24-PORT WEB-MANAGED GIGABIT ETHERNET SWITCH WITH 2 SFP PORTS

USER MANUAL

MODEL 560917

INT-560917-UM-0421-02

Table of Contents

Chapter 1 Product Introduction

Congratulations on your purchase of the Web-Managed Gigabit Ethernet Switch. Before you install and use this product, read this manual carefully for a full understanding of its functions.

1.1 Product Overview

The Web-Managed Gigabit Ethernet Switch provides a seamless network connection. It integrates 1000Mbps Gigabit Ethernet, 100Mbps Fast Ethernet and 10Mbps Ethernet network capabilities in a highly flexible package. With 24 10/100/1000Mbps Auto-Negotiation RJ45 ports, all ports support Auto MDI/MDIX function. The switch is a low-cost, easy-to-use, high-performance upgrade from your old network to a 1000Mbps Gigabit network, essential in helping solve network bottlenecks that frequently develop as more advanced computer users and newer applications continue to demand greater network resources.

For efficient management, the switch is equipped with a remote Web interface. The switch can be programmed for advanced switch management functions, such as Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, Security, Access Control, MAC Address Table, LLDP, Diagnostics, RMON and Maintenance.

1.2 Features

- Comply with IEEE802.3, IEEE802.3u, IEEE802.3ab, IEEE802.3x, IEEE802.3z, IEEE802.3ad standards
- Supports IEEE802.3x flow control for full duplex mode and backpressure for half duplex mode
- Supports MAC address auto-learning and auto-aging
- Store and forward mode
- Supports SNMP/RMON/TELENT
- Supports IEEE802.1Q VLAN, 4K VLAN table
- Supports IEEE802.1p Priority Queues
- Supports ACL Function, 1.5K-entry ALC table
- Supports Storm Control
- Supports QoS, Port Mirroring, Link Aggregation Protocol
- LED indicators for monitoring power, link/activity
- Web-based management support
- Internal power adapter supply

1.3 External Component Description

1.3.1 Front Panel

The front panel of the switch features 24 10/100/1000Mbps RJ45 ports, two SFP ports, one Console port, a Reset button and a series of LED indicators as shown below.

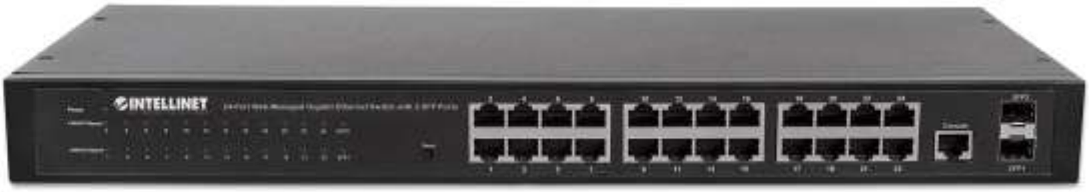


Figure 1 - Front Panel

10/100/1000Mbps RJ45 ports (1-24):
Designed to connect to the device with a bandwidth of 10Mbps, 100Mbps or 1000Mbps. Each has a corresponding 10/100/1000Mbps LED.

SFP ports (SFP1, SFP2):
Designed to install the SFP module and connect to the device with a bandwidth of 1000Mbps. Each has a corresponding 1000Mbps LED.

Console port (Console):
Designed to connect with the serial port of a computer or terminal for monitoring and configuring the switch.

Reset button (Reset):
Keep the device powered on and press the button for about 5 seconds. The system restores the factory default settings.

LED indicators:
The LED indicators will allow you to monitor, diagnose and troubleshoot any potential problem with the switch, connection or attached devices.

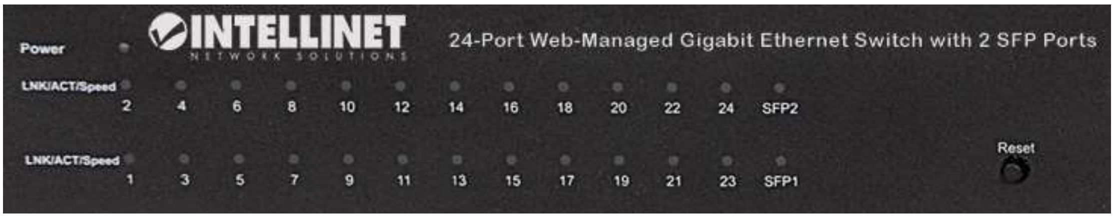

Power
INTELLINET
NETWORK SOLUTIONS
24-Port Web-Managed Gigabit Ethernet Switch with 2 SFP Ports
LNK/ACT/Speed
2 4 6 8 10 12 14 16 18 20 22 24 SFP2
LNK/ACT/Speed
1 3 5 7 9 11 13 15 17 19 21 23 SFP1
Reset

Figure 2 - LED Indicators

The following chart shows the LED indicators of the switch, along with an explanation of each indicator.

LED	COLOR	STATUS	STATUS DESCRIPTION
Power	Red	On	Power On
		Off	Power Off
LNK/ACT/ Speed (1~24)	10/100Mbps: Amber	On	A device is connected to the port
	1000Mbps: Green	Off	A device is disconnected to the port
		Flashing	Sending or receiving data
SFP1 SFP2	Green	On	A device is connected to the port
		Off	A device is disconnected to the port
		Flashing	Sending or receiving data

1.3.2 Rear Panel

The rear panel of the switch features an AC power connector and ground connection as shown below.

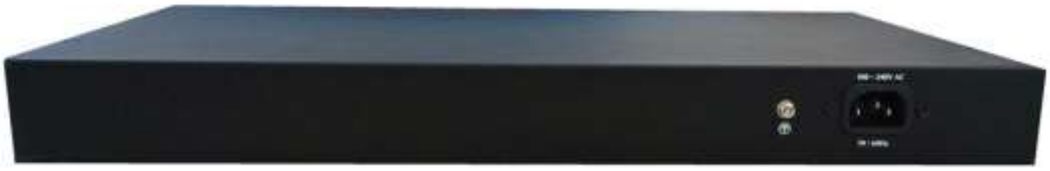


Figure 3 - Rear Panel

AC Power Connector:
Power is supplied through an external AC power adapter. It supports AC 100-240V, 50/60Hz.

Grounding Terminal:
The switch already comes with a lightning protection mechanism. You can also ground the switch through the PE cable on the AC cord or with a separate ground wire.

1.4 Package Contents

Before installing the switch, make sure that the following items are enclosed. If any part is missing or damaged, contact your local agent immediately.

- One Web-Managed Gigabit Ethernet Switch
- Four rubber feet, two mounting ears and eights screws
- AC power cord
- User manual

Chapter 2 Installing and Connecting the Switch

This part describes how to install your Web-Managed Gigabit Ethernet Switch and make connections to it.

2.1 Installation

The following steps will help prevent damage to the device while also helping to maintain proper security.

- Place the switch on a stable surface or desktop to minimize the chances of falling.
- Make sure the switch works in the proper AC input range and matches the voltage labeled on the switch.
- To keep the switch free from lightning damage, do not open the switch's chassis even if it fails to receive power.
- Make sure that there is proper heat dissipation from and adequate ventilation around the switch.
- Make sure the surface the switch is placed on can support the weight of the switch and its accessories.

2.1.1 Desktop Installation

When installing the switch on a desktop (if not in a rack), attach the enclosed rubber feet to the bottom corners of the switch to minimize vibration. Allow adequate space for ventilation between the device and the objects around it.

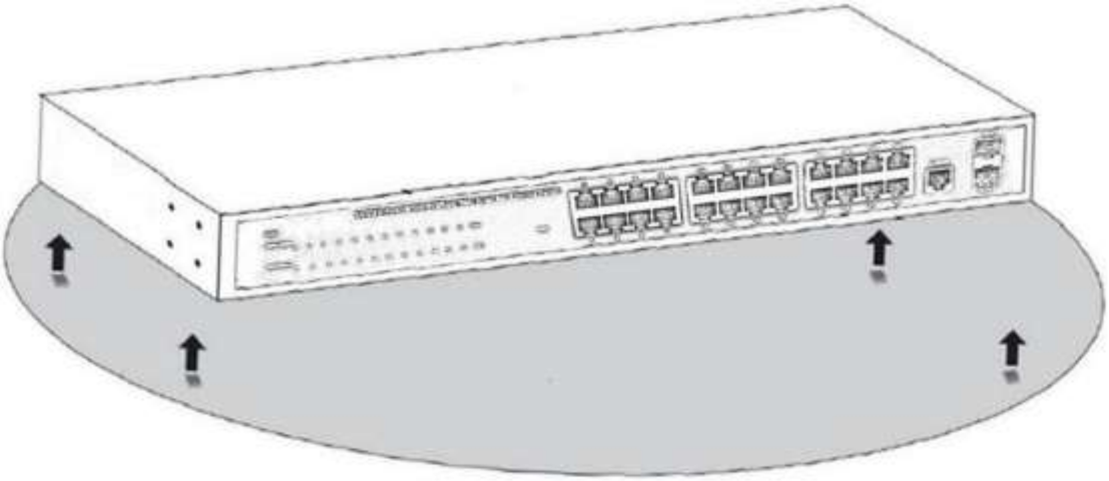


Figure 4 - Desktop Installation

2.1.2 Rack-mountable Installation in 19-inch Cabinet

The switch can be mounted in an EIA standard-sized, 19-inch rack, which can be placed in a wiring closet with other equipment. To install the switch, follow these steps:

a. Attach the mounting brackets on the switch's side panels (one on each side) and secure them with the screws provided.

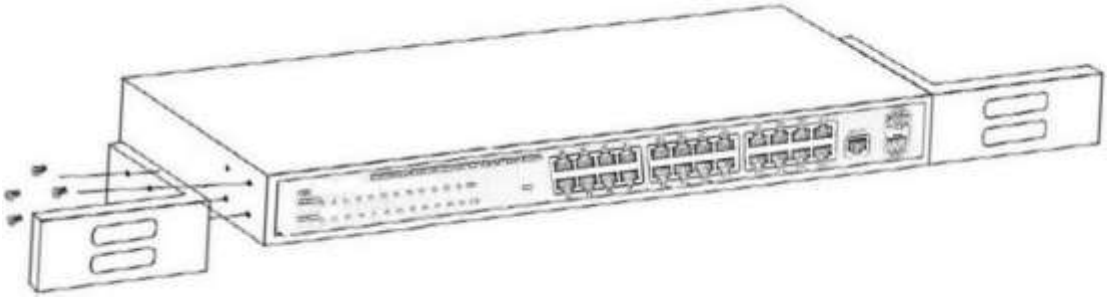


Figure 5 - Bracket Installation

b. Use the screws provided with the equipment rack to mount the switch on the rack and tighten it.

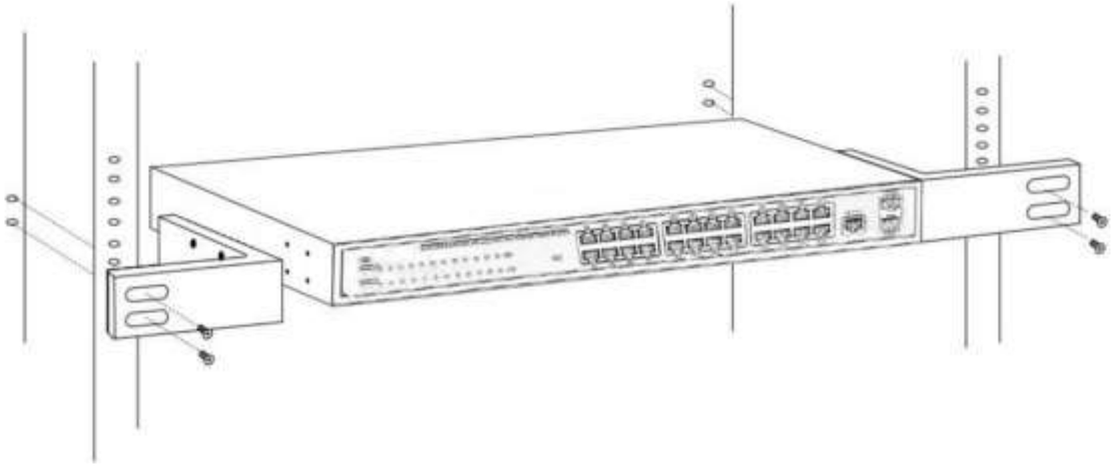


Figure 6 - Rack Installation

2.1.3 Power on the Switch

The switch is powered on by connecting it to an outlet using the AC 100-240V 50/60Hz internal high-performance power supply.

AC Electrical Outlet:
It is recommended to use a single-phase, three-wire receptacle with a neutral outlet or multifunctional computer professional receptacle. Be sure to connect the metal ground connector to the grounding source on the outlet.

AC Power Cord Connection:
Connect the AC power connector on the back panel of the switch to an external receptacle

with the included power cord, then check that the power indicator is ON. When it is ON, it indicates the power connection is okay.

Chapter 3 How to Login the Switch

3.1 Switch to End Node

Use standard Cat5/5e Ethernet cable (UTP/STP) to connect the switch to end nodes as described below. Switch ports will automatically adjust to the characteristics (MDI/MDI-X, speed, duplex) of the device to which they are connected.

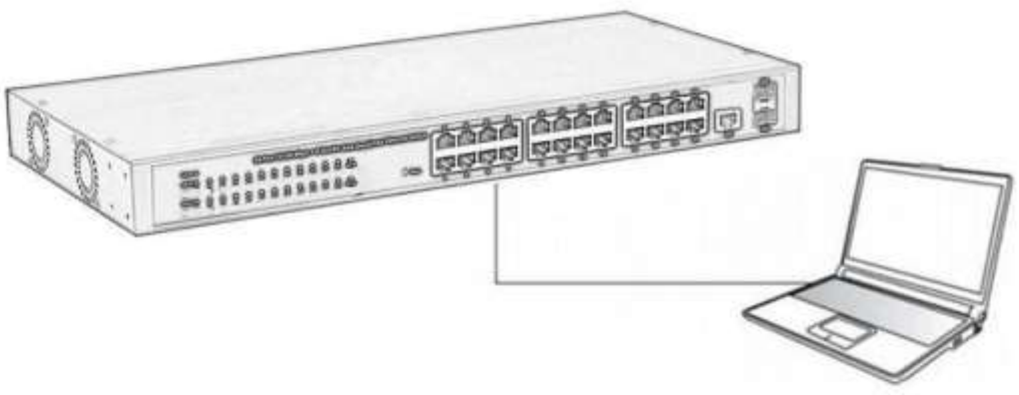


Figure 7 - PC Connect

The LNK/ACT/Speed LEDs for each port light when the link is available.

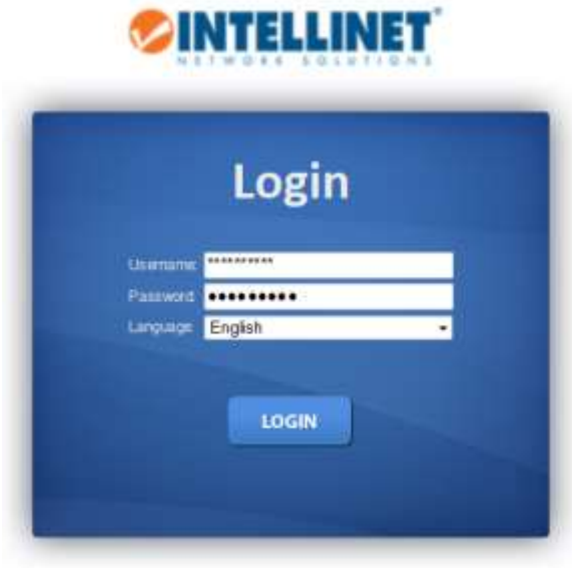
3.2 How to Login the Switch

As the switch provides Web-based management login, you can configure your computer's IP address manually to log on to the switch. The default settings of the switch are shown below.

Parameter	Default Value
Default IP address	192.168.2.1
Default Username	admin
Default Password	admin (or serial number on the bottom of the switch)

You can log on to the configuration window of the switch through following steps:

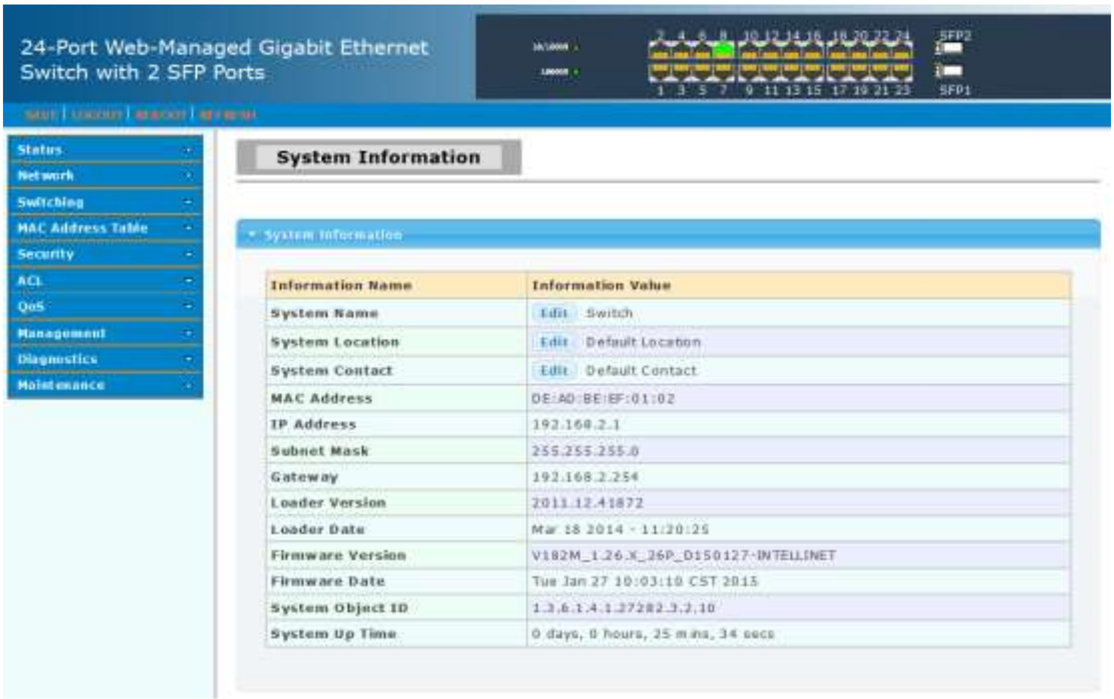
1. Connect the switch with the computer NIC interface.
2. Power on the switch.
3. Check whether the IP address of the computer is within this network segment: 192.168.2.xxx ("xxx" range is 2-254); for example, 192.168.2.100.
4. Open the browser, and enter *http://192.168.2.1* and then press "Enter." The switch login window appears, as shown below.



Username: **********
Password: ●●●●●●●●●
Language: English

Figure 8 - Login Window

5. Enter the Username and Password (the factory default Username is **admin** and Password is **admin *****), and then click “LOGIN” to log in to the switch configuration window as below.



Information Name	Information Value
System Name	Edit Switch
System Location	Edit Default Location
System Contact	Edit Default Contact
MAC Address	DE:AD:BE:EF:01:02
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Gateway	192.168.2.254
Loader Version	2011.12.41872
Loader Date	Mar 18 2014 - 11:20:25
Firmware Version	V182M_1.26.X_26P_D150127-INTELLINET
Firmware Date	Tue Jan 27 10:03:10 CST 2015
System Object ID	1.3.6.1.4.1.27282.3.2.10
System Up Time	0 days, 0 hours, 25 mins, 34 secs

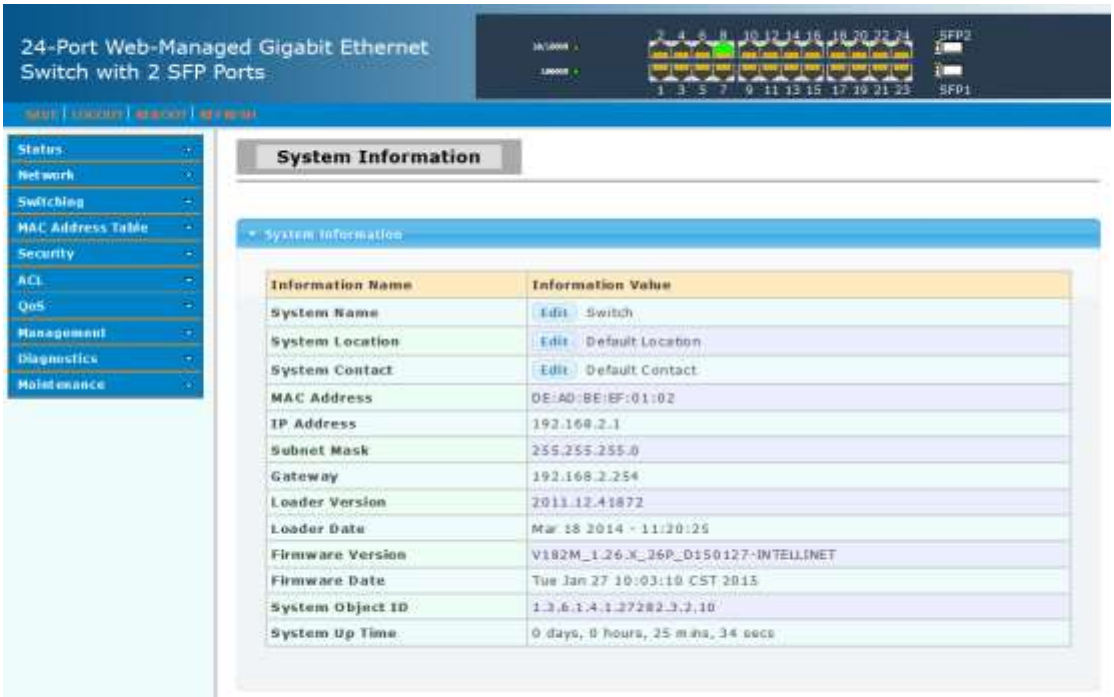
Figure 9 - Configuration Window

*** Later generation (2020 and later) models utilize the device serial number as the password. The serial number can be found on the bottom of the device.

