PIXE L3 8T 4X-R

Industrial Layer 3

10 Gbps Ethernet Switch

Web Manual

This page left blank intentionally

1 PRODUCT INTRODUCTION

The PIXE L3 8T 4X R is an industrial all-gigabit managed Ethernet switch. Designed and developed by Case Communications and designed to build a high-security and high-performance network. The system adopts a new software and hardware platform, provides a comprehensive security protection system, improves alarm input and output, and is simple to manage and maintain. .

1.1. Product Features

- Support alarm input
- Support alarm output
- Support temperature sensor input
- Support low voltage alarm
- Support high voltage alarm
- Support temperature alarm
- Humidity alarm supported
- Support port alarm
- Support system alarm
- MSTP rapid span tree protocol supporting one-key re network

1.2. [Version Update]

Ver 6.7.3

User optimization of the user experience

Resolves known issues and provides faster response.

Related functions are optimized to make management easier

This page left blank intentionally

2. HARDWARE SPECIFICATIONS

Specifications	Hardware		
Fixed Ports	8*10/100/1000Base-TX PoE port(Data/Power) 4*100/1000 / 2500/ 10000M SFP		
Power Over Ethernet	**Ports 1~2** support IEEE802.3af/at/PoE++/bt, Max 90W PoE out **Ports 3-8** support IEEE802.3af/at, Max 30W PoE out		
PoE Pin	**af (15.4w) /at (30w):** 12+ 36-	**PoE++/bt (90W)** : 12+ 45+ 36- 78-	
PoE Bridge	Max 360W		
CPU	MIPS-34Kc 800MHz	**DDR**	2G DDR3
FLASH	512MBytes	**RAM**	256Gbyte
Backplane	128Gbps	**Packet Forwarding**	71.42Mpps
MAC Addresses	16K	**Buffer**	12Mbit SRAM Packet Buffer
Jumbo Frames	Jumbo frame up to 12KB	Environment	IEEE 802.3az
VLAN Address	4K	**QoS Queue**	8
Link Aggregation	Supports 32 trunk groups with up to 8 members per group		
Layer 3 Routing	IPV4 supports 6K; IPV6 supports 2K;		
LED Indicators	**Port:1-8** LINK LED **Port:1-8** PoE LED **Port: 9-12** SFP LED **V1**: DC 1 IN **V2**: DC 2 IN **SYS:** PoE DOG on/off **PW**: POWER LED		
Power Input	Dual DC POWER Input	**Consumption**	DC48-57V MAX 400W
Temperature	Operating Temperature-40～+75°C; 5%～90% RH Non coagulation, Storage Temperature -45～+85°C; 5%～95% RH Non coagulation		
Dimensions	160mm*130mm*50mm Packaging 310mm*210mm*60mm		
Net Weight / Packaged	1.1kg/1.6kg	**Protection Level**	IP30
Lightning Protection	6KV 8/20us;	**Installation**	DIN Rail

Certifications	
FCC Part 15 Class B; RoHS;	IEC61000-4-6 (Radio Frequency): Level 3
CE-EMC EN55032;	IEC 61000-4-8 (PFMP): Level 5
CE-LVD EN62368;	IEC 60068-2-27 (Shock)
IEC61000-4-2 (ESD): Level 4	IEC 60068-2-6 Vibration
IEC61000-4-3 (RS): Level 4	IEC 60068-2-32 Freefall
IEC61000-4-4 (EFT): Level 4	EN60950-1, UL 60950-1,
IEC61000-4-5 (Surge): Level 4	CSA C22.2 NO 60950-1, UL 508

Features	Port Features
Port Shutdown	Supported
Port Speed	Supports auto-negotiate, full-1000, full-100, half-100, full-10, half-10
Control	Support full-duplex IEEE 802.3x, half-duplex back pressure
Storm Control	Supports rate limit for broadcast, multicast, and DLF packets
Storm Constrain	Supports the detection of broadcast packets, multicast packets, or unicast packets on the port, shutdown the port if the rate is over the threshold.
Port Mirror	Supported
Port Rate Limit	Supports port ingress and egress rate limit
Link Aggregation	Support for manual link aggregation Support for LACP dynamic link aggregation Supports up to 32 aggregation groups, each group up to 8 ports Support for source MAC, destination MAC, source destination MAC, source IP, destination IP, source destination IP routing strategy
Port Isolate	Supported
Jumbo Frame	Support for up to 16KB packet
Redundant Port	Supported
The DDM of fiber ports	Supported

MAC Addresses	
MAC Table Capacity	16K
MAC Table Management	Supported
Forwarding mode	Support IVL forwarding mode
Static MAC Address	Supported
MAC Address Binding	Supported
MAC Address Filtering	Supported
MAC Learning Control	Controls the MAC learning based on port
VLAN	
Number of VLANs	4K
802.1q-based VLAN	Supported
MAC-based VLAN	Supported
IP-based VLAN	Supported
Protocol-based VLAN	Supported
PVLAN	Supported
Voice VLAN	Supported
VLAN Mapping	Support for 1:1 mapping
Q in Q	Support for basic Q in Q and Support for flexible Q in Q
Reliability	
Spanning Tree Protocol	Support for STP/RSTP/MSTP
Port Loop Detection	Supported
EAPS	Supports RFC3619
ERPS	Supports G.8032/Y.1344 Ring Technology
LLDP	Supports LLDP & LLDP-MED
UDLD	Fully compatible with CISCO's UDLD protocol
VLLP (VRRP Layer-2 Loop Protection)	Supported, only used with VRRP
L3 Features	
ARP	Supports static and dynamic ARP
Static Route	Supports static route based on IPv4 and IPv6
VLAN Interface	Supports 32 VLAN interfaces
RIP	Supports RIP v1/v2 & IPv6 RIPng (Configured using the CLI)
OSPF	Supports OSPFv2 & IPv6 OSPFv3 (Configured using the CLI)
BGP	Supports BGP4 & IPv6 BGP4+ (Configured using the CLI)
Policy Routing	Supported
VRRP	Supported
Multicast	
Static Multicast MAC Address	Supported
IGMP SNOOPING	Support IGMP SNOOPING v1/v2/v3 Support IGMP Querier Support IGMP SNOOPING Filter
MVR	Supported
GMRP	Supported
IGMP	Support for IGMP v1/v2/v3
PIM-SM	Supported
Access Control Lists	
Standard IP-based ACL	Supported
Extended IP based ACL	Supported
MAC IP-based ACL	Supported
MAC ARP-based ACL	Supported
ACL Port Filtering	Supported
Time-based ACL	Supported

Quality of Service	
Port Queue Number	8
Port Queue Scheduling Mode	Support WRR, RR, WDRR, SP
Port-based Classification	Supported
802.1p-based Classification	Supported
DSCP-based Classification	Supported
ACL-based Classification	Support ed
QoS Policy	Supports packets mapping to queue Supports COS or DSCP Remarking Supports rate limits of data flow Supports data flow statistics Supports mirroring data flow
DHCP	
DHCP Client	Supported
DHCP Snooping	Supported
DHCP Relay	Supported
DHCP Server	Supported
DHCP option 82	Supported
Security	
Switch Management Security	Supports enabling and disabling TELNET, SSH, HTTP, HTTPS and SNMP services Supports TELNET, SSH, HTTP, HTTPS and SNMP services to bind to standard IP ACLs Support for limiting the number of TELNET and SSH connections
CPU Protection	The switch's own security protection prevents large data streams from attacking the switch itself.
AAA	Supports 802.1x and Support for a RADIUS Server Supports authentication, authorization, and accounting through RADIUS server Supports port-based and MAC-based 802.1x and Support 802.1x guest VLAN
IP MAC Binding	Supports static configuration of IP, MAC and port binding
DHCP SNOOPING	Supports dynamic ARP binding to prevent ARP spoofing Supports dynamic IP, MAC and port binding Support fixed port to connect to DHCP server to prevent private connection to DHCP server
Prevent ARP Spoofing	Supports manually configured MAC ARP-based ACL rules to prevent ARP spoofing. Supports the DHCP SNOOPING function. During the process of obtaining an IP address by DHCP, the switch dynamically binds ARP to the port to prevent ARP spoofing.
PoE	
Switch Control	Supports PoE powering of ports on and off
Power Control	Supports setting total power
Other Advanced Features	Supports PoE scheduling policy and PD online query, etc.
IPv6	
IPv4/IPv6 Dual Protocol Stack	Supported
IPv6 Address	Supports manual address configuration and stateless address auto-configuration
IPv6 Neighbor Discovery	Supported
ICMPv6	Supported
IPv6 Path MTU Discovery	Supported

Management	
CLI Management	Supports Console, Telnet and SSH Supports multiple TELNET connections based on IPv4 and IPv6 Supports multiple SSH connections based on IPv4 and IPv6
WEB Management	Supports HTTP based on IPv4 and IPv6 Supports HTTPS based on IPv4 and IPv6
SNMP Management	Supports SNMP v1, v2c, v3 Supports SNMP TRAP Supports lots of standard and private MIBs Supports SNMP and TRAP based on IPv4 and IPv6
User Management	Supports multiple user management
TACACS+	Supports switch authentication via TACACS+ server remote username and password Supports password encryption in PAP and CHAP mode Supports TACACS+ server to authorise the switch's commands Supports TACACS+ based on IPv4 and IPv6
Log Management	Supports local log management Supports SYSLOG
RMON	Supports RMON 1, 2, 3 and 9 groups
Cluster Management	Supports NDP and Support NTDP Supports manual and automatic joining of cluster groups Supports cluster unified management
Configuration File	Supports uploading and downloading configuration file Supports TFTP transmission based IPv4 and IPv6
Upgrade software	Support TFTP transmission based IPv4 and IPv6
Clock Management	Supports local clock management Supported SNTP
Diagnostics	
PING	Supported
PING6	Supported
TRACEROUTE	Supported
TELNET Client	Supports TELNET client based IPv4 and IPv6
SSH Client	Supports SSH client based IPv4 and IPv6

3. PIXE L3 8T 4X-R Hardware Guide

3.1. Hardware Features

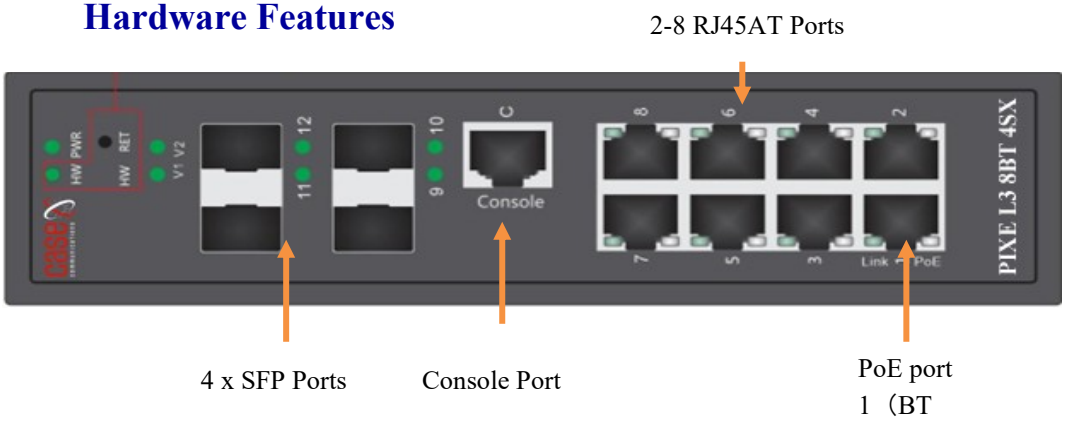


Figure 3-1 Front of the Switch

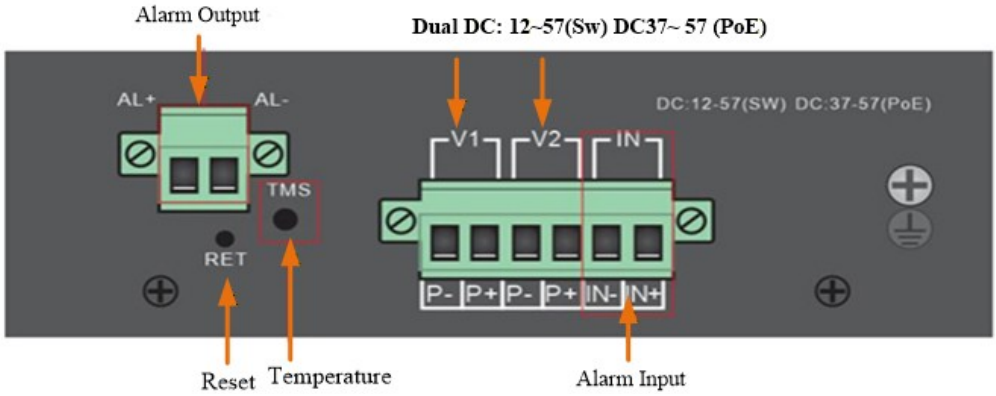


Figure 3-2 Top Interface of the Switch

3.2. Interface Display

Figure 3-2 above is the interface display page of the industrial network management type, which explains the interface function of the industrial network management type.

Alarm output: alarm in on-off mode (input voltage range: 0-57V)

Alarm input: 0-57V(DC) input , low voltage, high and low voltage, etc.

TMS: Temperature Sensor Input

3.3. LED Display

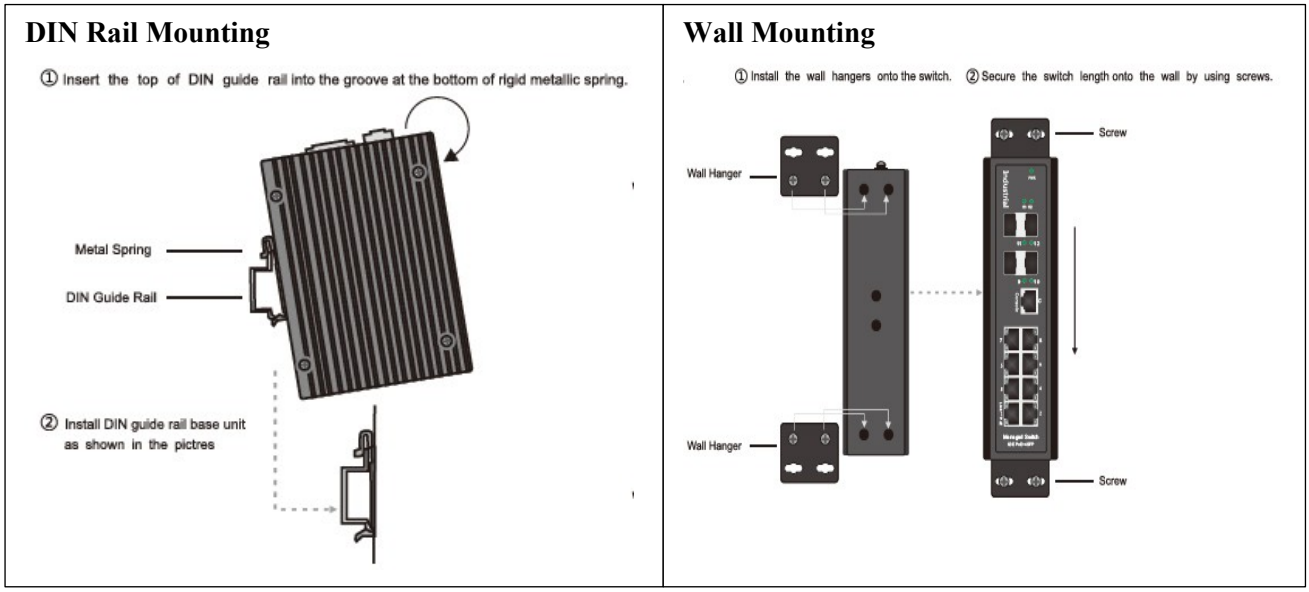
Indicator Front		Status	Description
PWR: Power System Indicator Lights		Always On	System Loading (<30S)/System Crashed (>30S)
		Always Off	Power off / disconnected
		Flicker 1s	System Operation Normal
Network Port Indicator Industrial 8GE + SFP	Giga-Orange	Always On	Corresponding ports operating at 1000M Mode
		Always Off	Corresponding ports at 100Mbps or not communicating
	Link Green	Always On	Corresponding ports operating at 100Mbps
		Always Off	Network Signal not communicated
PoE Port Indicator (Ports 1-8)	PoE Orange	Always On	Device connected and receiving power
		Always Off	Device connected not receiving power
	Link-Green	Always On	Network Signal received
		Always Off	Network Signal Not received

Main Power LEDS

Function Indicator	Status	Description	Function Indicator	Status	Description
N / A	N/A	N/A	9-12 SFP	Always On	SFP Connected
				Always Off	SFP Not Connected
V1 Master Power LED	Always On	V1 Power Normal	V2 Slave Power LED	Always On	V2 Power Normal
	Always Off	No V1 Power		Always Off	No V2 Power
	Flicker ¼ s	V1 Power Abnormal		Flicker ¼ s	V2 Power abnormal
	Flicker 1s	Power normal		Flicker 1s	V2 Power Normal

3.4. Installing on DIN Rail

Figure 3-4 Mounting the PIXE L3 8BT 4SX Switch



3.5. One-key ring network hardware switch

Figure 3-5 b e l o w show the switch to enable the ring network. The table below shows the one-button ring network switch.

One Key Ring Network Hardware Switch

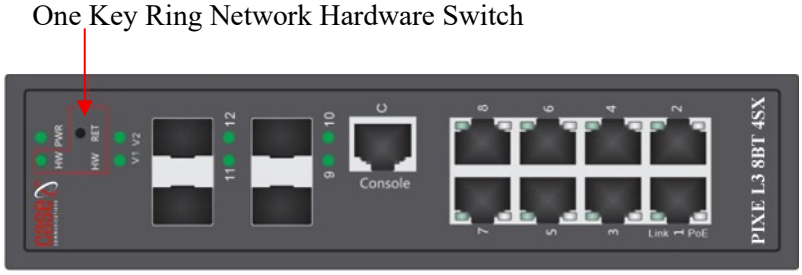


Figure 3-5 One Key Ring switch.

Status	HW indicator	Function	RET
1	Constant extinction	Optical port MSTP Rapid Spanning Tree Protocol shutdown	Open after long press ≥ 10 S
2	CL	Optical port MSTP fast spanning tree protocol enabled	Open and close after long press ≥ 18S

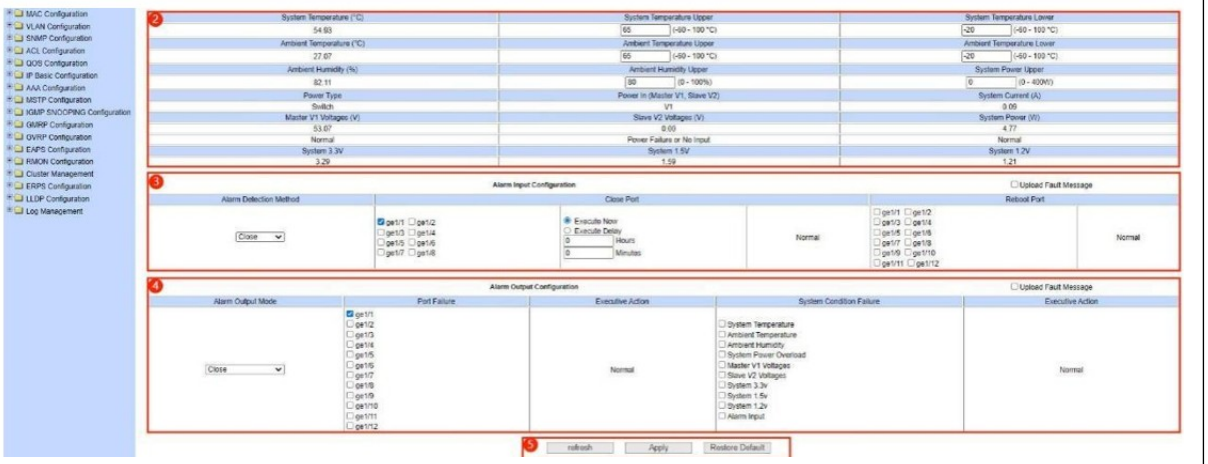
3.6. Introduction network management switch monitoring platform

The sections below explain the monitoring platform interface of the industrial switch, which is mainly divided into these five sections.

Ring network control interface

1. System information display interface
2. Alarm Output Configuration
3. Refresh: Click to refresh the current page.
4. Apply: Click to save the configuration information on this page.
5. Restore Default: Click to restore the configuration information on this page to the factory mode.

Figure 3-6 PIXE L3 8T 4X R monitoring platform page



3.7. Ring Network Control

Figure 3-7 shows the ring network control interface. This page controls the one-key ring network function through the software part.

Enable: Enable the fast ring network function, and the optical interface will start the MSTP rapid spanning tree protocol.

Close: Close the fast ring network function, and the optical interface will close the MSTP rapid spanning tree protocol.

Customization: After it is enabled, the ring network configuration can be customized.

Figure 3-7 Ring Network control	
Ring Control	Ring Status
◯ Enable ◯ Close ◯ Customise	Stop

3.8. Operating Parameters

Figure 3-8 Operating Parameters		
System Temperature (C)	**System Temp (Upper)**	**System Input (Lower)**
51.0	65 (60~00C)	-20 (-60 ~ 100)
Ambient temperature (C)	**Ambient Temp Upper**	**Ambient Temp Lower**
30.15	65 (80~100C)	-20 (-80 ~ 100)
Ambient Humidity %	**Ambient Humidity Upper**	**System Power Upper**
61.40	80 (0~ 100%)	3 (0 ~ 400W)
Power Type	**Power in (Master V1 Save V2)**	**System Current**
Switch	V1	0.09
Master V1 Volts	**Save V2 Voltage (V)**	**System Power (W)**
53.09	0.00	4.77
Normal	**Power Failure or no input**	**Normal**
System 3.3v	System 15v	System 12v
3.28	1.60	12.1

Figure 3-8 above shows the system operating parameters and their ranges

3.9. System Information Display Interface

System temperature – Figure 3-9-1

System temperature: the internal temperature of the switch itself.

Upper limit of system temperature: after setting, when the internal temperature of the switch itself exceeds the set temperature, an alarm will be triggered (alarm mode needs to be configured)

Lower limit of system temperature: after setting, when the internal temperature of the switch itself is lower than the set temperature, an alarm will be trigger ed (alarm mode needs to be configured)

Figure 3-9-1 System Temperature		
System Temp (C)	**System Temp Upper**	**System Temp Lower**
51	65 (60 ~ 100C)	-20 (60~ 100C)

Ambient temperature – Figure 3-9-2

Ambient temperature: display the ambient temperature (the sensor needs to be configured for use)

The upper limit of ambient temperature: After setting, when the ambient temperature of the switch exceeds the set temperature, an alarm will be triggered (the alarm mode needs to be configured)

Lower limit of ambient temperature: After setting, when the ambient temperature of the switch is lower than the set temperature, an alarm will be triggered (the alarm mode needs to be configured)

Figure 3-9-2 Ambient Temperature		
Ambient Temperature (C)	**Ambient Temperature Upper**	**Ambient Temperature Lower**
30.15	65 (60~ 100C)	-20 (-60 ~ 100C)

Power Supply Operating Mode – Figure 3-9-3

Figure 3-9-3 below is the power supply operating mode display page. This page displays the power supply operating mode and current

Figure 3-9-3 Supply Operating Mode		
Power Type	**Power Supply in (Master V1, Slave V2**	**System Current**
Switch	V1	0.09

Input display

Figure 3-9-4 below is the input display page, which shows the input voltage and total Power

Figure 3-9-4 Input Display		
Master V1 Voltage	**Slave V2 Voltage (V)**	**System Power (W)**
53.09	0	4.77
Normal	Power Failure or no input	Normal

3.10. Alarm Input Configuration

Alarm detection mode

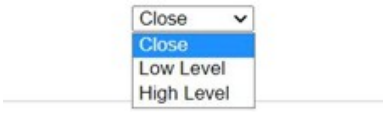
Figure 3-10 shows the alarm detection modes. There are mainly three alarm detection modes.

