



USER MANUAL

10GATS-8-L23

L3 Managed Ethernet Switch

Web Interface User Manual

Ver 1.01

PoE Texas

Contents

Notices	1
Copyright.....	1
Trademarks	1
About This Manual	1
Intended Audience	1
Conventions	2
Product Overview	3
Product Features.....	3
Port Features.....	3
MAC Address Features	4
VLAN Features.....	4
Ring and Redundancy Features	4
Layer 3 Routing Features.....	5
Multicast Features.....	5
ACL and QoS Features	5
DHCP Features.....	6
Management Features.....	6
Security Features.....	7
PoE Features.....	7
IPv6 Features.....	7
Version History	8
Part 1 — Web Interface Overview	9
1. Characteristics of Web Access	9
2. System Requirements for Web Browsing	9
3. Logging In to the Web Interface	9
4. Basic Composition of the Web Page	11
5. Page Buttons	11
6. Error Messages	12
7. Entry Fields.....	12
Part 2 — Web Page Reference	14
1. System Configuration	14
1.1 System Information	14
1.2 IP Address Configuration	14
1.3 User Management.....	15
1.4 Serial Port Information	15
1.5 SNMP Configuration	15
1.6 SNMP Community Configuration	16
1.7 SNMP Trap Configuration	16
1.8 Log Information	17

2. Port Configuration	17
2.1 Port Basic Configuration	17
2.2 Port Statistics.....	18
2.3 Port Storm Suppression.....	18
2.4 Port Speed Limit	19
2.5 Protection Port	19
2.6 Port Mirroring.....	20
2.7 Link Aggregation.....	21
2.8 DDM Information	21
3. PoE Configuration	22
3.1 PoE Port Configuration	22
3.2 PoE Scheduling Configuration	22
3.3 PD Query Configuration.....	23
4. VLAN Configuration	24
4.1 VLAN Configuration	24
4.2 Access Port Configuration	24
4.3 Trunk Port Configuration.....	25
4.4 Hybrid Port Configuration	25
4.5 GVRP Configuration.....	26
5. Layer 3 Configuration	27
5.1 IP Basic Configuration.....	27
5.2 RIP Configuration.....	28
5.3 OSPF Configuration.....	29
5.4 VRRP Configuration	30
6. Security Configuration	30
6.1 MAC Configuration	30
6.2 ACL Configuration.....	32
6.3 AAA Configuration.....	35
6.4 Management Security Configuration	37
7. DHCP Configuration	38
7.1 DHCP Client	38
7.2 DHCP Relay	38
7.3 DHCP Server	38
7.4 DHCP Snooping.....	39
8. Multicast Configuration.....	40
8.1 IGMP Snooping Configuration	40
8.2 GMRP Configuration.....	41
8.3 Multicast Routing Configuration	42
8.4 IGMP Configuration.....	42
8.5 PIM-SM Configuration	43
9. Ring Network Configuration.....	45
9.1 Spanning Tree Configuration	45
9.2 ERPS Configuration	45
9.3 EAPS Configuration.....	47
10. Advanced Configuration	49
10.1 QoS Configuration	49
10.2 LLDP Configuration	49
11. System Tools	50

11.1 Save Configuration	50
11.2 Back Up Configuration File	51
11.3 Restore Configuration File	51
11.4 Software Upgrade	52
11.5 Restore Factory Configuration.....	52
11.6 Restart	53

Notices

Copyright

© PoE Texas. All rights reserved.

No part of this manual may be extracted, reproduced, or distributed in any form by any organization or individual without the prior written permission of PoE Texas.

Trademarks

Microsoft®, Windows XP®, Windows Vista®, Windows 7®, and Windows 8® are registered trademarks of Microsoft Corporation. All other product names, trademarks, registered trademarks, and service marks are the property of their respective owners.

About This Manual

This manual describes the web management interface of the PoE Texas 10GATS-8-L23 L3 Managed Ethernet Switch. It explains how to reach the web interface and what each configuration page does.

The manual is a page-by-page reference to the web interface. For a full explanation of the switch features themselves, and for the equivalent command-line configuration, refer to the 10GATS-8-L23 CLI User Manual.

The manual is organized into two parts:

- **Part 1 — Web Interface Overview.** Browser requirements, how to log in, how the page is laid out, and the conventions used throughout the interface.
- **Part 2 — Web Page Reference.** A description of every configuration page, grouped the same way the interface groups them.

Intended Audience

This manual is written for:

- Network planners and designers
- On-site technical support and maintenance personnel
- Network administrators responsible for network configuration and maintenance

Conventions

Convention	Meaning
Bold	A field, button, menu item, or other element you interact with on screen.
<i>Italic</i>	A value you supply, or a term being defined.
Note	Supplementary information that helps you use a feature correctly.
Caution	Information you must read to avoid losing configuration, losing management access, or damaging the switch.

Product Overview

The PoE Texas 10GATS-8-L23 is a Layer 3 managed Ethernet switch designed for building high-security, high-performance networks. Built on a modern hardware and software platform, it serves as a convergence-layer switch for office networks, campus networks, small and medium-sized businesses, and branch offices.

The switch is fully managed and supports Layer 2 switching, Layer 3 routing, multicast, quality of service, access control, Power over Ethernet, and a complete set of management and security services over both IPv4 and IPv6.

Product Features

The tables below summarize the feature set of the 10GATS-8-L23. Availability of individual features depends on the firmware version.

Port Features

Feature	Details
Port shutdown	Individual ports can be administratively enabled or disabled.
Auto-negotiation	Port speeds of 10000M, 2500M, 1000M, 100M, 100M half-duplex, 10M, and 10M half-duplex.
Flow control	IEEE 802.3x flow control in full duplex; backpressure flow control in half duplex.
Storm suppression	Rate limiting for broadcast, multicast, and DLF (destination lookup failure) packets.
Storm constrain	Monitors the broadcast, multicast, or unicast packet rate on a port and shuts the port down when the rate exceeds a configured threshold.
Port mirroring	Supported.
Rate limiting	Independent ingress and egress rate limits per port.
Link aggregation	Manual link aggregation and LACP dynamic link aggregation. Up to 32 aggregation groups with up to 8 ports per group.
Load balancing	Source MAC, destination MAC, source + destination MAC, source IP, destination IP, and source + destination IP.
Port isolation	Supported.
Jumbo frames	Frames up to 12 KB.
Redundant port	Supported.
DDM	Digital diagnostic monitoring on fiber ports.

MAC Address Features

Feature	Details
MAC table capacity	16K entries.
MAC table management	Supported.
Forwarding mode	IVL (independent VLAN learning).
Static MAC	Static MAC addresses, MAC address binding, and MAC address filtering.
Learning control	MAC address learning can be controlled per port.

VLAN Features

Feature	Details
VLAN capacity	4K VLANs.
VLAN types	802.1Q-based, MAC-based, IP-subnet-based, and protocol-based VLANs.
Voice VLAN	Supported.
VLAN mapping	1:1 VLAN mapping.
QinQ	Basic QinQ and flexible QinQ.
GVRP	Supported.

Ring and Redundancy Features

Feature	Details
Spanning tree	STP, RSTP, and MSTP.
Loop detection	Port loop detection.
EAPS	RFC 3619.
ERPS	ITU-T G.8032 / Y.1344.
LLDP	LLDP and LLDP-MED.
UDLD	Fully compatible with the Cisco UDLD protocol.
VLLP	Supported with VRRP only.

Layer 3 Routing Features

Feature	Details
ARP	Static and dynamic ARP.
Static routing	IPv4 and IPv6 static routes.
VLAN interfaces	Up to 32 VLAN interfaces.
RIP	RIP v1/v2 and IPv6 RIPng.
OSPF	OSPFv2 and IPv6 OSPFv3.
BGP	BGP4 and IPv6 BGP4+.
Policy routing	Supported.
VRRP	Supported.

Multicast Features

Feature	Details
Static multicast	Static multicast MAC addresses.
IGMP Snooping	IGMP Snooping v1/v2/v3, IGMP Querier, and IGMP Snooping filtering.
IGMP	IGMP v1/v2/v3.
Other protocols	MVR, GMRP, and PIM-SM.

ACL and QoS Features

Feature	Details
IP ACLs	Standard and extended IP-based ACLs.
MAC ACLs	MAC-based, ARP-based, and time-based ACLs.
ACL application	ACLs can be applied to ports for packet filtering.
Port queues	8 queues per port.
Queue scheduling	WRR, WFQ, and SP.
Classification	Port-based, 802.1p-based, DSCP-based, and ACL-based.
Queue mapping	Packets can be mapped to queues.

Feature	Details
Remarking	CoS or DSCP remarking.
Data flow handling	Data flow statistics, rate limiting, and mirroring.

DHCP Features

Feature	Details
DHCP roles	DHCP Client, DHCP Server, DHCP Relay, and DHCP Snooping.
DHCP Option 82	Supported.

Management Features

Feature	Details
Access methods	Console, Telnet, and SSH.
Concurrent sessions	Multiple Telnet links and SSH connections over IPv4 and IPv6.
Web access	HTTP and HTTPS over IPv4 and IPv6.
SNMP	SNMP v1, v2, and v3, plus SNMP traps, over IPv4 and IPv6. Supports a wide range of standard and private MIBs.
User management	Multiple user accounts.
Logging	Local log management and SYSLOG.
RMON	RMON groups 1, 2, 3, and 9.
Discovery	NDP and NTP.
Clustering	Manual and automatic joining of cluster groups, with unified cluster management.
Configuration files	Configuration file upload and download, using TFTP over IPv4 and IPv6.
Clock	Local clock management and SNTP.
Service control	Telnet, SSH, HTTP, HTTPS, and SNMP services can each be enabled or disabled, and can be bound to standard IP ACLs. The number of Telnet and SSH connections can be limited.