Chapter 4 Switch Configuration

The Web-Managed Gigabit Ethernet Switch software provides rich Layer 2 functionality for switches in your networks. This chapter describes how to use the Web-based management interface (Web UI) for this switch to configure managed-switch software features.

In the Web UI, the left column shows the configuration menu. The top row shows the switch’s current link status. Green squares indicate the port link is up, while black squares indicate the port link is down. Below the switch panel, you can find a common toolbar to provide useful functions for users. The rest of the screen area displays the configuration settings.



Information Name	Information Value
System Name	Edit Switch
System Location	Edit Default Location
System Contact	Edit Default Contact
MAC Address	0E:A0:BE:EF:01:02
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Gateway	192.168.2.254
Loader Version	2011.12.41872
Loader Date	Mar 18 2014 - 11:20:25
Firmware Version	V182M_1.26.X_26P_D150127-INTELLINET
Firmware Date	Tue Jan 27 10:03:10 CST 2015
System Object ID	1.3.6.1.4.1.27282.3.2.10
System Up Time	0 days, 0 hours, 25 mins, 34 secs

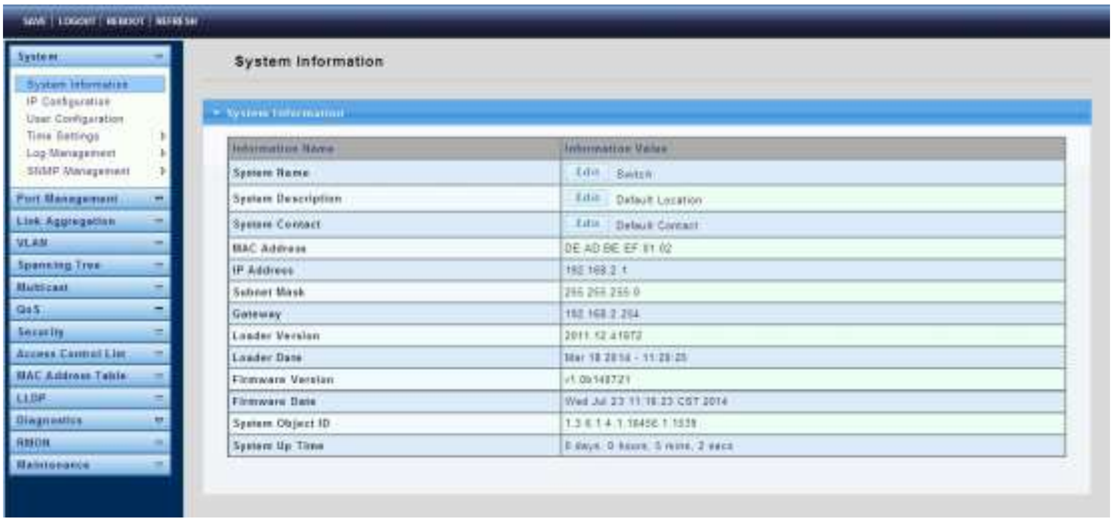
4.1 Status

Use the Status pages to view system information and status.

4.1.1 System Information

To display the System Information page, click **Status > System Information.**

This page allows you to configure System-related information and browse some system information, such as MAC address, IP address, firmware version, loader version and such.



System Information

System Information

Information Name	Information Value
System Name	Edit Switch
System Description	Edit Default Location
System Contact	Edit Default Contact
MAC Address	DE:AD:BE:EF:01:02
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Gateway	192.168.2.254
Loader Version	2011.12.41072
Loader Date	Mar 18 2014 - 11:28:25
Firmware Version	v1.09148721
Firmware Date	Wed Jul 23 11:18:23 CST 2014
System Object ID	1.3.6.1.4.1.18456.1.1539
System Up Time	0 days, 0 hours, 5 mins, 2 secs

System Name: System name of the switch. This name will also use as CLI prefix of each line. (“Switch>” or “Switch#”).

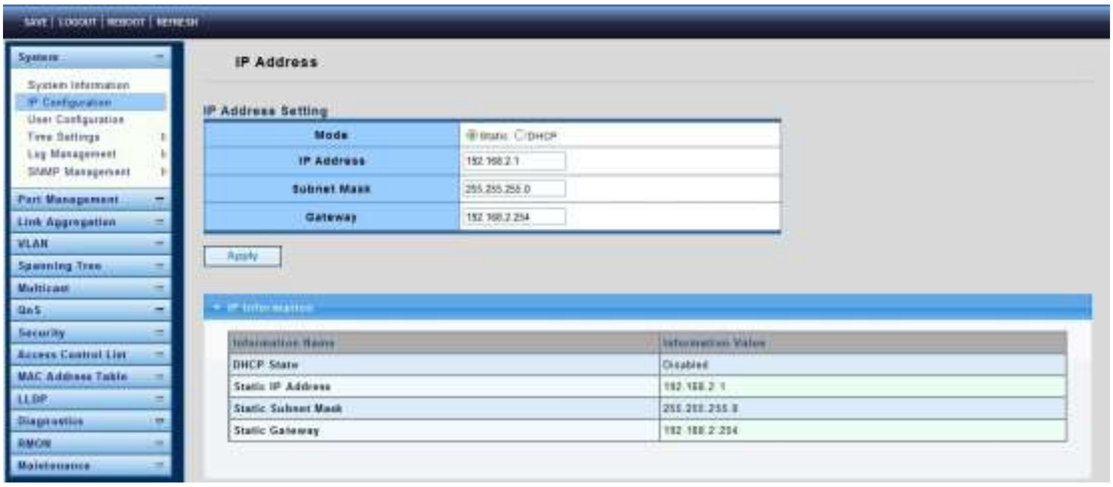
System Description: System location of the switch.

System Contact: System contact of the switch.

4.1.2 IP Configuration

To display the IP Configuration page, click **System > IP Configuration.**

This page allows you to edit the IP address, Subnet Mask and Gateway.



IP Address

IP Address Setting

Mode	● Static ○ DHCP
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Gateway	192.168.2.254

IP Information

Information Name	Information Value
DHCP State	Disabled
Static IP Address	192.168.2.1
Static Subnet Mask	255.255.255.0
Static Gateway	192.168.2.254

Mode: Select the mode of network connection.

- Static: Enable static IP address.
- DHCP: Enable DHCP to obtain IP information from a DHCP server on the network.

IP Address: If static mode is enabled, enter an IP address in this field.

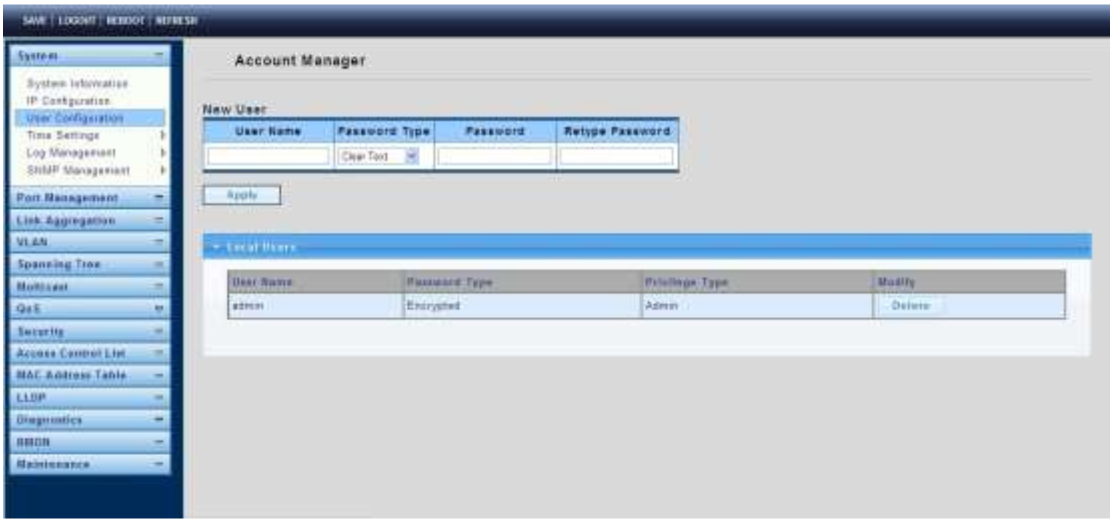
Subnet Mask: If static mode is enabled, enter a subnet mask in this field.

Gateway: If static mode is enabled, enter a gateway address in this field.

4.1.3 User Configuration

To display the User Configuration page, click **System > User Configuration.**

This page allows you to Input User Name, Password Type and Password.



Account Manager

New User

User Name	Password Type	Password	Retype Password
	Clear Text		

Local Users

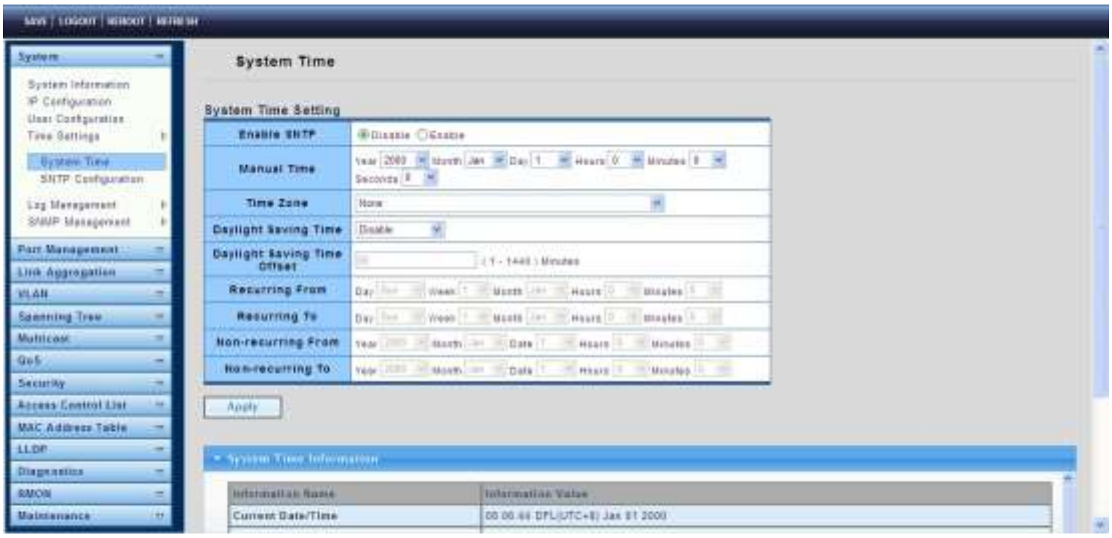
User Name	Password Type	Privilege Type	Modify
admin	Encrypted	Admin	Delete

4.1.4 Time Settings

4.1.4.1 System Time

To display the System Time page, click **System > Time Settings > System Time.**

System time settings include time zone and Daylight Saving time.



System Time

System Time Setting

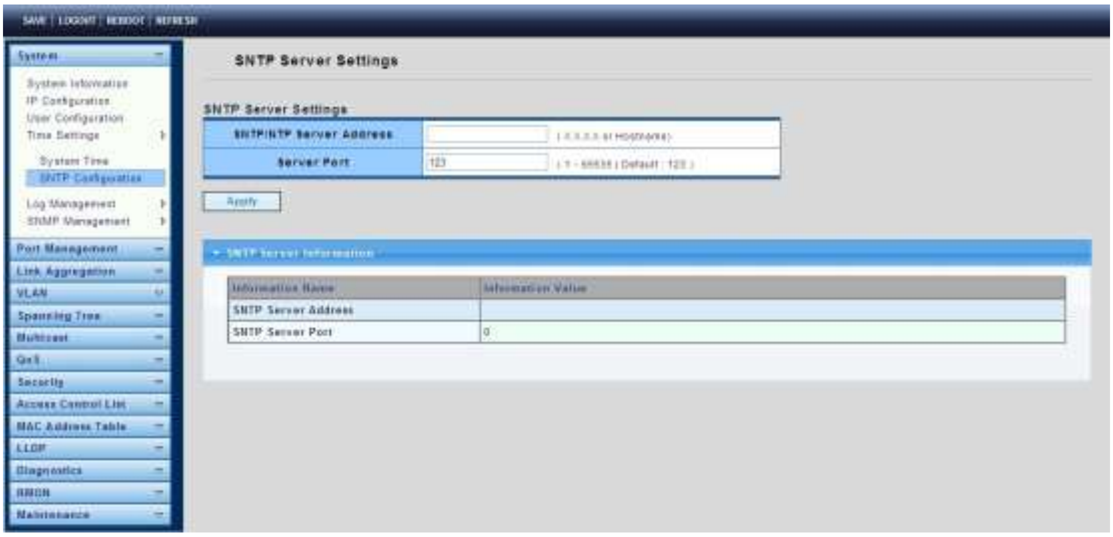
Enable SNTP	● Disable ○ Enable
Manual Time	Year 2000 Month Jan Day 1 Hours 0 Minutes 8 Seconds 8
Time Zone	None
Daylight Saving Time	Disable
Daylight Saving Time Offset	(1 - 1440) Minutes
Recurring From	Day Week Month Hours Minutes
Recurring To	Day Week Month Hours Minutes
Non-recurring From	Year Month Date Hours Minutes
Non-recurring To	Year Month Date Hours Minutes

System Time Information

Information Name	Information Value
Current Date/Time	00:00:44 DFL(UTC+8) Jan 01 2000

4.1.4.2 SNTP Configuration

To display the SNTP Configuration page, click **System > Time Settings > SNTP Configuration.**



SNTP Server Settings

SNTP Server Settings

SNTP/NTP Server Address		(X.X.X.X or Hostname)
Server Port	123	(1 - 65535) Default : 123)

SNTP Server Information

Information Name	Information Value
SNTP Server Address	
SNTP Server Port	0

SNTP Server Address: The IP address of the SNTP/NTP server.

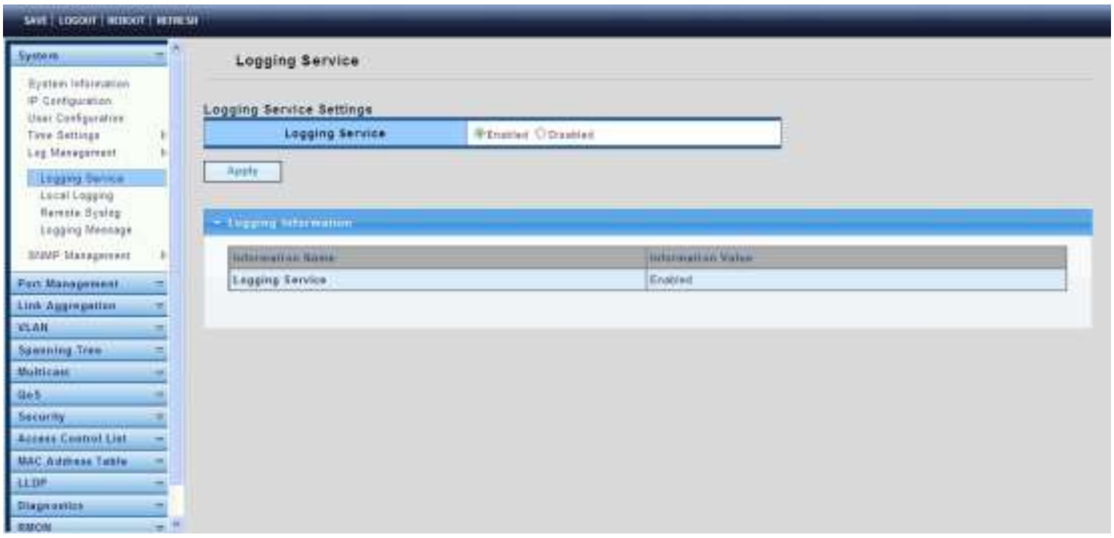
Server Port: The Port Number of the SNTP/NTP server.

4.1.5 Log Management

4.1.5.1 Logging Service

To display the Logging Service page, click **System > Log Management > Logging Service.**

This page allows you to enable or disable the logging service, and will display the information of logging.



Logging Service

Logging Service Settings

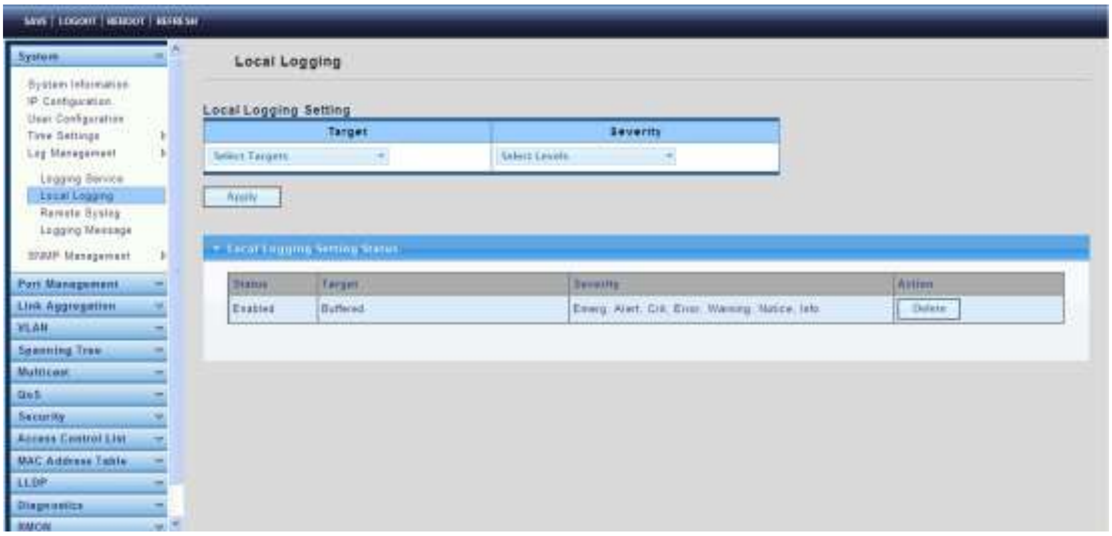
Logging Service	● Enabled ○ Disabled

Logging Information

Information Name	Information Value
Logging Service	Enabled

4.1.5.2 Local Logging

To display the Local Logging page, click **System > Log Management > Local Logging.**



Local Logging

Local Logging Setting

Target	Severity
Select Targets	Select Levels

Local Logging Setting Status

Status	Target	Severity	Action
Enabled	Buffered	Emerg, Alert, Crit, Error, Warning, Notice, Info	Delete

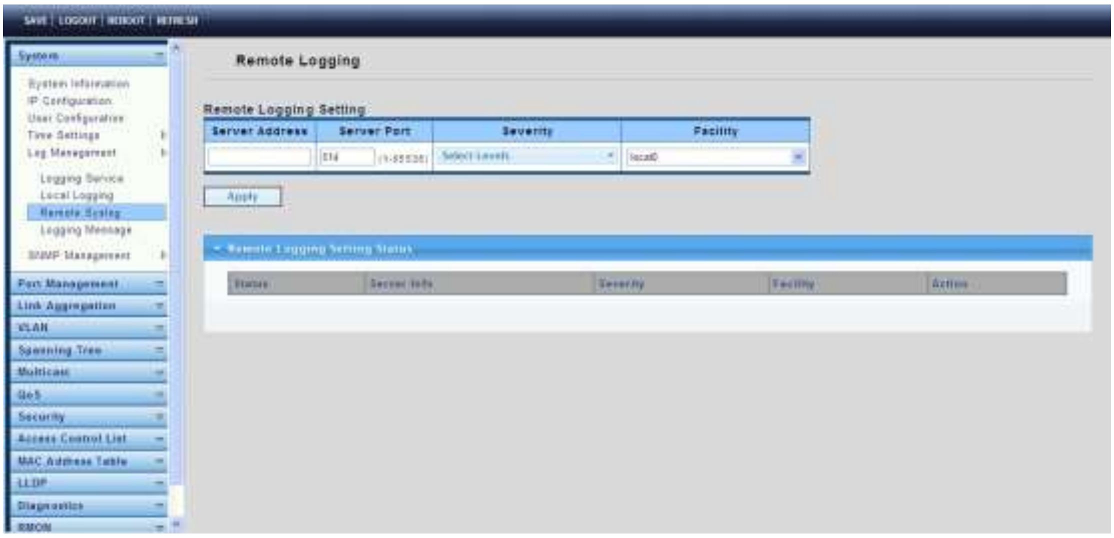
Target: Select the target to store log messages.

- RAM: Store log messages in RAM disk. All log messages will disappear after system reboot.
- FLASH: Store log messages in FLASH. All log messages will not disappear after system reboot.

Severity: Select the severity of log messages which will be stored.

4.1.5.3 Remote Syslog

To display the Remote Syslog page, click **System > Log Management > Remote Syslog.**



Remote Logging

Remote Logging Setting

Server Address	Server Port	Severity	Facility
	514 (1-65535)	Select Levels	local0

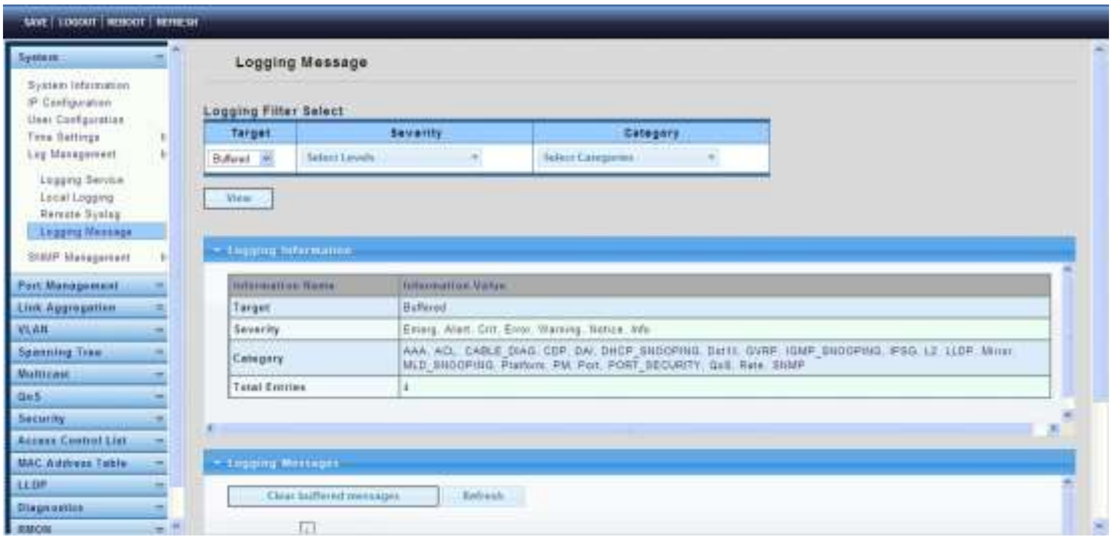
Remote Logging Setting Status

Status	Server Info	Severity	Facility	Action

Server Address: The IP address of the remote log server.
Server Port: The Port number of the remote log server.
Severity: Select the severity of log messages which will be sent.

