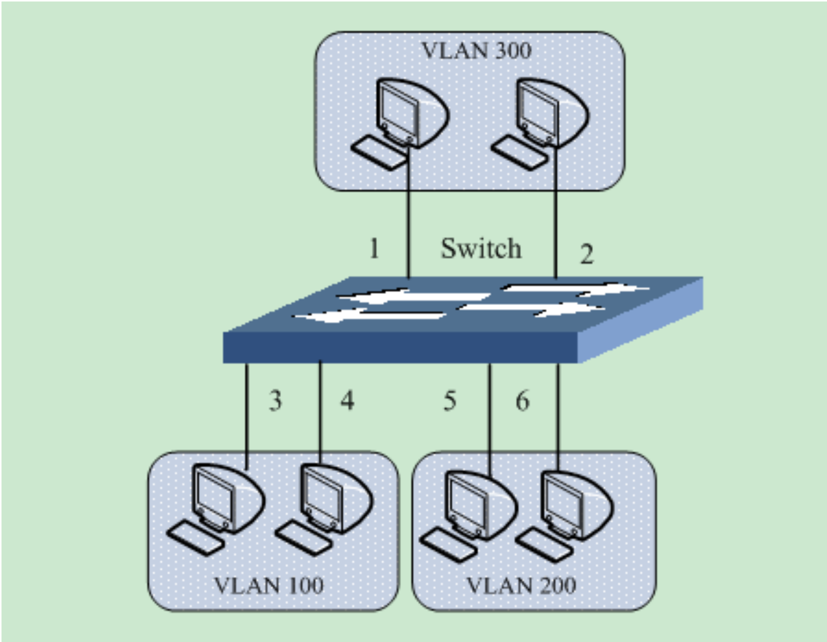


Figure 111 PVLAN Configuration Example

Switch configuration:

1. Configure ports 1, 2 to hybrid ports, port VLAN to 300, egress tagging to Untag All, allowed VLANs to 100,200,300.

2. Configure ports 3, 4 to hybrid ports, port VLAN to 100, egress tagging to Untag All, allowed VLANs to 100,300.

3. Configure ports 5, 6 to hybrid ports, port VLAN to 200, egress tagging to Untag All, allowed VLANs to 200,300.

4. Keep all the other parameters default.

7.2.4 VLAN STATUS

Check the port VLAN status, as shown below.

	Port																			
VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1											✓	✓							✓	
100	✓	✓	✓	✓																
200	✓	✓			✓	✓														
300	✓	✓	✓	✓	✓	✓														
1002							✓													
1003								✓												
1010																		✓		
2002															✓					
3500																				
3555																	✓			
3600									✓				✓							
3666																				
3777																				
3888														✓						
4001																				
4003										✓										

Figure 112 Port VLAN status

7.3 IP Configuration

7.3.1 IP Address Configuration

1. View the switch IP address through the Console port

Log in to the CLI of the switch through the console port. Run the command **show interface vlan 1** in the privileged user configuration mode to view the IP address of the switch, as shown in the red circle of Figure 113.

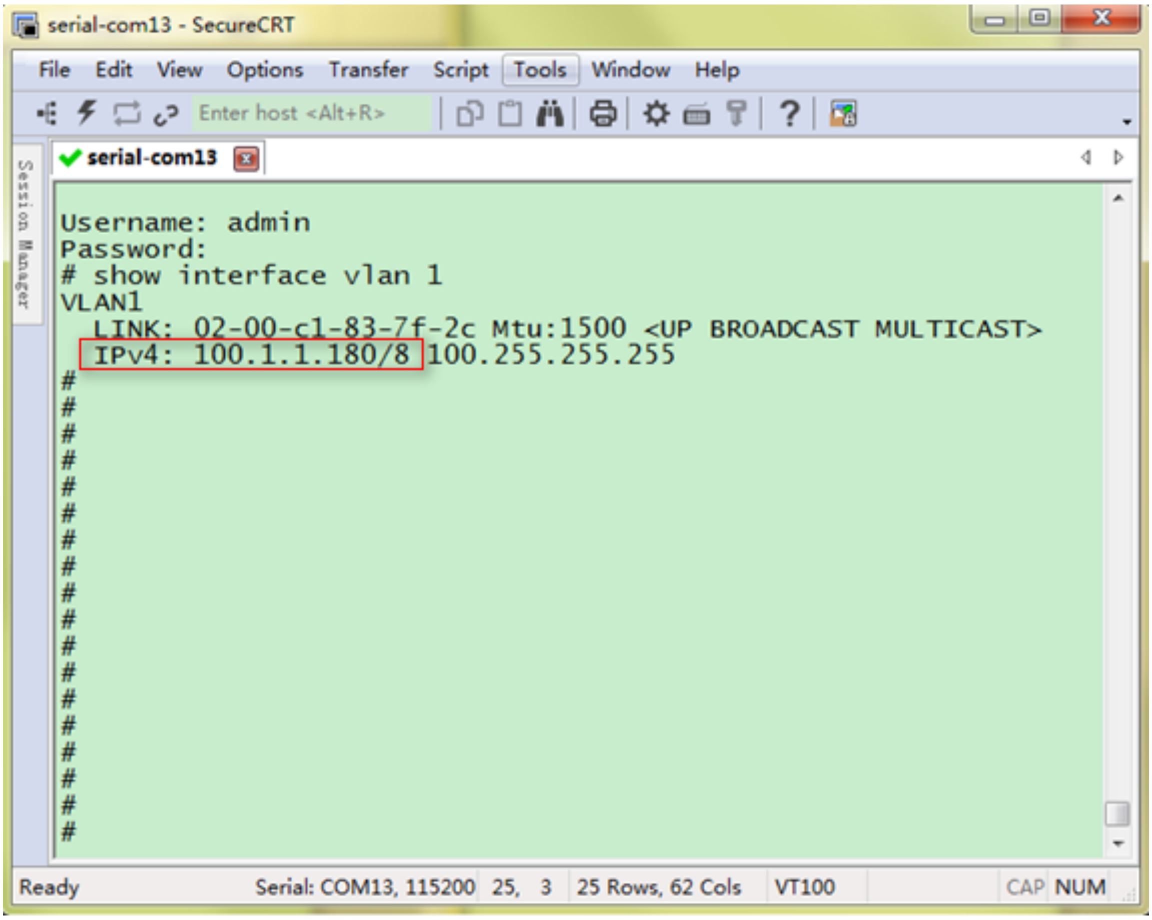


Figure 113 Displaying IP Address

2. Create IP 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 an IP interface.

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

3. Configure primary IP address

The primary IP address of the switch can be obtained by manual configuration and automatic, as shown below.

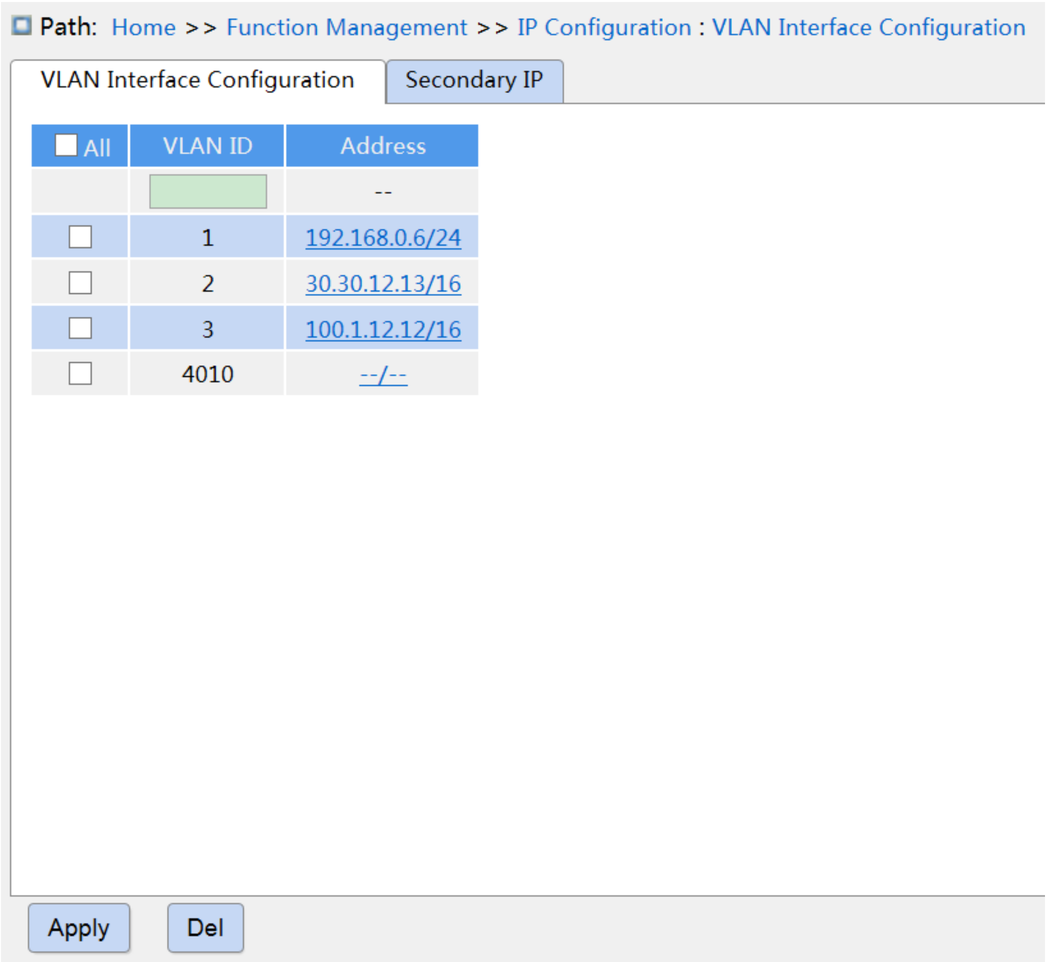


Figure 114 Vlan interface configuration

VLAN ID

Function: Configure VLAN property of IP interface, and only the VLAN member port can access the current IP interface.

Address

Function: IP address and mask obtained by the VLAN interface.

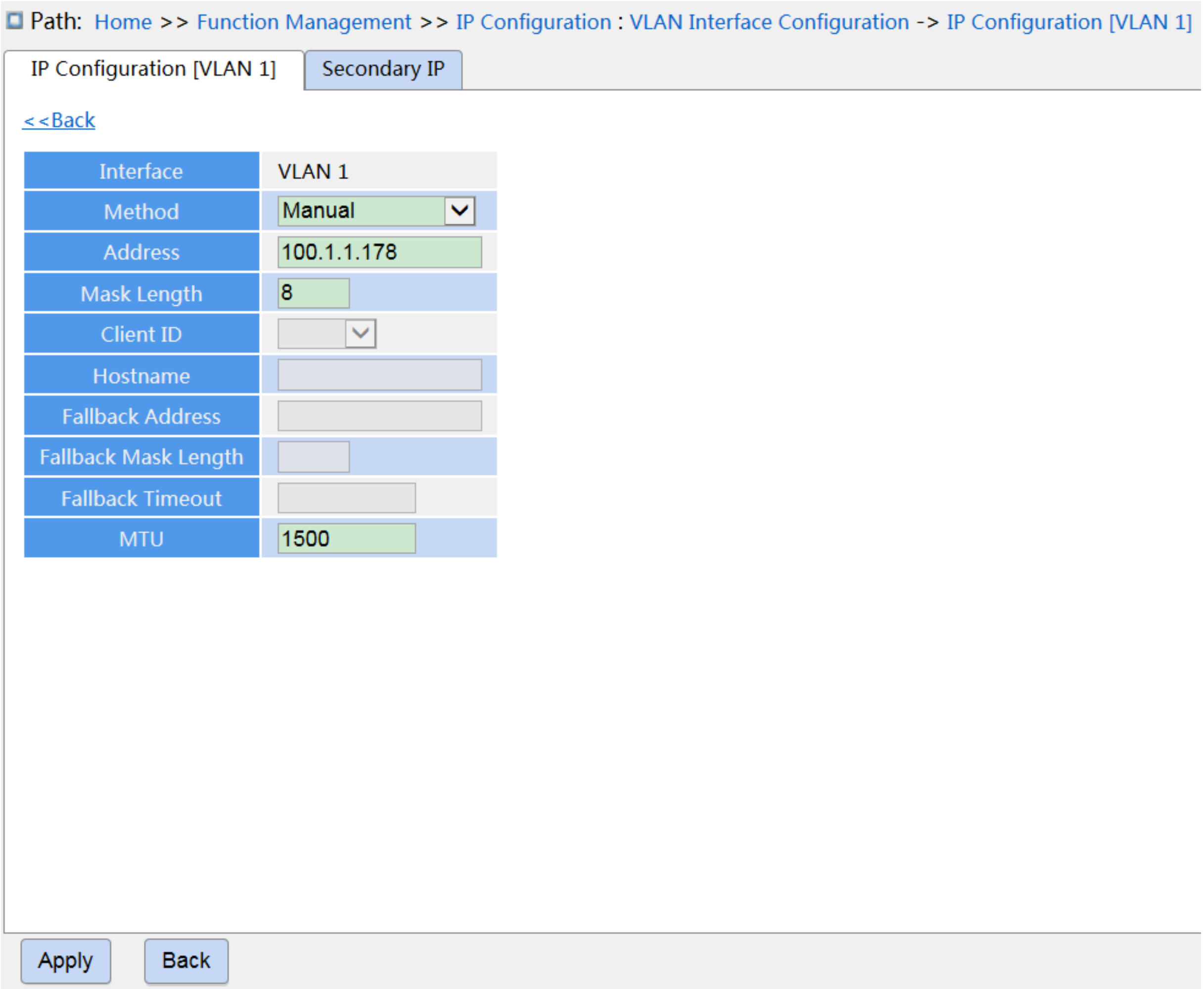


Figure 115 IP address configuration

Method

Configuration options: None/DHCP/Manual

Function: Manual, you need to manually configure the IP address and subnet mask. The switch automatically gets the IP address through DHCP protocol as DHCP client if enable DHCP, in this case, there should be DHCP server to assign IP address and subnet mask to client in the netwrok.

Address

Configuration format: A.B.C.D

Function: IP address of the Vlan interface.

Mask Length

Function: a subnet mask is a 32-bit number, consisting of a sequence "1" and a sequence "0". "1" corresponds to the network number field and the subnet number field, while "0" corresponds to the host number field. The mask length is the number of 1 in the mask.

Client ID

Configuration options: Hex/ASCII/Port

Function: The detail filled information of carried option61 filed when specified IP send the DHCP requirement. Hex refers to filling option61 with type 01+mac address. ASCII refers to filling option61 with type 00+string. Port refers to filling option61 with the corresponding interface mac.

Hostname

Configuration range: 0-63 characters

Function: Configure the host name of the VLAN interface.

Fallback Address

Configuration format: A.B.C.D

Function: After the Vlan interface obtains the IP address timeout through the DHCP protocol, set the address to the fallback IP address.

Fallback Mask Length

Function: a subnet mask is a 32-bit number, consisting of a sequence "1" and a sequence "0". "1" corresponds to the network number field and the subnet number field, while "0" corresponds to the host number field. The mask length is the number of 1 in the mask.

Fallback Timeout

Configuration range: 0~4294967295s

Function: when the value is non-zero, the switch obtains the IP address attempt time through the DHCP protocol, need to configure the IP address manually at this time, after the attempt time out, the manually configured IP address takes effect. When the value is zero, the switch will try again and again until the IP address is obtained through the DHCP protocol, no need to manually configure the IP address.

MTU

Configuration range: 68~9600

Dedault configuration：1500

Function: Configure the maximum packet length that can pass on the IP layer.

4. Secondary IP Configuration

Manually configure the secondary IP address of the switch's IP interface，as shown below.

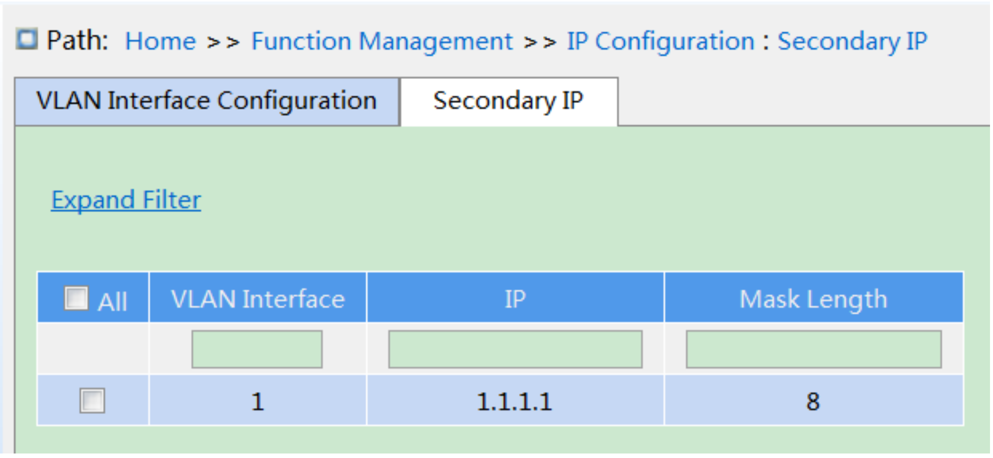


Figure 116 Secondary IP Configuration

VLAN Interface

Function: configure the VLAN property of the IP interface, and only this VLAN member port can access the current IP interface.

IP

Configure format: A.B.C.D

Function: manually configure IP address.

Mask Length

Function: a subnet mask is a 32-bit number, consisting of a sequence "1" and a sequence "0". "1" corresponds to the network number field and the subnet number field, while "0" corresponds to the host number field. The mask length is the number of 1 in the mask.

Caution:

- Each IP interface corresponds to a primary IP address and may correspond to multi-secondary IP addresses;
- Different IP interfaces should be configured with primary and secondary IP addresses for different network segments.

7.4 Port Aggregation

7.4.1 Static Aggregation

7.4.1.1 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.

7.4.1.2 Implementation

As shown in Figure 117, 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.

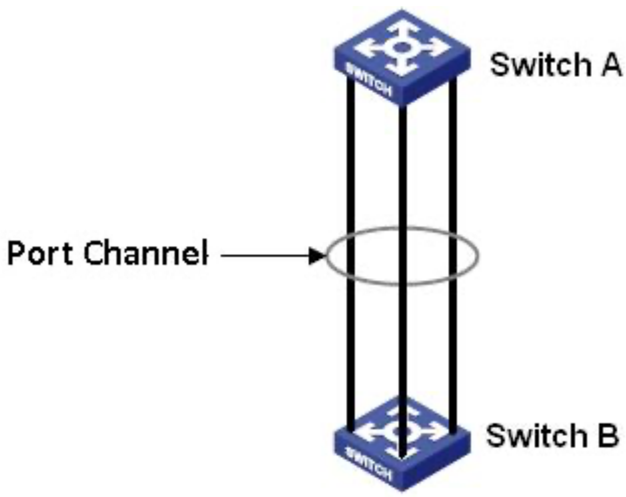


Figure 117 Port Channel

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.

Caution:

- A port can be added to only one port group.
- Only full duplex ports can join an aggregation.
- The port in a port channel cannot be enabled LACP, and a port enabled LACP 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.
- Redundant port in this document refers to DT-Ring port，DT-Ring backup port，DRP ring port, DRP backup port, RSTP port, and MSTP port.

7.4.1.3 Web Configuration

1. Static aggregation configuration, as shown below.

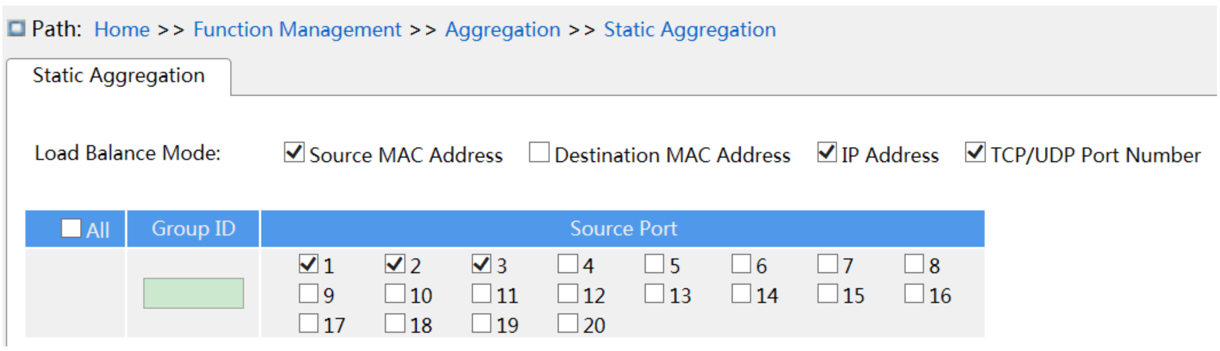


Figure 118 Static Aggregation Configuration

Load Balance Mode

Configuration options: Source MAC address/ destination MAC/IP address/ TCP/UDP port number

Default configuration: Source MAC address/IP address/ TCP/UDP port number

Function: configure load balance mode of aggregation group.

Description: the source mac address balances the traffic according to the source mac address; the destination mac address balances the traffic according to the destination mac address; the IP address balances the traffic according to the IP address; the port number of TCP / UDP balances the traffic according to the TCP/UDP port number.

Group ID

Configuration range: 1-10

Function: Configure group ID.

Description: the member ports of the same aggregation group have the same port properties. The number of aggregation groups depends on the device port, and each aggregation group supports up to 8 member ports.

Source Port

Configuration options: Enable/disable

Function: Select the port to join the specified aggregation group.

7.4.1.4 Typical Configuration Example

As shown in Figure 117, 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 1. 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 1, 2, and 3 of switch A to port group 1, as shown in Figure 118.
2. Add port 1, 2, and 3 of switch B to port group 1, as shown in Figure 118.

7.4.2 LACP

7.4.2.1 Introduction

Link Aggregation Control Protocol (LACP) is based on the IEEE802.3ad standard. It is used to exchange information with the peer port over Link Aggregation Control Protocol Data Unit (LACPDU), in order to select a member port in the dynamic aggregation group.

7.4.2.2 Implementation

A port enabled with LACP informs the peer port of its LACP priority of the local equipment, equipment MAC address, LACP priority of the port, port number and key value by sending an LACPDU message. The peer port negotiates with the local port after receiving the

LACPDU message:

1. Compare the IDs of the equipment at both ends (equipment ID = equipment LACP priority+ equipment MAC address). At first, compare the LACP priorities. If the LACP priorities are the same, compare their MAC addresses. Select the equipment with a smaller ID as the master equipment.

2. Compare the port IDs of the master equipment (port ID = LACP priority of the port + port number). At first, compare the LACP priorities of the ports. If the port LACP priorities are the same, compare the port numbers. Select the port with a smaller ID as the reference port.

3. If this port and reference port have the same key values, and the same port attribute configurations in Up state, and the peer ports of this port and the reference port have the same key values and port attribute configurations, this port can become a member port of the dynamic aggregation group.

7.4.2.3 Web Configuration

1. Configure LACP priority, as shown below.

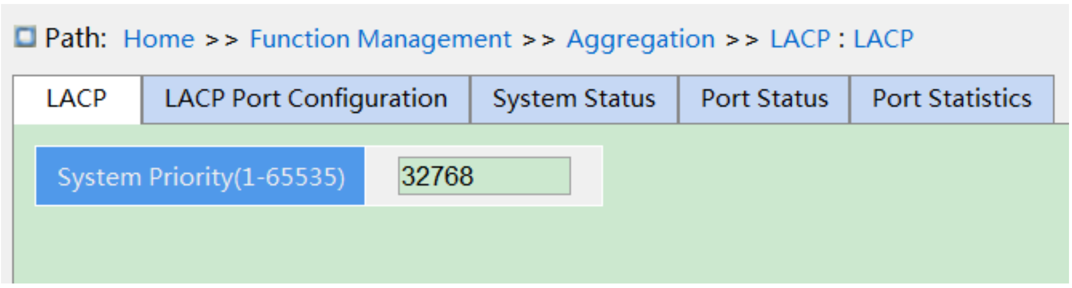


Figure 119 Configure LACP Priority

LACP

Configuration range: 1-65535

Default configuration: 32768

Function: Configure LACP priority, used to select the main device when LACP negotiation.

2. LACP Port Configuration, as shown below.

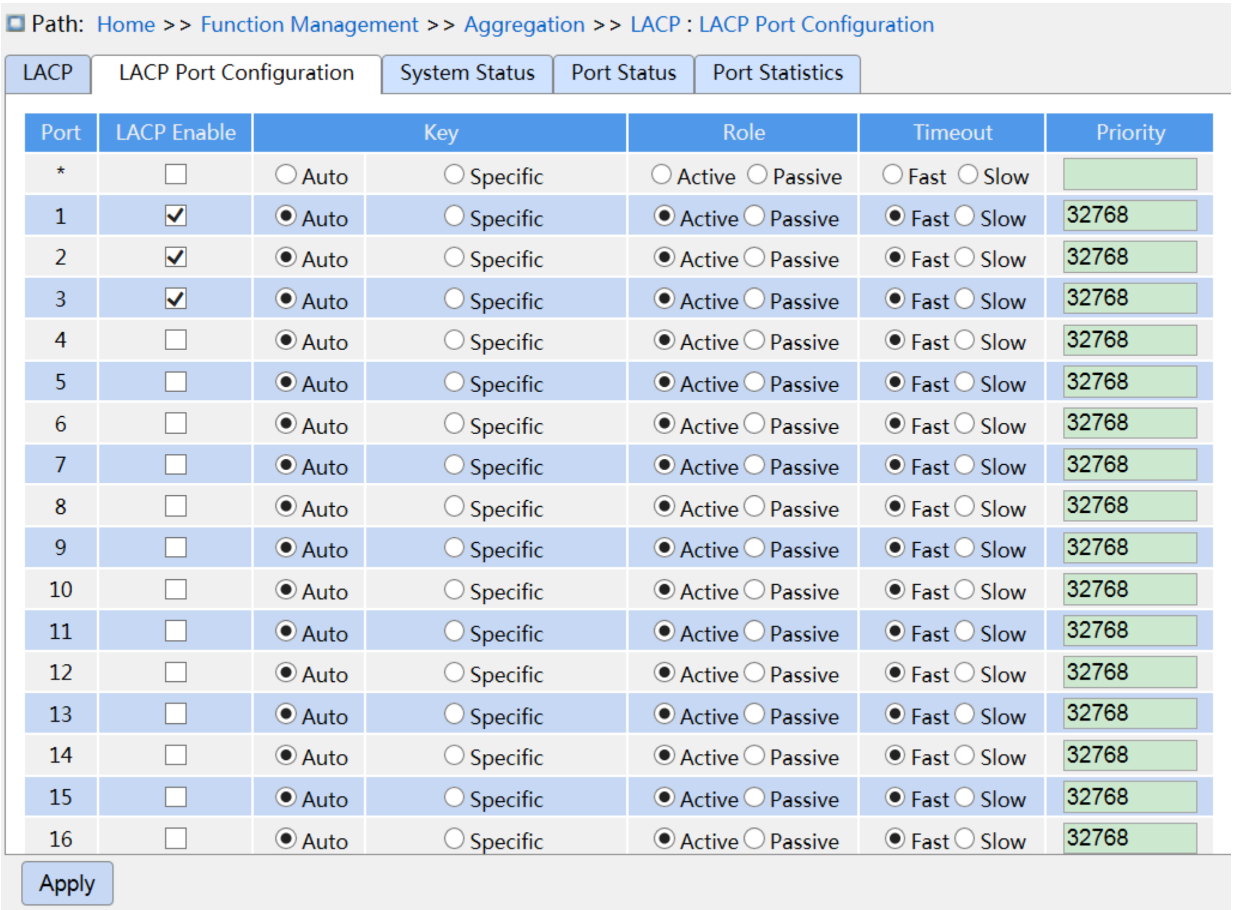


Figure 120 LACP port configuration

LACP Enable

Configuration options: Enable/disable

Default configuration: Diable

Function: whether enable LACP of port.

Key

Configuration options: Auto/specific（1~65535）

Default configuration: Auto

Function: Configure port key value. Key value is determined by port rate if selecting Auto, key=1（10Mb）；key=2（100Mb）；key=3（1000Mb），ports with different key values cannot be added to dynamic aggregation groups.

Role

Configuration options: Active/passtive

Default configuration: Active

Function: select the role of the LACP. The active port will send the LACPDU message to the end port actively; the passive port receives the LACPDU message to the opposite end and sends the LACPDU message to the end port.

Caution:

At least one of the two ports connected is active, otherwise the two ends will not be able to exchange information.

Timeout

Configuration options: Fast/slow

Default configuration: Fast

Function: Configure the active port to send LACPDU message time interval. The fast refers to time interval is 1s and the slow refers to time interval is 30s.

Priority

Configuration range: 1~65535

Default configuration: 32768

Function: Configure port LACP priority, use to select reference ports. Ports with low priority in the main device are selected as reference ports.

3. View LACP system status, as shown below.

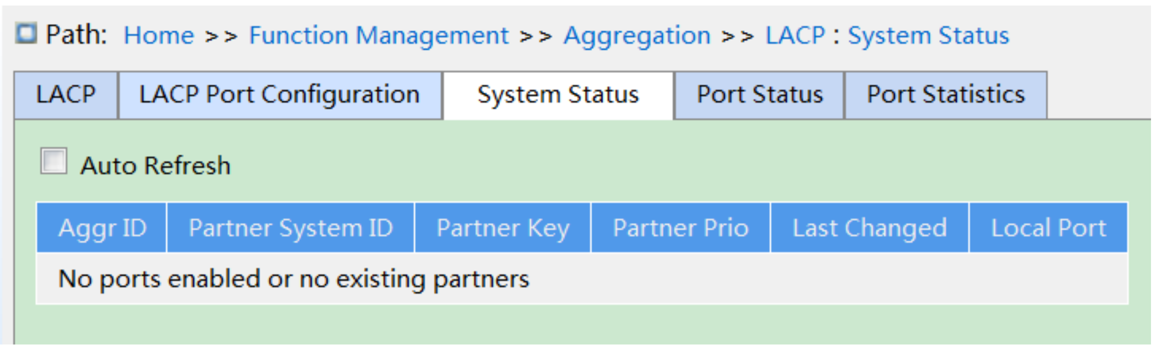
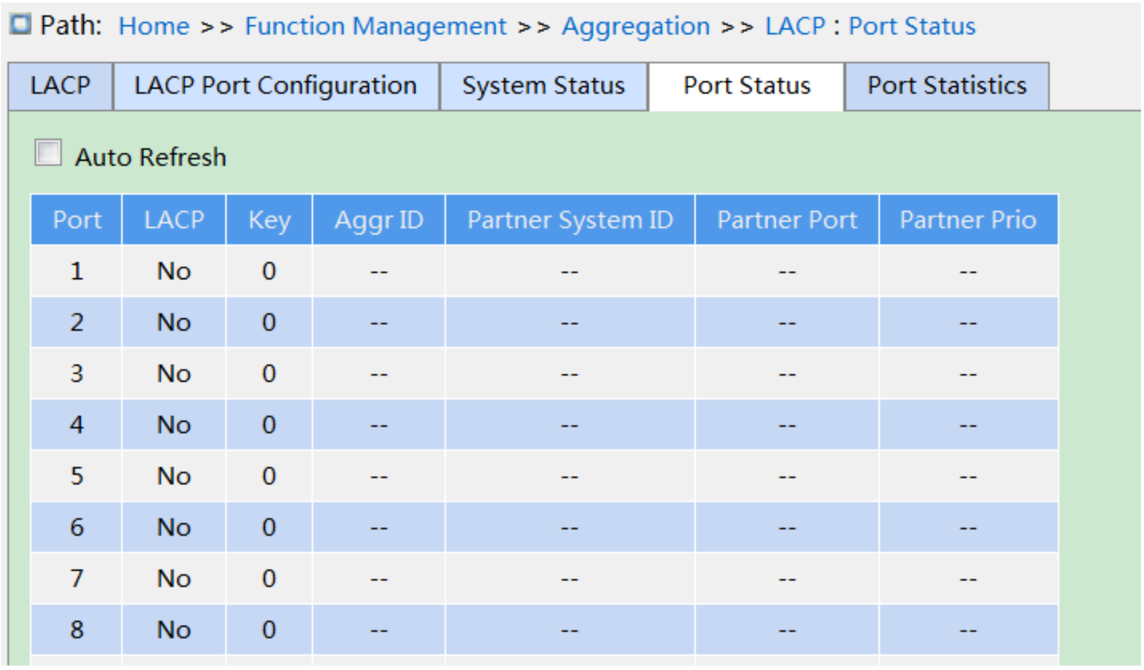


Figure 121 View LACP System Status

4. View LACP port status, as shown below.



Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	No	0	--	--	--	--
2	No	0	--	--	--	--
3	No	0	--	--	--	--
4	No	0	--	--	--	--
5	No	0	--	--	--	--
6	No	0	--	--	--	--
7	No	0	--	--	--	--
8	No	0	--	--	--	--

Figure 122 View LACP port status

LACP Status

Displaying options: Yes/No

Function: Display LACP status of port. “Yes” refers to LACP is enable and port is up status. “No” refers to LACP is disable and port is down status

5. View LACP port statistics, as shown below.

Path: Home >> Function Management >> Aggregation >> LACP : Port Statistics

LACP | LACP Port Configuration | System Status | Port Status | Port Statistics

☐ Auto Refresh

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0

Figure 123 View LACP Port Statistics

7.4.2.4 Typical Configuration Example

As shown in Figure 117, 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 1. 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. Enable LACP on port 1, 2, and 3 of switch A , as shown in Figure 120.
2. Enable LACP on port 1, 2, and 3 of switch B , as shown in Figure 120.

7.5 Redundancy

7.5.1 DT-Ring

7.5.1.1 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.

7.5.1.2 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.

7.5.1.3 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 124 CD Link Fault；

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.

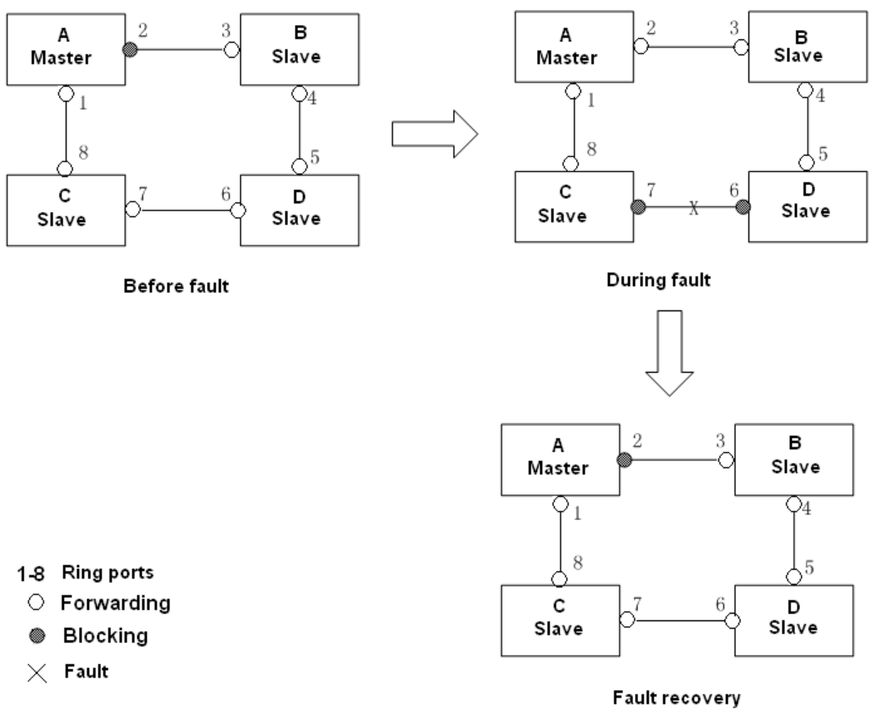


Figure 124 CD Link Fault

4. If link AC is faulty, as shown in Figure 125.

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.

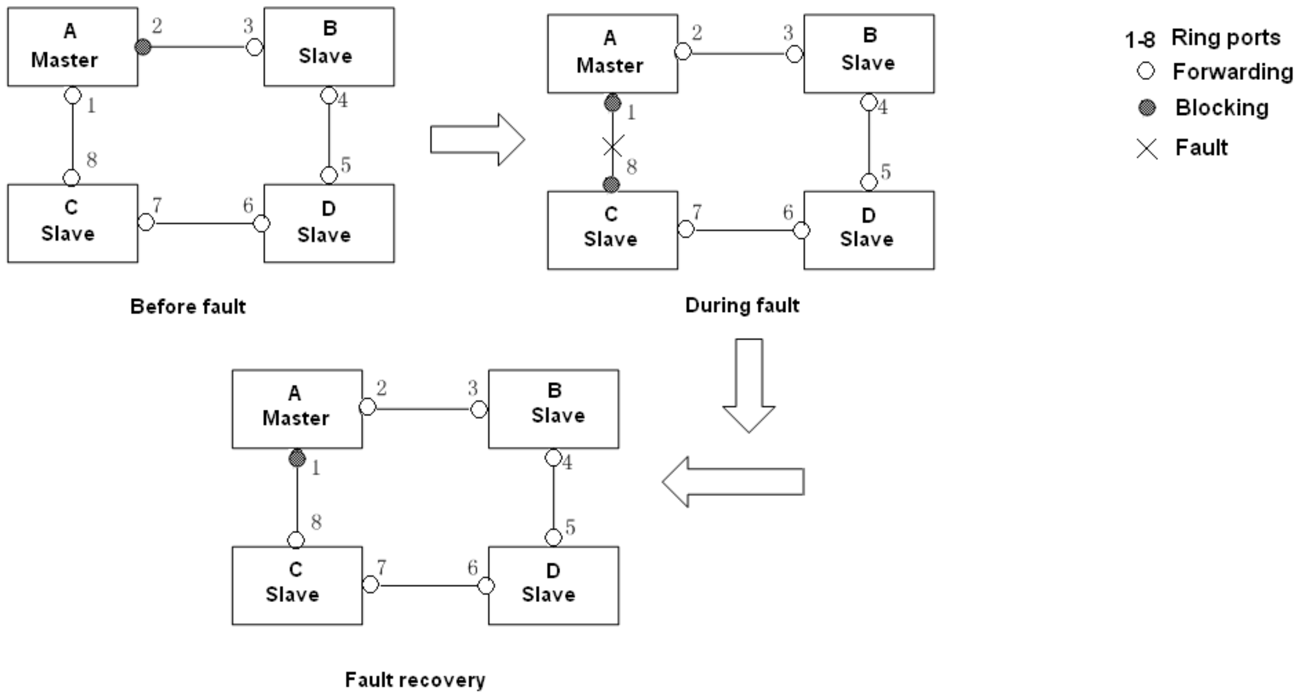


Figure 125 DT-Ring Link Fault

Caution:

Link status change affects the status of ring ports.

DT-Ring-VLAN Implementation

DT-Ring-VLAN allows the packets of different VLANs to be forwarded in different paths. Each forwarding path for a VLAN forms a DT-Ring-VLAN. Different DT-VLAN-Rings can have different masters. As shown in Figure 126, 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.

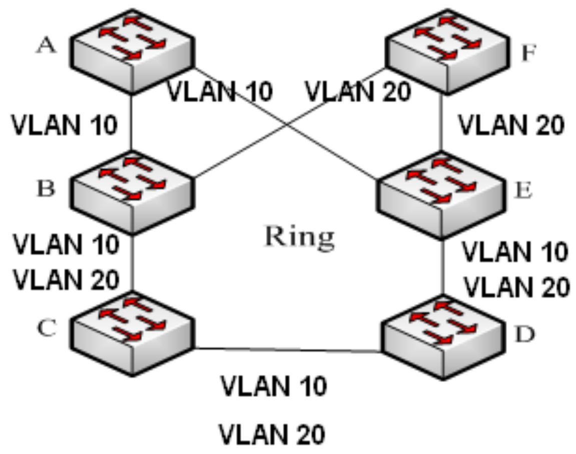


Figure 126 DT-Ring-VLAN

Note:

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

DT-Ring+ Implementation

DT-Ring+ can provide backup for two DT rings, as shown in Figure 127. 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.

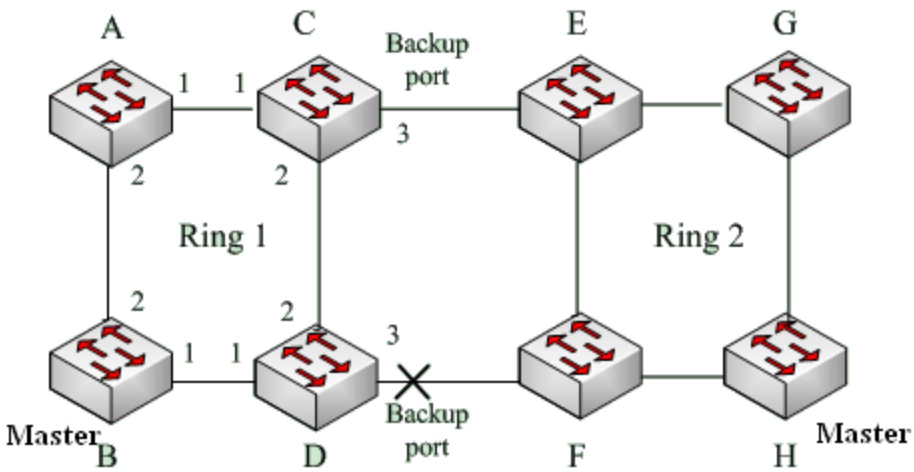


Figure 127 DT-Ring+ Topology

Caution:

Link status change affects the status of backup ports.

7.5.1.4 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.

7.5.1.5 Web Configuration

1. Configure DT-Ring redundant ring mode, as shown in Figure 128.

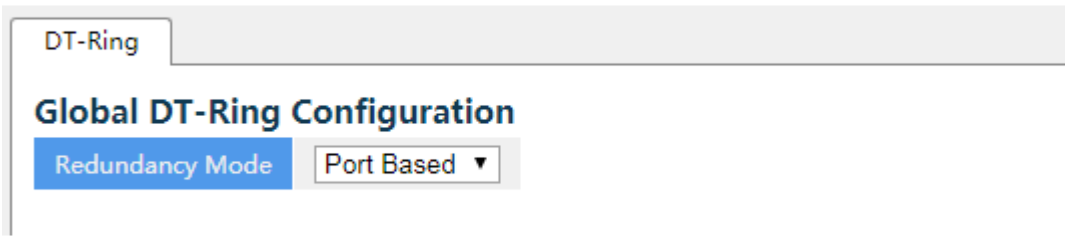


Figure 128 Redundant Ring Mode Configuration

Redundancy Mode

Options: Port Based/Vlan Based

Default: Port Based

Function: Choose DT-Ring 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. Configure DT-Ring-Port and DT-Ring-VLAN, as shown in Figure 129and Figure 130.

DT-Ring Configuration

All	Domain ID	Domain Name	Station Type	Ring Port-1	Ring Port-2	DT-Ring+	Backup Port	Vlan List
	1	a	Master	1	2	Enable	3	

Figure 129 DT-Ring-Port Configuration

DT-Ring Configuration

All	Domain ID	Domain Name	Station Type	Ring Port-1	Ring Port-2	DT-Ring+	Backup Port	Vlan List
	1	a	Master	1	2	Enable	3	1-3,5

Figure 130 DT-Ring-VLAN Configuration

Domain ID

Range: 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

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.
- 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 the isolation group are configured as DT-Ring ports and backup ports at the same time, and DT-Ring ports and backup ports cannot be added to the isolation group.

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.

CAUTION

Caution:

Do not configure a ring port as a backup port.

VLAN List

Options: all created VLANs

Function: Select the VLANs for the ring port. When there are multiple VLANs, you can separate the VLANs by a comma (,) and an en dash (-), where an en dash is used to separate two consecutive VLAN IDs and a comma is used to separate two inconsecutive VLAN IDs.

3. View and modify DT-Ring configuration, as shown in Figure 131.

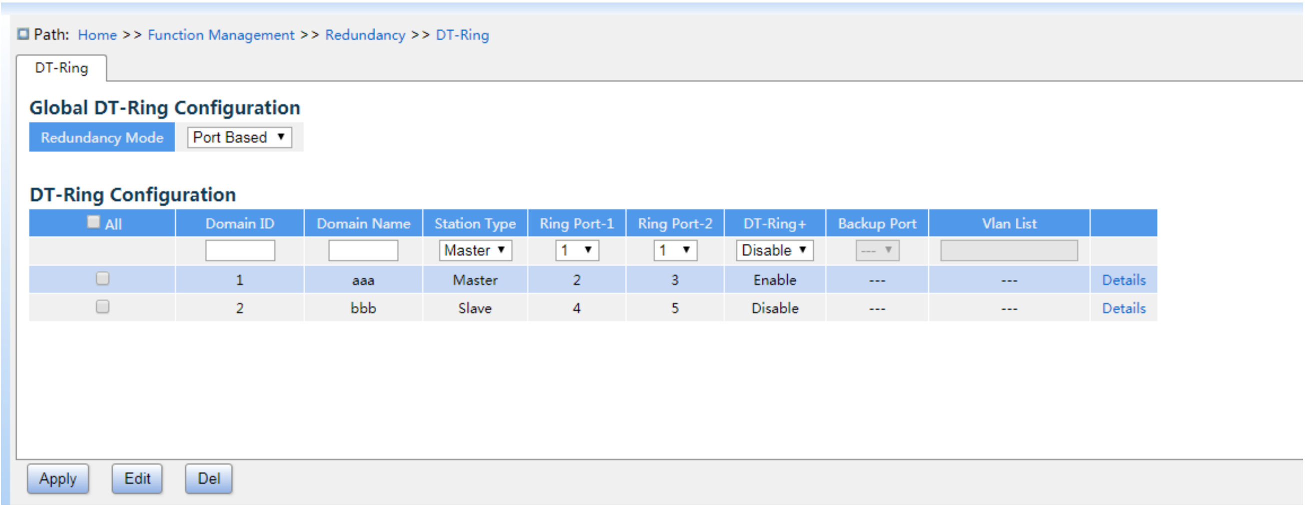


Figure 131 DT-Ring Configuration

Select a DT-Ring entry, click <Modify> to edit the DT-Ring entry configuration; click <Delete> to delete the designated DT-Ring entry.

4. Click a DT-Ring entry in Figure 131 to show DT-Ring and port status, as shown in Figure 132.

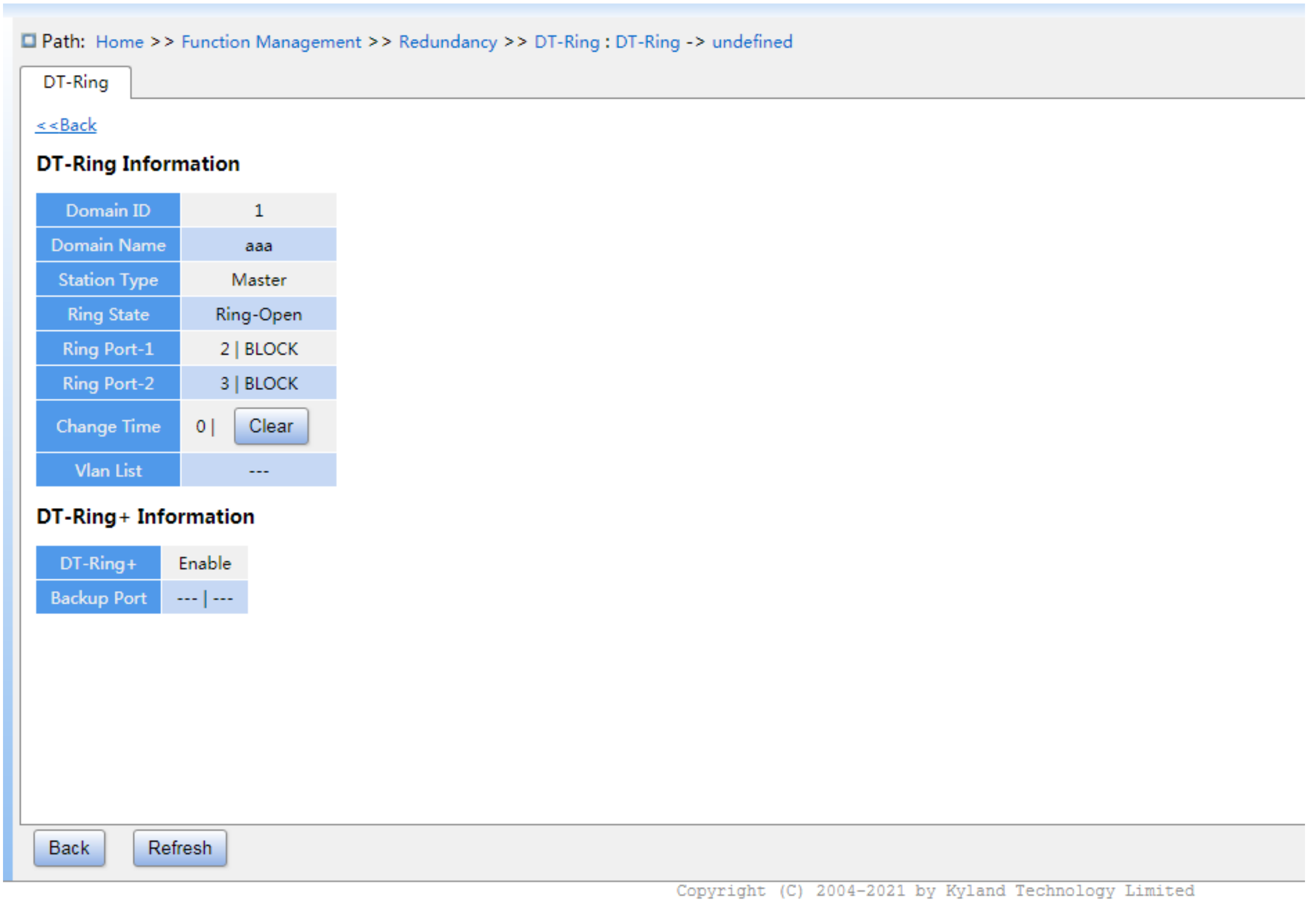


Figure 132 DT-Ring State

7.5.1.6 Typical Configuration Example

As shown in Figure 127 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. Configure domain ID to 1, domain name to a, ring port to 1, 2, station type to slave, DT-Ring+ to disable, do not set backup port, as shown in Figure 129.

Configuration on Switch B:

2. Configure domain ID to 1, domain name to a, ring port to 1, 2, station type to master, DT-Ring+ to disable, do not set backup port, as shown in Figure 129；

Configuration on Switch C and Switch D:

3. Configure domain ID to 1, domain name to a, ring port to 1, 2, station type to slave, DT-Ring+ to enable, backup port to 3, as shown in Figure 129；

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

4. Configure domain ID to 2, domain name to b, ring port to 1, 2, station type to slave, DT-Ring+ to disable, do not set backup port, as shown in Figure 129；

Configuration on Switch H:

5. Configure domain ID to 2, domain name to b, ring port to 1, 2, station type to master, DT-Ring+ to disable, do not set backup port, as shown in Figure 129；

7.5.2 DRP

7.5.2.1 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.

7.5.2.2 Concept

1. DRP Modes

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

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

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

2. DRP Port Statuses

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

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

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.

7.5.2.3 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 5 Vector of Announce Packet

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

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

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

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

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

The parameters in Table 5 Vector of Announce Packet are compared in the following procedure:

1. The value of link status is checked first. The device with a larger link status value is considered to have a larger vector.

2. If the two compared devices have the same link status value, the values of CRC degradation status are compared. The device with a larger CRC degradation status value is considered to have a larger vector. If the CRC degradation status value of all compared devices is 1, the device with a larger CRC degradation rate value is considered to have a larger vector.

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

Note:

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

➢ Implementation of DRP-Port-Based mode

The roles of switches are as follows:

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

The fault recovery procedure is shown in Figure 133 :

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.

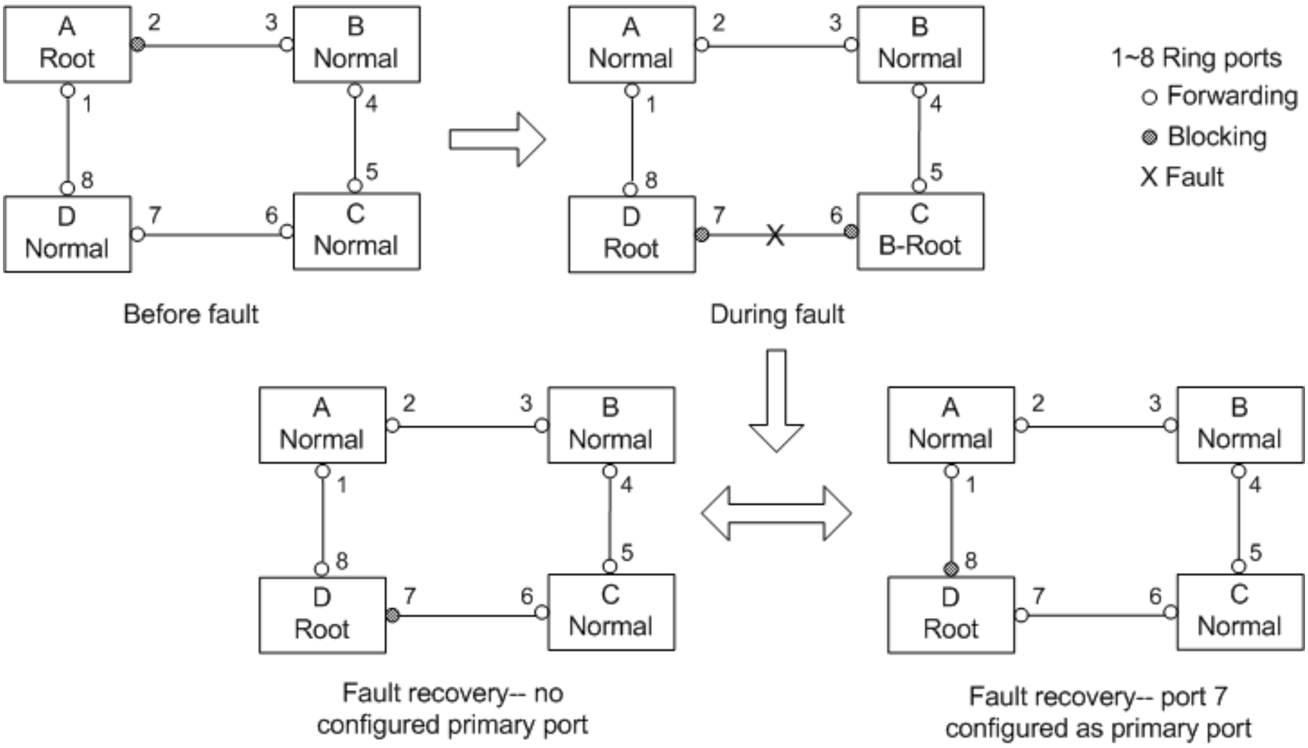


Figure 133 DRP Link Fault

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

DRP-VLAN-Based rings are configured.

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

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

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

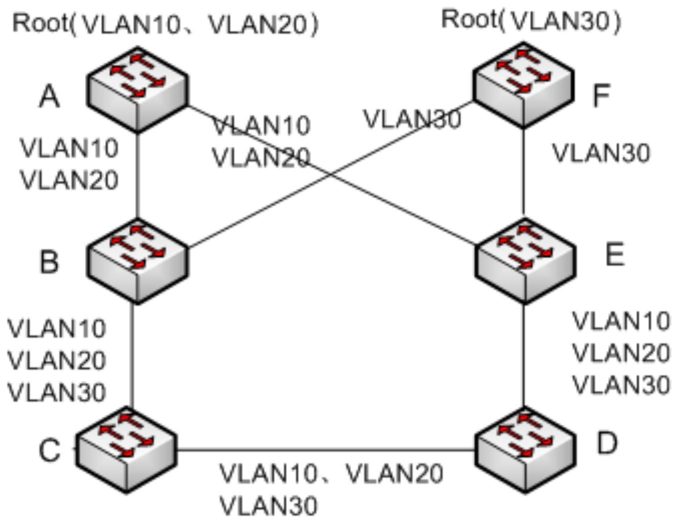


Figure 134 DRP-VLAN-Based

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 Figure 135, one backup port can be configured on each switch. The master backup port is in forwarding state and the other backup ports are in blocking state. If the master backup port or its link is faulty, a slave backup port will be selected to forward data.

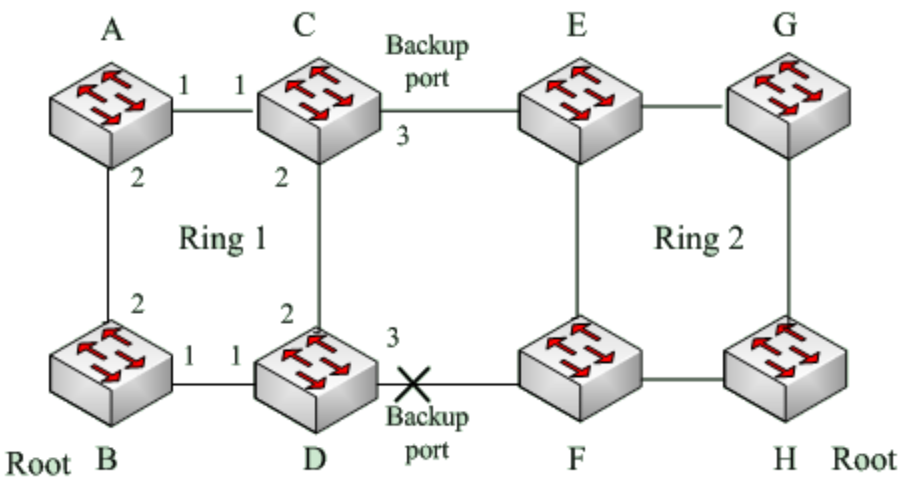


Figure 135 DRP Backup

Caution:

Link status change affects the status of backup ports.

7.5.3 DHP

7.5.3.1 Overview

As shown in Figure 136, A, B, C, and D are mounted to a ring. Dual Homing Protocol (DHP) achieves the following functions if it is enabled on A, B, C, and D:

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

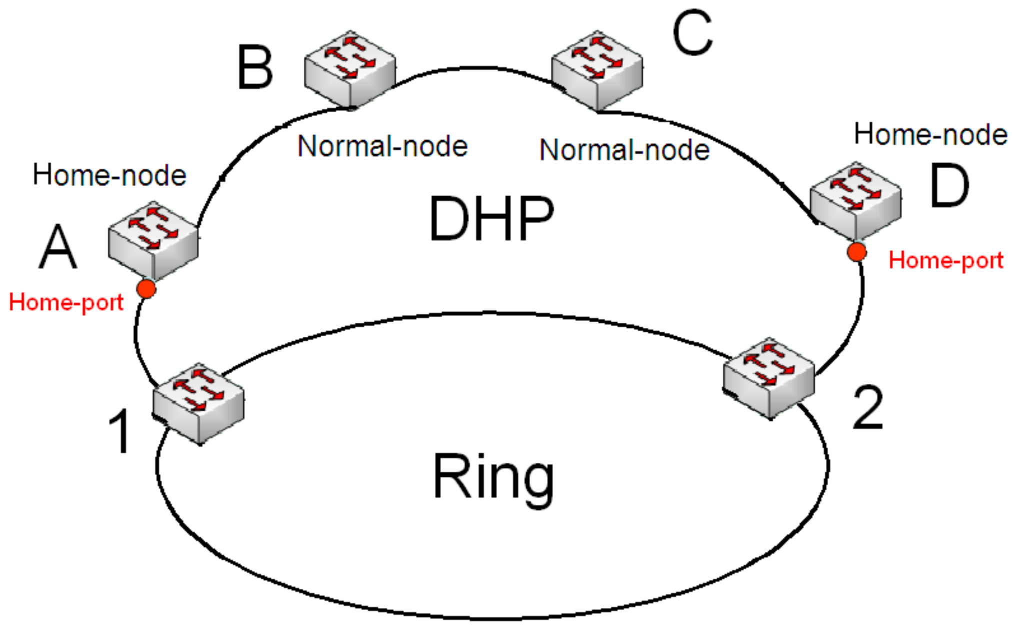


Figure 136 DHP Application

7.5.3.2 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.

7.5.3.3 Implementation

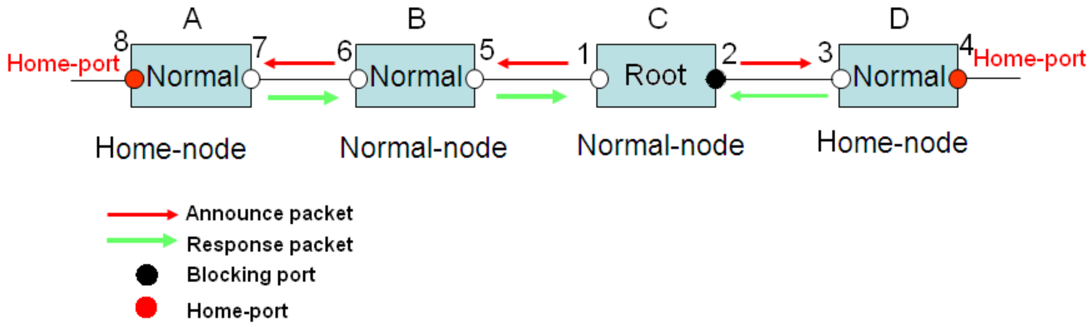


Figure 137 DHP Configuration

As shown in Figure 136, the configurations of A, B, C, and D in Figure 137 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 Figure 138.

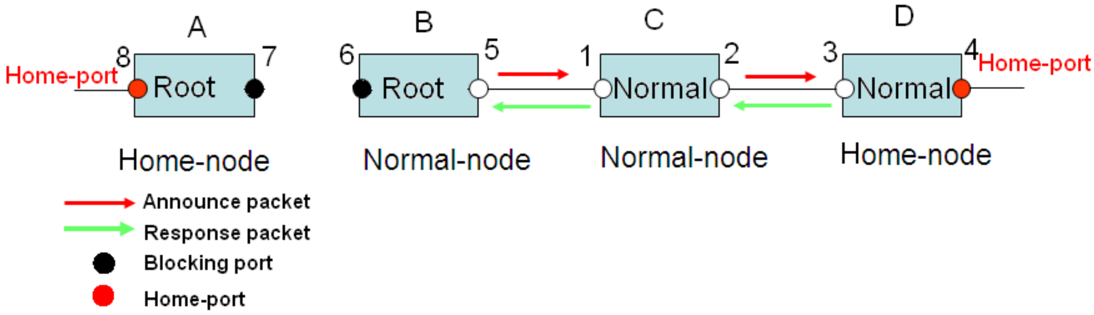


Figure 138 DHP Fault Recovery

7.5.3.4 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.

7.5.3.5 Web Configuration

1. Configure the DRP redundancy mode, as shown in Figure 139.

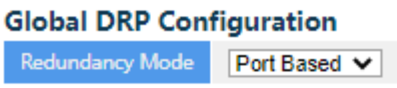


Figure 139 Configure the DRP Redundancy Mode

Redundancy Mode

Configuration options: Port Based/Vlan Based

Default configuration: Port Based

Function: Configure the DRP redundancy 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. Configure DRP-Port-Based and DRP-VLAN-Based, as shown in Figure 140 and Figure 141.

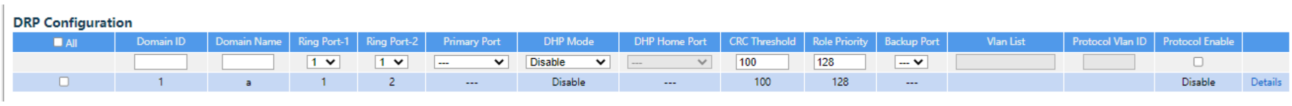


Figure 140 DRP-Port-Based Configuration

Figure 141 DRP-VLAN-Based Configuration

Domain ID

Configuration range: 1~32

Function: Each ring has a unique domain ID. One switch supports a maximum of 8 VLAN-based rings, the number of port-based rings depends on the number of switch ports.

Domain Name

Configuration range: 1~31 characters

Function: Configure the domain name.

Ring Port-1/Ring Port-2

Configuration options: all switch ports

Function: Select two ring ports.

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.
- 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; RSTP port cannot be configured as DRP-Port ring port or backup port.

Primary Port

Configuration options: --/Ring Port-1/Ring Port-2

Default configuration: --

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

DHP Mode

Configuration options: Disable/Normal-Node/Home-Node

Default configuration: Disable

Function: Disable DHP or configure the DHP mode.

DHP Home Port

Configuration 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

Configuration range: 25~65535

Default configuration: 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

Configuration range: 0~255

Default configuration: 128

Function: Configure the priority of a switch.

Backup Port

Configuration options: all switch ports

Function: Configure the backup port.

CAUTION

Caution:

Do not configure a ring port as a backup port.

VLAN List

Configuration options: All created VLANs

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

Protocol Vlan ID

Configuration range: 1~4093

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

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

Protocol Enable

Configuration options: Enable/Disable

Function: Enable the DRP protocol for the specified domain

3. View and modify DRP configuration, as shown below.

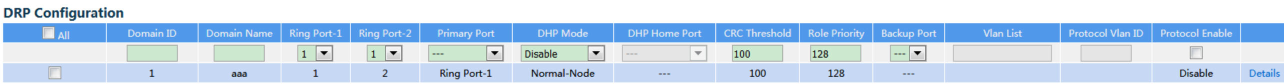


Figure 142 View and Modify DRP Configuration

Select a DRP entry, click <Modify> to edit the DRP entry configuration; click <Delete> to delete the designated DRP entry.