Security Features

Feature	Details
RADIUS	Authentication, authorization, and accounting through a RADIUS server.
TACACS+	Remote username and password authentication, command authorization, and operation over IPv4 and IPv6.
Password encryption	PAP and CHAP.
802.1X	Port-based and MAC-based 802.1X, with guest VLAN support.
Static binding	Static IP, MAC, and port binding.
Dynamic binding	Dynamic IP, MAC, and port binding, and dynamic ARP binding to prevent ARP spoofing.
DHCP protection	A fixed port can be designated for the DHCP server, preventing unauthorized DHCP servers from being connected.
ARP protection	MAC and ARP ACL rules can be configured manually to prevent ARP spoofing. With DHCP Snooping enabled, the switch dynamically binds ARP to the port during DHCP address acquisition, which also prevents ARP spoofing.

PoE Features

Feature	Details
PoE controllers	MAX5980, LTC4259, LTC4271, TPS23851, TPS23861, TPS22880, TPS23881, IP808, PD69100/69108, PD69200/69208, and Hasivo PoE.
Port power control	PoE power can be switched on or off per port.
Power budget	Total system power can be set.
Scheduling	PoE scheduling policy and PD online query.

IPv6 Features

Feature	Details
Dual stack	IPv4/IPv6 dual protocol stack, IPv6 neighbor discovery, ICMPv6, and IPv6 path MTU discovery.
Address configuration	Manual address configuration and stateless address autoconfiguration.
Diagnostics	PING, PING6, and traceroute.
Clients	Telnet client and SSH client over IPv4 and IPv6.

Version History

Version	Changes
Ver 1.0.1	General user experience improvements. Known issues resolved and response time improved. Full support for one-click switching between Chinese and English. Related functions optimized to simplify management.

Part 1 — Web Interface Overview

1. Characteristics of Web Access

The switch provides a web management interface. You can reach the switch with a standard web browser to manage and configure it. The main characteristics of web access are:

- **Easy access.** You can reach the switch from anywhere on the network.
- **Standard browsers.** Familiar browsers such as Mozilla Firefox, Google Chrome, Opera, and Microsoft Internet Explorer 8.0 or later can be used. Pages are presented in graphical and tabular form.
- **Broad coverage.** The web interface exposes most of the switch's functions, so almost all configuration and management can be done from the browser.
- **Logical grouping.** Pages are classified and grouped by function, which makes the relevant configuration and management page easy to find.

2. System Requirements for Web Browsing

The requirements for the management PC are listed below.

Item	Requirement
CPU	Pentium 586 or better
Memory	128 MB or more
Resolution	1024 × 768 or higher
Color depth	256 colors or more
Browser	Internet Explorer 8.0 or later, Firefox, Google Chrome, or Opera
Operating system	Microsoft® Windows XP®, Windows Vista®, Windows 7®, Windows 8®, Linux, or Unix

Table 1 Management PC requirements

NOTE

Microsoft®, Windows XP®, Windows Vista®, Windows 7®, and Windows 8® are registered trademarks of Microsoft Corporation. All other product names, trademarks, registered trademarks, and service marks are the property of their respective owners.

3. Logging In to the Web Interface

Before starting a web session, confirm the following:

- The switch has an IP address configured. By default, the VLAN 1 interface IP address is **192.168.0.1** with a subnet mask of **255.255.255.0**.

- A host with a web browser installed is connected to the network and can ping the switch.

Once both conditions are met, enter the switch's IP address in the browser address bar and press **Enter**. The login page opens, as shown in Figure 1. Access is granted only when the correct credentials are entered.

Item	Default value
User name	admin
Password	Empty (no password)

The image shows a web browser window displaying a login page. The title is "Sign in". Below the title is the URL "http://192.168.0.1". A warning message states "Your connection to this site is not private". There are two input fields: "Username" and "Password". The "Username" field is highlighted with a blue border. Below the input fields are two buttons: "Sign in" (blue) and "Cancel" (white with a blue border).

Figure 1 Web session login page

CAUTION

Set a password on the **admin** account before placing the switch into service. The account ships with no password.

4. Basic Composition of the Web Page

As shown in Figure 2, the web page consists of four areas: the banner, the category navigation bar, the menu pane, and the main pane.

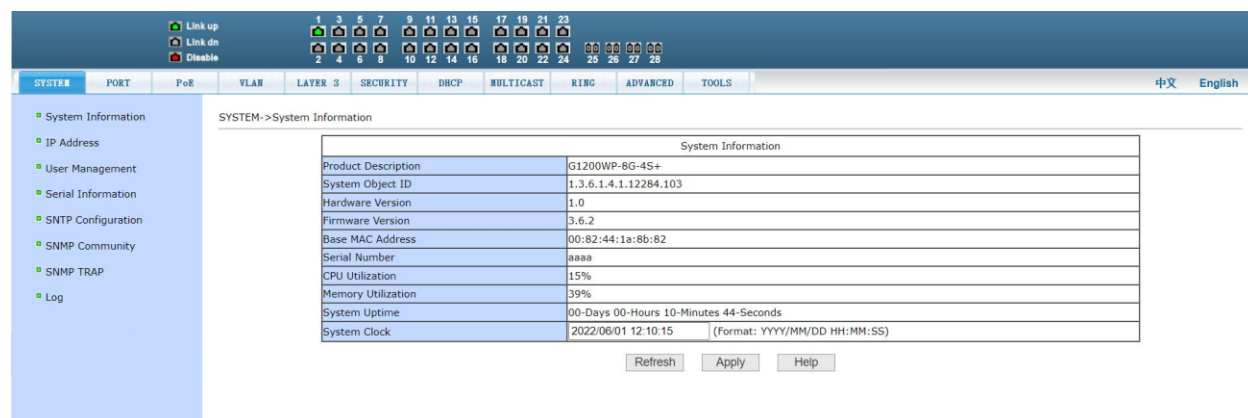


Figure 2 Basic composition of the switch web page

Area	Purpose
Banner	Displays the logo and the real-time port status.
Category navigation bar	The top-level function categories. Click a button to display the corresponding menu. The switch model, firmware version, and the logged-in user name are shown at the right side.
Menu pane	Displays the menu for the selected category. Menus may have primary and secondary levels. Click a menu item to open the corresponding page.
Main pane	Displays the page selected from the menu pane.

The port status indicators in the banner use the following colors:

Indicator	Meaning
Green	The port is connected.
Gray	The port is not connected.
Red	The port is down.

5. Page Buttons

The same set of buttons appears on many pages, and their behavior is consistent throughout the interface.

Button	Action
Refresh	Updates all fields on the page.
Apply	Writes the updated values into memory. Error checking is performed by the web server, so errors are not reported until this button is clicked.
Delete	Deletes the current record.
Help	Opens the help page with configuration instructions for the current page.

Table 2 Common page buttons

6. Error Messages

If the switch's web server encounters an error while processing a request, it displays the error in a dialog box. Figure 3 shows an example.

*Figure 3 Error message dialog*

7. Entry Fields

Some pages begin with an entry field, as shown in Figure 4. The entry field selects which record the page acts on. When you select a value in the entry field, the information for that row is displayed on the page and the row becomes editable. That row is referred to as the **active row**.

Link up

Link dn

Disable

1 3 5 7 9 11 13 15 17 19 21 23

2 4 6 8 10 12 14 16 18 20 22 24 25 26 27 28

SYSTEM

PORT

PoE

VLAN

LAYER 3

SECURITY

DHCP

MULTICAST

RING

ADVANCED

TOOLS

中文

English

System Information

IP Address

User Management

Serial Information

SNTP Configuration

SNMP Community

SNMP TRAP

Log

SYSTEM->User Management

User Management

User Name

User Level

Password

Confirm Password

normal

Attention: User name and password are case sensitive.

Refresh

Apply

Help

Item	User Name	User Level	Operation
1	admin	privilege	delete

Figure 4 Entry field

Part 2 — Web Page Reference

The web pages of the switch are organized into groups, and each group contains one or more pages. Each page is described below.

1. System Configuration

1.1 System Information

The System Information page lets you view the switch's system information and set the system clock.

Field	Description
Product model	The product model of the switch.
Firmware version	The firmware version currently running on the switch.
Bootrom version	The Bootrom version currently in use.
Base MAC address	The base MAC address of the switch.
Serial number	The serial number of the switch.
Serial port baud rate	The baud rate used by the console serial port.
System startup time	Time elapsed since the switch was started.
System clock	The current system clock. This field is editable; year, month, day, hour, minute, and second must all be entered.

SYSTEM->System Information

System Information	
Product Description	G1200WP-8G-4S+
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

Figure 1-1 System Information page

1.2 IP Address Configuration

Use this page to configure the IP address, subnet mask, and gateway address of the switch.

NOTE

The management VLAN is VLAN 1 by default and cannot be changed.

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

Figure 1-2 IP Address Configuration page

1.3 User Management

Use this page to configure user accounts.

NOTE

The default user is **admin**. This account cannot be deleted, but its password can be changed.

SYSTEM->User Management

User Management			
User Name			
User Level	normal ▼		
Password			
Confirm Password			
Attention: User name and password are case sensitive.			

Refresh Apply Help

Item	User Name	User Level	Operation
1	admin	privilege	delete

Figure 1-3 User Management page

1.4 Serial Port Information

Use this page to view the console serial port settings.

SYSTEM->Serial Information

Serial Information	
Baud Rate	38400
Character Size	8
Parity Code	None
Stop Bits	1
Flow Control	None

Refresh Help

Figure 1-4 Serial Port Information page

1.5 SNTP Configuration

Use this page to configure and view the system clock through SNTP.

