SICOM6800-D Series Industrial Ethernet Switch

Web Operation Manual

Publication Date: Mar, 2024

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

Preface

This manual mainly introduces the access methods and software features of SICOM6800-D series 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 (Local, FTP,TFTP) ➢ Language Update ➢ Restart ➢ About
5. Service	➢ SSL Configuration ➢ SNMPv1/v2c/v3 ➢ SSH Configuration ➢ TACACS+ Configuration ➢ RADIUS Configuration ➢ DNS

	➢ RMON
6. Alarm	➢ Basic Alarm ➢ Port Alarm ➢ Alarm about Ring ➢ DDM Alarm
7. Function Management	➢ Port Configuration ➢ VLAN ➢ IP Configuration ➢ Port Aggregation ➢ Redundancy ➢ ARP Configuration ➢ ACL Configuration ➢ MAC Address Configuration ➢ IGMP snooping ➢ DHCP Configuration ➢ IEEE802.1X Configuration ➢ GMRP ➢ PIM ➢ IGMP ➢ Route ➢ QoS ➢ VRRP ➢ NQA
8. Diagnosis	➢ Log ➢ Port Mirroring ➢ LLDP ➢ Trace Route ➢ Ping ➢ IP Source Guard

	➢ DDM

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 SICOM6800-D Series industrial Ethernet switch include:

Name of Document	**Content Introduction**
SICOM6800-D Series Industrial Ethernet Switches Hardware Installation Manual_V1.0.pdf	Describes the hardware structure, hardware specifications, mounting and dismounting methods.
SICOM6800-D Series Industrial Ethernet Switch Web Operation Manual	Describes the switch software functions, Web configuration methods, and steps of all functions.

1 Product Introduction

1.1 Overview

SICOM6800-D is Layer 3 DIN-Rail Managed Industrial Ethernet Switch. Supports DT-Ring (recovery time<50ms), DRP/DHP (recovery time<20ms), MSTP/RSTP/STP, VLAN, multicast, QoS, SSH and many other Layer 2 software features, and supports VRRP, OSPF, RIP, IGMP, PIM, static routing and many other Layer 3 software features, and supports CLI, Telnet, Web management methods, Kyvision centralized management based on SNMPv1/v2c/v3.

SICOM6800-D is especially designed for harsh environments,and can be deployed in Transportation, Oil & gas and many other industrial applications.

1.2 Software Features

SICOM6800-D provides abundant software features, satisfying customers' various requirements.

- Redundancy protocols: DRP, DT-Ring, STP/RSTP, VRRP and MSTP.
- Multicast protocols: IGMP Snooping, GMRP, PIM-SM, PIM-DM.
- Switching attributes: VLAN, GVRP, QoS, and ARP.
- Bandwidth management: port static aggregation, LACP, broadcast suppression.
- Security: user management, access management, SSH, SSL, TACACS+, RADIUS, IEEE802.1X, ACL, port isolation and IP source guard.
- Synchronization protocols: SNTP, NTP and PTP.
- Device management: software update, configuration file upload/download, and log record and upload.
- Device diagnosis: port mirroring, LLDP.
- Alarm function: power alarm, port alarm, ring alarm, IP/MAC address conflict alarm and DDM alarm.
- Network management: management by CLI, Telnet, Web and Kyvision network

management software, DHCP, and SNMPv1/v2c/v3 network monitoring.

- Network configuration: 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/SSH, 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 DB9-RJ45 console cable.

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

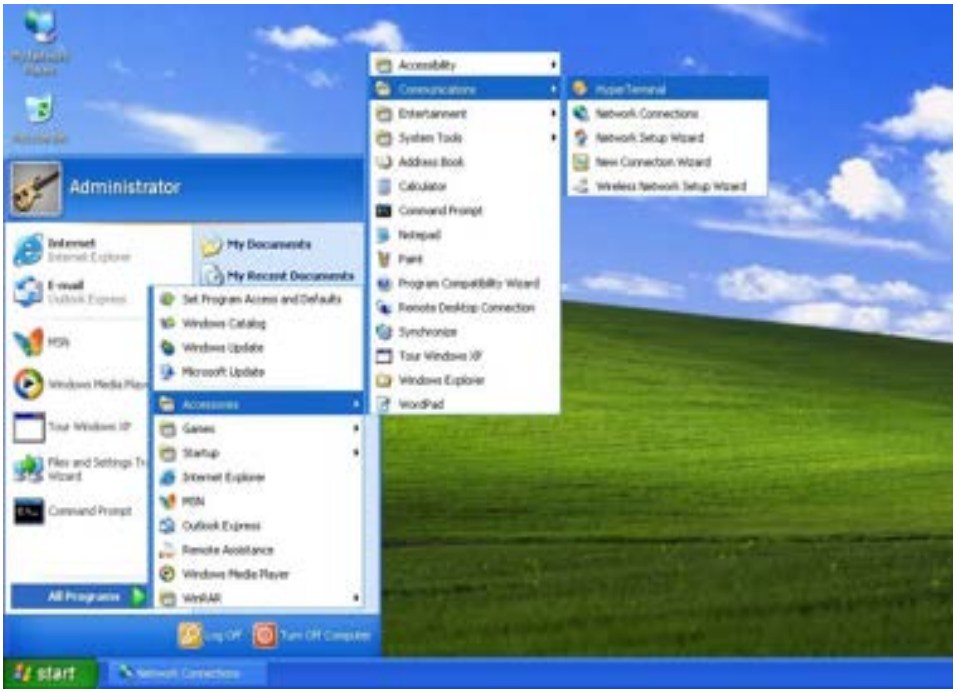


Figure 1 Start the Hyper Terminal

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

Figure 2 Create a New Connection

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

Figure 3 Select 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.

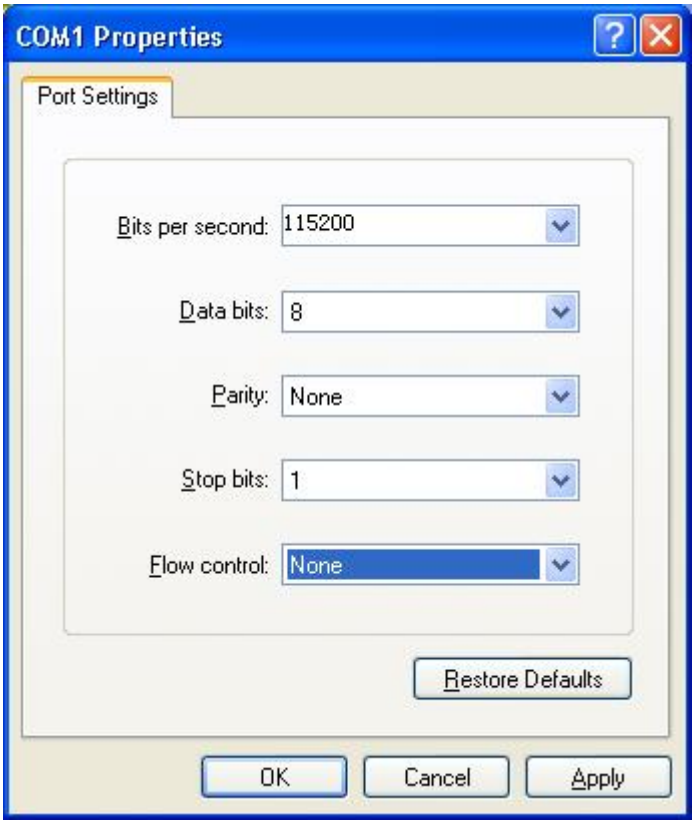


Figure 4 Set Port Parameters

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.

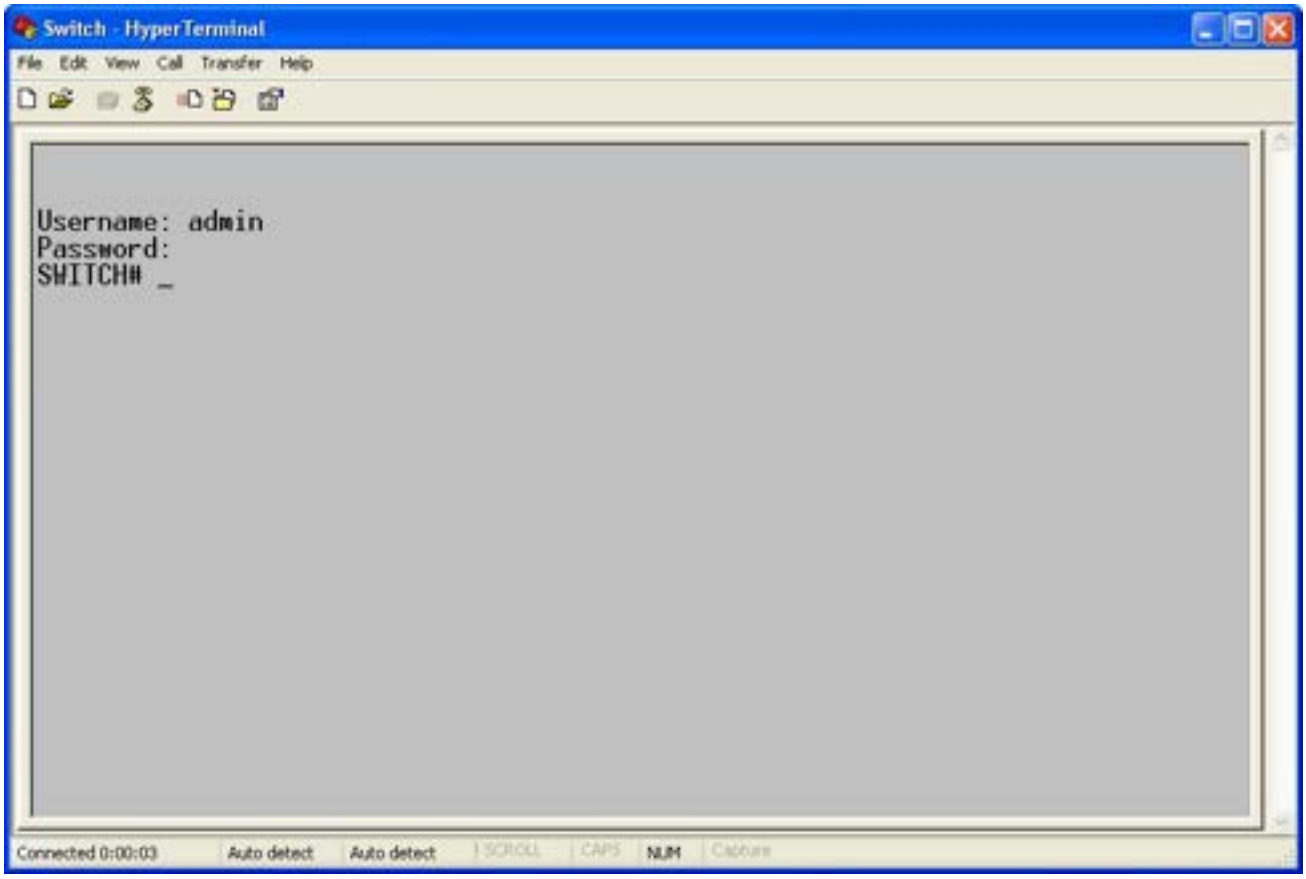


Figure 5 CLI

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.

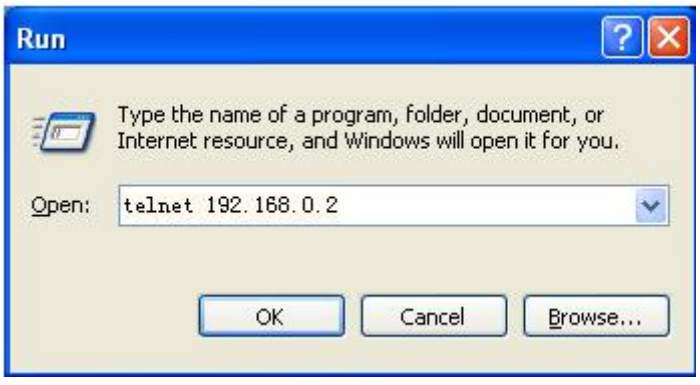


Figure 6 Telnet Access

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.

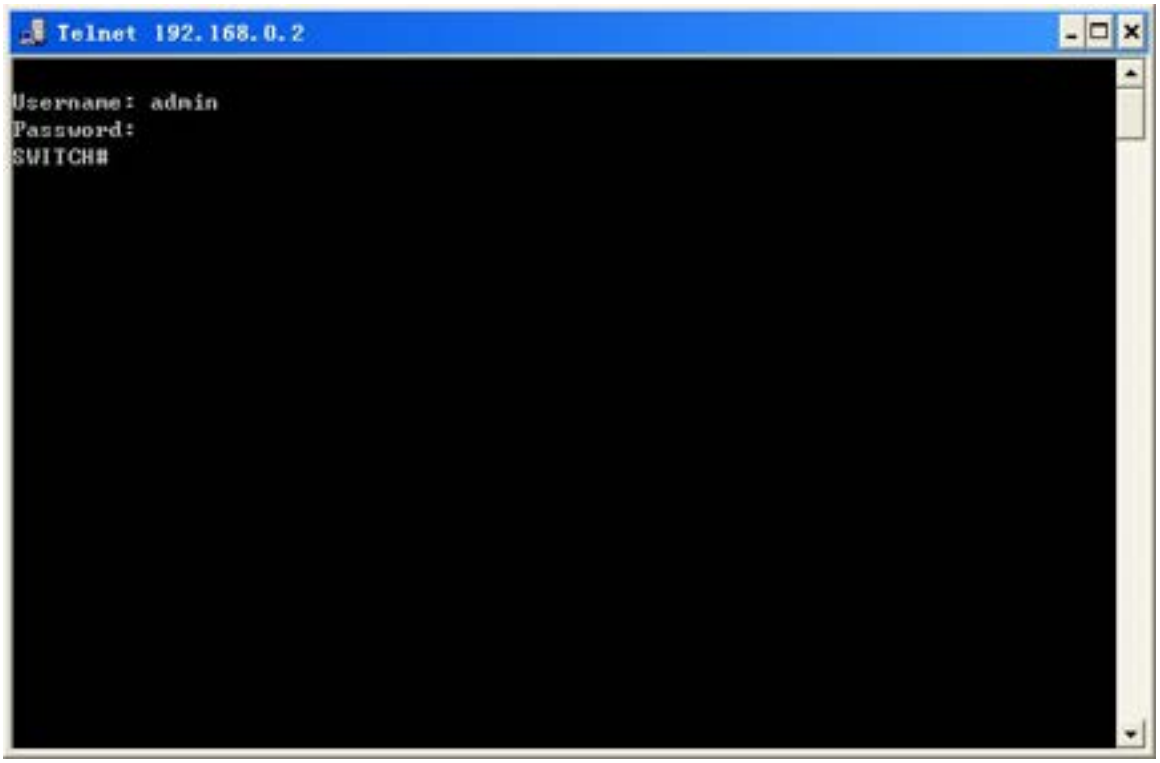


Figure 7 Telnet Interface

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. Click <OK>. You can also

input other created users and password.

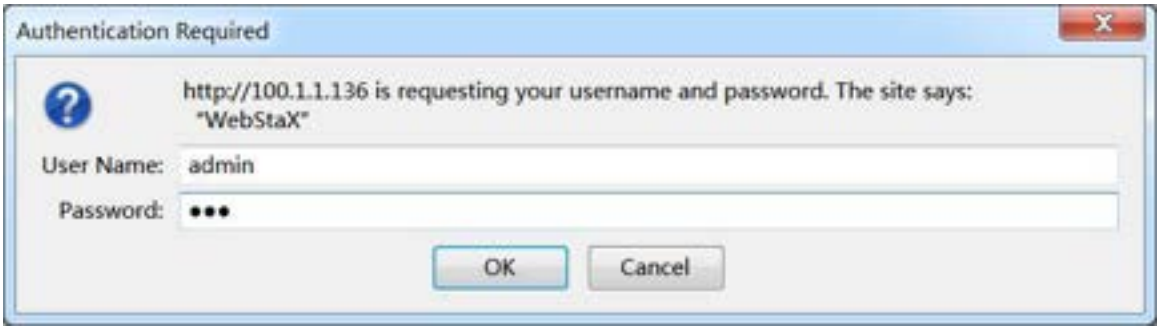


Figure 8 Web Login

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 Introduction

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

3.1.2 Web Configuration

1. Create a new user, as shown below.

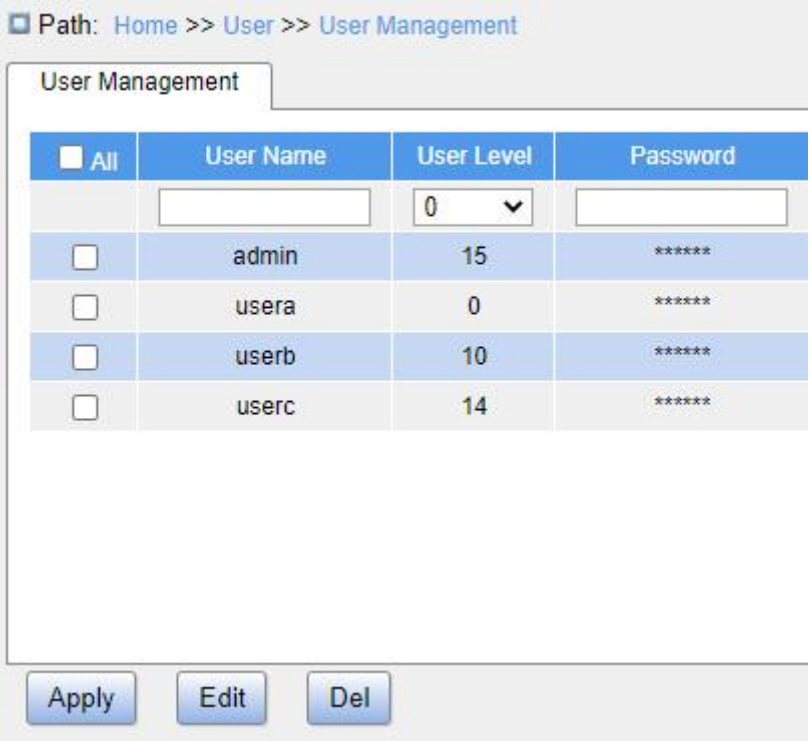


Figure 10 Create a New User

Add a new user in the user name formula bar, configure different user levels, and a maximum of 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.

Description: If the privilege level value is 15, it can access all groups, that is, it is granted the fully control of the device. User's privilege should be same or greater than the group privilege level to have the access of that group. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

Password

Configuration range: 1~31 characters

Function: Configure user login password.

2. Edit user configuration, as shown below.

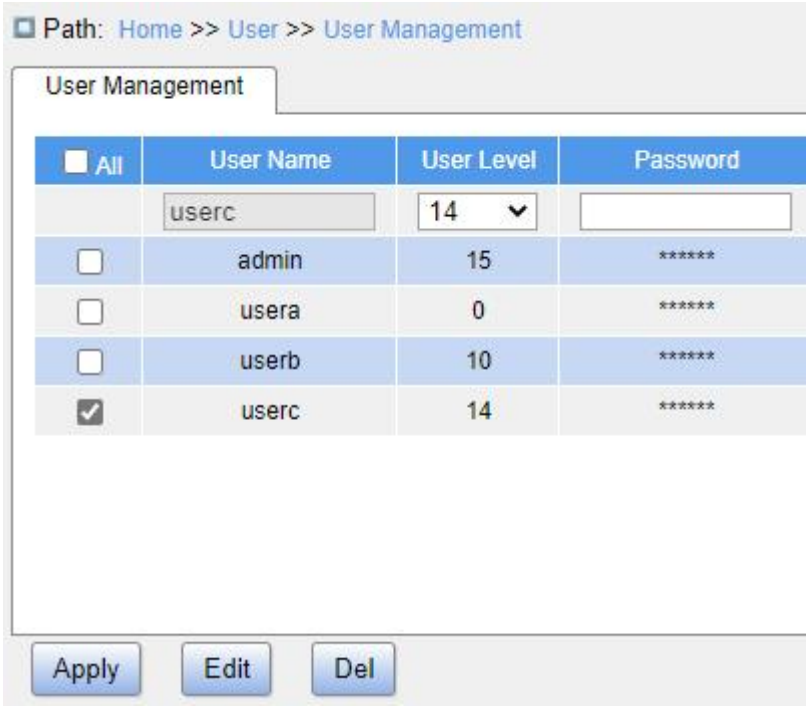


Figure 11 Edit User Configuration

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

Click <Del> button to delete the current user.

Note:

The default user admin cannot be deleted.

3. Configure group privilege level, as shown below.

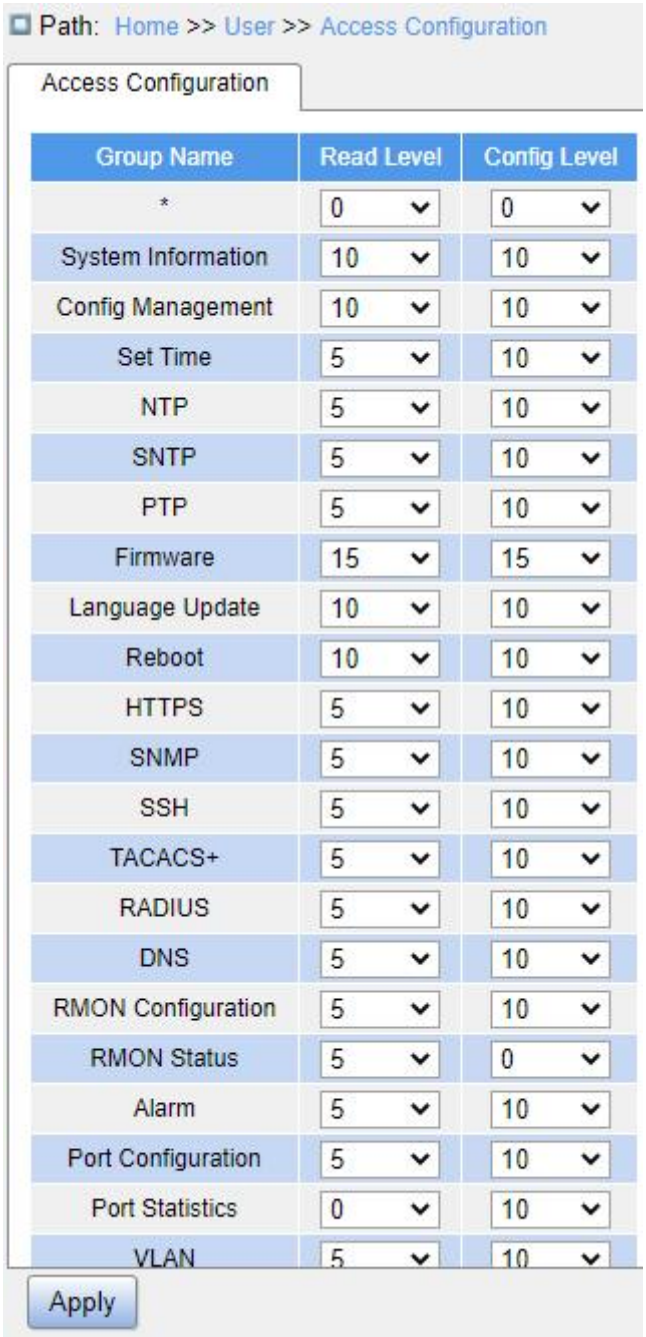


Figure 12 Configure Group Privilege Level

Group Name

Configuration options: All functional groups

Function: Select the switch function group for the operation.

Read Level

Configuration options: 0~15

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

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 equal to or greater than a group privilege level, the user can access or configure the group. The access or configuration range is based on the user privilege level.

3.2 Authentication Type

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

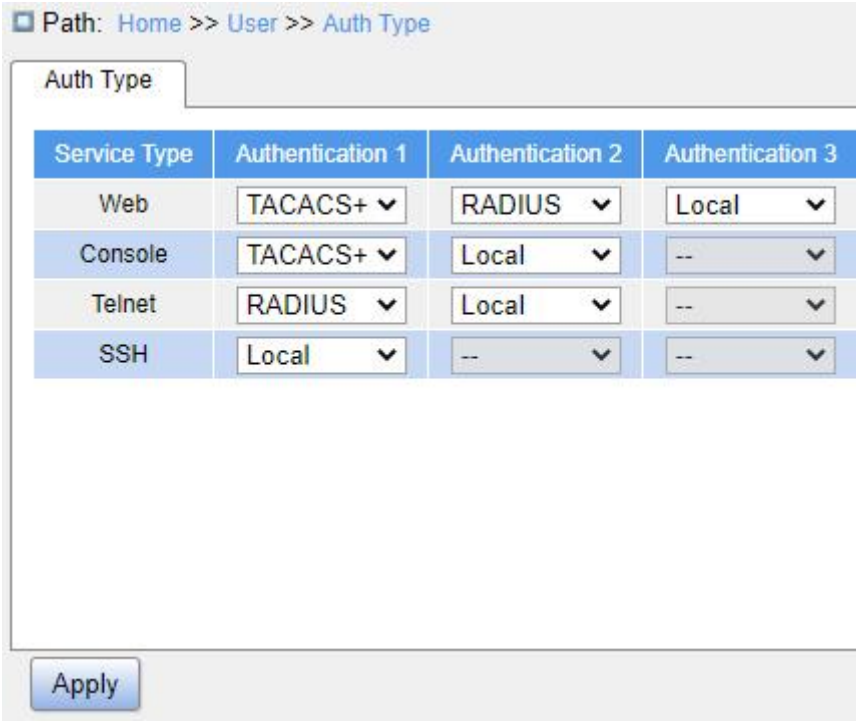


Figure 13 Authentication Login Configuration

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 Authentication 1, Authentication 2, and Authentication 3. 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.

- Local: Uses username and password set in local for authentication.
- TACACS+: Uses username and password set in TACACS+ server for authentication.
- RADIUS: Uses username and password set in RADIUS server for authentication.

Caution:

If “TACACS+/RADIUS” is selected for Authentication 1 and Authentication 2, it is recommended to configure Authentication 3 as “Local”. This will enable the management client to log in to the switch via the local user if none of the configured remote authentication servers is available.

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, System Uptime, Contact and Location, as shown below.

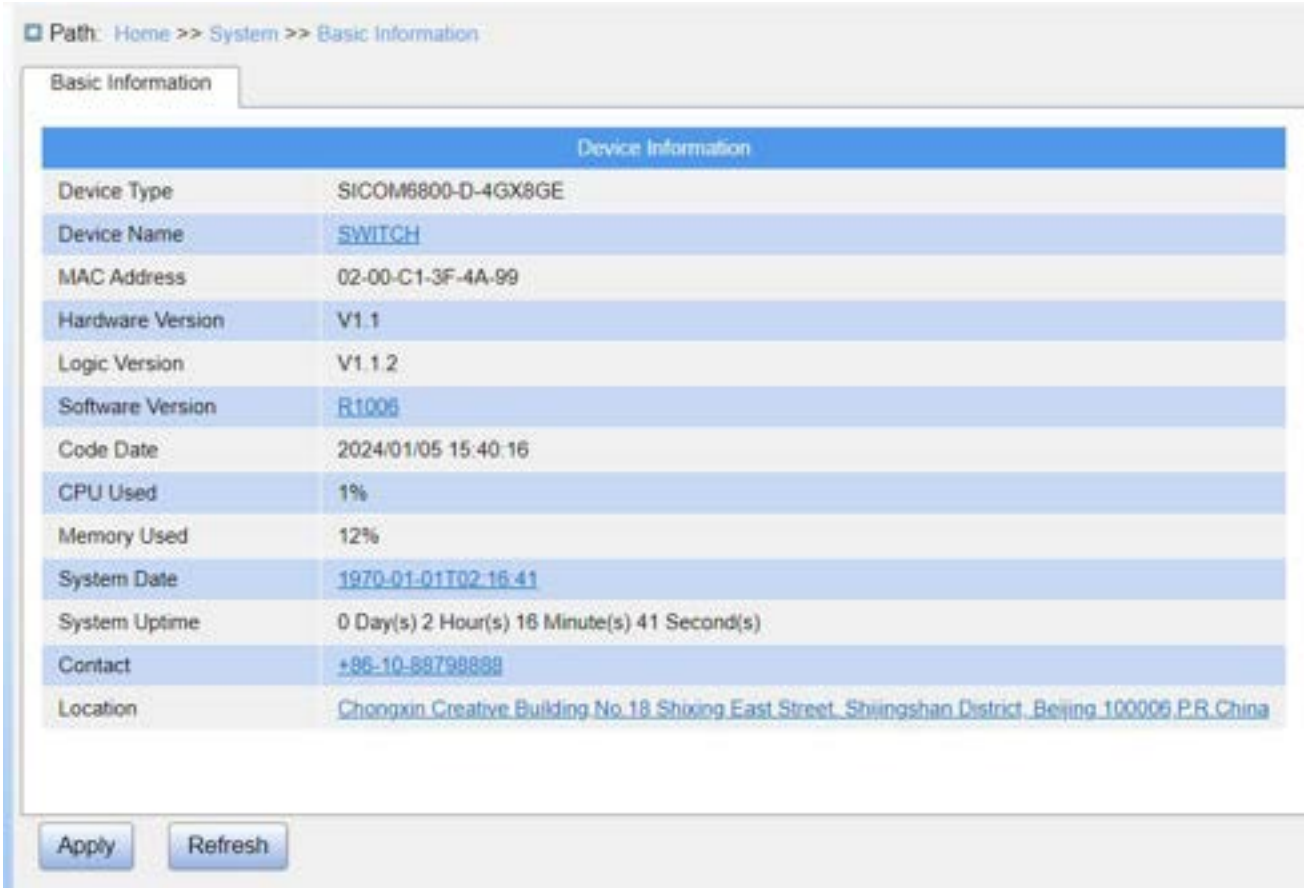


Figure 14 Basic Information

4.2 Config Management

1. Save the current configuration information, as shown below.

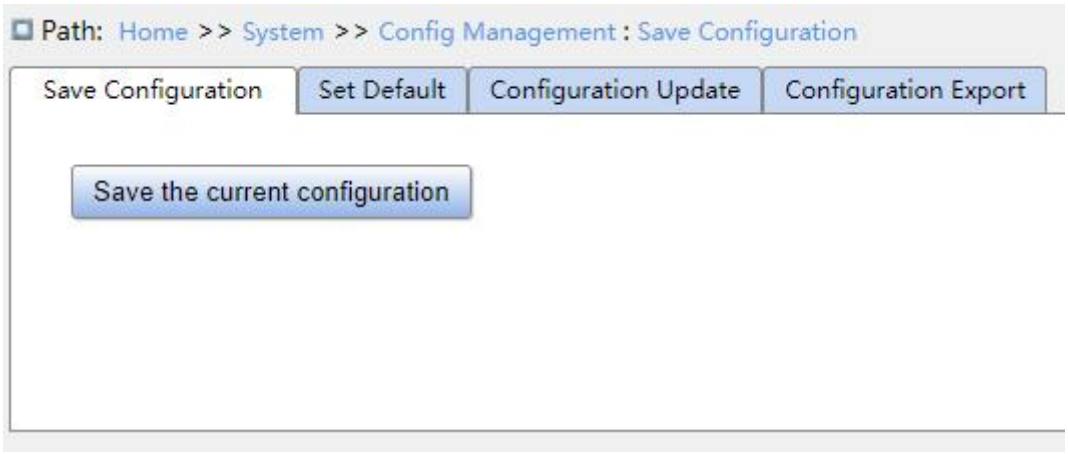


Figure 15 Save Current Configuration

2. Restore the factory configuration, as shown below.

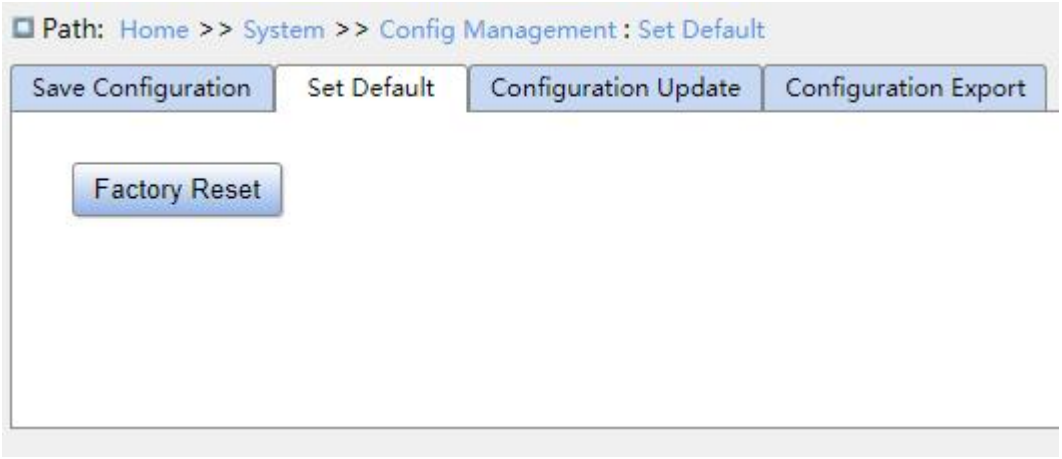


Figure 16 Restore Factory Configuration

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

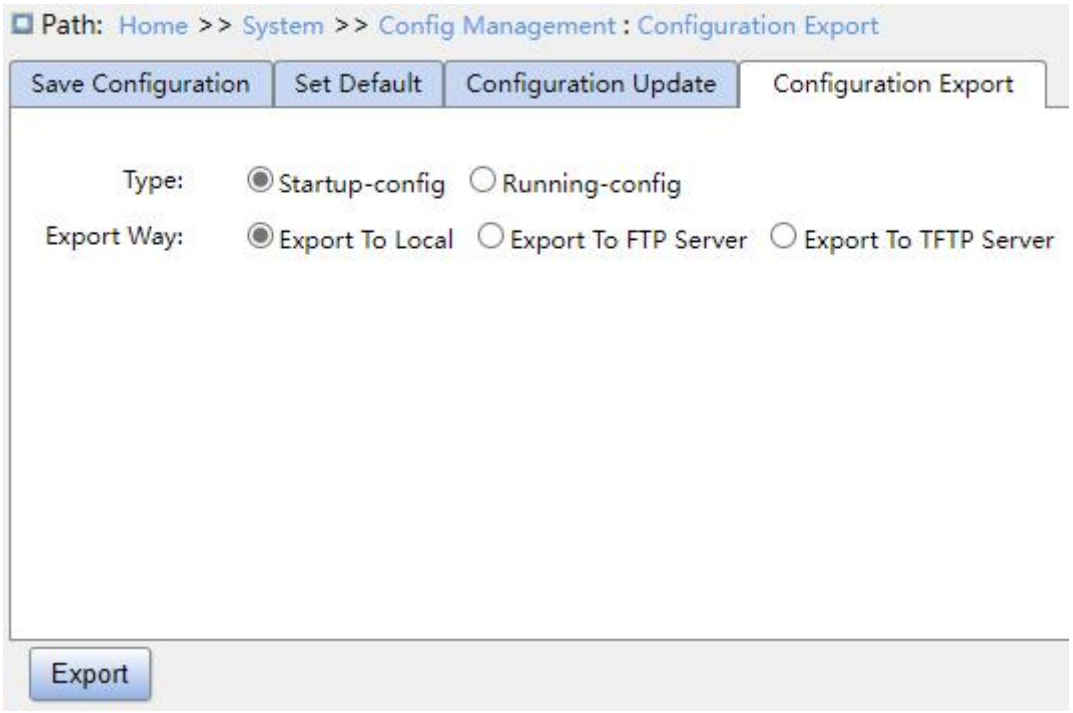


Figure 17 Export Configuration File - Local

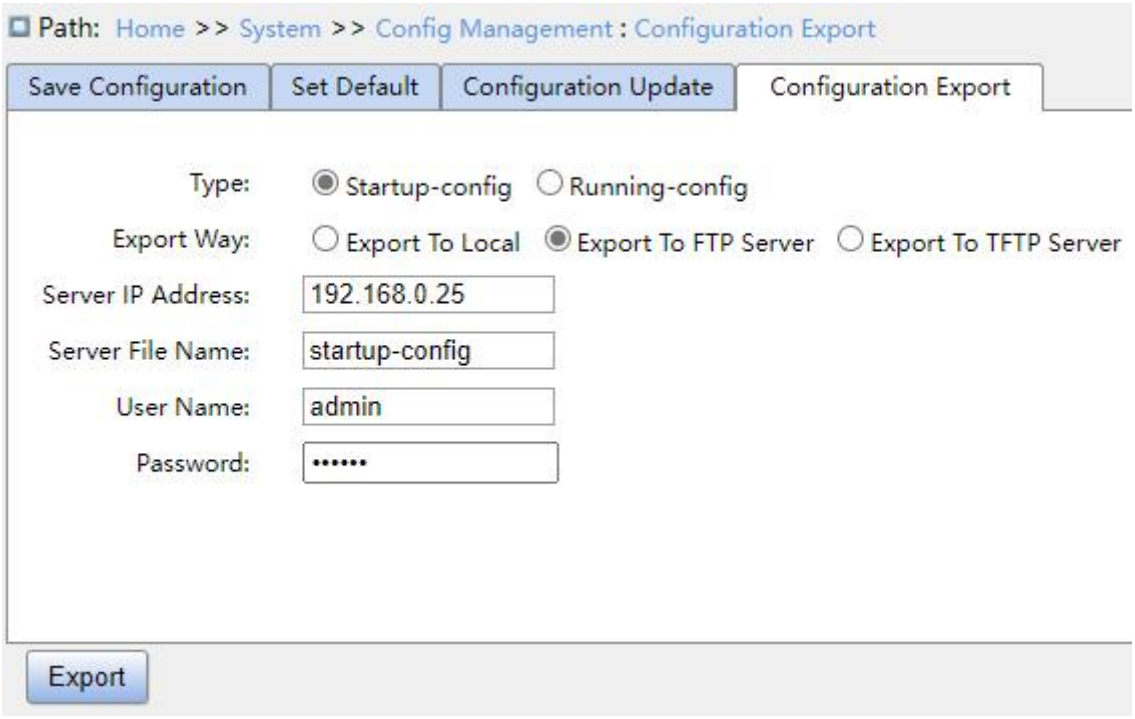


Figure 18 Export Configuration File - FTP

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 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:

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

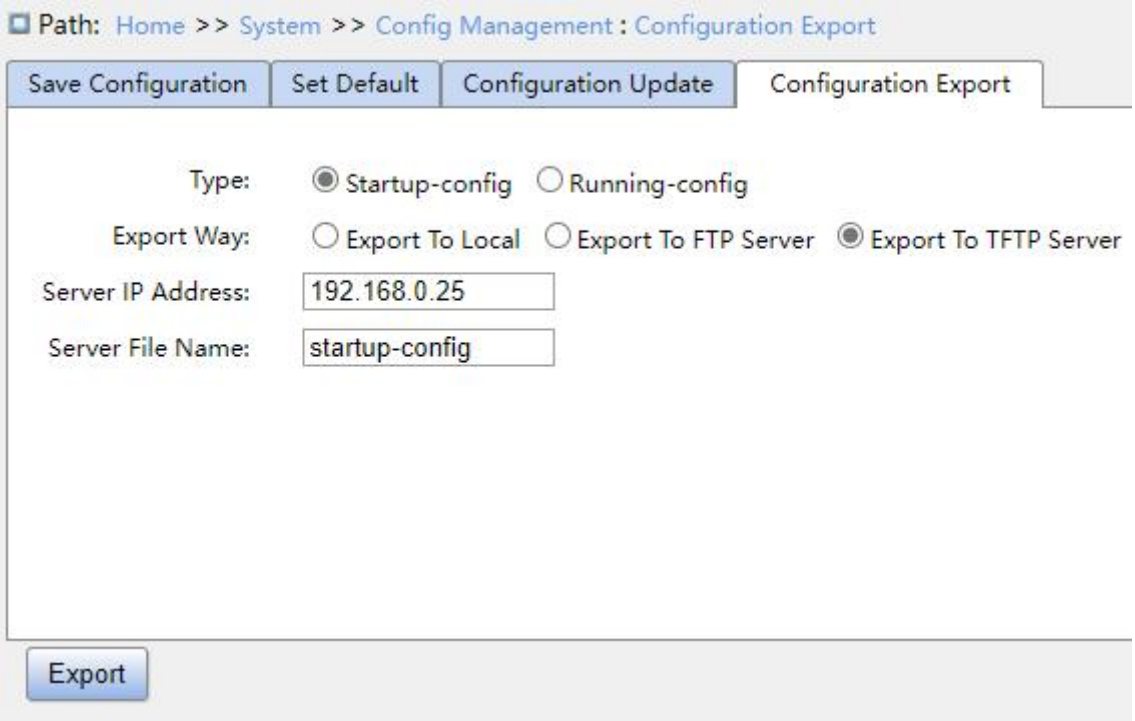


Figure 19 Export Configuration File - TFTP

Server IP address

Configuration format: A.B.C.D

Description: Configure the IP address of the TFTP server.

Server File Name

Configuration range: 1~63 characters

Description: Configure the configuration file name to be stored on the TFTP server.

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. Update configuration. Upload the configuration file from local/server to the switch as a new startup file for the switch, as shown in Figure 20 -Figure 22.

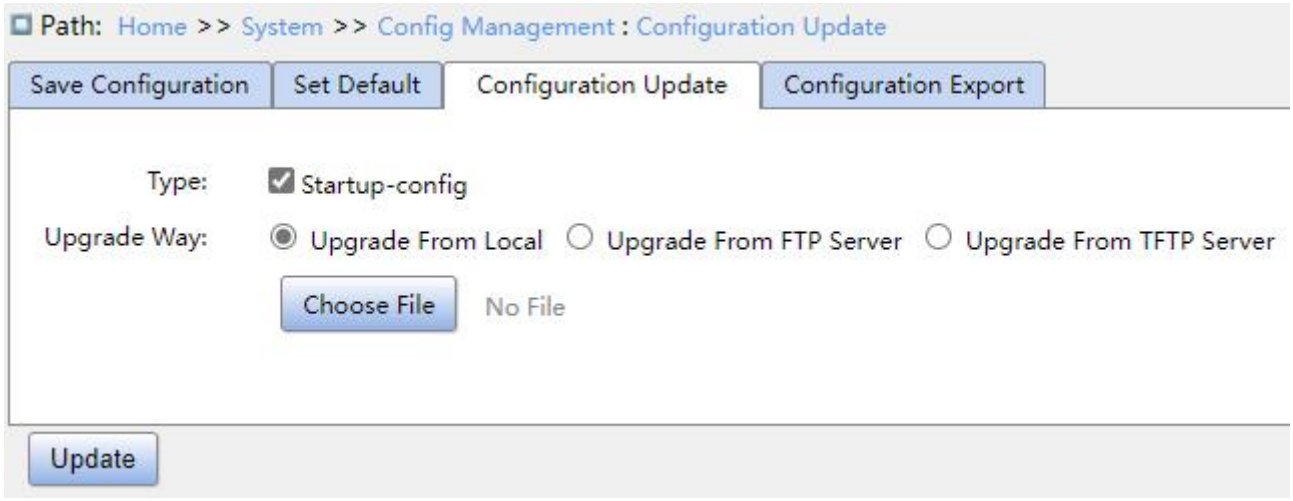


Figure 20 Upgrade from Configuration File - Local

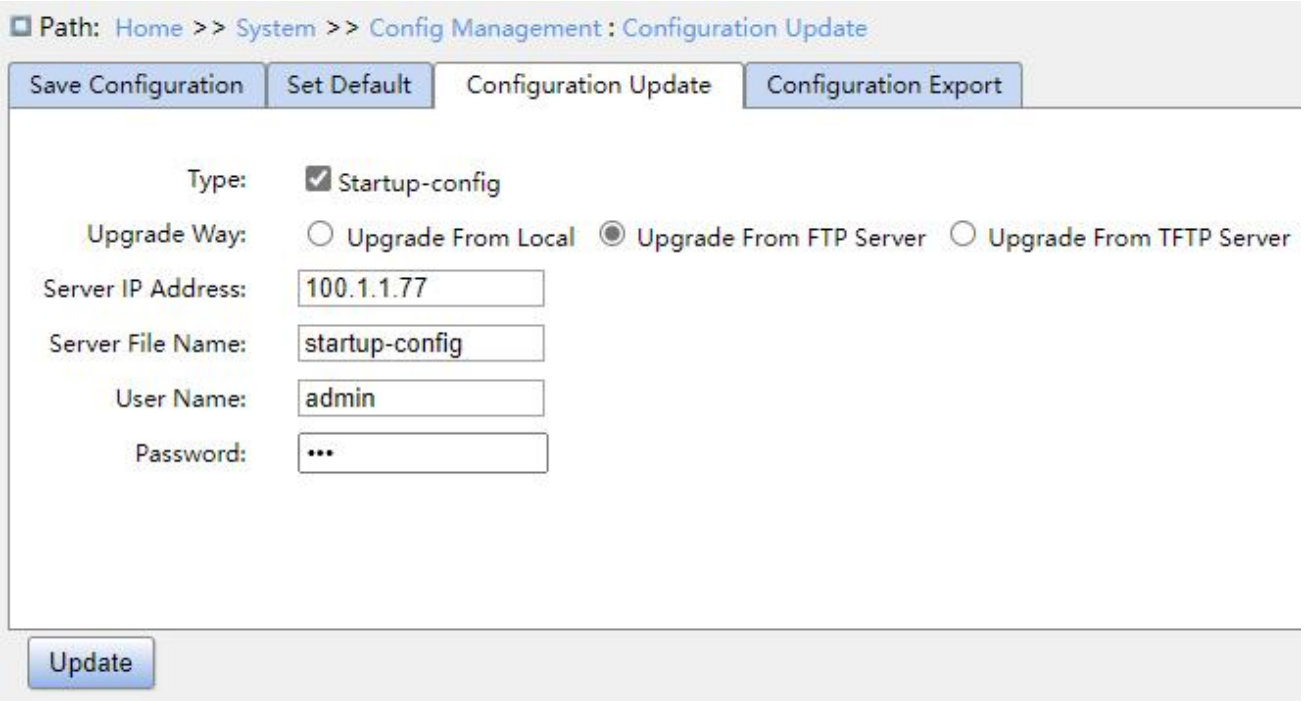


Figure 21 Upgrade from Configuration File - FTP

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.

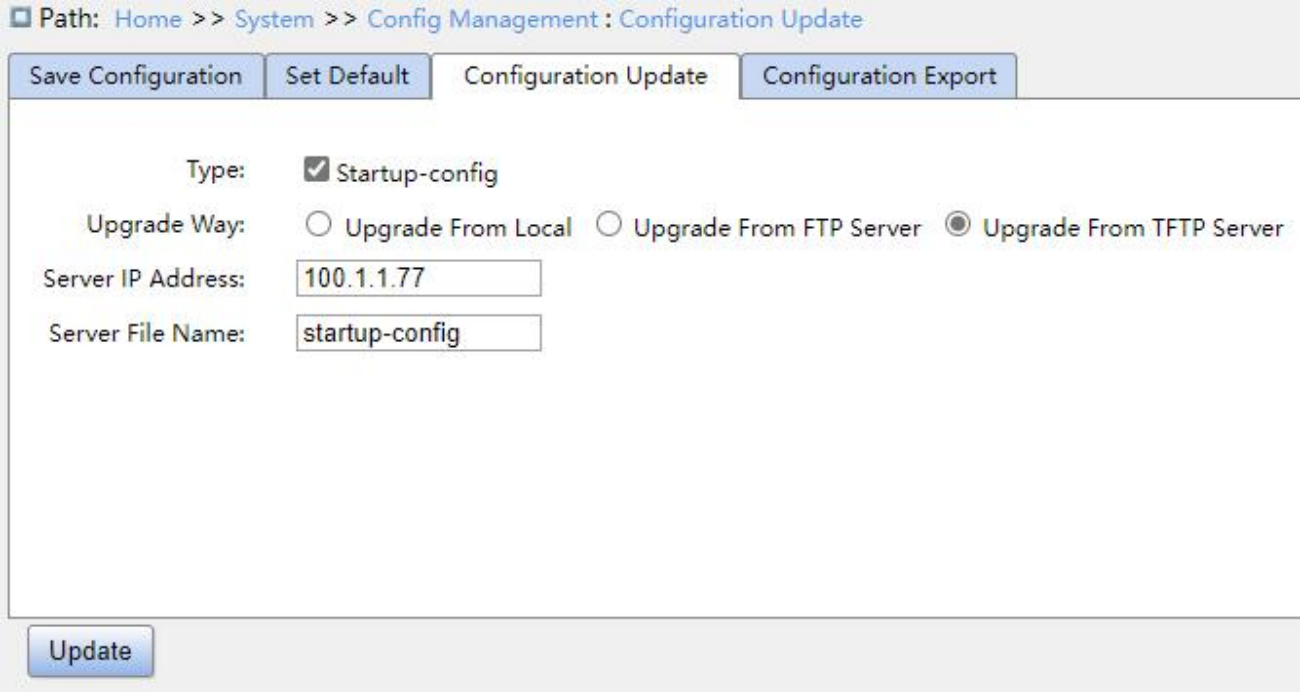


Figure 22 Upgrade from Configuration File - TFTP

Server IP Address

Configuration format: A.B.C.D

Description: Configure the IP address of the TFTP server.

Server File Name

Configuration range: 1~63 characters

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

You can upload the configuration file from the local/server to the switch as a new startup file. The new startup file will replace the original one. Click <Update> to upload the configuration file from local/server to the switch.

4.3 Clock Management

4.3.1 Time Configuration

1. Set DST, as shown below.

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

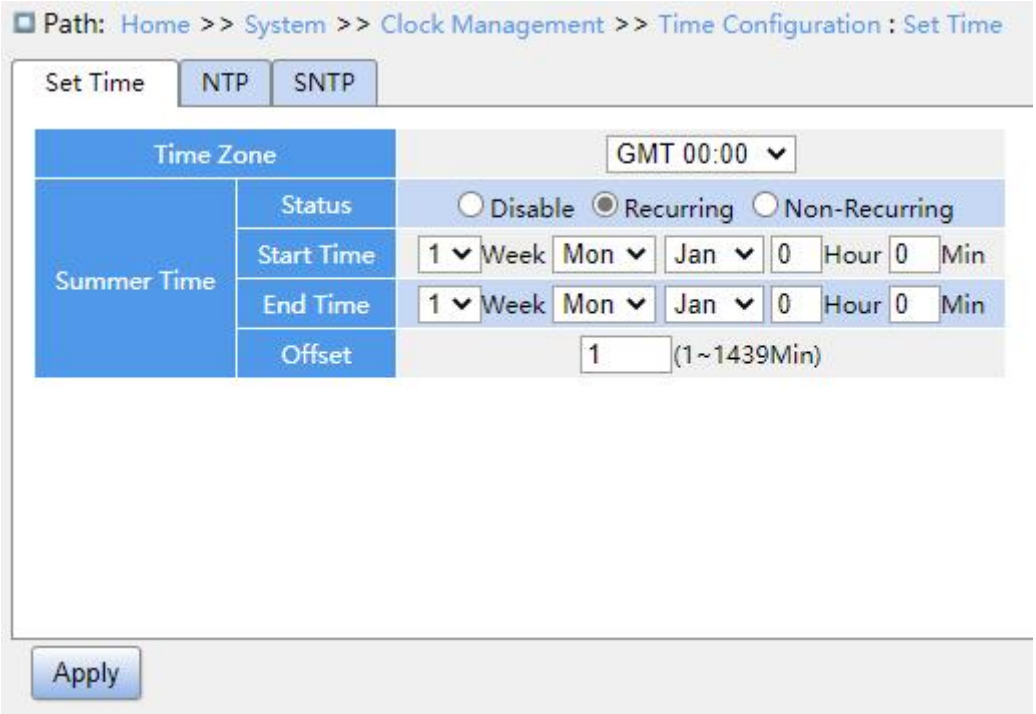


Figure 23 Recurring Configuration

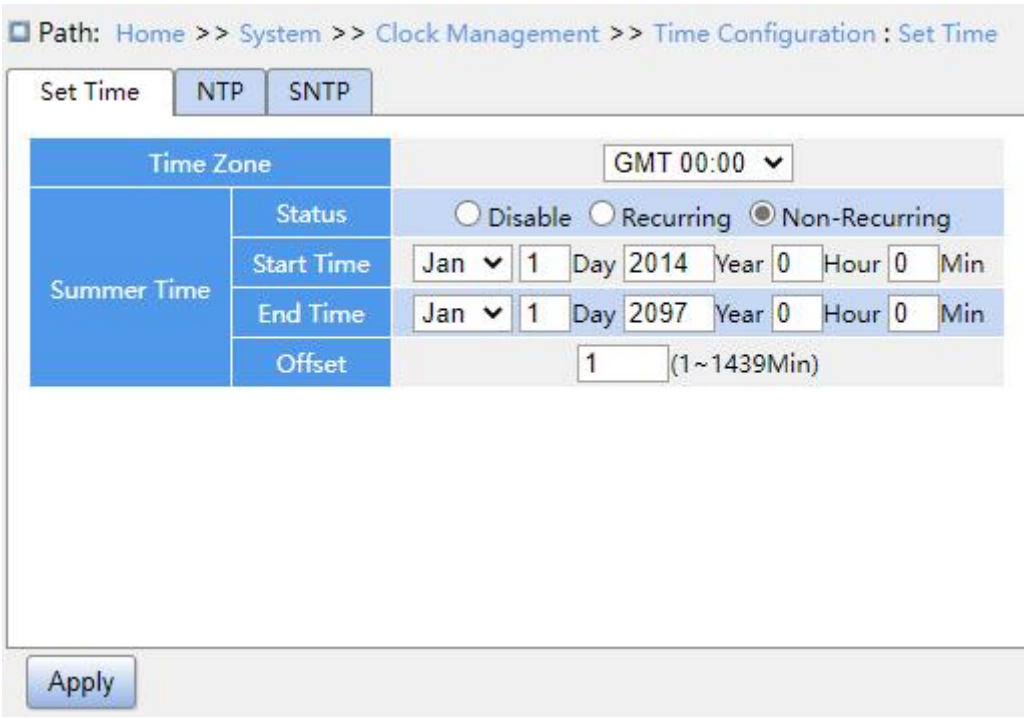


Figure 24 Non-Recurring Configuration

Time Zone

Function: Select local time zone.

Status

Configuration options: Disable/Recurring/Non-Recurring

Default configuration: Disable

Function: Whether to enable daylight saving time.

Start Time/End Time

Function: After enabling DST, set the time range of DST.

- For the non-recurring mode, you need to configure year, month, day, hour and minute to appoint the operation range of DST, as shown in Figure 23 (Set DST between 00:00 on 1 January in 2014 and 23:59 on 1 July in 2097).
- For the recurring mode, you need to configure month, week, date, hour and minute to appoint the operation range of DST per year, as shown in 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: 1~1439 min

Default configuration: 1 min

Function: Configure DST offset, that is, the advanced time when DST starts to be executed.

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 lasts from 10:00:00 on April 1st to 9:00:00 on October 1st, so the DST offset is 60 min.

Non-DST time runs to 10: 00: 00 on April 1st and jumps directly to 11: 00: 00 DST to begin DST. When DST runs to 9: 00: 00 on October 1st, 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, then the clock of all devices in the network is the 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.

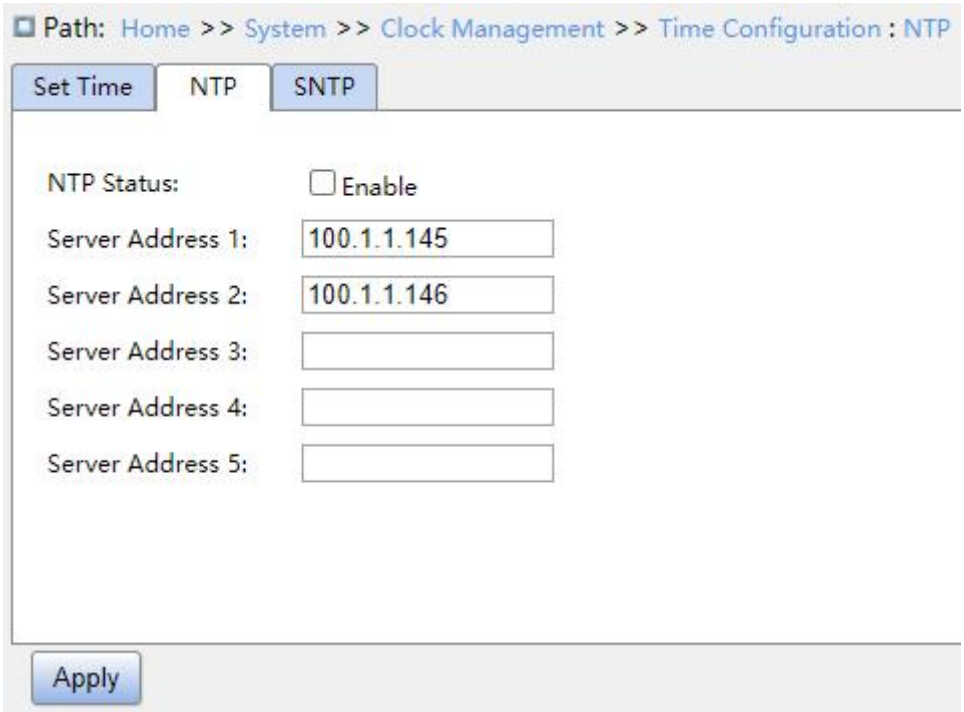


Figure 25 NTP Configuration

NTP Status

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable global NTP services.

Caution:

- NTP and SNTP protocol are mutually exclusive. Because NTP and SNTP use the same UDP port. They cannot be enabled at the same time.
- When NTP services are disabled, NTP services can be configured and saved, that is, enabling or disabling 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 calibrates the time according to the server's messages.

Caution:

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

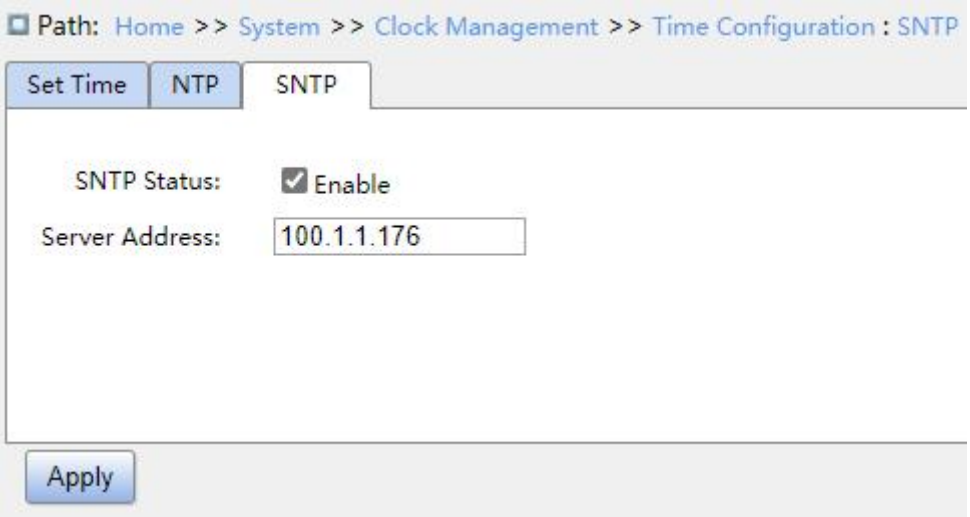


Figure 26 SNTP Configuration

SNTP Status

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to 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 server's message.

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

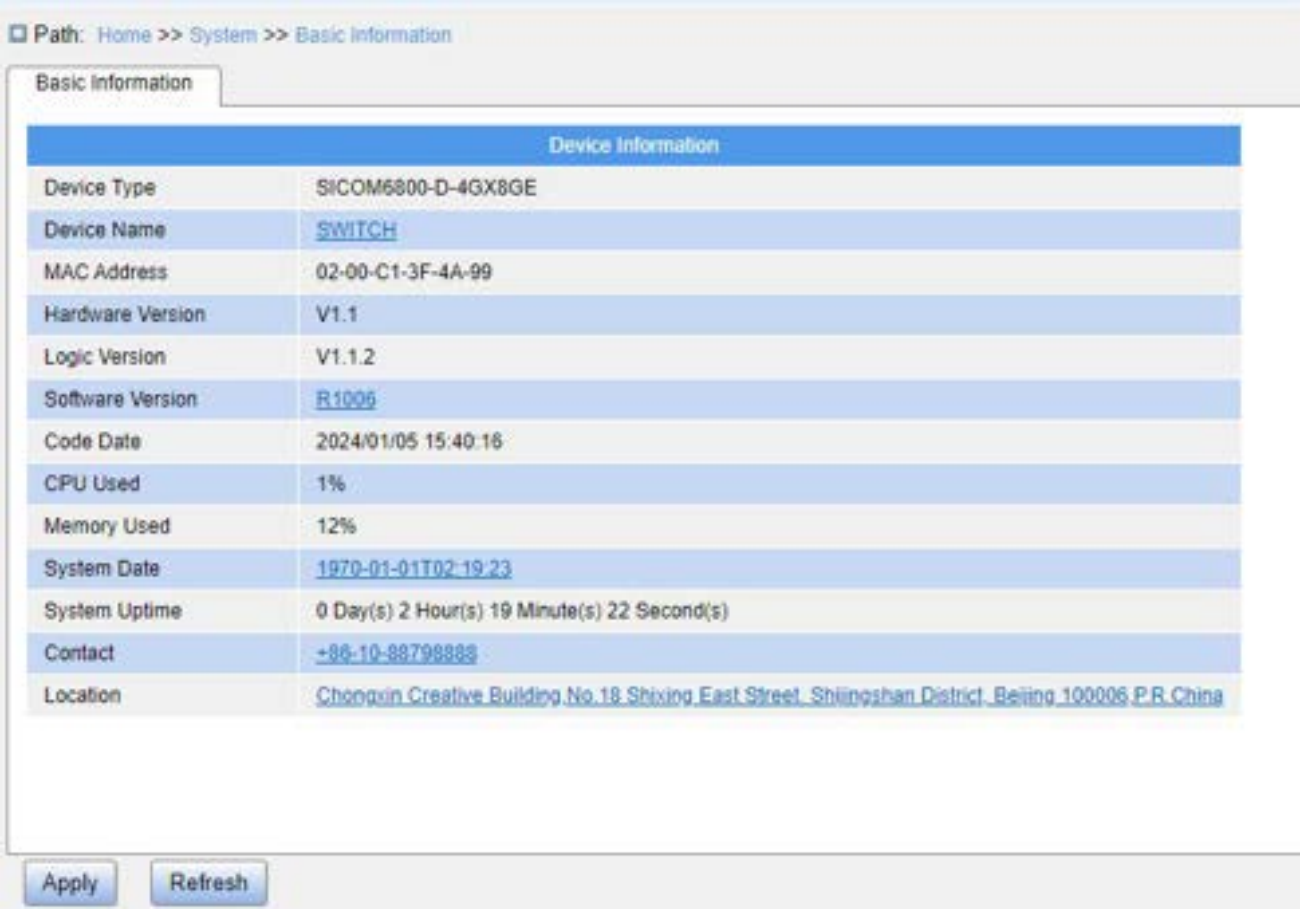


Figure 27 View Clock Information

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

4.3.2 PTP Configuration

4.3.2.1 Introduction

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

PTP Concepts

1. PTP domain

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

2. PTP port

A PTP-enabled port is called PTP port.

3. Clock node

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

- Ordinary Clock(OC)

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

- Boundary Clock (BC)

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

- Transparent Clock (TC)

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

- End-to-End Transparent Clock (E2ETC): directly forwards non-PTP packets and participates in delay calculation of the entire link.
- Peer-to-Peer Transparent Clock (P2PTC): directly forwards Sync, Follow_Up, and Announce packets, terminates other PTP packets, and participates in delay calculation of each segment of a link.

Relationship between a pair of synchronous clock nodes:

- The node sending synchronization clock information is the master mode, while the nodes receiving the information are slave nodes.
- The clock of the master node is master clock, while the clock of a slave node is slave clock.
- The port sending synchronization clock information is the master port, while the ports receiving the information are slave ports

4.3.2.2 Synchronization Principle

1. Selection of the grandmaster clock

All clock nodes select the grandmaster clock in the PTP domain by exchanging Announce packets with clock stratum and clock ID information. Then the master/slave relationship between nodes and master/slave ports on the nodes are determined. With this process, a spanning tree with the grandmaster clock as the root is established throughout the PTP domain. Then the master clock periodically sends Announce packets to slave clocks. If a slave clock does not receive Announce packets from the master clock within a period, the master clock is considered invalid and new selection is started. Announce packets contain the following information for grandmaster clock selection: grandmaster priority 1, clock stratum, clock accuracy, grandmaster priority 2, and clock ID.

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

2. Synchronization principle

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

PTP supports two delay measurement mechanisms:

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

4.3.2.3 Web Configuration

1. Configure PTP clock, as shown in Figure 1

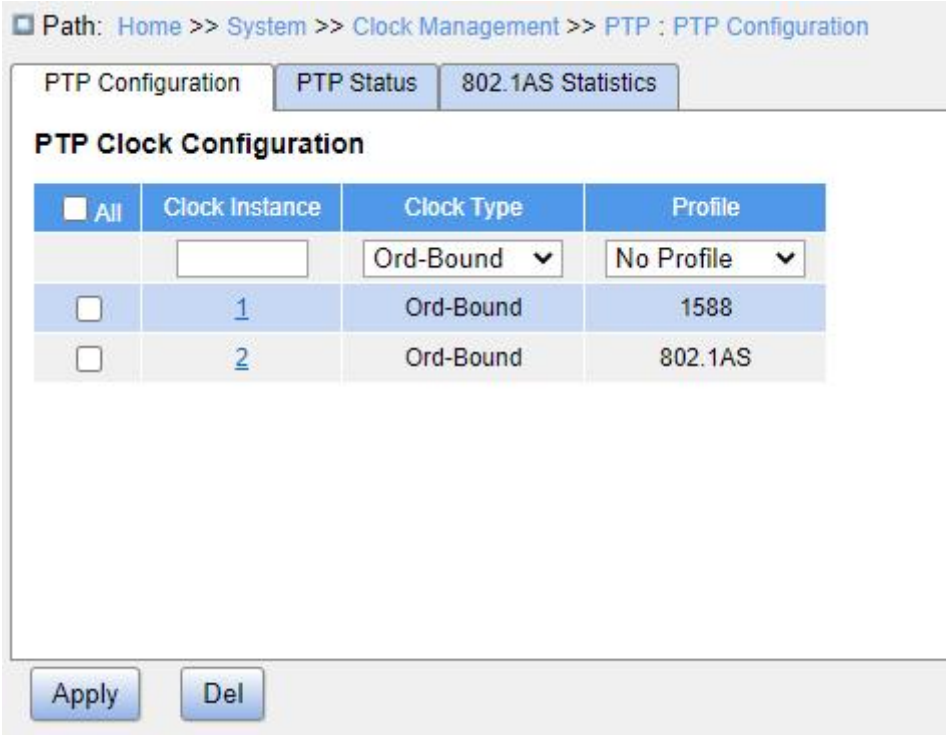


Figure 1 PTP Clock Configuration

Clock Instance

Configuration range: 0~3

Function: Configure the PTP instance ID.

Clock Type

Configuration range: Ord-Bound/P2pTransp/E2eTransp/Masteronly/Slaveonly

Function: Configure the PTP clock type.

- Ord-Bound: Clock's Device Type is Ordinary-Boundary Clock.
- P2PTransp: Clock's Device Type is Peer to Peer Transparent Clock.
- E2ETransp: Clock's Device Type is End to End Transparent Clock.
- MasterOnly: Clock's Device Type is Master Only.
- SlaveOnly: Clock's Device Type is Slave Only.

Profile

Configuration range: No Profile/1588/802.1AS

Function: Select the PTP description file.

- No Profile: No PTP profile will be applied and PTP will not run.
- 1588: Indicates the IEEE 1588 standard.
- 802.1AS: Indicates the IEEE 802.1AS standard.

2. Click the instance ID to enter the PTP detailed configuration page, as shown in Figure 2:

Figure 2 PTP Instance Detailed Configuration

2.1 View clock type and profile, as shown in the following figure.

Clock Type and Profile

Clock Instance	HW Domain	Device Type	Profile	Apply Profile Defaults	Filter Type
1	1	Ord-Bound	1588	Apply	BASIC

Figure 3 View Clock Type and Profile

Clock Instance

Function: Display the PTP instance ID.

Description: A network can be divided into multiple PTP domains so as to serve different types of service traffic. The devices through which the same clock signal passes should be added to the same PTP domain. Each clock instance is treated as a PTP parameter configuration profile, with specific parameter configured, and bound to a PTP domain. In this way, the clock instances are isolated from each other, meeting the clock synchronization requirements of different types of service traffic.

HW Domain

Function: Display the hardware domain ID used by the clock.

Description: By default, the hardware domain ID is the same with the PTP instance ID.

Device Type

Function: Display the clock type, including:

- Ord-Bound: Clock's Device Type is Ordinary-Boundary Clock.
- P2PTransp: Clock's Device Type is Peer to Peer Transparent Clock.
- E2ETransp: Clock's Device Type is End to End Transparent Clock.
- MasterOnly: Clock's Device Type is Master Only.
- SlaveOnly: Clock's Device Type is Slave Only.

Profile

Function: Display the PTP profile type used by the clock, No Profile, 1588 or 802.1AS.

Apply Profile Defaults

Function: If a PTP profile is configured for the clock, click the <Apply> button to restore user configurations to the default profile.

Filter Type

Function: Display the filter type, which can be either the basic filter or an advanced filter.

2.2 Enable and configure port PTP, as shown in the following figure.

Figure 4 Enable and Configure Port PTP

Port Enable

Function: Select one port to enable PTP.

Configuration

Click <Ports Configuration> to enter detailed port configuration page, as shown in Figure 5.

2.2.1 When the configured PTP profile type is No Profile or 1588, the port configuration page is shown as below.

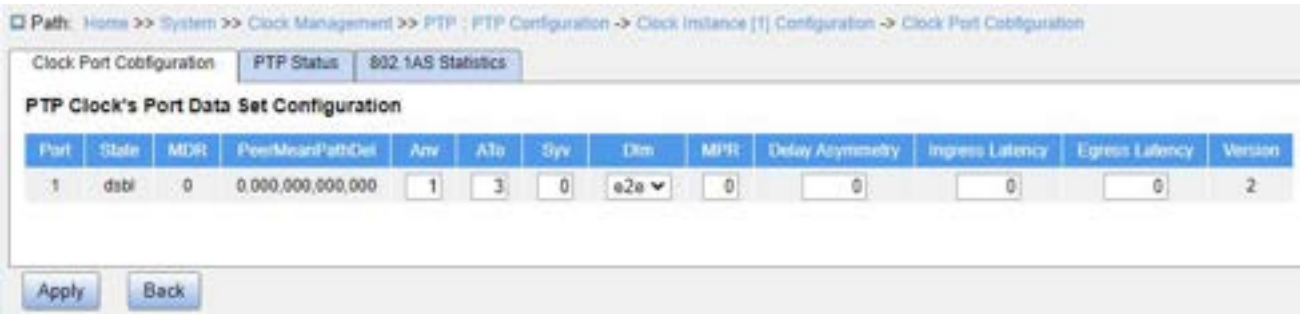


Figure 5 Configure Port PTP – IEEE 1588/No Profile

Port

Function: Display the port ID.

State

Display options: init/flty/lstn/pass/uncl/slve/pmst/mstr/dsbl/p2pt/e2et

Function: Display the link status of the port.

- init: Port is initializing and not ready to participate in PTP.
- flty: An error occurs on the port.
- lstn: It is the first state of the port ready to participate in PTP. The port starts to listen the master clock.
- pass: Port is aware of a clock better than the one it would advertise if it was in the master state.
- uncl: Port receives timestamps from the the master, but the router's clock is not yet

synchronized to the master.

- slve: Port receives timestamps from the the master, and the router's clock is synchronized to the master.
- pmst: Port is about to go into the master state.
- mstr: Port is in the master state and provides timestamps for other listening clocks.
- dsbl: PTP is not running on the port.
- p2pt: Port is in the P2P transparent state.
- e2et: Port is in the E2E transparent state.

MDR

Function: Display the minimum delay request interval announced by the master.

Description: The value is the logarithm to the base 2 of the current Pdelay_Req message transmission interval, in seconds.

PeerMeanPathDel

Function: Display the path delay measured by the port in P2P mode.

Description: The value of this parameter refers to the measured propagation delay, in ns, on the link attached to this port. In E2E mode, the value is 0.

Anv

Configuration range: -3~4

Default configuration: 1

Function: Configure the interval for issuing Announce messages in master state.

Description: The value is the logarithm to base 2 of the mean time interval, in seconds, between the sending of successive Announce messages.

ATo

Configuration range: 1~10

Default configuration: 3

Function: Configure the timeout value for receiving Announce messages on the port.

Description: The value of this attribute tells a slave port the number of announce intervals (in seconds) to wait without receiving an Announce message, before assuming that the master is no longer transmitting Announce messages, and that the Best Master Clock Algorithm (BMCA) needs to be run.

Syv

Configuration range: -7~4

Default configuration: 0

Function: Configure the interval for issuing Sync messages in master.

Description: The value is the logarithm to base 2 of the mean time interval, in seconds, between the sending of successive time-synchronization event messages.

Dlm

Configuration range: p2p/e2e

Function: Configure member delay measurement mechanism.

- e2e: Indicates the Delay mechanism. It calculates the time difference basd on the total link delay between the master and the slave clocks. This mechanism corresponds to the delay time synchronization mode.
- p2p: Indicates the Pdelay mechanism. It calculates the time difference based on the delay of each link between the master and slave clocks. This mechanism corresponds to the Pdelay time synchronization mode.

Description: The delay mechanism can be defined per port in an Ordinary-Boundary clock. In a transparent clock, all ports use the same delay mechanism, which is determined by the clock type and cannot be configured.

MPR

Configuration range: -7~5

Default configuration: 0

Function: Configure the interval for issuing Delay_Req messages for the port in E2E mode, or the interval for issuing Pdelay_Req messages for the port in P2P mode. This value is sent to the slave via the Announce packet from the master.

Description: The value is the logarithm to the base 2 of the mean value of the interval, in seconds, between Pdelay_Req/Delay_Req message transmissions.

Delay Asymmetry

Configuration range:-100000~100000 ns

Default configuration: 0

Function: Configure the asymmetry in the propagation delay on the link attached to this port.

Description: If the transmission delay for a link in not symmetric, the asymmetry can be configured here. The value should be positive when the master to slave propagation time is longer than the slave to master propagation time.

Ingress Latency

Configuration range:-100000~100000 ns

Default configuration: 0

Function: Configure ingress latency measured in ns.

Egress Latency

Configuration range:-100000~100000 ns

Default configuration: 0

Function: Configure egress latency measured in ns.

Version

Function: Display the PTP version. Only PTPv2 is supported.

2.2.2 When the configured PTP profile type is 802.1AS, the port configuration page is shown as below.

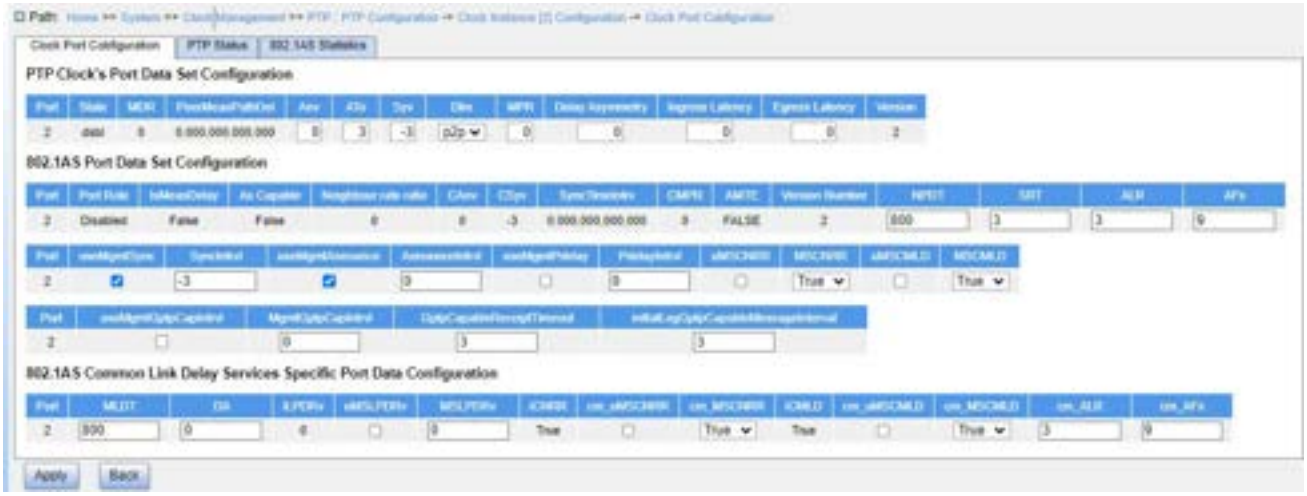


Figure 6 Configure Port PTP – IEEE 802.1AS

(1) Configure PTP clock's port data set, as shown in the following figure.

Figure 7 Configure Port Data Set

Port

Function: Display the port ID.

State

Display options: init/flty/lstn/pass/uncl/slve/pmst/mstr/dsbl/p2pt/e2et

Function: Display the link status of the port.

- init: Port is initializing and not ready to participate in PTP.
- flty: An error occurs on the port.
- lstn: It is the first state of the port ready to participate in PTP. The port starts to listen the master clock.
- pass: Port is aware of a clock better than the one it would advertise if it was in the master state.
- uncl: Port receives timestamps from the the master, but the router's clock is not yet synchronized to the master.
- slve: Port receives timestamps from the the master, and the router's clock is synchronized to the master.
- pmst: Port is about to go into the master state.
- mstr: Port is in the master state and provides timestamps for other listening clocks.
- dsbl: PTP is not running on the port.
- p2pt: Port is in the P2P transparent state.
- e2et: Port is in the E2E transparent state.

MDR

Function: Display the minimum delay request interval announced by the master.

Description: The value is the logarithm to the base 2 of the current Pdelay_Req message transmission interval, in seconds.

PeerMeanPathDel

Function: Display the path delay measured by the port in P2P mode.

Description: This parameter refers to the measured propagation delay, in ns, on the link attached to this port. In E2E mode, the value is 0.

Anv

Configuration range: -3~4

Default configuration: 0

Function: Configure the interval for issuing Announce messages in master state.

Description: The value is the logarithm to base 2 of the mean time interval, in seconds, between the sending of successive Announce messages.

ATo

Configuration range: 1~10

Default configuration: 3

Function: Configure the timeout value for receiving Announce messages on the port.

Description: The value of this attribute tells a slave port the number of announce intervals (in seconds) to wait without receiving an Announce message, before assuming that the master is no longer transmitting Announce messages, and that the BMCA needs to be run.

Syv

Configuration range: -7~4

Default configuration: -3

Function: Configure the interval for issuing Sync messages in master.

Description: The value is the logarithm to base 2 of the mean time interval, in seconds, between the sending of successive time-synchronization event messages.

Dlm

Configuration range: p2p/e2e

Function: Configure member delay measurement mechanism.

- e2e: Indicates the Delay mechanism. It calculates the time difference basd on the total link delay between the master and the slave clocks. This mechanism corresponds to the delay time synchronization mode.
- p2p: Indicates the Pdelay mechanism. It calculates the time difference based on the delay of each link between the master and slave clocks. This mechanism corresponds to the Pdelay time synchronization mode.

Description: The delay mechanism can be defined per port in an Ordinary-Boundary clock. In a transparent clock, all ports use the same delay mechanism, which is determined by the clock type and cannot be configured.

MPR

Configuration range: -7~5

Default configuration: 0

Function: Configure the interval for issuing Delay_Req messages for the port in E2E mode, or the interval for issuing Pdelay_Req messages for the port in P2P mode. This value is sent to the slave via the Announce packet from the master.

Description: The value is the logarithm to the base 2 of the mean value of the interval, in seconds, between Pdelay_Req/Delay_Req message transmissions.

Delay Asymmetry

Configuration range:-100000~100000 ns

Default configuration: 0

Function: Configure the asymmetry in the propagation delay on the link attached to this port.

Description: If the transmission delay for a link in not symmetric, the asymmetry can be configured here. The value should be positive when the master to slave propagation time is longer than the slave to master propagation time.

Ingress Latency

Configuration range:-100000~100000 ns

Default configuration: 0

Function: Configure ingress latency measured in ns.

Egress Latency

Configuration range:-100000~100000 ns

Default configuration: 0

Function: Configure egress latency measured in ns.

Version

Function: Display the PTP version. Only PTPv2 is supported.

(2) Configure 802.1AS port data set, as shown in the following figure.

Figure 8 Configure 802.1AS Port Data Set

Port

Function: Display the port ID.

Port Role

Display options: Disabled/Master/Slave/Passive/Unknown

Function: Display the role of the port.

- Disabled: The port is not running PTP.
- Master: Indicates the master port, which sends time information.
- Slave: Indicates the slave port, which receives time information.
- Passive: The port does not send and receive time information.
- Unknown: Unknown port.

IsMeasDelay

Display options: True/False

Function: Display whether the port is receiving Pdelay responses from the peer.

Description: This parameter is a Boolean. It is true if the port is measuring PTP Link propagation delay. For a full-duplex point-to-point PTP Link, the port is measuring PTP Link propagation delay if it is receiving Pdelay_Resp and Pdelay_Resp_Follow_Up messages from the port at the other end of the PTP Link (i.e., it performs the measurement using the peer-to-peer delay mechanism). There is one instance of this variable for all the domains (per port). The variable is accessible by all the domains.

As Capable

Display options: True/False

Function: Display whether the port supports IEEE 802.1AS.

Description: This parameter is a Boolean. It is true only when the port determines that the PTP instances on both ends of the link is capable of interoperation via IEEE 802.1AS.

Neighbor Rate Ratio

Function: Display the measured ratio of the frequency of the LocalClock entity of the timeaware system at the other end of the link attached to this port, to the frequency of the LocalClock entity of this time-aware system. The data type for neighborRateRatio is Float64.

CAnv

Function: Display the current value of the logarithm to base 2 of the mean time interval, in seconds, between the sending of successive Announce messages.

Csyv

Function: Display the current value of the logarithm to base 2 of the mean time interval, in seconds, between the sending of successive time-synchronization event messages.

SyncTimeIntrv

Function: Display the time interval after which sync receipt timeout occurs if time-synchronization information has not been received during the interval.

Description: The value of this attribute tells a slave port the number of sync intervals (in seconds) to wait without receiving synchronization information, before assuming that the master is no longer transmitting synchronization information and that the BMCA needs to be run.

CMPR

Function: Display the current value of the mean time interval between successive Delay_Req/Pdelay_Req messages.

Description: The value is the logarithm to the base 2 of the current Pdelay_Req message transmission interval, in seconds.

AMTE

Display options: True/False

Function: Display whether the acceptableMasterTable feature is enabled (always “False”).

Description: A PTP Instance that contains an ONU port shall maintain a configured table, the acceptable master clock table, and a per-PTP Port Boolean variable acceptableMasterTableEnabled (AMTE).This feature applies to a PTP instance containg the Optical Network Unit (ONU) port.

Version Number

Function: Display the PTP version (always “2”).

NPDT

Configuration range: 0~4000000000 ns

Default configuration: 800

Function: Configure the threshold for the mean link delay measured by the port.

Description: If the mean link delay measured by the port exceeds the threshold, the port is considered to be not capable of participating in the IEEE 802.1AS protocol.

SRT

Configuration range: 1~255

Default configuration: 3

Function: Configure the timeout value when the slave port waits for synchronization information from the master port. The value should be a multiple of the synchronization interval.

Description: If the slave port does not receive synchronization information within the timeout period, it assumes that the master is no loging transmitting synchronization information and that the BMCA needs to be run.

ALR

Configuration range: 0~10

Default configuration: 3

Function: Configure the threshold for the allowed number of lost Pdelay responses on the port.

Description: After the port sends a Pdelay_Req message, it will wait for a response. If no valid response is received, the port assumes that the response is lost. If the number of lost responses exceeds the configured threshold, the port is considered to be not exchanging peer delay messages with its neighbor.

AFs

Configuration range: 1~255

Default configuration: 9

Function: Configure the threshold for the allowed number of faults.

Description: Faults refer to conditions such as the mean link delay exceeds the threshold, the computation of neighborRateRatio is invalid, etc. When the number of faults exceeds the configured threshold, the port is considered to be not capable of interoperating with its neighbor via IEEE 802.1AS.

useMgmtSync

Configuration options: Enable/Disable

Default configuration: Enable

Function: Whether to enable useMgtSettableLogSyncInterval.

Description: useMgtSettableLogSyncInterval is a Boolean that determines the source of the synchronization interval. If enabled, the value of CSyv is set equal to the value of mgtSettableLogSyncInterval. If disabled, the value of CSyv is determined by the SyncIntervalSetting state machine.

SyncIntrvl

Configuration range: -7~4

Default configuration: -3

Function: Configure the value of mgtSettableLogSyncInterval.

Description: The value is the logarithm to base 2 of the sync interval if useMgmtSync is enabled. The value is not used if useMgmtSync is disabled.

useMgmtAnnounce

Configuration options: Enable/Disable

Default configuration: Enable

Function: Whether to enable useMgtSettableLogAnnounceInterval.

Description: useMgtSettableLogAnnounceInterval is a Boolean that determines the source of the announce interval. If enabled, the value of CAnv is set equal to the value of mgtSettableLogAnnounceInterval. If disabled, the value of CAnv is determined by the AnnounceIntervalSetting state machine.

AnnounceIntrvl

Configuration range: -3~4

Default configuration: 0

Function: Configure the value of mgtSettableLogAnnounceInterval.

Description: The value is the logarithm to base 2 of the announce interval used if useMgmtAnnounce is enabled. The value is not used if useMgmtAnnounce is disabled.

useMgmtPdelay

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable useMgtSettableLogPdelayReqInterval.

Description: useMgtSettableLogPdelayReqInterval is a Boolean that determines the source of the mean time interval between successive Pdelay_Req messages. If enabled, the value of SynTimeIntrv is set equal to the value of mgtSettableLogPdelayReqInterval. If disabled, the value of SynTimeIntrv is determined by the LinkDelayIntervalSetting state machine.

PdelayIntrvl

Configuration range: -7~5

Default configuration: 0

Function: Configure the value of mgtSettableLogPdelayReqInterval.

Description: The value is the logarithm to base 2 of the mean time interval between successive Pdelay_Req messages if useMgmtPdelay is enabled. The value is not used if useMgmtPdelay is disabled.

uMSCNRR

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable useMgtSettableComputeNeighborRateRatio.

Description: useMgtSettableComputeNeighborRateRatio is a Boolean that determines the source of the value of computeNeighborRateRatio, that is, whether the neighbor rate ratio is computed by the port. If enabled, the value of computeNeighborRateRatio is set equal to the value of mgtSettablecomputeNeighborRateRatio. If disabled, the value of currentComputeNeighborRateRatio is determined by the LinkDelayIntervalSetting state machine.

MSCNRR

Configuration options: True/False

Default configuration: True

Function: Configure the value of mgtSettablecomputeNeighborRateRatio.

uMSCMLD

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable useMgtSettableComputeMeanLinkDelay.

Description: useMgtSettableComputeMeanLinkDelay is a Boolean that determines the source of the value of computeMeanLinkDelay, that is, whether the mean link delay computed by the port. If enabled, the value of computeMeanLinkDelay is set equal to the value of mgtSettableComputeMeanLinkDelay. If disabled, the value of currentComputeMeanLinkDelay is determined by the LinkDelayIntervalSetting state machine.

MSCMLD

Configuration options: True/False

Default configuration: True

Function: Configure the value of mgtSettableComputeMeanLinkDelay.

useMgmtGptpCapIntrvl

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable useMgtSettableLogGptpCapableMessageInterval。

Description: useMgtSettableLogGptpCapableMessageInterval is a Boolean that determines the source of the gPTP capable message interval. If enabled, the value of currentLogGptpCapableMessageInterval is set equal to the value of mgtSettableLogGptpCapableMessageInterval. If disabled, the value of currentLogGptpCapableMessageInterval is determined by the GptpCapableMessageIntervalSetting state machine.

MgmtGptpCapIntrvl

Configuration range: -128~127

Default configuration: 0

Function: Configure the value of mgtSettableLogGptpCapableMessageInterval.

Description: The value is the logarithm to base 2 of the gPtpCapableMessageInterval if useMgmtGptpCapIntrvl is enabled. The value is not used if useMgmtGptpCapIntrvl is disabled. gPtpCapableMessageInterval is a variable. Its value is the mean time, in seconds, between the sending of successive Signaling messages that carry the gPTP-capable TLV.

GptpCapableReceiptTimeout

Configuration range: 1~255

Default configuration: 3

Function: Configure the timeout value of gPTP messages. The value should be a multiple of the gPTP message transmission interval.

Description: After the port send a gPTP message to its neighbor, it waits for a Signalling response which contains gPTP TLV. If no response is received within the specified timeout period, it considers that its neighbor is no longer running gPTP.

initialLogGptpCapableMessageInterval

Configuration range: -128~127

Default configuration: 3

Function: Configure the value of initialLogGptpCapableMessageInterval.

Description: The value is the logarithm to base 2 of the gPTP capable message interval used when (a) the PTP Port is initialized, or (b) a gPtpCapableMessage interval request TLV is received with the logGptpCapableMessageInterval field set to 126.

(3) Configure common link delay service specific port data, as shown in the following figure.

Figure 9 Configure Common Link Delay Service Port Data

Port

Function: Display the port ID.

MLDT

Configuration range: 0~4000000000 ns

Default configuration: 800

Function: Configure the threshold for the mean link delay measured by the port.

Description: If the mean link delay measured by the port exceeds the threshold, the port is considered to be not capable of participating in the IEEE 802.1AS protocol.

DA

Configuration range:-100000~100000 ns

Default configuration: 0

Function: Configure the asymmetry in the propagation delay on the link attached to this port.

Description: If the transmission delay for a link in not symmetric, the asymmetry can be configured here. The value should be positive when the master to slave propagation time is longer than the slave to master propagation time.

iLPDRv

Function: Display the initial value of Pdelay_Req message transmission interval.

Description: The value is the logarithm to the base 2 of the Pdelay_Req message transmission interval, in seconds.

uMSLPDRv

Configuration options: Enable/Disable

Default configuration:Disable

Function: Whether to enable useMgtSettableLogPdelayReqInterval.

Description: useMgtSettableLogPdelayReqInterval is a Boolean that determines the source of the mean time interval between successive Pdelay_Req messages, in seconds. If enabled, the value of SynTimeIntrv is set equal to the value of mgtSettableLogPdelayReqInterval. If disabled, the value of SynTimeIntrv is determined by the LinkDelayIntervalSetting state machine.

MSLPDRv

Configuration range: -7~5

Default configuration: 0

Function: Configure the value of mgtSettableLogPdelayReqInterval.