4.1.5.4 Logging Message

To display the Logging Message page, click **System > Log Management > Logging Message.**



Logging Message

Logging Filter Select

Target	Severity	Category
Buffered	Select Levels	Select Categories

Information Name	Information Value
Target	Buffered
Severity	Emerg, Alert, Crit, Error, Warning, Notice, Info
Category	AAA, ACL, CABLE_DIAG, CDP, DAI, DHCP_SNOOPING, Dot1X, GVRP, IGMP_SNOOPING, IPSG, L2, LLDP, Mirror, MLD_SNOOPING, Platform, PM, Port, PORT_SECURITY, QoS, Rate, SNMP
Total Entries	4

Target: Select the log message source to show on the table.

- RAM: Logs store in the RAM disk.
- DHCP: Logs store in the FLASH.

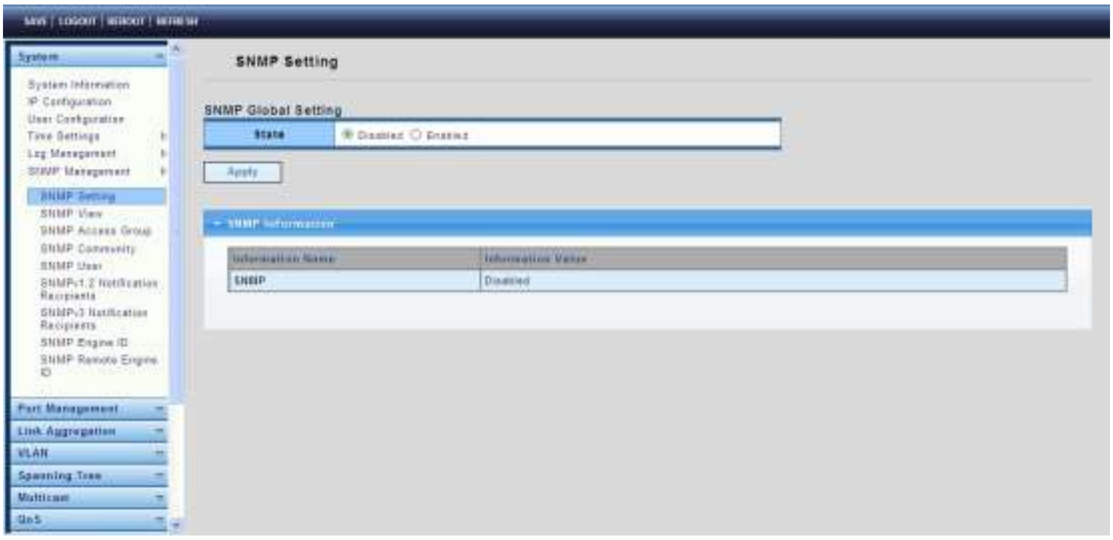
Severity: Select the severity to filter log messages.

Category: Select the category to filter log messages.

4.1.6 SNMP Management

4.1.6.1 SNMP Setting

To display the SNMP Setting page, click **System > SNMP Management > SNMP Setting.**



SNMP Setting

SNMP Global Setting

State	● Disabled ○ Enabled

Information Name	Information Value
SNMP	Disabled

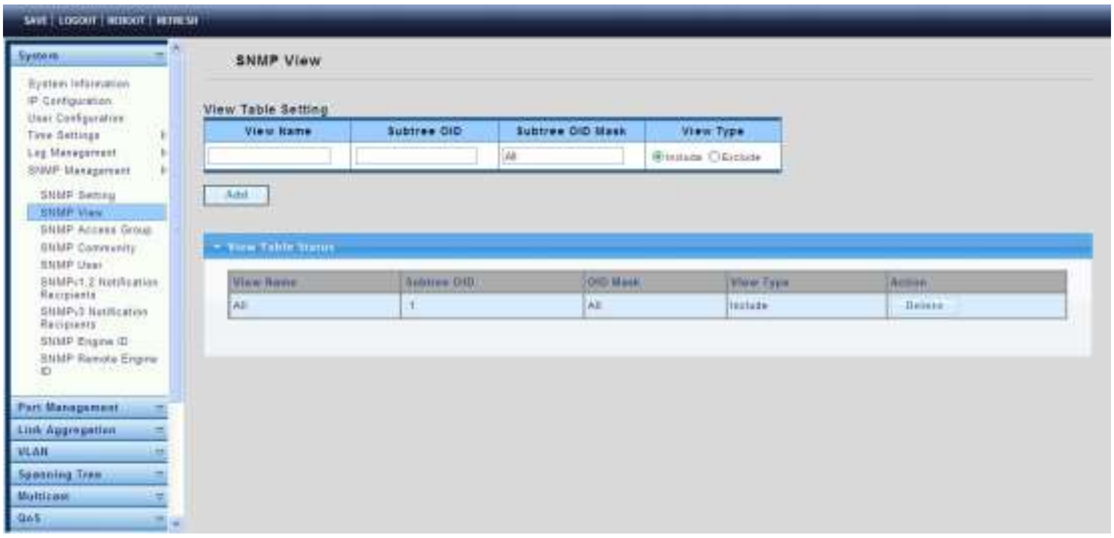
State: SNMP daemon state.

- Enabled: Enable SNMP daemon.
- Disabled: Disable SNMP daemon.

4.1.6.2 SNMP View

To display the SNMP View page, click **System > SNMP Management > SNMP View.**

This page is used to configure the SNMP View. Used in the SNMP message management variables (OID) to describe the switch in the management object, MIB (Management Information Base) is a set of the monitoring network equipment management variables. View is used to control how these variables are to be managed.



SNMP View

View Table Setting

View Name	Subtree OID	Subtree OID Mask	View Type
		All	● Include ○ Exclude

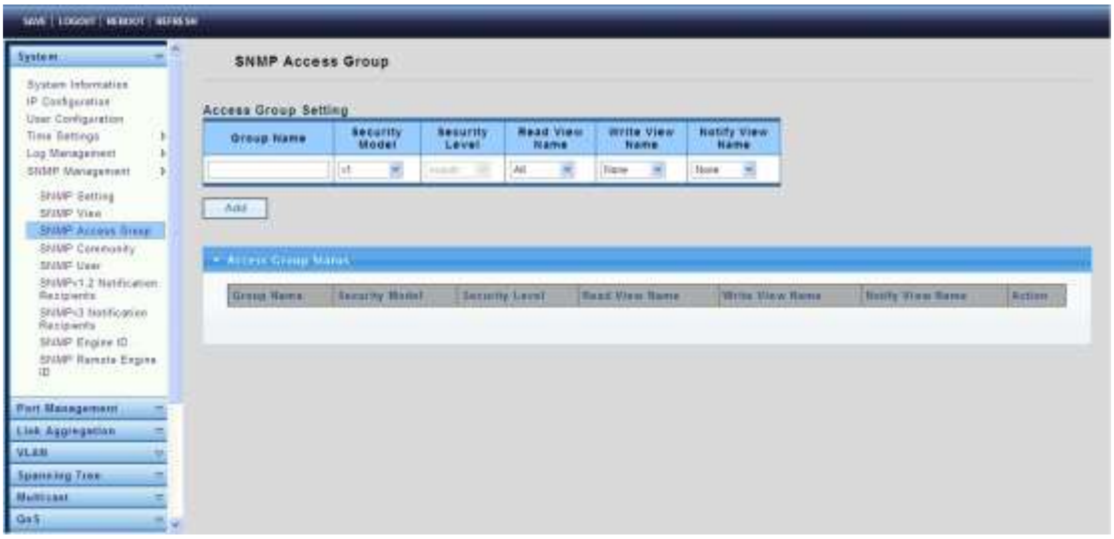
View Table Status

View Name	Subtree OID	OID Mask	View Type	Action
All	.1	All	include	Delete

4.1.6.3 SNMP Access Group

To display the SNMP Access Group page, click **System > SNMP Management > SNMP Access Group.**

This page is used to configure the SNMP group.



SNMP Access Group

Access Group Setting

Group Name	Security Model	Security Level	Read View Name	Write View Name	Notify View Name
	v1	noauth	All	None	None

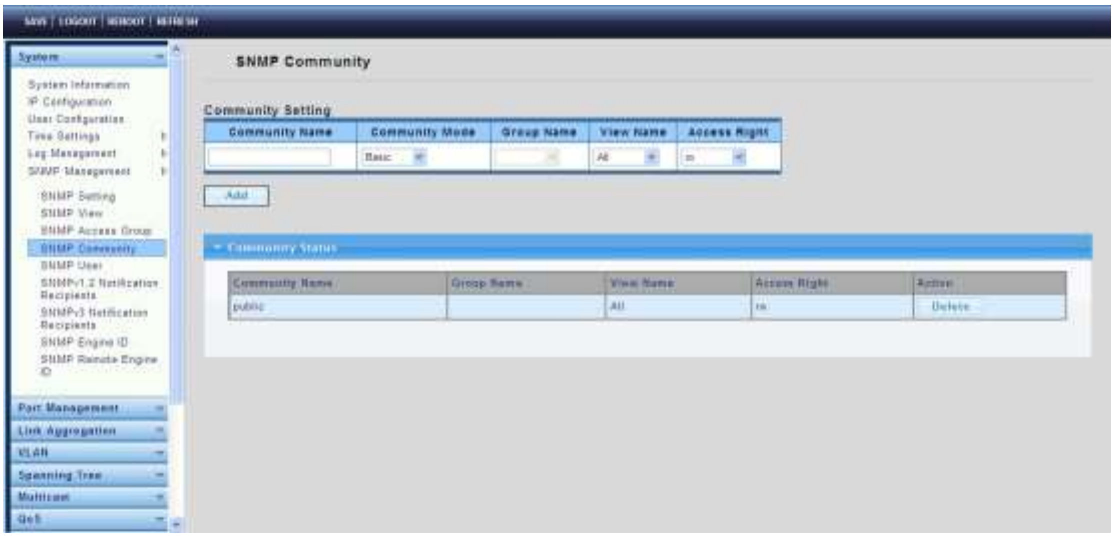
Access Group Status

Group Name	Security Model	Security Level	Read View Name	Write View Name	Notify View Name	Action

4.1.6.4 SNMP Community

To display the SNMP Community page, click **System > SNMP Management > SNMP Community.**

SNMP v1 and SNMP v2c use the group name (Community Name) certification, which plays a role similar to the password. If using SNMP v1 and SNMP v2c, you can go directly from the configuration settings to this page to configure the SNMP community.



SNMP Community

Community Setting

Community Name	Community Mode	Group Name	View Name	Access Right
	Basic		All	ro

Add

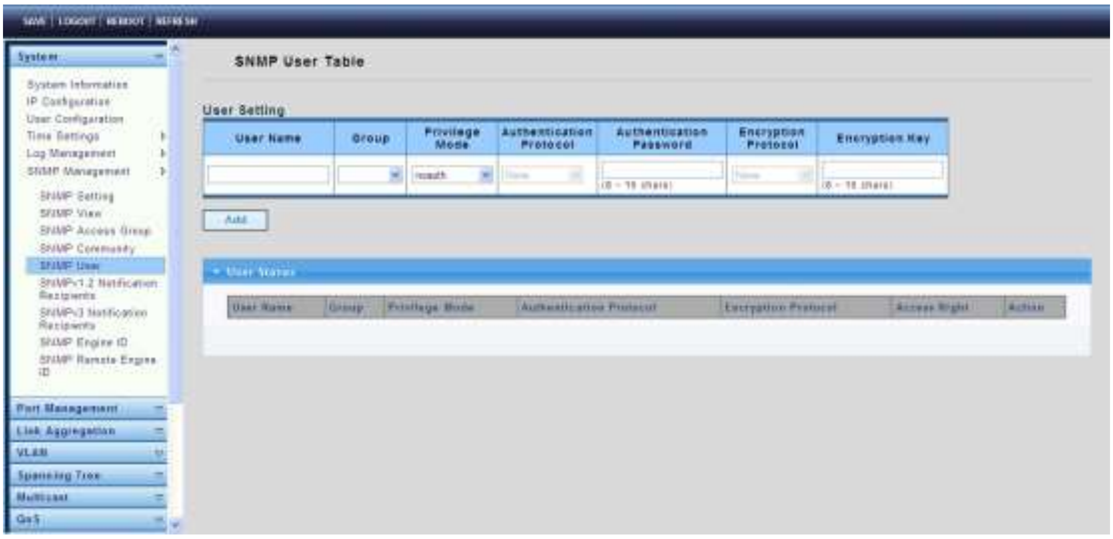
Community Status

Community Name	Group Name	View Name	Access Right	Action
public		All	ro	Delete

4.1.6.5 SNMP User

To display the SNMP User page, click **System > SNMP Management > SNMP User.**

This page is used to create SNMP users in a group, which would have the same level of security and access control permissions.



SNMP User Table

User Setting

User Name	Group	Privilege Mode	Authentication Protocol	Authentication Password	Encryption Protocol	Encryption Key
		noauth	None	(8 ~ 16 chars)	None	(8 ~ 16 chars)

Add

User Status

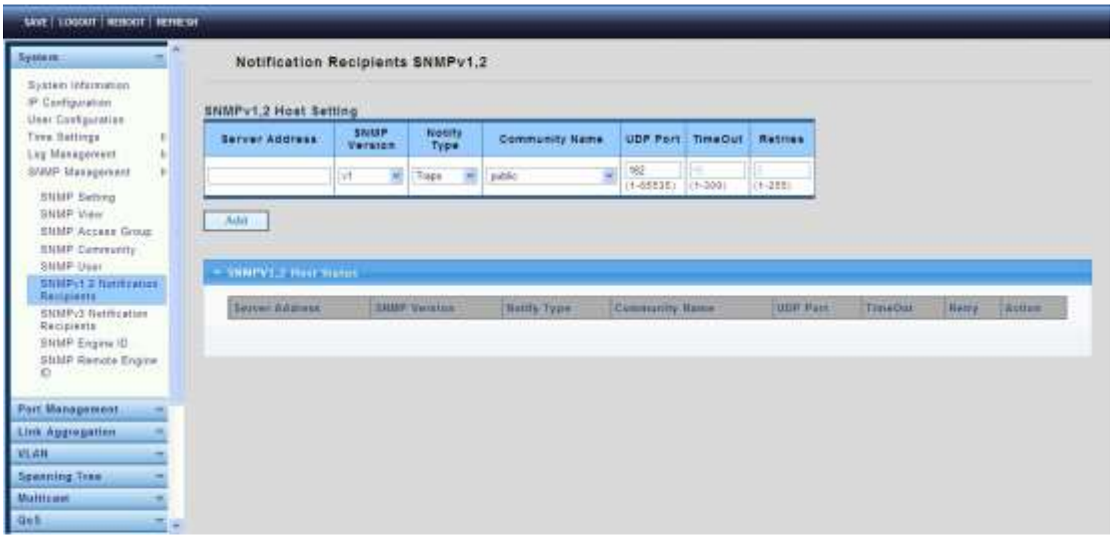
User Name	Group	Privilege Mode	Authentication Protocol	Encryption Protocol	Access Right	Action

4.1.6.6 SNMPv1,2 Notification Recipients

A trap receiver entry contains the IP address of the node and the SNMP credentials corresponding to the version that is included in the trap message. When an event arises that requires a trap message to be sent, it is sent to every node listed in the Notification Recipient Table.

To display the SNMPv1,2 Notification Recipients page, click **System > SNMP Management > SNMPv1,2 Notification Recipients.**

This page contains recipients for SNMPv1,2. It allows you configure the destination to which SNMP notifications are sent, and the types of SNMP notifications that are sent to each destination (traps or informs). The Add/Edit pop-ups enable configuring the attributes of the notifications.



Notification Recipients SNMPv1,2

SNMPv1,2 Host Setting

Server Address	SNMP Version	Notify Type	Community Name	UDP Port	TimeOut	Retries
	v1	Traps	public	162 (1-65535)	(1-300)	(1-255)

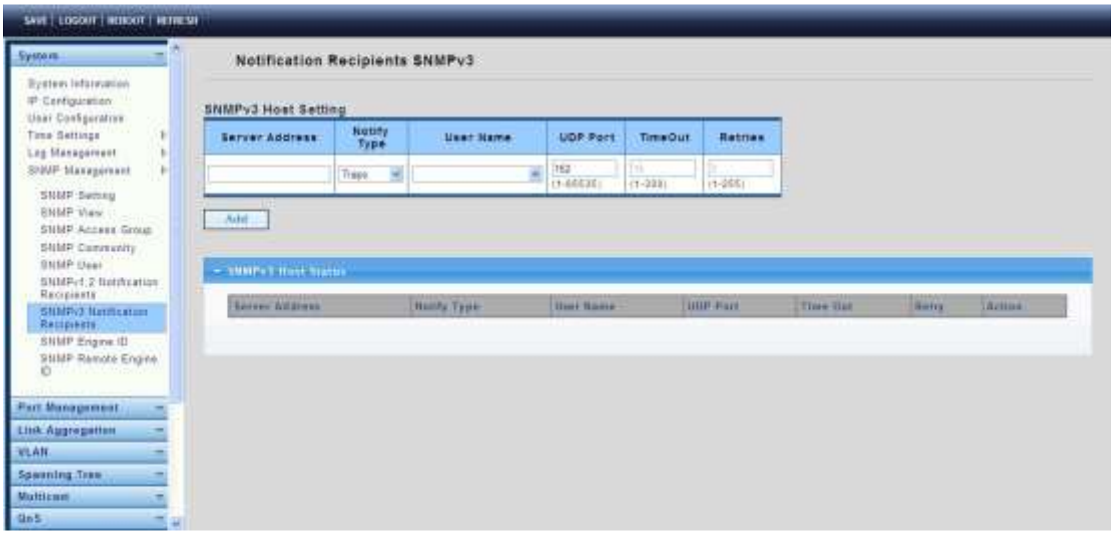
SNMPV1,2 Host Status

Server Address	SNMP Version	Notify Type	Community Name	UDP Port	TimeOut	Retry	Action

4.1.6.7 SNMPv3 Notification Recipients

To display the SNMPv3 Notification Recipients page, click **System > SNMP Management > SNMPv3 Notification Recipients.**

This page contains recipients for SNMPv3. It allows you to configure the destination to which SNMP notifications are sent, and the types of SNMP notifications that are sent to each destination (traps or informs). The Add/Edit pop-ups enable configuring the attributes of the notifications.



Notification Recipients SNMPv3

SNMPv3 Host Setting

Server Address	Notify Type	User Name	UDP Port	TimeOut	Retries
	Traps		162 (1-65535)	(1-300)	(1-255)

SNMPv3 Host Status

Server Address	Notify Type	User Name	UDP Port	Time Out	Retry	Action

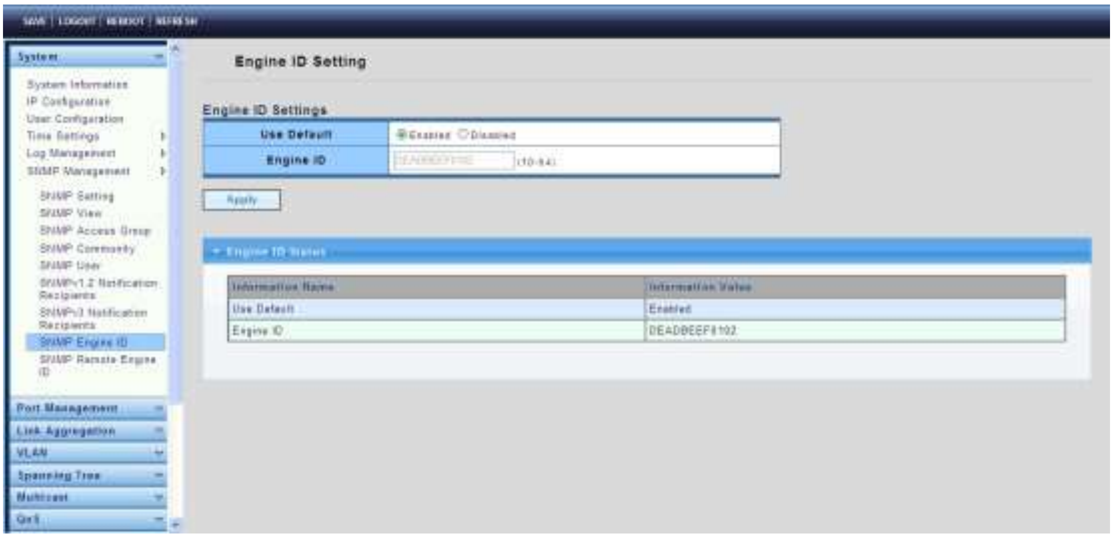
4.1.6.8 SNMP Engine ID

The Engine ID is used by SNMPv3 entities to uniquely identify them. An SNMP agent is considered an authoritative SNMP engine. This means that the agent responds to incoming messages (Get, GetNext, GetBulk, Set) and sends trap messages to a manager. The agent's local information is encapsulated in fields in the message.

Each SNMP agent maintains local information that is used in SNMPv3 message exchanges. The default SNMP Engine ID is composed of the enterprise number and the default MAC address. This engine ID must be unique for the administrative domain, so that no two devices in a network have the same engine ID.

To display the SNMP Engine ID page, click **System > SNMP Management > SNMP Engine ID.**

This page allows you to define the SNMP engine ID.



Engine ID Setting

Engine ID Settings

Use Default	● Enabled ○ Disabled
Engine ID	DEADBEEF8102 (10-64)

Information Name	Information Value
Use Default	Enabled
Engine ID	DEADBEEF8102

Use Default: Select the Use Default enable or disable.