4. Click **Details** in the DRP entry in Figure 142 to show the roles and port status of the switches in the DRP ring, as shown in Figure 143.

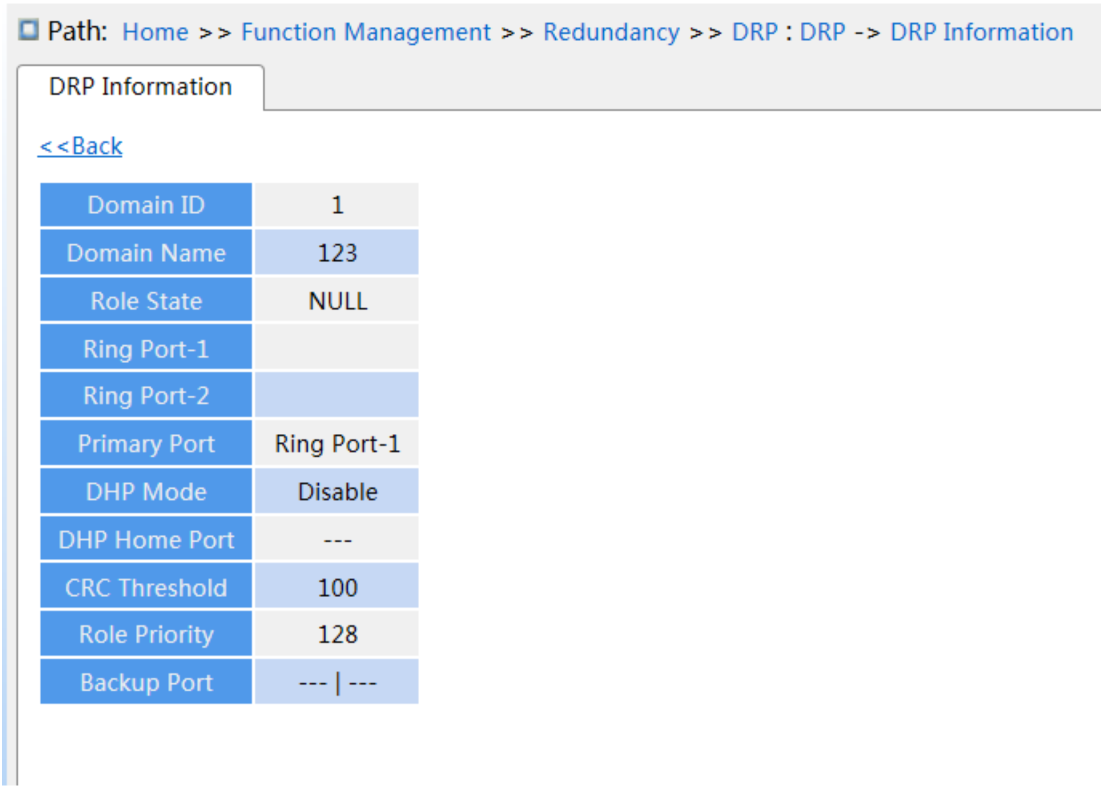


Figure 143 DRP State

7.5.3.6 Typical Configuration Example

As shown in Figure 135, 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 a. Select ring port 1 and ring port 2. Keep default values for role priority and backup port, as shown in Figure 140.

Configuration on switch C and switch D:

2. Set Domain ID to 1, Domain name to a, and Backup port to 3. Select ring port 1 and ring port 2. Keep the default value for role priority, as shown in Figure 140.

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

3. Set Domain ID to 2 and Domain name to b. Select ring port 1 and ring port 2. Keep default values for role priority and backup port, as shown in Figure 140.

7.5.4 RSTP/STP Configuration

7.5.4.1 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.

7.5.4.2 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.

7.5.4.3 BPDU Configuration Messages

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

Table 6 BPDU

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

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

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

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

Designated port ID: port priority+port number.

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

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

Hello time: interval for sending BPDUs.

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

7.5.4.4 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.

7.5.4.5 Web Configuration

1.Set the time parameters of the network bridge, as shown below.

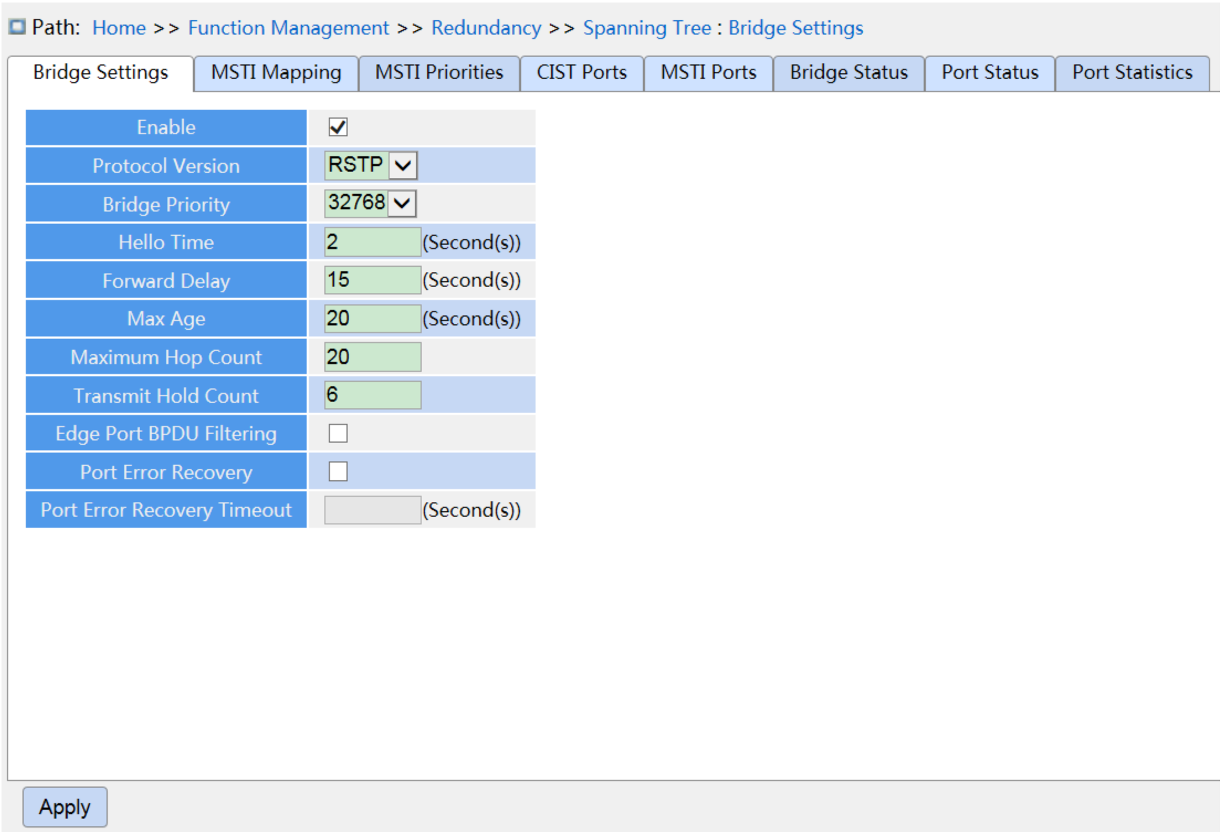


Figure 144 Setting Time Parameters of the Network Bridge

Global Cofiguration

Configuration options: Enable/Disable

Default configuration: Disable

Function: Disable or enable spanning tree.

Caution:

- Port-based ring protocols include RSTP and VLAN-based ring protocols include MSTP 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.

Protocol Priority

Configuration options: MSTP/RSTP/STP

Default configuration: MSTP

Function: Select the spanning tree protocol.

Brigde Priority

Configuration range: 0~61440. The step is 4096.

Default configuration: 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

Configuration range: 1~10s

Default configuration: 2s

Function: Configure the interval for sending BPDU.

Forward Delay

Configuration range: 4~30s

Default configuration: 15s

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

Max Age

Configuration range: 6~40s

Default configuration: 20s

Function: Maximum duration that a BPDU can be saved on a device.

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

CAUTION

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.

Maximum Hop Count

Configuration range: 6~40

Default configuration: 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

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.

Transmit Hold Count

Configuration range: 1~10

Default configuration: 6

Function: Set the maximum number of BPDU packets that can be sent by a port within each Hello Time.

Edge Port BPDU Filtering

Configuration options: Enable/Disable

Default configuration: Disable

Function: Control whether an edge port receives and forwards BPDU packets.

Port Error Recovery

Configuration options: Enable/Disable

Default configuration: Disable

Function: Control whether a port can automatically recover from the error state to the normal state.

Port Error Recovery Timeout

Configuration range: 30~86400s

Function: Set the time for a port to recover from the error state to the normal state.

2. Configure RSTP port, as shown below.

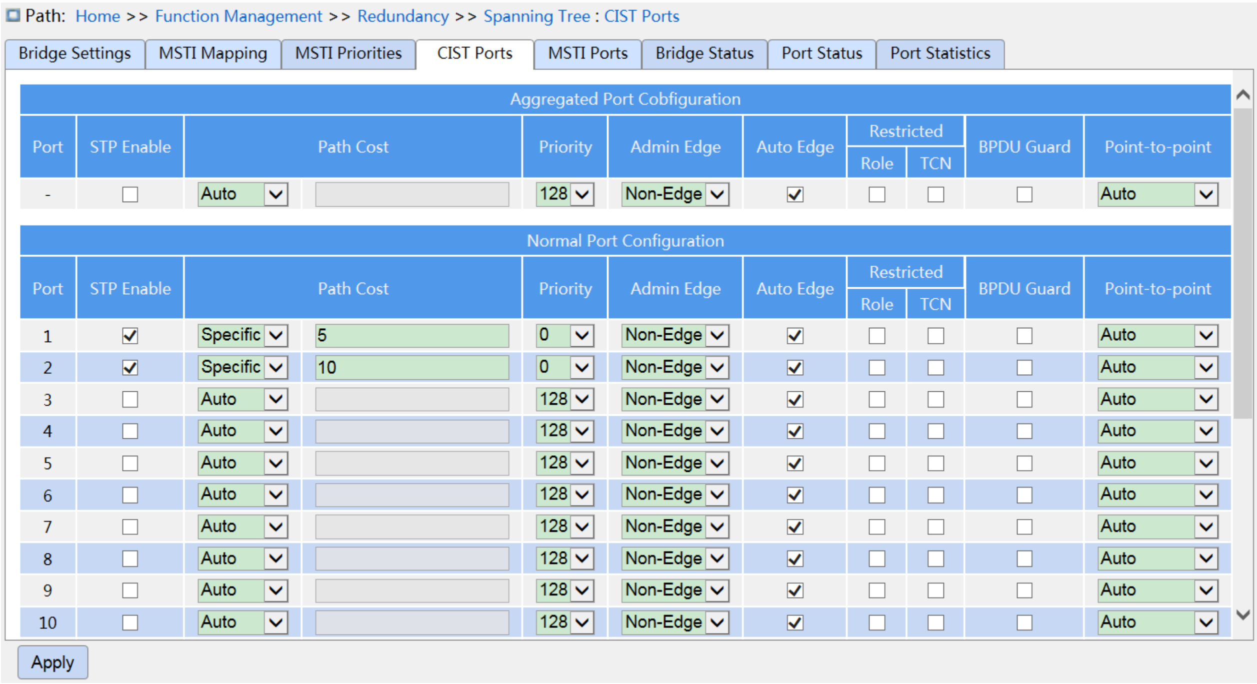


Figure 145 Configure RSTP Port

STP Enabled

Configuration options: Enable/Disable

Default configuration: 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.
- 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.

Path Cost

Configuration options: Auto/Specific (1~200000000)

Default configuration: Auto

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.

Priority

Configuration range: 0~240. The step is 16.

Default configuration: 128

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

Admin Edge

Configuration options: Non-Edge/Edge

Default configuration: Non-Edge

Function: Set whether the current port is an edge port.

Description: When a port is directly connected to a terminal and is not connected to other devices or a shared network segment, the port is considered as an edge port. An edge port can rapidly migrate from the blocking state to the forwarding state without waiting delay. After an edge port receives BPDU packets, it becomes a non-edge port.

Auto Edge

Configuration options: Enable/Disable

Default configuration: Enable

Function: Specify whether to enable the automatic detection function of an edge port.

Restricted Role

Configuration options: Enable/Disable

Default configuration: Disable

Function: A restricted port will be never selected as a root node even if it is granted the highest priority.

Restricted TCN

Configuration options: Enable/Disable

Default configuration: Disable

Function: A port with restricted TCN will not actively send TCN messages.

BPDU Guard

Configuration options: Enable/Disable

Default configuration: Disable

Function: Control whether an edge port enters the Error-Disable state and is shut down when receiving BPDU packets.

Point-to-point

Configuration options: Auto/Forced True/Forced False

Default configuration: Auto

Function: Set the connection type for a port. If a port is connected to a point-to-point link, the port can rapidly migrate to another state.

Description: **Auto** indicates that the switch automatically detects the link type based on the duplex status of a port. When a port works in full-duplex mode, the switch considers that the type of the link connected to the port is point-to-point; when a port works in half-duplex mode, the switch considers that the type of the link connected to the port is shared. Forced point-to-point refers that a link connected to a port is a point-to-point link and forced sharing refers that a link connected to a port is a shared link.

7.5.4.6 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 146.

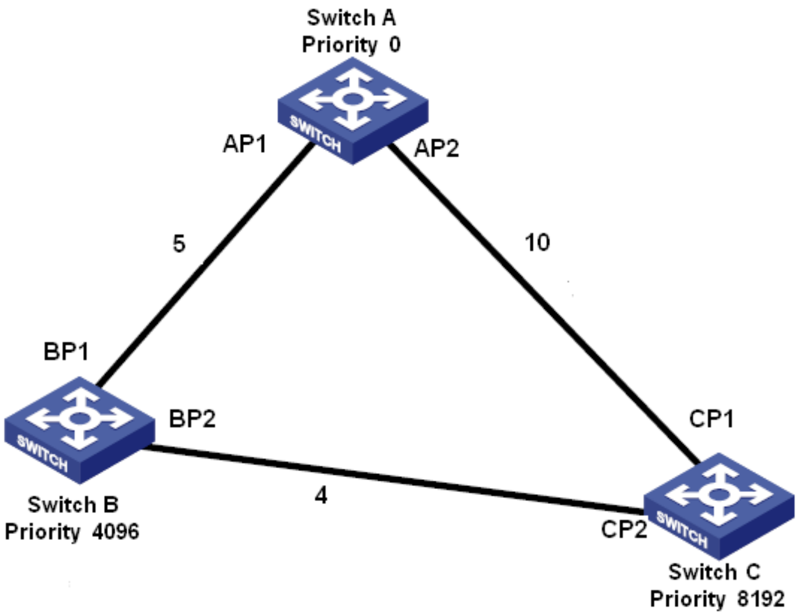


Figure 146 RSTP Configuration Example

Configuration on Switch A:

1. Set bridge priority to 0 and time parameters to default values, as shown in Figure 144.

2. Set the path cost of port 1 to 5 and that of port 2 to 10, as shown in Figure 145.

Configuration on Switch B:

1. Set bridge priority to 4096 and time parameters to default values, as shown in Figure 144.

2. Set the path cost of port 1 to 5 and that of port 2 to 4, as shown in Figure 145.

Configuration on Switch C:

1. Set bridge priority to 8192 and time parameters to default values, as shown in Figure 144.

2. Set the path cost of port 1 to 10 and that of port 2 to 4, as shown in Figure 145.

- 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.

7.5.5 MSTP Configuration

7.5.5.1 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 147, 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.

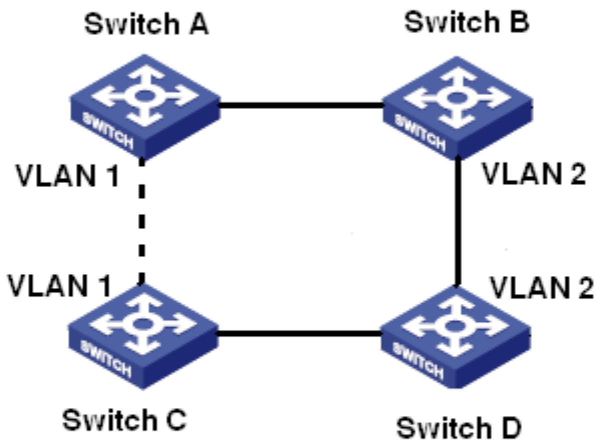


Figure 147 RSTP Disadvantage

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 147 forms the topology shown in Figure 148 . 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.

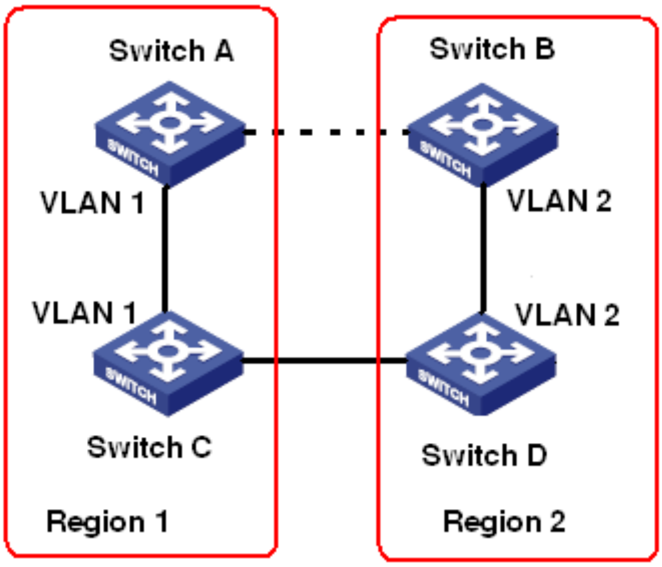


Figure 148 MSTP Topology

7.5.5.2 Basic Concepts

Learn MSTP concepts based onFigure 149 and Figure 152.

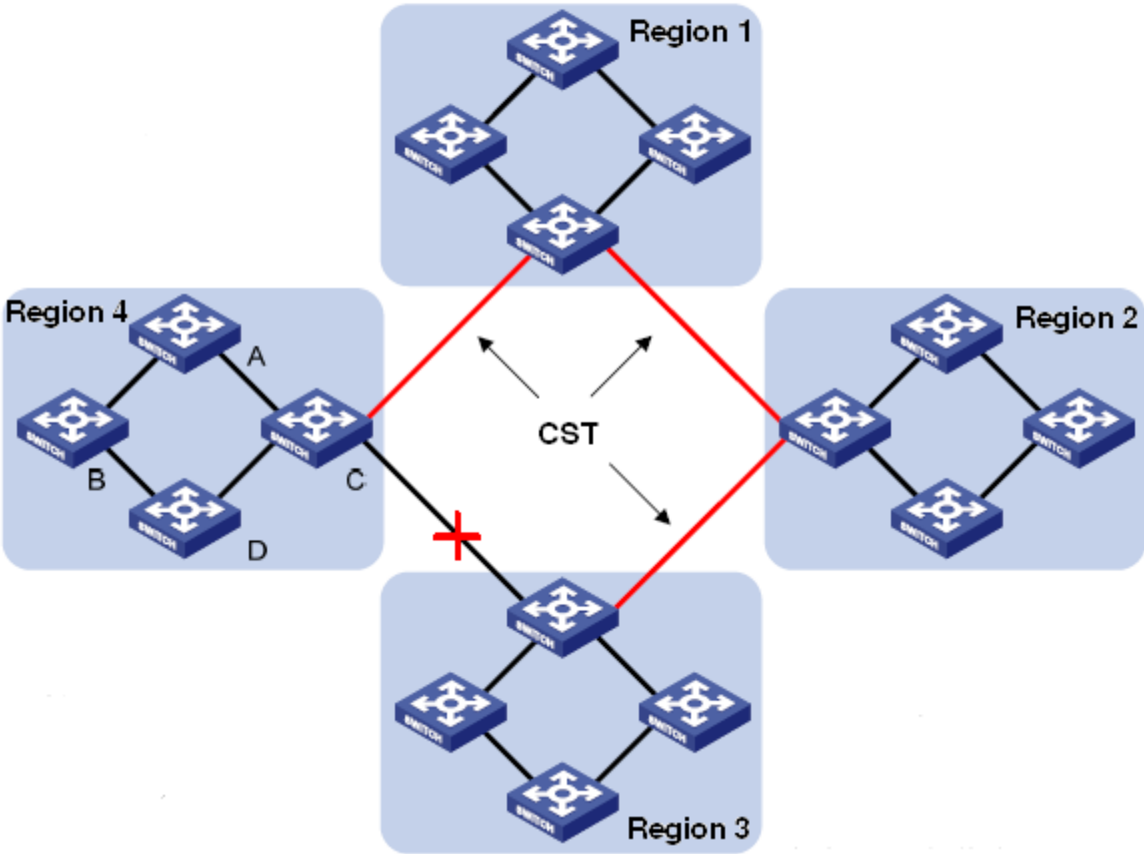


Figure 149 MSTP Concepts

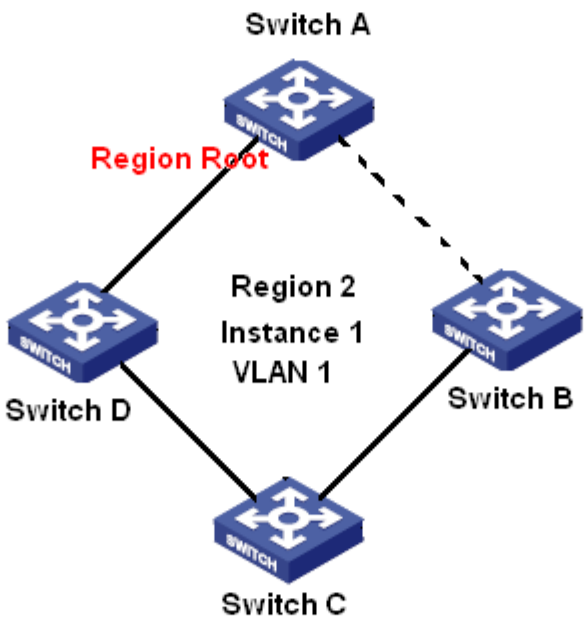


Figure 150 VLAN 1 Mapping to Instance 1

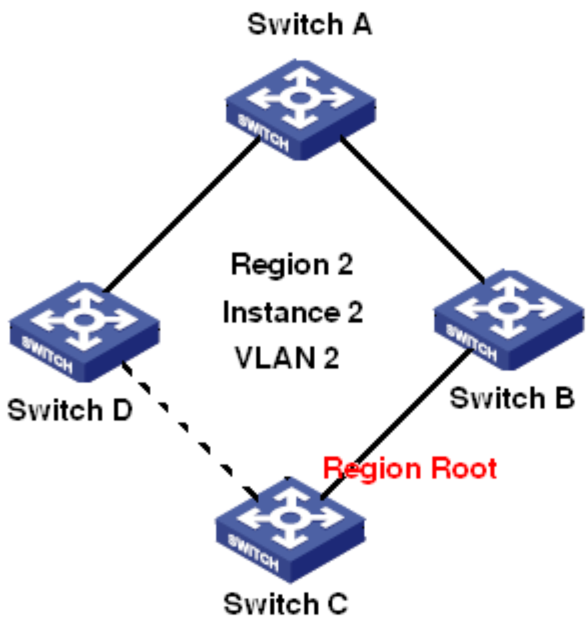


Figure 151 VLAN2 Mapping to Instance 2

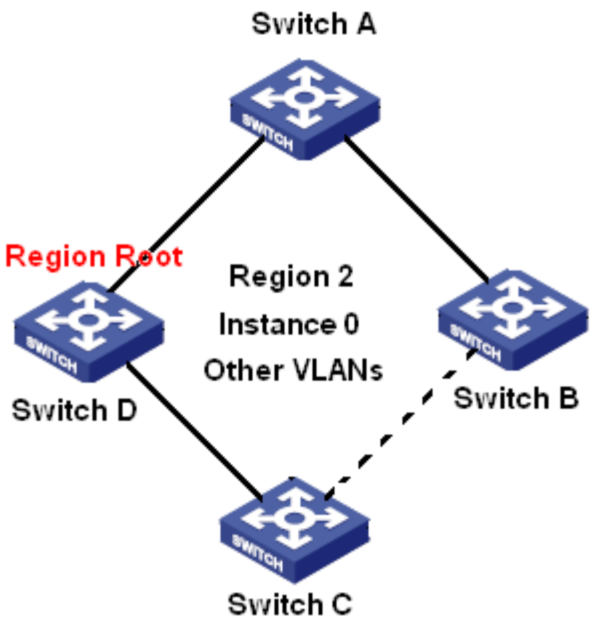


Figure 152 Other VLAN Mapping to Instance 0

Instance: a collection of multiple VLANs. One VLAN (as shown in Figure 150 and Figure 151) or multiple VLANs with the same topology (as shown in Figure 152) 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 149 , Region1, Region2, Region3, and Region4 are four different MST regions.

VLAN mapping table: consists of the mapping between VLANs and spanning trees. In Figure 149 , VLAN mapping table of region 2 is the mapping between VLAN 1 and instance 1, as shown in Figure 150; VLAN 2 is mapped to instance 2, as shown in Figure 151. The other VLANs are mapped to instance 0, as shown in Figure 152.

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 149 , 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 152.

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 149, 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 150 and Figure 151. 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 150, Figure 151, and Figure 152 , 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.

7.5.5.3 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.

7.5.5.4 Web Configuration

1. Set the time parameters of the network bridge, as shown below.

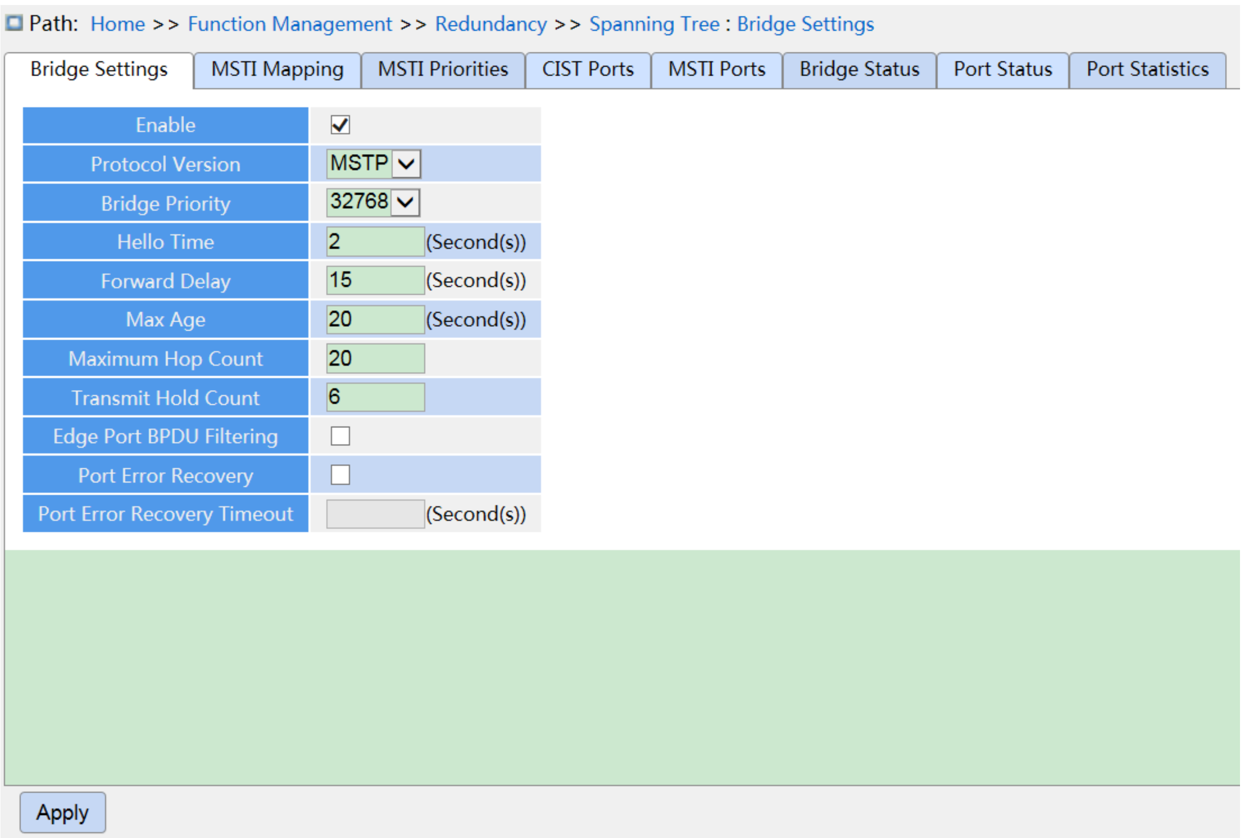


Figure 153 Setting Time Parameters of the Network Bridge

Global Configuratation

Configuration options: Enable/Disable

Default configuration: Disable

Function: Disable or enable spanning tree.

Caution:

- Port-based ring protocols include RSTP, DT-Ring-Por 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.

Protocol Priority

Configuration options: MSTP/RSTP/STP

Default configuration: MSTP

Function: Select the spanning tree protocol.

Brigde Priority

Configuration range: 0~61440. The step is 4096.

Default configuration: 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

Configuration range: 1~10s

Default configuration: 2s

Function: Configure the interval for sending BPDU.

Forward Delay

Configuration range: 4~30s

Default configuration: 15s

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

Max Age

Configuration range: 6~40s

Default configuration: 20s

Function: Maximum duration that a BPDU can be saved on a device.

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

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.

Maximum Hop Count

Configuration range: 6~40

Default configuration: 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.

Transmit Hold Count

Configuration range: 1~10

Default configuration: 6

Function: Set the maximum number of BPDU packets that can be sent by a port within each Hello Time.

Edge Port BPDU Filtering

Configuration options: Enable/Disable

Default configuration: Disable

Function: Control whether an edge port receives and forwards BPDU packets.

Port Error Recovery

Configuration options: Enable/Disable

Default configuration: Disable

Function: Control whether a port can automatically recover from the error state to the normal state.

Port Error Recovery Timeout

Configuration range: 30~86400s

Function: Set the time for a port to recover from the error state to the normal state.

2. Configure MSTI mapping, as shown below.

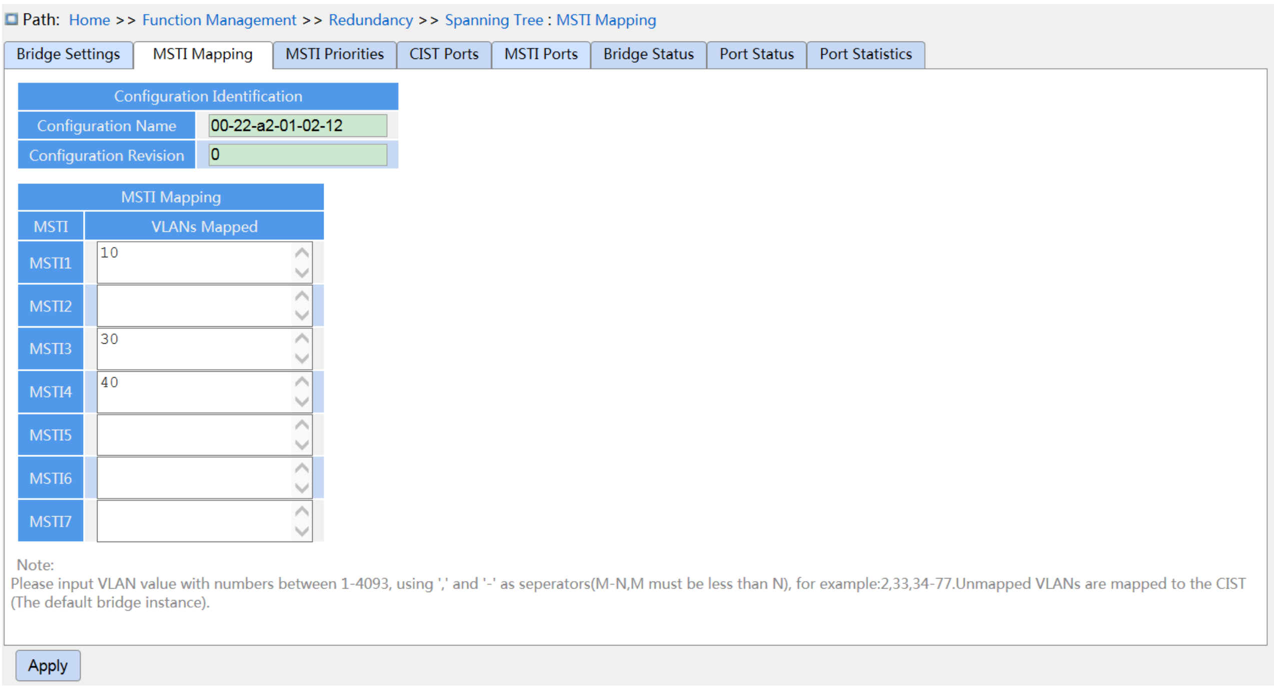


Figure 154 Configure MSTI Mapping

Configuration Name

Configuration range: 1-32 characters

Default configuration: device MAC address

Function: Configure the name of MST region.

Configuration Revision

Configuration options: 0~65535

Default configuration: 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.

VLANs Mapped

Configuration range: 1~4094

Function: Configure the VLAN mapping table in MST region. When there are multiple VLANs, you can separate the VLANs by a comma (,) and an en dash (-), where an en dash is used to separate two consecutive VLAN IDs and a comma is used to separate two inconsecutive VLAN IDs.

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.

3. Configure the bridge priority of the switch in designated instance, as shown below.

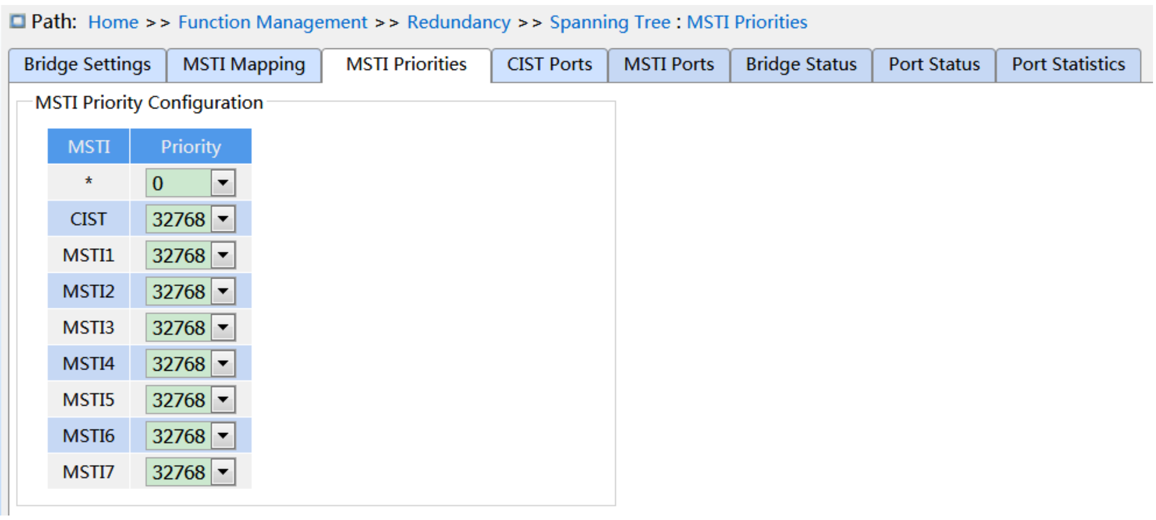


Figure 155 Configuring Bridge Priority in Designated Instance

Priority

Configuration range: 0~61440 with the step length of 4096

Default configuration: 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.

Click <Apply> to make current configurations take effect.

4. Configure CIST ports, as shown below.

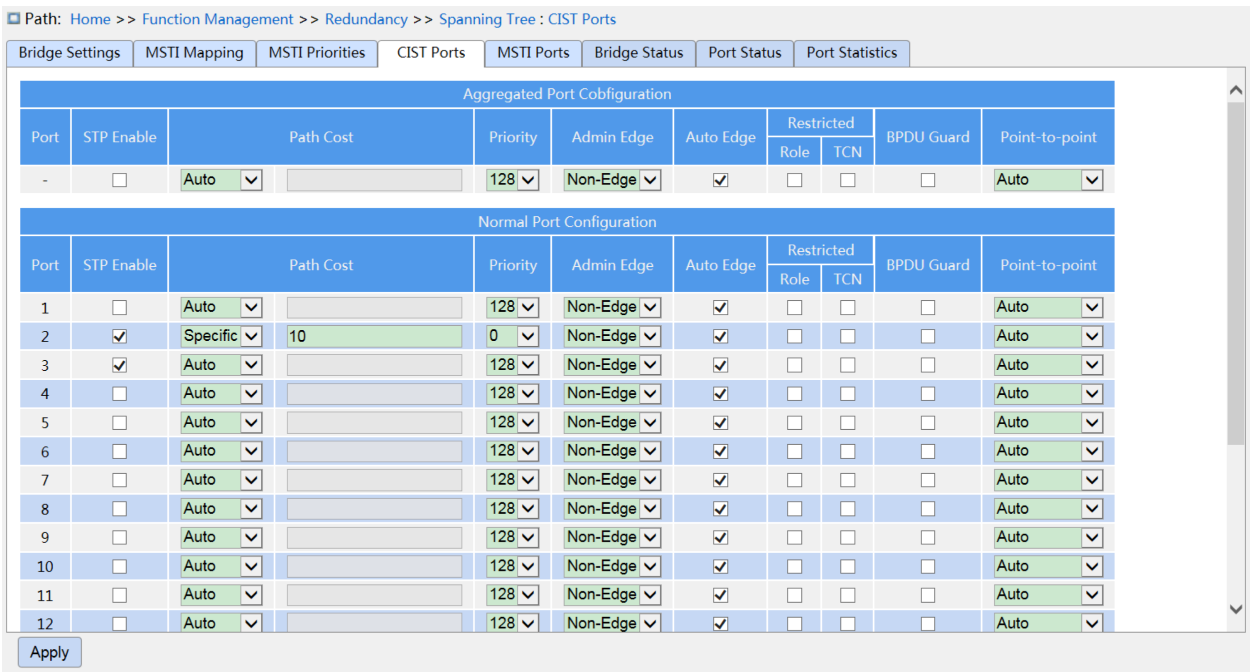


Figure 156 Configure CIST Ports

STP Enabled

Configuration options: Enable/Disable

Default configuration: Disable

Function: Enable or disable STP/RSTP on ports.

Caution:

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

Path Cost

Configuration options: Auto/Specific (1~200000000)

Default configuration: Auto

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.

Priority

Configuration range: 0~240. The step is 16.

Default configuration: 128

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

Admin Edge

Configuration options: Non-Edge/Edge

Default configuration: Non-Edge

Function: Set whether the current port is an edge port.

Description: When a port is directly connected to a terminal and is not connected to other devices or a shared network segment, the port is considered as an edge port. An edge can rapidly migrate from the blocking state to the forwarding state without waiting delay. After an edge port receives BPDU packets, it becomes a non-edge port.

Auto Edge

Configuration options: Enable/Disable

Default configuration: Enable

Function: Whether to enable the automatic detection function of an edge port.

Restricted Role

Configuration options: Enable/Disable

Default configuration: Disable

Function: A restricted port will be never selected as a root node even if it is granted the highest priority.

Restricted TCN

Configuration options: Enable/Disable

Default configuration: Disable

Function: A port with restricted TCN will not actively send TCN messages.

BPDU Guard

Configuration options: Enable/Disable

Default configuration: Disable

Function: Control whether an edge port enters the Error-Disable state and is shut down when receiving BPDU packets.

Point-to-point

Configuration options: Auto/Forced True/Forced False

Default configuration: Auto

Function: Set the connection type for a port. If a port is connected to a point-to-point link, the port can rapidly migrate to another state.

Description: Auto indicates that the switch automatically detects the link type based on the duplex status of a port. When a port works in full-duplex mode, the switch considers that the type of the link connected to the port is point-to-point; when a port works in half-duplex mode, the switch considers that the type of the link connected to the port is shared. Forced point-to-point refers that a link connected to a port is a point-to-point link, and forced sharing refers that a link connected to a port is a shared link.

5. Configure MSTI ports, as shown below.

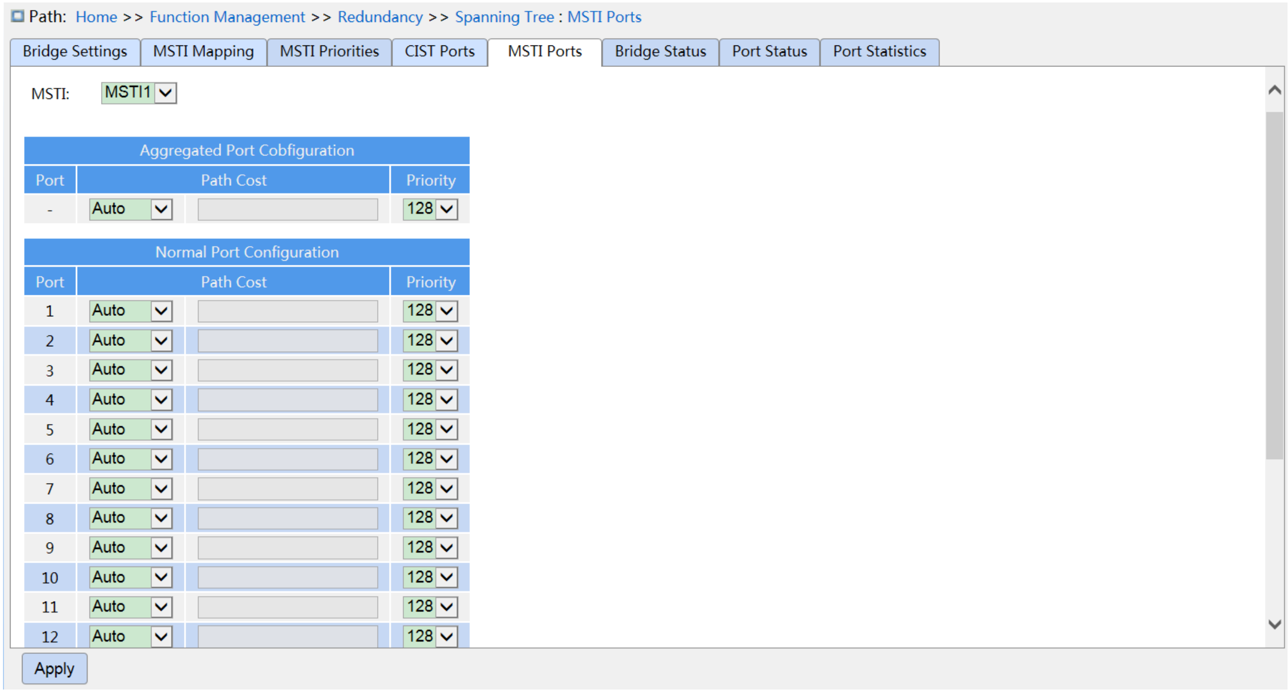


Figure 157 Select MSTI

Select MSTI

Configuration range: MST1~MST7

Default configuration: MST1

Function: Select a MSTI.

MSTI Aggregated Port Cobfiguration

Function: Configure the aggregation group as an MSTP port and configure its path cost and priority in the specified instance.

Path Cost

Configuration options: Auto/Specific (1~200000000)

Default configuration: Auto

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.

Priority

Configuration range: 0~240. The step is 16.

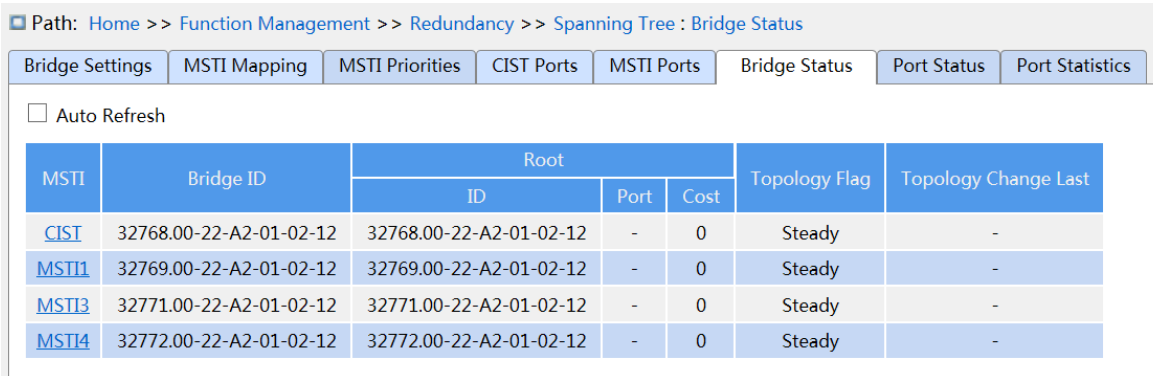
Default configuration: 128

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.

Click the <Apply> button to make the current configuration take effect.

6. View bridge status, as shown below.


Path: Home >> Function Management >> Redundancy >> Spanning Tree : Bridge Status

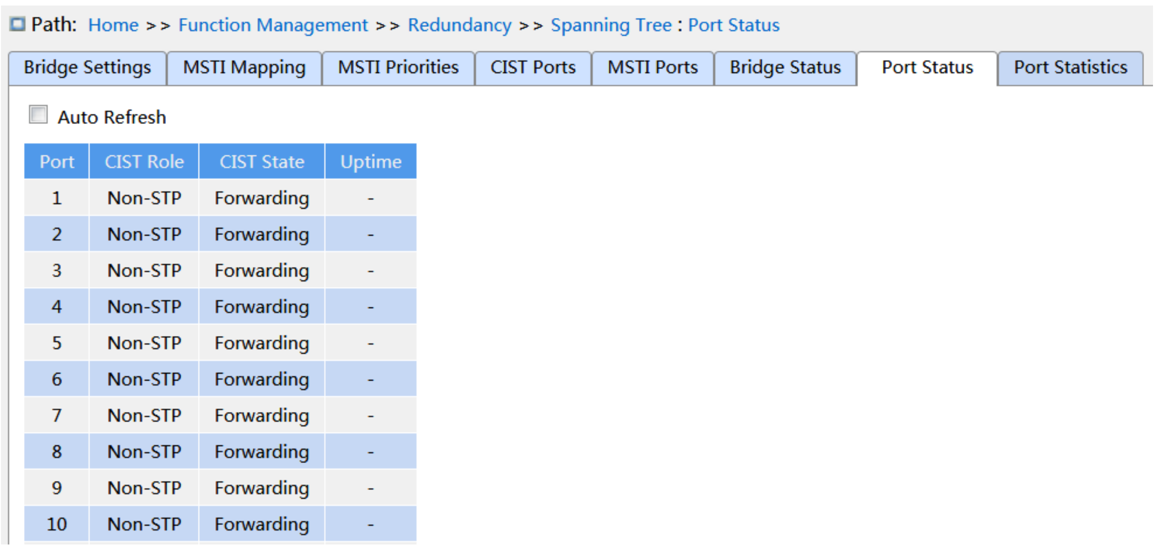
Bridge Settings | MSTI Mapping | MSTI Priorities | CIST Ports | MSTI Ports | Bridge Status | Port Status | Port Statistics

Auto Refresh

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-22-A2-01-02-12	32768.00-22-A2-01-02-12	-	0	Steady	-
MSTI1	32769.00-22-A2-01-02-12	32769.00-22-A2-01-02-12	-	0	Steady	-
MSTI3	32771.00-22-A2-01-02-12	32771.00-22-A2-01-02-12	-	0	Steady	-
MSTI4	32772.00-22-A2-01-02-12	32772.00-22-A2-01-02-12	-	0	Steady	-

Figure 158 View Bridge Status

7. View STP ports status, as shown below.


Path: Home >> Function Management >> Redundancy >> Spanning Tree : Port Status

Bridge Settings | MSTI Mapping | MSTI Priorities | CIST Ports | MSTI Ports | Bridge Status | Port Status | Port Statistics

Auto Refresh

Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-
8	Non-STP	Forwarding	-
9	Non-STP	Forwarding	-
10	Non-STP	Forwarding	-

Figure 159 View STP Ports Status

8. View STP ports packets statistics, as shown below.

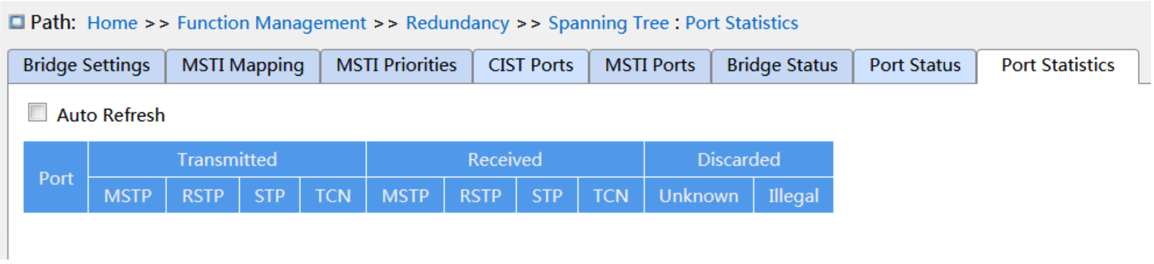


Figure 160 View STP Ports Packets Statistics

7.5.5.5 Typical Configuration Example

As shown in Figure 161, 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.

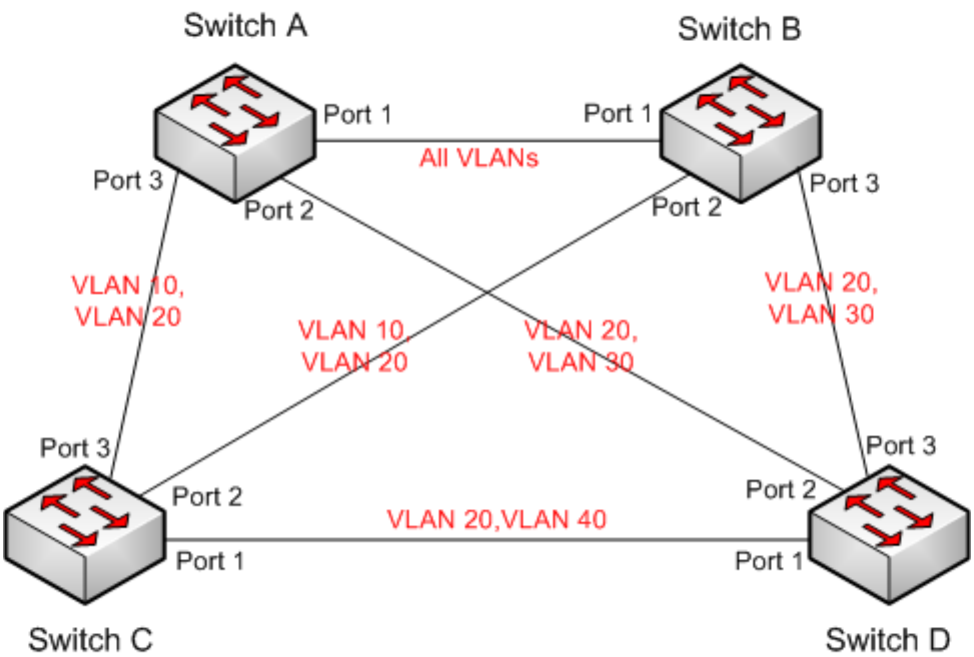


Figure 161 MSTP Typical Configuration Example

Configuration on Switch A:

1. Create VLAN 10, 20, and 30 on Switch A; set the ports and allow the packets of corresponding VLANs to pass through.
2. Enable global MSTP protocol, as shown in Figure 153.
3. Set the name of MST region to Region and the revision parameter to 0, as shown in Figure 157.
4. Create MSTI 1, 3, and 4 and map VLAN 10, 30, and 40 to instance 1, 3, and 4 respectively, as shown in Figure 157.
5. Set the switch bridge priority in MSTI 1 to 4096, and keep default priority in other instances, as shown in Figure 155.

Configuration on Switch B:

6. Create VLAN 10, 20, and 30 on Switch B; set the ports and allow the packets of corresponding VLANs to pass through.
7. Enable global MSTP protocol, as shown in Figure 153.
8. Set the name of MST region to Region and the revision parameter to 0, as shown in Figure 157.
9. Create MSTI 1, 3, and 4 and map VLAN 10, 30, and 40 to instance 1, 3, and 4 respectively, as shown in Figure 157.
10. Set switch bridge priority in MSTI 3 and MSTI 0 to 4096, and keep default priority in other instances, as shown in Figure 155.

Configuration on Switch C:

11. Create VLAN 10, 20, and 40 on Switch C; set the ports and allow the packets of corresponding VLANs to pass through.
12. Enable global MSTP protocol, as shown in Figure 153.
13. Set the name of MST region to Region and the revision parameter to 0, as shown in Figure 157.
14. Create MSTI 1, 3, and 4 and map VLAN 10, 30, and 40 to instance 1, 3, and 4 respectively, as shown in Figure 157.
15. Set switch bridge priority in MSTI 4 to 4096, and keep default priority in other instances, as shown in Figure 155.

Configuration on Switch D:

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

17. Enable global MSTP protocol, as shown in Figure 153.

18. Set the name of MST region to Region and the revision parameter to 0, as shown in Figure 157.

19. Create MSTI 1, 3, and 4 and map VLAN 10, 30, and 40 to instance 1, 3, and 4 respectively, as shown in Figure 157.

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

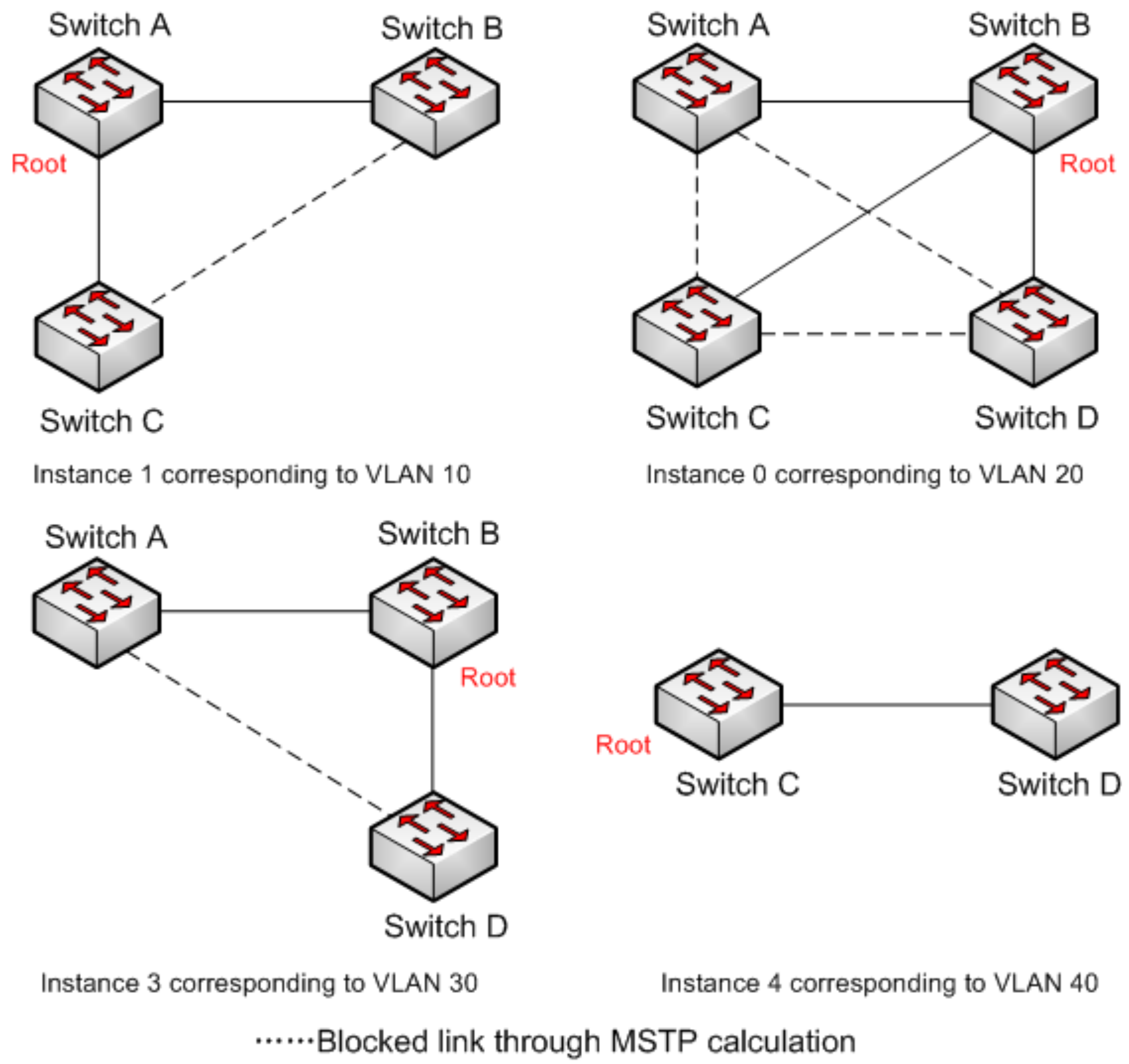


Figure 162 Spanning Tree Instance of each VLAN

7.6 ARP Configuration

7.6.1 Introduction

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

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.

7.6.2 Description

The ARP table items is divided into dynamic ARP table items and static ARP table items.

Dynamic table items are generated and maintained automatically through ARP message interaction, which can be aged, updated by new ARP messages and overwritten by static ARP table items.

Static table items are manually configured and maintained and are not aged or overwritten by dynamic ARP table items.

7.6.3 Proxy ARP

If the ARP request is sent from the host of one network to another host on the same network segment but not on the same physical network, then the gateway with proxy ARP function that directly connected to the source host can reply to the request message, which is called the proxy ARP.

The process of proxy ARP is as follows:

1、The source host sends a ARP request to the host of another physical network;

2、The gateway directly connected to the source host has enabled the proxy ARP function of the VLAN interface. If there is a normal route to the destination host, the destination host will be replaced to replay mac address of its own interface.

3、The IP messages which is sent by the source host to the destination host are sent to the enabled proxy ARP device.

4、Gateway performs normal IP routing forwarding of messages.

5、IP messages that sent to the destination host reach the destination host through the network.

7.6.4 Web Configuration

1. Configure the static ARP address table items, as shown below.

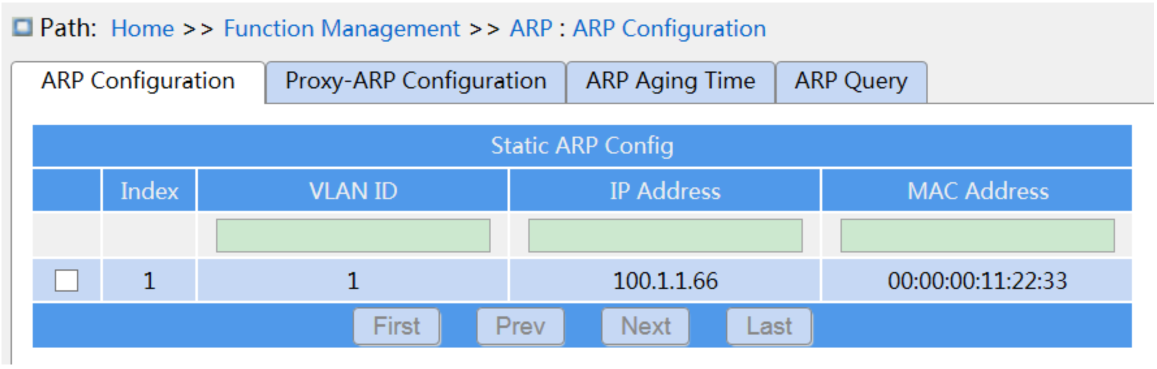


Figure 163 Configure static ARP table items

VLAN ID

Configuration content: Created L3 VLAN interface, range 1-4094

Function: select the L3 VLAN interface of the current ARP table item.

IP address

Configuration format: A.B.C.D

Function: configure IP addresses for static ARP table items.

MAC address

Configuration format: HH-HH-HH-HH-HH-HH (H is a hexadecimal number)

Function: configure the mac address of the static ARP table items.

Caution:

In general, the switch automatically learns ARP table items, and no need administrator configure static table items.

2. Proxy ARP Configuration, as shown below.

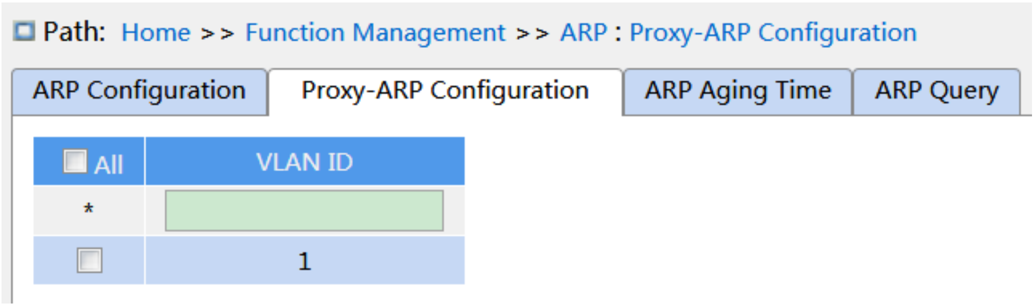


Figure 164 Proxy ARP Configuration

VLAN ID

Configuration range: 1-4094

Function: Select L3 interface of enabled proxy ARP.

3. ARP Aging Time Configuration, as shown below.

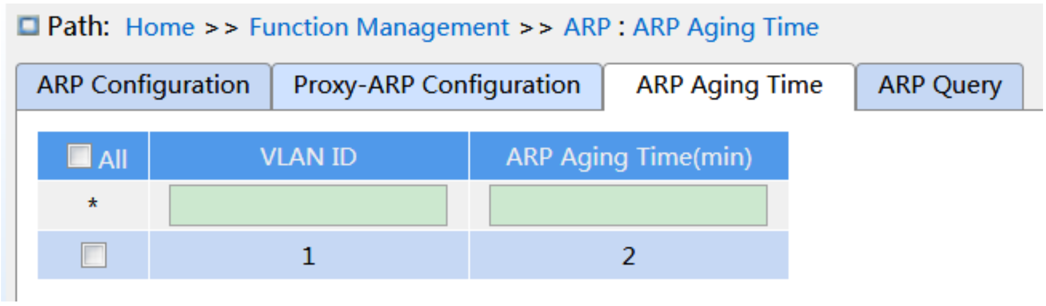


Figure 165 ARP Aging Time Configuration

VLAN ID

Configuration range: 1-4094

Function: specify the L3 interface with configuring ARP aging time

ARP Aging Time

Configuration range: 1 ~ 60min

Default configuration: 5min

Function: configure ARP aging time

Description: ARP aging time refers to start timing by adding a dynamic ARP table item to the address table, and the dynamic address table item will be deleted from the ARP list after the aging time is up.

4. ARP Query, as shown below.

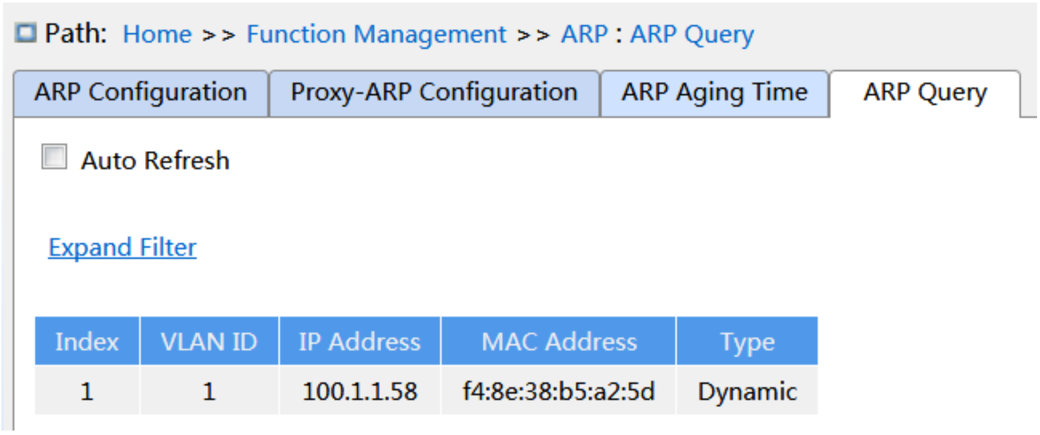


Figure 166 ARP Query

ARP Query

Display item: {index, VLAN ID, IP address, MAC address, type}

Function: display ARP table item

Description: The list displays all ARP table items corresponding to the linkup status port, includes static and dynamic table items.