Close: Close the detection mode after selection

Low voltage alarm: the alarm is triggered after 3V of power supply is detected.

High voltage alarm: the alarm is triggered when the detected voltage is ≥ 3V and ≤ 57V.

Figure 3-10 Alarm Detection method



3.11. Port Shutdown and Restart

Shutdown and Restart Port

Figure 3-11 below shows the interface for selecting the shutdown/restart port. Only one alarm status mode can be selected on this page.

Close the port:

Execute Now: After the alarm occurs, the port will be shut down.

Delayed execution: After the alarm occurs, the port is closed according to the set delay time, and the maximum set time is 100 hours.

Restart port: Restart Port: The port will be restarted after an alarm occurs.

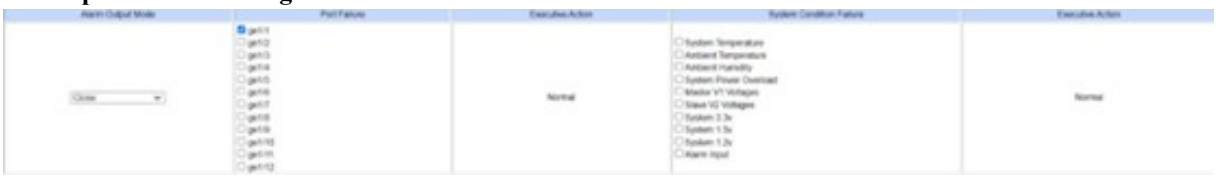
Figure 3-11 Shutdown Port and Restart Port Display

Note: The port alarm detection mode includes PoE power supply + data and non-PoE power supply + data.

3.12. Upload fault message

Figure 3-12 shows the alarm input interface, and the last message of the alarm information can be selected.

3-12 Upload fault message



3.13. Alarm Output Configuration

Alarm output mode

Figure 3-13 below is the display interface of alarm output modes. There are 4 alarm modes.

Alarm off: the default mode, in which the alarm output is in the pass-through state.

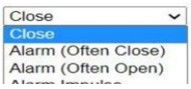
Alarm (normally closed): after the normally closed state is opened, the alarm output is normally off after the alarm is triggered.

Alarm (normally open): After the normally open is turned on, the alarm output is normally open after the alarm is triggered.

Cycle alarm: After the cycle is started, the alarm output is in the on-off cycle state after the alarm is triggered.

Figure 3-13 Alarm Output Mode

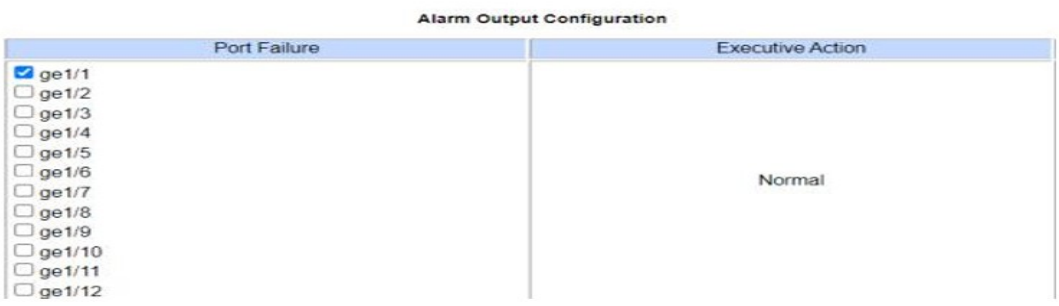
3.14. Port Selection



Port failure and execution action

Figure 13-14 shows the alarm output configuration. The corresponding alarm output port can be selected on this page (to be used in conjunction with the alarm port input setting).

Figure 3.14 Port Failure and Execution Action Display



3.15. System Conditional Failures and Execution Actions

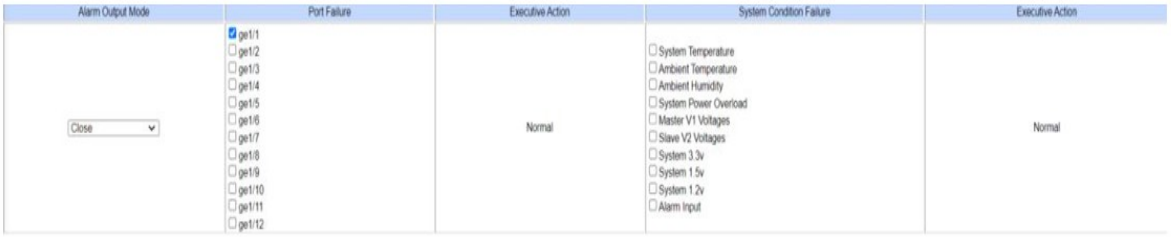
Figure 3-15 is the system and hardware output configuration interface. On this page, you can configure the system alarm information (to be set in conjunction with the system page) and alarm input (to be configured in conjunction with the alarm input).

Figure 3-15 System Conditional Failures and Execution Actions

3.16. Upload Fault Message

Figure 3-16 shows the alarm input interface, and the last message of the alarm information can be selected.

Figure 3-16 Uploading fault Messages



This page left blank intentionally

4. Using a Web Browser for Configuration

This part of the manual describes the WEB Browser in the PIXE L3 8T 4X-R Industrial Ethernet switch. This manual briefly introduces the operation of each WEB page.

4.1. Benefits of using WEB access

The PIXE L3 8T 4X-R provides Web access to the user. Users can access the switch through a Web browser to manage and configure the switch. The main features of WEB access are:

- Easy access: Users can easily access the switch from anywhere on the network.
- Users can use familiar browsers such as Firefox. Google Chrome. Oprea and Microsoft Inter net Explorer (8.0 and above) to access the WEB page on the switch.
  The WEB page is presented to the user in graphical and tabular form.
- The switch provides rich WEB pages.through which the user can configure and manage most of the functions of the switch.
- The classification and integration of WEB page functions are convenient for users to find rele vant pages for configuration and management.

4.2. System requirements for using a Web Browser

Before starting a Web browsing session. the user needs to confirm:
The switch has been configured for an IP address by default.

Table 2	
Hardware and software	System Requirements
CPU	Pentium 586Up
Memory	128MB or more
Resolution	1024 x768-up
colour	More than 256 colours
Browser	Internet Explorer 8.0 or above or Firefox or Google Chrome or Opera. Etc.
Operating system	Microsoft ® Windows XP ®/Windows Vista ®/Windows 7 ®/Windows 8 ®. Linux. Unix. Etc.

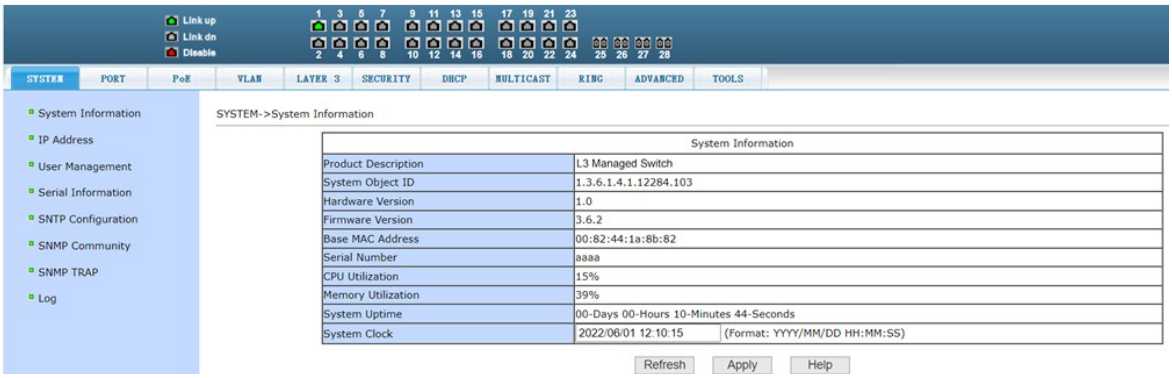
The interface IP address for VLAN 1 on the switch is **192.168.16.1** The subnet mask is 255.255.255.0
A host with a Web browser installed is connected to the network and is able to ping the switch.
After completing the above two tasks. the user enters the address of the switch in the address bar of the browser and presses Enter to enter the Web login page of the switch. as shown in Figure 1. The Web can be accessed only if the correct password is entered.
The default logon parameters are
User Name **root**. By default
Password is **Case** by default.

Figure 4. 2
Login page for a WEB browsing session

4.3. PIXE L3 8T 4X-R Banner Page Basic

As shown in **Figure 4-3** below. the WEB page is composed of four parts: title page. category navigation page. menu page and main page

Figure 4-3 The PIXE L3 8T 4X R banner Page



The banner page is used to display the logo and the real-time port status. as shown in the following figure：

A green light indicates that the port is connected.

A gray light indicates that the port is in an unconnected state.

A red light indicates that the port is down

The **category navigation page** is the function category entry of WEB. The user can click a button to view the corresponding category menu. The right side of the page is the switch model version and logi n user name.

The **menu page** displays the category menu selected by the user from the category navigation page. T here may be a primary or secondary menu. Click the menu item to open the corresponding page.

The **main page** is used to display the page selected by the user from the menu page.

4.4. Introduction to Page Buttons

There are some common buttons on the page. The functions of these buttons are shown in table 4-4 below which describes the functions of these buttons.

	Table 4.4
Button	**Action**
Refresh	Update all domains on the page
application	Place the updated value in memory.Because error checking is done by the Web server. there is no error checking until the user selects the button
delete	Delete the current record
help	Open the help page to view the configuration instructions for each section

4.5. Error Message

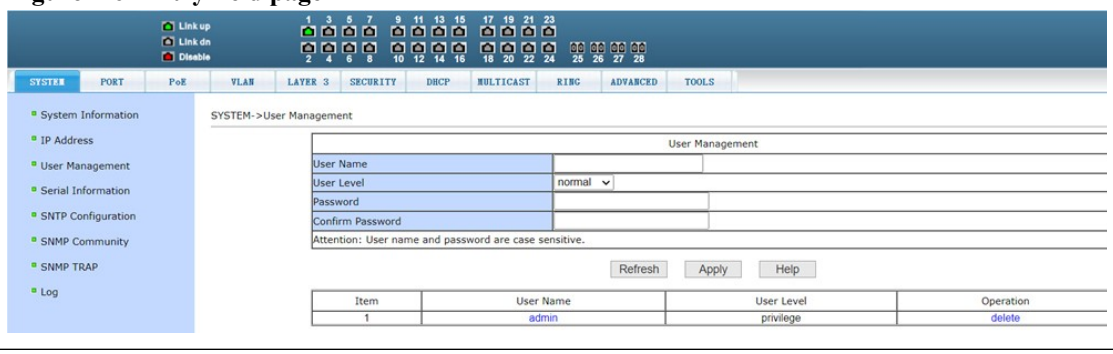
If an error occurs when the switch processes a user request. a corresponding error message is displayed in a dialog box.

Figure 4-5 showing an error message dialog box.

4.6. Entry Field

Some pages have an entry field at the beginning as shown in Figure 4-6 below, through which different entries can be accessed. When you select a value in an entry field. the corresponding information for that row is displayed on the page. and the contents of the row are edited. The row is also called the active row.

Figure 4-6 Entry field page



This page left blank intentionally

5. WEB Configuration Manual

The WEB pages of the PIXE L3 8T 4S-R switch are organized into groups. and each group includes one or more WEB pages. Each page is described below.

5.1. System configuration

Figure 5-1 below is the system information configuration page. through which the user can configure and view the system information of the **switch.**

Product Model: The product model description of the switch

Firmware Version Information: The firmware version currently used by the switch

Bootrom version information: The version of Bootrom currently used by the switch

Base MAC Address: The base MAC address of the switch

Serial Number: The serial number of the switch

Serial port baud rate: serial port baud rate used by the switch

System startup time: the time since the switch was started

System clock (modifiable): the current clock of the system; year. month. day. hour. minute and sec ond are required to be input

5-1 System Information Page

SYSTEM->System Information

System Information	
Product Description	L3 Managed Switch
System Object ID	1.3.6.1.4.1.12284.103
Hardware Version	1.0
Firmware Version	3.6.2
Base MAC Address	00:82:44:1a:8b:82
Serial Number	aaaa
CPU Utilization	2%
Memory Utilization	39%
System Uptime	00-Days 00-Hours 14-Minutes 00-Seconds
System Clock	2022/06/01 12:13:32 (Format: YYYY/MM/DD HH:MM:SS)

Refresh Apply Help

5.2. IP address configuration page

Figure 5-2 below is the IP address configuration page. The user can configure the IP address. subnet mask. and gateway address of the switch through this page. The management VLAN is 1 by default and cannot be modified.

Figure 5-2 IP Address Configuration Page

SYSTEM->IP Address

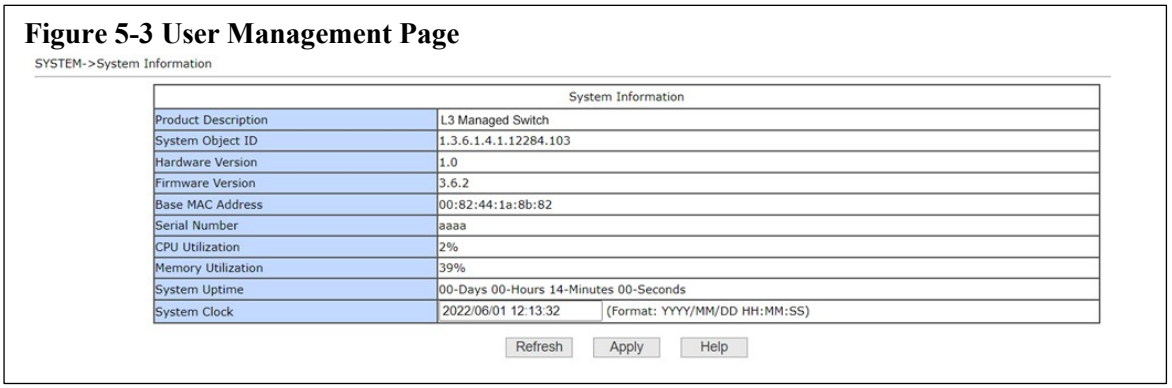
IP Address	
Admin VLAN	1
IP Address	192.168.2.220
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
MAC Address	00:82:44:1a:8b:82
Attention: Please configure carefully. If WEB connection is interrupted after the configuration, please try establish a new connection with the new IP Address.	

Refresh Apply Help

5.3. User management page

Figure 5-3 below is the user management page. through which user information can be configured. The default user name of the switch is **root**. which cannot be changed, and the default password is **case** can also be changed.

Figure 5-3 User Management Page



5.4. Serial port information

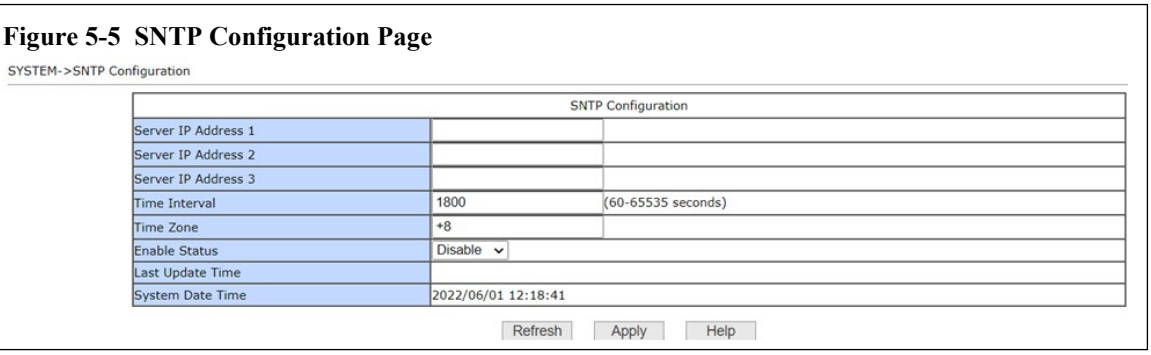
Figure 5-4 shown below is the serial port information page. through which you can view the serial port information.

Figure 5-4 Serial Port Information Page

5.5. SNTP Configuration

Figure 5-5 below is the SNTP configuration page. through which the administrator can configure and view the system clock.

Figure 5-5 SNTP Configuration Page

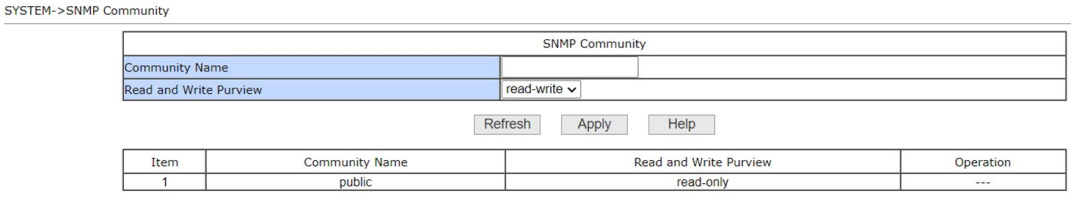


5.6. SNMP Community Configuration Page

Figure 5-6 below shows the SNMP Community Configuration page. This page allows the user to configure the name and read and write permissions of the community for the switch. A total of eight entries can be configured. By default. the switch has a community with a public name that is read-only. When the switch needs to be managed through SNMP. It is necessary to configure a common body with readable and writable permissions.

The configured community cannot be modified and cannot be added with the same name as the existing one. However. you can click the corresponding delete link to delete the community and then reconfigure it

Figure 5-6 SNMP Community Configuration Page



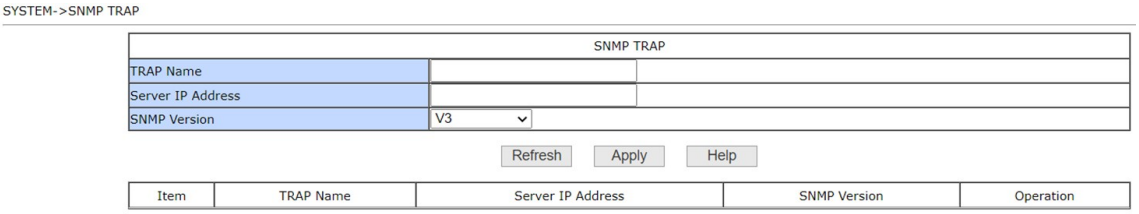
5.7. SNMP TRAP Configuration Page

Figure 5-7 below shows the SNMP TRAP configuration page. which allows the user to configure the IP address of the station receiving the TRAP message and some parameters of the TRAP protocol package.

Enter the TRAP name. the IP address of the TRAP server. and select the version number. If the confi guration is successful after submission. the SNMP TRAP function will work. Once link up or link do wn occurs. the switch will automatically send the TRAP packet to the target address.

Configured TRAP targets cannot be modified and added without duplicating an existing name. However. you can click the corresponding delete link to delete the TRAP target and then reconfigure it.

Figure 5-7 SNMP TRAP Configuration Page



5.8. Log information

Figure 5-8 below is the log information page through which the user can view the log. Select the priority from the drop-down list to view the log of this level. Click Refresh to view the latest log.

Figure 5-8 Log Information Page

This page left blank intentionally

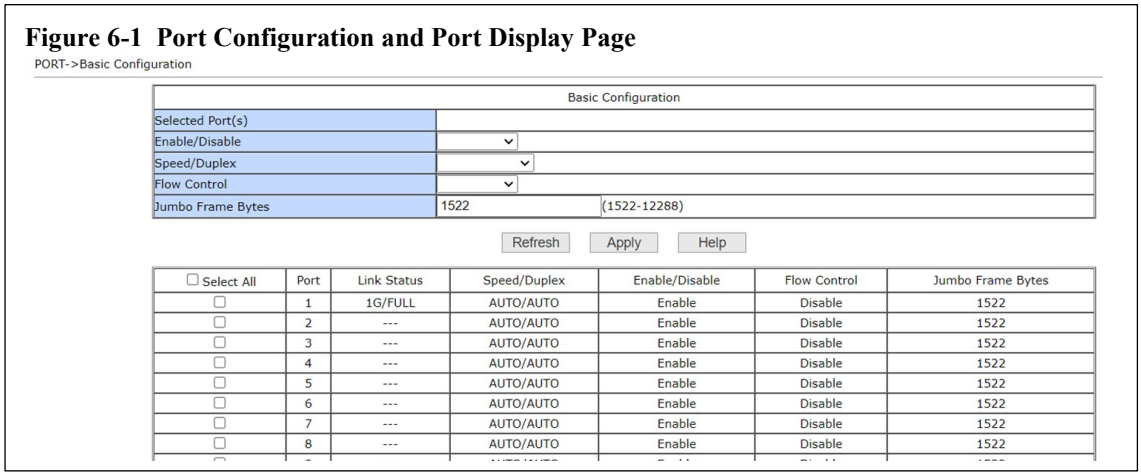
6. Port Configuration page

6.1 Basic Port Configuration

Figure 6-1 below shows the port basic configuration page. From this page. users can enable or disable ports. set port rates and flow control. or view the basic information of all ports.

To modify the port configuration. the user needs to check the left side of the corresponding port or use the "Select All" function. The selected ports will be displayed at the top of the page. and several consecutive ports will be represented by connection numbers. After successful setting. the selected port will be configured with the same parameters. The list on the page shows the configuration information for all ports

Figure 6-1 Port Configuration and Port Display Page



6.2 Port Statistics Page

Figure 6-2 below shown is the Port Statistics page. The page lists the number of packets sent. bytes sent. packets received. bytes received. error packets. and dropped packets for all ports.

Figure 6-2 Port Statistics Page

PORT->Port Statistics

Port	Send Packets Num	Send Octets Num	Received Packets Num	Received Octets Num	Error Packets Num	Discard Packets Num
1	1442	1117749	15061	2068397	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0
11	0	0	0	0	0	0
12	0	0	0	0	0	0
13	0	0	0	0	0	0
14	0	0	0	0	0	0
15	0	0	0	0	0	0
16	0	0	0	0	0	0
17	0	0	0	0	0	0
18	0	0	0	0	0	0
19	0	0	0	0	0	0
20	0	0	0	0	0	0
21	0	0	0	0	0	0
22	0	0	0	0	0	0
23	0	0	0	0	0	0
24	0	0	0	0	0	0
25	0	0	0	0	0	0
26	0	0	0	0	0	0
27	0	0	0	0	0	0
28	0	0	0	0	0	0

Refresh Help

6.3 Port Storm Suppression Page

Figure 6-3 below shows the port storm suppression page. This page is used to configure the suppression of broadcast. multicast. and DLF packets on a port.
Check on the left side of the corresponding port. or use the "Select All" function to select the port to turn on and off the broadcast suppression. multicast suppression and DLF suppression of the port. The suppression rate type item and the suppression rate item are used to select the suppression rate type and suppression rate value to be configured. The suppression rate range is 1-1024000. and the unit is kbits. The suppression rates of broadcast suppression. multicast suppression and DLF suppression can be configured independently. The list on the page shows the configuration information for all ports.

Figure 6-3 Broadcast Storm Suppression Page

PORT->Storm Control

Storm Control					
Selected Port(s)					
Broadcast Suppression		Multicast Suppression		DLF Suppression	
Ratelimit	(1-1024000 kbps)				

Refresh Apply Help

Select All	Port	Broadcast Suppression	Multicast Suppression	DLF Suppression	Ratelimit(kbps)
	1	Disable	Disable	Disable	64
	2	Disable	Disable	Disable	64
	3	Disable	Disable	Disable	64
	4	Disable	Disable	Disable	64
	5	Disable	Disable	Disable	64
	6	Disable	Disable	Disable	64
	7	Disable	Disable	Disable	64
	8	Disable	Disable	Disable	64
	9	Disable	Disable	Disable	64
	10	Disable	Disable	Disable	64
	11	Disable	Disable	Disable	64
	12	Disable	Disable	Disable	64

6.4 Port speed limit page

Figure 6-4 below shows the port speed limit page. This page is used to configure the port ingress and egress speed limits.
Check on the left side of the corresponding port. or use the "Select All" function to select the port. The inlet/outlet port speed limit can be enabled independently by checking. The speed limit range is 1-1024000. and the unit is kbits. If the check is cancelled. the speed is not limited. The list on the page shows the configuration information for all ports.