Description: The value is the logarithm to base 2 of the mean time interval between successive Pdelay_Req messages in seconds if useMgmtPdelay is enabled. The value is not used if useMgmtPdelay is disabled.

iCNRR

Function: Display the initial value of ComputeNeighborRateRatio, that is, whether the neighbor rate ratio is computed by the port.

cm_uMSCNRR

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable useMgtSettableComputeNeighborRateRatio.

Description: useMgtSettableComputeNeighborRateRatio is a Boolean that determines the source of the value of computeNeighborRateRatio, that is, whether the neighbor rate ratio is computed by the port. If enabled, the value of computeNeighborRateRatio is set equal to the value of mgtSettablecomputeNeighborRateRatio. If disabled, the value of currentComputeNeighborRateRatio is determined by the LinkDelayIntervalSetting state machine.

cm_MSCNRR

Configuration options: True/False

Default configuration: True

Function: Configure the value of mgtSettablecomputeNeighborRateRatio.

iCMLD

Function: Display the initial value of ComputeMeanLinkDelay, that is, whether the mean link delay is computed by the port.

cm_uMSCMLD

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable useMgtSettableComputeMeanLinkDelay.

Description: useMgtSettableComputeMeanLinkDelay is a Boolean that determines the source of the value of computeMeanLinkDelay, that is, whether the mean link delay is computed by the port. If enabled, the value of computeMeanLinkDelay is set equal to the value of mgtSettableComputeMeanLinkDelay. If disabled, the value of currentComputeMeanLinkDelay is determined by the LinkDelayIntervalSetting state machine.

cm_MSCMLD

Configuration options: True/False

Default configuration: True

Function: Configure the value of mgtSettableComputeMeanLinkDelay.

cm_ALR

Configuration range: 0~10

Default configuration: 3

Function: Configure the threshold for the allowed number of lost Pdelay responses on the port.

Description: After the port sends a Pdelay_Req message, it will wait for a response. If no valid response is received, the port assumes that the response is lost. If the number of lost responses exceeds the configured threshold, the port is considered to be not exchanging peer delay messages with its neighbor.

cm_AFs

Configuration range: 1~255

Default configuration: 9

Function: Configure the threshold for the allowed number of faults.

Description: Faults refer to conditions such as the mean link delay exceeds the threshold, the computation of neighborRateRatio is invalid, etc. When the number of faults exceeds the configured threshold, the port is considered to be not capable of interoperating with its neighbor via IEEE 802.1AS.

2.3 Configure local clock data set, as shown in the following figure.

Figure 10 Configure Local Clock Data Set

PTP Time

Function: Display the actual PTP time with nanosecond resolution.

Clock Adjustment Method

Display options: Internal Timer/PTP DPLL/DAC Option/Software/Synce DPLL/Unknown

Function: Display the actual clock adjustment method used by the clock, which is determined by the available hardware.

System Clock Sync to PTP Time/PTP Time Sync to System Clock.

Configuration options: True/False

Default configuration: False

Function: Configure the synchronization method.

Description: There are two methods for clock synchronization. Only one can be configured.

2.4 View the local clock data set, as shown in the following figure.

Clock Current Data Set

stpRm	Offset From Master	Mean Path Delay
0	0.000,000,000,000	0.000,000,000,000

Figure 11 View Current Data Set of Local Clock

stpRm

Function: Display the number of PTP clocks traversed from the grandmaster clock to the local clock.

Offset From Master

Function: Display the time difference between the grandmaster clock and the local clock, measured in ns.

Mean Path Delay

Function: Display the mean propagation time for the link between the grandmaster clock and the local slave clock, measured in ns.

2.5 View the parent clock data set, as shown in the following figure.

Clock Parent Data Set

Parent Port Identity	Port	PStat	Var	Change Rate	Grand Master Identity	Grand Master Clock Quality	Priority1	Priority2
02:00:c1:ff:fe:29:b2:8f	0	False	0	0	02:00:c1:ff:fe:29:b2:8f	Cl:248 Ac:Unknwn Va:65535	128	128

Figure 12 View Current Data Set of Parent Clock

Parent Port Identity

Function: Display the identity for the parent clock. If the local clock is not the slave clock, the clock's own ID will be displayed.

Port

Function: Display the parent clock's master port ID.

PStat

Funciton: Display statistics of the parent clock, which is always False.

Var

Function: Display the offset scaled log variance of the parent clock.

Change Rate

Function: Display the phase change rage of the parent clock, that is, the slave clock's rate offset compared to the master, measured in ns per second.

Grand Master Identity

Function: Display the clock identity of the grand master clock. If the local clock is not a slave, the clock's own ID will be displayed.

Grand Master Clock Quality

Function: Display the clock quality announced by the grand master.

- Clock class: Defines the Internatinal Atomic Time (TAI) traceability of the clock. The default value is 248. For details, refer to the IEEE 1588 standard.
- Clock accuracy: Defines the clock accuracy level. A smaller value indicates a higher accuracy. The default value is Unknown.
- OffsetScaledLogVariance: Defines the stability of the clock.

Description: For details, see the the IEEE 1588 standard.

Priority1

Function: Display clock priority 1 of the grand master clock.

Priority2

Function: Display clock priority 2 of the grand master clock.

2.6 Configure the clock default data set, as shown in the following figure.

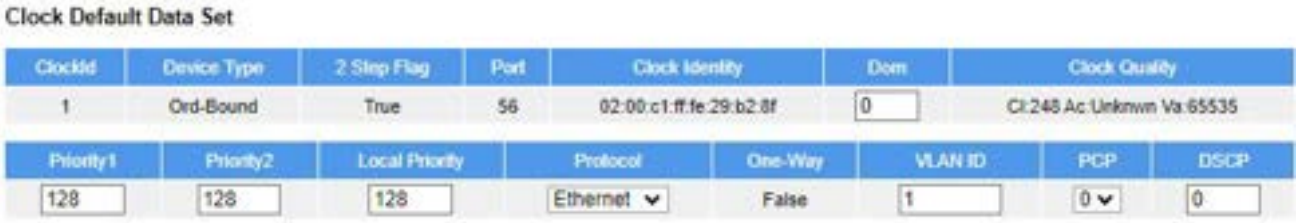


Figure 13 Configure Clock Default Data Set

ClockID

Function: Display the clock ID.

Device Type

Function: Display the clock type.

2 Step Flag

Display options: True/False

Function: Display the status of 2 step clocks.

- 1 step: Sync and Pdelay_Resp packets carry the timestamps indicating when the packets are sent.
- 2 step: Sync and Pdelay_Resp packets do not carry the timestamps indicating when the packets are sent. Instead, the timestamps are carried by subsequent Follow_Up and Pdelay_Resp_Follow_Up packets. This mode applies to devices that cannot add timestamps to Sync and Pdelay_Resp packets.

Port

Function: Display the number of ports.

Clock Identity

Function: Display the unique identifier of the clock.

Dom

Configuration range: 0~127

Function: Configure the domain ID of PTP instance.

Clock Quality

Function: Display clock quality.

- Clock class: Defines the Internatinal Atomic Time (TAI) traceability of the clock. The default value is 248. For details, refer to the IEEE 1588 standard.
- Clock accuracy: Defines the clock accuracy level. A smaller value indicates a higher accuracy. The default value is Unknown.
- OffsetScaledLogVariance: Defines the stability of the clock.

Description: For details, see the the IEEE 1588 standard.

Priority 1, Priority 2, Local Priority

Configuration range: 0~255

Default configuration: The default priority value for Priority 1, Priority 2 and Local Priority is 128 when the PTP profile is No Profile or 1588. The default priority value for Priority 1, Priority 2 and Local Priority is 246, 248 and 128 when the PTP profile is 802.1AS.

Function: Configure clock priority 1 used for master clock election. The smaller the value, the higher the priority.

Description: Clocks in the PTP domain elects the grandmaster clock based on Priority 1 and Priority 2 carried in the Announce packets when BMC protocol is used. Priority takes precedence over Priority 2. Local priority is required only when the PTP profile is G.8275.1 or G.8275.2.

Protocol

Configuration range: Ethernet/IPv4Multi

Default configuration: Ethernet

Function: Select the transport protocol used by the PTP protocol engine.

- Ethernet: PTP over Ethernet multicast
- IPv4Multi: PTP over IPv4 multicast

One-Way

Display options: True/False

Function: Display whether one-way measurement is enabled.

Description: If “True” is selected, one-way measurement is used. This parameter applies only to a slave. In one-way mode, no-delay measurement is performed, i.e. this is applicable if only frequency synchronization is needed. The master always responds to delay requests.

VLAN ID

Configuration range: 1~4094

Default configuration: 1

Function: Configure VLAN ID for marking PTP frames.

PCP

Configuration range: 0~7

Default configuration: 0

Description: Configure the Priority Code Point value used for PTP frames.

DSCP

Configuration range: 0~63

Default configuration: 0

Description: Configure the Differentiated Services Code Point value used for IPv4 frames.

2.7 Configure the clock time properties data set, as shown in the following figure.

Figure 14 Configure Clock Time Properties

UTC Offset

Configuration range: -32768~32767

Default configuration: 0

Function: Configure the UTC offset, which is used for time calibration.

Description: The value is the logarithm to base 2 of the UTC offset, in seconds.

Valid

Configuration range: True/False

Default configuration: False

Function: Configure whether UTC offset is valid.

Leap59, Leap61

Configuration range: True/False

Default configuration: False

Function: Whether to enable the leap second.

Description: A leap second is a second added to Coordinated Universal Time (UTC) in order to keep it synchronized with astronomical time.

Time Trac, Freq Trac

Configuration range: True/False

Default configuration: False

Function: Whether to enable time tracking and frequency tracking.

PTP Time Scale

Configuration range: True/False

Default configuration: True

Function: Whether to enable PTP timescale.

Time Source

Configuration range: 16/32/48/64/80/96/144/160

- 16 (0x10) ATOMIC_CLOCK
- 32 (0x20) GPS
- 48 (0x30) TERRESTRIAL_RADIO
- 64 (0x40) PTP
- 80 (0x50) NTP
- 96 (0x60) HAND_SET
- 144 (0x90) OTHER
- 160 (0xA0) INTERNAL_OSCILLATOR

Default configuration: 160

Function: Configure PTP time source.

2.8 Configure basic filter parameters, as shown in the following figure.

Figure 15 Basic Filter Parameter Configuration

Delay Filer

Configuration range: 0~6

Default configuration: 6

Function: Configure the value of delay filter.

Description: The default delay filter is a low pass filter, with a time constant of 2**Delay Filter*Delay Request Rate. The value 0 means to use the same filter function as for the offset measurement. The offset filter uses a minimum offset or a mean filter method, that is, the minimum measured offset during Period samples is used in the calculation. The distance between two calculations is Dist periods. Refer to the following two parameters.

Period

Configuration range: 1~10000

Default configuration: 1

Function: Configure the measurement period number, that is, the number of sync events.

Dist

Configuration range: 0~10 periods

Default configuration: 2

Function: Configure the distance between two calculations, that is, the number of periods.

2.9 Configure basic servo parameters, as shown in the following figure.

Figure 16 Basic Servo Parameter Configuration

Display

Configuration options: True/False

Default configuration: False

Function: Whether to record Offset From Master, Mean Path Delay and Clock Adjustment on the debug terminal.

Description: By default, the clock servo uses a PID regulator to calculate the current clock rate, that is,

clockAdjustment =

OffsetFromMaster / P constant +

Integral(OffsetFromMaster) / I constant +

Differential (OffsetFromMaster) / D constant

P-enable

Configuration options: True/False

Default configuration: True

Function: Whether to include the “P” constant part in the calculation.

P-enable

Configuration options: True/False

Default configuration: True

Function: Whether to include the “P” constant part in the calculation.

I-enable

Configuration options: True/False

Default configuration: True

Function: Whether to include the “I” constant part in the calculation.

D-enable

Configuration options: True/False

Default configuration: True

Function: Whether to include the “D” constant part in the calculation.

“P” constant

Configuration range: 1~1000

Default configuration: 3

Function: Configure the “P” constant.

“I” constant

Configuration range: 1~10000

Default configuration: 30

Function: Configure the “I” constant.

“D” constant

Configuration range: 1~10000

Default configuration: 40

Function: Configure the “D” constant.

Gain constant

Configuration range: 1~10000

Default configuration: 1

Function: Configure the “Gain” constant.

3. View PTP status, as shown in the following figure.

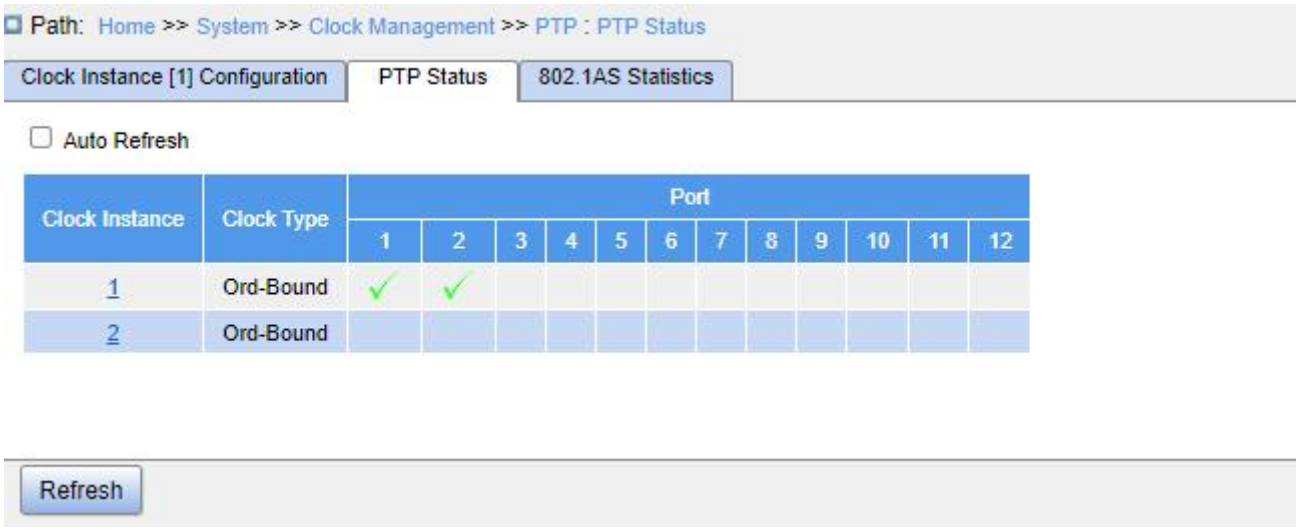


Figure 17 PTP Clock Configuration

Click the instance ID to view PTP instance detailed configuration, as shown in Figure 18.

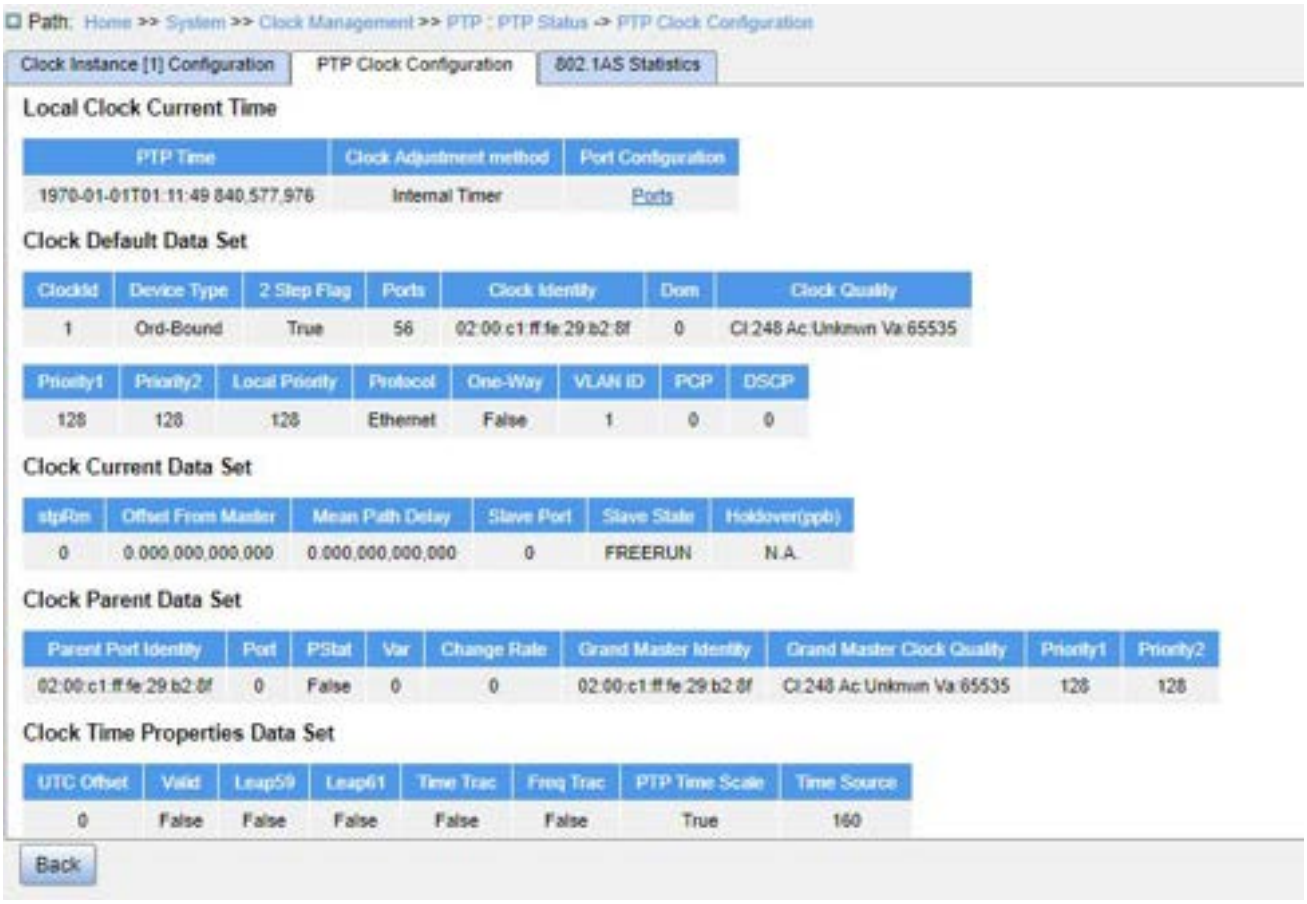


Figure 18 View PTP Instance Detailed Configuration

4. View 802.1AS statistics, including PTP packet counts on each port, as shown in the following figure.

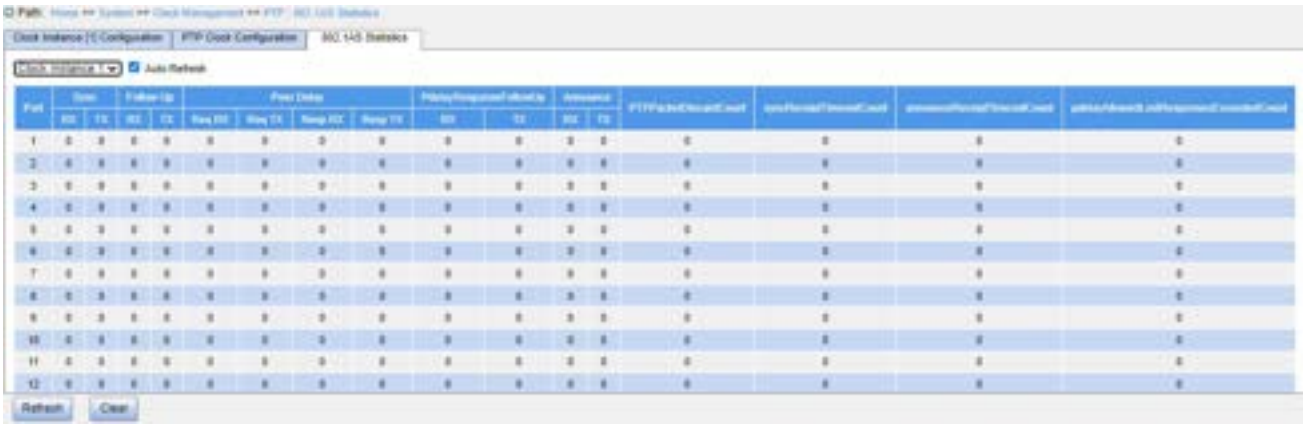


Figure 19 View 802.1AS Statistics

Sync RX

Function: Display the total number of Sync packets received without errors.

Sync TX

Function: Display the total number of Sync packets transmitted without errors.

Follow Up RX

Function: Display the total number of Follow_Up packets received without errors.

Follow Up TX

Function: Display the total number of Follow_Up packets transmitted without errors.

Peer Delay Req RX

Function: Display the total number of Pdelay_Req packets received without errors.

Peer Delay Req Tx

Function: Display the total number of Pdelay_Req packets transmitted without errors.

Peer Delay Resp RX

Function: Display the total number of Pdelay_Resp packets received without errors.

Peer Delay Resp TX

Function: Display the total number of Pdelay_Resp packets transmitted without errors.

PdelayResponseFollowUp RX

Function: Display the total number of Pdelay_Resp_Follow_Up packets received without errors.

PdelayResponseFollowUp TX

Function: Display the total number of Pdelay_Resp_Follow_Up packets transmitted

without errors.

Announce RX

Function: Display the total number of Announce packets received without errors.

Announce TX

Function: Display the total number of Announce packets transmitted without errors.

PTPPacketDiscardCount

Function: Display the total number of PTP packets discarded.

syncReceiptTimeoutCount

Function: Display the total number of received Sync packets with timeouts occurred.

announceReceiptTimeoutCount

Function: Display the total number of received Announce packets with timeouts occurred.

pdelayAllowedLostResponsesExceededCount

Function: Display the total number of times that the number of consecutive Pdelay_Req messages sent by the port exceeds the number of Pdelay_Req messages without valid responses.

4.3.2.4 Typical Configuration Example

As shown in Figure 20, port 1 of Switch A is connected to port 2 of Switch B, and port 3 of Switch B is connected to port 4 of Switch C. Switch A is a master clock (BC clock type). Switch B uses P2PTC clock type. Switch C is a slave clock (BC clock type), and synchronizes time from Switch A by using PTP protocols.

Figure 20 PTP Configuration Example

Configuration on Switch A:

1. Enable PTP on port 1 of Switch A.

2. Set the clock type to Boundary. Because Switch A is the master clock, it should have the best grandmaster priority1. In this example, set the grandmaster priority1 to 200 and the delay measurement mechanism to peer-to-peer, as shown in Figure 1, Figure 2.

Configuration on Switch B:

1. Enable PTP on port 2 and port 3 of Switch B.

2. Set the clock type to P2PTC, the grandmaster priority1 to 210, and the delay measurement mechanism to peer-to-peer, as shown in Figure 1, Figure 2.

Configuration on Switch C:

1. Enable PTP on port 4 of Switch C.

2. Set the clock type to Boundary, the grandmaster priority1 to 220, and the delay measurement mechanism to peer-to-peer, as shown in Figure 1, Figure 2.

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. The boot version is first upgraded and then 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. Upgrade software from the local file, as shown below.

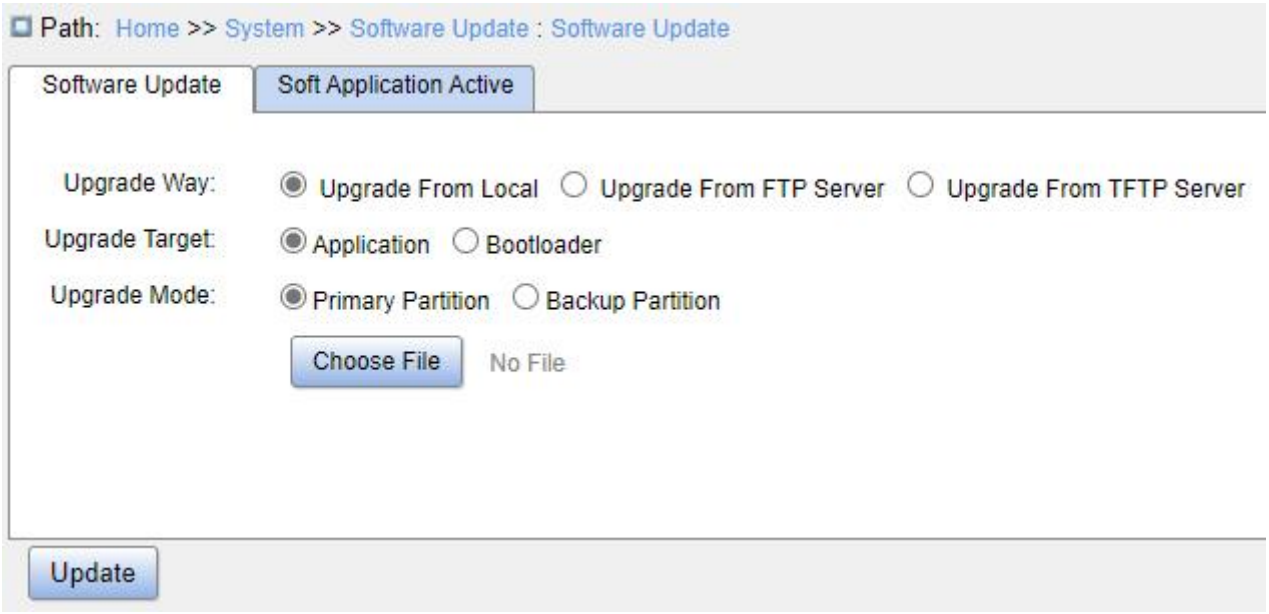


Figure 28 Upgrade Software - Local

Upgrade Way

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

Function: Select upgrade way.

Upgrade Target

Configuration options: Application/Boot Loader

Function: Select upgrade target.

Upgrade Mode

Configuration options: Primary Partition/Backup Partition

Function: Select the upgrade target.

Description: This switch can download two software versions, which can be the same or different.

Click <Choose File> to select the local update file and then click <Update>.

2. After a successful upgrade, activate the software version and restart the device, then check if the software version is the upgraded version in the system information.

Warning:

- After the software upgrade is successful, you must activate the software version and restart the device before the software version can take effect;

- Do not restart the switch if the upgrade fails to avoid version file loss.

4.4.2 FTP Update

Install an FTP server. The following example uses WFTPD software 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 29. Create a user name and password, for example, user name admin and password 123456. Click <OK>.

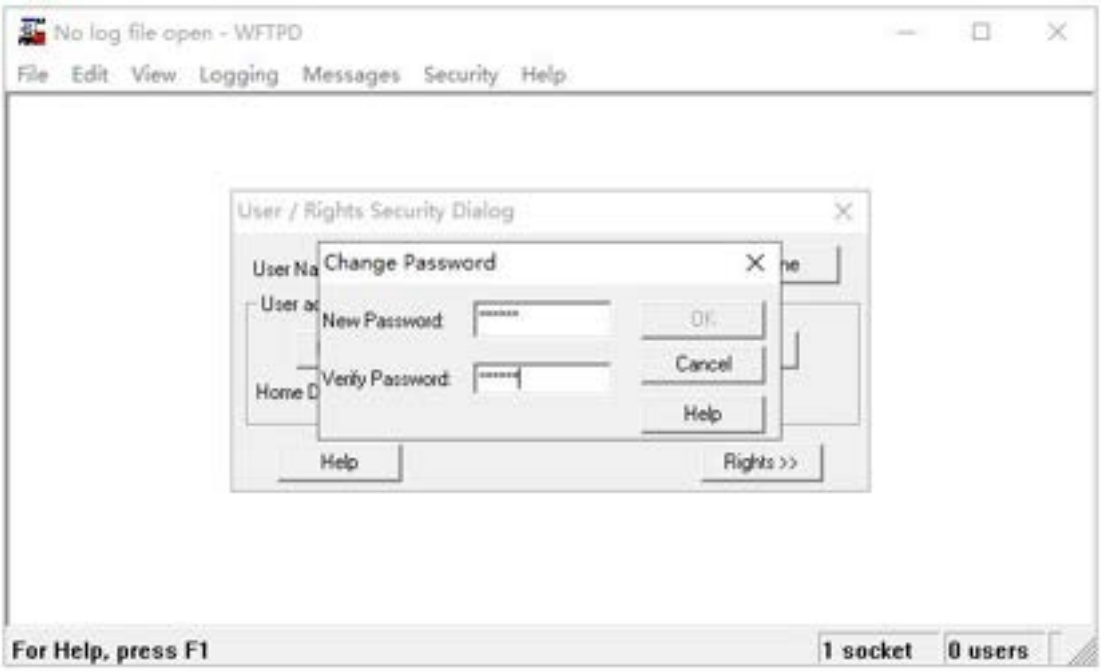


Figure 29 Create a New FTP User

2. Input the storage path of the update file in “Home Directory”, as shown in Figure 30. Click <Done>.

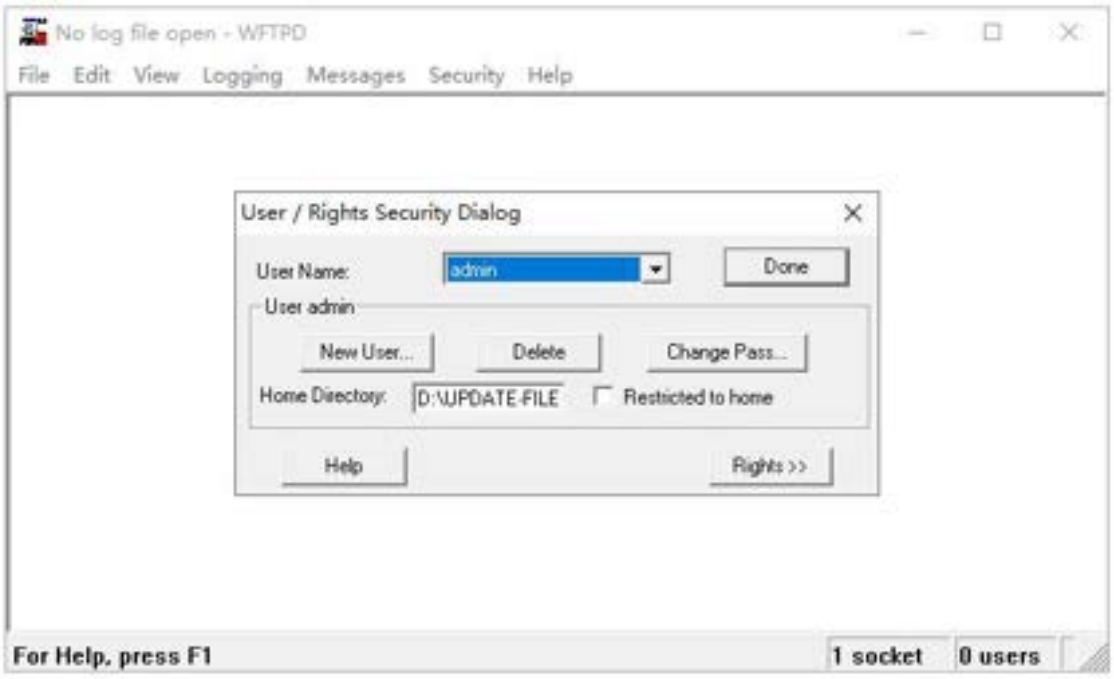


Figure 30 File Location

3. Click [System] → [Software Update] in the navigation tree to enter the software update page, as shown in Figure 31. Enter the IP address of FTP server, FTP user name, password, and file name on the server. Click <Update>.

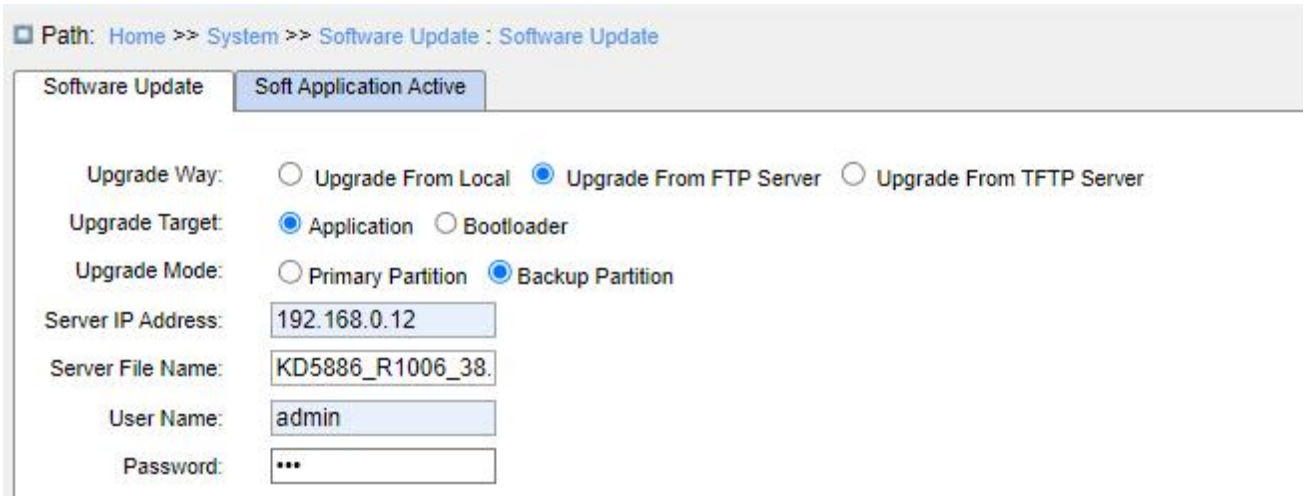


Figure 31 Software Update by FTP

Upgrade Way

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

Description: Select upgrade mode.

Upgrade Target

Configuration options: Application/Bootloader

Function: Select the upgrade target.

Description: This switch can download two software versions, which can be the same or different.

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 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.

Warning:

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

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

Figure 32 Normal Communication between FTP Server and Switch

Caution:

To display update log information as shown in Figure 32, you need to click [Logging] → [Log Options] in WFTPD and select Enable Logging and the log information to be displayed.

5. When the update is complete, reboot the device and open the switch “Basic Information” page to check whether the update succeeds and the new version is active.

Warning:

- In the software update process, keep the FTP server software running.
- When update is complete, select the software version to be activated and reboot the device to activate it.
- If update fails, do not reboot the device to avoid the loss of software file and abnormal startup.

4.4.3 TFTP Update

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

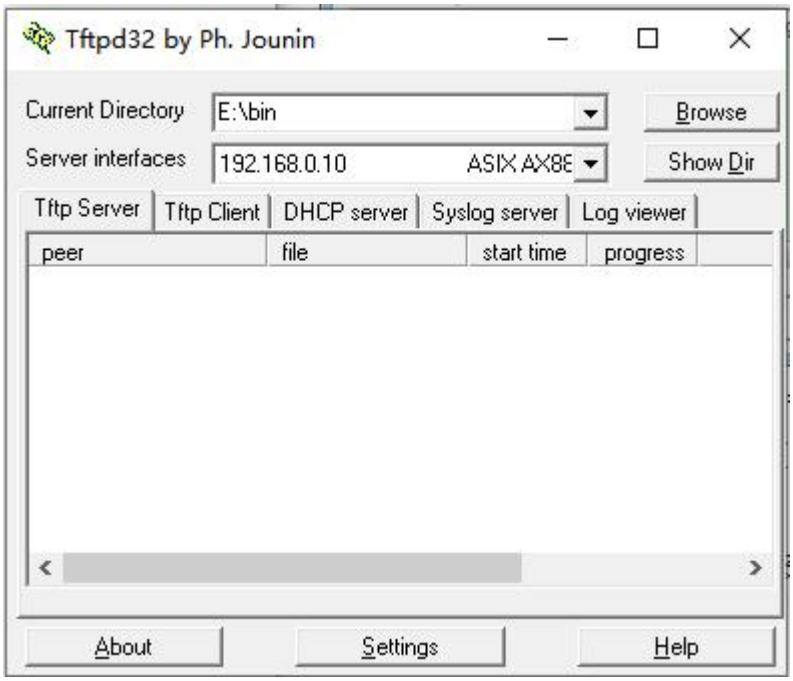


Figure 33 TFTP Server Configuration

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

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.

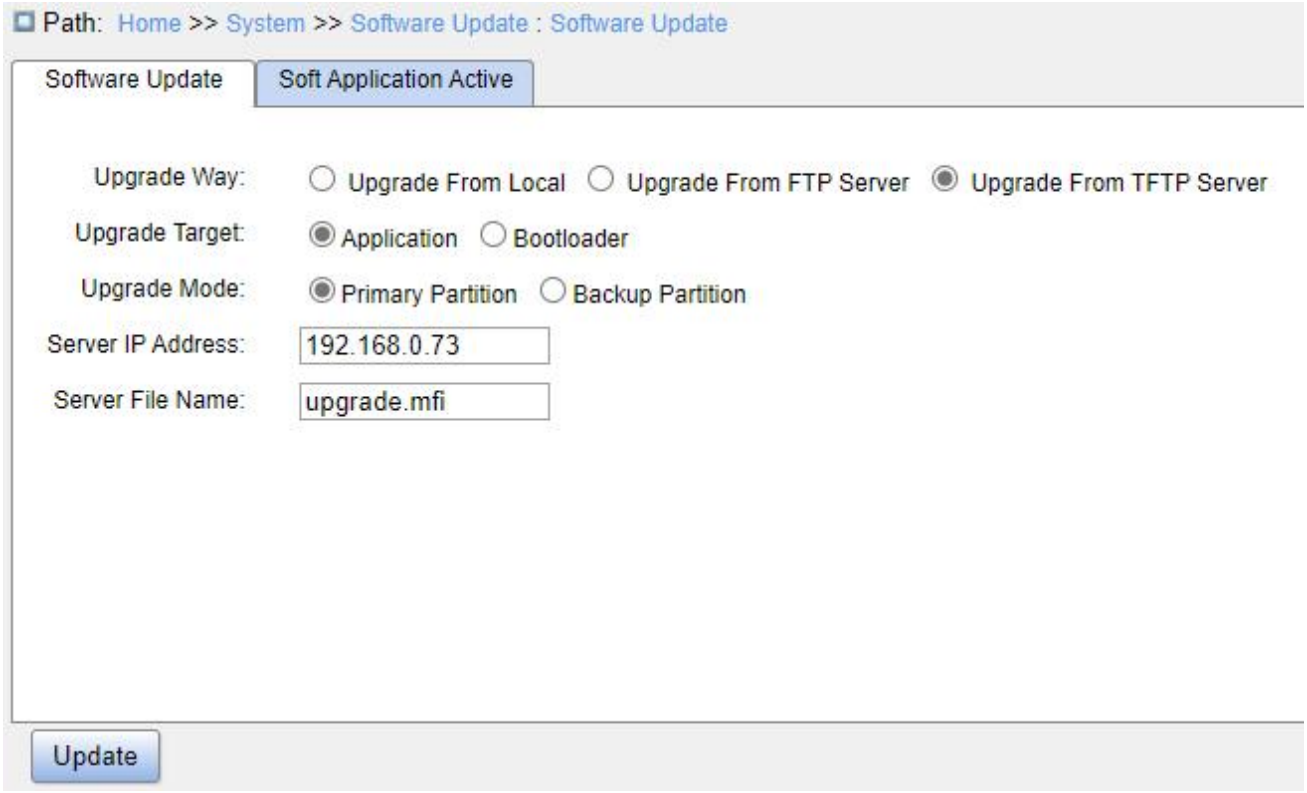


Figure 34 Software Update by TFTP

3. When the update is complete, activate the new version and reboot the device. Then, open the switch “Basic Information” page to check whether the update succeeds and the new version is active.

Warning:

- In the software update process, keep the TFTP server software running.
- When update is complete, select the software version to be activated and reboot the device.
- If update fails, do not reboot the device to avoid the loss of software file.

4.5 Soft Application Activation

Activate the firmware application, as shown in Figure 35.

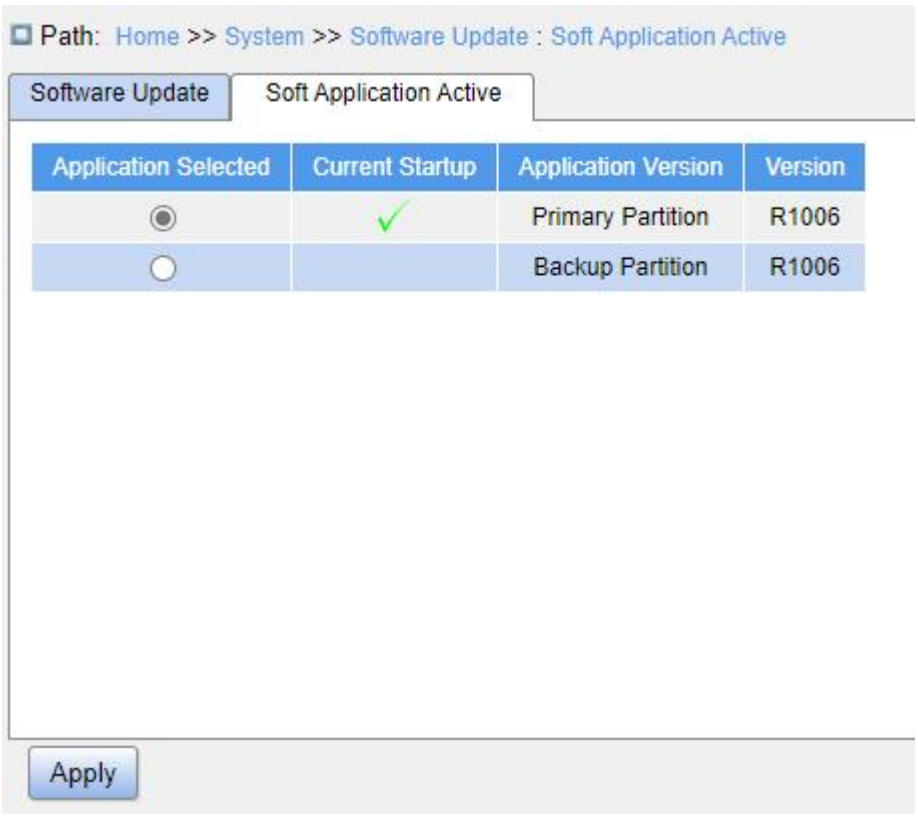


Figure 35 Activate the Firmware Application

Select one version and click <Apply> button to configure 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

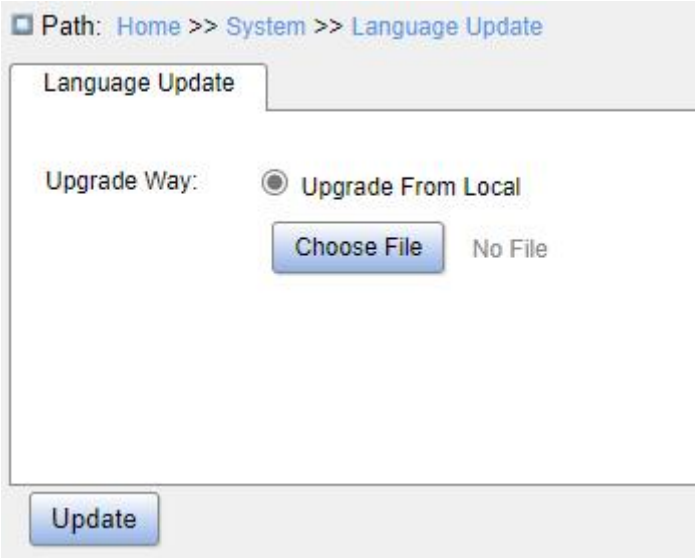


Figure 36 Update Language

Upgrade Way

Configuration options: Upgrade From Local

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

4.7 Restart

Restart the device, as shown below.

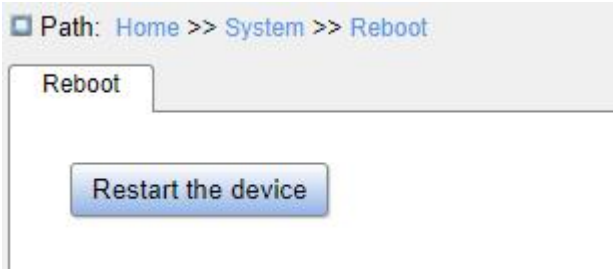


Figure 37 Restart Device

Before restarting the device, confirm whether to save the current configuration. If yes, 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

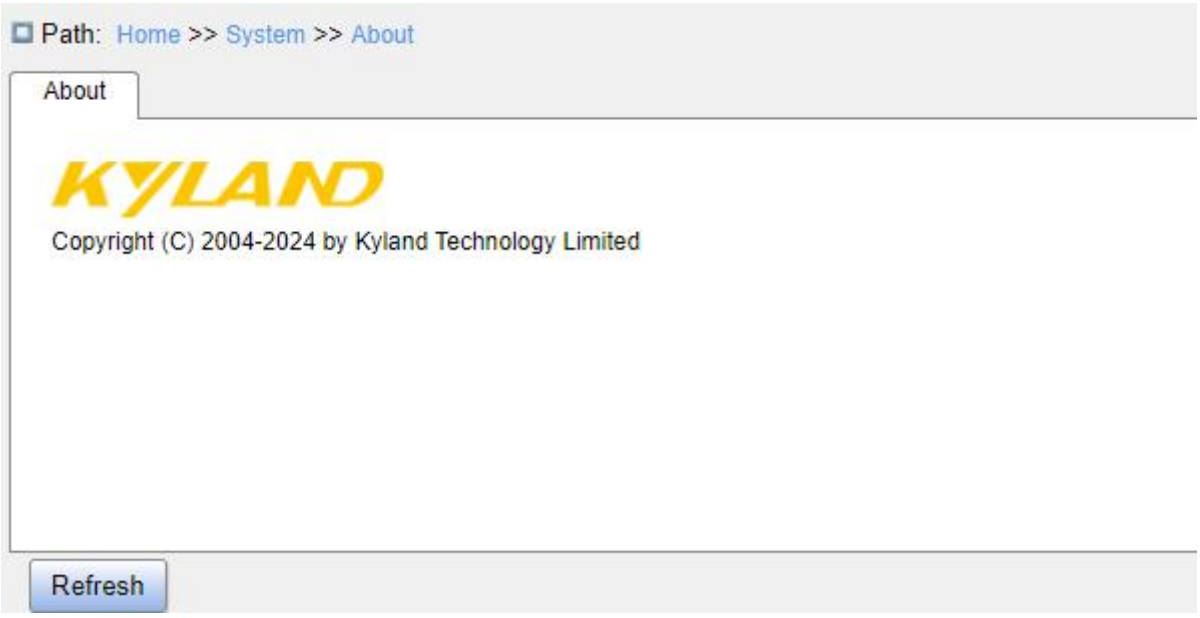


Figure 38 System related information

5 Service

5.1 SSL Configuration

5.1.1 Introduction

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.

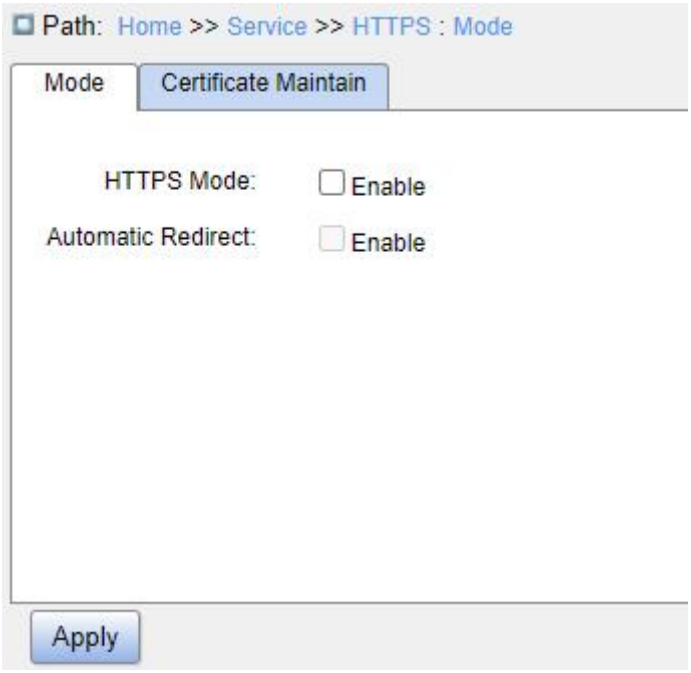


Figure 39 Enable HTTPS

HTTPS Mode

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable HTTPS. If enabled, log into the switch Web interface via http://*ip address* or secure link https://*ip address*. If disabled, users can log into the switch Web interface via http://*ip address* only.

Automatic Redirect

Configuration options: Enable/Disable

Default configuration: Disable

Function: This option can be configured only after HTTPS is enabled. When automatic redirect is enabled, a user attempting to access the switch via HTTP will be redirected to the HTTPS connection. That means the user can only log into the switch Web interface via the secure link https://*ip address*.

2. Certificate management, as shown below.

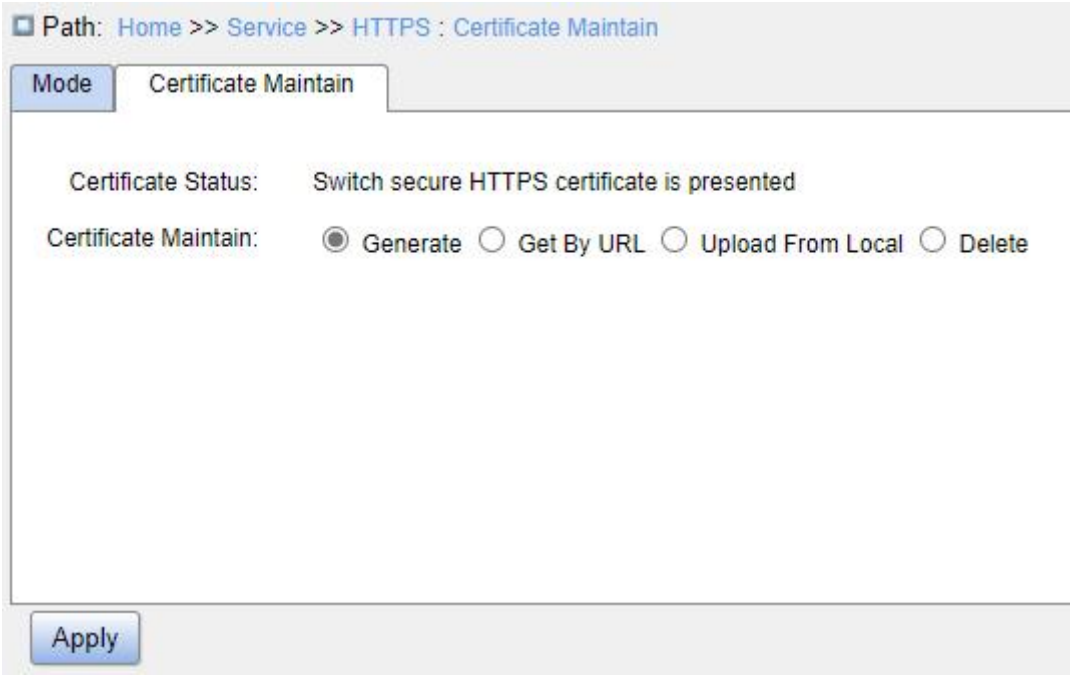


Figure 40 Generate Certificate

Certificate Maintain

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

Function: Select certificate maitanence operation.

- "Generate": Enable the switch to generate a correct HTTPS certificate.
- "Get by URL": Get an HTTPS certificate via the specified Web path, such as

https://10.10.10.10:80/new/new_image.dat.

- “Upload from local”: Select HTTPS certificates file from local.

5.2 SNMPv1/SNMPv2c

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 SNMPv2c. SNMPv2c is compatible with SNMPv1.

SNMPv1 uses community name for authentication. A community name acts as a password, limiting NMS's access to agents. If the community name carried by an SNMP packet is not acknowledged by the switch, the request fails and an error message is returned.

SNMPv2c also uses community name for authentication. It is compatible with SNMPv1, and extends the functions of SNMPv1.

To enable the communication between the NMS and agent, their SNMP versions must match. Different SNMP 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 41 shows the relationships among the NMS, agent, and MIB.

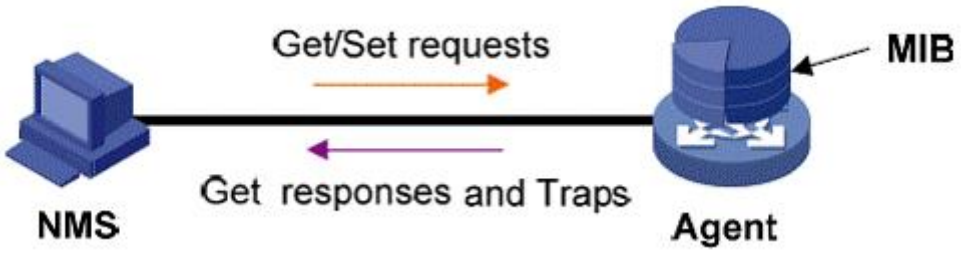


Figure 41 Relationship among NMS, Agent, and MIB

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 42, the OID of object A is 1.2.1.1.

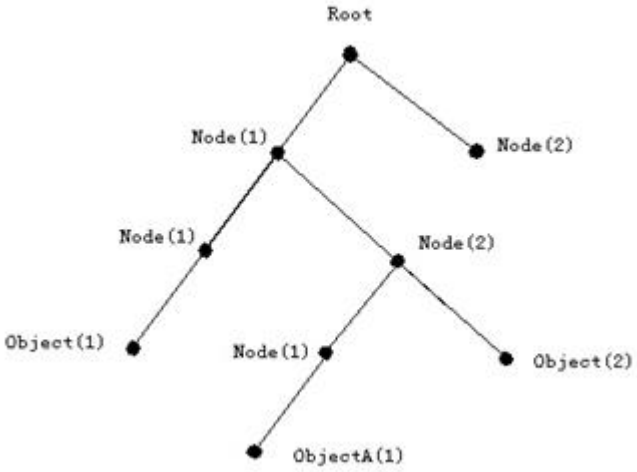


Figure 42 MIB Structure

5.2.5 Web Configuration

1. Enable SNMP, as shown below.

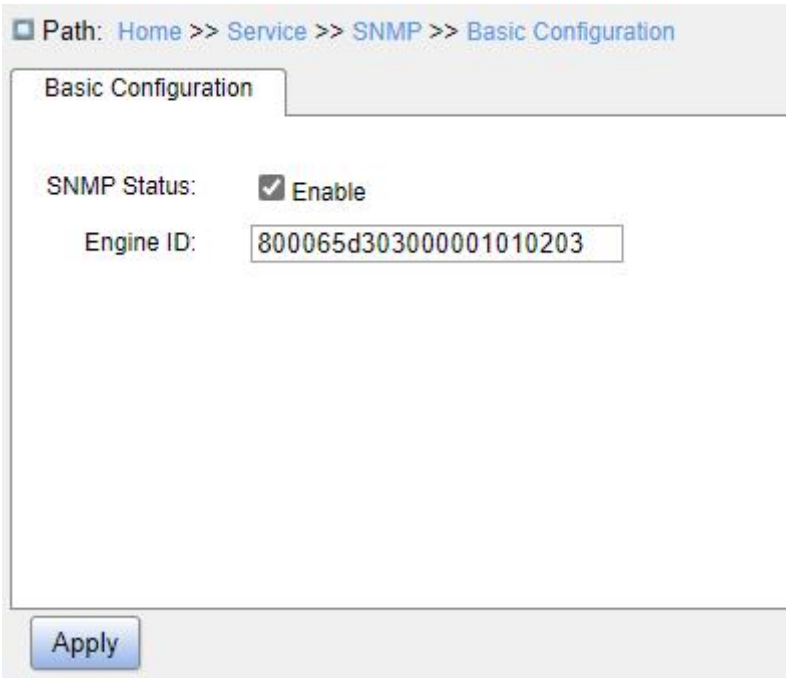


Figure 43 Enable SNMP

SNMP Status

Configuration options: Enable/Disable

Default configuration: Enable

Function: Whether to enable SNMP.

Engine ID

Configuration range: Hexadecimal bits; the number of bits must be an even number; cannot be all 0 or F; the value range of even number is 10~64.

Function: Configure SNMPv3 system engine ID. The user corresponding to the device ID in the user table will be cleared when the engine ID is modified.

2. Configure community, as shown below.

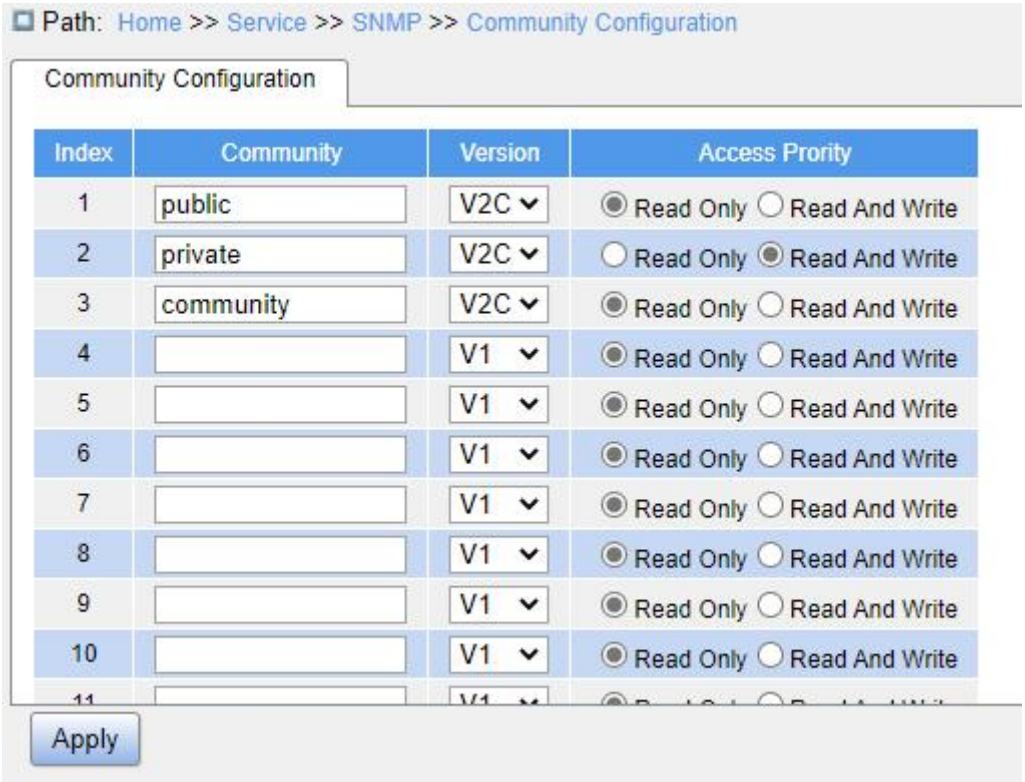


Figure 44 Configure Community

Community

Configuration range: 1~32 characters

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 to 16 community strings can be configured.

Version

Configuration options: V2C/V1

Function: Select the SNMP version.

Access Priority

Configuration options: Read Only/Read and Write

Default configuration: Read Only.

Function: Configure the access priority of MIB library.

- Read Only: The MIB library information can only be read with “Read Only” permissions;
- Read and Write: The MIB library information can be read and wrote with “Read and Write” permissions.

3. Configure Trap, as shown below.

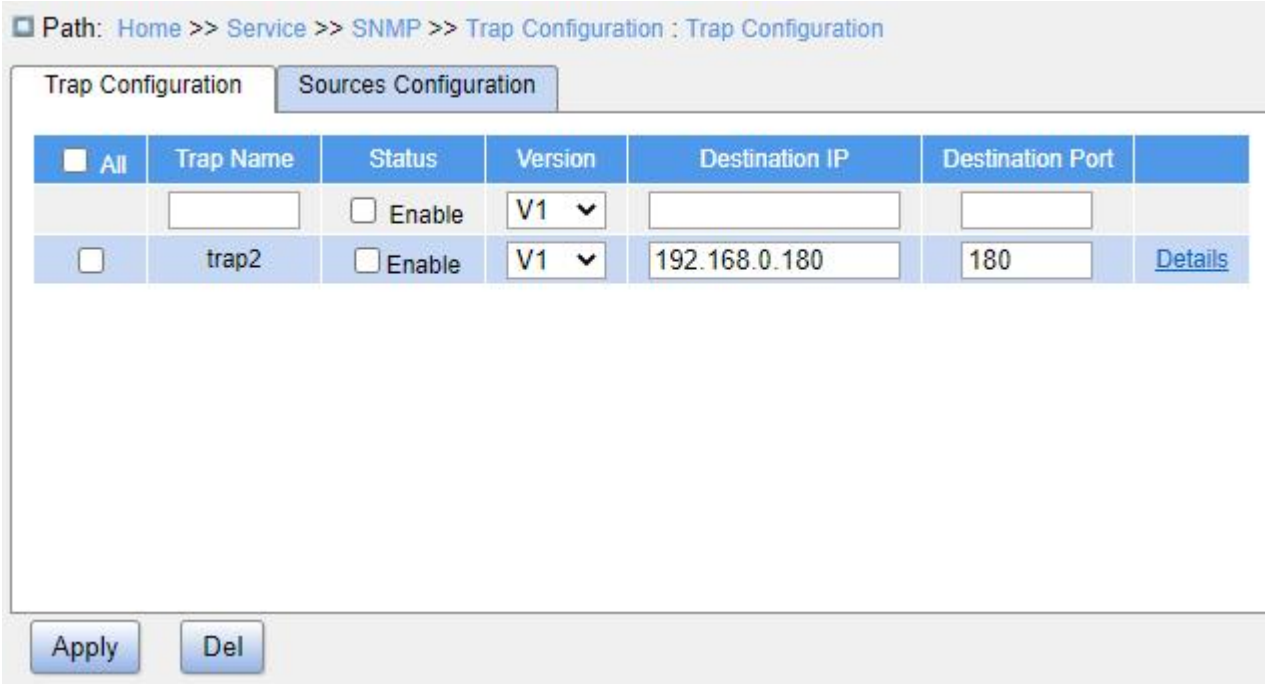


Figure 45 Configure Trap

Trap Name

Configuration range: 1~32 characters

Function: Configure Trap name.

Status

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable Trap. The switch sends the corresponding Trap message to the server if enabled.

Version

Configuration options: V1/V2C/V3

Default configuration: V1

Function: Configure the Trap message 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

Function: Configure the port number where the Trap message is received.

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

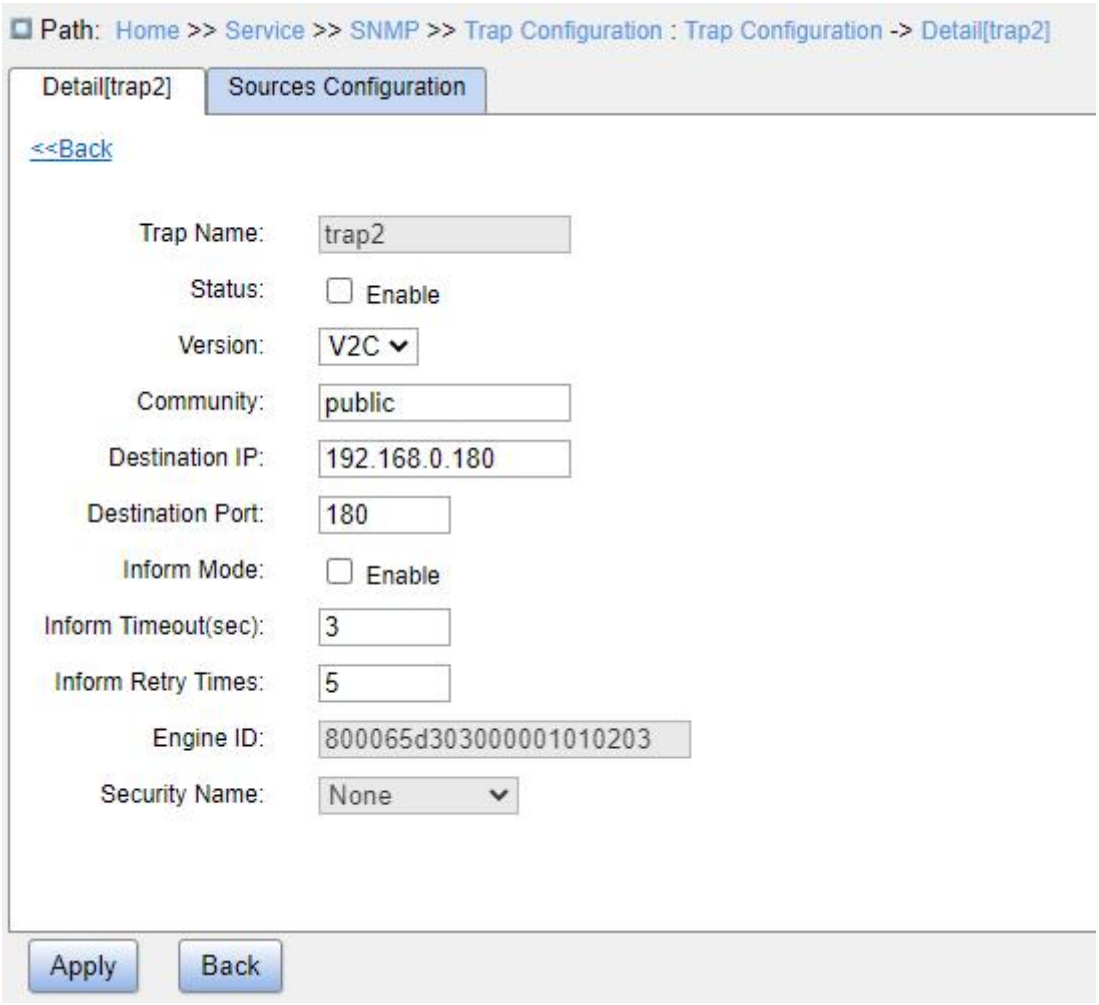


Figure 46 Trap Detail Information

Status

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable Trap. The switch sends the corresponding Trap message to the server if enabled.

Version

Configuration options: V1/V2C/V3

Default configuration: V1

Function: Configure the Trap message version number that the switch sends to the server.

Description: V1 or V2C should be selected.

Community

Configuration range: 0~255 characters

Default configuration: public

Function: Configure the community name that is carried in the sent Trap message.

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

Function: Configure the port number where the Trap message is received.

Inform Mode

Configuration options: Enable/Disable

Default configuration: Disable

Function: Configure 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 timeout value; after the switch sends the Trap message, if no response is received from the server within the specified time period, the switch will resend the Trap message.

Inform Retry Times

Configuration range: 0~255

Default configuration: 5

Function: Configure the number of times the Trap message is resent. If no response is received when the cumulative number of sending times exceeds the configured value, the sending of the Trap message is considered a failure.

5. Configure Trap event, as shown below.

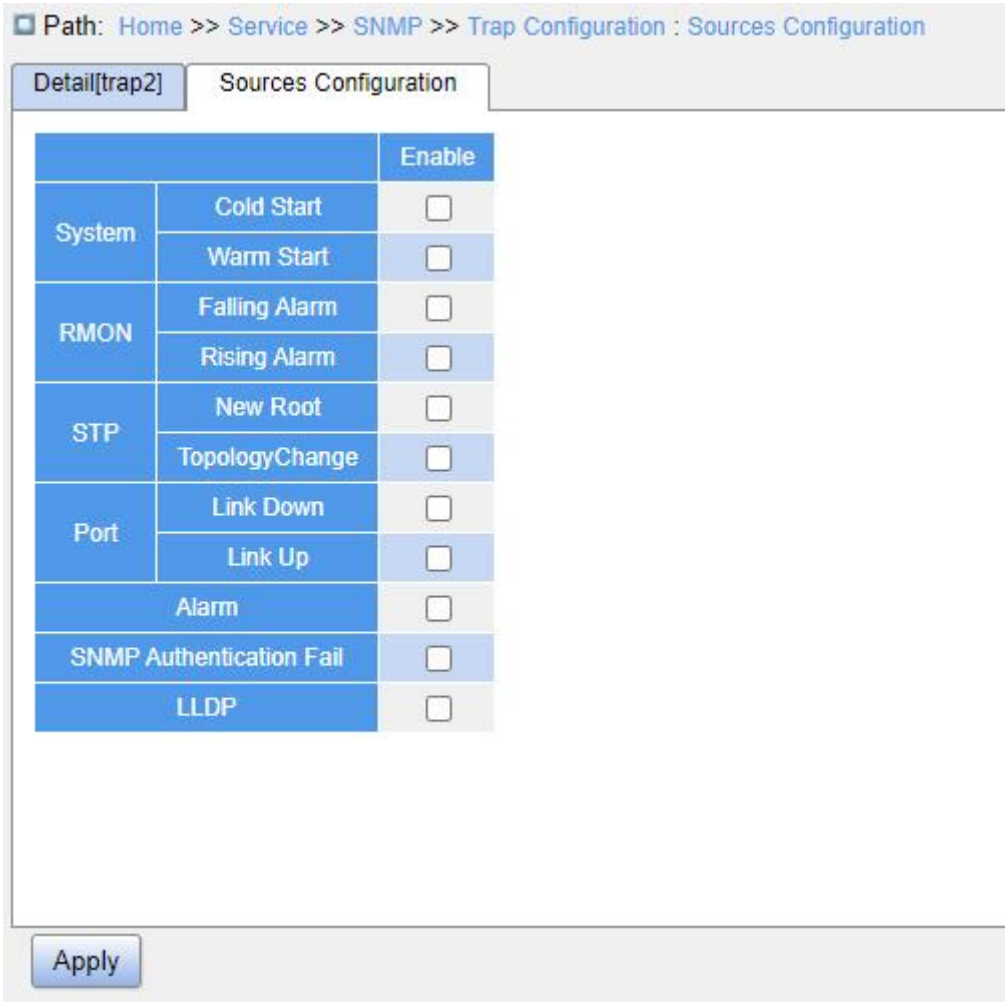


Figure 47 Trap Source Configuration

System Warm Start/Cold Start

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to send Trap message when the system experiences a warm start or cold start.

RMON Falling Alarm/Rising Alarm

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to send a Trap message when RMON generates a falling alarm or rising alarm.

STP New Root/Topology Change

Configuration options: Enable/Disable

Default configuration: Disable

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

Port Link Up/Down

Configuration options: Enable/Disable

Default configuration: Disable

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

Alarm

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to send a Trap message when there is alarm information.

SNMP Authentication Fail

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to send a Trap message when SNMP authentication fails.

LLDP

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to send an 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 SNMPv2c, 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 48.

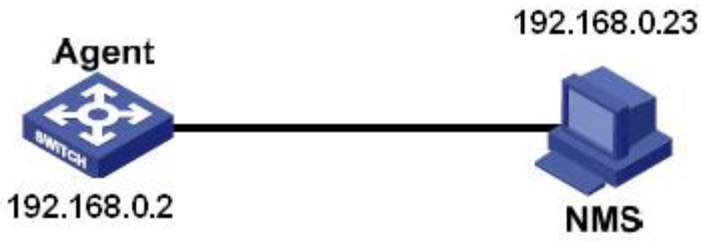


Figure 48 SNMPv2c Configuration Example

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 43, Figure 44.

2. Configure global Trap mode, as shown in Figure 45.

3. Create Trap entry 111, enable Trap mode; set the Trap version to SNMPv2c, 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 46. Figure 47.

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 Introduction

SNMPv3 provides a User-Based Security Model (USM) authentication mechanism. You can configure authentication and encryption functions. Authentication is used for verifying the validity of packet sender, preventing illegitimate users' access. Encryption is used for encrypting packets transmitted between the NMS and the Agent to avoid 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 versions can be configured on an agent, so that it can use different versions to communicate with different NMSs.

5.3.2 Implementation

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

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

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.

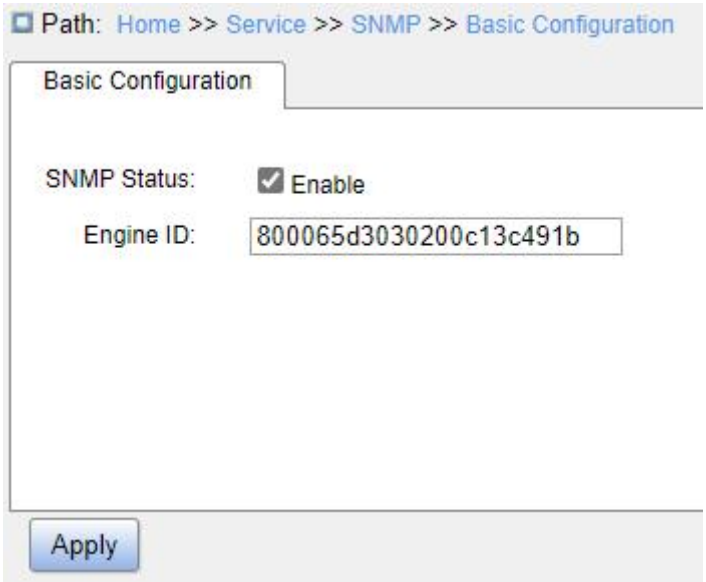


Figure 49 Enable SNMP

SNMP Status

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable SNMP.

Engine ID

Configuration range: Hexadecimal bits; the number of bits must be an even number; cannot be all 0 or F; the value range of even number is 10~64.

Function: Configure SNMPv3 system engine ID. The user corresponding to the device ID in the user table will be cleared when the engine ID is modified.

2. Configure Trap, as shown below.

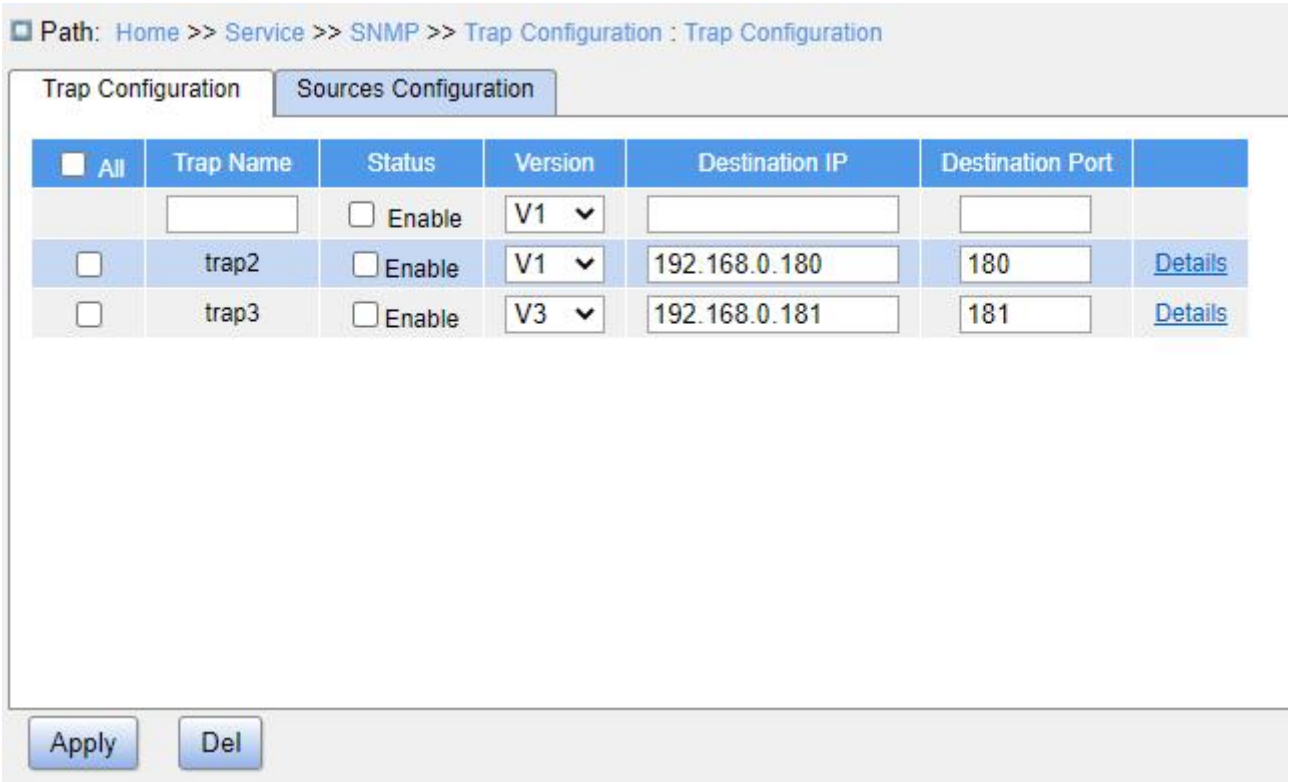


Figure 50 Configure Trap

Trap Name

Configuration range: 1~32 characters

Function: Configure Trap name.

Status

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable Trap. The switch sends the corresponding Trap message to the server if enabled.

Version

Configuration options: SNMPv1/SNMPv2c/SNMPv3

Default configuration: SNMPv1

Function: Configure the Trap message 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

Function: Configure the port number where the Trap message is received.

3. Click the Trap configuration item details to see and configure the Trap configuration details, as shown below.

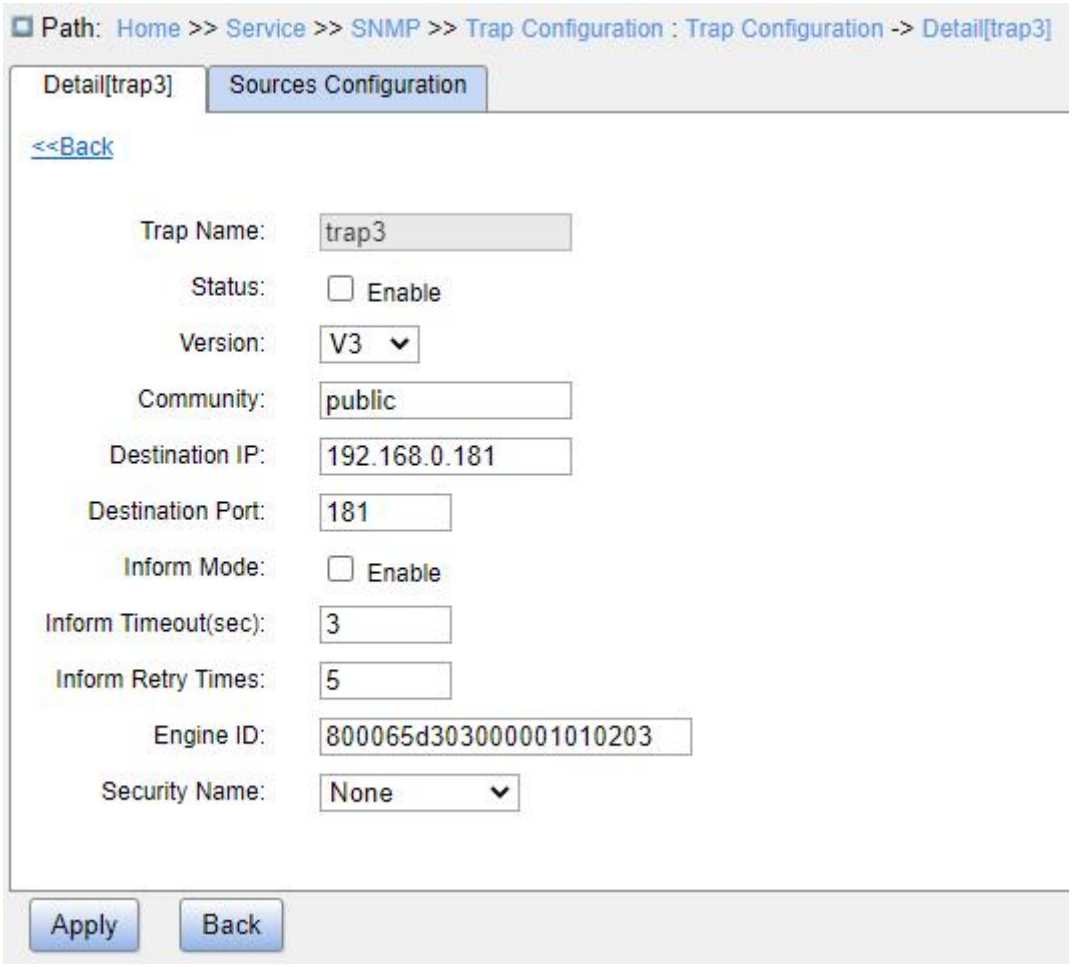


Figure 51 Trap Details

Status

Configuration options: Enable/Disable

Function: Whether to enable Trap. The switch sends the corresponding Trap message to the server if enabled.

Version

Configuration options: V1/V2C/V3

Function: Configure the Trap message version number that the switch sends to the server.

Community

Configuration range: 1~255 characters

Function: Configure the community name that is carried in the sent Trap message.

Inform Mode

Configuration options: Enable/Disable

Function: Configure whether the server sends a reply message to the switch after receiving the Trap message.

Inform Timeout

Configuration range: 0~2147s

Default configuration: 3

Function: Configure the Trap message timeout value; after the switch sends the Trap message, if no response is received from the server within the specified time period, the switch will resend the Trap message.

Inform Retry Times

Configuration range: 0~255

Default configuration: 5

Function: Configure the number of times the Trap message is resent. If no response is received when the cumulative number of sending times exceeds the configuration value, the sending of the Trap message is considered a failure.

Engine ID

Configuration range: Hexadecimal number is even, and cannot 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 SNMPv3 Trap message.

Security Name

Configuration options: created security names/None

Function: Select the security name.

4. Configure Trap event, as shown below.

Figure 52 Trap Source Configuration

System Warm Start/Cold Start

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to send Trap message when the system experiences a warm start or cold start.

RMON Falling Alarm/Rising Alarm

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to send a Trap message when RMON generates a falling alarm or rising alarm.

STP New Root/Topology Change

Configuration options: Enable/Disable

Default configuration: Disable

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

Port Link Up/Down

Configuration options: Enable/Disable

Default configuration: Disable

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

Alarm

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to send a Trap message when there is alarm information.

SNMP Authentication Fail

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to send a Trap message when SNMP authentication fails.

LLDP

Configuration options: Enable/Disable

Default configuration: Disable

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

5. Configure user name table, as shown below.

Figure 53 Configure SNMPv3 User Name Table

Security Name

Configuration range: 1~32 characters

Function: Create user name.

Engine ID

Configuration range: Hexadecimal bits; the number of bits must be an even number; cannot 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 SNMPv3 Trap message.

Security Level

Configuration options: NoAuthNoPriv/AuthNoPriv/AuthPriv

Function: Configure the security level of the current user.

- NoAuthNoPriv: Requires neither authentication nor encryption;
- AuthNoPriv: Requires authenticate but not encryption;
- 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: 8~32 characters (SHA protocol)/8~40 characters (MD5 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 for “AuthPriv” at the security level.

Privacy Password

Configuration range: 8~32 characters

Function: Create privacy password.

5. Configure group table, as shown below.

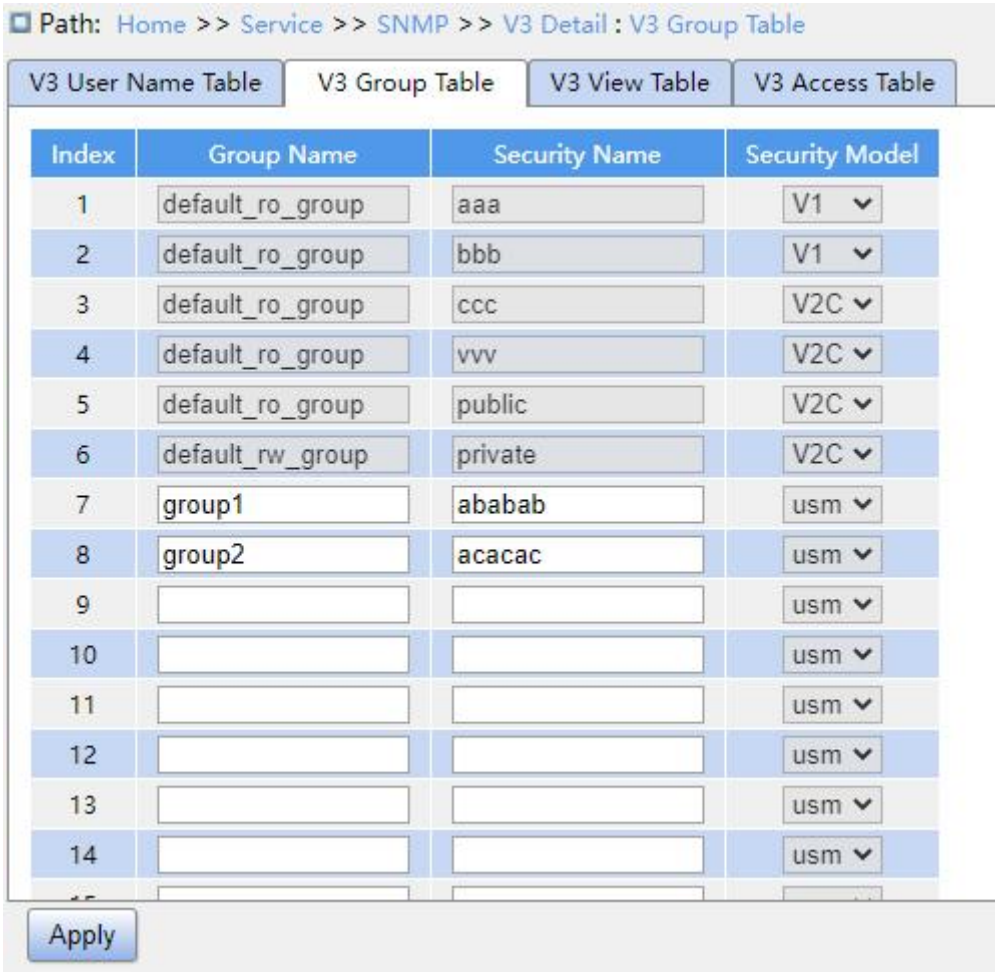


Figure 54 Configure SNMPv3 Group Table

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 Name

Configuration range: created SNMPv3 user names

Function: Configure security name, which should match the user name in the SNMPv3 user table. Users with the same group name belong to the same group.

Security Model

Default configuration: usm (mandatory)

Function: Select the security model of current group. SNMPv3 uses USM (security model based on user) technology. This option is mandatory on the SNMPv3 model currently.

Up to 32 group tables can be configured.

6. Configure view table, as shown below.

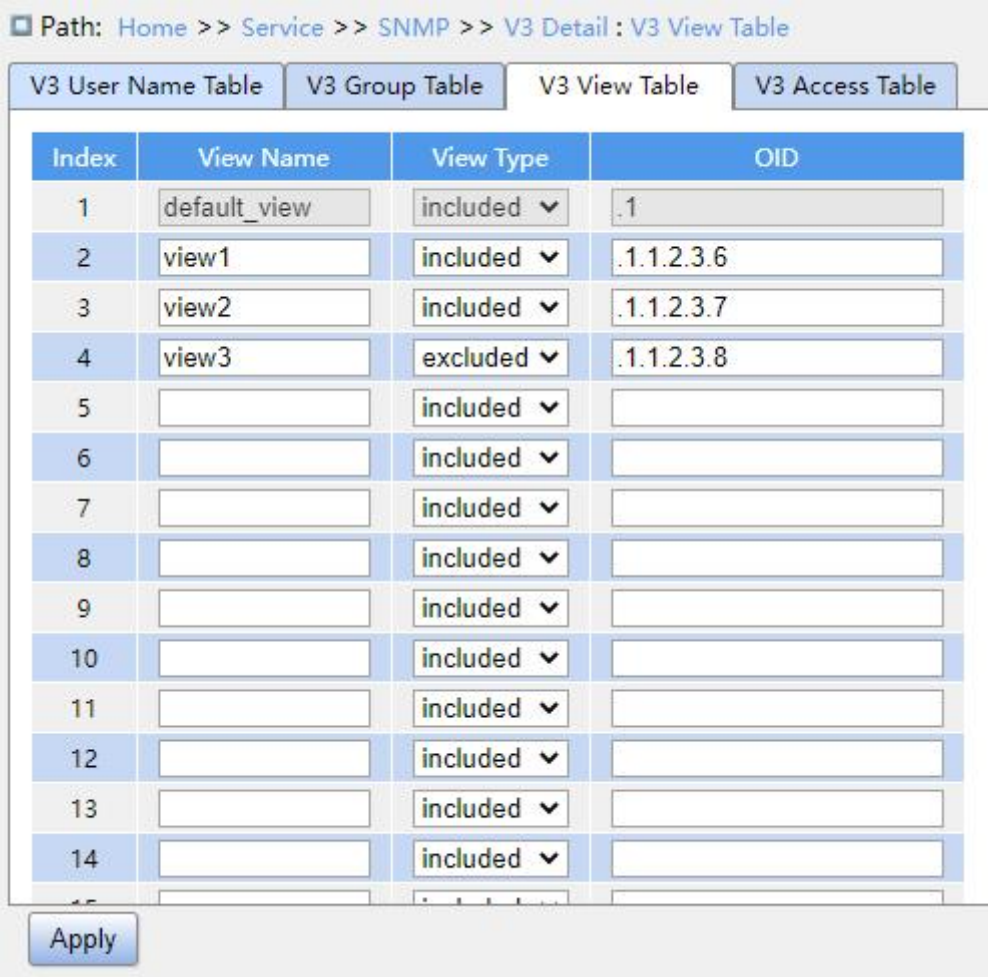


Figure 55 Configure SNMPv3 View Table

View Name

Configuration range: 1~32 characters

Function: Configure view name.

View Type

Configuration options: included/excluded

Function: Configure SNMPv3 view type.

- included: indicates that the current view includes all the nodes of the MIB subtree.
- excluded: indicates that the current view does not include any nodes of the MIB subtree.

OID

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

Up to 16 view tables can be configured.

Note:

The switch has a default view table “default_view”, which includes all nodes of subtree 1.