7.7 ACL Configuration

7.7.1 Overview

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

7.7.2 Implementation

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

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

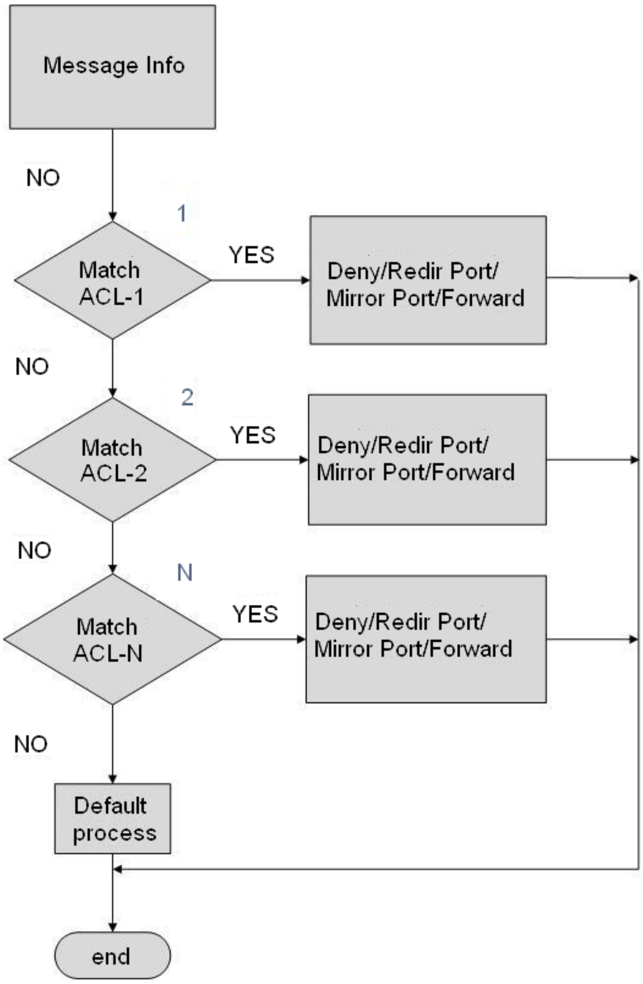


Figure 167 ACL Processing Flowchart

Note:

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

7.7.3 Web Configuration

1. ACL Rate Limiters Configuration, as shown below.

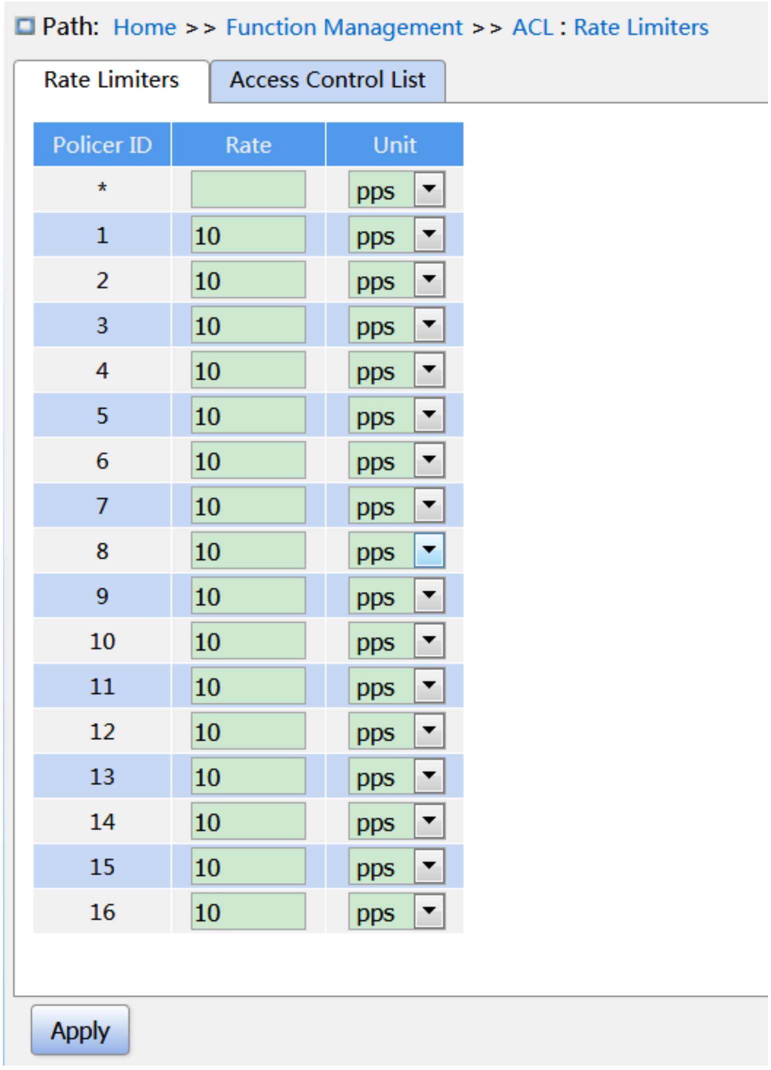


Figure 168 ACL Rate Limiters Configuration

Rate Unit

Configuration range: 0~5000000 pps(step 10)/ 0~10000000Kbps(step 25)

Default configuration: 10 pps

Function: configure the limit rate corresponding to the rate limit ID.

2. Configure ACL table item, as shown below.

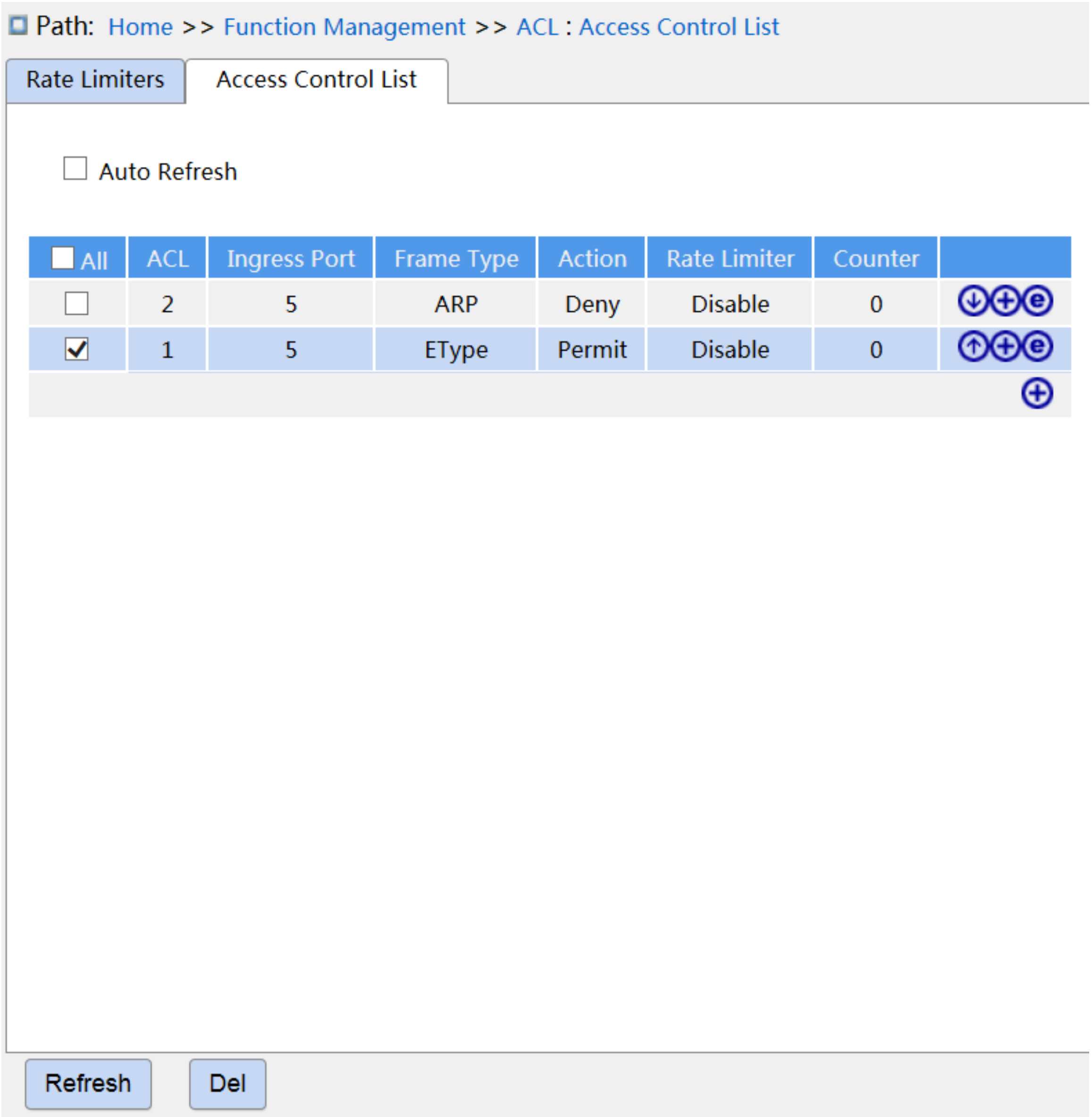


Figure 169 Configure ACL table item

When multiple ACL table items exist, the device compares messages to ACL table items one by one (in top to bottom order), once the message find a matching first ACL table item, Perform the corresponding action immediately.

Click<>button, create an ACL table item. Click<> button, edit current table item. Click<> button, move up current table item. Click<> button, move down current table item. Click <>, then click the <Delete> button, delete current table item.

3、Configure the rule of ACL table item

➢ Configure parameters of ACL table item, as shown below.

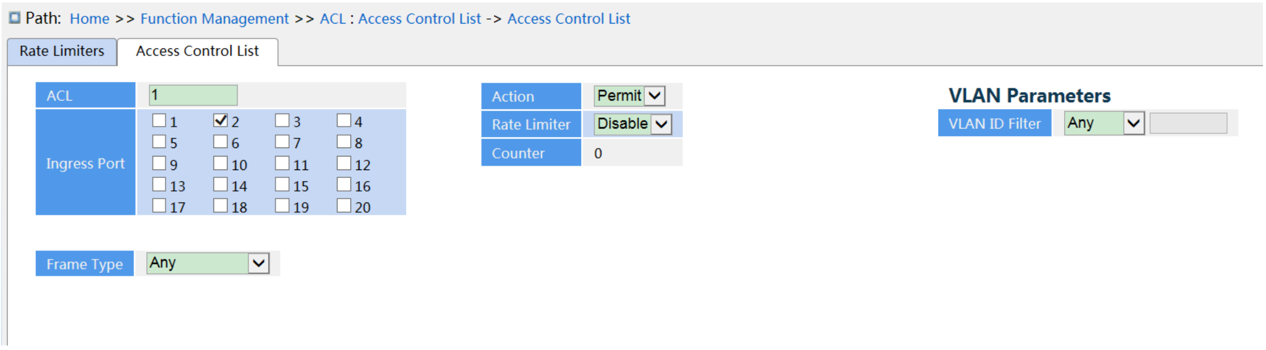


Figure 170 Configure parameters of ACL table item

ACL

Configuration range: 1-512

Function: configure ACL table item ID.

Ingress port

Configuration options: any specified port

Function: select the port of this item ACL.

Frame type

Configuration options: Any/Ethernet Type/IPv4/ARP

Default configuration: Any

Function: configure ACL conditional parameter - frame type. The condition matches successfully when the frame type received by the ingress port meets the parameter configuration.

Action

Configuration options: Deny/Permit

Default configuration: Permit

Function: the processing method of port matching ACL table item frame. Deny: discard the frame of matching ACL table item. Permit: forward the frame of matching ACL table item.

Rate limiter

Configuration range: Disable/1~16

Default configuration: Disable

Function: Enable or disable the port rate limiter, and select rate limiter ID.

Counter

Function: count the number of frames received by the imgress port that match the ACL.

VLAN ID filter

Configuration options: Any/ Specific（1~4094）

Default configuration: Any

Function: Configure condition parameterc—VID, when selecting “Specific”, need to configure VID value. When the VID of received frame from imgress port satisfies the configured parameter, the condition matches successfully.

- Configure Ethernet Type frame parameters, as shown below.

Figure 171 Configure EtherType frame parameters

SMAC filter

Configuration options: Any/ Specific

Default configuration: Any

Function: configure conditional parameter-source MAC address, if select “specific”, need to configure a source MAC address. When the source MAC address of received frame from imgress port satisfies the configured parameter, the condition matches successfully.

DMAC Filter

Configuration options: Any/ Specific

Default configuration: Any

Function: configure conditional parameter-destination MAC address, if select “specific”, need to configure a destination MAC address. When the destination MAC address of received frame from imgress port satisfies the configured parameter, the condition matches successfully.

Ether Type Filter

Configuration options: Any/ Specific（0x600~0xFFFF）

Default configuration: Any

Function: configure conditional parameter-ethernet type, if select “specific”, need to configure ethernet type. When the received ethernet frame from imgress port satisfies the configured parameter, the condition matches successfully.

➢Configure ARP frame parameters, as shown below.

Figure 172 Configure ARP Parameters

SMAC Filter

Configuration options: Any/ Specific

Default configuration: Any

Function: configure conditional parameter-source MAC address, if select “specific”, need to configure a source MAC address. When the source MAC address of received frame from imgress port satisfies the configured parameter, the condition matches successfully.

ARP/RARP

Configuration options: Any/ ARP/RARP

Default configuration: Any

Function: configure conditional parameter-frame type, when the received frame type from imgress port satisfies the configured parameter, the condition matches successfully.

Source IP Filter

Configuration options: Any/Host/Network

Default configuration: Any

Function: configure conditional parameter-source IP address, if select “Host”, need to configure an IP address. if select “Network”, need to configure an IP address and mask. When the source IP address of received frame from imgress port satisfies the configured parameter, the condition matches successfully.

Destination IP Filter

Configuration options: Any/Host/Network

Default configuration: Any

Function: configure conditional parameter-destination IP address, if select “Host”, need to configure an IP address. if select “Network”, need to configure an IP address and mask. When the destination IP address of received frame from imgress port satisfies the configured parameter, the condition matches successfully.

➢ Configure IPv4 frame parameters, as shown below.

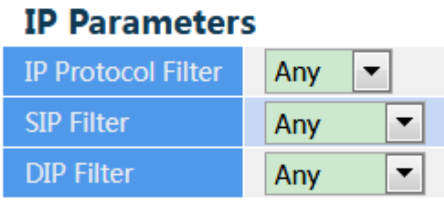


Figure 173 Configure IPv4 frame parameters

IP Protocol Filter

Configuration options: Any/ ICMP/ UDP/ TCP/ Other (0~255)

Default configuration: Any

Function: configure conditional parameter- IPv4 frame protocol type, if select “ICMP/ UDP/ TCP”, need to configure the corresponding parameters. if select “Other”, need to configure protocol number. When the protocol type of received IPv4 frame from imgress port satisfies the configured parameter, the condition matches successfully.

SIP Filter

Configuration options: Any/Host/Network

Default configuration: Any

Function: configure conditional parameter-source IP address, if select “Host”, need to configure an IP address. if select “Network”, need to configure an IP address and mask. When the source IP address of received IPv4 frame from imgress port satisfies the configured parameter, the condition matches successfully.

DIP Filter

Configuration options: Any/Host/Network

Default configuration: Any

Function: configure conditional parameter-destination IP address, if select “Host”, need to configure an IP address. if select “Network”, need to configure an IP address and mask. When the destination IP address of received IPv4 rame from imgress port satisfies the configured parameter, the condition matches successfully.

➢ Configure ICMP Parameters, as shown below.

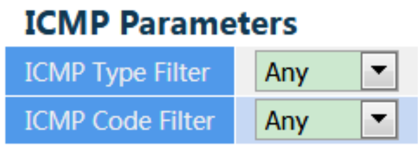


Figure 174 Configure ICMP Paremeters

ICMP Type Filter

Configuration options: Any/Specific（0~255）

Default configuration: Any

Function: configure conditional parameter-ICMP type value, if select “Specific”, need to configure an ICMP type value. When the ICMP type value of received IPv4 rame from imgress port satisfies the configured parameter, the condition matches successfully.

ICMP Code Filter

Configuration options: Any/Specific（0~255）

Default configuration: Any

Function: configure conditional parameter-ICMP code value, if select “Specific”, need to configure an ICMP code value. When the ICMP code value of received IPv4 rame from imgress port satisfies the configured parameter, the condition matches successfully.

➢ Configure UDP Parameters, as shown below.

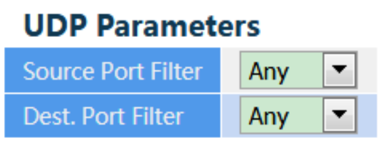


Figure 175 Configre UDP Parameters

Source Port Filter/ Destination Port Filter

Configuration options: Any/ Range（0~65535）

Default configuration: Any

Function: configure conditional parameter-UDP source and destination port number, if select “Range”, need to configure the range of port number. When the UDP port number of received IPv4 rame from imgress port satisfies the configured parameter, the condition matches successfully.

➢ Configure TCP Parameters, as shown below.

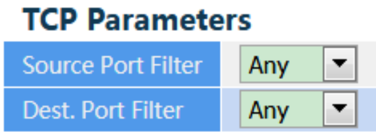


Figure 176 Configure TCP Parameters

Source Port Filter/ Destination Port Filter

Configuration options: Any/ Range（0~65535）

Default configuration: Any

Function: configure conditional parameter-TCP source and destination port number, if select "Range", need to configure the range of port number. When the TCP port number of received IPv4 rame from imgress port satisfies the configured parameter, the condition matches successfully.

7.7.4 Typical Configuration Example

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

Configuration steps:

1. Create ACL1, set ingress port to 2, action to Permit, as shown in Figure 170.
2. Configure ACL1 entry, frame type to Ethernet Type, as shown in Figure 171.
3. Configure ACL1 entry, parameters of Ethernet Type, Set SMAC filter to 02-02-02-02-02-02, as shown in Figure 171.
4. Create ACL, set ingress port to 2, action to Deny, as shown in Figure 170.
5. Keep all the other parameters default or empty.

7.8 MAC Address Configuration

7.8.1 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.

7.8.2 Web Configuration

1. Configure MAC address aging time, as shown below.

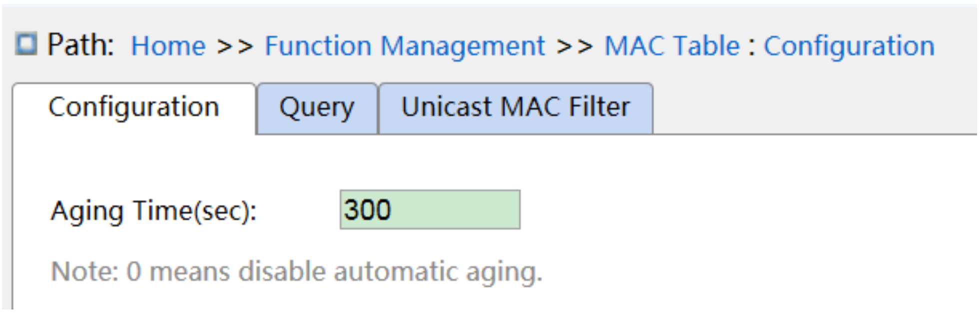


Figure 177 MAC Address Aging Time Configuration

Aging Time

Configuration range: 0 or 10~1000000s

Default configuration: 300s

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

2. Configure static MAC address table items, as shown below.

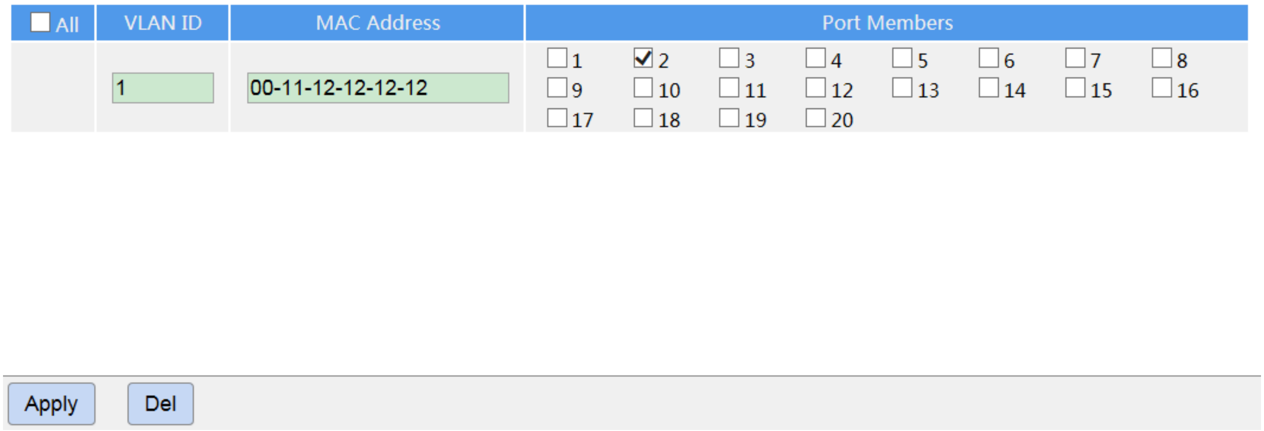


Figure 178 Configure Static MAC Address table items

VLAN ID

Configuration options: all created VLAN IDs

Default configuration: VLAN 1

Function: Configuration the VLAN ID of static MAC address。

MAC address

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

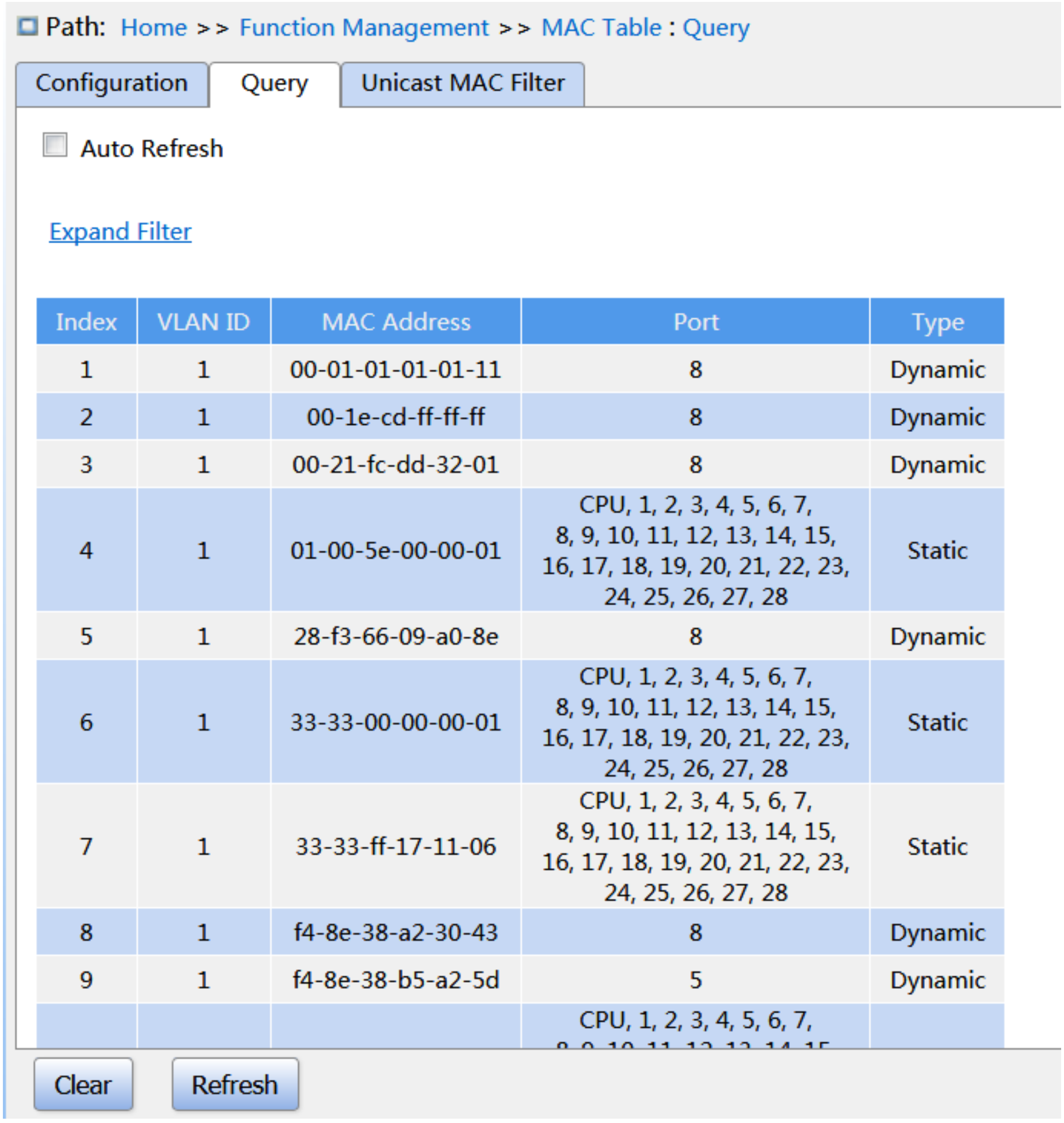
Function: Configure MAC address. For unicast MAC address, the lowest bit in the first byte is 0. For multicast MAC address, the lowest bit in the first byte is 1.

Port Members

Function: Select ports to forward the packets with this destination MAC address.

Click <Add New Static Entry> to configure static MAC address entry. A maximum of 64 static MAC address entries are supported.

3. View MAC address table, as shown below.



Index	VLAN ID	MAC Address	Port	Type
1	1	00-01-01-01-01-11	8	Dynamic
2	1	00-1e-cd-ff-ff-ff	8	Dynamic
3	1	00-21-fc-dd-32-01	8	Dynamic
4	1	01-00-5e-00-00-01	CPU, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28	Static
5	1	28-f3-66-09-a0-8e	8	Dynamic
6	1	33-33-00-00-00-01	CPU, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28	Static
7	1	33-33-ff-17-11-06	CPU, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28	Static
8	1	f4-8e-38-a2-30-43	8	Dynamic
9	1	f4-8e-38-b5-a2-5d	5	Dynamic
			CPU, 1, 2, 3, 4, 5, 6, 7,	

Figure 179 View MAC address table

VLAN ID

Configuration options: */>=/<=/select range

Default configuration: *

Function: display the MAC table according to the configured VLAN ID.

MAC Address

Configuration options: */>=/<=/select range

Default configuration: *

Function: display the MAC table according to the configured MAC address.

Port

Configuration options: */include/not include

Default configuration: *

Function: display the MAC table according to the configured port.

Type

Configuration options: */static/dynamic

Default configuration: *

Function: display the MAC table according to the configured type.

7.9 PoE

7.9.1 Introduce

POE (Power Over Ethernet) means that the switch can supply power over twisted-pair remotely through Ethernet port, and reliable powered distance is up to 100m. It effectively solve the problem of centralized power supply for IP phone, wireless AP, portable device charger, card brushing machine, camera, data acquisition and so on, without considering the wiring of the indoor power supply system, it can supply the power to the equipment at the same time as it is connected to the network.

The serial switch POE meet IEEE 802.3at standard, it includes PSE and PD, PSE (Power Sourcing Equipment) is the device that supply power to other device, and PD (Powered Device) is the device that powered in the poe power supply system.

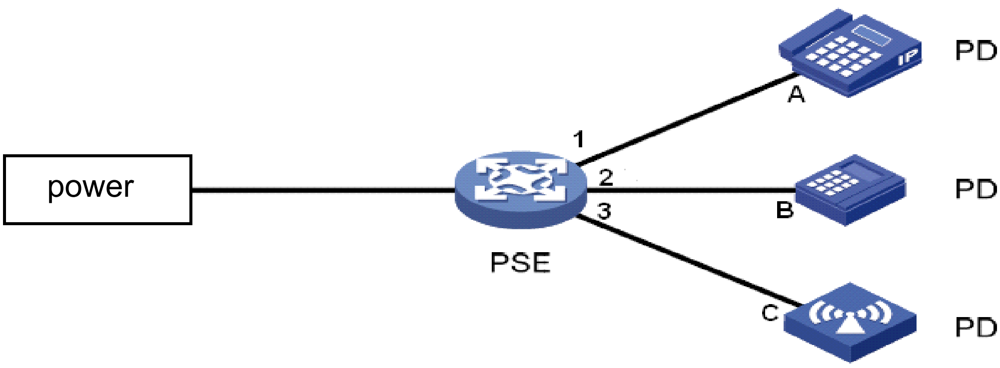


Figure 180 POE power supply system

7.9.2 Web Configuration

1. POE Global Configuration, as shown below.

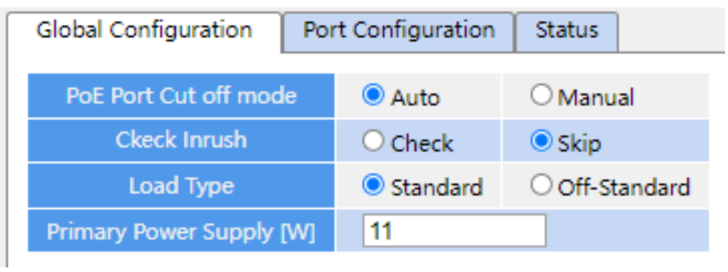


Figure 181 POE Global Configuration

PoE Port Cut off mode

Configuration options: Auto/Manual

Default configuration: Auto

Function: configure the power supply management mode of PoE.

Description: when the total power consumption of all PD devices is greater than the maximum power that PSE can provide, in manual mode, PSE supplies power according to the order of PD device access, that is, the first access PD device is supplied first. In auto mode, PSE supplies power to connected PD devices according to port power priority.

Check Inrush (Check load start current)

Configuration options: Check/skip

Default configuration: Check

Function: Check the start current of PD device.

Load Type

Configuration options: Standard/off-standard

Default configuration: Standard

Function: configure the type of PD device that can be powered.

Primary Power Supply

Configuration options: 1-120(without Auxiliary Power); 1-240(with Auxiliary Power)

Default configuration: 120

Features: Configure the maximum power the PSE device can provide. When the device is used as PSE, the maximum power that the whole machine can provide: no auxiliary power supply, the maximum power is 120W; the external auxiliary power supply, the maximum power is 240W. If the total power consumption by all PD devices exceeds the configuration value, the last accessed PD device (manual mode) or the lowest priority PD device (auto mode) can’t be powered.

1. Configure PoE of port, as shown below.

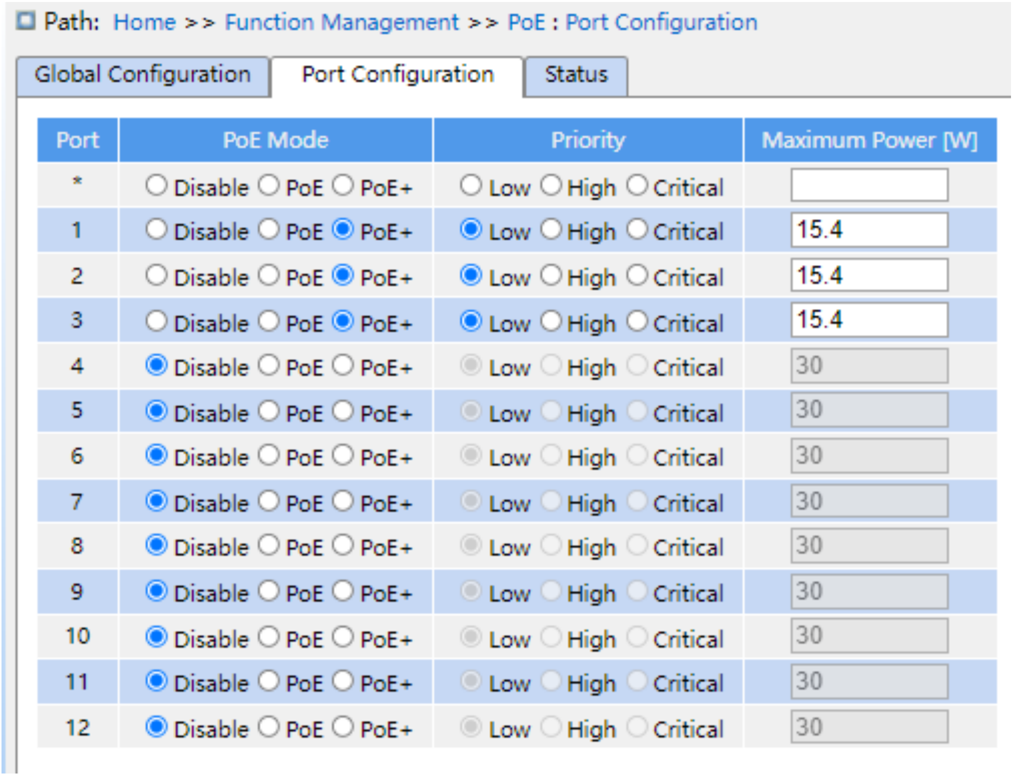


Figure 182 Port PoE Configuration

PoE Mode

Configuration options: Disable/PoE/PoE+

Default configuration: Disable

Functiona: Whether enable POE of the port. PoE: the 100M ethernet supports PoE output that meet IEEE802.3af; PoE+: 100M ethernet supports PoE output that meet IEEE802.3at.

Prioxy

Configuration options: Low/High/Critical

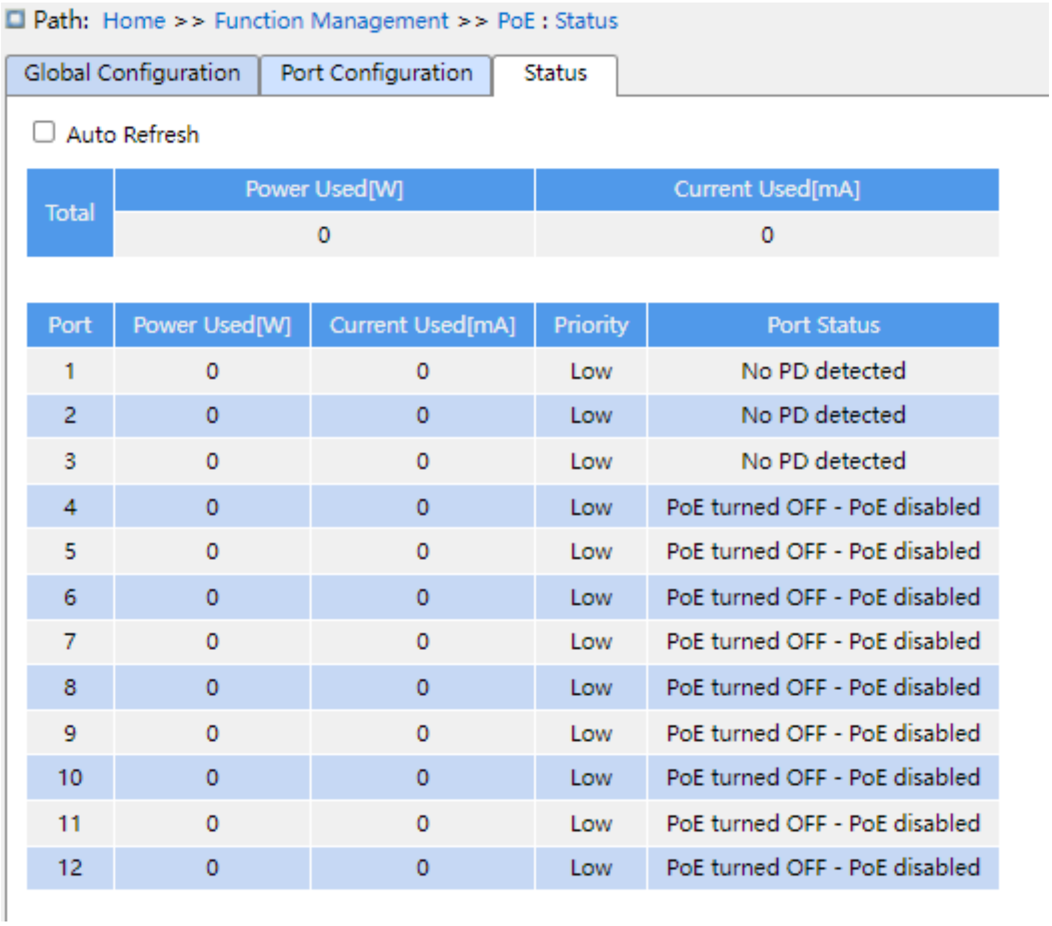
Function: configure port supply power priority. “Low” is the lowest priority and “High” is the secondary priority and “Critical” is the highest priority.

Maximum Power [W]

Configuration range: 1~15.4w（PoE）/1~30.0w（PoE+）

Function: configure the maximum output power of the PoE port. If the power consumption by the port connected PD device exceeds this configuration value, the PD device can’t be powered. According to the actual requirments, the user can reasonably configure the output power limit of each port of the switch, so as to meet the power supply requirment of each port effectively.

2. View PoE Status, as shown below.



Total	Power Used[W]	Current Used[mA]
	0	0

Port	Power Used[W]	Current Used[mA]	Priority	Port Status
1	0	0	Low	No PD detected
2	0	0	Low	No PD detected
3	0	0	Low	No PD detected
4	0	0	Low	PoE turned OFF - PoE disabled
5	0	0	Low	PoE turned OFF - PoE disabled
6	0	0	Low	PoE turned OFF - PoE disabled
7	0	0	Low	PoE turned OFF - PoE disabled
8	0	0	Low	PoE turned OFF - PoE disabled
9	0	0	Low	PoE turned OFF - PoE disabled
10	0	0	Low	PoE turned OFF - PoE disabled
11	0	0	Low	PoE turned OFF - PoE disabled
12	0	0	Low	PoE turned OFF - PoE disabled

Figure 183 Display PoE Port Status

Power Used/Current Used/Priority

Function: Displays power consumption, current, and priority parameters for PoE ports.

Port Status

Display options：No PD detected/Invalid PD/PoE turned ON/PoE turned OFF-PoE disabled/ PoE turned OFF-Power budget exceeded/PoE turned OFF-PD overload/ PoE turned ON-PD forced ON

Function: Displays PoE status of port.

Explain：” No PD detected” refers to enable PoE, but do not detect the PD device.

“Invalid PD” refers to enable PoE, dectect the PD but power supply is abnormal.

“PoE turned ON” refers to enable PoE, detect the PD device and power supply is normal.

“PoE turned OFF-PoE disabled” refers to diable PoE.

“PoE turned OFF-Power budget exceeded” refers to enable PoE, detect the PD device, but when the access of the PD device causes the total power consumption of all PD devices to exceed the maximum power consumption provided by the whole device, the PD device can't be powered.

"PoE turned OFF-PD overload" refers to enable PoE, detect the PD device, and the total power consumption by all PD devices does not exceed the maximum power consumption provided by the whole device, but the PD device power consumption exceed the maximum output power of the PoE port, the PD device can't be powered.

"PoE turned ON-PD forced ON" refers to enable PoE, and enable forced power.

7.9.3 Typical Application Example

As shown in Figure 180, the maximum power provided by the switch as PSE is 11W, the switch port 1 and 2 are connected to device A and B, the maximum power consumption of A is 5W, the maximum power consumption of B is 4W, and the switch port 3 is expected to connect to the device C, and the maximum power consumption of C is 5w.

Requirement:

1. The switch is connected only to device A and B, it can supply power normally;
2. If the PD device C is connected to port 3 of the switch, the total power consumption by all PD devices is greater than the maximum power that the switch can provide, need to ensure power to device C which is connected with port 3 of switch first.

PSE Configuration as following:

1. Configuare the cut off mode to Auto, Primary Power Supply is 11W, as showin in Figure 181.
2. Enable the PoE function of port 1~3, configure the priority of port 3 is "Critical", the other configuration as default, as shown in Figure 182.

7.10 IGMP Snooping

7.10.1 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.

There are three versions of the Internet Group Message Protocol (IGMP): IGMPv1, IGMPv2, and IGMPv3. IGMPv1 is defined in RFC1112, IGMPv2 is defined RFC2236, and IGMPv3 is defined in RFC3376.

IGMPv1 supports two types of packets (report and query packets) and defines the basic group member query and report process.

IGMPv2, on the basis of IGMPv1, provides the leave packet of the fast leave mechanism for group members. With this mechanism, when the last member leaves a multicast group, the router is instructed to conduct fast convergence. In comparison with IGMPv1, IGMPv2 supports two types of query packets: general query packet and group-specific query packet. The switch periodically sends a general query packet to query the membership. When a host leaves a multicast group, after the switch receives a leave message, the switch sends a group-specific query packet to determine whether all members leave the multicast group.

The host source filtering function is added to IGMPv3. This function enables a host to specify whether to receive or reject packets from some specific multicast group sources.

7.10.2 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.

IGMP snooping proxy: The IGMP snooping proxy function is configured on an edge device to reduce the number of IGMP report packets and leave packets received by an upstream device, thereby improving the overall performance of the upstream device. A device on which the IGMP snooping proxy function is configured functions as a host of its upstream device, and functions as a querier of its downstream host.

7.10.3 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).

7.10.4 Web Configuration

1. Enable IGMP Snooping, as shown below.

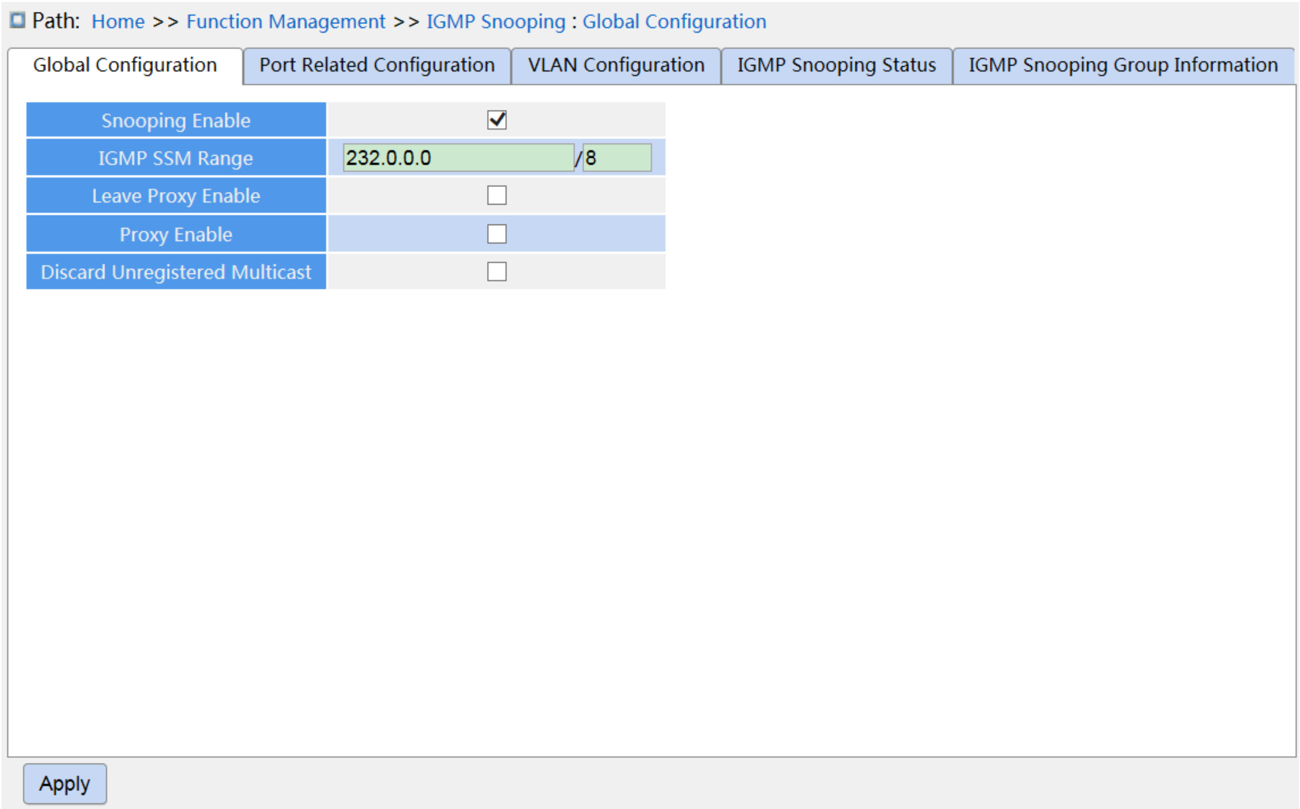


Figure 184 Configure IGMP Snooping

Snooping Enabled

Configuration options: Enable/Disable

Default configuration: Disable

Function: Enable or disable the global IGMP Snooping protocol.

IGMP SSM Range

Configuration Format: A.B.C.D/ 4~32

Default configuration: 232.0.0.0/8

Function: Only hosts and routers with the address within the value of this parameter can run the service model of IGMP source specific multicast (SSM) provided that the hosts and routers support the IGMP SSM service model. The SSM service model provides users with a transmission service of specifying multicast sources for a client.

Leave Proxy Enabled

Configuration options: Enabled/Disabled

Default configuration: Disabled

Function: Specify whether to forward leave packets to the querier. When it is enabled, leave packets are not forwarded.

Proxy Enabled

Configuration options: Enabled/Disabled

Default configuration: Disabled

Function: Specify whether to forward leave packets and member report packets to the querier. When it is enabled, leave packets and member report packets are not forwarded.

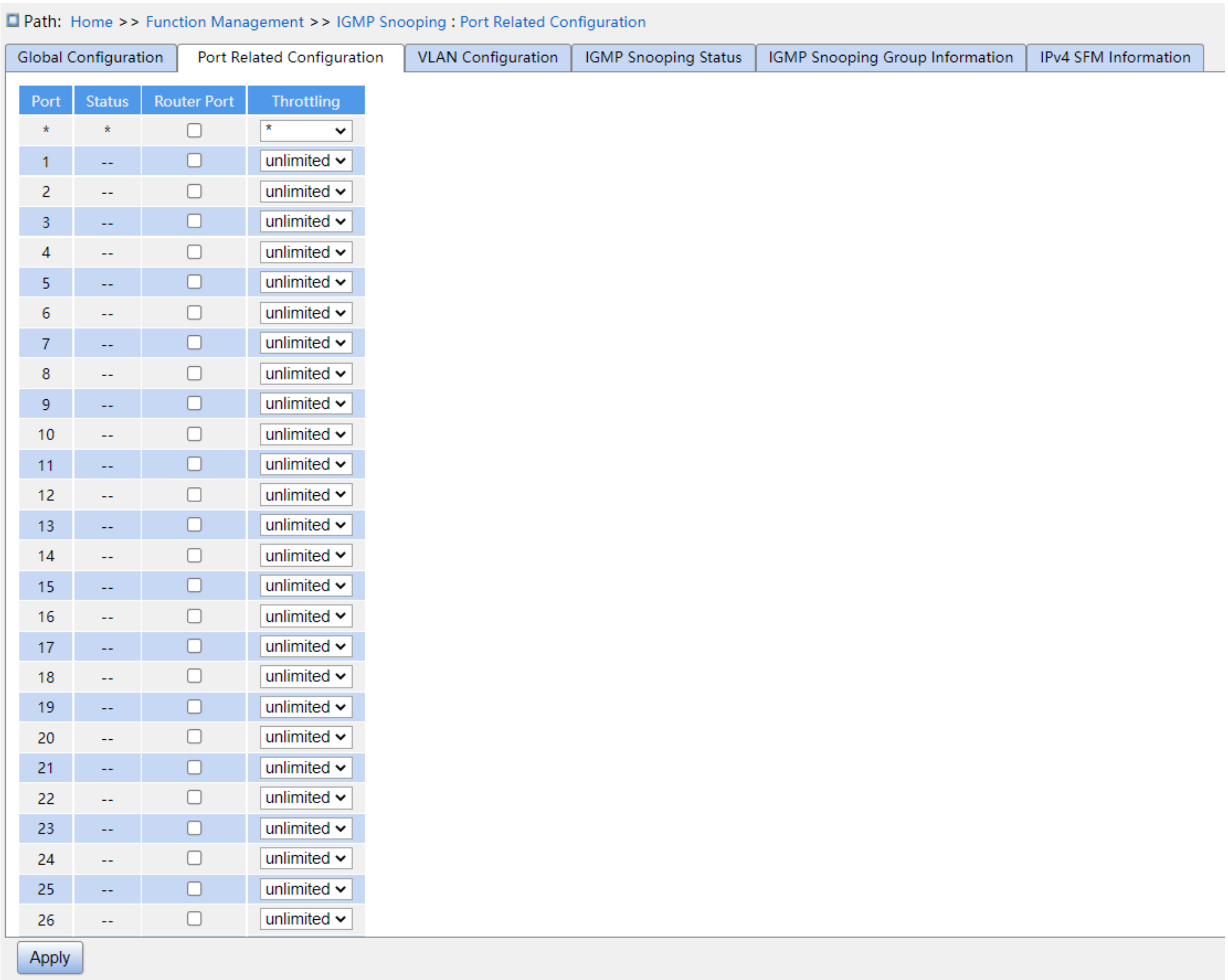
Discard Unregistered Multicast

Configuration options: Enabled/Disabled

Default configuration: Disabled

Function: Whether the switch discards when it receives unknown multicast packets.

2. Configure IGMP port, as shown below.



Port	Status	Router Port	Throttling
*	*	☐	*
1	--	☐	unlimited
2	--	☐	unlimited
3	--	☐	unlimited
4	--	☐	unlimited
5	--	☐	unlimited
6	--	☐	unlimited
7	--	☐	unlimited
8	--	☐	unlimited
9	--	☐	unlimited
10	--	☐	unlimited
11	--	☐	unlimited
12	--	☐	unlimited
13	--	☐	unlimited
14	--	☐	unlimited
15	--	☐	unlimited
16	--	☐	unlimited
17	--	☐	unlimited
18	--	☐	unlimited
19	--	☐	unlimited
20	--	☐	unlimited
21	--	☐	unlimited
22	--	☐	unlimited
23	--	☐	unlimited
24	--	☐	unlimited
25	--	☐	unlimited
26	--	☐	unlimited

Figure 185 Configure IGMP Port

Status

Configuration options: --/static/dynamic/both

Function: Displays the router port status. **static** indicates that the port is statically configured as a routed port; **dynamic** indicates that the port is dynamically learned as a routed port. **Both** indicates that the port is dynamically configured as a routing port and dynamically learns to route the port.

Router Port

Configuration options: Enabled/Disabled

Default configuration: Disabled

Function: Configure router port.

Throttling

Configuration options: unlimited/1~10

Default configuration: unlimited

Function: Whether to limit the number of multicast entries learnt by a port.

3. Configure IGMP Snooping VLAN, as shown below.

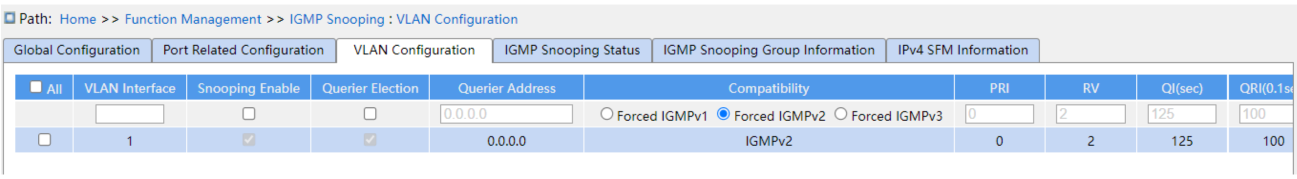


Figure 186 Configure IGMP Snooping VLAN

VLAN Interface

Configuration options: all created VLAN IDs

Snooping Enabled

Configuration options: Enable/Disable

Default configuration: Disable

Function: Enable or disable the VLAN IGMP Snooping function. The precondition of this function is to enable global IGMP Snooping function.

Querier Election

Configuration options: Enable/Disable

Default configuration: Enable

Function: Enable or disable the IGMP query function for the selected VLAN. The precondition of this function is to enable global IGMP Snooping function and the VLAN 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.

Querier Address

Configuration Format: A.B.C.D

Function: Configure the source IP address of sending the query packet. When set as 0.0.0.0, the IP address of the VLAN port is used as the querier address.

Compatibility

Configuration options: Forced IGMPv1/Forced IGMPv2/Forced IGMPv3

Default configuration: Forced IGMPv2

Function: Configure IGMP version.

PRI（Priority of Interface）

Configuration range: 0~7

Default configuration: 0

Function: Configure the priority of IGMP control packet.

RV（Robustness Variable）

Configuration range: 1~255

Default configuration: 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.

QI（Query Interval）

Configuration range: 1~31744s

Default configuration: 125s

Function: Configure the interval of sending general query packet.

QRI（Query Response Interval）

Configuration range: 0~31744（unit: 0.1s）

Default configuration: 100

Function: Configure the max response time of responding general query packet.

LLQI（Last Member Query Interval）

Configuration range: 0~31744（unit: 0.1s）

Default configuration: 10

Function: Configure the max response time of responding specific query packet.

CAUTION

Caution:

QI, QRI, and LLQI configuration is valid only for querier.

URI（Unsolicited Report Interval）

Configuration range: 0~31744s

Default configuration: 1s

Function: Set the interval for a host to re-send a report packet for joining a multicast group

Click <Add New IGMP VLAN> to configure IGMP Snooping VLAN entry. A maximum of 32 IGMP Snooping VLAN entries are suppoted.

4. View IGMP Snooping status, as shown below.

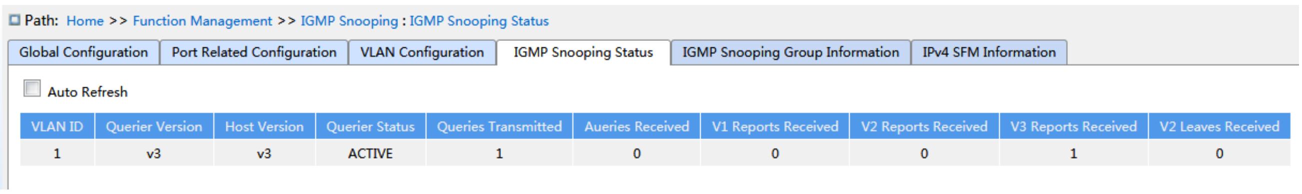


Figure 187 View IGMP Snooping Status

5. View the multicast member list, as shown below.

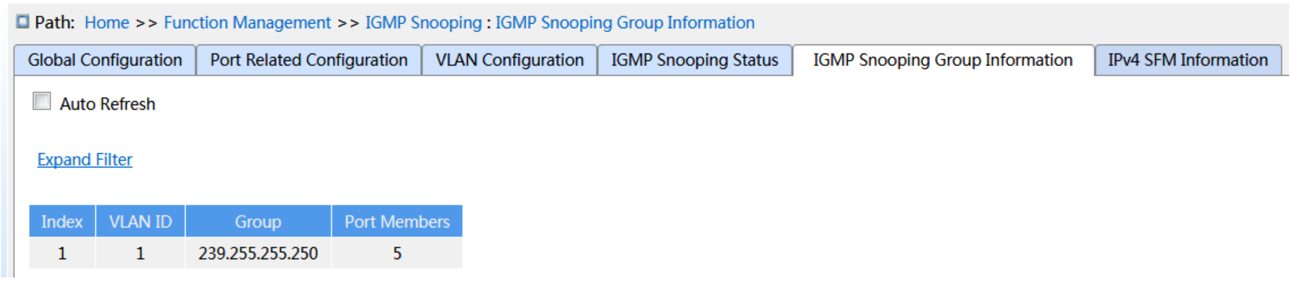


Figure 188 IGMP Snooping Member List

VLAN ID

Configuration options: */>=/<=/selection range

Default configuration: *

Function: Display the group information according to configured VLAN ID.

Group

Configuration options: */>=/<=/selection range

Default configuration: *

Function: Display the group information according to configured group address.

Port

Configuration options: */include/not include

Default configuration: *

Function: Display the group information according to configured port.

6. View the IPv4 SMF information, as shown below.

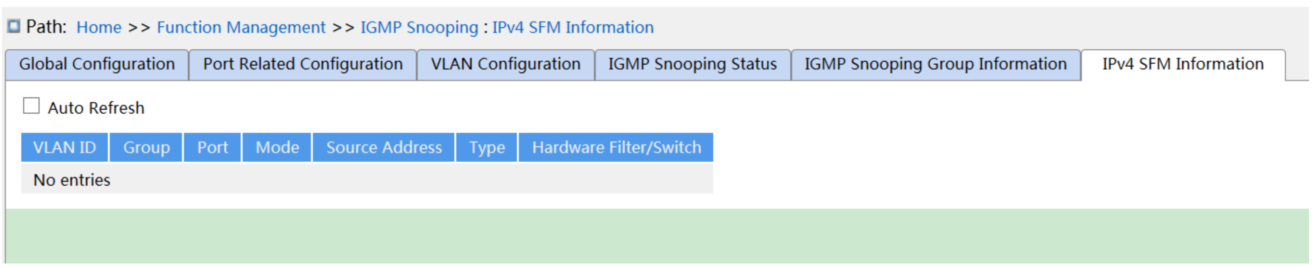


Figure 189 IGMP Snooping IPv4 SFM information

7.10.5 Typical Application Example

As shown in Figure 190, 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.

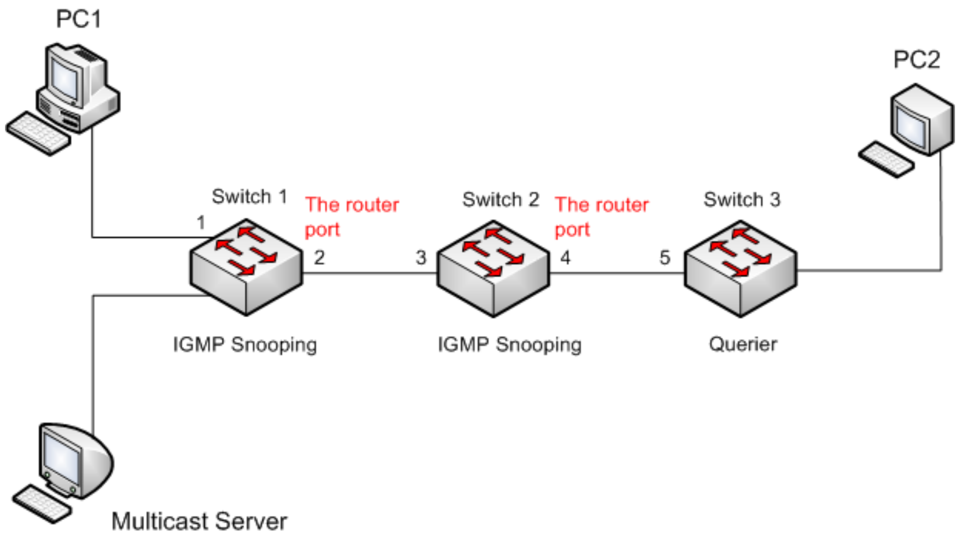


Figure 190 IGMP Snooping Application Example

- 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.

7.11 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 191.

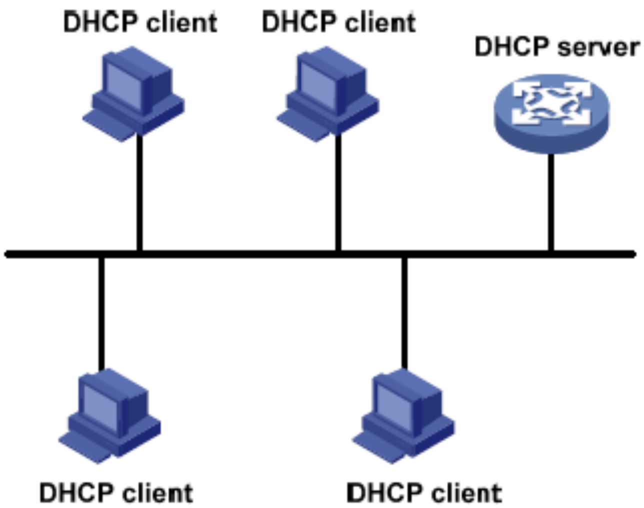


Figure 191 DHCP Typical Application

Caution:

In the process of dynamic obtainment of IP addresses, the messages are transmitted in the way of broadcast, so it is required that the DHCP client and the DHCP server are in a same segment. If they are in the different segments, the client can communicate with the server via a DHCP relay to get IP addresses and other configuration parameters.

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. The tenancy term for static allocation is permanent.

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.

7.11.1 DHCP Server Configuration

7.11.1.1 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.

7.11.1.2 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.

7.11.1.3 Web Configuration

1. Enable DHCP server, as shown below.

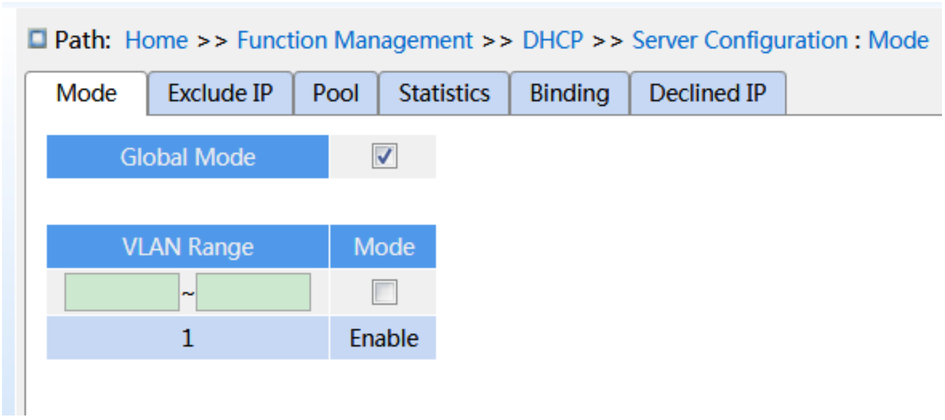


Figure 192 Enable DHCP Server

Global Mode

Configuration options: Disabled/Enabled

Default configuration: Disabled

Function: Select the current switch to the DHCP server to allocate an IP address to a client or not.

{VLAN Range, Mode}

Configuration range: {1~4093, Disabled/Enabled}

Function: If the VLAN of a client that applies for an IP address is set to Enabled, the DHCP server allocates an IP address to the client. Otherwise, the DHCP server does not allocate an IP address to the client.

2. Create DHCP address pool, as shown below.

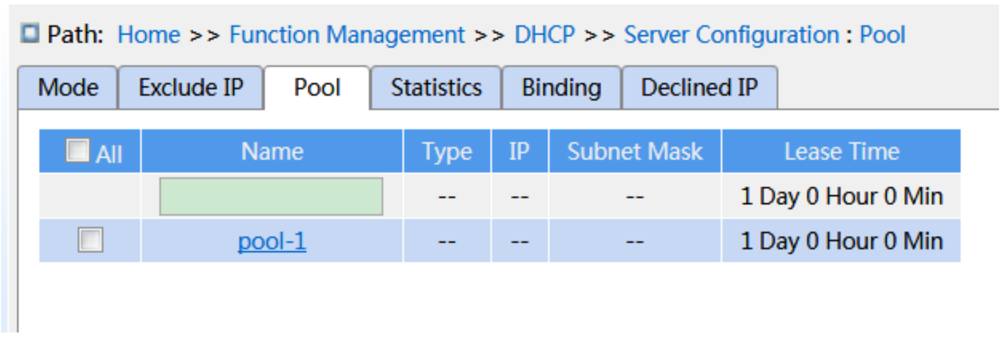


Figure 193 Create DHCP Address Pool

Name

Configuration range: 1~32 characters

Function: configure the name of the IP address pool.

Click <Apply> to create a new DHCP address pool.

3. Configure the DHCP address pool, click <Name> in Figure 193 to configure the DHCP address pool, as shown below.

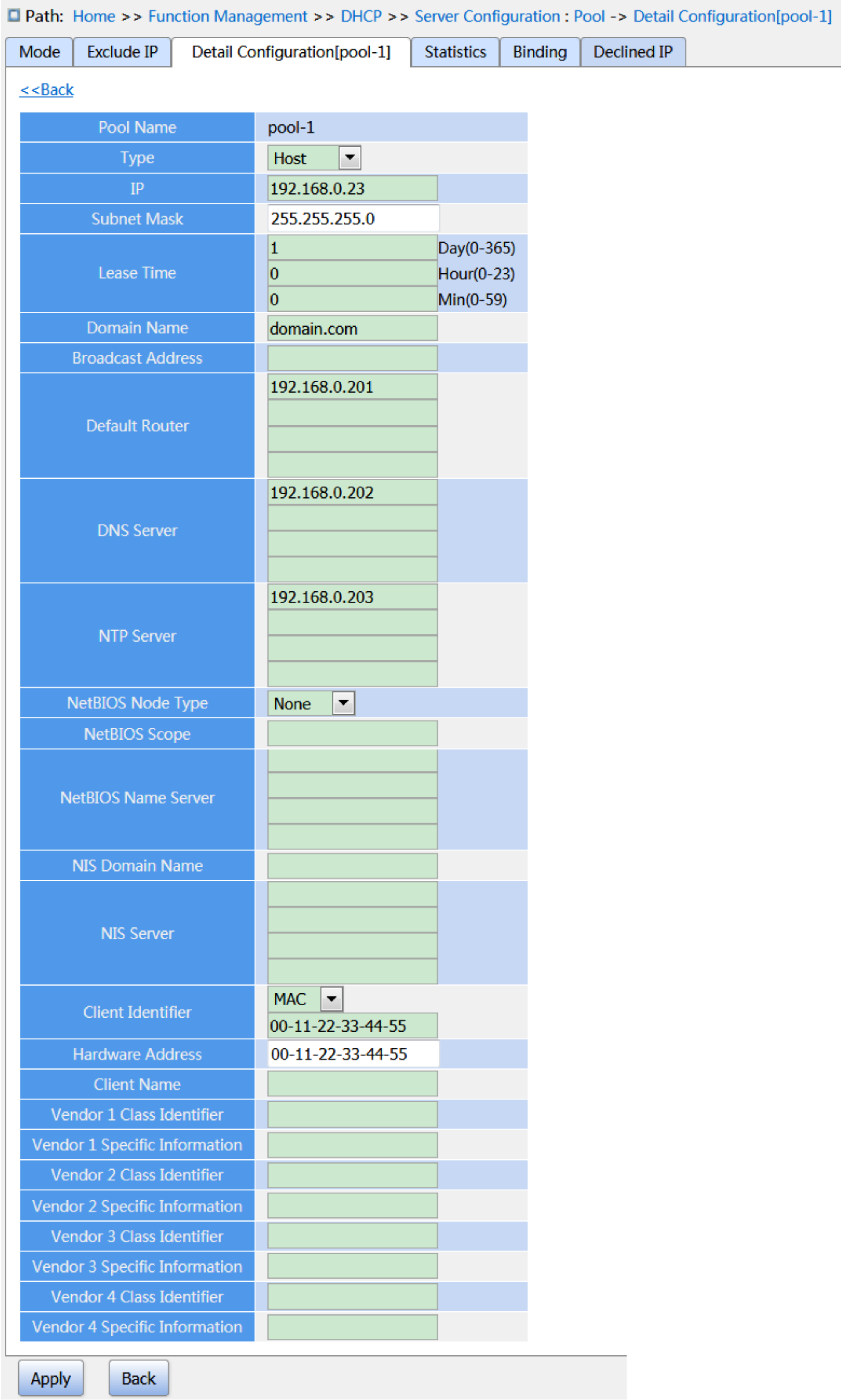

Path: Home >> Function Management >> DHCP >> Server Configuration : Pool -> Detail Configuration[pool-1]
Mode
Exclude IP
Detail Configuration[pool-1]
Statistics
Binding
Declined IP
<<Back
Pool Name
pool-1
Type
Host
IP
192.168.0.23
Subnet Mask
255.255.255.0
Lease Time
1
Day(0-365)
0
Hour(0-23)
0
Min(0-59)
Domain Name
domain.com
Broadcast Address
Default Router
192.168.0.201
DNS Server
192.168.0.202
NTP Server
192.168.0.203
NetBIOS Node Type
None
NetBIOS Scope
NetBIOS Name Server
NIS Domain Name
NIS Server
Client Identifier
MAC
00-11-22-33-44-55
Hardware Address
00-11-22-33-44-55
Client Name
Vendor 1 Class Identifier
Vendor 1 Specific Information
Vendor 2 Class Identifier
Vendor 2 Specific Information
Vendor 3 Class Identifier
Vendor 3 Specific Information
Vendor 4 Class Identifier
Vendor 4 Specific Information
Apply
Back

Figure 194 Configure IP Address Pool

Type

Configuration options: None/Network/Host

Default configuration: None

Function: Configure the address pool type. Network: the switch dynamically allocates IP addresses to multiple DHCP clients. Host: the switch supports static allocation of IP addresses to special DHCP clients.