Figure 6-4 Port Speed Limit Page

PORT->Port Rate

Port Rate	
Selected Port(s)	
Receive Packets Rate Control	enable (1-10240000 kbps)
Send Packets Rate Control	enable (1-10240000 kbps)

Refresh Apply Help

Select All	Port	Receive Packets Rate Control(kbps)	Send Packets Rate Control(kbps)
	1	---	---
	2	---	---
	3	---	---
	4	---	---
	5	---	---
	6	---	---
	7	---	---
	8	---	---
	9	---	---
	10	---	---

6.5 Protection Port

Figure 6-5 below is the protection port setting interface. This page is used to configure/display protection port information.

Figure 6-5 Protection Port Page

PORT->Protected Port

Select All	Port	Is Protected Port
☐	1	No
☐	2	No
☐	3	No
☐	4	No
☐	5	No
☐	6	No
☐	7	No
☐	8	No
☐	9	No
☐	10	No
☐	11	No
☐	12	No
☐	13	No
☐	14	No
☐	15	No
☐	16	No
☐	17	No
☐	18	No

6.6 Port mirroring configuration page

Figure 6-6 below shows the port mirroring configuration page. which allows the user to configure port mirroring. Port mirroring is to monitor the data packets output by the mirrored output port and the data packets input by the mirrored input port through the mirroring port. Only one mirror port can be selected. and multiple mirrored output ports and mirrored input ports can be selected. When configuring. select a mirror port first. and select "Do not mirror" to cancel the mirror configuration. Then select the port and direction to be mirrored from the other ports. When the ingress port in the monitoring direction is selected. it means to monitor the received data packets. and the egress port means to monitor the sent data packets. Ticking both means to monitor all the sent and received data packets.

Figure 6-6 Port Mirror Configuration Page

PORT->Port Mirror

Listen Port: unset

Port	Listen Direction	Port	Listen Direction
1	☐ recieve ☐ transmit	2	☐ recieve ☐ transmit
3	☐ recieve ☐ transmit	4	☐ recieve ☐ transmit
5	☐ recieve ☐ transmit	6	☐ recieve ☐ transmit
7	☐ recieve ☐ transmit	8	☐ recieve ☐ transmit
9	☐ recieve ☐ transmit	10	☐ recieve ☐ transmit
11	☐ recieve ☐ transmit	12	☐ recieve ☐ transmit
13	☐ recieve ☐ transmit	14	☐ recieve ☐ transmit
15	☐ recieve ☐ transmit	16	☐ recieve ☐ transmit
17	☐ recieve ☐ transmit	18	☐ recieve ☐ transmit
19	☐ recieve ☐ transmit	20	☐ recieve ☐ transmit
21	☐ recieve ☐ transmit	22	☐ recieve ☐ transmit
23	☐ recieve ☐ transmit	24	☐ recieve ☐ transmit
25	☐ recieve ☐ transmit	26	☐ recieve ☐ transmit
27	☐ recieve ☐ transmit	28	☐ recieve ☐ transmit

Attention: select the unset option and click the button Apply to delete the configuration.

Refresh Apply Help

6.7 Link Aggregation Configuration Part

Figure 6-7-1 below shows the link aggregation configuration page. The page lists all ports vertically and all aggregation groups horizontally. To add a port to an aggregation group. just click the radio box at the intersection of the row and column. You can also select the aggregation method at the bottom of each aggregation group. If you want to cancel the aggregation configuration of the specified port. click the leftmost radio box corresponding to the port.

Figure 6-7-1 Create Aggregation Group Page

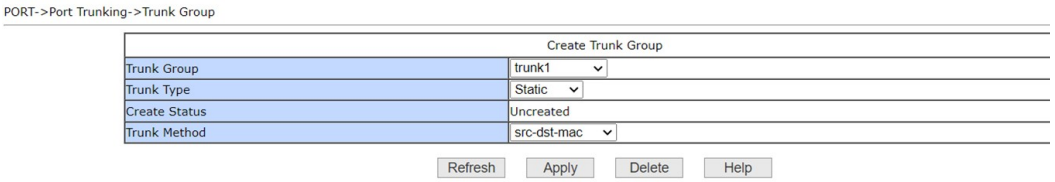


Figure 6-7-2 below shows the interface for configuring the aggregation group. This page is used to configure the aggregation group.

Figure 6-7-2 Configure Aggregation Group Page

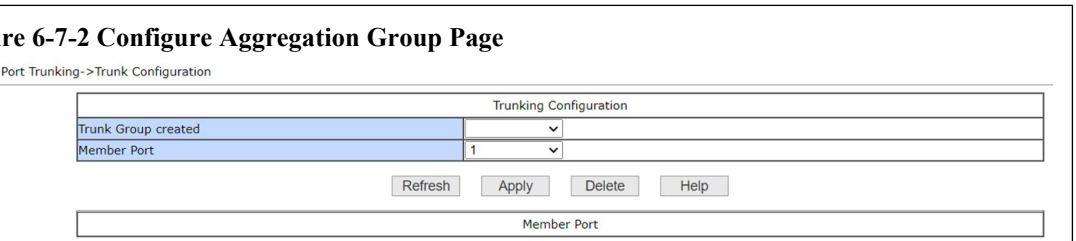
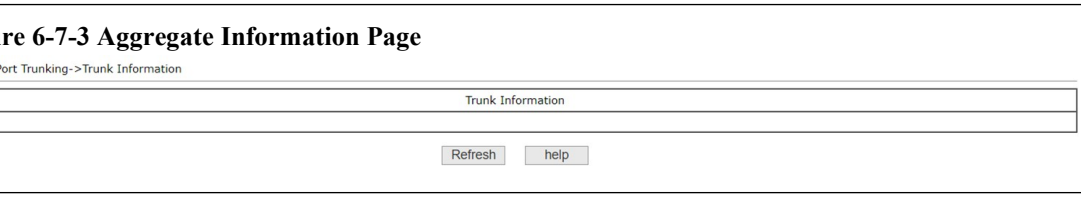


Figure 6-7-3 below shows the interface for viewing aggregated information. This page is used to view aggregation information for a link aggregation.

Figure 6-7-3 Aggregate Information Page



6.8 DDM information

Figure 6-8 below shows the DDM information viewing interface. This page is used to view the corresponding information of the optical module

Figure 6-8 DDM Information Page

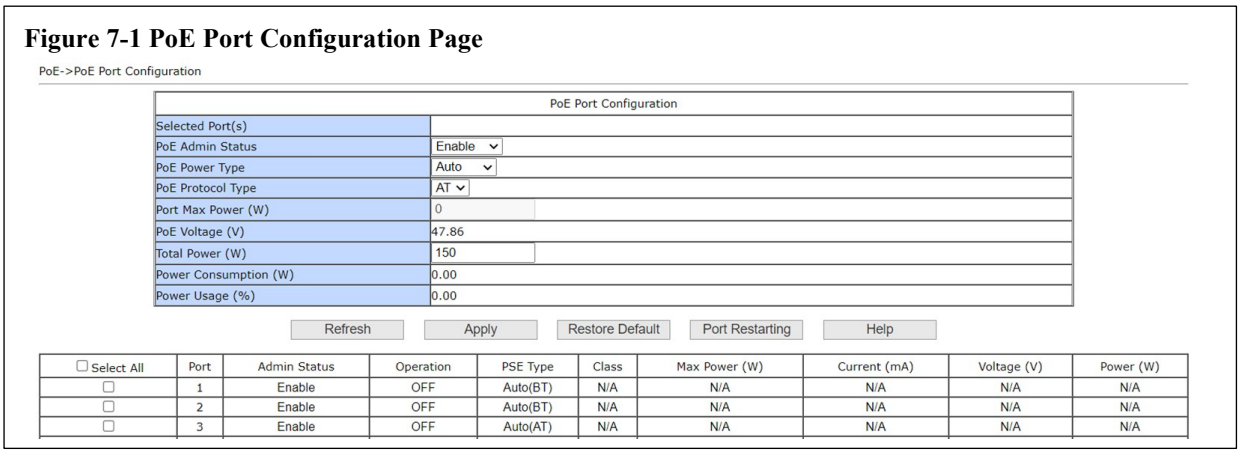
7. PoE Configuration

7.1 PoE Port Configuration

Figure 7-1 below is the PoE port configuration page. through which you can configure the total power of the PoE device (to be updated by the system). PoE single-port power (to be updated by the system). and PoE on or off; through this page. you can view the relevant information of the current PoE device.

- PoE port: Select the power supply port number (1-24)
- PoE port status: enable or disable

Figure 7-1 PoE Port Configuration Page

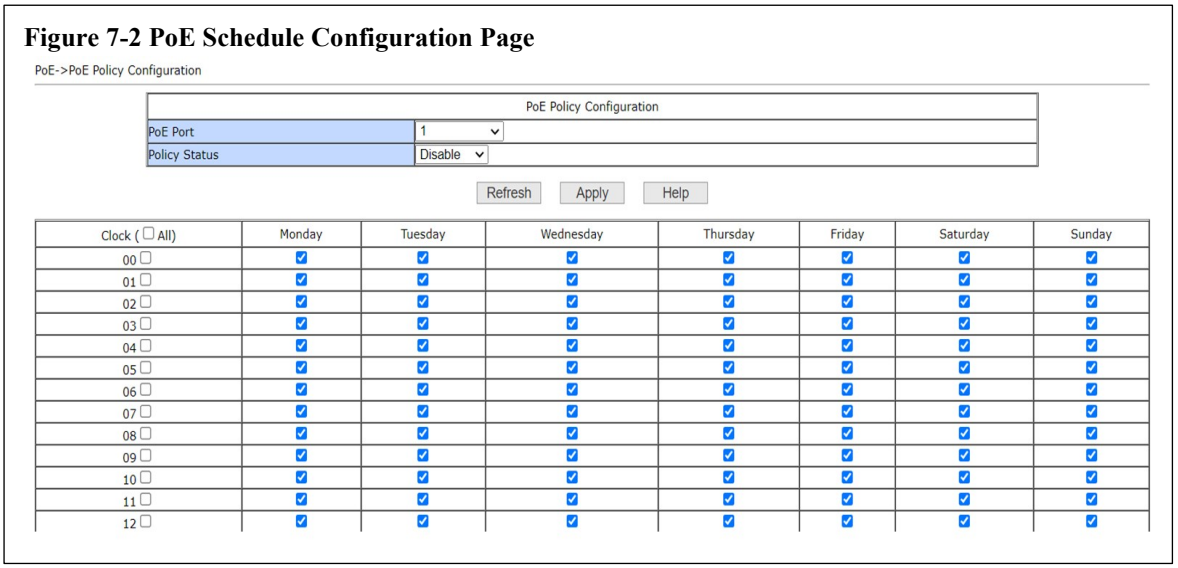


7.2 PoE scheduling configuration

Figure 7-2 shown below is the PoE scheduling configuration page. Through the scheduling management. the PoE power supply can be turned on or off according to the actual needs. The control mode is hour + week.

- **Control Port:** Used to select the port (1-24) to be scheduled for management
- **Control function**: enable or disable

Figure 7-2 PoE Schedule Configuration Page



7.3 PD Query Configuration

Figure 7-3 shown below shows the PD query configuration page. through which the PD online device status detection can be realized.

PoE Port: used to select the port connected to the PD device to be queried

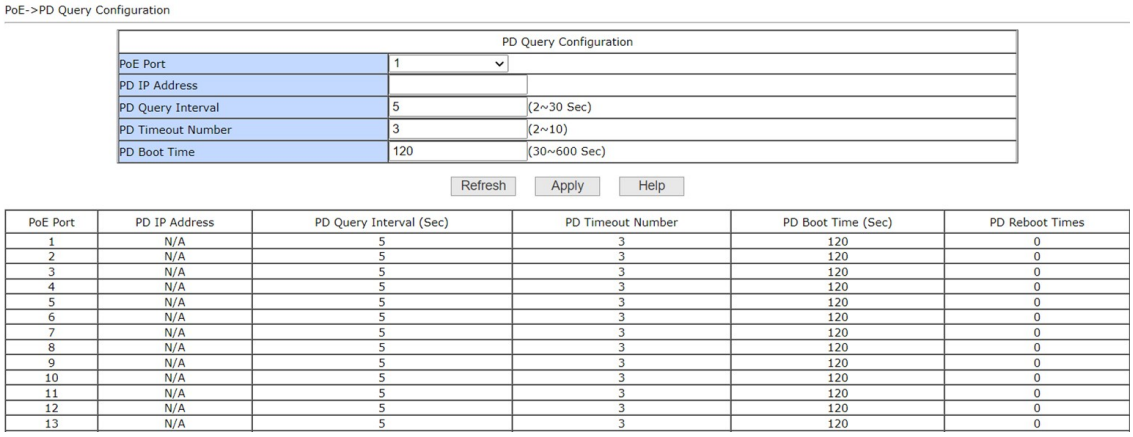
PD IP address: IP address of the PD device.

PD query interval: the time interval for querying PD devices (5 seconds by default).

Maximum times of PD query without response: used to query the maximum times of PD device without response (3 times by default)

Maximum time required for PD startup: used to query the maximum time required for PD device startup (default 120 seconds)

Figure 7-3 PD Query Configuration Page



PoE Port	PD IP Address	PD Query Interval (Sec)	PD Timeout Number	PD Boot Time (Sec)	PD Reboot Times
1	N/A	5	3	120	0
2	N/A	5	3	120	0
3	N/A	5	3	120	0
4	N/A	5	3	120	0
5	N/A	5	3	120	0
6	N/A	5	3	120	0
7	N/A	5	3	120	0
8	N/A	5	3	120	0
9	N/A	5	3	120	0
10	N/A	5	3	120	0
11	N/A	5	3	120	0
12	N/A	5	3	120	0
13	N/A	5	3	120	0

8. VLAN Configuration

8.1 Configuration Page

Figure 8-1 below shows the VLAN configuration page. This page allows the user to create VLANs and displays information for all VLANs.

If you want to create a new VLAN. enter the VID in the active line from 2 to 4094. The switch creates VLAN 1 by default. and VLAN 1 cannot be deleted.

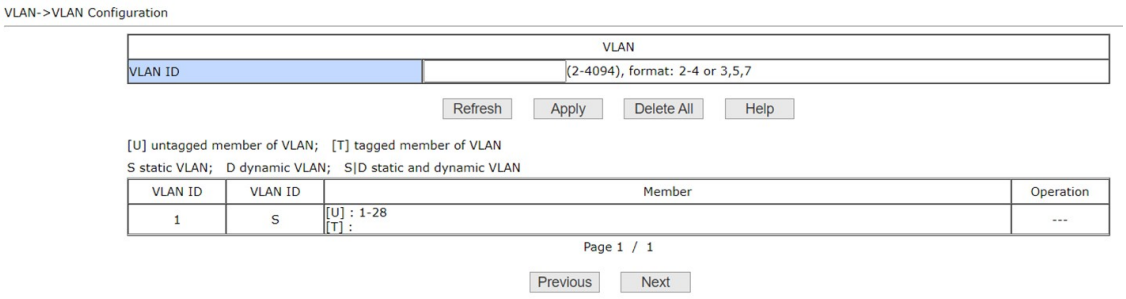
If you want to create a new VLAN. enter the VID in the active line from 2 to 4094. The switch creates VLAN 1 by default. and VLAN 1 cannot be deleted.

The VLAN list displays all created VLANs and indicates the port membership of each VLAN. A port may not be a member of a VLAN. and may be a tagged or untagged member of a VLAN. The characters before the port on the page have the following meanings:

T tagged The port is a tagged member of this VLAN

U untagged The port is an untagged member of this VLAN

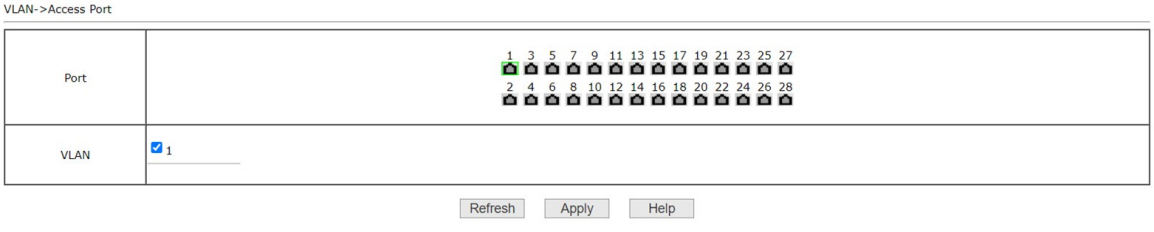
Figure 8-1 VLAN Configuration Page



8.2 Access Port Configuration Page

Figure 8-2 below shows the Access Port Configuration page. which displays and configures the Port Access Mode and the VLAN to which it belongs. The page is divided into two parts: port list and VLAN list. Hover the mouse on the port to see the VLAN mode of the port. Click a port to display/configure the VLAN of the port. If the port is in Access mode. its VLAN can be displayed when it is selected. If other VLANs are selected and applied. the VLAN of the port is changed. If the port is not in Access mode. the port is changed to Access mode after configuration and the VLAN is set. **Note** that only one VLAN can be selected in Access mode

Figure 8-2 Access Port Configuration Page

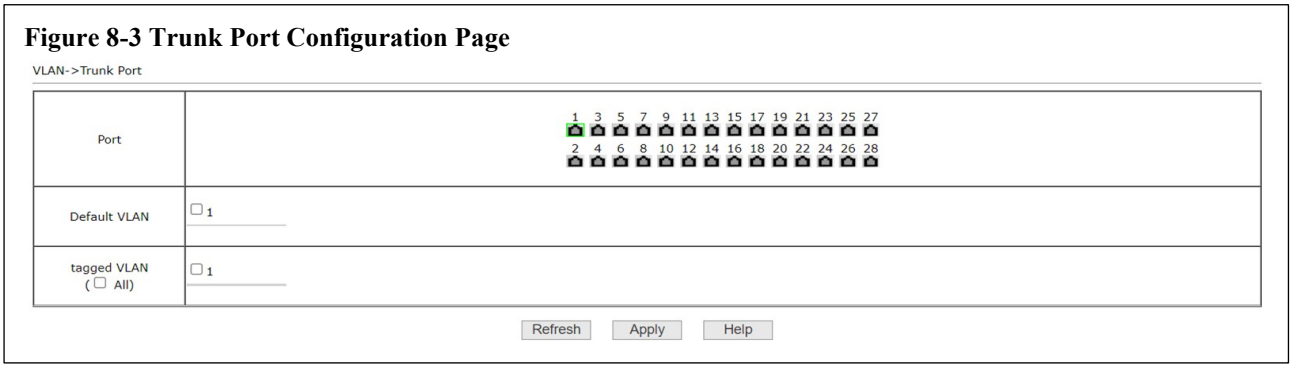


8.3 Trunk Port Configuration Part

Figure 8-3 below shows the Trunk Port Configuration page. which displays and configures the port Trunk mode and the VLAN to which it belongs. This page is divided into two parts:
port list and VLAN list.
For the operation of the port, please refer to Section 2 (Access Port Configuration Page).
If the port is in Trunk mode, its VLAN can be displayed when it is selected. If other VLANs are selected and applied the VLAN of the port is changed.
If the port is not in Trunk mode after configuration the port is changed to Trunk mode and the VLAN is set. Multiple VLANs can be selected in Trunk mode.
To select a group of consecutive VLANs.

- Select the first one.
- press and hold the Shift key.
- Then select the last one

Figure 8-3 Trunk Port Configuration Page

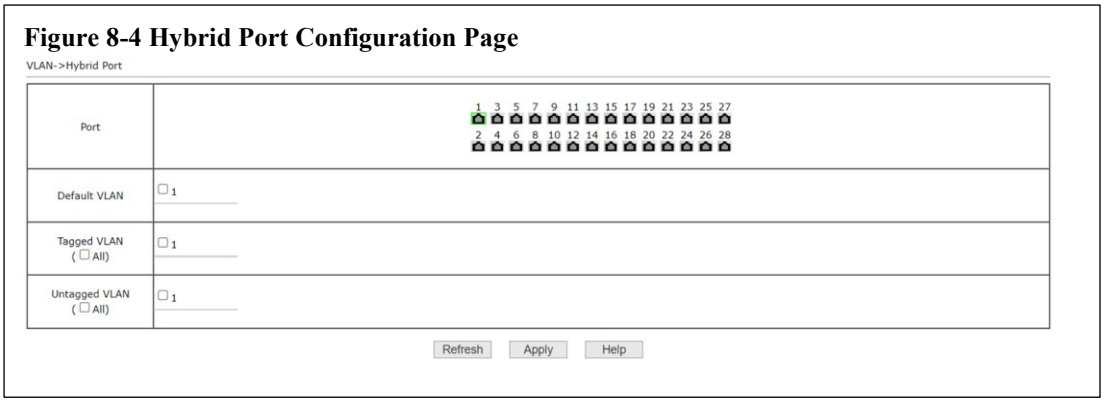


8.4 Hybrid Port Configuration Page

Figure 8-4 below shows the Hybrid port configuration page, which displays and configures the port in Hybrid mode and the VLAN to which it belongs.

This page is divided into two parts: port list and VLAN list. For the operation of port part. please refer to Section 2 (Access Port Configuration Page). If the port is in Hybrid mode. its VLAN can be displayed when it is selected. If other VLANs are selected and applied. the VLAN of the port is changed.
If the port is not in Hybrid mode. After configuration. the port is changed to Hybrid mode and the VLAN is set. The default VLAN must be configured and only one can be selected. Any number of tagged VLANs and untagged VLANs can be selected. However. for a VLAN. only one of the three modes can be selected. If a VLAN is configured with a tagged VLAN. The VLAN cannot be designated as a default VLAN or an untagged VLAN'

Figure 8-4 Hybrid Port Configuration Page



8.5. GVRP Configuration

8.5.1. GVRP Global Configuration

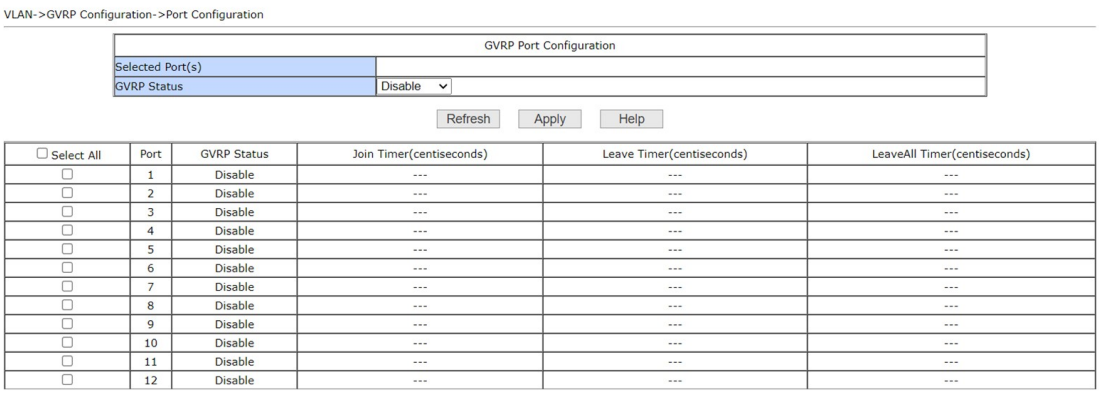
Figure 8-5-1 shown below the GVRP global configuration page through which the user can enable GVRP.

Figure 8-5-1 GVRP Global Configuration Page

8.5.2. GVRP Port Configuration

Figure 8-5-2 shown below is the GVRP port configuration page, through which the user can enable GVRP on the port and view port information.

Figure 8-5-2 GVRP Port Configuration Page



8.5.3. GVRP state machine

Figure 8-5-3 shown below is the GVRP state machine page. through which the user can view the state machine information established by GVRP.