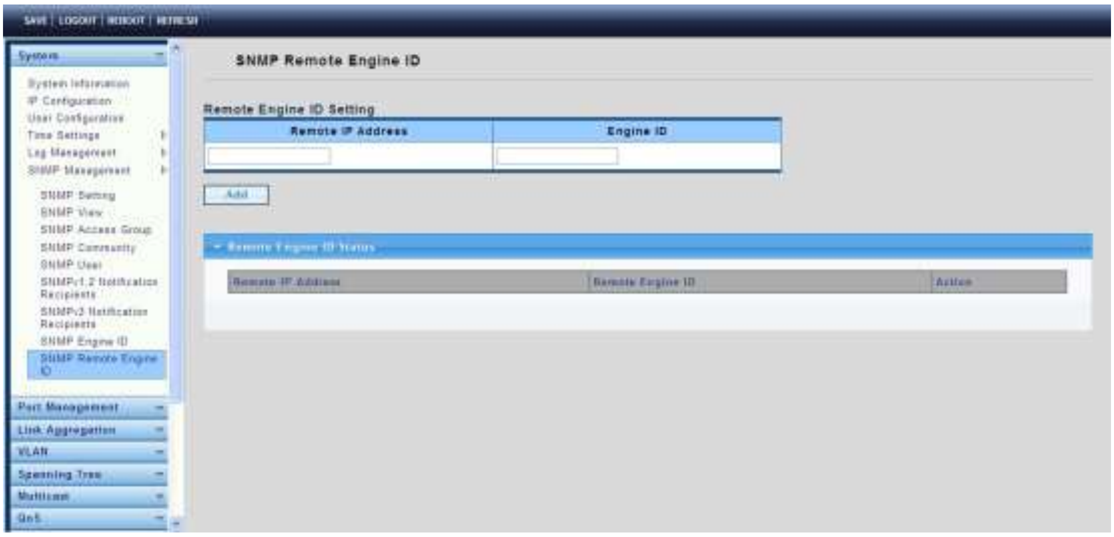
Engine ID: Enter the local device engine ID. The field value is a hexadecimal string (range: 10 - 64). Each byte in the hexadecimal character strings is represented by two hexadecimal digits.

All remote engine IDs and their IP addresses are displayed in the Remote Engine ID table.

4.1.6.9 SNMP Remote Engine ID

To display the SNMP Remote Engine ID page, click **System > SNMP Management > SNMP Remote Engine ID.**

This page allows you to create an SNMP Remote Engine ID.



SNMP Remote Engine ID

Remote Engine ID Setting

Remote IP Address	Engine ID

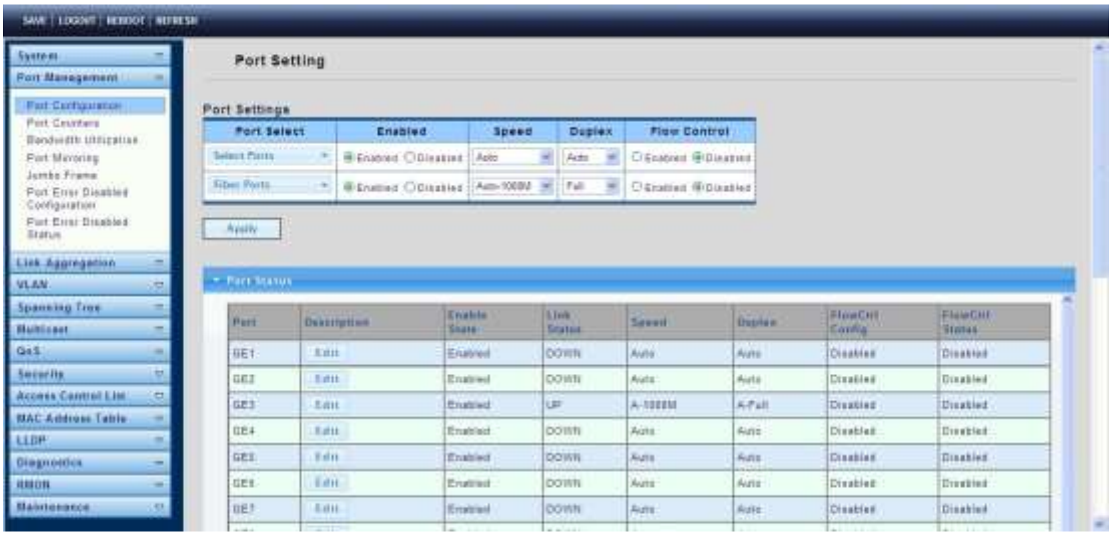
Remote IP Address	Remote Engine ID	Action

4.2 Port Management

4.2.1 Port Configuration

To display the Port Configuration page, click **Port Management > Port Configuration.**

This page allows you to configure ports, such as enabling or disabling, setting Ethernet link speeds, duplex modes and flow control.



Port Setting

Port Settings

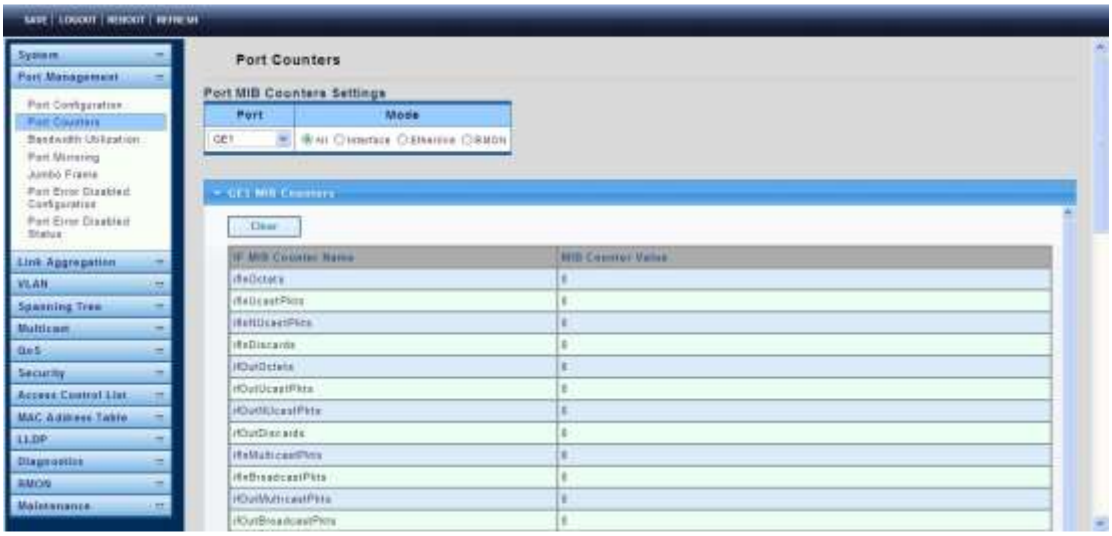
Port Select	Enabled	Speed	Duplex	Flow Control
Select Ports	● Enabled ○ Disabled	Auto	Auto	○ Enabled ● Disabled
Fiber Ports	● Enabled ○ Disabled	Auto-1000M	Full	○ Enabled ● Disabled

Port	Description	Enable State	Link Status	Speed	Duplex	FlowCtrl Config	FlowCtrl Status
GE1	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE2	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE3	Edit	Enabled	UP	A-1000M	A-Full	Disabled	Disabled
GE4	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE5	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE6	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE7	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled

4.2.2 Port Counters

To display the Port Counters page, click **Port Management > Port Counters.**

This page displays standard counters of network traffic using modes like Interface, Ethernetlike and RMON. Interfaces and Ethernetlike counters display errors on the traffic passing through each port. RMON counters provide a total count of different frame types and sizes passing through each port.



Port Counters

Port MIB Counters Settings

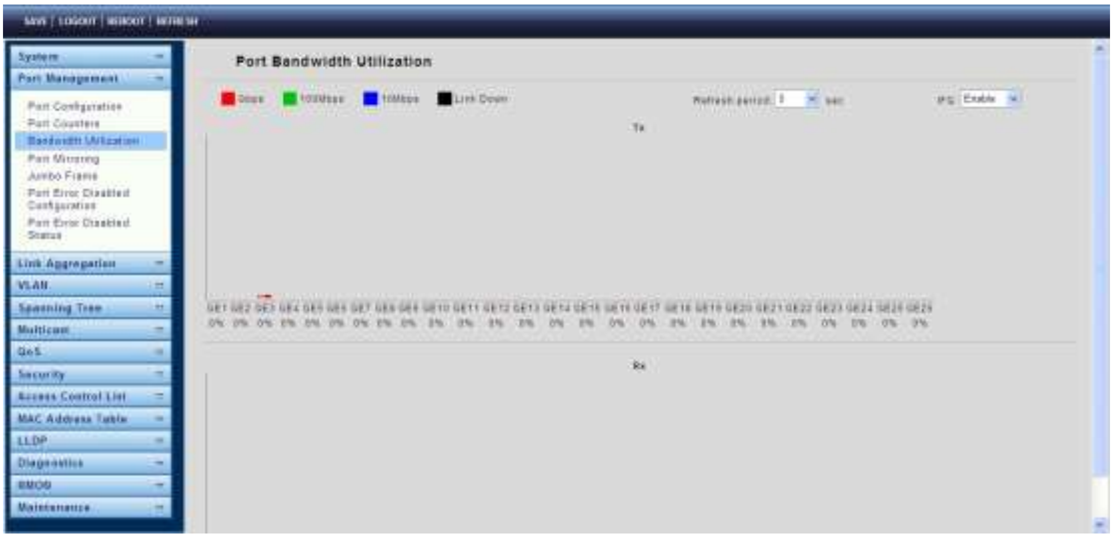
Port	Mode
GE1	● All ○ Interface ○ Etherlike ○ RMON

IF MIB Counter Name	MIB Counter Value
ifInOctets	0
ifInUcastPkts	0
ifInNUcastPkts	0
ifInDiscards	0
ifOutOctets	0
ifOutUcastPkts	0
ifOutNUcastPkts	0
ifOutDiscards	0
ifInMulticastPkts	0
ifInBroadcastPkts	0
ifOutMulticastPkts	0
ifOutBroadcastPkts	0

4.2.3 Bandwidth Utilization

To display the Bandwidth Utilization page, click **Port Management > Bandwidth Utilization.**

This page displays and lets you switch each port’s TX and RX bandwidth utilization.



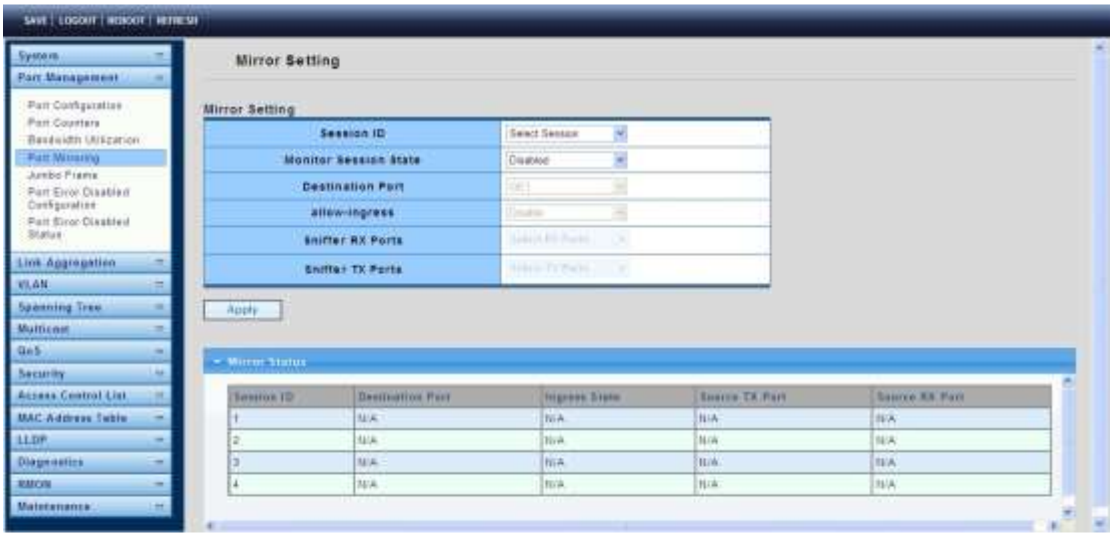
Refresh period: 3 sec

IFG: Enable

4.2.4 Port Mirroring

To display the Port Mirroring page, click **Port Management > Port Mirroring.**

Port mirroring copies the TX/RX data flow from the source port to the target, or destination, port.



Mirror Setting

Mirror Setting

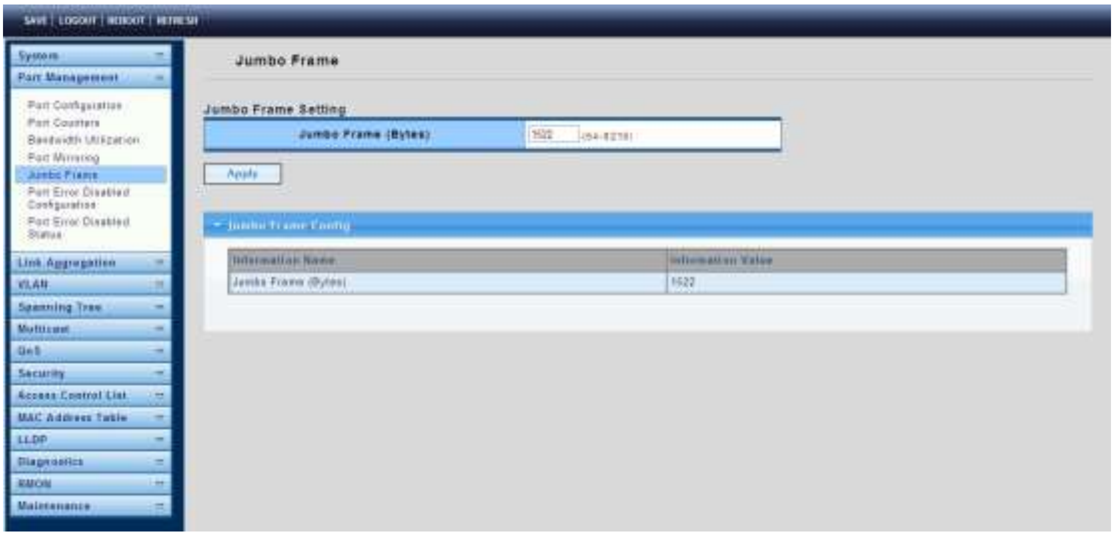
Session ID	Select Session
Monitor Session State	Disabled
Destination Port	GE1
allow-ingress	Disable
Sniffer RX Ports	Select RX Ports
Sniffer TX Ports	Select TX Ports

Mirror Status

Session ID	Destination Port	Ingress State	Source TX Port	Source RX Port
1	N/A	N/A	N/A	N/A
2	N/A	N/A	N/A	N/A
3	N/A	N/A	N/A	N/A
4	N/A	N/A	N/A	N/A

4.2.5 Jumbo Frame

To display the Jumbo Frame page, click **Port Management > Jumbo Frame.**



Jumbo Frame

Jumbo Frame Setting

Jumbo Frame (Bytes)	1522 (64-9216)

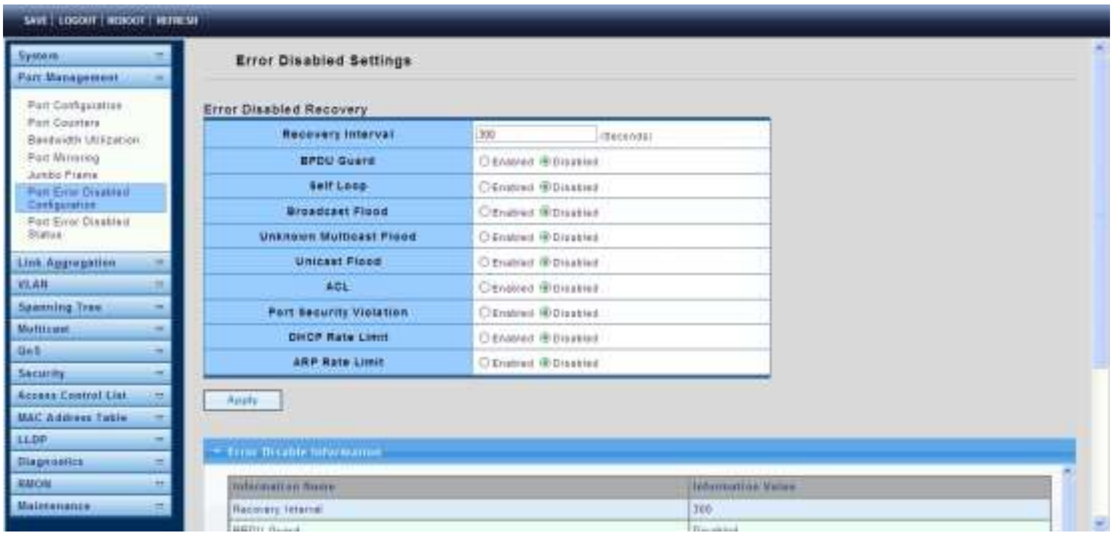
Information Name	Information Value
Jumbo Frame (Bytes)	1522

Jumbo Frame: The valid size range is 64 bytes – 9216 bytes.

4.2.6 Port Error Disabled Configuration

To display the Port Error Disabled Configuration page, click **Port Management > Port Error Disabled Configuration.**

This page allows you to browse ports disabled by certain protocols, such as BPDU Guard, Loop Back and UDLD. The “Recovery” button will re-enable those error-disabled ports.



Error Disabled Settings

Error Disabled Recovery

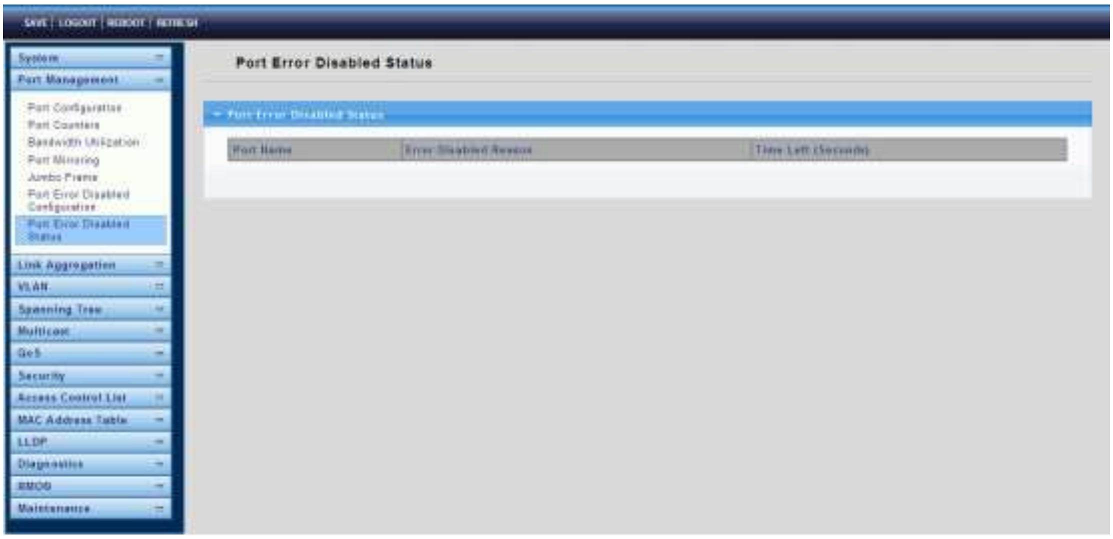
Recovery Interval	300 (Seconds)
BPDU Guard	○ Enabled ● Disabled
Self Loop	○ Enabled ● Disabled
Broadcast Flood	○ Enabled ● Disabled
Unknown Multicast Flood	○ Enabled ● Disabled
Unicast Flood	○ Enabled ● Disabled
ACL	○ Enabled ● Disabled
Port Security Violation	○ Enabled ● Disabled
DHCP Rate Limit	○ Enabled ● Disabled
ARP Rate Limit	○ Enabled ● Disabled

Information Name	Information Value
Recovery Interval	300
BPDU Guard	Disabled

4.2.7 Port Error Disabled Status

To display the Port Error Disabled Status page, click **Port Management > Port Error Disabled Status.**

This page is used to display the port error disabled status.



Port Error Disabled Status

Port Error Disabled Status

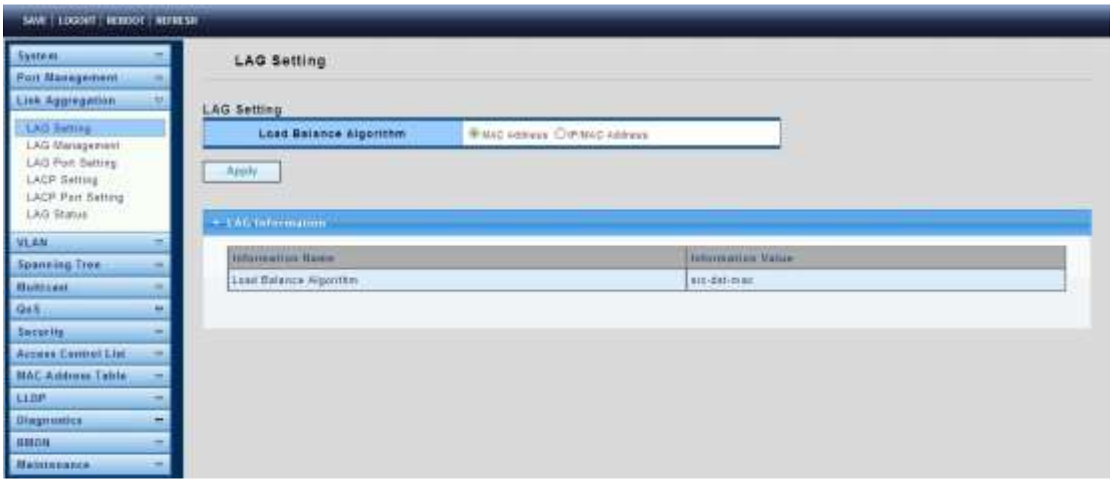
Port Name	Error Disabled Reason	Time Left (Seconds)

4.3 Link Aggregation

4.3.1 LAG Setting

To display the LAG Setting page, click **Link Aggregation > LAG Setting.**

This page allows you to configure ports’ aggregation rules by selecting MAC Address or IP/MAC Address.