{IP，Subnet Mask}

Function: Network indicates that you can 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.

Host indicates that you can configure the IP address of the client statically bounded. 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.

Lease Time

Configuration range: 0 day 0 hour 0 minute~365 days 23 hours 59 minutes

Default configuration: 1 day 0 hour 0 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.

Domain Name

Configuration range: 1~36 characters

Configuration 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.

Broadcast Address

Format: A.B.C.D

Function: Configure the client broadcast address allocated by DHCP server.

Default Router

Format: A.B.C.D

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 4 gateways.

DNS Server

Format: A.B.C.D

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 4 DNS servers.

NTP Server

Format: A.B.C.D

Function: Configure the client NTP server address allocated by DHCP server.

NetBIOS Node Type

Configuration options: None/B-node/P-node/M-node/H-node

Default configuration: None

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 B-node obtains the mapping in broadcast mode. The P-node obtains the mapping by sending a unicast packet to communicate with the WINS server. The M-node obtains the mapping by sending a broadcast packet the first time. If the M-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 H-node obtains the mapping by sending a unicast packet to communicate with the WINS server the first time. If the H-node fails to obtain the mapping the first time, it obtains the mapping by sending a broadcast packet the second time.

NetBIOS Scope

Configuration range: 1~36 characters

Function: Configure the NetBIOS name.

NetBIOS Name Server

Format: A.B.C.D

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 4 WINS servers.

NIS Domain Name

Configuration range: 1~36 characters

Function: Configure the client NIS domain name allocated by DHCP server.

NIS Server

Format: A.B.C.D

Function: Configure the client NIS server address allocated by DHCP server.

Client Identifier

Configuration options: None/FQDN/MAC

Default configuration: None

Function: When the pool type is host, specify client's unique identifier

Hardware Address

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

Function: When the pool type is host, configure the MAC address of the client statically bounded.

Client Name

Configuration range: 1~32 characters

Function: Configure client user name.

Vendor i Class Identifier

Configuration range: 1~64 characters

Function: Configure the client Vendor Class Identifier allocated by DHCP server.

Vendor i Specific Information

Configuration range: 1~64 hexadecimal numbers

Function: Configure the client Vendor Specific Information allocated by DHCP server.

4. Configure excluded IP addresses(IP addresses are not allocated dynamically in the DHCP address pool), as shown below.

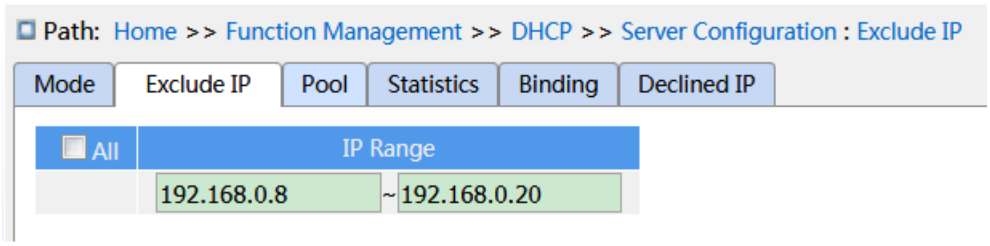


Figure 195 Configure Excluded IP Addresses

IP Range

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.

5. View DHCP server statistics information, as shown below.

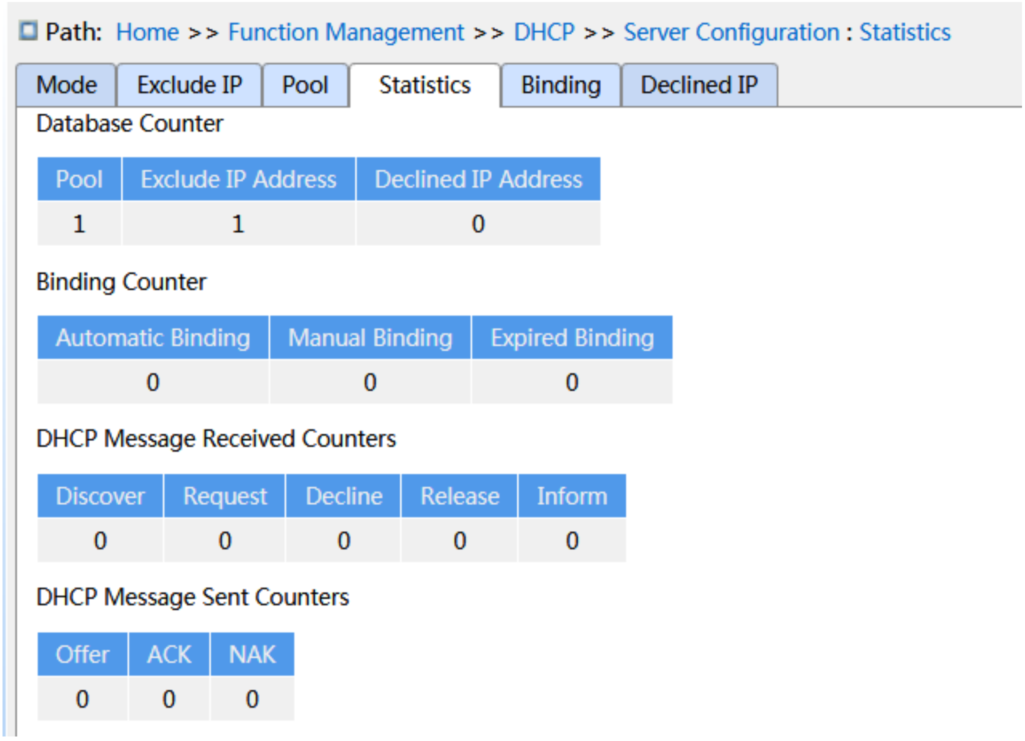


Figure 196 View DHCP Server Statistics Information

6. View information about IP addresses allocated by the DHCP server, as shown below.

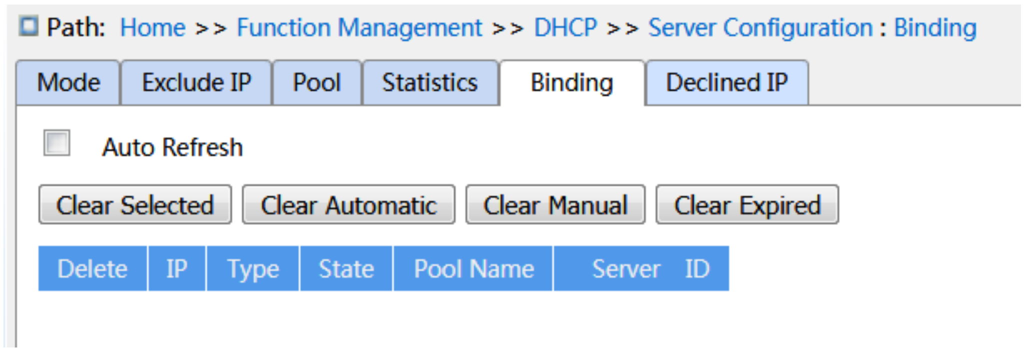


Figure 197 View Information About IP Addresses Allocated by the DHCP Server

7. View the IP addresses declined by DHCP clients, as shown below.

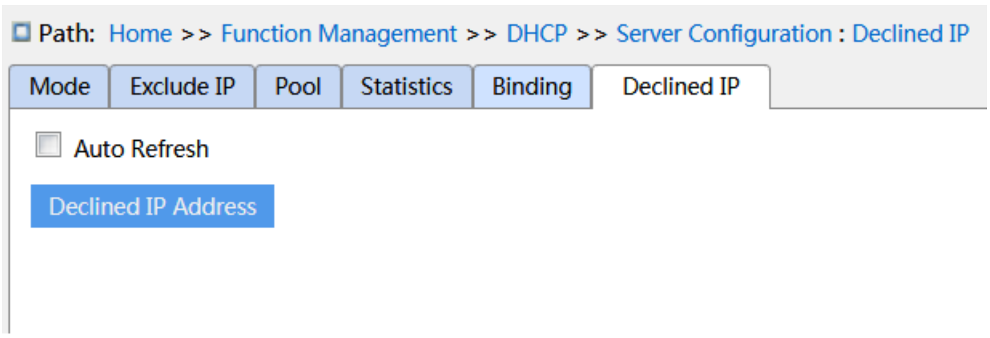


Figure 198 View the IP addresses Declined by DHCP Clients

When a client detects that an IP address allocated by the server conflicts with a static IP address in the same network segment, it sends a decline packet to the server to reject this IP address. The server records the IP address rejected by the client, and will not allocate this IP address to other clients within a certain period of time.

7.11.1.4 Typical Configuration Example

As Figure 199 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 192.168.0.1~192.168.0.10 when DHCP server dynamically allocates IP address.

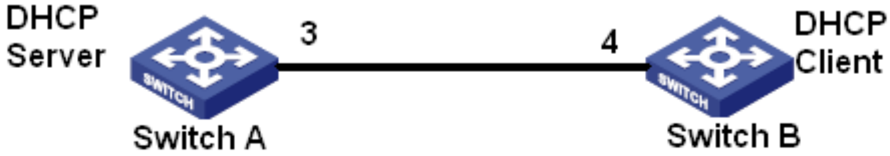


Figure 199 DHCP Typical Configuration Example

Statically allocate IP address

➢ Switch A configuration:

1. Enable DHCP server status in correspond VLANs, as shown in Figure 192.
2. Create a DHCP IP pool: pool-1, as shown in Figure 193.
3. Set the pool type as Host; IP address as 192.168.0.6; mask as 255.255.255.0; Bind the MAC address of switch B: 00-11-22-33-44-55, as shown in Figure 194.

➢ Switch B configuration:

1. Set switch B automatically obtains an IP address through DHCP.
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 200.

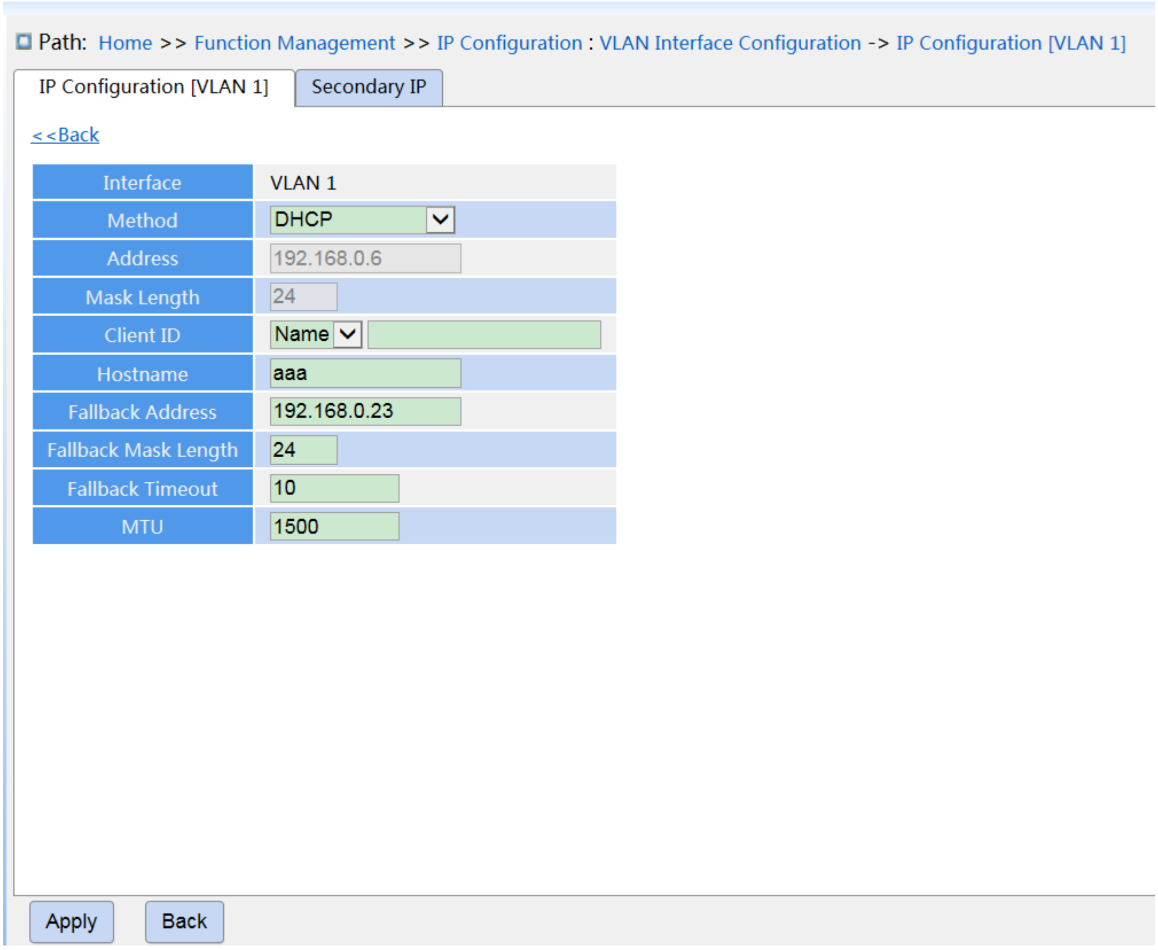


Figure 200 DHCP Client Obtain IP Address-1

Dynamically allocate IP address

➢ Switch A configuration:

1. Enable DHCP server status in correspond VLANs, as shown in Figure 192.

2. Create a DHCP IP pool: pool-1, as shown in Figure 193.

3. Set the pool type as Network; IP address as 192.168.0.6; mask as 255.255.255.0, the rest is the Default configuration.

4. Configure excluded IP address range as 192.168.0.1~192.168.0.10, as shown in Figure 195.

➢ Switch B configuration:

1. Set switch B automatically obtains an IP address through DHCP.

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 201.

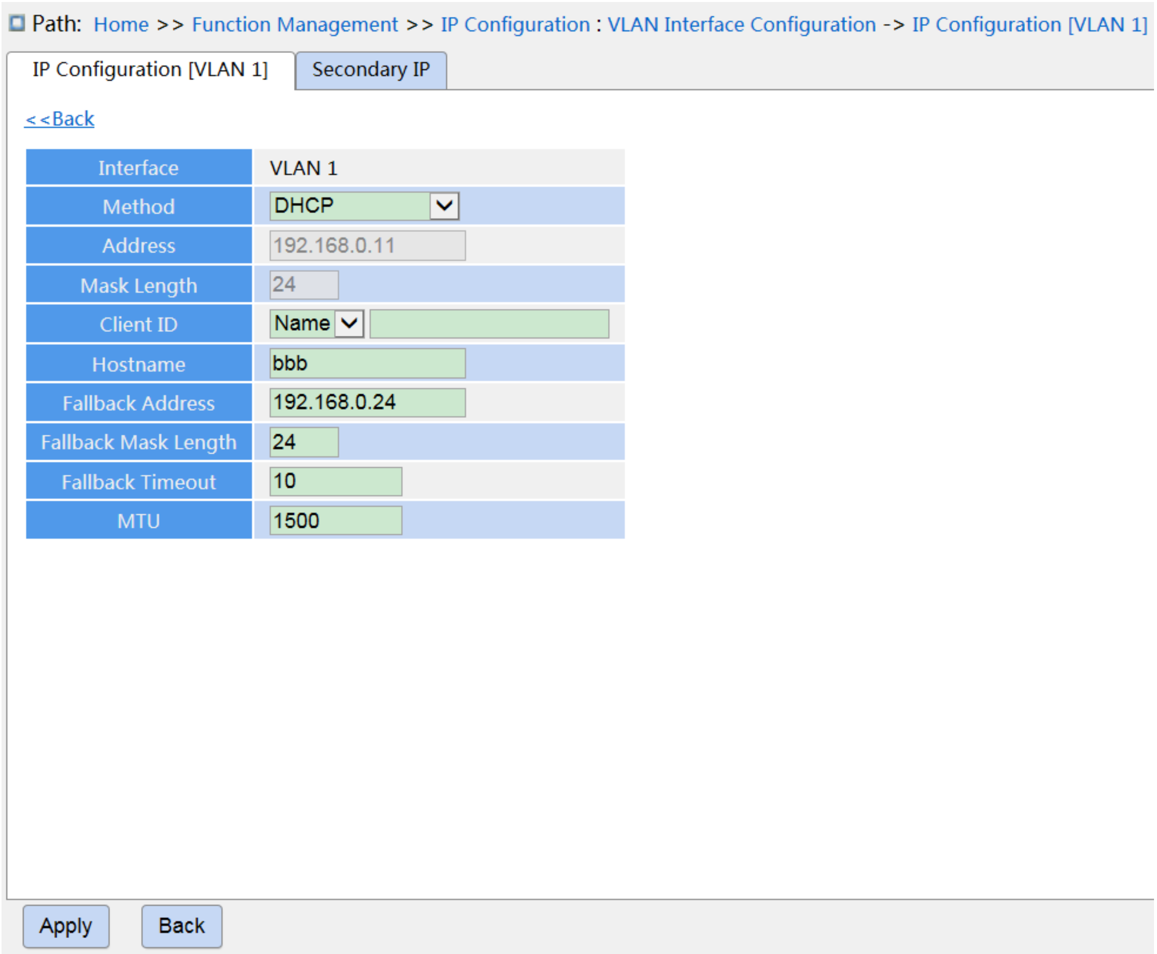


Figure 201 DHCP Client Obtain IP Address-2

7.11.2 DHCP Snooping

7.11.2.1 Introduce

DHCP Snooping is a monitoring function of DHCP services on layer 2 and is a security feature of DHCP, ensuring the security of the client further. The DHCP Snooping security mechanism can control that only the trusted port can forward the request message of the DHCP client to the legal server, meanwhile, it can control the source of the response message of the DHCP server, ensuring the client to obtain an IP address from the valid server and preventing the fake or invalid DHCP server from allocating IP addresses or other configuration parameters to other hosts.

DHCP Snooping security mechanism divides port to trusted port and untrusted port.

Trusted port: it is the port that connects with the valid DHCP server directly or indirectly. Trusted port normally forwards the request messages of DHCP clients and the response messages of DHCP servers to guarantee that DHCP clients can obtain valid IP addresses.

Untrusted port: it is the port that connects with the invalid DHCP server. Untrusted port does not forward the request messages of DHCP clients and the response messages of DHCP servers to prevent DHCP clients from obtaining invalid IP addresses.

7.11.2.2 Web Configuration

1. Enable DHCP Snooping function, as shown below.

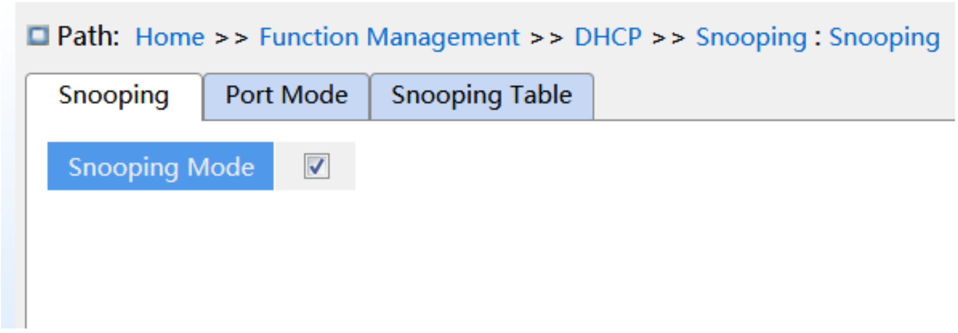


Figure 202 DHCP Snooping State

DHCP Snooping Mode

Configuration options: Enable/Disable

Default configuration: Disable

Function: Enable/Disable switch DHCP Snooping function.

Caution:

The switch working as DHCP server and client cannot enable DHCP Snooping function.

2. Configure trusted ports, as shown below.

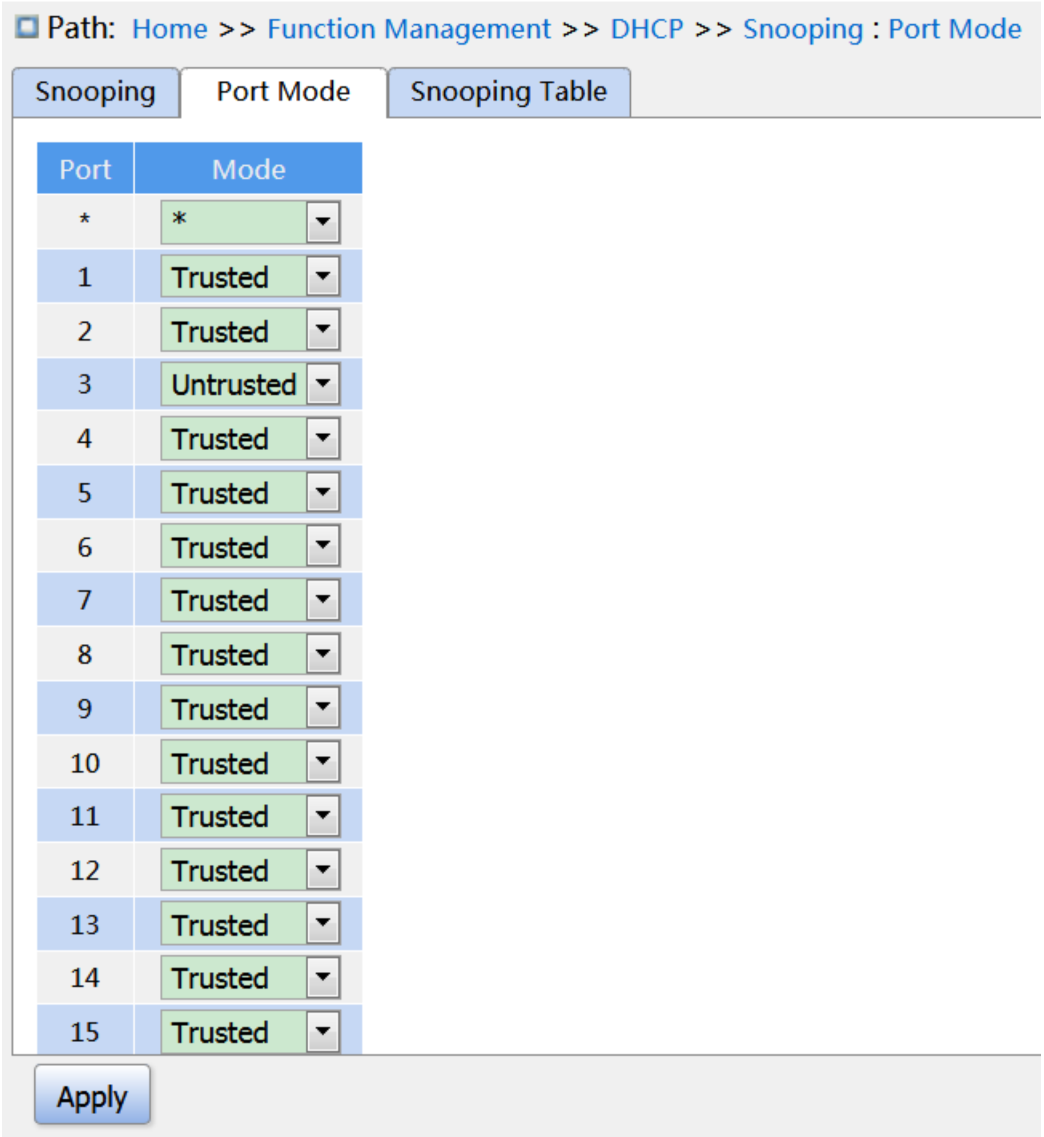


Figure 203 Configure Trust Port

Mode

Configuration options: Trusted/Untrusted

Default configuration: Untrusted

Function: set the port to a trusted port or an untrusted port. The ports that connect with valid DHCP servers directly or indirectly are trusted ports.

3. View DHCP snooping entries, as shown below.

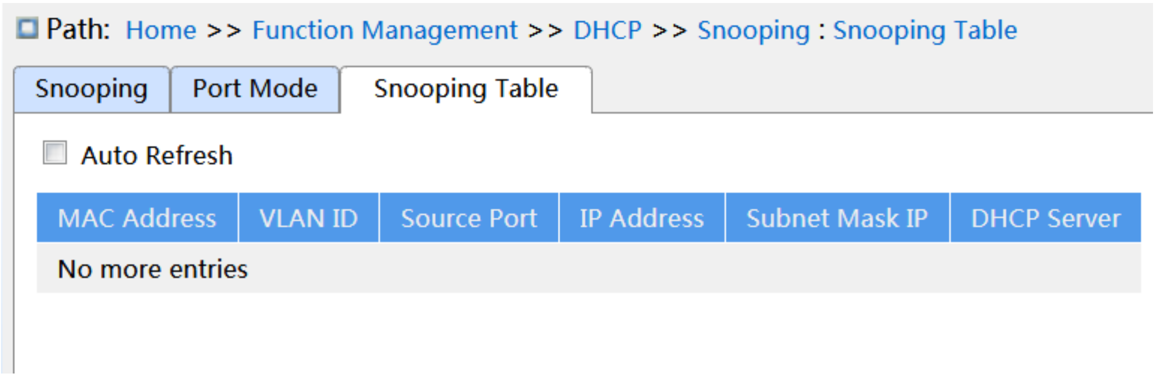


Figure 204 View DHCP snooping entries

7.11.2.3 Typical Configuration Example

As Figure 205 shows, the DHCP client requests an IP address from the DHCP server. An unauthorized DHCP server exists in the network. Set port 1 to a trusted port by DHCP Snooping to forward the request message of the DHCP client to the DHCP server and forward the response message of the DHCP server to the DHCP client. Set port 3 to an untrusted port that cannot forward the request message of the DHCP client and the response message of the unauthorized DHCP server, ensuring that the client can obtain a valid IP address from the valid DHCP server.

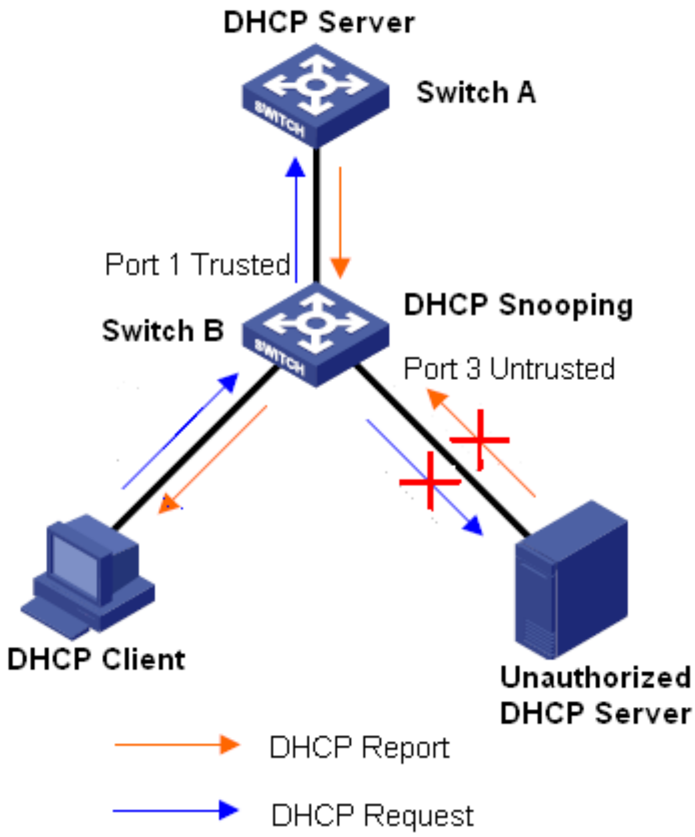


Figure 205 DHCP Snooping Typical Configuration Example

Switch B configuration:

➢ Enable DHCP Snooping function, as shown inFigure 202.

➢ Set the port 1 of switch B to a trusted port and set the port 3 to an untrusted port, as shown in Figure 203.

7.11.3 DHCP Relay

7.11.3.1 Introduction

1. DHCP Realy

DHCP relay is the forwarding of DHCP packets between the DHCP server and the client. When the DHCP client is not on the same subnet as the server, there must be a DHCP relay to forward DHCP request and reply messages. The data forwarding of the DHCP relay is different from the normal route forwarding. The normal route forwarding is relatively transparent, and the device generally does not modify the IP packet content. However, after receiving the DHCP message, the DHCP relay will regenerate a DHCP message and then forward it out. In the view of the DHCP client, the DHCP relay agent is like a DHCP server; in the view of the DHCP server, the DHCP relay agent is like a DHCP client.

The DHCP relay forwards the received DHCP request packet to the DHCP server in unicast mode, and forwards the received DHCP response packet to the DHCP client. The DHCP relay is equivalent to a forwarding station and is responsible for communicating DHCP clients and DHCP servers located on different network segments. It realizes dynamic IP management for multiple network segments as long as a DHCP server is installed, that is, DHCP dynamic IP management in Client-Relay-Server mode, as shown below.

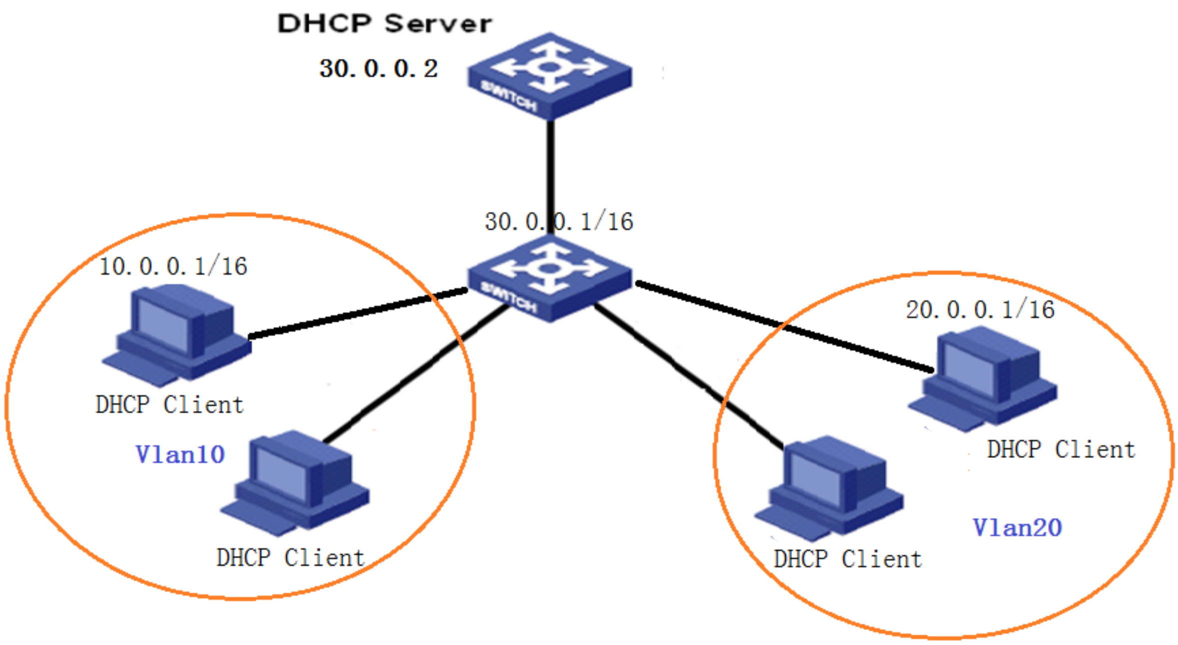


Figure 206 Client—Relay—Server Mode

2. DHCP Relay Agent Information (option 82)

When the relay device performs DHCP relay, you can add some options to specify some network information of the DHCP client, so that the server can assign different IP addresses to users according to more accurate information. According to RFC3046, the option number of the option option used is 82, so it is also called option 82.

Option 82 (Relay Agent Information Entry) records the client information. When the Option 82 supported DHCP Snooping receives the request message from the DHCP client, it add the corresponding Option 82 field into the messages and then forward the message to the DHCP server. The server supporting Option 82 can flexibly allocate addresses according to the Option 82 message.

Once Option 82 is enabled, the Option 82 field will be added into the message. The Option 82 field of this series switches contains two sub-options: sub-option 1 (Circuit ID) and sub-option 2 (Remote ID). The formats of two sub-options are shown below:

➢ Sub-option 1 contains the VLAN ID and number of the port that receives the request message from the DHCP client, as shown in Table 7

Table 7 Sub-option 1 Field Format

Sub-option type（0x01）	Length（0x04）	VLAN ID	Port number

One byte	One byte	Two bytes	Two bytes

Sub-option type: the type of the sub-option 1 is 1.

Length: the number of bytes that VLAN ID and Port number occupy.

VLAN ID: On DHCP Relay device, the VLAN ID of the port that receives the request message from the DHCP client.

Port number: On DHCP Realy device, the number of the port that receives the request message from the DHCP client.

- The content of Sub-option 2 is the MAC address of the DHCP Relay device that receives the request message from the DHCP client, as shown in Table 8.

Table 8 Sub-option 2 Field Format-MAC Address

Sub-option type（0x02）	Length（0x06）	MAC Address
One byte	One byte	6 bytes

Sub-option type: the type of the sub-option 2 is 2

Length: the number of bytes that sub-option2 content occupies. MAC address occupies 6 bytes and character string occupies 16 bytes.

MAC address: the content of sub-option2 is the MAC address of the DHCP Realy device that receives the request message from the DHCP client.

If DHCP Relay supports Option 82 function, when the DHCP Relay receives a DHCP request message, it will process the request message according to whether the message contains Option 82 and the client policy, and then forward the processed message to the DHCP server. The specific processing method is shown in Table 9.

Table 9 The treatment request message by DHCP Relay

Receive the request message from the DHCP client	**Configuration policy**	**DHCP Relay device processing the request message**
The request message	Drop	Drop the request message

contains Option 82	Keep	Keep the message format unchanged and forward the message
	Replace	Replace the Option 82 field in the message with the Option 82 field of the Snooping device and forward the new message
The request message does not contain Option 82	Drop/Keep/Replace	Add the Option 82 field of the Relay device into the message and forward it

When the DHCP Relay device receives the response message from the DHCP server, if the message contains Option 82 field, remove the Option 82 field and forward the message to the client.

7.11.3.2 Web Configuration

1. DHCP Relay Global Configuration, as shown below.

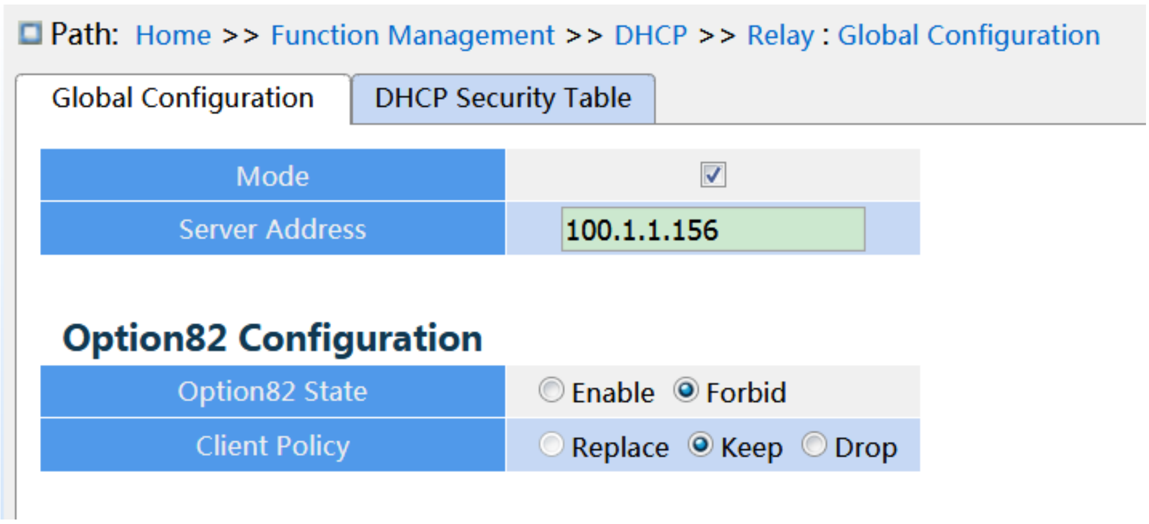


Figure 207 DHCP Relay Global Configuration

Mode

Configuration options: Enable/disable

Default configuration: Disable

Function: whether enable DHCP relay.

Server Address

Function: configure DHCP server address.

Option82 Sate

Configuration options: Enable/forbid

Default configuration: Forbid

Function: whether enable option82 DHCP relay.

Client Policy

Configuration options: Replace/keep/drop

Default configuration: Keep

Function: configure the client policy, DHCP relay process the request message sent by client according to the client policy. The specific treatment as shown in Table 9.

2. View DHCP Security table items, as shown below.

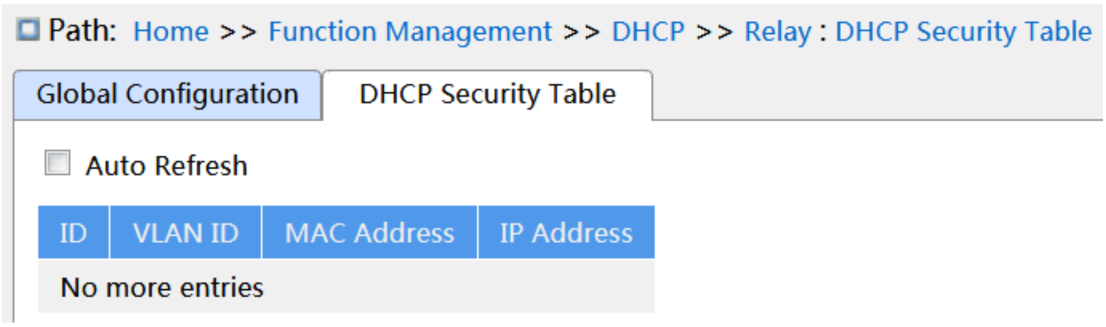


Figure 208 view DHCP Security Table

7.11.3.3 Typical Configuration Example

As shown below, Switch A as the DHCP server, switch B as the DHCP relay, switch C as the DHCP client, and port 1 of switch A connect to port 1 of switch B, port 2 of switch B connect to port 2 of switch C. DHCP server is not in the same LAN as DHCP client. Client dynamically obtain IP address and other network parameters by DHCP mode through DHCP relay.

Figure 209 DHCP typcal configuration example

➢ Switch A configuration:

1. Create the VLAN1 and configure the IP: 100.1.1.156, as shown in Figure 115;
2. Open the dhcp server state on the VLAN 1, as shown in Figure 115;
3. Create the address pool pool-33, as shown in Figure 193;
4. elect the address pool type as Network; IP address: 33.1.1.6; Mask: 255.0.0.0；

➢ Switch B configuration:

1. Create the VLAN1 and configure the IP: 100.1.1.180, as shown in Figure 115;
2. Create the VLAN33 and configure IP: 33.1.1.2, as shown in Figure 115;
3. Enable DHCP relay, as shown in Figure 207;
4. Configure server IP address: 100.1.1.156, as shown in Figure 207；

➢ Switch C configuration:

1. Create VLAN33 and enable DHCP Client, as shown in Figure 115;
2. Switch A assign IP address 33.0.0.1 to switch C.

7.12 IEEE802.1X Configuration

7.12.1 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, as shown in below. User authentication and authorization of port-based access control requires the following elements:

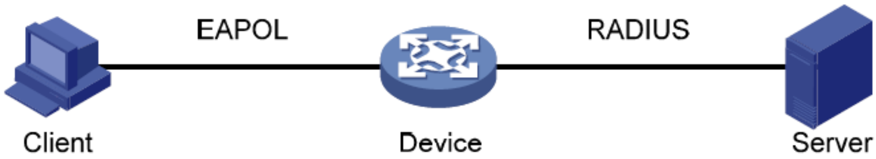


Figure 210 IEEE802.1X Structure

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. The client should support EAPOL (Extensible Authentication Protocol over LAN).

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.

7.12.2 Web Configuration

1. 802.1X Task Manager Configuration, as shown below.

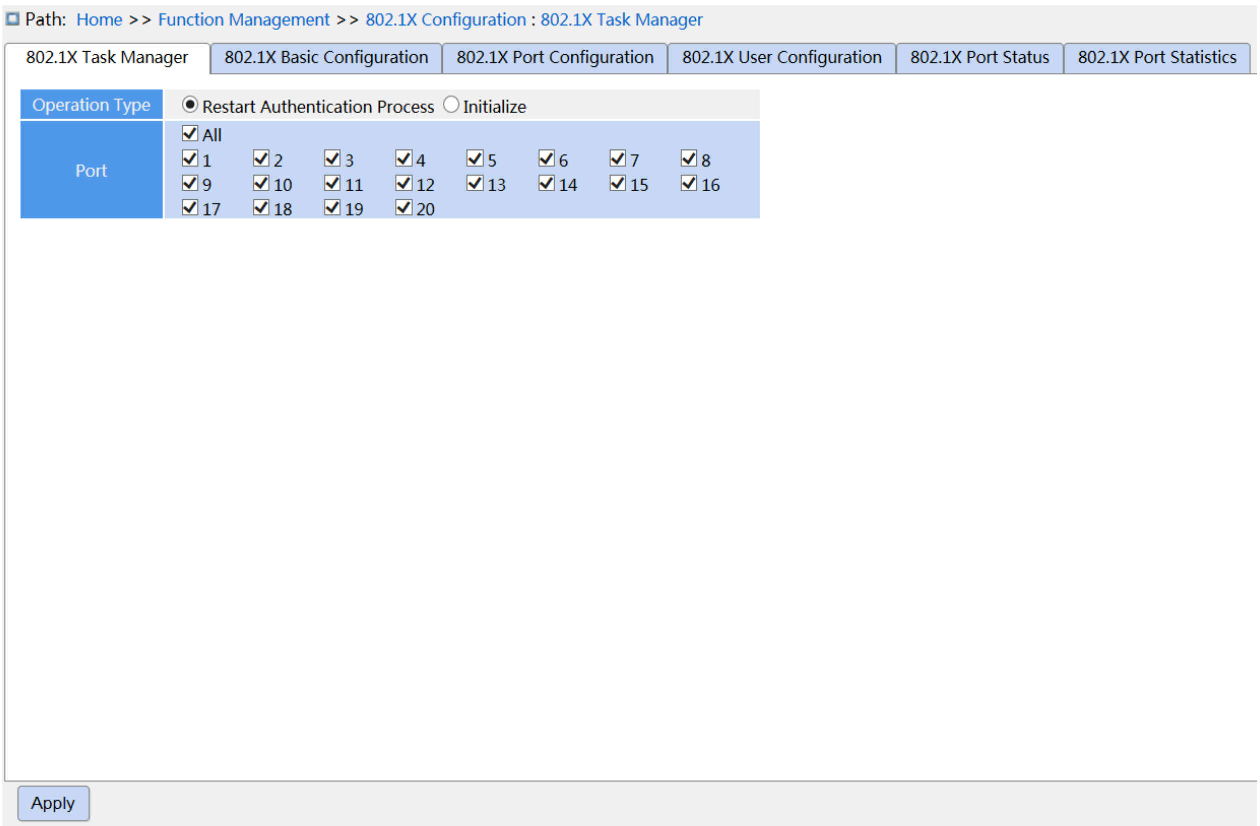


Figure 211 Task Manager configuration

Operation Type

Configuration options: Restart Authentication Process /initialization

Function: When the port selects **Mac-Based** and **port-based** 802.1X authentication mode, you can select <Restart Authentication Process>/<Initialize> to re-authenticate. During the re-authentication process, the port status is switched to the unauthenticated state.

Port

Select the port that needs to Restart Authentication Process /initialize.

2. IEEE802.1X Basic Configuration, as shown below.

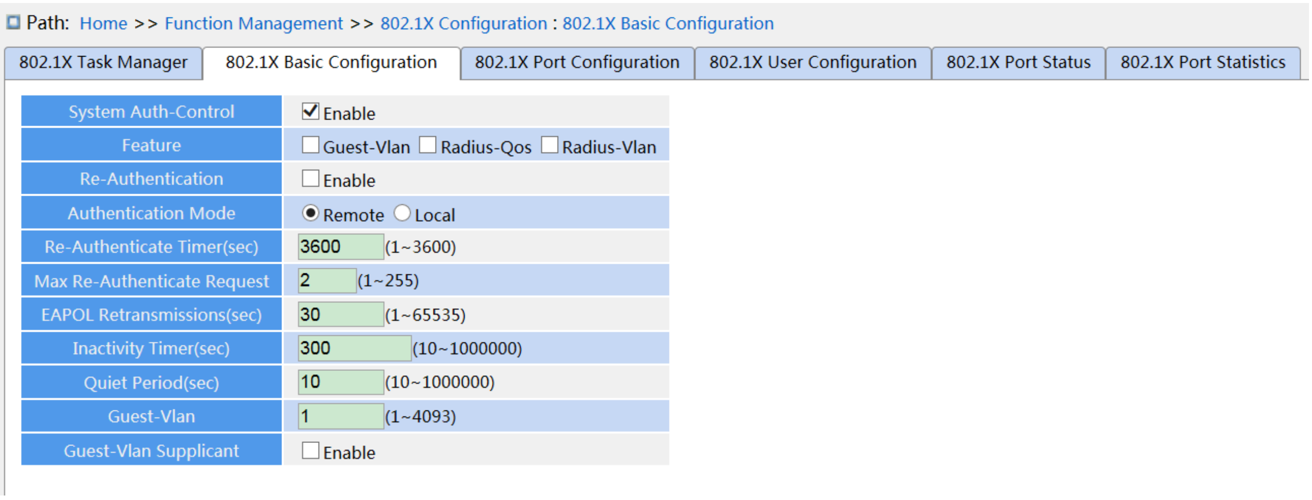


Figure 212 IEEE802.1X Basic Configuration

System Auth-Control

Configuration options: Enable/Disable

Default configuration: Disable

Function: Enable/Disable global IEEE802.1x security function.

Guest-VLAN

Configuration options: Enable/Disable

Default configuration: Disable

Function: When enabled, if a user is not authenticated or fails to be authenticated, the device adds the client authentication port to the guest VLAN. All users that access this port are authorized to access the resources in the guest VLAN.

RADIUS-QOS

Configuration options: Enable/Disable

Default configuration: Disable

Function: When enabled, after the client passes authentication, the server transfers authorization information to the device. If **RADIUS-QOS** is checked on the server, the authorization information includes CoS information assigned for authorization. The equipment will modify the CoS value of the client authentication port based on the assigned value.

RADIUS-VLAN

Configuration options: Enable/Disable

Default configuration: Disable

Function: When enabled, after the client passes authentication, the server transfers authorization information to the device. If **RADIUS-VLAN** is checked on the server, the authorization information includes VLAN information assigned for authorization. The equipment will add the client authentication port to the assigned VLAN.

Re-Authentication

Configuration options: Enable/Disable

Default configuration: Disable

Function: Configure whether regular re-authentication is required when authentication succeeds.

Authentication Mode

Configuration options:Remote/Local

Default configuration: Remote

Function: Configure the radius authentication mode as remote authentication or local authentication.

Re-Authenticate Timer(sec)

Configuration range: 1~3600s

Default configuration: 3600s

Function: When authentication succeeds, set the time interval for re-authentication.

"**Re-Authenticate Timer**" can be configured only if enabling "**Re-Authentication**".

Max Re-Authenticate Request

Configuration range: 1~255

Default configuration: 2

Function: Set the maximum retransmission attempts for Identity EAPOL request packets. If the device still receives no response packets from the client after maximum retransmission attempts, the device will consider authentication fails.

EAPOL Retransmissions

Configuration range: 1~65535s

Default configuration: 30s

Function: Set the overtime for response from the client. After sending a Identity EAPOL request packet, the device will retransmit a Identity EAPOL request packet if it still receives no response from the client after the specified time.

Inactivity Timer

Configuration range :10~1000000s

Default configuration :300s

Function:

After MAC address authentication, if the authentication succeeds, if no packets pass during this time, the corresponding security entry is deleted.

Quiet Period(sec)

Configuration range: 10~1000000s

Default configuration: 10s

Function: If authentication fails, the device enters to quiet period. During the quiet period, the device does not respond to authentication requests from the client.

Guest-VLAN

Configuration range: 1~4095

Default configuration: 1

Function: Configure guest VLAN ID .

Guest-VLAN Supplicant

Configuration options: Enable/Disable

Default configuration: Disable

Function: When enabled, if a user is not authenticated or fails to be authenticated, the device adds the client authentication port to the guest VLAN. When disabled, the device adds the port to the guest VLAN only when this port has no EAPOL frame record.

Caution:

- The precondition for configuring "**Guest-VLAN**", "**Max Re-Authenticate Request**", and

"**Guest-Vlan Supplicant**" is enabling **"Guest -VLAN**".

- It is recommended to disable "Radius-Vlan" and "**Guest -VLAN**", when the authentication port type is Trunk or Hybrid.
- The CoS value assigned for authorization does not change or affect the configuration of the port. However, the priority of the COS value assigned for authorization is higher than a COS value configured by a user. In other words, what is valid after authentication is the CoS value assigned for authorization. If a user fails to be authenticated or goes offline, the CoS value configured by the user take effects.
- The VLAN assigned for authorization or the guest VLAN does not change or affect the configuration of the port. However, the VLAN assigned for authorization or the guest VLAN has a higher priority than a VLAN configured by a user.

After a user initiates authentication, and if the authentication is successful:

If the port enables **RADIUS-VLAN**, the port is added to the VLAN assigned by the RADIUS server.

If the port does not enable **RADIUS-VLAN**, the port is added to the VLAN configured by the user.

If a user fail to be authenticated or goes offline:

If the port enables **Guest-VLAN** and **Guest-Vlan Supplicant**, the port is added to the VLAN.

If the port enables **Guest-VLAN** but does not enable **Guest-Vlan Supplicant**, the port is added to the guest VLAN when no EAPOL fame record is available, and is added to the VLAN configured by the user when EAPOL frame record is available.

If the port does not enable **Guest-VLAN**, the port is added to the VLAN configured by the user.

3. Configure IEEE802.1X port, as shown below.

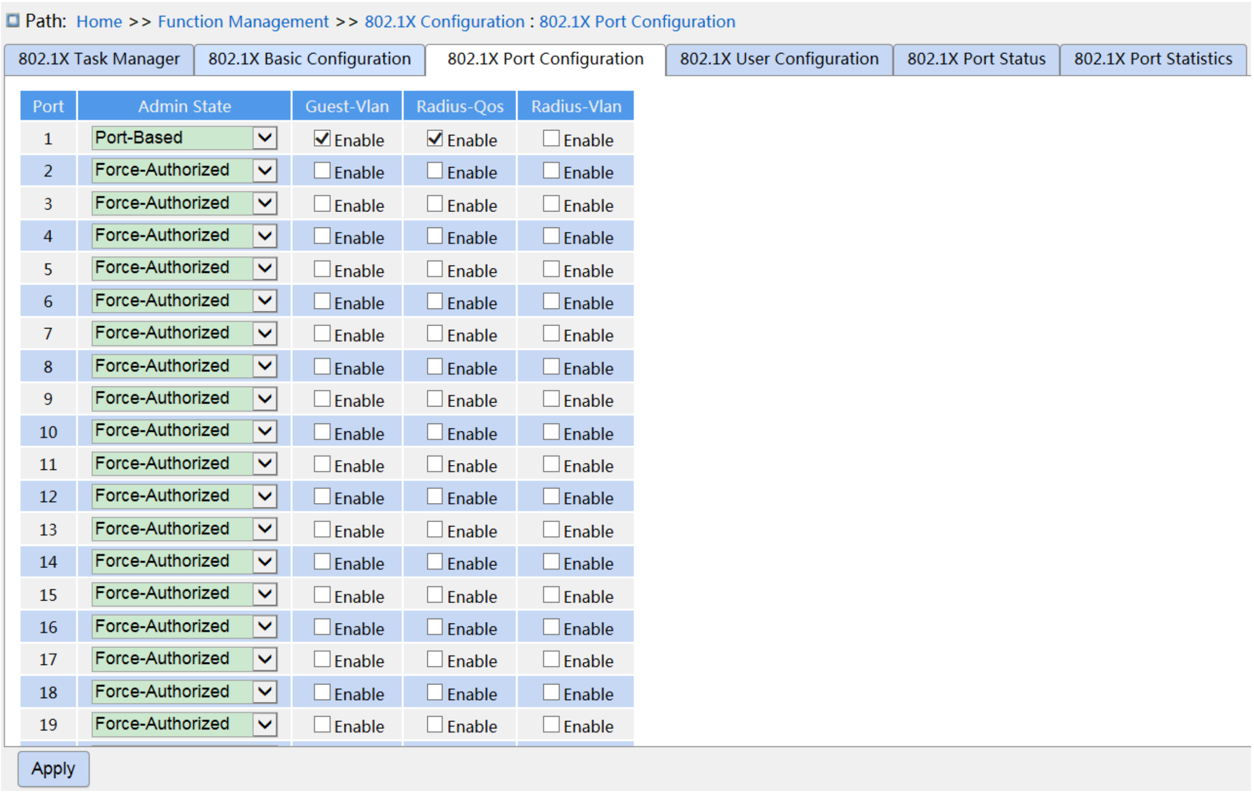


Figure 213 Configure IEEE802.1X port

Port

Configuration options: all switch ports.

Admin State

Configuration options: Force Authorized/Force Unauthorized/Port-based/MAC-based

Default configuration: Force Authorized

Function: Select the port authentication mode.

Description: **Force Authorized** means port is always in an authorized state and allows users to access network resource without authentication.

Force Unauthorized 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. **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.

RADIUS-QOS

Configuration options: Enable/ Disable

Default configuration: Disable

Function: Enable or disable RADIUS-Assigned QoS on port.

RADIUS-VLAN

Configuration options: Enable/ Disable

Default configuration: Disable

Function: Enable or disable RADIUS-Assigned VLAN on port.

Note:

This function is available only when **RADIUS-QOS / RADIUS-VLAN** is enabled at both the global and port levels.

4. IEEE802.1X User Configuration, as shown below.

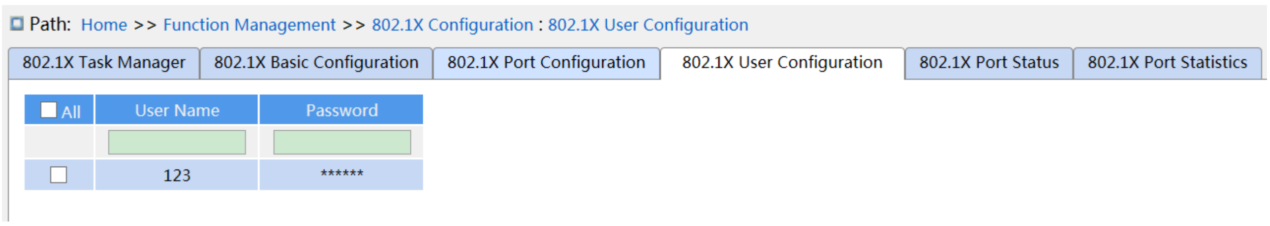


Figure 214 IEEE802.1X User Configuration

User Name

Configuration range: 1-16 character

Default configuration: None

Function: Configure the local authentication username.

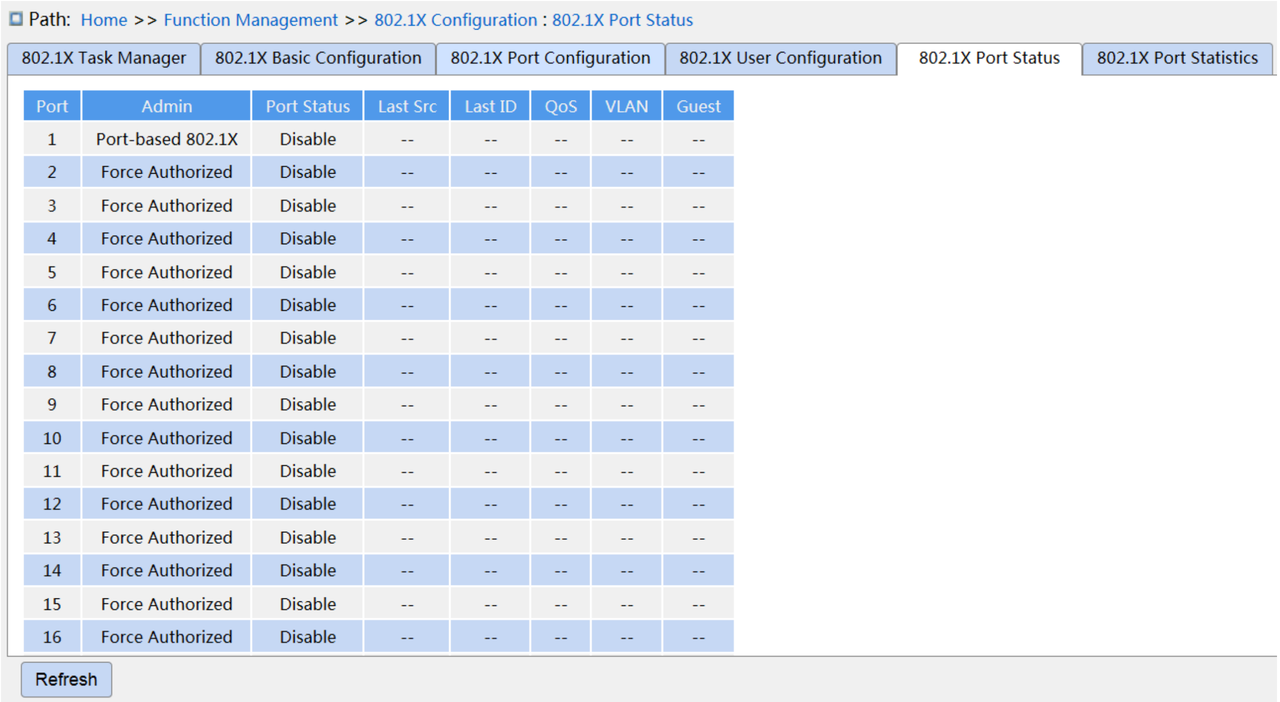
Password

Configuration range: 1-16 character

Default configuration:None

Function: Configure the local authentication password.

5. View IEEE802.1X Port Status, as shown below.



Port	Admin	Port Status	Last Src	Last ID	QoS	VLAN	Guest
1	Port-based 802.1X	Disable	--	--	--	--	--
2	Force Authorized	Disable	--	--	--	--	--
3	Force Authorized	Disable	--	--	--	--	--
4	Force Authorized	Disable	--	--	--	--	--
5	Force Authorized	Disable	--	--	--	--	--
6	Force Authorized	Disable	--	--	--	--	--
7	Force Authorized	Disable	--	--	--	--	--
8	Force Authorized	Disable	--	--	--	--	--
9	Force Authorized	Disable	--	--	--	--	--
10	Force Authorized	Disable	--	--	--	--	--
11	Force Authorized	Disable	--	--	--	--	--
12	Force Authorized	Disable	--	--	--	--	--
13	Force Authorized	Disable	--	--	--	--	--
14	Force Authorized	Disable	--	--	--	--	--
15	Force Authorized	Disable	--	--	--	--	--
16	Force Authorized	Disable	--	--	--	--	--

Figure 215 IEEE802.1X Port Status

Port Status

Configuration options: Globally Disabled, Authorized, Unauthorized, Link Down, x Auth/y Unauth

Disable、Auth、UnAuth、DOWN、x A/y UnA

Function: Display port authentication state. **Disable** indicates IEEE802.1X is diabled globally; **Auth** indicates the user connected to the port passes authentication; **UnAuth** indicates the user connected to the port fails to pass authentication; **DOWN** indicates the port is link down; **x A/y UnA** indicates x users are authorized and y users are unauthorized when the port authentication mode is MAC-based Auth.

6. View IEEE802.1X statistic, as shown below.

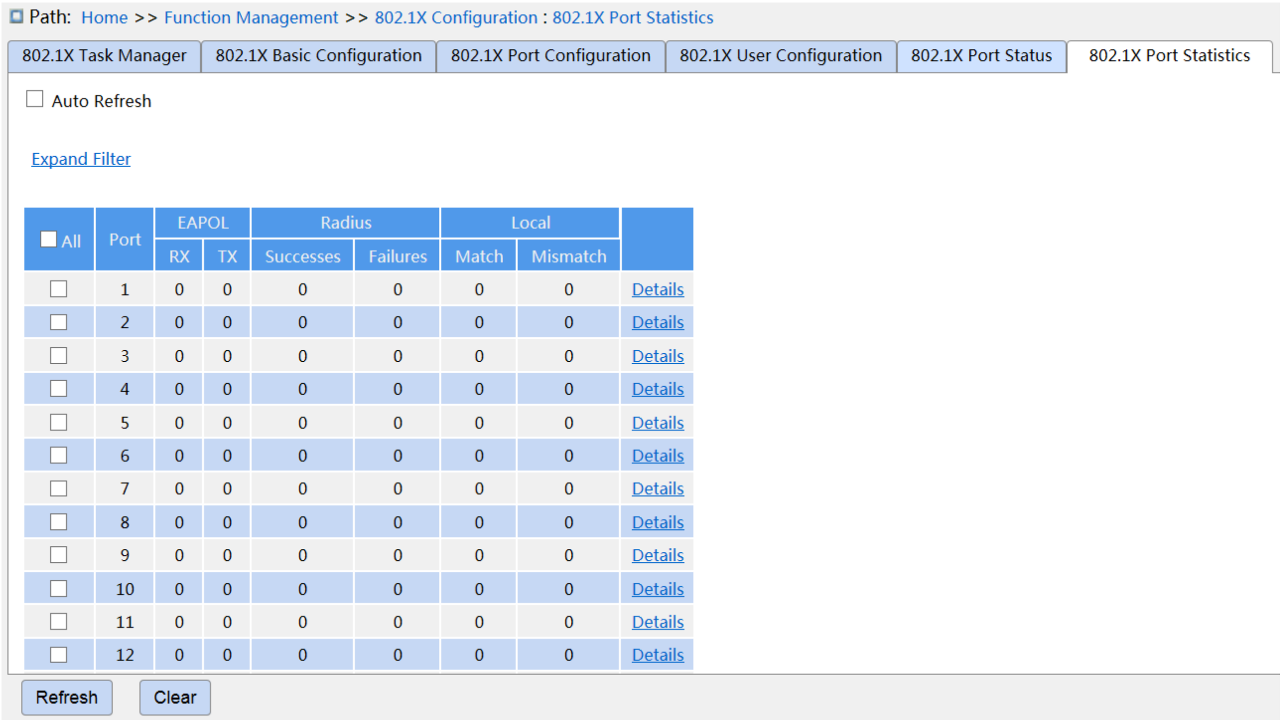


Figure 216 View IEEE802.1X Statistics

Click port **Details** to enter the IEEE802.1X information statistics interface of the corresponding port, as shown below.