SYSTEM->SNTP Configuration

SNTP Configuration	
Server IP Address 1	
Server IP Address 2	
Server IP Address 3	
Time Interval	1800 (60-65535 seconds)
Time Zone	+8
Enable Status	Disable ▾
Last Update Time	
System Date Time	2022/06/01 12:18:41

Refresh Apply Help

Figure 1-5 SNTP Configuration page

1.6 SNMP Community Configuration

Use this page to configure the SNMP community names of the switch and their read and write permissions. Up to eight communities can be configured.

By default the switch has one community named **public** with read-only permission. To manage the switch over SNMP, configure a community with read and write permission.

NOTE

A community that has already been configured cannot be modified, and a new community cannot reuse an existing name. To change a community, click its **Delete** link and then create it again.

SYSTEM->SNMP Community

SNMP Community	
Community Name	
Read and Write Purview	read-write ▾

Refresh Apply Help

Item	Community Name	Read and Write Purview	Operation
1	public	read-only	---

Figure 1-6 SNMP Community Configuration page

1.7 SNMP Trap Configuration

Use this page to configure the IP address of the station that receives trap messages, along with the trap protocol parameters.

Enter the trap name and the IP address of the trap server, then select the SNMP version. Once the configuration is submitted successfully, the SNMP trap function becomes active: whenever a link up or link down event occurs, the switch automatically sends a trap packet to the target address.

NOTE

A trap target that has already been configured cannot be modified, and a new target cannot reuse an existing name. To change a target, click its **Delete** link and then create it again.

SYSTEM->SNMP TRAP

SNMP TRAP	
TRAP Name	
Server IP Address	
SNMP Version	V3

Item	TRAP Name	Server IP Address	SNMP Version	Operation
------	-----------	-------------------	--------------	-----------

Figure 1-7 SNMP Trap Configuration page

1.8 Log Information

Use this page to view the system log. Select a priority from the drop-down list to view the log entries at that level, and click **Refresh** to load the latest entries.

SYSTEM->Log

Log	
Priority	All

Figure 1-8 Log Information page

2. Port Configuration

2.1 Port Basic Configuration

Use this page to enable or disable ports, set port speed and flow control, and view the basic information for all ports.

To change a port's configuration, select the checkbox to the left of the port, or use **Select All**. The selected ports appear at the top of the page; a run of consecutive ports is shown as a range. When the setting is applied, every selected port receives the same parameters. The list at the bottom of the page shows the configuration of all ports.

PORT->Basic Configuration

Basic Configuration	
Selected Port(s)	
Enable/Disable	
Speed/Duplex	
Flow Control	
Jumbo Frame Bytes	1522 (1522-12288)

☐ Select All	Port	Link Status	Speed/Duplex	Enable/Disable	Flow Control	Jumbo Frame Bytes
☐	1	1G/FULL	AUTO/AUTO	Enable	Disable	1522
☐	2	---	AUTO/AUTO	Enable	Disable	1522
☐	3	---	AUTO/AUTO	Enable	Disable	1522
☐	4	---	AUTO/AUTO	Enable	Disable	1522
☐	5	---	AUTO/AUTO	Enable	Disable	1522
☐	6	---	AUTO/AUTO	Enable	Disable	1522
☐	7	---	AUTO/AUTO	Enable	Disable	1522
☐	8	---	AUTO/AUTO	Enable	Disable	1522
☐	9	---	AUTO/AUTO	Enable	Disable	1522
☐	10	---	AUTO/AUTO	Enable	Disable	1522

Figure 2-1 Port Basic Configuration page

2.2 Port Statistics

This page lists, for every port, the number of packets sent, bytes sent, packets received, bytes received, error packets, and dropped packets.

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

Figure 2-2 Port Statistics page

2.3 Port Storm Suppression

Use this page to configure suppression of broadcast, multicast, and DLF packets on a port.

Select the checkbox to the left of the port, or use **Select All**, to choose the ports on which to enable or disable broadcast suppression, multicast suppression, and DLF suppression. Use the suppression rate type and suppression rate fields to select the rate type and value. Broadcast, multicast, and DLF suppression rates can each be configured independently. The list on the page shows the configuration of all ports.

Parameter	Range
Suppression rate	1 to 1,024,000 kbit/s

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

Figure 2-3 Port Storm Suppression page

2.4 Port Speed Limit

Use this page to configure ingress and egress rate limits on a port.

Select the checkbox to the left of the port, or use **Select All**, to choose the ports. The ingress and egress rate limits are enabled independently by selecting their checkboxes; clearing a checkbox removes the rate limit. The list on the page shows the configuration of all ports.

Parameter	Range
Speed limit	1 to 1,024,000 kbit/s

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	---	---

Figure 2-4 Port Speed Limit page

2.5 Protection Port

Use this page to configure and display protection port information.

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

Figure 2-5 Protection Port page

2.6 Port Mirroring

Use this page to configure port mirroring. Port mirroring lets a mirror port monitor the packets sent by a mirrored output port and the packets received by a mirrored input port.

Only one mirror port can be selected, but multiple mirrored output ports and mirrored input ports can be selected. To configure mirroring:

1. Select the mirror port. To cancel an existing mirror configuration, select **Do not mirror**.
2. From the remaining ports, select the ports to be mirrored and the direction to monitor.

Direction selected	Traffic monitored
Ingress	Packets received by the mirrored port.
Egress	Packets sent by the mirrored port.
Both	All packets sent and received by the mirrored port.

PORT->Port Mirror

Listen Port

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.

Figure 2-6 Port Mirroring Configuration page

2.7 Link Aggregation

The link aggregation pages list all ports vertically and all aggregation groups horizontally. To add a port to an aggregation group, click the radio button at the intersection of the port's row and the group's column. The aggregation method is selected at the bottom of each group column. To remove a port from its aggregation group, click the leftmost radio button on the port's row.

2.7.1 Create Aggregation Group

Use this page to create an aggregation group.

PORT->Port Trunking->Trunk Group

Create Trunk Group	
Trunk Group	trunk1
Trunk Type	Static
Create Status	Uncreated
Trunk Method	src-dst-mac

Refresh Apply Delete Help

Figure 2-7-1 Create Aggregation Group page

2.7.2 Configure Aggregation Group

Use this page to configure an existing aggregation group.

PORT->Port Trunking->Trunk Configuration

Trunking Configuration	
Trunk Group created	
Member Port	1

Refresh Apply Delete Help

Member Port

Figure 2-7-2 Configure Aggregation Group page

2.7.3 Aggregation Information

Use this page to view the information for a link aggregation.

PORT->Port Trunking->Trunk Information

Trunk Information	

Refresh help

Figure 2-7-3 Aggregation Information page

2.8 DDM Information

Use this page to view the digital diagnostic monitoring information reported by the optical modules.

PORT->DDM Information

DDM Information	

Refresh Help

Figure 2-8 DDM Information page

3. PoE Configuration

3.1 PoE Port Configuration

Use this page to configure the total PoE power of the device, the PoE power of a single port, and whether PoE is on or off. The page also shows the current status of the PoE system.

Field	Description
PoE port	Selects the power supply port number (1–8).
PoE port status	Enable or disable PoE on the selected port.
Total power	The total PoE power budget for the device. Updated by the system.
Single-port power	The PoE power for an individual port. Updated by the system.

PoE->PoE Port Configuration

PoE Port Configuration

Selected Port(s)	
PoE Admin Status	Enable ▾
PoE Power Type	Auto ▾
PoE Protocol Type	AT ▾
Port Max Power (W)	0
PoE Voltage (V)	47.86
Total Power (W)	150
Power Consumption (W)	0.00
Power Usage (%)	0.00

Refresh

Apply

Restore Default

Port Restarting

Help

☐ Select All	Port	Admin Status	Operation	PSE Type	Class	Max Power (W)	Current (mA)	Voltage (V)	Power (W)
☐	1	Enable	OFF	Auto(BT)	N/A	N/A	N/A	N/A	N/A
☐	2	Enable	OFF	Auto(BT)	N/A	N/A	N/A	N/A	N/A
☐	3	Enable	OFF	Auto(AT)	N/A	N/A	N/A	N/A	N/A
☐	4	Enable	OFF	Auto(AT)	N/A	N/A	N/A	N/A	N/A
☐	5	Enable	OFF	Auto(AT)	N/A	N/A	N/A	N/A	N/A

Figure 3-1 PoE Port Configuration page

3.2 PoE Scheduling Configuration

Use this page to turn PoE power on or off according to a schedule. The control mode is hour plus day of week.

Field	Description
Control port	Selects the port (1–8) to be scheduled.
Control function	Enable or disable scheduling on the selected port.

PoE->PoE Policy Configuration

PoE Policy Configuration

PoE Port	1
Policy Status	Disable

Clock (☐ All)	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
00 ☐	☒	☒	☒	☒	☒	☒	☒
01 ☐	☒	☒	☒	☒	☒	☒	☒
02 ☐	☒	☒	☒	☒	☒	☒	☒
03 ☐	☒	☒	☒	☒	☒	☒	☒
04 ☐	☒	☒	☒	☒	☒	☒	☒
05 ☐	☒	☒	☒	☒	☒	☒	☒
06 ☐	☒	☒	☒	☒	☒	☒	☒
07 ☐	☒	☒	☒	☒	☒	☒	☒
08 ☐	☒	☒	☒	☒	☒	☒	☒
09 ☐	☒	☒	☒	☒	☒	☒	☒
10 ☐	☒	☒	☒	☒	☒	☒	☒
11 ☐	☒	☒	☒	☒	☒	☒	☒
12 ☐	☒	☒	☒	☒	☒	☒	☒

Figure 3-2 PoE Scheduling Configuration page

3.3 PD Query Configuration

Use this page to configure detection of the online status of powered devices (PDs).

Field	Description
PoE port	Selects the port connected to the PD to be queried.
PD IP address	The IP address of the PD.
PD query interval	The interval between queries to the PD. Default: 5 seconds.
Maximum queries without response	The number of unanswered queries allowed before the PD is treated as unresponsive. Default: 3.
Maximum PD startup time	The maximum time allowed for the PD to start up. Default: 120 seconds.