LAG Setting

LAG Setting

Load Balance Algorithm: ● MAC Address ○ IP/MAC Address

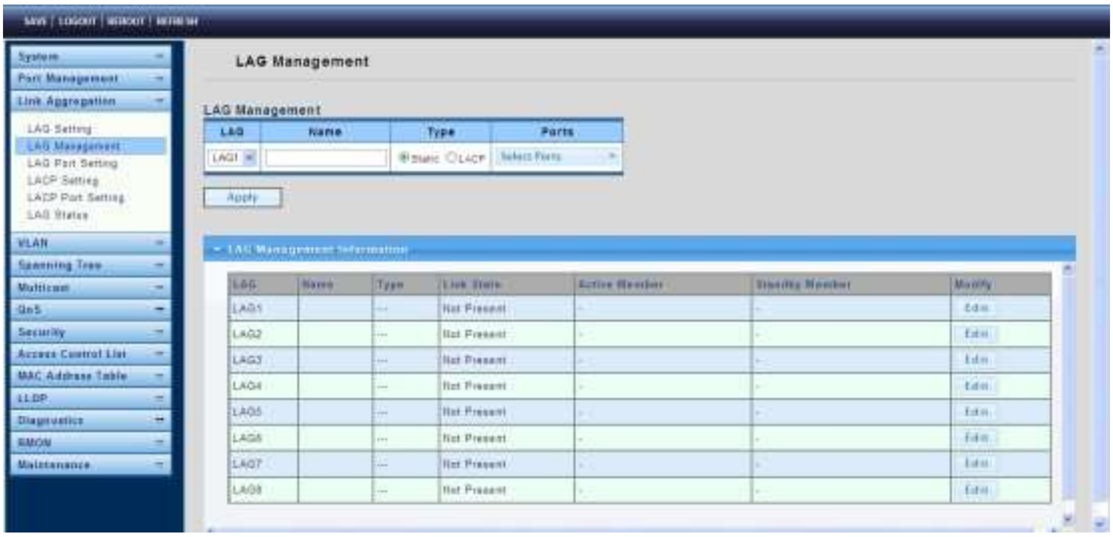
LAG Information

Information Name	Information Value
Load Balance Algorithm	src-dst-mac

4.3.2 LAG Management

To display the LAG Management page, click **Link Aggregation > LAG Management.**

This page is used to create new LAGs, configure ports' aggregation type, and select member ports.



LAG Management

LAG Management

LAG	Name	Type	Ports
LAG1		● Static ○ LACP	Select Ports

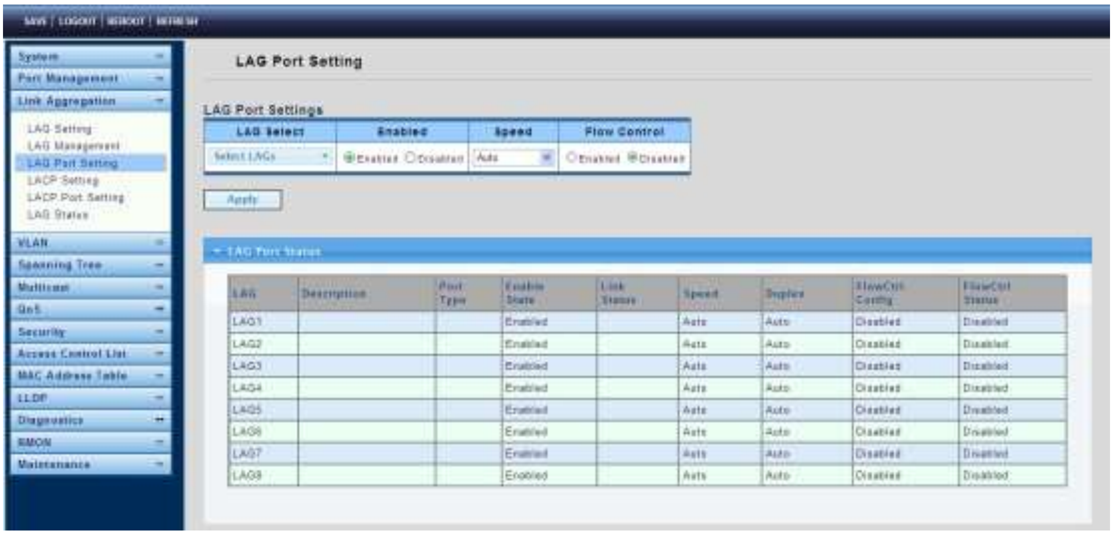
LAG Management Information

LAG	Name	Type	Link State	Active Member	Standby Member	Modify
LAG1		---	Not Present	-	-	Edit
LAG2		---	Not Present	-	-	Edit
LAG3		---	Not Present	-	-	Edit
LAG4		---	Not Present	-	-	Edit
LAG5		---	Not Present	-	-	Edit
LAG6		---	Not Present	-	-	Edit
LAG7		---	Not Present	-	-	Edit
LAG8		---	Not Present	-	-	Edit

4.3.3 LAG Port Setting

To display the LAG Port Setting page, click **Link Aggregation > LAG Port Setting.**

This page is used to set LAG status, speed and flow control functions.



LAG Port Setting

LAG Port Settings

LAG Select	Enabled	Speed	Flow Control
Select LAGs	● Enabled ○ Disabled	Auto	○ Enabled ● Disabled

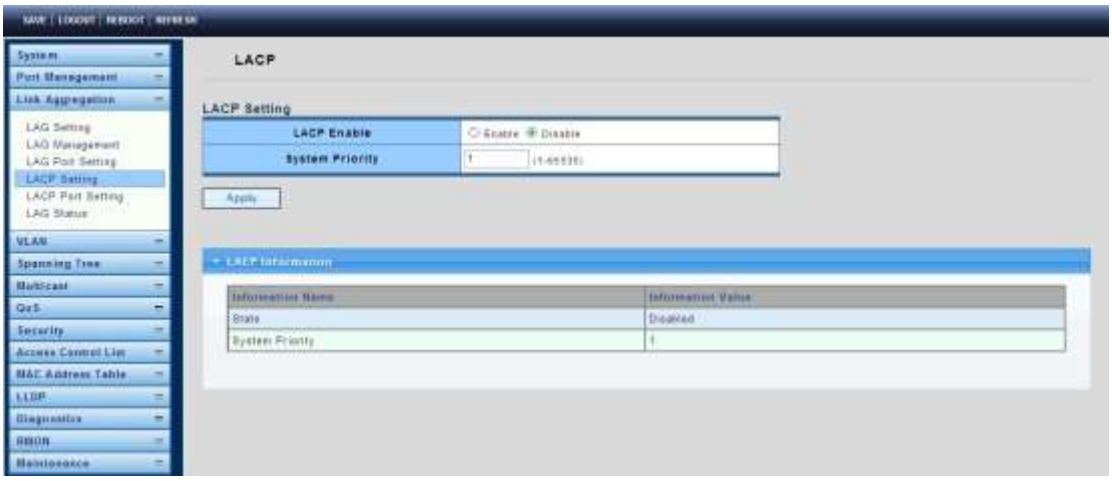
LAG Port Status

LAG	Description	Port Type	Enable State	Link Status	Speed	Duplex	FlowCtrl Config	FlowCtrl Status
LAG1			Enabled		Auto	Auto	Disabled	Disabled
LAG2			Enabled		Auto	Auto	Disabled	Disabled
LAG3			Enabled		Auto	Auto	Disabled	Disabled
LAG4			Enabled		Auto	Auto	Disabled	Disabled
LAG5			Enabled		Auto	Auto	Disabled	Disabled
LAG6			Enabled		Auto	Auto	Disabled	Disabled
LAG7			Enabled		Auto	Auto	Disabled	Disabled
LAG8			Enabled		Auto	Auto	Disabled	Disabled

4.3.4 LACP Setting

To display the LACP Setting page, click **Link Aggregation > LACP Setting.**

This page is used to configure the system priority of LACP.



LACP

LACP Setting

LACP Enable	○ Enable ● Disable
System Priority	1 (1-65535)

LACP Information

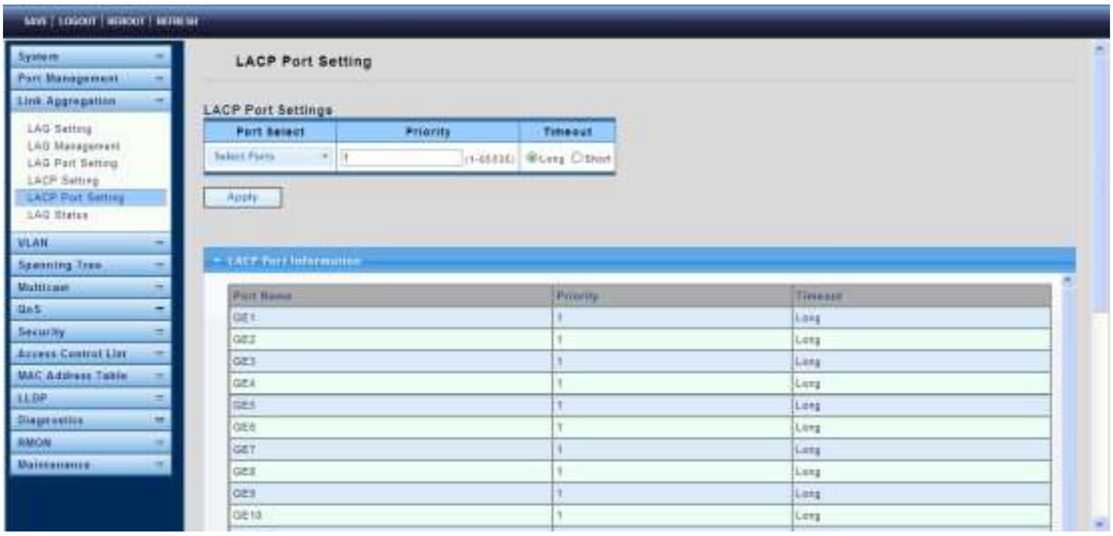
Information Name	Information Value
State	Disabled
System Priority	1

System Priority: Configure the system priority of LACP. This decides the system priority field in LACP PDU.

4.3.5 LACP Port Setting

To display the LACP Port Setting page, click **Link Aggregation > LACP Port Setting.**

This page is used to determine LACP member ports.



LACP Port Setting

LACP Port Settings

Port Select	Priority	Timeout
Select Ports	1 (1-65535)	● Long ○ Short

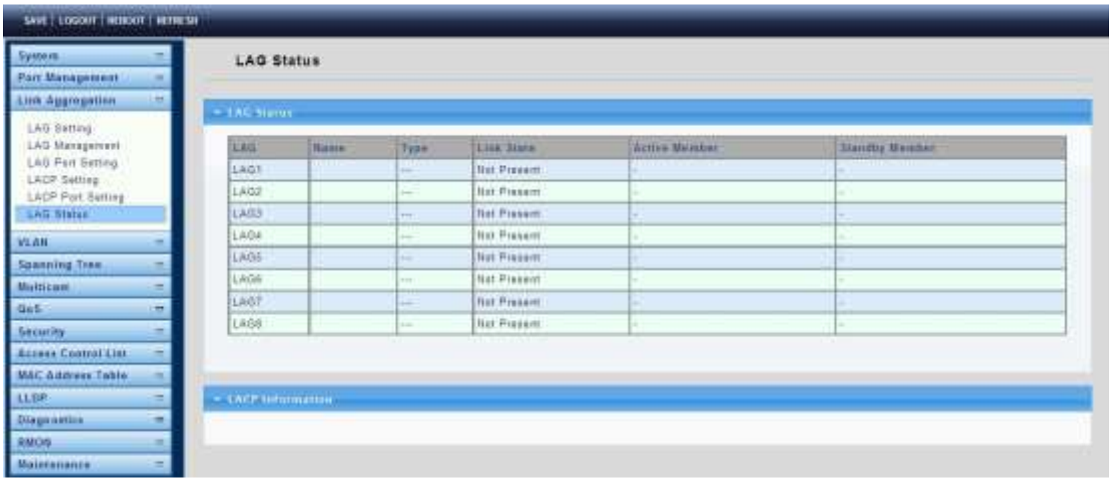
LACP Port Information

Port Name	Priority	Timeout
GE1	1	Long
GE2	1	Long
GE3	1	Long
GE4	1	Long
GE5	1	Long
GE6	1	Long
GE7	1	Long
GE8	1	Long
GE9	1	Long
GE10	1	Long

4.3.6 LAG Status

To display the LAG Status page, click **Link Aggregation > LAG Status.**

This page displays trunk information such as trunk situation, functional ports and alternative ports.



LAG Status

LAG Status

LAG	Name	Type	Link State	Active Member	Standby Member
LAG1		---	Not Present	-	-
LAG2		---	Not Present	-	-
LAG3		---	Not Present	-	-
LAG4		---	Not Present	-	-
LAG5		---	Not Present	-	-
LAG6		---	Not Present	-	-
LAG7		---	Not Present	-	-
LAG8		---	Not Present	-	-

LAG: LAG ID.

Name: LAG name.

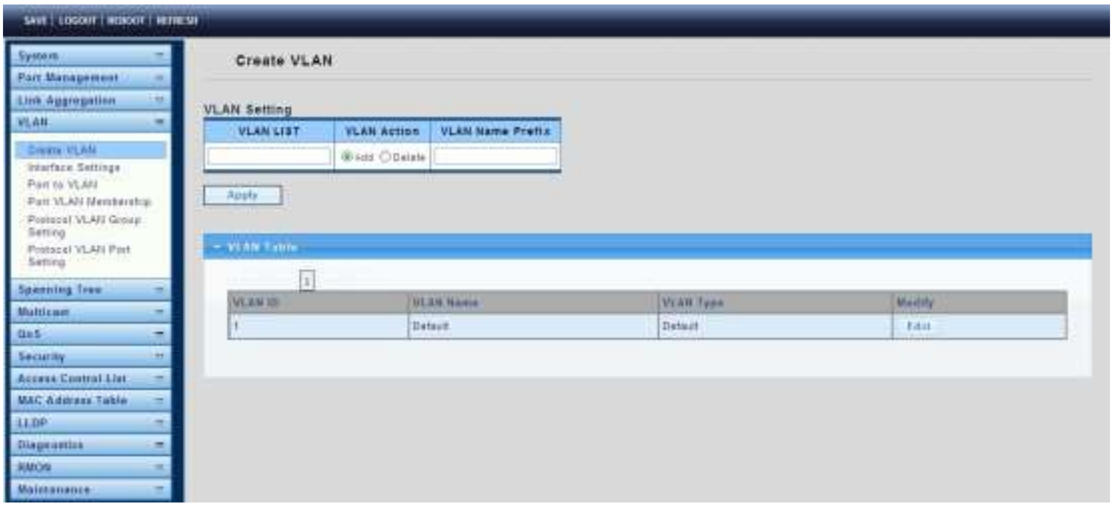
Type: The type of the LAG group: a static LAG or an LACP LAG.

4.4 VLAN

4.4.1 Create VLAN

To display the Create VLAN page, click **VLAN > Create VLAN.**

This page allows you to add, delete or edit VLAN settings.



Create VLAN

VLAN Setting

VLAN LIST	VLAN Action	VLAN Name Prefix
	● Add ○ Delete	

VLAN Table

VLAN ID	VLAN Name	VLAN Type	Modify
1	Default	Default	Edit

VLAN LIST: VLAN list for the new VLAN.

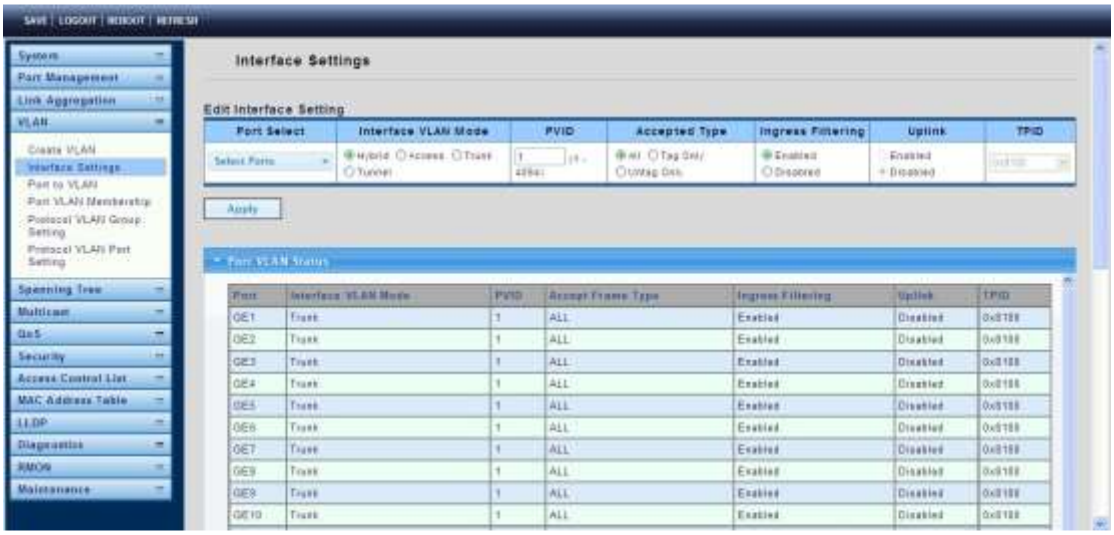
VLAN Action: Add or delete VLAN.

VLAN Name Prefix: VLAN name prefix for the new VLAN.

4.4.2 Interface Settings

To display the VLAN Interface Settings page, click **VLAN > Interface Settings.**

This page allows you to set the port type of a VLAN and manage various parameters.



Interface Settings

Edit Interface Setting

Port Select	Interface VLAN Mode	PVID	Accepted Type	Ingress Filtering	Uplink	TPID
Select Ports	● Hybrid ○ Access ○ Trunk ○ Tunnel	1 (1 - 4094)	● All ○ Tag Only ○ Untag Only	● Enabled ○ Disabled	○ Enabled ● Disabled	0x8100

Port VLAN Status

Port	Interface VLAN Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
GE1	Trunk	1	ALL	Enabled	Disabled	0x8100
GE2	Trunk	1	ALL	Enabled	Disabled	0x8100
GE3	Trunk	1	ALL	Enabled	Disabled	0x8100
GE4	Trunk	1	ALL	Enabled	Disabled	0x8100
GE5	Trunk	1	ALL	Enabled	Disabled	0x8100
GE6	Trunk	1	ALL	Enabled	Disabled	0x8100
GE7	Trunk	1	ALL	Enabled	Disabled	0x8100
GE8	Trunk	1	ALL	Enabled	Disabled	0x8100
GE9	Trunk	1	ALL	Enabled	Disabled	0x8100
GE10	Trunk	1	ALL	Enabled	Disabled	0x8100

Port Select: Select one or multiple ports to configure.

Interface VLAN Mode: VLAN port mode.

- Hybrid: Port hybrid model.
- Access: Port hybrid model.
- Trunk: Port hybrid model.
- Tunnel: Port hybrid model.

PVID: VLAN ID for the selected ports.

Accepted Type: Port accepted type.

- All: Accept tagged and untagged frames.
- Tag Only: Only accept tagged frame.
- Untag Only: Only accept untagged frame.

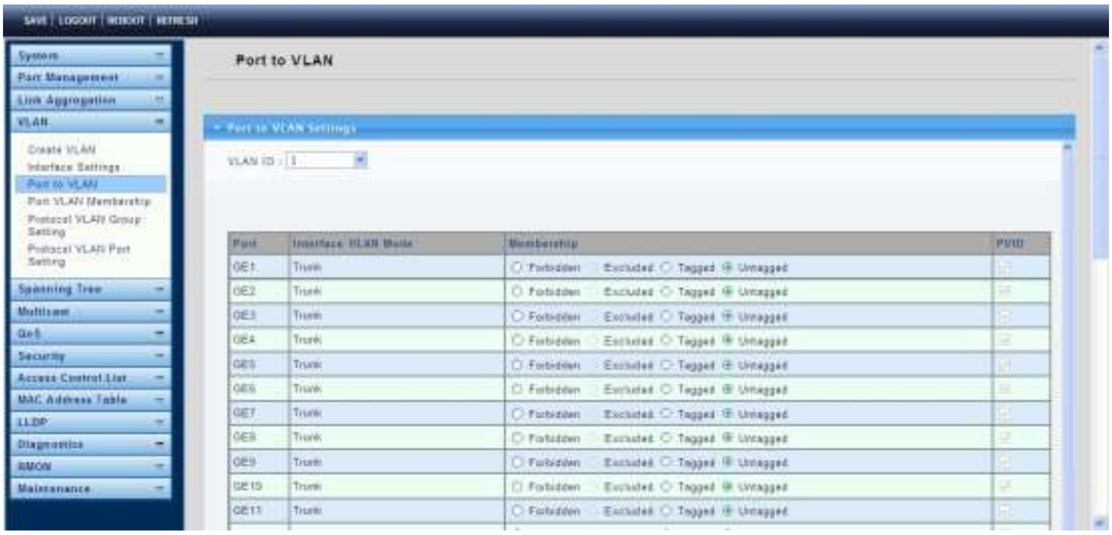
Ingress Filtering: Choose filter port open and close.

Uplink: Select port Uplink open or close.

4.4.3 Port to VLAN

To display the Port to VLAN page, click **VLAN > Port to VLAN.**

Add ports to a VLAN and select their parameters.