<<Back

Statistics		
Eapol	Rx Total	0
	Tx Total	0
	Rx RespId	0
	Tx ReqId	0
	Rx RespMD5	0
	Tx ReqMD5	0
	Rx Resp	0
	Tx Req	0
	Rx Start	0
	Rx LogOff	0
	Rx Invalid Type	0
	Rx Invalid Len	0
Radius	Rx Access Challenges	0
	Rx Other Requests	0
	Rx Auth Successes	0
	Rx Auth Failures	0
	Tx Responses	0
	Mac Address	--
Local	MD5-Challenge Match	0
	MD5-Challenge Mismatch	0
	Error User	0
	Error Decode	0
	Error InvalidNethod	0

Figure 217 View detailed statistics of IEEE802.1X ports

7.12.3 Typical Configuration Example

As shown below, client is connected to port 1 of the switch. Enable IEEE802.1x on port 1 and select **Port-based** authentication mode. The username and password of the remote authentication are both ddd, the rest of the configuration are the default.

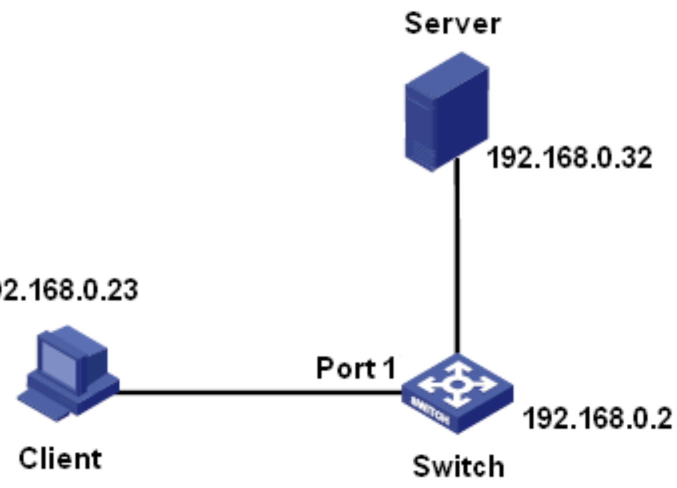


Figure 218 IEEE802.1x Configuration Example

You can refer to the typical configuration example in “5.6 RADIUS Configuration”.

7.13 GMRP

7.13.1 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.

7.13.2 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.

7.13.3 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.

7.13.4 Web Configuration

1. Enable the global GMRP protocol and configure the global timer, as shown below.

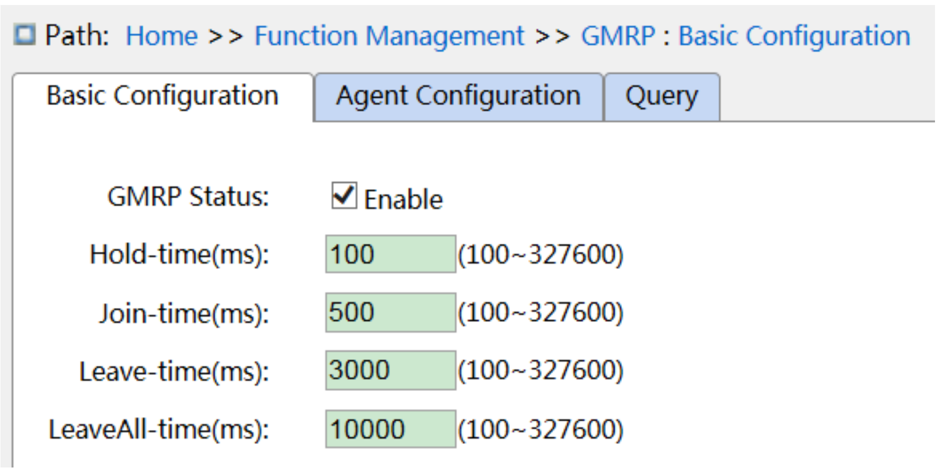


Figure 219 GMRP Global Configuration

GMRP Status

Configuration options: Enable/Disable

Default configuration: Disable

Function: Enable/Disable the global GMRP function. The function cannot be used together with the IGMP Snooping function.

Hold-timer

Configuration range: 100ms~327600ms

Default configuration: 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

Configuration range: 100ms~327600ms

Default configuration: 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

Configuration range: 100ms~327600ms

Default configuration: 3000ms

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

LeaveAll-timer

Configuration range: 100ms~327600ms

Default configuration: 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 below.

Port	GMRP Enable	GMRP Agent Enable	Last PDU Origin
1	☑	☑	00-00-00-00-00-00
2	☑	☐	00-00-00-00-00-00
3	☐	☐	--
4	☐	☐	--
5	☐	☐	--
6	☐	☐	--
7	☐	☐	--
8	☐	☐	--
9	☐	☐	--
10	☐	☐	--
11	☐	☐	--
12	☐	☐	--

Figure 220 Port GMRP Configuration

GMRP Enable

Configuration options: Enable/Disable

Default configuration: Disable

Function: Enable GMRP function on port or not

GMRP Agent Enable

Configuration options: Enable/Disable

Default configuration: Disable

Function: Enable GMRP agent function on port or not

Last PDU Origin

Function: Source MAC address of the protocol packet received last by the port.

Caution:

➢Agent port cannot propagate agent entry.

➢The premise of enabling GMRP agent function on port is to enable GMRP function on port.

3. Add a GMRP agent entry, as shown below.

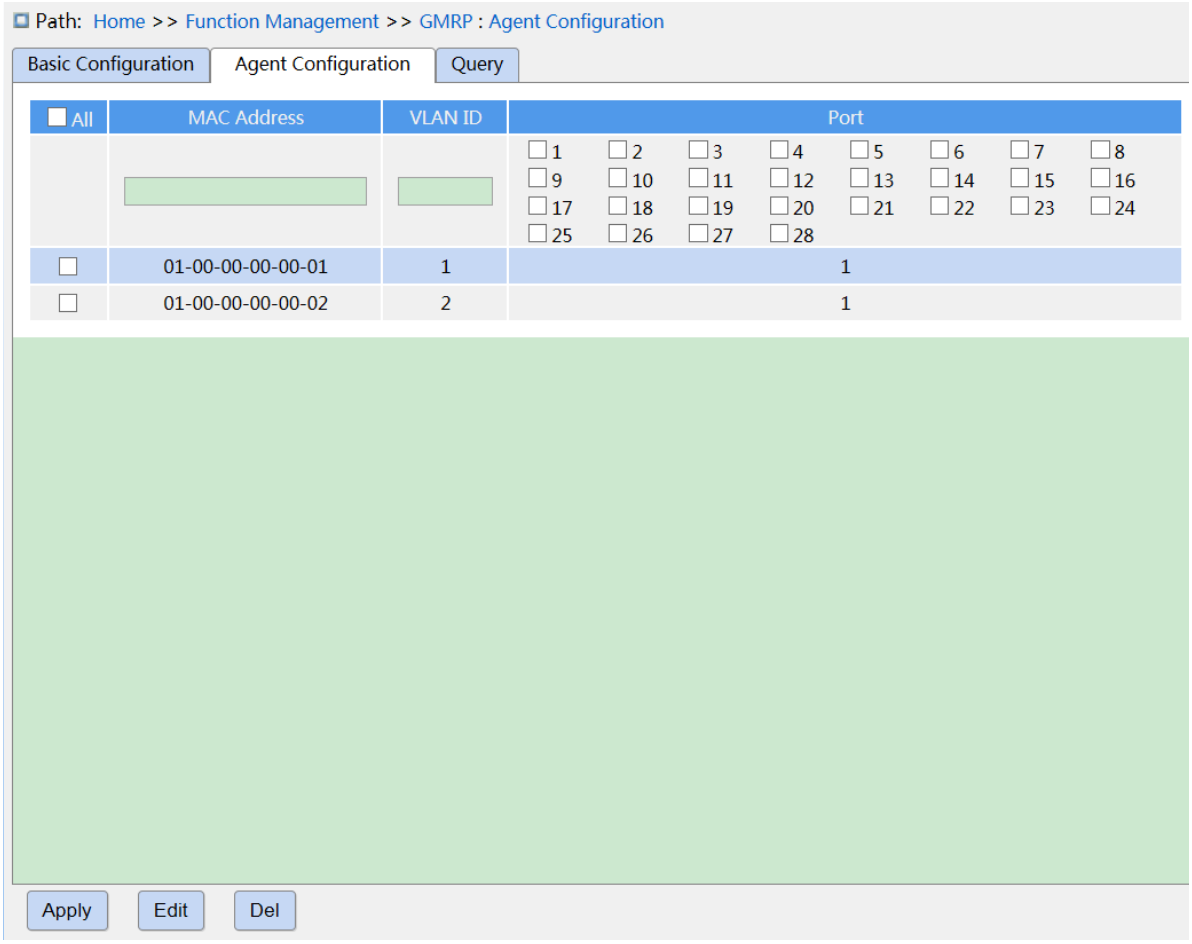


Figure 221 GMRP Agent Entry Configuration

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 ID

Configuration 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.

Port

Configuration options: all configured agent ports

4. View GMRP configuration, as shown below.

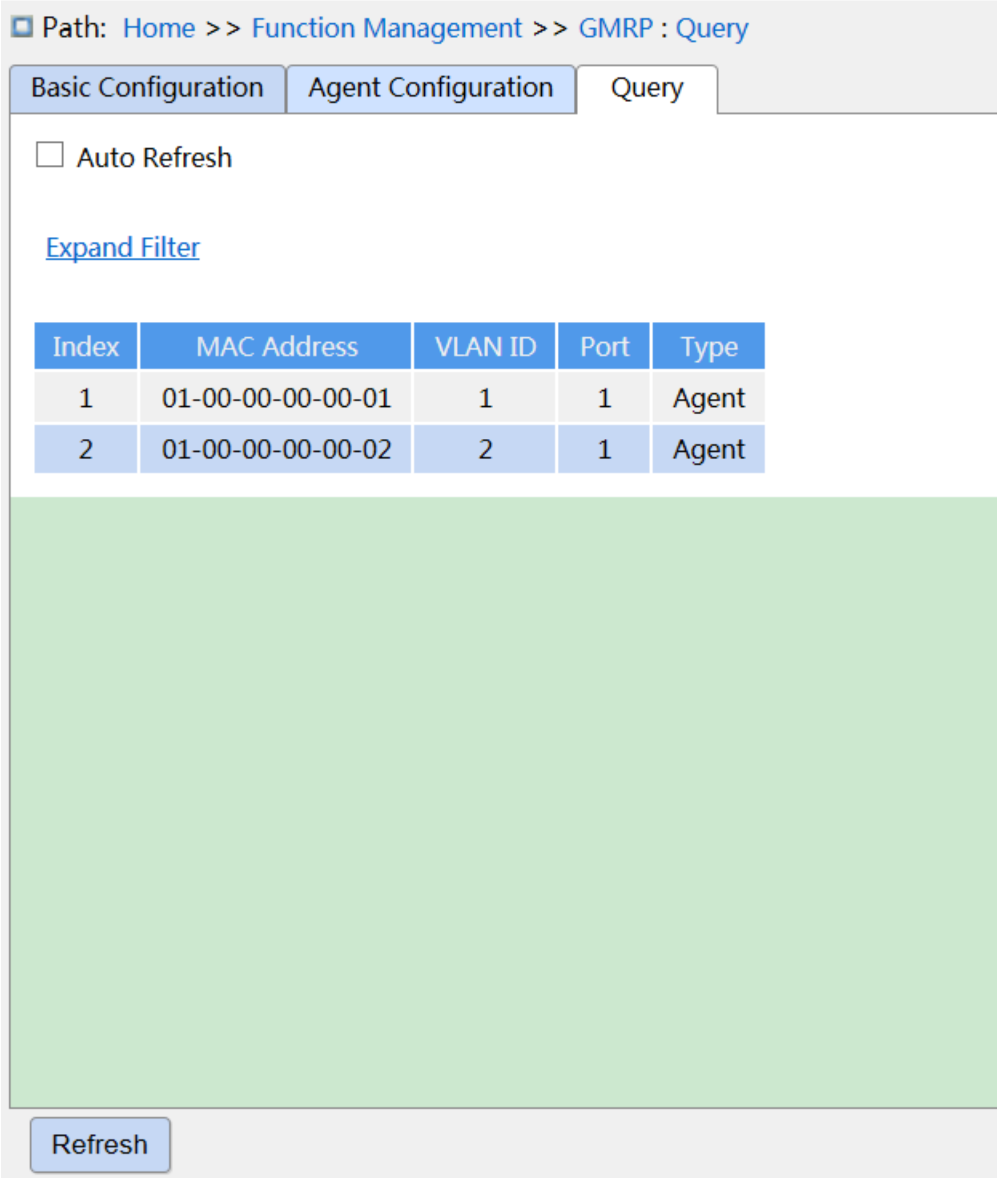


Figure 222 View GMRP configuration information

7.13.5 Typical Configuration Example

As shown below, 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.

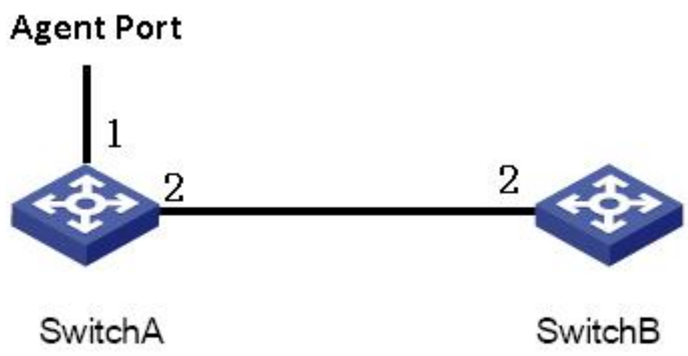


Figure 223 GMRP Networking

Configuration on Switch A:

1. Enable global GMRP function in switch A; set timer to the default value, as shown in Figure 219.

2. Enable GMRP function and agent function in port 1; enable only GMRP function in port 2; as shown in Figure 220.

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 221.

Configuration on Switch B:

4. Enable global GMRP function in switch B; set timer to the default value, as shown in Figure 219.

5. Enable GMPR function in port 2; set the timers to default values, as shown in Figure 220.

Table 10 lists the dynamically learned GMRP multicast entries in Switch B.

Table 10 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

7.14 NAT

7.14.1 Introduction

NAT(Network Address Translator) is a method for changing the source or destination address in an IP packet. It enables multiple hosts on a LAN to access external resources using a small number of legitimate addresses, or as required. Set internal WWW, FTP, TELNET services for external network use. NAT effectively hides the host IP address of the internal LAN and plays a role in security protection.

7.14.2 Principle

The basic principle of NAT is that only the internal network host needs to access the Internet to be assigned a valid public network address, while the internal network uses the internal network address.When a packet accessing the Internet passes through the NAT gateway, the NAT gateway replaces the source IP address in the original packet with a valid public network address and records the conversion. After the packet returns from the Internet side, The NAT gateway looks up the original record, replaces the destination address of the packet with the original intranet address, and sends it back to the requesting host. Thus, in the view of internal or external network devices, this process is no different from ordinary network access.

In the example shown in the following figure, host 10.1.1.1 sends an outgoing packet to the border device configured with NAT. The border device recognizes that this IP address is an internal local IP address. The target is the external network, which translates the internal local IP address and logs the conversion results to the NAT table.

This packet is sent to the external interface using the new source address after conversion. The external host returns this packet to the destination host, and the NAT router uses the NAT table to translate the internal global IP address to the internal local IP address.

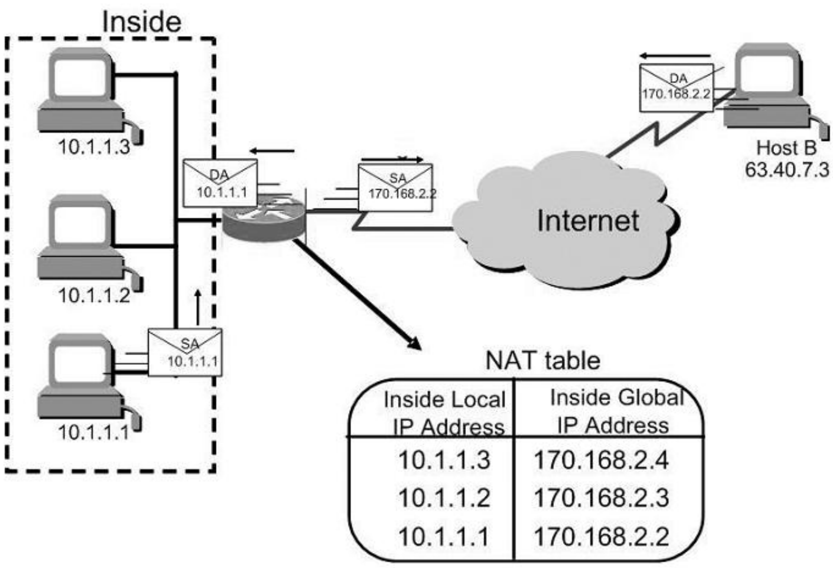


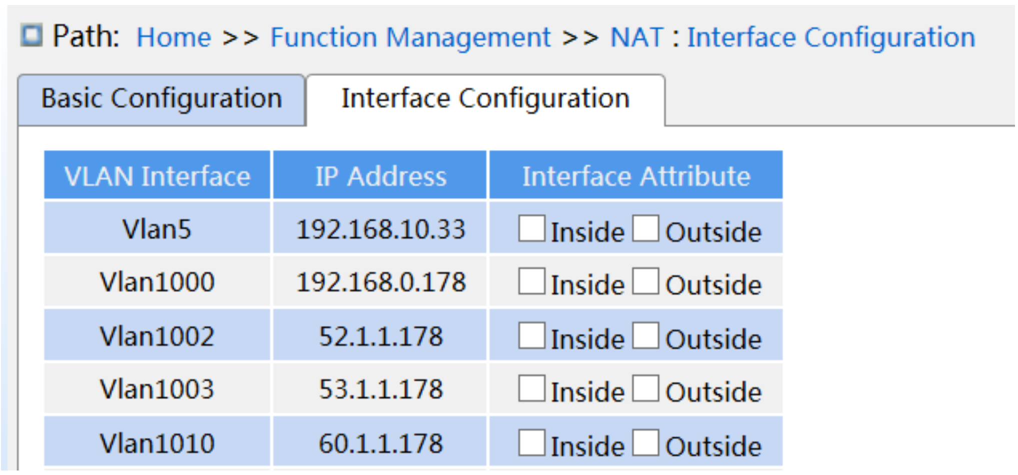
Figure 224 Basic NAT translation

Note: the NAT function supported in this series of products is layer 3 switch SICOM3024GS-L3G series.

7.14.3 Web Configuration

1. NAT interface configuration

Click the navigation tree [Function Management] → [NAT] → [Interface Configuration] menu to enter the NAT interface configuration interface, as shown below.



Path: Home >> Function Management >> NAT : Interface Configuration

Basic Configuration | Interface Configuration

VLAN Interface	IP Address	Interface Attribute
Vlan5	192.168.10.33	☐Inside ☐Outside
Vlan1000	192.168.0.178	☐Inside ☐Outside
Vlan1002	52.1.1.178	☐Inside ☐Outside
Vlan1003	53.1.1.178	☐Inside ☐Outside
Vlan1010	60.1.1.178	☐Inside ☐Outside

Figure 225 NAT interface configuration

VLAN Interface

Function: View all created Layer 3 interfaces of the device (excluding VLAN1, VLAN1 does not support NAT translation)

IP Address

Function: Displays the primary IP address of all Layer 3 interfaces on the device (excluding VLAN 1).

Interface Attribute

Configuration options: Enable/Disable

Default configuration: None

Function: Configure the interface role for Layer 3 interface NAT translation.

2. NAT basic configuration

Click the navigation tree [Function Management] → [NAT] → [Basic Configuration] menu to enter the NAT basic configuration interface, as shown below.

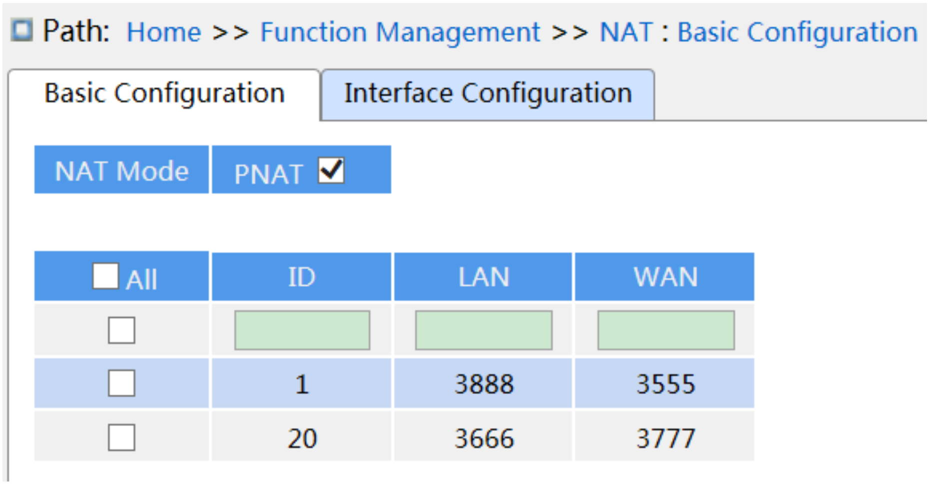


Figure 226 NAT basic configuration

NAT Mode-PNAT

Configuration options: Enable/Disable

Default configuration: None

Function: Whether to enable PNAT function.

ID

Configuration range: 1~100

Function: Configure the ID index of the PNAT rule.

LAN

Configuration range: 2~4093

Function: Configure the VLAN ID of the LAN-side interface of the PNAT rule. The value of the NAT interface must be configured as the intranet.

WAN

Configuration range: 2~4093

Function: Configure the VLAN ID of the WAN-side interface of the PNAT rule. The value of the NAT interface must be configured as the external network.

7.14.4 Typical Configuration Example

After the FTP CLIENT of the intranet is converted by DUT1 NAT, access the FTP SERVER of the external network.

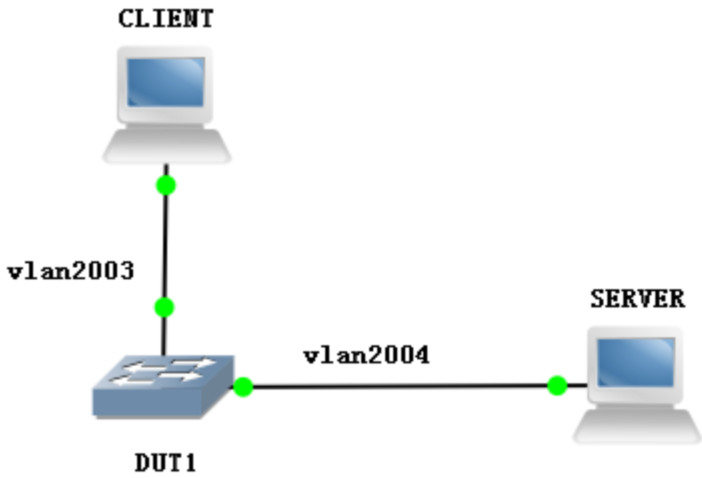


Figure 227 NAT Typical Configuration Example

1. Set the IP address of the VLAN2003 interface: 113.1.1.176, subnet mask: 255.0.0.0; configure the IP address of the VLAN2004 interface: 104.1.1.176, subnet mask: 255.0.0.0;
2. The IP address on the CLIENT side is 113.1.1.100/8, the address of the configuration gateway is 113.1.1.176, and the IP address on the SERVER side is 104.1.1.100/8.
3. The VLAN2003 and VLAN2004 interfaces on the DUT1 are respectively the internal network and the external network, as shown in Figure 225.
4. Enable NAT on DUT1 and configure PNAT rules to convert LAN-side VLAN 2003 to WAN-side VLAN 2004, as shown in Figure 226.

7.15 PIM Configuration

The Protocol Independent Multicast (PIM) conducts the Reverse Path Forwarding (RPF) check on multicast packets by using the existing unicast routing table so as to create multicast routing entries and establish a multicast forwarding tree. PIM supports two modes: PIM – Dense Mode (PIM-DM) and PIM – Sparse Mode (PIM-SM).

Note:

- Routers in this chapter refer to Layer-3 switches.
- The PIM protocol supports the Layer 3 switch SICOM3024GS-L3G series.

7.15.1 PIM-SM Configuration

7.15.1.1 PIM-SM introduction

PIM-SM uses the "pull" mode to establish a multicast forwarding tree between data receivers and a transmitter according to requirements of the data receivers.

The PIM-SM forwarding tree is established in two steps: Step 1: Establish a forwarding tree composed of both the Rendezvous Point Tree (RPT) and Shortest Point Tree (SPT), with the center of the Rendezvous Point (RP). Step 2: Switch to the SPT that is established between data receivers and a transmitter.

The PIM-SM forwarding tree is established with the center of RP. A multicast source transmits data to the RP along the SPT, and the RP forwards the multicast data to receivers along the RPT.

7.15.1.2 Basic Concepts

RP is a very important router in the PIM-SM forwarding tree. It converges the Prune/Join messages of receivers as well as multicast data of a multicast source.

RPT: establishes a forwarding tree between receivers and the RP, and is also called RPT forwarding tree.

A Bootstrap Router (BSR) mainly spreads the RP position and relevant information to routers on the network. Candidate BSRs (C-BSRs) and candidate RPs (C-PRs) are configured by network administrators and one or more C-BSRs and C-PRs can be configured. The C-BSR with a higher priority is finally elected as the authentic BSR.

7.15.1.3 PIM-SM Principle

1. Neighbor Discovery:

In the PIM domain, the router periodically sends PIM Hello messages (Hereinafter referred to as Hello packets) to all PIM routers (224.0.0.13) to discover PIM neighbors and maintain PIM neighbors between routers. Relationships to build and maintain SPT.

2. DR election:

With Hello packets, you can also elect a DR for a shared network (such as Ethernet), which will act as the sole forwarder of multicast data in the shared network. Whether it is a network connected to a multicast source or a network connected to a receiver, DR election is required. The DR on the receiver side is responsible for sending the join message to the RP. The DR on the multicast source side is responsible for sending the registration message to the RP.

The DR election process is as follows:

(1) Each router on the shared network sends Hello packets (with the parameters of the DR priority), and the router with the highest priority becomes the DR.

(2) If the priority is the same, or at least one router in the network does not support the parameter of the DR priority in the Hello packet, the DR is elected according to the IP address of each router. The router with the largest IP address becomes the DR. .

When the DR fails, the other routers still fail to receive Hello packets from the DR after the timeout, which triggers a new DR election process.

3. RP Discovery:

The RP is the core device in the PIM-SM domain. In a small network with a simple structure, the amount of multicast information is small, and the entire network only needs one RP to forward multicast information. In this case, the location of the RP can be statically specified on each router in the PIM-SM domain. In more cases, the size of the PIM-SM domain is large, and the amount of multicast information forwarded through the RP is huge. To alleviate the RP and optimize the RPT topology, you can configure multiple C-RPs (Candidate-RPs) in the PIM-SM domain to dynamically elect RPs through the bootstrap mechanism. A multicast group needs to be configured with a BSR (BootStrap Router). A

BSR is the management core of a PIM-SM domain. A PIM-SM domain can have only one BSR, but multiple C-BSRs (Candidate-BSRs) can be configured. In this way, once the BSR fails, the remaining C-BSRs can automatically generate new BSRs to ensure that services are not interrupted.

The BSR is responsible for collecting advertisement messages sent by the C-RP in the network.The message carries the address and priority of the C-RP and the range of the service group. The BSR aggregates the information into an RP-Set (RP set, that is, the mapping relationship between the multicast group and the RP). In the Bootstrap Message and published to the entire PIM-SM domain.

Each router in the network selects its corresponding RP for a specific multicast group from multiple C-RP based on the information provided by the RP-Set. The specific rules are as follows:

(1) First compare the priority of the C-RP, and the winner with the highest priority wins.

(2) If the priorities are the same, the hash value is calculated using a hash function, and the larger one wins.

(3) If the priority and hash values are the same, the one with the larger C-RP address wins.

4. Build RPT

The RPT build process is as follows:

(1) When a receiver joins a multicast group G, it first informs the directly connected DR through the IGMP message.

(2) After mastering the information of the receiver of the multicast group G, the DR sends the join message hop by hop to the RP direction corresponding to the group;

(3) The routers that pass from the DR to the RP form a branch of the RPT. These routers generate (*, G) entries in their forwarding tables, where "*" indicates that they are from any multicast source. RPT takes RP as the root and DR as the leaf.

When multicast data destined for multicast group G flows through the RP, the data arrives at the DR along the established RPT and reaches the receiver.

When a receiver is no longer interested in the information of the multicast group G, the directly connected DR sends the prune message hop by hop to the RP of the group. The upstream node receives the packet after it receives the packet. Delete the interface connected to the downstream node and check whether the receiver of the multicast group is available. If not, continue to forward the prune message to the upstream device.

5. Multicast source registration mechanism:

Because the BSR router sends the location of the RP router to the entire PIM-SM network in multicast mode, the multicast source also knows the location of the RP. When the multicast source finds that multicast data needs to be forwarded, multicast will be generated. The data is encapsulated in the registration message and sent to the RP corresponding to the group of data in unicast mode. The RP router decapsulates the anchor data from the registration message and forwards it to the receiver.

When the RP router receives the registration message sent by the multicast source, the RP router sends a Join (S, G) packet to the multicast source S. When being forwarded to the DR router of the multicast source hop by hop, all the routers passing through the path establish an (S, G) entry. At this time, an SPT forwarding tree from the RP to the multicast source S is established. The multicast source uses this SPT forwarding tree to send multicast data to the RP router.

When the RP router receives the multicast data sent by the multicast source, it sends a registration stop packet to the multicast source to tell the multicast source that the multicast data does not need to be encapsulated in the registration packet. Send it. This process is called a registration stop mechanism.

6. SPT switch

When the multicast source is far away from the RP and close to the receiver, it will be very troublesome to transit through the RP router, which increases the delay of the receiver. The SPT switching mechanism can solve this problem.

When the receiver DR router receives the multicast data, it considers that the data has been forwarded along the path from the multicast source to the DR router to the receiver; therefore, the DR router sends a Join(S, G) to the multicast source S. In the packet, all the routers in the path establish an (S, G) entry. When the join message reaches the multicast source S hop by hop, an SPT forwarding tree is established between the receiver and the multicast source DR router.

When the receiver receives the multicast data forwarded by the multicast data along the

SPT forwarding tree, it sends a prune message to the RP route, telling it that the multicast data has been forwarded by the multicast source to the receiver through the SPT forwarding tree. , no longer need RPT forwarding tree. The router that passes the prune message deletes the outbound interface corresponding to the (S, G) entry and updates the (*, G) entry.

SPT switching is not required, that is, the multicast router can choose to use SPT forwarding or RPT forwarding.

7. Assert:

If multiple multicast routers exist on a network segment, the same multicast packet may be sent to the network segment repeatedly. In order to avoid this, it is necessary to select a unique multicast data forwarder through the Assert mechanism.

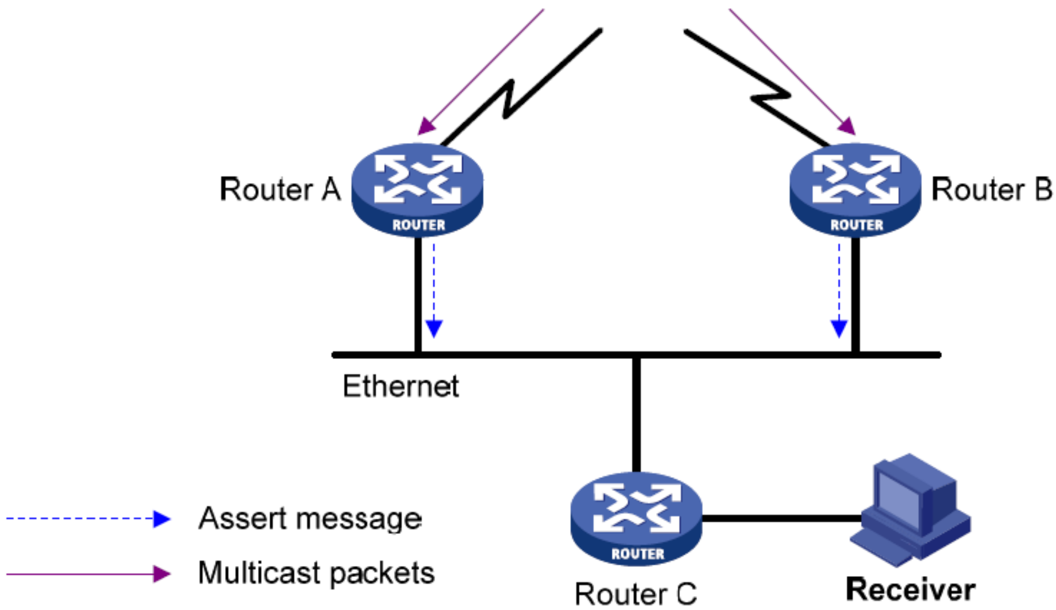


Figure 228 Assert mechanism diagram

As shown in the above figure, when Router A and Router B receive the (S, G) multicast packet from the upstream node, the packet will be forwarded to the local network segment, and the downstream node Router C will receive two copies. On the same multicast packet, Router A and Router B receive the multicast packets forwarded by the peer interface. At this time, Router A and Router B send the Assert Message to the PIM routers (224.0.0.13) in the multicast mode. The packets carry the following information: multicast source address S, group. The multicast group address G, the priority and metric of the unicast route to the multicast source. After the parameters are compared, the winners of Router A and Router B become the forwarders of the (S, G) multicast packets on the local network segment. The comparison rules are as follows:

(1) The higher priority of the unicast route to the multicast source wins;

(2) If the unicast routes to the multicast source have the same priority, the one with the smaller metric to the multicast source wins;

(3) If the metrics to the multicast source are also equal, the one with the larger local interface IP address wins.

7.15.1.4 Web Configuration

1. Basic configuration of PIM-SM, as shown below.

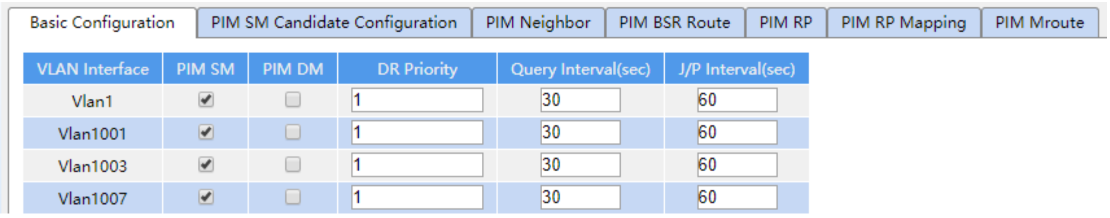


Figure 229 PIM-SM Basic Configuration

VLAN Interface

Configuration options: Created layer-3 Vlan interface

PIM-SM

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable the PIM-SM function of the Layer-3 interface.

DR Priority (0-4294967294)

Configuration range: 0-4294967294

Default configuration: 1

Function: Configure the priority of the Layer 3 VLAN interface.

Query-Interval(1-18724sec)

Configuration range: 1s-18724s

Default configuration: 30s

Function: Configure the interval for hello packets on the Layer 3 interface and discover neighboring PIM routers.

J/P Interval(1-65535sec)

Configuration range: 1s-65535s

Default configuration: 60s

Function: Configure the interval at which the Layer 3 interface sends join/prune messages.

2. PIM SM Candidate Configuration, as shown below.

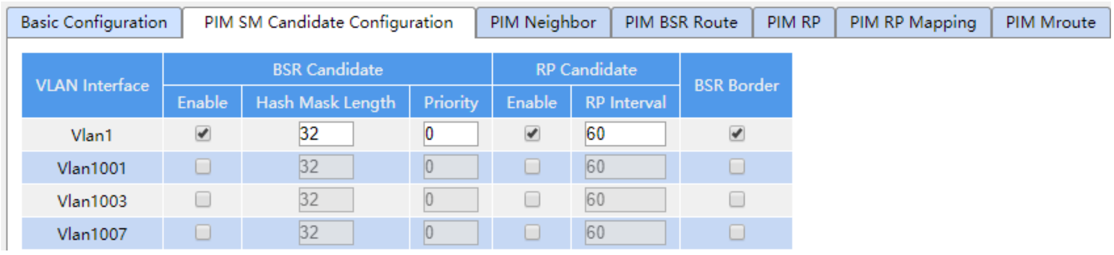


Figure 230 Configure the PIM-SM candidate interface

VLAN Interface

Configuration options: Created layer-3 Vlan interface

BSR Candidate-Enable

Configuration options: Enable/Disable

Default configuration: Disable

Function: Configure the IP address of the Layer 3 VLAN as the candidate BSR address and send BSR messages to all its PIM neighbors.

BSR Candidate-Hash Mask Length

Configuration range: 0-32

Default configuration: 32

Function: Configure the hash mask length. The hash mask length is the number of former bits in the hash mask to be used in the AND operation with the multicast address.

BSR Candidate-Priority

Configuration range: 0-255

Default configuration: 0

Function: Configure the priority of candidate BSR

RP Candidate-Enable

Configuration options: Enable/Disable

Default configuration: Disable

Function: Configure the IP address of the Layer 3 VLAN as the IP address of the candidate

RP. This address will be used as the IP address to receive registration packets, join/prune messages, and establish a forwarding tree.

RP Candidate-Interval

Configuration range: 1s-16383s

Default configuration: 60

Function: Interval for the candidate RP to send notification packets to the BSR.

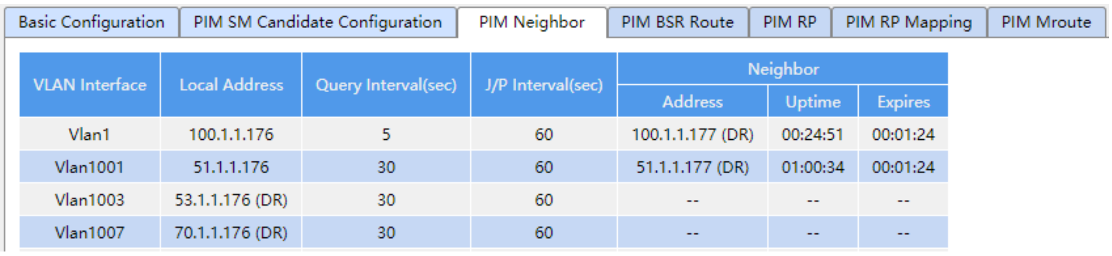
BSR Border

Configuration options: Enable/Disable

Default configuration: Disable

Function: Configure the Layer 3 VLAN interface that has been added to the PIM-SM network to configure the Layer 3 VLAN interface as the PIM-SM BSR boundary.

3. View PIM neighbor, as shown below.



VLAN Interface	Local Address	Query Interval(sec)	J/P Interval(sec)	Neighbor		
				Address	Uptime	Expires
Vlan1	100.1.1.176	5	60	100.1.1.177 (DR)	00:24:51	00:01:24
Vlan1001	51.1.1.176	30	60	51.1.1.177 (DR)	01:00:34	00:01:24
Vlan1003	53.1.1.176 (DR)	30	60	--	--	--
Vlan1007	70.1.1.176 (DR)	30	60	--	--	--

Figure 231 Display PIM neighbor interface

The fields in the display information are described in the following table.

Table 11 Description of each field of the PIM neighbor

VLAN Interface	The Layer 3 Vlan port of the switch that reaches the corresponding multicast group.
Local Address	IP address of the corresponding interface
Query Interval(sec)	Hello packet sending interval of the corresponding interface
J/P Interval(sec)	Interval at which the corresponding interface sends join/prune messages
Neighbor Address	PIM neighbor IP address of the corresponding interface
Neighbor Uptime	The PIM neighbor relationship of the corresponding interface has expired and is displayed in the format of "hour:minute:second".
Neighbor Expires	How long does the PIM neighbor of the corresponding interface expire, in the format of "hour:minute:second"

4.View PIM BSR Route information, as shown below.

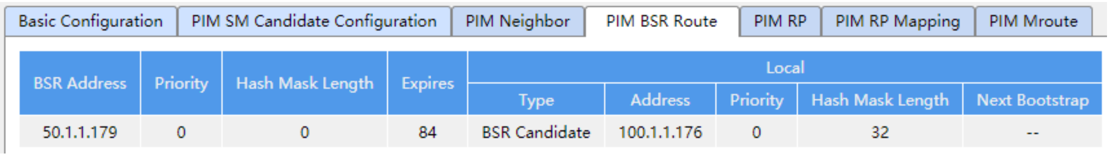


Figure 232 PIM BSR routing interface

The fields in the display information are described in the following table.

Table 12 Description of each field of the PIM BSR route

BSR Address	Current network BSR address
Priority	BSR priority
Hash Mask Length	BSR hash mask length
Expires	BSR expiration time (seconds)
Local Type	Candidate BSR type (BSR/BSR candidate) on this machine
Local Address	The candidate BSR address on this machine, if it is selected as BSR, no display.
Local Priority	The candidate BSR priority on the local device. If it is selected as the BSR, no display.
Local Hash Mask Length	The length of the candidate BSR hash mask on this machine. If it is selected as BSR, no display.
Local Next Bootstrap	The BSR on the local device sends the next Bootstrap packet interval. If it is a candidate BSR, no display.

5. View PIM RP information, as shown below.

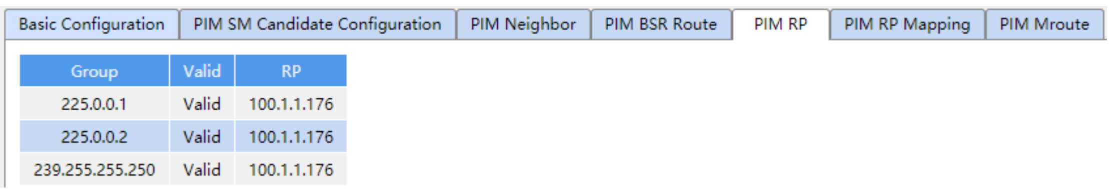


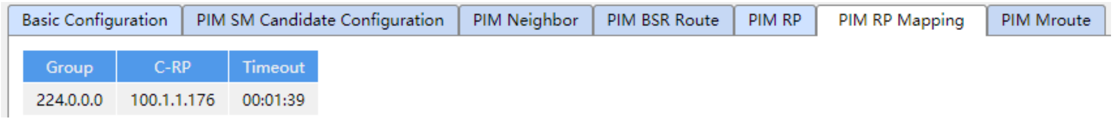
Figure 233 PIM RP information

The fields in the display information are described in the following table.

Table 13 Description of each field of the PIM RP

Group	Group address
Valid	RP is valid or not
RP	RP corresponding to the group address

6. View PIM RP mapping information, as shown below.



Group	C-RP	Timeout
224.0.0.0	100.1.1.176	00:01:39

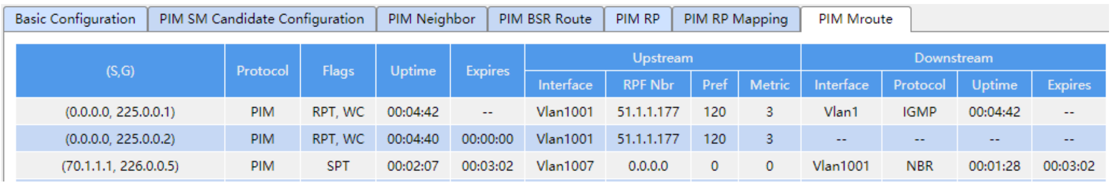
Figure 234 PIM RP mapping information

The fields in the display information are described in the following table.

Table 14 Description of each field of the PIM RP mapping

Group	Group address
C-RP	C-RP corresponding to the group address
Timeout	C-RP timeout, displayed in "hour:minute:second" format

7. View PIM Mroute information, as shown below.



(S,G)	Protocol	Flags	Uptime	Expires	Upstream				Downstream			
					Interface	RPF Nbr	Pref	Metric	Interface	Protocol	Uptime	Expires
(0.0.0.0, 225.0.0.1)	PIM	RPT, WC	00:04:42	--	Vlan1001	51.1.1.177	120	3	Vlan1	IGMP	00:04:42	--
(0.0.0.0, 225.0.0.2)	PIM	RPT, WC	00:04:40	00:00:00	Vlan1001	51.1.1.177	120	3	--	--	--	--
(70.1.1.1, 226.0.0.5)	PIM	SPT	00:02:07	00:03:02	Vlan1007	0.0.0.0	0	0	Vlan1001	NBR	00:01:28	00:03:02

Figure 235 PIM Mroute information

The fields in the display information are described in the following table.

Table 15 Description of each field of the PIM Mroute

(S,G)	(*, G) or (S, G) entries created by the receiver or multicast stream
Protocol	Currently running protocol
Flags	Flags of (S, G) or (*, G) entries in the PIM routing table
Uptime	(*, G) or (S, G) has been alive
Expires	(*, G) or (S, G) expiration time

Upstream-Interface	Incoming interface of (S, G) or (*, G) entry
	For (*, G), the Incoming interface is the interface towards the RP
	For (S, G), the Incoming interface is the interface towards S

Upstream- RPF Nbr	An RPF neighbor that indicates an (S, G) or (*, G) entry. The RPF

	neighbor for (*, G) is the interface neighbor facing the RP. The RPF neighbor for (S, G) is the interface neighbor facing S: For a (*, G) entry, when the router is an RP, the RPF neighbor of the (*, G) entry is 0.0.0.0. For the (S, G) entry, when the router is directly connected to the source, the (S, G) entry RPF neighbor is 0.0.0.0
Upstream- Pref	Management Distance of RPF Neighbor Routing for (S, G) or (*, G) Table Items
Upstream- Metric	Routing overhead of RPF neighbor routing for (S, G) or (*, G) table entries
Downstream-Interface	Outgoing Interfaces for (S, G) or (*, G) Table Items
Downstream-Protocol	Types of protocols used by downstream interfaces
Downstream-Uptime	The existence time of the downstream interface
Downstream- Expires	Timeout of downstream interface

7.15.1.5 Typical Configuration Example

As shown below, Router1, Router2, Router3 , Router4 can support PIM-SM protocol, S means source and R means receivers.

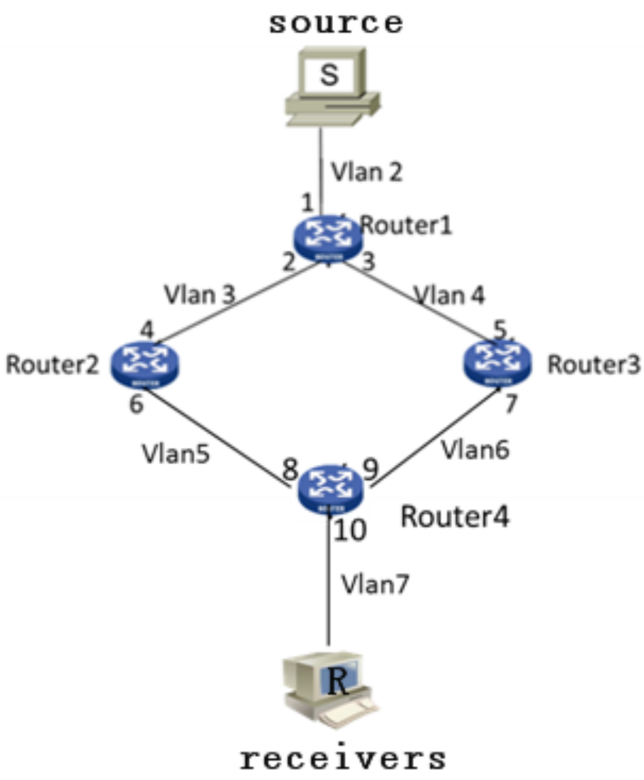


Figure 236 PIM SM Example

1. Configure router IDs and enable the Open Shortest Path First (OSPF) protocol. For the detailed configuration process, see "7.17.3 OSPF Configuration".

2. Router1 Configuration:

➢Create VLAN 2, VLAN 3, and VLAN 4, and add Port 1 to VLAN 2, Port 2 to VLAN 3, and Port 3 to VLAN 4. For the detailed configuration process, see "7.2 VLAN Configuration".

➢Configure Layer-3 interfaces, Set the IP address of the Layer-3 interface of Port 1 to 20.0.0.2, the IP address of the Layer-3 interface of Port 2 to 30.0.0.2, and the IP address of the Layer-3 interface of Port 3 to 40.0.0.4. For the detailed configuration process, see "7.3 L3 Interface Configuration".

➢Enable PIM-SM, as shown in Figure 308. Enable PIM-SM on each created Layer-3 VLAN interface and configure the packet query interval, as shown in Figure 230.

3. Router2 Configuration:

➢Create VLAN 3, VLAN 5, and add Port 4 to VLAN 3, Port 6 to VLAN 5.

➢Configure Layer-3 interfaces, Set the IP address of the Layer-3 interface of Port 4 to

30.0.0.4, the IP address of the Layer-3 interface of Port 6 to 50.0.0.4.

➢Enable PIM-SM, as shown in Figure 308, Enable PIM-SM on each created Layer-3 VLAN interface and configure the packet query interval, as shown in Figure 230.

4. Router3 Configuration:

➢Create VLAN 4, VLAN 6, and add Port 5 to VLAN 4, Port 7 to VLAN 6;

➢Configure Layer-3 interfaces, Set the IP address of the Layer-3 interface of Port 5 to 30.0.0.4, the IP address of the Layer-3 interface of Port 7 to 60.0.0.4.

➢Enable PIM-SM, as shown in Figure 308, Enable PIM-SM on each created Layer-3 VLAN interface and configure the packet query interval, as shown in Figure 230.

5. Router4 Configuration:

➢Create VLAN 5, VLAN 6, and VLAN 7, and add Port 8 to VLAN 5, Port 9 to VLAN 6, and Port 10 to VLAN 7.

➢Configure Layer-3 interfaces, Set the IP address of the Layer-3 interface of Port 8 50.0.0.8，the IP address of the Layer-3 interface of Port 9 to 60.0.0.9，the IP address of the Layer-3 interface of Port 10 to 70.0.0.10；

➢Enable PIM-SM, as shown in Figure 308, Enable PIM-SM on each created Layer-3 VLAN interface and configure the packet query interval, as shown in Figure 230.

6. Configure the BSR border (optional): as shown in Figure 231, set the Layer-3 interface as PIM-SM BSR border.

7. Configure the C-BSR: as shown in Figure 231, set the Port 2 of Router1 as C-BSR, and the default value of the priority is 0, and the default value of hash mask length is 0.

8. Configure the C-RP: as shown in Figure 231, set the Port 4 of Router4 and Port 5 of Router3 as C-RP, the default value of query interval is 60 seconds.

9. View the configuration, refer to the web operation in this chapter.

Note:

➢Router 1, Router 2, and Router 3 can be configured as C-BSRs, the authentic BSR can be determined by means of election, or a specific router can be specified as the BSR.

➢After an interface is configured as the BSR border, the interface will block the receiving or transmission of BSR messages. You need to configure the BSR border only on the interface that should block BSR messages. The BSR border does not need to be configured for all routers.

7.15.2 PIM-DM Configuration

7.15.2.1 Introduction to PIM-DM

PIM-DM (PIM Dense Mode) uses the Push mode to transmit multicast data, and is usually applied to small networks with relatively dense multicast group members.

The basic principles of PIM-DM are as follows:

PIM-DM assumes that at least one multicast group member exists in each subnet in the network, so the multicast data will be flooded to all nodes in the network. Then, PIM-DM prunes the branch without multicast data forwarding, leaving only the branch containing the receiver. This "Flooding-pruning" phenomenon occurs periodically, and the pruned branches can also be periodically restored to forwarding state.

When the member of the multicast group appears on the node to be prune, PIM-DM uses the Graft mechanism to actively resume the forwarding of multicast data in order to reduce the time required for the node to return to the forwarding state.

Generally, the forwarding path of a data packet in a dense mode is a Source Tree (a forwarding tree taking the multicast source as the "root" and a multicast group member as "leaf"). Since the Source Tree uses the shortest path from the multicast source to the receiver, it is also called the Shortest Path Tree (SPT).

7.15.2.2 Working principle of PIM-DM

1.Neighbor Discovery:

PIM-DM uses a neighbor discovery mechanism similar to PIM-SM, see section 1.2.4 for details.

2.Build SPT:

The process of building SPT is also the process of "Flooding-pruning":

(1) In the PIM-DM domain, when the multicast source S sends multicast message to the multicast group G, it first floods the multicast message: After the router passes the RPF check on the message, the router creates one (S, G) entry, and forwards the message to all downstream nodes in the network. After the flooding, the (S, G) entry will be created on each router in the PIM-DM domain.

(2) Then prune the downstream nodes that have no receivers: the downstream node without the receiver sends a Prune Message to the upstream node to notify the upstream node to delete the corresponding interface from the corresponding outcoming interface list of its multicast forwarding entry (S, G), and the message of such multicast group will not be forwarded to the node any more.

The pruning process is initiated by the leaf router first, as shown in Figure 2, the router (such as the router directly connected to Host A) without Receiverinitiates pruning and continues pruning until only necessary branches left in the PIM-DM domain, these necessary branches together form the SPT.

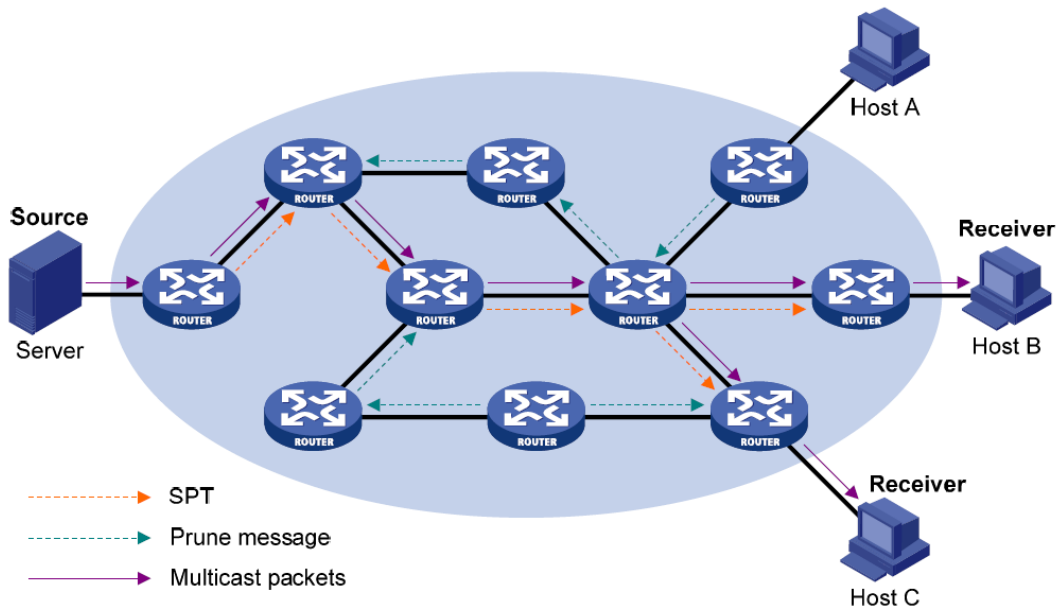


Figure 237 Schematic diagram for building SPT in PIM-DM

The process of "Flooding-pruning" occurs periodically. Each pruned node provides a timeout mechanism, the process will be restarted when the pruning times out.

3. Grafting:

When the member of the multicast group appears on the node being pruned, in order to reduce the time required for the node to recoverto the forwarding state, the PIM-DM uses the grafting mechanism to actively recover the forwarding of the multicast data. The process is as follows:

(1) The node that needs to recover receiving the multicast data sends a Graft Message to its upstream node to apply for rejoining into the SPT.

(2) When the upstream node receives the message, it recovers the forwarding state of the downstream node, and responds to it with a Graft-Ack Message for confirmation;

(3) If the downstream node sending the Graft Message does not receive the Graft-Ack Message from its upstream node, it will resend the Graft Message until it is confirmed.

4. Assertion:

PIM-DM uses an assertion mechanism similar to PIM-SM, see section 1.2.4 for details.

7.15.2.3 Web Configuration

1. Basic configuration of PIM-DM, as shown below.

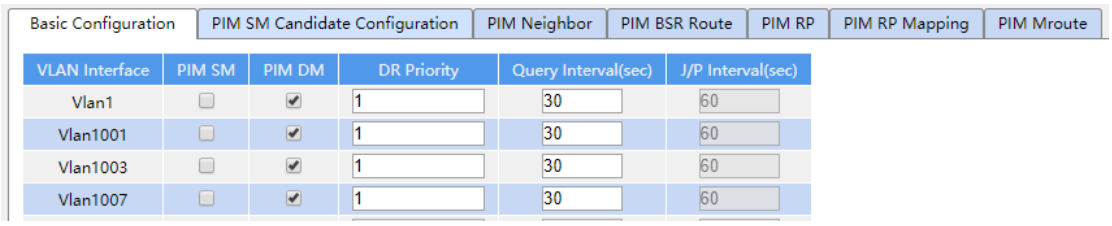


Figure 238 Basic configuration of PIM-DM

VLAN Interface

Configuration options: Created layer-3 Vlan interface

PIM-DM

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable the PIM-DM function of the Layer-3 interface.

DR Priority (0-4294967294)

Configuration range: 0-4294967294

Default configuration: 1

Function: Configure the priority of the Layer 3 VLAN interface.

Query-Interval(1-18724sec)

Configuration range: 1s-18724s

Default configuration: 30s

Function: Configure the interval for hello packets on the Layer 3 interface and discover neighboring PIM routers.

2. View PIM neighbor information

As with PIM-SM, see section 7.14.1.4.

3. View PIM Mroute information

As with PIM-SM, see section 7.14.1.4.

7.15.2.4 Typical Configuration Example

As shown below,Router1,Router2,Router3 ,Router4 can support PIM-SM protocol, S means source and R means receivers.

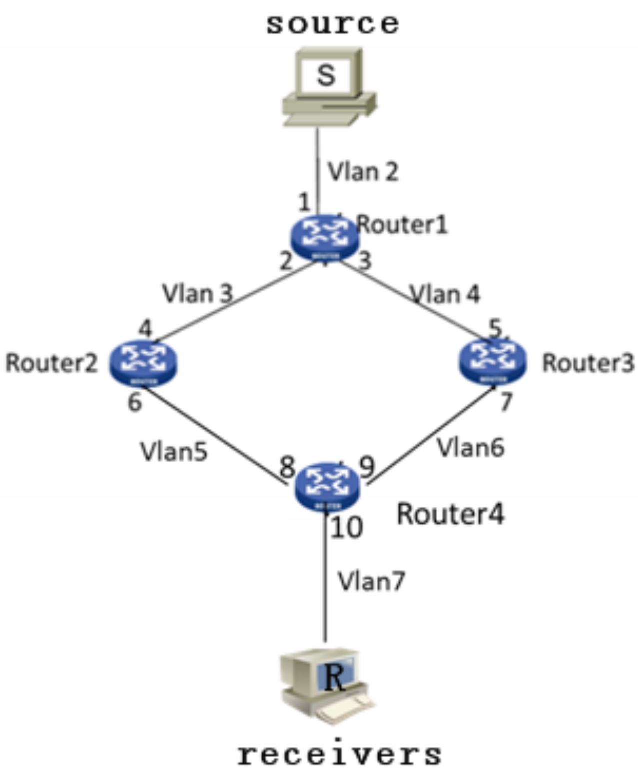


Figure 239 PIM DM Example

1. Configure router IDs and enable the Open Shortest Path First (OSPF) protocol. For the detailed configuration process, see "7.17.3 OSPF Configuration".

2. Router1 Configuration:

➢Create VLAN 2, VLAN 3, and VLAN 4, and add Port 1 to VLAN 2, Port 2 to VLAN 3, and Port 3 to VLAN 4. For the detailed configuration process, see "7.2 VLAN Configuration".

➢Configure Layer-3 interfaces, Set the IP address of the Layer-3 interface of Port 1 to 20.0.0.2, the IP address of the Layer-3 interface of Port 2 to 30.0.0.2, and the IP address of the Layer-3 interface of Port 3 to 40.0.0.4. For the detailed configuration process, see "7.3 L3 Interface Configuration".

➢Enable PIM-DM, as shown in Figure 308. Enable PIM-DM on each created Layer-3 VLAN interface and configure the packet query interval, as shown in Figure 238.

3. Router2 Configuration:

➢Create VLAN 3, VLAN 5, and add Port 4 to VLAN 3, Port 6 to VLAN 5.

➢Configure Layer-3 interfaces, Set the IP address of the Layer-3 interface of Port 4 to 30.0.0.4, the IP address of the Layer-3 interface of Port 6 to 50.0.0.4.

➢Enable PIM-DM, as shown in Figure 308, Enable PIM-DM on each created Layer-3 VLAN interface and configure the packet query interval, as shown in Figure 238.

4. Router3 Configuration:

➢Create VLAN 4, VLAN 6, and add Port 5 to VLAN 4, Port 7 to VLAN 6;

➢Configure Layer-3 interfaces, Set the IP address of the Layer-3 interface of Port 5 to 30.0.0.4, the IP address of the Layer-3 interface of Port 7 to 60.0.0.4.

➢Enable PIM-DM, as shown in Figure 308, Enable PIM-DM on each created Layer-3 VLAN interface and configure the packet query interval, as shown in Figure 238.

5. Router4 Configuration:

➢Create VLAN 5, VLAN 6, and VLAN 7, and add Port 8 to VLAN 5, Port 9 to VLAN 6, and Port 10 to VLAN 7.

➢Configure Layer-3 interfaces, Set the IP address of the Layer-3 interface of Port 8 50.0.0.8，the IP address of the Layer-3 interface of Port 9 to 60.0.0.9，the IP address of the Layer-3 interface of Port 10 to 70.0.0.10；

➢Enable PIM-DM, as shown in Figure 308, Enable PIM-DM on each created Layer-3 VLAN interface and configure the packet query interval, as shown in Figure 238.

6. View the PIM neighbor and PIM routing forwarding table. For details, see section 1.25 for information.

7.16 IGMP Configuration

7.16.1 Introduction

The Internet Group Management Protocol (IGMP) is a protocol for managing the multicast group membership. It works at the tail end of a network and establishes and maintains the multicast group membership between an IP host and adjacent multicast routers.

There are three versions of IGMP: IGMPv1, IGMPv2, and IGMPv3. This device does not support IGMPv3.

The major differences between IGMPv1 and IGMPv2 are as follows:

(1)IGMPv2 uses a formal querier election mechanism, which elects the router with a lower IP address as the querier. IGMPv1 does not have the querier election mechanism. Different routing protocols use different election mechanisms.

(2) IGMPv2 adds a Leave Group message. When a host leaves a group, the host actively sends the Leave Group packet. IGMPv1 does not actively send the Leave Group packet.

(3) Max Resp Time: a new field added to the Query packets. It indicates the allowable maximum response time set by a querier. The default value is 10 seconds.

(4) Group-Specific Query message: A querier is allowed to perform the query operation on a specified group rather than on all groups by sending the Group-Specific Query message.

Note:

Routers in this chapter refer to Layer-3 switches.

7.16.2 Work Principle

The following uses IGMPv2 as an example to describe the implementation mechanism of IGMP.

(1) Querier election mechanism: All IGMPv2 routers deem that they are queriers initially and send the Query packet. When a router receives the Query packet from a router whose IP address is lower than its IP address, it abandons the querier role and becomes a non-querier. A router with the lowest IP address is elected as the querier finally.

General Query packet: A querier periodically sends the General Query packet to check whether there are member ports in the multicast group. The destination IP address of the packet is always 224.0.0.1.

Membership Report packet: When a host in a group receives a Query packet, it returns the member response packet. When a host is willing to join a group, it actively sends the IGMP Report packet to the querier so as to join the multicast group that the host is interested in.

(2) Member suppression mechanism: When a host receives a Query packet, it starts the response latency timer, with the value ranging from 0 to D (maximum value). When the timer of a host times out prior to other timers of hosts in the same network segment, the host sends the Membership Report packet. When receiving the Membership Report packet, other hosts stop their timers and do not generate the Membership Report packet. This process is called member suppression mechanism.

(3) Leave mechanism: When a host intends to leave a multicast group, it sends the Leave Group packet, with the destination IP address of 224.0.0.2.

Group-Specific Query packet: A host sends the Leave Group packet when leaving a multicast group. After receiving the Leave Group packet from the host, the querier sends the Group-Specific Query packet to check whether the host is last member of the multicast group. If the querier receives Report packets from other members in the group, the querier continues to maintain the multicast group. Otherwise, the querier stops forwarding data to the multicast group.

Querier

Query interval: 125s, indicating the interval for sending the General Query packet.

Last Listener Query Interval: Max Resp Time in the Group-Specific Query packet, that is, transmission interval. The default value is 1s.

Query Response Interval: Max Resp Time in the General Query packet. The default value is 10s. A host that receives the General Query packet must give a response within this interval. The value must be smaller than the query interval.

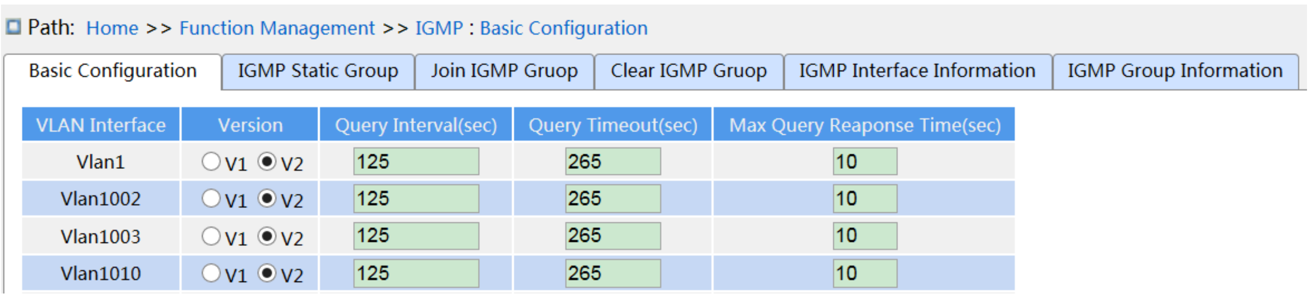
7.16.3 Web Configuration

1. Enable the IGMP protocol

IGMP is started along with the startup of the Protocol Independent Multicast (PIM). It cannot be started separately.