PoE->PD Query Configuration

PD Query Configuration

PoE Port	1
PD IP Address	
PD Query Interval	5 (2~30 Sec)
PD Timeout Number	3 (2~10)
PD Boot Time	120 (30~600 Sec)

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

Figure 3-3 PD Query Configuration page

4. VLAN Configuration

4.1 VLAN Configuration

Use this page to create VLANs and to display the information for all VLANs.

To create a VLAN, enter a VID in the active row. Valid VIDs are 2 to 4094.

NOTE

The switch creates VLAN 1 by default, and VLAN 1 cannot be deleted.

The VLAN list shows every VLAN that has been created and indicates the port membership of each one. A port may not be a member of a VLAN at all, or it may be a tagged or an untagged member. The character shown before a port number has the following meaning:

Character	Meaning
T (tagged)	The port is a tagged member of this VLAN.
U (untagged)	The port is an untagged member of this VLAN.

VLAN->VLAN Configuration

VLAN			
VLAN ID	(2-4094), format: 2-4 or 3,5,7		
Refresh Apply Delete All Help			
[U] untagged member of VLAN; [T] tagged member of VLAN S static VLAN; D dynamic VLAN; S/D static and dynamic VLAN			
VLAN ID	VLAN ID	Member	Operation
1	S	[U] : 1-28 [T] :	---

Page 1 / 1

Previous Next

Figure 4-1 VLAN Configuration page

4.2 Access Port Configuration

Use this page to display and configure ports in Access mode and the VLAN they belong to. The page is divided into a port list and a VLAN list.

Hover the mouse over a port to see its VLAN mode. Click a port to display and configure its VLAN:

- If the port is already in Access mode, its VLAN is shown when the port is selected. Selecting a different VLAN and applying the change moves the port to that VLAN.
- If the port is not in Access mode, applying the configuration changes the port to Access mode and sets the VLAN.

NOTE

Only one VLAN can be selected in Access mode.

VLAN->Access Port

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

Figure 4-2 Access Port Configuration page

4.3 Trunk Port Configuration

Use this page to display and configure ports in Trunk mode and the VLANs they belong to. The page is divided into a port list and a VLAN list; the port list works the same way as on the Access Port Configuration page (see section 4.2).

- If the port is already in Trunk mode, its VLANs are shown when the port is selected. Selecting different VLANs and applying the change updates the port's VLAN membership.
- If the port is not in Trunk mode, applying the configuration changes the port to Trunk mode and sets the VLANs.

Multiple VLANs can be selected in Trunk mode. To select a range of consecutive VLANs, click the first VLAN, hold **Shift**, and click the last VLAN.

VLAN->Trunk Port

Port	1 3 5 7 9 11 13 15 17 19 21 23 25 27 2 4 6 8 10 12 14 16 18 20 22 24 26 28
Default VLAN	☐ 1
tagged VLAN (☐ All)	☐ 1

Figure 4-3 Trunk Port Configuration page

4.4 Hybrid Port Configuration

Use this page to display and configure ports in Hybrid mode and the VLANs they belong to. The page is divided into a port list and a VLAN list; the port list works the same way as on the Access Port Configuration page (see section 4.2).

- If the port is already in Hybrid mode, its VLANs are shown when the port is selected. Selecting different VLANs and applying the change updates the port's VLAN membership.
- If the port is not in Hybrid mode, applying the configuration changes the port to Hybrid mode and sets the VLANs.

A default VLAN must be configured, and only one default VLAN can be selected. Any number of tagged VLANs and untagged VLANs can be selected.

NOTE

A given VLAN can be assigned only one of the three roles. For example, a VLAN configured as a tagged VLAN cannot also be designated as the default VLAN or as an untagged VLAN.

VLAN->Hybrid Port

Port	1 3 5 7 9 11 13 15 17 19 21 23 25 27 2 4 6 8 10 12 14 16 18 20 22 24 26 28
Default VLAN	☐ 1
Tagged VLAN (☐ All)	☐ 1
Untagged VLAN (☐ All)	☐ 1

Refresh Apply Help

Figure 4-4 Hybrid Port Configuration page

4.5 GVRP Configuration

4.5.1 GVRP Global Configuration

Use this page to enable GVRP globally.

VLAN->GVRP Configuration->Global Configuration

GVRP Global Configuration	
Global GVRP	Disable

Refresh Apply Help

Figure 4-5-1 GVRP Global Configuration page

4.5.2 GVRP Port Configuration

Use this page to enable GVRP on a port and to view port information.

VLAN->GVRP Configuration->Port Configuration

GVRP Port Configuration	
Selected Port(s)	
GVRP Status	Disable

Refresh Apply Help

☐ Select All	Port	GVRP Status	Join Timer(centiseconds)	Leave Timer(centiseconds)	LeaveAll Timer(centiseconds)
☐	1	Disable	---	---	---
☐	2	Disable	---	---	---
☐	3	Disable	---	---	---
☐	4	Disable	---	---	---
☐	5	Disable	---	---	---
☐	6	Disable	---	---	---
☐	7	Disable	---	---	---
☐	8	Disable	---	---	---
☐	9	Disable	---	---	---
☐	10	Disable	---	---	---
☐	11	Disable	---	---	---
☐	12	Disable	---	---	---

Figure 4-5-2 GVRP Port Configuration page

4.5.3 GVRP State Machine

Use this page to view the state machine information established by GVRP.

VLAN->GVRP Configuration->State Machine

Port Name	VLAN ID	Applicant State	Registrar State

Refresh Help

Figure 4-5-3 GVRP State Machine page

5. Layer 3 Configuration

5.1 IP Basic Configuration

5.1.1 VLAN Interface Configuration

Use this page to configure the IP address of a VLAN interface, delete an interface IP address, and view interface information.

NOTE

The switch has a VLAN 1 interface by default, which cannot be deleted. Only one interface can be configured per VLAN.

LAYER 3->IP Basic->VLAN Interface

VLAN Interface			
VLAN ID			
IP Address / Subnet Prefix		(format: 192.168.0.1/24)	
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			

VLAN ID	IP Address / Subnet Prefix	MAC Address	Operation
1	192.168.2.220/24	0082.441a.8b82	Delete

Figure 5-1-1 VLAN Interface Configuration page

5.1.2 ARP Interface Configuration

This page displays the switch's complete ARP table. From here you can add a static ARP entry, delete an ARP entry, and convert a dynamic ARP entry into a static entry.

To add a static ARP entry, enter the IP address and the MAC address, then click **Apply**. The MAC address must be a unicast MAC address. To delete an ARP entry, click the corresponding **Delete** link in the list.

LAYER 3->IP Basic->ARP Configuration

ARP Configuration				
IP Address				
MAC Address		(format: HHHH.HHHH.HHHH)		
Refresh Apply Help				

Item	IP Address	Mac Address	Type	Operation
1	192.168.2.74	04:7c:16:81:21:1c	Dynamic	Delete

Figure 5-1-2 ARP Interface Configuration page

5.1.3 Static Route Configuration

Use this page to add or delete static routes. By default, the switch has no static routes configured. A default route can be configured here by entering a destination address and subnet prefix of **0.0.0.0/0**.

LAYER 3->IP Basic->Static Routes

Static Routes Configuration		
Target Address/Subnet prefix		(format: 10.1.1.0/24)
Next Hop		
Attention: please use 0.0.0.0/0 to set default router.		
Refresh Apply Help		
Item	Target Address/Subnet prefix	Next Hop
State	Operation	

Figure 5-1-3 Static Route Configuration page

5.1.4 Routing Table Information

Use this page to view the switch's routing table.

LAYER 3->IP Basic->Routing Table

Route Display Conditions	
Route State	All (All includes Active and Inactive)
Route Type	All (All includes Connected, Static, RIP and OSPF etc.)
Display Help	
Routing Table Information	
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area > - selected route, * - FIB route, p - stale info C *> 127.0.0.0/8 is directly connected, lo C *> 192.168.2.0/24 is directly connected, vlan1	

Figure 5-1-4 Routing Table Information page

5.2 RIP Configuration

5.2.1 RIP Configuration

Use this page to enable or disable RIP and to declare the network segments RIP advertises.

LAYER 3->RIP Configuration->RIP Configuration

RIP Configuration	
RIP State	Disable
Network	(Format: A.B.C.D/M, as 2.0.0.0/24)
Refresh Apply Help	
Network	Operation

Figure 5-2-1 RIP Configuration page

5.2.2 RIP Interface Information

Use this page to view RIP interface information.

LAYER 3->RIP Configuration->RIP Interface

RIP Interface Information	
Refresh Help	

Figure 5-2-2 RIP Interface Information page

5.2.3 RIP Routing Information

Use this page to view the routing information learned and advertised by RIP.

LAYER 3->RIP Configuration->RIP Route

RIP Route Information	
Refresh	Help

Figure 5-2-3 RIP Routing Information page

5.3 OSPF Configuration

5.3.1 OSPF Configuration

Use this page to configure OSPF.

LAYER 3->OSPF Configuration->OSPF Configuration

OSPF Configuration	
OSPF ID	0 (0-65535)
OSPF State	Disable ▾
Network	(Format: A.B.C.D/M, as 2.0.0.0/24)
Area ID	(0-4294967295 or IP address)
Refresh	Apply Help

OSPF ID	Network	Area ID	Operation
---------	---------	---------	-----------

Figure 5-3-1 OSPF Configuration page

5.3.2 OSPF Interface Information

Use this page to view OSPF interface information.

LAYER 3->OSPF Configuration->OSPF Interface

OSPF Interface Information	
Refresh	Help

Figure 5-3-2 OSPF Interface Information page

5.3.3 OSPF Neighbor Information

Use this page to view OSPF neighbor information.