Figure 8-5-3 GVRP State Machine Page Diagram

This page left blank intentionally

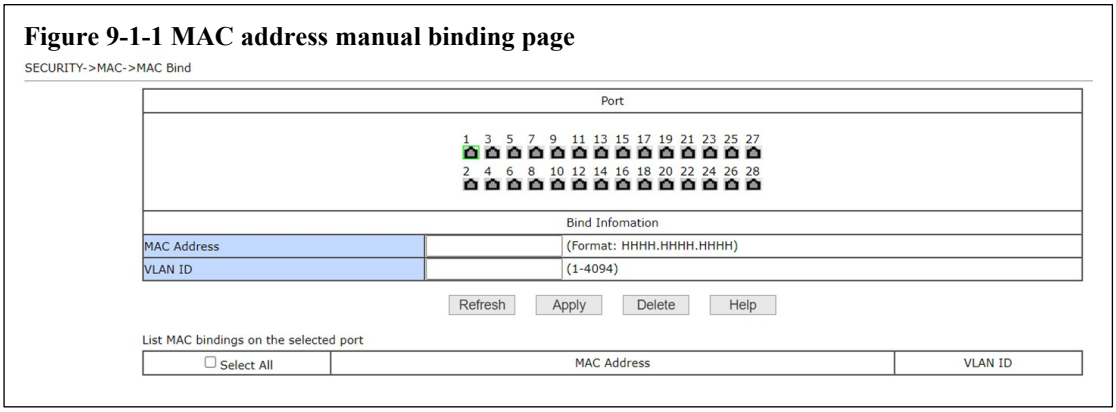
9. Security Configuration

9.1. MAC configuration

9.1.1. MAC address manual binding

Figure 9-1-1 shown below is the MAC binding configuration page.
This page is used to implement the binding of port and MAC address.
The MAC entry on the page is used to enter the bound MAC address. and the VLAN ID entry is used to enter the VLAN to which the MAC address belongs.

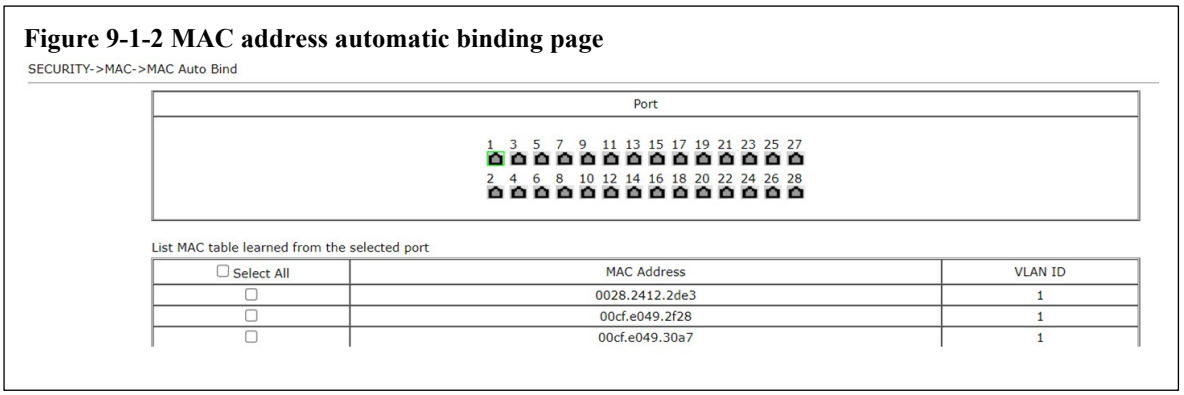
Figure 9-1-1 MAC address manual binding page



9.1.2. Automatic MAC address binding

Figure 9-1-2 below shows the MAC address automatic binding page. This page is used to automatically bind the MAC address to the port.
Displays the existing dynamic MAC address of the port in the Layer 2 hardware forwarding table and the VLAN to which the port belongs. You can select one of the entries and convert it to a static binding.

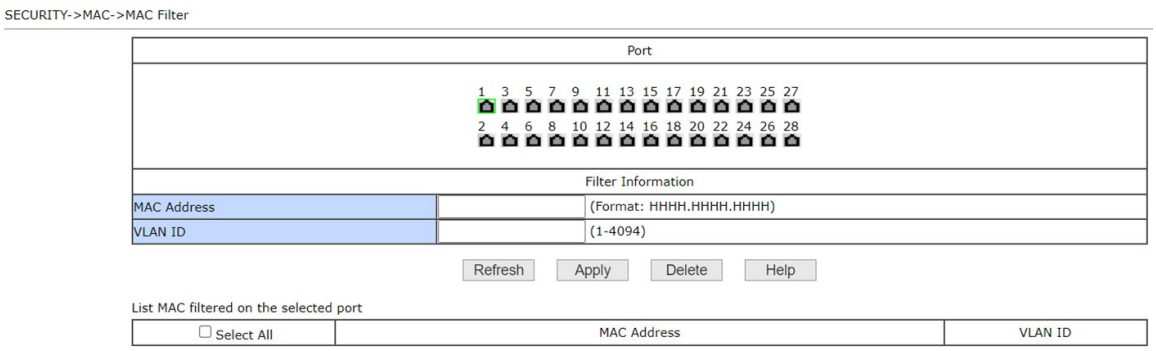
Figure 9-1-2 MAC address automatic binding page



9.1.3. MAC address filtering configuration

Figure 9-1-3 below shows the MAC address filtering configuration page. This page is used to configure port MAC address filtering.
The MAC entry on the page is used to enter the MAC address for filtering. and the VLAN number entry is used to enter the VLAN to which the MAC address belongs.

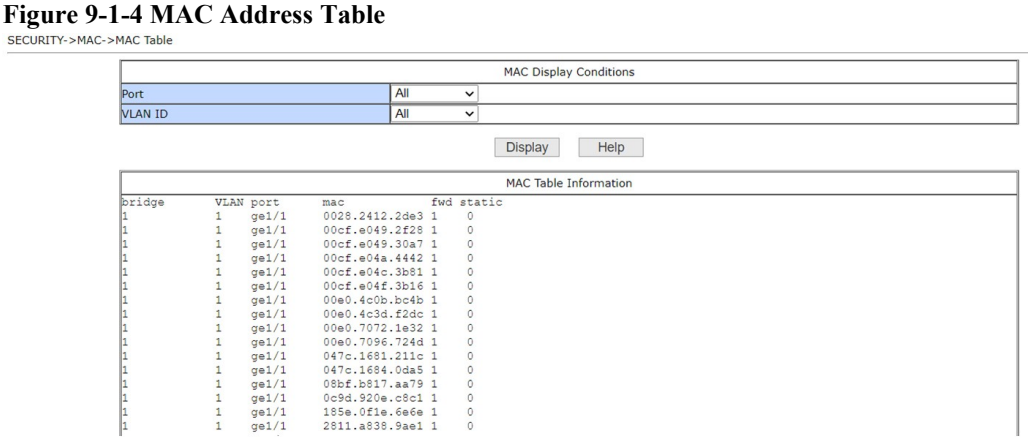
Figure 9-1-3 MAC Address Filtering Configuration



9.1.4. MAC address table

Figure 9-1-4 below is the MAC address table. This page is used to configure the MAC display condition of the port.

Figure 9-1-4 MAC Address Table

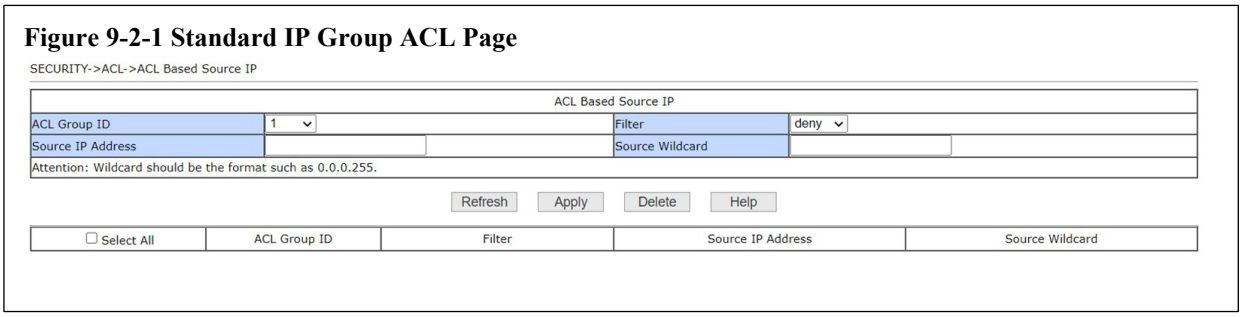


9.2. ACL Configuration

9.2.1. Standard IP group ACL

Figure 9-2-1 below is the standard IP group ACL page. through which the user can establish the rule base of ACL standard IP. Users can select an ACL group number (in the range of 1-99. or 1300-1999) to create one or more rules in that group. The only field that can be matched in a rule is the source IP address (with a mask).

Figure 9-2-1 Standard IP Group ACL Page



When the user configures the rule. the source IP address needs to be masked. and the rule can match the set of IP addresses. The mask of the address is represented by the complement. If the rule is to

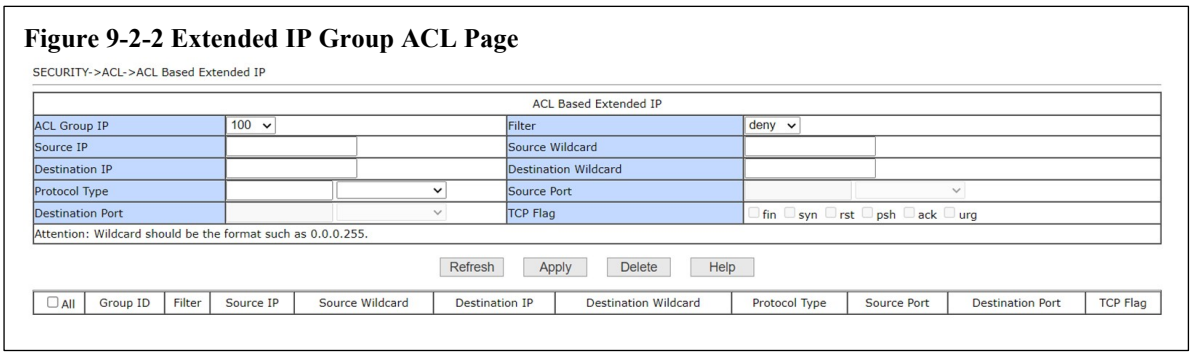
match the IP address range 192.168. 0.0 to 192.168. 0.255. the IP address can be 192.168. 0.1 and its mask is 0.0.0.255.
When the user configures rules. each rule must have a filter mode: Allow or Deny.

When a user creates a rule in a rule group. the system will automatically assign a rule number to the rule. When a rule in a rule group is deleted. other rules remain unchanged. and the system will automatically sort the rules in a rule group. If the user wants to delete the whole rule group. he can select all first. and then click the delete button.

9.2.2. ACL Extended IP Group ACL

Figure 9-2-2 below is the ACL page of the extended IP group. through which the user can establish the rule base of the ACL extended IP. Users can select an ACL group number (in the range of 100-199. or 2000-2699) to create one or more rules in that group. Fields that can be matched in a rule are source IP address (with mask). destination IP address (with mask). protocol type (such as ICMP. TCP. UDP. etc.). source port and destination port (valid only for TCP and UDP protocols). and TCP control flags.

Figure 9-2-2 Extended IP Group ACL Page



When the user configures the rule. the source IP address needs to be masked. and the rule can match the set of IP addresses. The mask of the address is represented by the complement. If the rule is to match the IP address range 192.168. 0.0 to 192.168. 0.255. the IP address can be 192.168. 0.1 and its mask is 0.0. 0.255.

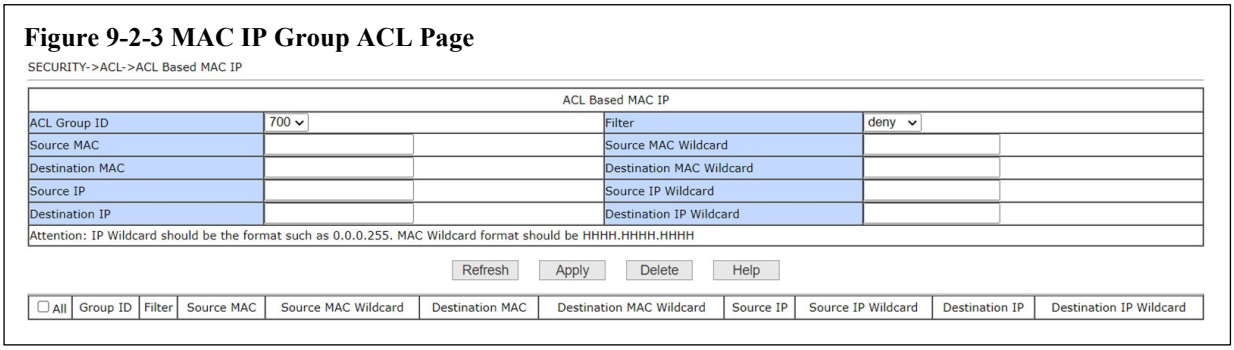
When the user configures rules. each rule must have a filter mode: Allow or Deny.

When a user creates a rule in a rule group. the system will automatically assign a rule number to the rule. When a rule in a rule group is deleted. other rules remain unchanged. and the system will automatically sort the rules in a rule group. If the user wants to delete the whole rule group. he can select all first. and then click the delete button.

9.2.3. MAC IP Group ACL Part

Figure 9-2-3 is the MAC IP group ACL page. through which the user can establish the rule base of ACL MAC IP. Users can select an ACL group number (in the range of 700-799) to create one or more rules in that group. The fields that can be matched in a rule are source MAC address (with address match bits). source IP address (with address match bits). and destination IP address (with address match bits).

Figure 9-2-3 MAC IP Group ACL Page

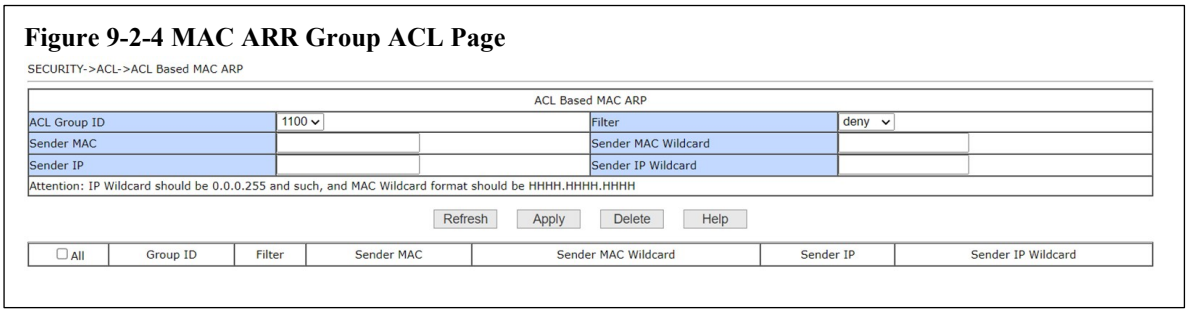


When a user creates a rule in a rule group. the system will automatically assign a rule number to the rule. When a rule in a rule group is deleted. other rules remain unchanged. and the system will automatically sort the rules in a rule group. If the user wants to delete the whole rule group. he can select all first. and then click the delete button.

9.2.4. MAC ARP Group ACL Part

Figure 9-2-4 is the MAC ARP group ACL page. through which the user can establish the rule base of ACL MAC ARP. Users can select an ACL group number (in the range of 1100-1199) to create one or more rules in that group. The fields that can be matched in a rule are the ARP operation type. the sending MAC address (with address match bits). and the sending IP address (with address match bits).

Figure 9-2-4 MAC ARR Group ACL Page

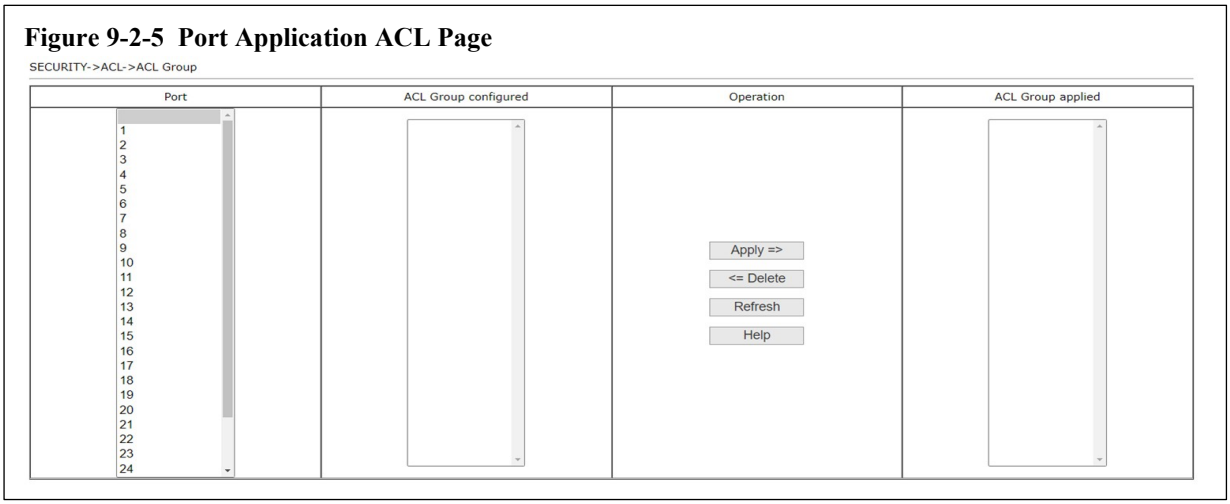


When the user configures the rule. the source IP address needs to be masked. and the rule can match the set of IP addresses. The mask of the address is represented by the complement. If the rule is to match the IP address range 192.168. 0.0 to 192.168. 0.255. the IP address can be 192.168. 0.1 and its mask is 0.0. 0.255.
When the user configures rules. each rule must have a filter mode: Allow or Deny.
When a user creates a rule in a rule group. the system will automatically assign a rule number to the rule. When a rule in a rule group is deleted. other rules remain unchanged. and the system will automatically sort the rules in a rule group. If the user wants to delete the whole rule group. he can select all first. and then click the delete button

9.2.5. Port Apply ACLs pack

Figure 9-2-5 is the port application ACL page. through which the user can select an ACL group for a port. write the rules in this ACL group into the port hardware logic. and make the port perform ACL filtering on the received packets according to these rules.
When selecting an ACL group on a port. you can select IP Standard. IP Extended. MAC IP. and MAC ARP ACL groups. The selected ACL group must exist. Select from the ACL Rule Group list and press the Add key. To delete an ACL group. select an ACL group from the list of referenced rule groups and press the Delete key.

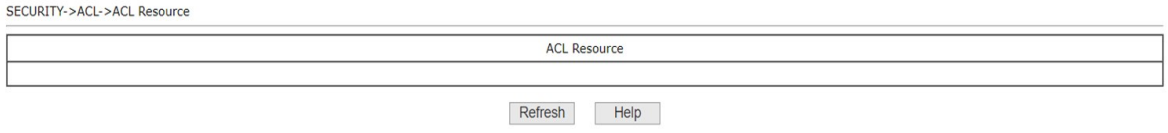
Figure 9-2-5 Port Application ACL Page



9.2.6. ACL Configuration Information Part

Figure 9-2-6 shows the ACL configuration information page. which displays all the rules and reference information configured in the current ACL.

Figure 9-2-6 ACL Configuration Information Page



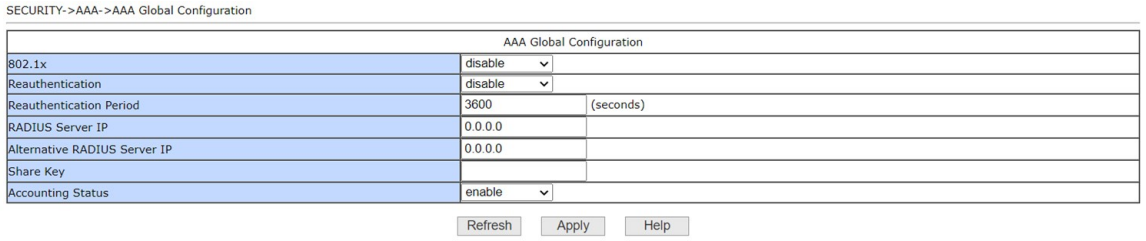
9.3. AAA Configuration

9.3.1. AAA Global Configuration Page

Figure 9-3-1 is the AAA global configuration page. The user can configure the information related to AAA. The information that can be set includes:

- Whether to start the 802.1x protocol, The 802.1x protocol must be started during authentication and accounting.
- Whether to enable the re-authentication function is not enabled by default. and it is determined according to the actual situation when performing authentication billing. Turning on the recertification function will make users more reliable when using authentication billing. but it will slightly increase the traffic of the network.
- Set the time interval for re-authentication. which is valid only when the re-authentication function is enabled. The default value is 3600 seconds. Set the value according to the actual situation when performing authentication billing. but the value should not be too small.
- The IP address of the RADIUS server. This field must be set during authentication and accounting.
- Backup RADIUS server IP address. This field can be set if there is a backup RADIUS server.
- The shared key is used to set the encrypted shared password between the switch and the Radius server. This field must be set during authentication and billing. and must be the same as the setting on the Radius server.
- Whether to start charging, It is started by default. Charging is generally started during authentication and charging.

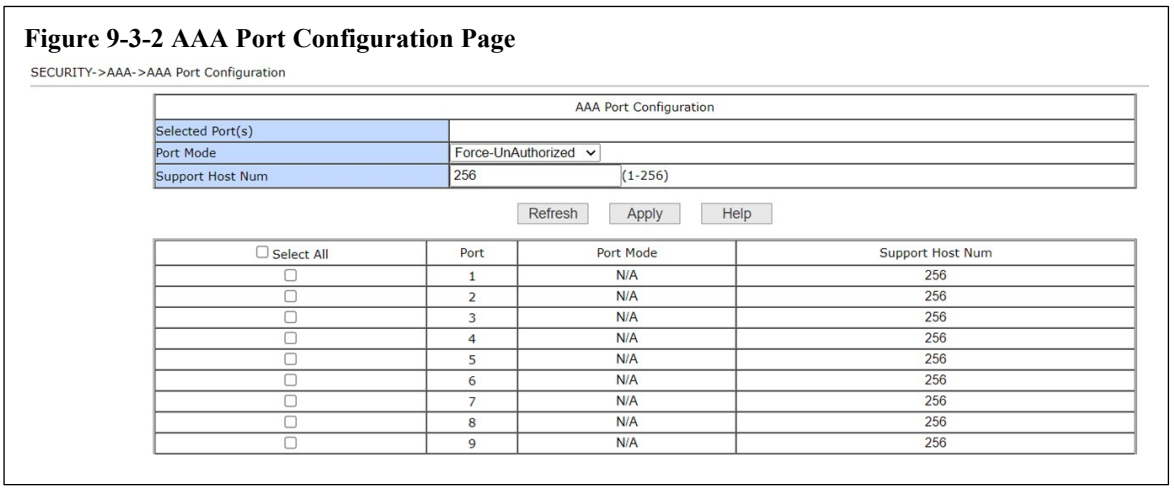
Figure 9-3-1 AAA Global Configuration Page



9.3.2. AAA Port Configuration Part

Figure 9-3-2 is the AAA port configuration page. through which the user can configure the authentication port mode and the maximum number of hosts supported. and view the configuration of each port. To modify the port AAA configuration. the user needs to check the left side of the corresponding port. or use the "Select All" function. The selected ports will be displayed at the top of the page. and several consecutive ports are represented by connection numbers. After successful setting. the selected port will be configured with the same parameters. There are four types of AAA port modes: N/A state. Auto state. Force-authorized state. and Force-unauthorized state. When 802.1 X authentication is required for a port. the port must be set to the Auto state. If the port is not authenticated. it can access the network. The port must be set to the N/a state. The other two States are rarely used in practical applications.