7. Configure access table, as shown below.

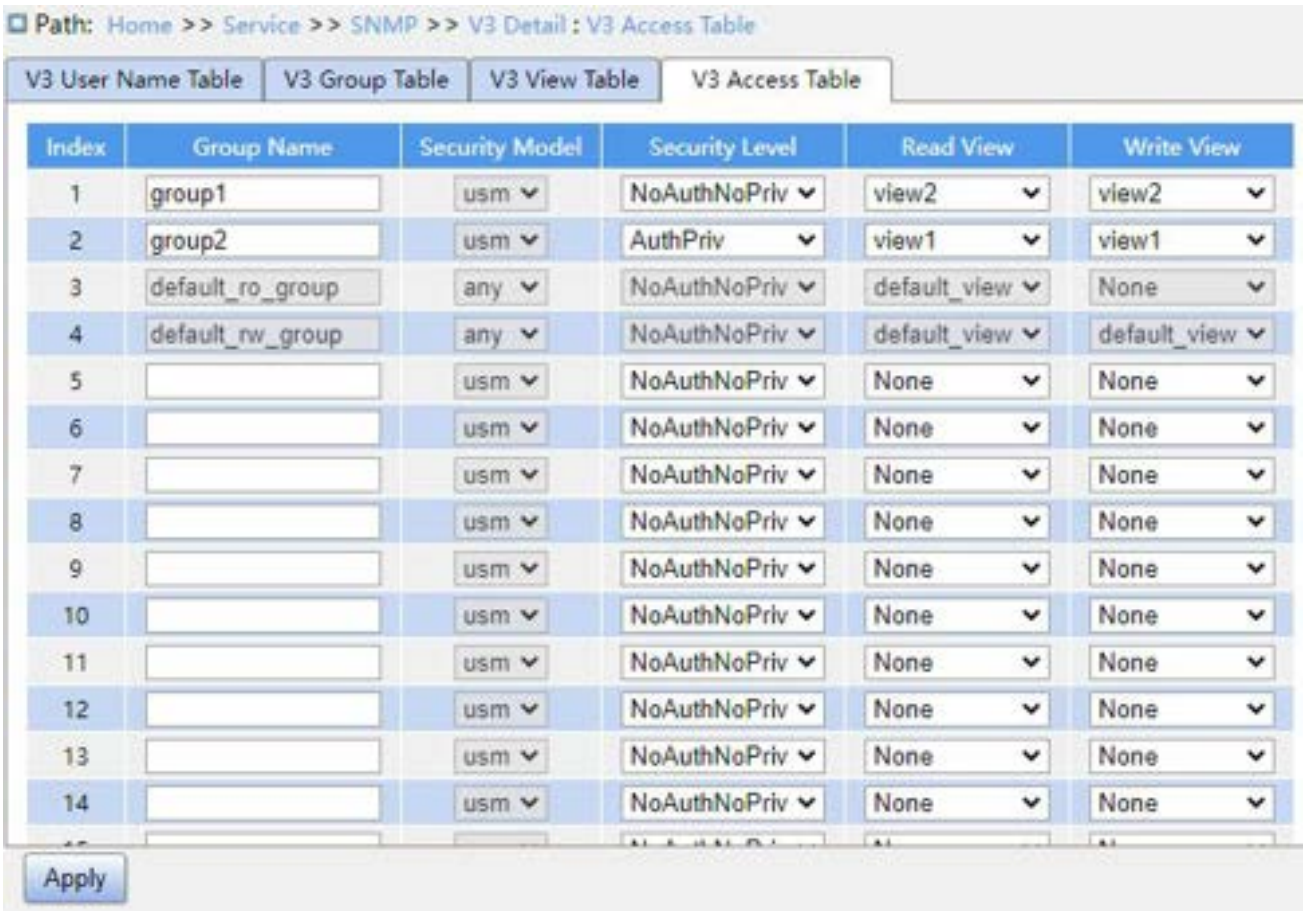


Figure 56 Configure SNMPv3 Access Table

Group Name

Configuration range: 1~32 characters

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

Security Model

Default configuration: any/usm

Function: Select the security model of current group. SNMPv3 uses USM (security model based on user) technology. This option is mandatory on the SNMPv3 model currently. “any” indicates any security model. The group name and security model configurations should be the same as that in the SNMPv3 group table.

Security Level

Configuration options: NoAuthNoPriv/AuthNoPriv/AuthPriv

Function: Configure the security level of current group.

- NoAuthNoPriv: Requires neither authentication nor encryption;
- AuthNoPriv: Requires authentication but not encryption;
- AuthPriv: Requires both authentication and encryption.

Description: 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” increases in turn. A low level of security level allows access by a higher level of security. If a group is configured with the security level “AuthNoPriv”, users with the security level “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 the security level “NoAuthNoPriv” 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 names.

Up to 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 SNMPv3. 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 SNMPv3 messages to the NMS proactively, as shown in Figure 57.

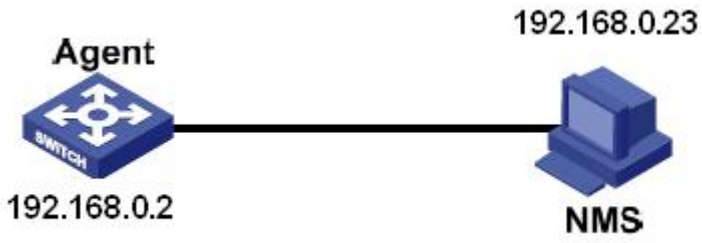


Figure 57 SNMPv3 Configuration Example

Configuration on the Agent:

1. Enable SNMP, as shown in Figure 49.

2. Configure the SNMPv3 user table

Set a user name to 1111, security level to “AuthPriv”, 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 “AuthPriv”, authentication protocol to “SHA”, authentication password to “bbbbbbbb”, privacy protocol to “AES”, and privacy password to “yyyyyyyy”, as shown in Figure 53.

3. Create group, set security model to “usm”, and add user 1111 and user 2222 to the group, as shown in Figure 54.

4. Configure the SNMPv3 access table

Set the group name to “group”, security model to “usm”, security level to “AuthNoPriv”, read view to “default_view”, and write view to “None”, as shown in Figure 56.

5. Create Trap entry 222, enable Trap mode; set the Trap version to “SNMPv3”, 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 46. Figure 47.

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 the session request is accepted.

5.4.3 Web Configuration

1. Enable SSH protocol, as shown below.

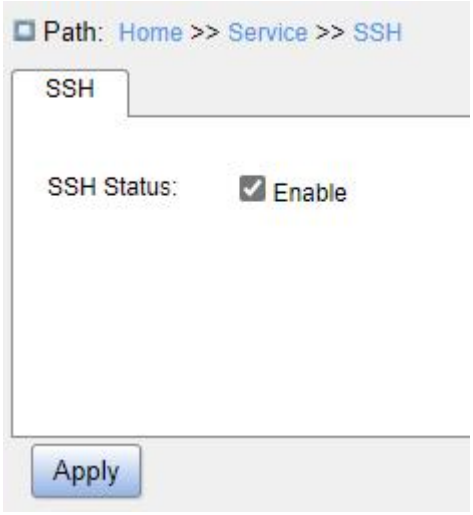


Figure 58 Enable SSH Protocol

SSH Status

Configuration options: Enable/Disable

Default configuration: Enable

Function: Whether to enable 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 59.

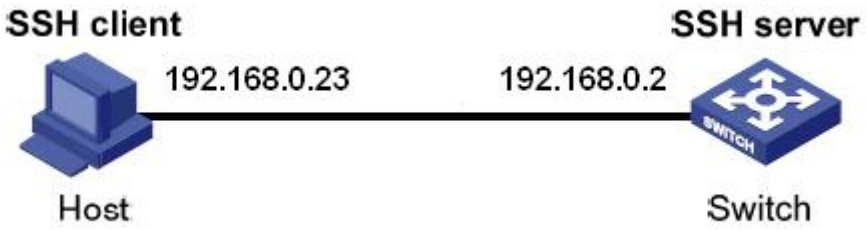


Figure 59 SSH Configuration Example

1. Enable SSH protocol, as shown in Figure 58;

2. Establish the connection with the SSH server. First, run the PuTTY.exe software, as shown in Figure 60; input the IP address of the SSH server 192.168.0.2 in the space of Host Name (or IP address).

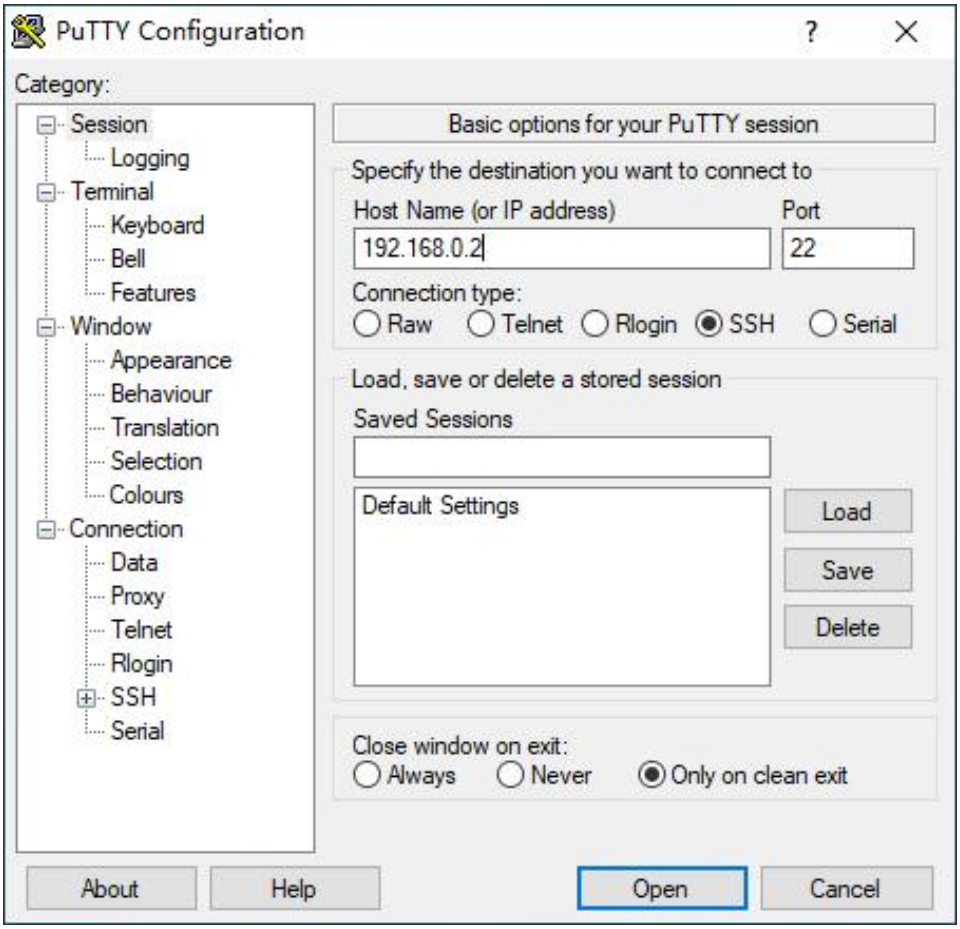


Figure 60 SSH Client Configuration

2.Click <Open> button and following warning message appears shown in Figure 61, click the <Yes> button.

Figure 61 Warning Message

4. Input the user name “admin” and the password “123” to enter the switch configuration interface, as shown in Figure 62.

Figure 62 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 the client for the server. Figure 63 shows the structure.

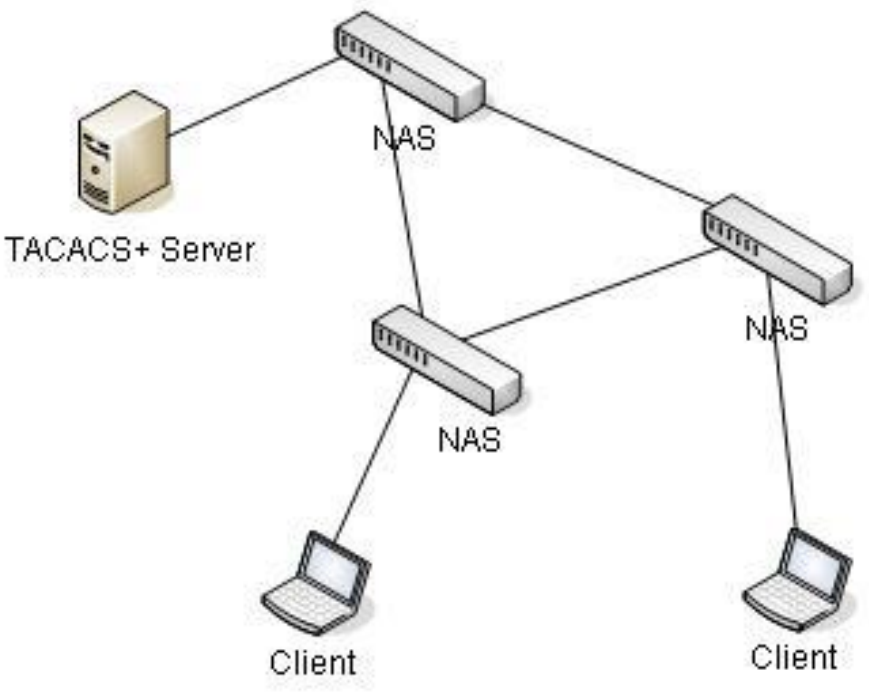


Figure 63 TACACS+ Structure

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.

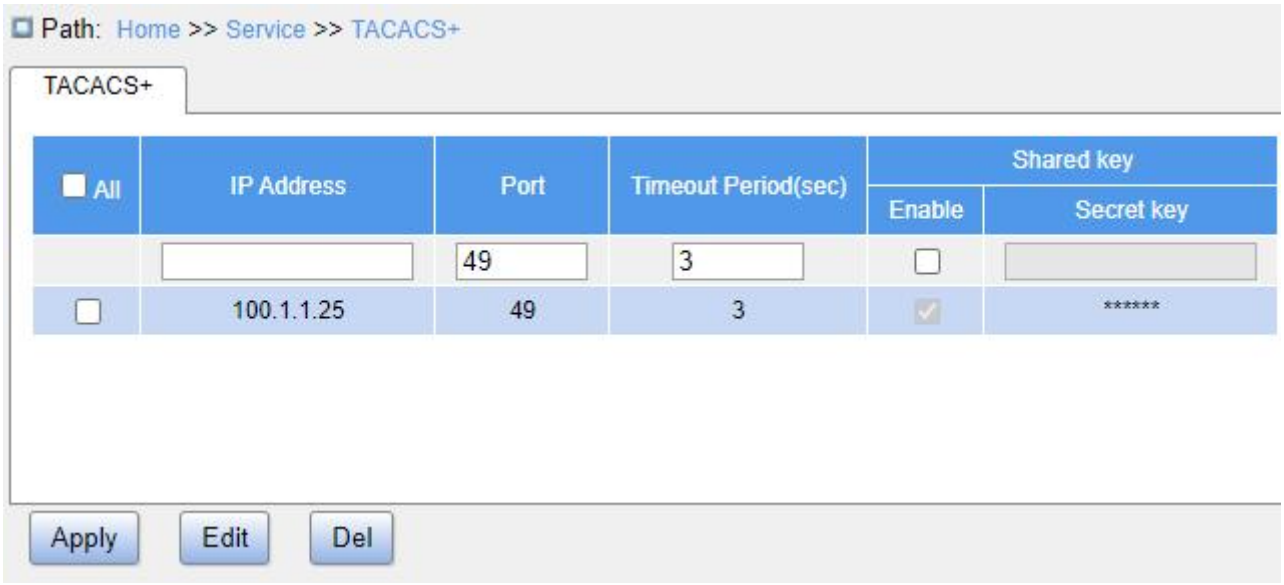


Figure 64 TACACS+ Server Configuration

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

Default configuration: 3

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.

Shared Key – Enable

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable encryption by shared key to improve the communication security between the client and the TACACS+ server.

Shared Key – Secret Key

Configuration range: 0~63 characters

Function: Set the key the two parties use 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 65, 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”.

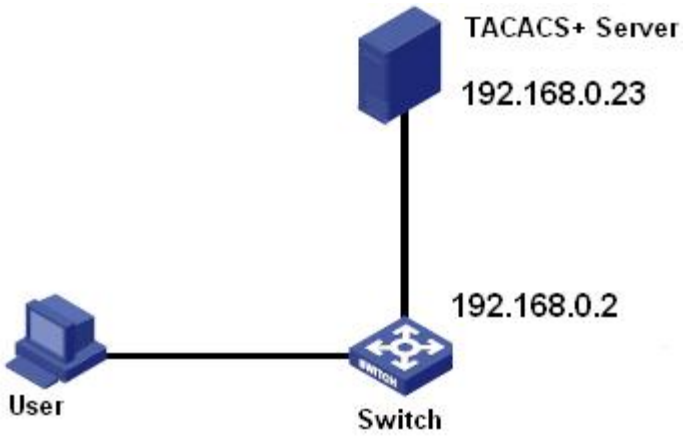


Figure 65 TACACS+ Authentication Example

Configuration process:

1. TACACS+ server configuration. Set the server IP address to 192.168.0.23 and key to “aaa”, as shown in Figure 64.

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”, and 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 the client for the RADIUS server. Figure 66 shows the structure.

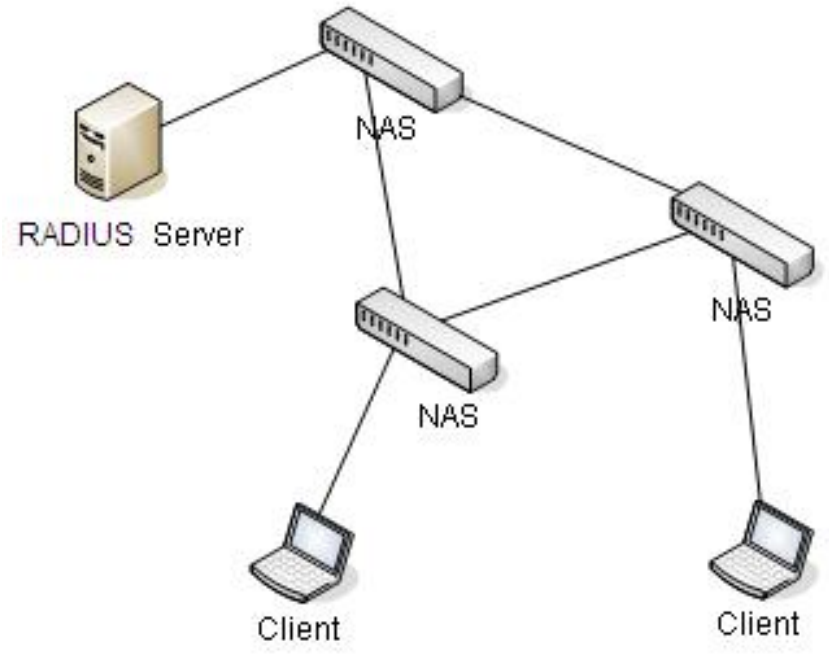


Figure 66 RADIUS Structure

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.

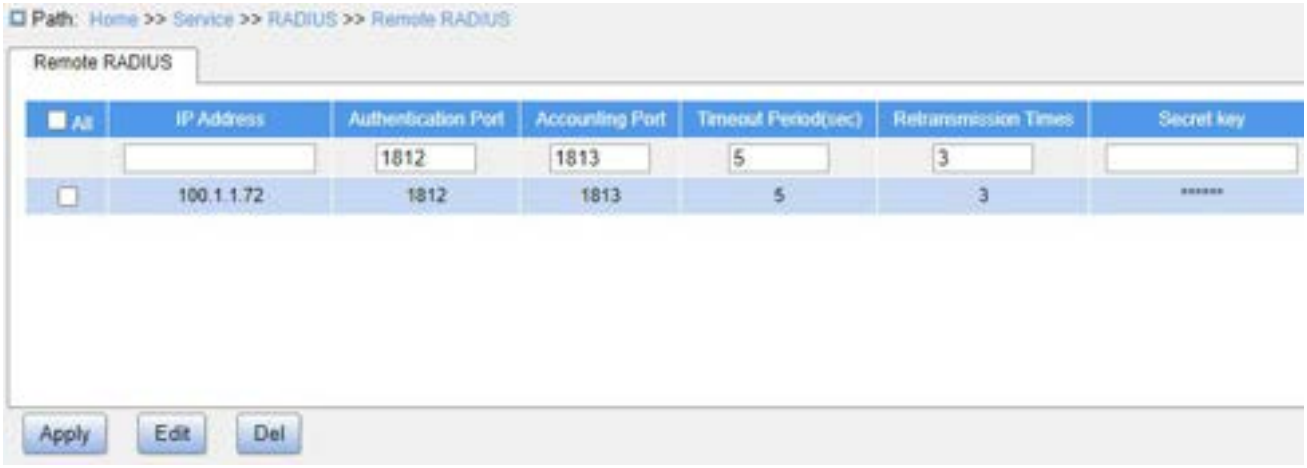


Figure 67 Configure the RADIUS Server

IP Address

Configuration format: A.B.C.D

Function: Configure the IP address 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 Period (sec)

Configuration range: 1~1000s

Default configuration: 5

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

Default configuration: 3

Function: Set the maximum retransmission attempts for RADIUS request packets. If the device still receives no response packets from the RADIUS server after maximum retransmission attempts, 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 the device and

the 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 key is the same. Therefore, make sure the configured key is the same as the key on the RADIUS server.

Note:

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

2. Configure global RADIUS, as shown below.

Figure 68 Global Configuration

RADIUS Enable

Configuration options: Enable/Disable

Default configuration: Disable

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

3. Configure client RADIUS, as shown below.

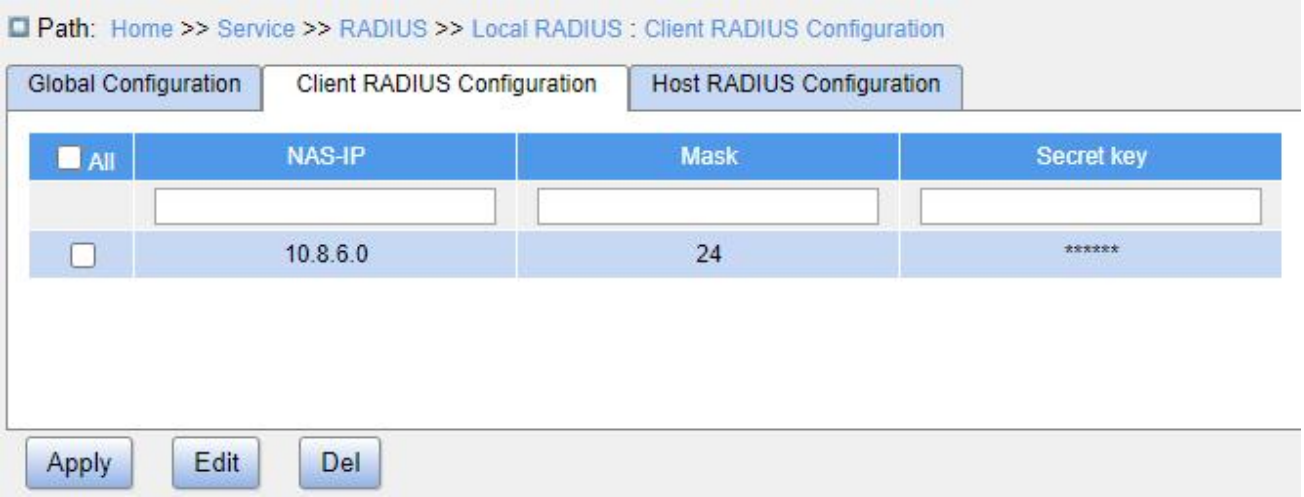


Figure 69 Client RADIUS Configuration

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. Only one segment needs to be configured for different IP address belonging to the same segment.

Secret key

Configuration range: 1~63 characters

Function: Configure the shared key the device and the RADIUS client use to verify the validity of the message. The device and the client will accept each other's packets and make responses only when the shared key is the same. Therefore, make sure the secret key configured on the device is the same with that on the RADIUS client.

4. Configure RADIUS host, as shown below.

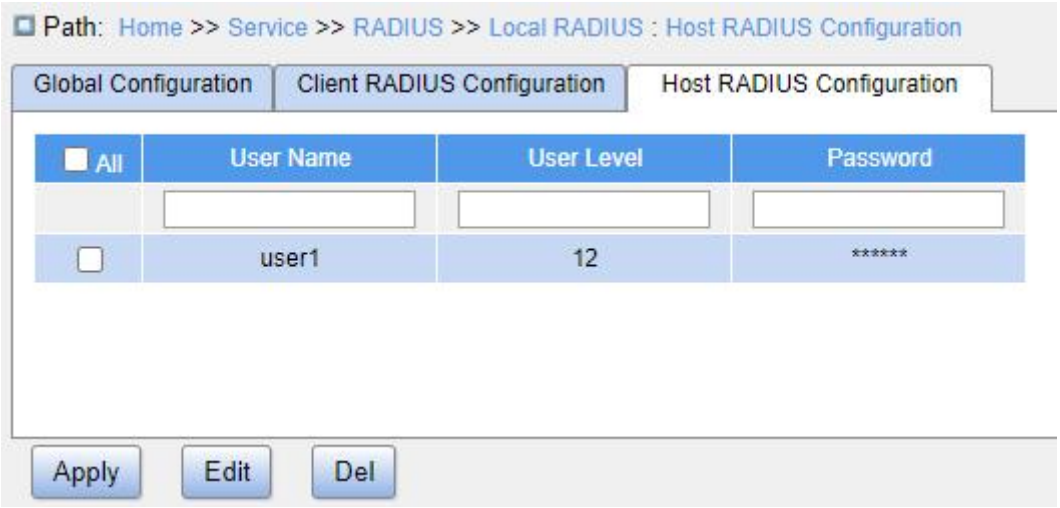


Figure 70 Host RADIUS Configuration

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 authority 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 71, 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”.

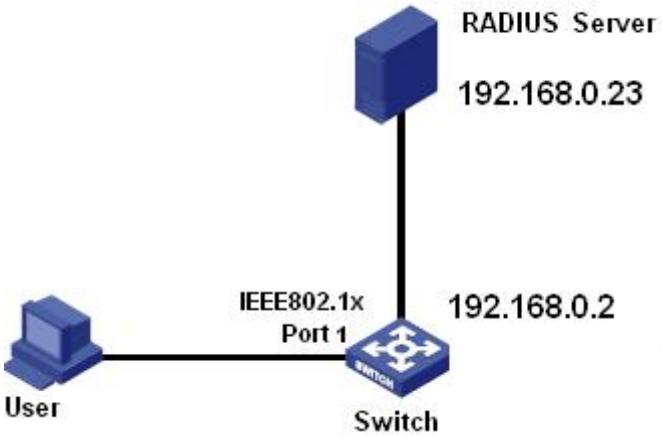


Figure 71 RADIUS Authentication Configuration Example

Configuration process:

1. Set the IP address of the authentication server to 192.168.0.23 and password to “aaa”, as shown in Figure 67.

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 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, as shown in the following figure.

Figure 72 Configure DNS

DNS Proxy

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable DNS proxy.

Domain Name

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

Default configuration: None

Function: After failing to obtain a resolution result for the domain name directly

requested by the client, the device will add the domain suffix to the domain name and request resolution again from the DNS server.

2. Configure the DNS server, as shown in the following figure.

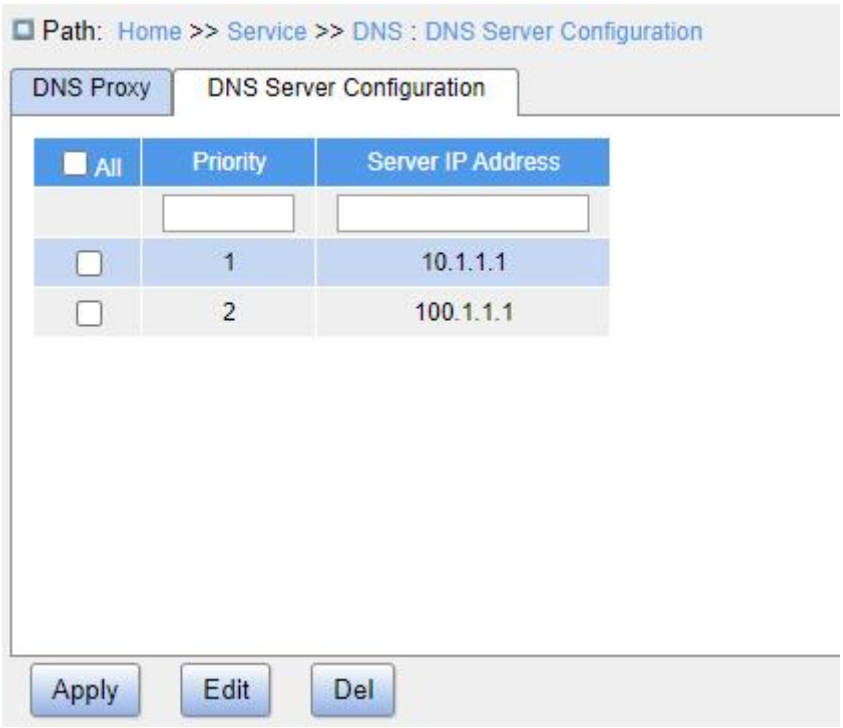


Figure 73 Configure the DNS Server

Priority

Configuration range: 0~2

Default configuration: None

Function: The proxy device resolves the address to the specified DNS server in priority order until the resolution is successful. A smaller value indicates a higher priority.

Server IP Address

Configuration format: A.B.C.D

Function: Manually configure the DNS server IP address.

5.7.3 Typical Configuration Example

As shown in Figure 71, sometimes the DNS client cannot or must not be directly configured with the DNS server address. At this time, the DNS address of the client can be set directly to the DNS proxy address and the switch should have DNS proxy enabled. With the domain name suffix configured, the DNS proxy will automatically add the configured

suffix to the domain name when sending the DNS resolution request again after a resolution failure.

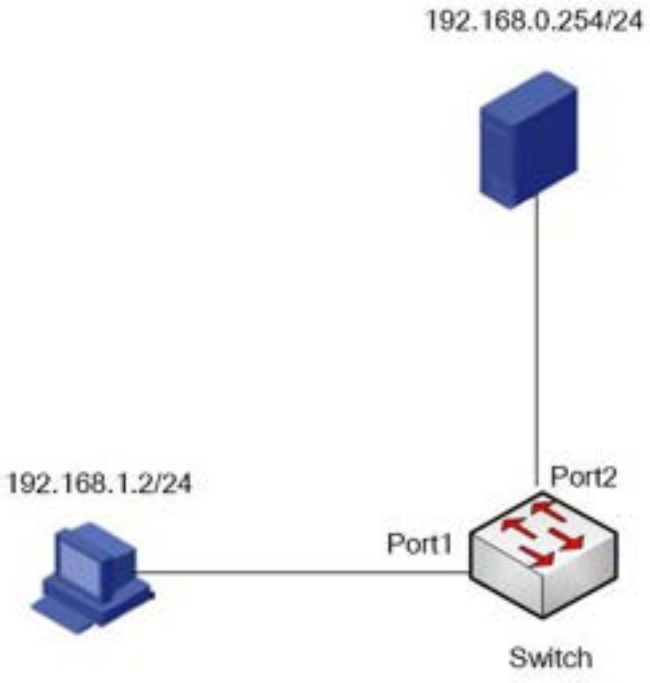


Figure 74 DNS proxy configuration example

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

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

3. Configure Port1 as Access mode to join VLAN 1 and configure Layer 3 interface IP as 192.168.1.1/24; Configure Port2 as Access mode to join VLAN 2 and configure Layer 3 interface IP as 192.168.0.1/24；

4. Enable DNS proxy on the switch, configure DNS Server IP as 192.168.0.254, and 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 Introduction

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 save 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 handling 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 informs the NMS of the event.

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

None: Indicates no action.

- Alarm group

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

Caution:

If a sampled value of alarm variable exceeds the threshold multiple times in the same direction, then the alarm event is triggered only at 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.

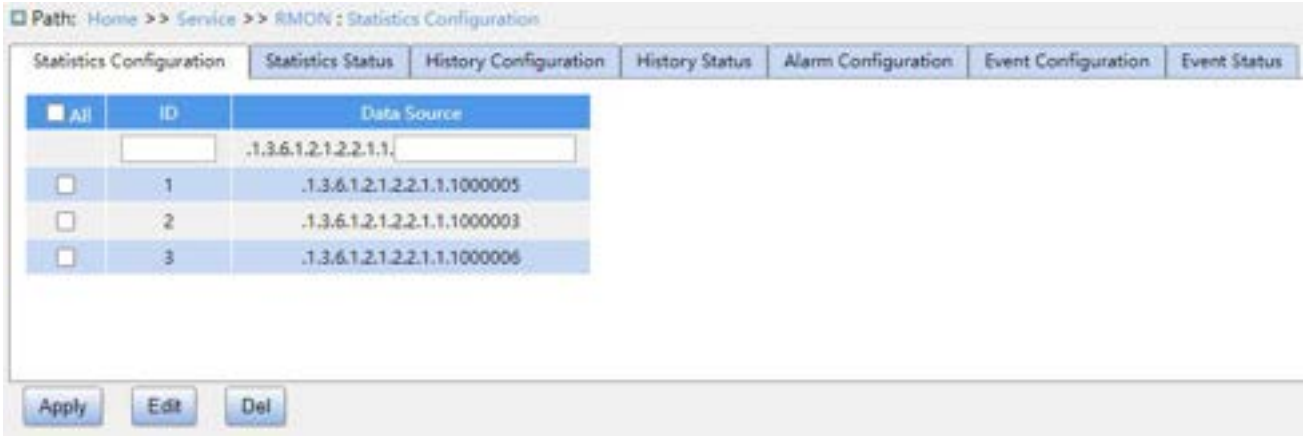


Figure 75 Configure RMON Statistics Table

ID

Configuration range: 1~65535

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

Data Source

Configuration range: 1000000 + Port ID

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

Description: For example, to collect statistics of port 6, input 1000006.

2. View statistics group status, as shown below.

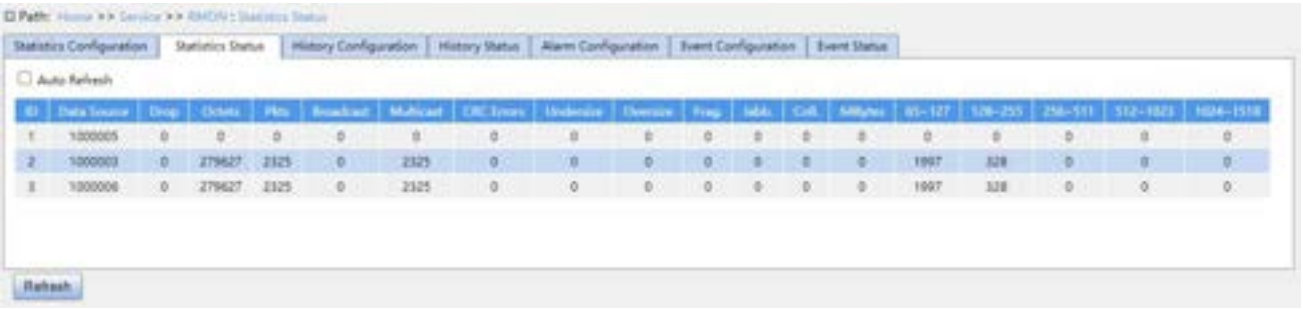


Figure 76 View Statistics Group Status

- 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.
- 1024~1518: the number of packets with a length of between 1024 and 1518 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.

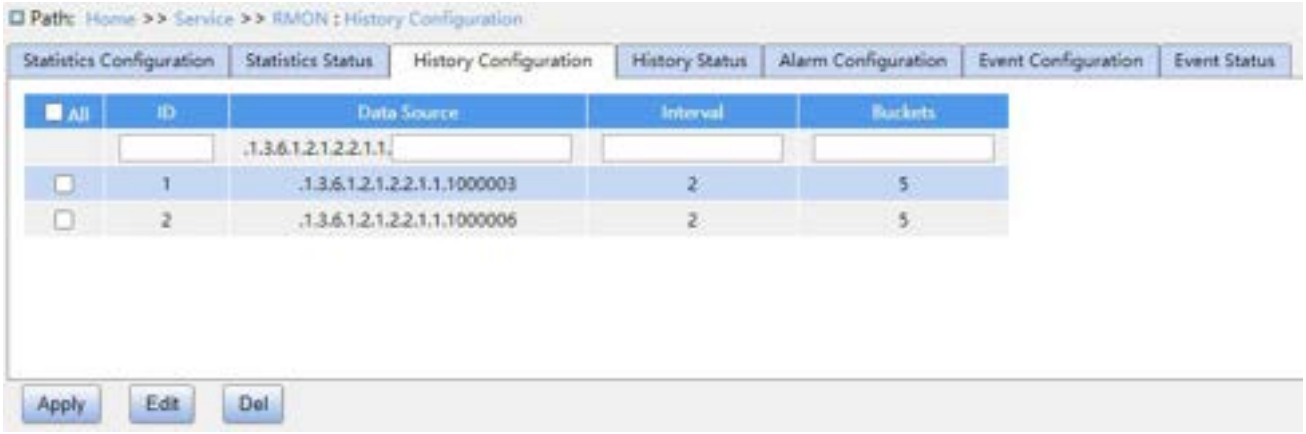


Figure 77 Configure History Table

ID

Configuration range: 1~65535

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

Data Source

Configuration options: 1000000 + Port ID

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

Description: For example, to collect statistics of port 6, input 1000006.

Interval

Configuration range: 1~3600s

Function: Configure the sampling period of the port.

Buckets

Configuration range: 1~65535

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

4. View history group status, as shown below.

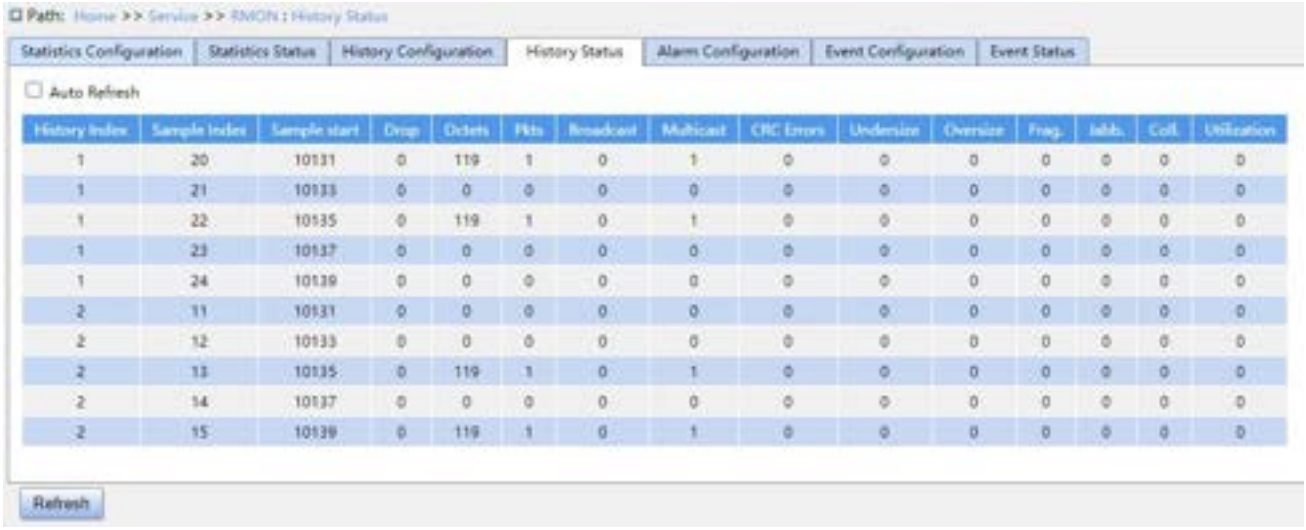


Figure 78 Overview History Group Status

5. Configure event table, as shown below.

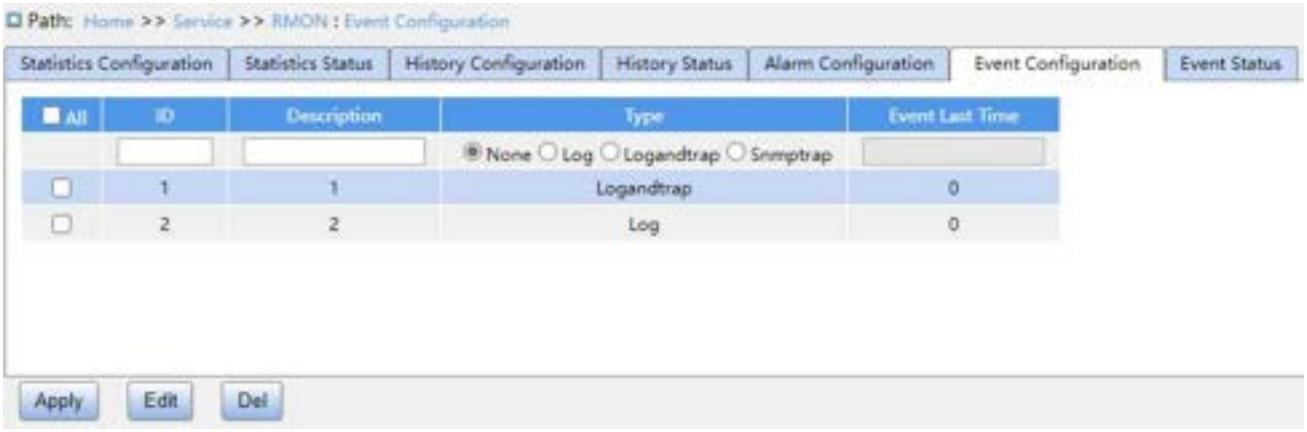


Figure 79 Configure Event Table

ID

Configuration range: 1~65535

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

Description

Configuration range: 1~127 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: Display the value of sysUpTime when the event is used last time.

6. Configure alarm table, as shown below.

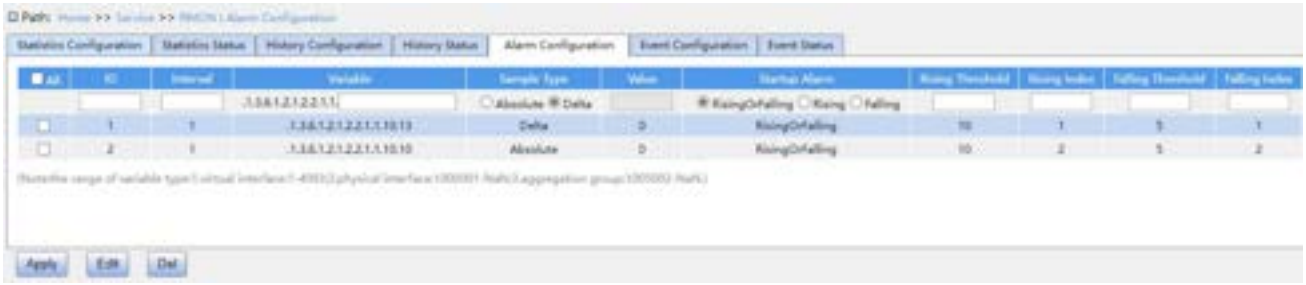


Figure 80 Configure Alarm Table

ID

Configuration range: 1~65535

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

Interval

Configuration range: 1~2147483647s

Default configuration: 30s

Function: Configure the sampling period.

Variable

Configuration format: A.1000000 + Port ID/A.VLAN ID

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.

- Absolute: Directly compares each sampling value with the threshold;
- Delta: Use the sampling value to minus the previous sampling value, then use the difference to compare with the 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 handling 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.

7. View event group status, as shown below.

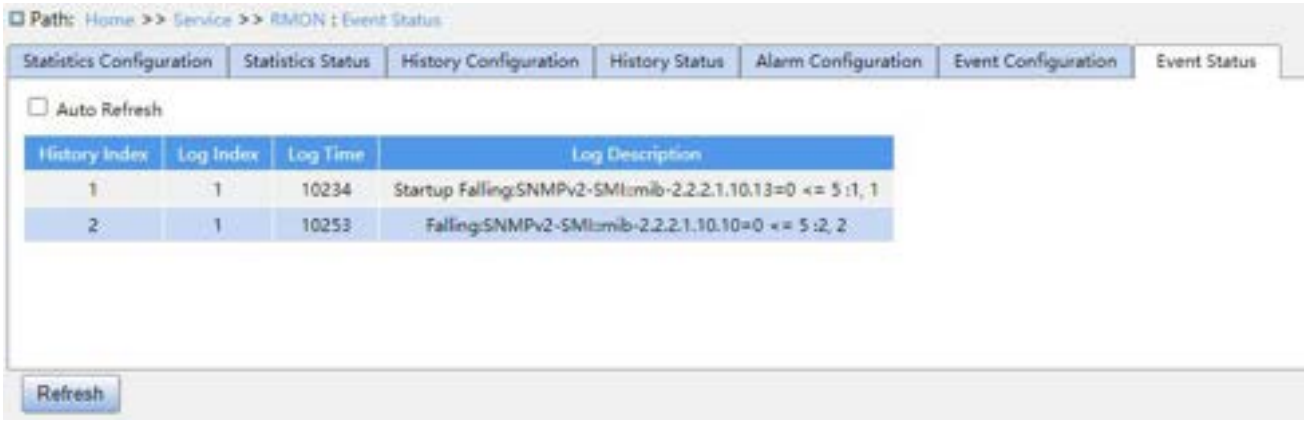


Figure 81 View Event Group Status

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.
- DDM alarm: If this function is enabled, an alarm is triggered when the optical powere crosses the threshold.
- Voltage Alarm: The voltage alarms typically arise from voltages exceeding the designated range.

6.2 Web Configuration

1. Configure and display basic alarm, as shown below.

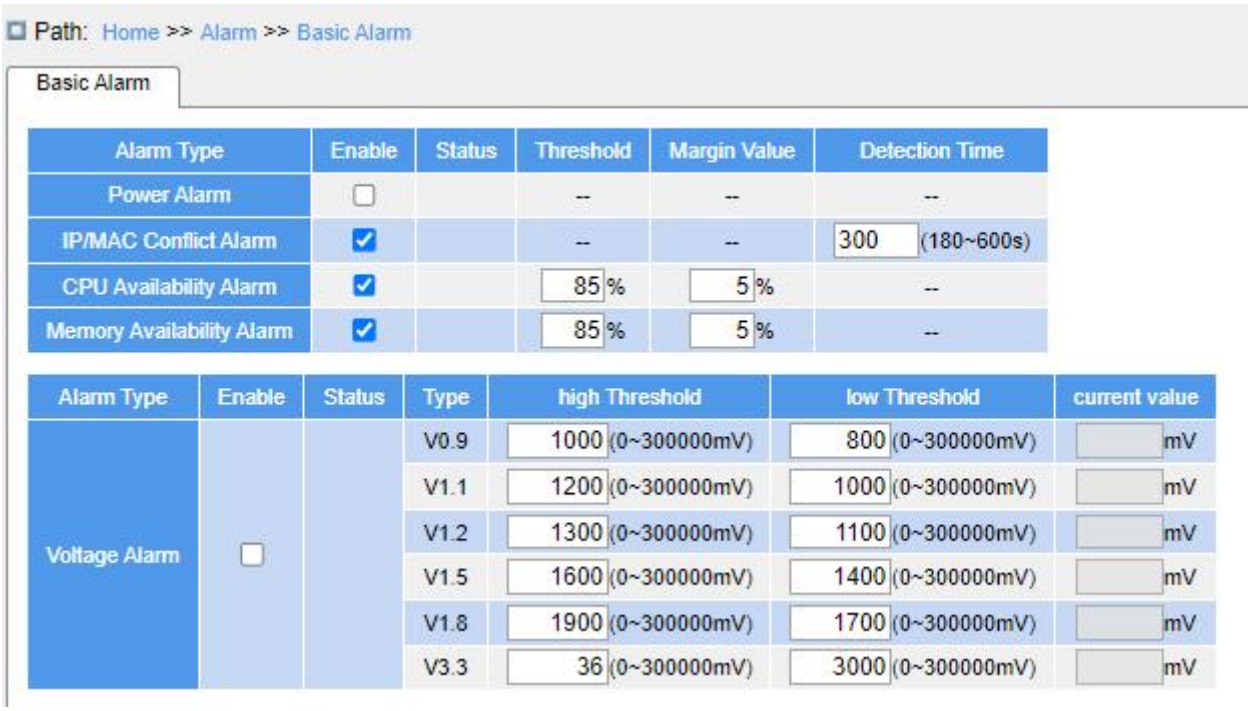


Figure 82 Basic Alarm

Power Alarm

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable 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 Alarm

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable IP/MAC conflict alarm.

Status

Configuration options: Conflict/No Conflict

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

Detection 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: Disable

Function: Whether to enable 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, 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%.

Voltage Alarm

Configuration options: Enable/Disable

Default configuration: Disable

Function: Enable/Disable Voltage Alarm.

V0.9/V1.1/V1.2/V1.5/V1.8/V3.3 high Threshold

Configuration range: 0~300000mV

Function:Configure High Threshold Voltage Alarm.

V0.9/V1.1/V1.2/V1.5/V1.8/V3.3 low Threshold

Configuration range:0~300000mV

Function:Configure low Threshold Voltage Alarm.

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

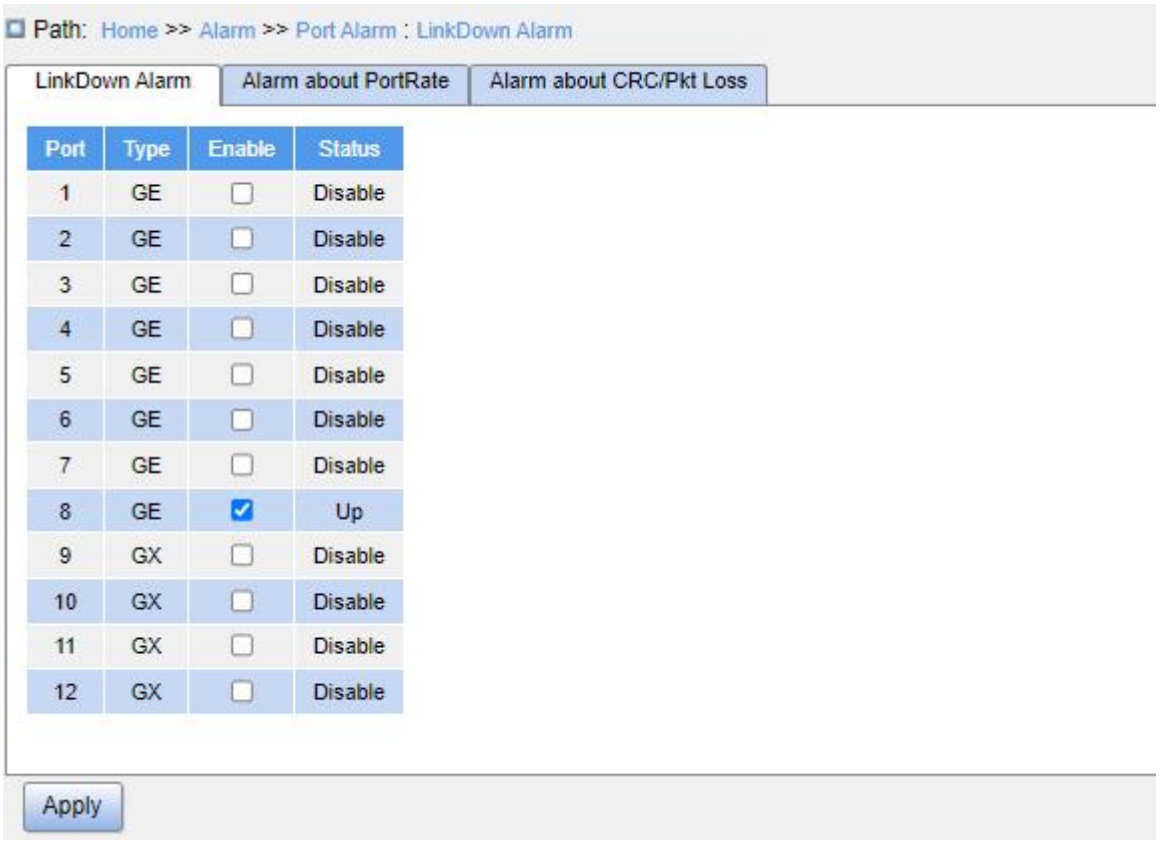


Figure 83 Port Alarm

LinkDown Alarm

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable port alarm.

Status

Configuration options: Up/Down

- Up: means the port is in connection state and supports normal communication.
- Down: means the port is disconnected or in abnormal connection (communication

failure).

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

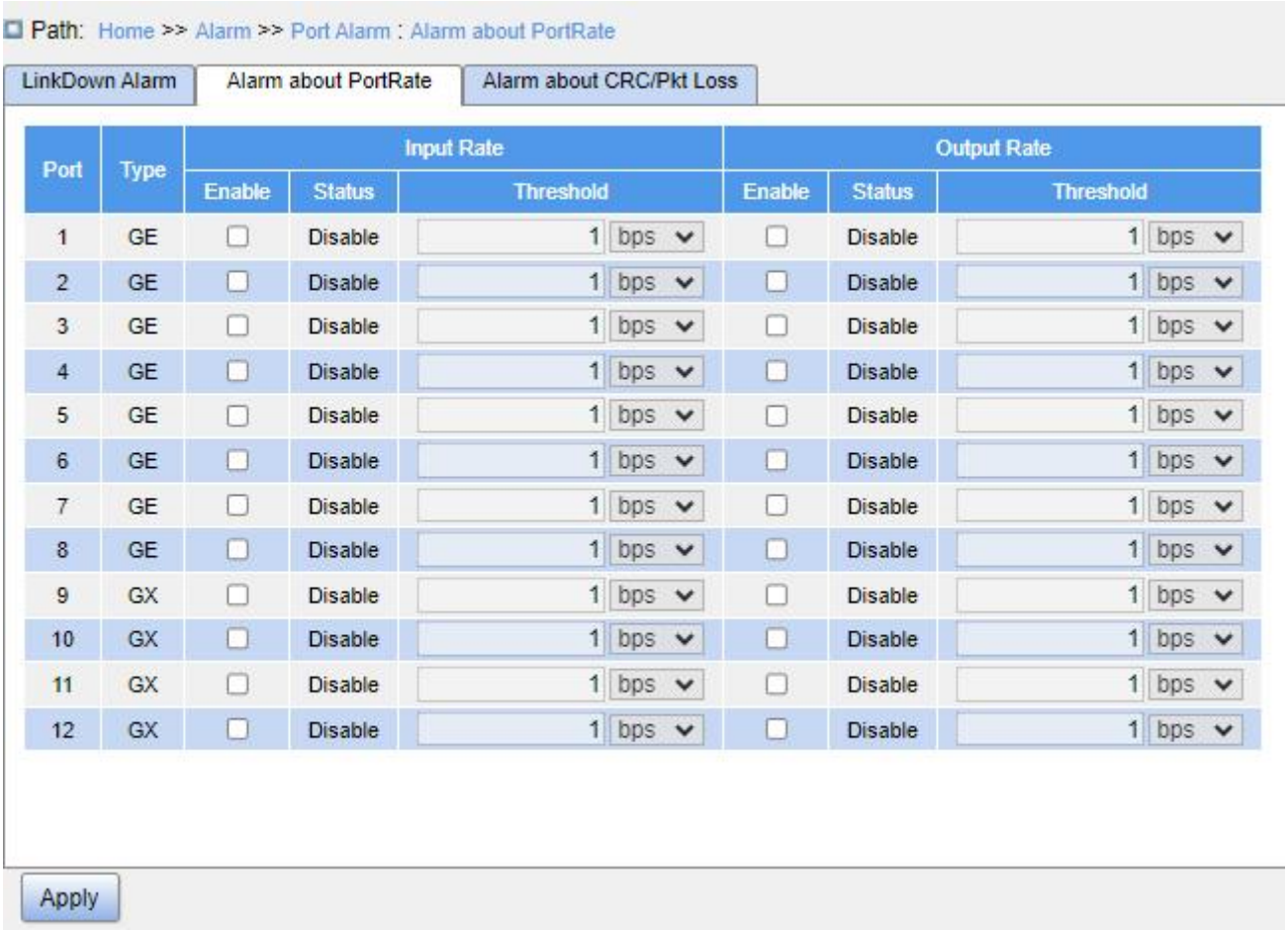


Figure 84 Port Traffic Alarm Configuration

Alarm about Portrate - Input Rate/Output Rate

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable port rate alarm.

Threshold

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

Function: Configure the threshold for port traffic.

Status

Configuration options: Disable/Alarm/Normal

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

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

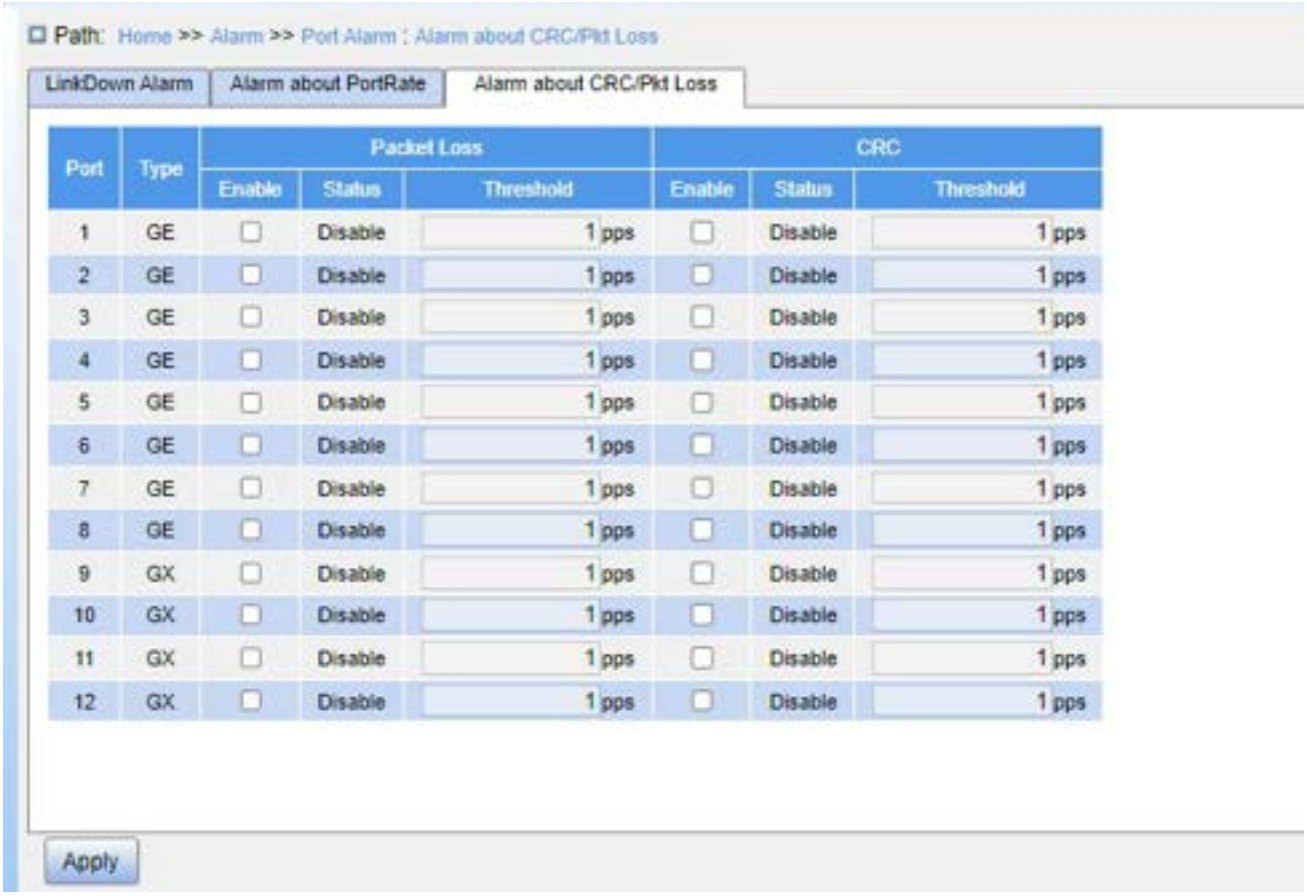


Figure 85 CRC Error/Pkt Loss Alarm Configuration

Alarm about CRC/Pkt Loss

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable CRC and packet loss alarm.

Threshold

Configuration range: 1 to 1000000 PPS

Function: Configure the threshold for the port CRC and packet loss alarm.

Status

Configuration options: Disable/Alarm/ Normal

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

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

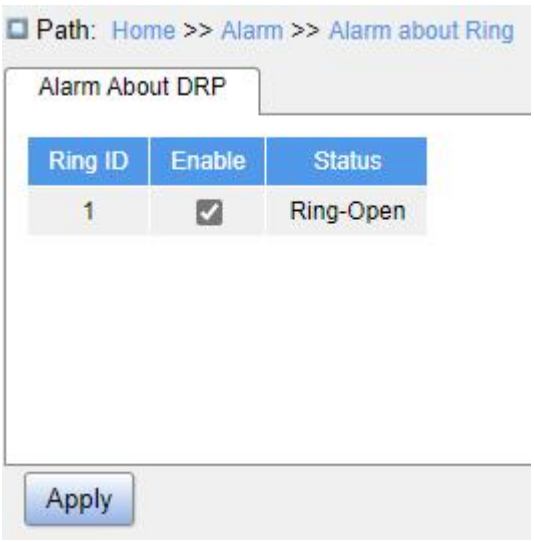


Figure 86 Ring Alarm Configuration

Alarm about DRP

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable DRP alarm.

Status

Configuration options: DRP Open/DRP Close/Disable

Function: View the DRP status.

- "DRP Open" means DRP is open.
- "DRP Close" means DRP is closed.

6. Configure and display DDM software alarm, as shown below.

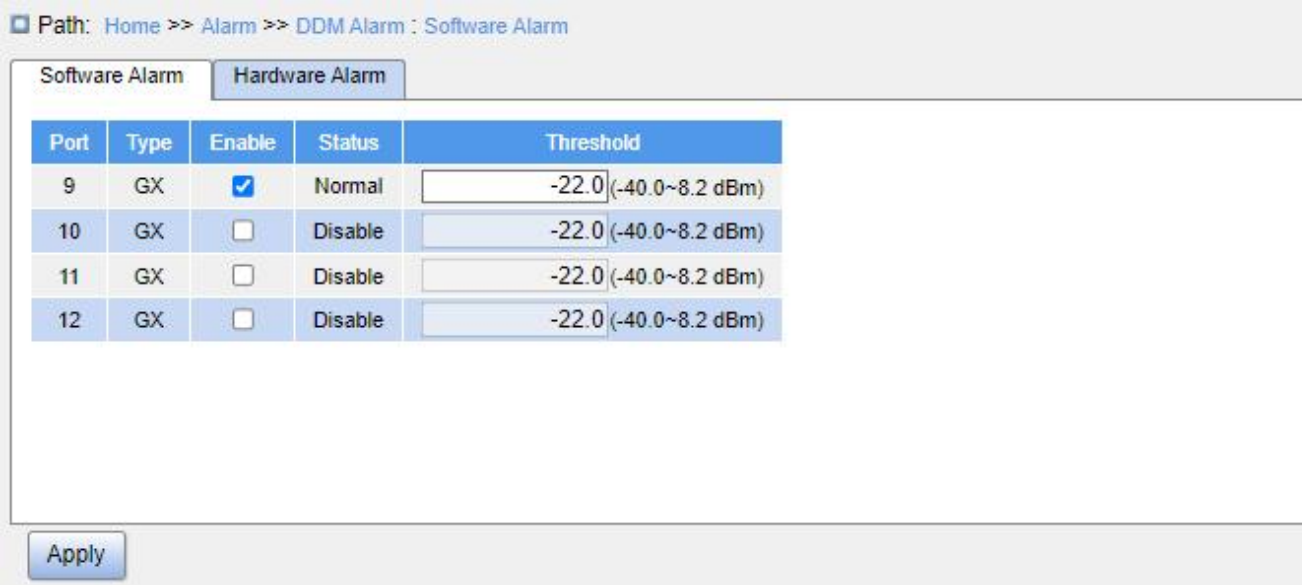


Figure 87 DDM Software Alarm Configuration

Software Alarm

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable SFP port RX power alarm.

Threshold

Configuration range: -40~8.2 (unit: dBm)

Default configuration: -22.0 dBm

Function: Configure the threshold for the SFP port RX power alarm.

Status

Configuration options: Normal/Alarm

Description: Software alarm refers to the port receiving optical power alarm, which requires the SFP module to support DDM function. If a DDM-supported SFP module is inserted, the receiving optical power is lower than the threshold, then alarm will be generated, the status is “Alarm”. If a DDM-supported SFP module is inserted, the receiving optical power is not lower than the threshold, then the status is “Normal”.

7. Configure and display SFP power hardware alarm, as shown below.

Figure 88 SFP Power Hardware Alarm Configuration

Hardware Alarm – DDM Alarm Enable

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable SFP power hardware alarm. When the current value is lower than the low threshold, a low alarm is generated. When the current value is higher than the high threshold, a high alarm is generated.

Caution:

The low and high thresholds vary by hardware and cannot be configured.

7 Function Management

7.1 Port Configuration

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

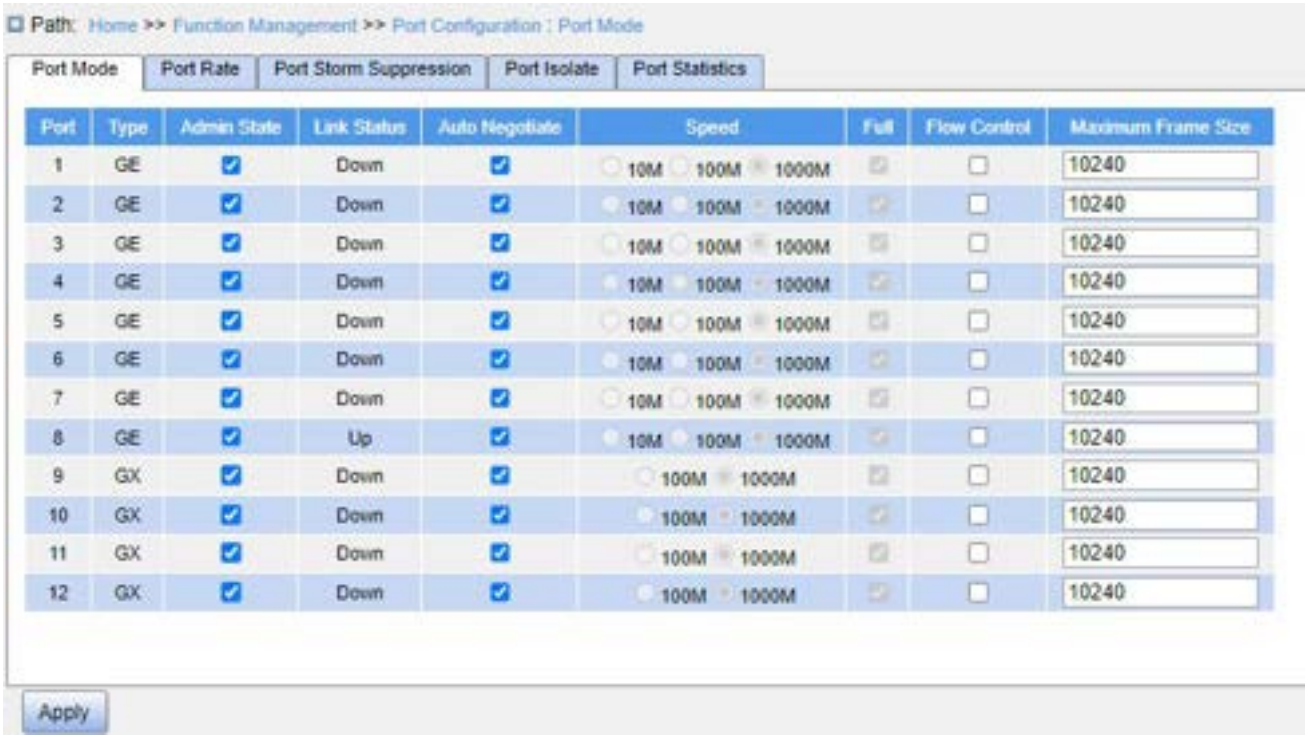


Figure 89 Configure Port Mode

Admin State

Configuration options: Enable/Disable

Default configuration: Enable

Function: Whether the port is allowed to transfer data.

Description: If enabled, the port is allowed to transfer data. If disabled, the port will be closed. This option directly affects the hardware status of the port and triggers port alarms.

Link Status

Function: Display 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.

For auto negotiation, port rate and duplex mode are automatically negotiated according to the connection status of both ports. It is recommended that the user configure the speed and duplex mode of the port to automatic negotiation to avoid connection problems caused by the mismatch of the port configuration. If the user configures the port to forced rate/duplex mode, make sure connection rate/duplex mode configuration on both ends are the same.

Caution:

- The Gigabit electronic port can be configured as auto negotiation, 10M full duplex, 10M half duplex, 100M full duplex, 100M half duplex, 1000M full duplex and 1000M half duplex.
- The Gigabit SFP port can be configured as auto negotiation, 100M full duplex and 1000M full duplex.
- The 10G SFP port is mandatorily configured as 10G full duplex.

Speed

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

Function: Configure port speed.

Description: When port mode is configured as 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. With port speed manually configured, the port can negotiate within only the specified rate range so as to control rate negotiation.

Caution:

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

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 only receive data at any one time. When the port mode is configured as automatic negotiation, the port duplex mode is determined by negotiation by default. The negotiated duplex mode can be either full duplex or half duplex. With duplex mode configured, the port can negotiate only one duplex mode, thus controlling the duplex mode negotiation.

Flow Control

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable flow control.

Description: After port flow control is enabled, 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 range: 1518~10240 bytes

Default configuration: 10240

Function: Configure the maximum frame size that is allowed by the port. Frames larger than the specified value will be discarded.

2. Configure port rate, as shown below.

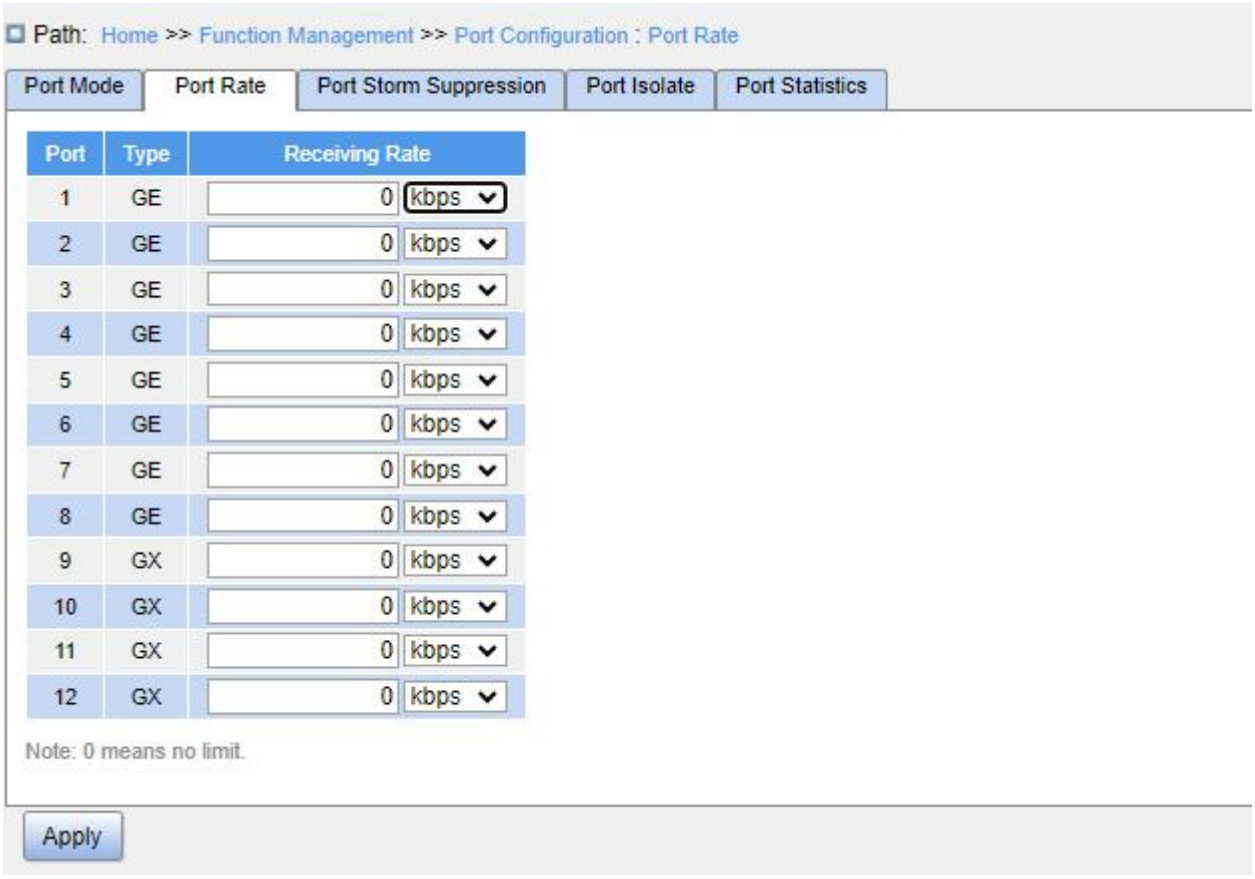


Figure 90 Port Rate Configuration

Receiving Rate

Configure options: 0/10~13128147 Kbps/fps, 0/25~13128147 Mbps/Kfps

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

Function: Configure port rate limit threshold. The packets that exceed the threshold will be discarded.

3. Configure port storm suppression, as shown below.

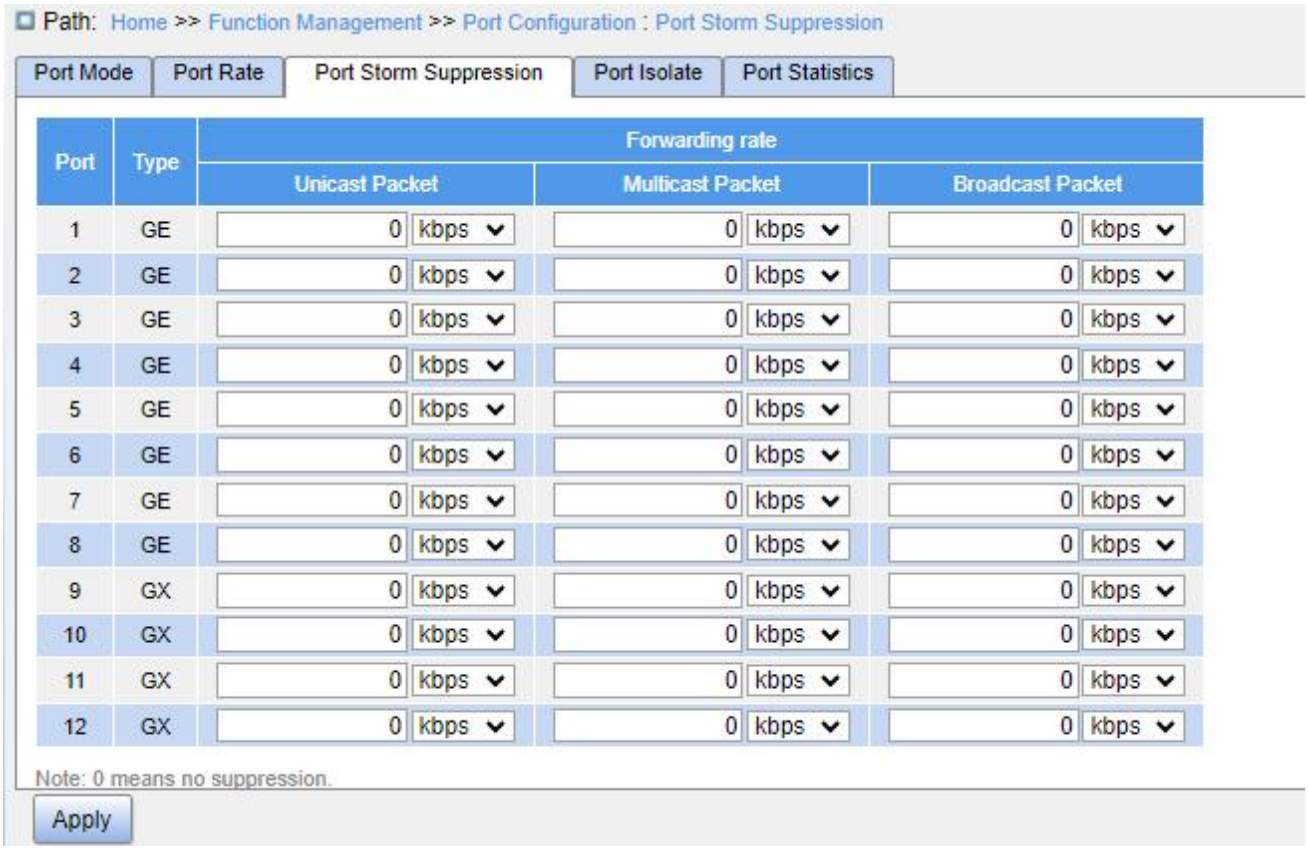


Figure 91 Port Storm Suppression

Forwarding Rate

Configuration options: Unicast Packet/Multicast Packet/Broadcast Packet

Configure options: 0/10~13128147 Kbps/fps, 0~13128 Mbps/Kfps

Default configuration: 0, value 0 means to disable storm suppression

Function: Configure port forwarding rate threshold. The specified type of packets that exceeds the threshold will be discarded.

4. Configure port isolation, as shown below.

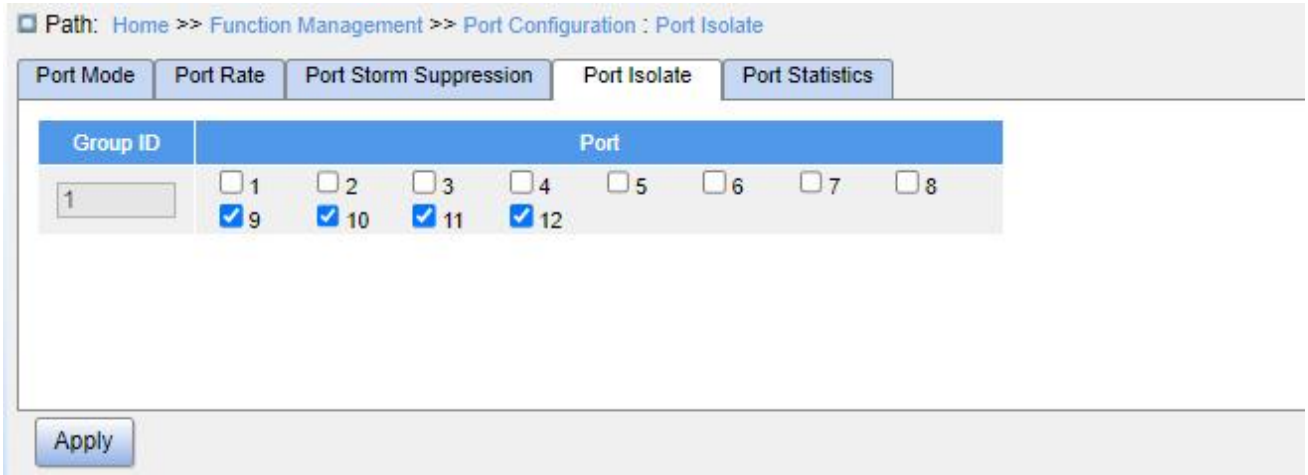


Figure 92 Port Isolation

Port Isolate

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable port isolation.

Note: There is only one port isolation group.

5. Configure port statistics, as shown below.

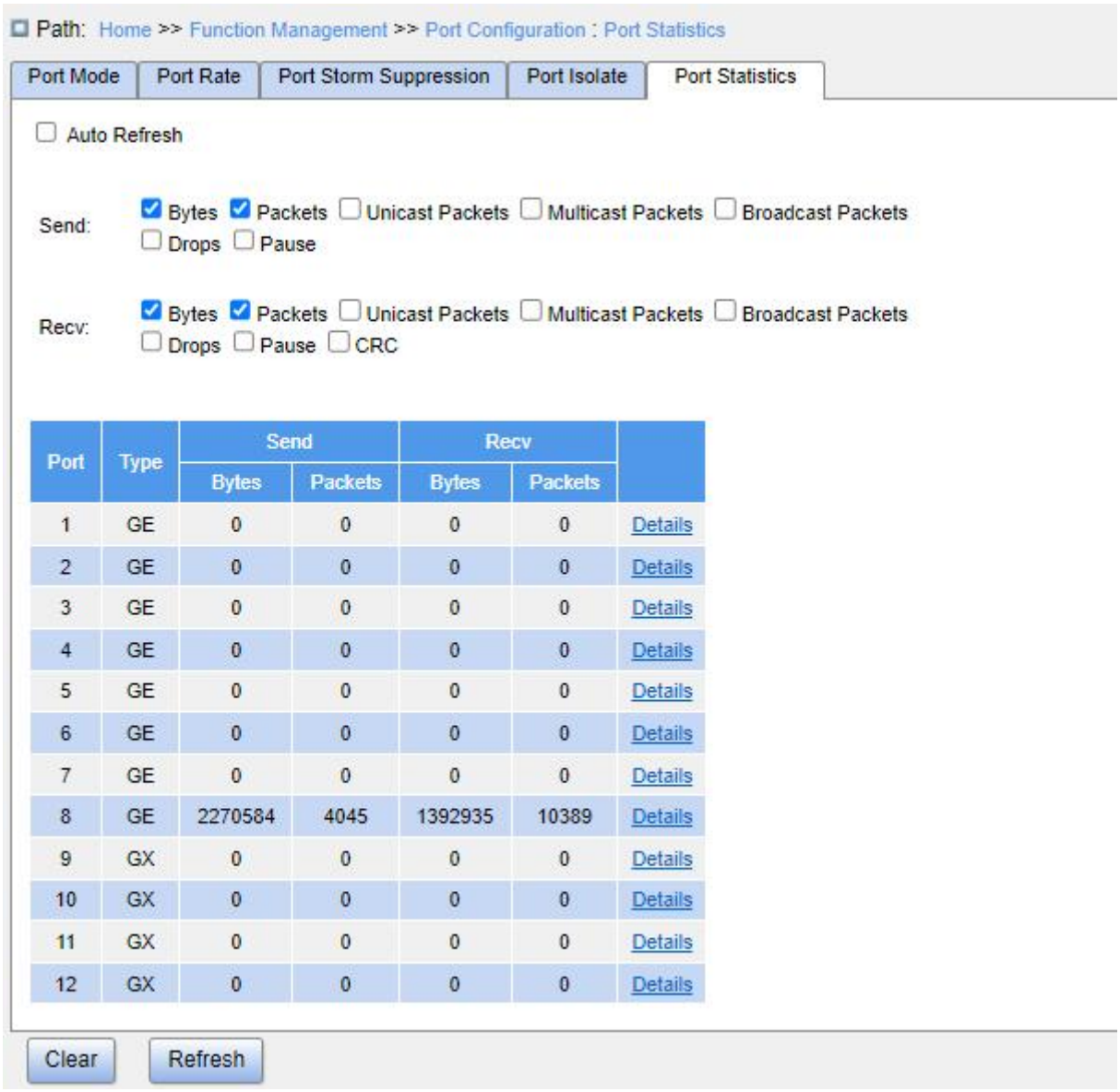


Figure 93 Port Statistics

Bytes

Function: Count the number of received/sent bytes.

Packets

Function: Count the number of received/sent packets.

Unicast Packets

Function: Count the number of received/sent unicast packets.

Multicast Packets

Function: Count the number of received/sent multicast packets.

Broadcast Packets

Function: Count the number of received/sent broadcast packets.

Drops

Function: Count the number of messages dropped due to receiving/sending conflicts.

Pause

Function: Count the number of received/sent Pause frames.

CRC

Function: Count the number of received/sent CRC messages.

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

3. View port detail information statistics, as shown below.

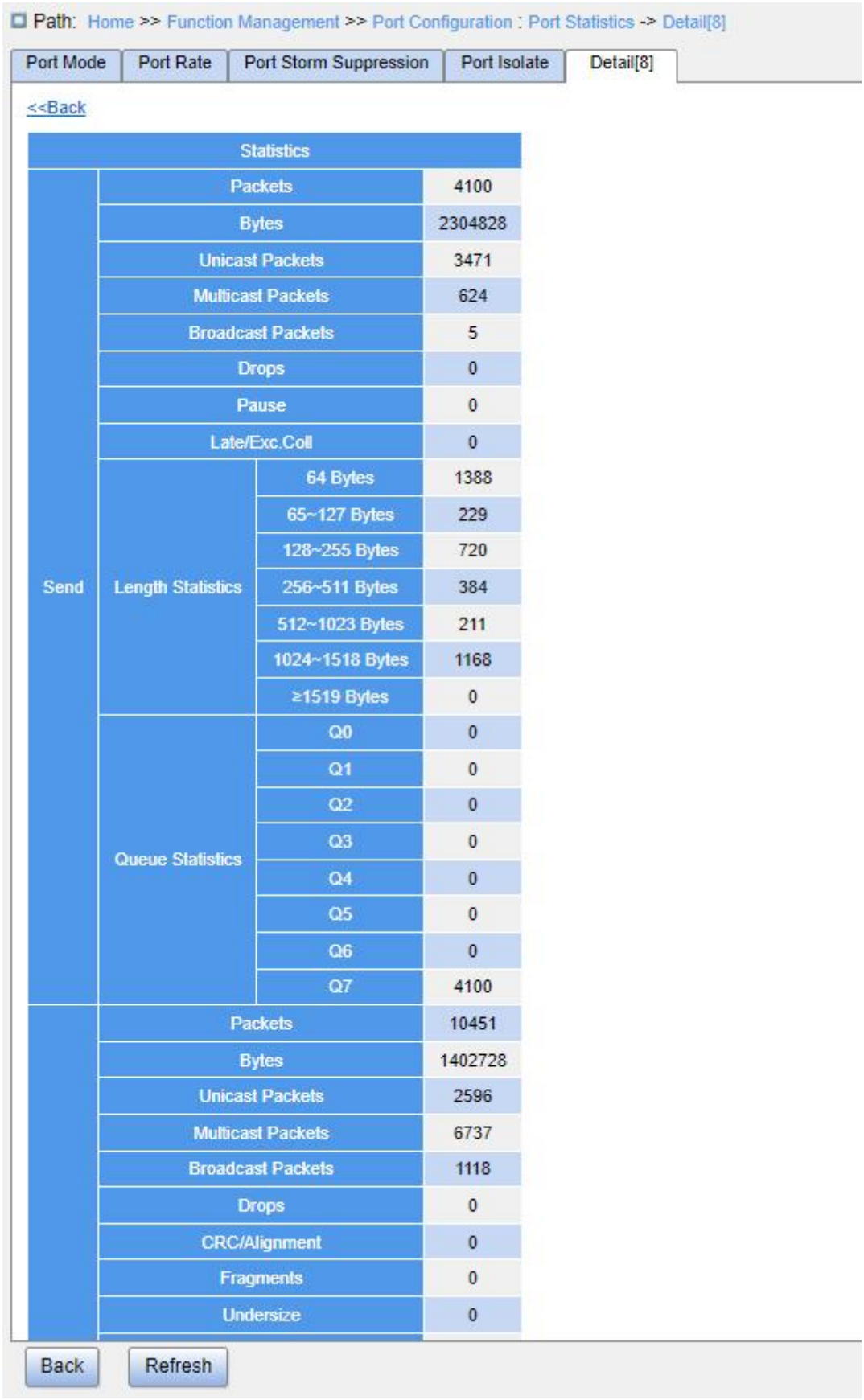


Figure 94 Port Detail Information Statistics

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, identifying a data frame carrying a VLAN tag. The value is 0x8100. The value of TPID specified in the 802.1Q protocol is 0x8100.

PRI: 3 bits, identifying the 802.1p priority of a packet.

CFI: 1 bit, specifying 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 249 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

Processing of Received Packets		**Processing of Packets to Be Forwarded**	
Untagged packets	**Tagged packets**	**Port Mode**	**Packet Processing**
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.	➢ 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.	Access	Forward the packet after removing the tag.
		Trunk	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.
		Hybrid	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 through, forward the packet after removing the tag.

7.2.1.4 Web Configuration

1. Configure port link mode, as shown below.

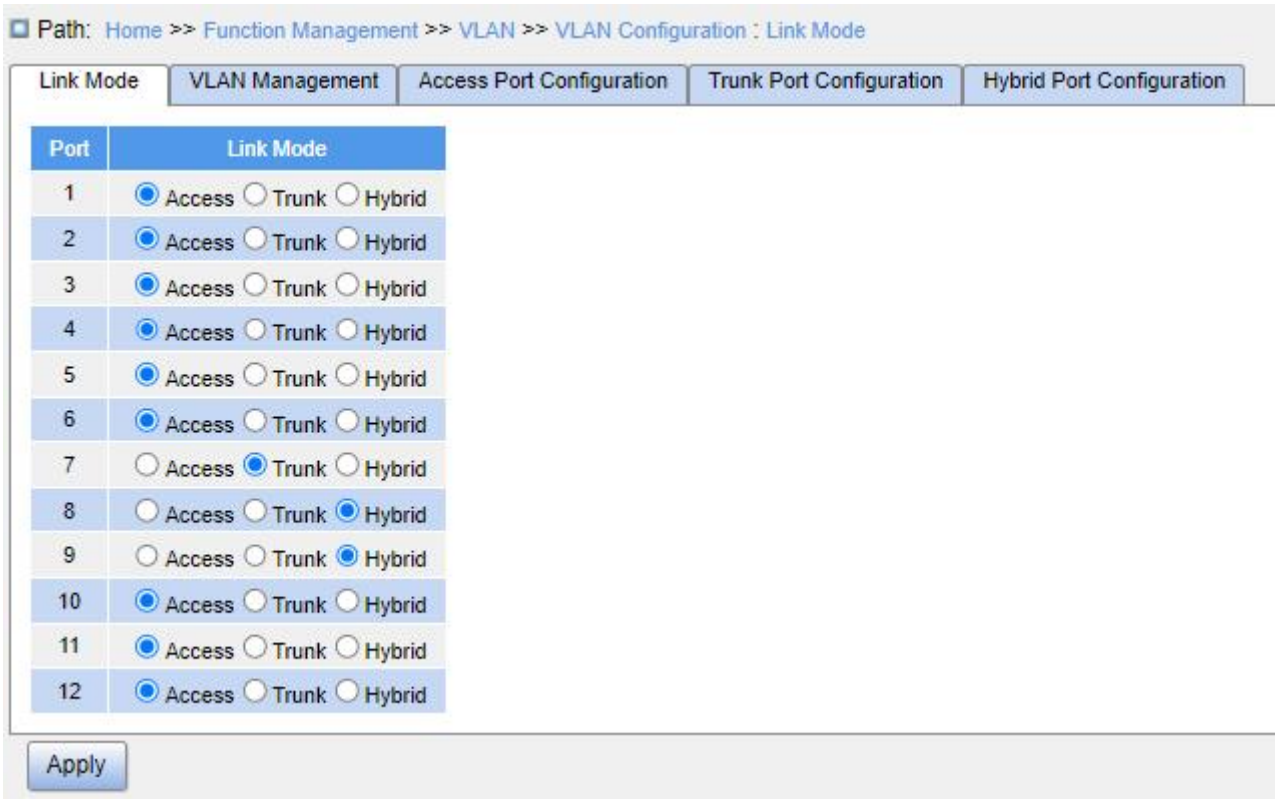


Figure 95 Configure Port Link Mode

Link Mode

Configuration options: Access/Trunk/Hybrid

Default configuration: Access

Function: Configure the specified port link mode.