LAYER 3->OSPF Configuration->OSPF Neighbor

OSPF Neighbor Information	
Refresh	Help

Figure 5-3-3 OSPF Neighbor Information page

5.3.4 OSPF Link State Information

Use this page to view OSPF link state information.

LAYER 3->OSPF Configuration->OSPF LSA

OSPF LSA Information	
Refresh	Help

Figure 5-3-4 OSPF Link State Information page

5.3.5 OSPF Routing Information

Use this page to view OSPF routing information.

LAYER 3->OSPF Configuration->OSPF Route

OSPF Route Information	
Refresh Help	

Figure 5-3-5 OSPF Routing Information page

5.4 VRRP Configuration

5.4.1 VRRP Configuration

Use this page to configure VRRP.

LAYER 3->VRRP Configuration->VRRP Configuration

VRRP Configuration	
Virtual Router ID	1
Virtual Interface	none
Virtual IP Address	☐ Owner
Priority	100 (1-255)
Advertisement Interval	1 (1-10s)
Preempt Mode	Enable
Authentication	none
Simple Password	
Virtual Router State	Disable
Attention: Please configure carefully. If WEB connection is interrupted after the configuration, please wait a while then refresh or try establish a new connection with the new IP Address.	
Refresh Apply Delete Help	

Figure 5-4-1 VRRP Configuration page

5.4.2 VRRP Information

Use this page to view VRRP status information.

LAYER 3->VRRP Configuration->VRRP Information

VRRP Information	
Refresh Help	

Figure 5-4-2 VRRP Information page

6. Security Configuration

6.1 MAC Configuration

6.1.1 Manual MAC Address Binding

Use this page to bind a MAC address to a port. Enter the MAC address to be bound in the **MAC** field and the VLAN the MAC address belongs to in the **VLAN ID** field.

SECURITY->MAC->MAC Bind

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

Bind Information	
MAC Address	(Format: HHHH.HHHH.HHHH)
VLAN ID	(1-4094)

Refresh Apply Delete Help

List MAC bindings on the selected port

☐ Select All	MAC Address	VLAN ID
-------------------------------------	-------------	---------

Figure 6-1-1 Manual MAC Address Binding page

6.1.2 Automatic MAC Address Binding

Use this page to bind a MAC address to a port automatically. The page displays the dynamic MAC addresses currently present in the Layer 2 hardware forwarding table for the port, together with the VLAN the port belongs to. Select an entry to convert it into a static binding.

SECURITY->MAC->MAC Auto Bind

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

List MAC table learned from the selected port

☐ Select All	MAC Address	VLAN ID
☐	0028.2412.2de3	1
☐	00cf.e049.2f28	1
☐	00cf.e049.30a7	1

Figure 6-1-2 Automatic MAC Address Binding page

6.1.3 MAC Address Filtering

Use this page to configure MAC address filtering on a port. Enter the MAC address to filter in the **MAC** field and the VLAN the MAC address belongs to in the **VLAN** field.

SECURITY->MAC->MAC Filter

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

Filter Information	
MAC Address	(Format: HHHH.HHHH.HHHH)
VLAN ID	(1-4094)

Refresh Apply Delete Help

List MAC filtered on the selected port

☐ Select All	MAC Address	VLAN ID
-------------------------------------	-------------	---------

Figure 6-1-3 MAC Address Filtering Configuration page

6.1.4 MAC Address Table

Use this page to set the conditions under which the MAC addresses of a port are displayed.

SECURITY->MAC->MAC Table

MAC Display Conditions	
Port	All
VLAN ID	All

Display Help

MAC Table Information					
bridge	VLAN	port	mac	fwd	static
1	1	ge1/1	0028.2412.2de3	1	0
1	1	ge1/1	00cf.e049.2f28	1	0
1	1	ge1/1	00cf.e049.30a7	1	0
1	1	ge1/1	00cf.e04a.4442	1	0
1	1	ge1/1	00cf.e04c.3b81	1	0
1	1	ge1/1	00cf.e04f.3b16	1	0
1	1	ge1/1	00e0.4c0b.bc4b	1	0
1	1	ge1/1	00e0.4c3d.f2dc	1	0
1	1	ge1/1	00e0.7072.1e32	1	0
1	1	ge1/1	00e0.7096.724d	1	0
1	1	ge1/1	047c.1681.211c	1	0
1	1	ge1/1	047c.1684.0da5	1	0
1	1	ge1/1	08bf.b817.aa79	1	0
1	1	ge1/1	0c9d.920e.c8c1	1	0
1	1	ge1/1	185e.0f1e.6e6e	1	0
1	1	ge1/1	2811.a838.9ae1	1	0

Figure 6-1-4 MAC Address Table page

6.2 ACL Configuration

The following rules apply to every ACL page in this section.

- **Address masks are wildcards.** When configuring a rule, the source IP address is supplied together with a mask so that the rule matches a set of addresses. The mask is expressed as a complement (wildcard). For example, to match the range 192.168.0.0 to 192.168.0.255, enter an IP address of 192.168.0.1 with a mask of 0.0.0.255.
- **Every rule needs a filter mode.** Each rule must be set to either **Allow** or **Deny**.
- **Rule numbers are assigned automatically.** When a rule is created in a rule group, the system assigns it a rule number. When a rule is deleted, the remaining rules are unaffected and the system re-sorts the group automatically. To delete an entire rule group, click **Select All** and then **Delete**.

6.2.1 Standard IP Group ACL

Use this page to build the rule base for standard IP ACLs. Select an ACL group number and create one or more rules within it. The only field a standard IP rule can match is the source IP address, with a mask.

Parameter	Range
ACL group number	1–99 or 1300–1999

SECURITY->ACL->ACL Based Source IP

ACL Based Source IP			
ACL Group ID	1	Filter	deny
Source IP Address		Source Wildcard	

Attention: Wildcard should be the format such as 0.0.0.255.

Refresh Apply Delete Help

☐ Select All	ACL Group ID	Filter	Source IP Address	Source Wildcard
-------------------------------------	--------------	--------	-------------------	-----------------

Figure 6-2-1 Standard IP Group ACL page

6.2.2 Extended IP Group ACL

Use this page to build the rule base for extended IP ACLs. Select an ACL group number and create one or more rules within it.

An extended IP rule can match the following fields:

- Source IP address, with mask
- Destination IP address, with mask
- Protocol type, such as ICMP, TCP, or UDP
- Source port and destination port — valid for TCP and UDP only
- TCP control flags

Parameter	Range
ACL group number	100–199 or 2000–2699

SECURITY->ACL->ACL Based Extended IP

ACL Based Extended IP			
ACL Group IP	100	Filter	deny
Source IP		Source Wildcard	
Destination IP		Destination Wildcard	
Protocol Type		Source Port	
Destination Port		TCP Flag	☐ fin ☐ syn ☐ rst ☐ psh ☐ ack ☐ urg

Attention: Wildcard should be the format such as 0.0.0.255.

Refresh Apply Delete Help

☐ All	Group ID	Filter	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol Type	Source Port	Destination Port	TCP Flag
------------------------------	----------	--------	-----------	-----------------	----------------	----------------------	---------------	-------------	------------------	----------

Figure 6-2-2 Extended IP Group ACL page

6.2.3 MAC IP Group ACL

Use this page to build the rule base for MAC IP ACLs. Select an ACL group number and create one or more rules within it.

A MAC IP rule can match the following fields:

- Source MAC address, with address match bits
- Source IP address, with address match bits
- Destination IP address, with address match bits

Parameter	Range
ACL group number	700–799

SECURITY->ACL->ACL Based MAC IP

ACL Based MAC IP										
ACL Group ID	700	Filter	deny							
Source MAC		Source MAC Wildcard								
Destination MAC		Destination MAC Wildcard								
Source IP		Source IP Wildcard								
Destination IP		Destination IP Wildcard								
Attention: IP Wildcard should be the format such as 0.0.0.255. MAC Wildcard format should be HHHH.HHHH.HHHH										
Refresh Apply Delete Help										
☐ All	Group ID	Filter	Source MAC	Source MAC Wildcard	Destination MAC	Destination MAC Wildcard	Source IP	Source IP Wildcard	Destination IP	Destination IP Wildcard

Figure 6-2-3 MAC IP Group ACL page

6.2.4 MAC ARP Group ACL

Use this page to build the rule base for MAC ARP ACLs. Select an ACL group number and create one or more rules within it.

A MAC ARP rule can match the following fields:

- ARP operation type
- Sending MAC address, with address match bits
- Sending IP address, with address match bits

Parameter	Range
ACL group number	1100–1199

SECURITY->ACL->ACL Based MAC ARP

ACL Based MAC ARP							
ACL Group ID	1100	Filter	deny				
Sender MAC		Sender MAC Wildcard					
Sender IP		Sender IP Wildcard					
Attention: IP Wildcard should be 0.0.0.255 and such, and MAC Wildcard format should be HHHH.HHHH.HHHH							
Refresh Apply Delete Help							
☐ All	Group ID	Filter	Sender MAC	Sender MAC Wildcard	Sender IP	Sender IP Wildcard	

Figure 6-2-4 MAC ARP Group ACL page

6.2.5 Apply ACLs to a Port

Use this page to apply an ACL group to a port. The rules in the selected group are written into the port's hardware logic, and the port then filters received packets according to those rules.

Standard IP, extended IP, MAC IP, and MAC ARP ACL groups can all be applied to a port. The group being applied must already exist.

- To apply a group, select it from the **ACL Rule Group** list and click **Add**.
- To remove a group, select it from the list of referenced rule groups and click **Delete**.