Figure 9-3-2 AAA Port Configuration Page

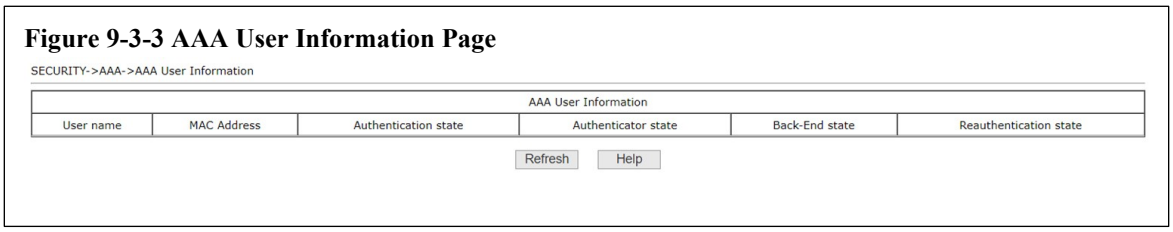


During 802.1x authentication. the maximum number of hosts accessed by the port is 256 by default. The user can modify this field to support 256 hosts at most.

9.3.3. AAA User Information Page

Figure 9-3-3 is the AAA user information page. through which the user can view the status information of all users connected to a port.

Figure 9-3-3 AAA User Information Page



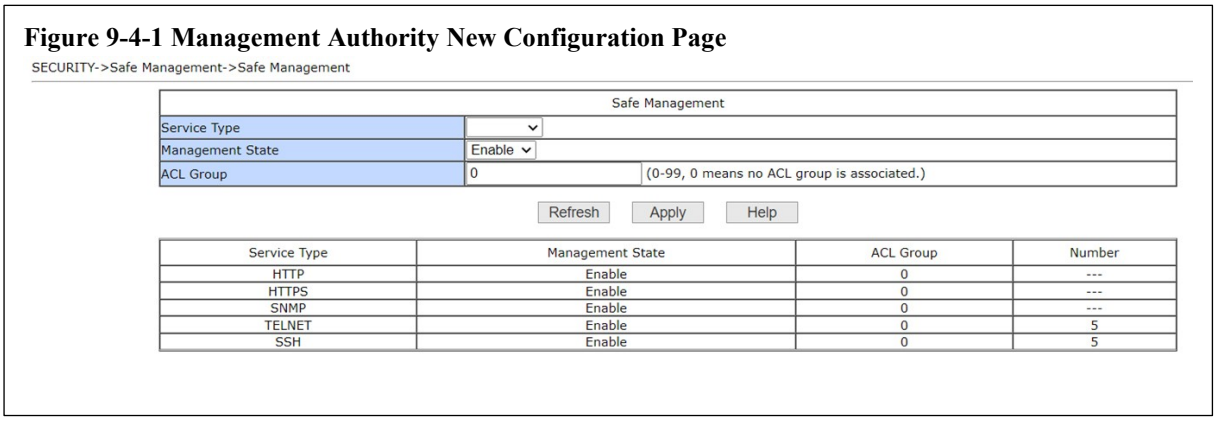
9.4 Native Management Security Configuration

9.4.1. Management permission configuration page

Figure 9-4-1 is the management authority configuration page. Through the configuration of this page. the administrator can control the network management services TELNET. WEB and SNMP. enable or disable these services. and attach these services to the ACL group of IP standard to implement source IP address control. Controls host access to these services.

By default. the TELNET. WEB. and SNMP services of the switch are turned on without ACL filtering. that is. all hosts can access these three services of the switch. If the administrator does not want to provide one or more of these services to other users for the sake of security. one or more of these services can be turned off. If the administrator only wants specific hosts to access one or more of these services. one or more of these services can be filtered by ACL. When a service needs ACL filtering. the service needs to be opened and an ACL group (1-99) of IP standard needs to be selected. At this time. the ACL group must exist.
It should be noted that if the administrator controls the WEB service on this page (such as closing the WEB service). the user may no longer be able to use the WEB page. At this time. the user can log in to the switch in other ways and control the WEB service so that the user can use the WEB page (such as opening the WEB service).

Figure 9-4-1 Management Authority New Configuration Page



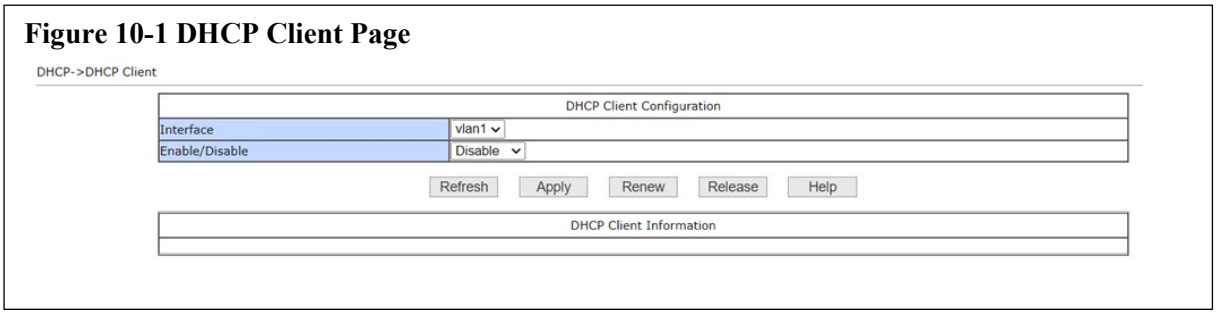
This page left blank intentionally

10. DHCP Configuration

10.1. DHCP client

Figure 10-1 shows the DHCP client configuration. This page is used to configure the DHCP client configuration

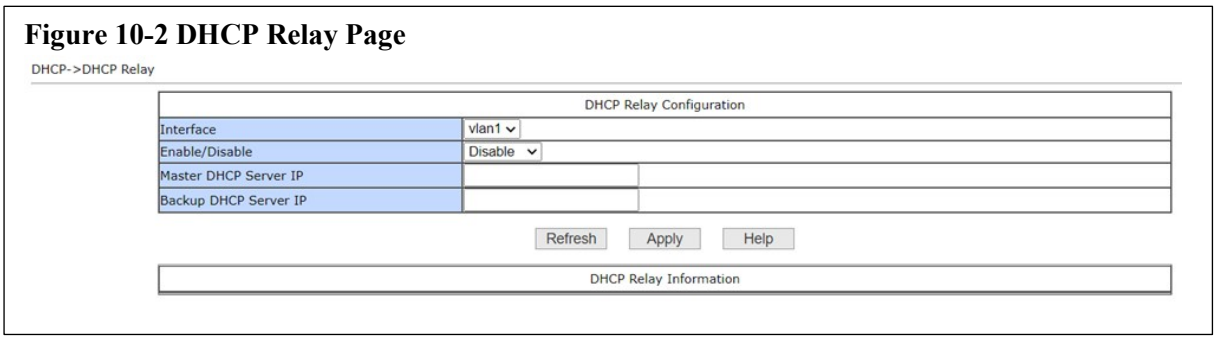
Figure 10-1 DHCP Client Page



10.2. DHCP Relay

Figure 10-2 shows the DHCP relay configuration. This page is used to configure the DHCP relay configuration

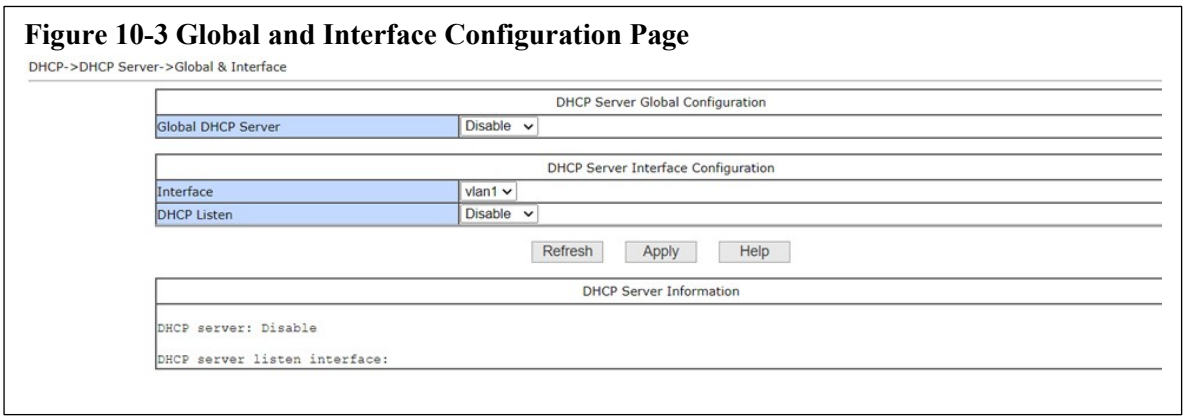
Figure 10-2 DHCP Relay Page



10.3. DHCP server

Figure 10-3 Shows the DHCP server interface configuration. This page is used to configure the DHCP server interface configuration.

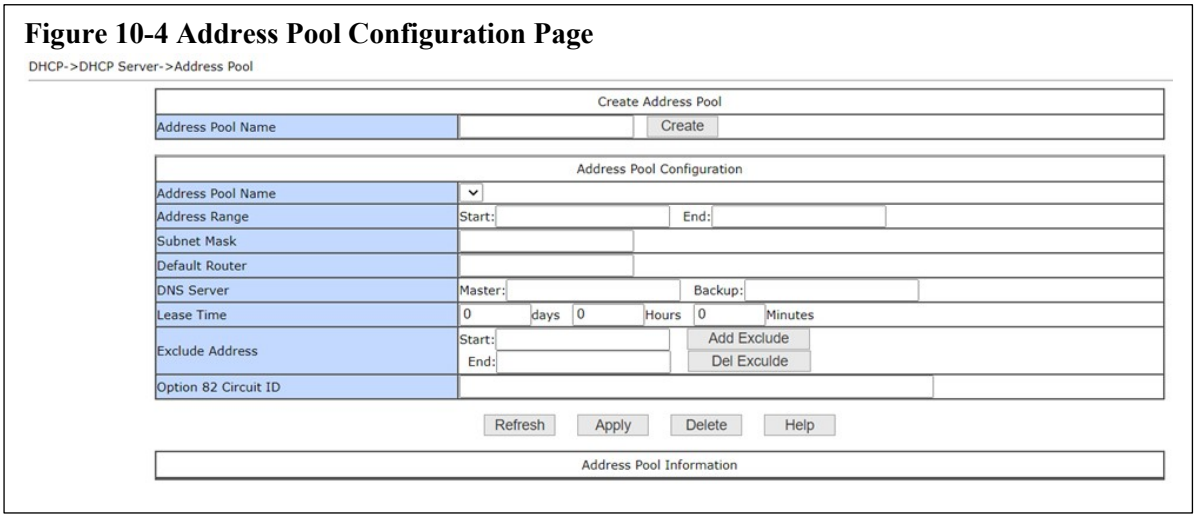
Figure 10-3 Global and Interface Configuration Page



10.4. Address Pool Configuration

Figure 10-4 shows the DHCP server address pool configuration. This page is used to configure the DHCP server address pool configuration.

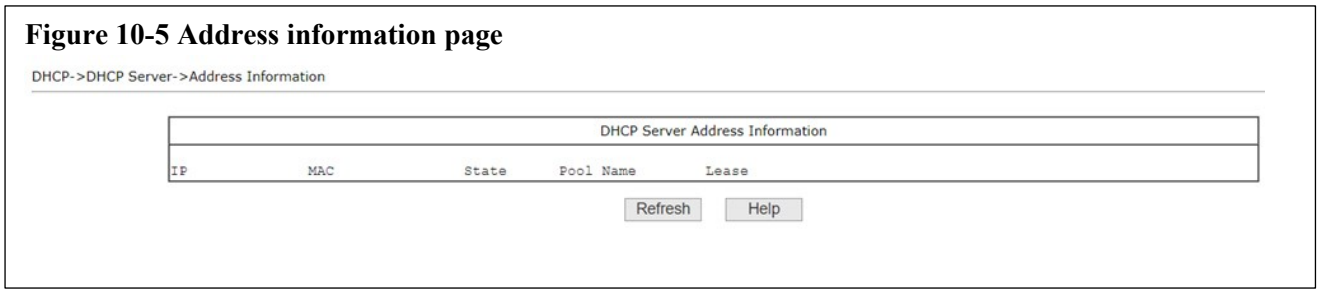
Figure 10-4 Address Pool Configuration Page



10.5. Address Information

Figure 10-5 is the DHCP server address information viewing interface. This page is used to view the address information of the DHCP server.

Figure 10-5 Address information page

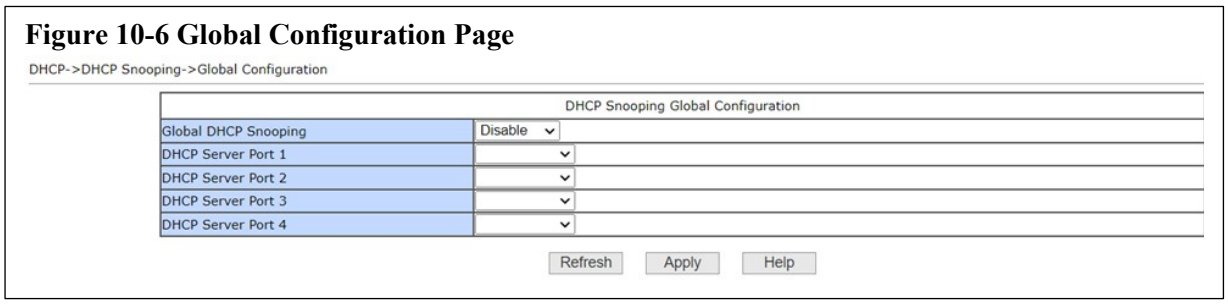


10.6. DHCP snooping

Global Configuration

Figure 10-6 is the global DHCP snooping configuration interface. which is used to configure the global DHCP snooping configuration

Figure 10-6 Global Configuration Page



10.7. Interface configuration

Figure 10.7.1 is the DHCP listening port configuration interface. which is used to configure the DHCP listening interface configuration.

.

Figure 10.7.1 Interface configuration page

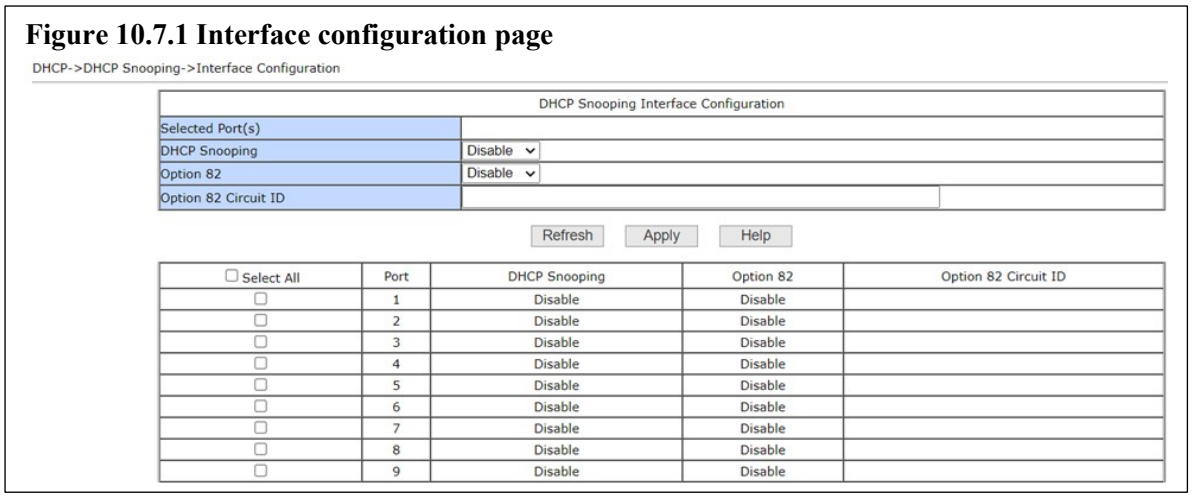
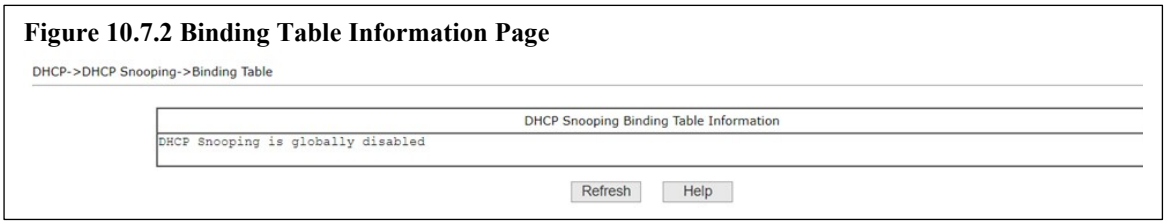


Figure 10.7.2 is the interface for viewing the address information of the DHCP server. This page is used to view the address information of the DHCP server.

Figure 10.7.2 Binding Table Information Page



This page left blank intentionally

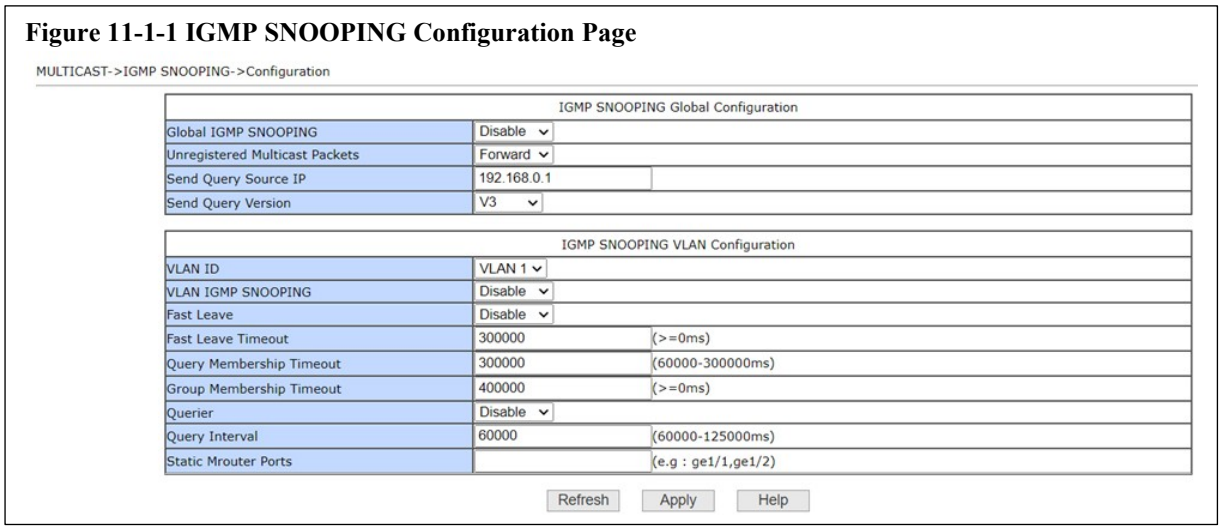
11. Multicast configuration

11.1. IGMP Snooping

11.1.1. IGMP SNOOPING Configuration Page

Figure 11-1-1 is the IGMP SNOOPING configuration page. Users can enable IGMP Snooping from this page.

Figure 11-1-1 IGMP SNOOPING Configuration Page



11.1.2. Multicast group information page

Figure 11-1-2 is the multicast group information page. through which the user can view the IGMP SNOOPING multicast information.

Figure 11-1-2 Multicast Group Information Page

11.2. CMRP Configuration

11.2.1. CMRP Global Configuration

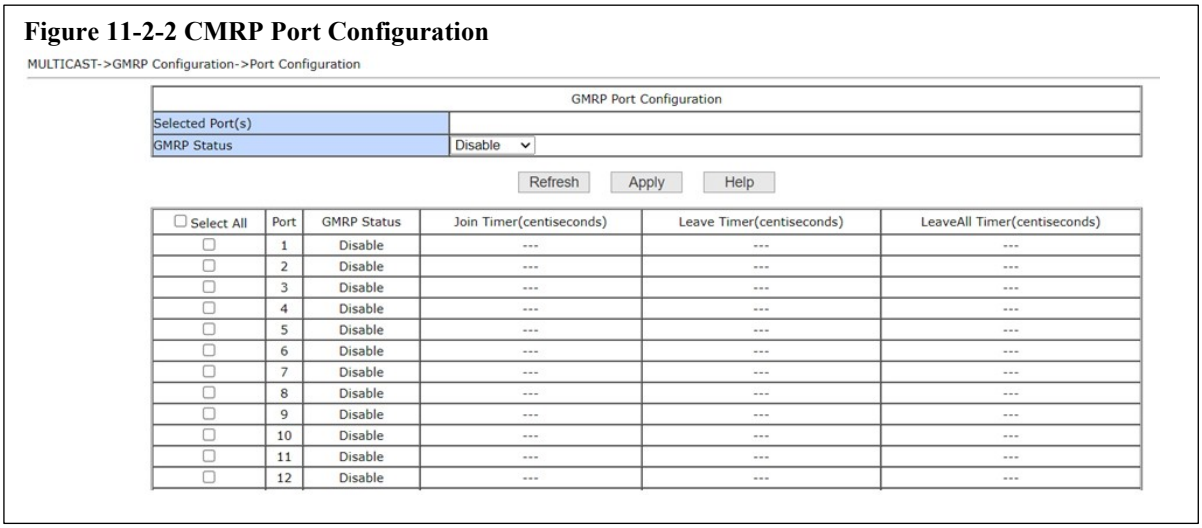
Figure 11-2-1 is the CMRP omnipotent configuration interface. which is used to configure the global GMRP

Figure 11-2-1 CMRP Global Configuration Page

11.2.2. CMRP Port Configuration

Figure 11-2-2 shows the CMRP port configuration interface. which is used to configure the CMRP port status.

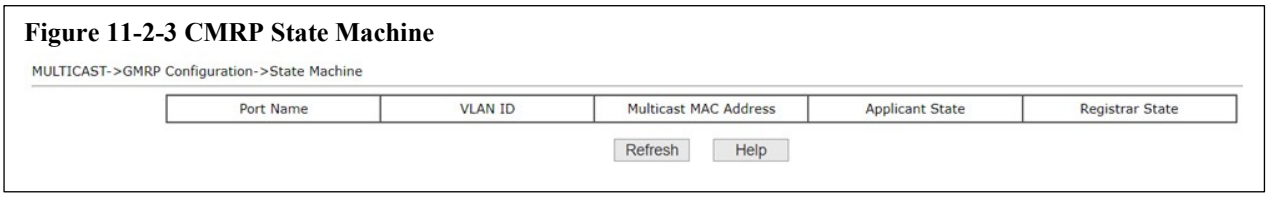
Figure 11-2-2 CMRP Port Configuration



11.2.3. CMRP state machine

Figure 11-2-3 is the CMRP state machine viewing interface. This page is used to view the status of the CMRP state machine for the CMRP configuration

Figure 11-2-3 CMRP State Machine

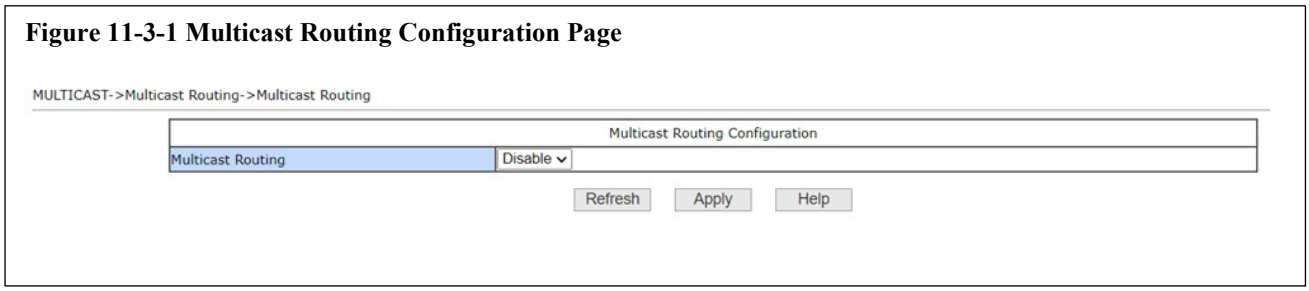


11.3. Multicast routing configuration

11.3.1. Multicast routing configuration

Figure 11-3-1 shows the multicast routing configuration. This page is used to configure the multicast routing switch

Figure 11-3-1 Multicast Routing Configuration Page



11.3.2. Multicast routing table

Figure 11-3-2 shows the multicast routing table viewing interface. This page is used to view the multicast routing table of the multicast routing configuration

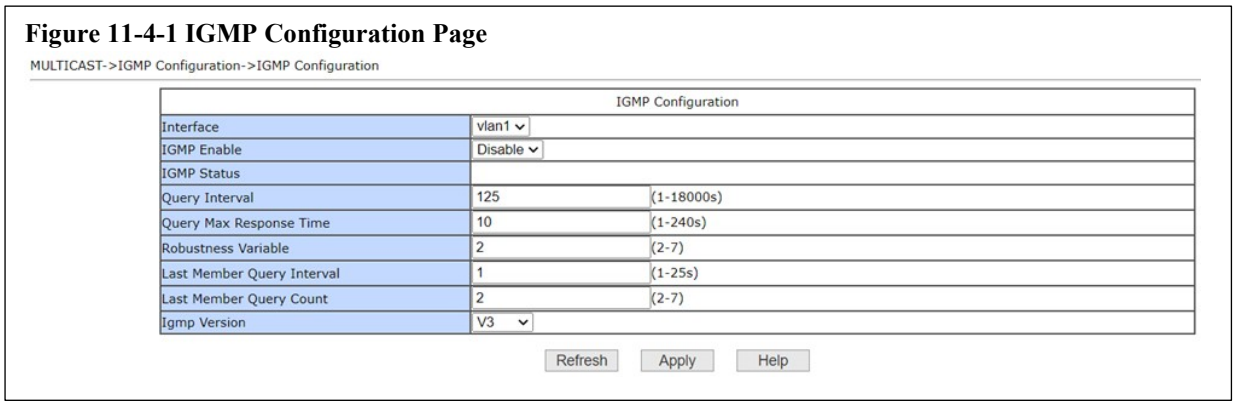
Figure 11-3-2 Multicast Routing Table Page

11.4. IGMP configuration

11.4.1 IGMP configuration

Figure 11-4-1 shows the IGMP port configuration interface. which is used to configure the IGMP switch parameters.