Port to VLAN

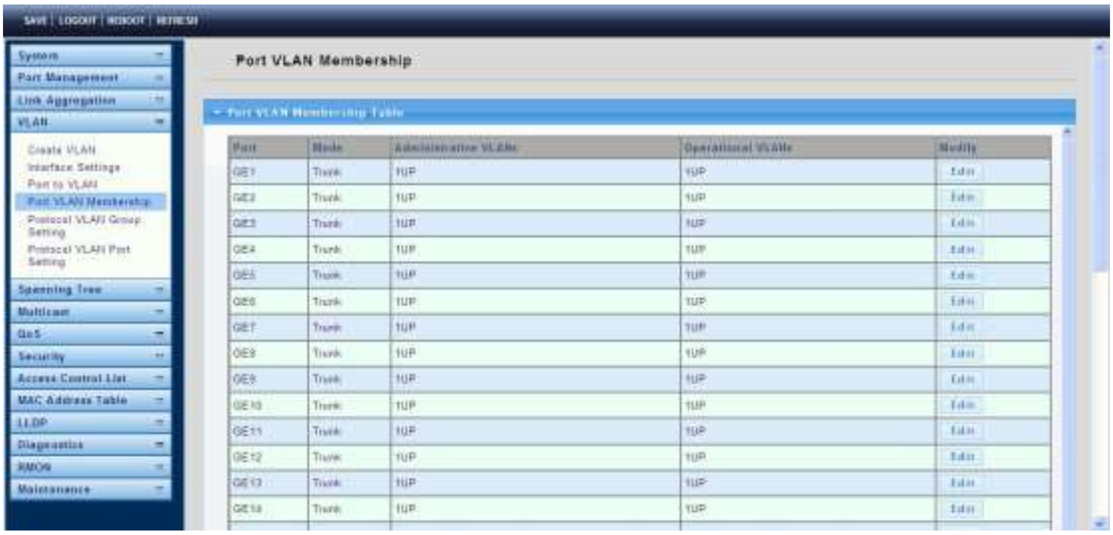
Port to VLAN Settings

VLAN ID : 1

Port	Interface VLAN Mode	Membership	PVID
GE1	Trunk	○ Forbidden Excluded ○ Tagged ● Untagged	☑
GE2	Trunk	○ Forbidden Excluded ○ Tagged ● Untagged	☑
GE3	Trunk	○ Forbidden Excluded ○ Tagged ● Untagged	☑
GE4	Trunk	○ Forbidden Excluded ○ Tagged ● Untagged	☑
GE5	Trunk	○ Forbidden Excluded ○ Tagged ● Untagged	☑
GE6	Trunk	○ Forbidden Excluded ○ Tagged ● Untagged	☑
GE7	Trunk	○ Forbidden Excluded ○ Tagged ● Untagged	☑
GE8	Trunk	○ Forbidden Excluded ○ Tagged ● Untagged	☑
GE9	Trunk	○ Forbidden Excluded ○ Tagged ● Untagged	☑
GE10	Trunk	○ Forbidden Excluded ○ Tagged ● Untagged	☑
GE11	Trunk	○ Forbidden Excluded ○ Tagged ● Untagged	☑

4.4.4 Port VLAN Membership

To display the Port VLAN Membership page, click **VLAN > Port VLAN Membership.**



Port VLAN Membership

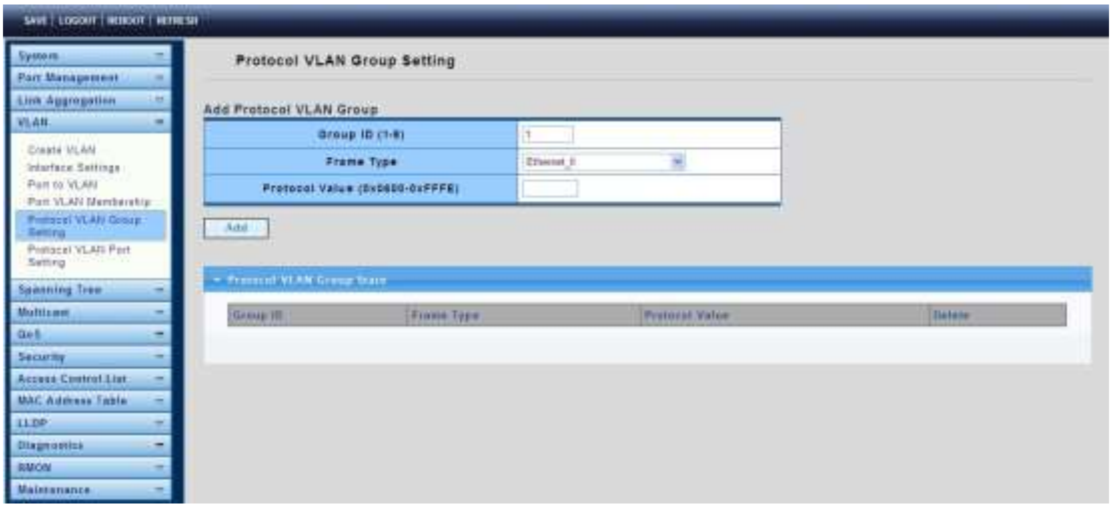
Port VLAN Membership Table

Port	Mode	Administrative VLANs	Operational VLANs	Modify
GE1	Trunk	1UP	1UP	Edit
GE2	Trunk	1UP	1UP	Edit
GE3	Trunk	1UP	1UP	Edit
GE4	Trunk	1UP	1UP	Edit
GE5	Trunk	1UP	1UP	Edit
GE6	Trunk	1UP	1UP	Edit
GE7	Trunk	1UP	1UP	Edit
GE8	Trunk	1UP	1UP	Edit
GE9	Trunk	1UP	1UP	Edit
GE10	Trunk	1UP	1UP	Edit
GE11	Trunk	1UP	1UP	Edit
GE12	Trunk	1UP	1UP	Edit
GE13	Trunk	1UP	1UP	Edit
GE14	Trunk	1UP	1UP	Edit

4.4.5 Protocol VLAN Group Setting

To display the Protocol VLAN Group Setting page, click **VLAN > Protocol VLAN Group Setting.**

The VLAN group setting lets you send the same type of message to a group within a specific VLAN.



Protocol VLAN Group Setting

Add Protocol VLAN Group

Group ID (1-8)	1
Frame Type	Ethernet_II
Protocol Value (0x0600-0xFFFE)	

Protocol VLAN Group State

Group ID	Frame Type	Protocol Value	Delete

Group ID (1-8) : Enter an ID number of the group, between 1 and 8.

Frame Type: This function maps packets to protocol-defined VLANs by examining the type octet within the packet header to discover the type of protocol associated with it.

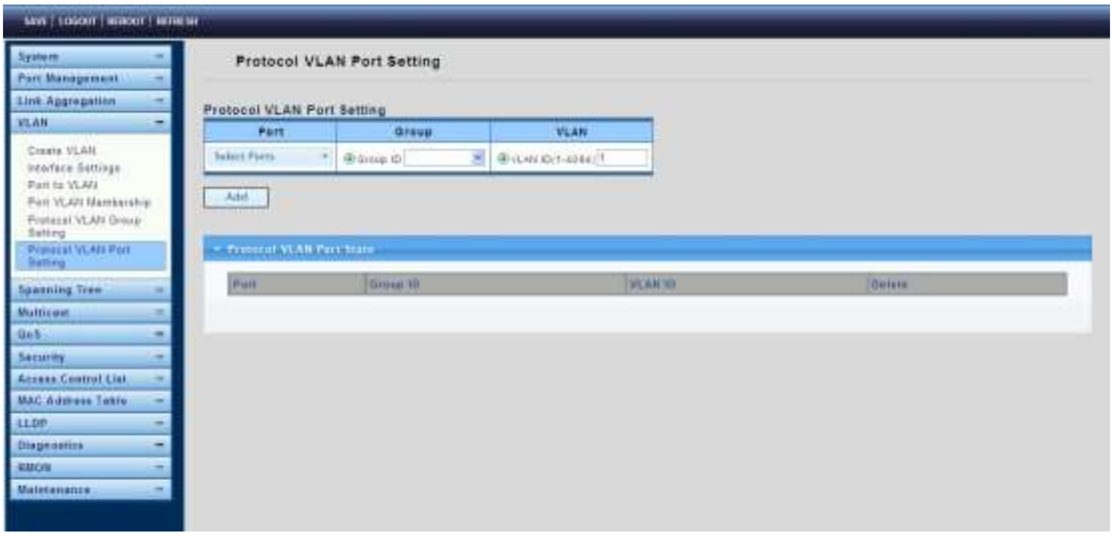
- Ethernet_II: packet type is Ethernet version 2.
- IEEE802.3_LLC_Other: packet type is 802.3 packet with LLC other header.
- RFC_1042: packet type is RFC 1042 packet.

Protocol Value (0x0600-0xFFFE): Enter the Ether type of the target protocol.

4.4.6 Protocol VLAN Port Setting

To display the Protocol VLAN Port Setting page, click **VLAN > Protocol VLAN Port Setting.**

This page is used to divide the ports into groups and map them to the VLAN.



Protocol VLAN Port Setting

Protocol VLAN Port Setting

Port	Group	VLAN
Select Ports	● Group ID	● VLAN ID(1-4094) 1

Port	Group ID	VLAN ID	Delete

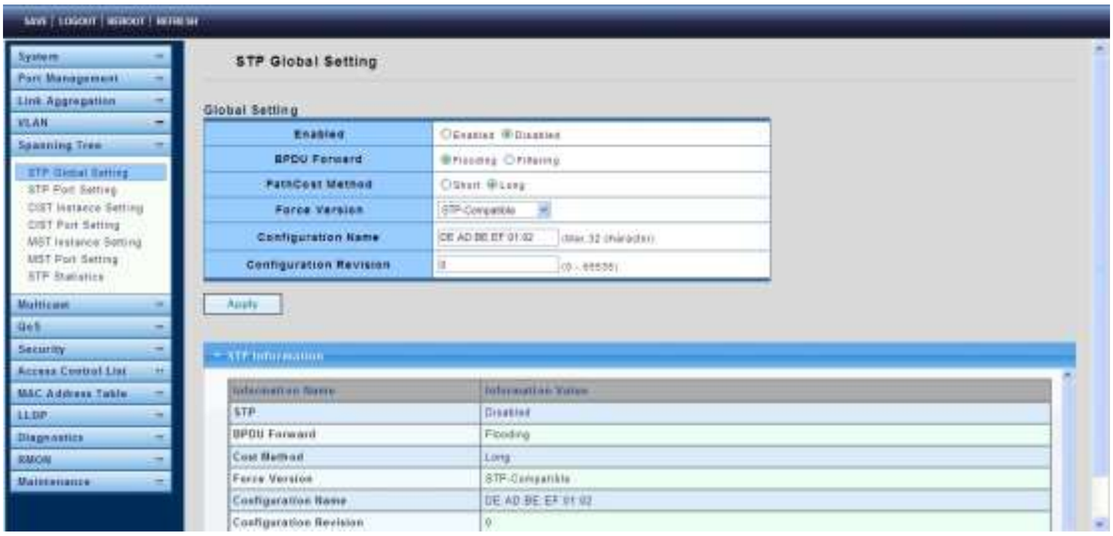
Port: Select the specified ports you wish to configure by selecting them in this list.
Group: Click the corresponding radio button to select a previously configured Group ID or Group Name.
VLAN: Click the corresponding radio button to select a previously configured VLAN ID or VLAN Name.

4.5 Spanning Tree

The Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network.

4.5.1 STP Global Setting

To display the STP Global Setting page, click **Spanning Tree > STP Global Setting.**



STP Global Setting

Global Setting

Enabled	○ Enabled ● Disabled
BPDU Forward	● Flooding ○ Filtering
PathCost Method	○ Short ● Long
Force Version	STP-Compatible
Configuration Name	DE AD BE EF 01 02 (Max. 32 characters)
Configuration Revision	0 (0 - 65535)

STP Information

Information Name	Information Value
STP	Disabled
BPDU Forward	Flooding
Cost Method	Long
Force Version	STP-Compatible
Configuration Name	DE AD BE EF 01 02
Configuration Revision	0

Enabled: Set the STP status to be enabled/disabled on the switch.
BPDU Forward: Choose BPDU packets is a flood or filtering.

Path Cost Method: Choose the path overhead is short or long.

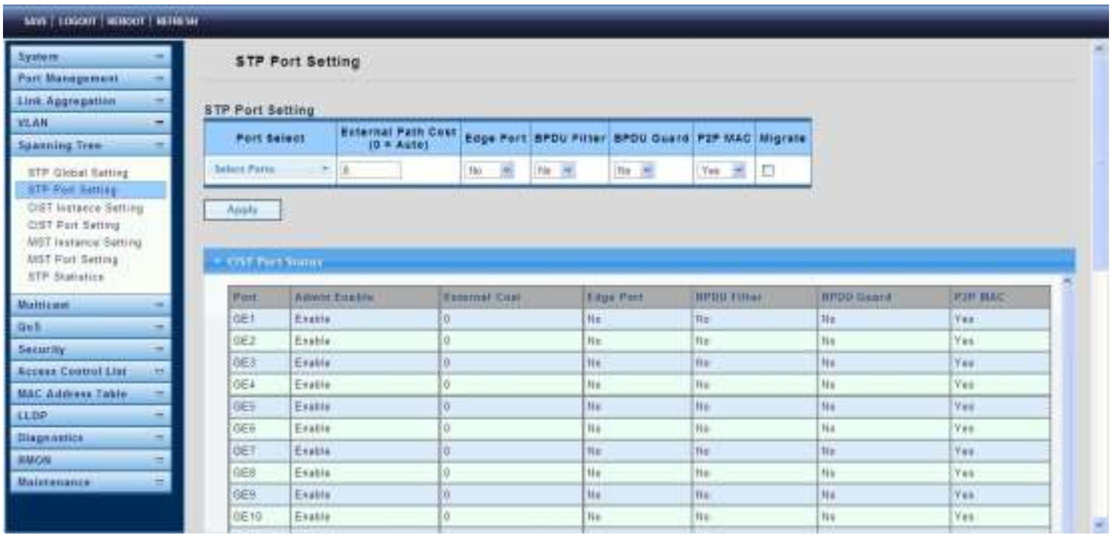
Force Version: Select the operating mode of STP.

- STP-Compatible: 802.1D STP operation.
- RSTP-Operation: 802.1w operation.
- MSTP-Operation: 802.1s operation.

Configuration Revision: Set the Revision of the Configuration Identification (range: 0-65535).

4.5.2 STP Port Setting

To display the STP Port Setting page, click **Spanning Tree > STP Port Setting.**



STP Port Setting

STP Port Setting

Port Select	External Path Cost (0 = Auto)	Edge Port	BPDU Filter	BPDU Guard	P2P MAC	Migrate
Select Ports	0	No	No	No	Yes	□

CIST Port Status

Port	Admin Enable	External Cost	Edge Port	BPDU Filter	BPDU Guard	P2P MAC
GE1	Enable	0	No	No	No	Yes
GE2	Enable	0	No	No	No	Yes
GE3	Enable	0	No	No	No	Yes
GE4	Enable	0	No	No	No	Yes
GE5	Enable	0	No	No	No	Yes
GE6	Enable	0	No	No	No	Yes
GE7	Enable	0	No	No	No	Yes
GE8	Enable	0	No	No	No	Yes
GE9	Enable	0	No	No	No	Yes
GE10	Enable	0	No	No	No	Yes

Port Select: Select the port list to specify which ports should apply this setting.
External Path Cost: Set the port's contribution. When it is the root port, the root path cost for the bridge. (0 means Auto).
Edge Port: Set the edge port configuration.

- No: Force to false state (as link to a bridge).
- Yes: Force to true state (as link to a host).

BPDU Filter: Set the BPDU Filter configuration.

- No: Disable BPDU filter function.

- Yes: Enable BPDU filter function.

To avoid transmitting BPDU from the specified ports.

BPDU Guard: Set the BPDU Guard configuration.

- No: Disable BPDU guard function.
- Yes: Enable BPDU filter function.

To drop directly the received BPDU from the specified ports.

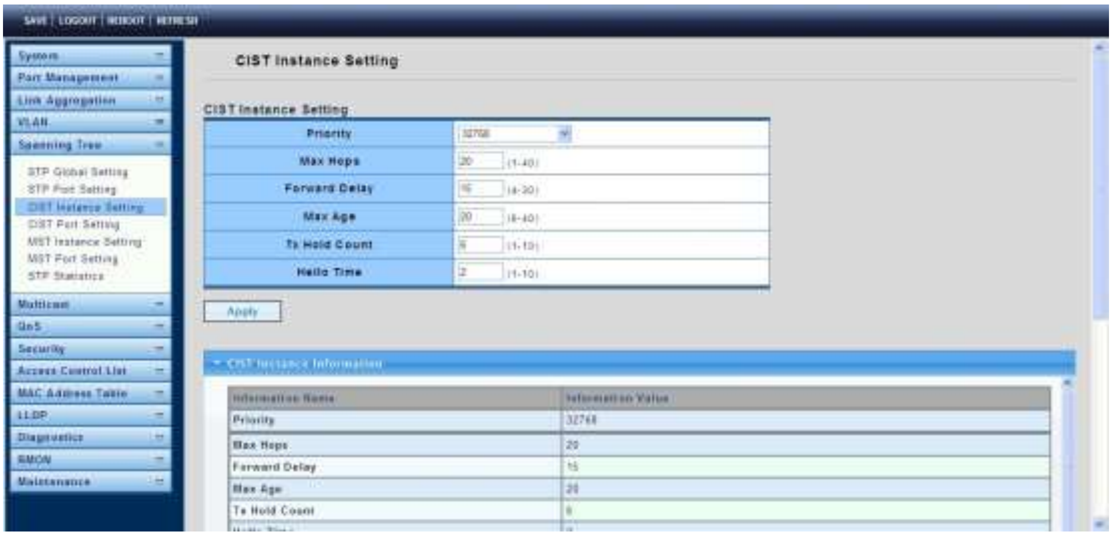
P2P MAC: Set the Point-to-Point port configuration.

- No: Force to false state.
- Yes: Force to true state.

Migrate: Forces the port to try to use the new MST/RST BPDUs, and hence to test the hypothesis that all legacy systems that do not understand the new BPDU formats have been removed from the LAN segment on the port(s).

4.5.3 CIST Instance Setting

To display the CIST Instance Setting page, click **Spanning Tree > CIST Instance Setting.**



CIST Instance Setting

CIST Instance Setting

Priority	32768
Max Hops	20 (1-40)
Forward Delay	15 (4-30)
Max Age	20 (6-40)
Tx Hold Count	6 (1-10)
Hello Time	2 (1-10)

Information Name	Information Value
Priority	32768
Max Hops	20
Forward Delay	15
Max Age	20
Tx Hold Count	6

Priority: Set the Bridge Priority in the specified CIST instance.

Max Hops: Set the value of the maximum number of hops in the region.

Forward Delay: Set the delay time an interface takes to converge from blocking state to forwarding state.

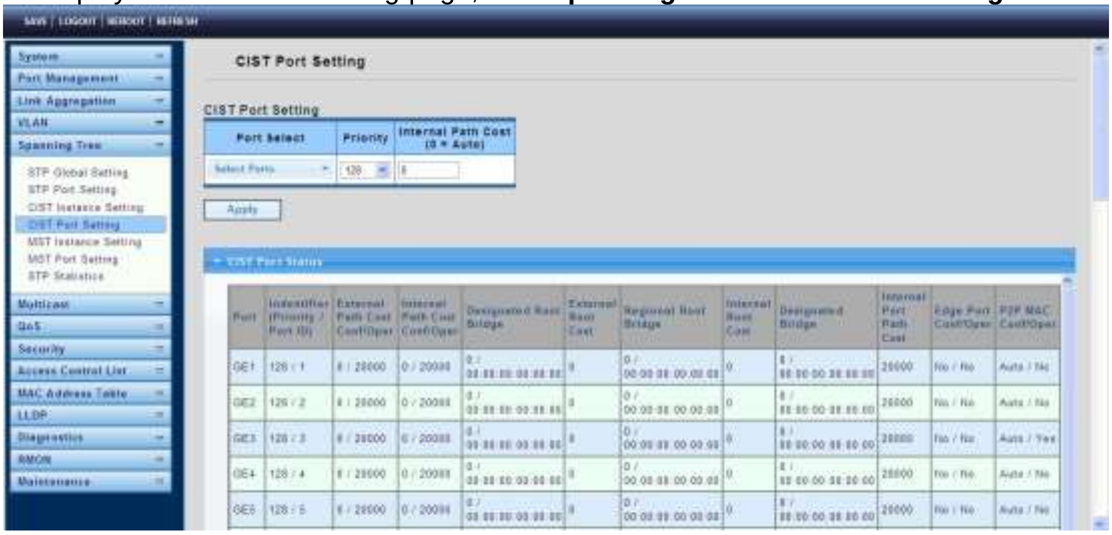
Max Age: Set the time any switch should wait before trying to change the STP topology after unhearing Hello BPDU.

Tx Hold Count: Set the Transmit Hold Count used to limit BPDIU transmission rate.

Hello Time: Set the interval between periodic transmissions of BPDU by Designated Ports.