2. Configure VLANs, as shown below.

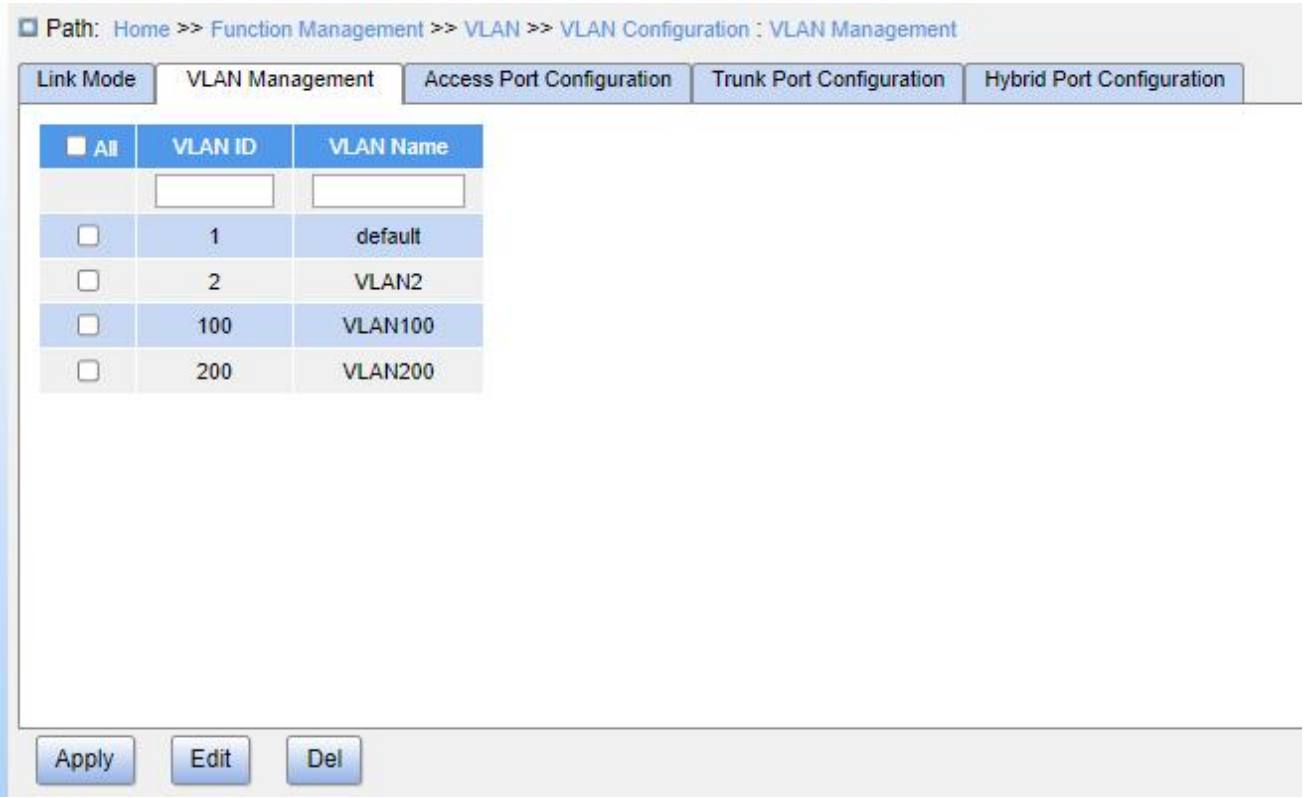


Figure 96 VLAN Management

VLAN ID

Configuration range: 1~4093

Default configuration: 1

Function: Create VLAN.

VLAN Name

Configuration range: 1~32 characters, supporting capital letters, lowercase letters, numbers, and underscores.

Function: Configure VLAN name.

3. Configure Access ports, as shown below.

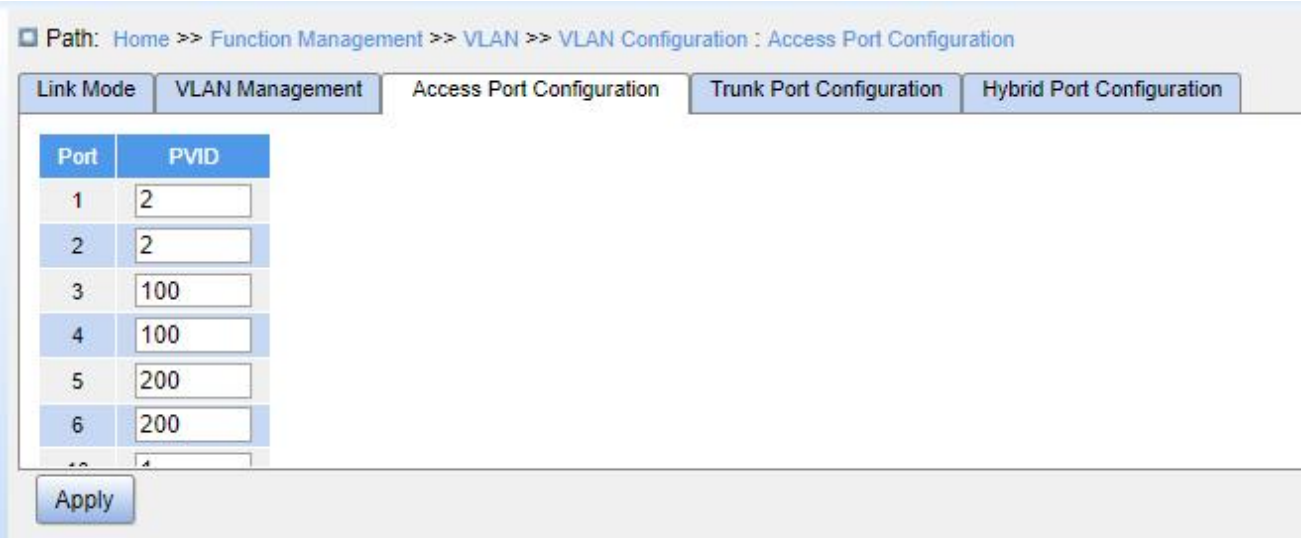


Figure 97 Configure Access port

PVID

Configuration range: 1~4093

Default configuration: 1

Function: Configure the default VLAN for the Access port.

Caution:

The VLANs need to be created before you configure the VLAN ID of Access port, the Trunk port, or Hybrid port.

4. Configure Trunk ports, as shown below.

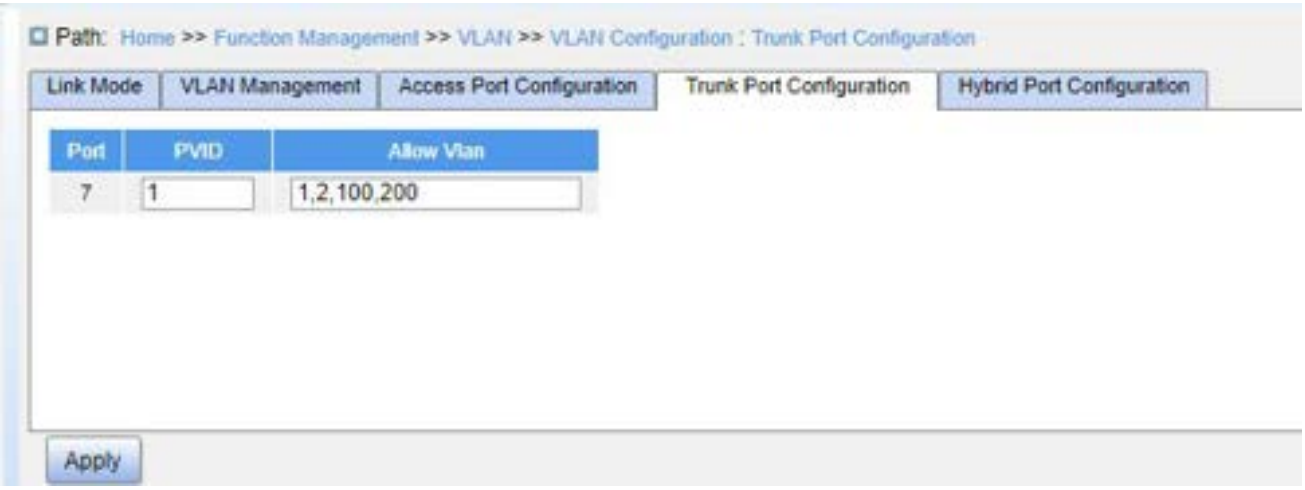


Figure 98 Trunk port Configuration

PVID

Configuration range: 1~4093

Default configuration: 1

Function: Configure the default VLAN of Trunk port.

Allow 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 the allowed VLANs of Trunk port.

5. Configure Hybrid port, as shown below.

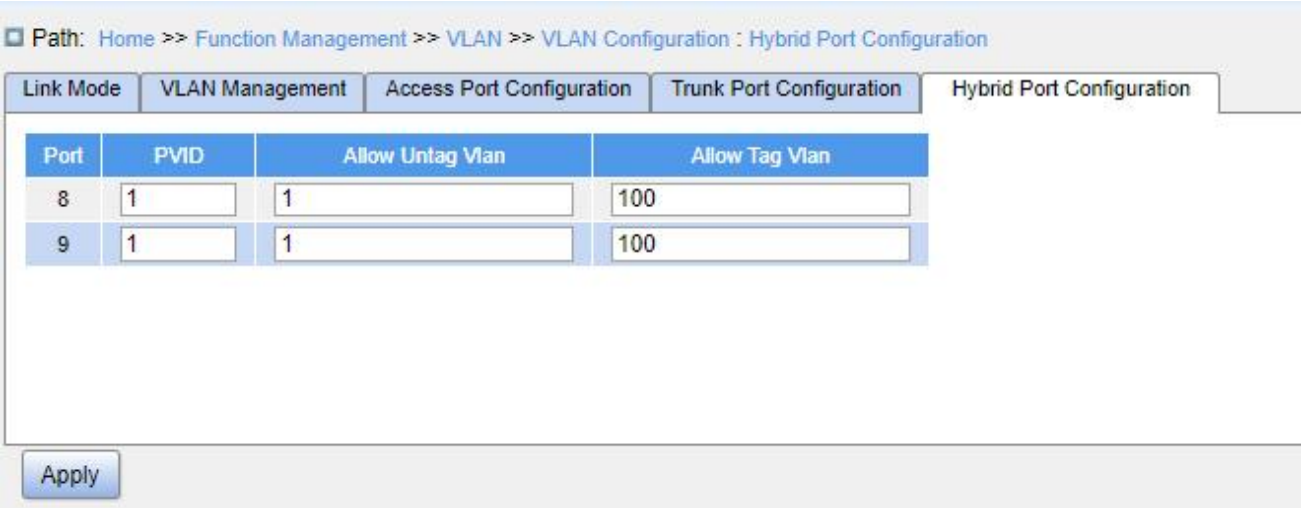


Figure 99 Hybrid port Configuration

PVID

Configuration range: 1~4093

Default configuration: 1

Function: Configure the default VLAN of Hybrid port.

Allow 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 the allowed Untag VLANs of Hybrid port.

Allow 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 the allowed Tag VLANs of Hybrid port.

7.2.1.5 Typical Configuration Example

As shown in Figure 100, 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, VLAN 100, and VLAN 200 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.

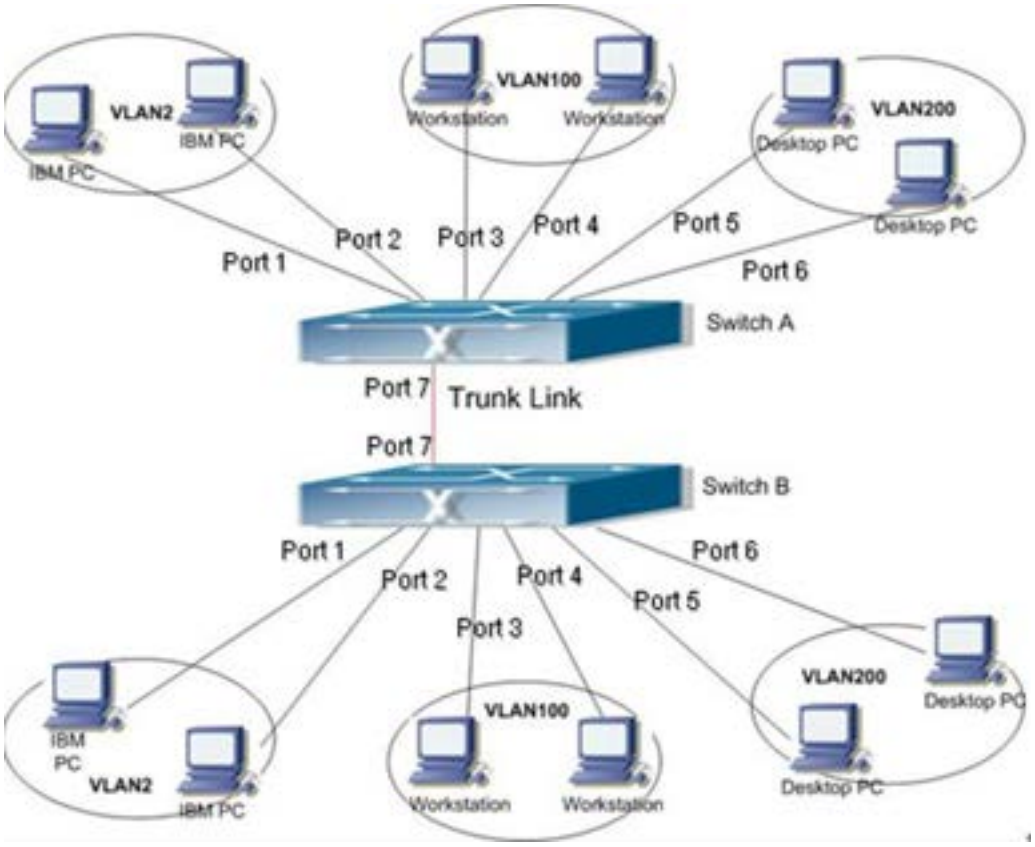


Figure 100 VLAN Application

Configurations on Switch A and Switch B:

1. Configure allowed access VLANs to 1, 2, 100, 200, as shown in Figure 97.

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 98.

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 other GARP members to register or cancel its own configuration information by means of Join/Leave message respectively. The member also registers or cancels the configuration information of other members based on Join/Leave messages sent by other members.

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

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

When a GARP application entity wants to cancel its own information on other switches, the entity sends a Leave message.

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

Note:

An application entity indicates a GARP-enabled port.

GARP timers include Hold timer, Join timer, Leave timer, 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 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:

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. Enable global GVRP protocol, and configure timers, as shown below.

Figure 101 GVRP Global Configuration

GVRP Enable

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable GVRP.

Join-time

Configuration options: 1~20 centisecond

Default configuration: 20

Function: Configure Join timer value.

Leave-time

Configuration options: 60~300 centisecond

Default configuration: 60

Function: Configure Leave timer value.

LeaveAll-time

Configuration options: 1000~5000 centisecond

Default configuration: 1000

Function: Configure LeaveAll timer value.

Description: if the LeaveAll timer for different devices times out at the same time, multiple LeaveAll messages are sent simultaneously, which increases 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 LeaveAll timer is a random value, which is greater than the LeaveAll timer value and less than 1.5 times the LeaveAll timer value.

Max VLANs

Configuration range: 1~4093

Default configuration: 20

Function: Configure the maximum number of dynamically registered VLANs of GVRP port.

Caution:

Disable GVRP before configuring GVRP timer and Max VLANs.

2. Configure GVRP port, as shown below.

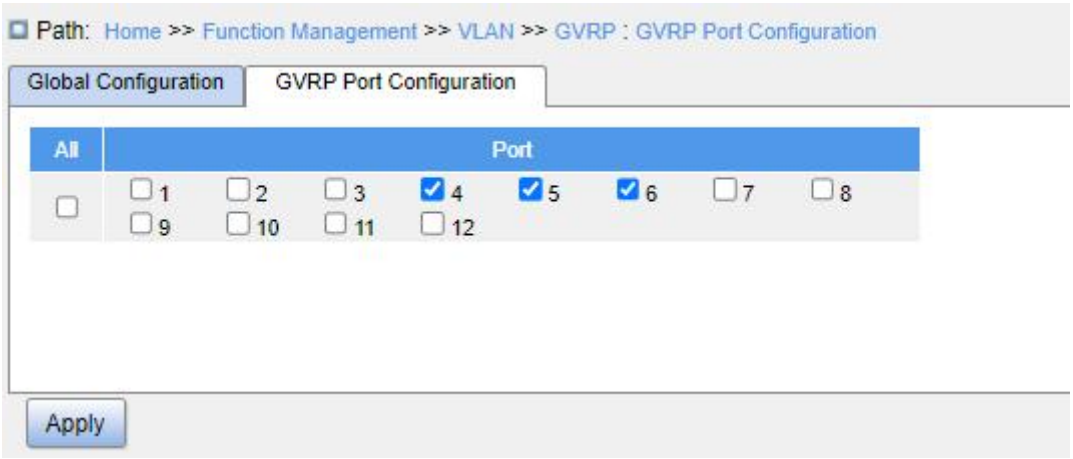


Figure 102 GVRP Port Configuration

Port

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable 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 103 shows, GVRP needs to be enabled on devices so that VLAN information is dynamically registered and updated between device A and device B.

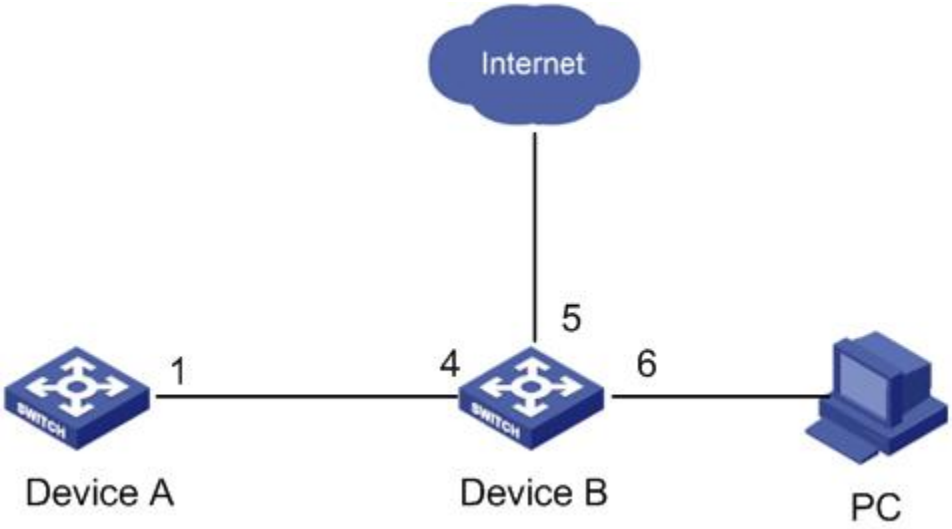


Figure 103 GVRP Configuration Example

Device A Configurations:

1. Configure port 1 to Trunk port, allowed VLANs to 1.
2. Enable global GVRP, as shown in Figure 101.
3. Enable GVRP on port 1, as shown in Figure 102.

Device B Configurations:

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 101.
3. Enable GVRP on port 4, 5, 6, as shown in Figure 102.

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

7.2.3 VLAN Status

Check the port VLAN status, as shown below.

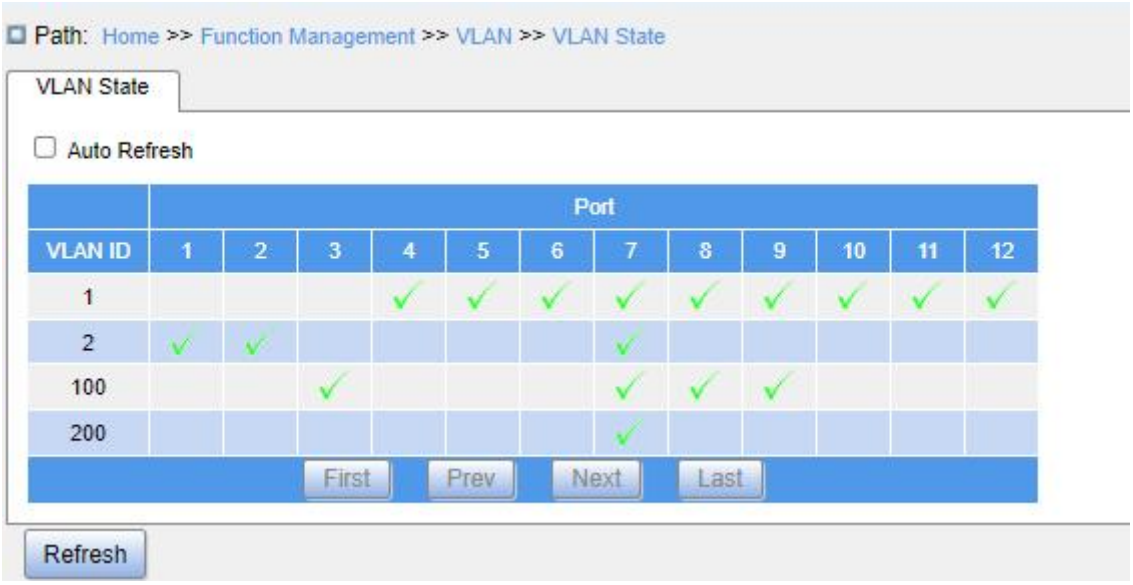


Figure 104 Port VLAN Status

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 105.

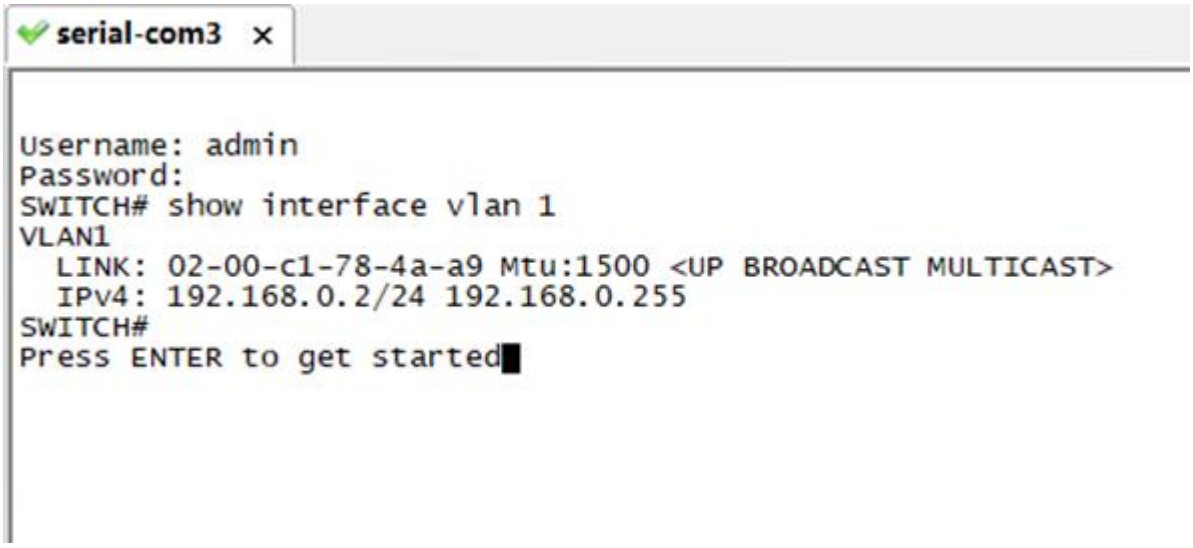


Figure 105 Display IP Address

2. Create VLAN interface.

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

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

3. Configure primary IPv4 address.

The primary IPv4 address of the switch can be obtained automatically or be manually configured as shown below.

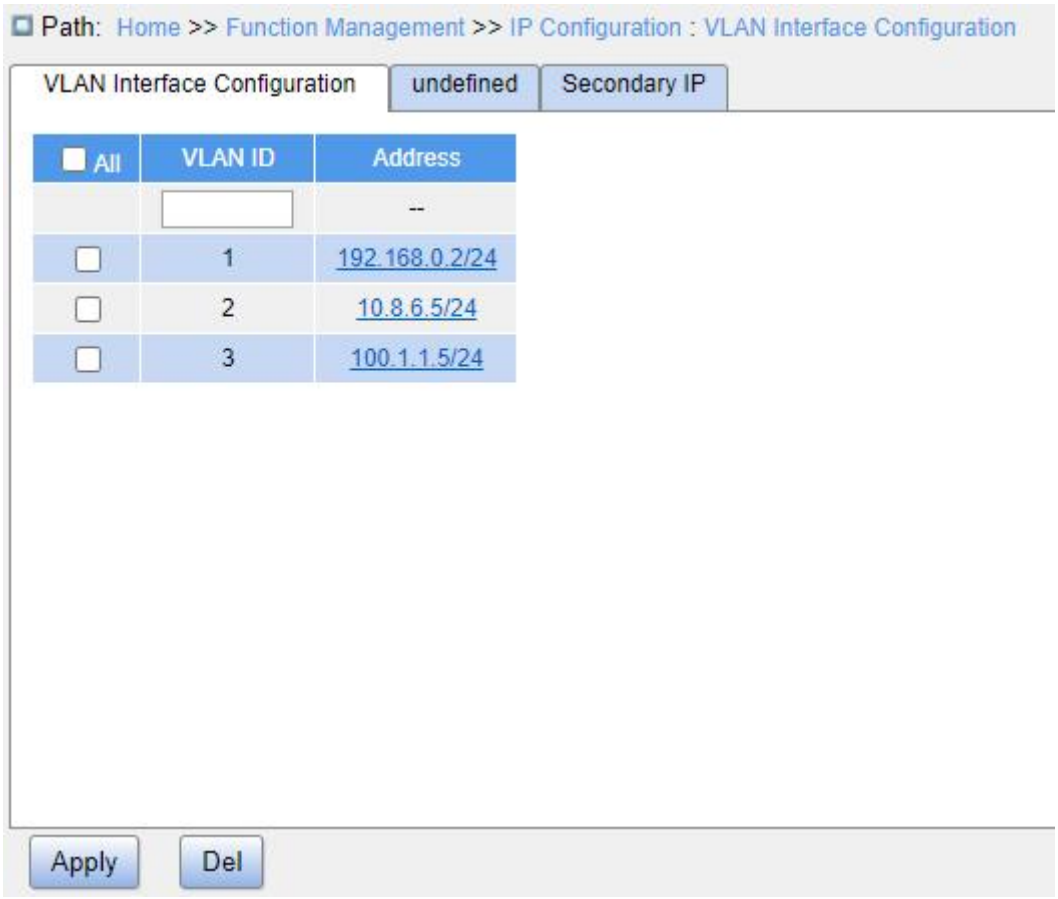


Figure 106 VLAN Interface Configuration

VLAN ID

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

Address

Function: Configure the IPv4 address and mask obtained by the VLAN interface.

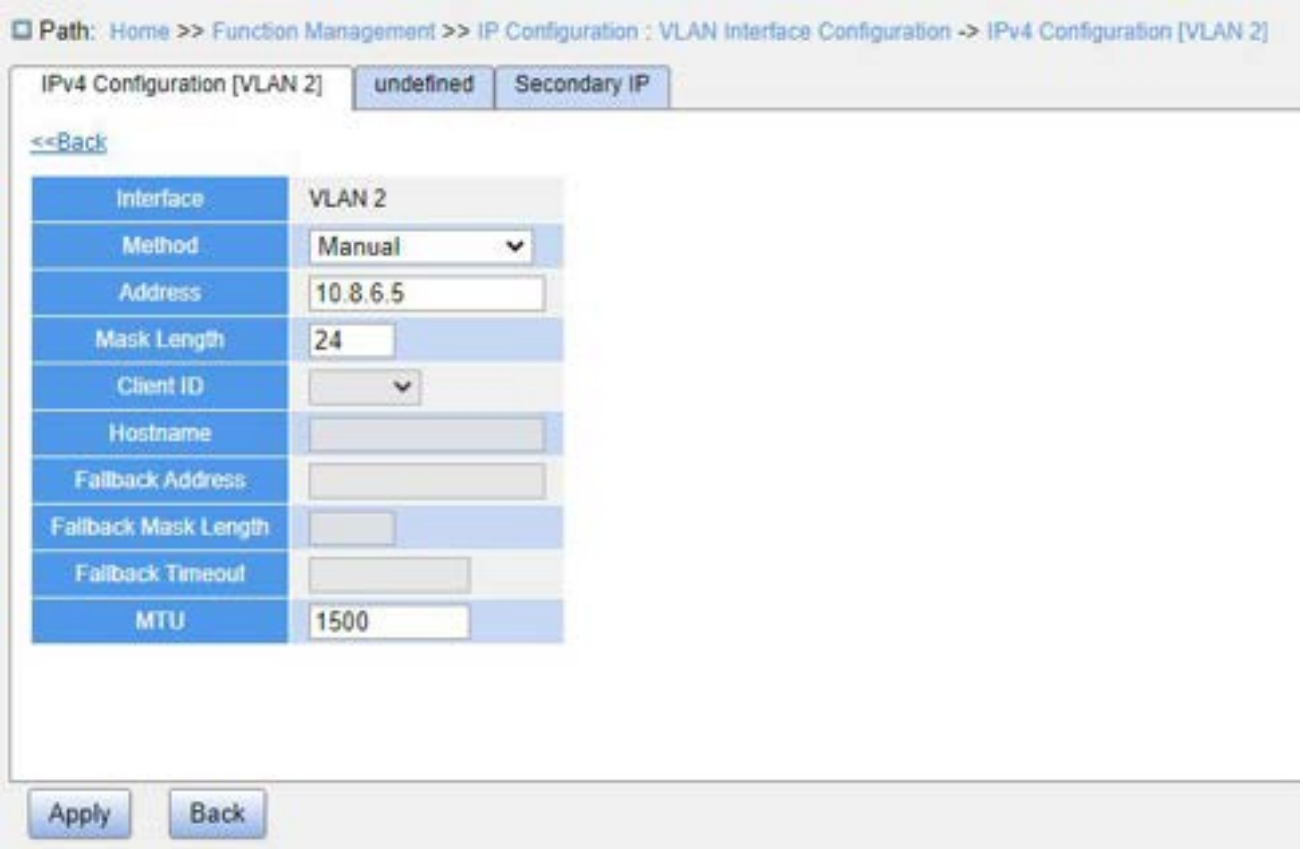


Figure 107 IP Address Configuration

Method

Configuration options: None/DHCP/Manual

- Manual: You need to manually configure the IP address and subnet mask.
- DHCP: The switch automatically gets the IP address through DHCP protocol as DHCP client. In this case, there should be DHCP server to assign IP address and subnet mask to clients in the network.

Address

Configuration format: A.B.C.D

Function: Configure the IP address of the VLAN interface.

Mask Length

Configuration range: 1~30

Function: Configure the mask length of the IP address.

Client ID

Configuration options: Hex/Name/Port

Function: When a VLAN interface sends a DHCP request, it will carry the Option61 field.

The field can be padded in the following ways:

- Hex: type01 + MAC address
- Name: type00 + string
- Port: MAC address of the corresponding interface

Hostname

Configuration range: 0~63 characters

Function: Configure the host name of the switch.

Fallback Address

Configuration format: A.B.C.D

Function: After the IP address obtained by the VLAN interface times out, this IP address will be set to the fallback address.

Fallback Mask Length

Configuration range: 1~30

Function: Configure the mask length of the fallback IP address.

Fallback Timeout

Configuration range: 0~4294967295s

Function: When the value is not 0, the value specifies the length of attempt time that the switch tries to obtain an IP address through the DHCP protocol. In this case, you need to manually configure an IP address. When the attempt time times out, the manually configured IP address takes effect. When the value is 0, the switch will repeatedly attempt to obtain an IP address through the DHCP protocol until one is assigned. In this case, a manually configured IP address is not necessary.

MTU

Configuration range: 68~9600

Default configuration: 1500

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

4. Configure secondary IPv4 address. Manually configure the secondary IPv4 address of the switch's VLAN interface, as shown below.

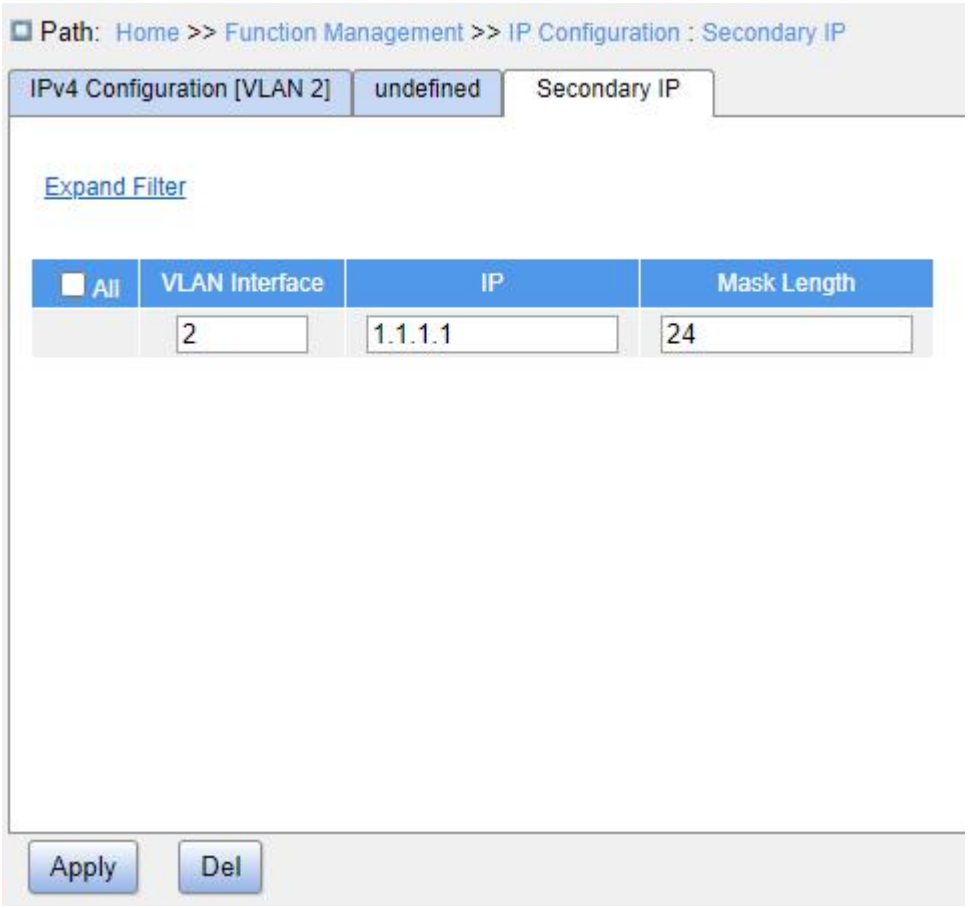


Figure 108 Secondary IP Configuration

VLAN Interface

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

IP

Configure format: A.B.C.D

Function: Manually configure the IPv4 address.

Mask Length

Configuration range: 1~30

Function: Configure the IPv4 address's mask length.

Description: A subnet mask is a 32-bit number, composed of a sequence of bits 1 and a sequence of bits 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 VLAN interface corresponds to a primary IP address and may correspond to multiple secondary IP addresses;
- Different VLAN interfaces should be configured with primary and secondary IP addresses for different network segments.

5. Configure IPv6 address.

The IPv6 address of the VLAN interface can be manually configured as shown below.

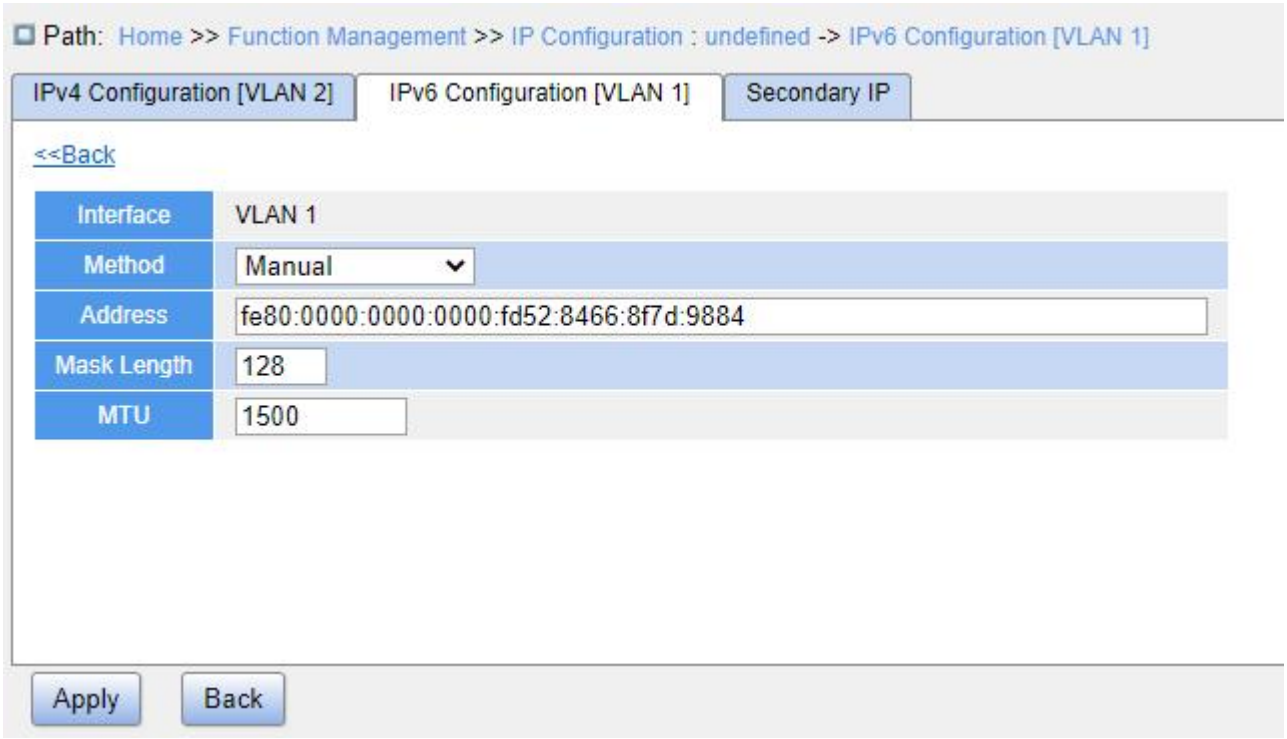


Figure 109 IPv6 Address Configuration

Method

Configuration options: None/Manual

Description: The IPv6 address can only be configured manually.

Address

Configuration format: XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX

Function: Configure the IPv6 address of the VLAN interface.

Mask Length

Configuration range: 0~128

Function: Configure the prefix length of the IPv6 address.

7.4 Loopback Configuration

The TCP/IP protocol defines the IP addresses on the network segment 127.0.0.0 as loopback addresses. The interfaces configured with a loopback address are called loopback interfaces. A loopback interface is a virtual interface. It has the following characteristics:

- A loopback interface is always up after being created.
- The netmask of a loopback interface configured with an IPv4 address must be 32.
- A loopback interface can be enabled with dynamic routing protocols.

The IP address of a loopback interface is treated as the identifier of a device and is always configured as the source address of IP packets originated by the device.

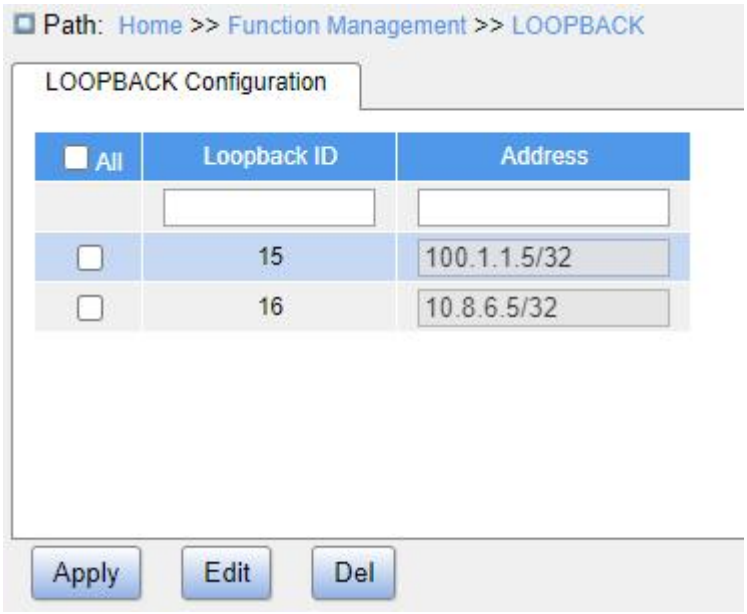


Figure 110 Loopback Interface Configuration

Loopback ID

Configuration range: 1~16

Function: Set the loopback interface ID.

Address

Configuration format: A.B.C.D/M

Function: Set the IP address and netmask of the loopback interface. The netmask must be 32.

7.5 Port Aggregation

7.5.1 Static Aggregation

7.5.1.1 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.

7.5.1.2 Implementation

As shown in Figure 111, 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.

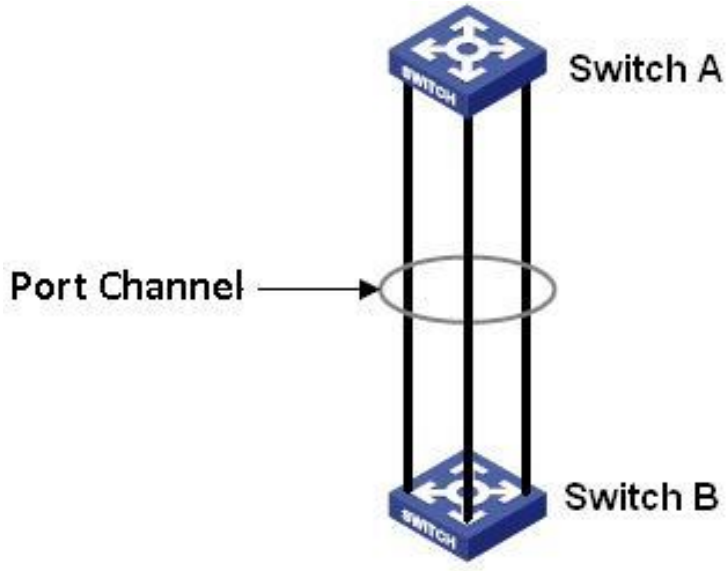


Figure 111 Port Channel

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.
- 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 DRP ring port, DRP backup port, RSTP port, and MSTP port.

7.5.1.3 Web Configuration

1. Configure static aggregation, as shown below.

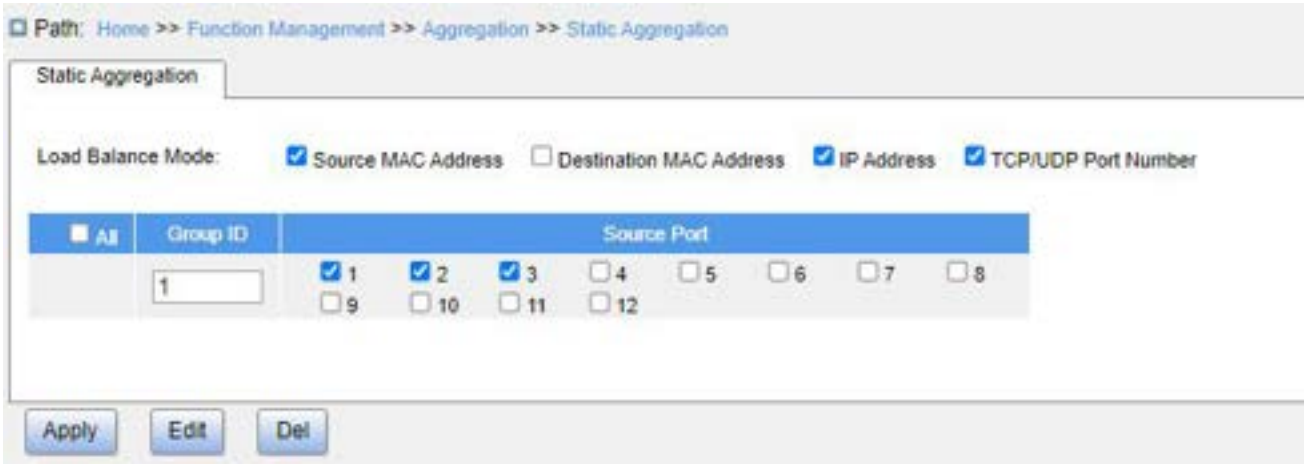


Figure 112 Static Aggregation Configuration

Load Balance Mode

Configuration options: Source MAC Address/Destination MAC Address/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.

- Source MAC Address: Balances the traffic according to the source MAC address;

- Destination MAC Address: Balances the traffic according to the destination MAC address;
- IP Address: Balances the traffic according to the IP address;
- TCP/UDP Port Number: Balances the traffic according to the TCP/UDP port number.

Group ID

Configuration range: 1~N (N = Number of ports/2)

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 ports to join the specified aggregation group.

7.5.1.4 Typical Configuration Example

As shown in Figure 111, 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 112.
2. Add port 1, 2, and 3 of switch B to port group 1, as shown in Figure 112.

7.5.2 LACP

7.5.2.1 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.

7.5.2.2 Implementation

A port enabled with LACP informs the peer port of its LACP priority of the local equipment, equipment MAC address, and 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:

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. It compares the IDs of the equipment at both ends (equipment ID = equipment LACP priority+ equipment MAC address). At first, it compares the LACP priorities. If the LACP priorities are the same, it compares their MAC addresses and selects the equipment with a smaller ID as the master equipment.

2. It compares the port IDs of the master equipment (port ID = LACP priority of the port + port number). At first, it compares the LACP priorities of the ports. If the port LACP priorities are the same, it compares the port numbers and selects 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.

7.5.2.3 Web Configuration

1. Configure LACP priority, as shown below.

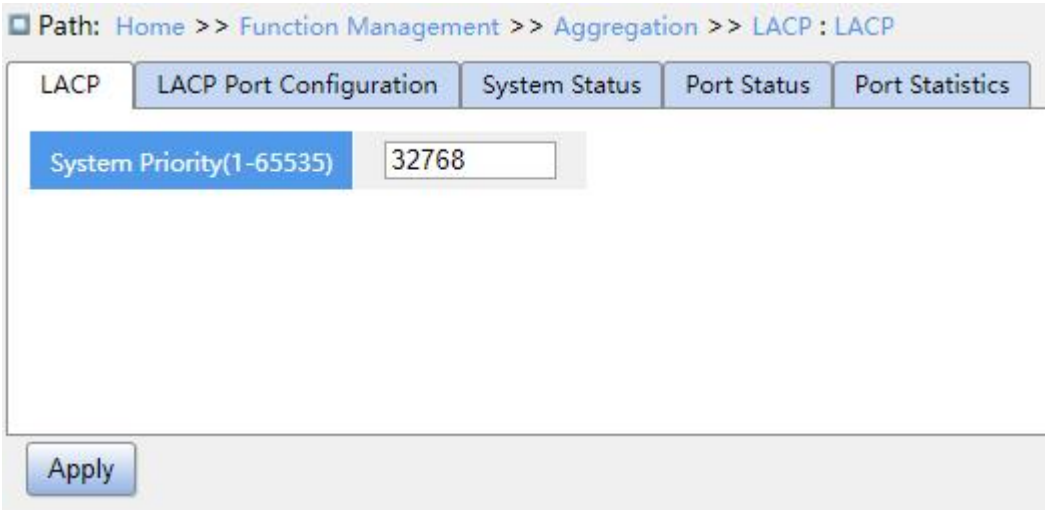


Figure 113 Configure LACP Priority

LACP

Configuration range: 1~65535

Default configuration: 32768

Function: Configure LACP priority, which is used to select the master device during LACP negotiation.

2. Configure LACP port, as shown below.

Figure 114 LACP Port Configuration

LACP Enable

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to 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 when “Auto” is selected:

- key=1 (10Mb);
- key=2 (100Mb);
- key=3 (1000Mb).

Ports with different key values cannot be added to the same dynamic aggregation groups.

Role

Configuration options: Active/Passive

Default configuration: Active

Function: Select the role of LACP. The active port will send the LACPDU messages to the end port actively; the passive port sends an LACPDU message to the end port only after receiving an LACPDU message from it.

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 time interval at which the active port sends LACPDU messages.

- Fast: Time interval is 1s;
- Slow: Time interval is 30s.

Priority

Configuration range: 1~65535

Default configuration: 32768

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

3. View LACP system status, as shown below.

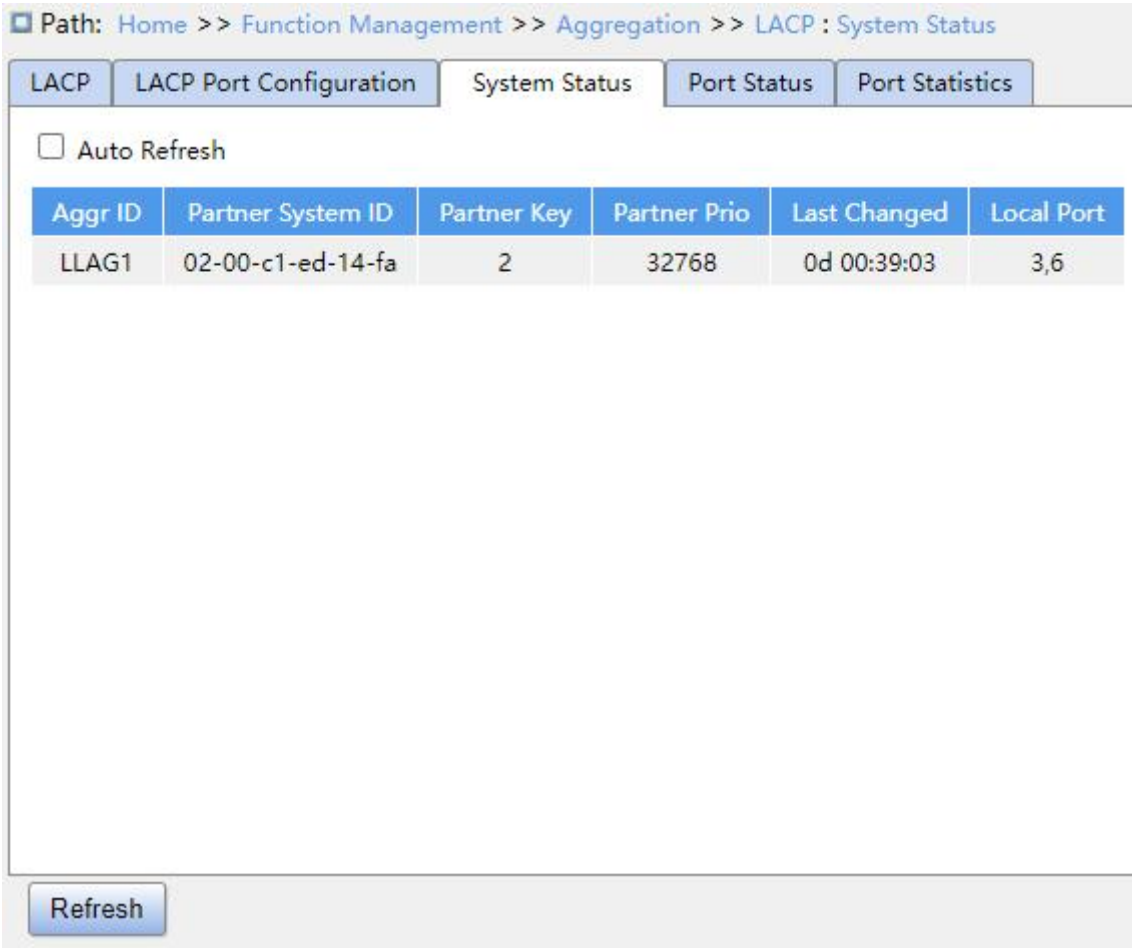


Figure 115 View LACP System Status

Aggr ID

Function: Display the aggregation group ID.

Partner System ID

Function: Display the partner device ID, identified by the MAC address.

Partner Key

Function: Display the Key value of the partner ports.

Partner Prio

Function: Display the system priority of the partner device.

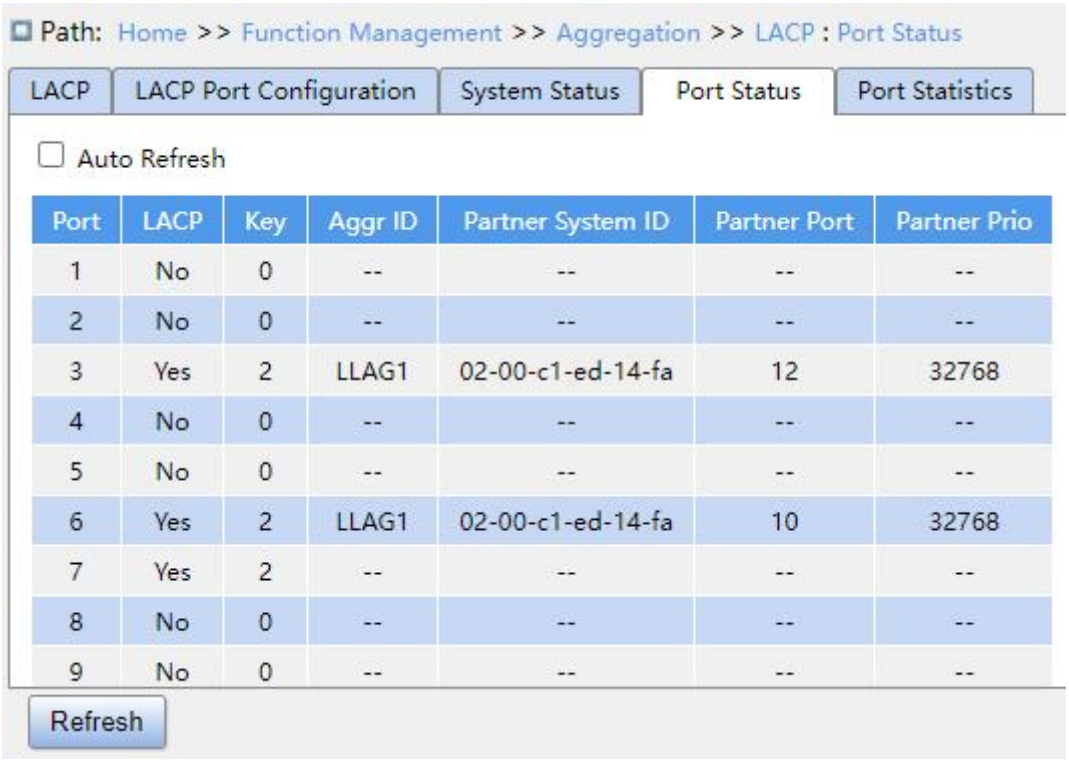
Last Changed

Function: Display the time elapsed since the last LACP switch.

Local Port

Function: Display the local port IDs enabled with LACP.

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	Yes	2	LLAG1	02-00-c1-ed-14-fa	12	32768
4	No	0	--	--	--	--
5	No	0	--	--	--	--
6	Yes	2	LLAG1	02-00-c1-ed-14-fa	10	32768
7	Yes	2	--	--	--	--
8	No	0	--	--	--	--
9	No	0	--	--	--	--

Figure 116 View LACP Port Status

LACP

Display options: Yes/No

Function: Display LACP status of port.

- Yes: LACP is enabled and port is Up.
- No: LACP is disabled or port is Down.

Key

Function: Display the Key value of the local ports.

Aggr ID

Function: Display the aggregation group ID.

Partner System ID

Function: Display the partner device ID, identified by the MAC address.

Partner Port

Function: Display the ID of the partner ports.

Partner Prio

Function: Display the priority of the partner ports.

5. View LACP port statistics, as shown below.

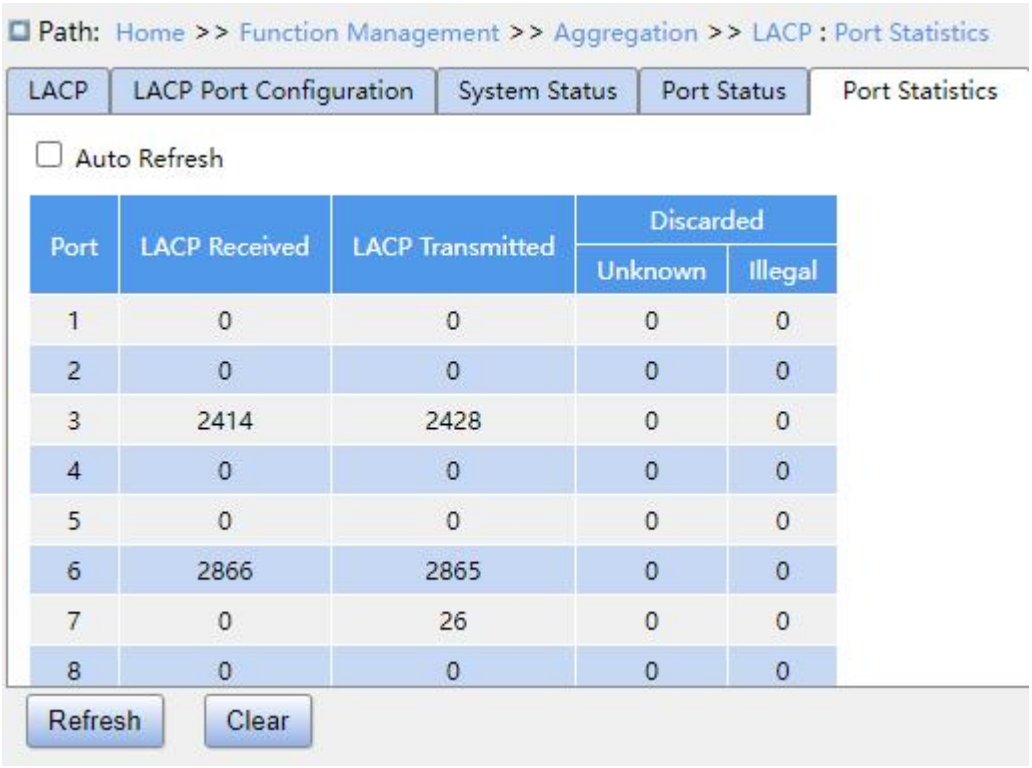


Figure 117 View LACP Port Statistics

Port

Function: Display the port ID.

LACP Received

Function: Display the number of LACP packets received by the port.

LACP Transmitted

Function: Display the number of LACP packets sent from the port.

Discarded Unknown/Illegal

Function: Display the number of unknown and illegal LACP packets discarded by the port.

7.5.2.4 Typical Configuration Example

As shown in Figure 111, use network cables to connect port 1, port 2 and port 3 of Switch A to port 1, port 2 and port 3 of Switch B to implement 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 114.
2. Enable LACP on port 1, 2, and 3 of switch B, as shown in Figure 114.

7.6 Redundancy

7.6.1 DT-Ring

7.6.1.1 Introduction

DT-Ring and DT-Ring+ are Kyland-proprietary redundancy protocols. They enable a network to recover within 50 ms 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.

7.6.1.2 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.

7.6.1.3 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 118.

- 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.
- 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.

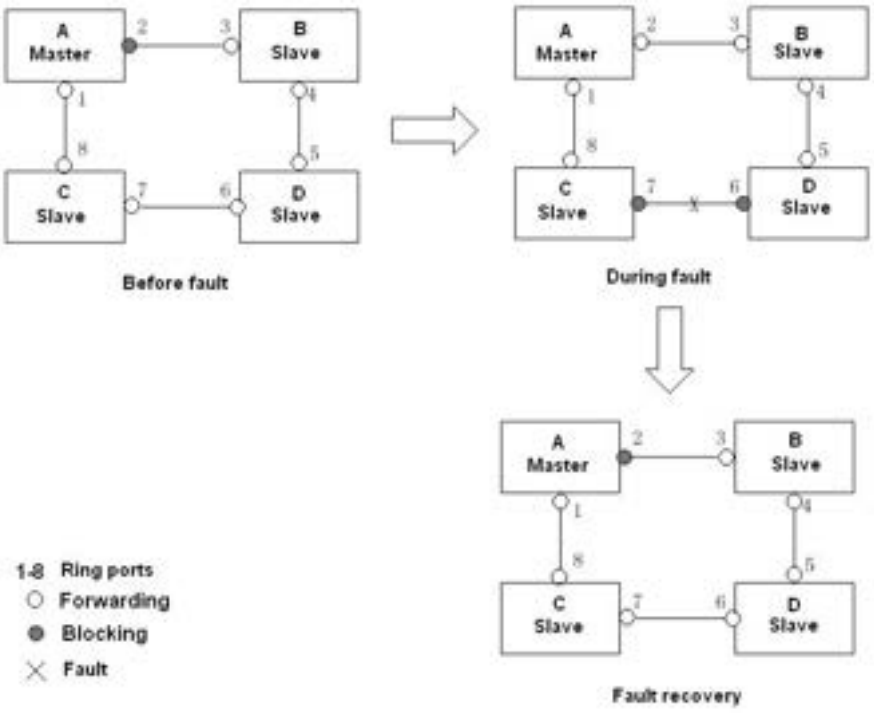


Figure 118 CD Link Fault

4. If link AC is faulty, as shown in Figure 119.

- When link AC is faulty, Port 1 is in blocking state and Port 2 changes to forwarding state, ensuring normal link communication.
- After the fault is rectified, Port 1 is still in blocking state and Port 8 is in forwarding state. No switchover occurs.

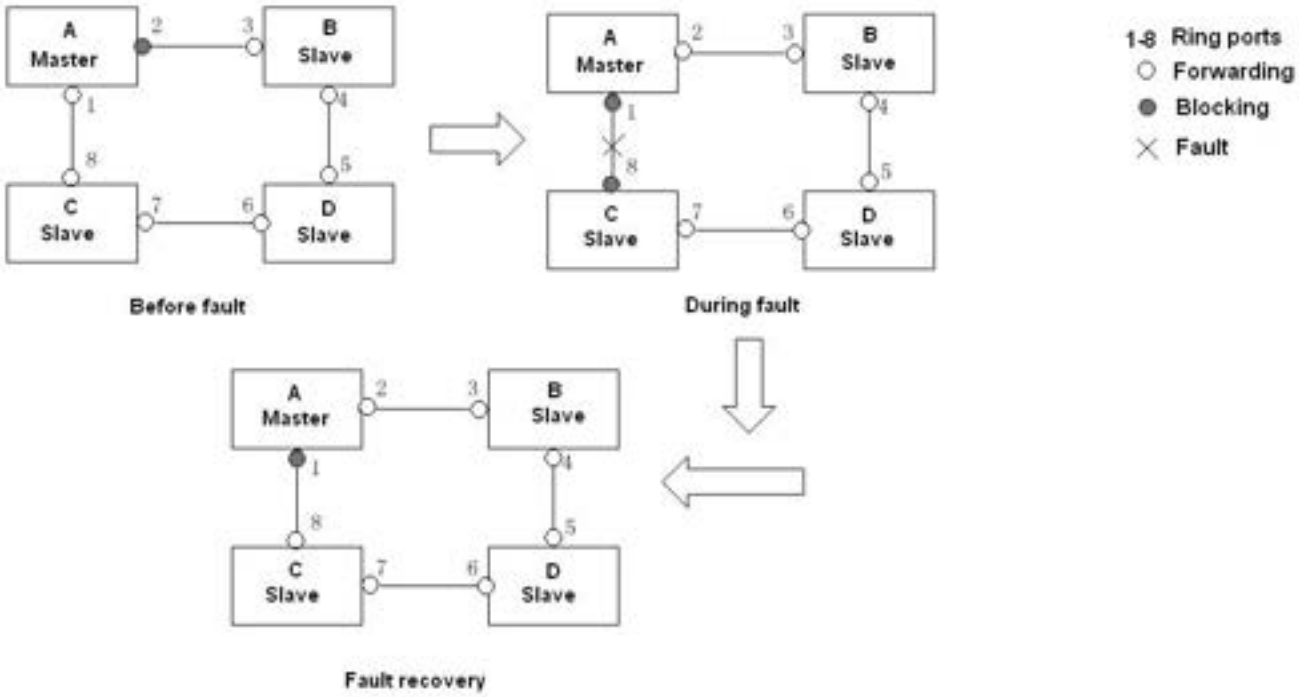


Figure 119 DT-Ring Link Fault

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 120, 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.

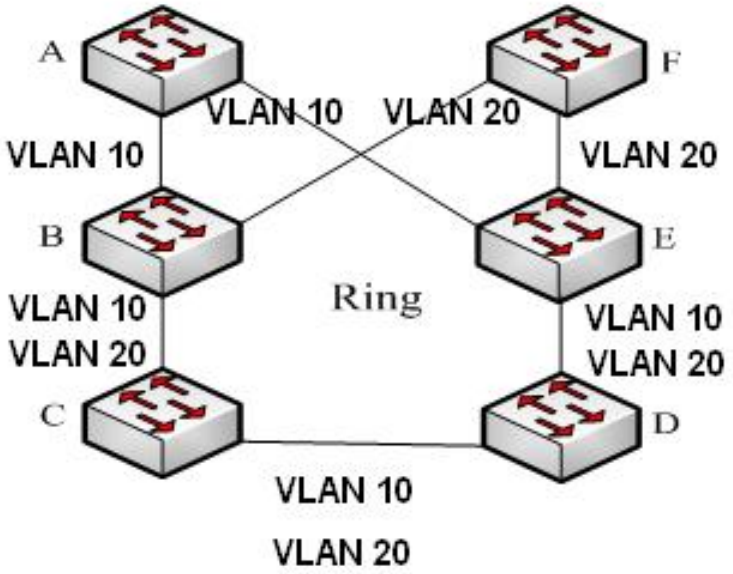


Figure 120 DT-Ring-VLAN

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 121. One backup port is configured respectively on Switch C and Switch D. Which port is the master's backup port depends on the MAC addresses of the two ports. If the master's backup port or its link fails, the slave's backup port will forward packets, preventing loops and ensuring normal communication between redundant rings.

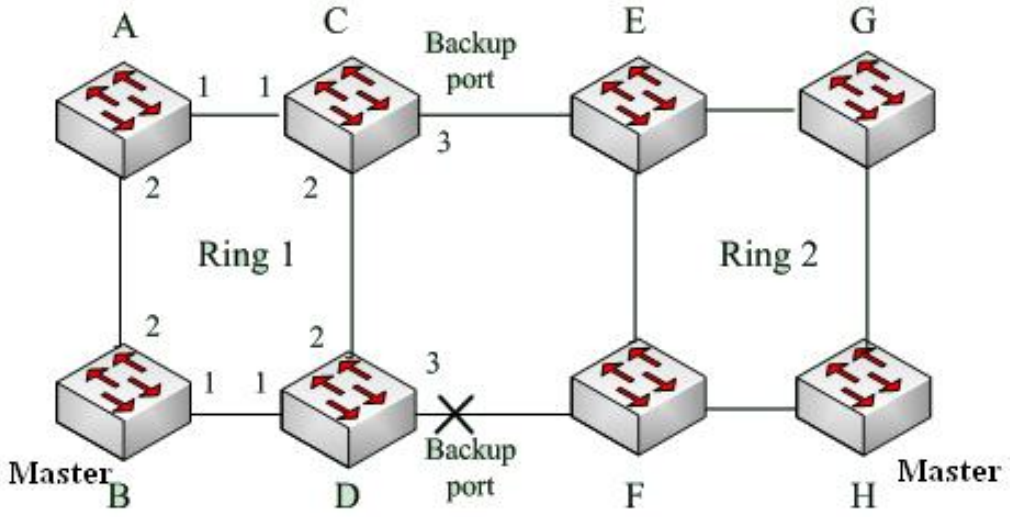


Figure 121 DT-Ring+ Topology

Caution:

Link status change affects the status of backup ports.

7.6.1.4 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.

7.6.1.5 Web Configuration

1. Configure DT-Ring redundant ring mode, as shown below.

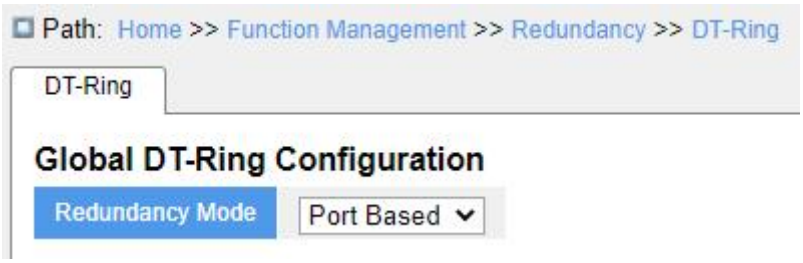


Figure 122 Redundant Ring Mode Configuration

Redundancy Mode

Configuration options: Port Based/VLAN Based

Default configuration: 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 one 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 below.

Figure 123 DT-Ring-Port Configuration

Figure 124 DT-Ring-VLAN Configuration

Domain ID

Configuration 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

Configuration range: 1~31 characters

Function: Configure the domain name.

Station Type

Configuration options: Master/Slave

Default configuration: Master

Function: Select the switch role in a ring.

Ring Port-1/Ring Port-2

Configuration options: All switch ports

Function: Select two ring ports.

Caution:

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

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable DT-Ring+.

Backup Port

Configuration options: All switch ports

Function: Set a port to backup port.

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

Caution:

Do not configure a ring port as a backup port.

VLAN ID

Configuration 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 125.

Figure 125 DT-Ring Configuration

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

4. Click a DT-Ring entry in Figure 125 to show DT-Ring and port status, as shown in Figure 126.

Figure 126 DT-Ring State

7.6.1.6 Typical Configuration Example

As shown in Figure 121, 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:

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 123.

Configuration on Switch B:

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 123;

Configuration on Switch C and Switch D:

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 123;

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

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 123;

Configuration on Switch H:

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 123;

7.6.2 DRP

7.6.2.1 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 20 ms, 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.

7.6.2.2 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 Status

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.

7.6.2.3 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:

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.

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 127:

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.

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.

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.

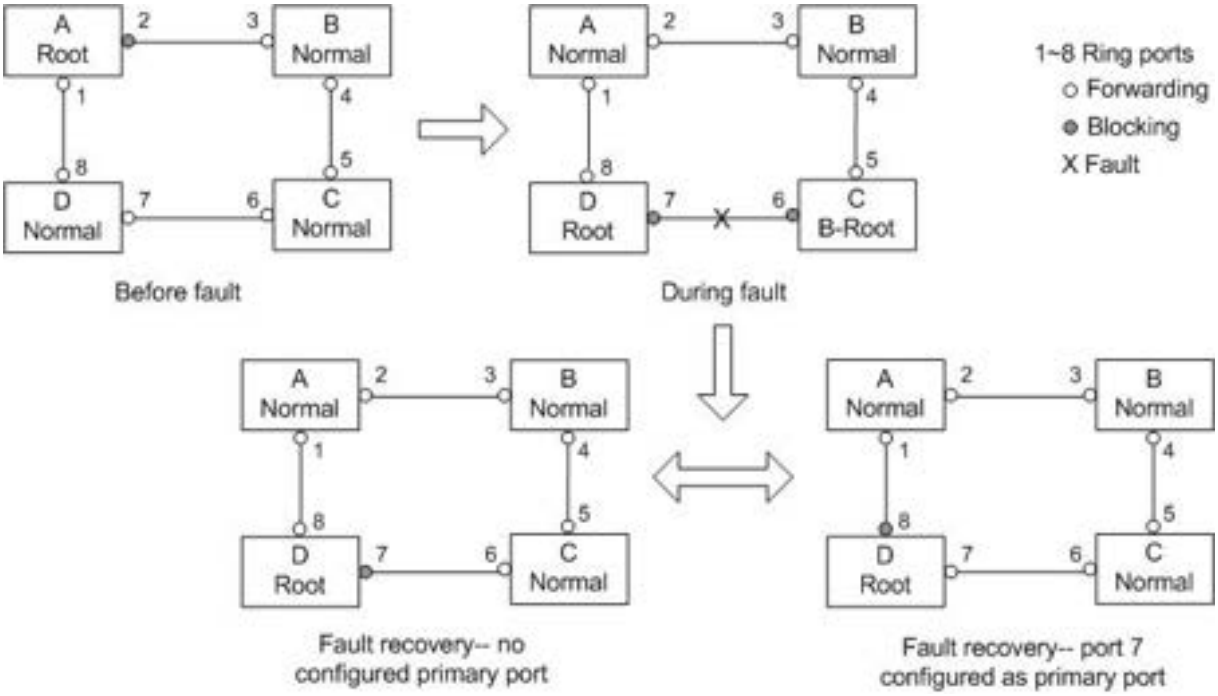


Figure 127 DRP Link Fault

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

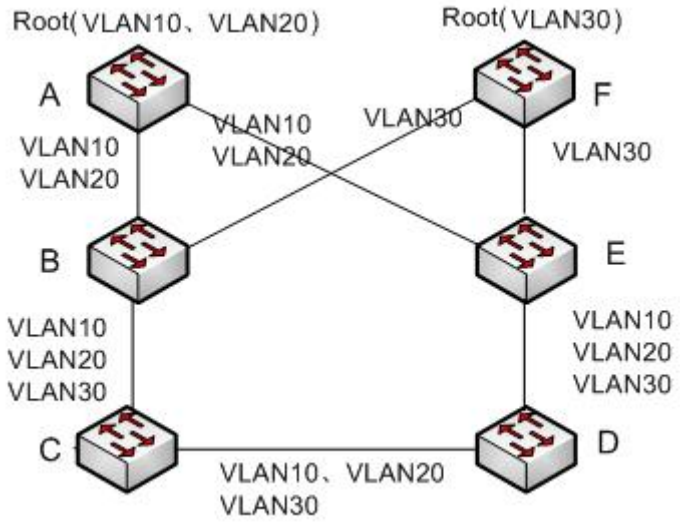


Figure 128 DRP-VLAN-Based

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's backup port, which is in forwarding state. All the other backup ports are slave. They are in blocking state.

As shown in Figure 129, one backup port can be configured on each switch. The master's backup port is in forwarding state and the other backup ports are in blocking state. If the master's backup port or its link is faulty, a slave's backup port will be selected to forward data.

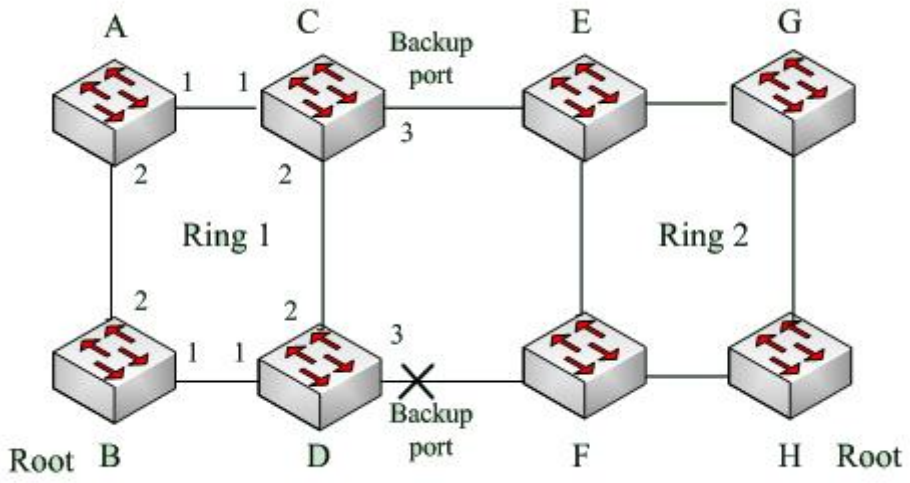


Figure 129 DRP Backup

Caution:

Link status change affects the status of backup ports.

7.6.3 DHP

7.6.3.1 Overview

As shown in Figure 130, 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.

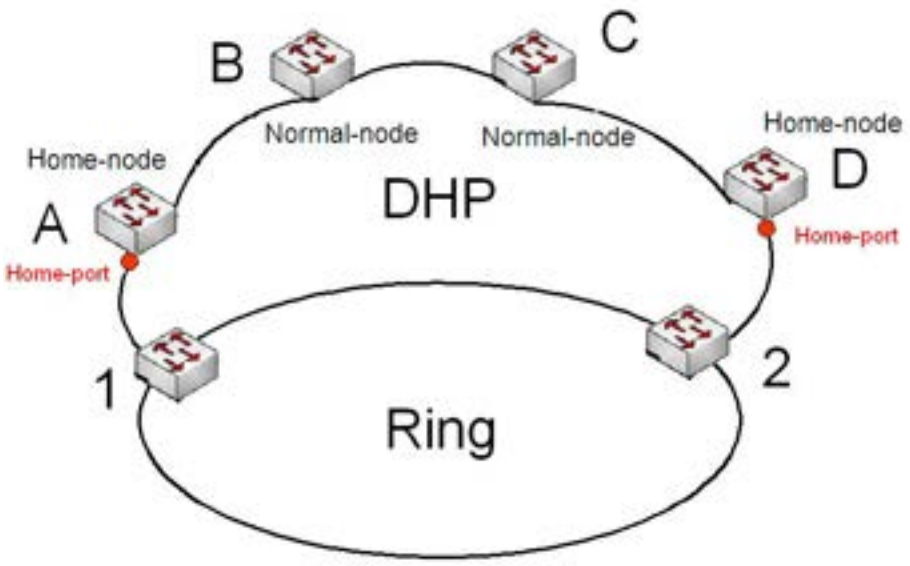


Figure 130 DHP Application

7.6.3.2 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.

7.6.3.3 Implementation

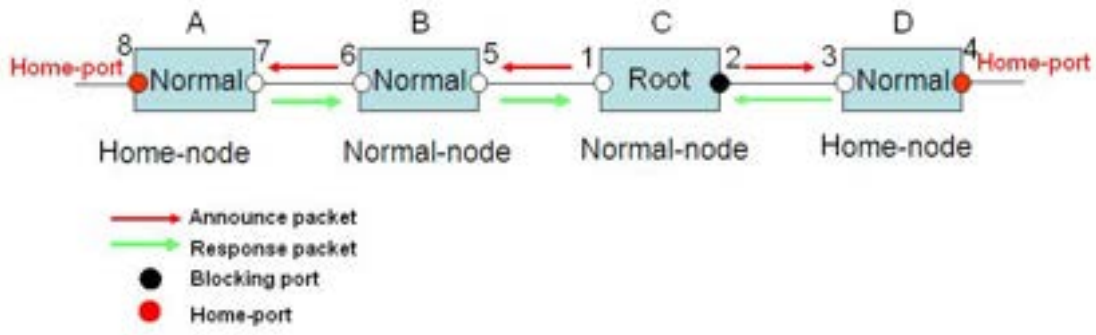


Figure 131 DHP Configuration

The configurations of A, B, C, and D are shown in Figure 131:

- DRP configuration: C is the Root; port 2 is in blocking state; A, B, and D are Normal; all 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.

DHP Implementation:

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.

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 132.

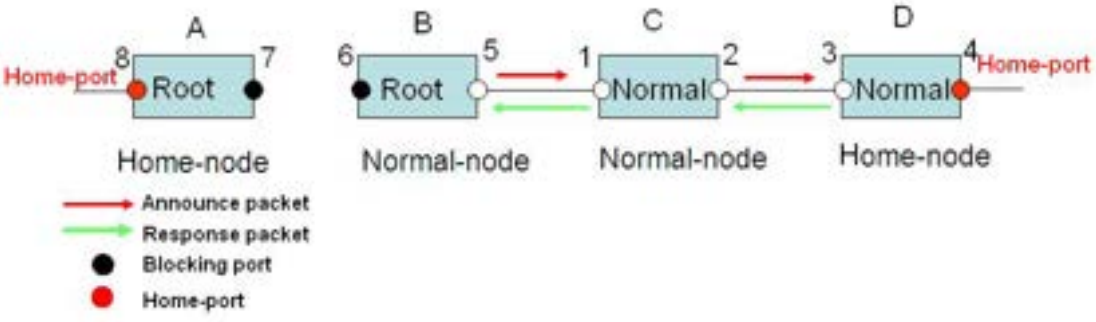


Figure 132 DHP Fault Recovery

7.6.3.4 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.

7.6.3.5 Web Configuration

1. Configure the DRP redundancy mode, as shown in Figure 133.

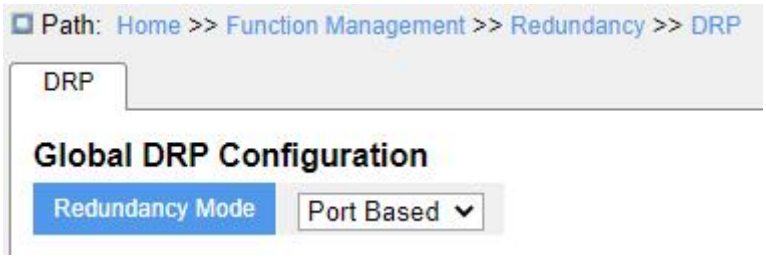


Figure 133 Configure the DRP Redundancy Mode

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 134 and Figure

135.

Figure 134 DRP-Port-Based Configuration

Figure 135 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, 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:

Do not configure a ring port as a backup port.

VLAN List

Configuration options: All created VLANs

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

Protocol VLAN ID

Configuration range: 1~4093

Function: Configure the protocol VLAN ID.

Description: The VLAN ID must be one of the service VLANs. User can use DRP packets with the VLAN ID as the basis for the diagnosis and maintenance of the DRP-VLAN-Based ring.

Protocol Enable

Configuration options: Enable/Disable

Function: Whether to enable the DRP protocol for the specified domain

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

Figure 136 View and Modify DRP Configuration

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

4. Configure Out-Home-Port, as shown below.

Figure 137 Configure Out-Home-Port

Port

Configuration range: 1~28

Function: After configuring the out-home-port, the ring network formed by the downstream link and the main ring will enter the ring-close state to keep normal communications between all devices.

5. Click **Details** in the DRP entry in Figure 136 to show the roles and port status of the switches in the DRP ring, as shown in Figure 138.

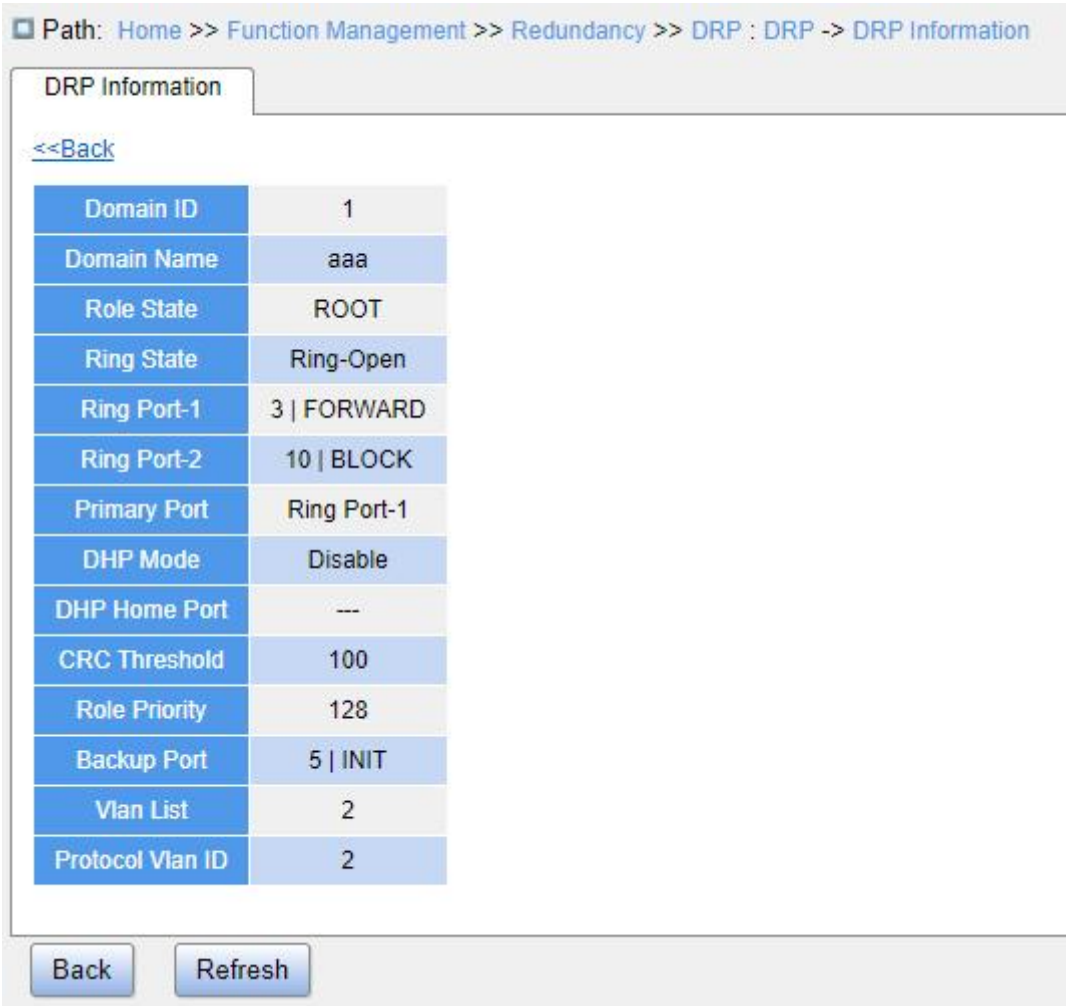


Figure 138 DRP State

7.6.3.6 Typical Configuration Example

As shown in Figure 129, A, B, C and D form Ring 1; E, F, G and H form Ring 2; C-E and D-F are the backup links of Ring 1 and Ring 2.

Configuration on switch A and switch B:

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 134.

Configuration on switch C and switch D:

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 134.

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

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 134.

7.6.4 RSTP/STP Configuration

7.6.4.1 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.

7.6.4.2 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 the 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.

7.6.4.3 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).

7.6.4.4 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.

7.6.4.5 Web Configuration

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

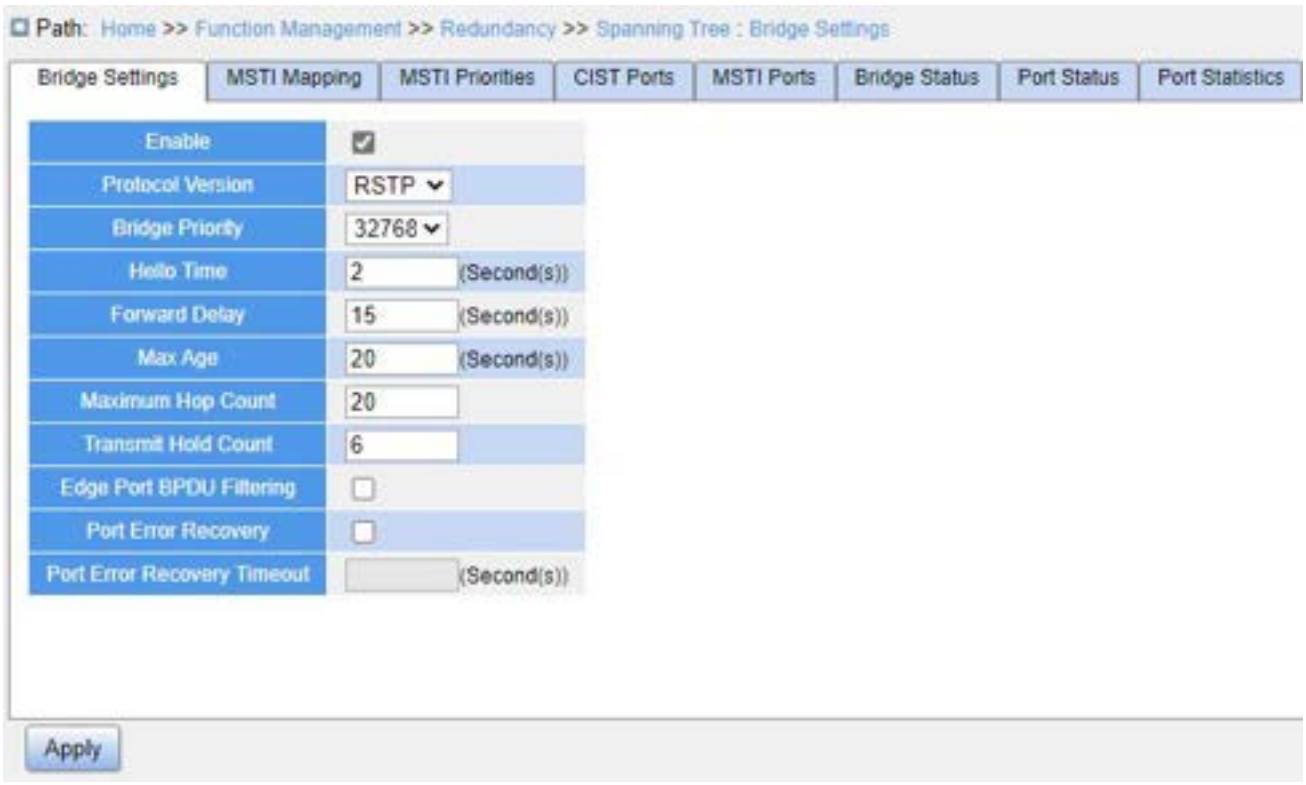


Figure 139 Setting Parameters of the Network Bridge

Enable

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to 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 Version

Configuration options: MSTP/RSTP/STP

Default configuration: MSTP

Function: Select the spanning tree protocol.

Bridge 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 BPDUs.

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: Configure the 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 RSTP port, as shown below.

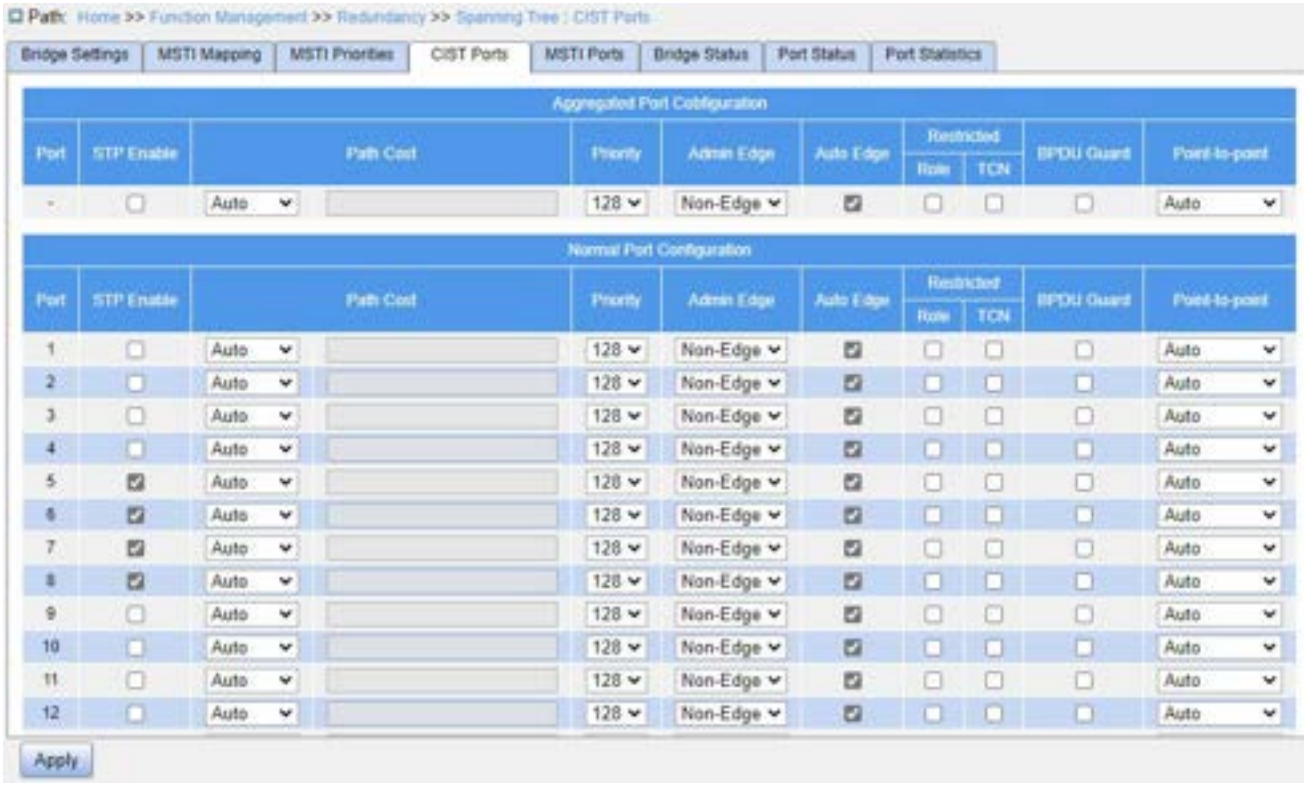


Figure 140 Configure RSTP Port

STP Enable

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable 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.