Figure 11-4-1 IGMP Configuration Page



11.4.2 IGMP Interface Information

Figure 11-4-2 shows the IGMP interface information viewing interface. This page is used to view the IGMP interface information for the IGMP configuration.

Figure 11-4-2 IGMP Interface Information Page

11.4.3 IGMP Group Information

Figure 11-4-3 shows the IGMP group information viewing interface. This page is used to view IGMP group information for the IGMP configuration

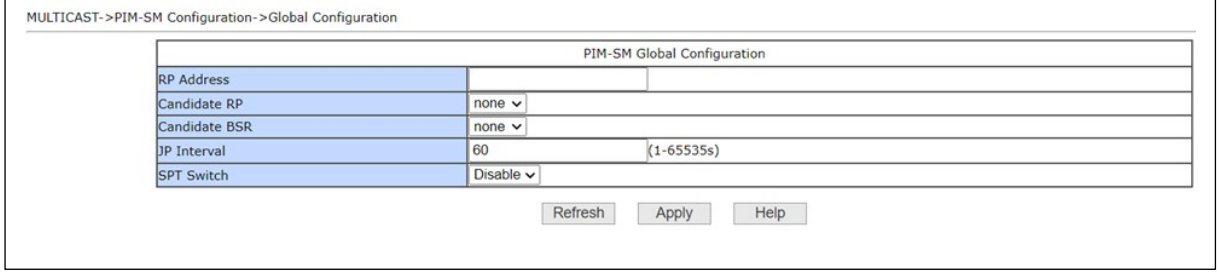
Figure 11-4-3 IGMP Group Information Page

11.5. PIM-SM Configuration

11.5.1. Global Configuration

Figure **11-5-1** shows the PIM-SM global configuration interface. which is used to configure the global PIM-SM parameters.

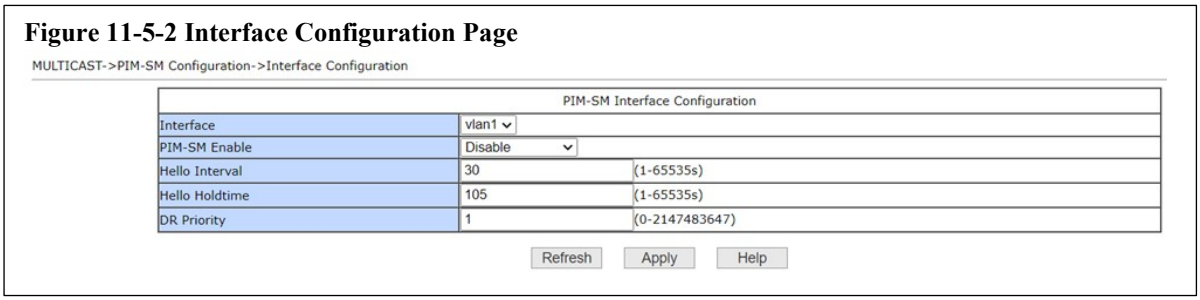
Figure 11-5-1 Global Configuration Page



11.5.2. Interface configuration

Figure 11-5-2 shows the PIM-SM interface configuration interface. which is used to configure PIM-SM interface parameters

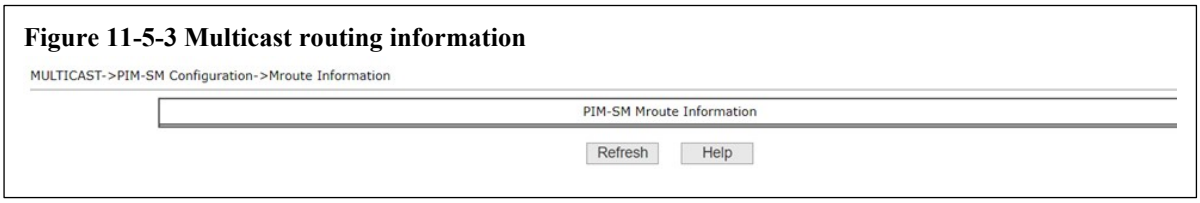
Figure 11-5-2 Interface Configuration Page



11.5.3. Multicast routing information

Figure 11-5-3 shows the multicast routing information viewing interface. This page is used to view the multicast routing information configured by PIM-SM.

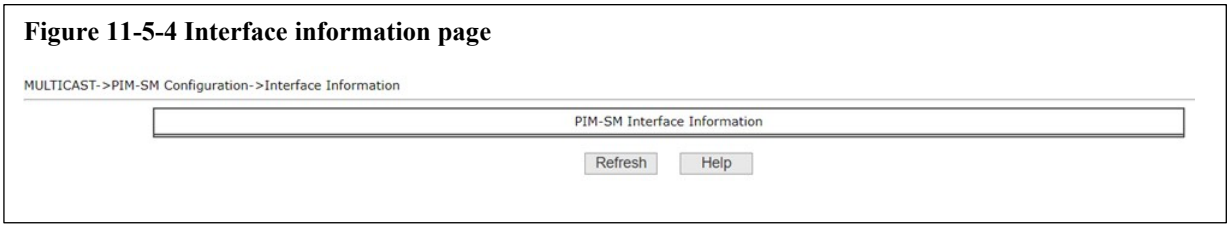
Figure 11-5-3 Multicast routing information



11.5.4. Interface information

Figure 11-5-4 shows the interface for viewing interface information. This page is used to view the interface information configured by PIM-SM.

Figure 11-5-4 Interface information page



11.5.5. Neighbour information

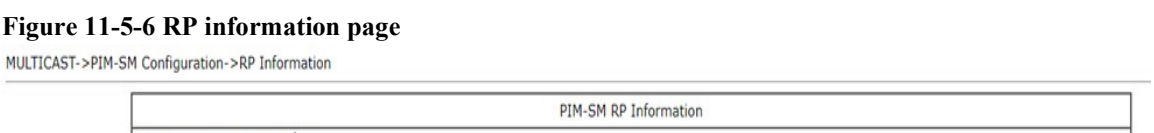
Figure 11-5-5 shows the neighbour information viewing interface. This page is used to view the neighbour information configured by PIM-SM.

Figure 11-5-5 Neighbour Information Page

11.5.6. RP information

Figure 11-5-6 shows the RP information viewing interface. This page is used to view the RP information for the PIM-SM configuration

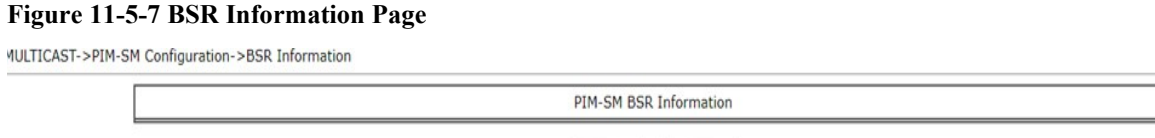
Figure 11-5-6 RP information page



11.5.7. BSR information

Figure 11-5-7 shows the BSR information viewing interface. This page is used to view the BSR information for the PIM-SM configuration.

Figure 11-5-7 BSR Information Page



This page left blank intentionally

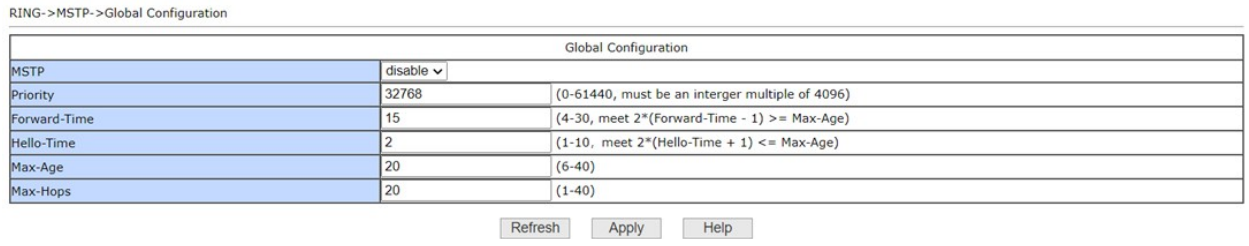
12 Ring Network Configuration

12.1. Spanning Tree Configuration

12.1.1. Spanning Tree Global Configuration

Figure 12-1-1 shows the global configuration page of spanning tree. through which the user can configure global spanning tree parameters.

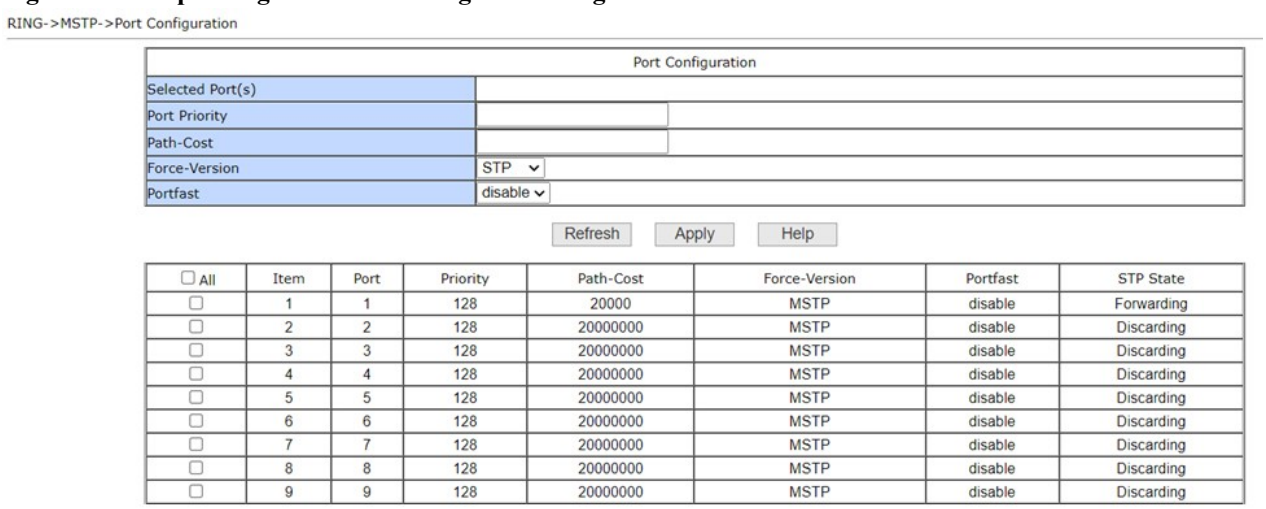
Figure 12-1-1 Spanning Tree Global Configuration Page



12.1.2. Spanning Tree Port Configuration

Figure 12-1-2 is the Spanning Tree Port Configuration page. through which the user can view the specific status of the port MSTP.

Figure 12-1-2 Spanning Tree Port Configuration Page

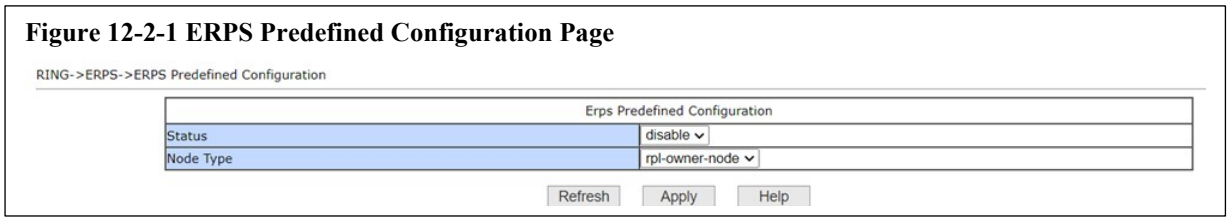


12.2. ERPS Configuration

12.2.1. ERPS Predefined Configuration

Figure 12-2-1 is the ERPS Predefined Configuration page. which enables the ERPS Predefined Configuration. When you enable the ERPS predefined configuration. you can specify the node type: Primary or Transport.
Specific predefined configuration: ERPS instance number is 1.
ERPS change number is 1. ring mode is main ring mode.
Protocol VLAN is VLAN3001. data VLAN is VLAN1.
RPL port is 51. rl port is 52. recovery behaviour is recoverable.
Hold-off time is 0. guard time is 500 ms.
The wtr time is 5 minutes.
WTB time is 5 seconds and the protocol message sending time is 5 seconds.

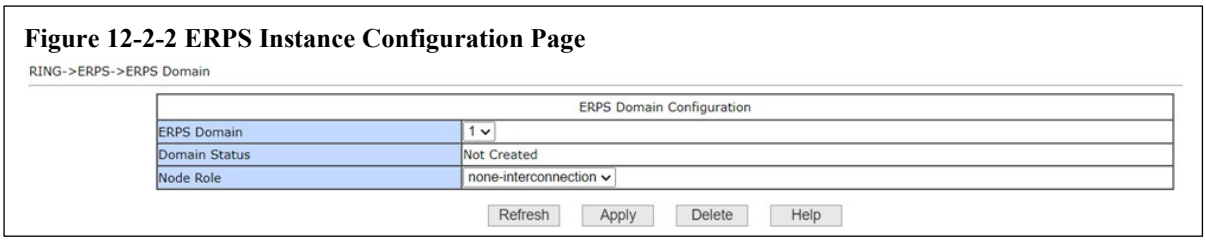
Figure 12-2-1 ERPS Predefined Configuration Page



12.2.2. ERPS Instance Configuration

Figure 12-2-2 shows the ERPS instance configuration page. through which the ERPS instance can be configured. When an instance is not created. click Apply to create and assign a role. When an instance is created but not associated with a ring. you can modify the role. If an instance is created and associated with a ring. you cannot modify the instance. Click Delete to delete the selected instance. You can configure up to 8 instances.

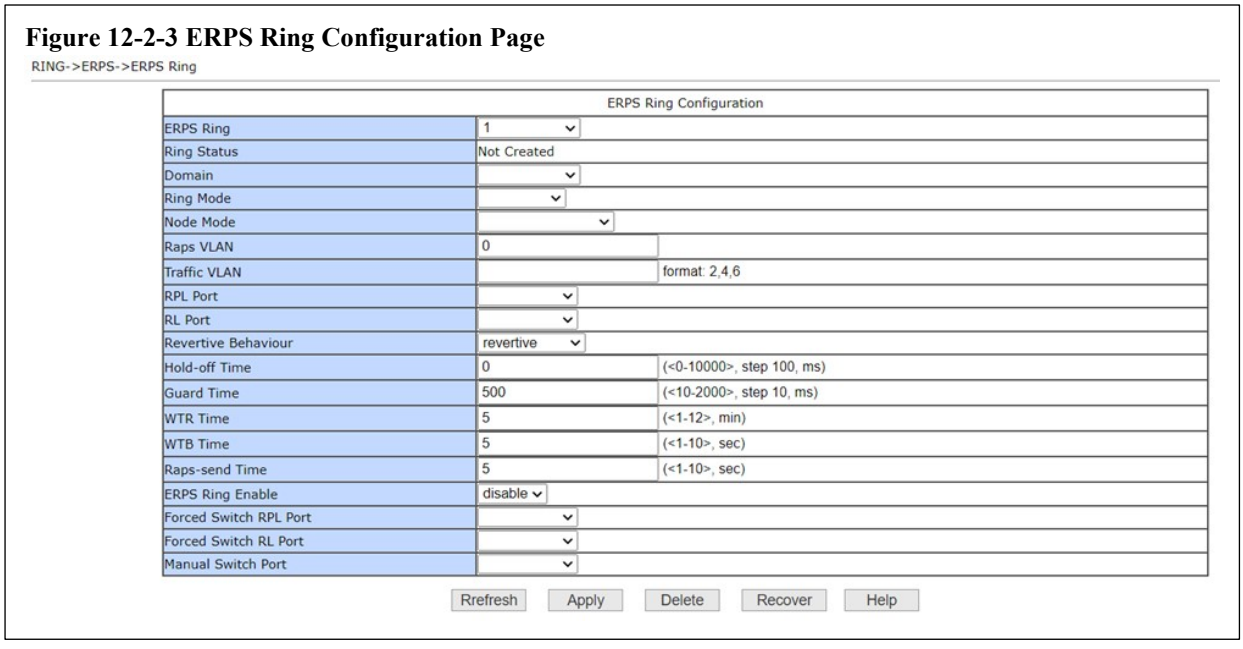
Figure 12-2-2 ERPS Instance Configuration Page



12.2.3. ERPS Ring Configuration

Figure 12-2-3 is the ERPS Ring Configuration page. which allows you to create and configure an ERPS ring. Select a ring. Click the Apply button to create the ring and set the configuration information when the ring is not created. If the ring is created. the configuration information can be modified. Click the Delete button to delete the selected ring. A ring must and can only be associated to one instance. A maximum of 32 rings can be configured. When a ring fault is detected. click the Manual Recovery button to recover.

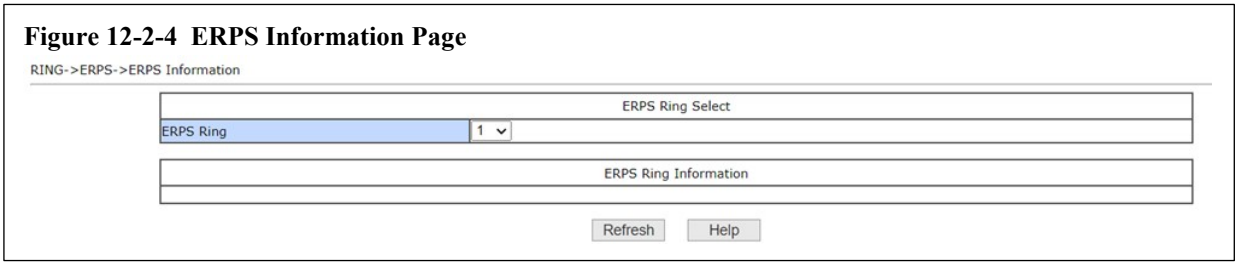
Figure 12-2-3 ERPS Ring Configuration Page



12.2.4. ERPS Information

Figure 12-2-4 is the ERPS information page. Select the ring number to display the configuration and status information of the relevant ERPS ring

Figure 12-2-4 ERPS Information Page



12.3. EAPS Configuration

12.3.1. EAPS Ring Configuration

Figure 12-3-1 This page is used to create and configure EAPS information. and also to delete and display EAPS information.

EAPS ring number: specific ring number. value range 1-16. can be selected usin the drop-down box

Creation status: Not Created and Created. In case of no creation. it is necessary to create first

Modes: Master and Transit. which can be configured according to specific needs.

Main port: EAPS main port. such as fe1/1. ge1/1

Alternate port: EAPS 2nd port

Control VLAN: control VLAN of EAPS ring. value 2-4094

Protected VLAN: EAPS ring protected VLAN

Hello Interval The interval at which Hello messages are sent. The default is 1s

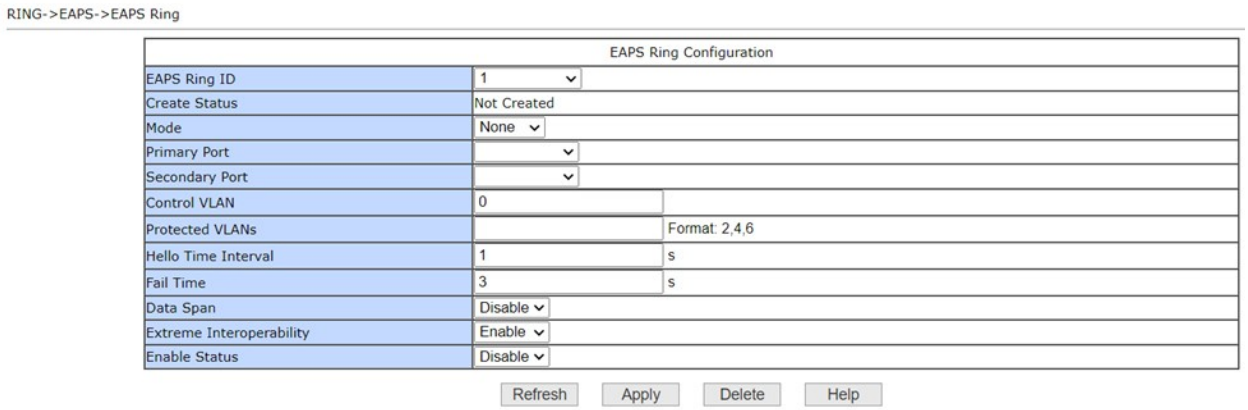
Fail time: the time to detect the fault. which is 3s by default

In the case of data trans-ring forwarding and multi-ring forwarding. this function shall be enabled when the data needs to be trans-ring forwarded. Not turned on by default

EXtreme Interoperability Compatibility with other network devices. on by default

Enable status. last EAPS ring enable condition

Figure 12-3-1 EAPS Ring Configuration Page



12.3.2. EAPS Information

Figure 13-3-2 is the EAPS information page. through which the user can view the EAPS configuration information.

Figure 1233-2 EAPS Information Page

13 Advanced Configuration

13.1 QoS Configuration

13.1.1. QoS Application Configuration

Figure 13-1-1 is the Qos application page. through which the user can configure the Qos type of the port and modify the default user priority. The list shows the port's Qos type and user default priority in real time.

Figure 13-1-1 QoS Application Configuration Page

ADVANCED->QoS Configuration->QoS Apply

QoS Apply Configuration	
Selected Port(s)	
QoS Type	COS-based
Policy ID	0 (1-256)
User Priority	0

Refresh Apply Help

Select All	Port	QoS Type	Policy ID	User Priority
☐	1	COS-based	---	0
☐	2	COS-based	---	0
☐	3	COS-based	---	0
☐	4	COS-based	---	0
☐	5	COS-based	---	0
☐	6	COS-based	---	0
☐	7	COS-based	---	0
☐	8	COS-based	---	0
☐	9	COS-based	---	0
☐	10	COS-based	---	0

13.1.2. QoS Scheduling Configuration page

Figure 13-1-2 is the QoS scheduling page. through which the user can configure the Qos scheduling mode of the port and modify the priority of the queue. The list displays the scheduling mode of the port and the weight value of each queue in real time.