SECURITY->ACL->ACL Group

Port	ACL Group configured	Operation	ACL Group applied
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24		Apply => <= Delete Refresh Help	

Figure 6-2-5 Port Application ACL page

6.2.6 ACL Configuration Information

Use this page to view all rules currently configured in the ACLs and where they are referenced.

SECURITY->ACL->ACL Resource

ACL Resource

Refresh

Help

Figure 6-2-6 ACL Configuration Information page

6.3 AAA Configuration

6.3.1 AAA Global Configuration

Use this page to configure the global AAA settings.

Field	Description
802.1X protocol	Enables or disables 802.1X. The 802.1X protocol must be enabled for authentication and accounting to work.
Re-authentication	Enables or disables periodic re-authentication. Disabled by default. Enabling it makes authentication and accounting more reliable, at the cost of a small increase in network traffic.
Re-authentication interval	The interval between re-authentications. Valid only when re-authentication is enabled. Default: 3600 seconds. Set the value to suit the deployment, but do not set it too low.
RADIUS server IP address	The IP address of the RADIUS server. This field must be set for authentication and accounting.
Backup RADIUS server IP address	The IP address of a backup RADIUS server, if one is available.
Shared key	The encrypted shared password between the switch and the RADIUS server. This field must be set for authentication and accounting, and must match the setting on the RADIUS server.
Accounting	Enables or disables accounting. Enabled by default. Accounting is normally enabled when authentication and accounting are in use.

SECURITY->AAA->AAA Global Configuration

AAA Global Configuration	
802.1x	disable
Reauthentication	disable
Reauthentication Period	3600 (seconds)
RADIUS Server IP	0.0.0.0
Alternative RADIUS Server IP	0.0.0.0
Share Key	
Accounting Status	enable

Refresh Apply Help

Figure 6-3-1 AAA Global Configuration page

6.3.2 AAA Port Configuration

Use this page to configure the authentication mode of a port and the maximum number of hosts it supports, and to view the configuration of each port.

To change a port's AAA configuration, select the checkbox to the left of the port, or use **Select All**. The selected ports appear at the top of the page; a run of consecutive ports is shown as a range. When the setting is applied, every selected port receives the same parameters.

There are four AAA port modes:

Mode	Behavior
N/A	The port is not authenticated and can access the network. Use this mode for ports that should not require 802.1X.
Auto	802.1X authentication is required. Use this mode for ports that must authenticate.
Force-authorized	The port is always treated as authorized. Rarely used in practice.
Force-unauthorized	The port is always treated as unauthorized. Rarely used in practice.

During 802.1X authentication, the maximum number of hosts allowed on a port is 256 by default. This field can be modified, up to a maximum of 256 hosts.

SECURITY->AAA->AAA Port Configuration

AAA Port Configuration			
Selected Port(s)			
Port Mode	Force-UnAuthorized		
Support Host Num	256	(1-256)	
Refresh Apply Help			
☐ Select All	Port	Port Mode	Support Host Num
☐	1	N/A	256
☐	2	N/A	256
☐	3	N/A	256
☐	4	N/A	256
☐	5	N/A	256
☐	6	N/A	256
☐	7	N/A	256
☐	8	N/A	256
☐	9	N/A	256

Figure 6-3-2 AAA Port Configuration page

6.3.3 AAA User Information

Use this page to view the status of all users connected to a port.

SECURITY->AAA->AAA User Information

AAA User Information					
User name	MAC Address	Authentication state	Authenticator state	Back-End state	Reauthentication state
Refresh Help					

Figure 6-3-3 AAA User Information page

6.4 Management Security Configuration

6.4.1 Management Permission Configuration

Use this page to control the Telnet, web, and SNMP management services. Each service can be enabled or disabled, and each can be attached to a standard IP ACL group so that access is restricted by source IP address.

By default, the Telnet, web, and SNMP services are all enabled with no ACL filtering, which means any host can reach all three services. To tighten this:

- To stop offering a service altogether, disable it on this page.
- To restrict a service to specific hosts, leave the service enabled and select a standard IP ACL group (1–99) for it. The ACL group must already exist.

CAUTION

If you restrict or disable the web service on this page — for example by turning the web service off — you may lose access to the web interface. If that happens, log in to the switch by another method, such as the console port or Telnet, and re-enable the web service.

SECURITY->Safe Management->Safe Management

Safe Management			
Service Type			
Management State	Enable		
ACL Group	0 (0-99, 0 means no ACL group is associated.)		
Refresh Apply Help			

Service Type	Management State	ACL Group	Number
HTTP	Enable	0	---
HTTPS	Enable	0	---
SNMP	Enable	0	---
TELNET	Enable	0	5
SSH	Enable	0	5

Figure 6-4-1 Management Permission Configuration page

7. DHCP Configuration

7.1 DHCP Client

Use this page to configure the switch as a DHCP client.

DHCP->DHCP Client

DHCP Client Configuration	
Interface	vlan1
Enable/Disable	Disable
Refresh Apply Renew Release Help	

DHCP Client Information	

Figure 7-1 DHCP Client page

7.2 DHCP Relay

Use this page to configure DHCP relay.

DHCP->DHCP Relay

DHCP Relay Configuration	
Interface	vlan1
Enable/Disable	Disable
Master DHCP Server IP	
Backup DHCP Server IP	
Refresh Apply Help	

DHCP Relay Information	

Figure 7-2 DHCP Relay page

7.3 DHCP Server

7.3.1 Global and Interface Configuration

Use this page to configure the global and interface settings of the DHCP server.

DHCP->DHCP Server->Global & Interface

DHCP Server Global Configuration	
Global DHCP Server	Disable ▼

DHCP Server Interface Configuration	
Interface	vlan1 ▼
DHCP Listen	Disable ▼

DHCP Server Information	
DHCP server: Disable	
DHCP server listen interface:	

Figure 7-3-1 DHCP Server Global and Interface Configuration page

7.3.2 Address Pool Configuration

Use this page to configure the DHCP server's address pools.

DHCP->DHCP Server->Address Pool

Create Address Pool	
Address Pool Name	Create

Address Pool Configuration	
Address Pool Name	▼
Address Range	Start: End:
Subnet Mask	
Default Router	
DNS Server	Master: Backup:
Lease Time	0 days 0 Hours 0 Minutes
Exclude Address	Start: Add Exclude End: Del Exclude
Option 82 Circuit ID	

Address Pool Information	
--------------------------	--

Figure 7-3-2 DHCP Server Address Pool Configuration page

7.3.3 Address Information

Use this page to view the addresses the DHCP server has assigned.

DHCP->DHCP Server->Address Information

DHCP Server Address Information				
IP	MAC	State	Pool Name	Lease

Figure 7-3-3 DHCP Server Address Information page

7.4 DHCP Snooping

7.4.1 Global Configuration

Use this page to configure the global DHCP Snooping settings.

DHCP->DHCP Snooping->Global Configuration

DHCP Snooping Global Configuration	
Global DHCP Snooping	Disable ▾
DHCP Server Port 1	▾
DHCP Server Port 2	▾
DHCP Server Port 3	▾
DHCP Server Port 4	▾

Refresh Apply Help

Figure 7-4-1 DHCP Snooping Global Configuration page

7.4.2 Interface Configuration

Use this page to configure DHCP Snooping on an interface.

DHCP->DHCP Snooping->Interface Configuration

DHCP Snooping Interface Configuration				
Selected Port(s)				
DHCP Snooping	Disable ▾			
Option 82	Disable ▾			
Option 82 Circuit ID				

Refresh Apply Help

☐ Select All	Port	DHCP Snooping	Option 82	Option 82 Circuit ID
☐	1	Disable	Disable	
☐	2	Disable	Disable	
☐	3	Disable	Disable	
☐	4	Disable	Disable	
☐	5	Disable	Disable	
☐	6	Disable	Disable	
☐	7	Disable	Disable	
☐	8	Disable	Disable	
☐	9	Disable	Disable	

Figure 7-4-2 DHCP Snooping Interface Configuration page

7.4.3 Binding Table Information

Use this page to view the DHCP Snooping binding table.

DHCP->DHCP Snooping->Binding Table

DHCP Snooping Binding Table Information
DHCP Snooping is globally disabled

Refresh Help

Figure 7-4-3 DHCP Snooping Binding Table page

8. Multicast Configuration

8.1 IGMP Snooping Configuration

8.1.1 IGMP Snooping Configuration

Use this page to enable IGMP Snooping.

MULTICAST->IGMP SNOOPING->Configuration

IGMP SNOOPING Global Configuration		
Global IGMP SNOOPING	Disable	
Unregistered Multicast Packets	Forward	
Send Query Source IP	192.168.0.1	
Send Query Version	V3	

IGMP SNOOPING VLAN Configuration		
VLAN ID	VLAN 1	
VLAN IGMP SNOOPING	Disable	
Fast Leave	Disable	
Fast Leave Timeout	300000	(>=0ms)
Query Membership Timeout	300000	(60000-300000ms)
Group Membership Timeout	400000	(>=0ms)
Querier	Disable	
Query Interval	60000	(60000-125000ms)
Static Mrouter Ports		(e.g : ge1/1,ge1/2)

Figure 8-1-1 IGMP Snooping Configuration page

8.1.2 Multicast Group Information

Use this page to view the multicast group information learned by IGMP Snooping.

MULTICAST->IGMP SNOOPING->Group Information

VLAN ID	Address	Port
---------	---------	------

Figure 8-1-2 Multicast Group Information page

8.2 GMRP Configuration

8.2.1 GMRP Global Configuration

Use this page to configure GMRP globally.

MULTICAST->GMRP Configuration->Global Configuration

GMRP Global Configuration	
Global GMRP	Disable

Figure 8-2-1 GMRP Global Configuration page

8.2.2 GMRP Port Configuration

Use this page to configure the GMRP status of a port.