Default configuration: Disable

2. Configure Basic IGMP parameters, as shown below.



VLAN Interface	Version	Query Interval(sec)	Query Timeout(sec)	Max Query Reaponse Time(sec)
Vlan1	○V1 ◉V2	125	265	10
Vlan1002	○V1 ◉V2	125	265	10
Vlan1003	○V1 ◉V2	125	265	10
Vlan1010	○V1 ◉V2	125	265	10

Figure 240 Basic configuration of IGMP

VLAN Interface

Configuration options: Created layer-3 Vlan interface

Version

Configuration options: v1/v2

Default configuration: v2

Function: Configure the interface to run version 1 or version 2.

Query Interval (1-65535s)

Configuration range: 1s-65535s

Default configuration:125s

Function: Configure the query interval for the IGMP querier to periodically send query messages.

Query Timeout (60-300s)

Configuration range:60s-300s

Default configuration:265s

Function: Configure the timeout time of IGMP query packets for an interface.

Description: If a non-querier fails to receive the Query packet from the querier within an interval, the interface on the non-querier automatically becomes the querier. This interval is called timeout time. In general, the timeout time is twice of the query interval plus the maximum response time.

Max Query Reaponse Time(1-25s)

Configuration range:1s-25s

Default configuration:10s

Function: Configure the maximum time of interface response to IGMP query packets.

Description: When hosts are willing to join a multicast group, the host that first responds to a Query Packet from a querier and is willing to join the multicast group must send the Membership Report packet to the querier within the maximum response time. This maximum response time is the maximum query time. If the host fails to send the Membership Report packet within the maximum query time, the querier deems that the branch where the host resides has no member and this branch will be pruned.

3. Configure an IGMP Static Group, as shown below.

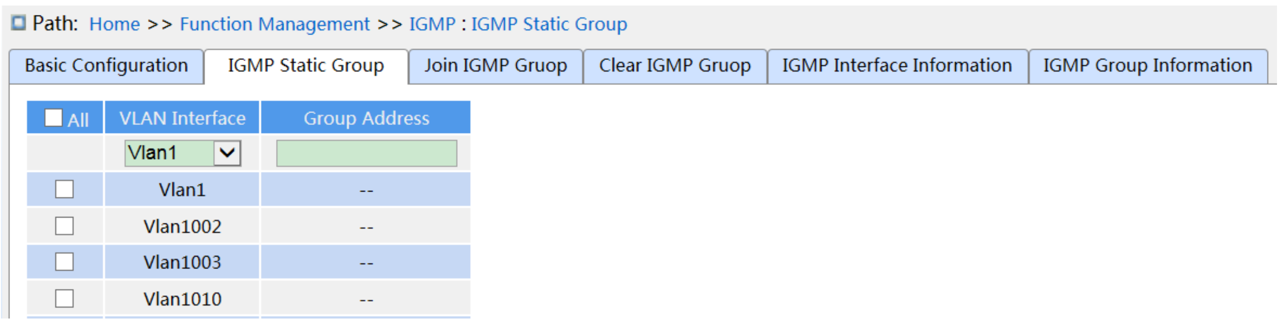


Figure 241 Configure an IGMP Static Group

Vlan ID

Configuration options: Created Layer-3 VLAN interface

Default configuration: Vlan 1

Function: Select the Layer-3 interface to be configurated.

Group Address

Format: A.B.C.D

Function: Specify the IP address of the multicast group to which a Layer-3 interface of the switch needs to be statically added.

4. Configure an IGMP join group, as shown below.

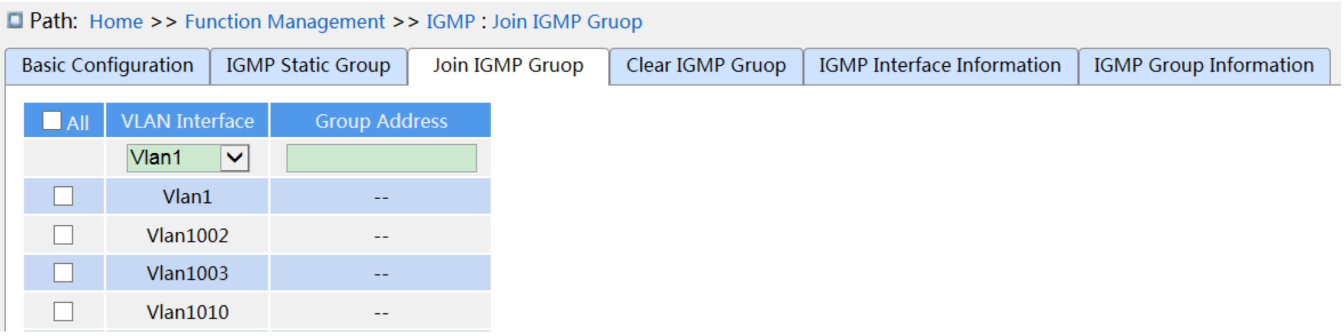


Figure 242 join IGMP Group configuration

Vlan Interface

Configuration options: Created Layer-3 VLAN interface

Default configuration: Vlan 1

Function: Select the Layer-3 interface to be configurated.

Group Address

Format: A.B.C.D

Function: Specify the IP address of the multicast group to which the switch is to be added, and add a Layer-3 interface of the switch to a multicast group with a specified multicast address. By default, no multicast member is defined for a multicast group.

5. Clear the IGMP group, as shown below.

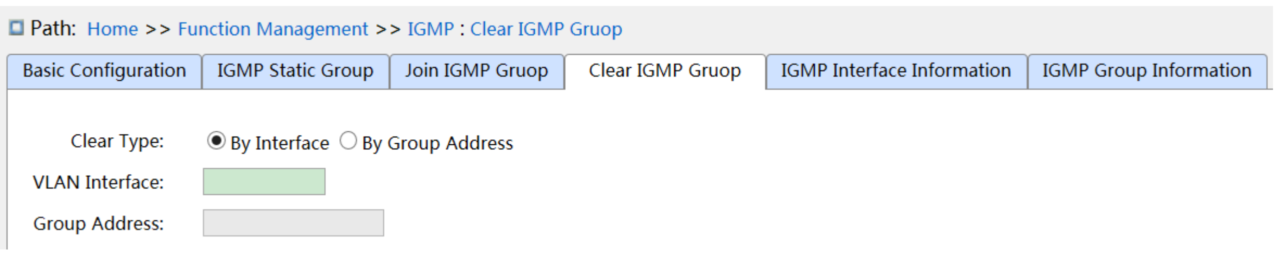


Figure 243 Clear the IGMP group

Clear Type

Configuration options: By Interface/ By Group address

Default configuration: By Interface

Function: Configure the method for clearing IGMP dynamic group information.

Vlan Interface

Configuration options: Created Layer-3 VLAN interface

Default configuration: None

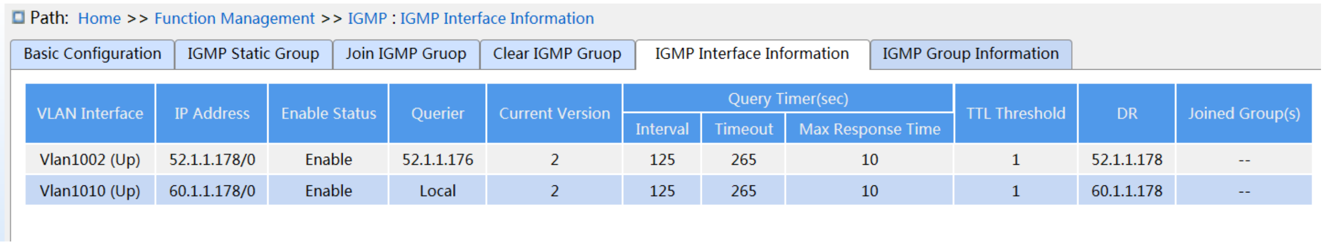
Function: Configure a VLAN interface to clear IGMP dynamic group information.

Group Address

Format: A.B.C.D

Function: Specify the IGMP group address to be cleared.

6. The IGMP Interface Information is displayed, as shown below.



VLAN Interface	IP Address	Enable Status	Querier	Current Version	Query Timer(sec)			TTL Threshold	DR	Joined Group(s)
					Interval	Timeout	Max Response Time			
Vlan1002 (Up)	52.1.1.178/0	Enable	52.1.1.176	2	125	265	10	1	52.1.1.178	--
Vlan1010 (Up)	60.1.1.178/0	Enable	Local	2	125	265	10	1	60.1.1.178	--

Figure 244 the Information of IGMP Interface information

The fields in the display information are described in the following table.

Table 16 Description of each field of the IGMP Interface Information

VLAN Interface	Layer 3 VLAN interface with IGMP enabled and the status is UP
IP Address	IP address of the corresponding Vlan interface
Enable Status	IGMP enabled status of the corresponding VLAN interface
Querier	The querier corresponding to the Vlan interface is displayed as "A.B.C.D", and "this machine" indicates itself as the querier.
Current Version	IGMP version of the corresponding Vlan interface
Query Timer(s)-Interval	IGMP query interval corresponding to the VLAN interface
Query Timer(s)-Timeout	Timeout time of IGMP query messages corresponding to the VLAN interface
Query Timer(s)-Max Response Time	Maximum response time of IGMP query messages corresponding to the VLAN interface
TTL Threshold	The TTL threshold of the IGMP messages corresponding to the VLAN interface. The IGMP messages that exceed the threshold are not processed.

DR	The DR address corresponding to the Vlan interface
Joined Group(s)	Group address added to the corresponding VLAN interface

7. IGMP group information, as shown below.

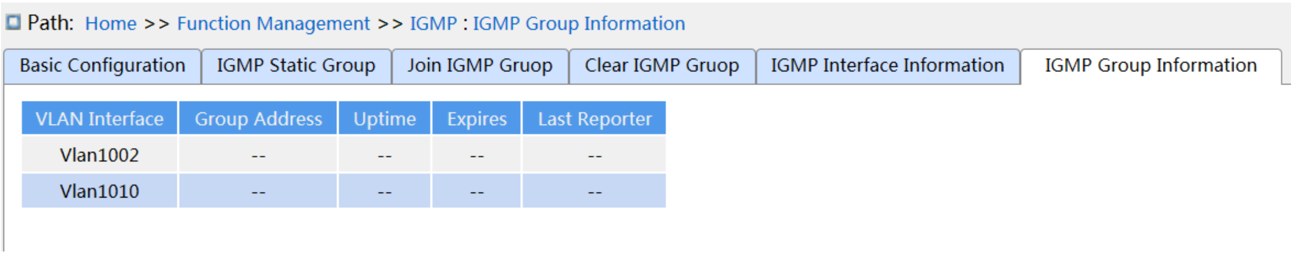


Figure 245 IGMP group information

The fields in the display information are described in the following table.

Table 17 Description of each field of the IGMP group information

VLAN Interface	The layer-3 Vlan port of the switch that reaches the corresponding multicast group
Group Address	IP address of the multicast group
Uptime	The time when the corresponding multicast group has survived is displayed in the format of "hour:minute:second".
Expires	The multicast group expiration time is displayed in the format of "hour:minute:second". "stopped" indicates that the multicast group timer never times out.
Last Reporter	Finally join the host IP address of the multicast group.

7.17 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.
Note: In the series switches, SICOM3024GS-L3G Series support routing protocols.

7.17.1 Routing Table

7.17.1.1 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.

7.17.1.2 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.

7.17.1.3 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.

7.17.1.4 Web Configuration

1. Static routing configuration, as shown below.

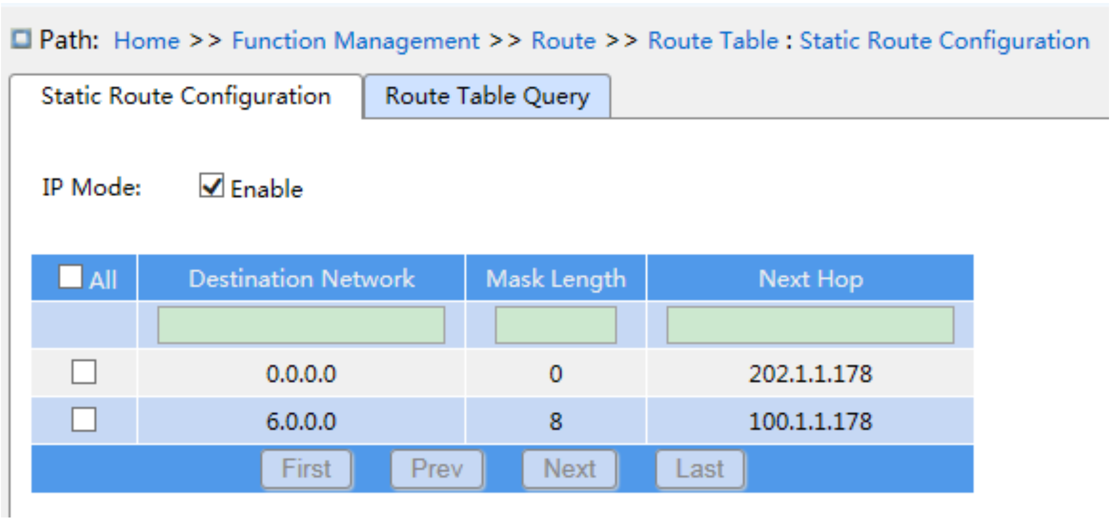


Figure 246 Static routing configuration

IP Mode

Configuration options: Enable/disable

Default configuration: For Layer 3 devices, the default is enabled. For Layer 2 devices, the default is not enabled.

Function: Enable or disable IP mode.

Destination Network

Configuration format: A.B.C.D

Function: configure the target network address in the static route table.

Mask Length

Function: a subnet mask is a 32-bit number, consisting of a sequence "1" and a sequence "0". "1" corresponds to the network number field and the subnet number field, while "0" corresponds to the host number field. The mask length is the number of 1 in the mask.

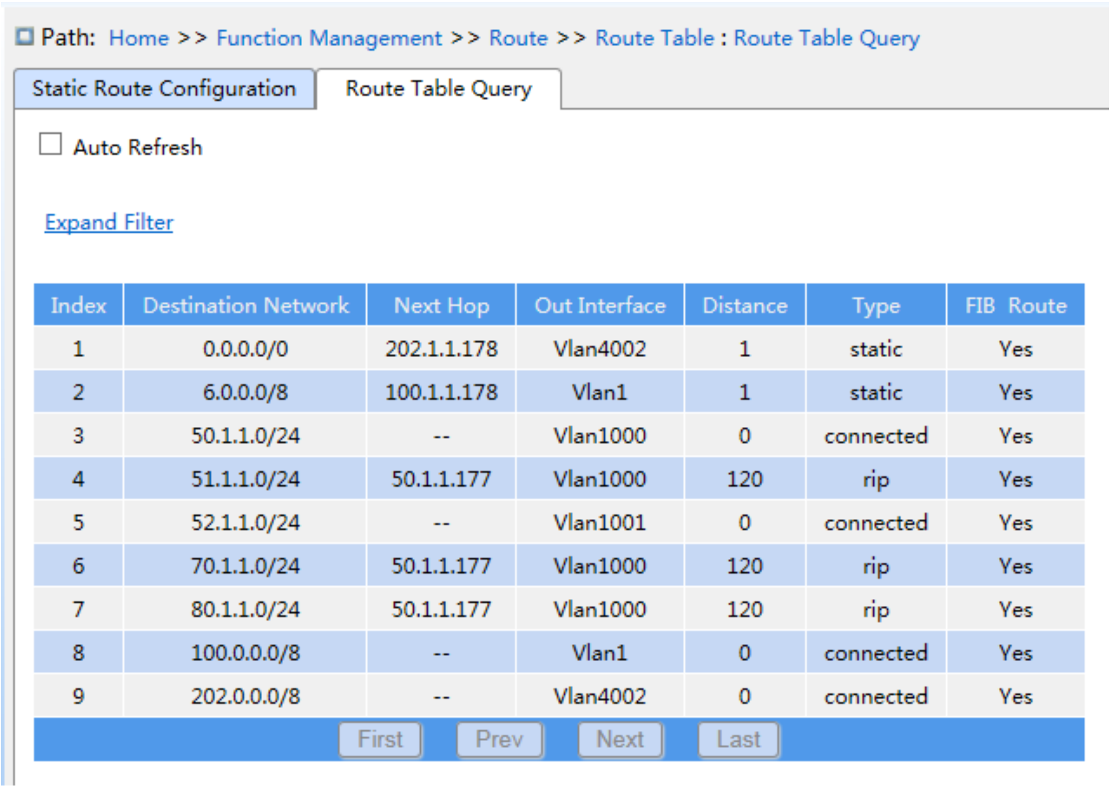
Next Hop

Configuration format: A.B.C.D

Function: Configure the next hop IP address.

2.Route Table Query

View device routing table information, including static and dynamic routes, as shown below.



Index	Destination Network	Next Hop	Out Interface	Distance	Type	FIB Route
1	0.0.0.0/0	202.1.1.178	Vlan4002	1	static	Yes
2	6.0.0.0/8	100.1.1.178	Vlan1	1	static	Yes
3	50.1.1.0/24	--	Vlan1000	0	connected	Yes
4	51.1.1.0/24	50.1.1.177	Vlan1000	120	rip	Yes
5	52.1.1.0/24	--	Vlan1001	0	connected	Yes
6	70.1.1.0/24	50.1.1.177	Vlan1000	120	rip	Yes
7	80.1.1.0/24	50.1.1.177	Vlan1000	120	rip	Yes
8	100.0.0.0/8	--	Vlan1	0	connected	Yes
9	202.0.0.0/8	--	Vlan4002	0	connected	Yes

Figure 247 Route Table Query

7.17.1.5 Typical Configuration Example

As shown below, 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.

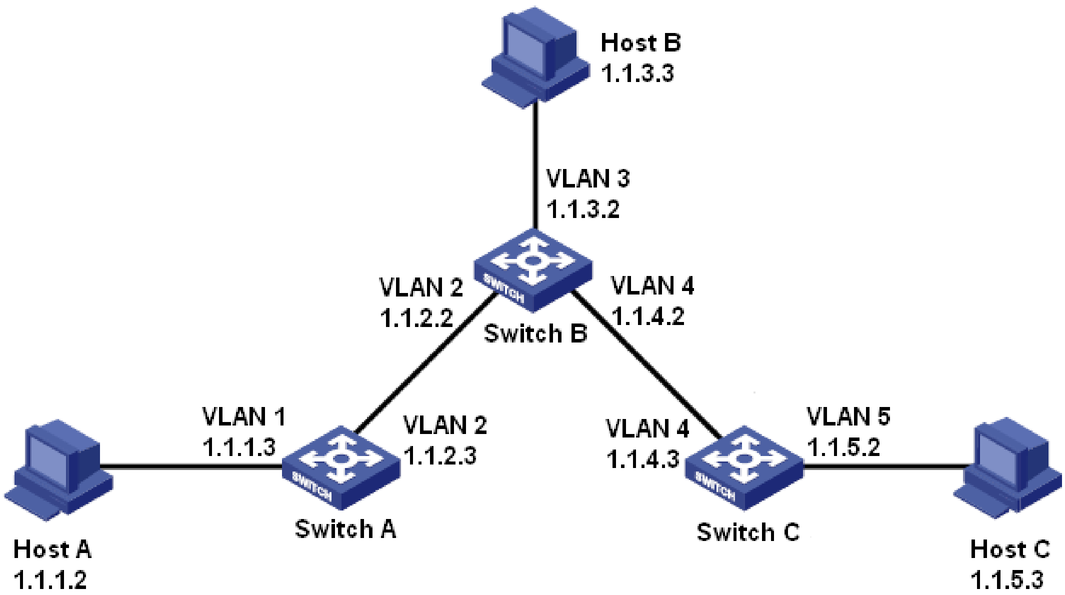


Figure 248 Example for Configuring Static Routes

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 246.

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 246.

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 246.

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 246.

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 246.

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.

7.17.2 RIP Configuration

7.17.2.1 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.

7.17.2.2 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.

7.17.2.3 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.

7.17.2.4 Web Configuration

1. Basic configuration, as shown below.

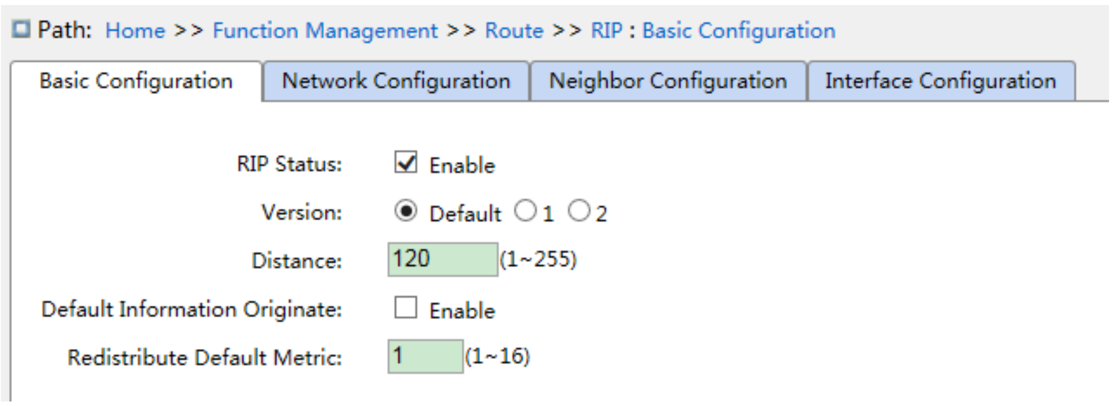


Figure 249 Basic configuration

RIP Status

Configuration options: Enable/disable

Default configuration: Disable

Function: Enable or disable RIP.

Vesion

Configuration options: Default/1/2

Default configuration: Default

Function: Select the version of the RIP protocol. By default, RIP-2 is sent and RIP-1 and RIP-2 are received. Configuration 1 indicates that all interfaces of the Layer 3 switch send/receive RIP-1 packets. Configuration 2 indicates that all interfaces of the Layer 3 switch send/receive RIP-2 packets.

Distance

Configuration range: 1-255

Default configuration: 120

Function: Specifies the route preference of the RIP protocol. The smaller the value, the higher the priority. The priority level will determine which routing algorithm gets the best route for the route in the core routing table.

Deafault Information Originate

Configuration options: Enable/Disable

Default configuration: Disable

Function: Enable or disable broadcast default route.

Redistribute Default Metric

Configuration range:1-16

Default configuration:1

Function: Configure the default route metric for importing external routes.

2. Redistribute

The redistributed configuration is shown below.

Redistribute		
Protocol	Enable	Metric
Connected	☐	(1~16)
Static	☐	(1~16)
OSPF	☐	(1~16)

Figure 250 Redistributed configuration

Protocol

Configuration options: Connected/Static/OSPF

Enable

Configuration options: Enable/Disable

Default configuration: Disable

Function: Routes generated by other protocols are redistributed in the RIP route. Only routes with the active route status can be imported.

Metric

Configuration range:1-16

Default configuration:None

Function: Configure the metric of the imported route. This parameter is an optional configuration item. If this parameter is not configured, the metric of the redistributed route is re-published by default.

3. Timer

The configuration of the timer is as shown below.

Timer		
Routing Table Update	30	(5~2147483647Second(s))
Routing Information Timeout	180	(5~2147483647Second(s))
Garbage Collection	120	(5~2147483647Second(s))

Figure 251 Timer configuration

Routing Table Update

Configuration range: 5s-2147483647s

Default configuration: 30s

Function: Configure the interval at which RIP sends update packets.

Routing Information Timeout

Configuration range: 5s-2147483647s

Default configuration: 180s

Function: Configure the RIP route timeout period. If no routing table update information is received from a neighbor in this period, all the routes from the device are regarded as invalid routes, and the route enters the suppression state. The route invalid time configuration should be greater than the route update time.

Garbage Collection

Configuration range: 5s-2147483647s

Default configuration: 120s

Function: Configure the RIP route to be in the suppressed state. If the device does not receive the update information, the routes are deleted from the routing table. The route suppression time should be greater than the route update time.

4. Network Configuration

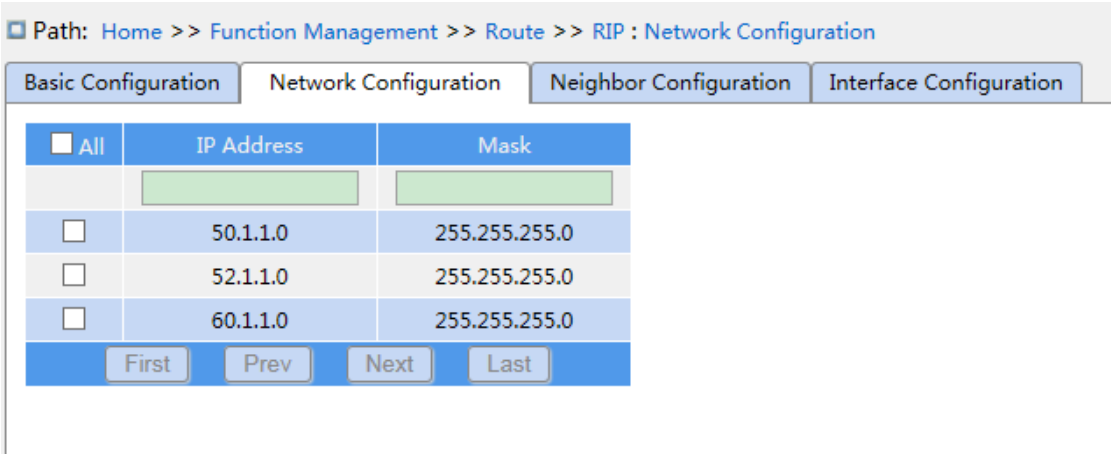


Figure 252 Network configuration

IP Address

Configuration format: A.B.C.D

Function: Declare running RIP protocol on a network segment.

Mask

Configuration format: A.B.C.D

Function: a subnet mask is a 32-bit number, consisting of a sequence "1" and a sequence "0". "1" corresponds to the network number field and the subnet number field, while "0" corresponds to the host number field. The mask length is the number of 1 in the mask.

5. Neighbor Configuration

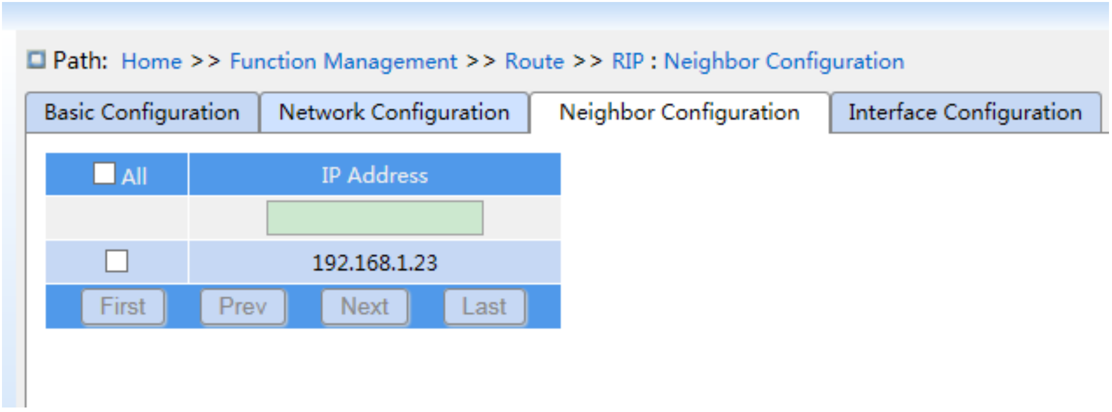


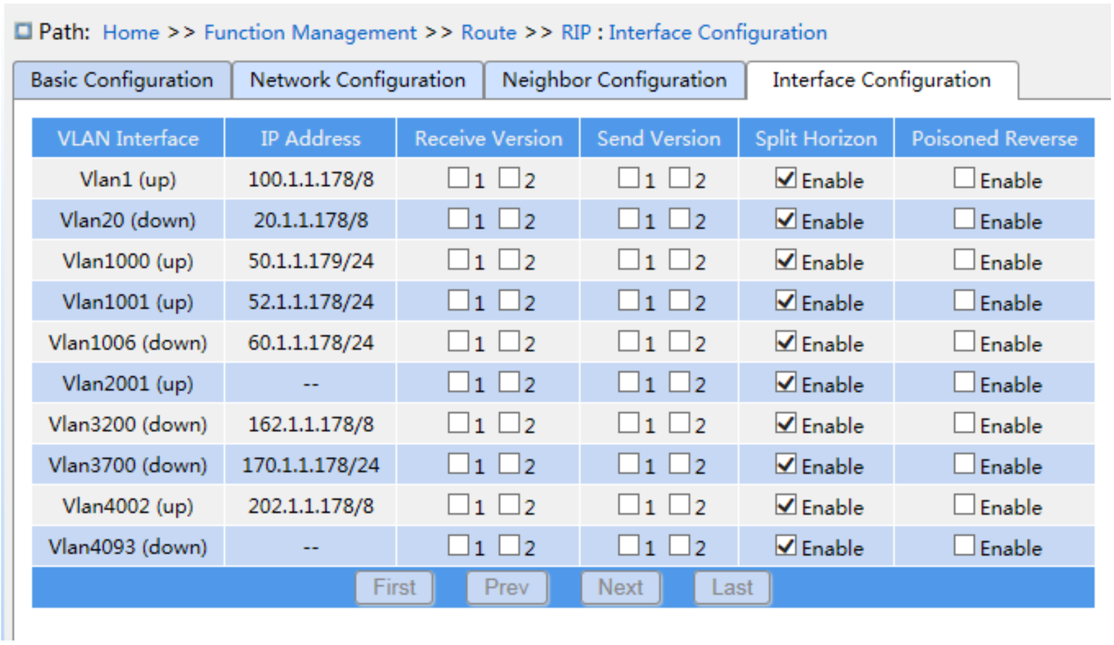
Figure 253 Neighbor configuration

IP Address

Configuration format: A.B.C.D

Function: Configure the neighbor device IP address.

6. Interface configuration



VLAN Interface	IP Address	Receive Version	Send Version	Split Horizon	Poisoned Reverse
Vlan1 (up)	100.1.1.178/8	☐1 ☐2	☐1 ☐2	☑Enable	☐Enable
Vlan20 (down)	20.1.1.178/8	☐1 ☐2	☐1 ☐2	☑Enable	☐Enable
Vlan1000 (up)	50.1.1.179/24	☐1 ☐2	☐1 ☐2	☑Enable	☐Enable
Vlan1001 (up)	52.1.1.178/24	☐1 ☐2	☐1 ☐2	☑Enable	☐Enable
Vlan1006 (down)	60.1.1.178/24	☐1 ☐2	☐1 ☐2	☑Enable	☐Enable
Vlan2001 (up)	--	☐1 ☐2	☐1 ☐2	☑Enable	☐Enable
Vlan3200 (down)	162.1.1.178/8	☐1 ☐2	☐1 ☐2	☑Enable	☐Enable
Vlan3700 (down)	170.1.1.178/24	☐1 ☐2	☐1 ☐2	☑Enable	☐Enable
Vlan4002 (up)	202.1.1.178/8	☐1 ☐2	☐1 ☐2	☑Enable	☐Enable
Vlan4093 (down)	--	☐1 ☐2	☐1 ☐2	☑Enable	☐Enable

Figure 254 Interface configuration

VLAN Interface

All VLAN interfaces on the switch

IP address

IP address of the interface

Receive Version

Configuration options: 1/2

Default configuration: None

Function: Configure the interface to receive the version of RIP packets. 1 means receiving RIP-1 messages; 2 means receiving RIP-2 messages; none of them are unchecked to receive RIP-1 and RIP-2 messages.

send Version

Configuration options: 1/2

Default configuration: None

Function: Configure the version of the interface to send RIP packets. 1 indicates that RIP-1 packets are sent; 2 indicates that RIP-2 packets are sent; none of them are selected to send RIP-2 packets.

Split Horizon

Configuration options: Enable/Disable

Default configuration: Enable

Function: Enable or disable **split horizon**. Horizontal splitting is used to prevent routing loops, that is, prevent Layer 3 switches from sending routes learned from an interface from this interface.

Poisoned Reverse

Configuration options: Enable/Disable

Default configuration: Disable

Function: Enable or disable **Poisoned Reverse**. Toxic reversal is used after IP learns a route from an interface, sets the metric of the route to 16 (unreachable), and sends it back to the neighbor router from the original interface.

7.17.2.5 Typical Configuration Example

As shown below, 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.

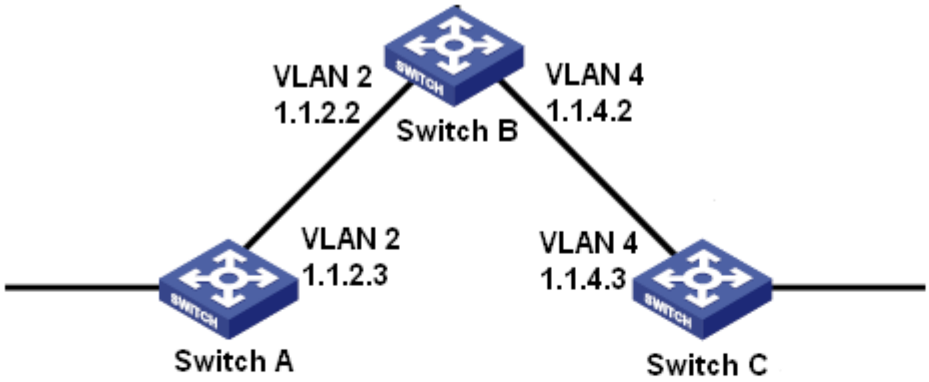


Figure 255 RIP Configuration Example

Configuration on Switch A:

1. Set IP address for VLAN 2 interface.

2. Enable RIP protocol, as shown in Figure 249.

3. Enable VLAN 2 interface to transmit/ receive RIP message, as shown in Figure 254.

Configuration on Switch B:

1. Set IP addresses for VLAN 2 and VLAN 4 interfaces.

2. Enable RIP protocol, as shown in Figure 249.

3. Enable VLAN 2 and VLAN 4 interfaces to transmit/ receive RIP message, as shown in Figure 254.

Configuration on Switch C:

1. Set IP address for VLAN 4 interface.

2. Enable RIP protocol, as shown in Figure 249.

3. Enable VLAN 4 interface to transmit/ receive RIP message, as shown in Figure 254.

7.17.3 OSPF Configuration

7.17.3.1 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.

7.17.3.2 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.

7.17.3.3 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 256. 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.

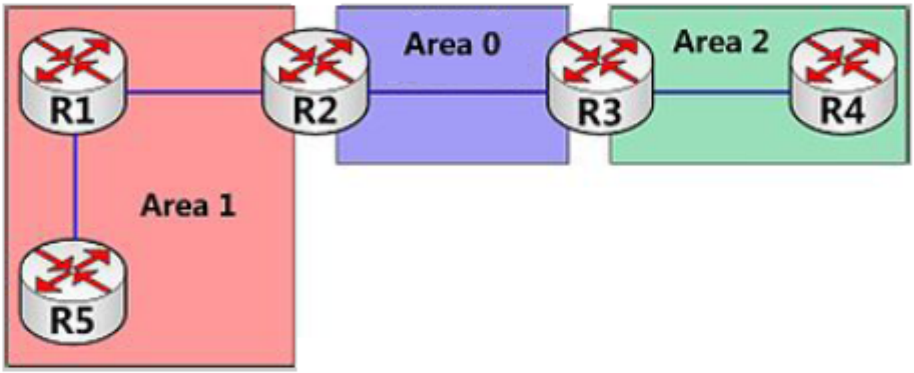


Figure 256 Area Partition

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 257.

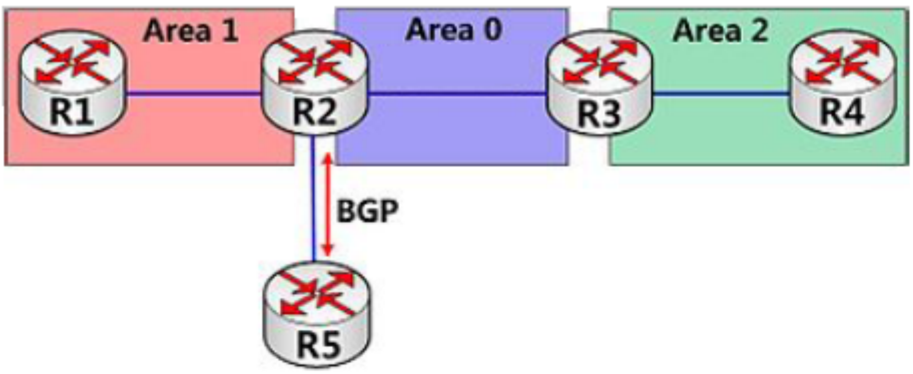


Figure 257 OSPF Router Types

Internal router: All interfaces on an internal router belong to one OSPF area. For example, R1 and R4 in Figure 257.

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 257.

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 257.

ASBR: A router exchanging routing information with another AS is an ASBR. For example, R2 in Figure 257.

One router can be of multiple types. For example, R2 in Figure 257 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.

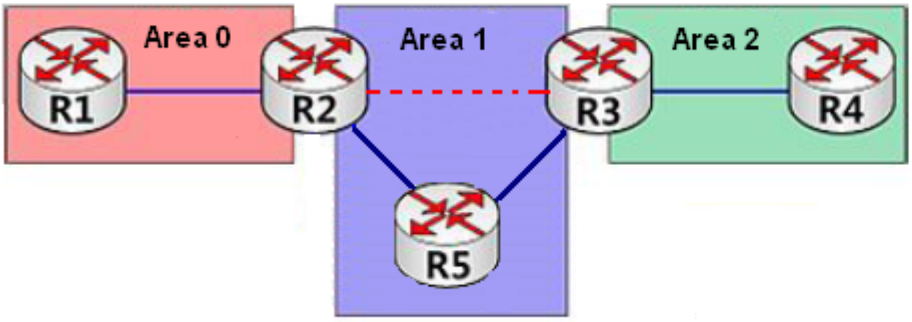


Figure 258 Virtual Link

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 258 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.

7.17.3.4 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.

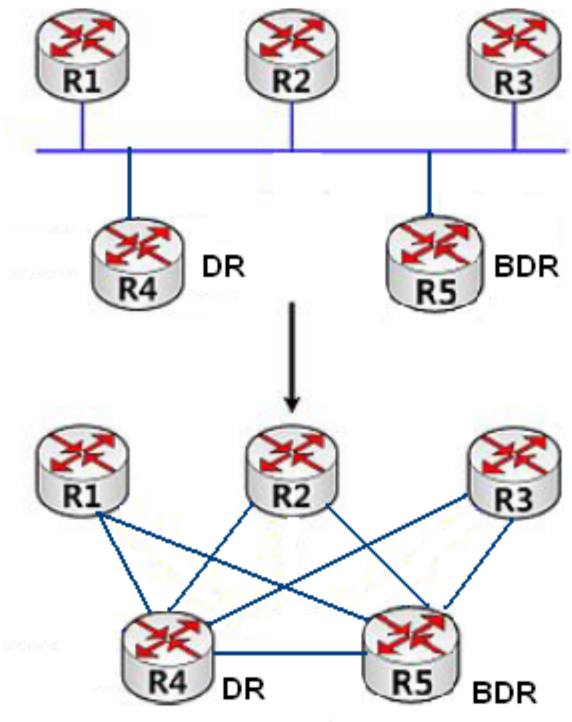


Figure 259 DR and DBR

As shown in Figure 259, 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.

7.17.3.5 Web Configuration

1. OSPF Basic configuration

Click the navigation tree [Function Management]→[Route]→[OSPF]→[Basic Configuration] menu to enter the OSPF basic configuration interface, as shown below.

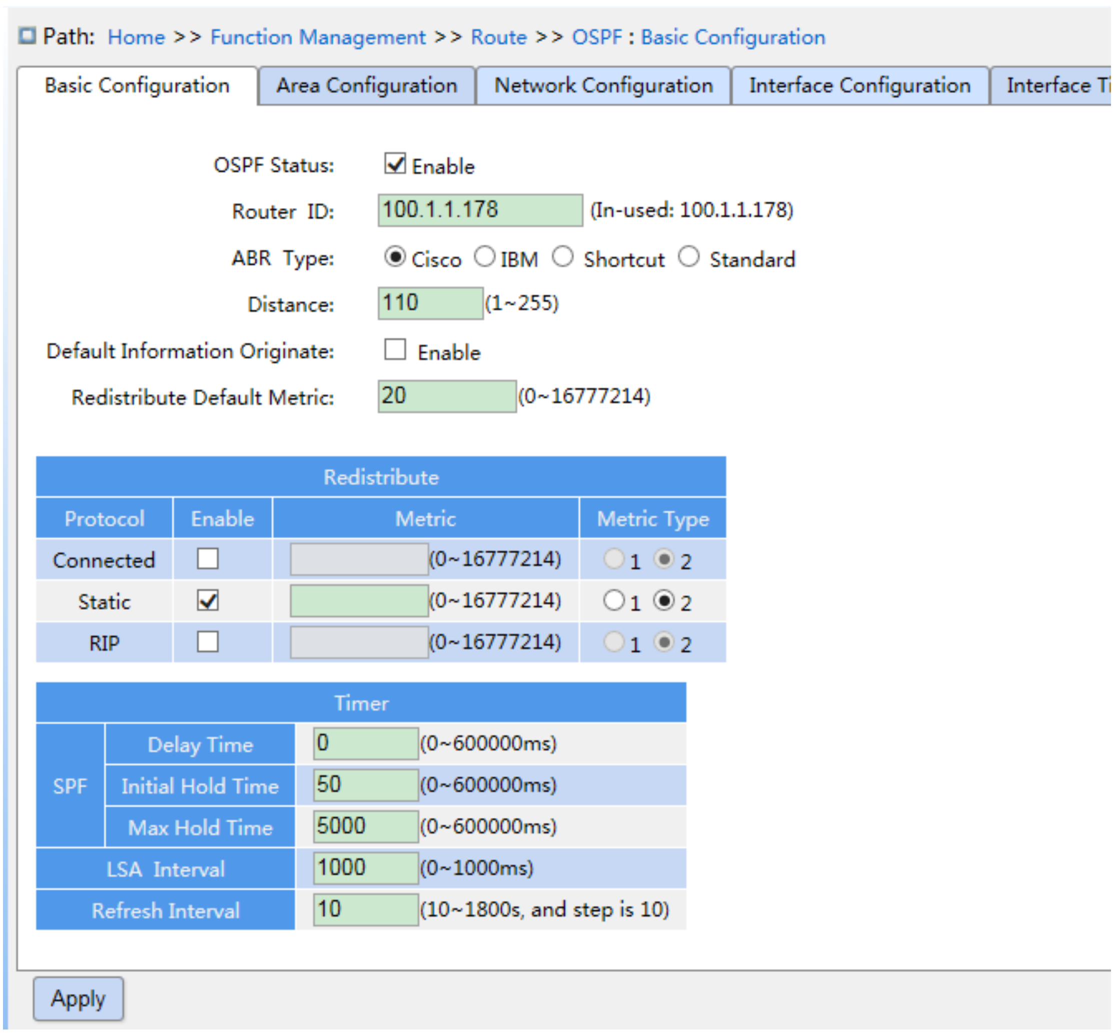


Figure 260 OSPF basic configuration

OSPF Status

Configuration options: Enable/Disable

Default configuration: Disable

Function: Enable or disable OSPF.

Router ID

Configuration format: A.B.C.D

Default configuration: The minimum of all configured IPs of the switch.

Function: Configure the RID of the OSPF switch. Each switch enabled with OSPF has a unique RID ID in the AS.

CAUTION

Caution:

RID changes only work after the OSPF process is restarted.

Router ID (In-Used)

Function: Display the current actual RID.

ABR Type

Configuration options: Cisco/IBM/Shortcut/Standard

Default configuration: Cisco

Function: Configure the ABR type of the router.

Description：

Cisco：Configure at least two areas, each of which contains at least one non-down state interface, and one of them is area 0. This router can be counted as a Cisco type ABR.

IBM：Configure at least two zones, each zone containing at least one non-down state interface. And area 0 is configured, and area 0 contains an interface of any state, this router can be counted as IBM type ABR. Area 0 can be counted in at least two non-down areas.

Shortcut/Standard: Configure at least two areas, each of which contains at least one non-down state interface. This router can be regarded as the standard/shortest path type ABR regardless of whether or not area 0 is included.

Distance

Configuration range: 1-255

Default configuration: 110

Function: Configure the administrative distance of OSPF routes.

Deafault Information Originate

Configuration options: Enable/Disable

Default configuration: Disable

Function: Enables OSPF to broadcast the default route 0.0.0.0 to the OSPF domain. This function takes effect only if the route 0.0.0.0 exists in the local routing table.

Redistribute Default Metric

Configuration range: 0-16777214

Default configuration: 20

Function: Configure the default route metric for importing external routes.

Redistribute-Protocol

Protocol Type: Connected/Static/RIP

Function: Mark the protocol type for republishing external routes.

Description：**Connected** indicates that the direct route is imported as the external route information. **Static** indicates that the static route is imported as the external route information. **RIP** indicates that the route discovered by the RIP protocol is imported as the external route information.

Redistribute-Enable

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to republish an external route of the specified type.

Redistribute-Metric

Configuration range: 0-16777214

Default configuration: None

Function: Configure the cost of OSPF to redistribute external routes of the specified type. The effective value of this value is higher than the global configuration of the re-release default metric.

Redistribute- Metric Type

Configuration options: 1/2

Default configuration: 2

Function: Configure the default type when redistributing external routes.

Description：**1** represents the first type of external route, and **2** represents the second type of external route. The cost of the external route to the first type is equal to the sum of the overhead of the router to the corresponding ASBR and the cost of the ASBR to the destination address; the cost of the external route to the second type is equal to the cost of the ASBR to the destination address.

SPF Delay Time

Configuration range: 0-600000ms

Default configuration: 0

Function: Set the minimum interval for calculating OSPF routes.

SPF Initial Hold Time

Configuration range: 0-600000ms

Default configuration: 50ms

Function: Set the initial interval for calculating OSPF routes.

SPF Max Hold Time

Configuration range: 0-600000ms

Default configuration: 5000ms

Function: Set the maximum interval for calculating OSPF routes.

LSA Interval

Configuration range: 0-1000ms

Default configuration: 1000ms

Function: Set the minimum arrival time of the LSA

Refresh Interval

Configuration range: 10s~1800s, step size is 10

Default configuration: 10

Function: Set the LSA refresh timer interval.

2. Stub/NSSA area configuration

Click the navigation tree [Function Management]→[Route]→[OSPF]→[Area Configuration] menu to enter the OSPF area configuration interface, as shown below.

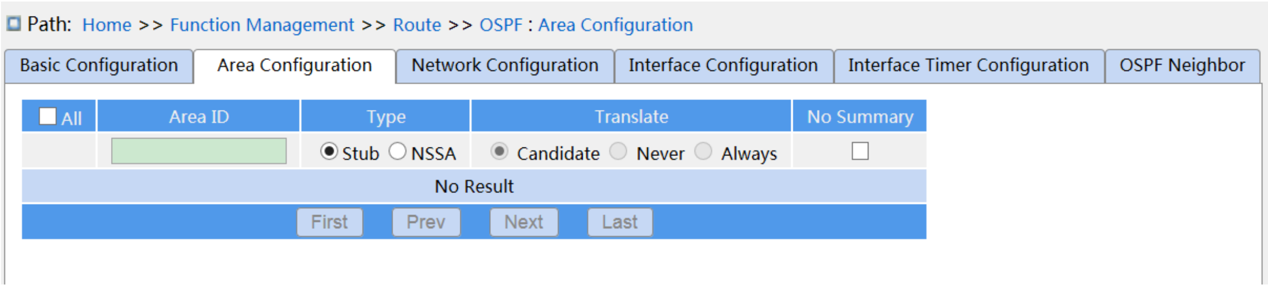


Figure 261 OSPF Area configuration

Area ID

Configuration format: A.B.C.D

Configuration range: 0.0.0.0~255.255.255.255

Function: Configure the specified area as a stub/NSSA area.

Type

Configuration options: Stub/NSSA

Default configuration: Stub

Function: Configure the specified area as the Stub/NSSA area.

Translate

Configuration options: Candidate / Never/ Always

Default configuration: Candidate

Function: Configure the conversion rules of ABRs for Type 7 LSAs in the NSSA area.

Description: **Candidate**: The ABR in the NSSA area is elected according to the RID size to determine whether to convert the Type 7 LSA. The RID has a high priority. **Never**: ABR in the NSSA area never performs 7 types of LSA conversion. **Always**: ABR in the NSSA area always performs Type 7 LSA conversion.

No Summary

Configuration options: Enable/Disable

Default configuration: Disable

Function: Configure whether the specified area is a full Stub/NSSA area, that is, whether Class 3 LSA injection is allowed.

3. Network Configuration

Click the navigation tree [Function Management] → [Route] → [OSPF] → [Network Configuration] menu to enter the OSPF network configuration, as shown below.

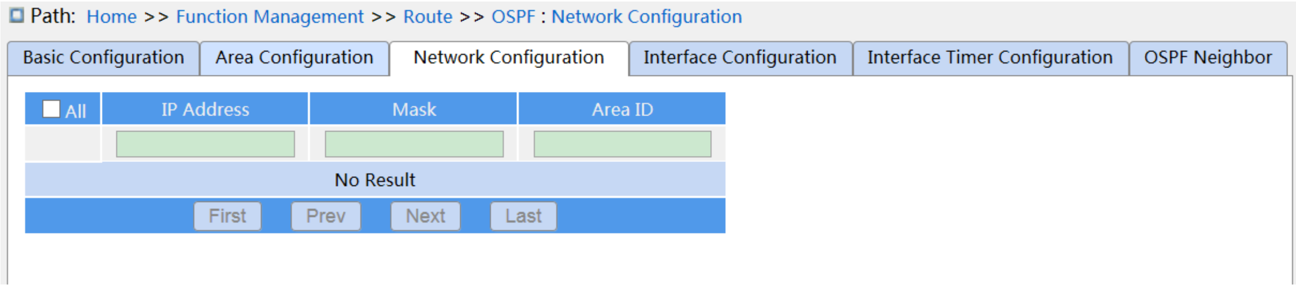


Figure 262 OSPF network configuration

IP Address

Configuration format: A.B.C.D

Function: Configure network IP address.

Mask

Function: Configuring the network's subnet mask.

Description: The mask and network address together determine a network range.

Area ID

Configuration format: A.B.C.D

Configuration range: 0.0.0.0~255.255.255.255

Function: Configure the network-wide region

Description: Once a network is added to the area, all internal routes of the network are no longer broadcast independently to other areas, but only the summary information of the entire network-wide route is broadcast.

4. Interface configuration

Click the navigation tree [Function Management] → [Route] → [OSPF] → [Interface Configuration] menu to enter the OSPF interface configuration, as shown below.

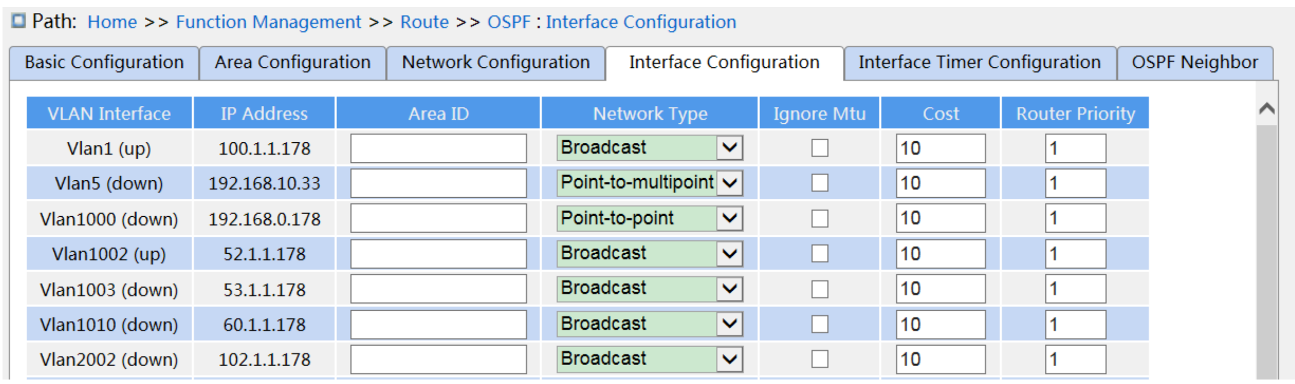


Figure 263 Configure the area and parameters of the VLAN interface

Area ID

Configuration format: A.B.C.D

Configuration range: 0.0.0.0~255.255.255.255

Function: Configure the area to which the VLAN interface belongs.

Description: Adding a VLAN interface to an OSPF area means enabling the OSPF protocol for the VLAN interface.

Network Type

Configuration options: Broadcast/Point to multipoint/Point to point

Default configuration: Broadcast

Function: Configure the OSPF network type of the specified interface.

Ignore Mtu

Configuration options: Enable/Disable

Default configuration: Disable

Function: Configure whether the specified interface checks the MTU of received DD packets.

Description: If the interface MTU value in the neighbor router DD message is inconsistent with the local interface MTU value, OSPF adjacency cannot be formed. If this function is enabled, the DD message is ignored and the adjacency relationship is established.

Cost

Configuration range: 1-65535

Default configuration: 10

Function: Configure the path cost of an OSPF interface.

Router priority

Configuration range: 0-255

Default configuration: 1

Function: Configure the VLAN interface priority for starting OSPF.

Description: When DR and BDR are selected on the network segment, the device with the highest priority value is selected as the DR.

5. Interface Timer Configuration

Click the navigation tree [Function Management]→[Route]→[OSPF]→[Interface Timer Configuration] menu to enter the OSPF Interface Timer configuration, as shown below.

Path: Home >> Function Management >> Route >> OSPF : Interface Timer Configuration

Basic Configuration | Area Configuration | Network Configuration | Interface Configuration | Interface Timer Configuration | OSPF Neighbor

VLAN Interface	IP Address	Dead Time		Hello Interval		Retransmit Interval		Transmission Delay	
Vlan1 (up)	100.1.1.178	40	(1~65535Second(s))	10	(1~65535Second(s))	5	(3~65535Second(s))	1	(1~900Second(s))
Vlan5 (down)	192.168.10.33	40	(1~65535Second(s))	10	(1~65535Second(s))	5	(3~65535Second(s))	1	(1~900Second(s))
Vlan1000 (down)	192.168.0.178	40	(1~65535Second(s))	10	(1~65535Second(s))	5	(3~65535Second(s))	1	(1~900Second(s))
Vlan1002 (up)	52.1.1.178	40	(1~65535Second(s))	10	(1~65535Second(s))	5	(3~65535Second(s))	1	(1~900Second(s))
Vlan1003 (down)	53.1.1.178	40	(1~65535Second(s))	10	(1~65535Second(s))	5	(3~65535Second(s))	1	(1~900Second(s))

Figure 264 Configure OSPF interface timer configuration

Dead Time

Configuration range: 1s-65535s

Default configuration: 40s

Function: Configure the timeout interval of the neighboring switch on the specified interface.

Description: When the switch does not receive the HELLO packet sent by the neighboring device within the time range, the switch considers that the neighboring device is unreachable and invalid.

Hello Interval

Configuration range: 1s-65535s

Default configuration: 10s

Function: Configure the interval for sending HELLO packets on the specified interface.

Description: The switch periodically sends HELLO packets to neighboring devices to discover and maintain adjacencies and elect DR and BDR.

Retransmit Interval

Configuration range: 3s-65535s

Default configuration: 5s

Function: Configure the retransmission interval when transmitting LSAs between a specified interface and a neighboring switch.

Description: When a switch transmits an LSA to its neighboring device, it will hold the LSA until it receives an acknowledgment from the other party. If no acknowledgment message is received within that time interval, the LSA is retransmitted.

Transmission Delay

Configuration range: 1s-900s

Default configuration: 1s

Function: Configure the delay of transmitting LSAs on the specified interface.

Caution:

To ensure the normal operation of OSPF, the timer parameters of OSPF neighbors must be consistent.

6. OSPF Neighbor

Click the navigation tree [Function Management]→[Route]→[OSPF]→[OSPF Neighbor] menu to enter the OSPF Neighbor information, as shown below.

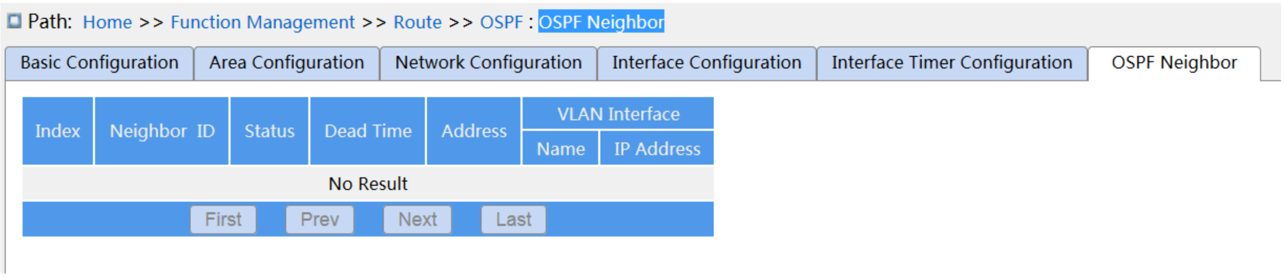


Figure 265 OSPF neighbor information

7.17.3.6 typical Configuration Example

R1 and R2 run OSPF. R1 imports external static routes into the OSPF area.

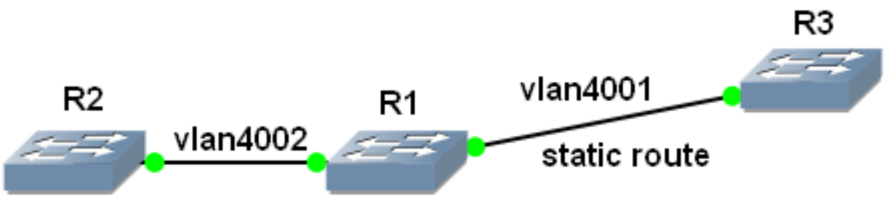


Figure 266 OSPF Configuration Example

Configuration on R1:

1. Set the IP address of VLAN 4002 interface: 202.1.1.178, subnet mask: 255.0.0.0; configure the IP address of VLAN 4001 interface: 201.1.1.178, subnet mask: 255.0.0.0;

2. Set a static route with the destination address being 6.0.0.0/8 and the next hop being 201.1.1.176.

3. Set the router ID as 100.1.1.178, as shown in Figure 260.
4. Start the OSPF protocol, as shown in Figure 260.
5. Set the area 0 of the VLAN 4002 interface, as shown in Figure 261.
6. Configure OSPF to redistribute static routes, as shown in Figure 262.

Configuration on R2:

1. Set the IP address of VLAN 4002 interface: 202.1.1.177, subnet mask: 255.0.0.0;
2. Set the router ID to be 100.1.1.177.
3. Start the OSPF protocol.
4. Set the area 0 of the VLAN 4002 interface.

Configuration on R3:

1. Set the IP address of VLAN 4001 interface: 201.1.1.178, subnet mask: 255.0.0.0.

At this point, the neighbor relationship is successfully established on R1, as shown in Figure 265.

7.18 QoS Configuration

7.18.1 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.

Traffic classification, traffic policing, traffic shaping, congestion management, and congestion avoidance are the main concepts of QoS deployment. They mainly complete the following functions:

Traffic classification: identifies an object based on certain matching rules. It is the basis and prerequisite of QoS.

Traffic policing: supervises the traffic rate of packets that are transmitted to a device. When the traffic rate exceeds the specified traffic rate, the device adopts restriction or penalty measures to protect network resources against damage. Traffic policing is classified into port-based traffic policing and queue-based traffic policing.

Traffic shaping: proactively adjusts traffic output rate. It aims at adapting traffic to available network resources of a downstream device to prevent unnecessary packet discarding and congestion. Traffic shaping is classified into port-based traffic shaping and queue-based traffic shaping.

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.

Traffic policing, traffic shaping, congestion management, and congestion avoidance control the network traffic and allocated resources from different aspects. They are the specific embodiment of QoS. For example, the switch supervises packets that are transmitted to a network based on the committed rate. It conducts shaping on the packets before the packets leave the switch. It conducts queue scheduling management in the case of congestion, and adopts congestion avoidance measures when the congestion is intensifying.

7.18.2 Principle

Each port of this series switches supports 8 cache queues, from 0 to 7 in priority ascending order.

When a frame reaches the port, the switch determines the queue for the frame according to the frame information and port. This series switches support traffic classification in the following queue mapping modes: port, 802.1Q header information, differentiated services code point (DSCP), and QoS control list (QCL), with the priority in ascending order.

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: 6 Queues Weighted and SP（Strict Priority）.

WRR (Weighted Round Robin) 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.

SP mode forwards high-priority packets preferentially. It is mainly used for transmitting sensitive signals. If a frame enters the high-priority queue, the switch stops scheduling the low-priority queues and starts to process the data of the high-priority queue. When the high-priority queue contains no data, the switch starts to process the data of the queue with lower priority.

6 Queues Weighted indicates that queue 6 and queue 7 use the Strict Priority scheduling mode, and queue 0 ~ queue 5 use the WRR scheduling mode. Data in queue 7 is processed prior to data in queue 6. When both queue 7 and queue 6 are empty, data in queue 0 ~ queue 5 is scheduled based on the weight ratio.

7.18.3 Web Configuration

1. Configure queue mapping mode based on port, as shown below.

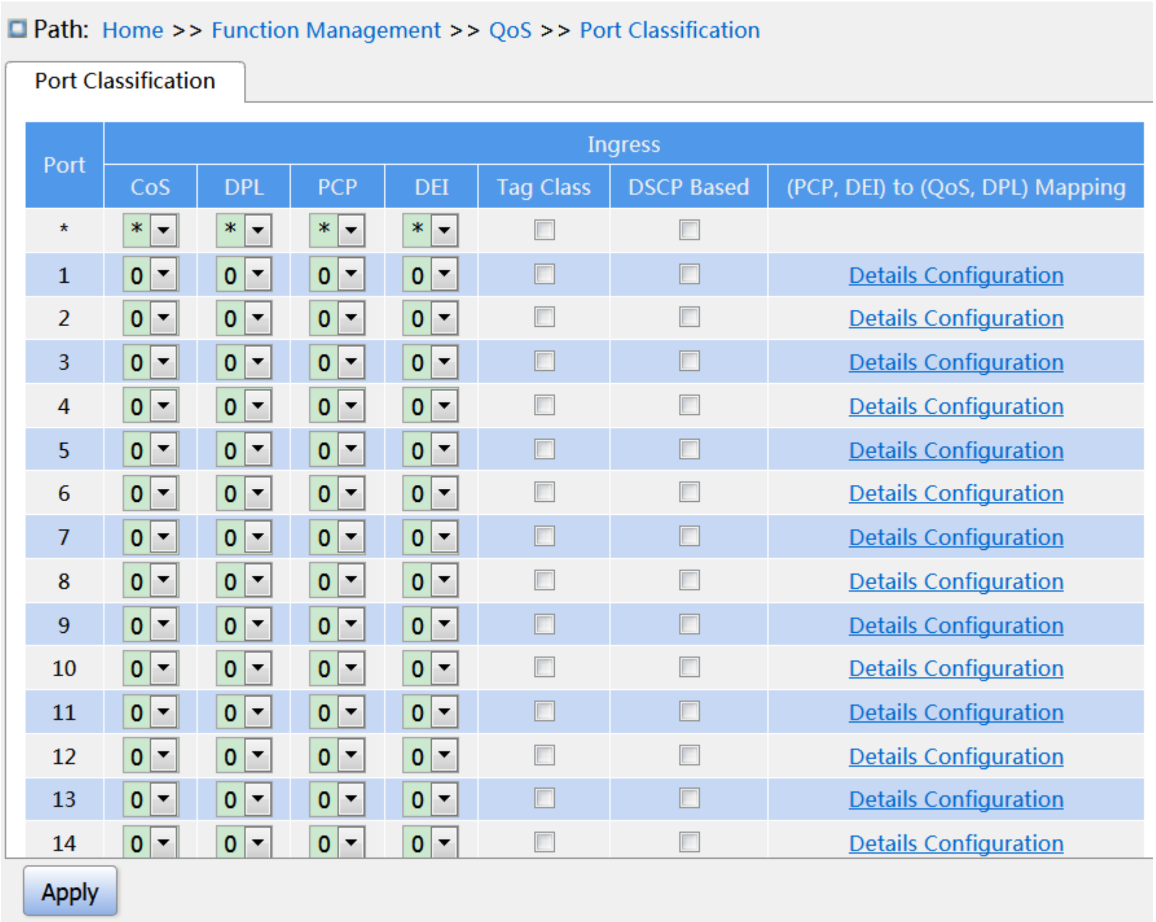


Figure 267 Configure queue mapping mode based on port

CoS

Configuration range: 0~7

Default configuration: 0

Function: Configure the default COS value of the port.