Figure 13-1-2 QoS Scheduling Configuration Page

ADVANCED->QoS Configuration->QoS Schedule

QoS Schedule Configuration					
Selected Port(s)					
QoS Schedule Mode	WRR				
Weight of queue 0	1	(1-127)	Weight of queue 1	2	(1-127)
Weight of queue 2	4	(1-127)	Weight of queue 3	8	(1-127)
Weight of queue 4	16	(1-127)	Weight of queue 5	32	(1-127)
Weight of queue 6	64	(1-127)	Weight of queue 7	127	(1-127)

Refresh Apply Help

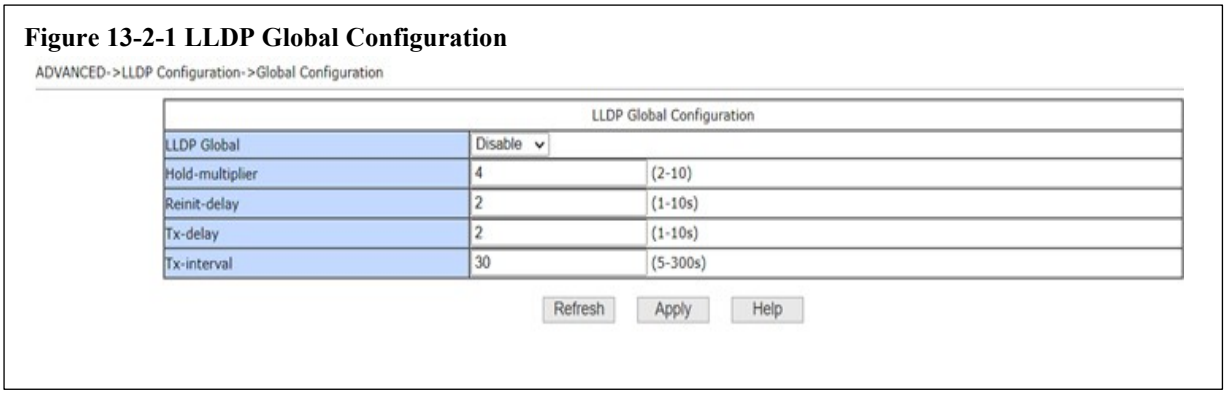
Select All	Port	QoS Schedule Mode	Weight of queue 0	Weight of queue 1	Weight of queue 2	Weight of queue 3	Weight of queue 4	Weight of queue 5	Weight of queue 6	Weight of queue 7
☐	1	WRR	1	2	4	8	16	32	64	127
☐	2	WRR	1	2	4	8	16	32	64	127
☐	3	WRR	1	2	4	8	16	32	64	127
☐	4	WRR	1	2	4	8	16	32	64	127
☐	5	WRR	1	2	4	8	16	32	64	127
☐	6	WRR	1	2	4	8	16	32	64	127
☐	7	WRR	1	2	4	8	16	32	64	127
☐	8	WRR	1	2	4	8	16	32	64	127

13.2 LLDP configuration

13.2.1. LLDP Global Configuration

Figure 13-2-1 shows the LLDP global configuration interface. which is used to display and configure global LLDP parameters

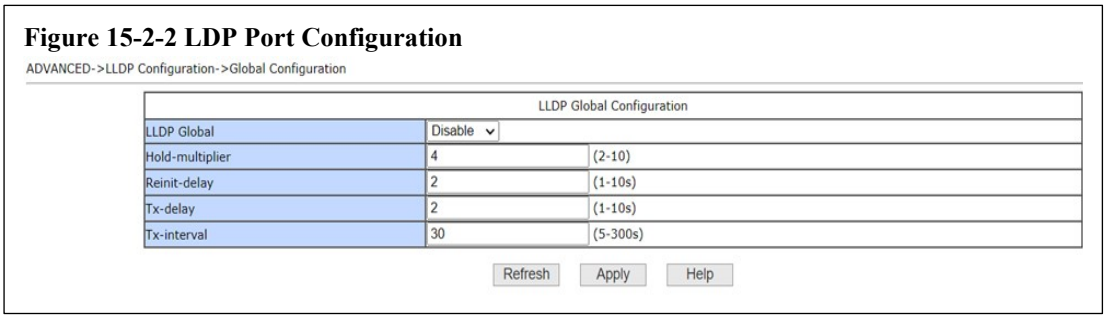
Figure 13-2-1 LLDP Global Configuration



13.2.2. LLDP Port Configuration

Figure 15-2-2 shows the LLDP port configuration interface. which is used to display and configure LLDP port parameters.

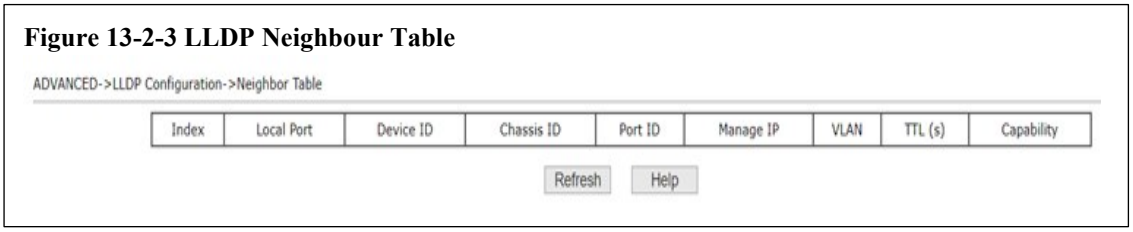
Figure 15-2-2 LDP Port Configuration



13.2.3. LLDP Neighbour Table

Figure 15-2-3 shows the LLDP neighbour table viewing interface. This page is used to view the LLDP neighbour table information for the LLDP configuration.

Figure 13-2-3 LLDP Neighbour Table



14 Configuring Layer 3 Routing

14.1. Connecting to the CLI Management

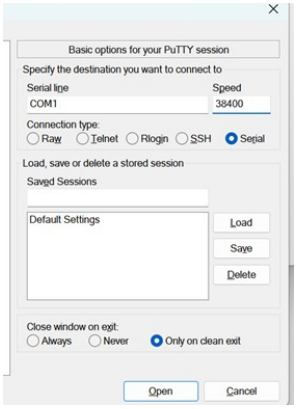
Layer 3 functions are configured using the Command Line Interface on the switch.
This chapter describes the CLI command line interface in detail, mainly including the following contents:

- Accessing the CLI of the switch
- Introduction to CLI Mode
- Command Syntax Introduction
- Command Line Shortcut
- History Command

Accessing the CLI of the Switch using a serial port
Step 1: Connect the serial port of the PC to the Console port of the switch through the configuration cable, as shown in the following figure:

Step 2: Start the terminal emulation program on the PC (such as HyperTerminal of Windows), and configure the communication parameters of the terminal emulation program. The communication parameters of the terminal are configured as follows:
Baud rate: 38400 (or 115200) (Note: subject to the actual product)
Data bits: 8
Parity: Non
Stop bit: 1
Data flow control: none

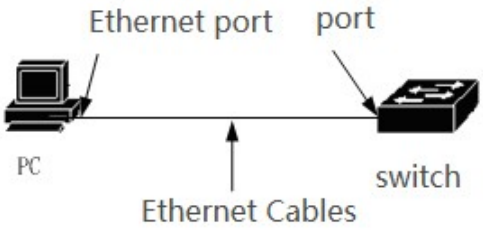
Configuration of PC with Putty



Step 3: Start the switch. After the switch is started, the CLI prompt (the default is Switch >) will be displayed on the terminal. The user can enter commands at this prompt, so that the user can access the CLI of the switch.

Users can access the switch through its ports.
The IP address of the port of the switch is 192.168.16.1 by default (note: the actual product shall prevail). The operation steps for accessing the switch through the port are as follows:
Step 1: Connect the Ethernet port of the PC to the port of the switch through the Ethernet cable. See the following figure:

Connecting using an Ethernet Port



Step 2: Set the IP address of the Ethernet port of the PC. The IP address must be in the 192.168. 0.0/24 segment (such as IP address 192.168. 0.100). Determine the connectivity between the PC and the switch by pinging the 192.168.16.1.
Step 3: If the PC is connected to the switch, Telnet 192.168.16.1 enters the Telnet terminal interface. See the following figure:

```
C:\telnet 192.165.16.1
```

Step 4: If the system does not set a password, the Telnet interface directly enters the CLI, and the CLI prompt appears (the default is Switch >); if the system sets a password, you need to enter the password on the Telnet interface to enter the CLI.
The default username is 'root' and password is 'case'

There are two points to pay special attention to:
The IP address of the switch port is established on the VLAN three-layer interface. Before accessing the switch, the IP address of a VLAN interface must be set. The default IP address of VLAN1 is 192.168. 16.1 (Note: The actual product shall prevail) can be used directly. The IP address of the VLAN interface can be configured through the Console port.

The user accesses the switch through the port and can directly connect the PC and the port through an Ethernet cable, or connect through a network, as long as the PC and a VLAN of the switch can communicate with each other.

CLI modes are divided into four categories: normal mode, privileged mode, global configuration mode and configuration submode. The configuration submode is composed of many CLI modes. Normal users have access only to normal mode, and privileged users have access to all CLI modes.

Console and Telnet terminals first enter the normal mode, enter the enable command in the normal mode, and enter the privileged mode after successfully verifying the password. On a Telnet terminal, a normal user can only stay in normal mode and cannot enter privileged mode. Enter configure terminal in privileged mode to enter CLI mode into global configuration mode. Each configuration submode can be entered by entering the relevant command in the global configuration mode.

A CLI command consists of two parts: a keyword and a parameter.
The first word must be a keyword, and the following words can be keywords or parameters.
Keywords and parameters can appear alternately.
A command must have a keyword, but it can have no parameters.
For example, the command write has one keyword and no arguments; the command show version has two keywords and no arguments; the command VLAN < vlan-id > has one keyword and one argument;
The command instance < instance-id > VLAN < vlan-id > has two keywords and two arguments, and the keywords and arguments alternate.

There are two types of parameters for CLI commands: required and optional.
Required parameters must be entered when entering a command, while optional parameters may or may not be entered. If the parameter in the command VLAN < vlan-id > is a required parameter, it must be entered when entering the command; while the parameter in the command show interface [if-name] is an optional parameter, it may or may not be entered when entering the command.

1) The following rules must be met when describing commands with text:
Keywords are expressed directly in words.
Uch as the command show version.

2) Parameters must be enclosed in < >.
Uch as the command VLAN < vlan-id >

3) If it is an optional parameter, the parameter must be enclosed in a].
Uch as the command show VLAN < vlan-id >]
In this case, the < > of the parameter can be omitted and changed to:
Command show VLAN VLAN-ID]
Command show VLAN VLAN-ID]
If it is a required parameter, the parameter cannot have].

The following table lists the main CLI modes for the switch

Pattern	Describe	Prompt	Command to enter mode	Command to exit mode
Normal Mode	Provides the display command to view status information for the switch	**Switch>**	The mode that the terminal enters first.	There is no exit mode command on the Console terminal. Use the exit or quit command on the Telnet terminal to exit the Telnet terminal
Privileged Mode	In addition to providing display commands to view the status information of the switch, it also provides commands such as debugging, version upgrade, and configuration maintenance.	**Switch#**	Enter the enable command in normal mode.	Use the disable command to return to normal mode. Use the exit or quit command on the Console terminal to exit to normal mode and the exit or quit command
Global Configuration Mode	Provides generic commands that cannot be implemented within the configuration submode, such as the configure static route command.	**Switch(config)#**	Enter configure in privileged model The terminal command.	Use the exit, quit, or end command to exit to privileged mode
Interface Configuration Mode	Provides commands for configuring ports and VLAN interfaces.	**Port：Switch (configge1/1)#** **VLANInterface：Switch (config-vlan1)#**	Enter the interface < if-name > command in global configuration mode.	Use the exit or quit command to exit to global configuration mode and use the end command to exit to privileged mode.
VLAN Configuration Mode	Commands to configure VLANs are provided. Such as commands to create and delete VLANs.	**Switch(config-vlan)#**	Enter the VLAN database command in global configuration mode.	Use the exit or quit command to exit to global configuration mode and use the end command to exit to privileged mode.
MSTP Configuration Mode	Commands to configure MSTP are provided. such as the commands to create and delete an MSTP instance.	**Switch(config-mst)#**	Enter the spanning-tree mst configuration command in global configuration mode	Use the exit or quit command to exit to global configuration mode and use the end command to exit to privileged mode.
Terminal Configuration Mode	Commands are provided to configure Console and Telnet terminals, such as a timeout for the terminal.	**Switch(config-line)#**	Enter the line vty command in global configuration mode.	Use the exit or quit command to exit to global configuration mode and use the end command to exit to privileged mode

14.2. Configuring RIP

14.2.1. RIP Information

RIP (Routing Information Protocol) is a dynamic routing protocol developed earlier, which uses distance vector algorithm and is mostly used in small networks. RIP protocol packets are encapsulated in UDP packets using UDP port 520. The main idea of RIP is to use the hop count to measure the distance to the host, and the hop count increases by 1 every time a router passes through, so as to calculate the weight of the route.(Its Metric) for routing.

The RIP convention has a maximum hop count of 15, and a hop count of 16 is marked as unreachable. RIP uses the method of broadcasting the entire routing table to synchronize the routing information of the routers in the network. It updates the message regularly every 30 seconds. If a route entry does not receive an update message from a neighbour within 180 seconds, it marks it as unreachable. If it does not receive a valid update within 120 seconds, it deletes the route.

RIP is easy to implement because of its simple idea, but it also brings the corresponding routing loop problem. In order to prevent the routing loop, RIP introduces the split horizon mechanism to avoid the spoofing between routers. Split horizon means that routing updates are not published out the receiving interface. Split horizon with poison reverse publishes routing updates out the receiving interface, but with the metric marked unreachable, allowing neighbouring routers to quickly identify loops without waiting for the metric to increase to unreachable.

Route entries in the routing table should contain a destination address (host or network), a next-hop address, a forwarding interface, a routing metric, a timer that is reset when a routing update is received, and a routing tag.

When RIP is started, it immediately sends a full table request message in the form of broadcast (RIP-1) or multicast (RIP2), and the adjacent router receives the request message and sends back its own complete routing table as a response message. When the router receives the response message, it will process the route one by one and modify its own routing table. When there is a new route, it will immediately generate a trigger update message. After a series of updates, RIP eventually converges, and each router in the network maintains the latest and consistent routing information. After the network is stable, RIP still broadcasts the local routing table to the neighbors every 30 seconds, and each router maintains its own routing information according to the received routing update message to select the most preferred route. RIP uses a timeout mechanism to handle routing entries that have not been updated for a long time to ensure that the route is correct in real time.

RIP is mostly used in campus networks and relatively continuous regional networks with simple struct ure, and it is not competent for large and complex networks.

14.2.2. RIP Configuration

After starting the RIP protocol, you can configure each function and attribute of RIP. RIP is mostly co nfigured in RIP configuration mode and interface configuration mode.

- The configuration of RIP includes:
- Start RIP and enter RIP configuration model
- Enable RIP interface
- Configure unicast message transmission
- Configure the working status of the interface
- Configure the default route weight
- Configuration management distance
- Configure the timer
- Configuration version
- Introducing external routing
- Configure route filtering
- Configure additional routing metric
- Configure the RIP version of the interface
- Configure the receiving and sending status of the interface
- Configure split horizon
- Message authentication
- Configure interface weight

14.2.3. Start RIP and enter RIP configuration

Mode: Global Configuration Mode

Command：router rip Start rip and enter rip configuration model

Command：no router rip Turn off the rip protocol

Default: Do not run the rip protocol

14.2.4. Enable RIP Interface

When RIP works, certain interfaces can be designated, and the network where the interfaces are located can be configured as a RIP network, so that RIP protocol messages can be sent and received on the RIP network.

Mode: RIP configuration model

Command：network <network-address> Enable rip interface

Command：no network <network-address> Shut down the rip interface

Parameters: There are two forms: A. B. C. D/M and A. B. C. D A. B. C. D. The former specifies the network IP and mask length, while the latter specifies the network IP and mask.

Default: RIP is disabled on all interfaces when it is started

When the RIP protocol is started, it must specify the network segment on which it operates. RIP can only run on interfaces that are on the specified network segment. For those interfaces that are not on the specified network segment, RIP will neither receive nor forward routes. Interfaces that are not in the specified network segment do not exist in the RIP view. The parameter network-address is the enabled or disabled network address, which can be configured as the interface IP address. The network command enables the interface of the network segment of the address. For example, if the IP address of an interface is 192.160. 1.1, use the command network 192.160. 1.1/24, and use the show running-config command to see the network 192.160. 1.0/24.

14.2.5. Configure Unicast Message Transmission

RIP version 1 uses broadcasts to exchange messages, and version 2 uses multicasts (224.0, 0.9) to exchange messages. When RIP is running on a link that does not support broadcasts, it is necessary to specify a specific unicast address to exchange messages.

Mode: RIP configuration model
Command : neighbor <ip-address> Configure peer unicast IP address
Command : no neighbor <ip-address> Cancel setting of peer unicast IP address
Parameters: ip-address is the specified unicast IP address
Default: RIP does not send messages to any unicast address

14.2.6. Configure the working status of the interface

The RIP protocol operates in some networks where you may only need RIP interface routes and do not want to broadcast RIP routes on that interface. Use the network command to specify that RIP protocol messages are sent and received on the interface, and you can learn the route of the interface. Use the passive-interface command to simply learn the route for that interface and block broadcasts for that interface.

Mode: RIP configuration model
Command : passive-interface <if-name> Configure the interface to be passive
Command : no passive-interface <if-name> Cancel the passive state of the interface
Parameter: if-name is the agreed name of the three-layer interface (for example: vlan1, vlan2 …)
Default: none of the enabled RIP interfaces are passive

14.2.7. Configure the default route weight

When an external route is introduced, a route metric is specified; when it is not specified, the default route metric is used.

Mode: RIP configuration model
Command : default-metric <metric> Set the default route metric when importing an external rout
Command : no default-metric [metric]The default route metric is the default value of 1 when the external route is restored
Parameter: metric value is between 1 and 16, greater than 1 and less than 16.
Default: The metric value is 1. Use the no default-metric command to return to the default value.

14.2.8. Configure Management Distance

Each protocol has an agreed priority, and the administrative distance is the priority with which the route is selected when a routing policy is used. When there are two identical routes (from different routing protocols) to the same destination, the smaller the administrative distance, the route of the protocol is preferred.

Mode: RIP configuration model
Command : distance <distance> Setting the Administrative Distance Value
Command : no distance [distance] The recovery administrative distance is the default
Parameter: distance is between 1 and 255Parameter: distance is between 1 and 255
Default: The distance value is 120. Use the no distance command to return to the default value.

14.2.9. Configure The Timer

The RIP protocol has three timers, one in which the full routing table is broadcast to all RIP interfaces every 30 seconds, and the other in which each route in the RIP routing table is marked with a metric of 16 if it does not receive an update for 180 seconds. The third is that each route in the RIP routing table is deleted from the routing table if it has not been effectively updated for 120 seconds after the metric is 16.

Mode: RIP configuration model

Command：timers basic <update> <timeout> <garbage> Set three timer values

Command：no timers basic Resume timer as default

Parameters: The first parameter update is the timer for regularly updating the entire RIP routing table; the second parameter timeout is the timer for not updating each route after timeout; the third parameter garbage is the timer to be deleted after timeout after each route is marked as invalid; the value range of the three timers is 5~(231-1).

Default: update is once every 30 seconds; timeout is 180 seconds, marked as invalid; garbage is deleted in 120 seconds

14.2.10. Configuration Version

The RIP protocol currently has version 1 (RFC1058) and version 2 (RFC2453), and the configured version value will be reflected in the version field of the protocol message.

Mode: RIP configuration model

Command：version <version> Set the RIP protocol to version 1 or version 2

Command：no version [version] Restore RIP protocol version to default

Parameter: version can take the value 1 or 2

Default: Version 2

14.2.11. Introducing External Routing

RIP allows the user to import routing information from other protocols into the routing table of RIP. The routing protocols (types) that RIP can import include: connected, static, OSPF, IS-is, and BGP.

Mode: RIP configuration model

Command：redistribute {kernel | connected | static | ospf | isis | bgp} [metric <metric> | route-map <route-map-name>] Introducing Other Protocol Routine

Command：no redistribute {kernel | connected | static | ospf | isis | bgp} [metric <metric> | route-map <route-map-name>]Cancel Incoming Route

Parameters: The first parameter is the name of other protocols to be introduced, including direct connection, static, OSPF, IS-is, and BGP; the second parameter is the value set during introduction, ranging from 1 to 16; the third parameter is the name of the referenced route-map, which is configured in the global configuration mode. Please refer to the command manual.

Default: RIP protocol does not introduce any external protocol

14.2.12. Configure Route Filtering

RIP provides the function of route filtering, and configures policy rules to filter the received routes and published routes through the specified access control list and address prefix list.

Mode: RIP configuration model

Command：distribute-list <acl-name> {in | out} [if-name] Use access-list to filter the input and output of the interface

Command：no distribute-list <acl-name> {in | out} [if-name] Suppress access-list filtering

Parameters: acl-name indicates the name of the referenced access-list; if-name indicates the RIP interface to which the application is applied; in and out indicate whether the application is applied in the direction in which the route was received or in the direction in which the route was published.

Command：distribute-list prefix <pre-name> {in | out} [if-name]Filtering with prefix-list
Command：no distribute-list prefix <pre-name> {in | out} [if-name]Suppress prefix-list filtering
Parameters: pre-name indicates the name of the referenced prefix-list; if-name indicates the RIP interface to which it is applied; in and out indicate whether it is applied in the direction in which the route was received or in the direction in which the route was published.
Default: RIP does not filter any incoming or outgoing route
The access-list and prefix-list are configured in global configuration mode and can be found in the command manual.

14.2.13. Configure additional routing metric

The additional routing metric is an offset value added to the routing metric of the RIP protocol when it is input or output. It does not directly change the metric of the route in the routing table, but adds an offset when the interface receives and sends the route.
Mode: RIP configuration model
Command：offset-list <acl-name> {in | out} <offset> [if-name]
Use the access-list to add an offset to the weight of the interface's input and output route
Command：no offset-list <acl-name> {in | out} <offset> [if-name] Offset to cancel the weight of the input/output route
Parameters: acl-name indicates the access-list name of the reference; in and out indicate whether the application is in the input or output direction; offset indicates the value of the offset between 0 and 16; if-name indicates the RIP interface to which the application is applied.
Default: The additional weight value of each route is 1 when receiving a message, and 0 when sending a message.

14.2.14. Configure RIP Version of the interface

RIP is divided into two versions, RIP-1 and RIP-2, and the RIP message version processed by the interface of the enabled RIP protocol can be specified. The receiving direction can be divided into receiving only RIP-1 messages, receiving only RIP-2 messages, and receiving both RIP-1 and RIP-2 messages. In the sending direction, it can be divided into sending RIP-1 messages, sending RIP-2 messages (in the broadcast mode), sending RIP-2 messages (in the multicast mode), and sending both RIP-1 and RIP-2 messages. RIP-2 has two ways to send messages: broadcast and multicast. Using multicast can not only prevent the hosts that do not run RIP in the same network from not receiving the broadcast messages of RIP, but also prevent the hosts that run RIP-1 from processing the routing with subnet mask of RIP-2 incorrectly.