MULTICAST->GMRP Configuration->Port Configuration

GMRP Port Configuration					
Selected Port(s)					
GMRP Status		Disable ▾			
Refresh Apply Help					
☐ Select All	Port	GMRP Status	Join Timer(centiseconds)	Leave Timer(centiseconds)	LeaveAll Timer(centiseconds)
☐	1	Disable	---	---	---
☐	2	Disable	---	---	---
☐	3	Disable	---	---	---
☐	4	Disable	---	---	---
☐	5	Disable	---	---	---
☐	6	Disable	---	---	---
☐	7	Disable	---	---	---
☐	8	Disable	---	---	---
☐	9	Disable	---	---	---
☐	10	Disable	---	---	---
☐	11	Disable	---	---	---
☐	12	Disable	---	---	---

Figure 8-2-2 GMRP Port Configuration page

8.2.3 GMRP State Machine

Use this page to view the status of the GMRP state machine.

MULTICAST->GMRP Configuration->State Machine

Port Name	VLAN ID	Multicast MAC Address	Applicant State	Registrar State
Refresh Help				

Figure 8-2-3 GMRP State Machine page

8.3 Multicast Routing Configuration

8.3.1 Multicast Routing Configuration

Use this page to enable or disable multicast routing.

MULTICAST->Multicast Routing->Multicast Routing

Multicast Routing Configuration	
Multicast Routing	Disable ▾
Refresh Apply Help	

Figure 8-3-1 Multicast Routing Configuration page

8.3.2 Multicast Routing Table

Use this page to view the multicast routing table.

MULTICAST->Multicast Routing->Multicast Routing Table

Multicast Routing Table
IP Multicast Routing Table Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed Timers: Uptime/Stat Expiry Interface State: Interface (TTL)
Refresh Help

Figure 8-3-2 Multicast Routing Table page

8.4 IGMP Configuration

8.4.1 IGMP Configuration

Use this page to configure the IGMP parameters of the switch.

MULTICAST->IGMP Configuration->IGMP Configuration

IGMP Configuration		
Interface	vlan1 ▼	
IGMP Enable	Disable ▼	
IGMP Status		
Query Interval	125	(1-18000s)
Query Max Response Time	10	(1-240s)
Robustness Variable	2	(2-7)
Last Member Query Interval	1	(1-25s)
Last Member Query Count	2	(2-7)
Igmp Version	V3 ▼	

Refresh Apply Help

Figure 8-4-1 IGMP Configuration page

8.4.2 IGMP Interface Information

Use this page to view IGMP interface information.

MULTICAST->IGMP Configuration->IGMP Interface

IGMP Interface Information
% IP multicast-routing not enable

Refresh Help

Figure 8-4-2 IGMP Interface Information page

8.4.3 IGMP Group Information

Use this page to view IGMP group information.

MULTICAST->IGMP Configuration->IGMP Group

IGMP Group Information
% IP multicast-routing not enable

Refresh Help

Figure 8-4-3 IGMP Group Information page

8.5 PIM-SM Configuration

8.5.1 Global Configuration

Use this page to configure the global PIM-SM parameters.

MULTICAST->PIM-SM Configuration->Global Configuration

PIM-SM Global Configuration		
RP Address		
Candidate RP	none ▼	
Candidate BSR	none ▼	
IP Interval	60	(1-65535s)
SPT Switch	Disable ▼	

Refresh Apply Help

Figure 8-5-1 PIM-SM Global Configuration page

8.5.2 Interface Configuration

Use this page to configure the PIM-SM interface parameters.

MULTICAST->PIM-SM Configuration->Interface Configuration

PIM-SM Interface Configuration		
Interface	vlan1	
PIM-SM Enable	Disable	
Hello Interval	30	(1-65535s)
Hello Holdtime	105	(1-65535s)
DR Priority	1	(0-2147483647)

Refresh Apply Help

Figure 8-5-2 PIM-SM Interface Configuration page

8.5.3 Multicast Routing Information

Use this page to view the multicast routing information produced by PIM-SM.

MULTICAST->PIM-SM Configuration->Mroute Information

PIM-SM Mroute Information	
Refresh Help	

Figure 8-5-3 PIM-SM Multicast Routing Information page

8.5.4 Interface Information

Use this page to view the PIM-SM interface information.

MULTICAST->PIM-SM Configuration->Interface Information

PIM-SM Interface Information	
Refresh Help	

Figure 8-5-4 PIM-SM Interface Information page

8.5.5 Neighbor Information

Use this page to view the PIM-SM neighbor information.

MULTICAST->PIM-SM Configuration->Neighbor Information

PIM-SM Neighbor Information	
Refresh Help	

Figure 8-5-5 PIM-SM Neighbor Information page

8.5.6 RP Information

Use this page to view the PIM-SM rendezvous point (RP) information.

MULTICAST->PIM-SM Configuration->RP Information

PIM-SM RP Information	
PIM Group-to-RP Mappings	
Refresh Help	

Figure 8-5-6 PIM-SM RP Information page

8.5.7 BSR Information

Use this page to view the PIM-SM bootstrap router (BSR) information.

MULTICAST->PIM-SM Configuration->BSR Information

PIM-SM BSR Information	
Refresh	Help

Figure 8-5-7 PIM-SM BSR Information page

9. Ring Network Configuration

9.1 Spanning Tree Configuration

9.1.1 Spanning Tree Global Configuration

Use this page to configure the global spanning tree parameters.

RING->MSTP->Global Configuration

Global Configuration		
MSTP	disable ▾	
Priority	32768	(0-61440, must be an interger multiple of 4096)
Forward-Time	15	(4-30, meet 2*(Forward-Time - 1) >= Max-Age)
Hello-Time	2	(1-10, meet 2*(Hello-Time + 1) <= Max-Age)
Max-Age	20	(6-40)
Max-Hops	20	(1-40)

Refresh Apply Help

Figure 9-1-1 Spanning Tree Global Configuration page

9.1.2 Spanning Tree Port Configuration

Use this page to view the MSTP status of each port.

RING->MSTP->Port Configuration

Port Configuration							
Selected Port(s)							
Port Priority							
Path-Cost							
Force-Version	STP ▾						
Portfast	disable ▾						

Refresh Apply Help

☐ All	Item	Port	Priority	Path-Cost	Force-Version	Portfast	STP State
☐	1	1	128	20000	MSTP	disable	Forwarding
☐	2	2	128	20000000	MSTP	disable	Discarding
☐	3	3	128	20000000	MSTP	disable	Discarding
☐	4	4	128	20000000	MSTP	disable	Discarding
☐	5	5	128	20000000	MSTP	disable	Discarding
☐	6	6	128	20000000	MSTP	disable	Discarding
☐	7	7	128	20000000	MSTP	disable	Discarding
☐	8	8	128	20000000	MSTP	disable	Discarding
☐	9	9	128	20000000	MSTP	disable	Discarding

Figure 9-1-2 Spanning Tree Port Configuration page

9.2 ERPS Configuration

9.2.1 ERPS Predefined Configuration

Use this page to apply the ERPS predefined configuration. When you enable it, specify the node type: **Primary** or **Transport**.

The predefined configuration applies the following values:

Parameter	Value
ERPS instance number	1
ERPS change number	1
Ring mode	Main ring mode
Protocol VLAN	VLAN 3001
Data VLAN	VLAN 1
RPL port	51
RL port	52
Recovery behavior	Recoverable
Hold-off time	0
Guard time	500 ms
WTR time	5 minutes
WTB time	5 seconds
Protocol message interval	5 seconds

RING->ERPS->ERPS Predefined Configuration

Erps Predefined Configuration	
Status	disable ▼
Node Type	rpl-owner-node ▼

Refresh Apply Help

Figure 9-2-1 ERPS Predefined Configuration page

9.2.2 ERPS Instance Configuration

Use this page to configure ERPS instances. Up to 8 instances can be configured.

- If the instance has not been created, click **Apply** to create it and assign a role.
- If the instance has been created but is not yet associated with a ring, its role can be modified.
- If the instance has been created and is associated with a ring, it cannot be modified.
- Click **Delete** to delete the selected instance.

RING->ERPS->ERPS Domain

ERPS Domain Configuration	
ERPS Domain	1 ▼
Domain Status	Not Created
Node Role	none-interconnection ▼

Refresh Apply Delete Help

Figure 9-2-2 ERPS Instance Configuration page

9.2.3 ERPS Ring Configuration

Use this page to create and configure ERPS rings. Up to 32 rings can be configured.

- Select a ring, then click **Apply** to create the ring and set its configuration.
- If the ring already exists, its configuration can be modified.
- Click **Delete** to delete the selected ring.
- When a ring fault is detected, click **Manual Recovery** to recover the ring.

NOTE

A ring must be associated with exactly one instance.

RING->ERPS->ERPS Ring

ERPS Ring Configuration	
ERPS Ring	1
Ring Status	Not Created
Domain	
Ring Mode	
Node Mode	
Raps VLAN	0
Traffic VLAN	format 2,4,6
RPL Port	
RL Port	
Revertive Behaviour	revertive
Hold-off Time	0 (<0-10000>, step 100, ms)
Guard Time	500 (<10-2000>, step 10, ms)
WTR Time	5 (<1-12>, min)
WTB Time	5 (<1-10>, sec)
Raps-send Time	5 (<1-10>, sec)
ERPS Ring Enable	disable
Forced Switch RPL Port	
Forced Switch RL Port	
Manual Switch Port	

Refresh Apply Delete Recover Help

Figure 9-2-3 ERPS Ring Configuration page

9.2.4 ERPS Information

Use this page to view the configuration and status of an ERPS ring. Select the ring number to display its information.

RING->ERPS->ERPS Information

ERPS Ring Select	
ERPS Ring	1

ERPS Ring Information	

Refresh Help

Figure 9-2-4 ERPS Information page

9.3 EAPS Configuration

9.3.1 EAPS Ring Configuration

Use this page to create, configure, display, and delete EAPS rings.