Description: The CoS value determines the storage queue of the message, which corresponds to the queue 0 ~ 7 in turn. When a message enters the switch, the switch assigns CoS value to the message. If the message is tag type and disable tag class, or if the message is untag, the CoS value of the message is the default CoS value of the receiving port.

DPL

Configuration range: 0~1

Default configuration: 0

Function: configure port default DPL vaule（Drop Priority Level）

Description: Specified DPLs is default DPLs of port when Untag messages or disable tag class tag messages enter the switch.

PCP

Configuration range: 0~7

Default configuration: 0

Function: configure port default PCP vaule（Priority Code Point）.

Description: The priority value in the tag added after the untag message enters the switch is the port default PCP value.

DEI

Configuration range: 0~1

Default configuration: 0

Function: Configure port default DEI value（Drop Eligible Indicator）.

Description: The CFI value in the tag added after the untag message enters the switch is the port default DEI value.

2、Configure queue mapping mode based on 802.1Q header information.

As shown in Figure 267, check <tag class> of port, and click <details configuration> of (PCP, DEI) to (QOS, DPL) mapping, enter the corresponding interface's queue mapping mode configuration interface based on 802.1q header information, as shown below.

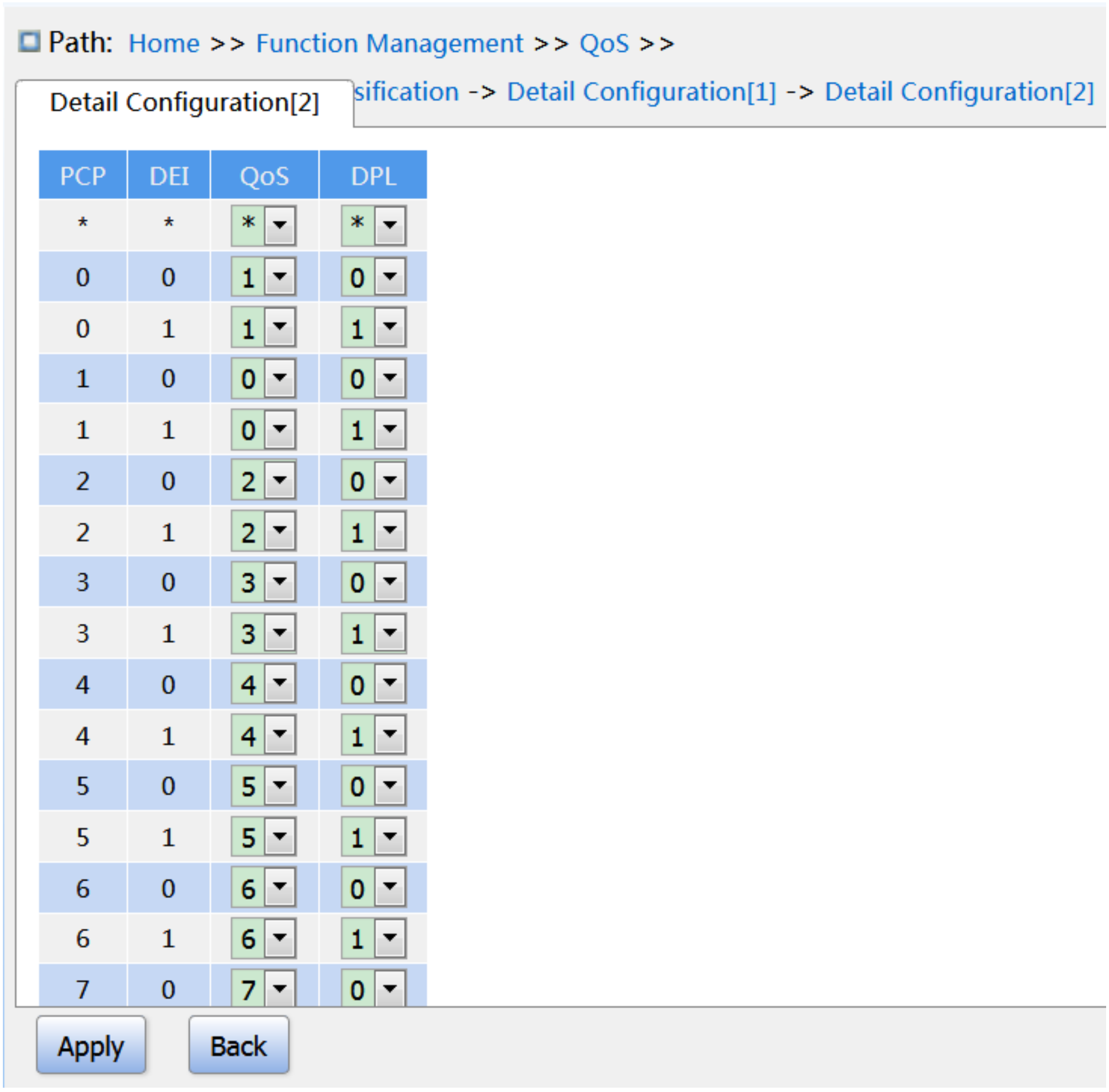


Figure 268 Configure queue mapping mode based on 802.1Q header information

Caution:

The queue mapping mode based on 802.1Q header information is only suitable for received messages is tag.

(PCP, DEI) to (QoS class, DP level) mapping

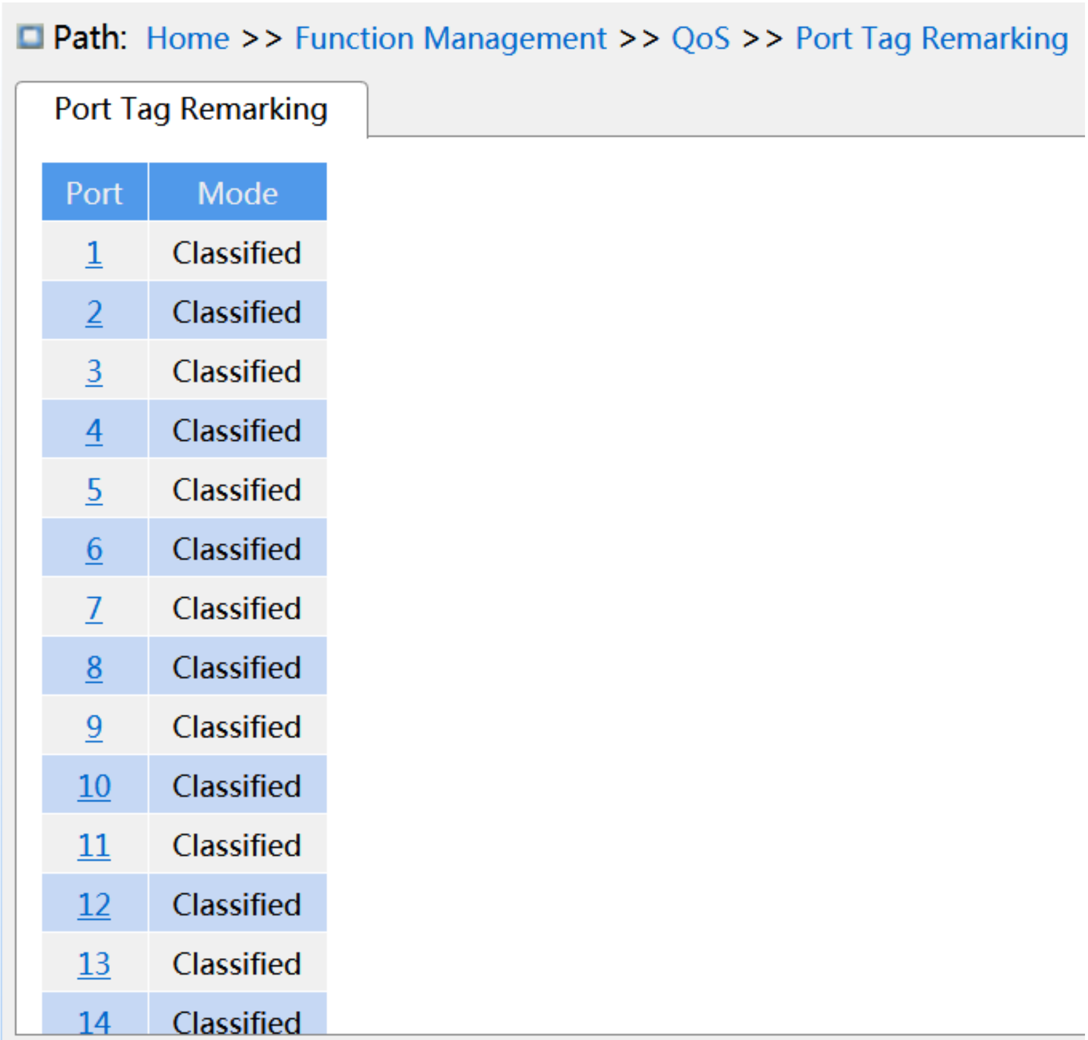
Configuration range: 0~7 (QoS type) 0~1 (DP level)

Default configuration: PCP value 0, 1, 2, 3, 4, 5, 6, 7 map to QoS class 1, 0, 2, 3, 4, 5, 6, 7; DEI value 0, 1 map to DP level 0, 1.

Function: Configure (PCP, DEI) to (CoS, DPL) mapping according to PCP and DEI value in the message.

Description: The QoS class is equal to the CoS value, which determines the storage queue of the message, corresponding to the queue 0 - 7 in turn. When a message enters the switch, the switch assigns CoS and DPL values to the message. If the message type is tag and enable tag class, the CoS and DPL values of the message are the mapping value from (PCP, DEI) to (CoS, DPL) .

3. Configure 802.1p remarking, as shown below.



Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified
11	Classified
12	Classified
13	Classified
14	Classified

Figure 269 Configure 802.1p remarking

Click <Port >button, enter 802.1p remarking configuraton page, as shown in Figure 270. This page shows the mode of remarking 802.1p when the port forwards the message. The 802.1p remarking indicates PCP and DEI value in the updated message when the port forwards the message.

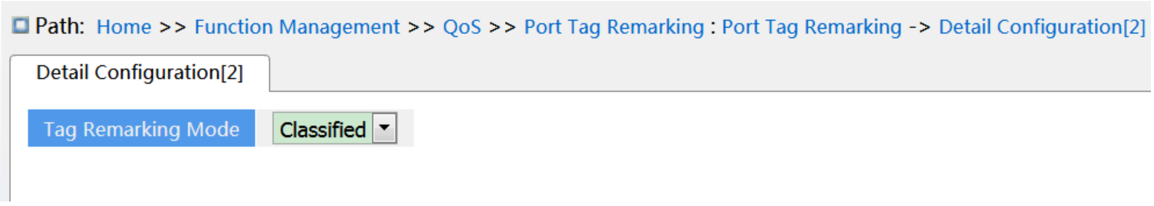


Figure 270 Configure the 802.1p remarking mode of specified port

Caution:

If there is no tag in the forwarded port message, the 802.1p remarking is invalid.

➢Configure 802.1p remarking mode as Classified, as shown in Figure 270.

Tag Remarking Mode

Configuration options: Classified/Mapped/Default

Default configuration: Classified

Function: configure 802.1p remarking mode. Classified mode: The PCP and DEI values in the message are not updated when the egressport forwards the message.

➢ Configure 802.1p remarking mode as Default, as shown below.

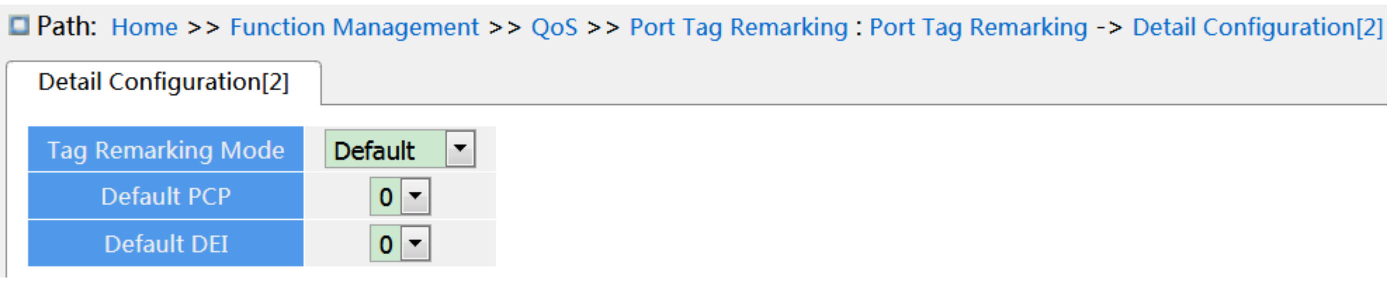


Figure 271 Configure Default Remarking Mode

Tag Remarking Mode

Configuration options: Classified/Mapped/Default

Default configuration: Classified

Function: configure 802.1p remarking mode. Default mode: When the egressport forwards the message, the PCP and DEI values in the updated message are the default values of the egressport. (configuration as below)。

Default PCP

Configuration range: 0~7

Default configuration: 0

Function: configure the default PCP value of the egressport.

Default DEI

Configuration range: 0~1

Default configuration: 0

Function: configure the default DEI value of the egressport.

➢ Configure 802.1p remarking mode as Mapped, as shown below.

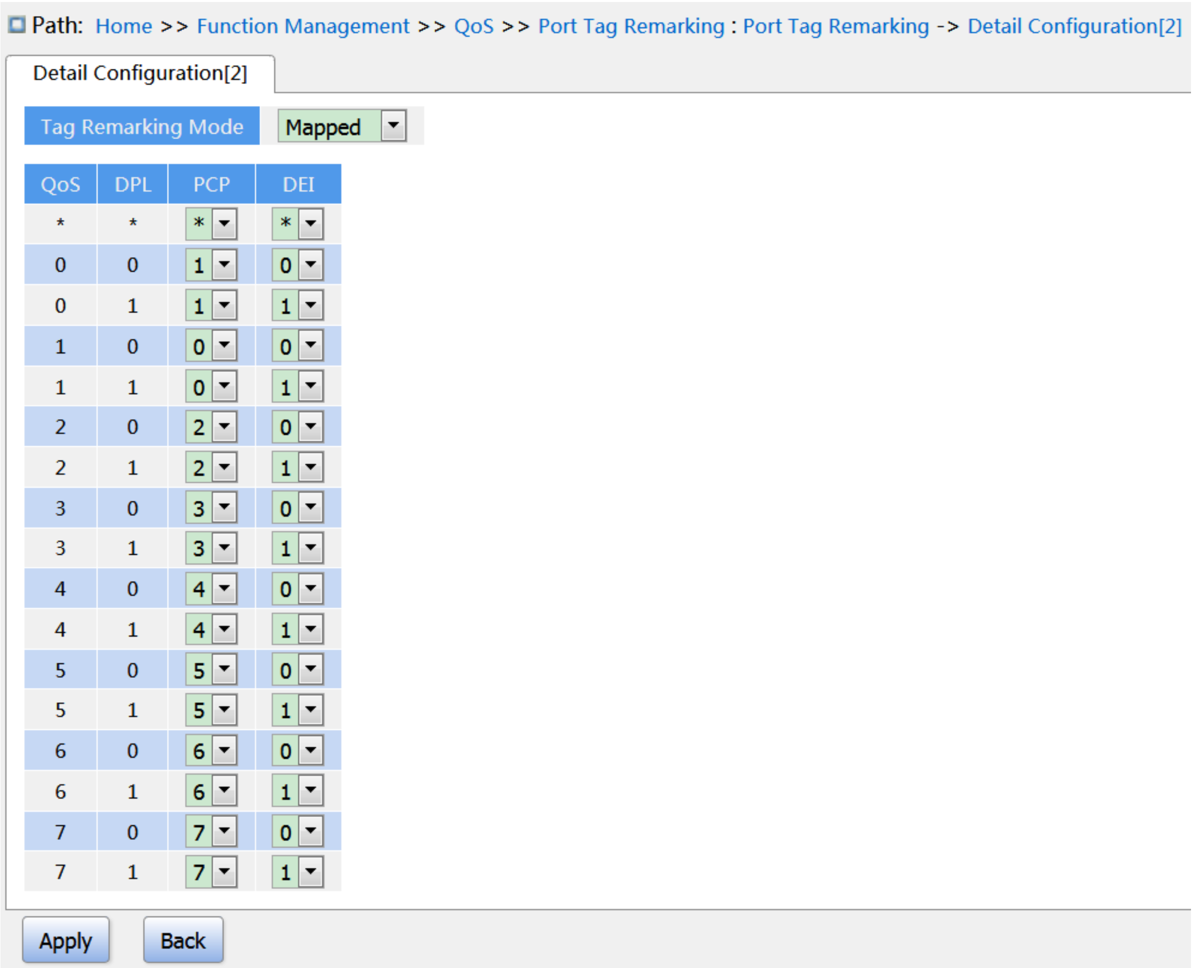


Figure 272 Configure Mapped Remarking mode

Tag Remarking Mode

Configuration options: Classified/Mapped/Default

Default configuration: Classified

Function: configure 802.1p remarking mode. Mapped mode: When the egressport forwards the message, PCP and DEI values in the updated message are mapping value from（CoS, DPL）to（PCP, DEI）.（mapping confguraton as below）.

（QoS class, DP level）to（PCP, DEI）mapping

Configuration options: 0~7（PCP）0~1（DEI）

Default configuration: QoS class 0, 1, 2, 3, 4, 5, 6, 7 map to PCP value 1, 0, 2, 3, 4, 5, 6, 7; DP level 0, 1 map to DEI value 0, 1.

Function: according to CoS and DPL value in the message, configure（CoS, DPL）to（PCP, DEI）mapping.

4. Enable queue mapping mode based on DSCP, as shown below.

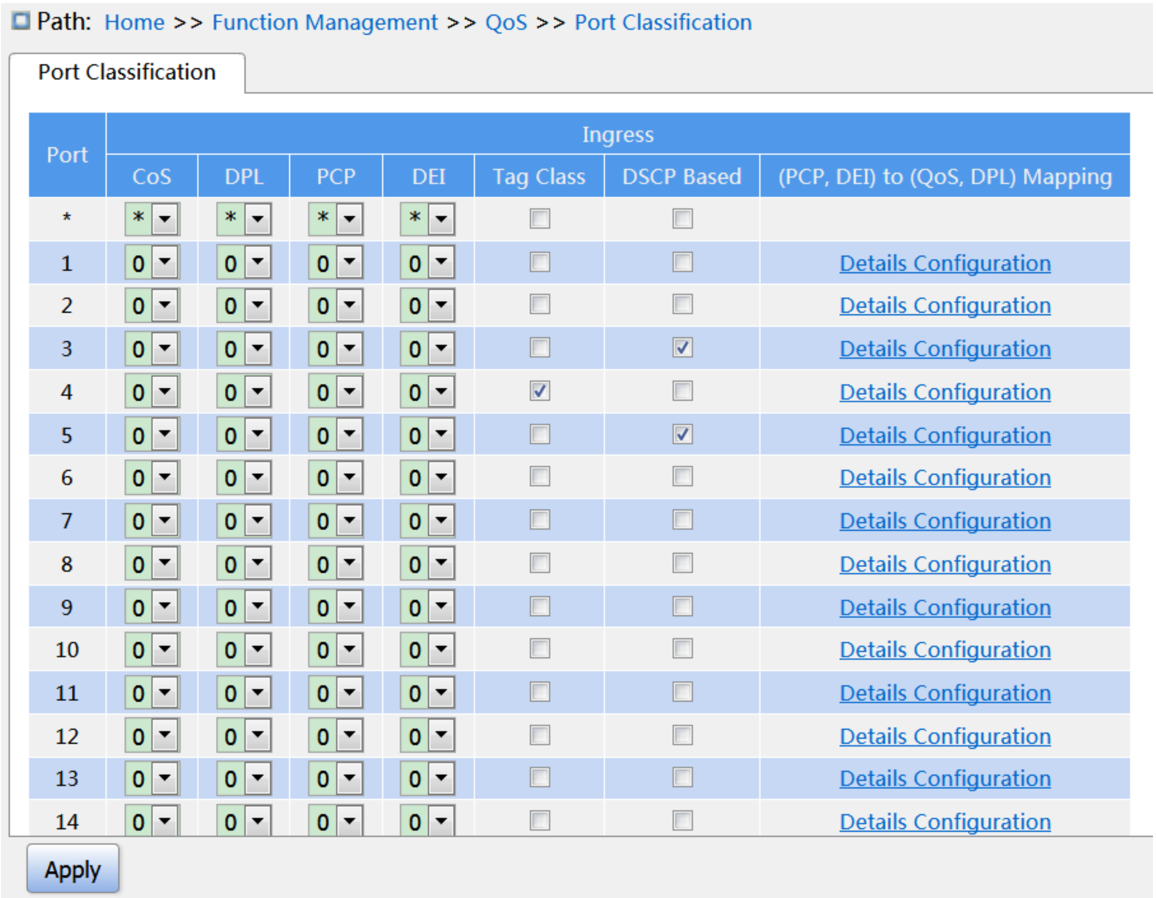


Figure 273 Enable queue mapping mode based on DSCP

DSCP Based

Configuration options: Enable/disable

Default configuration: Disable

Function: whether enable queue mapping mode based on DSCP, the queue mapping mode priority is higher than the queue mapping mode based on 802.1Q header information.

5. Enable Translate of ingress port, rewrite of egress port, as shown below.

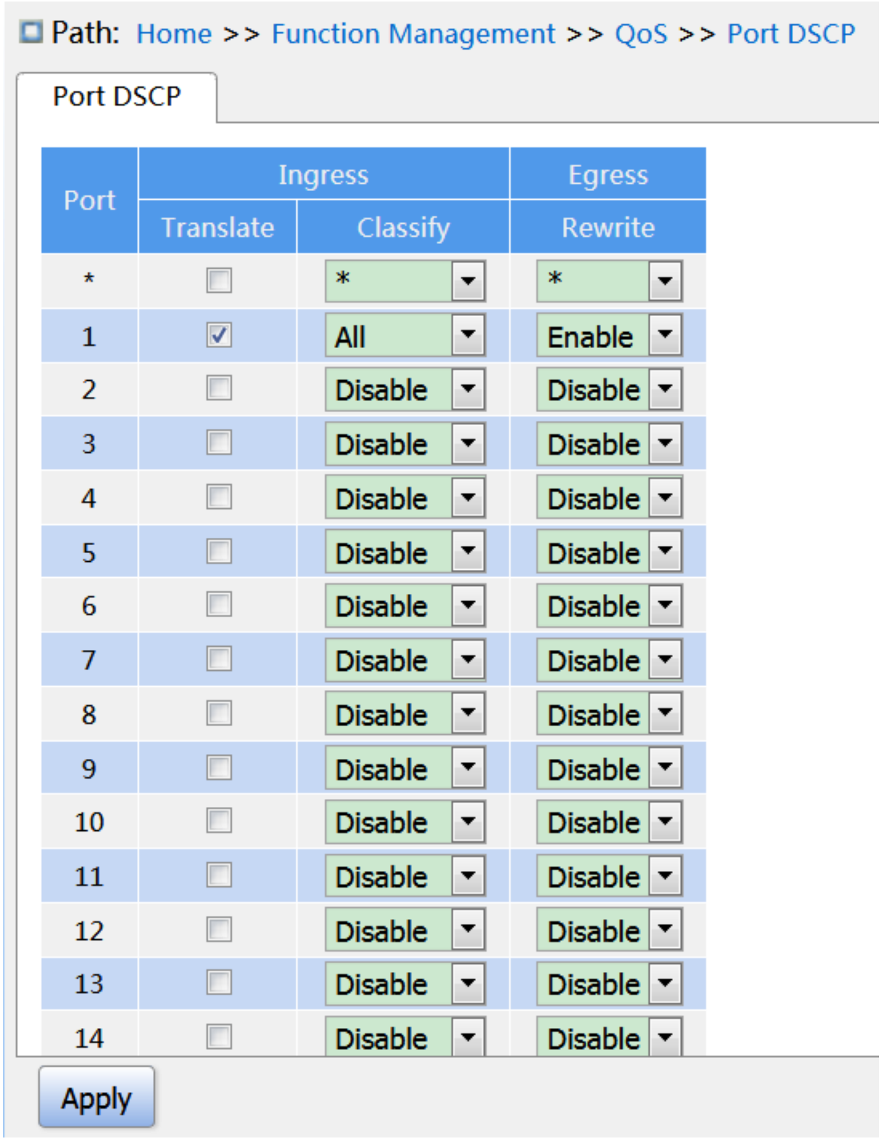


Figure 274 Configure Port DSCP

Translate

Configuration options: Enable/disable

Default configuration: Disable

Function: After the ingress port receives the message, whether translating the dscp value in the message. If enable, the DSCP value is translated according to the DSCP translation table. (the “translate” column in Figure 276).

Classify

Configuration options: Disable/DSCP=0/Selected/All

Default configuration: Disable

Function: Rewrite is configured as Enable, this parameter selects the DSCP value that the egress port rewrite.

Disable: When egress port forwards the message, the DSCP value in the message is not rewritten;

DSCP=0: When egress port forwards the message, if DSCP=0 in the message, then the DSCP value in the message is rewritten according to the classify rule in Figure 277;

Selected: When egress port forwards the message, if DSCP is selected value (the “classify” column in Figure 276, then the DSCP value in the message is rewritten according to the classify rule in Figure 277;

All: When egress port forwards the message, the DSCP is rewritten according to the classify rule in Figure 277.

Rewrite

Configuration options: Disable/enable/remap

Default configuration: Disable

Function: Configure rewrite mode of the DSCP value when the egress port forwards message.

Disable: When egress port forwards the message, the DSCP value in the message is not rewritten;

Enable: When egress port fo rwards the message, whether to rewrite the DSCP value in the message according to the classify configuration.

Remap: When egress port fo rwards the message, the DSCP in the message is rewritten according to (DSCP，DPL) to DSCP mapping (“remap DP0, DP1” in Figure 276).

6. Configure queue mapping mode based on DSCP, as shown below.

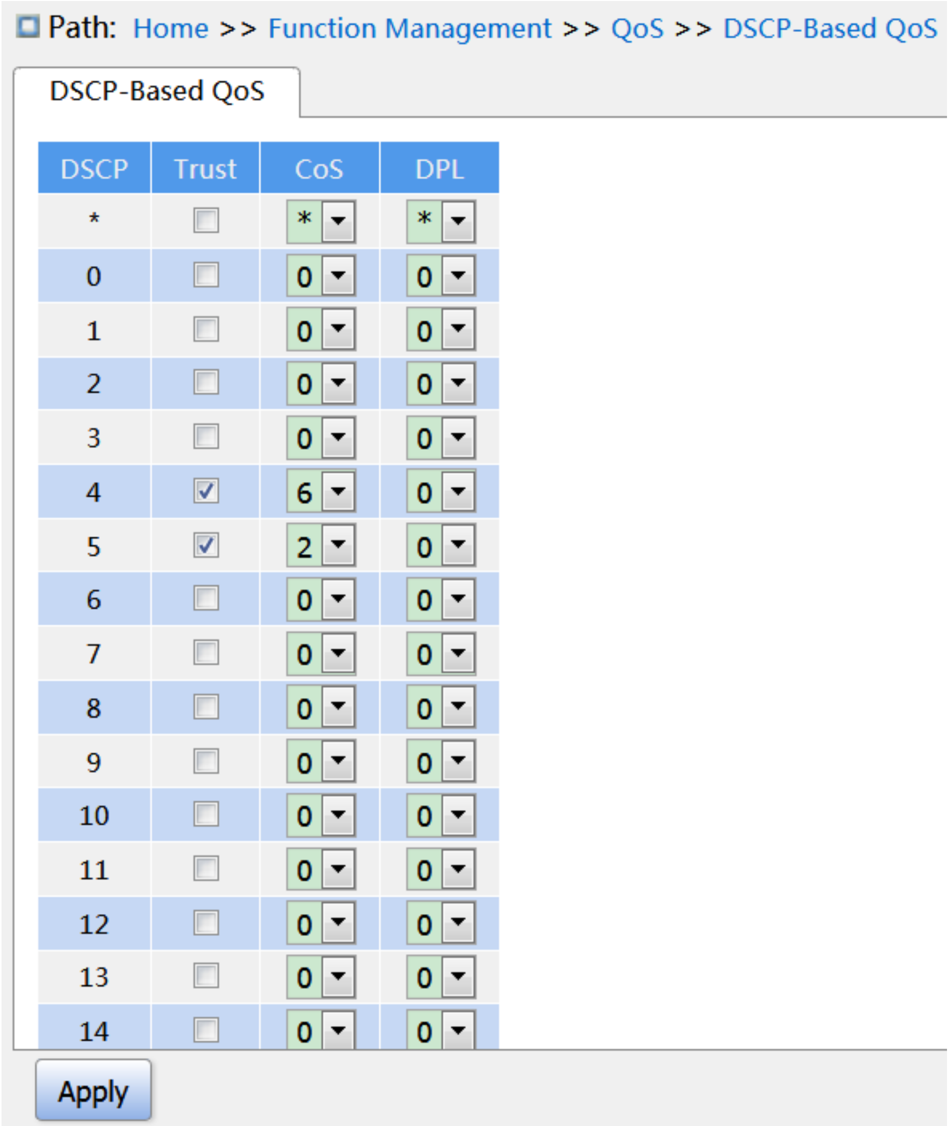


Figure 275 Configure queue mapping mode based on DSCP

Trust

Configuration options: Enable/disable

Default configuration: Disable

Function: whether trust the DSCP value.

Caution:

The queue mapping mode based on DSCP only applies to the DSCP value of the message received by the port as trust value.

COS

Configuration range: 0~7

Default configuration: 0

Function: Configure DSCP to CoS mapping.

Description: The CoS value determines the stored queue of message, CoS value 0 ~ 7 corresponds to the queue 0~7 in turn. When a message with a DSCP value as trust enters the switch, the switch assigns CoS value to the message according to DSCP to CoS mapping

---

Caution:

When the ingress port enables translate, the switch assigns the CoS value according to the translated DSCP value; otherwise, the switch assigns the CoS value according to the original DSCP value in the message.

DPL

Configuration range: 0~1

Default configuration: 0

Function: Configure DSCP to DPL mapping

Description: After the message with DSCP value as trust enters the switch, the switch assigns the DPL value to the message according to DSCP to DPL mapping.

7. Configure DSCP translate and rewrite, as shown below.

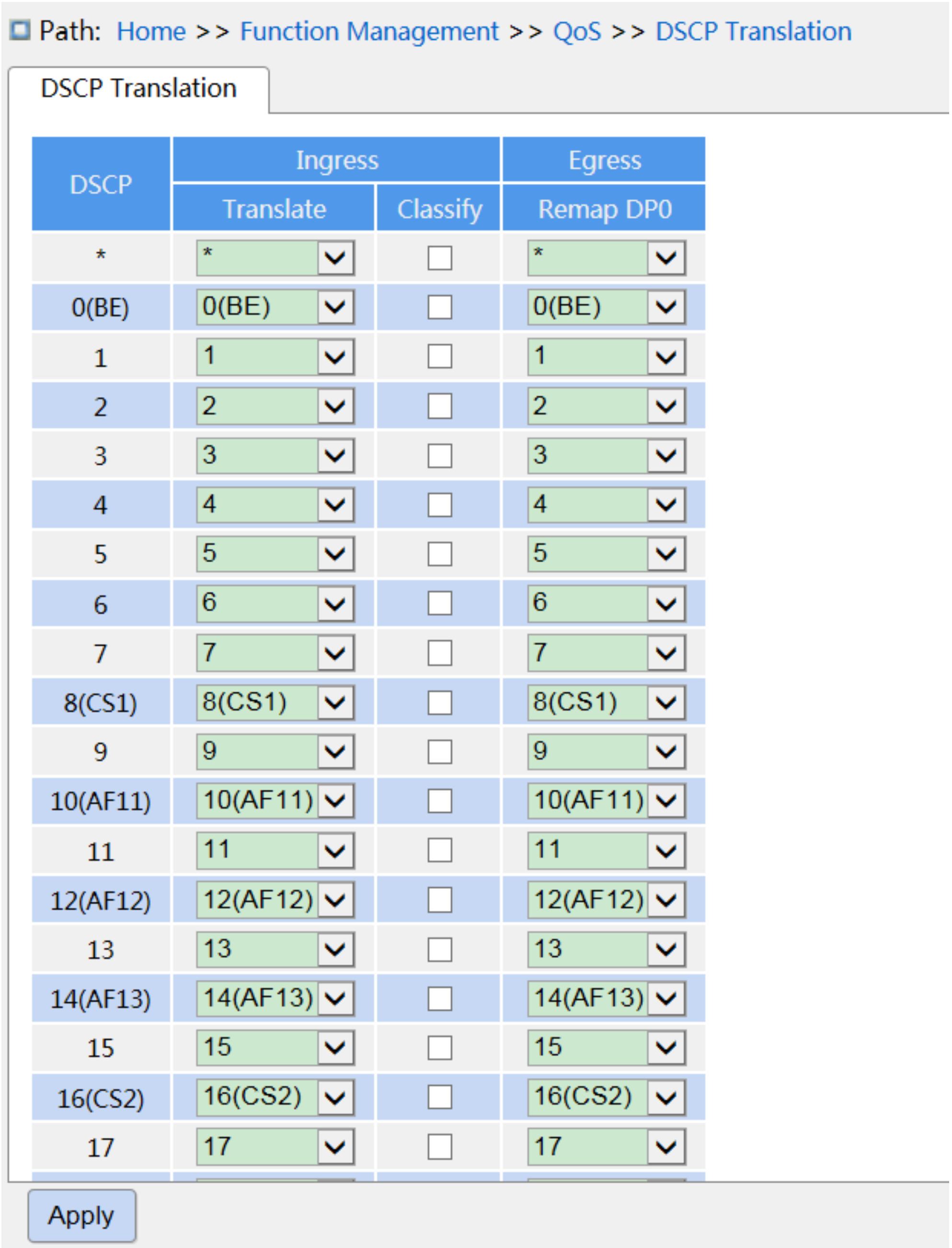


Figure 276 Configure DSCP translate and rewrite

Translate

Configuration range: 0~63

Function: configure translation table of dscp value.

Classify

Configuration options: Enable/disable

Default configuration: Disable

Function: Configure “Classify” in Figure 274 to Selected, this parameter configures the selected DSCP value.

Caution:

When the ingress port enable “translate”, the selected value is the translated value; Otherwise, the selected DSCP value is the original DHCP value in the message.

Remap DP0

Configuraton range: 0~63

Function: Configure（DSCP，DPL）to DSCP mapping.

8. Configure DSCP Classification, as shown below.

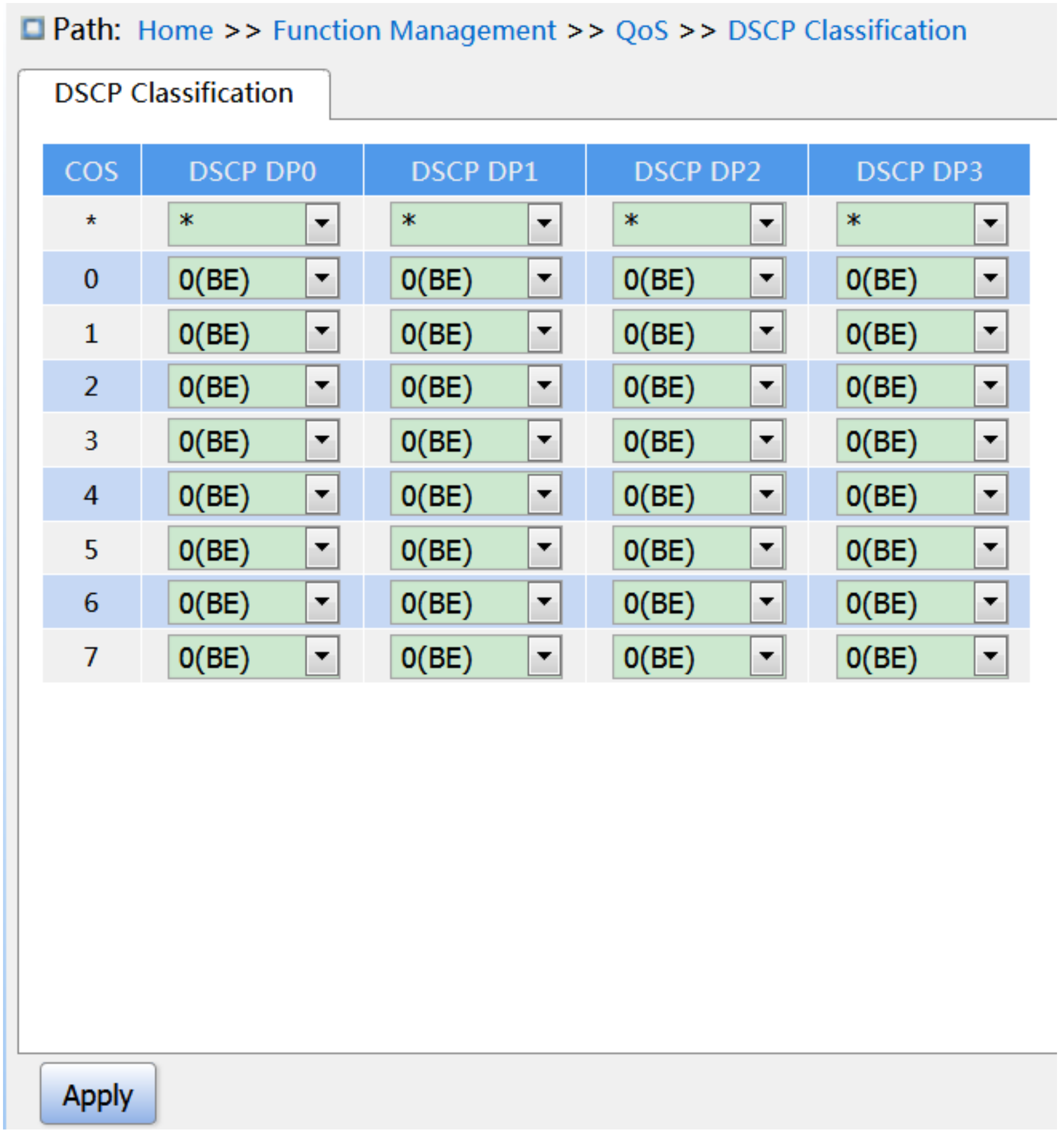


Figure 277 Configure DSCP Classification

DSCP DP0/DSCP DP1

Configuraton range: 0~63

Function: Configure（CoS，DPL） to DSCP mapping. QoS classifition is equal to the CoS value, which determines the storage queue of the message, CoS value corresponds to the queue 0 ~ 7 in turn.

9. Configure QCL table items, as shown below.

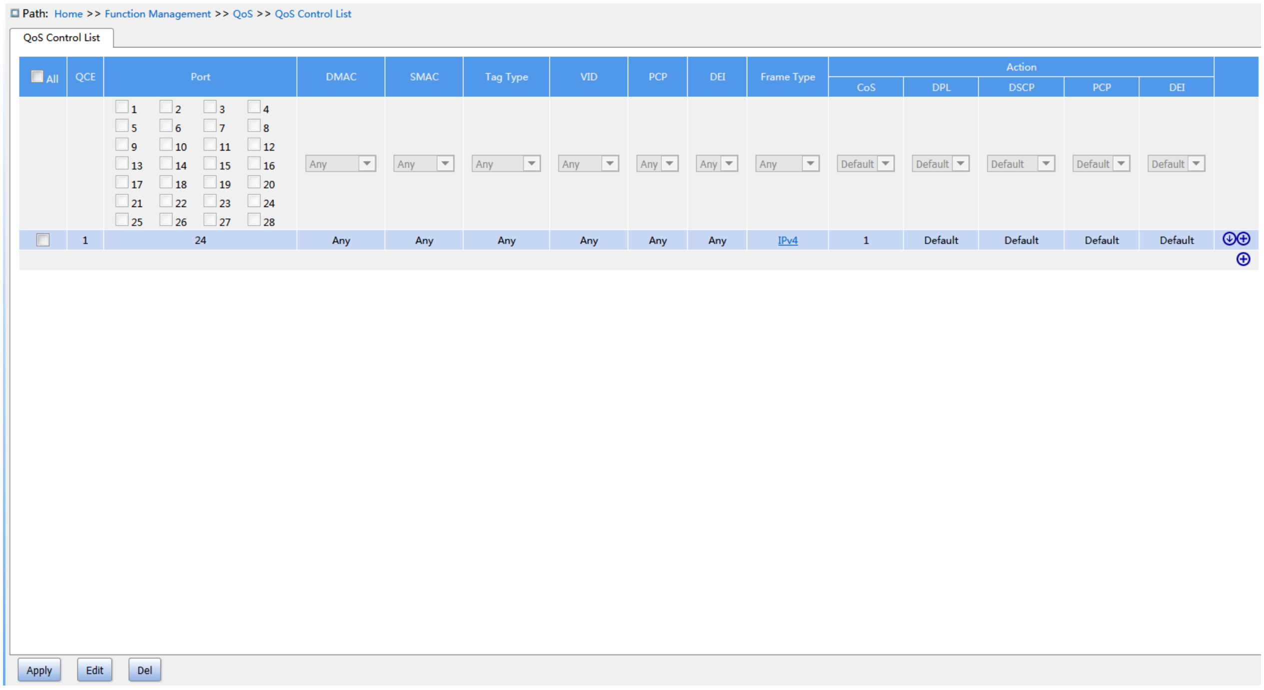


Figure 278 Configure QCL table

The queue mapping of messages is realized by matching QCL table, each QCL table item has several QCL conditions, these conditions are the relation of " and “, and the message received by the member port only meet all conditions then it can be as match QCL table. There is no dependency between each QCL table.

When there are multi QCL table items, the device compares the message to the QCL table items one by one (from top to bottom order in the table), once the message finds the matching first QCL table item, an action is performed.

Click<⊕>button, create a QCL table item; check one table item, click <Edit> button, edit current table item; check one table item, click <Del>button, delete current table item.

QCE is QCLtable ID number, sequentially numbered according to create table order.

Port

Function: Select the active port of the current QCL table item.

➢ Configure QCL table parameters, as shown below.

DMAC

Configuration options: Any/ Unicast/ Multicast / Broadcast

Default configuration: Any

Function: configure condition parameter— destination MAC address, when the destination MAC address in the message received by the member port satisfies the parameter configuration, the condition matches successfully.

SMAC

Configuration options: Any/ Specific

Default configuration: Any

Function: configure condition parameter—source MAC address, select Specific, need to configure a MAC address, when the source MAC address in the message received by the member port satisfies the parameter configuration, the condition matches successfully.

Tag

Configuration options: Any/ Untagged/ Tagged

Any

Function: configure condition parameter –Tag. When the message received by the member port satisfies the parameter configuration, the condition matches successfully.

VID

Configuration options: Configuration options:Any/ Specific（1~4093）/ Range（1~4093）

Default configuration: Any

Function: configure condition parameter --VID，select Specific, need to configure VID value; Select Range, need to configure VID range. when the VID in the message received by the member port satisfies the parameter configuration, the condition matches successfully. When tag parameter configured as Untagged, the parameter can’t be configured.

PCP

Configuration options: Any/0/1/2/3/4/5/6/7/0-1/2-3/4-5/6-7/0-3/4-7

Default configuration: Any

Function: configure condition parameter –PCP. When the PCP in the message received by the member port satisfies the parameter configuration, the condition matches successfully. When tag parameter configured as Untagged, the parameter can’t be configured.

DEI

Configuration options: Any/0/1

Default configuration: Any

Function: configure condition parameter –DEI. When the DEI in the message received by the member port satisfies the parameter configuration, the condition matches successfully. When tag parameter configured as Untagged, the parameter can't be configured.

Frame Type

Configuration options: Any/ EtherType/ LLC/ SNAP/ IPv4

Default configuration: Any

Function：Select frame type.

Click any QCL frame type field to enter the detail configuration interface.

➢ Configure EtherType frame parameters, as shown below.

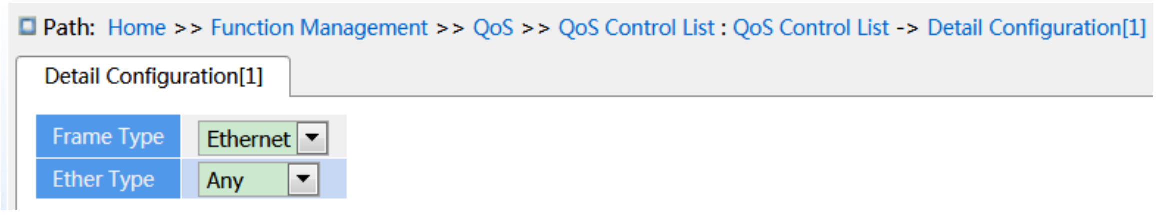


Figure 279 Configure EtherType frame parameters

Ether Type

Configuration options: Any/ Specific（0x600-0x7FF,0x801-0x86DC,0x86DE-0xFFFF）

Default configuration: Any

Function: configure condition parameter –ethernet type, select Specific, need to configure ethernet type value. When the ethernet frame received by the member port satisfies the parameter configuration, the condition matches successfully.

➢ Configure LLC frame parameters, as shown below.

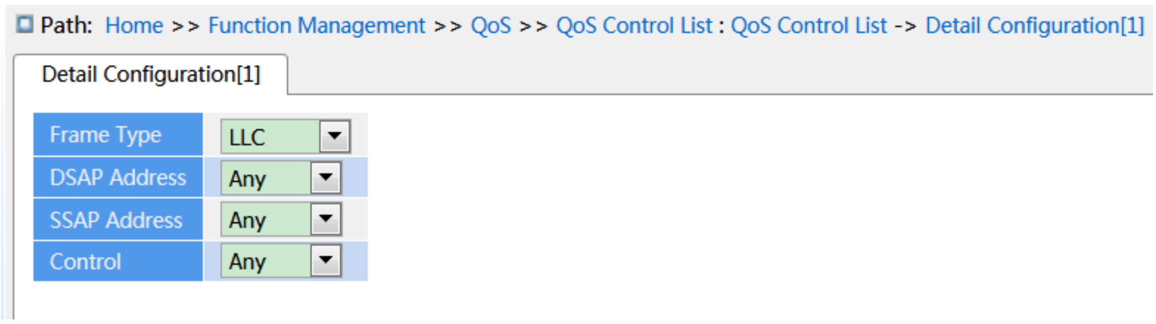


Figure 280 Configure LLC frame parameters

DSAP Address/SSAP Address/Control

Configuration options: Any/Specific（0x00~0xFF）

Default configuration: Any

Function: configure condition parameter –LLC frame parameters, select Specific, need to configure detail value. When the LLC frame received by the member port satisfies the parameter configuration, the condition matches successfully.

➢ Configure SNAP frame parameters, as shown below.

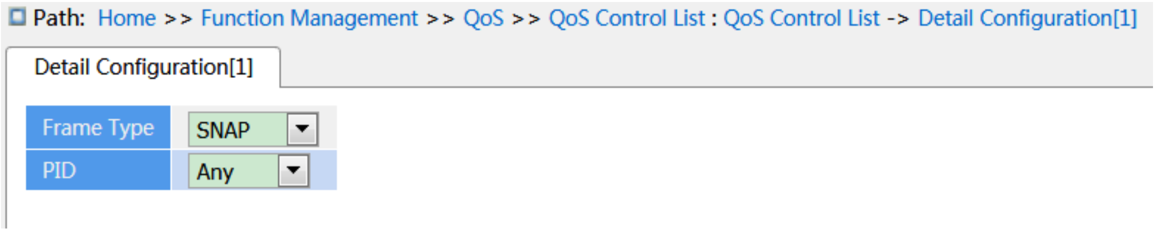


Figure 281 Configure SNAP frame parameters

PID

Configuration options: Any/ Specific（0x0000~0xFFFF）

Default configuration: Any

Function: configure condition parameter –SNAP frame parameters, select Specific, need to configure PID value. When the PID in the SNAP frame received by the member port satisfies the parameter configuration, the condition matches successfully.

➢Configure IPv4 frame parameters, as shown below.

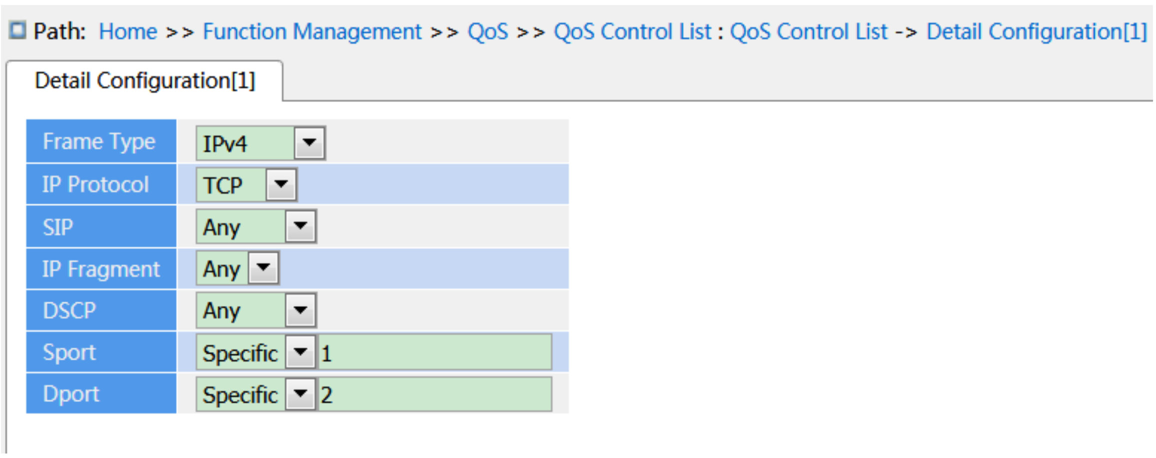


Figure 282 Configure IPv4 frame parameters

Protocol

Configuration options: Any/ UDP/ TCP/ Other（0~255）

Default configuration: Any

Function: configure condition parameter --IPv4 frame protocol type. Select UDP/ TCP, need to configure source and destination port number; Select Other, need to configure protocol number. When the protocol type in the IP frame received by the member port satisfies the parameter configuration, the condition matches successfully.

Sport/ Dport

Configuration options: Any/ Specific（0~65535）/ Range（0~65535）

Default configuration: Any

Function: Configure condition parameter --TCP/ UDP source and destination port number, select Specific, need to configure port number; select Range, need to configure port number range. When the port number in the IP frame received by the member port satisfies the parameter configuration, the condition matches successfully.

SIP

Configuration options: Any/ Specific

Default configuration: Any

Function: Configure condition parameter –source IP address and source IP mark, select Specific, need to configure IP address and mark. When the SIP in the IP frame received by the member port satisfies the parameter configuration, the condition matches successfully.

IP Fragment

Configuration options: Any/ Yes/ No

Default configuration: Any

Function: Configure condition parameter –IP fragement frame. When the Fragment in the IPv4 frame received by the member port satisfies the parameter configuration, the condition matches successfully.

DSCP

Configuration options: Any/ Specific（0~63）/ Range（0~63）

Default configuration: Any

Function: Configure condition parameter –DSCP value, select Specific, need to configure DSCP value; Select Range, need to configure DSCP range. When the DSCP in the IP frame received by the member port satisfies the parameter configuration, the condition matches successfully.

➢ Configure QCL table action, as shown inFigure 278.

CoS

Configuration options: 0~7/ Default

Default configuration: Default

Function: When the frame received by the member port matches the QCL table item, modify the CoS of frame to this configuration value. The value of CoS determines that the stored queue of frame, the CoS value of 0 ~ 7 corresponding to the queue of 0 ~ 7 in turn, default means do not modify the CoS value of frame.

DPL

Configuration options: Default/ 0/ 1

Default configuration: Default

Function: When the frame received by the member port matches the QCL table item, modify the DPL of frame to this configuration value. Default means do not modify the DPL value of frame.

DSCP

Configuration options: Default/ 0~63

Default configuration: Default

Function: When the frame received by the member port matches the QCL table item, modify the DSCP of frame to this configuration value. Default means do not modify the DSCP value of frame.

PCP

Configuration options: Default/ 0~7

Default configuration: Default

Function: When the frame received by the member port matches the QCL table item, modify the PCP of frame to this configuration value. Default means do not modify the PCP value of frame.

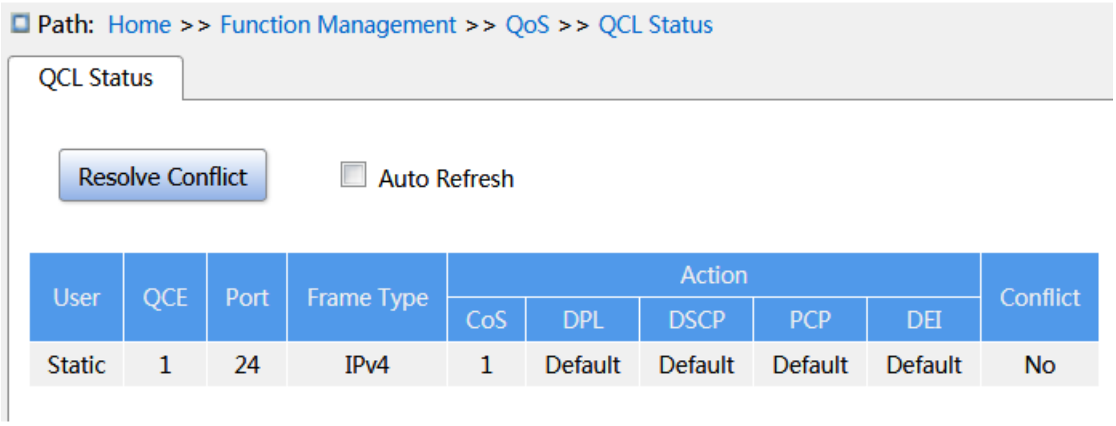
DEI

Configuration options: Default/ 0/ 1

Default configuration: Default

Function: When the frame received by the member port matches the QCL table item, modify the DEI of frame to this configuration value. Default means do not modify the DEI value of frame.

➢ View QCL table item, as shown below.



User	QCE	Port	Frame Type	Action					Conflict
				CoS	DPL	DSCP	PCP	DEI	
Static	1	24	IPv4	1	Default	Default	Default	Default	No

Figure 283 View QCL Table item

Conflict

Display configuration: No/Yes

Function: Display conflict status of QCL table itme. If there are not enough resources to create an QCL table, the table item conflict state is Yes. otherwise is No.

Click <Resolve Conflict > button, releases the required resources for conflicting QCL table items to eliminate conflicts.

10. Configure traffic monitoring based on queue, as shown below.

Figure 284 Configure Queue Policing

Enable

Configuration options: Enable/disable

Default configuration: Disable

Function: Whether enable queue policing, need to configure rate and unit parameters after enable.

Rate, Unit

Configuration range: 25~13128147kbps/ 1~13128Mbps

Default configuration: 500kbps

Function: Limit the rate of the amount of frame received by queue on a port, and drop the frame exceed the limited value.

11. Configure port queue scheduler mode, as shown in Figure 285 and Figure 286.

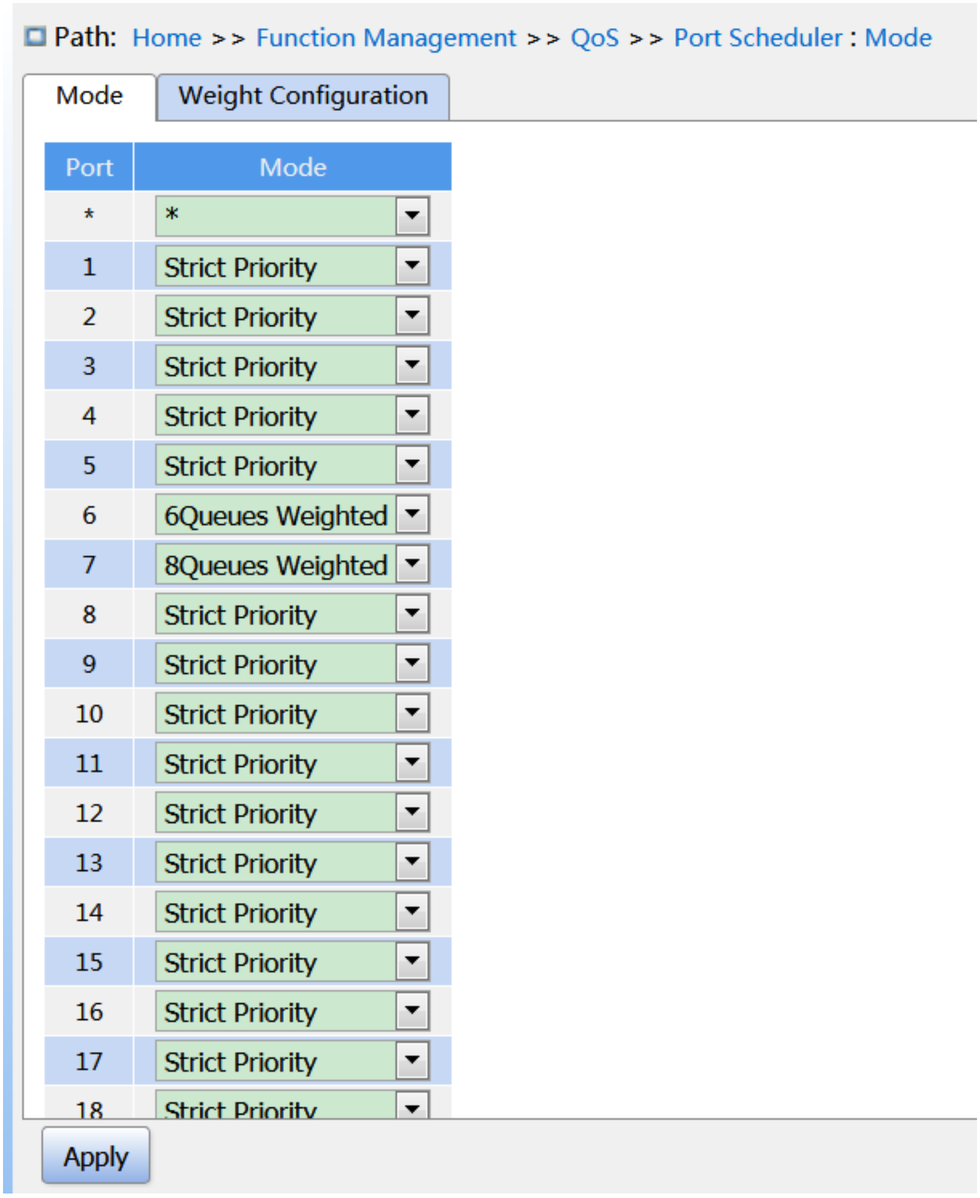
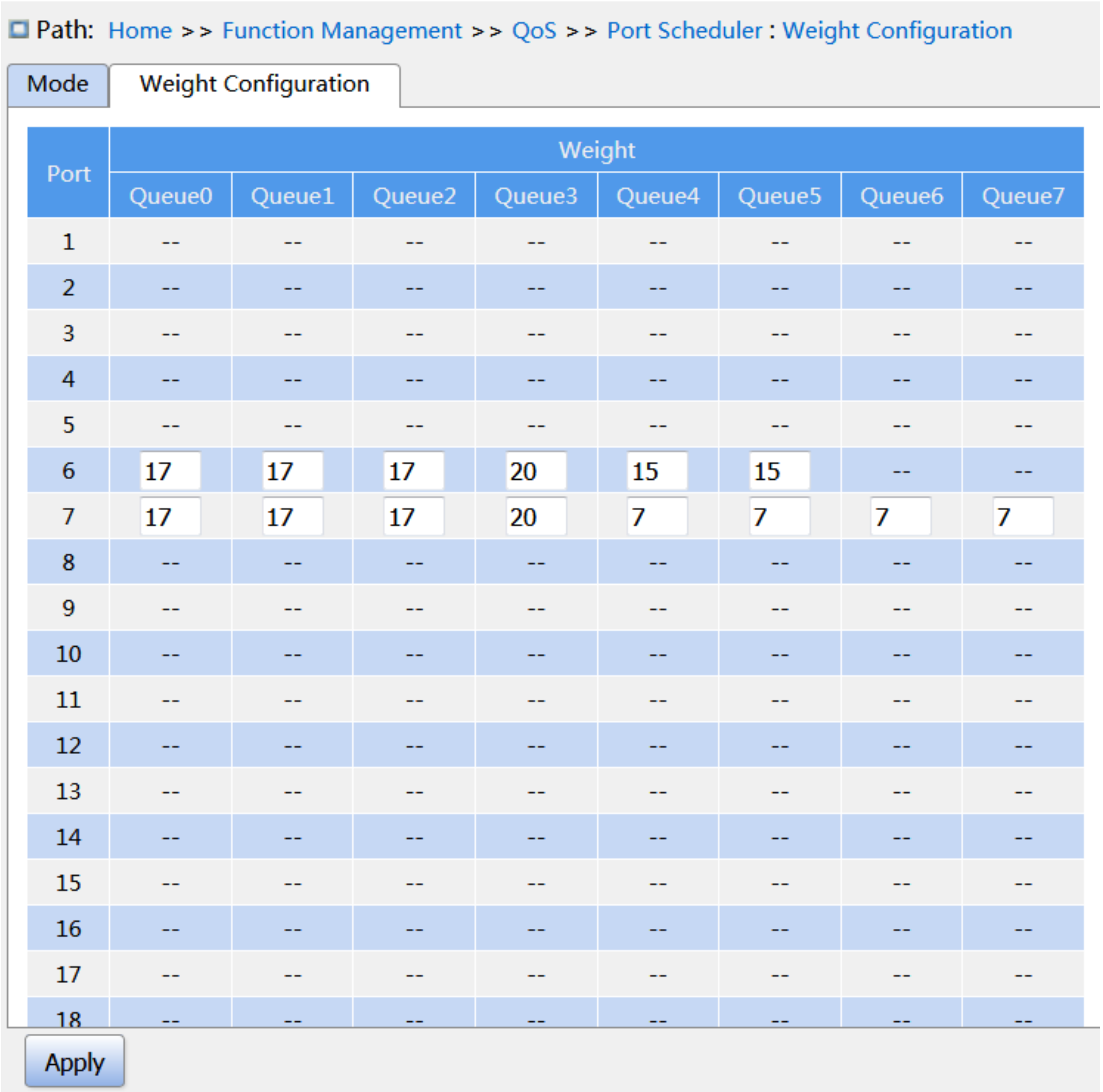


Figure 285 Configure port queue scheduler mode



Port	Weight							
	Queue0	Queue1	Queue2	Queue3	Queue4	Queue5	Queue6	Queue7
1	--	--	--	--	--	--	--	--
2	--	--	--	--	--	--	--	--
3	--	--	--	--	--	--	--	--
4	--	--	--	--	--	--	--	--
5	--	--	--	--	--	--	--	--
6	17	17	17	20	15	15	--	--
7	17	17	17	20	7	7	7	7
8	--	--	--	--	--	--	--	--
9	--	--	--	--	--	--	--	--
10	--	--	--	--	--	--	--	--
11	--	--	--	--	--	--	--	--
12	--	--	--	--	--	--	--	--
13	--	--	--	--	--	--	--	--
14	--	--	--	--	--	--	--	--
15	--	--	--	--	--	--	--	--
16	--	--	--	--	--	--	--	--
17	--	--	--	--	--	--	--	--
18	--	--	--	--	--	--	--	--

Figure 286 Configure port wrr weight of scheduler

Schdduler Mode

Configuration options: Strict Priority /2-8 queues weighted

Default configuration: Strict Priority

Function: Configure port queue scheduler mode.

Weight

Configuration range: 1~100

Default configuration: 17

Function: Configure queue weight.