- 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. ;
- Force True: Indicates that a link connected to a port is a point-to-point link.

- Force False: Indicates that a link connected to a port is a shared link.

7.6.4.6 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 141.

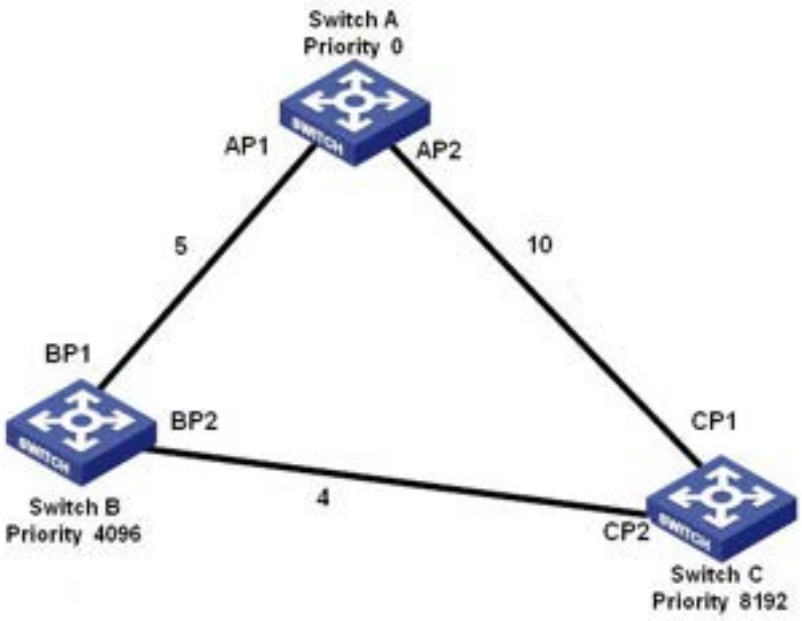


Figure 141 RSTP Configuration Example

Configuration on Switch A:

1. Set bridge priority to 0 and time parameters to default values, as shown in Figure 139.

2. Set the path cost of port 1 to 5 and that of port 2 to 10, as shown in Figure 140.

Configuration on Switch B:

1. Set bridge priority to 4096 and time parameters to default values, as shown in Figure 139**.**

2. Set the path cost of port 1 to 5 and that of port 2 to 4, as shown in Figure 140.

Configuration on Switch C:

1. Set bridge priority to 8192 and time parameters to default values, as shown in Figure 139.

2. Set the path cost of port 1 to 10 and that of port 2 to 4, as shown in Figure 140.

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.

7.6.5 MSTP Configuration

7.6.5.1 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 142, 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.

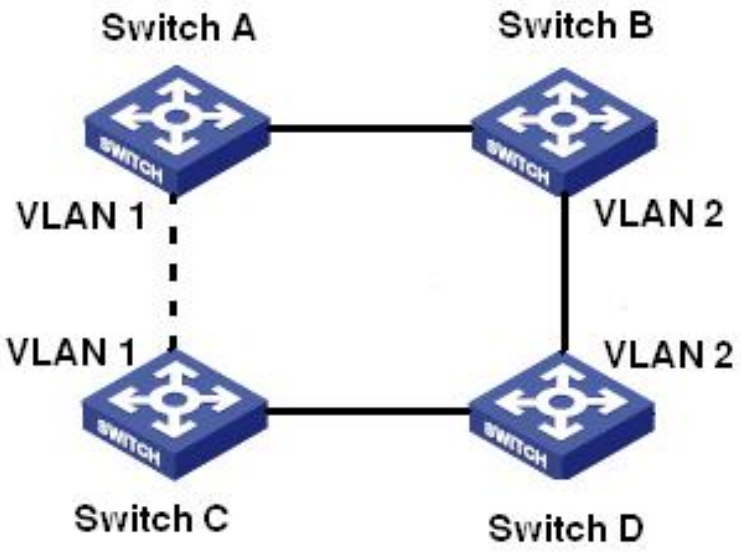


Figure 142 RSTP Disadvantage

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 142 forms the topology shown in Figure 143 . 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.

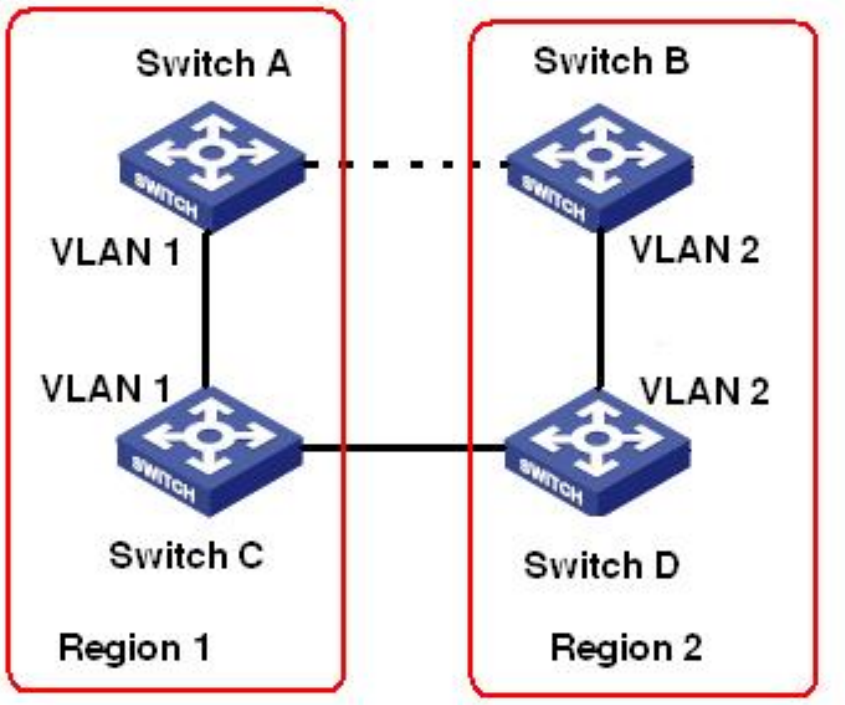


Figure 143 MSTP Topology

7.6.5.2 Basic Concepts

Learn MSTP concepts based on Figure 144 and Figure 147.

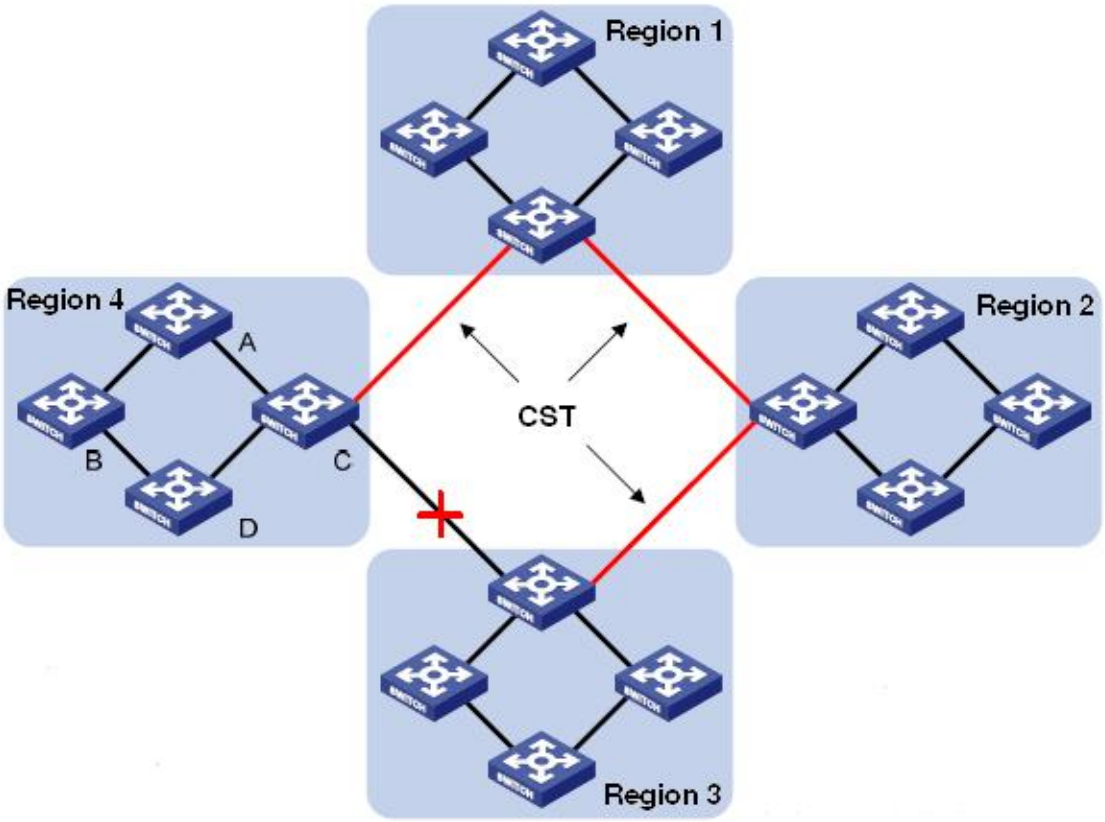


Figure 144 MSTP Concepts

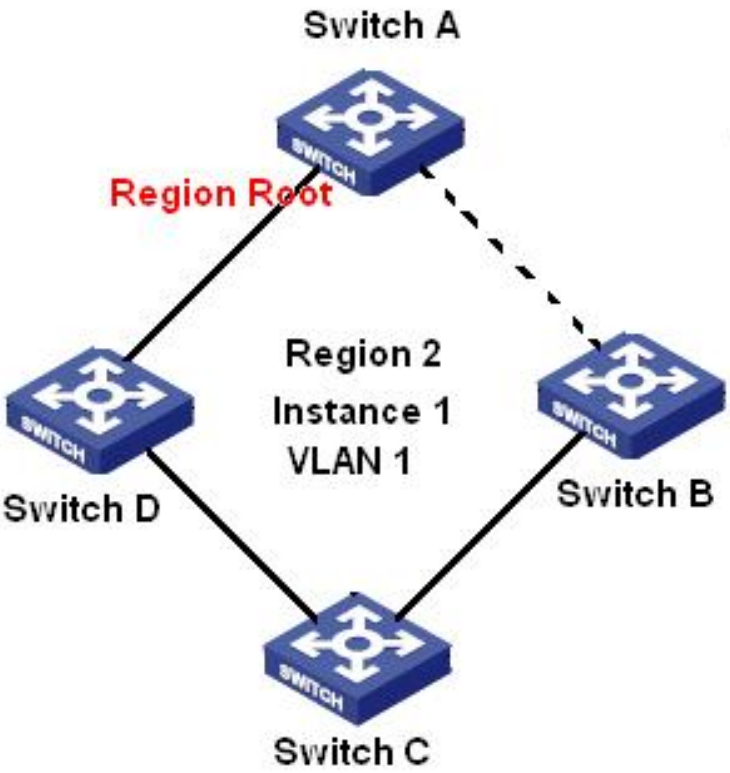


Figure 145 VLAN 1 Mapping to Instance 1

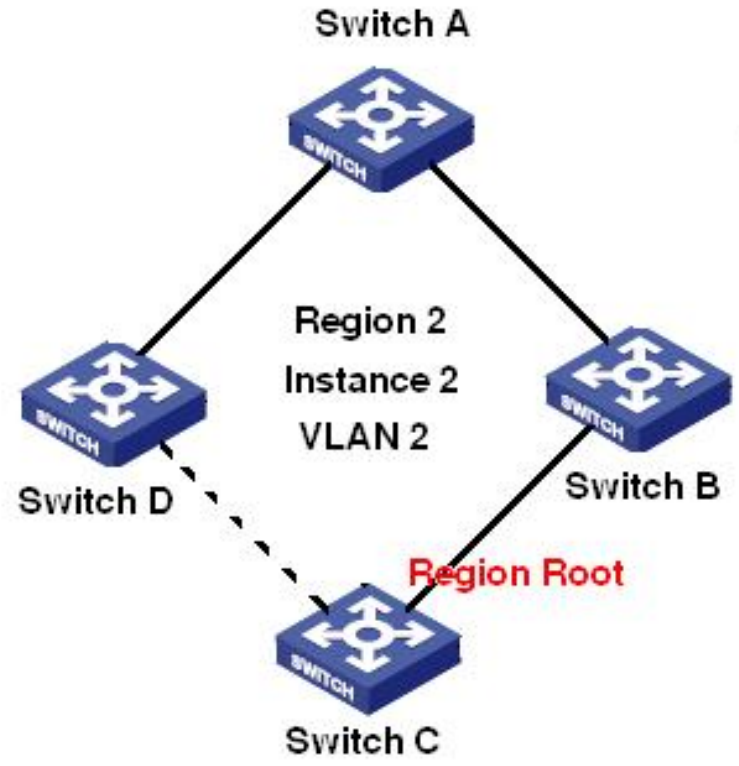


Figure 146 VLAN2 Mapping to Instance 2

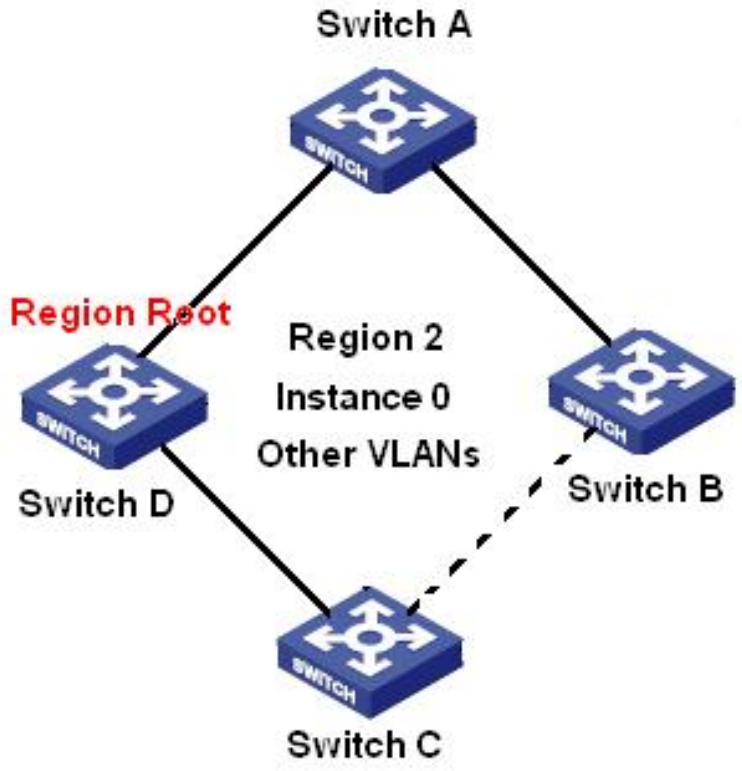


Figure 147 Other VLAN Mapping to Instance 0

Instance: A collection of multiple VLANs. One VLAN (as shown in Figure 145 and Figure

146) or multiple VLANs with the same topology (as shown in Figure 147) 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 144 , Region1, Region2, Region3, and Region4 are four different MST regions.

VLAN mapping table: Consists of the mapping between VLANs and spanning trees. In Figure 144 , VLAN mapping table of region 2 is the mapping between VLAN 1 and instance 1, as shown in Figure 145; VLAN 2 is mapped to instance 2, as shown in Figure 146. The other VLANs are mapped to instance 0, as shown in Figure 147.

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 144 , 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 147.

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 144, 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 145 and Figure 146. 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 145, Figure 146, and Figure 147, 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.

7.6.5.3 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.

7.6.5.4 Web Configuration

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

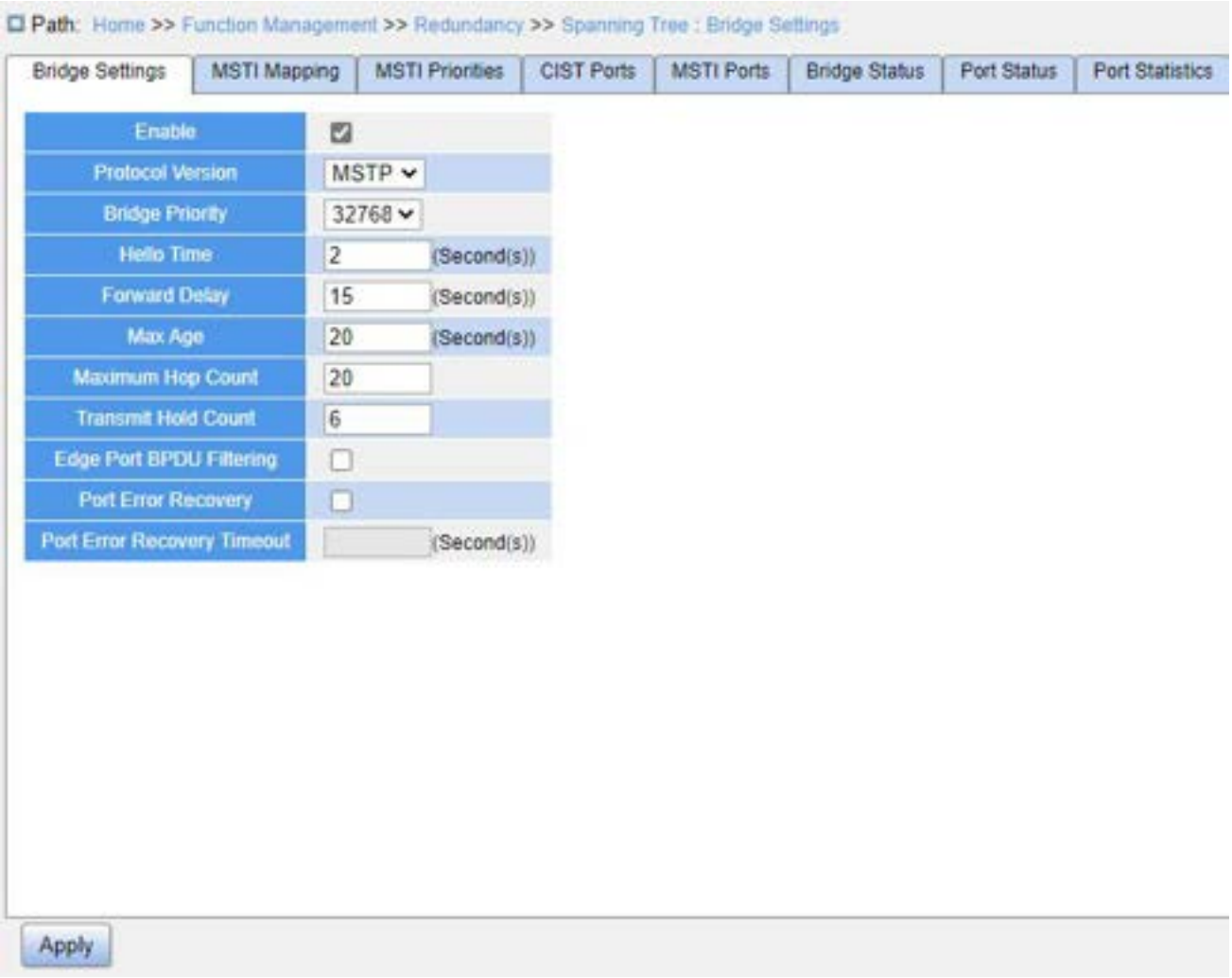


Figure 148 Setting Parameters of the Network Bridge

Enable

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable spanning tree.

Caution:

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

Protocol Version

Configuration options: MSTP/RSTP/STP

Default configuration: MSTP

Function: Select the spanning tree protocol.

Bridge 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 BPDUs.

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.

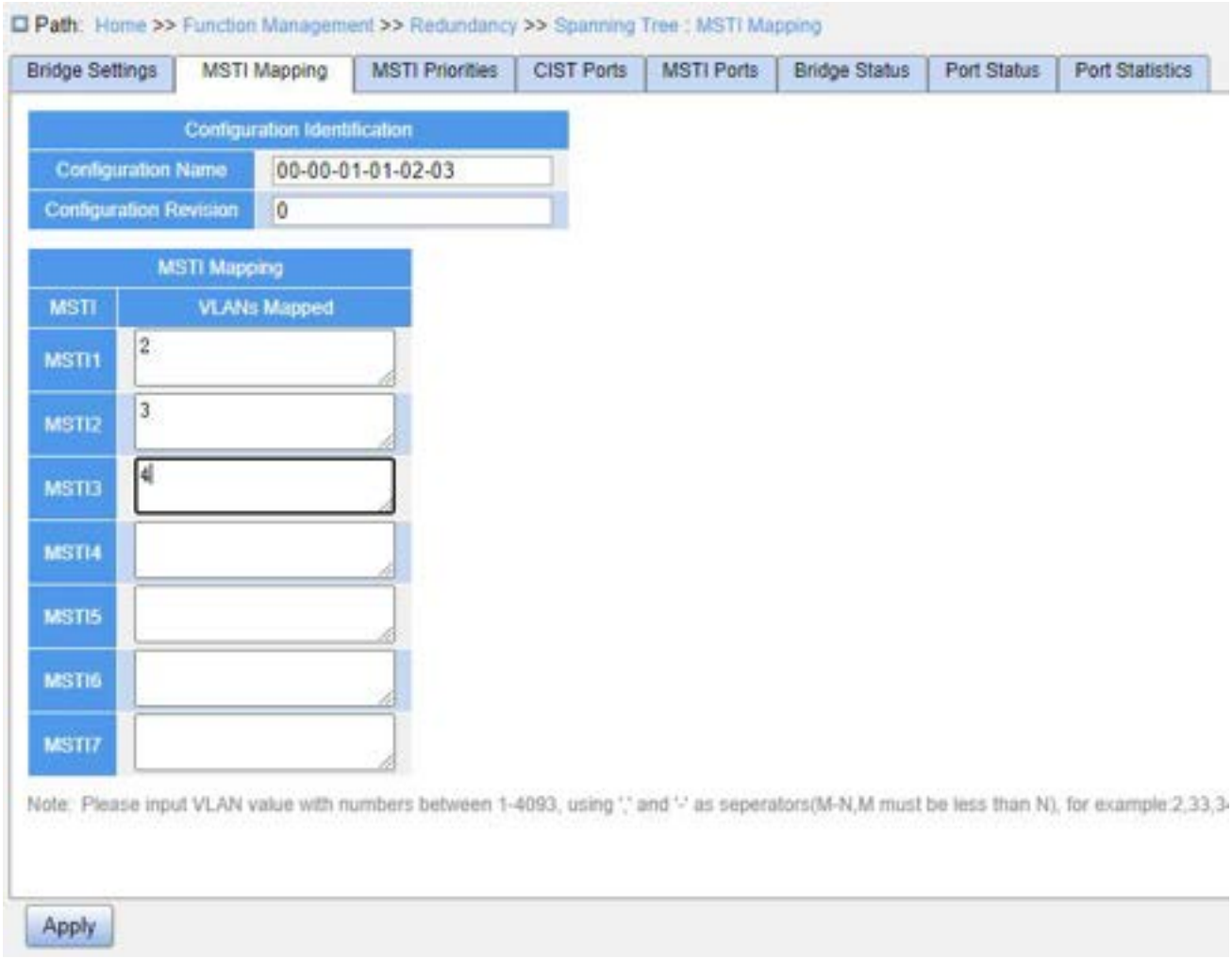


Figure 149 Configure MSTI Mapping

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 codetermine the MST region that the device belongs to. When all configurations are the same, the devices are in the same MST region.

VLANs Mapped

Configuration range: 1~4093

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 150 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.

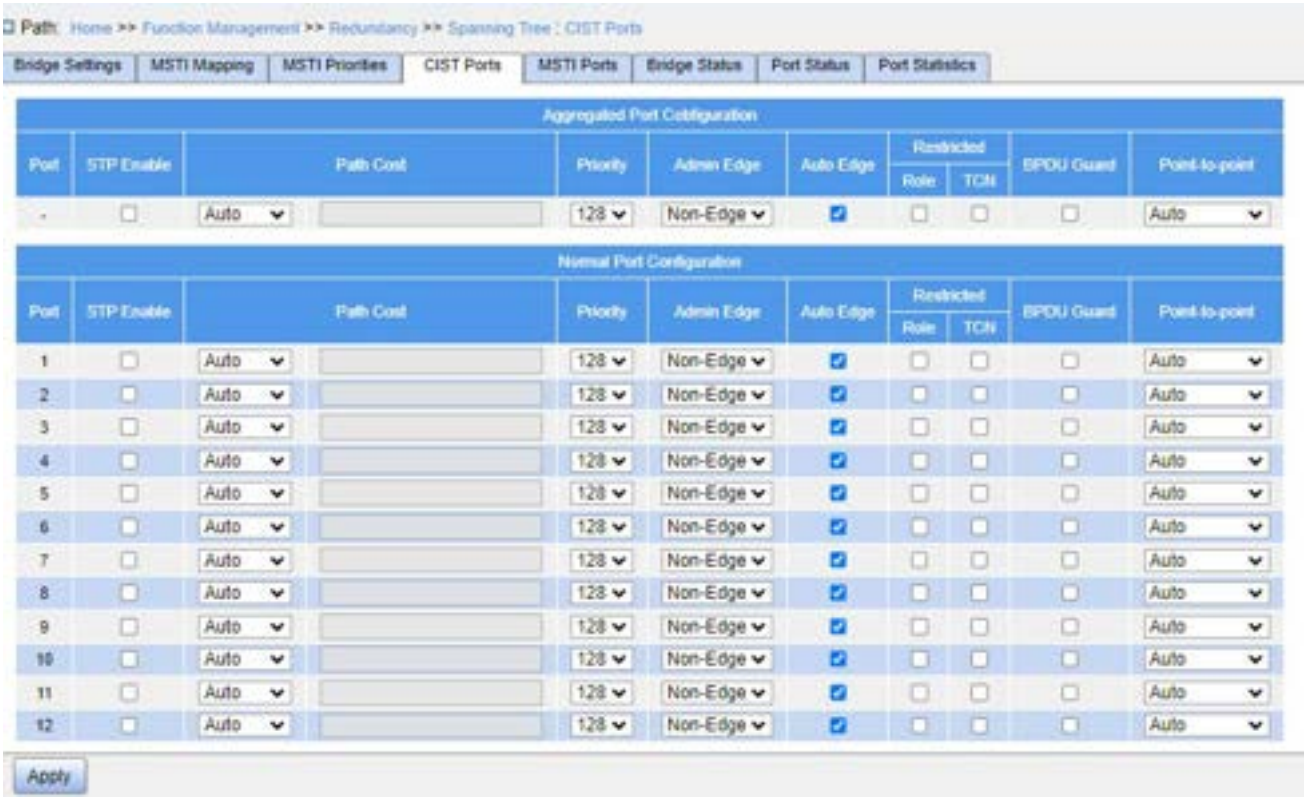


Figure 151 Configure CIST Ports

STP Enable

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable spanning tree protocol 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/Force True/Force 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.

- 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.
- Force True: Indicates that a link connected to a port is a point-to-point link,
- Force False: Indicates that a link connected to a port is a shared link.

5. Configure MSTI ports, as shown below.

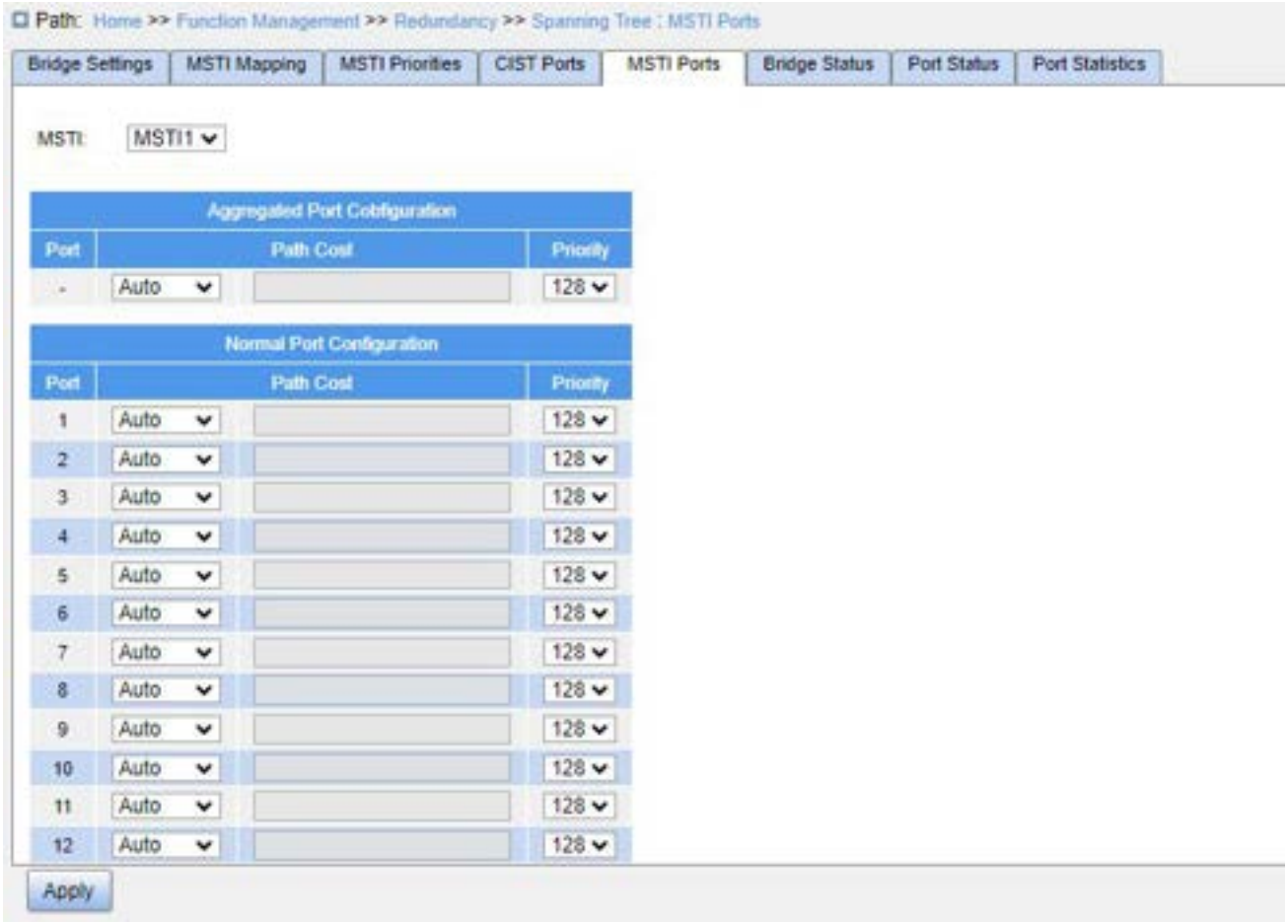


Figure 152 Select MSTI

MSTI

Configuration range: MST1~MST7

Default configuration: MST1

Function: Select a MSTI.

MSTI Aggregated Port Configuration

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.

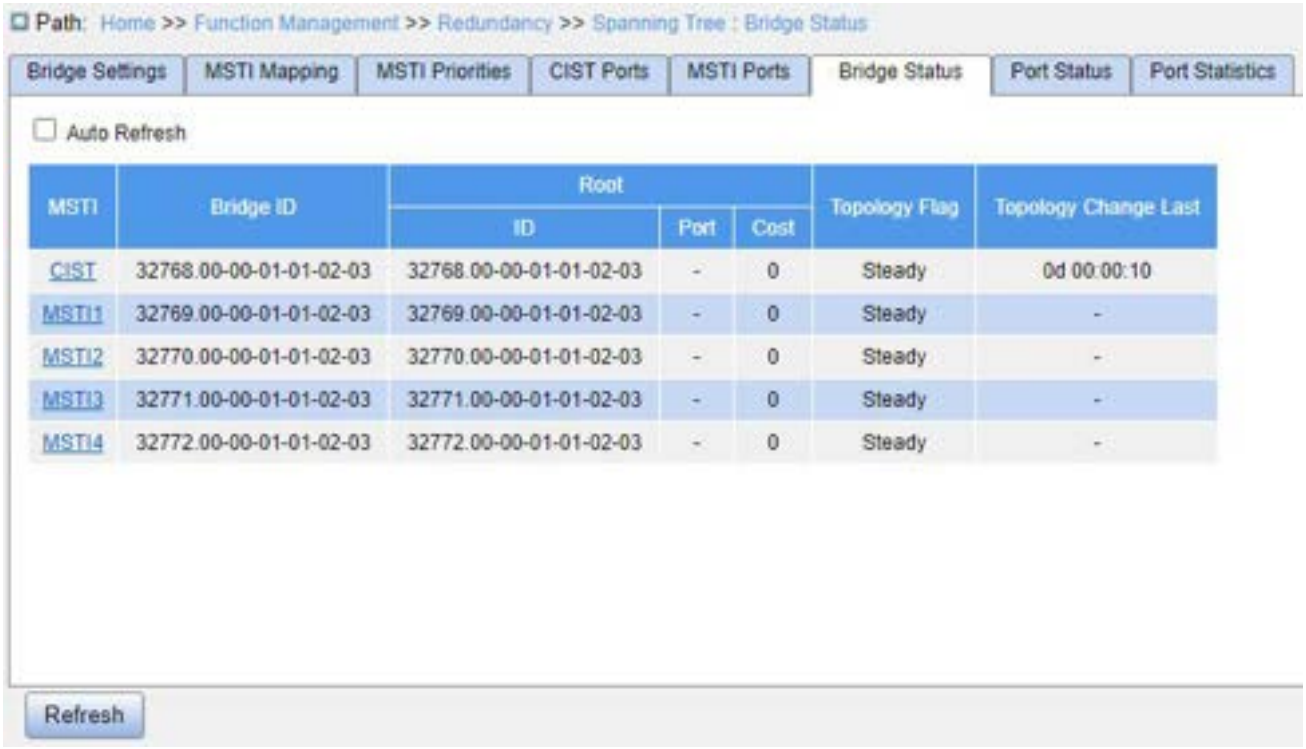


Figure 153 View Bridge Status

MSTI

Function: Indicates the spanning tree instance.

- CIST: Indicates the default CIST instance when STP/RSTP is used.
- MSTI: Indicates the instance of each spanning tree when MSTP is used.

Bridge ID

Function: Indicates the bridge ID of the current spanning tree, composed of the bridge priority valu and MAC address.

Root

Function: Indicates the root bridge information of the current spanning tree.

- ID: Indicates the root bridge ID.
- Port: Indicates the root port ID.
- Cost: indicates the path cost from the root port to the root bridge.

Topology Flag

Function: Indicates the running status of the current spanning tree instance.

Topology Change Last

Function: Indicates the time elapsed since the last topology change.

7. View STP ports status, as shown below.

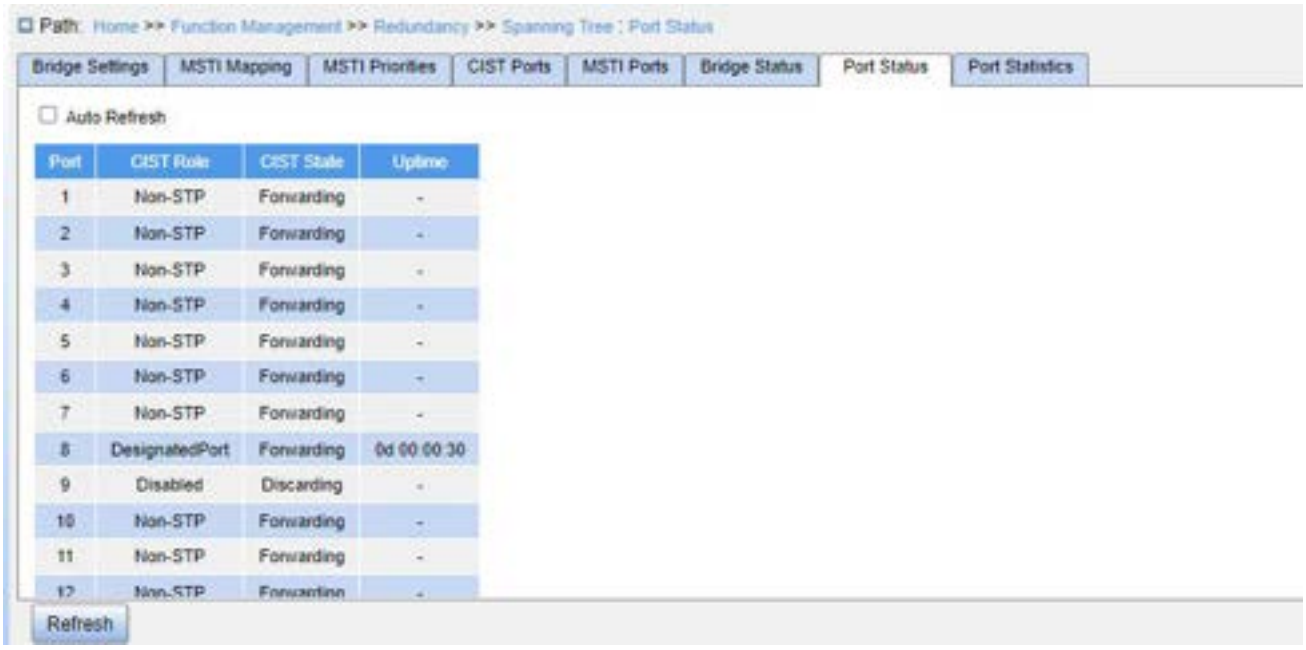


Figure 154 View STP Ports Status

Port

Function: Indicates the port ID.

CIST Role

Function: Indicates the role of the port in the CIST.

CIST State

Function: Indicates the state of the port in the CIST.

Uptime

Function: Indicates the time elapsed since the port starts to run STP in the CIST.

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

Figure 155 View STP Ports Packets Statistics

Transmitted

Function: Display the number of MST/RSTP/STP/TCN packets received by and sent from the port.

Discarded

Function: Display the number unknown and illegal STP packets discarded by the port.

7.6.5.5 Typical Configuration Example

As shown in Figure 156, 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.

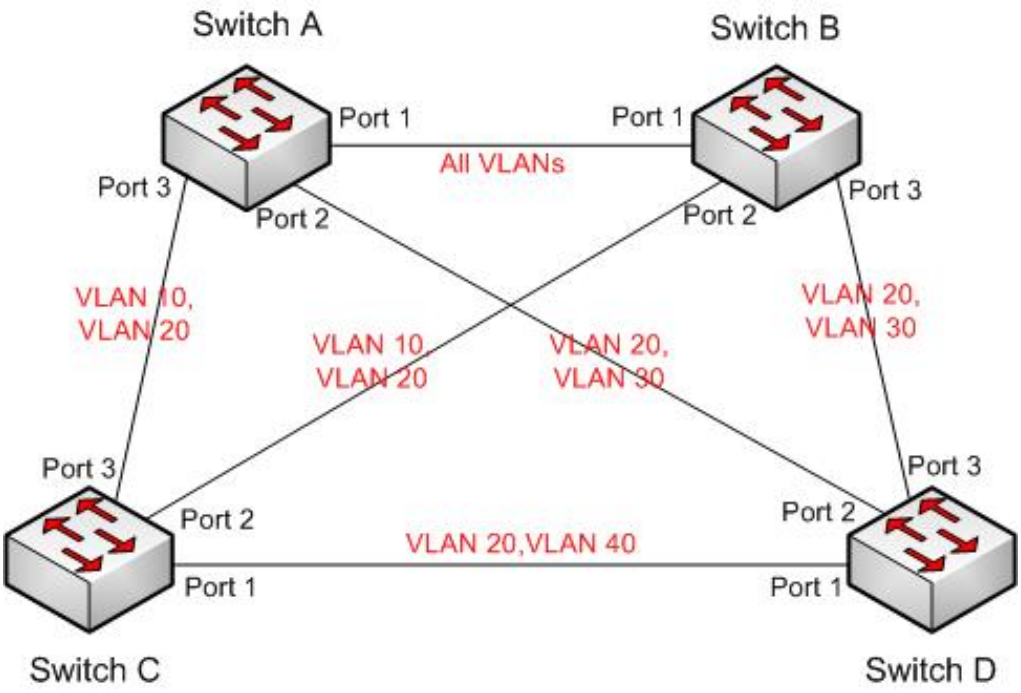


Figure 156 MSTP Typical Configuration Example

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 148.

3. Set the name of MST region to “Region” and the revision parameter to 0, as shown in Figure 152.

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 152.

5. Set the switch bridge priority in MSTI 1 to 4096, and keep default priority in other instances, as shown in Figure 150.

Configuration on Switch B:

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

2. Enable global MSTP protocol, as shown in Figure 148.

3. Set the name of MST region to “Region” and the revision parameter to 0, as shown in Figure 152.

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 152.

5. Set switch bridge priority in MSTI 3 and MSTI 0 to 4096, and keep default priority in other instances, as shown in Figure 150.

Configuration on Switch C:

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

2. Enable global MSTP protocol, as shown in Figure 148.

3. Set the name of MST region to “Region” and the revision parameter to 0, as shown in Figure 152.

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 152.

5. Set switch bridge priority in MSTI 4 to 4096, and keep default priority in other instances, as shown in Figure 150.

Configuration on Switch D:

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

2. Enable global MSTP protocol, as shown in Figure 148.

3. Set the name of MST region to “Region” and the revision parameter to 0, as shown in Figure 152.

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 152.

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

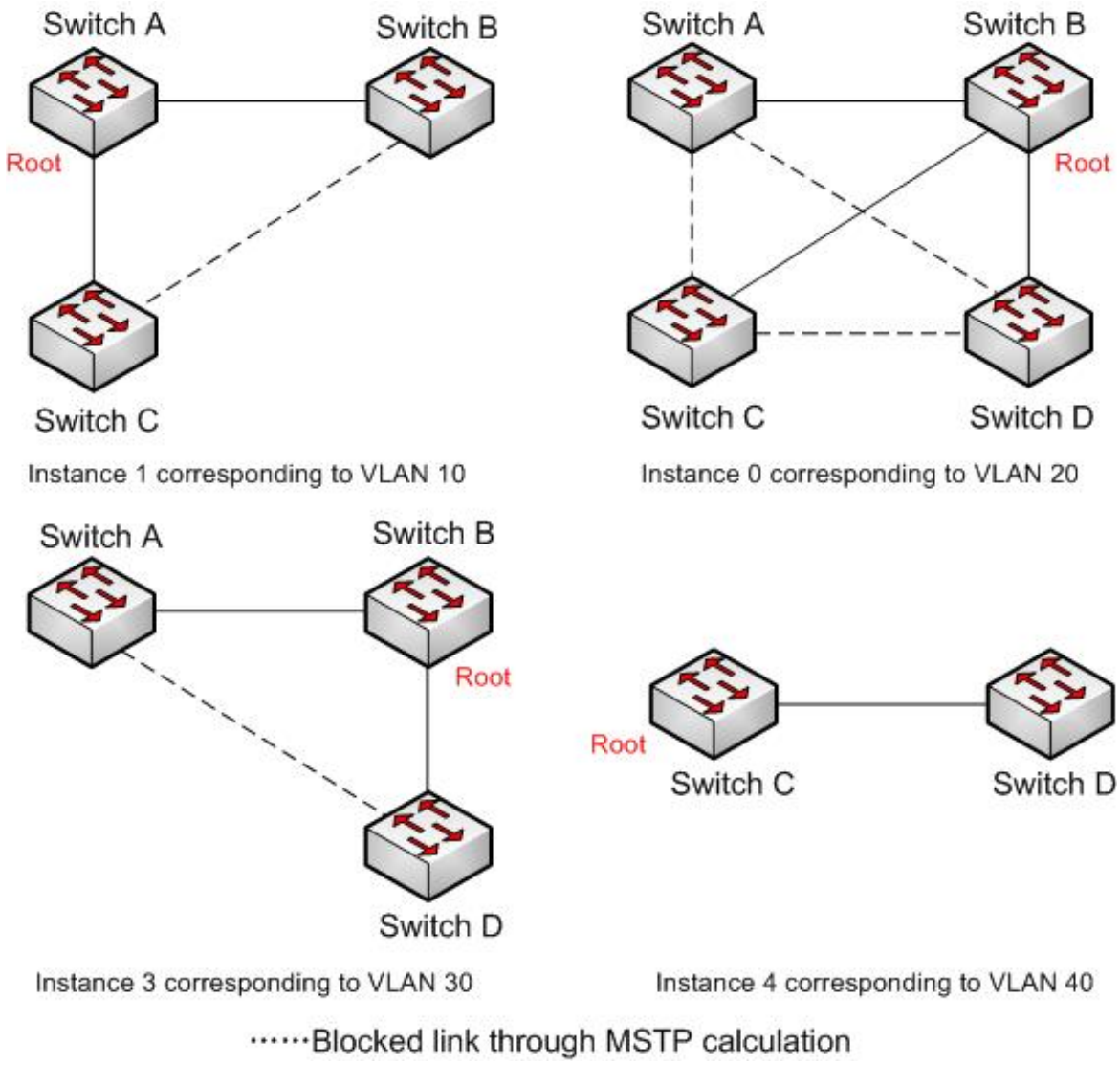


Figure 157 Spanning Tree Instance of Each VLAN

7.7 ARP Configuration

7.7.1 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.

7.7.2 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.

7.7.3 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 an 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 reply MAC address of its own interface.

3. The IP messages 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.

7.7.4 Web Configuration

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

Figure 158 Configure Static ARP Table Items

VLAN ID

Configuration range: Created Layer 3 VLAN interface, range 1~4093

Function: Select the Layer 3 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. Administrators do not need to configure static ARP entries.

2. Proxy ARP configuration, as shown below.

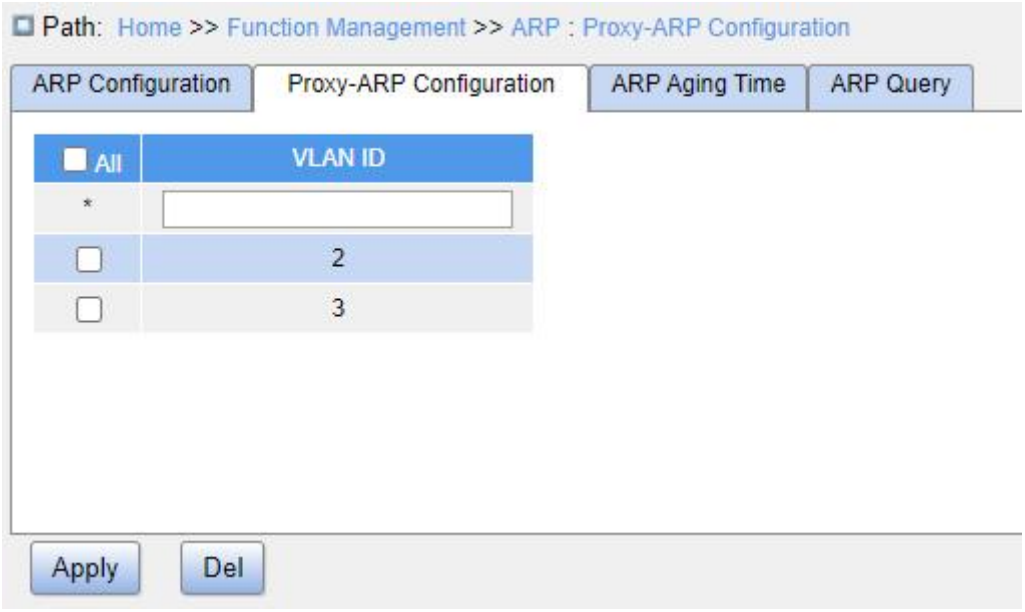


Figure 159 Proxy ARP Configuration

VLAN ID

Configuration range: 1~4093

Function: Select Layer 3 interface for which proxy ARP will be enabled.

3. ARP aging time configuration, as shown below.

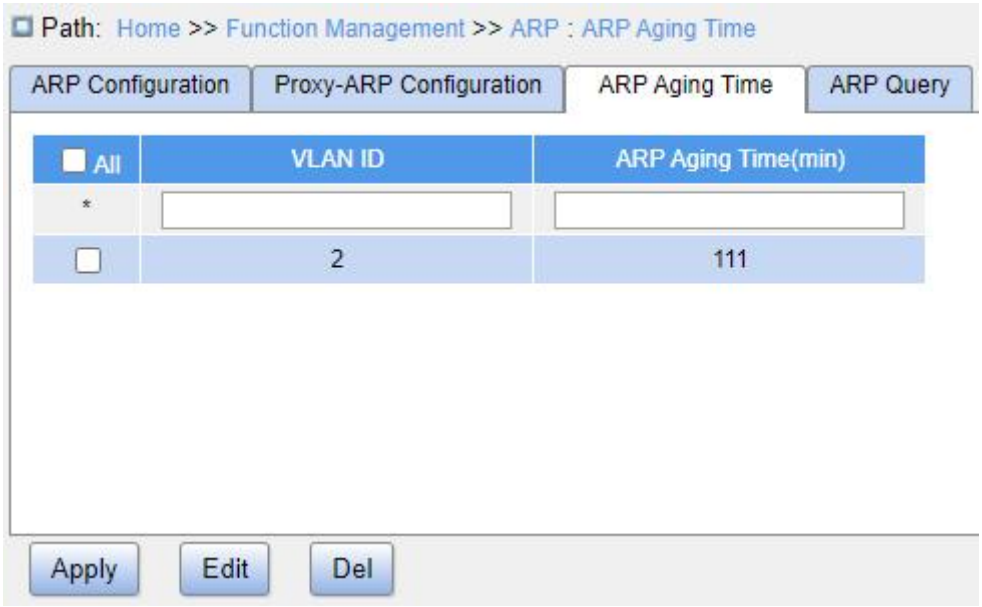


Figure 160 ARP Aging Time Configuration

VLAN ID

Configuration range: 1~4093

Function: Specify the Layer 3 interface for which ARP aging will be configured.

ARP Aging Time

Configuration range: 1~10000 min

Function: Configure ARP aging time

Description: The ARP aging timer starts when a dynamic ARP entry is added to the ARP table, and the entry is deleted when the timer elapses.

4. Query ARP entries, as shown below.

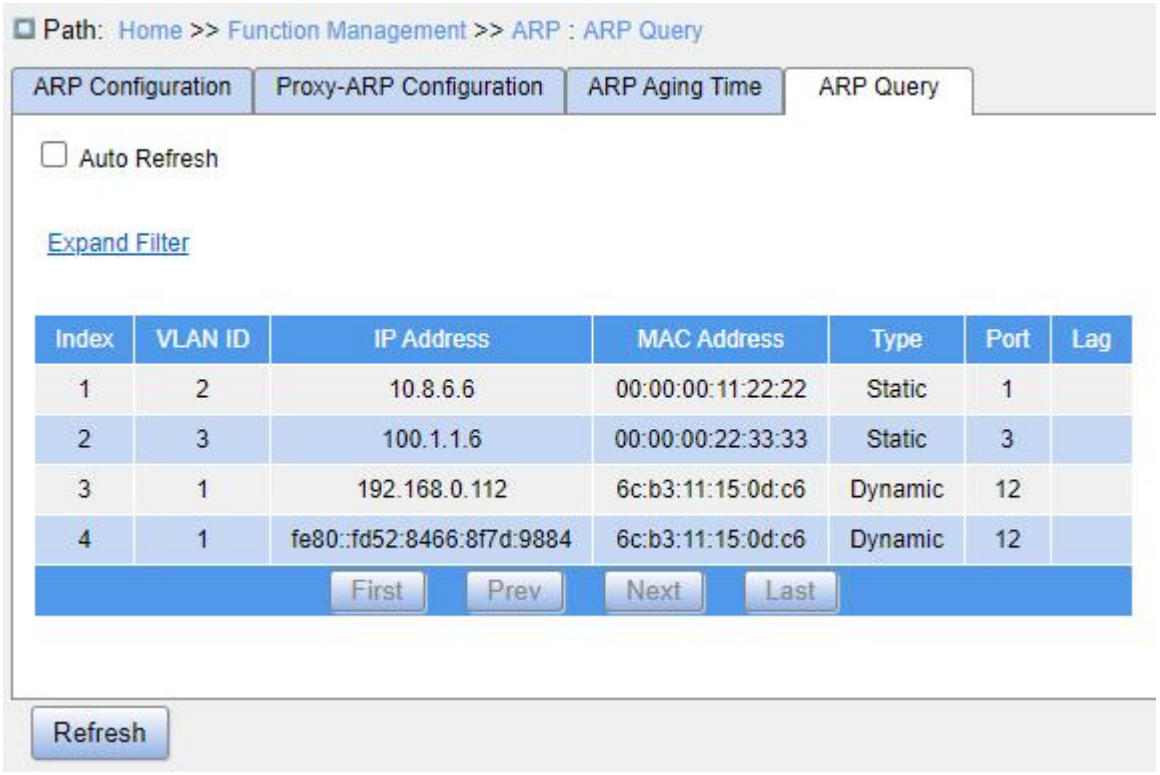


Figure 161 ARP Query

ARP Query

Display item: {Index, VLAN ID, IP Address, MAC Address, Type, Status}

Function: Display ARP table items.

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

7.8 ACL Configuration

7.8.1 Overview

With the development of network technologies, security issues have become increasingly prominent, calling for access control mechanism. With the Access Control List

(ACL) function, the switch matches packets with the list to implement access control.

7.8.2 Implementation

The series switches filter packets according to the matched ACL entry. 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.

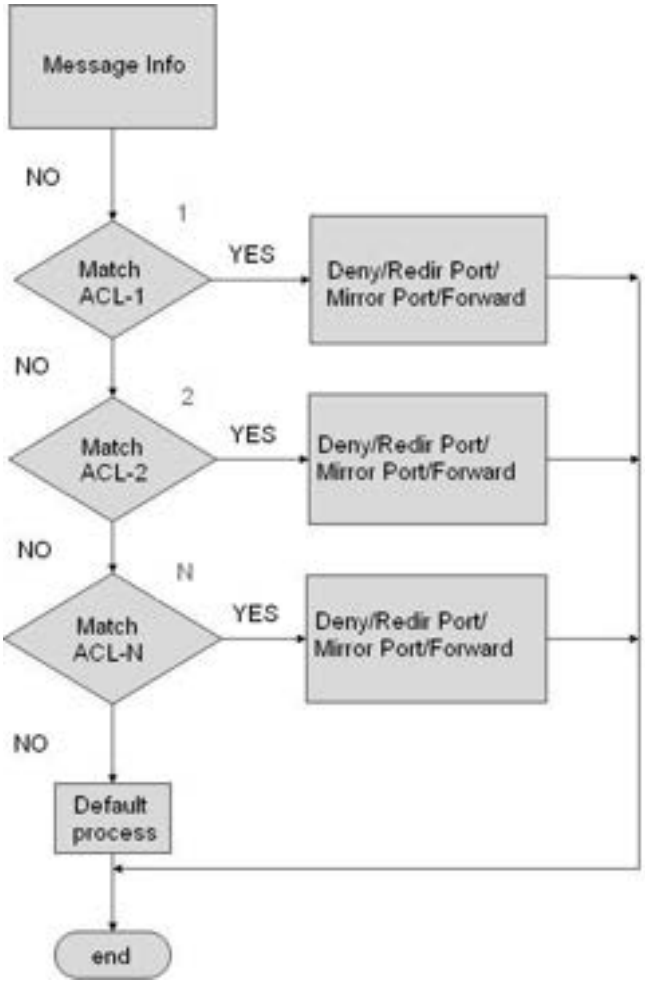


Figure 162 ACL Processing Flowchart

Note:

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

7.8.3 Web Configuration

1. Configure ACL entry, as shown below.

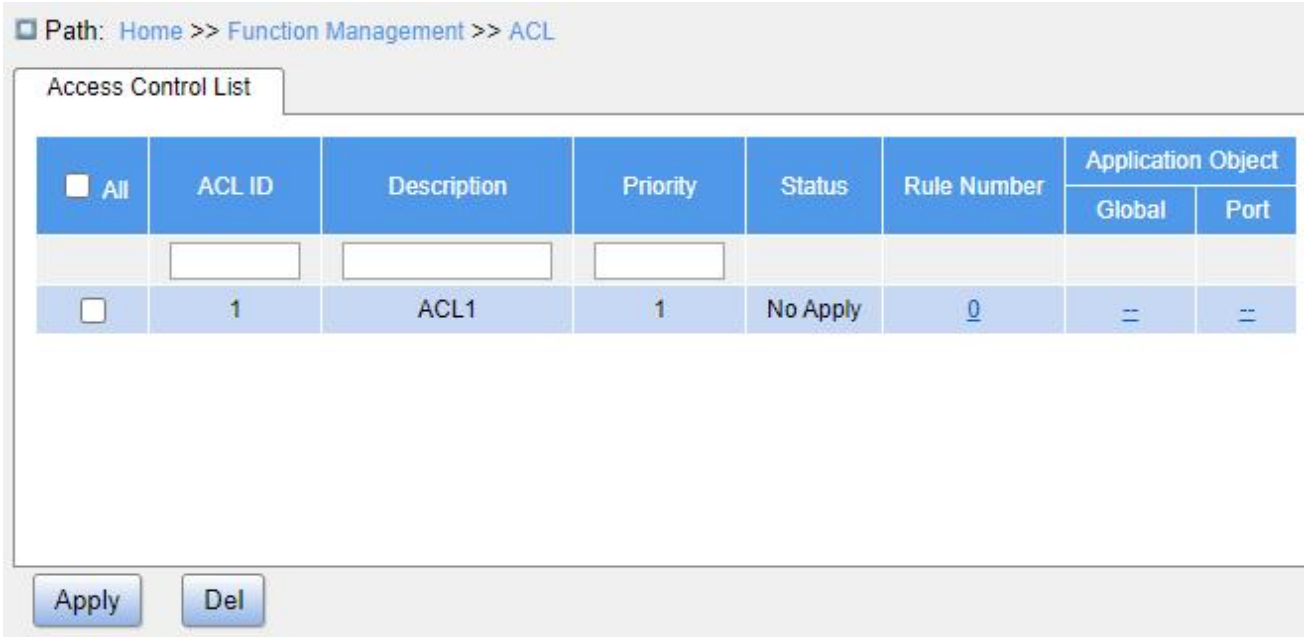


Figure 163 Configure ACL Entry

ACL ID

Configuration range: 1~1024

Function: Configure ACL ID.

Description: The device supports up to 512 ACL entries. If an ACL entry is applied to multiple ports, then each application is counted as an ACL entry.

Note:

There exists some system ACL entries. Therefore, the number of ACL entries that users can configure is smaller than 1024.

Description

Configuration range: 0~127 characters

Function: Add ACL entry description.

Priority

Configuration range: 1~1024

Default configuration: 256

Function: A smaller value indicates a higher priority.

2. Click the value in the “Rule Number” column of an entry, as shown in Figure 163, to enter the page as shown in Figure 164. Then Click <Add> to create ACL rules.

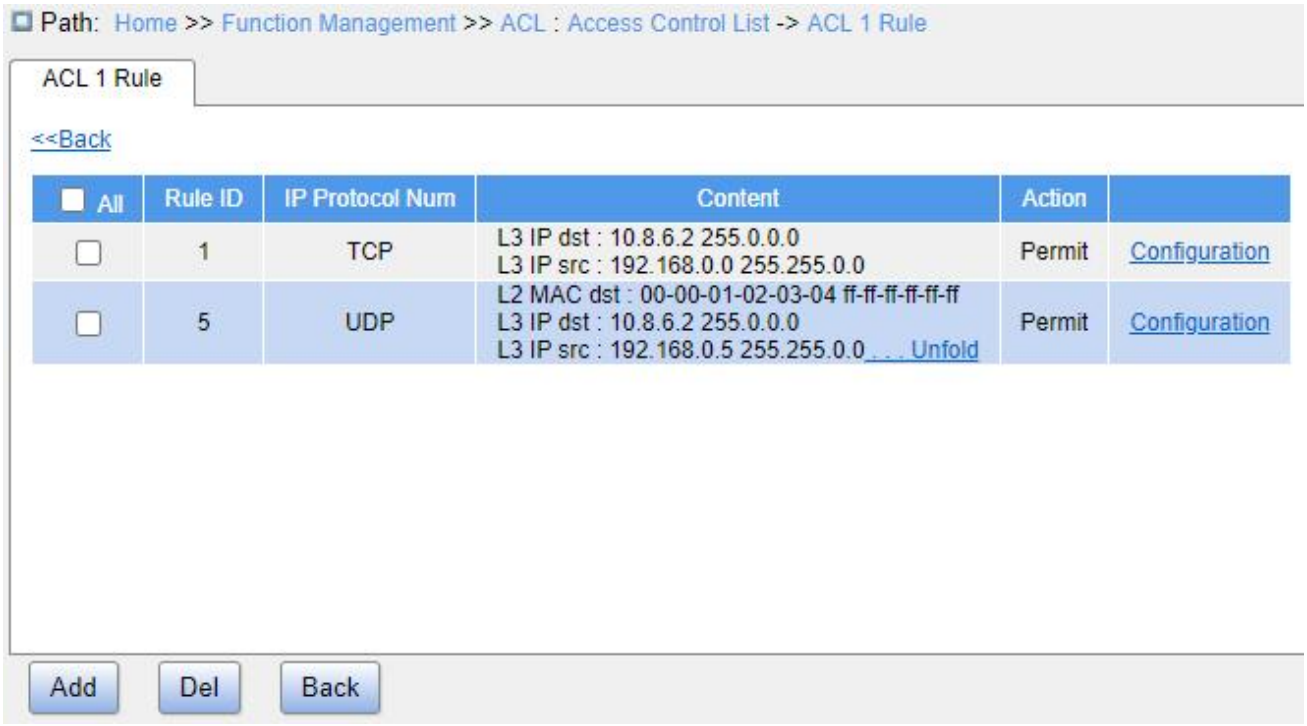


Figure 164 Edit ACL Entry

3. Configure rules for ACL1, as shown below.

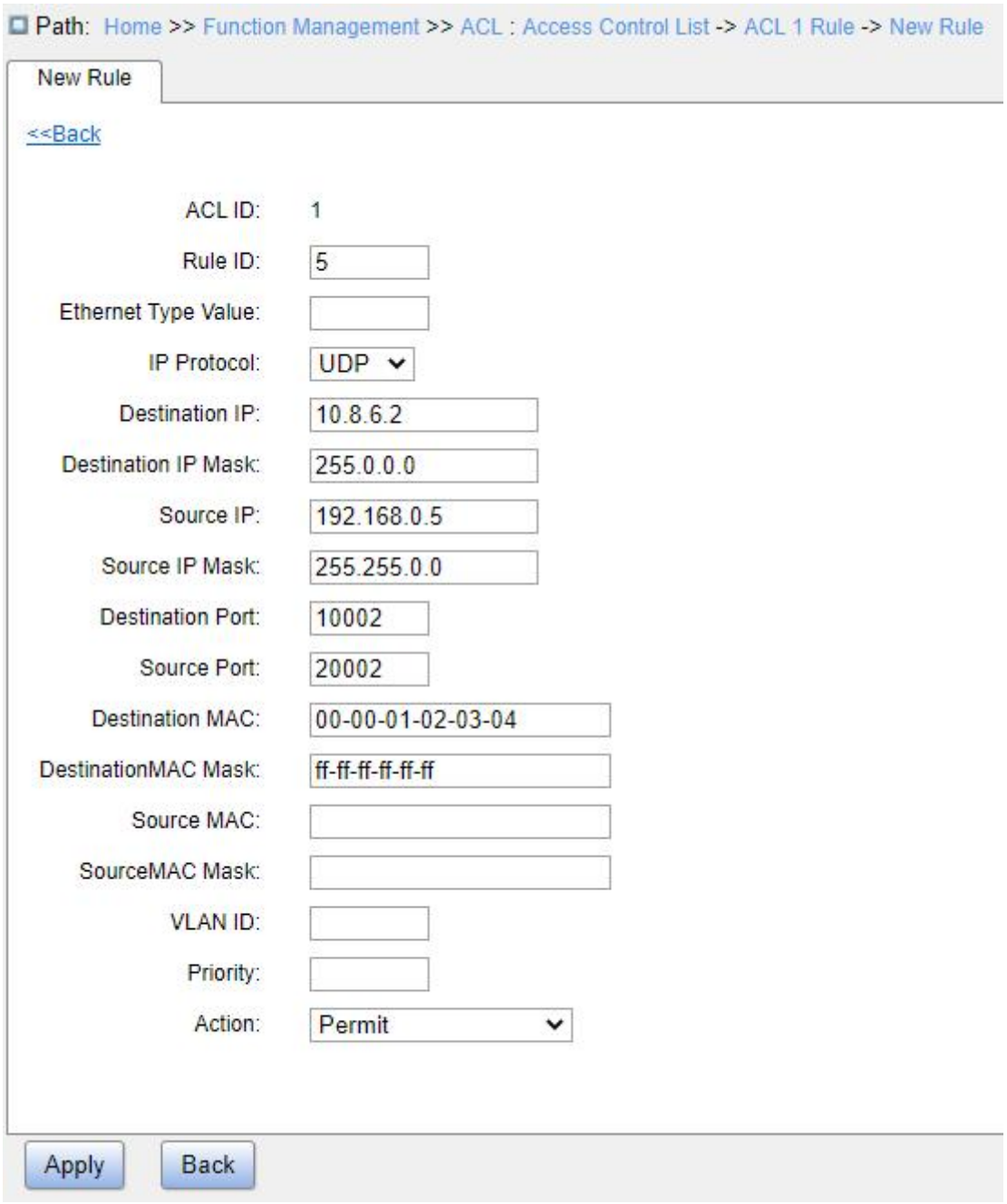


Figure 165 Configure ACL Rule

Rule ID

Configuration range: 1~1024

Function: Configure ACL rule ID.

Description: Each ACL entry supports up to 512 rules, and the total number of rules for all ACL entries cannot exceed 512.

Ethernet Type Value

Configuration range: 0x600~0xFFFF

Function: Configure the protocol type.

IP Protocol

Configuration options: Any/ICMP/TCP/UDP/Other

Default configuration: Any

Function: Configure the matching condition - IP protocol. For “Other”, the protocol number should be configured.

Description: When the IP protocol of an IPv4 packet received by the ingress port matches the parameter configuration, the rule is matched.

Destination IP/Destination IP Mask

Configuration format: A.B.C.D

Function: Configure the matching condition - destination IP address.

Description: The bits 1 in the mask indicates the IP address bits that need to be matched. The bits 0 indicates the IP address bits that do not need to be matched. When the destination IP address of an IPv4 packet received by the ingress port matches the parameter configuration, the rule is matched.

Source IP/Source IP Mask

Configuration format: A.B.C.D

Function: Configure the matching condition - source IP address.

Description: The bits 1 in the mask indicates the IP address bits that need to be matched. The bits 0 indicates the IP address bits that do not need to be matched. When the source IP address of an IPv4 packet received by the ingress port matches the parameter configuration, the rule is matched.

Destination Port

Configuration range: 0~65535

Function: Configure the matching condition - destination port number.

Description: When the destination port number of an IPv4 packet received by the ingress port matches the parameter configuration, the rule is matched.

Source Port

Configuration range: 0~65535

Function: Configure the matching condition - source port number.

Description: When the source port number of an IPv4 packet received by the ingress port matches the parameter configuration, the rule is matched.

Destination MAC/Destination MAC Mask

Configuration format: HH-HH-HH-HH-HH-HH (“H” is a hexadecimal digit)

Function: Configure the matching condition - destination MAC address.

Description: The bits 1 in the mask indicates the MAC address bits that need to be matched. The bits 0 indicates the MAC address bits that do not need to be matched. Description: When the destination MAC address of an IPv4 packet received by the ingress port matches the parameter configuration, the rule is matched.

Source MAC/Source MAC Mask

Configuration format: HH-HH-HH-HH-HH-HH (“H” is a hexadecimal digit)

Function: Configure the matching condition - source MAC address.

Description: The bits 1 in the mask indicates the MAC address bits that need to be matched. The bits 0 indicates the MAC address bits that do not need to be matched. When the source MAC address of an IPv4 packet received by the ingress port matches the parameter configuration, the rule is matched.

VLAN ID

Configuration range: 1~4093

Function: Configure the matching condition - VLAN ID.

Description: When the VLAN ID of an IPv4 packet received by the ingress port matches the parameter configuration, the rule is matched.

Priority

Configuration range: 0~7 (CoS value)

Function: Configure the matching condition - CoS value.

Description: When an IPv4 packet received by the ingress port matches the parameter configuration, the rule is matched.

Action

Configuration options: Permit/Deny/Mirror to CPU/Mirror to Port/Redirect to CPU/Redirect to Port/Limit to kbps/Limit to mbps/Limit to pps/Modify DSCP/Modify Queue/Modify VLAN/Modify CoS

Default configuration: Permit

Function: Configure the action to be performed on the matched packets.

- Permit: The matched packets will be permitted to pass through.
- Deny: The matched packets will be dropped.
- Mirror to CPU: The matched packets will be permitted to pass through and meanwhile mirrored to CPU.
- Mirror to Port: The matched packets will be permitted to pass through and meanwhile mirrored to the specified port.
- Redirect to CPU: The matched packets will be redirected to CPU.
- Redirect to Port: The matched packets will be redirected to the specified port.
- Limit to kbps: The kbps rate of the matched packets will be restricted.
- Limit to mbps: The mbps rate of the matched packets will be restricted.
- Limit to pps: The pps rate of the matched packets will be restricted.
- Modify DSCP: The DSCP value of the matched packets will be modified.
- Modify Queue: The queue value of the matched packets will be modified.
- Modify Cos: The CoS value of the matched packets will be modified.

4. Click <--> in the Application Object column to configure the target to which ACL1 will be applied, as shown below.

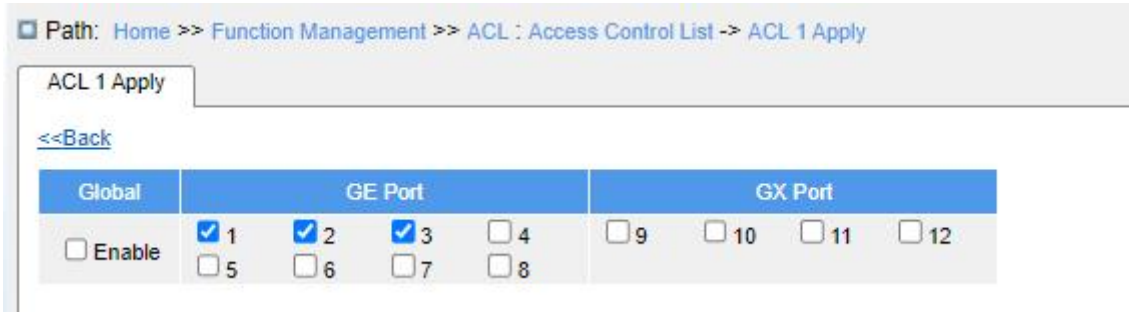


Figure 166 Configure ACL Entry Application Target

ACL1 Apply

Configuration options: Global/Specific Ports

Function: Apply the ACL entry to the global or specific ports.

7.9 MAC Address Configuration

7.9.1 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.

7.9.2 Web Configuration

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

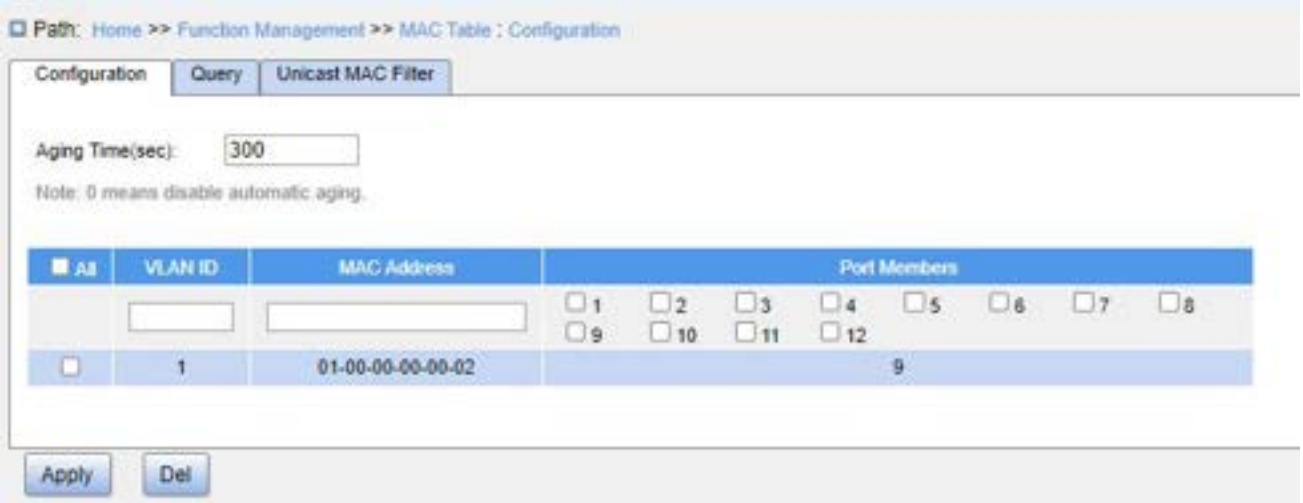


Figure 167 MAC Address Aging Time Configuration

Aging Time

Configuration range: 0 or 10~1000000s

Default configuration: 300

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

VLAN ID

Configuration range: 1~4093

Function: Configure the VLAN ID.

MAC Address

Configuration format: HH:HH:HH:HH:HH:HH or HH-HH-HH-HH-HH-HH (“H” is a hexadecimal value)

Function: Configure the MAC address.

Port Members

Configuration range: All switch ports

Function: Configure the port.

2. View MAC address table, as shown below.

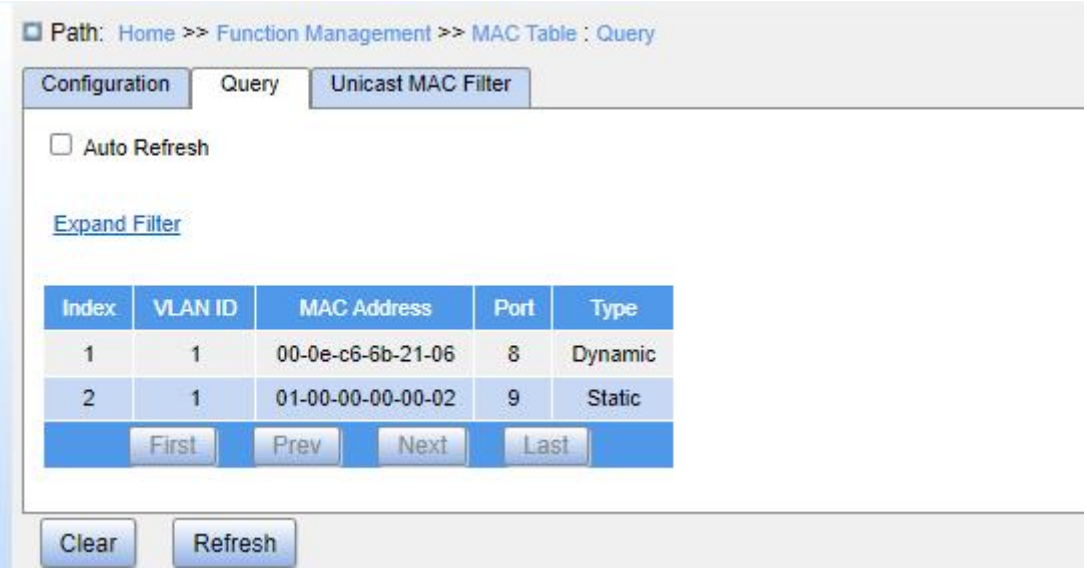


Figure 168 View MAC Address Table

VLAN ID

Configuration options: */>=/<=/Range

Default configuration: *

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

MAC Address

Configuration options: */>=/<=/Range

Default configuration: *

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

Port

Configuration options: */Include/Exclude

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.

3. Configure unicast MAC filter, as shown below.

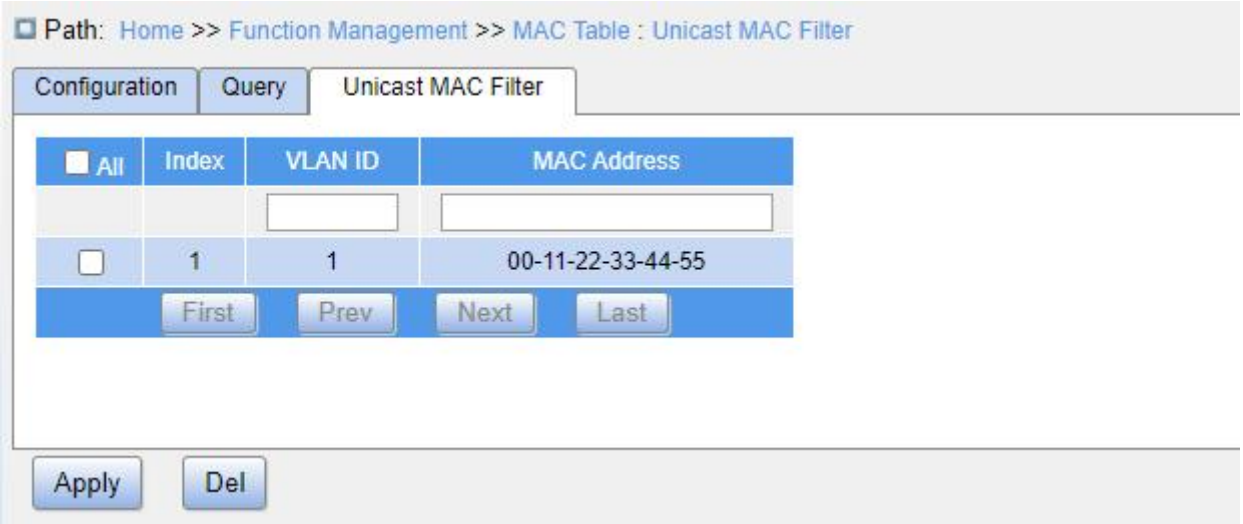


Figure 169 Configure Unicast MAC Filter

VLAN ID

Configuration range: All created VLAN IDs

Function: Configure the VLAN of the static MAC table.

MAC Address

Configuration format: HH-HH-HH-HH-HH-HH or HH:HH:HH:HH:HH:HH (H is a hexadecimal value)

Function: Configure the MAC address. For the unicast MAC address, the least significant bit in the most significant octet is 0; for the multicast MAC address, the value is 1.

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.

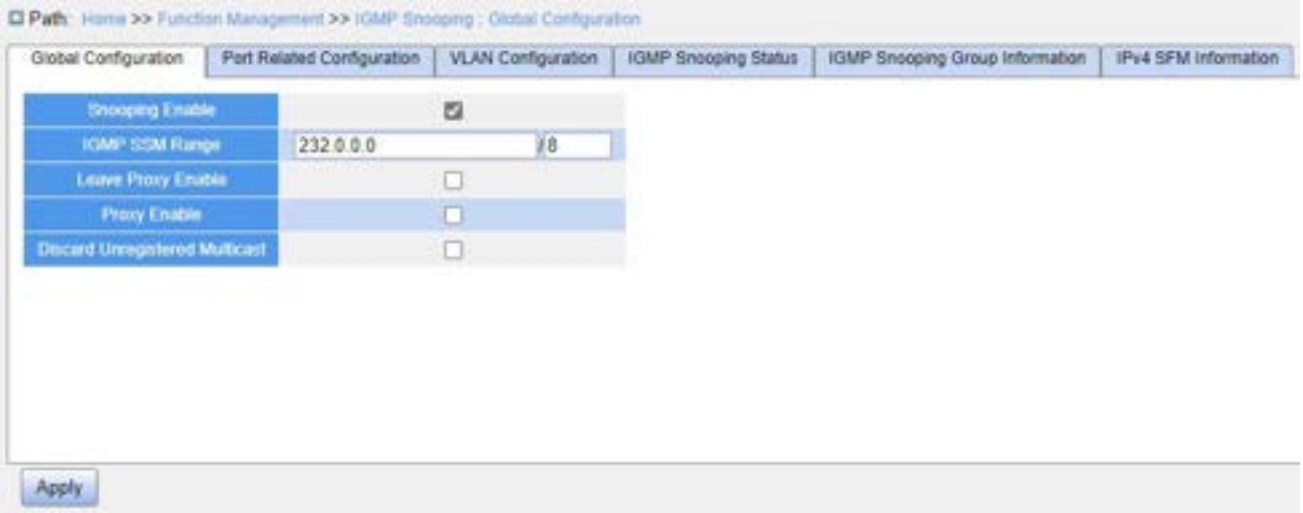


Figure 170 Configure IGMP Snooping

Snooping Enable

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable 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 Enable

Configuration options: Enable/Disable

Default configuration: Disable

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

Proxy Enable

Configuration options: Enable/Disable

Default configuration: Disable

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: Enable/Disable

Default configuration: Disable

Function: Whether the switch discards unknown multicast packets.

2. Configure IGMP port, as shown below.

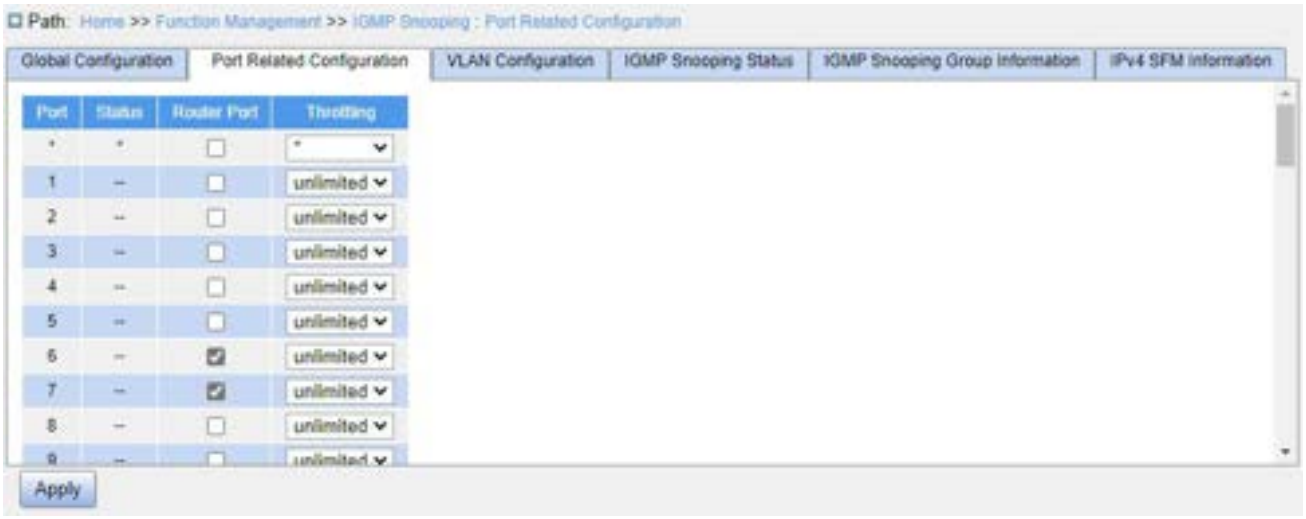


Figure 171 Configure IGMP Port

Status

Configuration options: --/Static/Dynamic

Function: Displays the router port status.

- Static: Indicates that the port is statically configured as a router port;
- Dynamic: Indicates that the port is dynamically learned as a router port.

Router Port

Configuration options: Enable/Disable

Default configuration: Disable

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.

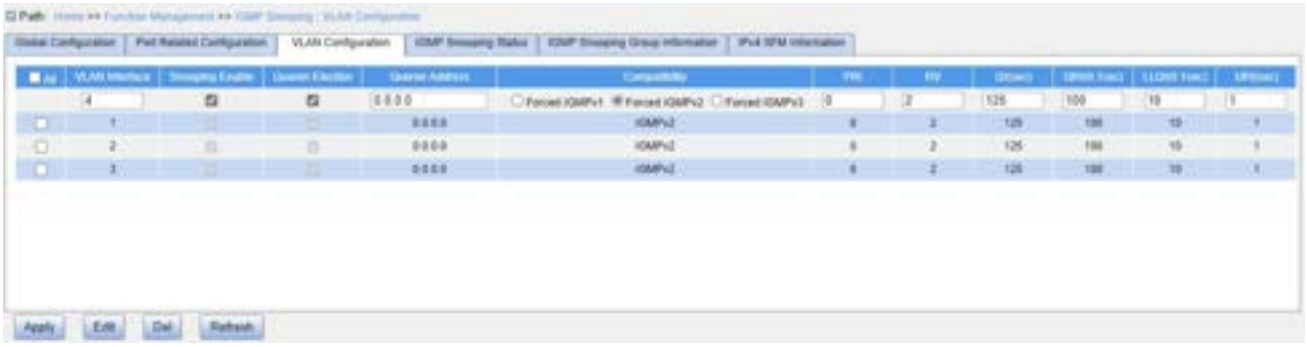


Figure 172 Configure IGMP Snooping VLAN

VLAN Interface

Configuration options: All created VLAN IDs

Snooping Enable

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable 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: Whether to enable 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 the 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. Users can set a suitable robustness parameter according to the actual network.

QI (Query Interval)

Configuration range: 1~31744s

Default configuration: 125

Function: Configure the interval of sending general Query packets.

QRI (Query Response Interval)

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

Default configuration: 100

Function: Configure the max response time of 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 specific Query packet.

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

4. View IGMP Snooping status, as shown below.

Figure 173 View IGMP Snooping Status

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

Figure 174 IGMP Snooping Member List

VLAN ID

Configuration options: */>=/<=/Range

Default configuration: *

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

Group

Configuration options: */>=/<=/Range

Default configuration: *

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

Port

Configuration options: */Include/Exclude

Default configuration: *

Function: Display the group information according to configured port.

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

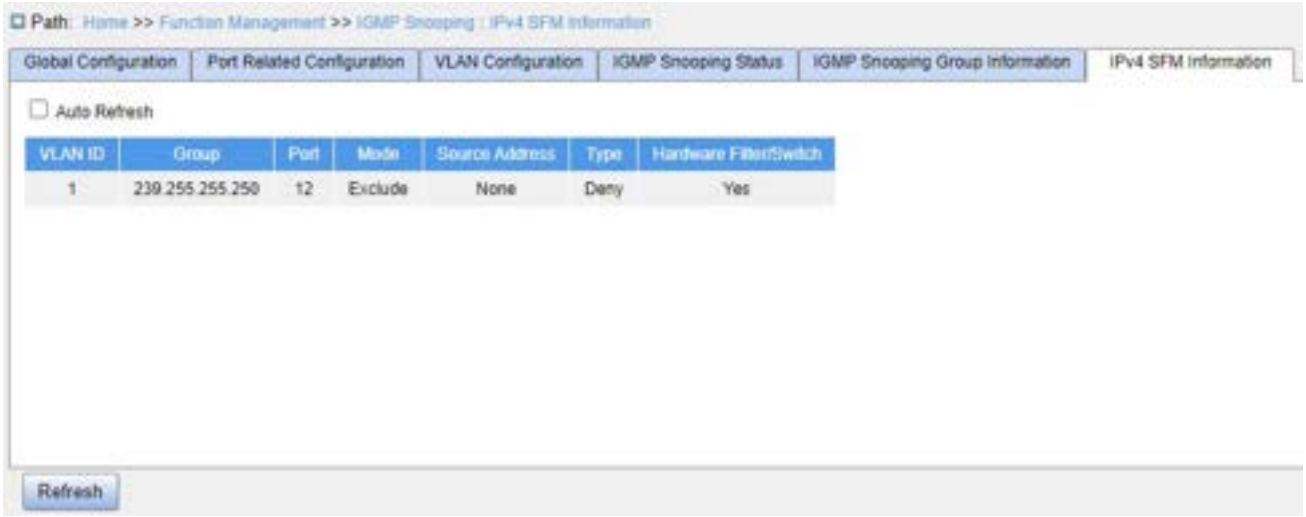


Figure 175 IGMP Snooping IPv4 SFM information

7.10.5 Typical Application Example

As shown in Figure 176, 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.

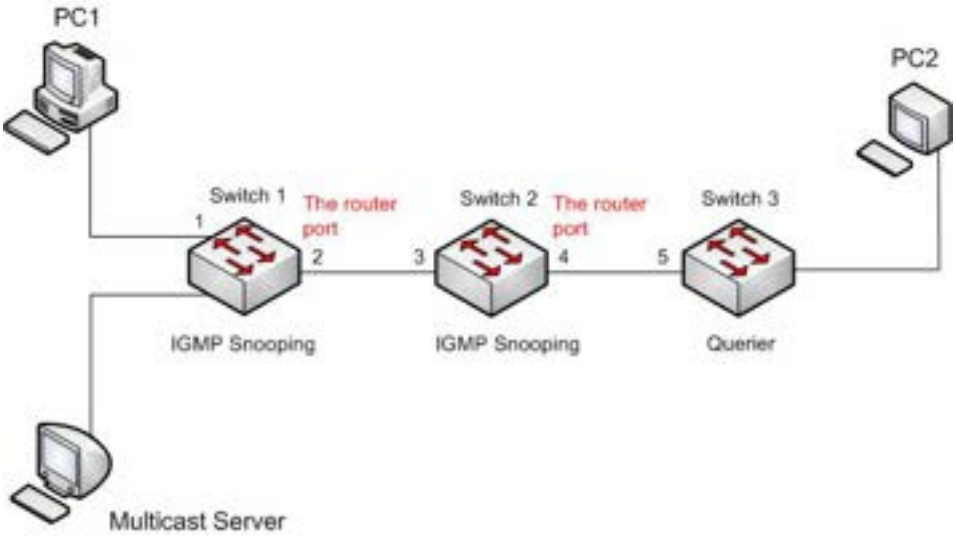


Figure 176 IGMP Snooping Application Example

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. 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 177.

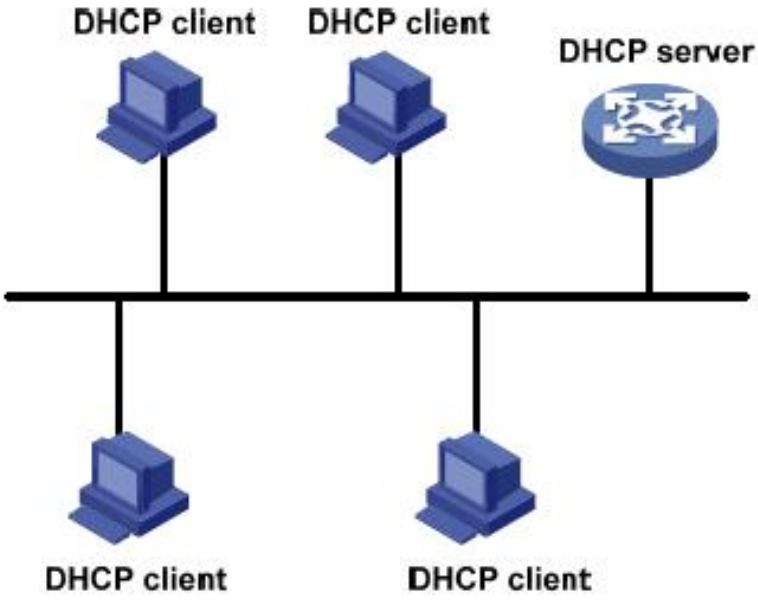


Figure 177 DHCP Typical Application

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.