Field	Description
EAPS ring number	The ring number, selected from the drop-down list. Range: 1–16.
Creation status	Not Created or Created . A ring must be created before it can be configured.
Mode	Master or Transit , depending on the role of this switch in the ring.
Main port	The EAPS primary port, for example fe1/1 or ge1/1.
Alternate port	The EAPS secondary port.
Control VLAN	The control VLAN of the EAPS ring. Range: 2–4094.
Protected VLAN	The VLAN or VLANs protected by the EAPS ring.
Hello interval	The interval between Hello messages. Default: 1 second.
Fail time	The time taken to detect a fault. Default: 3 seconds.
Cross-ring forwarding	Enable this when data must be forwarded across rings, such as in multi-ring topologies. Disabled by default.
Extreme interoperability	Compatibility with other vendors' network devices. Enabled by default.
Enable status	The enable state of the EAPS ring.

RING->EAPS->EAPS Ring

EAPS Ring Configuration	
EAPS Ring ID	1
Create Status	Not Created
Mode	None
Primary Port	
Secondary Port	
Control VLAN	0
Protected VLANs	Format: 2,4,6
Hello Time Interval	1 s
Fail Time	3 s
Data Span	Disable
Extreme Interoperability	Enable
Enable Status	Disable

Refresh Apply Delete Help

Figure 9-3-1 EAPS Ring Configuration page

9.3.2 EAPS Information

Use this page to view the EAPS configuration information.

RING->EAPS->EAPS Information

EAPS Ring Information	

Refresh Help

Figure 9-3-2 EAPS Information page

10. Advanced Configuration

10.1 QoS Configuration

10.1.1 QoS Application Configuration

Use this page to configure the QoS type of a port and to modify its default user priority. The list shows the QoS type and default user priority of each port in real time.

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

Figure 10-1-1 QoS Application Configuration page

10.1.2 QoS Scheduling Configuration

Use this page to configure the QoS scheduling mode of a port and to modify the priority of each queue. The list shows the scheduling mode of each port and the weight of each queue in real time.

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

Figure 10-1-2 QoS Scheduling Configuration page

10.2 LLDP Configuration

10.2.1 LLDP Global Configuration

Use this page to display and configure the global LLDP parameters.

ADVANCED->LLDP Configuration->Global Configuration

LLDP Global Configuration		
LLDP Global	Disable	
Hold-multiplier	4	(2-10)
Reinit-delay	2	(1-10s)
Tx-delay	2	(1-10s)
Tx-interval	30	(5-300s)

Refresh Apply Help

Figure 10-2-1 LLDP Global Configuration page

10.2.2 LLDP Port Configuration

Use this page to display and configure the LLDP parameters of a port.

ADVANCED->LLDP Configuration->Port Configuration

LLDP Port Configuration								
Selected Port(s)								
LLDP Status	Enable							
Admin Status	TxRx							
Manage IP								
Check Change Interval	0 (0-30s)							
DOT1-TLV	Enable							
DOT3-TLV	Enable							
MED-TLV	Enable							

Refresh Apply Help

☐ Select All	Port	LLDP Status	Admin Status	Manage IP	Check Change Interval	DOT1-TLV	DOT3-TLV	MED-TLV
☐	1	Enable	TxRx	0.0.0.0	0	Enable	Enable	Enable
☐	2	Enable	TxRx	0.0.0.0	0	Enable	Enable	Enable
☐	3	Enable	TxRx	0.0.0.0	0	Enable	Enable	Enable
☐	4	Enable	TxRx	0.0.0.0	0	Enable	Enable	Enable
☐	5	Enable	TxRx	0.0.0.0	0	Enable	Enable	Enable
☐	6	Enable	TxRx	0.0.0.0	0	Enable	Enable	Enable
☐	7	Enable	TxRx	0.0.0.0	0	Enable	Enable	Enable
☐	8	Enable	TxRx	0.0.0.0	0	Enable	Enable	Enable

Figure 10-2-2 LLDP Port Configuration page

10.2.3 LLDP Neighbor Table

Use this page to view the LLDP neighbor table.

ADVANCED->LLDP Configuration->Neighbor Table

Index	Local Port	Device ID	Chassis ID	Port ID	Manage IP	VLAN	TTL (s)	Capability
Refresh Help								

Figure 10-2-3 LLDP Neighbor Table page

11. System Tools

11.1 Save Configuration

Use this page to view the switch's current running configuration and save it to the configuration file.

Click **Save** to write the current configuration to the configuration file. Saving erases and rewrites the flash chip, so it takes a few moments to complete.

CAUTION

Changes made on the configuration pages are held in memory only. If you have made changes and want them to survive a restart, click **Save** on this page before leaving it. Otherwise the changes are lost when the switch restarts.

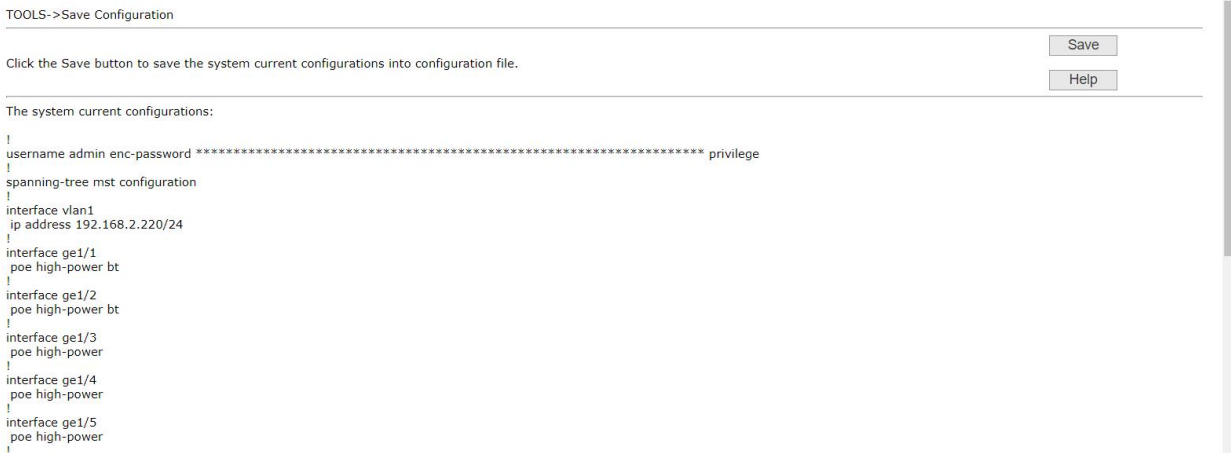


Figure 11-1 Save Configuration page

11.2 Back Up Configuration File

Use this page to view and download the switch's startup configuration. The startup configuration is the configuration file stored in flash; when no configuration file is present in flash, the switch starts with the factory default configuration.

Click **Backup** to open a dialog where you can choose the directory to save the configuration file to. The downloaded file is named **switch.cfg** by default.



Figure 11-2 Back Up Configuration File page

11.3 Restore Configuration File

Use this page to upload a configuration file to the switch.

3. Click **Browse** and select the configuration file on the PC. The file name must end in **.cfg**.
4. Click **Upload** to transfer the file to the switch.

CAUTION

Do not open another page or restart the switch before the transfer result page appears. Doing so causes the file transfer to fail and the system to crash.

TOOLS->Restore Configuration

Click the View button to Select a configuration file, the postfix of file must be *.cfg. And then click the Restore button to restore the configuration file.

Restore

选择文件 未选择任何文件

Help

Attention:

1. If the file restore happens, do not restart switch, cut off power or do anything else with the Web page.
2. If operation fail, to re-restore configuration file before restart the switch.
3. To put the new configuration into effect, restart the switch.

Figure 11-3 Restore Configuration File page

11.4 Software Upgrade

Use this page to upload a firmware image to the switch.

5. Click **Browse** and select the image file on the PC. The image must be supplied by the manufacturer and the file name must end in **.img**.
6. Click **Upload** to transfer the image to the switch.

CAUTION

Do not open another page or restart the switch before the transfer result page appears. Doing so causes the file transfer to fail and the system to crash.

TOOLS->Upgrade

Click the View button to Select a upgrade file, the postfix of file must be *.tar.gz. And then click the Upgrade button to upgrade.

Upgrade

选择文件 未选择任何文件

Help

Attention:

1. During upgrading, do not reboot the switch, cut off power or do anything else with the Web page to avoid system crashes.
2. If operation fail, to re-upgrade before reboot the switch.
3. Upgrade take effect after you reboot the switch.

Figure 11-4 Software Upgrade page

11.5 Restore Factory Configuration

Use this page to delete the configuration file in flash and return the switch to its factory configuration.

Click **Restore Factory Configuration**. A dialog appears asking you to confirm. Once the factory configuration is restored, the switch restarts automatically so that the factory configuration takes effect.

CAUTION

After the factory configuration is restored, log in again using the factory default IP address and password.

TOOLS->Factory Reboot

Click the Factory Reboot button to remove startup configuration file and then reboot the switch.

Factory Reboot ...

Help

Attention:

1. If operation is done and the switch is rebooting, you should use the default IP address, default username and password to log in.
2. Connection between PC and switch will break off while switch is rebooting.

Figure 11-5 Restore Factory Configuration page

11.6 Restart

Use this page to restart the switch. Click **Restart**; a dialog appears asking you to confirm. Click **OK** to restart the switch, or **Cancel** to abandon the restart.

NOTE

Web pages are unavailable while the switch is restarting.

TOOLS->System Reboot

Click the Reboot button to reboot the switch. If you want the system to maintain current configuration, please save before rebooting.

Reboot ...

Help

Attention: Connection between PC and switch will break off while switch is rebooting.

Figure 11-6 Restart page