12. Configure Port Shaping, as shown below.

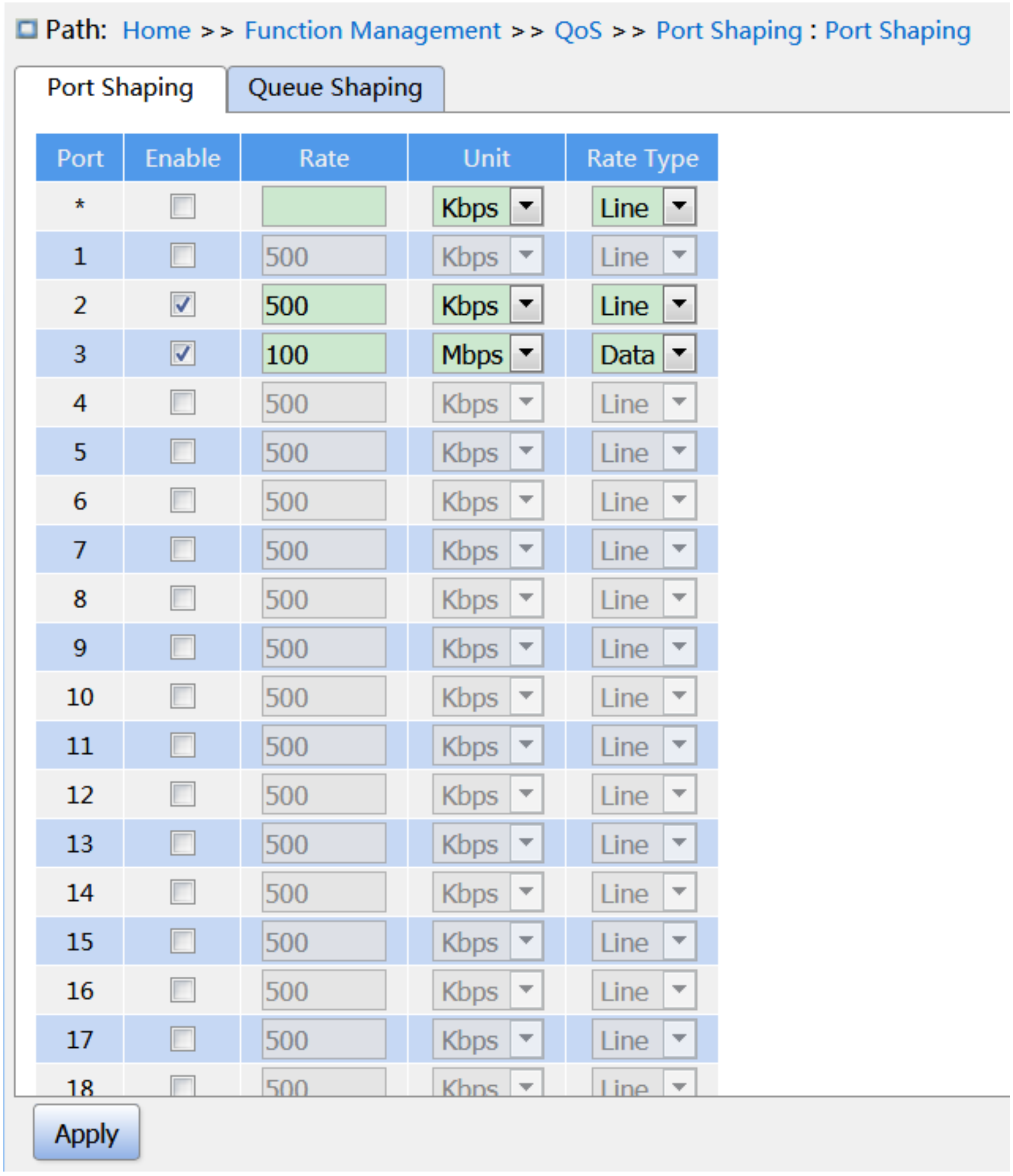


Figure 287 Configure Port Shaping

Enable

Configuration options: Enable/disable

Default configuration: disable

Function: whether enable port shaping. Port traffic shaping through the port rate limit to achieve.

Rate, Unit

Configuration range: 100~13107100kbps/ 1~13107Mbps

Default configuration: 500kbps

Function: Limit the rate of the amount of frame transmitted by port, and drop the frame exceed the limited value.

Rate type

Configuration range: Line/Data

Default configuration: Line

Function: Specify the shaping limit value effective mode. Line refers to limit rate for the total length of a frame, Data refers to limit rate for the effective length of frame.

13. Configure Queue shaping, as shown below.

Figure 288 Configure Queue shaping

Enable

Configuration options: Enable/disable

Default configuration: disable

Function: whether enable queue shaping.

Rate, Unit

Configuration range: 100~13107100kbps/ 1~13107Mbps

Default configuration: 500kbps

Function: Limit the rate of the amount of frame transmitted by queue on port, and drop the frame exceed the limited value.

Rate type

Configuration options: Line/Data

Default configuration: Line

Function: Specify the shaping limit value effective mode. Line refers to limit rate for the total length of a frame, Data refers to limit rate for the effective length of frame.

7.18.4 Typical Configuration Example

As shown in Figure 289, port1~port5 forward packet to port 6. Among them,

The packets received by port1 are Untag, and the packets entering port 1 are mapped to queue 2.

The PCP value of port 2 received packet is 0, DEI value is 1, and the packets entering port 2 are mapped to queue 3.

The DSCP value of port 3 received packet is 4, and the packets entering port 3 are mapped to queue 6.

Port 4 maps all received packets with the source MAC address of 00-00-00-00-00-23 to queue 5 and changes the DSCP value in these packets to 9 for forwarding.

The DSCP value of port 5 received packet is 5, and the packets entering port 5 are mapped to queue 2.

Port 6 adopts SP+WRR scheduling mode.

Configuration process:

1. Set the CoS value of port 1 is 2, as shown in Figure 267.
2. Enable Tag Class of port 2, and map (PCP=0, DEI=1) to CoS=3, as shown in Figure 268.
3. Enable DSCP Based of port 3 and port 5, as shown in Figure 273.
4. Trust DSCP value 4 and 5, and map DSCP value 4 to queue 6 and DSCP value 5 to queue 2, as shown in Figure 275.
5. Congiure a QCL entry for port 4, set SMAC to 00-00-00-00-00-23, entry action parameters: set CoS value to 5 and DSCP value to 9, as shown in Figure 278.
6. Configure port 6 queue scheduling mode to 6 Queues Weighted, queue weight of Q0~Q5 to 20, 40, 40, 20, 20, 20, as shown in Figure 285 and Figure 286.

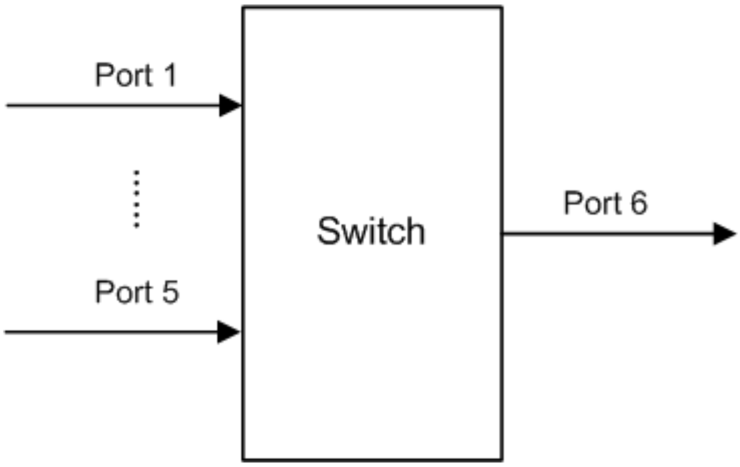


Figure 289 QoS Configuration Example

Port1 and port5 packets enter queue 2, port2 packets enter queue 3, port3 packets enter queue 6, port4 packets enter queue 5.

Queue 6 and queue 7 use the strict priority scheduling mode, and queues 0 through 5 uses the WRR scheduling mode. Data in queue 6 is processed first. When queue 6 is empty, data in queues 0 through 5 is scheduled by weight ratio.

The queue weight are 20, 40, 40, 20, 20, 20. So the bandwidth proportion allocated to the packets in ingress queue 2 is 40/（20+40+40+20+20+20）=25%, that allocated to the packets in ingress queue 3 is 20/（20+40+40+20+20+20）=13%, and that allocated to the packets in ingress queue 5 is 20/（20+40+40+20+20+20）=13%. Among them, port 1 and port 5 packets both enter queue 2, so they are forwarded according to the rule of First In, First out (FIFO), but the total bandwidth proportion of port 1 and port 5 must be 25%.

7.19 VRRP

Note：

Routers in this chapter refer to Layer-3 switches.

7.19.1 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.

Note: In the series switches, only SICOM3024GS-L3G supports VRRP.

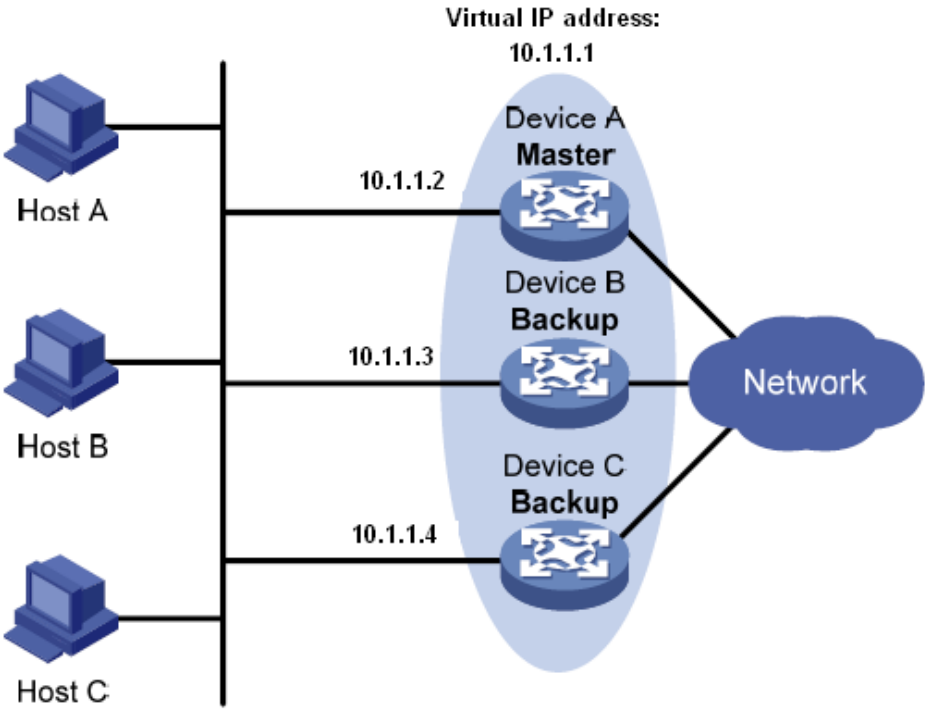


Figure 290 VRRP

As shown in Figure 290, 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.

7.19.2 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.

7.19.3 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.

7.19.4 Web Configuration

1. Create/Edit/Delete a VRRP backup group, as shown below.

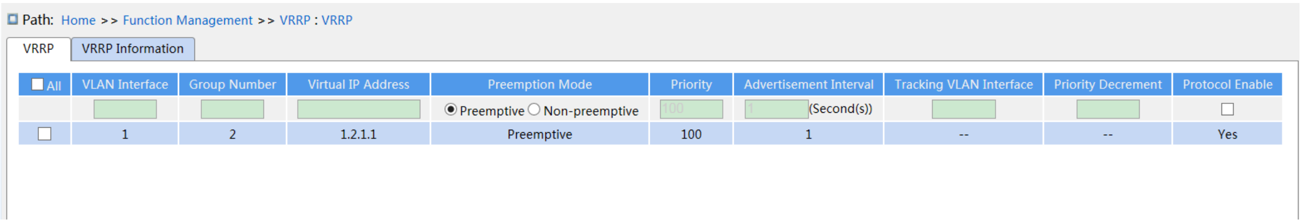


Figure 291 Create a VRRP backup group

VLAN Interface

Configuration range: 0~4093

Function: Configure the VLAN interface of the specified virtual router backup group.

Group Number

Configuration Range: 1~255

Function: Set the ID of the VRRP group.

Virtual IP Address

Configuration 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.

Preemption Mode

Configuration options: Preemptive/ Non-preemptive

Function: **Preemption** mode: If the backup router finds that its priority is higher than that of the current master, it will send VRRP advertisements to the backup group, causing the new master to be re-elected in the backup group.

Non-preemptive mode: As long as the master router does not fail, the backup router will not become the master router even if it is configured with a higher priority.

Priority

Configuration Range: 1-254

Default configuration: 100(For non-IP address owners)

Function: Configure the priority of the router in the VRRP group. The router with the highest priority is elected as the master router.

Advertisement Interval

Configuration Range: 1s-255s

Default configuration: 1s

Function: Set the interval for the master router to send VRRP advertisements.

CAUTION

Caution:

The interval of advertising packets of the members in the same virtual router backup group must be the same.

Tracking VLAN Interface

Configuration Range: 1-4093

Function: Select the monitored VLAN interface.

Priority Decrement

Configuration Range: 1-255

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.

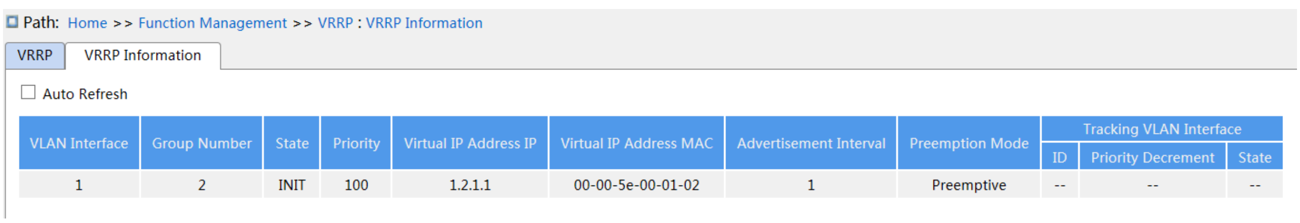
➢The priority of the master router after decrement must be smaller than that of a backup router.

Protocol Enable

Configuration options: Enable/ Disable

Function: Whether to enable the virtual router backup group function.

2. VRRP information display page, as shown below.



VLAN Interface	Group Number	State	Priority	Virtual IP Address IP	Virtual IP Address MAC	Advertisement Interval	Preemption Mode	Tracking VLAN Interface		
								ID	Priority Decrement	State
1	2	INIT	100	1.2.1.1	00-00-5e-00-01-02	1	Preemptive	--	--	--

Figure 292 VRRP information

7.19.5 Typical Configuration Example

As shown below, 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.

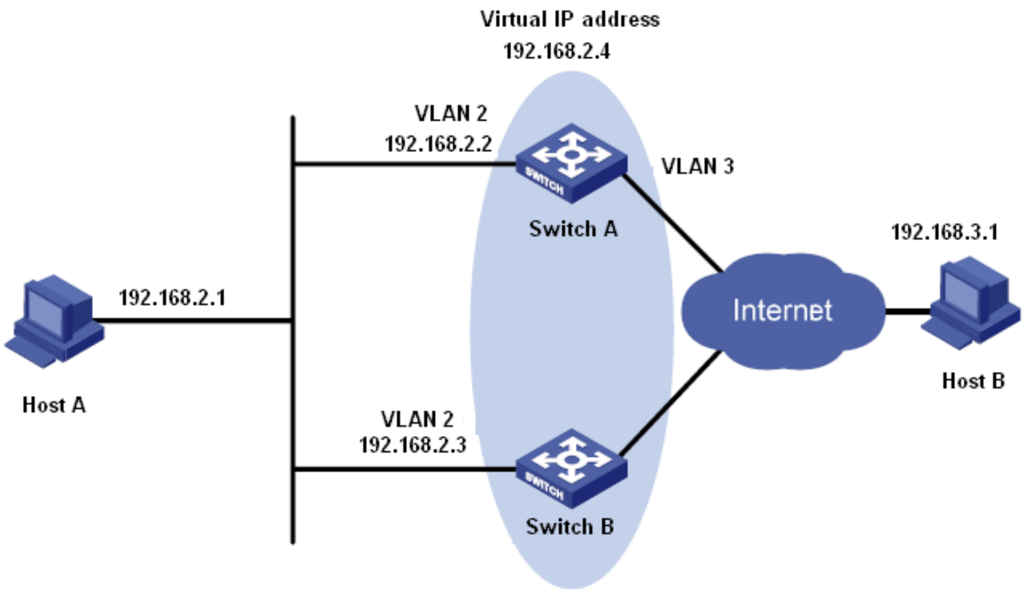


Figure 293 VRRP Typical Configuration Example

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 291.

3. Set the virtual IP address of VRRP group 1 to 192.168.2.4, and router type to Backup, as shown in Figure 291.

4. Configure VLAN 2 as the Layer-3 interface for VRRP group 1, as shown in Figure 291.

5. Set the priority of Switch A in the VRRP group to 110, and preemptive mode to false, as shown in Figure 291.

6. Configure VLAN 3 as the monitored interface and set the priority decrement to 30, as shown in Figure 291.

7. Enable VRRP group 1, as shown in Figure 291.

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 291.
3. Set the virtual IP address of VRRP group 1 to 192.168.2.4, and router type to Backup, as shown in Figure 291.
4. Configure VLAN 2 as the Layer-3 interface for VRRP group 1, as shown in Figure 291.
5. Set the priority of Switch B in the VRRP group to 100, and preemptive mode to false, as shown in Figure 291.
6. Enable VRRP group 1, as shown in Figure 291.

8 Diagnosis

8.1 Log

8.1.1 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.

Log contains information about alarms, broadcast storm, reboot, memory, and information about users' operations.

8.1.2 Web Configuration

1. Configure system log, as shown below.

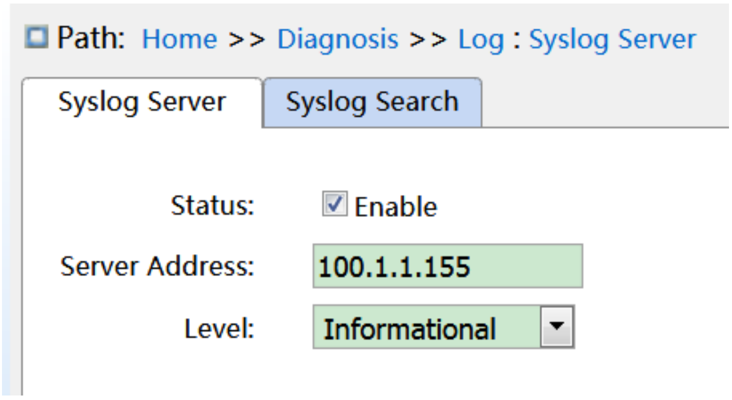


Figure 294 Configure Syslog Server

Status

Configuration options: Enable/disable

Default configuration: Disable

Function: whether enable syslog server.

Server address

Configuration format: A.B.C.D

Function: configure IP address of syslog server.

Level

Configuration options: Error/Warning/Notice/Information

Default configuration: Information

Function: Select displayed log information level.

2. Syslog search, as shown below.

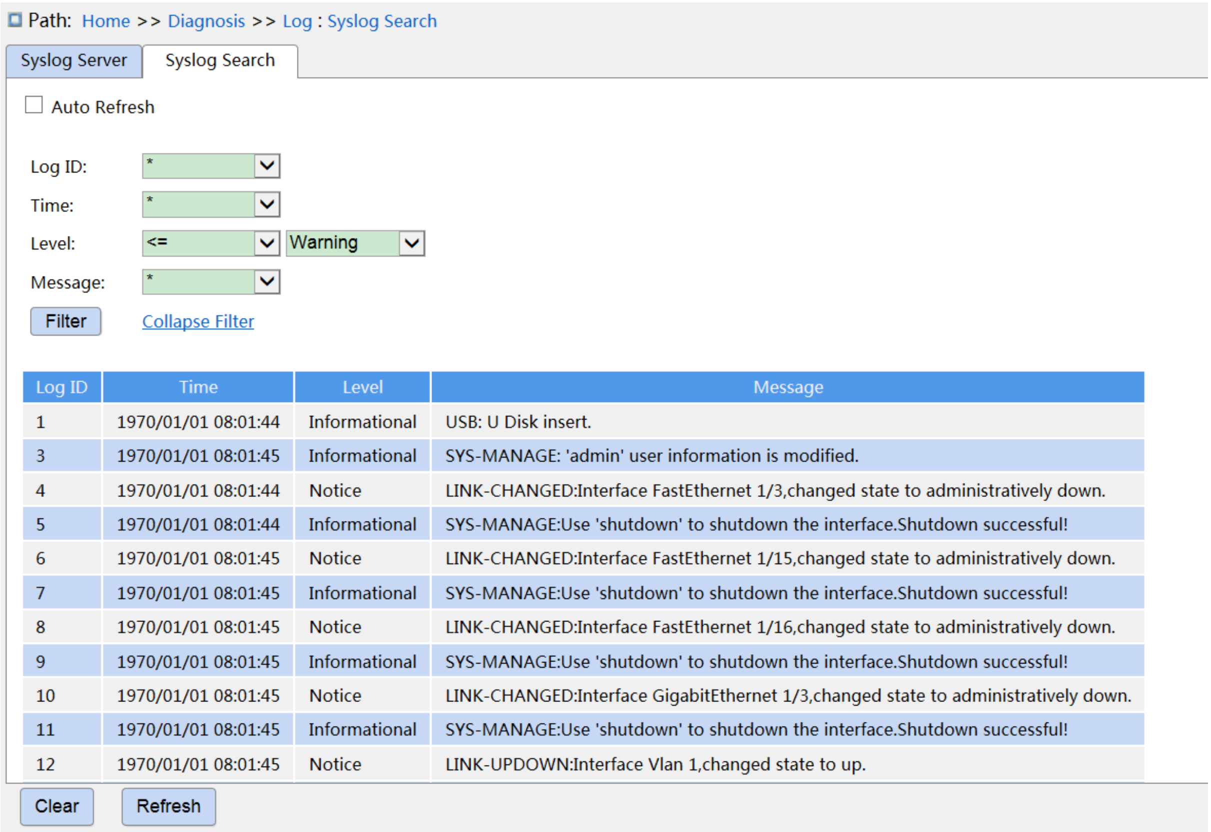


Figure 295 Syslog search

Auto Refresh

Configuration options: check/uncheck

Default configuration: uncheck

Function: whether enable auto refresh.

Log ID

Configuration options: */>=/<=/select range

Default configuration: *

Function: Select filtered Log ID，“*” is all ID log, “>=” is Filter logs greater than or equal to an ID, “<=” is filiter less than or equal to an ID, “select range” enter an ID range logs manually.

Time

Configuration options: */Start/end/select range

Default configuration: *

Function: Select filtered time range, “*”is all time log, “Start”is the start time of log, “end” is the end time of log, “select range” enter a time range logs manually.

Level

Configuration options: */>=/<=/select range

Default configuration: *

Function: Select filtered level range, “*” is all level log, “>=” is filter logs greater than or equal to a level, “<=” is filter logs less than or equal to a level, “select range” enter a level range logs manually, the levels includes Error, Warning, Notice, Information.

Message

Configuration options: */include/not include

Default configuration: *

Function: Select filtered message, “*” is all logs, “include”include Logs for some fields, ”not include” do not include logs for some fields.

3. Clear logs, as shown below.

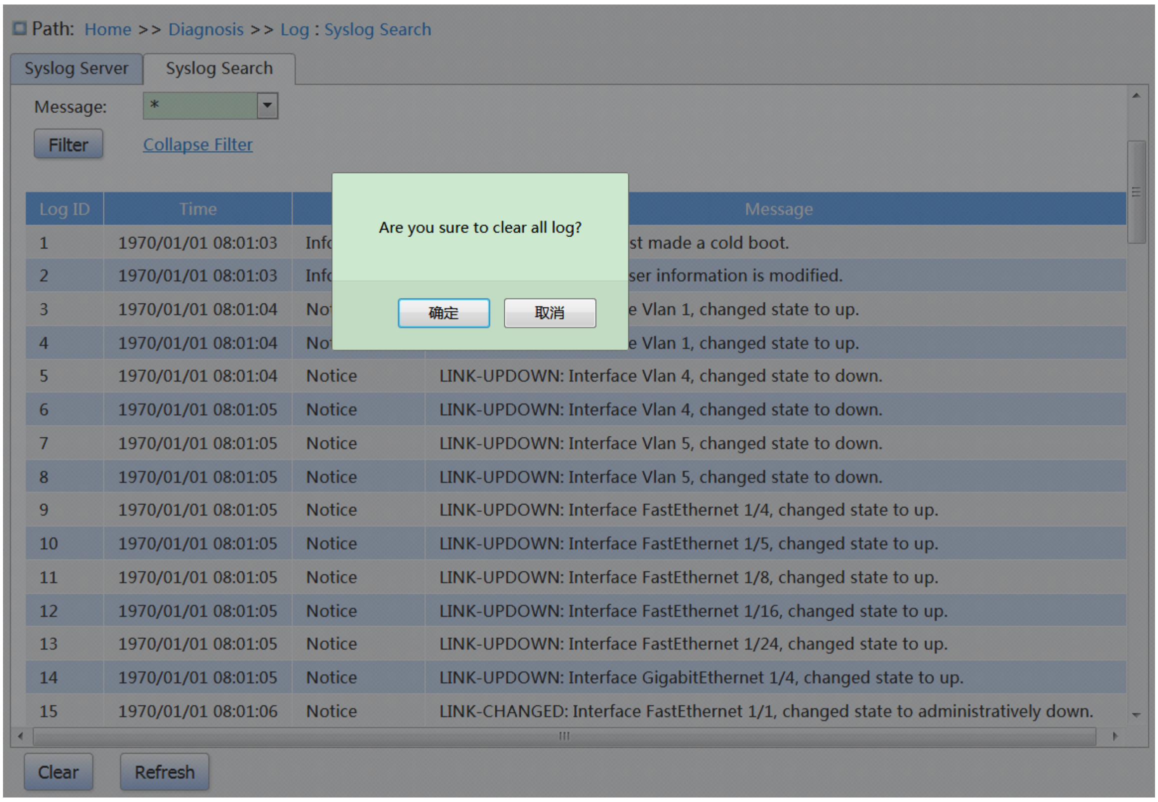


Figure 296 Clear logs

After the query log is finished, click lower left quarter <clear>button, clear logs.

The server of the syslog protocol can choose to install the software supporting syslog server on the PC, such as Tftp32. The log information can be viewed in real time through syslog server, as shown below.

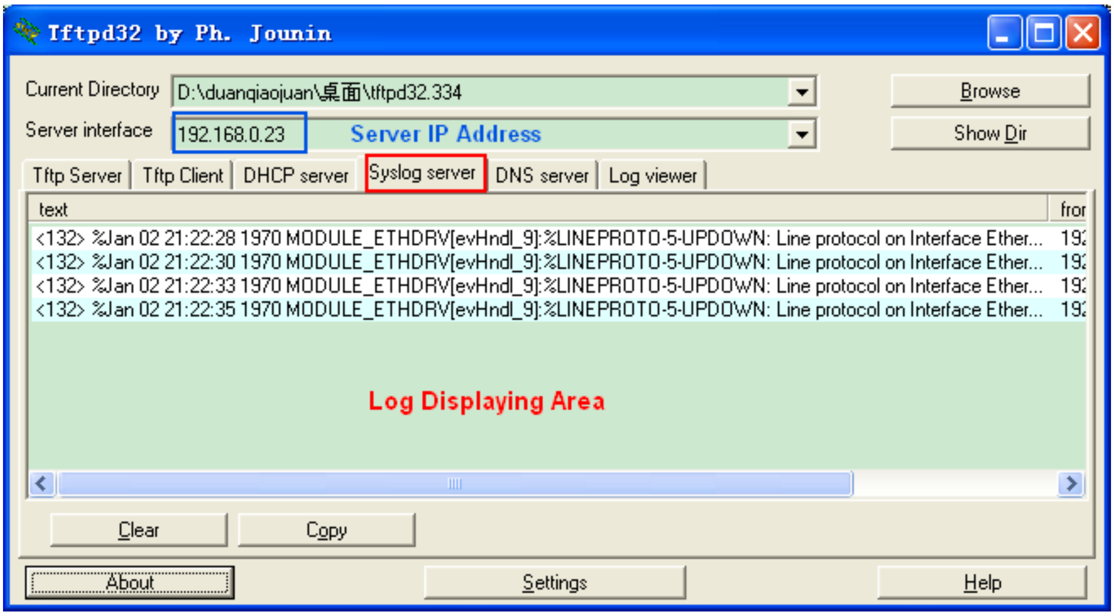


Figure 297 Real-time upload log information

8.2 Port Mirror

8.2.1 Introduction

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

8.2.2 Explanation

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

Multiple source ports can be either in the same VLAN, or in different VLANs. Mirrorsource 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:

The dynamic MAC address learning must be disabled on a destination port.

8.2.3 Web Configuration

1. Cofigure port mirror function, as shown below.

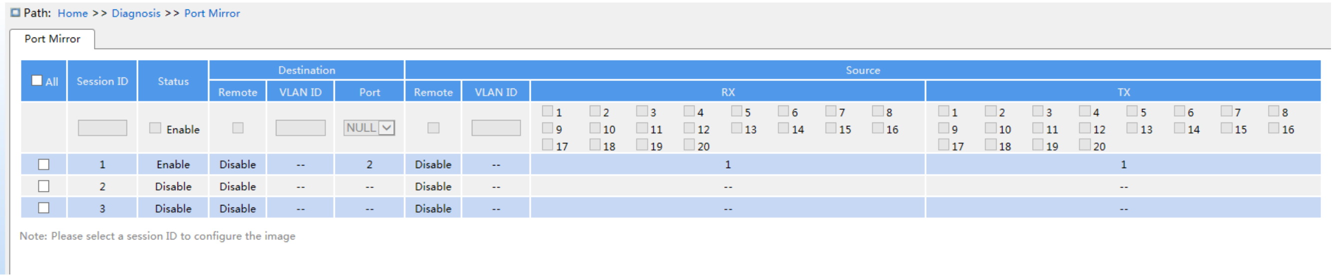


Figure 298 Cofigure Port Mirror Function

ALL

Configuration options: Check/uncheck

Default configuration: Uncheck

Function: Check this mirrored group to edit and modify.

Status

Configuration options: Enable/disable

Function: whether enable port mirror.

Destination Port

Configuration options: NULL/port number

Default configuration: NULL

Function: Select the mirror destination port , only one mirror destination port .

Rx

Configuration options: Enable/disable

Default configuration: Disable

Function: Whether to mirror frames received from the source port.

Tx

Configuration options: Enable/disable

Default configuration: Disable

Function: Whether to mirror frames trasnmitted from the source port.

2. Configure Remote Mirror, as shown below.

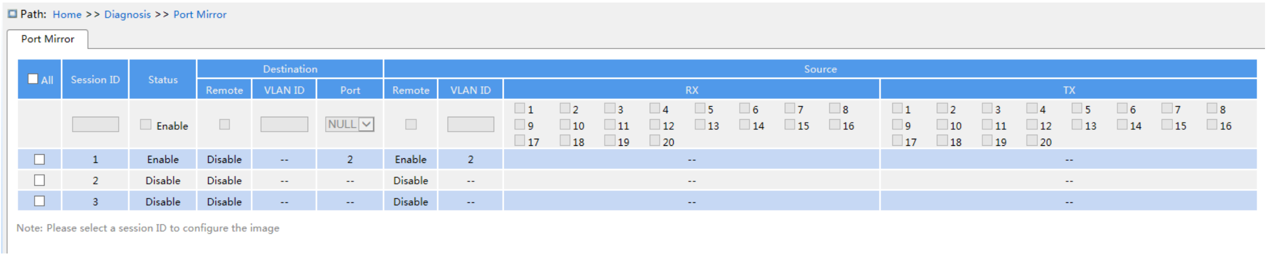


Figure 299 Configure Remote Mirror

All

Configuration options: Check/uncheck

Default configuration: Uncheck

Function: Check this mirrored group to edit and modify.

Status

Configuration options: Enable/disable

Function: whether enable port mirror.

Destination Remote

Configuration options: Enable/disable

Default configuration: Disable

Function: Whether enable destination remote mirror, desination and source remote cannot be enabled at the same time.

Destination VLAN ID

Configuration range: 1~4093

Function: Configure VLAN ID of destination remote mirror.

Destination Port

Configuration options: NULL/Port number

Default configuration: NULL

Function: When configuring the destination remote mirror, the destination port is used as the reflection port, and when configuring the source remote mirror, the destination port is the remote mirror destination port.

Source Remote

Configuration options: Enable/disable

Default configuration: Disable

Function: Whether enable source remote mirror, desination and source remote cannot be enabled at the same time.

Source VLAN ID

Configuration range: 1~4093

Function: Configure VLAN ID of source remote mirror.

Source Port

Configuration options: Disable/RX/TX

Default configuration: Disable

Function: When configuring the destination remote mirror, configrure the remote mirror source port if mirror the receiving or sending frame, and when the source remote image is configured, the source port cannot be configured.

8.2.4 Typical Configuration Example

As shown in Figure 300, the mirror destination port is port 2 and the mirror source port is port 1. Both transmitted and received packets on port 1 are mirrored to port 2.

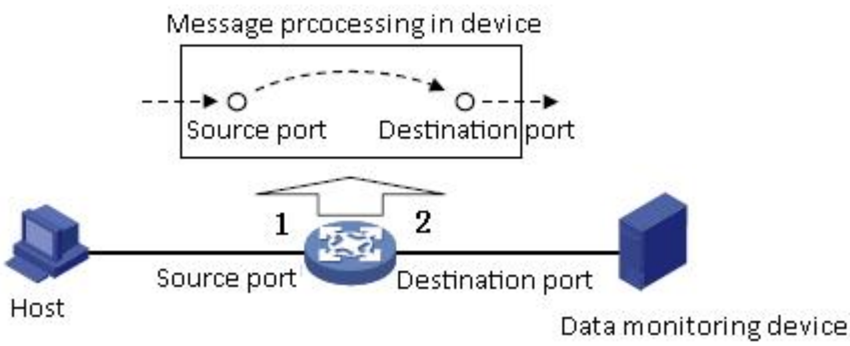


Figure 300 Port Mirror Example

Configuration process:

1. Enable port mirror function, as shown in Figure 298.

2. Set port 2 to the mirror destination port, port 1 to the mirror source port and the port mirror mode to both, as shown in Figure 298.

8.3 LLDP

8.3.1 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.

8.3.2 Web Configuration

1. Configure LLDP, as shown below.

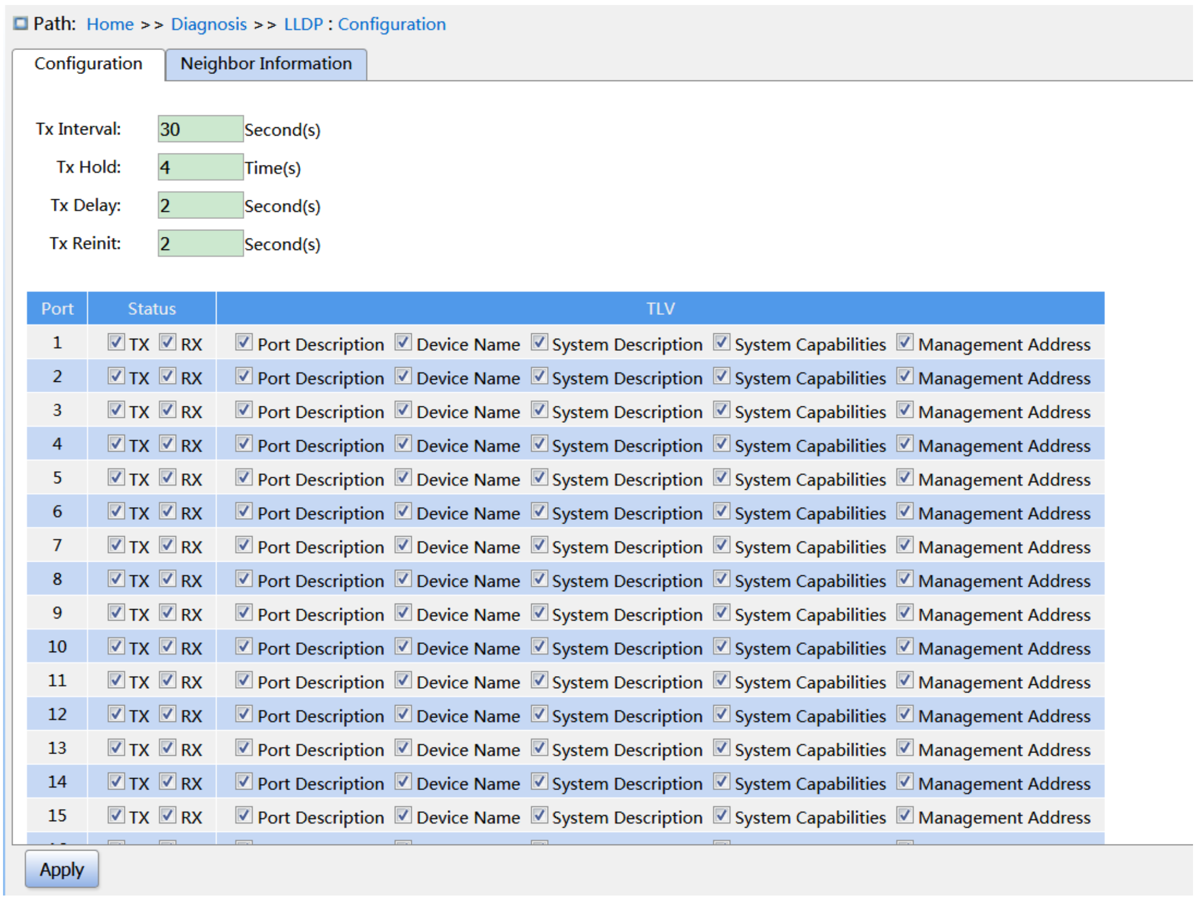


Figure 301 Configure LLDP

Tx Interval

Configuration range: 5~32768s

Default configuration: 30s

Function: Configutr the time interval for sending LLDP packets.

Tx Hold

Configuration range: 2~10 times

Default configuration: 4 times

Function: Set the number of Tx holding times. Effective duration of an LLDP packet = Tx Interval x Tx Hold.

Tx Delay

Configuration range: 1~8192s

Default configuration: 2s

Function: Set the transmission interval between a new LLDP packet and the previous LLDP packet after configuration information is changed. The value of Tx Delay cannot be larger than 1/4 of the value of Tx Interval.

Tx Reinit

Configuration range: 1~10s

Default configuration: 2s

Function: After LLDP is disabled on a port or a switch is restarted, the switch sends an LLDP shutdown frame to a neighboring node to announce that the previous LLDP packet is invalid. Tx Reinit refers to the interval between transmission of the LLDP shutdown frame and re-initialization of an LLDP packet.

Status

Configuration options:Disable/TX/RX/TX&RX

Default configuration: TX&RX

Function: Configure the LLDP packet mode. Enabling TX&RX mode means that the switch sends both LLDP packets and also receives and identifies LLDP packets; Disable mode means that the switch neither sends LLDP packets nor receives LLDP packets; Only the Rx mode means that the switch only receives and recognizes LLDP packets and does not send LLDP packets; Only the Tx mode means that the switch only sends LLDP packets and does not receive LLDP packets.

Port Descripition

Configuration options: Enabled/Disabled

Default configuration: Enabled

Function: Enable indicates LLDP packets will carry port description.

Device Name

Configuration options: Enabled/Disabled

Default configuration: Enabled

Function: Enable indicates LLDP packets will carry system name.

System Descripition

Configuration options: Enabled/Disabled

Default configuration: Enabled

Function: Enable indicates LLDP packets will carry system description.

Sys Capapability

Configuration options: Enabled/Disabled

Default configuration: Enabled

Function: Enable indicates LLDP packets will carry system capability.

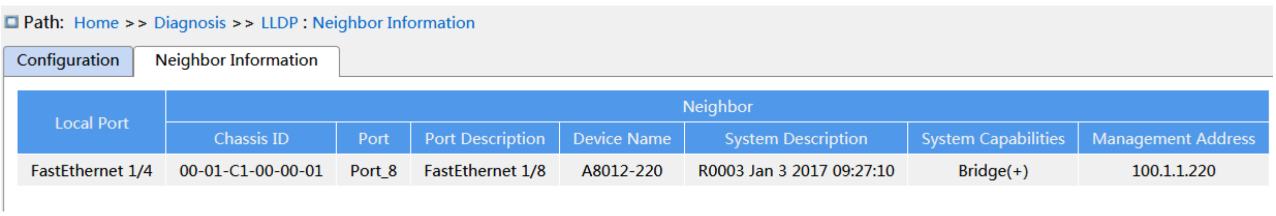
Management Address

Configuration options: Enabled/Disabled

Default configuration: Enabled

Function: Enable indicates LLDP packets will carry management address.

2. View LLDP information, as shown below.



Local Port	Neighbor						
	Chassis ID	Port	Port Description	Device Name	System Description	System Capabilities	Management Address
FastEthernet 1/4	00-01-C1-00-00-01	Port_8	FastEthernet 1/8	A8012-220	R0003 Jan 3 2017 09:27:10	Bridge(+)	100.1.1.220

Figure 302 View LLDP Information

Caution:

To display LLDP information, LLDP must be enabled on the two connected devices.

8.4 Trace Route

Trace route allows us to see the route of IP data packets from one host to another.

1. Configure Trace route, as shown below.

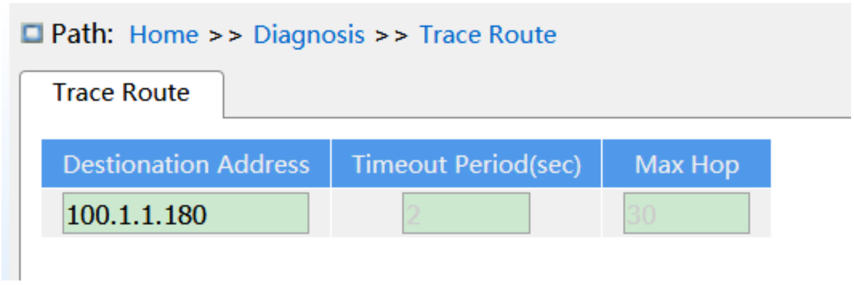


Figure 303 Configure Traceroute

Destination address

Configuration format: A.B.C.D

Function: Configure IP address of destination device.

Timeout Period

Configuration range: 1~10s

Default configuration: 2s

Function: Configure timeout period, If the sending end does not receive a response message from the receiving end within this time, the communication failed.

Max Hop

Default Configuration range: 1~255

Default configuration: 30

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

2. View Traceroute command output information, as shown below.

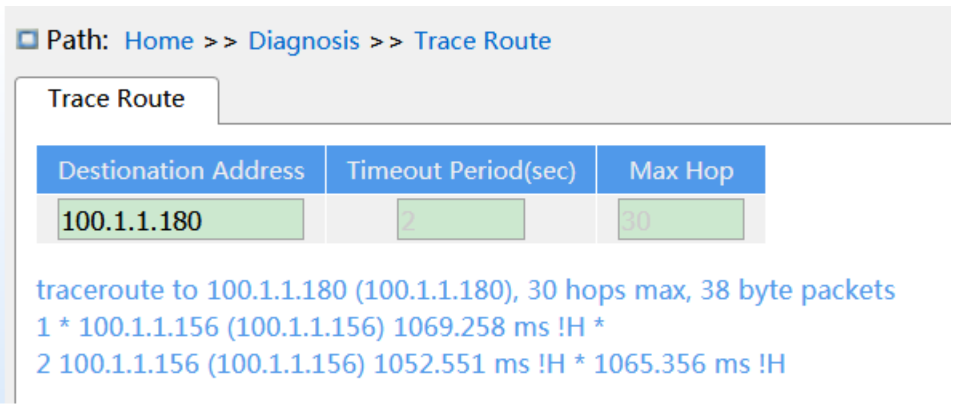


Figure 304 View output

8.5 Ping

Users can run the ping command to check whether the device of a specified address is reachable and whether the network connection is faulty during routine system maintenance.

1. Configure ping command, as shown below.

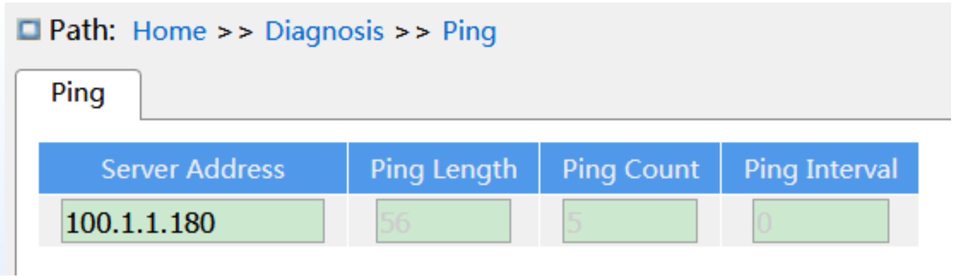


Figure 305 Configure Ping Command

Server Address

Format: A.B.C.D

Description: Input the IP address of the destinate device.

Ping Length

Configuration range: 2~1452 bytes

Default configuration: 56 bytes

Function: Specify the length of an ICMP request (excluding the IP and ICMP packet header) for transmission.

Ping Count

Configuration range: 1~60

Default configuration: 5

Function: Specify the number of times for sending an ICMP request.

Ping Interval

Configuration range: 0~30s

Default configuration: 0s

Function: Specify the interval for sending an ICMP request.

2. View ping output, as shown below.

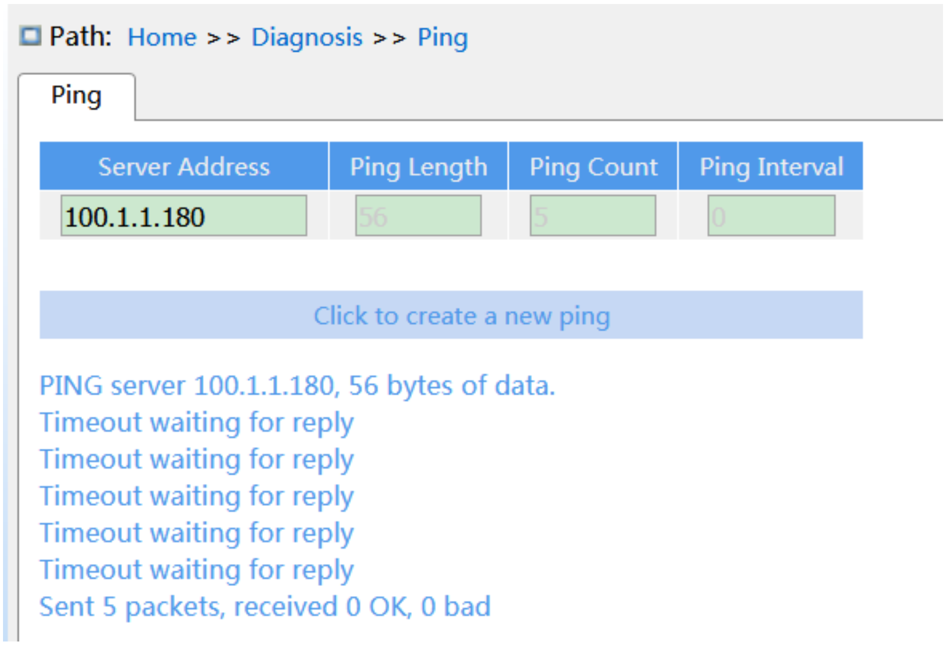


Figure 306 Viewe Ping Output

The output of the ping command includes response of the destination device to each ICMP request packet and packet statistics collected during the running of the ping command.

8.6 IP Source Guard

8.6.1 Introduce

Through the binding function of IP Source Guard, the messages forwarded by the port can be filtered to prevent the illegal messages pass through the port, thus it limits the illegal use of network resource (such as illegal host counterfeit legitimate user IP access the network), improving the security of the port.

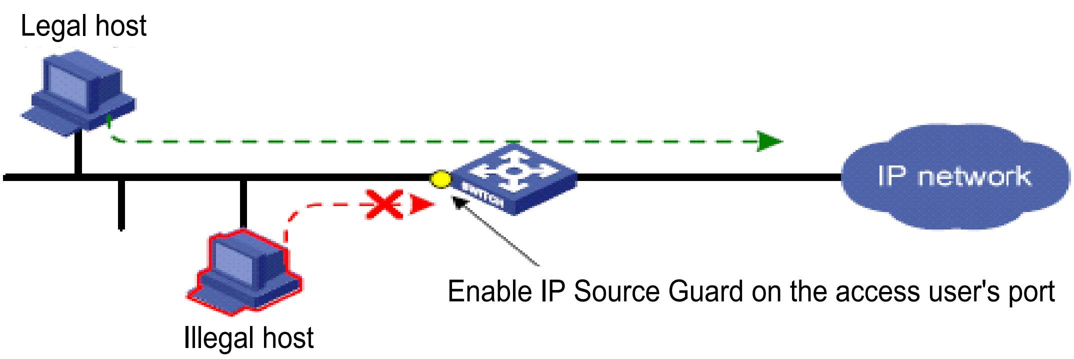


Figure 307 IP Source Guard function diagram

8.6.2 Principle

The configured port with this feature search IP Source Guard binding table after receiving the message, If the feature item in the message matches the recorded feature item in the binding table, the port forwards the message, otherwise, drop the message. Binding function is for the port, one port is binding, only this port is restricted, the other ports are not affected by the binding.

The feature item of IP Source Guard includes: source IP address, source MAC address, and VLAN tage. And it supports the combination of ports with the following features item (binding table item in short):

➢IP、MAC、IP+MAC

➢IP+VLAN、MAC+VLAN、IP+MAC+VLAN

The supported type of binding table items by the port is related to the type of the device, depending on the actual situation of the device.

IP Source Guard is divided into static binding and dynamic binding according to the generation mode of binding table items:

➢**Static binding:** By manually configuring binding table items to control the port, it is suitable for the case that the number of hosts in the local network is less or a host need to bind separately.

➢**Dynamic binding:** The port control function is accomplished by automatically obtaining the binding table items of DHCP Snooping or DHCP Relay, which is suitable for many hosts in local area network and using DHCP to configure dynamic hosts, it can effectively prevent IP address conflicts and embezzlement. The principle is that whenever DHCP assigns a table item to a user, the dynamic binding function adds a binding table item accordingly to allow the user to access the network. If a user sets the IP address privately, the user will not be able to access the network because it does not trigger the DHCP assignment table item, and the dynamic binding function does not add the corresponding access permission rule.

8.6.3 Web Configuration

1. Enable IP Source Guard, as shown below.

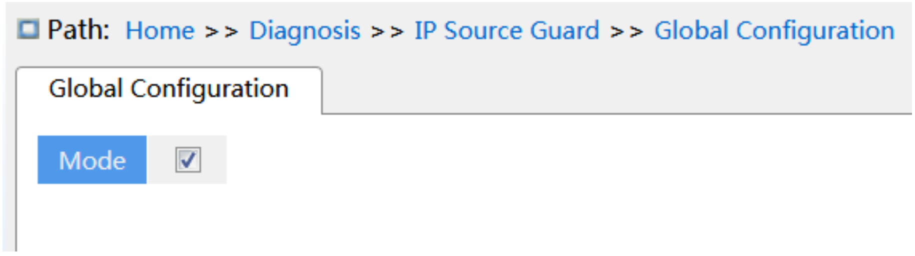


Figure 308 Configure IP Source Guard

Mode

Configuration options: Enable/disable

Default configuration: Disabel

Function: Whether enable global IP Source Guard.

2. Configure Port IP Source Guard, as shown below.

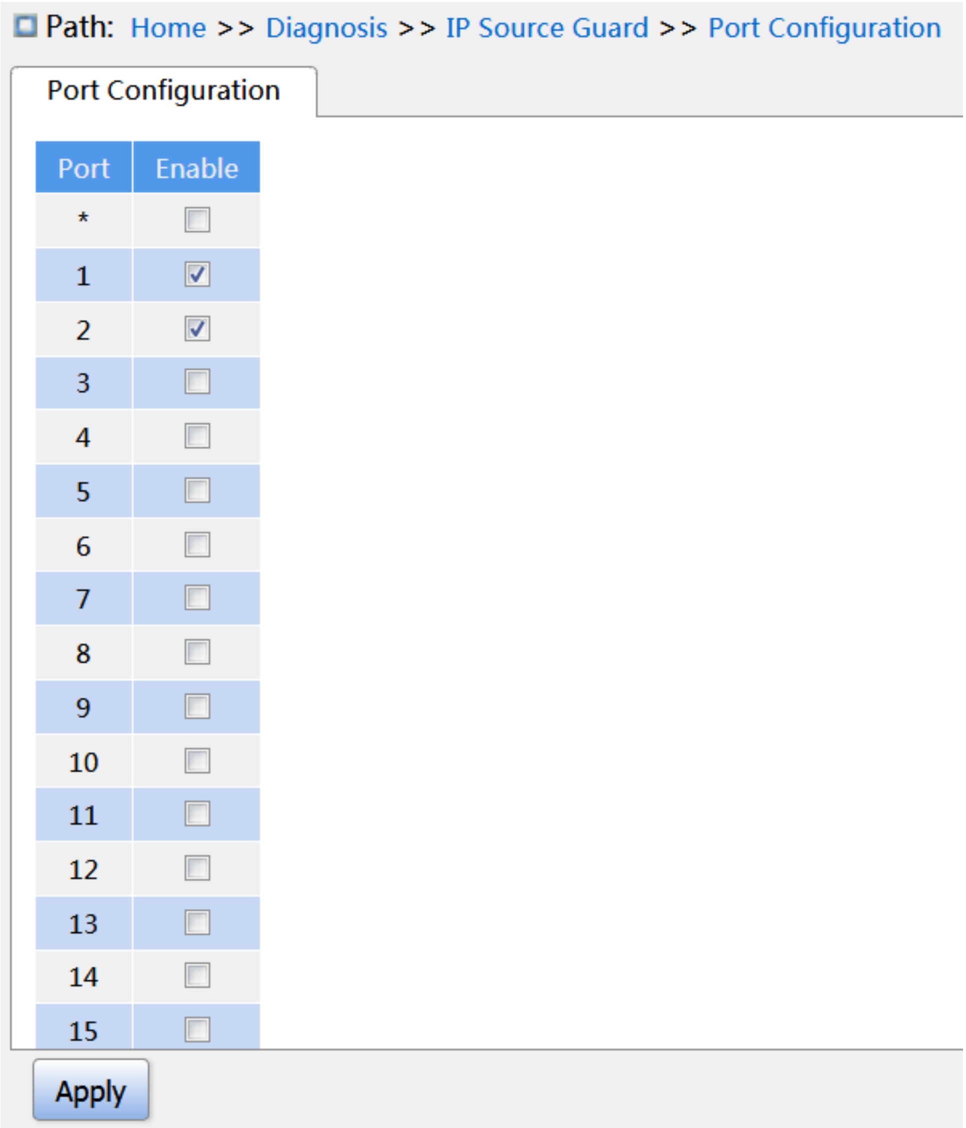


Figure 309 Configure Port IP Source Guard

Enable

Configuration options: Enable/disable

Default configuration: Disable

Function: Whether enable port IP Source Guard.

3. Static Binding Configuration, as shown below.

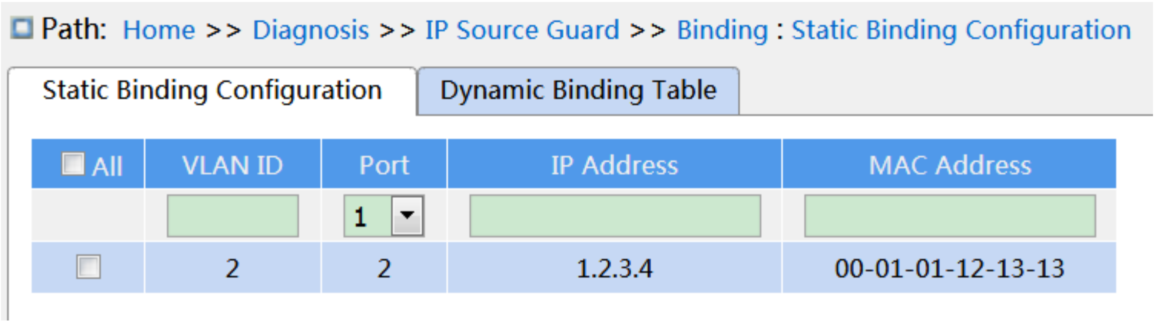


Figure 310 Static Binding Configuration

VLAN ID

Configuration options: All VLAN ID

Function: configure VLAN ID of static binding table.

Port

Function: Select member port of the static binding table.

IP address

Configuration format: A.B.C.D

Function: configure IP address of static binding table.

MAC address

Configuration format: HH-HH-HH-HH-HH-HH 或 HH:HH:HH:HH:HH:HH（H is a hexadecimal number）

Function: Configure MAC address of static binding table, only configure as unicast MAC address.

4. View Dynamic Binding table, as shown below.

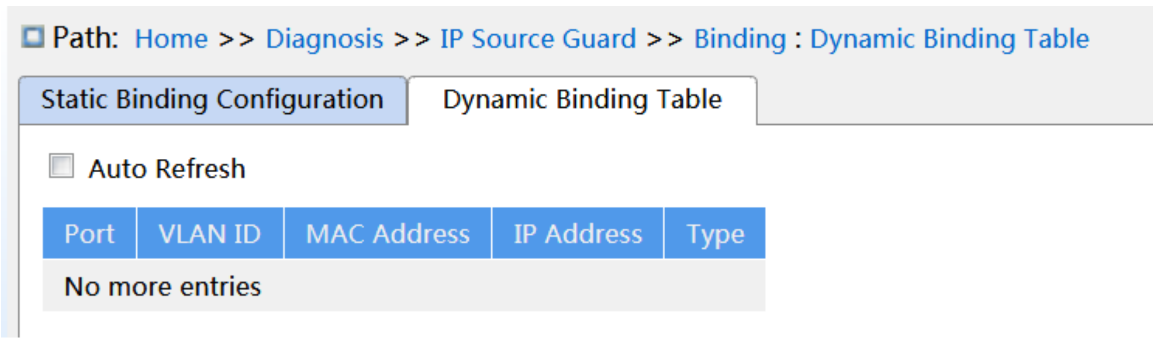


Figure 311 View Dynamic Binding table

Type

Display options: Relay/Snooping

Description: The dynamic binding table is generated by DHCP Relay and DHCP Snooping devices, the table items of Relay type is generated after enable global IP Source Guard, table items of type snooping are generated after both the global and ports that connect to the DHCP client enable IP Source Guard.

8.6.4 Typical Configuration Example

1. Relay type IP Source Guard table items

As shown in Figure 312, Switch A as the DHCP server, switch B as the DHCP relay, switch C as the DHCP client, and 1 port of switch A connected to the 1 port of switch B, 2 port of switch B connect to 2 port of switch C. DHCP server is not in the same LAN as the DHCP client. After the relay device enable IP Source Guard, the client dynamically obtains the IP address and other network parameters with DHCP mode through DHCP relay. The relay device forms IP Source Guard table items.

Figure 312 DHCP typical configuration example

➢ Switch A configuration:

1. Create VLAN1 and configure IP address: 100.1.1.156;

2. Open the DHCP server state in VLAN 1, as shown in Figure 192;

3. Create address pool pool-33, as shown in Figure 193;

4. Select address pool type as Network; IP address: 33.1.1.6; Mark: 255.0.0.0, as shown in Figure 194;

➢ Switch B configuration:

1. Create VLAN1 and configure IP address: 100.1.1.180；

2. Create VLAN33and configure IP address: 33.1.1.2；

3. Enable DHCP delay, as shown in Figure 207:

4. Configure Server IP address: 100.1.1.156, as shown in Figure 207;

5. Enable global IP Source Guard, as shown in Figure 308;

➢ Switch C configuration:

1. Create VLAN33 and enable DHCP Client;

2. Switch A assigns address 33.0.0.1 to Switch C;

After the switch C gets the address, the IP Source Guard table can be viewed on the switch B, as shown in Figure 311.

2. Snooping tyepe IP Source Guard table items

As shown below, Switch A as the DHCP server, switch B as the DHCP Snooping, switch C as the DHCP client, and 1 port of switch A connected to the 1 port of switch B, 2 port of switch B connect to 2 port of switch C. DHCP server is not in the same LAN as the DHCP client. After Snooping device enable IP Source Guard, the client dynamically obtains the IP address and other network parameters with DHCP mode through DHCP Snooping. The relay device forms IP Source Guard table items.

Figure 313 DHCP typical configuration example

➢ Switch A configuration:

1. Create VLAN1 and configure IP address: 100.1.1.156;

2. Open the DHCP server state in VLAN 1, as shown in Figure 192;

3. Create address pool pool-1;

4. Select address pool type as Network; IP address: 33.1.1.6; Mark: 255.0.0.0;

➢Switch B configuration:

1. Create VLAN1 and configure IP address: 100.1.1.180;

2. Enable DHCP Snooping;

3. Configure 1 port as trust port, as shown in Figure 203;

4. Enalbe global IP Source Guard, as shown in Figure 308;

5. Port 2 enable IP Source Guard, as shown in Figure 309;

➢Switch C configuration:

1. Create VLAN1 and enable DHCP Client;

2. Switch A assigns address 100.0.0.1 to Switch C;

After the switch C gets the address, the IP Source Guard table can be viewed on the switch B.

8.7 DDM

8.7.1 Introduce

Digital diagnosis is an effective method for monitoring important performance parameters of optical modules. The parameters it monitors include: transmitted optical power, received optical power, temperature, operating voltage, bias current, and their alarm information. Through the digital diagnosis function of the optical module, the network management unit can access the optical module through the two-wire serial bus, and monitor the temperature, working voltage, bias current, transmitted optical power and received optical power of the module in real time.

8.7.2 Web Configuration

1. Basic Information

According to the path below, click to view the basic information of the optical module inserted into the device, as shown in the following figure.

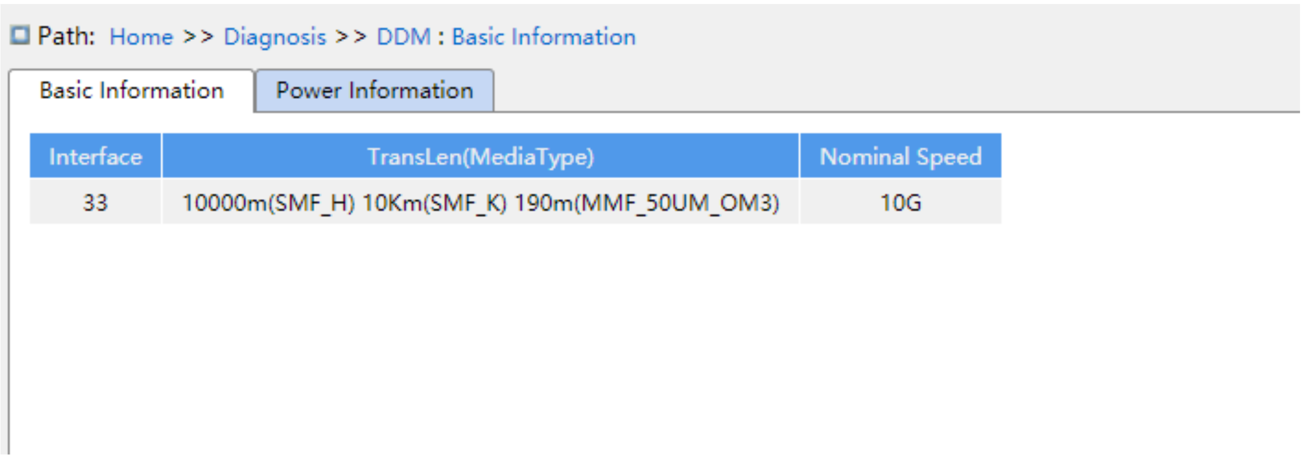
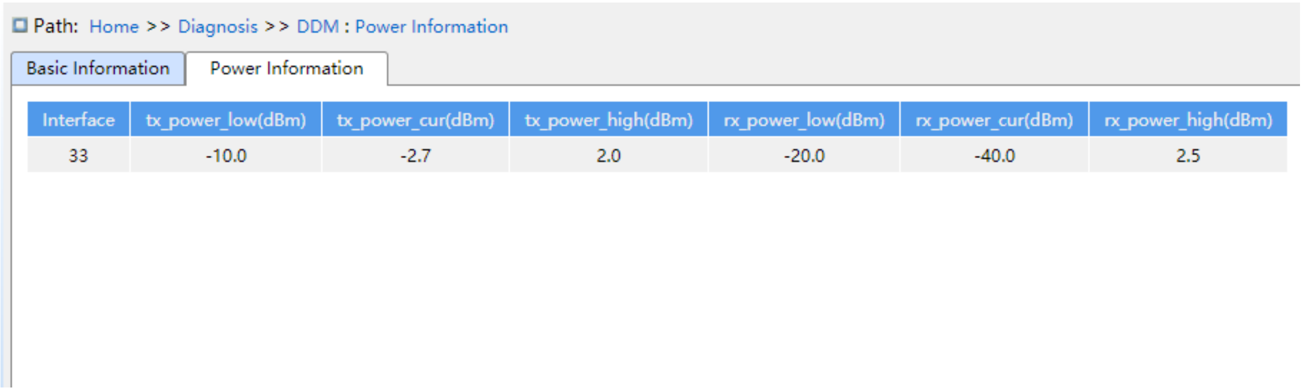


Figure 314 Basic information of optical module

2. Power Information

According to the following path, click to view the optical power information of the optical module, as shown in the figure below.



Interface	tx_power_low(dBm)	tx_power_cur(dBm)	tx_power_high(dBm)	rx_power_low(dBm)	rx_power_cur(dBm)	rx_power_high(dBm)
33	-10.0	-2.7	2.0	-20.0	-40.0	2.5

Figure 315 Basic information of optical power

Appendix: Acronyms

Acronym	Full Spelling
ACE	Access Control Entry
ACL	Access Control List
ARP	Address Resolution Protocol
BootP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
CIST	Common and Internal Spanning Tree
CLI	Command Line Interface
CoS	Class of Service
CST	Common Spanning Tree
DHCP	Dynamic Host Configuration Protocol
DHP	Dual Homing Protocol
DNS	Domain Name System
DRP	Distributed Redundancy Protocol
DSCP	Differentiated Services CodePoint
DST	Daylight Saving Time
EAPOL	Extensible Authentication Protocol over LAN
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
IGMP	Internet Group Management Protocol
IGMP Snooping	Internet Group Management Protocol Snooping
IST	Internal Spanning Tree
LACP	Link Aggregation Control Protocol
LACPDU	Link Aggregation Control Protocol Data Unit

LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
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
PCP	Priority Code Point
PVLAN	Private VLAN
QCL	QoS Control List
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RMON	Remote Network Monitoring
RSTP	Rapid Spanning Tree Protocol
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SP	Strict Priority
SSH	Secure Shell
SSL	Secure Sockets Layer
SSM	Source Specific Multicast
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USM	User-Based Security Model

VLAN	Virtual Local Area Network
WINS	Windows Internet Naming Service
WRR	Weighted Round Robin