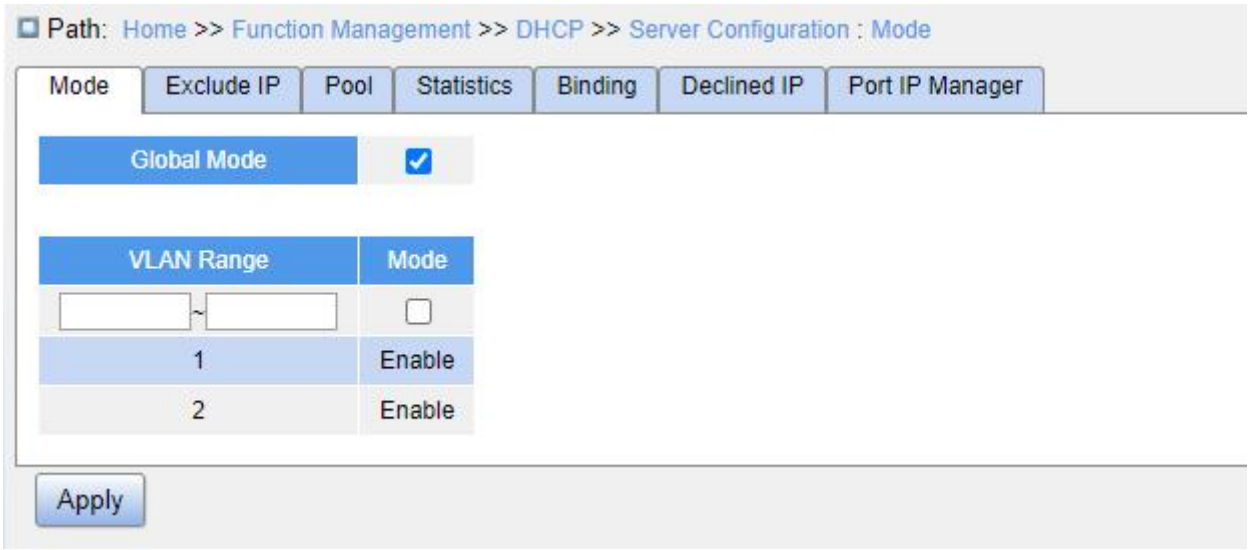


Figure 178 Enable DHCP Server

Global Mode

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable the current switch to work as the DHCP server.

{VLAN Range, Mode}

Configuration range: {1~4093, Enable/Disable}

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.

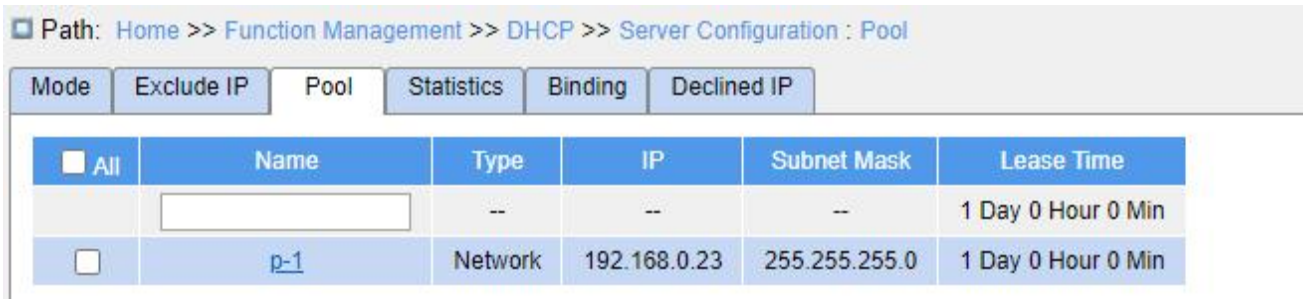


Figure 179 Create DHCP Address Pool

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 a pool name in Figure 179 to configure the DHCP address pool, as shown below.

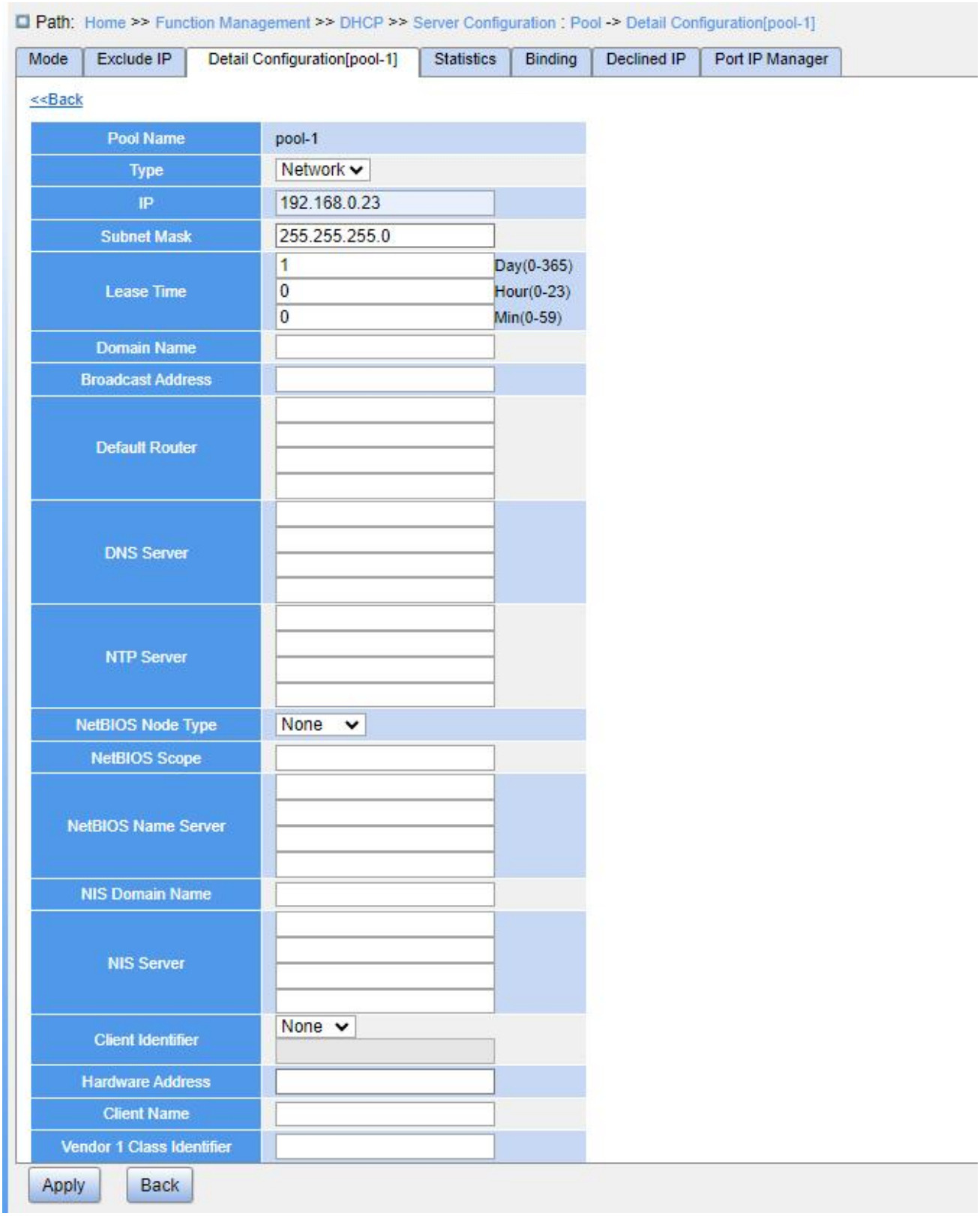


Figure 180 Configure IP Address Pool

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: For the “Network” type, 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 a string of bits 1 and a string of bits 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.

For the “Host” type, 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, the server sends the domain name suffix to the client too.

Broadcast Address

Configuration format: A.B.C.D

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

Default Router

Configuration format: A.B.C.D

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

Description: 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 a maximum of 4 gateways.

DNS Server

Configuration format: A.B.C.D

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

Description: 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 a maximum of 4 DNS servers.

NTP Server

Configuration 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.

- 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

Configuration format: A.B.C.D

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

Description: 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 a maximum of 4 WINS servers.

NIS Domain Name

Configuration range: 1~36 characters

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

NIS Server

Configuration 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 the client's unique identifier.

Hardware Address

Configuration 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 1/2/3/4 Class Identifier

Configuration range: 1~64 characters

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

Vendor 1/2/3/4 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.

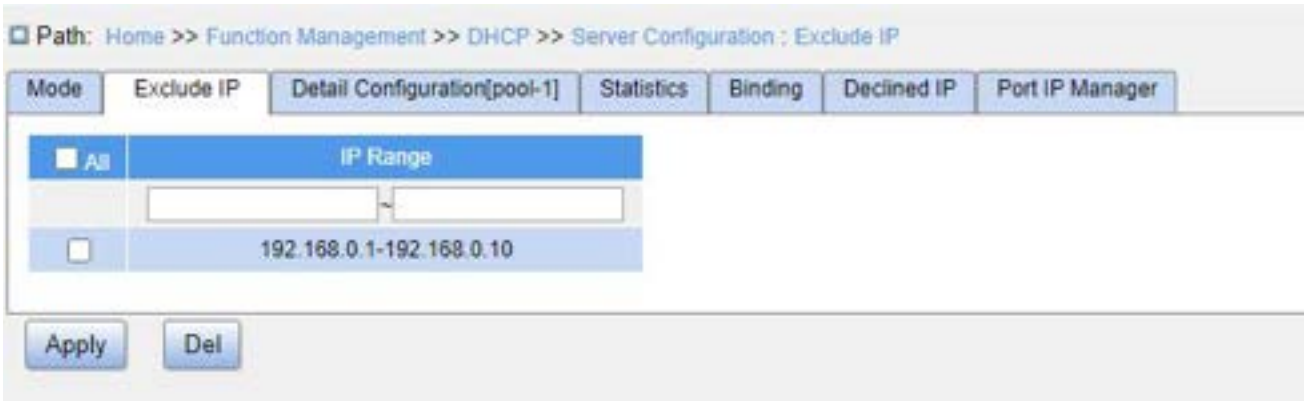


Figure 181 Configure Excluded IP Addresses

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 conflicts.

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

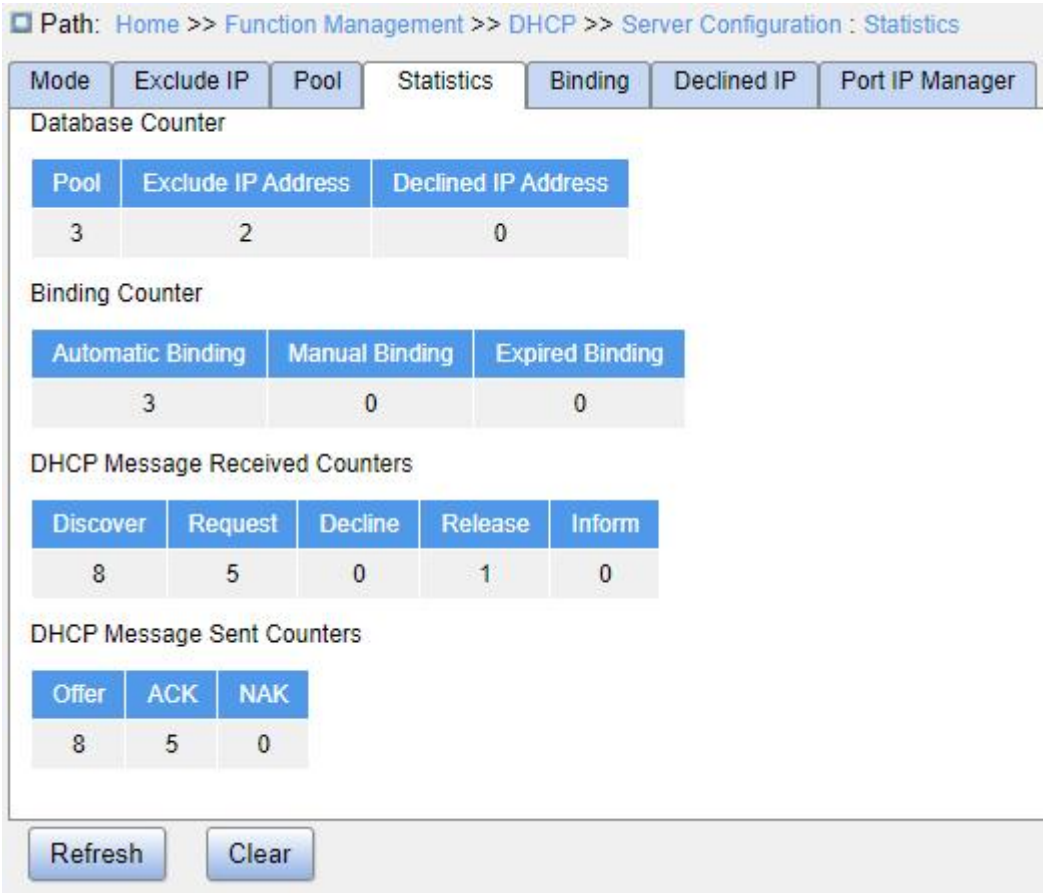


Figure 182 View DHCP Server Statistics Information

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

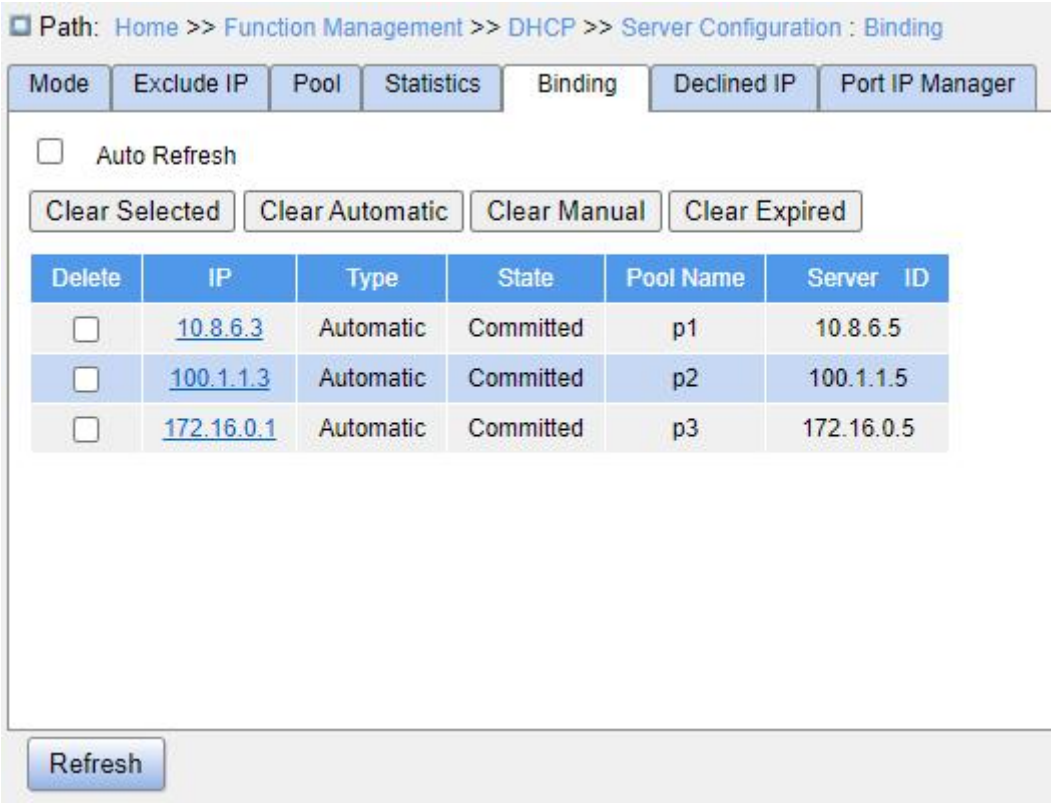


Figure 183 View Information about IP Addresses Allocated by the DHCP Server

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

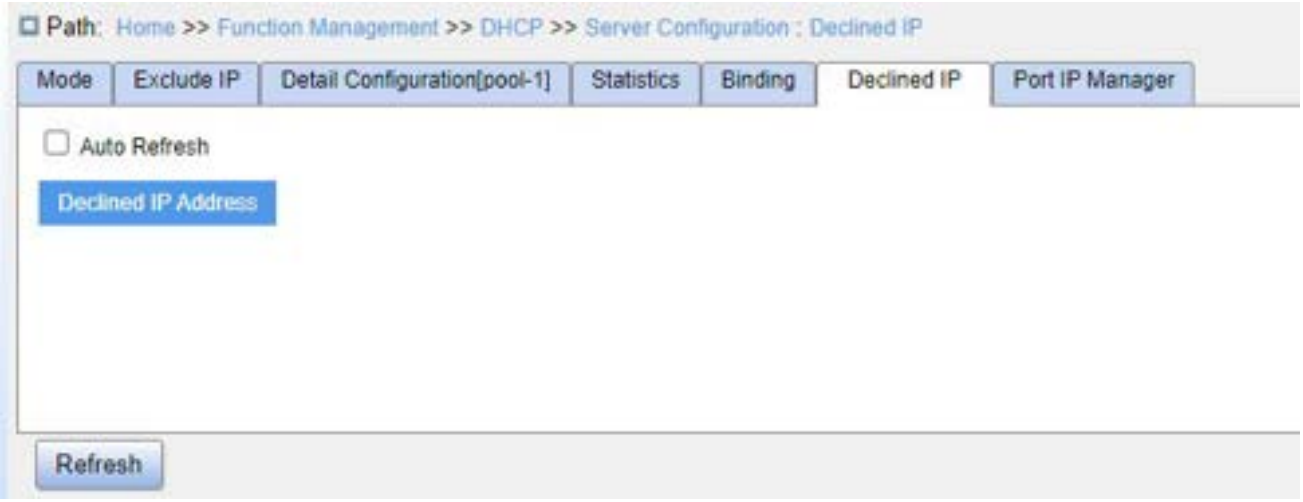


Figure 184 View the IP Addresses Declined by DHCP Clients

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.

8. Configure port IP manager, as shown below.

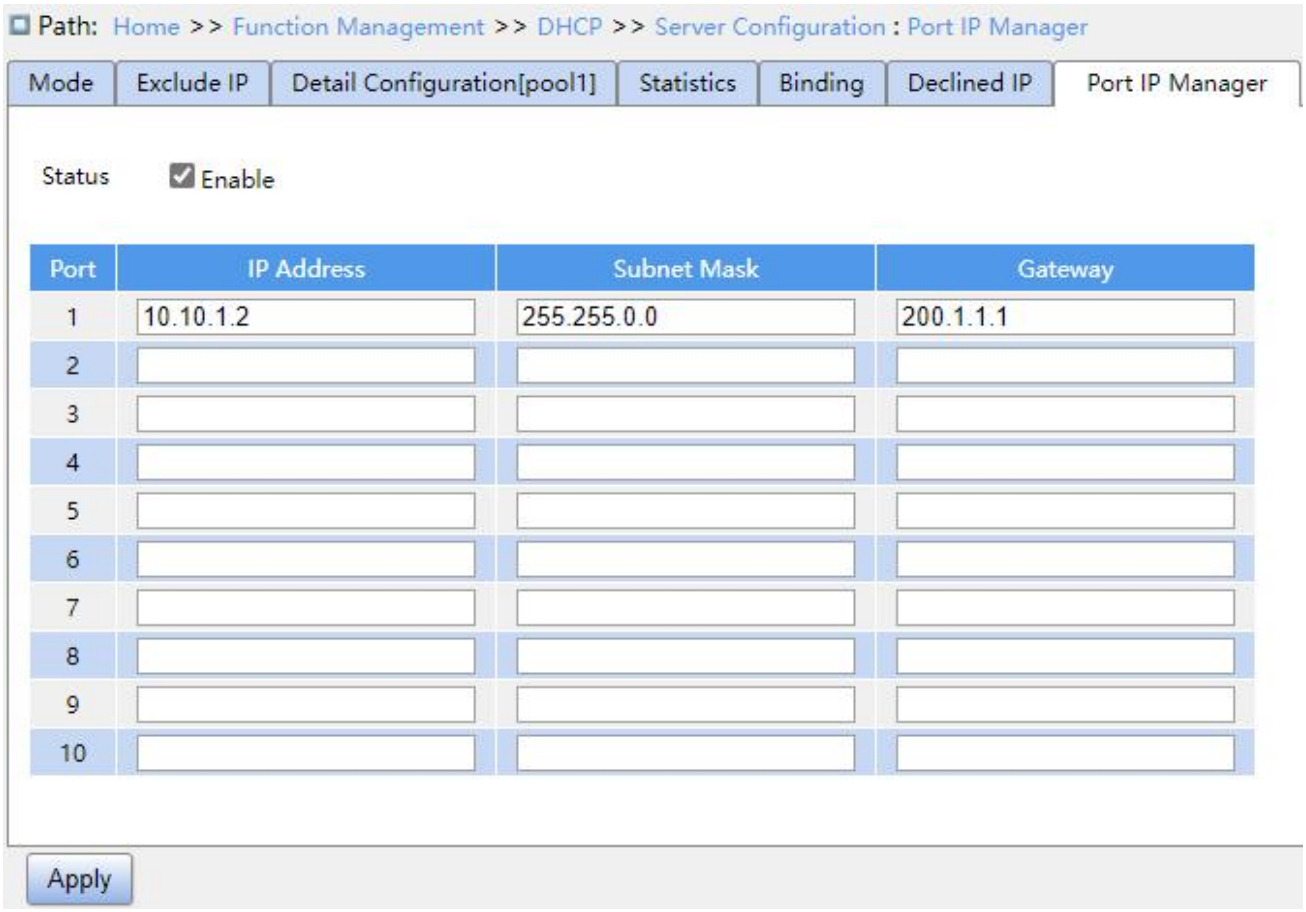


Figure 185 Configure Port-Based DHCP

Status

Configuration options: Enable/Disable

Default configuration: Disable

Function: Configure DHCP server's allocation mode.

Description: When this option is enabled, the DHCP server works in the port mode. When it is disabled, the DHCP server works in the common mode. In common mode, the DHCP server allocates IP addresses dynamically or based on static binding. In port mode, you need to manually bind an IP address to a port. When the port receives a DHCP request message from a client, the DHCP server will allocate the bound IP address to the client.

Caution:

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

IP Address

Configuration format: A.B.C.D

Function: Configure the IP address bound to this port.

Mask

Configuration format: A.B.C.D

Function: Configure the netmaks of the bound IP address.

Gateway

Configuration format: A.B.C.D

Function: Configure the gateway address allocated to the client.

7.11.1.4 Typical Configuration Example

As shown in Figure 186, 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.

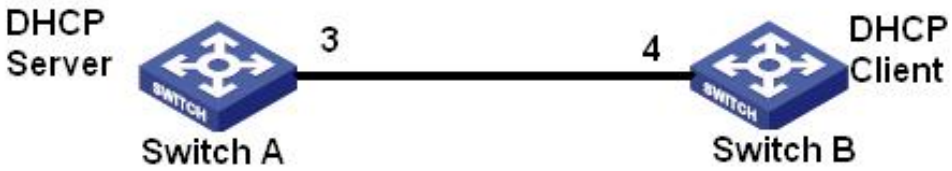


Figure 186 DHCP Typical Configuration Example

Static Allocation

Switch A configuration:

1. Enable DHCP server status in correspond VLANs, as shown in Figure 178.

2. Create a DHCP IP pool “pool-1”, as shown in Figure 179.

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 180.

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 187.

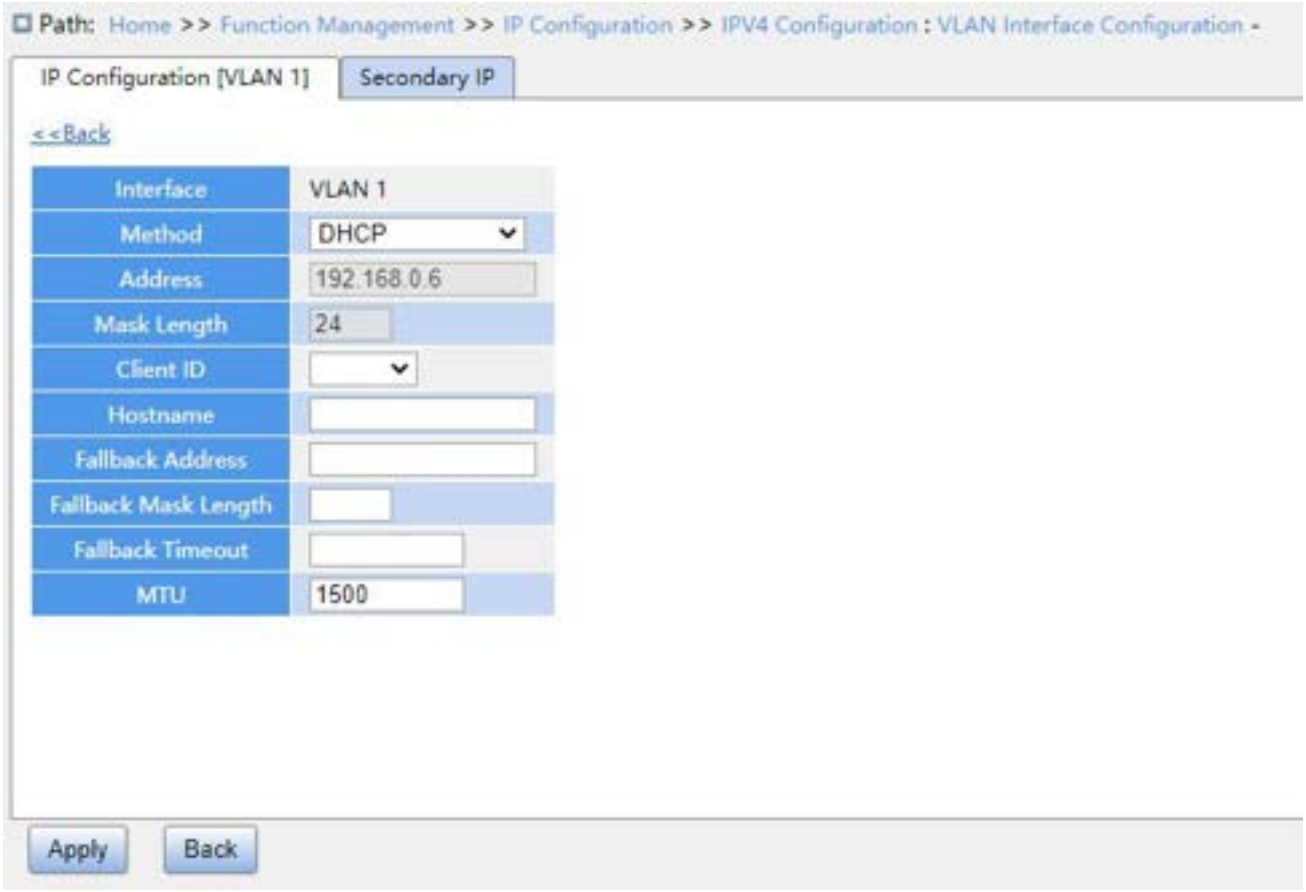


Figure 187 DHCP Client Obtain IP Address-1

Dynamic Allocation

Switch A configuration:

1. Enable DHCP server status in correspond VLANs, as shown in Figure 178.

2. Create a DHCP IP pool “pool-1”, as shown in Figure 179.

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 181.

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 188.

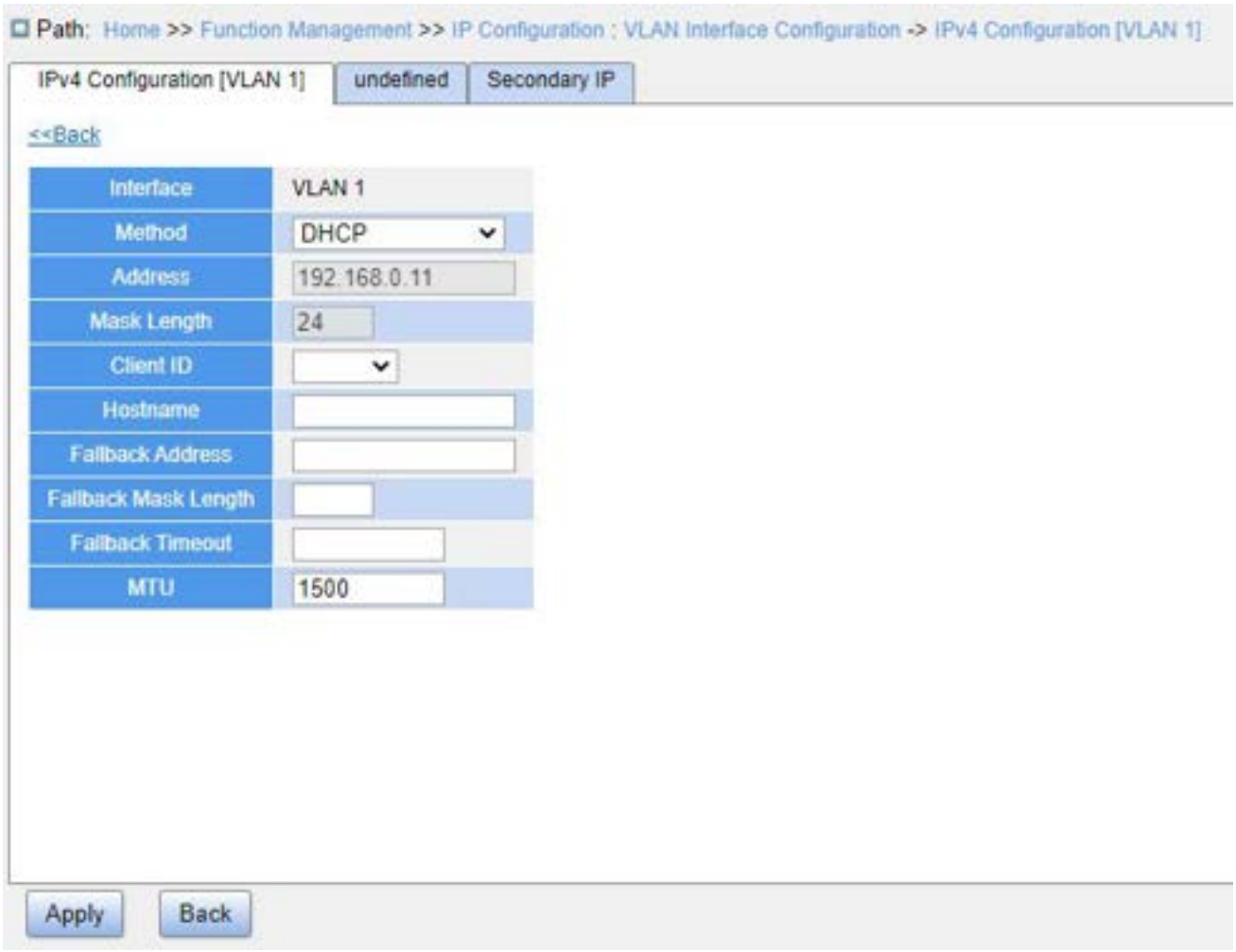


Figure 188 DHCP Client Obtain IP Address-2

7.11.2 DHCP Snooping

7.11.2.1 Introduction

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.

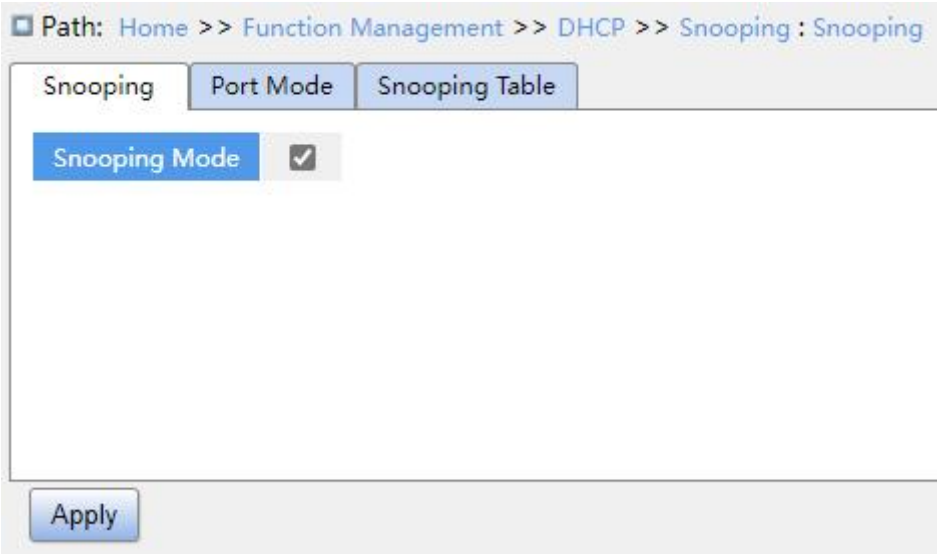


Figure 189 DHCP Snooping State

Snooping Mode

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable 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.

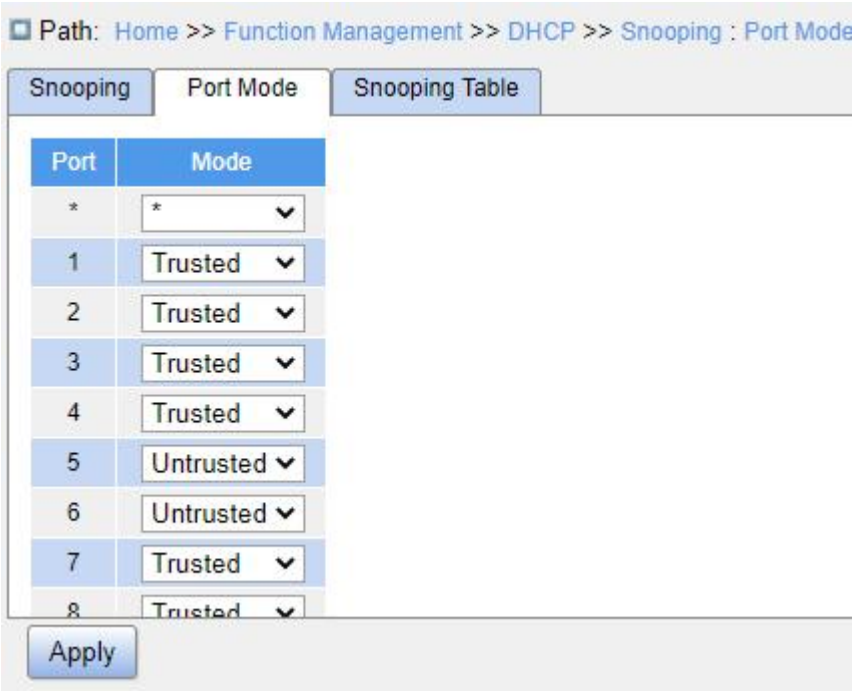


Figure 190 Configure Trust Port

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.

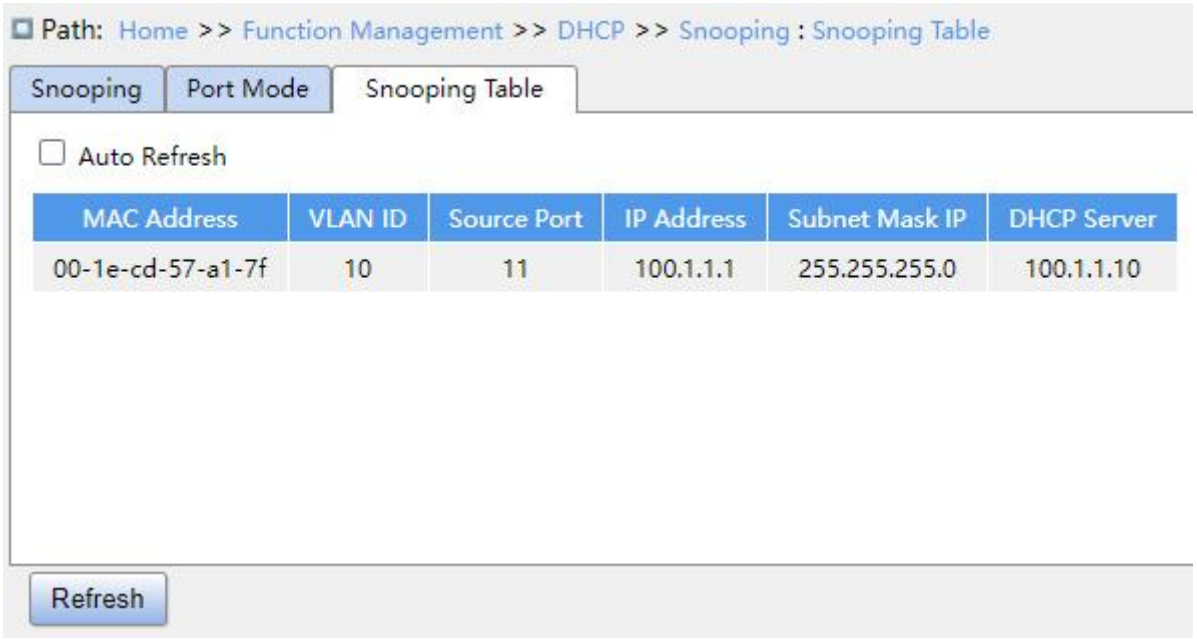


Figure 191 View DHCP Snooping Entries

7.11.2.3 Typical Configuration Example

As shown in Figure 192, 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.

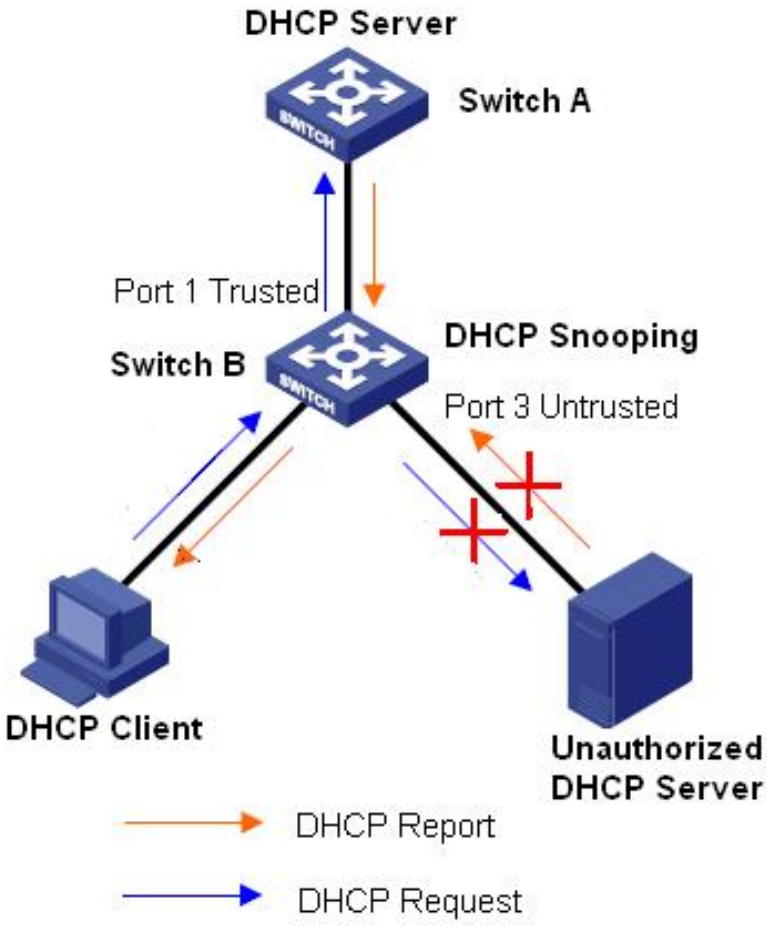


Figure 192 DHCP Snooping Typical Configuration Example

Switch B Configuration:

1. Enable DHCP Snooping function, as shown in Figure 189.

2. Set the port 1 of switch B to a trusted port and set the port 3 to an untrusted port, as shown in Figure 190.

➢

7.11.3 DHCP Relay

7.11.3.1 Introduction

1. DHCP Relay

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.

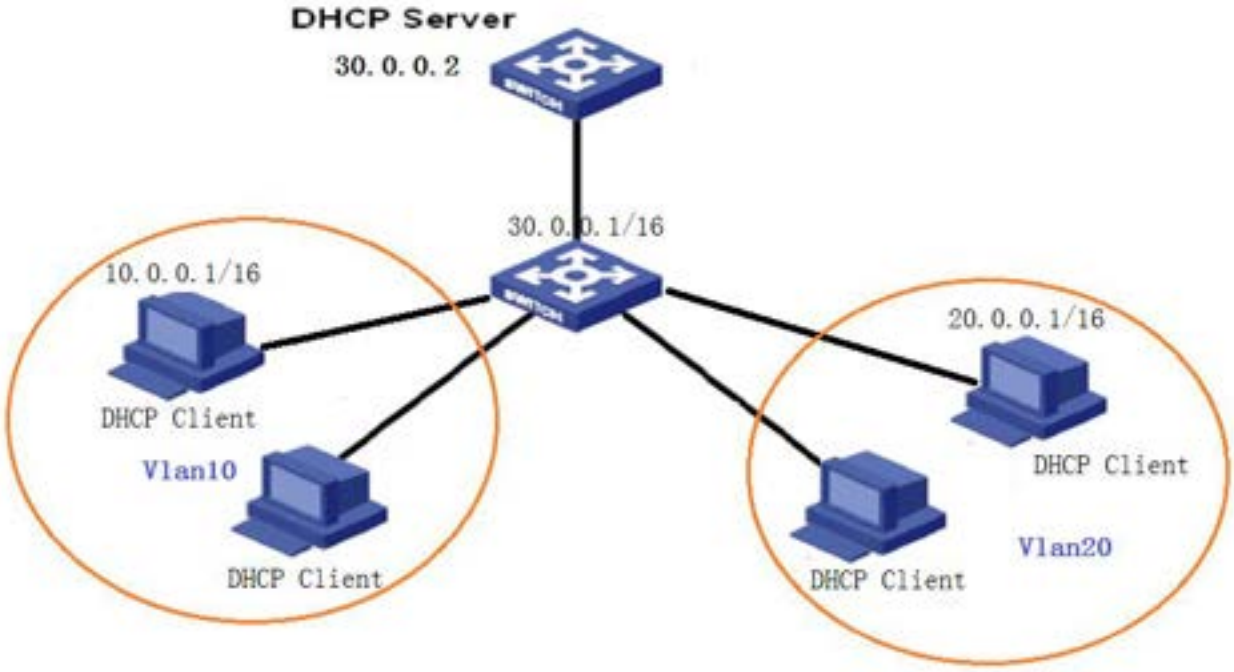


Figure 193 Client – Relay - Server Mode

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 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 adds the corresponding Option 82 field into the messages and then forwards 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 Relay 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 Relay 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 Processing of Request Message by DHCP Relay

Whether the request message contains Option 82	**Configuration policy**	**Processing of the request message**
The request message contains Option 82.	Drop	Drop the request message
	Keep	Keep the message format unchanged and forward the message
	Replace	Replace the Option 82 field in the message with the Option 82 field of the Snooping device and forward the new message
The request message does not contain Option 82.	Drop/Keep/Replace	Add the Option 82 field of the 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, it removes the Option 82 field and forwards the message to the client.

7.11.3.2 Web Configuration

1. Configure global DHCP relay, as shown below.

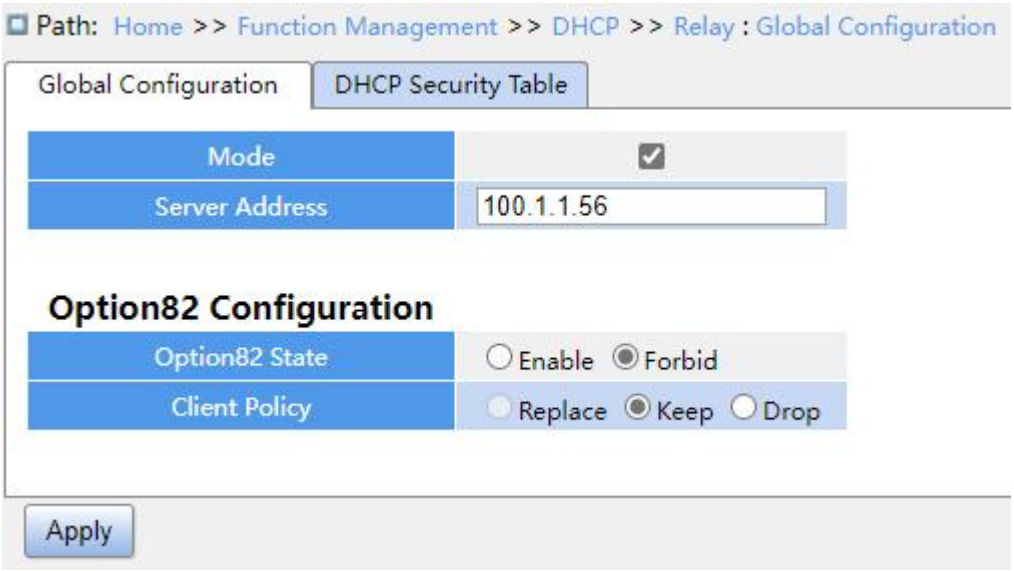


Figure 194 DHCP Relay Global Configuration

Mode

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable DHCP relay.

Server Address

Function: Configure DHCP server address.

Option82 State

Configuration options: Enable/Forbid

Default configuration: Forbid

Function: Whether to enable Option 82 for DHCP relay.

Client Policy

Configuration options: Replace/Keep/Drop

Default configuration: Keep

Function: Configure the client policy, DHCP relay processes the request message sent by client according to the client policy. The specific treatment is shown in Table 9.

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

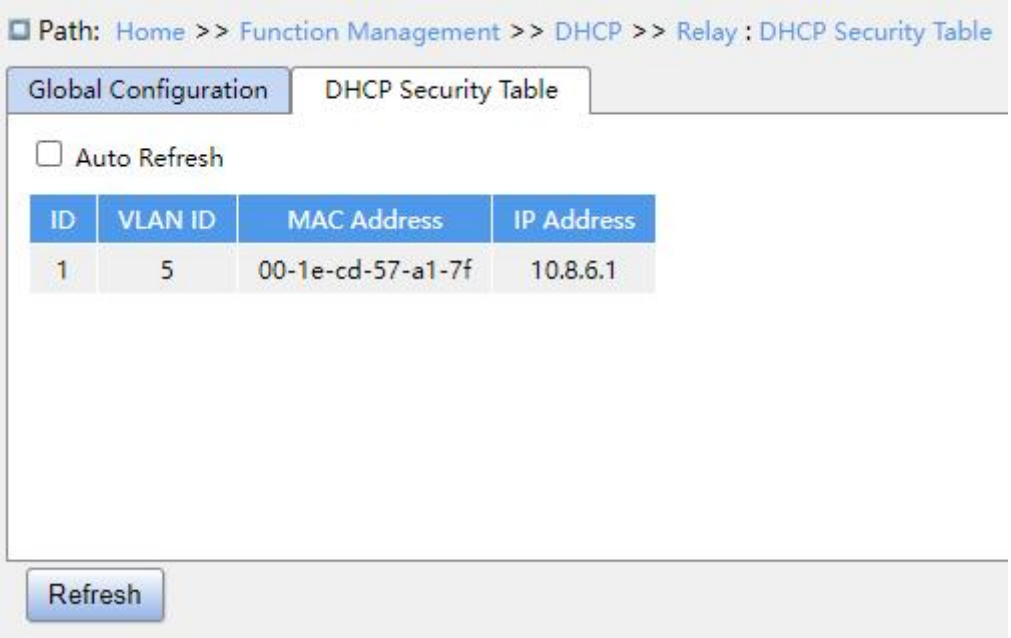


Figure 195 View DHCP Security Table

7.11.3.3 Typical Configuration Example

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

Figure 196 DHCP Typical Configuration Example

Switch A Configuration:

1. Create “VLAN1” and configure IP 100.1.1.156, as shown in Figure 107;
2. Open the DHCP server state on VLAN 1, as shown in Figure 107;
3. Create address pool “pool-33”, as shown in Figure 179;
4. Select the address pool type as “Network”; IP address 33.1.1.6; Mask 255.0.0.0;

Switch B Configuration:

1. Create “VLAN1” and configure IP 100.1.1.180, as shown in Figure 107;
2. Create the “VLAN33” and configure IP 33.1.1.2, as shown in Figure 107;
3. Enable DHCP relay, as shown in Figure 194;
4. Configure server IP address 100.1.1.156, as shown in Figure 194;

Switch C Configuration:

1. Create “VLAN33” and enable DHCP Client, as shown in Figure 107;
2. Switch A assigns 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 method. 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 below. User authentication and authorization of port-based access control requires the following elements:

Figure 197 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. Configure 802.1X task manager, as shown below.

Figure 198 Task Manager Configuration

Operation Type

Configuration options: Restart Authentication Process/Initialize

Function: When the port mode is MAC-Based or VLAN-Based, 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

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

2. Configure IEEE802.1X basic parameters, as shown below.

Figure 199 IEEE802.1X Basic Configuration

System Auth-Control

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable 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 enabled 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 enabled 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: 3600

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: 30

Function: Set the overtime for response from the client. After sending an Identity EAPOL request packet, the device will retransmit an 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: 300

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: 10

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: 1~4093

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 that “Guest -VLAN” is enabled.
- 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 fails 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.

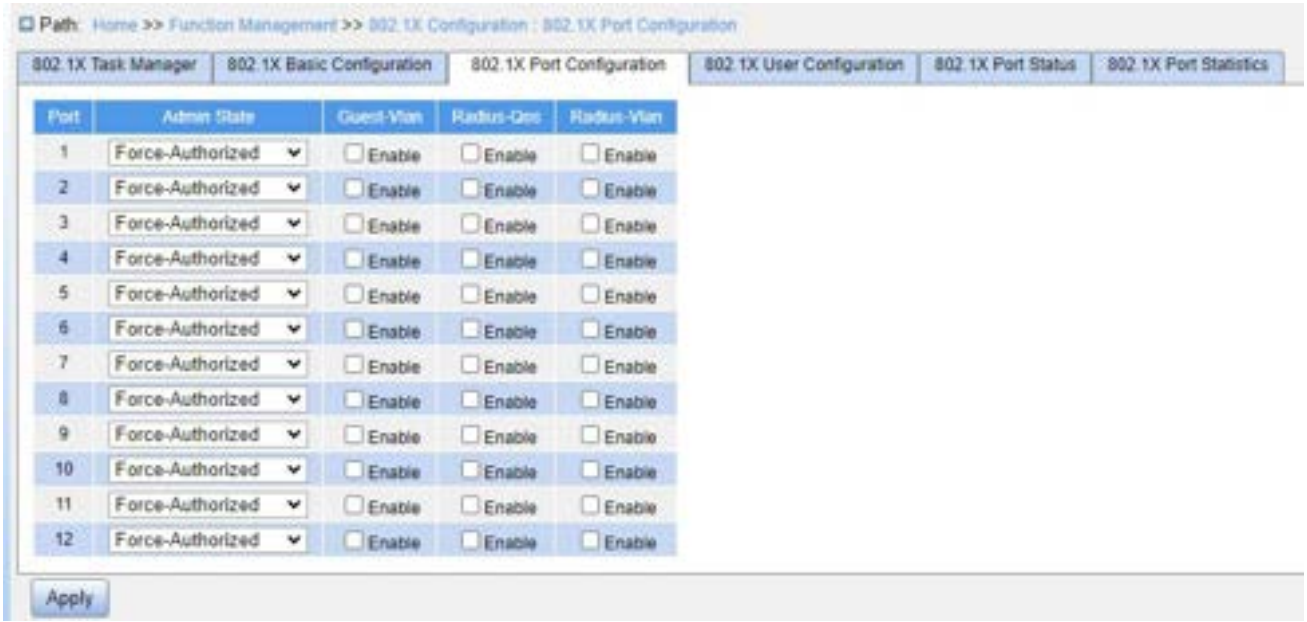


Figure 200 Configure IEEE802.1X port

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.

- Force Authorized: Port is always in an authorized state and allows users to access network resource without authentication.
- Force Unauthorized: 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: Users using the port need to be authenticated respectively. When a user is offline, only the user cannot use the network.
- Port-based: 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.

Guest-VLAN

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable Guest-VLAN on port.

RADIUS-QoS

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable RADIUS-Assigned QoS on port.

RADIUS-VLAN

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable 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. Configure IEEE802.1X users, as shown below.

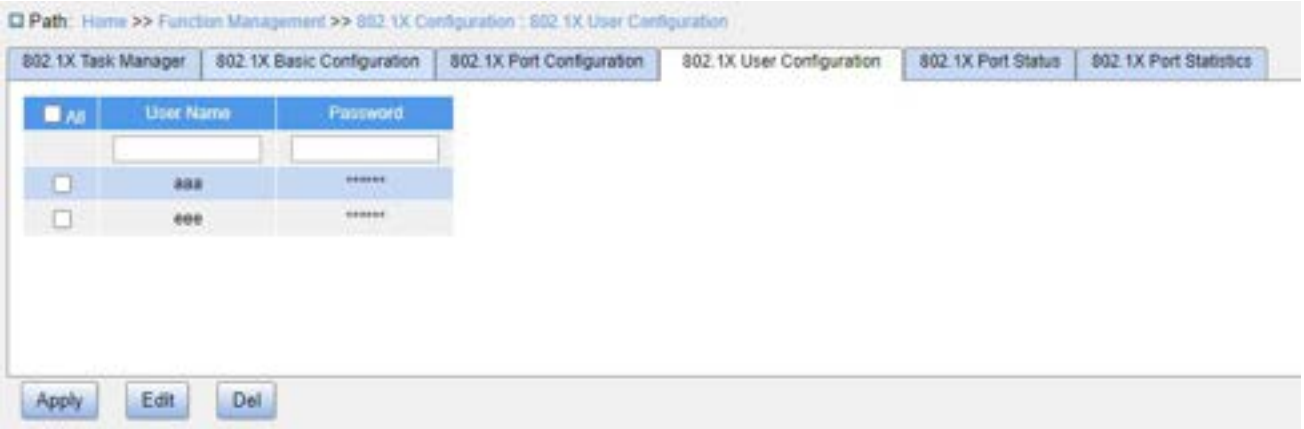


Figure 201 IEEE802.1X User Configuration

User Name

Configuration range: 1~16 characters

Default configuration: None

Function: Configure the local authentication username.

Password

Configuration range: 1~16 characters

Default configuration: None

Function: Configure the local authentication password.

5. View IEEE802.1X port status, as shown below.

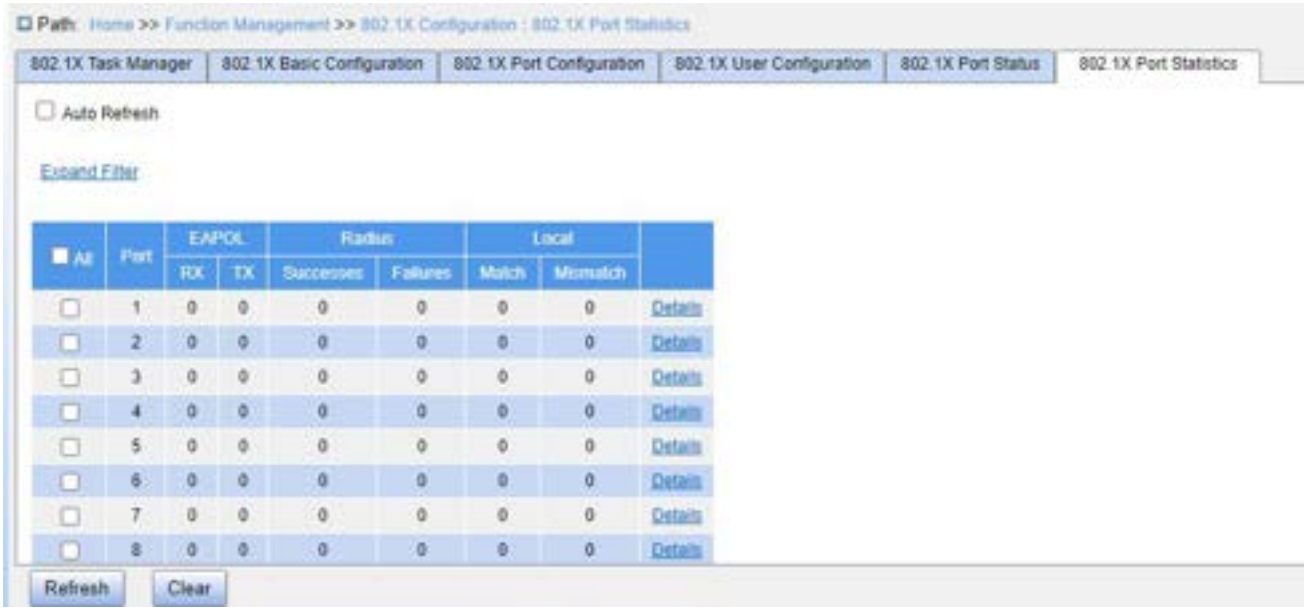


Figure 202 IEEE802.1X Port Status

Port Status

Configuration options: Disable/Auth/UnAuth/Down/x A/y UnA

Function: Display port authentication state.

- Disable: Indicates IEEE802.1X is disabled 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.

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

Figure 203 View IEEE802.1X Statistics

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

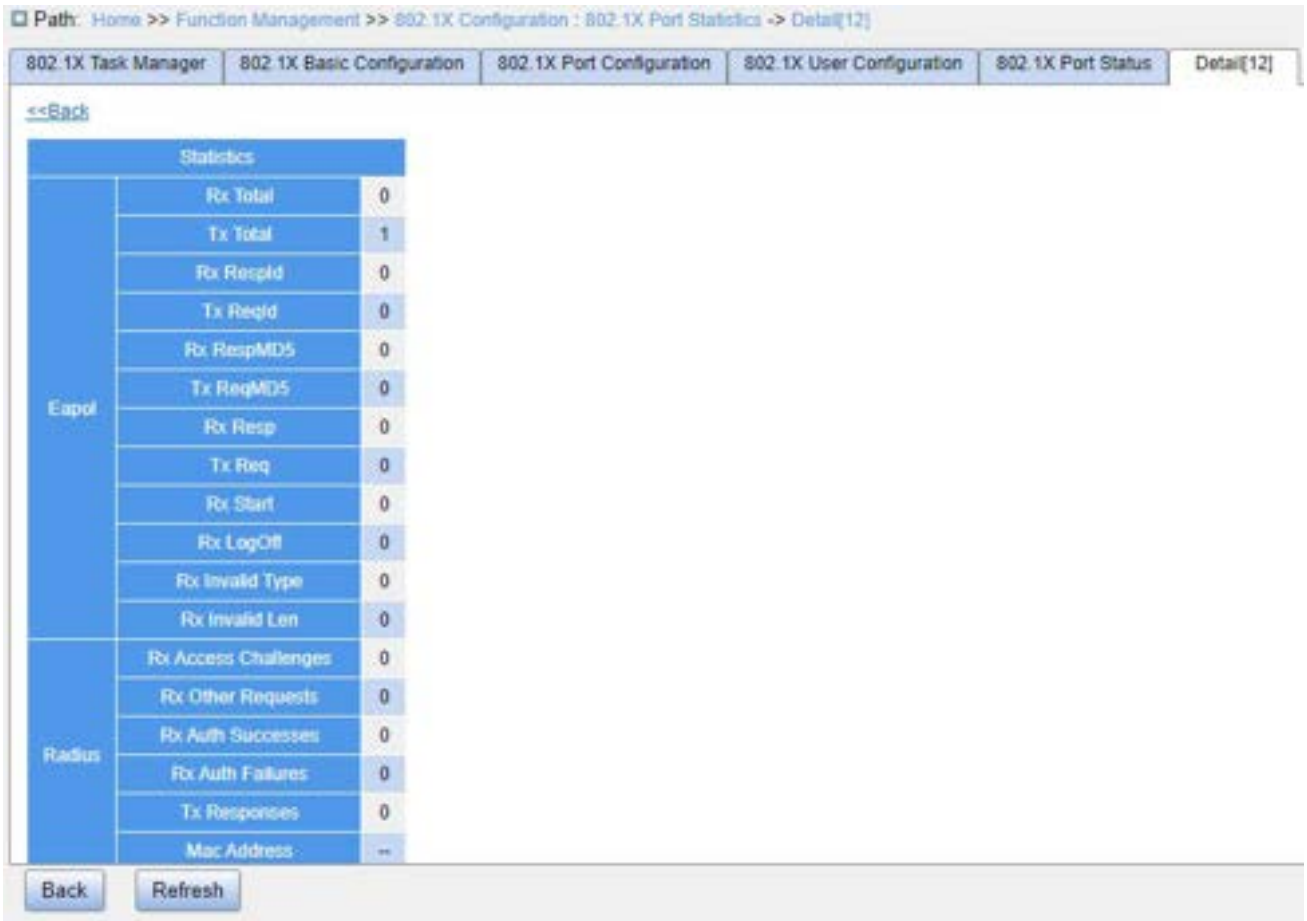


Figure 204 View detailed statistics of IEEE802.1X ports

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”, and the rest of the configuration are the default.

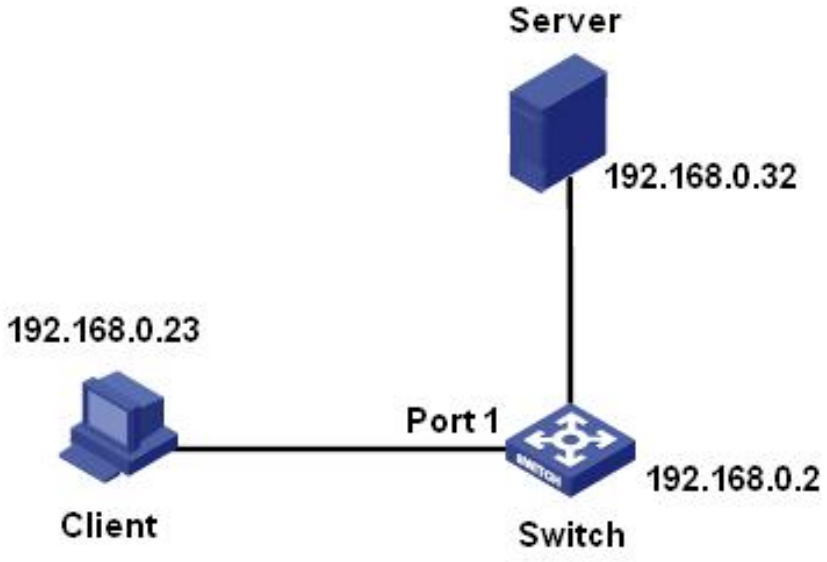


Figure 205 IEEE802.1x Configuration Example

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.

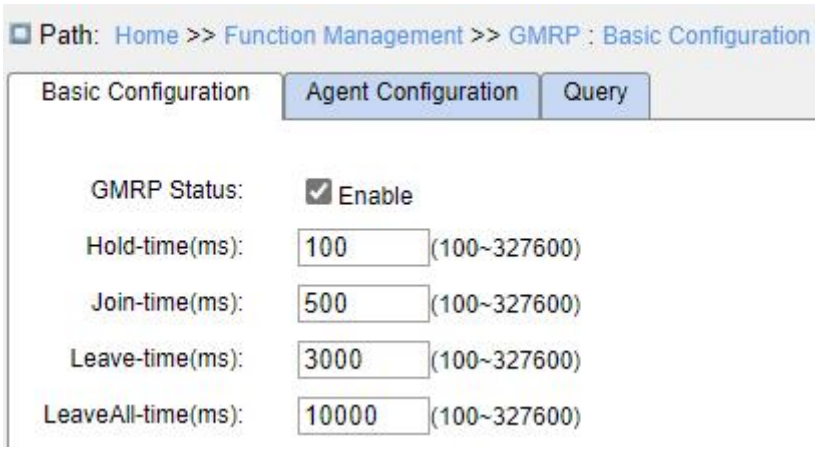


Figure 206 GMRP Global Configuration

GMRP Status

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable the global GMRP function. The function cannot be used together with the IGMP Snooping function.

Hold-time

Configuration range: 100~327600 ms

Default configuration: 100

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-time

Configuration range: 100~327600 ms

Default configuration: 500

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

Leave-time

Configuration range: 100~327600 ms

Default configuration: 3000

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

LeaveAll-time

Configuration range: 100 ms~327600 ms

Default configuration: 10000 ms

Function: The time interval for sending LeaveAll packets. The value must be a multiple of 100.

Description: 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 the GMRP function on port, as shown below.

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

Figure 207 Port GMRP Configuration

GMRP Enable

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable GMRP function on port.

GMRP Agent Enable

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable GMRP agent function on port.

Last PDU Origin

Function: Display 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.

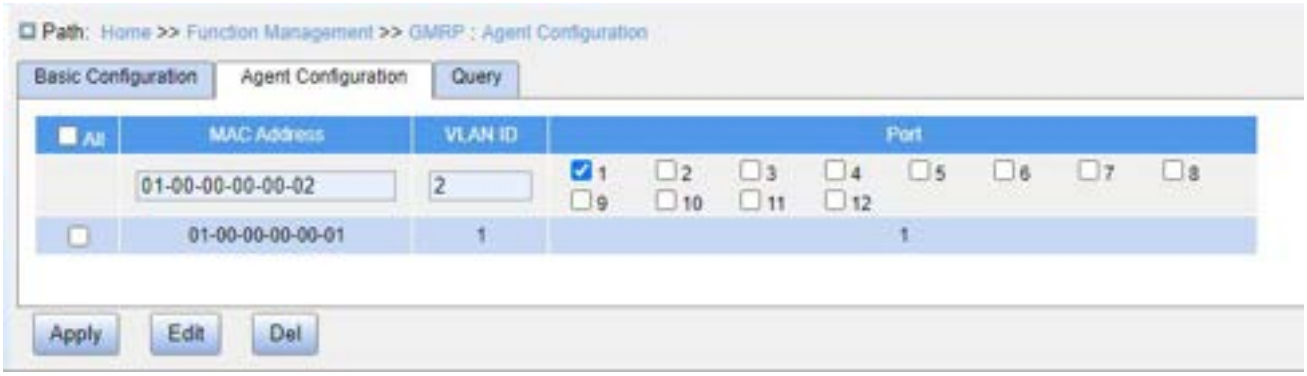


Figure 208 GMRP Agent Entry Configuration

MAC Address

Configuration 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.

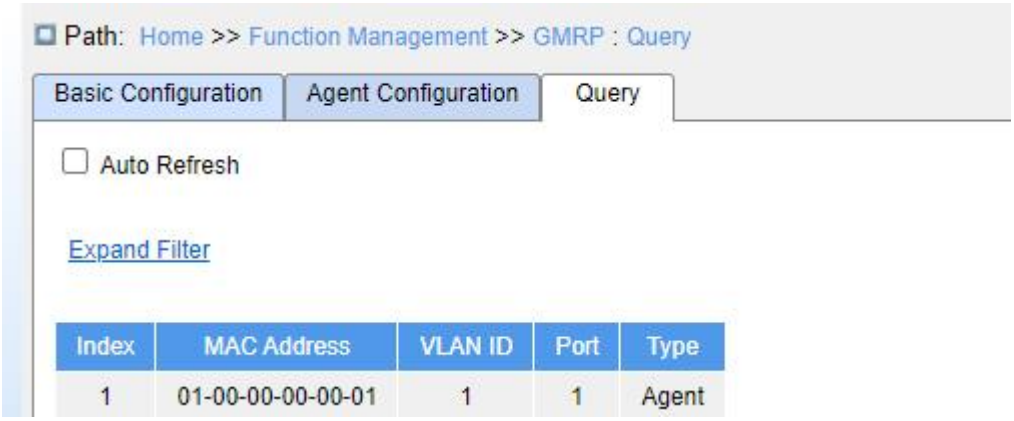


Figure 209 View GMRP Configuration Information

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.

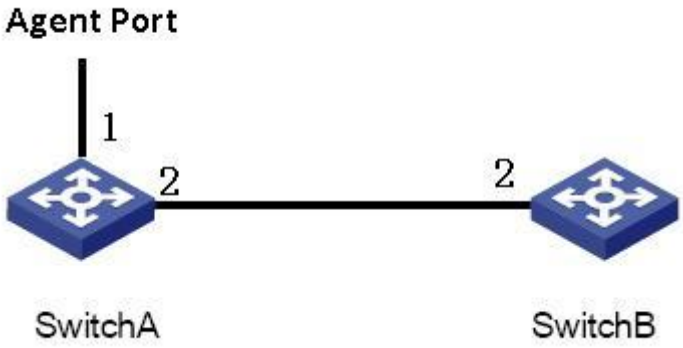


Figure 210 GMRP Networking

Configuration on Switch A:

1. Enable global GMRP function in switch A; set timer to the default value, as shown in Figure 206.

2. Enable GMRP function and agent function in port 1; enable only GMRP function in port 2; as shown in Figure 207.

3. Configure agent multicast entry. Set the 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 208.

Configuration on Switch B:

1. Enable global GMRP function in switch B; set timer to the default value, as shown in Figure 206.

2. Enable GMPR function in port 2; set the timers to default values, as shown in Figure 207.

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 PIM

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.

7.14.1 PIM-SM

7.14.1.1 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 the Shortest Point Tree (SPT), with the Rendezvous Point (RP) being the center.

Step 2: Switch to the SPT that is established between data receivers and a transmitter.

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

7.14.1.2 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-RPs) are configured by network administrators and one or more C-BSRs and C-RPs can be configured. The C-BSR with a higher priority is finally elected as the authentic BSR.

7.14.1.3 Working 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 neighbor relationships between routers to build and maintain SPT.

2. DR election:

Hello packets are also used to elect a DR for a shared network (such as Ethernet),

which acts 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, if other routers still fail to receive Hello packets from the DR after the timeout period, a new DR election process will be triggered.

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 in the PIM-SM domain to dynamically elect RPs through the bootstrap mechanism. A multicast group needs to be configured with a BSR. A BSR is the management core of a PIM-SM domain. A PIM-SM domain can have only one BSR, but multiple C-BSRs can be configured. In this way, once the BSR fails, the remaining C-BSRs can automatically generate a new BSR 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), encapsulates the RP-Set in the Bootstrap Message and publishes it to the entire PIM-SM domain.

Each router in the network selects the RP for a specific multicast group from multiple C-RPs based on the information provided by the RP-Set. The specific rules are as follows:

(1) First compare the priorities of the C-RPs, and the one 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 both the priorities and the 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 receiver information 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 the Join message passes from the DR to the RP form a branch of the RPT. These routers generate (*, G) entries in their forwarding tables, where "*" indicates any multicast sources. 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 deletes the interface connected to the downstream node after receiving the Prune message and check whether the receiver of the multicast group is available. If not, it continues 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, it will encapsulate the multicast data in the registration message and send it to the RP corresponding to the group in unicast mode. The RP router decapsulates the 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) message to the multicast source S. When being forwarded to the DR router of the multicast source hop by hop, each router along the path establishes 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 not to encapsulate the multicast data in the registration packet but to send it. This process is called the registration stop mechanism.

6. SPT switch:

When the multicast source is far away from the RP but 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 and then the receiver; therefore, the DR router sends a Join (S, G) message to the multicast source S. Each router along the path for transmitting the message establishes 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 along the SPT forwarding tree, it sends a Prune message to the RP router, telling it that the multicast data has been forwarded by the multicast source to the receiver through the SPT forwarding tree and the RPT forwarding tree is no longer needed. Then each router that forwards the Prune message along the path deletes the outbound interface corresponding to the (S, G) entry and updates the (*, G) entry.

SPT switching is not mandatory, 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.

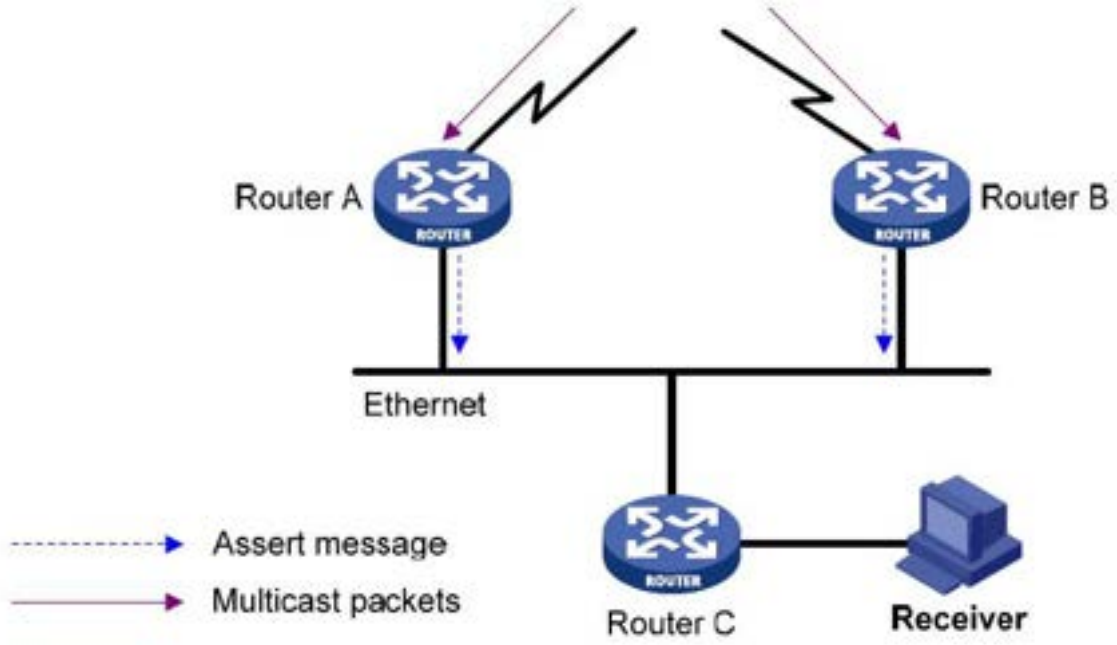


Figure 211 Assert mechanism diagram

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. Router A and Router B will also receive the multicast packet on their own local interface from each other. At this time, Router A and Router B send the Assert Message to all PIM routers (224.0.0.13) in the multicast mode from the local interface. The Assert Message carries the following information: multicast source address S, multicast group address G, the priority and metric of the unicast route to the multicast source. After the parameters are compared, the winner between Router A and Router B become the forwarder of the (S, G) multicast packets on the local network segment. The comparison rules are as follows:

(1) The one with 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.

7.14.1.4 Web Configuration

1. Configure basic parameters of PIM-SM, as shown below.

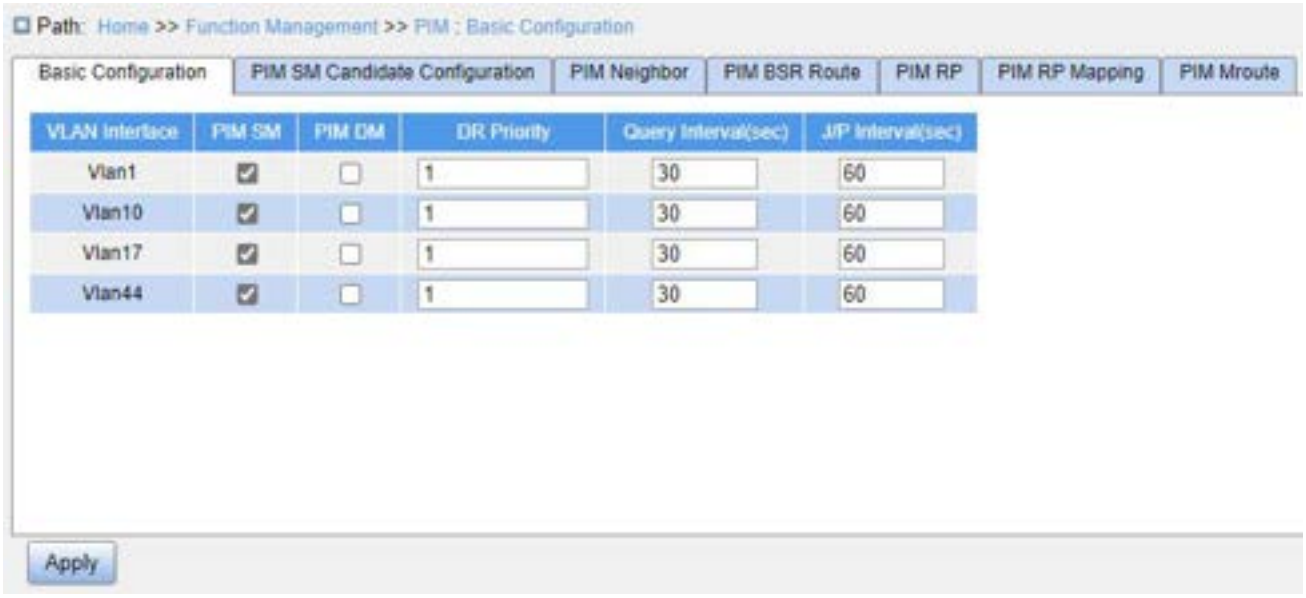


Figure 212 PIM-SM Basic Configuration

VLAN Interface

Configuration options: Created Layer 3 VLAN interfaces

PIM-SM

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable the PIM-SM function of the Layer 3 interface.

DR Priority

Configuration range: 0~4294967294

Default configuration: 1

Function: Configure the DR priority for the Layer 3 VLAN interface.

Query Interval

Configuration range: 1~18724s

Default configuration: 30

Function: Configure the interval for sending Hello packets on the Layer 3 interface to discover neighboring PIM routers.

J/P Interval

Configuration range: 1~65535s

Default configuration: 60

Function: Configure the interval at which the Layer 3 interface sends Join/Prune messages.

2. Configure PIM-SM candidates, as shown below.

Figure 213 PIM-SM Candidate Configuration

VLAN Interface

Configuration options: Created Layer 3 VLAN interfaces

BSR Candidate-Enable

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to configure the IP address of the VLAN interface as the candidate BSR address and send BSR messages to all of its PIM neighbors.

BSR Candidate-Hash Mask Length

Configuration range: 0~32

Default configuration: 32

Function: Configure the hash mask length.

Description: The hash mask length refers to the number of preceding 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: Whether to configure the IP address of the VLAN interface as the candidate RP address. This address will be used to receive registration messages and Join/Prune messages and to establish a forwarding tree.

RP Candidate-RP Interval

Configuration range: 1~16383s

Default configuration: 60

Function: Configure the interval for the candidate RP to send notification packets to the BSR.

BSR Border

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to configure the VLAN interface that has joined the PIM-SM network as the PIM-SM BSR border.

Note:

- All multicast groups with the same hash mask length communicate with the same RP. For example, if the hash mask length is set to 20, multicast groups with the same former 20 bits in their multicast addresses share the same RP.
- A larger priority value indicates a lower priority. The C-BSR with the highest priority is the authentic BSR. If C-BSRs share the same priority, the C-BSR with the highest IP address is the authentic BSR.

3. View PIM neighbors, as shown below.

Figure 214 Display PIM Neighbor Interface

The fields in the display information are described in the following table.

Table 11 Description of Each Field of PIM Neighbor

VLAN Interface	The Layer 3 VLAN interface through which the corresponding multicast group will be reached
Local Address	IP address of the VLAN interface
Query Interval(sec)	Interval at which Hello packets are sent from the VLAN interface
J/P Interval(sec)	Interval at which Join/Prune messages are sent from the VLAN interface
Neighbor Address	IP address of the VLAN interface's PIM neighbor
Neighbor Uptime	Uptime of the VLAN interface's PIM neighbor, in "hour:minute:second" format
Neighbor Expires	Remain time length after which the VLAN interface's PIM neighbor will expire, in "hour:minute:second" format

4. View PIM BSR route information, as shown below.

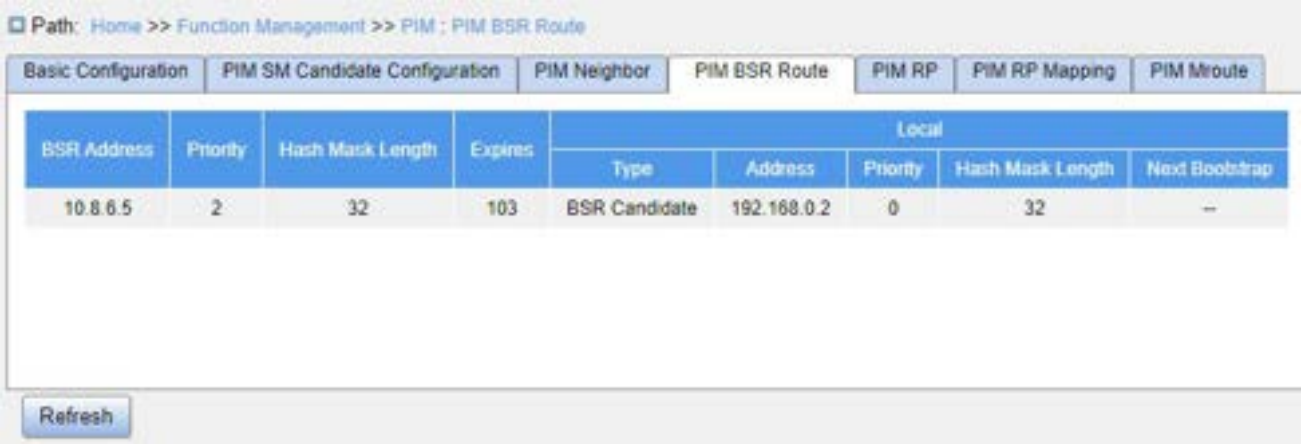


Figure 215 PIM BSR Routing Interface

The fields in the display information are described in the following table.

Table 12 Description of Each Field of PIM BSR Route

BSR Address	IP address of BSR on the current network
Priority	Priority of the BSR
Hash Mask Length	Hash mask length of the BSR
Expires	Remaining time length after which the BSR will expire (seconds)
Local Type	Type of the candidate BSR (BSR or BSR candidate) on this switch
Local Address	IP address of the candidate BSR on this device (no display for the elected BSR)
Local Priority	Priority of the candidate BSR on this device (no display for the elected BSR)
Local Hash Mask Length	Hash mask length of the candidate BSR on this device (no display for the elected BSR)
Local Next Bootstrap	Remaining time length after which the BSR on this device sends the next Bootstrap packet (no display for the elected BSR)

5. View PIM RP information, as shown below.

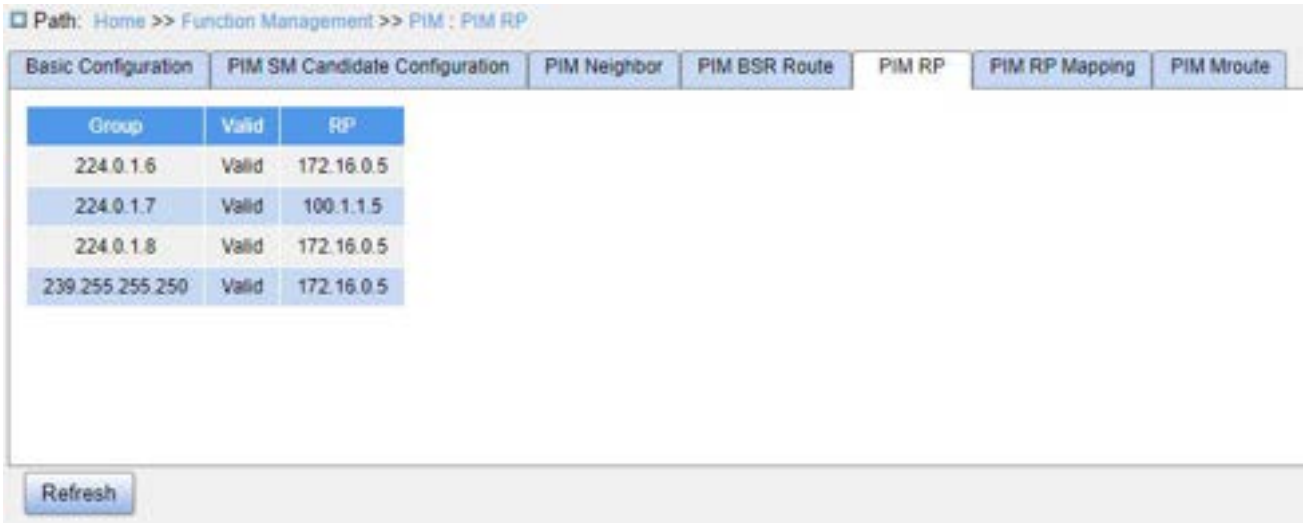


Figure 216 PIM RP information

The fields in the display information are described in the following table.

Table 13 Description of Each Field of PIM RP

Group	IP address of the multicast group
Valid	Whether RP is valid or not
RP	IP address of the RP corresponding to the multicast group

6. View PIM RP mapping information, as shown below.

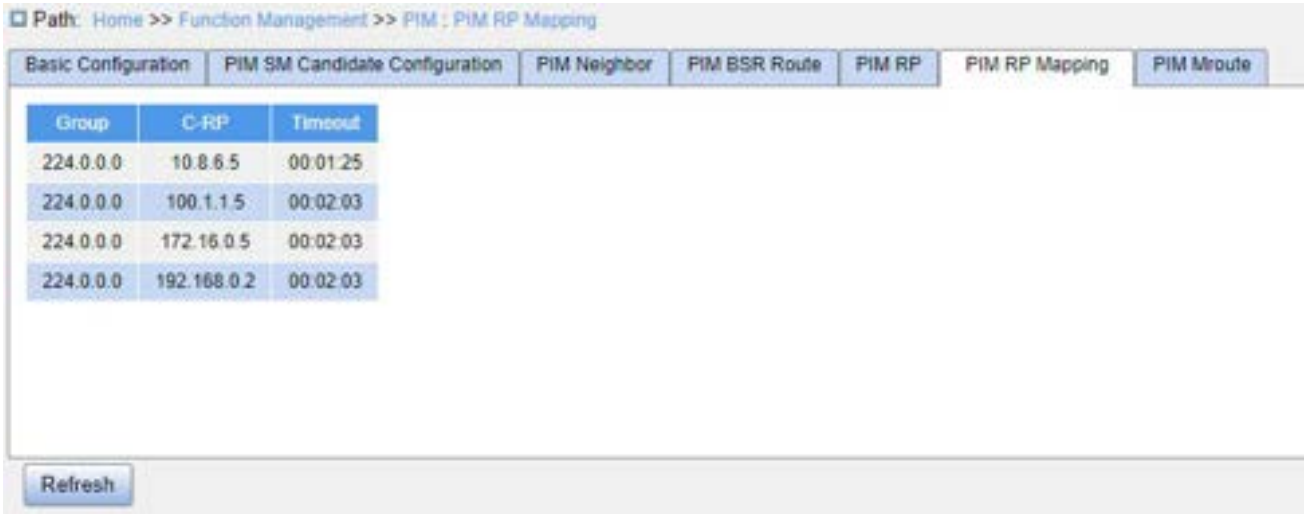


Figure 217 PIM RP Mapping Information

The fields in the display information are described in the following table.

Table 14 Description of Each Field of PIM RP Mapping

Group	IP address of the multicast group

C-RP	IP address of the C-RP corresponding to the multicast group
Timeout	Remaining time length after which the C-RP will time out, in "hour:minute:second" format

7. View PIM Mroute information, as shown below.

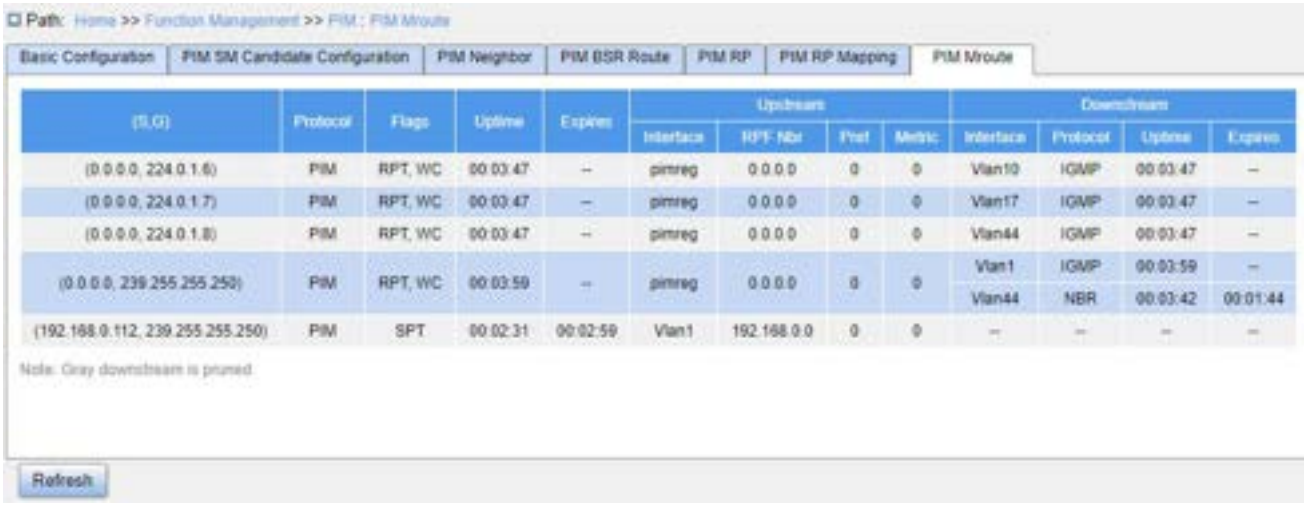


Figure 218 PIM Mroute information

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	Uptime of (*, G) or (S, G) entries
Expires	Remaining time length after which the (*, G) or (S, G) entry will expire
Upstream Interface	Ingress interface of the (S, G) or (*, G) entry For the (*, G) entry, the ingress interface is the one facing the RP. For the (S, G) entry, the ingress interface is the one facing S.
Upstream RPF Nbr	RPF neighbor of the (S, G) or (*, G) entry The RPF neighbor of (*, G) is the interface facing the RP. The RPF neighbor for (S, G) is the interface facing S. For the (*, G) entry, when the router is an RP, the RPF neighbor of

	the entry is 0.0.0.0. For the (S, G) entry, when the router is directly connected to the source, the RPF neighbor of the entry is 0.0.0.0.
Upstream Pref	Management distance of the RPF neighbor route for the (S, G) or (*, G) entry
Upstream Metric	Route cost of the RPF neighbor route for the (S, G) or (*, G) entry
Downstream Interface	Egress interface for the (S, G) or (*, G) entry
Downstream Protocol	Type of protocol used by the downstream interface
Downstream Uptime	Existence time of the downstream interface
Downstream Expires	Remaining time length after which the downstream interface will time out

7.14.1.5 Typical Configuration Example

As shown below, Router1, Router2, Router3, Router4 have PIM-SM protocol enabled, S means source and R means receivers.