4.5.4 CIST Port Setting

To display the CIST Port Setting page, click **Spanning Tree > CIST Port Setting.**



CIST Port Setting

CIST Port Setting

Port Select	Priority	Internal Path Cost (0 = Auto)
Select Ports	128	0

Port	Identifier (Priority / Port ID)	External Path Cost Conf/Oper	Internal Path Cost Conf/Oper	Designated Root Bridge	External Root Cost	Regional Root Bridge	Internal Root Cost	Designated Bridge	Internal Port Path Cost	Edge Port Conf/Oper	P2P MAC Conf/Oper
GE1	128 / 1	0 / 20000	0 / 20000	0 / [illegible]	0	0 / 00:00:00:00:00:00	0	0 / [illegible]	20000	No / No	Auto / No
GE2	128 / 2	0 / 20000	0 / 20000	0 / [illegible]	0	0 / 00:00:00:00:00:00	0	0 / [illegible]	20000	No / No	Auto / No
GE3	128 / 3	0 / 20000	0 / 20000	0 / [illegible]	0	0 / 00:00:00:00:00:00	0	0 / [illegible]	20000	No / No	Auto / Yes
GE4	128 / 4	0 / 20000	0 / 20000	0 / [illegible]	0	0 / 00:00:00:00:00:00	0	0 / [illegible]	20000	No / No	Auto / No
GE5	128 / 5	0 / 20000	0 / 20000	0 / [illegible]	0	0 / 00:00:00:00:00:00	0	0 / [illegible]	20000	No / No	Auto / No

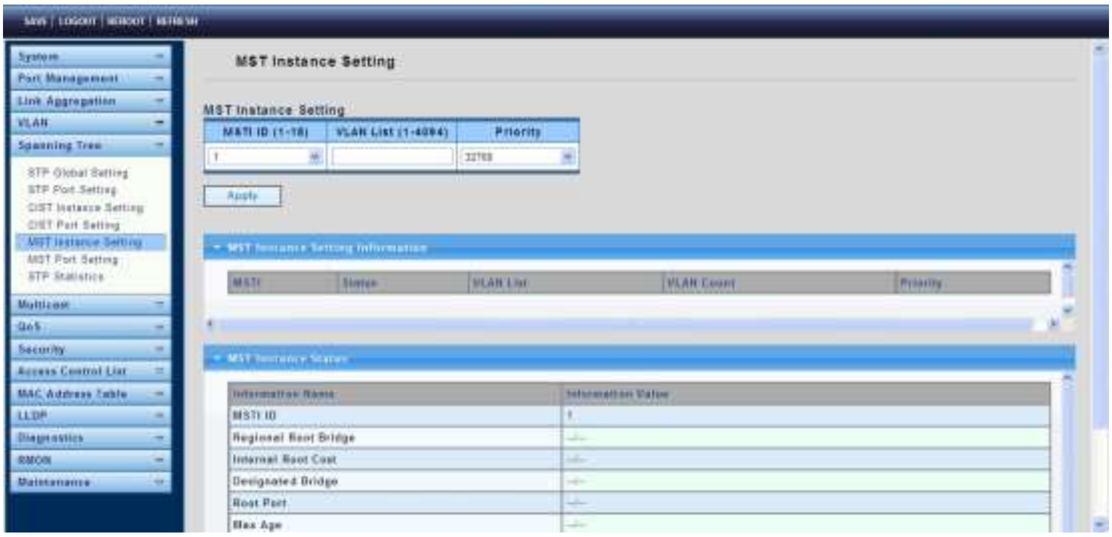
Port Select : Select the port list to specify which ports should apply this setting.

Priority: Set the Port Priority to the selected ports in the specified CIST instance.

Internal Path Cost: Set the Internal Path Cost to the selected ports in the specified CIST instance. (0 means Auto)

4.5.5 MST Instance Setting

To display the MST Instance Setting page, click **Spanning Tree > MST Instance Setting.**



MST Instance Setting

MST Instance Setting

MSTI ID (1-15)	VLAN List (1-4094)	Priority
1		32768

MSTI	Status	VLAN List	VLAN Count	Priority

Information Name	Information Value
MSTI ID	1
Regional Root Bridge	-.--
Internal Root Cost	-.--
Designated Bridge	-.--
Root Port	-.--
Max Age	-.--

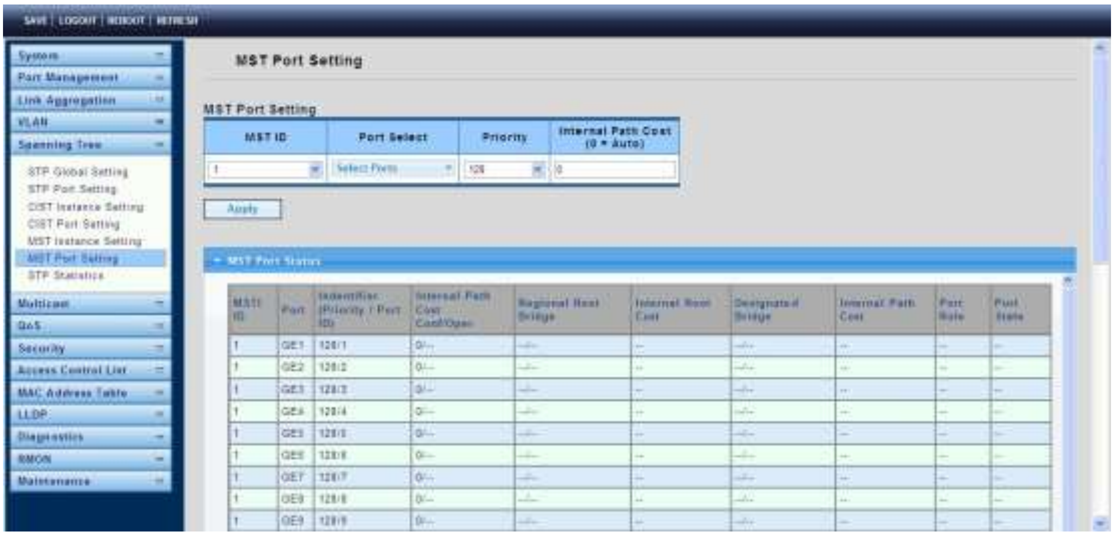
MSTI ID: Set the MSTI ID to specified the MST instance.

VLAN List: Set the VLAN List.

Priority: Set the Bridge Priority in the specified MST instance.

4.5.6 MST Port Setting

To display the MST Port Setting page, click **Spanning Tree > MST Port Setting.**



MST Port Setting

MST Port Setting

MST ID	Port Select	Priority	Internal Path Cost (0 = Auto)
1	Select Ports	128	0

MSTI ID	Port	Identifier (Priority / Port ID)	Internal Path Cost Conf/Oper	Regional Root Bridge	Internal Root Cost	Designated Bridge	Internal Path Cost	Port Role	Port State
1	GE1	128/1	0/--	--/--	--	--/--	--	--	--
1	GE2	128/2	0/--	--/--	--	--/--	--	--	--
1	GE3	128/3	0/--	--/--	--	--/--	--	--	--
1	GE4	128/4	0/--	--/--	--	--/--	--	--	--
1	GE5	128/5	0/--	--/--	--	--/--	--	--	--
1	GE6	128/6	0/--	--/--	--	--/--	--	--	--
1	GE7	128/7	0/--	--/--	--	--/--	--	--	--
1	GE8	128/8	0/--	--/--	--	--/--	--	--	--
1	GE9	128/9	0/--	--/--	--	--/--	--	--	--

MST ID: Set the MSTI ID to specify MST instance.

Port Select : Select the port list to specify which ports should apply this setting.

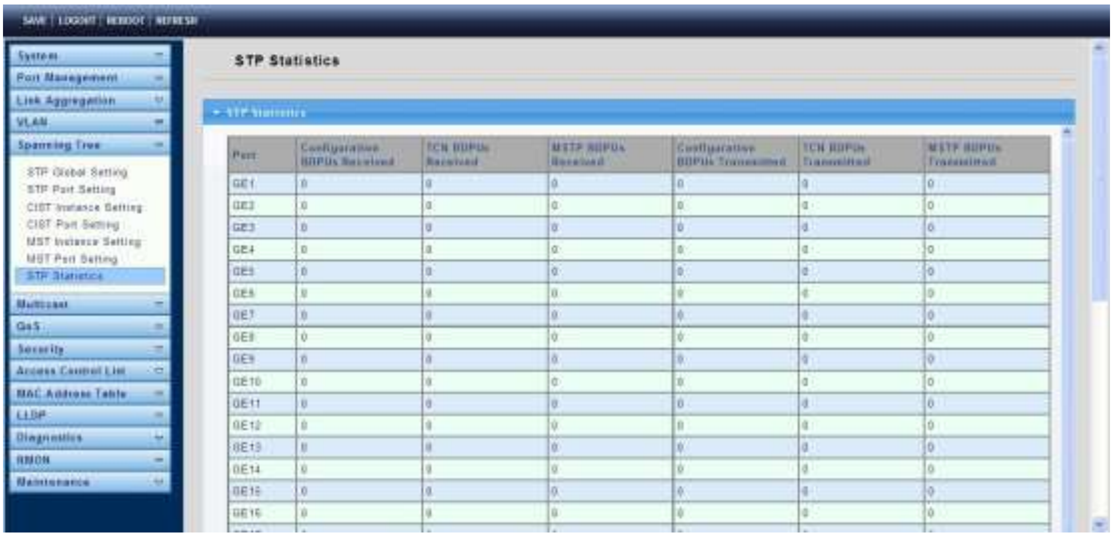
Priority: Set the Port Priority to the selected ports in the specified MST instance.

Internal Path Cost: Set the Internal Path Cost to the selected ports in the specified MST instance. (0 means Auto)

4.5.7 STP Statistics

To display the STP Statistics page, click **Spanning Tree > STP Statistics.**

This page displays each type of receiving and sending BPDUs.



STP Statistics

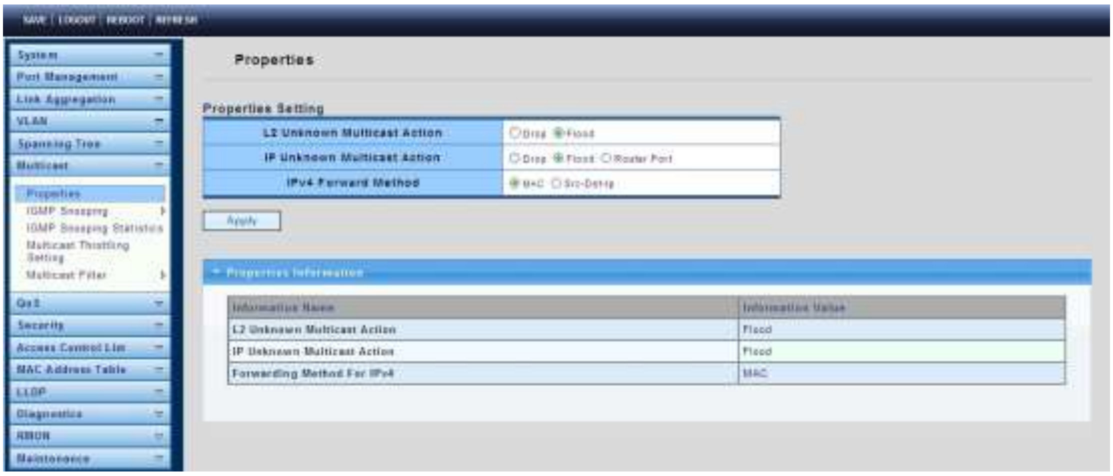
Port	Configuration BPDUs Received	TCN BDPUs Received	MSTP BDPUs Received	Configuration BDPUs Transmitted	TCN BDPUs Transmitted	MSTP BDPUs Transmitted
GE1	0	0	0	0	0	0
GE2	0	0	0	0	0	0
GE3	0	0	0	0	0	0
GE4	0	0	0	0	0	0
GE5	0	0	0	0	0	0
GE6	0	0	0	0	0	0
GE7	0	0	0	0	0	0
GE8	0	0	0	0	0	0
GE9	0	0	0	0	0	0
GE10	0	0	0	0	0	0
GE11	0	0	0	0	0	0
GE12	0	0	0	0	0	0
GE13	0	0	0	0	0	0
GE14	0	0	0	0	0	0
GE15	0	0	0	0	0	0
GE16	0	0	0	0	0	0

4.6 Multicast

4.6.1 Properties

To display the Properties page, click **Multicast > Properties.**

The Properties page enables you to configure the Bridge Multicast filtering status. It contains L2 or IP Unknown Multicast Action and ipv4 Forward Method.



Properties

Properties Setting

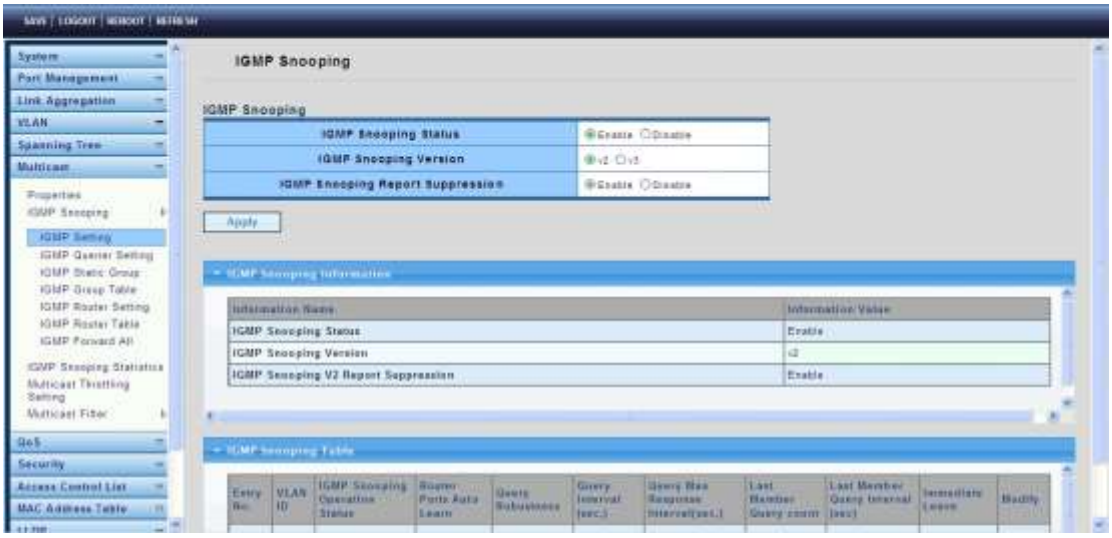
L2 Unknown Multicast Action	○ Drop ● Flood
IP Unknown Multicast Action	○ Drop ● Flood ○ Router Port
IPv4 Forward Method	● MAC ○ Src-Dst-Ip

Information Name	Information Value
L2 Unknown Multicast Action	Flood
IP Unknown Multicast Action	Flood
Forwarding Method For IPv4	MAC

4.6.2 IGMP Snooping

4.6.2.1 IGMP Setting

To display the Properties page, click **Multicast > IGMP Snooping > IGMP Setting.**



IGMP Snooping

IGMP Snooping

IGMP Snooping Status	● Enable ○ Disable
IGMP Snooping Version	● v2 ○ v3
IGMP Snooping Report Suppression	● Enable ○ Disable

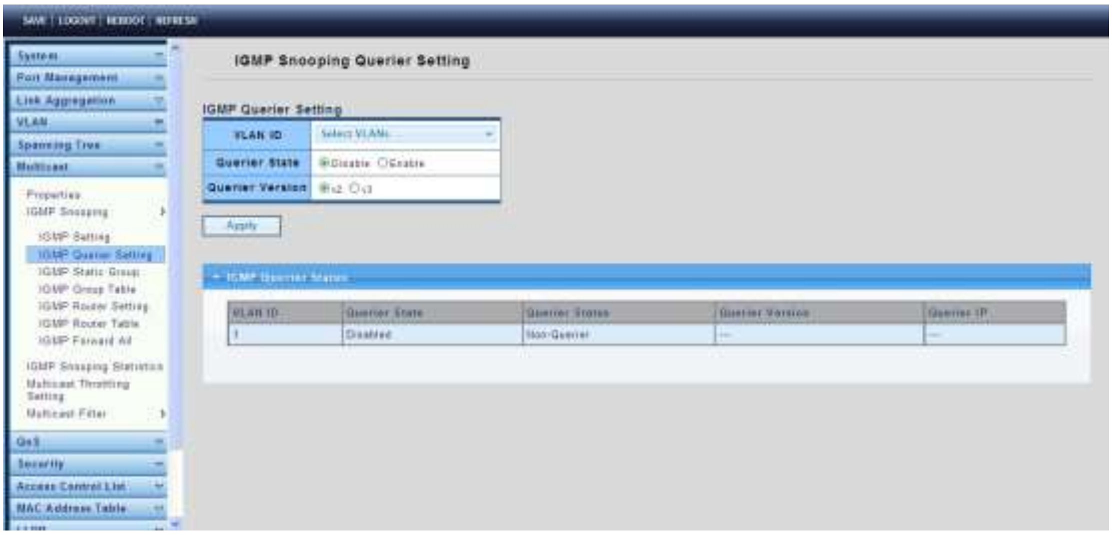
Information Name	Information Value
IGMP Snooping Status	Enable
IGMP Snooping Version	v2
IGMP Snooping V2 Report Suppression	Enable

Entry No.	VLAN ID	IGMP Snooping Operation Status	Router Ports Auto Learn	Query Robustness	Query Interval (sec.)	Query Max Response Interval(sec.)	Last Member Query count	Last Member Query Interval (sec)	Immediate Leave	Modify

IGMP Snooping Status: Enable or disable.
IGMP Snooping Version: Select the IGMP Snooping Version, IGMPv2 or IGMPv3.
IGMP Snooping Report Suppression: Enable or disable.

4.6.2.2 IGMP Querier Setting

To display the IGMP Querier Setting page, click **Multicast > IGMP Snooping > IGMP Querier Setting.**



IGMP Snooping Querier Setting

IGMP Querier Setting

VLAN ID	Select VLANs...
Querier State	● Disable ○ Enable
Querier Version	● v2 ○ v3

IGMP Querier Status

VLAN ID	Querier State	Querier Status	Querier Version	Querier IP
1	Disabled	Non-Querier	---	---

VLAN ID: Select the VLANs to configure.

Querier State: Set the enabling status of IGMP Querier Election on the chosen VLANs.

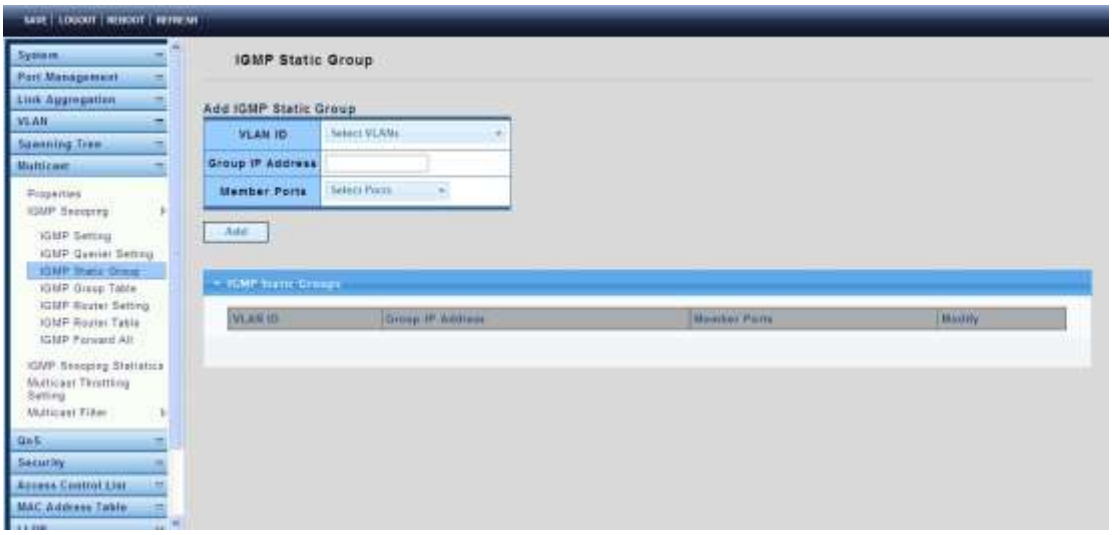
- Enable: Enable IGMP Querier Election.
- Disable: Disable IGMP Querier Election.

Version: Select the Querier Version, IGMPv2 or IGMPv3.

4.6.2.3 IGMP Static Group

To display the IGMP Static Setting page, click **Multicast > IGMP Snooping > IGMP Static Group.**

This page is used to configure specified ports as static member ports.



IGMP Static Group

Add IGMP Static Group

VLAN ID	Select VLANs
Group IP Address	
Member Ports	Select Ports

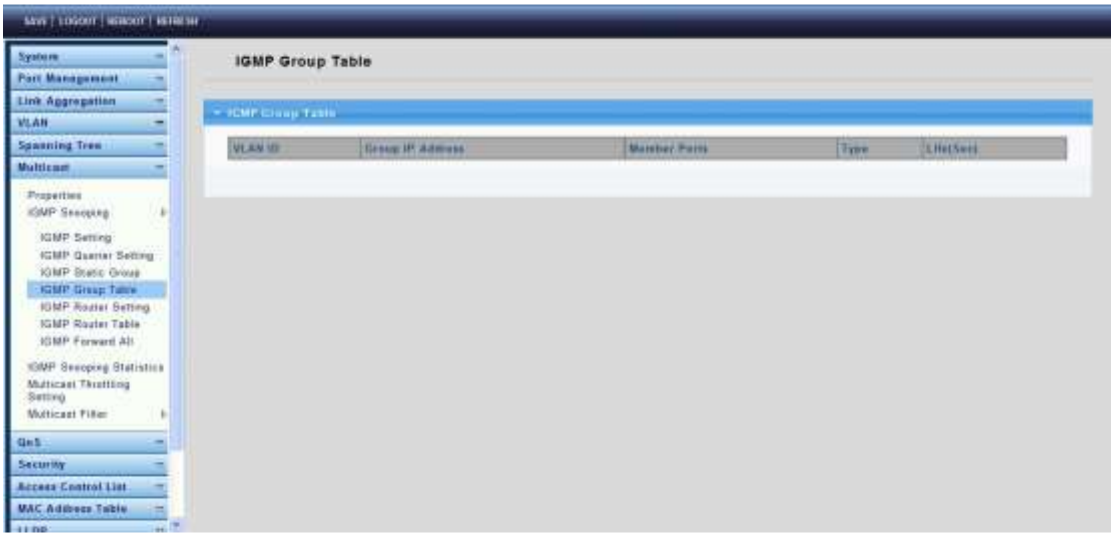
IGMP Static Groups

VLAN ID	Group IP Address	Member Ports	Modify

4.6.2.4 IGMP Group Table

To display the IGMP Group Table page, click **Multicast > IGMP Snooping > IGMP Group Table.**

This page is used to display IGMP Group Table statistics information.