Mode: Interface configuration model
Command：ip rip receive version {1 | 2} Set the interface to receive only version 1 messages or only version 2 message
Parameter: Version 1 or Version 2
Command：ip rip receive version {1 2 | 2 1} Set the interface to receive both version 1 and version 2 messages
Parameter: can be written as 1 2 or 2 1
Command：no ip rip receive version [1 | 2 | 1 2 | 2 1] Recover the setting of interface receiving message to the default value
Default: Version 2 multicast mode
Command：ip rip send version {1 | 2 | 1-compatible} Set the interface to send only messages of version 1 or only messages of version 2

Parameter: version 1 or version 2; 1-compatible indicates that the interface of version 2 sends a message compatible with version 1, that is, a broadcast message rather than a multicast message.
Command：ip rip send version {1 2 | 2 1}Set the interface to send both version 1 and version 2 messages
Parameter: can be written as 1 2 or 2 1
Command：no ip rip send version [1 | 2 | 1-compatible | 1 2 | 2 1]The message sent by the recovery interface is set as the default value.
Default: Version 2 multicast mode

14.2.15. Configure the receiving and sending status of the interface

After the RIP interface is enabled by using the network command in the RIP mode, you can also specify the status of receiving and sending protocol messages, whether to receive protocol messages, or whether to send protocol messages in the interface mode.
Mode: Interface configuration model
Command：ip rip receive-packet Configure interface to receive protocol message
Command：no ip rip receive-packet Configure the interface not to receive the protocol message
Command：ip rip send-packet Configure interface to send protocol message
Command：no ip rip send-packet Configure the interface not to send protocol message
Default: enable to receive and send protocol message

Note the difference. The network command enables a network to run the RIP protocol. The interface in the network sends and receives protocol messages. The interface route is included in the routing table. After the network command takes effect, the passive-interface command prevents the interface from sending and receiving protocol messages, but the interface route is still included in the routing table. The IP rip receive-packet and IP rip send-packet commands also specify whether the interface is to receive or send a protocol packet after the network command comes into effect.

14.2.16. Configure Split Horizon

Split horizon means that a route received from this interface is not sent out this interface. Split horizon with poison reverse means that the route received from this interface is still sent out this interface, but its metric value is marked as 16. Split horizon can avoid loops to some extent. Split horizon with poison reversal is more efficient than normal split horizon, and direct marking is unreachable. But on NBMA networks, you need to disable split the horizon to get the correct route.
Mode: Interface configuration model
Command：ip rip split-horizon [poisoned] Enable interface split horizon or with poison reverse
Command：no ip rip split-horizon Disables the split horizon feature on the interface
Parameters: no poisoned parameter means normal split horizon function is enabled, and poisoned parameter means split horizon function with poison reversal is enabled.
Default: Split horizon with poison reversal

14.2.17. Message Authentication

RIP-1 does not support message authentication. RIP-2 supports message authentication. There are two authentication methods, plaintext authentication and MD5 authentication. The unencrypted authentication data in plaintext authentication is transmitted with the message, which cannot provide security guarantee and cannot be applied to the network with high security requirements.

There are two kinds of password settings: the common key and the key chain. The common key stores an independent string, and the key chain manages the ID, content, receiving lifetime, and sending lifetime of the key. Key chain management is detailed in the command reference manual.

Mode: Interface configuration model

Command：ip rip authentication mode {text | md5} Set authentication mode plaintext or MD5

Command：no ip rip authentication mode [text | md5] Decertification

Parameter: text is plaintext authentication, MD5 authentication.

Default: No authentication

Command：ip rip authentication string <password> Set the password string for authentication

Command：no ip rip authentication string [password] Unauthenticated password string

Parameter: 16-byte authentication password

Command：ip rip authentication key-chain <key-chain-name>Set the key-chain for authentication

Command: no IP rip authentication key-chain key-chain-name] unauthenticated key-chain

Parameter: The name of the referenced key-chain; the key-chain is configured in the global configuration mode. See the command manual.

14.2.18. Configure Interface Weight

Mode: Interface configuration model

Command：ip rip metric <metric> Configure interface weight

Command：no ip rip metric Restore interface weights to default values

Parameter: The metric value is between 1 and 16, indicating the metric to be increased for the routing entry learned by the interface.

Default: 1

14.2.19. Display Information

Mode: Normal or Privileged

Command：show ip protocols Displays information about all protocols that are running

Command：show ip protocols rip Displaying RIP Protocol Information

Command：show ip rip Displaying RIP Routine

Command：show ip rip database. Show RIP Database

Command：show ip rip database count . Displays the number of RIP database entries

Command：show ip rip interface [if-name] Displaying RIP Interface Information

Parameter: if-name is the agreed three-layer interface name

Mode: Privileged Mode

Command：show running-config. Displays the current configuration of the switch, including RIP configuration.

Command：show running-config rip. Displays the current configuration of the RIP protocol.

14.2.20. Sample RiP Configuration

The three switches are connected in pairs and have six network segments respectively, and rip protocol is enabled, so that the three PCs can communicate with each other in pairs.

On Switch 1:

Switch# configure terminal

Switch(config)#router rip

Switch(config-rip)#network 192.168.1.0/24

Switch(config-rip)#network 10.1.1.0/24

Switch(config-rip)#network 10.1.2.0/24

On Switch 2:

Switch# configure terminal

Switch(config)#router rip

Switch(config-rip)#network 192.168.2.0/24

Switch(config-rip)#network 10.1.2.0/24

Switch(config-rip)#network 10.1.3.0/24

On Switch 3:

Switch# configure terminal

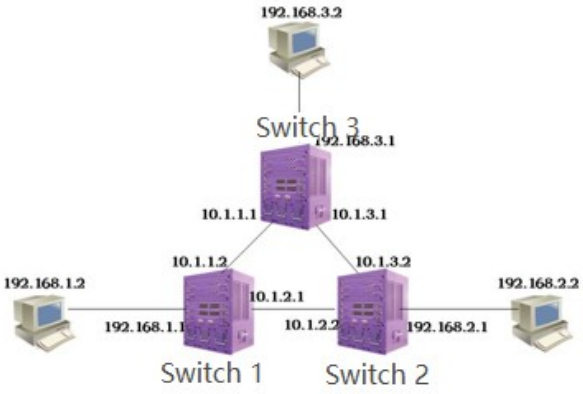
Switch(config)#router rip

Switch(config-rip)#network 192.168.3.0/24

Switch(config-rip)#network 10.1.1.0/24

Switch(config-rip)#network 10.1.3.0/24

Sample Rip Configuration



(2) Verification

Use the following command to view RIP information:

show ip protocols rip

show ip rip database

show ip rip interface

14.3. Configuring RIPng

14.2.1. RIPng Introduction

RIPng is a relatively simple internal gateway protocol, which is the application of rip in IPv6 network. RIPng is mainly used in smaller networks, such as campus networks and regional networks with simple structure. Since the implementation of RIPng is relatively simple, and it is much easier than OSPFv3 and IS-IS for IPv6 in configuration and maintenance management, RIPng is still widely used in practical networking

With the construction of IPv6 network, dynamic routing protocol is also needed to provide accurate and effective routing information for IPv6 message forwarding. Therefore, on the basis of retaining the advantages of rip, IETF forms Rip (RIP next generation) for IPv6 network modification. RIPng is mainly used to provide routing function in IPv6 network. It is an important protocol of routing technology in IPv6 network.

Differences between RIPng and rip

In order to realise the application in IPv6 network, RIPng modifies the original rip protocol ：

- RIPng uses port 521 of UDP (RIP uses port 520) to send and receive routing information.
- The destination address of RIPng uses a 128-bit prefix length (mask length).
- RIPng uses a 128-bit IPv6 address as the next hop address.
- RIPng uses the link local address fe80:: / 10 as the source address to send RIPng routing information update message.
- RIPng sends routing information periodically by multicast and uses ff02:: 9 as the router multicast address within the local range of the link.
- RIPng messages are composed of header and multiple route table entries. In the same RIPng message, the maximum number of RTE is determined according to the MTU value of the interface.

14.2.2. RIPng Configuration

After starting RIPng protocol, you can configure various functions and attributes of RIPng. RIPng is mostly configured in RIPng configuration mode and interface configuration mode.

- RIPng configuration includes:
- Start RIPng and enter RIPng configuration mode
- Enable RIPng interface
- Configure specific neighbors to send updates
- Configure the working state of the interface
- Configure default routing weights
- Configure timer
- Introducing external routing
- Configure routing filtering
- Configure additional routing weights
- Configure horizontal segmentation
- Configure interface weights

14.2.3. Start RIPng and enter RIPng Configuration

1Start RIPng and enter RIPng configuration mode

Mode: global configuration mode

Command: router IPv6 rip Start RIPng and enter RIPng configuration mode

Command: no router IPv6 rip Close RIPng protocol

Default: RIPng protocol is not run

14.2.4. Enable RIPng Interface

When RIPng works, some interfaces can be specified, and the network it is in can be configured as RIPng network, on which RIPng protocol messages can be sent and received.
Mode: interface configuration mode
Command: IPv6 Router rip Enable RIPng interface

Command: no IPv6 Router rip Close RIPng interface
Parameter: none.
Default: disabled on all interfaces after RIPng protocol is started
After RIPng protocol is started, its working interface must be specified, and RIPng can only run on the specified interface.

14.2.5. Configure specific neighbours to send updates

Specify neighbours and send updates to specific neighbours.
Mode: Rip configuration mode
Command: neighbor < neighbor address > < ifname > Configure IPv6 addresses for specific neighbours
Command: neighbor < neighbor address > < ifname >Cancel specific neighbor configuration
Parameter: neighbor address is the IPv6 address of a specific neighbor

14.2.6. Configure the working state of the interface

RIPng protocol runs in some networks. It may only need RIPng interface routing and does not want to broadcast RIPng routing on this interface. Use the passive interface command to only know the route of the interface and block the broadcast of the interface.
Mode: RIPng configuration mode
Command: passive interface < if name > Configure the interface to be passive
Command: no passive interface < if name > Cancel interface passive state
Parameter: if name is the agreed three-tier interface name (for example: vlan1, vlan2...)

14.2.7. Configure default routing weights

When introducing an external route, you need to specify a route weight; When the routing weight is not specified, this default routing weight is used.
Mode: RIPng configuration mode
Command: default metric < metric > Set the default route weight when introducing external routes
Command: no default metric [Metric] When the external route is restored, the default route weight is 1
Parameter: metric value is between 1 and 16, greater than 1 and less than 16.
Default: the metric value is 1. Use the no default metric command to restore to the default value.

14.2.8. Configure timer

RIPng protocol has three timers. One is that the complete routing table broadcasts to all RIPng interfaces every 30 seconds. The other is that each route in RIPng routing table is marked with metric of 16 if it does not receive update in 180 seconds. The third is that each route in RIPng routing table is deleted from the routing table if it is marked with metric of 16 and not effectively updated in 120 seconds.
Mode: RIPng configuration mode
Command: timers basic < update > < timeout > < garbage > Set three timer values
Command: no timers basic The recovery timer is the default
Parameters: the first parameter update is the timer for regularly updating the entire RIPng routing table, the second parameter timeout is the timer for each route timeout without updating, and the third

parameter garbage is the timer to be deleted after each route is marked as invalid; The value range of the three timers is 5 ~ (231-1).
Default: update every 30 seconds; When timeout is 180 seconds, it is marked as invalid; Garbage is deleted in 120 seconds.

14.2.9. Introducing external routing

RIPng allows users to introduce the routing information of other protocols into the routing table of rip. The routing protocols (types) that RIPng can introduce include connected, static, OSPF, IS-IS and BGP.
Mode: RIPng configuration mode
Command: redistribute {kernel | connected | static | ospf6 | Isis | BGP} [Metric < metric > | route map < route map name >] Introducing other protocol routes
Command: no redistribute {kernel | connected | static | ospf6 | Isis | BGP} [Metric < metric > | route map < route map name >] Cancel incoming route
Parameter: the first parameter is the name of the imported other protocols, including direct connection, static, OSPF, is is and BGP; The second parameter is the weight set during import, with a value between 1 and 16; The third parameter is the name of the referenced route map. Route map is configured in the global configuration mode. Please refer to the command manual.
Default: RIPng protocol does not introduce any external protocols

14.2.10. Configure routing filtering

RIPng provides the function of route filtering. It filters the received routes and published routes and configures policy rules through the specified access control list and address prefix list.
Mode: RIPng configuration mode
Command: distribute list < ACL name > {in | out} [if name] Use access list to filter the input and output of the interface
Command: no distribute list < ACL name > {in | out} [if name] Cancel access list filtering
Parameter: ACL name indicates the name of the referenced access list; If name indicates the RIPng interface applied to; In and out indicate whether the application is in the direction of receiving routes or publishing routes.
Command: distribute list prefix < pre name > {in | out} [if name] Filter using prefix list
Command: no distribute list prefix < pre name > {in | out} [if name] Cancel using prefix list filtering
Parameter: pre name indicates the name of the referenced prefix list; If name indicates the RIPng interface applied to; In and out indicate whether the application is in the direction of receiving routes or publishing routes.
Default: RIPng protocol does not filter any received and sent routes
Access list and prefix list are configured in global configuration mode. Please refer to the Command Line Manual

14.2.11. Configure additional routing weight

The additional routing weight is an offset value added to the routing weight of RIPng protocol during input and output. It does not directly change the weight of the route in the routing table, but adds an offset when the interface receives and sends the route.
Mode: RIPng configuration mode
Command: offset list < ACL name > {in | out} < offset > [if name] Use access list to add an offset to the weight of interface input-output route
Command: no offset list < ACL name > {in | out} < offset > [if name] Cancel the offset of the weight of the input-output route

Parameter: ACL name indicates the access list name of the reference; In and out indicate whether the application is in the input or output direction; Offset represents the value of the offset, which is between 0 and 16; If name indicates the RIPng interface applied to.
Default: when receiving a message, the additional weight of each route is 1, and when sending a message, the additional weight of each route is 0.

14.2.12. Configure horizontal segmentation

Horizontal segmentation means that the route received from this interface is not sent from this interface. Horizontal segmentation with toxic inversion means that the route received from this interface is still sent from this interface, but its metric value is marked as 16. Horizontal segmentation can avoid loops to a certain extent. The horizontal segmentation with toxic inversion is more efficient than ordinary horizontal segmentation, and direct labeling is not reachable. However, in nBMA network, it is necessary to prohibit horizontal segmentation to obtain the correct route.
Mode: interface configuration mode
Command: IPv6 rip split horizon [poisoned] Start the horizontal division function of the interface or with toxic inversion
Command: no IPv6 rip split horizon The horizontal division function of the interface is prohibited
Parameters: no poisoned parameter means to start the normal horizontal segmentation function, and with poisoned parameter means to start the horizontal segmentation function with toxic inversion.
Default: horizontal segmentation with toxic inversion

14.2.13. Configure Interface Weights

Mode: interface configuration mode
Command: IPv6 rip metric offset < metric > Configure interface weight
Command: no IPv6 rip metric offset < metric > Restore the interface weight to the default value
Parameter: the metric value is between 1-16, indicating the weight to be added to the routing entry learned by the interface.
Default: 1

14.2.14. Display Information

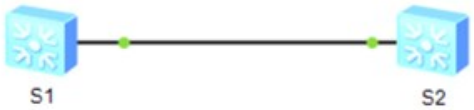
Mode: normal mode or privileged mod
Command: Show IPv6 rip Displays information about the current system RIPng
Command: Show IPv6 route rip Displays the currently active RIPng routing information

14.2.15. RIPng configuration example

S1 switch is configured as follows

```
Switch(config)#
Switch(config)#int vlan1
Switch(config-vlan1)#ipv6 address 3ffe:506::1/64
Switch(config-vlan1)#exit
Switch(config)#router ipv6 rip
Switch(config-router)#exit
Switch(config)#int vlan1
Switch(config-vlan1)#
Switch(config-vlan1)#ipv6 router rip
Switch(config-vlan1)#
```

RIPng Example



S2 switch is configured as follows

```
Switch(config)#
Switch(config)#int vlan1
Switch(config-vlan1)#ipv6 address 3ffe:506::2/64
Switch(config-vlan1)#exit
Switch(config)#router ipv6 rip
Switch(config-router)#exit
Switch(config)#int vlan1
Switch(config-vlan1)#
Switch(config-vlan1)#ipv6 router rip
Switch(config-vlan1)#
```

14.4. Please Refer to the CLI Manual for advanced configuration options

Some examples are

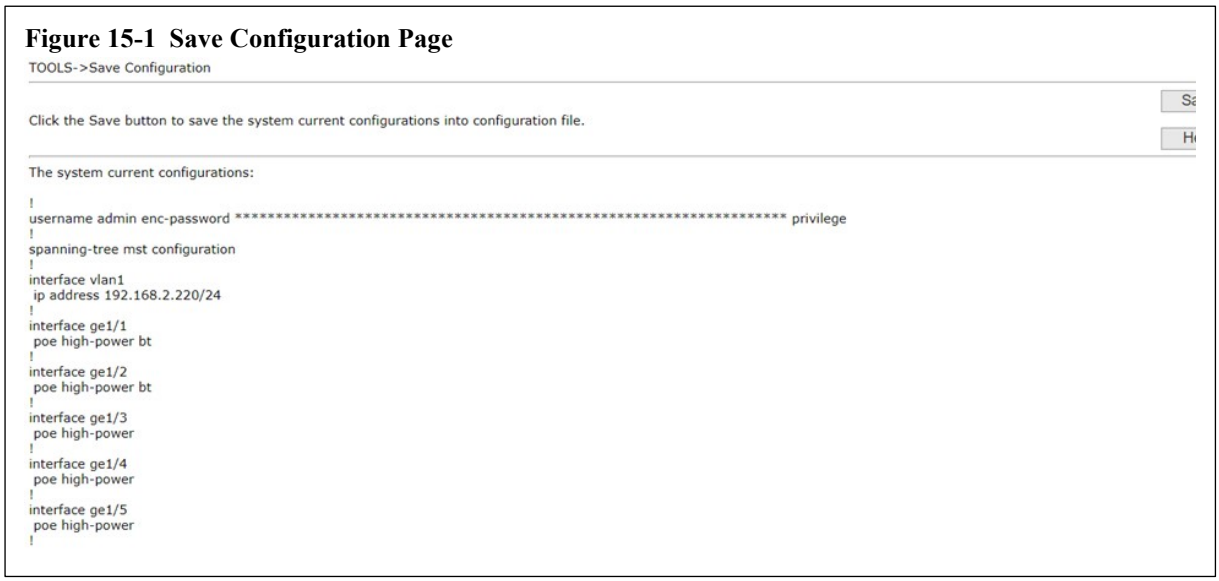
- Configuring OSPF and OSPFv3
- Configuring BGP4
- Configuring VRRP
- Configuring VLLP
- Configuring Policy Routing
- Configuring IPv6
- Configuring Neighbour Discovery Protocol
- Configuring IPv6 Static Route Configuration
- Configuring MLD Snooping
- Configuring Layer-2 dynamic multicast
- Configuring GVRP

15 System Tools

15.1 Save Configuration

Figure 15-1 is the Save Configuration page. This page allows the user to view the current configuration of the switch. The Save button is used to save the current configuration of the system to the configuration file. Because the storage operation needs to erase the FLASH chip. which takes a certain amount of time. When the user has made the configuration on the page and wants to restart the switch without losing the configuration. he must click the Save button on the current configuration page before exiting the page.

Figure 15-1 Save Configuration Page



15.2 Backup configuration films

Figure 15-2 is the Backup Profile page. This page allows the user to view the initial configuration of the system. The initial configuration is actually the configuration file in FLASH. When there is no configuration file in FLASH. the default configuration is used when the system is started. Click the Backup button. a dialog box will pop up and the user can select the directory path and save the configuration file. The filename of the downloaded configuration file defaults to the switch. CFG.

Figure 15-2 Backup Profile Page

15.3 Restore Configuration File

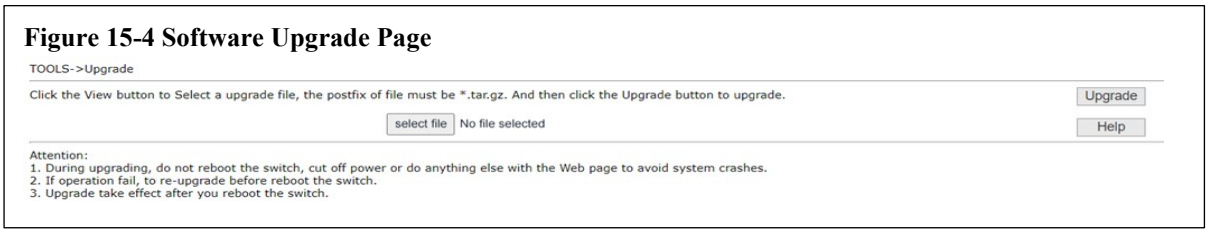
Figure 15-3 shows the Restore Configuration File page. which allows the user to upload a configuration file to the switch. Click the Browse button to select the directory path of the uploaded configuration file on the PC. Click the Upload button to upload the configuration file. The suffix of the configuration file must be *.cfg. Please do not click other pages or restart the switch before returning to the transfer result page; otherwise. the file transfer will fail and the system will crash.

Figure 15-3 Restore Profile Page

15.4 Software upgrade

Figure 15-4 shows the Software Upgrade page. which allows users to upload image files to the switch. Click the Browse button to select the directory path of the uploaded image file on the PC. Click the Upload button to upload the image file. which must be provided by the manufacturer and the file name suffix must be *.img. Please do not click other pages or restart the switch before returning to the transfer result page; otherwise. the file transfer will fail and the system will crash.

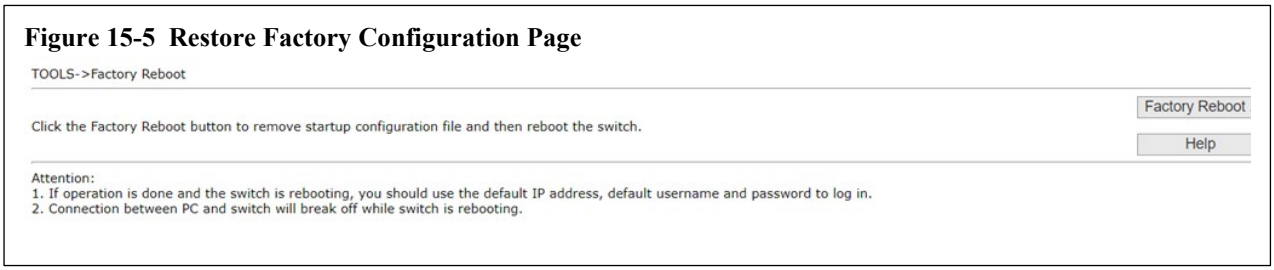
Figure 15-4 Software Upgrade Page



15.5 Restore Factory Configuration

Figure 15-5 shows the Restore Factory Configuration page. This page allows the user to delete the configuration file in FLASH to return to the factory configuration. Click the Restore Factory Configuration button. and a dialog box will pop up to prompt the user whether to confirm. After the factory configuration is restored. the switch will automatically restart to make the factory configuration take effect. Please use the factory default IP address and password when logging in

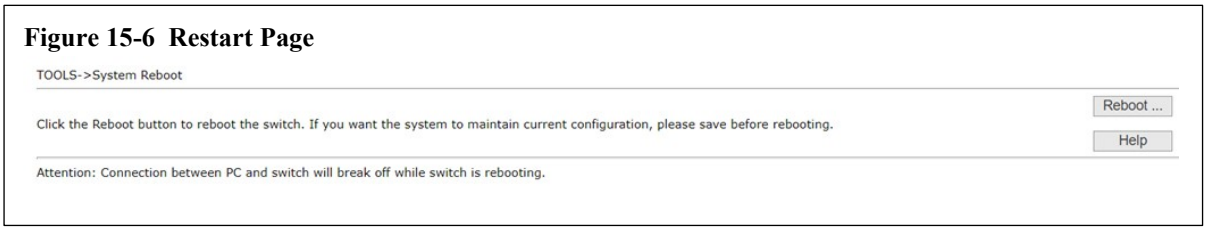
Figure 15-5 Restore Factory Configuration Page



15.6 Restart

Figure 15-6 shows the restart page through which the user restarts the switch. When the Restart button is clicked. a dialog box will pop up to prompt the user whether to restart the switch. If yes. press the OK button. otherwise press the Cancel button. Web pages will no longer open when you restart.

Figure 15-6 Restart Page



This page left blank Intentionally

Case Communications
www.casecomms.com