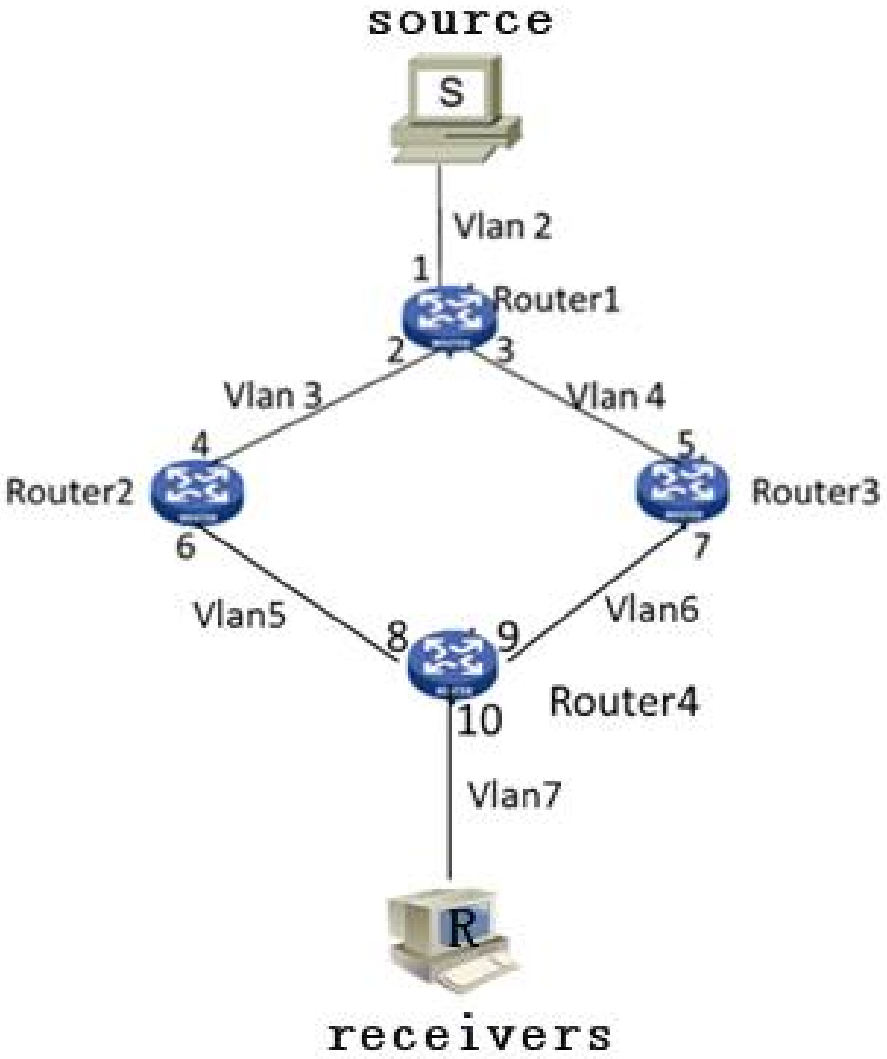


Figure 219 PIM SM Example

1. Configure router IDs and enable the Open Shortest Path First (OSPF) protocol. For the detailed configuration process, see "7.16.3 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 IP 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 213.

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 213.

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 213.

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 213.

6. Configure the BSR border (optional): as shown in Figure 214, set the Layer 3 interface as PIM-SM BSR border.

7. Configure the C-BSR: as shown in Figure 214, 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 214, 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.

7.14.2 PIM-DM

7.14.2.1 Introduction

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, keeping only the branch containing the receiver. This "Flooding-pruning" phenomenon occurs periodically, and the pruned branches can also be periodically restored to the forwarding state.

When the member of the multicast group appears on the node to be pruned, 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).

7.14.2.2 Working Principle

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 a multicast message to the multicast group G, it first floods the multicast message. After the router performs the RPF check on the message, it creates a (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 PIM-DM prunes the downstream nodes that have no receivers. The downstream node without receivers sends a Prune Message to the upstream node to notify the upstream node to delete the corresponding egress interface of the multicast forwarding entry (S, G), and will not forward the packets of this multicast group 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 receivers initiates pruning and continues pruning until only necessary branches are left in the PIM-DM domain. These necessary branches together form the SPT.

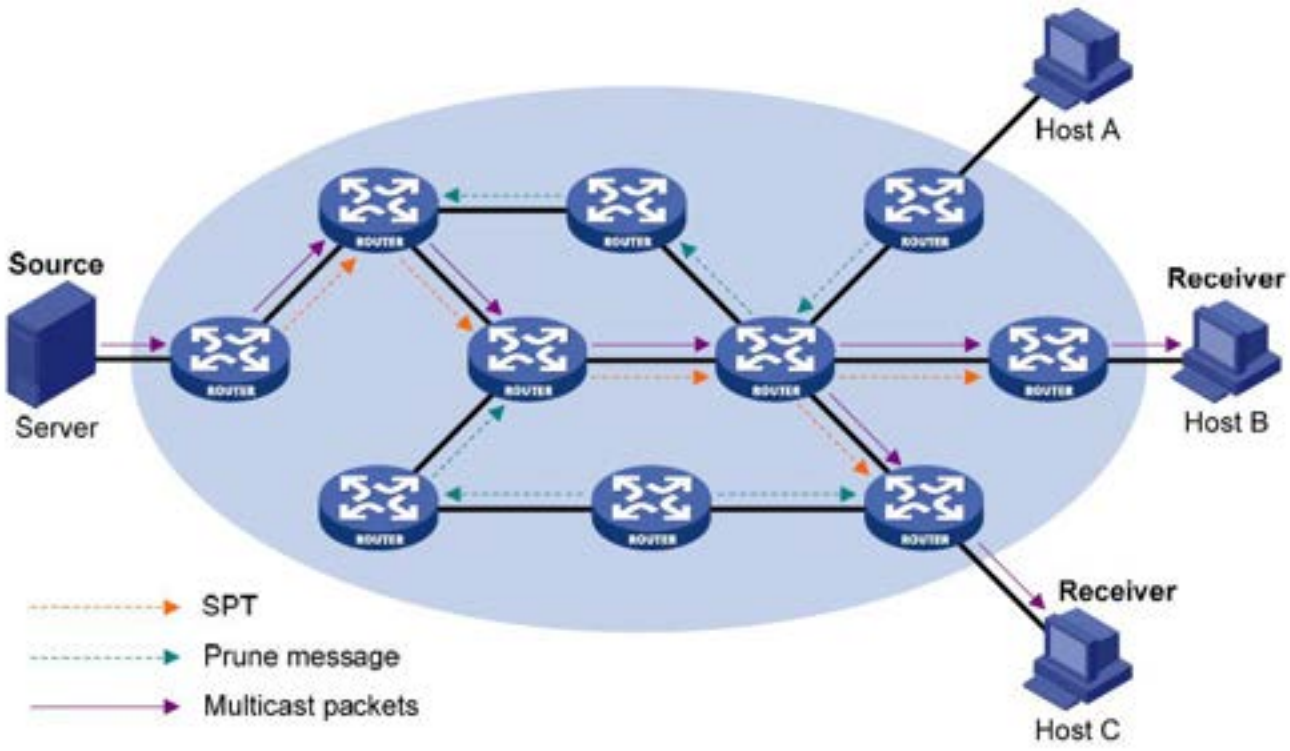


Figure 220 Schematic Diagram for Building SPT in PIM-DM

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. Graft:

When the member of a multicast group appears on the node being pruned, in order to reduce the time required for the node to recover to the forwarding state, PIM-DM uses the Graft 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 7.14.1.3 Working Principle for details.

7.14.2.3 Web Configuration

1. Configure PIM-DM, as shown below.

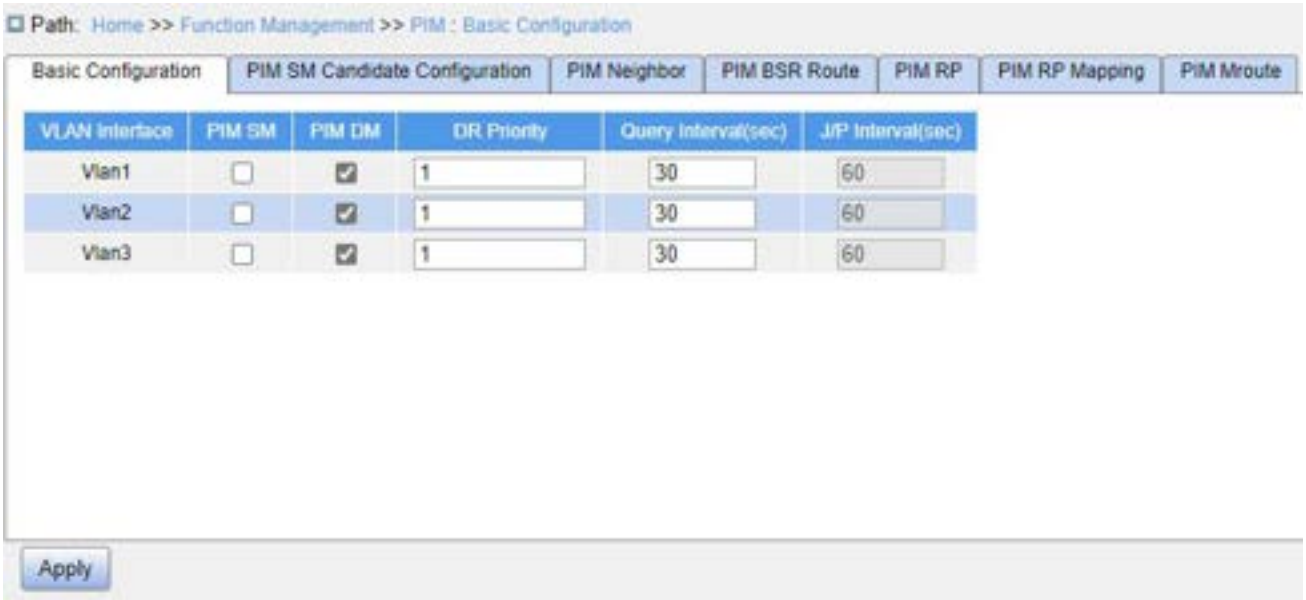


Figure 221 Basic Configuration of PIM-DM

VLAN Interface

Configuration options: Created Layer 3 VLAN interfaces

PIM-DM

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable the PIM-DM function of the Layer 3 interface.

DR Priority

Configuration range: 0~4294967294

Default configuration: 1

Function: Configure the DR priority of the Layer 3 VLAN interface.

Query Interval

Configuration range: 1~18724s

Default configuration: 30

Function: Configure the interval for sending Hello packets on the Layer 3 interface to discover neighboring PIM routers.

2. View PIM neighbor information.

This is similar to PIM-SM. See section 7.14.1.4.

3. View PIM Mroute information.

This is similar to PIM-SM. See section 7.14.1.4.

7.14.2.4 Typical Configuration Example

As shown below, Router1, Router2, Router3, Router4 can support the PIM-SM protocol, S means source and R means receivers.

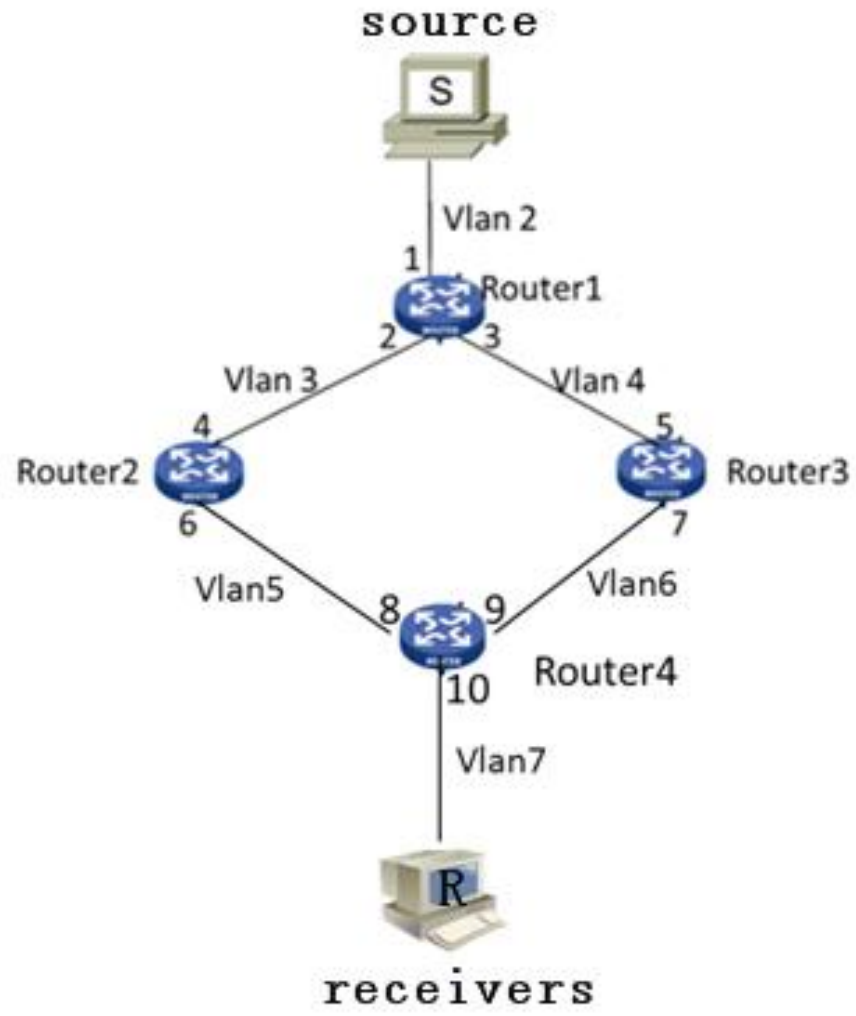


Figure 222 PIM DM Example

1. Configure router IDs and enable the Open Shortest Path First (OSPF) protocol. For the detailed configuration process, see "7.16.3 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 IP 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 221.

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 221.

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 221.

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 221.

6. View the PIM neighbor and PIM routing forwarding table. For details, see Web Configurations for information.

7.15 IGMP

7.15.1 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 smaller IP address as the querier. IGMPv1 does not have the querier election mechanism. Different routing protocols use different election mechanisms.

(2) IGMPv2 is added a Leave Group message. When a host leaves a group, the host actively sends the Leave Group message. IGMPv1 does not actively sends the Leave Group message.

(3) Max Resp Time: a new field added to the Query message. 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.

7.15.2 Working 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 smaller, it abandons its querier role and becomes a non-querier. A router with the smallest 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.

7.15.3 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.

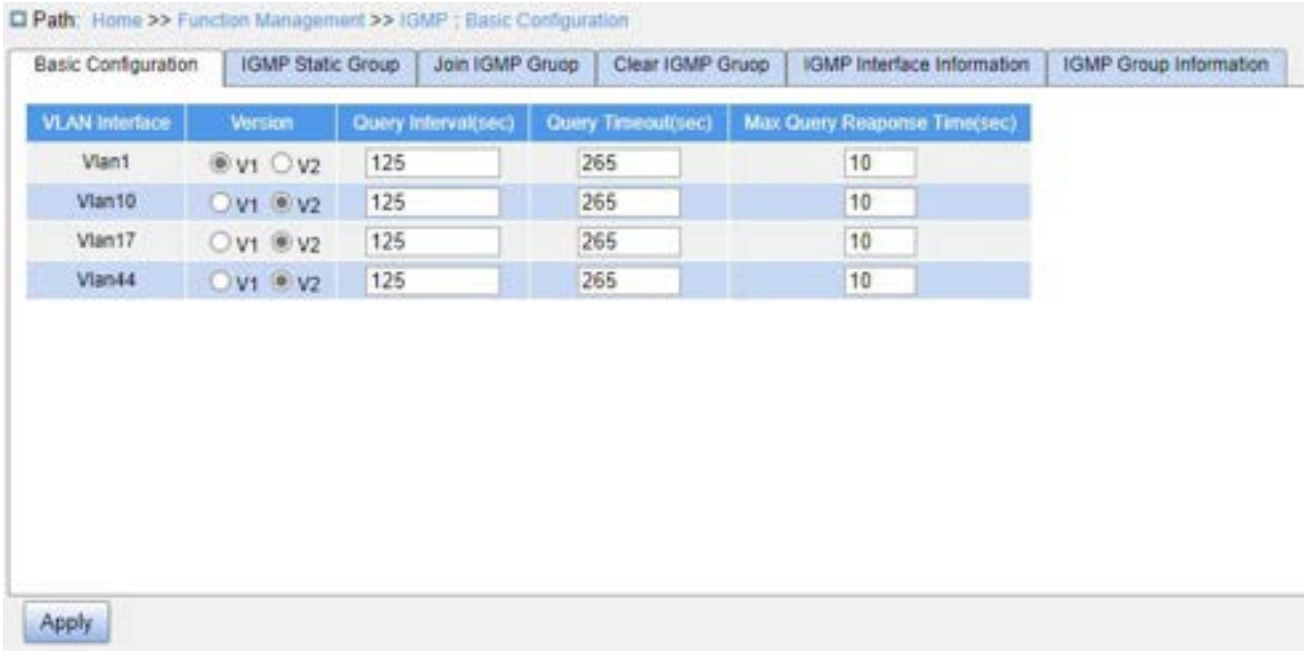


Figure 223 Basic configuration of IGMP

VLAN Interface

Configuration options: Created Layer 3 VLAN interfaces

Version

Configuration options: v1/v2

Default configuration: v2

Function: Configure the interface to run IGMP v1 or IGMP v2.

Query Interval

Configuration range: 1~65535s

Default configuration: 125

Function: Configure the interval at which the IGMP querier sends Query messages.

Query Timeout

Configuration range: 60~300s

Default configuration: 265

Function: Configure the timeout value for sending IGMP Query messages.

Description: If a non-querier fails to receive the Query message from the querier within the specified timeout period, the interface on the non-querier automatically becomes the

querier. This interval is called timeout time. In general, the timeout value equals twice the query interval plus the maximum response time.

Max Query Response Time

Configuration range: 1~25s

Default configuration: 10

Function: Configure the maximum response time that the interface response to an IGMP Query message.

Description: When there are hosts willing to join a multicast group indicated in the Query message, the first host must respond to the Query message with a Member Report message within the maximum response time. If not, the querier deems that the branch has no member and this branch will be pruned.

3. Configure IGMP static groups, as shown below.

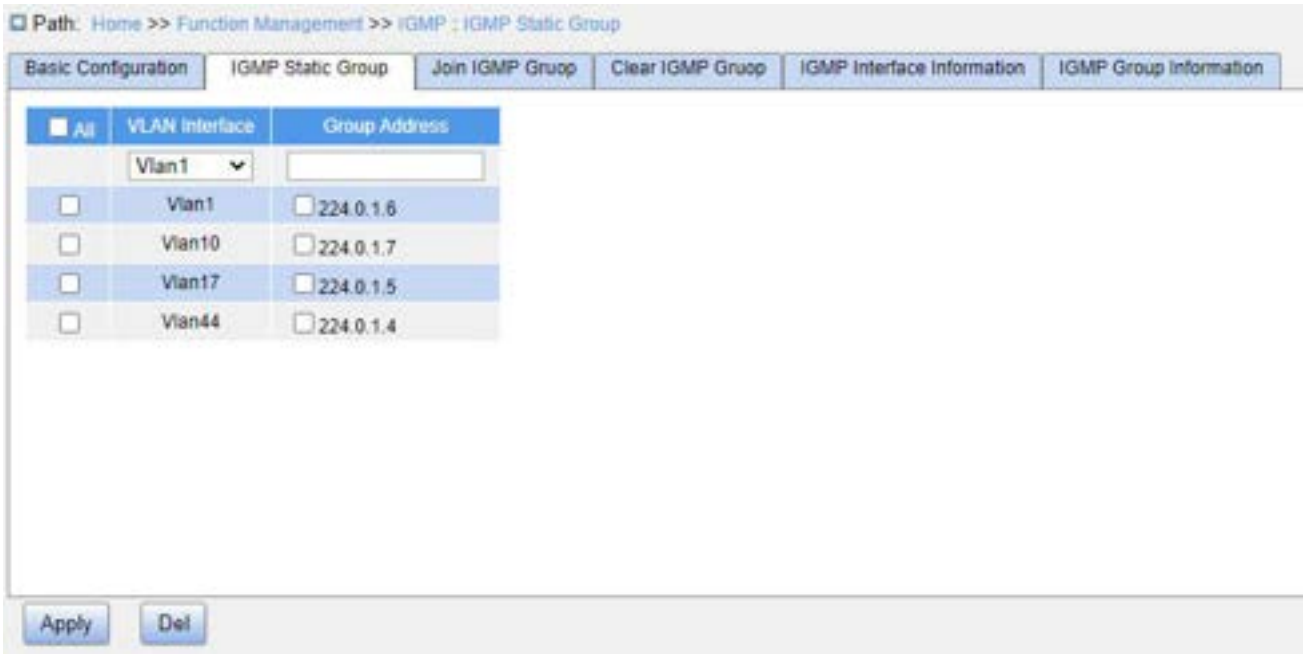


Figure 224 Configure an IGMP Static Group

VLAN ID

Configuration options: Created Layer 3 VLAN interfaces

Default configuration: VLAN 1

Function: Select the Layer 3 interface to be configured.

Group Address

Format: A.B.C.D

Function: Specify the IP address of the multicast group.

4. Configure the VLAN interface to join IGMP groups, as shown below.

Figure 225 Configure VLAN Interface to Join IGMP Group

VLAN Interface

Configuration options: Created Layer 3 VLAN interfaces

Default configuration: VLAN 1

Function: Select the Layer 3 interface to be configured.

Group Address

Format: A.B.C.D

Function: Specify the IP address of the multicast group that the VLAN interface will join.

By default, no multicast member is defined for a multicast group.

5. Clear the IGMP group information, as shown below.

Figure 226 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 clear IGMP dynamic group information.

6. View IGMP interface information, as shown below.

Figure 227 View 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 VLAN interface
Enable Status	IGMP enabled status of the VLAN interface
Querier	IP address of the querier for the VLAN interface, and "Local" indicates the querier is the device itself.
Current Version	IGMP version of the VLAN interface
Query Timer (sec) - Interval	IGMP Query interval of the VLAN interface
Query Timer (sec) - Timeout	IGMP Query Timeout value of the VLAN interface
Query Timer (sec) - Max Response Time	Maximum response time for IGMP Query message on the VLAN interface
TTL Threshold	TTL threshold of the IGMP messages on the VLAN interface. The IGMP messages carrying a threshold exceeding the threshold are not processed.
DR	IP address of the DR for the VLAN interface
Joined Group(s)	IP address of multicast groups that the VLAN interface has joined

7. View IGMP group information, as shown below.

Figure 228 View 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 interface through which the corresponding multicast group will be reached
Group Address	IP address of the multicast group
Uptime	Uptime of the multicast group, in "hour:minute:second" format
Expires	Remaining time length after which the multicast group will expire, in "hour:minute:second" format. “stopped” means the multicast group never times out.
Last Reporter	IP address of the last host that join the multicast group

7.16 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.

7.16.1 Routing Table

7.16.1.1 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.

7.16.1.2 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 bits 1. It can be expressed in dotted decimal format or by the number of bits 1.
- 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.

7.16.1.3 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.

7.16.1.4 Web Configuration

1. Configure static routing, as shown below.

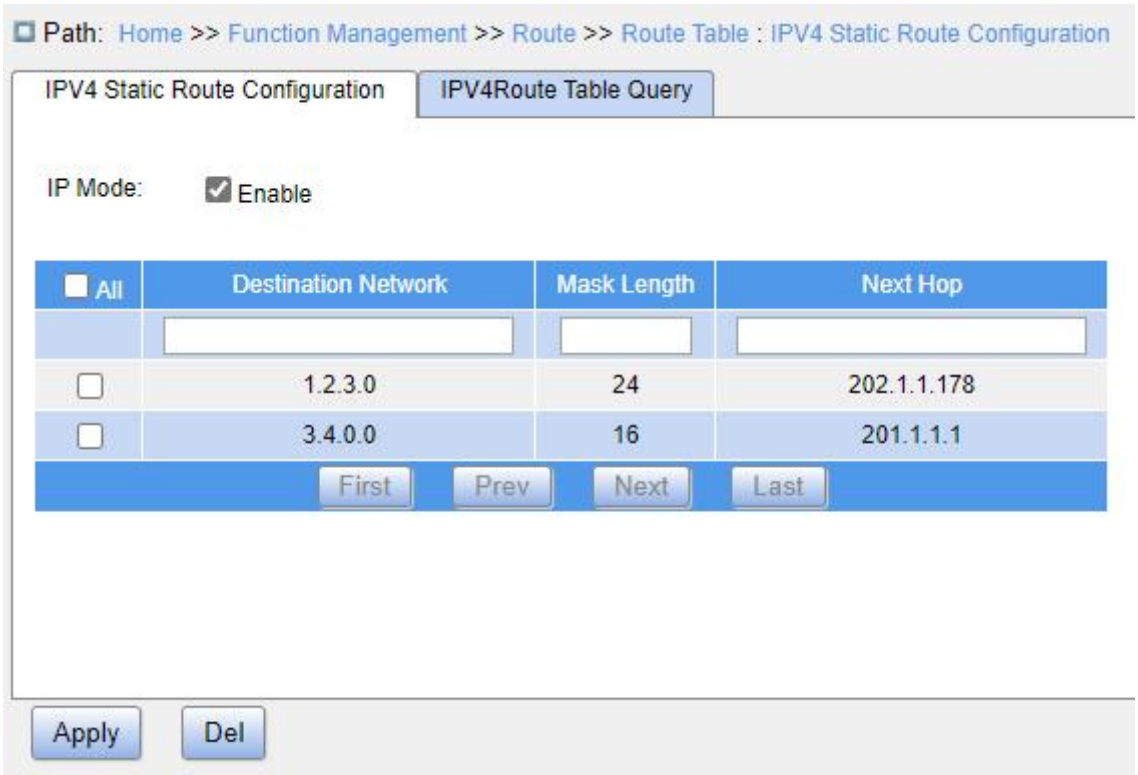


Figure 229 Static Routing Configuration

IP Mode

Configuration options: Enable/Disable

Default configuration: Enable

Function: Whether to enable IP mode.

Destination Network

Configuration format: A.B.C.D

Function: Configure the target network address in the static route table.

Mask Length

Configuration range: 1~32

Function: Configure the subnet mask of the target network address.

Description: A subnet mask is a 32-bit string, consisting a sequence of bits 1 and a sequence of bits 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 bits 1 in the mask.

Next Hop

Configuration format: A.B.C.D

Function: Configure the next hop IP address.

2. View IPv4 routing table, as shown in the following figure.

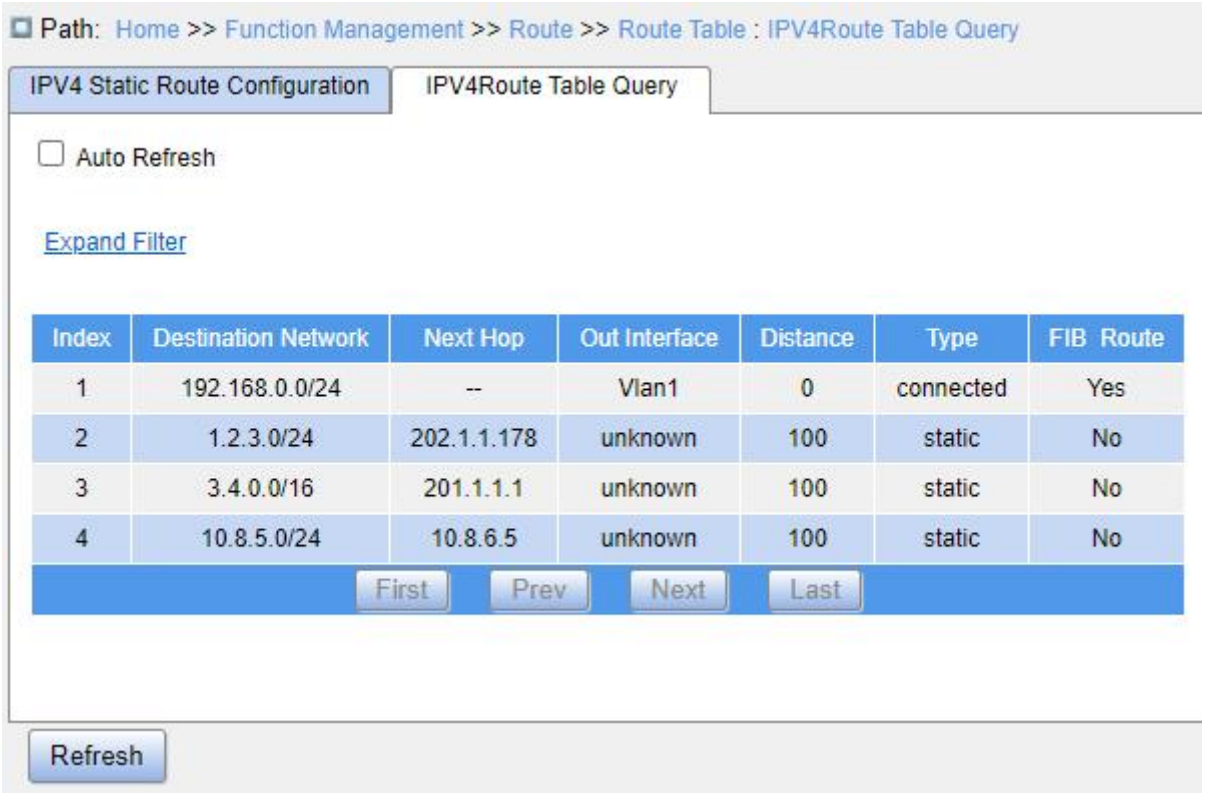


Figure 230 View Routing Table

7.16.1.5 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.

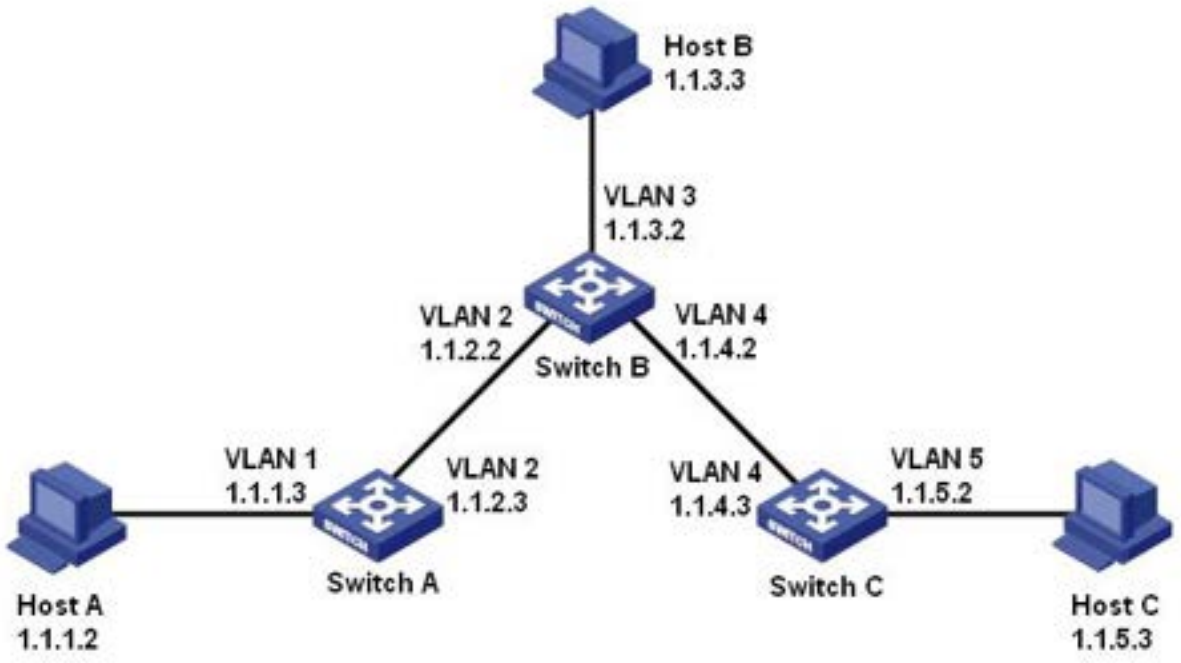


Figure 231 Example for Configuring Static Routes

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; next hop: 1.1.2.2, as shown in Figure 229.

Destination IP address: 1.1.5.0; destination network mask: 255.255.255.0; next hop: 1.1.2.2, as shown in Figure 229.

Configuration on Switch B:

1. Set IP addresses for VLAN interfaces.

2. Configure a static route with the following parameters:

Destination IP address: 1.1.1.0; destination network mask: 255.255.255.0; next hop: 1.1.2.3, as shown in Figure 229.

Destination IP address: 1.1.5.0; destination network mask: 255.255.255.0; default gateway: 1.1.4.3, as shown in Figure 229.

Configuration on Switch C:

1. Set IP addresses for VLAN interfaces.

2. Configure a static route with the following parameters:

Destination IP address: 0.0.0.0; destination network mask: 0.0.0.0; next hop: 1.1.4.2, as shown in Figure 229.

3. 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.

7.16.2 RIP

7.16.2.1 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 Layer 3 switch that runs RIP has a routing database. The routing database contains routing entries to all reachable destinations of this Layer 3 switch based on which a routing table is established. When a Layer 3 switch running RIP sends route update packets to its neighboring devices, this packet carries the entire routing table established by this Layer 3 switch based on routing database. Therefore, on a large-scale network, each Layer 3 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 checked. 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 a 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 messages in multicast mode, receives RIP-1 and RIP-2 messages.

RIP uses the 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.

7.16.2.2 Routing Loops Prevention

On a network running RIP, when an RIP route becomes unreachable, the RIP Layer 3 switch will not send a route update packet immediately until the route update interval (30s) elapses. If a neighboring Layer 3 switch sends a packet carrying its own routing table information to the Layer 3 switch before a route update packet is received, infinite counting will occur. That is, the metric for selecting a route to the unreachable Layer 3 switch increases incrementally. This affects the routing time and route aggregation time remarkably.

To avoid infinite counting, RIP provides the split horizon mechanism 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 broadcasted immediately without considering the status of the 30-second update timer.

7.16.2.3 Operation

After RIP is enabled, the router sends request messages to neighboring routers.

Neighboring routers return response messages including information about their routing tables.

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 latest routing information.

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 a Layer 3 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.

7.16.2.4 Web Configuration

1. Configure basic RIP parameters, as shown below.

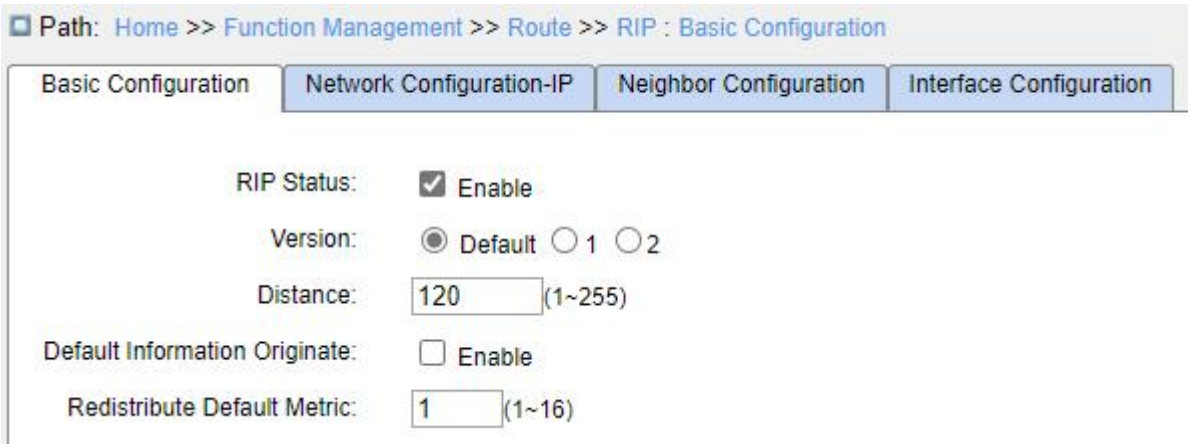


Figure 232 Basic RIP Configuration

RIP Status

Configuration options: Enable/disable

Default configuration: Disable

Function: Whether to enable RIP.

Version

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. The value 1 indicates that all interfaces of the Layer 3 switch send/receive RIP-1 packets. The value 2 indicates that all interfaces of the Layer 3 switch send/receive RIP-2 packets.

Distance

Configuration range: 1~255

Default configuration: 120

Function: Specify 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 in the core routing table.

Default Information Originate

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable broadcasting of the default route.

Redistribute Default Metric

Configuration range: 1~16

Default configuration: 1

Function: Configure the default route metric for importing external routes.

2. Configure route redistribution, as shown in the following figure.

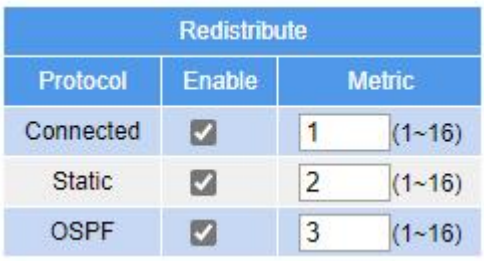


Figure 233 Redistribution Configuration

Protocol

Configuration options: Connected/Static/OSPF

Enable

Configuration options: Enable/Disable

Default configuration: Disable

Function: Routes generated by other protocols are redistributed in RIP. Only routes with the active route status can be imported.

Metric

Configuration range: 1~16

Default configuration: 1

Function: Configure the metric of the imported route. This parameter is an optional configuration item. If this parameter is not configured, the default metric for redistribution will be adopted.

3. Configure timers, as shown in the following figure.

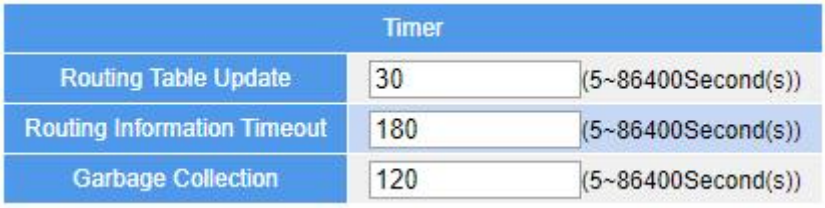


Figure 234 Timer Configuration

Routing Table Update

Configuration range: 5~86400s

Default configuration: 30

Function: Configure the interval at which RIP sends update packets.

Routing Information Timeout

Configuration range: 5~86400s

Default configuration: 180

Function: Configure the RIP route timeout period. If no routing table update information is received from a neighbor in this period, all routes from the device are regarded as invalid routes, and the route enters the suppression state. The route timeout value should be greater than the route update time.

Garbage Collection

Configuration range: 5~86400s

Default configuration: 120

Function: Configure the time length that the RIP routes are 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. Enable RIP for networks, as shown in the following figure.

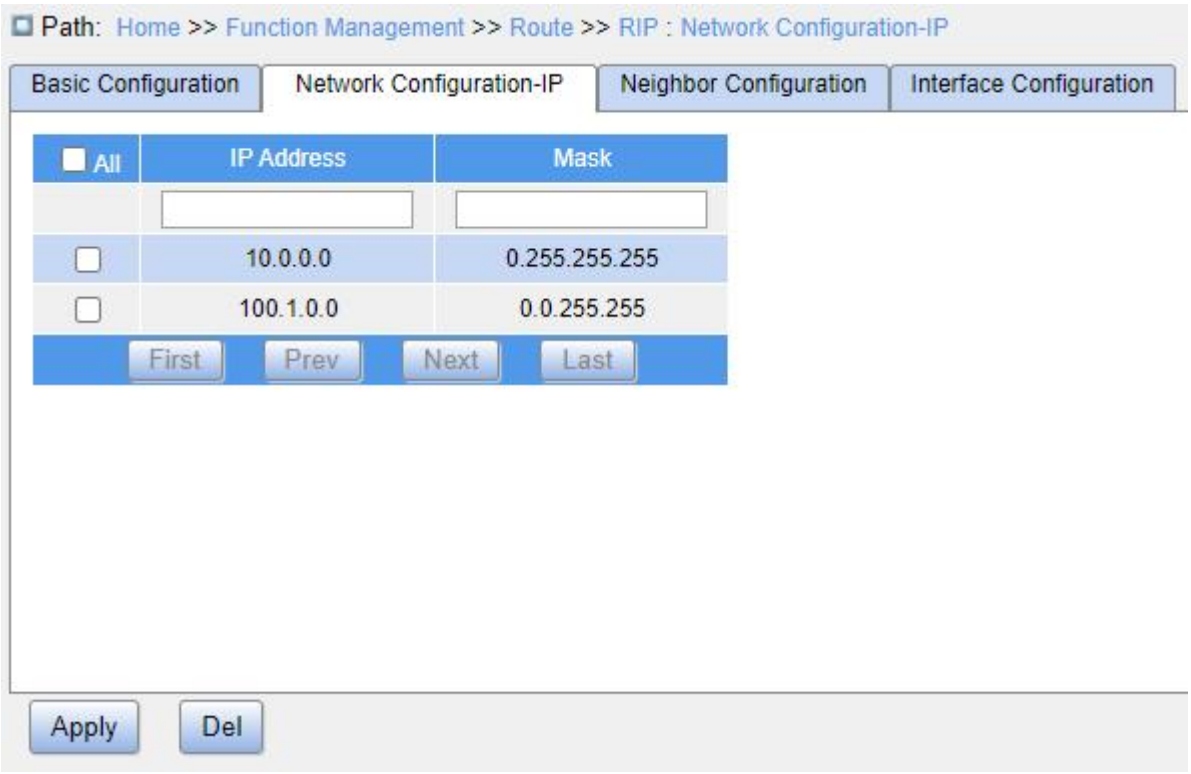


Figure 235 Network configuration

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: Configure the wildcard mask for the IP address. In the mask, 1 indicates the bits that need to be matched, and 0 indicates the bits that do not need to be matched.

Description: 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. Configure RIP neighbors, as shown in the following figure.

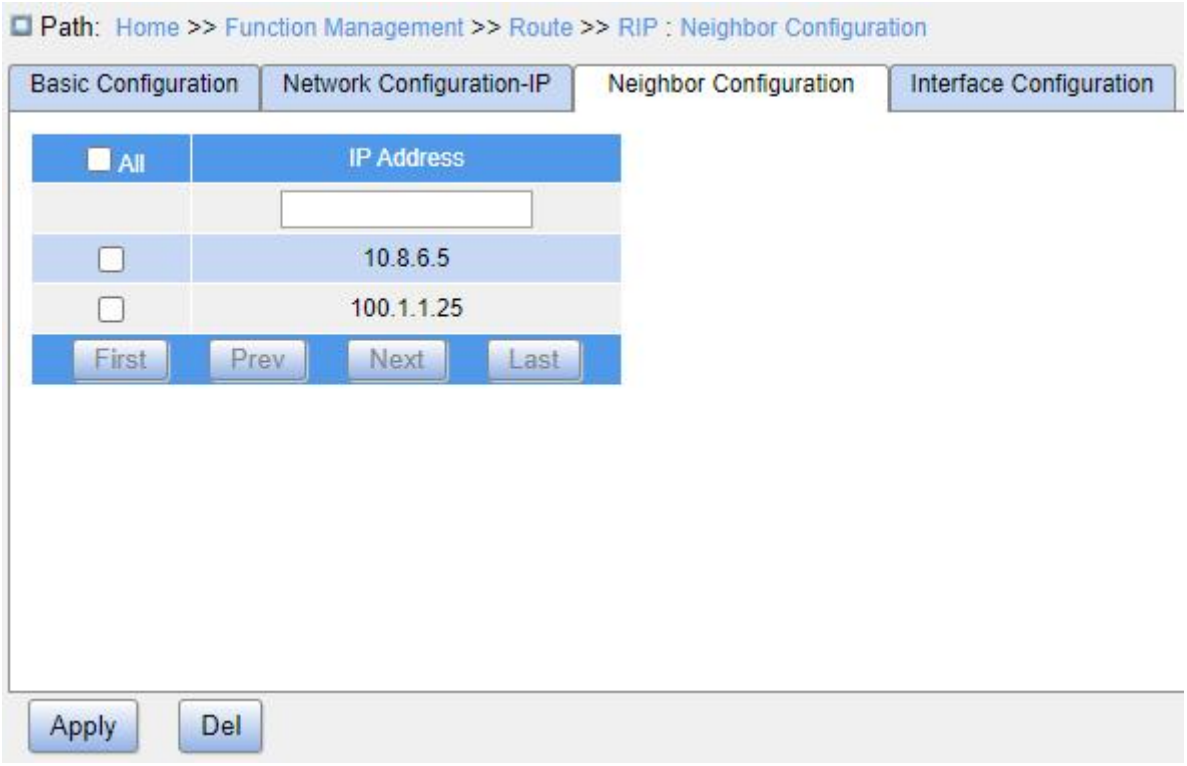


Figure 236 Neighbor Configuration

IP Address

Configuration format: A.B.C.D

Function: Configure the neighbor device IP address.

6. Configure RIP interfaces, as shown in the following figure.

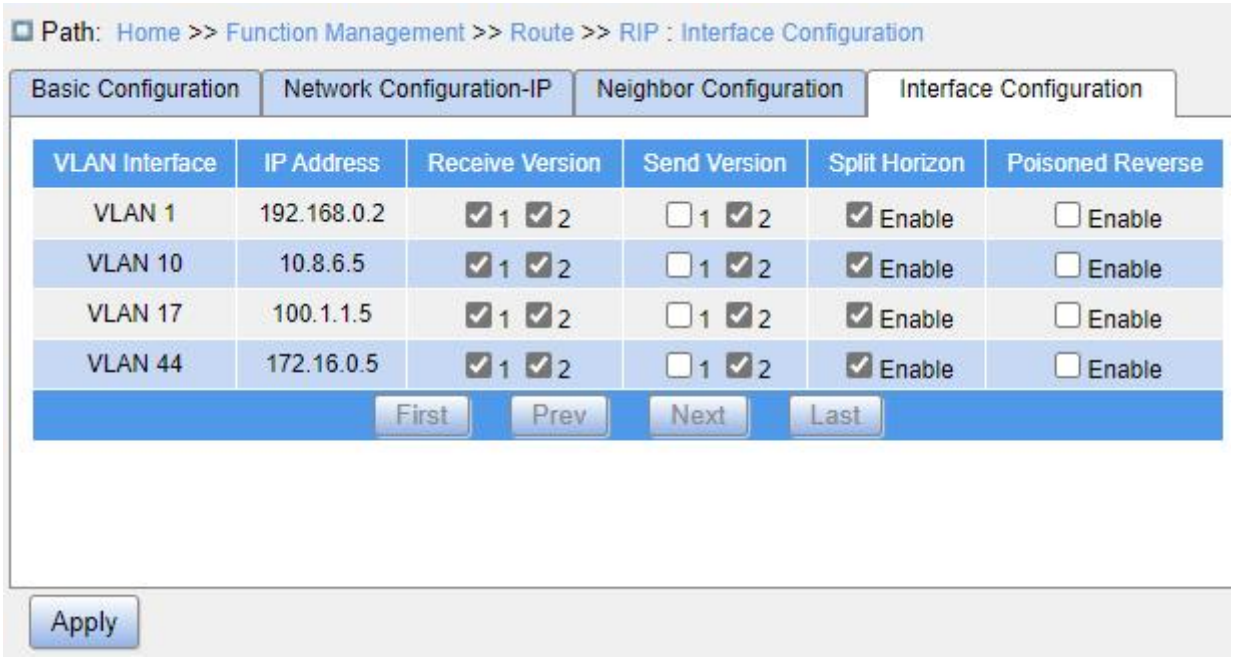


Figure 237 Interface Configuration

VLAN Interface

Configuration options: All created VLAN interfaces

IP Address

Function: Display the IP address of the VLAN interface.

Receive Version

Configuration options: 1/2

Default configuration: 1 and 2

Function: Configure the version of RIP packets that the VLAN interface supports to receive. 1 means RIP-1 messages. 2 means RIP-2 messages. If both are checked, the interface can receive RIP-1 and RIP-2 messages.

Send Version

Configuration options: 1/2

Default configuration: 2

Function: Configure the version of RIP packets that the VLAN interface supports to send. 1 means RIP-1 messages. 2 means RIP-2 messages. If both are checked, the interface can send RIP-1 and RIP-2 messages.

Split Horizon

Configuration options: Enable/Disable

Default configuration: Enable

Function: Whether to enable split horizon. Horizontal splitting is used to prevent routing loops, that is, preventing Layer 3 switches from sending routes via the same interface where the route is learned.

Poisoned Reverse

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable poisoned reverse.

Description: With poisoned reverse enabled, the routes learned via an interface can be sent out from this interface, but the route metric will be set to 16 (unreachable), so as to prevent routing loops between adjacent routers.

7.16.2.5 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 run RIP routing protocol. The network masks of all switches on the network are 255.255.255.0.

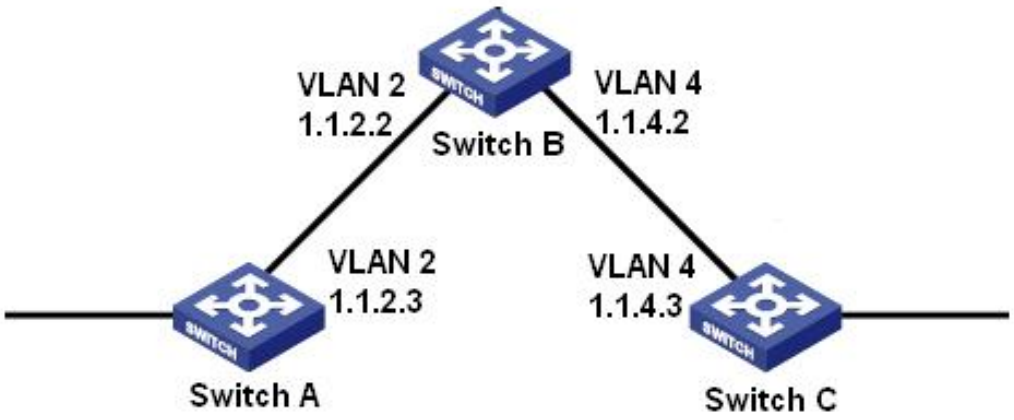


Figure 238 RIP Configuration Example

Configuration on Switch A:

1. Set IP address for VLAN 2 interface.
2. Enable RIP protocol, as shown in Figure 232.
3. Enable VLAN 2 interface to transmit/receive RIP messages, as shown in Figure 237.

Configuration on Switch B:

1. Set IP addresses for VLAN 2 and VLAN 4 interfaces.

2. Enable RIP protocol, as shown in Figure 232.

3. Enable VLAN 2 and VLAN 4 interfaces to transmit/receive RIP messages, as shown in Figure 237.

Configuration on Switch C:

1. Set IP address for VLAN 4 interface.

2. Enable RIP protocol, as shown in Figure 232.

3. Enable VLAN 4 interface to transmit/ receive RIP messages, as shown in Figure 237.

7.16.3 OSPF

7.16.3.1 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.

Note:

Routers in this chapter refer to Layer 3 switches.

7.16.3.2 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 smallest IP address of the VLAN interface 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.

7.16.3.3 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 239. 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.

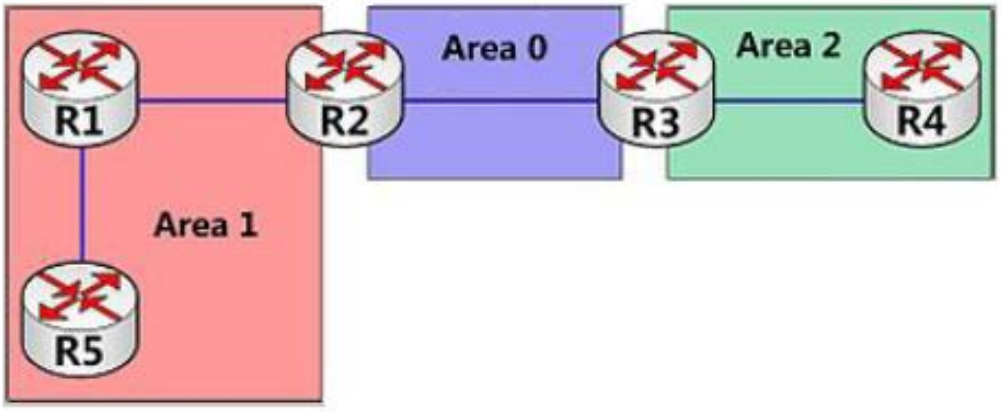


Figure 239 Area Partition

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 240.

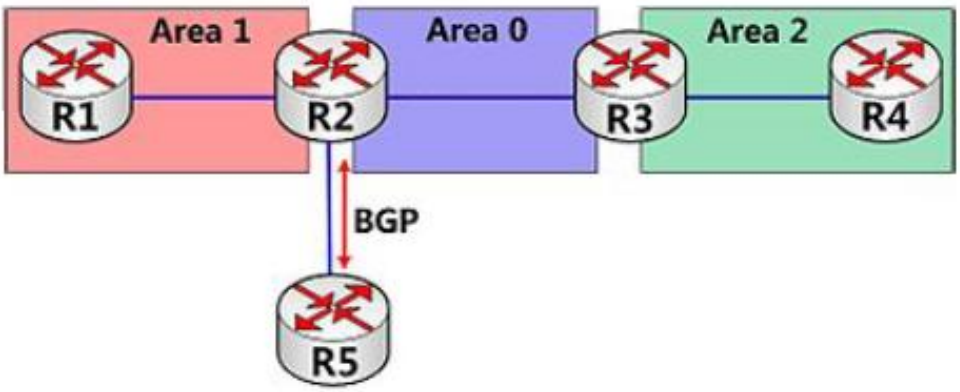


Figure 240 OSPF Router Types

Internal router: All interfaces on an internal router belong to one OSPF area. For example, R1 and R4 in Figure 240.

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 240.

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 240.

ASBR: A router exchanging routing information with another AS is an ASBR. For example, R2 in Figure 240.

One router can be of multiple types. For example, R2 in Figure 240 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.

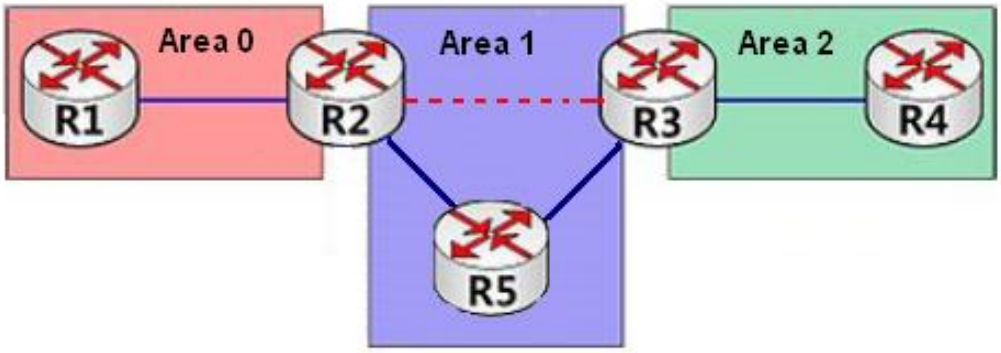


Figure 241 Virtual Link

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 241 is a virtual link and Area 1 is the transit area for the virtual link.

4. Route types

OSPF prioritizes 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.

7.16.3.4 DR and BDR

On Non-Broadcast Multiple Access (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 BDR becomes DR. Since the adjacent relationships with other routers have been established, the DR failure imposes tiny impact on the network.

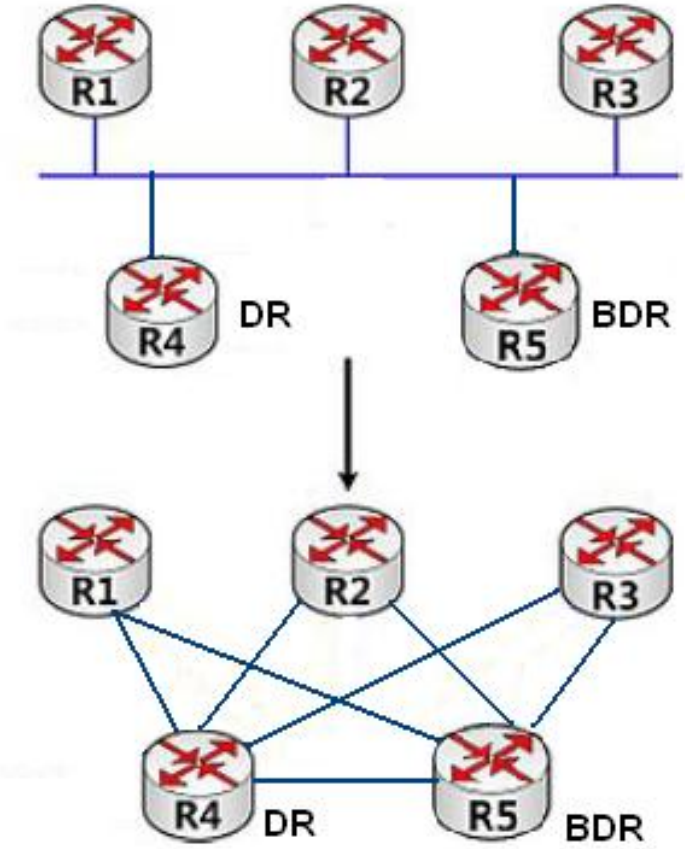


Figure 242 DR and DBR

As shown in Figure 242, the first figure shows Ethernet physical connections, and the second figure shows 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.

7.16.3.5 Web Configuration

1. Configure OSPF basic parameters, as shown in the following figure.

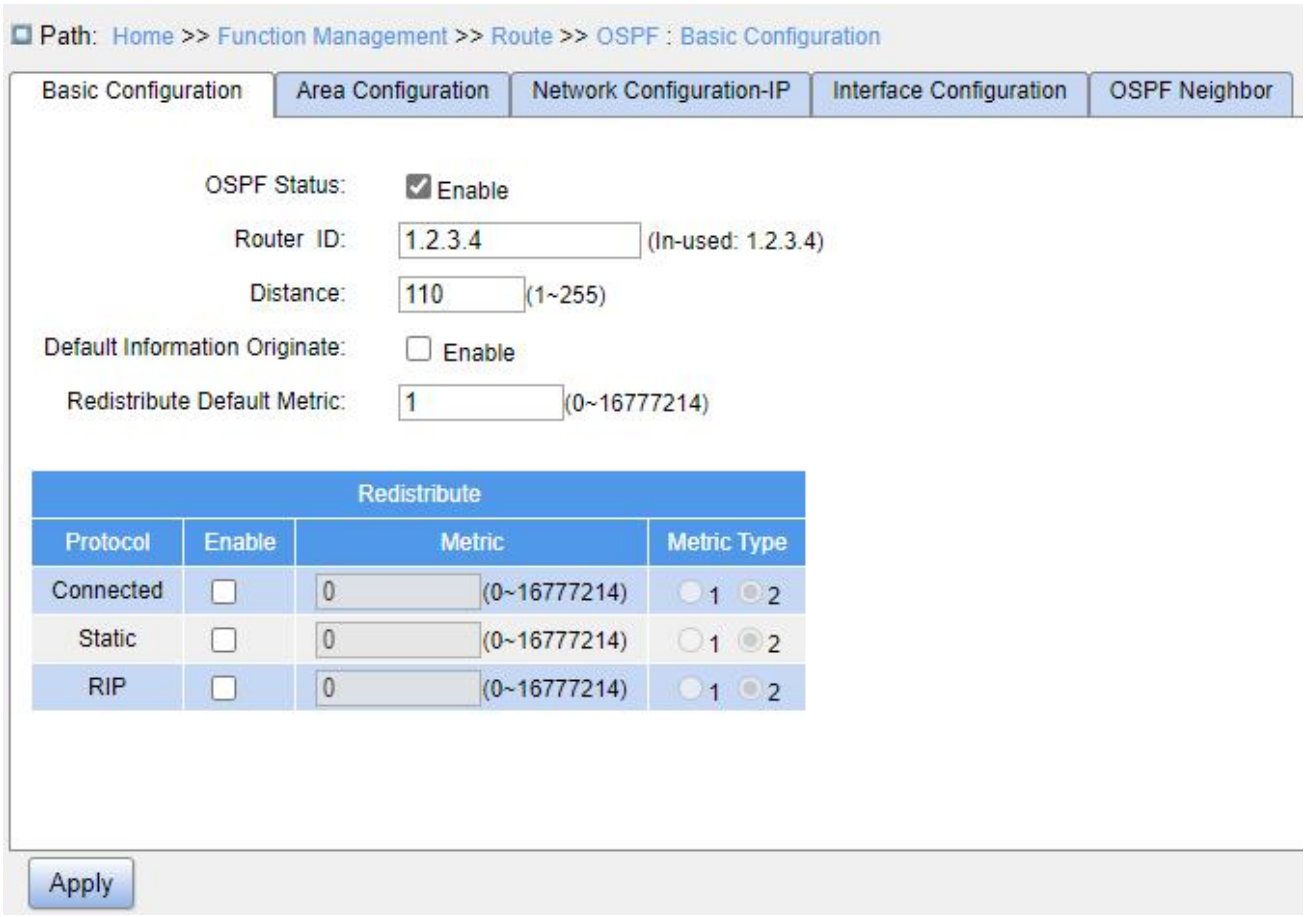


Figure 243 OSPF Basic Configuration

OSPF Status

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable 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:

RID changes only work after the OSPF process is restarted.

Router ID (In-Used)

Function: Display the current actual RID.

Distance

Configuration range: 1~255

Default configuration: 110

Function: Configure the administrative distance of OSPF routes.

Default Information Originate

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable broadcasting of 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: 0

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.

- 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 redistribution 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.

2. Configure OSPF areas, as shown in the following figure.

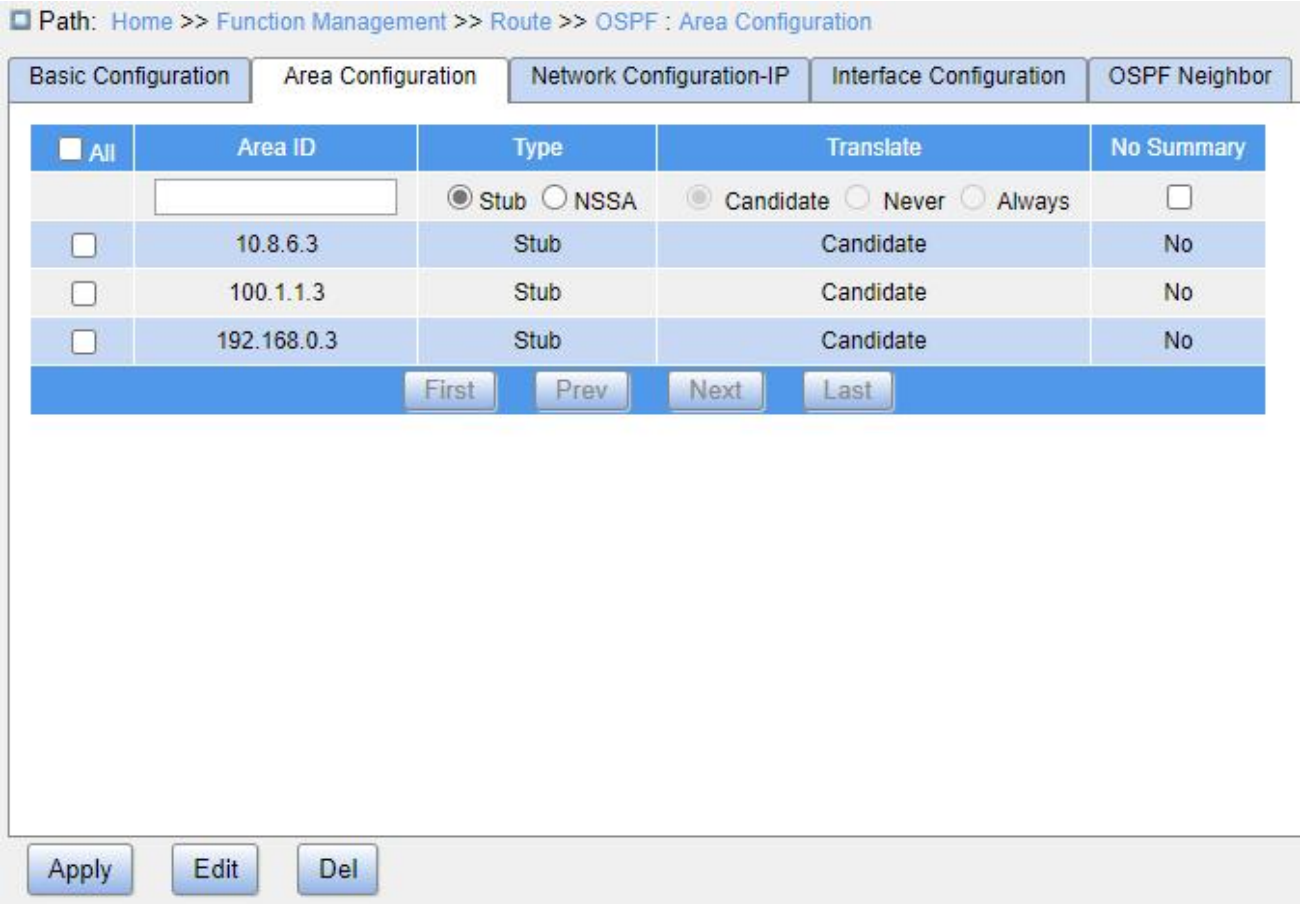


Figure 244 OSPF Area Configuration

Area ID

Configuration format: A.B.C.D

Configuration range: 0.0.0.0~255.255.255.255

Function: Configure the area ID.

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.

- Candidate: The ABR in the NSSA area is elected according to the RID size to determine whether to convert the Type 7 LSA. The larger 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. Configure OSPF network, as shown below.

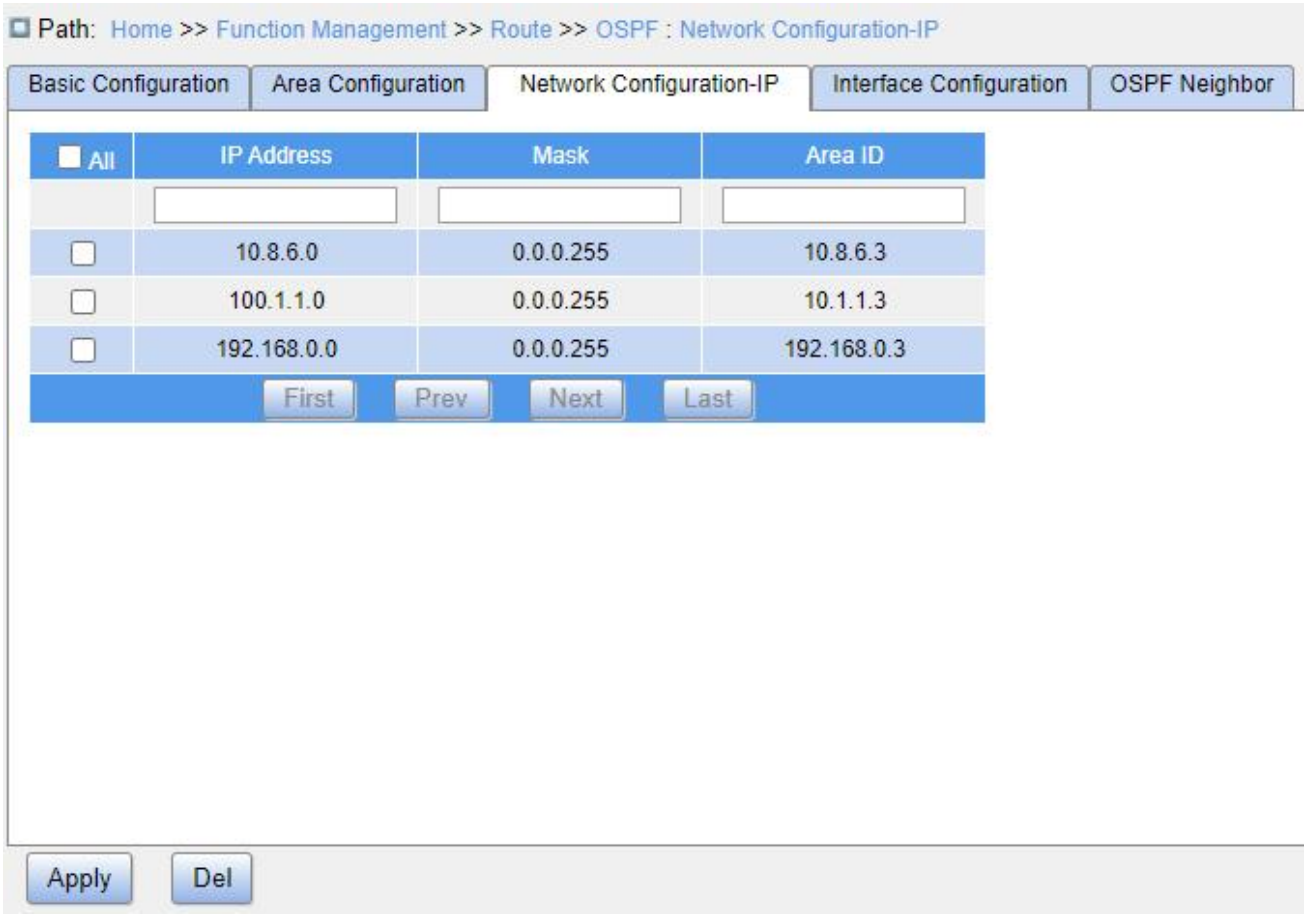


Figure 245 OSPF Network Configuration

IP Address

Configuration format: A.B.C.D

Function: Configure the network IP address.

Mask

Configuration format: A.B.C.D

Function: Configure the wildcard mask for the IP address. In the mask, 1 indicates the

bits that need to be matched, and 0 indicates the bits that do not need to be matched.

Description: 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.

Area ID

Configuration format: A.B.C.D

Configuration range: 0.0.0.0~255.255.255.255

Function: Configure the OSPF area ID.

Description: Once a network is added to the area, all internal routes of the network are no longer broadcasted independently to other areas. Only the summary information of the entire network-wide routes is broadcasted.

4. Configure OSPF interfaces, as shown in the following figure.

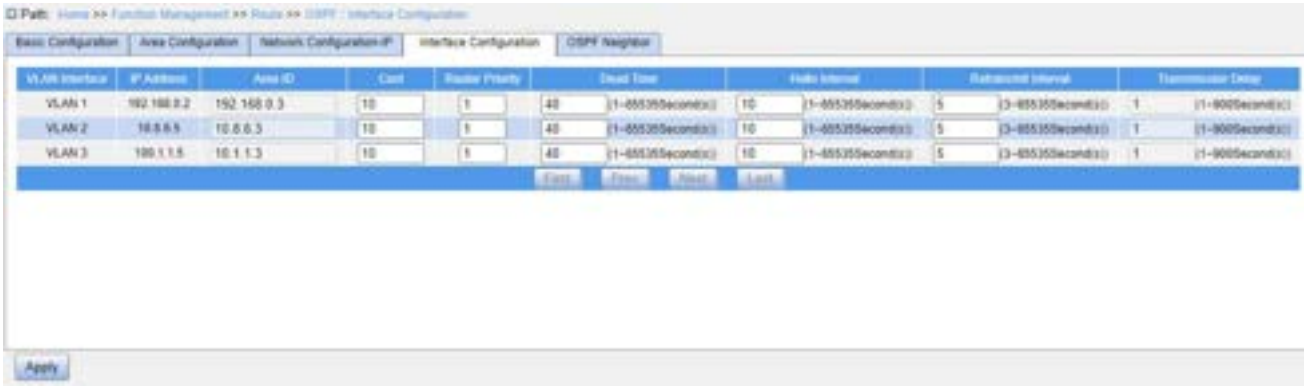


Figure 246 Configure OSPF Interfaces

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. When the IP address of the VLAN interface belongs to an OSPF network, this VLAN interface is added to the OSPF area.

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 OSPF priority of the VLAN interface.

Description: When DR and BDR are selected on the network segment, the device with the highest priority value is selected as the DR.

Dead Time

Configuration range: 1~65535s

Default configuration: 40

Function: Configure the expiration time of the neighboring device.

Description: If the interface fails to receive a Hello packet from the neighboring device within the specified dead time period, the neighboring device is considered unreachable and invalid.

Hello Interval

Configuration range: 1~65535s

Default configuration: 10

Function: Configure the interval at which the VLAN interface sends Hello packets.

Retransmit Interval

Configuration range: 3~65535s

Default configuration: 5

Function: Configure the interval after which an LSA is retransmitted to the neighboring device.

Description: After a device transmits an LSA to its neighbor, it will wait for a confirmation from the neighbor. If no confirmation is received after the specified interval, it will retransmit the LSA.

Transmission Delay

Configuration range: 1~900s

Default configuration: 1

Function: Configure the delay for transmitting an LSA.

5. View OSPF neighbor information, as shown in the following figure.

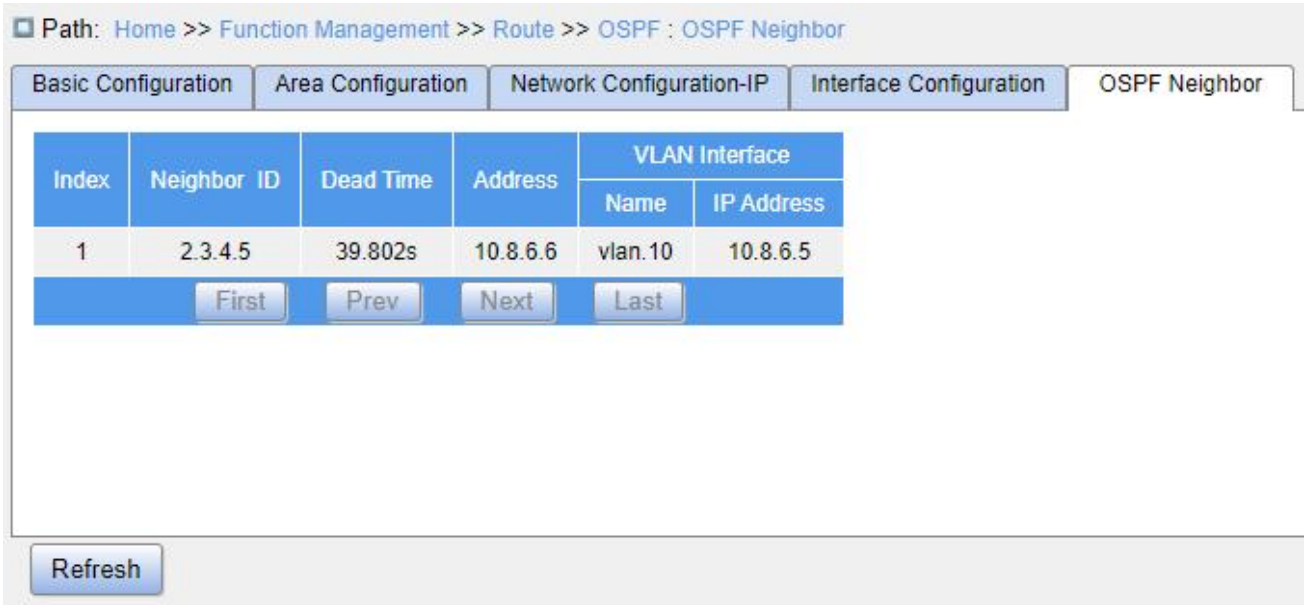


Figure 247 OSPF Neighbor Information

7.16.3.6 Typical Configuration Example

R1 and R2 run OSPF. R1 imports external static routes into the OSPF area.

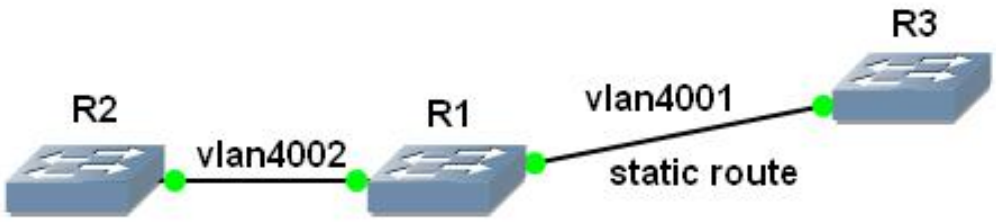


Figure 248 OSPF Configuration Example

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. Start the OSPF protocol and set the router ID as 100.1.1.178, as shown in Figure 243.

4. Set the area of the VLAN 4002 interface, as shown in Figure 244.

5. Configure OSPF to redistribute static routes, as shown in Figure 243.

Configuration on R2:

1. Set the IP address of VLAN 4002 interface: 202.1.1.177, subnet mask: 255.0.0.0;

2. Start the OSPF protocol and set the router ID to be 100.1.1.177, as shown in Figure 243.

3. Set the area of the VLAN 4002 interface, as shown in Figure 244.

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 247.

7.17 QoS Configuration

7.17.1 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.

7.17.2 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: 2~8 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.

For example, 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.

7.17.3 Web Configuration

1. Configure port classification, as shown below.

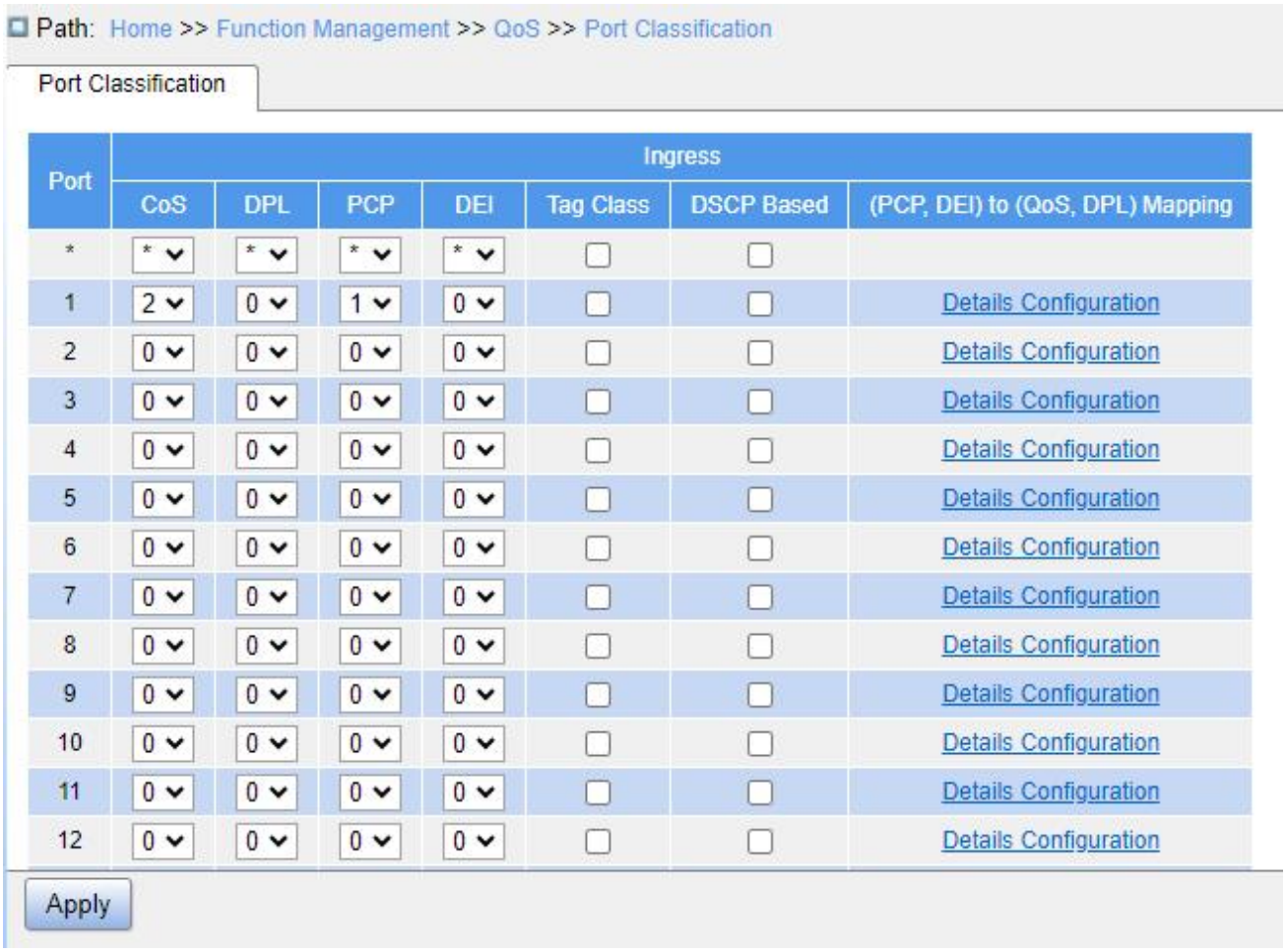


Figure 249 Configure Queue Mapping Mode Based on Port

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 disables 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 the port's default DPL (Drop Priority Level) value.

Description: For received untag messages or tag message without tag class enabled, the DPL value is the default DPL value of the port.

PCP

Configuration range: 0~7

Default configuration: 0

Function: Configure the port's default PCP (Priority Code Point) value.

Description: For received untag messages, the priority value in the added tag is the default PCP value of the port.

DEI

Configuration range: 0~1

Default configuration: 0

Function: Configure the port's default DEI (Drop Eligible Indicator) value.

Description: For received untag messages, the CFI value in the added tag is the default DEI value of the port.

2. Configure queue mapping mode based on 802.1Q header information.

As shown in Figure 249, check <Tag Class> of port, and click <Detailed 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.

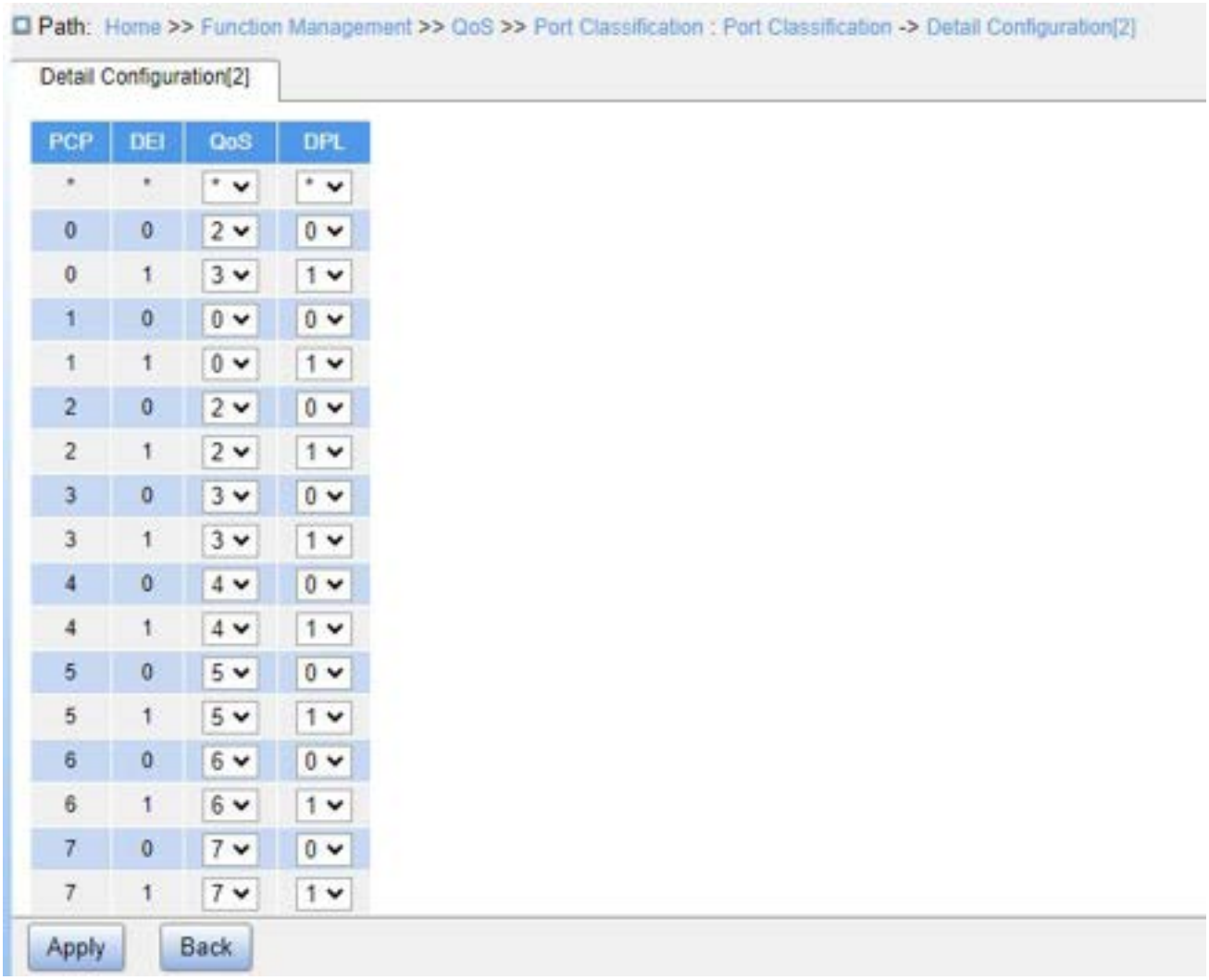


Figure 250 Configure Queue Mapping Mode Based on 802.1Q Header Information

Caution:

The queue mapping mode based on 802.1Q header information is only suitable for received tag messages.

(PCP, DEI) to (QoS class, DP level) mapping

Configuration range: 0~7 (QoS), 0~1 (DPL)

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 DPL value 0, 1.

Function: Configure (PCP, DEI) to (QoS, 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 enables 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.

Figure 251 Configure 802.1p Remarking

Click a port ID and enter 802.1p remarking configuration page, as shown in Figure 252. This page shows the mode of remarking 802.1p when the port forwards the message. The 802.1p remarking indicates that the port will update the PCP and DEI value in the forwarded packet.

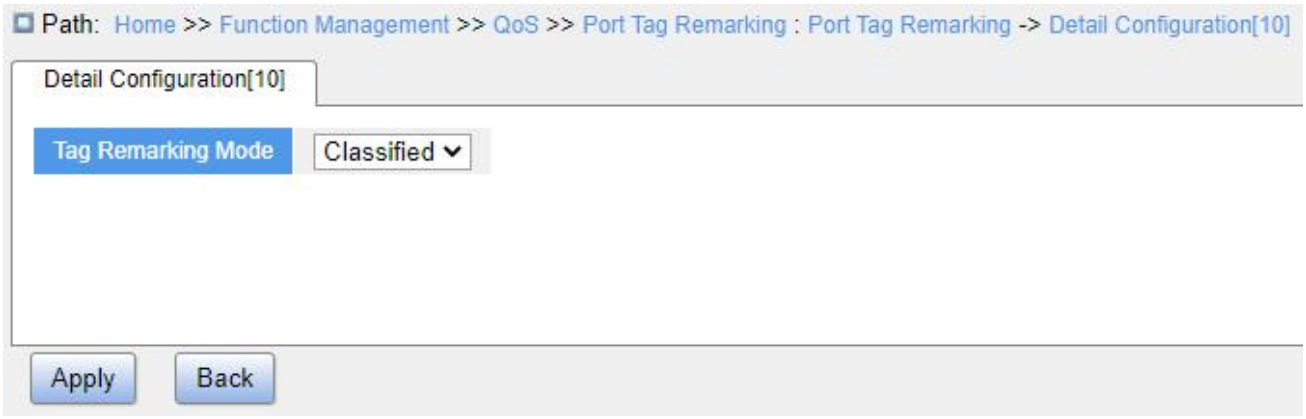


Figure 252 Configure 802.1p Port Remarking Mode

Caution:

If there is no tag in the forwarded port message, 802.1p remarking does not work.

(1) Configure 802.1p remarking mode as Classified, as shown in Figure 252.

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 egress port forwards the message.

(2) Configure 802.1p remarking mode as Default, as shown below.

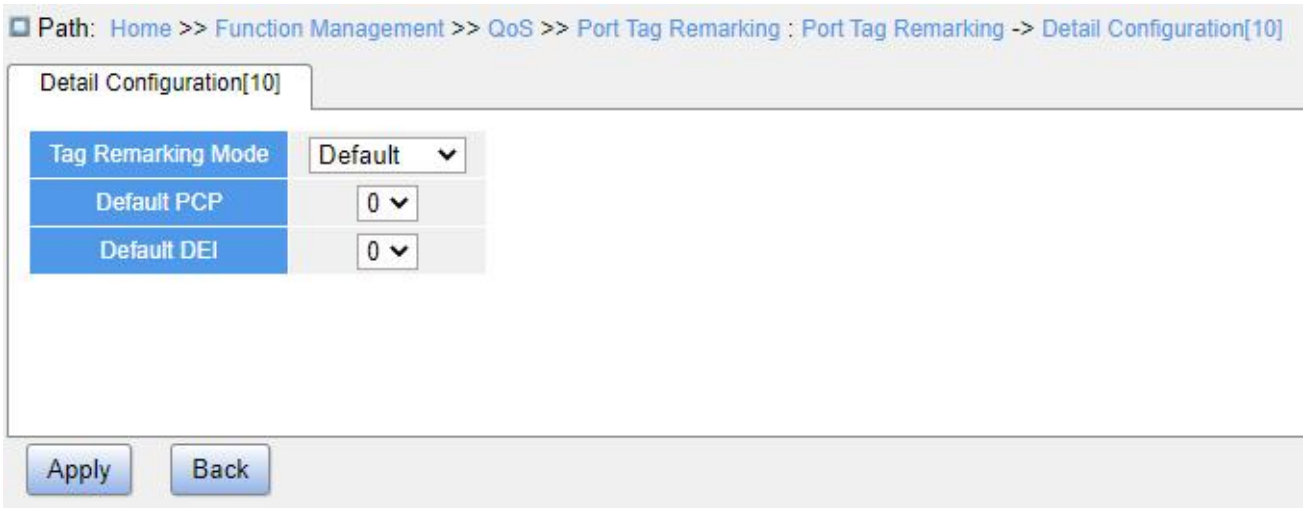


Figure 253 Configure Default Remarking Mode

Tag Remarking Mode

Configuration options: Classified/Mapped/Default

Default configuration: Classified

Function: Configure 802.1p remarking mode. Default mode: When the egress port forwards the message, the PCP and DEI values in the message are changed to the default values of the egress port. (configuration as below)。

Default PCP

Configuration range: 0~7

Default configuration: 0

Function: Configure the default PCP value of the egress port.

Default DEI

Configuration range: 0~1

Default configuration: 0

Function: Configure the default DEI value of the egress port.

(3) Configure 802.1p remarking mode as Mapped, as shown below.

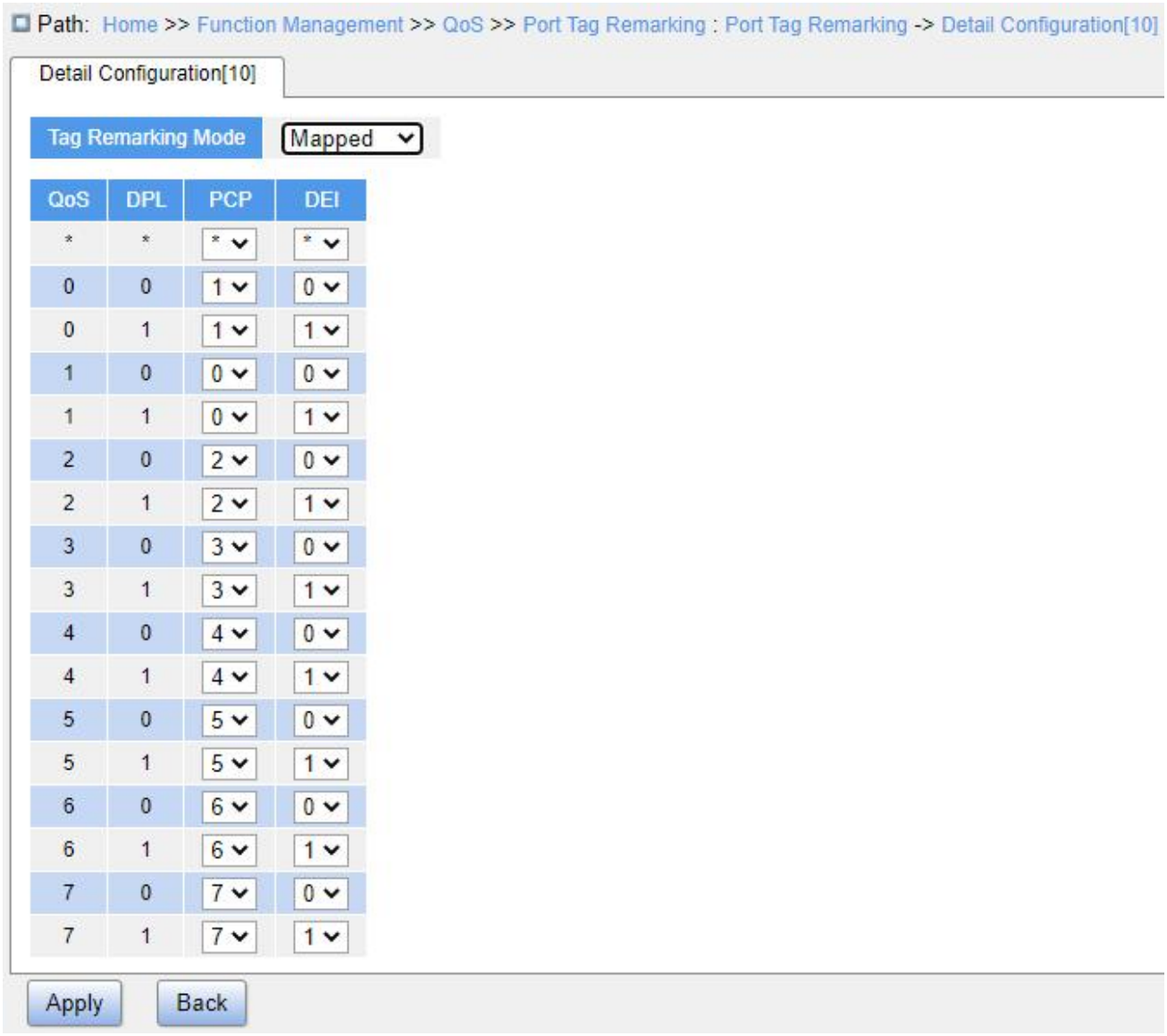


Figure 254 Configure Mapped Remarking Mode

Tag Remarking Mode

Configuration options: Classified/Mapped/Default

Default configuration: Classified

Function: configure 802.1p remarking mode. Mapped mode: When the egress port forwards the message, PCP and DEI values in the message are updated based on the mapping between (QoS, DPL) and (PCP, DEI). The mapping configurations are as follows.

(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; DPL value 0, 1 map to DEI value 0, 1.

Function: Configure (QoS, DPL) to (PCP, DEI) mapping.

4. Enable queue mapping mode based on DSCP, as shown below.

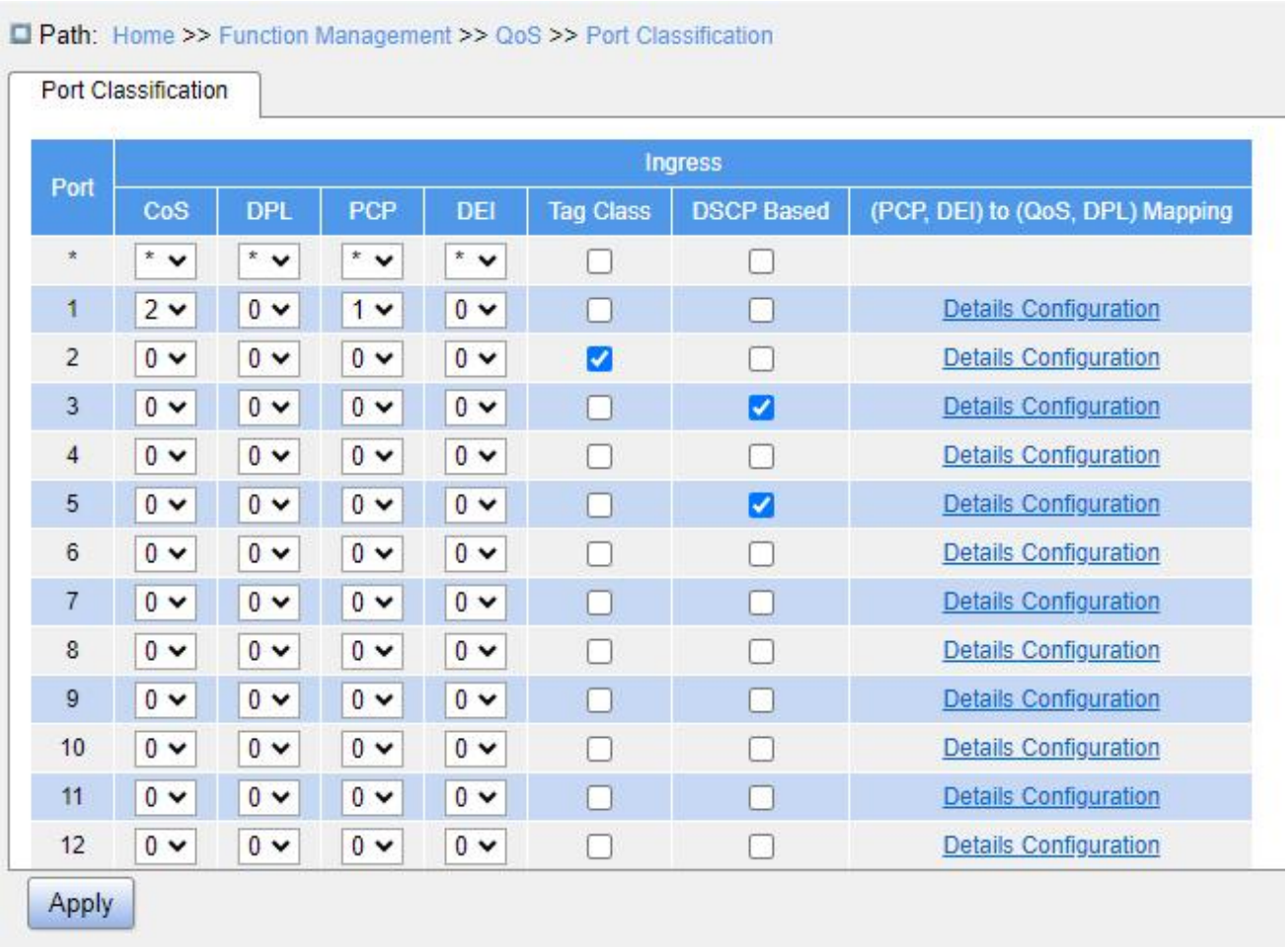


Figure 255 Enable Queue Mapping Mode Based on DSCP

DSCP Based

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable queue mapping mode based on DSCP. The queue mapping mode based on DSCP takes precedence over the queue mapping mode based on 802.1Q header information.

5. Enable DSCP translation of ingress port, DSCP rewrite of egress port, as shown below.

Figure 256 Configure Port DSCP

Translate

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to translate the DSCP value in the received message. If enabled, the DSCP value is translated according to the DSCP translation table, that is, the “translate” column in Figure 258.

Classify

Configuration options: Disable/DSCP=0/Selected/All

Default configuration: Disable

Function: Configure DSCP classification mode.

- Disable: No classification.
- DSCP=0: Classify to new DSCP if DSCP in received packet is 0.
- Selected: Classify to new DSCP if classification is enabled for specific DSCP values

in the global DSCP classification mapping configuration.

- All: Classify to new DSCP always.

Rewrite

Configuration options: Disable/Enable/Remap

Default configuration: Disable

Function: Configure rewrite mode of the DSCP value when the egress port forwards a message.

- Disable: When egress port forwards the message, the DSCP value in the message is not rewritten;
- Enable: When egress port forwards the message, it determines whether to rewrite the DSCP value in the message according to the classification configuration.
- Remap: When egress port forwards the message, the DSCP in the message is rewritten according to (DSCP, DPL) to DSCP mapping (“remap DP0, DP1” in Figure 258).

6. Configure queue mapping mode based on DSCP, as shown below.

Figure 257 Configure Queue Mapping Mode Based on DSCP

Trust

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to trust the DSCP value. Only frames with trusted DSCP values are mapped to a specific QoS class and DPL. Frames with untrusted DSCP values are treated as a non-IP frames.

Caution:

The queue mapping mode based on DSCP only applies to the scenario where the DSCP values of the messages received by the port are trusted.

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 being trusted enters the switch, the switch assigns CoS value to the message according to DSCP to CoS mapping.

Caution:

When translation is enabled on the ingress port, 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 being trusted enters the switch, the switch assigns the DPL value to the message according to the DSCP to DPL mapping.

7. Configure DSCP translation and rewrite, as shown below.

Figure 258 Configure DSCP Translation and Rewrite

Translate

Configuration range: 0~63

Function: Configure DSCP translation table.

Classify

Configuration options: Enable/Disable

Default configuration: Disable

Function: Configure “Classify” in Figure 256 to Selected, this parameter configures the selected DSCP value. When “Classify” is configured as “Selected” in Figure 256, this parameter should be enabled and the translated DSCP value configured here refers to the

selected value.

Caution:

When the ingress port enables “translate”, the selected value is the translated value; Otherwise, the selected DSCP value is the original DHCP value in the message.

Remap DP0

Configuration range: 0~63

Function: Configure (DSCP, DPL) to DSCP mapping.

8. Configure DSCP classification, as shown below.

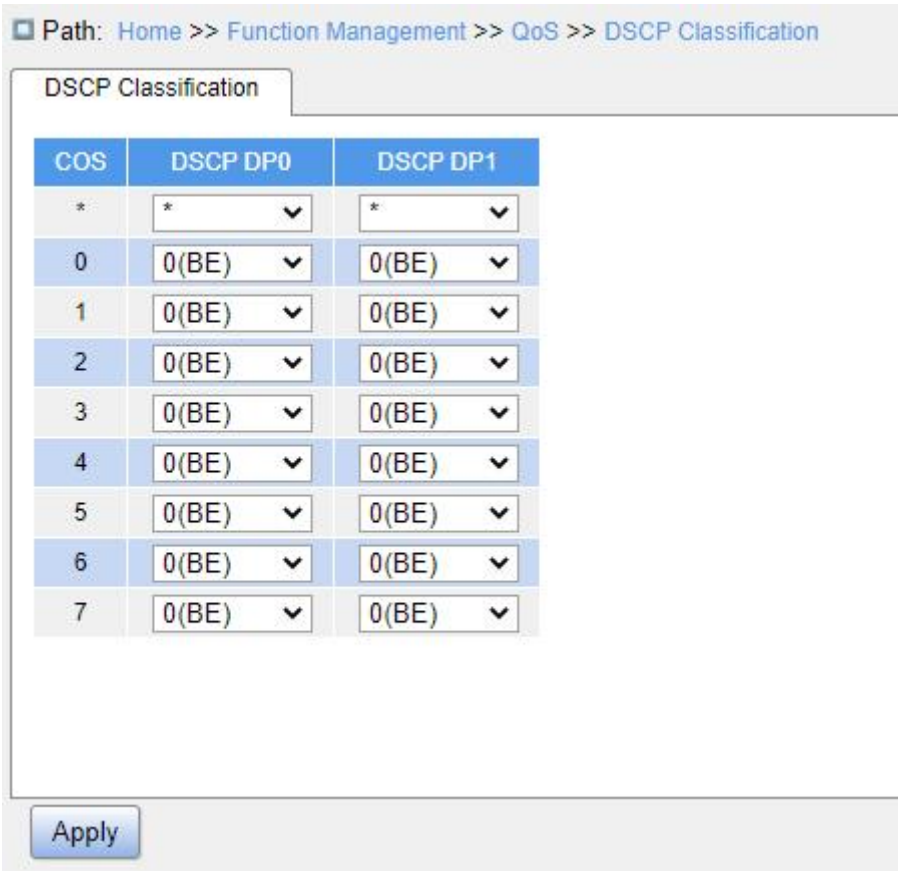


Figure 259 Configure DSCP Classification

DSCP DP0/DSCP DP1

Configuration range: 0~63

Function: Configure (CoS, DPL) to DSCP mapping. QoS classification 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 traffic monitoring based on queue, as shown below.

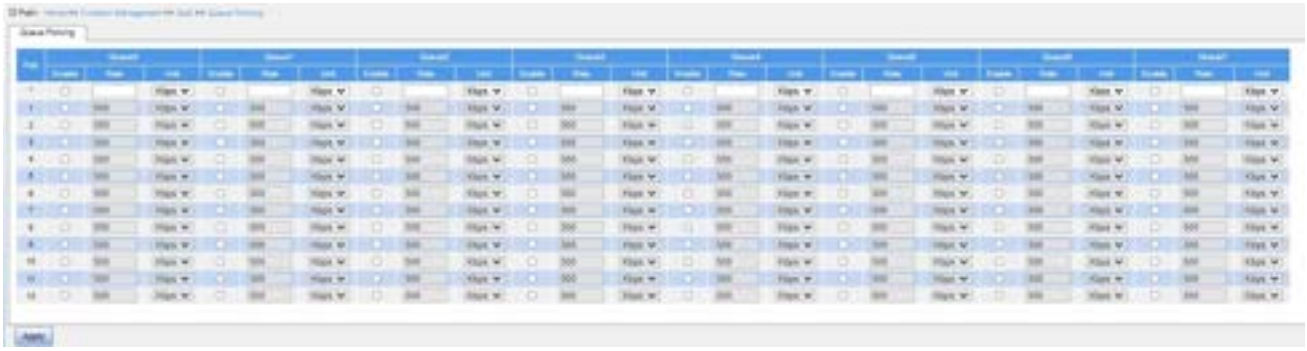


Figure 260 Configure Queue Policing

Enable

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable queue policing. When it is enabled, configure the rate and unit parameters.

Rate, Unit

Configuration range: 25~13128147 Kbps/ 1~13128 Mbps

Default configuration: 500 Kbps

Function: Limit the rate of frames received by queues on a port. Frames exceeding the specified rate will be dropped.

10. Configure the port queue scheduler mode, as shown in Figure 261 and Figure 262.

Figure 261 Configure Port Queue Scheduler Mode

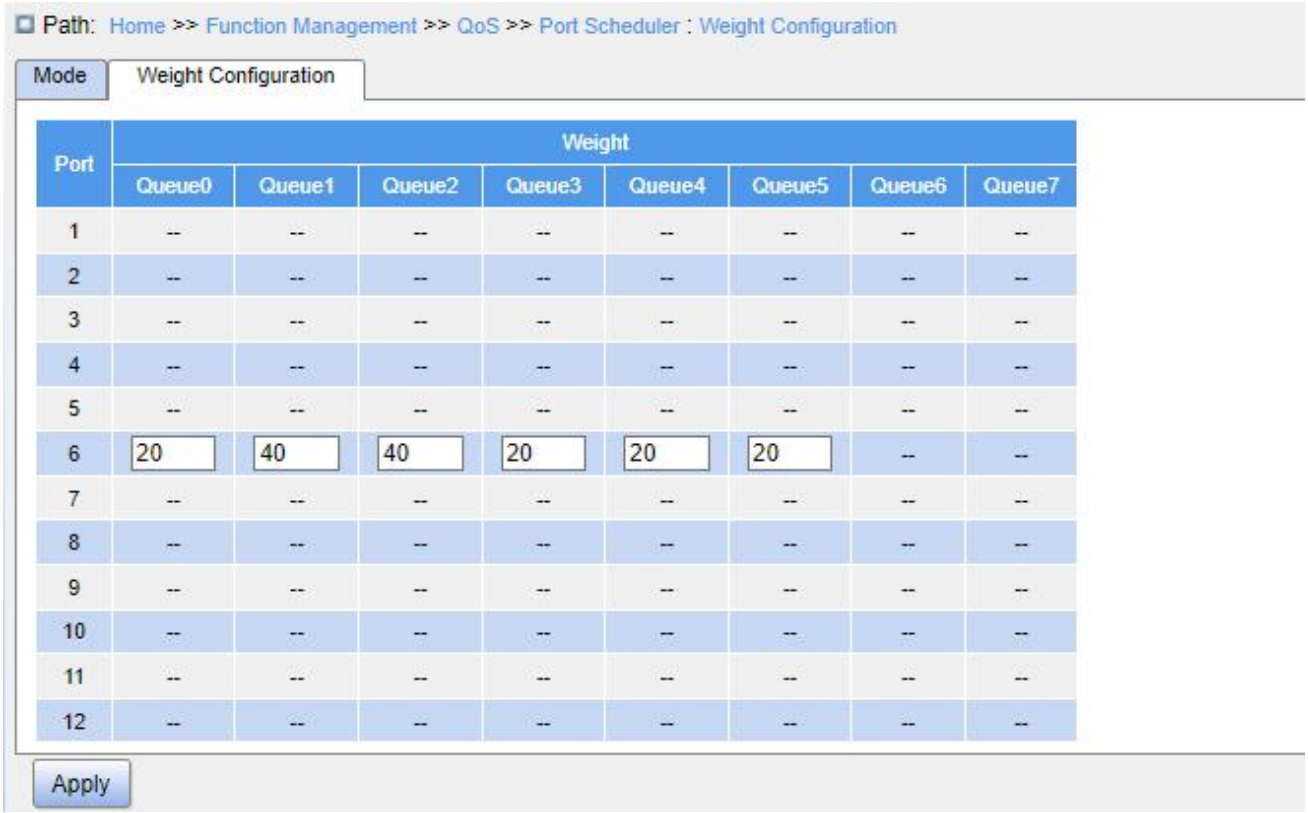


Figure 262 Configure Port WRR Weight of Scheduler

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.

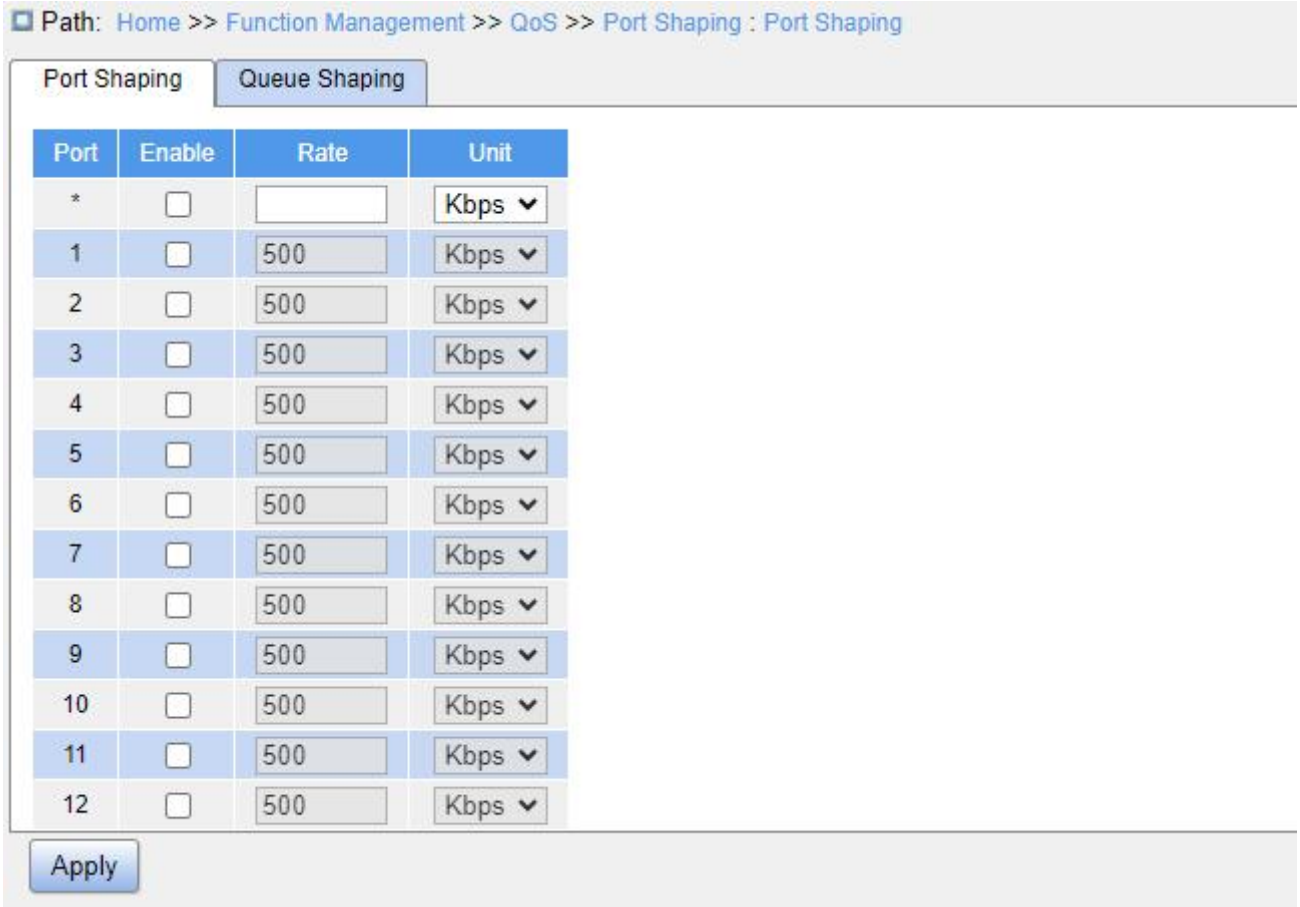


Figure 263 Configure Port Shaping

Enable

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable port shaping. Port traffic shaping is implemented by limiting the port rate.

Rate, Unit

Configuration range: 100~13107100 Kbps/ 1~13107 Mbps

Default configuration: 500 Kbps

Function: Limit the rate of frames transmitted by the port, and drop the frames exceeding the specified rate.

13. Configure queue shaping, as shown below.

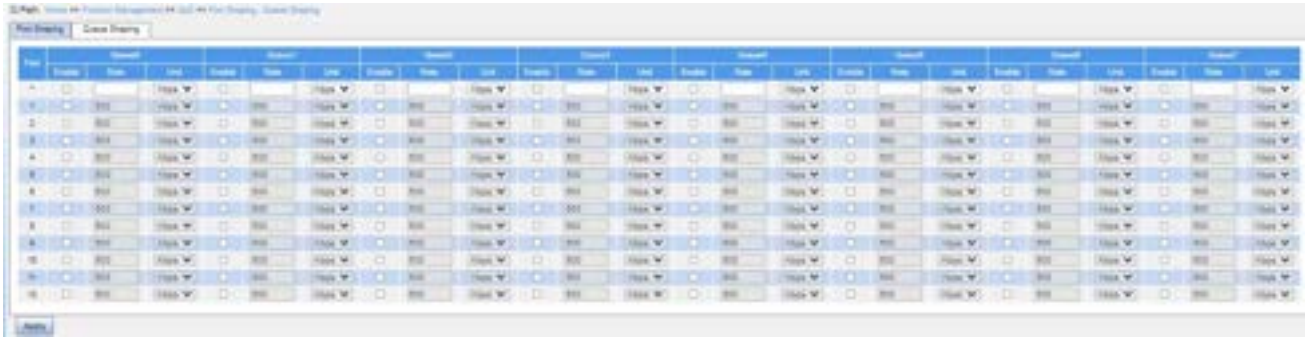


Figure 264 Configure Queue Shaping

Enable

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable queue shaping.

Rate, Unit

Configuration range: 100~13107100 Kbps/ 1~13107 Mbps

Default configuration: 500 Kbps

Function: Limit the rate of frames transmitted by the port, and drop the frames exceeding the specified rate.

7.17.4 Typical Configuration Example

As shown in Figure 265, port 1~port 5 forward packets to port 6.

- The packets received by port 1 are Untag, and the packets entering port 1 are mapped to queue 2.
- The PCP value of packets received by port 2 is 0, DEI value is 1, and the packets entering port 2 are mapped to queue 3.
- The DSCP value of packets received by port 3 is 4, and the packets entering port 3 are mapped to queue 6.

- Port 4 is enabled for testing traffic shaping. As traffic shaping takes effect in the egress direction, the configuration is delivered to port 6.
- The DSCP value of packets received by port 5 is 5, and the packets entering port 5 are mapped to queue 2.
- Port 6 adopts the SP+WRR scheduling mode.

Configuration Process:

1. Set the CoS value of port 1 to 2, as shown in Figure 249.

2. Enable tag classification of port 2, and map (PCP=0, DEI=1) to CoS=3, as shown in Figure 250.

3. Enable queue mapping mode based on DSCP for port 3 and port 5, as shown in Figure 255.

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 257.

5. Enable traffic shaping for port 6 and limit the egress rate of port 4 to 500 Kbps, as shown in Figure 263.

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 261 and Figure 262.

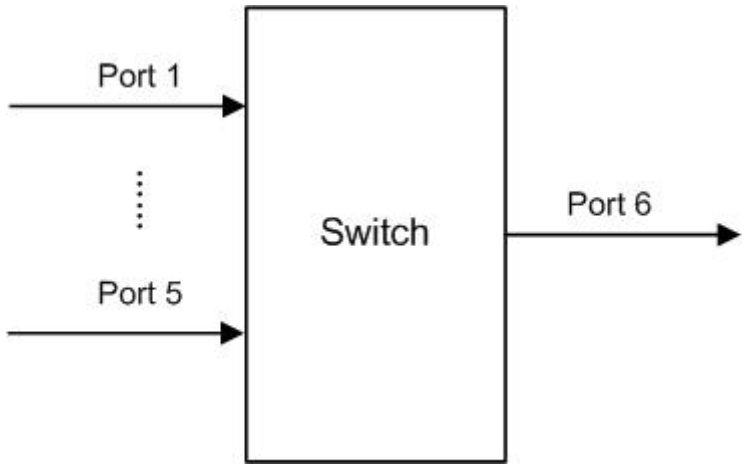


Figure 265 QoS Configuration Example

Packets from port 1 and port 5 packets enter queue 2, from port 2 enter queue 3, from port 3 enter queue 6, from port 4 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, pacekts from port 1 and port 5 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%.

7.18 VRRP

Note:

Routers in this chapter refer to Layer 3 switches.

7.18.1 Introduction

Virtual Router Redundancy Protocol (VRRP) adds multiple routers that can act as network gateways to a VRRP group, which forms a virtual router. Routers in the VRRP group elect a master through the VRRP election mechanism and the other routers in the group become backups. When the master fails, the backups elect a new master to undertake the responsibility of the failed master. This ensures uninterrupted data communication without configuration changes.

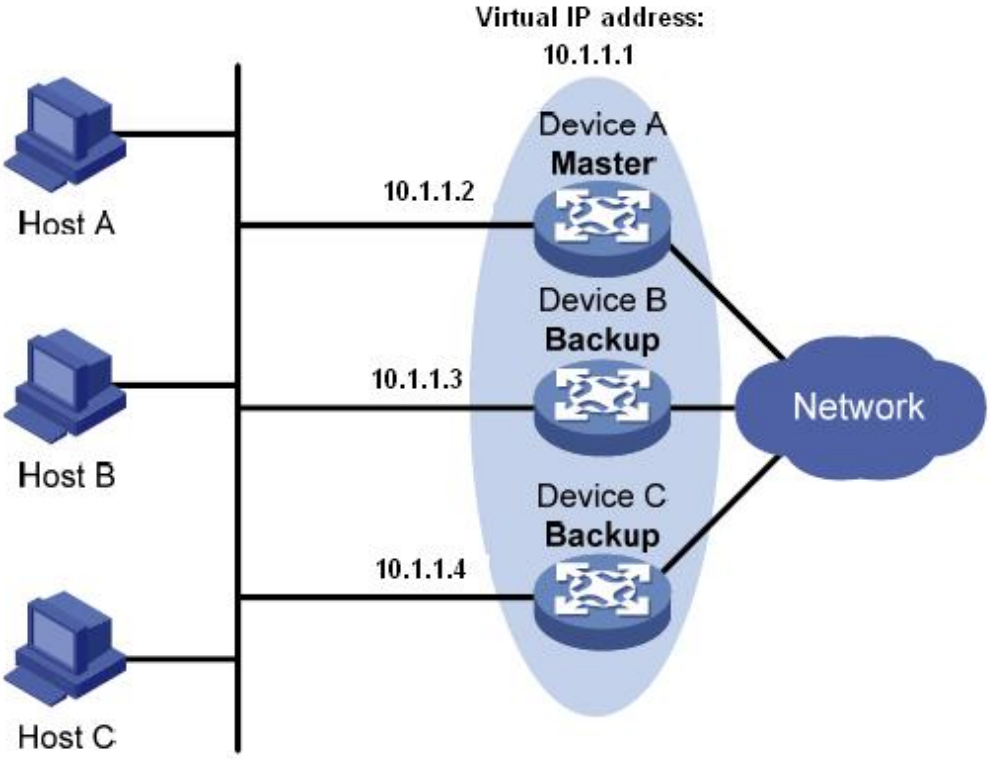


Figure 266 VRRP

As shown in Figure 266, 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, 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.

7.18.2 Master Election

VRRP selects the master by election.

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.

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.

7.18.3 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 or associating with an NQA instance. 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.

7.18.4 Web Configuration

1. Create a VRRP backup group, as shown below.

Figure 267 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

- Preemptive 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: 1~255s

Default configuration: 1

Function: Set the interval for the master router to send VRRP advertisements.

Caution:

The interval of advertising packets of the members in the same virtual router backup group must be the same.

Monitoring Target

Configuration options: VLAN/NQA

Function: Select the monitoring target type to be associated with VRRP.

Tracking VLAN Interface/NQA Instance

Configuration range: 1~4093/1~32

Function: Select the monitored VLAN interface or NQA instance ID.

Priority Decrement

Configuration range: 1~255

Function: Set the value of the priority decrement.

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. View VRRP information, as shown below.

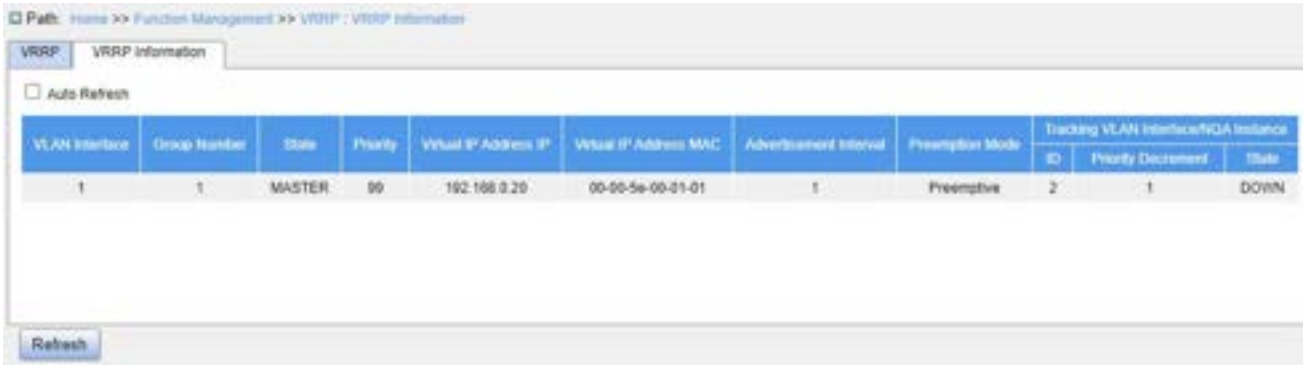


Figure 268 VRRP information

7.18.5 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.

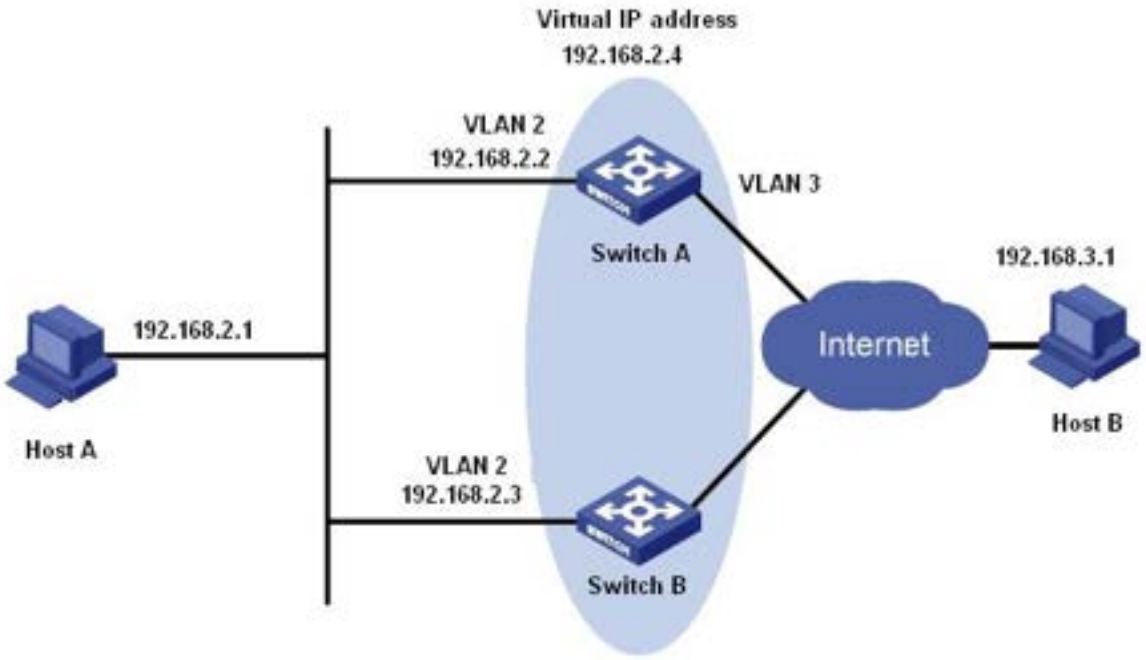


Figure 269 VRRP Typical Configuration Example

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 267.

3. Set the virtual IP address of VRRP group 1 to 192.168.2.4, and router type to Backup, as shown in Figure 267.

4. Configure VLAN 2 as the Layer 3 interface for VRRP group 1, as shown in Figure 267.

5. Set the priority of Switch A in the VRRP group to 110, and preemptive mode to false, as shown in Figure 267.

6. Configure VLAN 3 as the monitored interface and set the priority decrement to 30, as shown in Figure 267.

7. Enable VRRP group 1, as shown in Figure 267.

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 267.

3. Set the virtual IP address of VRRP group 1 to 192.168.2.4, and router type to Backup, as shown in Figure 267.

4. Configure VLAN 2 as the Layer 3 interface for VRRP group 1, as shown in Figure 267.

5. Set the priority of Switch B in the VRRP group to 100, and preemptive mode to false, as shown in Figure 267.

6. Enable VRRP group 1, as shown in Figure 267.

7.19 NQA

Network Quality Analyzer (NQA) is used to judge whether a destination is reachable by sending ICMP-Echo detection packets. Other function modules, such VRRP, can bind an NQA instance for monitoring the interface status to implement fast switchover when the interface experiences a failure.

Configure an NQA instance, as shown in the following figure.

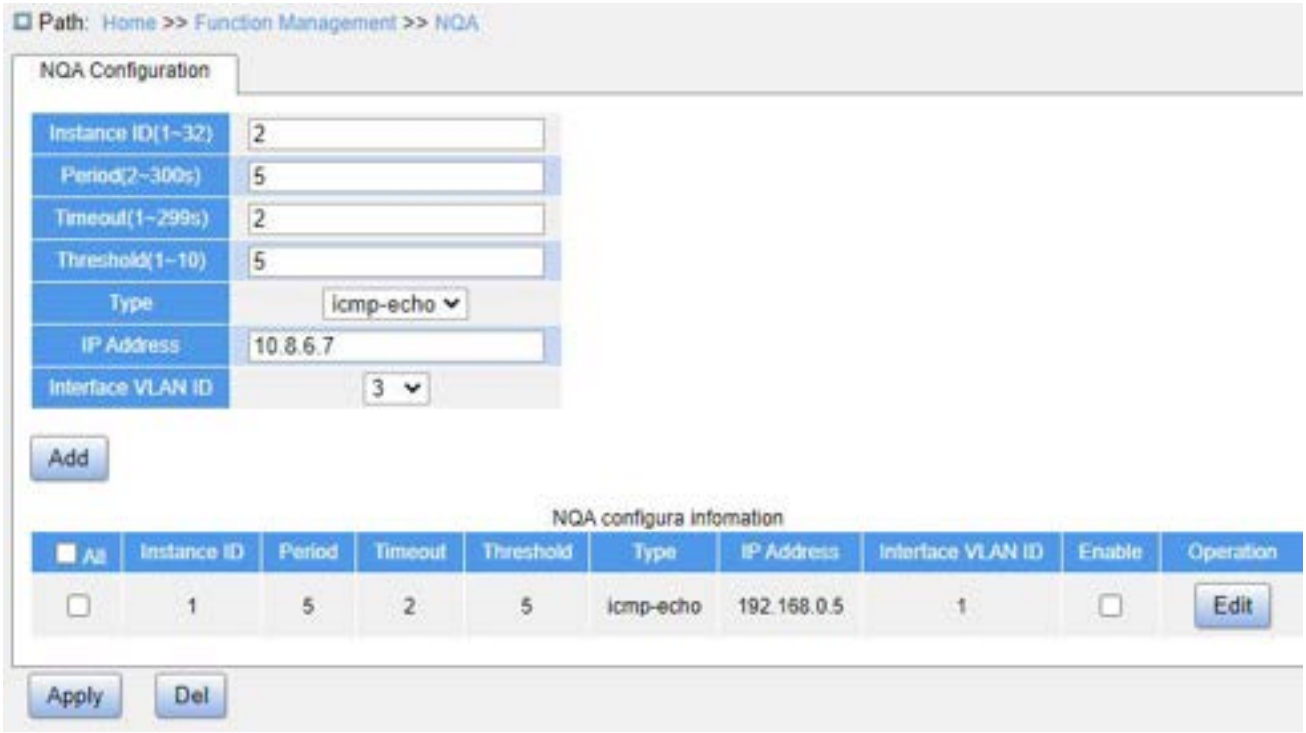


Figure 270 Configure NQA Instance

Instance ID

Configuration range: 1~32

Function: Configure the NQA instance ID.

Period

Configuration range: 2~300s

Default configuration: 5

Function: Configure the interval at which detection packets are sent.

Timeout

Configuration range: 1~299s

Default configuration: 2

Function: Configure the timeout value of detection packets.

Threshold

Configuration range: 1~10

Default configuration: 5

Function: Configure the consecutive number of detection failures for determining a destination is unreachable.

IP Address

Configuration format: A.B.C.D

Function: Configure the destination IP address of detection packets.

Interface VLAN ID

Configuration options: All created VLAN interfaces

Function: Configure the output interface of detection packets.

Enable

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable the NQA instance.

Click <Edit> button to modify NQA instance configurations.

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.

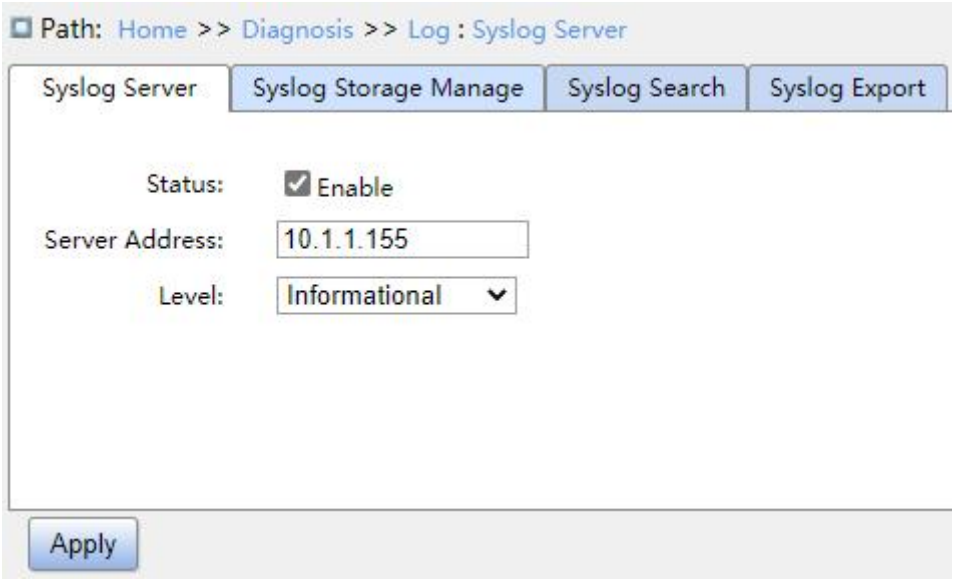


Figure 271 Configure Syslog Server

Status

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to 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. Search logs based on filters, as shown below.

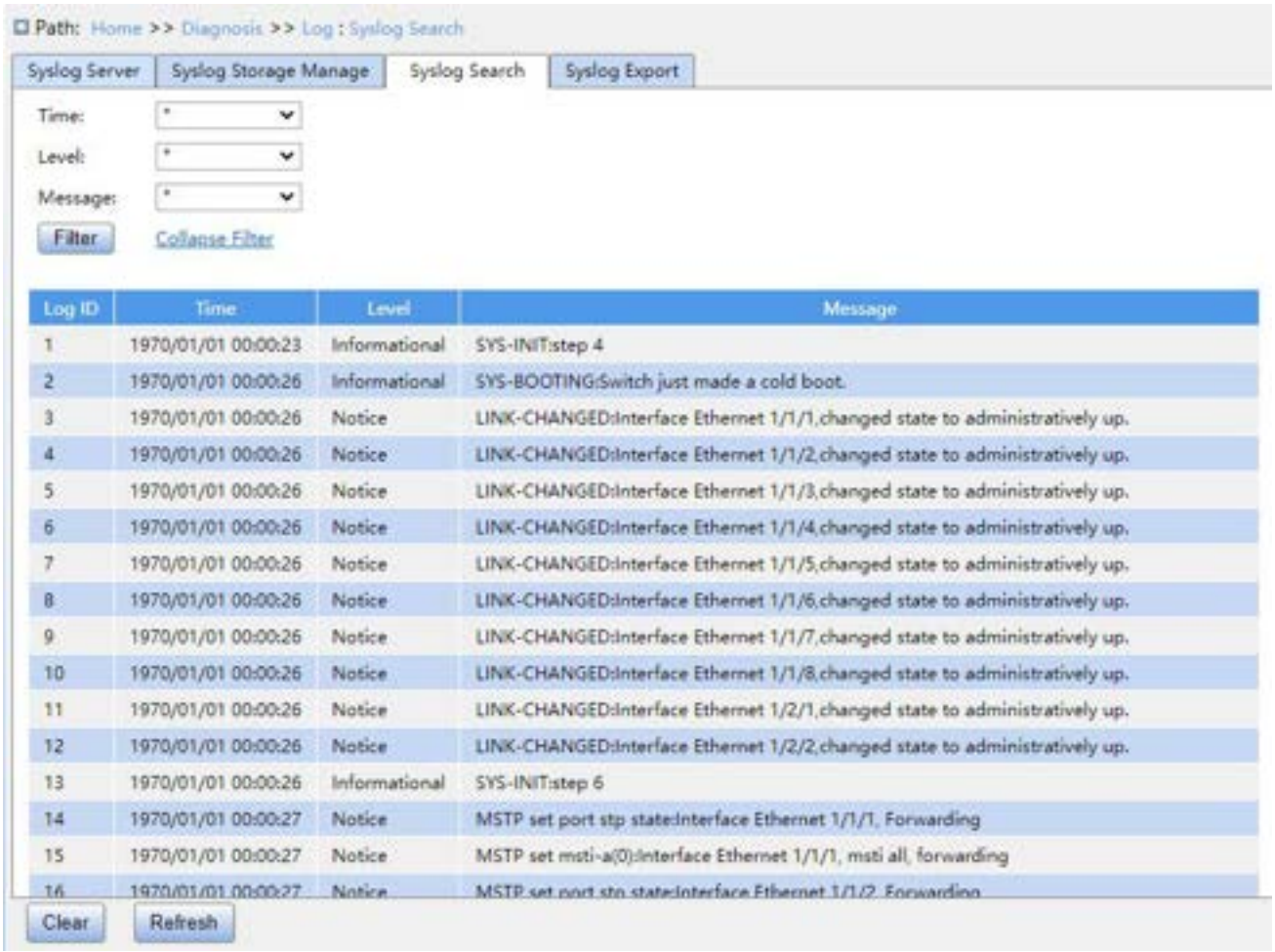


Figure 272 Syslog Search

Auto Refresh

Configuration options: check/uncheck

Default configuration: uncheck

Function: Whether to enable auto refresh.

Log ID

Configuration options: */>=/<=/Range

Default configuration: *

Function: Select filtered Log ID.

- *: Indicates all log IDs.
- >=: Filters log IDs that are greater than or equal to an ID.
- <=: Filters log IDs that are smaller than or equal to an ID.
- Range: Enter an ID range manually.

Time

Configuration options: */Start time/End time/Range

Default configuration: *

- *: Indicates all time.
- >=: Filters logs generated since the start time.
- <=: Filters logs generated before the end time.
- Range: Filters logs generated within a time range

Level

Configuration options: */>=/<=/Range

Default configuration: *

Function: Select filtered log levels.

- *****: Indicates all log levels.
- >=: Filters log levels that are greater than or equal to a level.
- <=: Filters log levels that are smaller than or equal to a level.
- Range: Enter a level range manually.

Message

Configuration options: */Include/Exclude

Default configuration: *

Function: Select filtered messages.

- *: Indicates all log messages.
- Include: Filters logs including the specified field.
- Exclude: Filters logs excluding the specified field.

3. Configure log storage, as shown in the following figure.

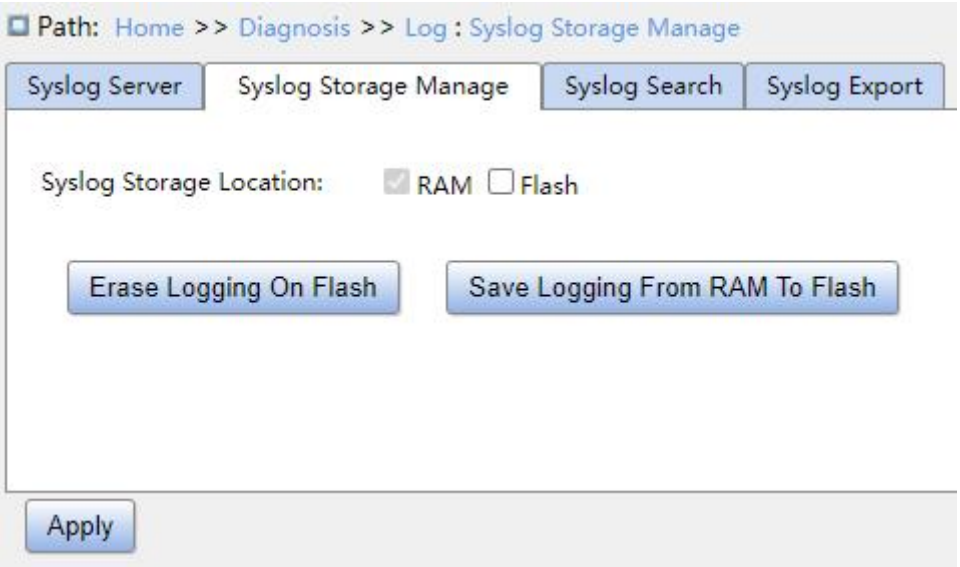


Figure 273 Log Storage Configuration

Syslog Storage Location

Configuration options: RAM/Flash

Function: Select the log storage place, which can be RAM, Flash or both.

Click <Erase Logging On Flash> to clear logs saved in Flash.

Click <Save Logging From RAM to Flash> to save logs stored in RAM to Flash.

4. Export logs to a local file, as shown in the following figure.

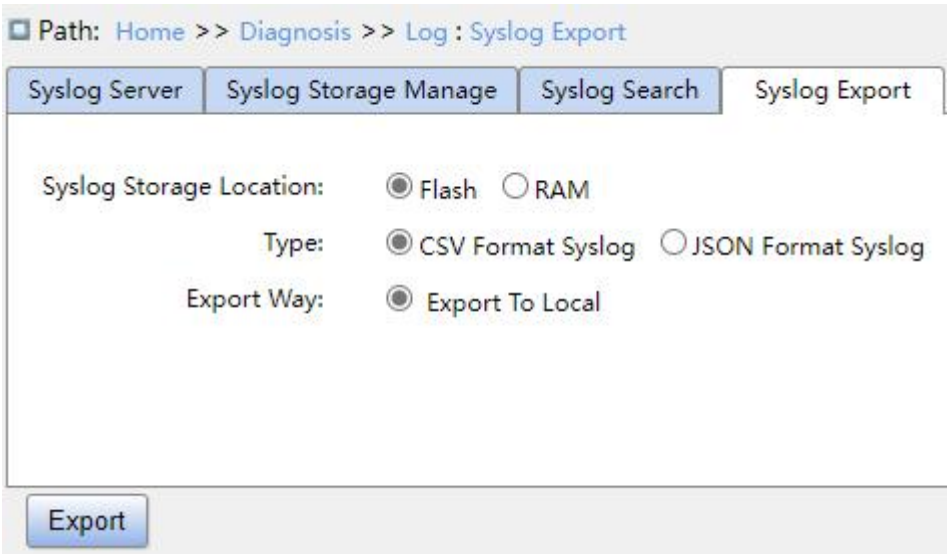


Figure 274 Log Export

Syslog Storage Location

Configuration options: RAM/Flash

Function: Select the log storage place, which can be RAM, Flash or both.

Type

Configuration options: RAW Syslog/CSV Format Syslog/JSON Format Syslog

Function: Select the type of file to be exported to local.

Export Way

Configuration options: Export to Local

Function: Logs can be exported to local files only.

5. Clear logs, as shown in the following figure.

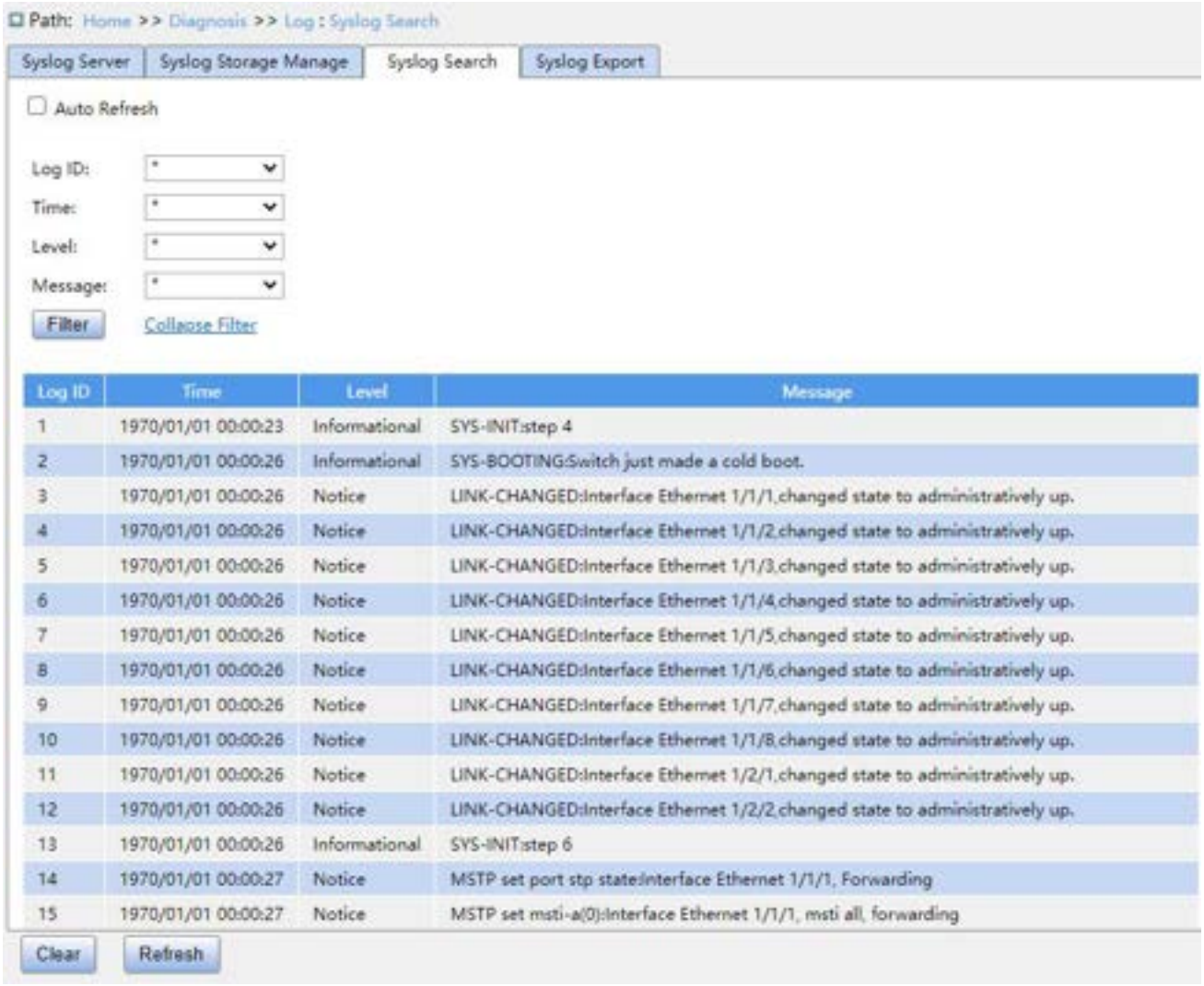


Figure 275 Log Clearance

Click the <Clear> button to clear all logs.

You can install syslog server software on PC to view logs in real time. What is shown in the following figure is an example.

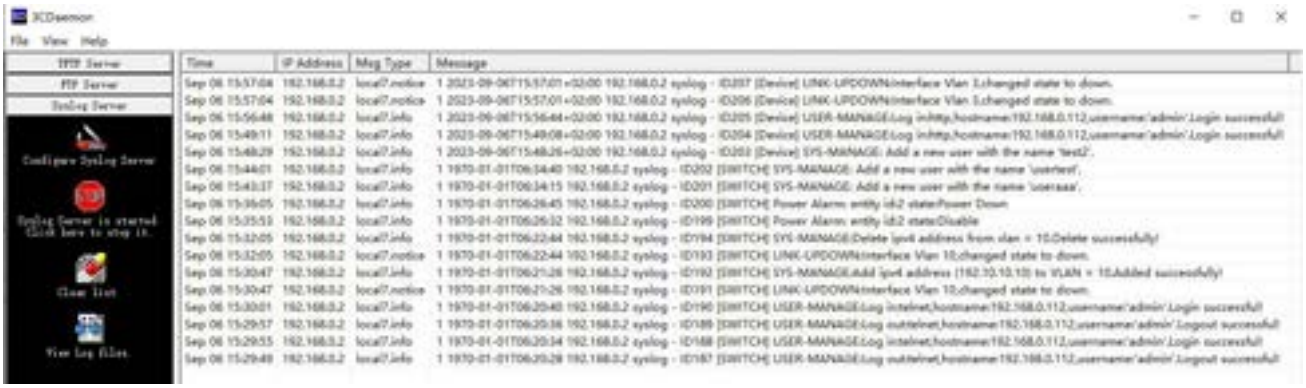


Figure 276 View Log on Syslog Server

8.2 Port Mirroring

8.2.1 Introduction

With port mirroring function, the switch copies all received or transmitted data frames or both in a port (mirroring source port) to another port (mirroring destination port).

Port mirroring can be classified into local port mirroring and remote port mirroring.

- Local port mirroring: The source device is directly connected to a protocol analyzer or RMON monitor for network monitor, management, and fault diagnosis. The source device sends mirrored packets from the mirroring source port to the mirroring destination port, both of which are located on the same device. Then the mirroring destination port forwards mirrored packets to the connected protocol analyzer or RMON monitor, as shown in the following figure.

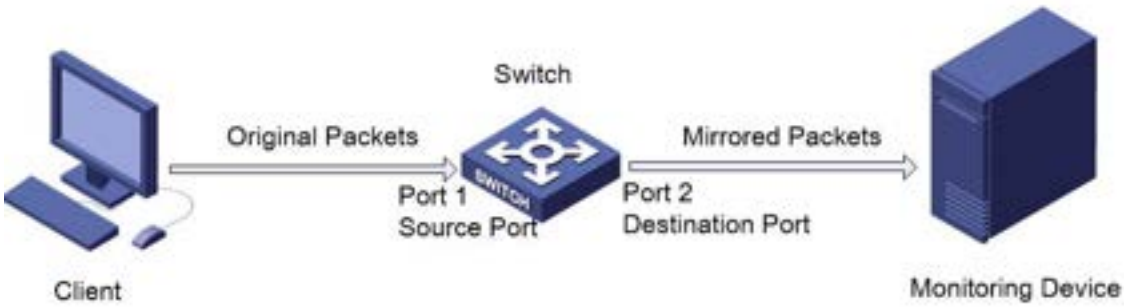


Figure 277 Local Port Mirroring

- Remote port mirroring: The source device is not directly connected to a protocol analyzer or RMON monitor, but via an intermediate device. The mirroring source

port and the mirroring destination port are located on different devices. The forwarding process of mirrored packets is show in the following figure.

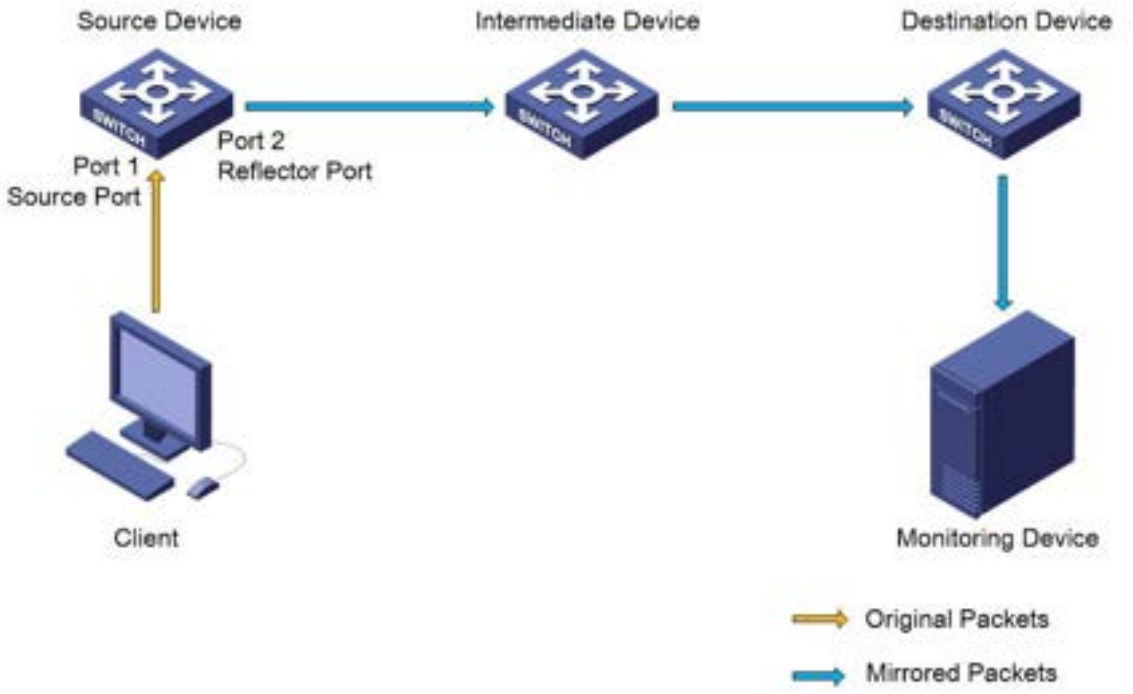


Figure 278 Remote Port Mirroring

(1) The source device sends mirrored packets from the mirroring source port to the reflector port.

(2) The reflector port sends the mirrored packets via the probe VLAN to the intermediate device.

(3) The intermediate device sends the mirrored packets to the destination device via the probe VLAN.

(4) The destination device sends the mirrored packets to the connected protocol analyzer of RMON monitor.

8.2.2 Explanation

A switch supports at most two mirroring destination ports but multiple mirroring source ports. Multiple mirroring source ports can be either in the same VLAN, or in different VLANs. Mirroring source port and mirroring destination port can be in the same VLAN or in different VLANs. The mirroring source port and mirroring destination port cannot be the same port.

Caution:

Dynamic MAC address learning must be disabled on a mirroring destination port.

8.2.3 Web Configuration

1. Configure local port mirroring function, as shown below.

Figure 279 Configure Local Port Mirroring Function

ALL

Configuration options: Check/Uncheck

Default configuration: Uncheck

Function: Check this mirroring group to edit and modify.

Status

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable the port mirroring group.

Destination Port1/Port2

Configuration options: NULL/Port ID

Default configuration: NULL

Function: Select the mirroring destination ports.

Source Rx

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to mirror frames received on the mirroring source port.

Source Tx

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to mirror frames transmitted from the source port.

2. Configure remote port mirroring, as shown below.

Figure 280 Configure Remote Port Mirroring

All

Configuration options: Check/uncheck

Default configuration: Uncheck

Function: Check this mirroring group to edit and modify.

Status

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable the port mirroring group.

Destination Remote

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable the switch to work as the source device in remote port mirroring.

Destination VLAN ID

Configuration range: 1~4093

Function: Configure VLAN ID for remote port mirroring.

Destination Port1/Port2

Configuration options: NULL/Port number

Default configuration: NULL

Function: Configure the mirroring destination port.

Description: When the switch works as the source device in remote port mirroring, the

configured destination port is used as the reflector port.

Source Rx

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to mirror packets received on the mirroring source port.

Source Tx

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to mirror packets sent from the mirroring source port.

8.2.4 Typical Configuration Example

As shown in Figure 281, the mirroring destination port is port 2 and the mirroring source port is port 1. Both transmitted and received packets on port 1 are mirrored to port 2.

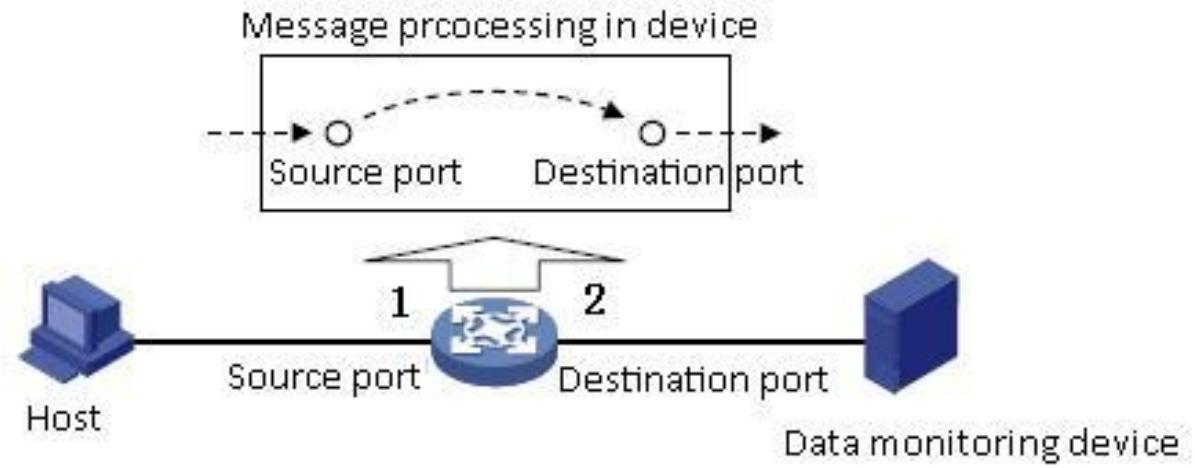


Figure 281 Port Mirroring Example

Configuration process:

1. Enable the local port mirroring function, as shown in Figure 279.

2. Set port 2 to the mirroring destination port, port 1 to the mirroring source port and select port 1 for both Rx and TX, as shown in Figure 279.

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.

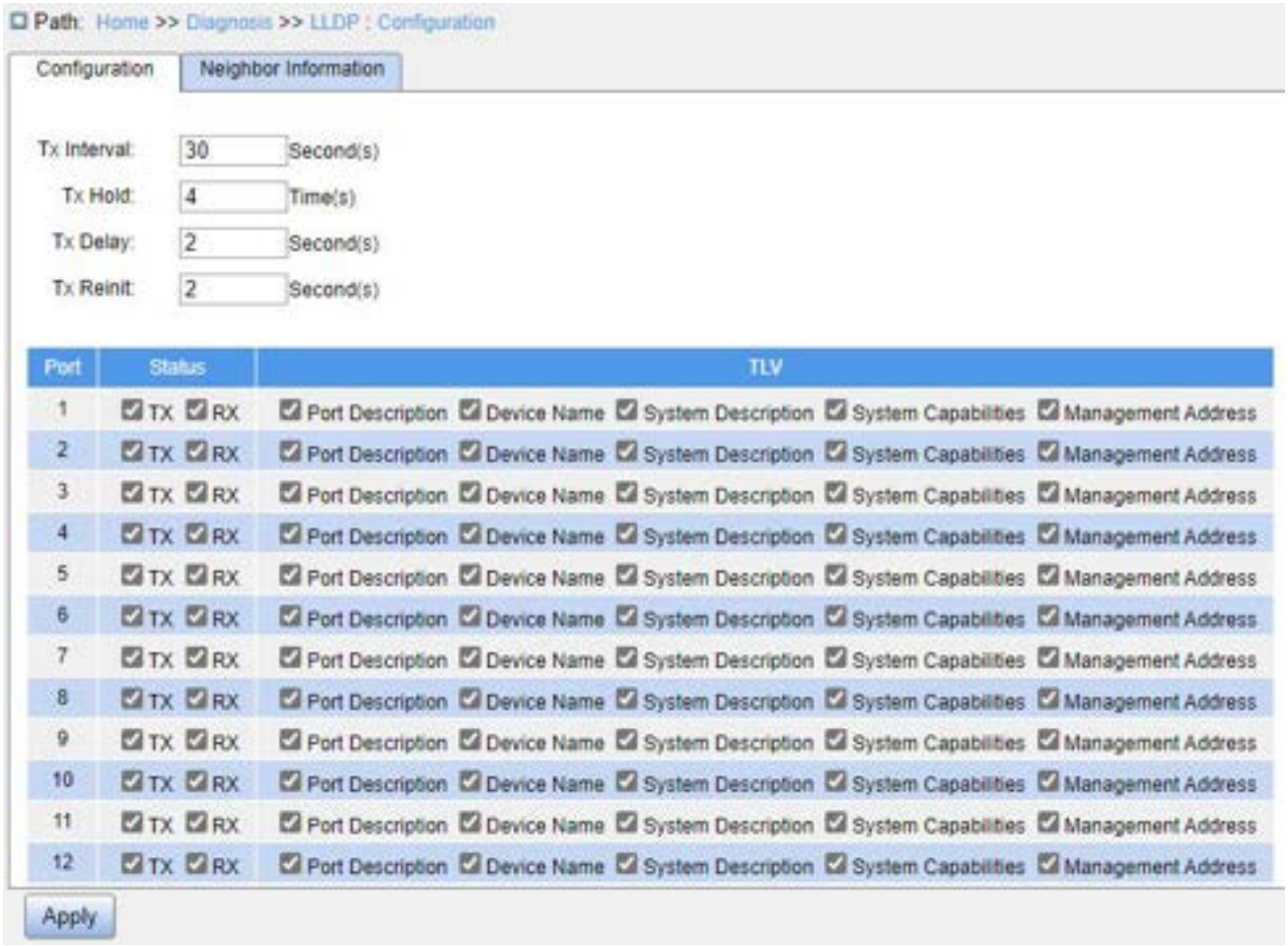


Figure 282 Configure LLDP

TX Interval

Configuration range: 5~32768s

Default configuration: 30

Function: Configure the time interval for sending LLDP packets.

Tx Hold

Configuration range: 2~10 times

Default configuration: 4

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: 2

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: 2

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;
- Disabling 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 Description

Configuration options: Enable/Disable

Default configuration: Enable

Function: “Enable” indicates LLDP packets will carry port description.

Device Name

Configuration options: Enable/Disable

Default configuration: Enable

Function: “Enable” indicates LLDP packets will carry system name.

System Description

Configuration options: Enabled/Disable

Default configuration: Enable

Function: “Enable” indicates LLDP packets will carry system description.

System Capabilities

Configuration options: Enabled/Disable

Default configuration: Enable

Function: “Enable” indicates LLDP packets will carry system capability.

Management Address

Configuration options: Enable/Disable

Default configuration: Enable

Function: “Enable” indicates LLDP packets will carry management address.

2. View LLDP information, as shown below.

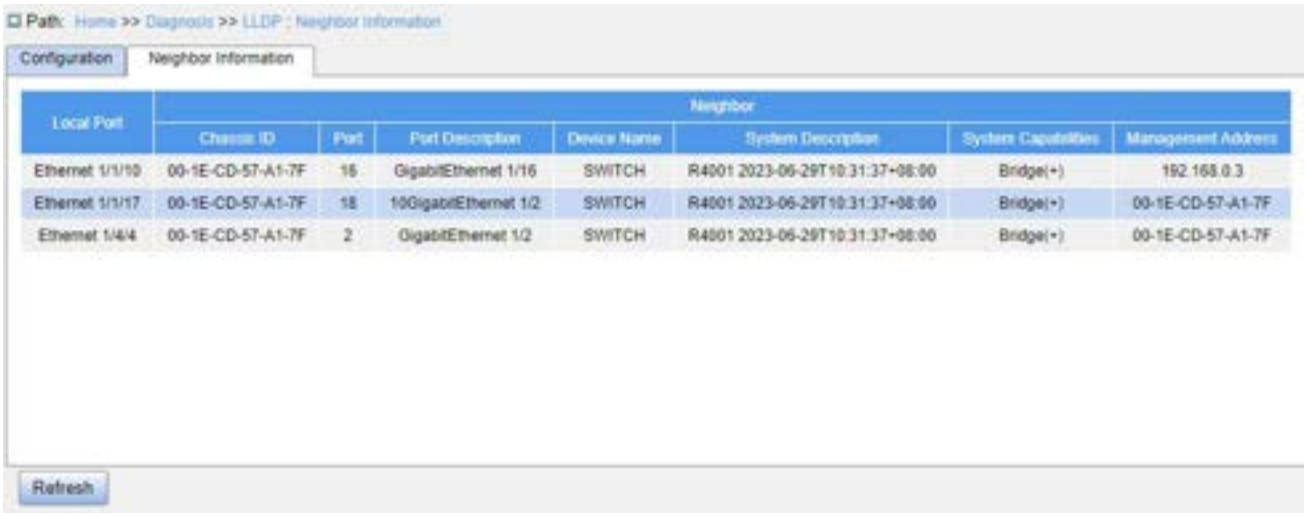


Figure 283 View LLDP Information

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.

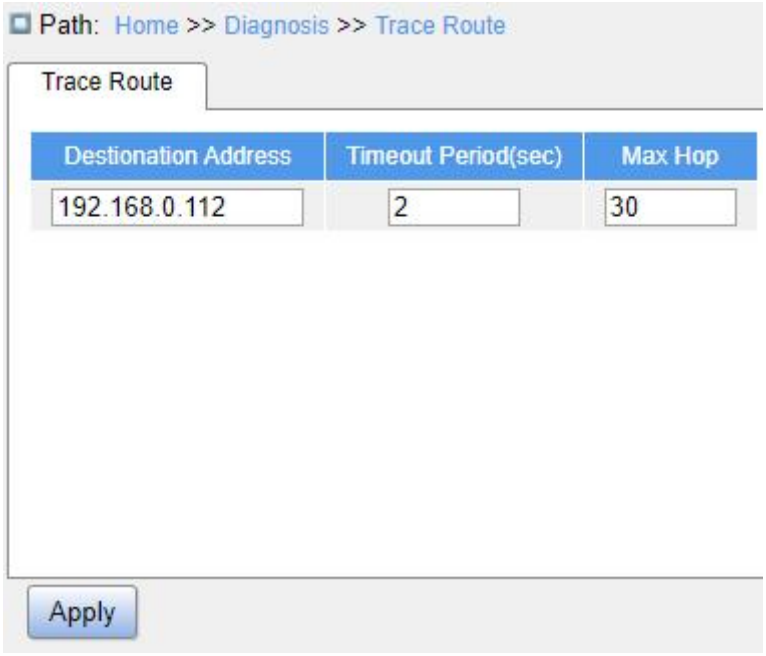


Figure 284 Configure Traceroute

Destination address

Configuration format: A.B.C.D

Function: Configure IP address of destination device.

Timeout Period

Configuration range: 1~10s

Default configuration: 2

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.

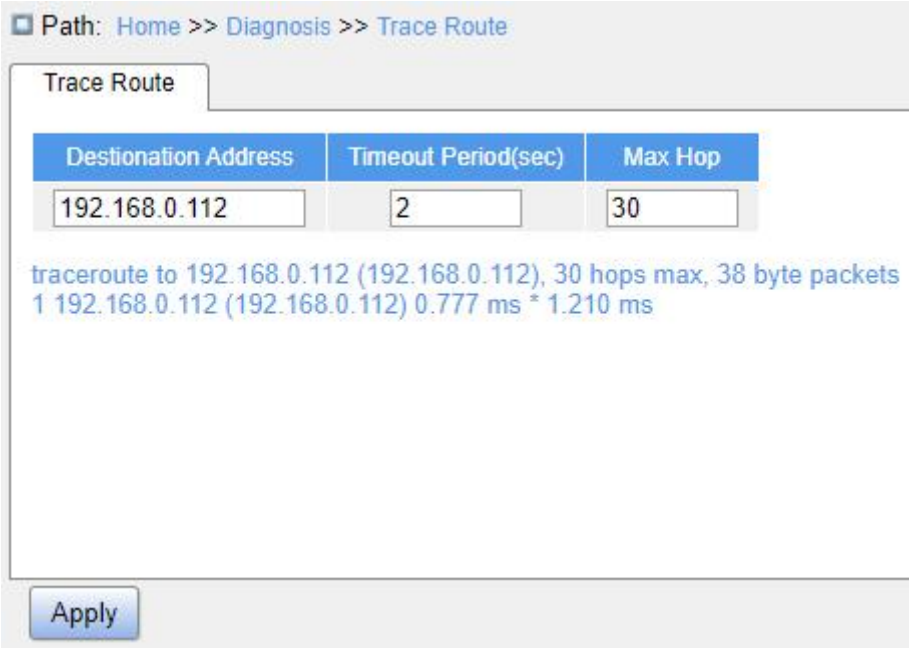


Figure 285 View Output

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 286 Configure Ping Command

Server Address

Configuration format: A.B.C.D

Description: Input the IP address of the destination device.

Ping Length

Configuration range: 2~1452 bytes

Default configuration: 56

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: 1~30s

Default configuration: 1

Function: Specify the interval for sending an ICMP request.

2. View ping output, as shown below.

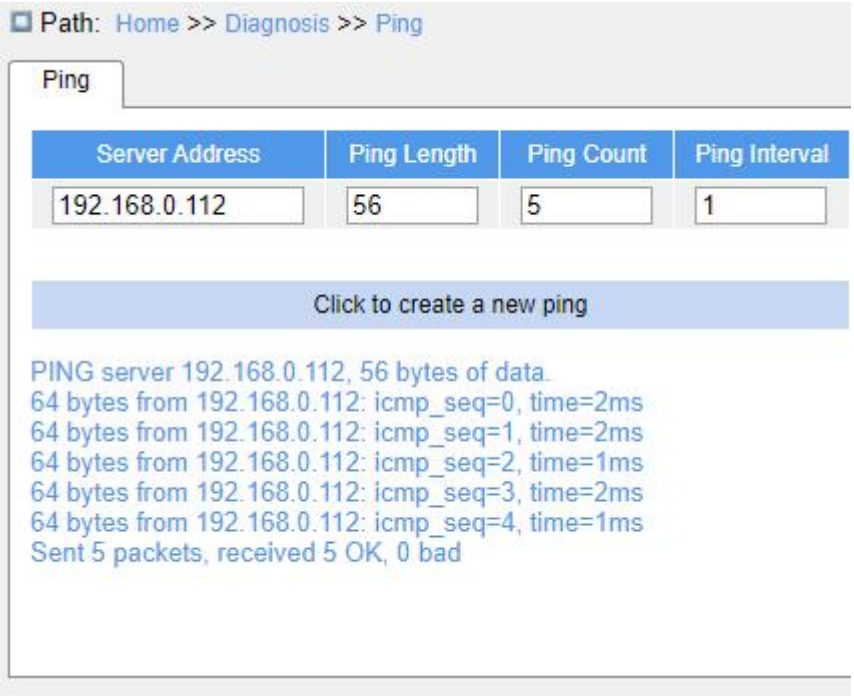


Figure 287 View Ping Output

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 Introduction

Through the binding function of IP source guard, the messages forwarded by the port can be filtered to prevent the illegal messages from passing 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.

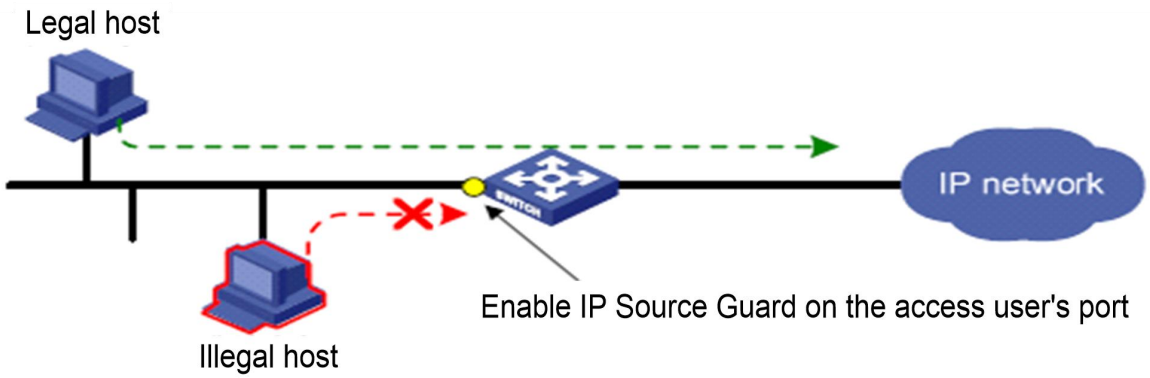


Figure 288 IP Source Guard Function Diagram

8.6.2 Principle

The port configured with this feature searches the 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, it drops the message. Binding function is based on the port. When one port is configured with the binding function, only this port is restricted, while other ports are not affected by the binding.

The feature item of IP source guard includes: source IP address, source MAC address, and VLAN tag. 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 type of binding table items supported by the port is related to the type of the device and depends 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 needs 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 the scenario where there are many hosts in local area network and the

network uses DHCP to configure dynamic hosts. This mode 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.

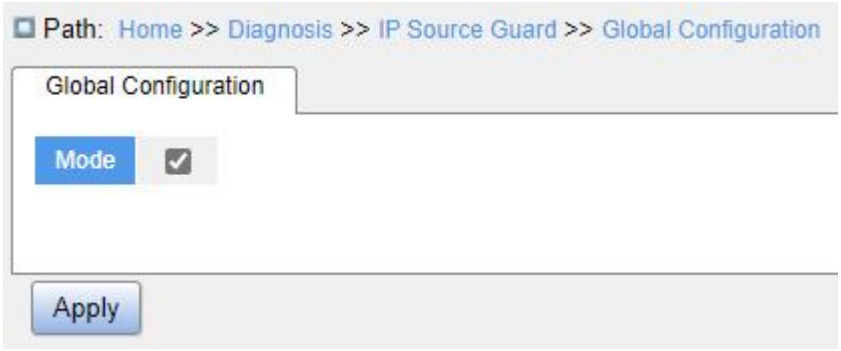


Figure 289 Configure IP Source Guard

Mode

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable global IP source guard.

2. Configure port IP source guard, as shown below.

Figure 290 Configure Port IP Source Guard

Enable

Configuration options: Enable/Disable

Default configuration: Disable

Function: Whether to enable port IP source guard.

3. Configure static binding, as shown below.

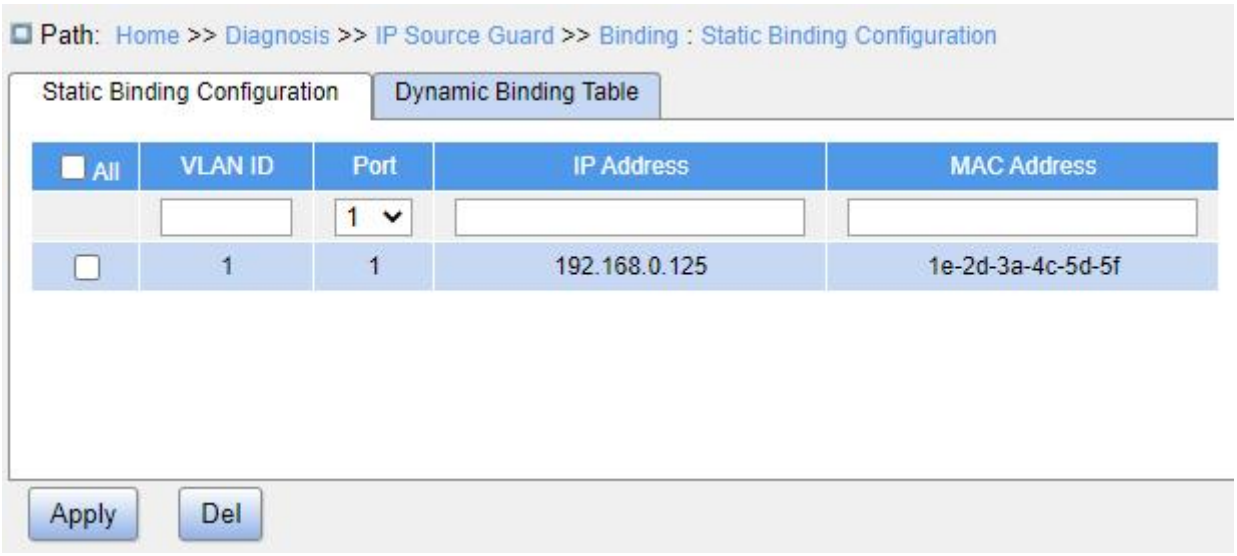


Figure 291 Cofnigure Static Binding

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 or HH:HH:HH:HH:HH:HH (H is a hexadecimal number)

Function: Configure MAC address of static binding table (unicast MAC address).

4. View dynamic binding table, as shown below.

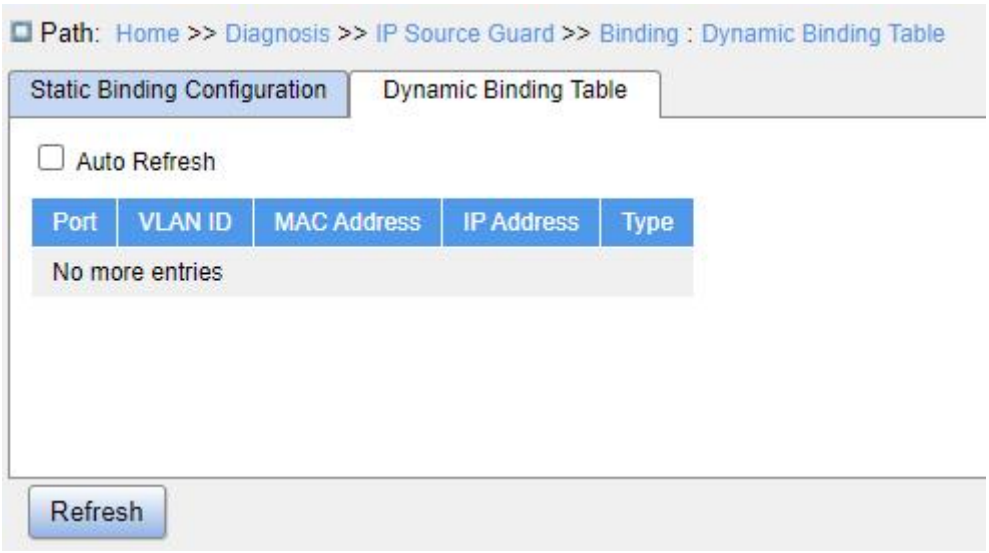


Figure 292 View Dynamic Binding Table

Type

Display options: Relay/Snooping

Description: The dynamic binding table is generated by DHCP Relay and DHCP Snooping devices. The table items of type “Relay” are generated after global IP source guard is enabled. The table items of type “Snooping” are generated after both the global and

ports that connect to the DHCP client have IP source guard enabled.

8.6.4 Typical Configuration Example

8.6.4.1 Relay type IP source guard table items

As shown in Figure 293, Switch A functions as the DHCP server, switch B functions as the DHCP relay, switch C functions as the DHCP client, and 1 port of switch A is connected to the 1 port of switch B, 2 port of switch B is connected to 2 port of switch C. DHCP server is not in the same LAN as the DHCP client. After the relay device enables IP Source Guard, the client dynamically obtains the IP address and other network parameters with DHCP mode through DHCP relay. The relay device generates IP source guard table items.

Figure 293 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 178;
3. Create address pool “pool-33”, as shown in Figure 179;
4. Select address pool type as “Network”; IP address: 33.1.1.6; Mark: 255.0.0.0, as shown in Figure 180;

Switch B configuration:

1. Create VLAN1 and configure IP address: 100.1.1.180;
2. Create VLAN33 and configure IP address: 33.1.1.2;
3. Enable DHCP delay, as shown in Figure 194:
4. Configure server IP address: 100.1.1.156, as shown in Figure 194;
5. Enable the global IP source guard, as shown in Figure 289;

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 switch B, as shown in Figure 292.

8.6.4.2 Snooping type IP Source Guard table items

As shown below, Switch A functions as the DHCP server, switch B functions as the DHCP Snooping, switch C functions as the DHCP client, and 1 port of switch A is connected to the 1 port of switch B, 2 port of switch B is connected to 2 port of switch C. DHCP server is not in the same LAN as the DHCP client. After Snooping device enables IP Source Guard, the client dynamically obtains the IP address and other network parameters with DHCP mode through DHCP Snooping. The relay device generates IP source guard table items.

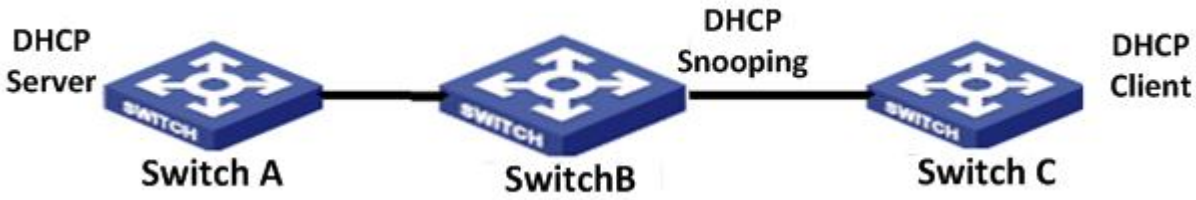


Figure 294 DHCP Typical Configuration Example

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 178;
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 190;
4. Enable global IP source guard, as shown in Figure 289;
5. Enable IP source guard on Port 2, as shown in Figure 290;

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 Introduction

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. View 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.

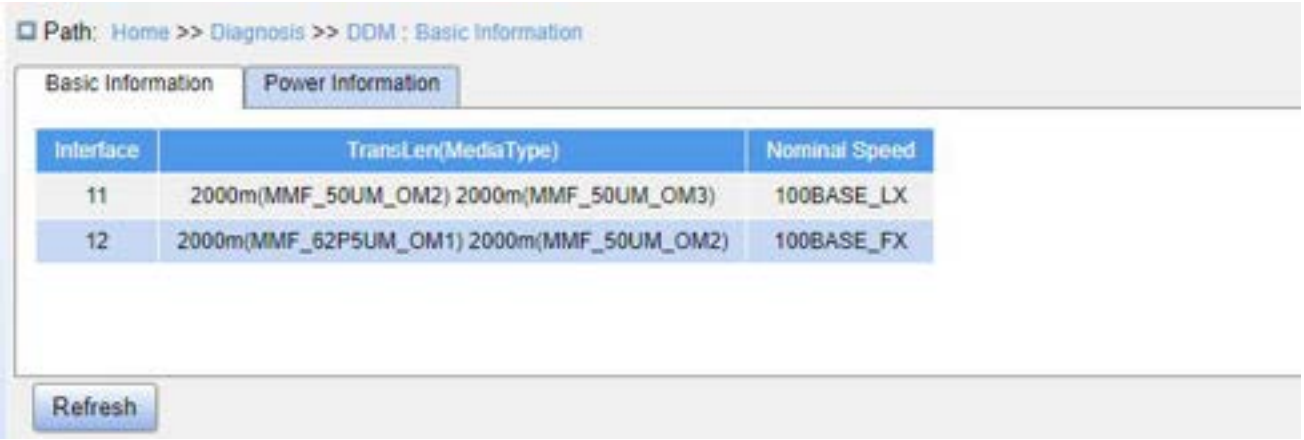


Figure 295 Basic Information of Optical Module

2. View power information.

According to the following path, click to view the optical power information of the optical

module, as shown in the figure below.

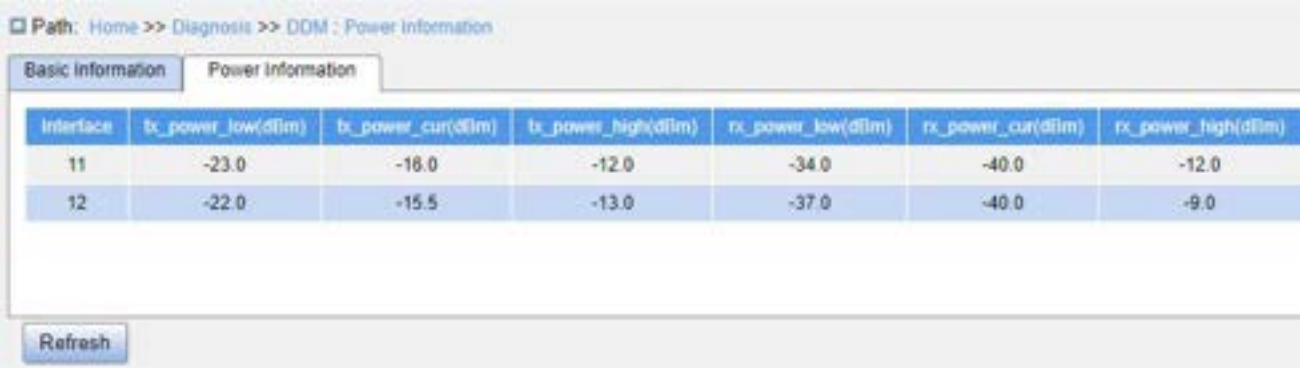


Figure 296 View Power Information

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