IGMP Group Table

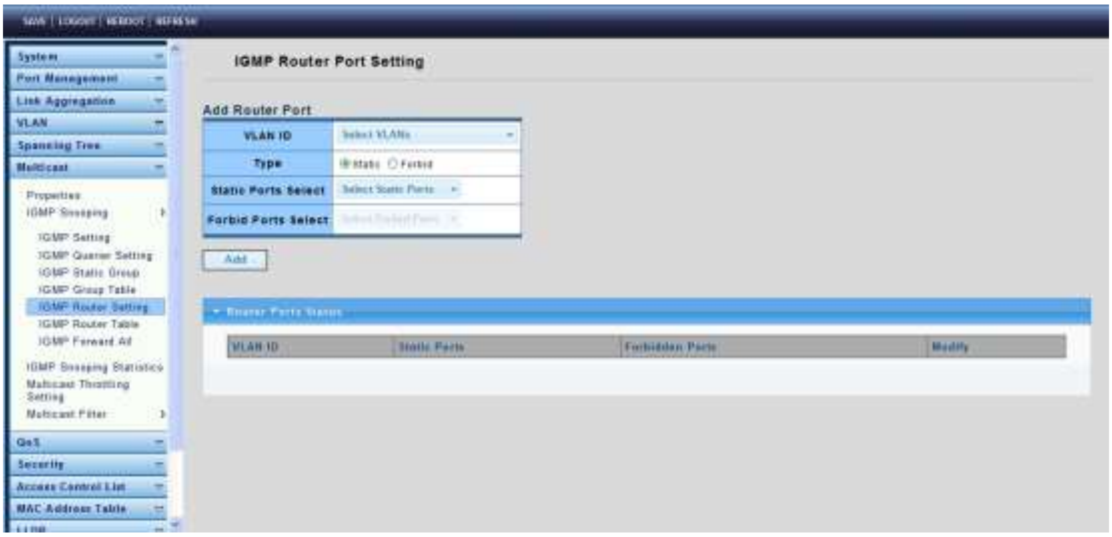
▾ IGMP Group Table

VLAN ID	Group IP Address	Member Ports	Type	Life(Sec)

4.6.2.5 IGMP Router Setting

To display the IGMP Router Port Setting page, click **Multicast > IGMP Snooping > IGMP Router Setting.**

This page is used to configure specified ports as static route ports.



IGMP Router Port Setting

Add Router Port

VLAN ID	Select VLANs
Type	● Static ○ Forbid
Static Ports Select	Select Static Ports
Forbid Ports Select	Select Forbid Ports

Add

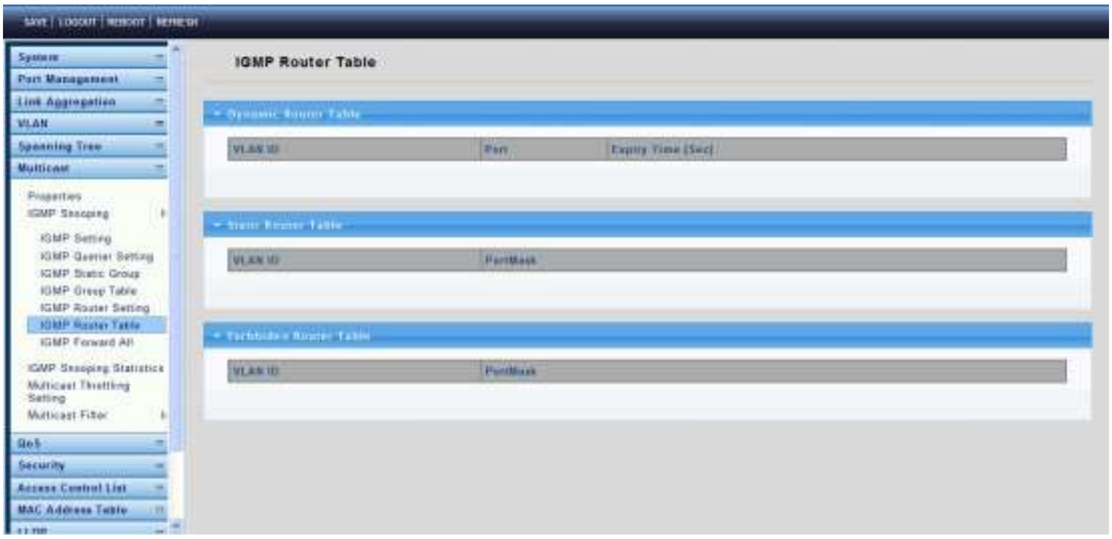
▾ Router Ports Status

VLAN ID	Static Ports	Forbidden Ports	Modify

4.6.2.6 IGMP Router Table

To display IGMP Router Table web page, click **Multicast > IGMP Snooping > IGMP Router Table**

This page is used to display IGMP Router Table statistics information.



IGMP Router Table

Dynamic Router Table

VLAN ID	Port	Expiry Time (Sec)

Static Router Table

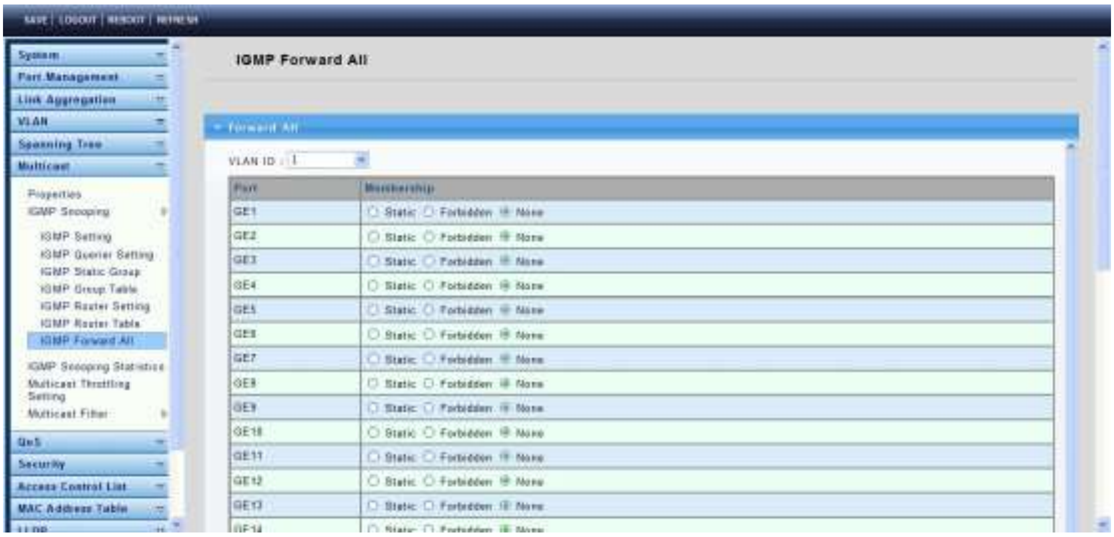
VLAN ID	PortMask

Forbidden Router Table

VLAN ID	PortMask

4.6.2.7 IGMP Forward All

To display IGMP Forward All web page, click **Multicast > IGMP Snooping > IGMP Forward All**



IGMP Forward All

Forward All

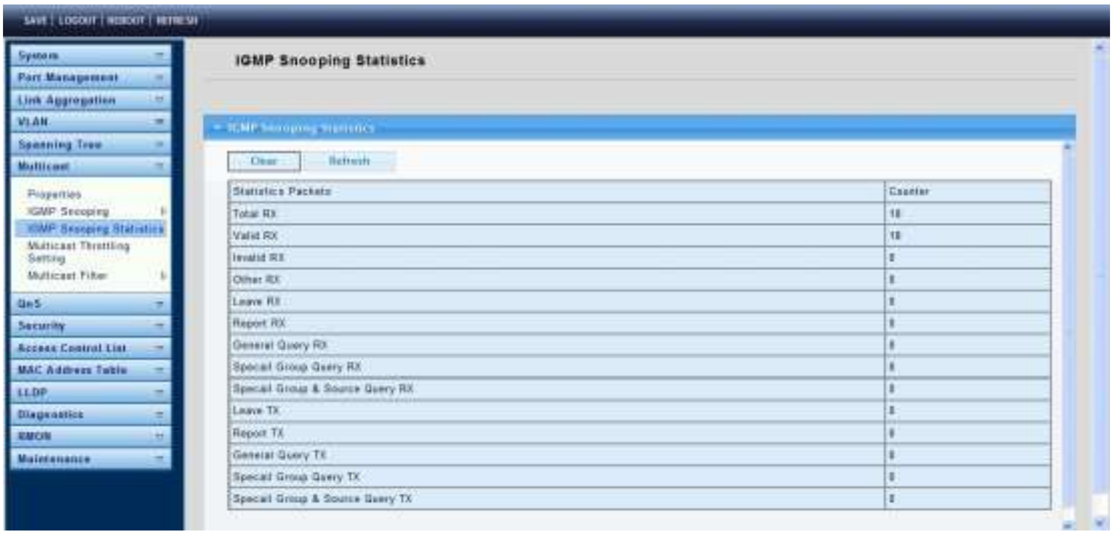
VLAN ID : 1

Port	Membership
GE1	○ Static ○ Forbidden ● None
GE2	○ Static ○ Forbidden ● None
GE3	○ Static ○ Forbidden ● None
GE4	○ Static ○ Forbidden ● None
GE5	○ Static ○ Forbidden ● None
GE6	○ Static ○ Forbidden ● None
GE7	○ Static ○ Forbidden ● None
GE8	○ Static ○ Forbidden ● None
GE9	○ Static ○ Forbidden ● None
GE10	○ Static ○ Forbidden ● None
GE11	○ Static ○ Forbidden ● None
GE12	○ Static ○ Forbidden ● None
GE13	○ Static ○ Forbidden ● None
GE14	○ Static ○ Forbidden ● None

4.6.3 IGMP Snooping Statistics

To display the IGMP Snooping Statistics page, click **Multicast > IGMP Snooping Statistics.**

This page is used to display IGMP Snooping statistics information.



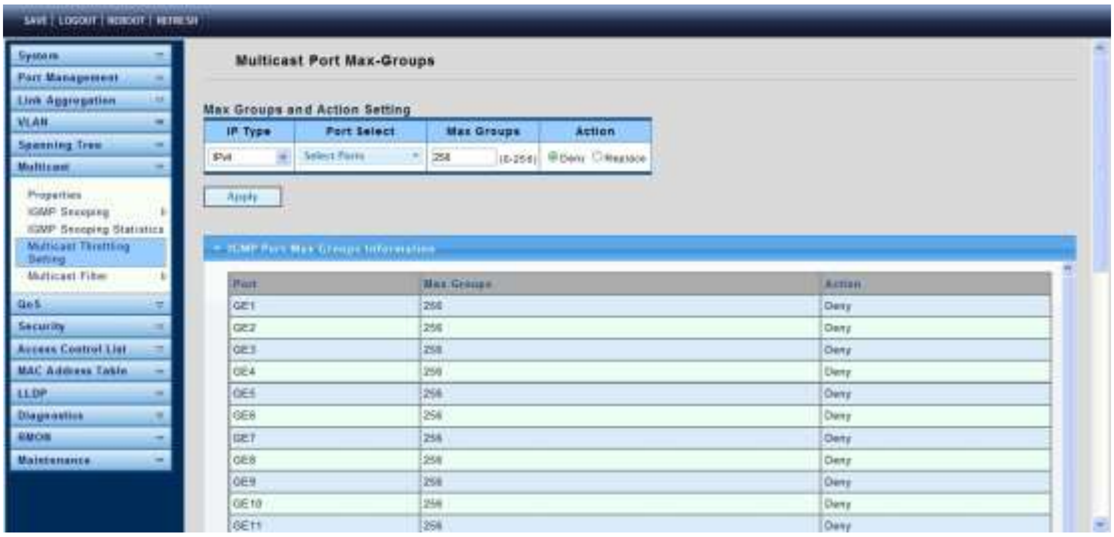
IGMP Snooping Statistics

Statistics Packets	Counter
Total RX	18
Valid RX	18
Invalid RX	0
Other RX	0
Leave RX	0
Report RX	0
General Query RX	0
Special Group Query RX	0
Special Group & Source Query RX	0
Leave TX	0
Report TX	0
General Query TX	0
Special Group Query TX	0
Special Group & Source Query TX	0

4.6.4 Multicast Throttling Setting

To display the Multicast Throttling Setting page, click **Multicast > Multicast Throttling Setting.**

This page allows you to set Multicast Port Max-Groups to limit a port's bandwidth and to select Multicast Action.



Multicast Port Max-Groups

Max Groups and Action Setting

IP Type	Port Select	Max Groups	Action
IPv4	Select Ports	256 (0-256)	● Deny ○ Replace

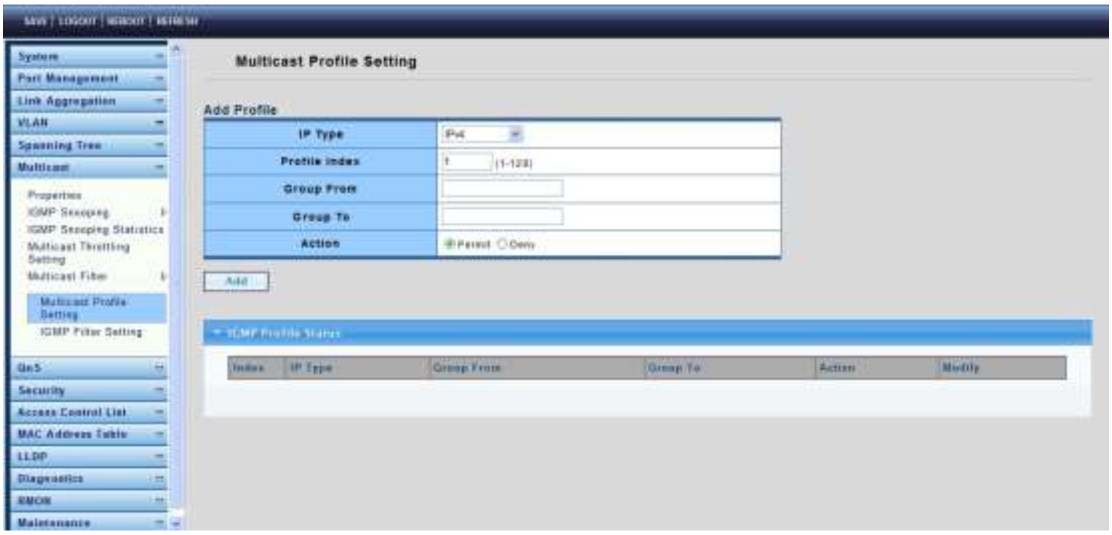
Port	Max Groups	Action
GE1	256	Deny
GE2	256	Deny
GE3	256	Deny
GE4	256	Deny
GE5	256	Deny
GE6	256	Deny
GE7	256	Deny
GE8	256	Deny
GE9	256	Deny
GE10	256	Deny
GE11	256	Deny

4.6.5 Multicast Filter

4.6.5.1 Multicast Profile Setting

The Multicast Filter Profile Settings page allows you to add a profile to which multicast address(es) reports are to be received on specified ports on the switch. This function will therefore limit the number of reports received and the number of multicast groups configured on the switch. You may set an IP Multicast address or a range of IP Multicast addresses to accept reports (Permit) that come into the specified switch ports.

To display the Multicast Profile Setting page, click **Multicast > Multicast Filter > Multicast Profile Setting.**



Multicast Profile Setting

Add Profile

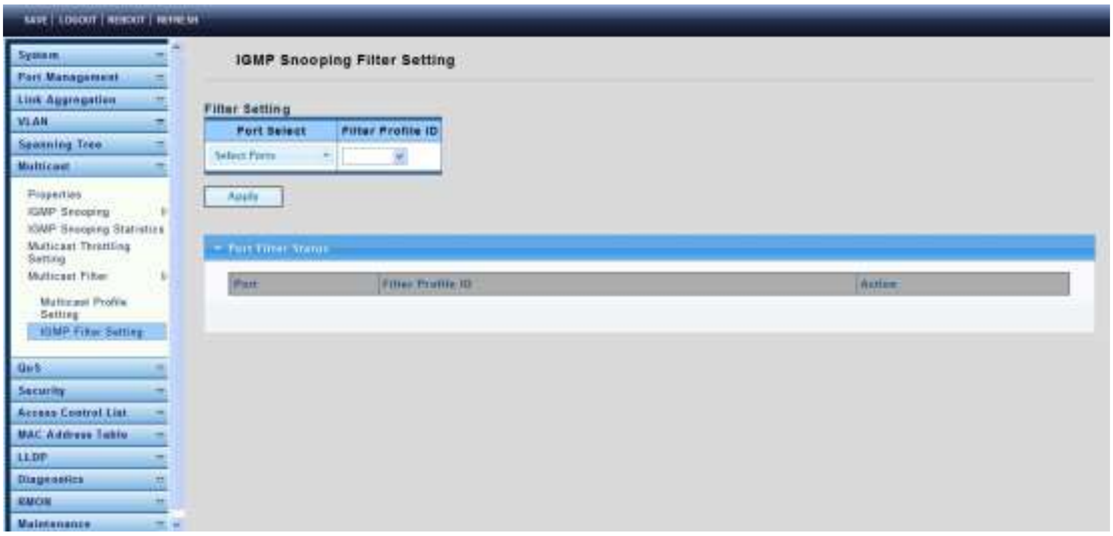
IP Type	IPv4
Profile Index	1 (1-128)
Group From	
Group To	
Action	● Permit ○ Deny

Index	IP Type	Group From	Group To	Action	Modify

4.6.5.2 IGMP Filter Setting

To display the IGMP Filter Setting page, click **Multicast > Multicast Filter > IGMP Filter Setting.**

This page is used to set filters on a port.



IGMP Snooping Filter Setting

Filter Setting

Port Select	Filter Profile ID
Select Ports	

Port	Filter Profile ID	Action

4.7 QoS

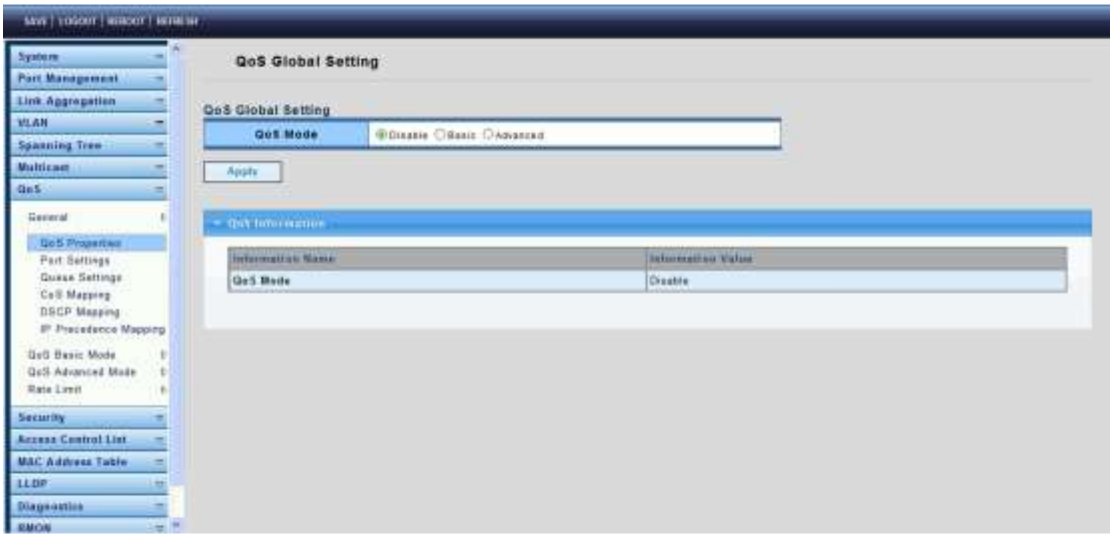
Use the QoS pages to configure settings for the switch QoS interface and how the switch connects to a remote server to get services.

4.7.1 General

4.7.1.1 QoS Properties

To display the QoS properties page, click **QoS > General > QoS properties.**

This page allows you to set the QoS mode: basic or advanced.



QoS Global Setting

QoS Global Setting

QoS Mode	● Disable ○ Basic ○ Advanced

Apply

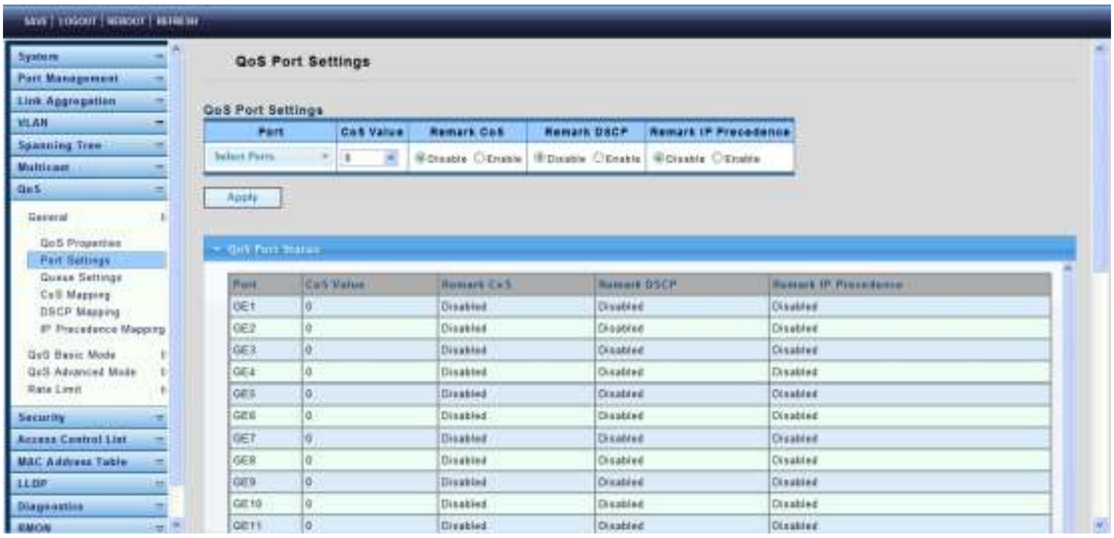
QoS Information

Information Name	Information Value
QoS Mode	Disable

4.7.1.2 Port Settings

To display the Port Settings page, click **QoS > General > Port Settings.**

This page is used to configure various QoS parameters.



QoS Port Settings

QoS Port Settings

Port	CoS Value	Remark CoS	Remark DSCP	Remark IP Precedence
Select Ports	0	● Disable ○ Enable	● Disable ○ Enable	● Disable ○ Enable

Apply

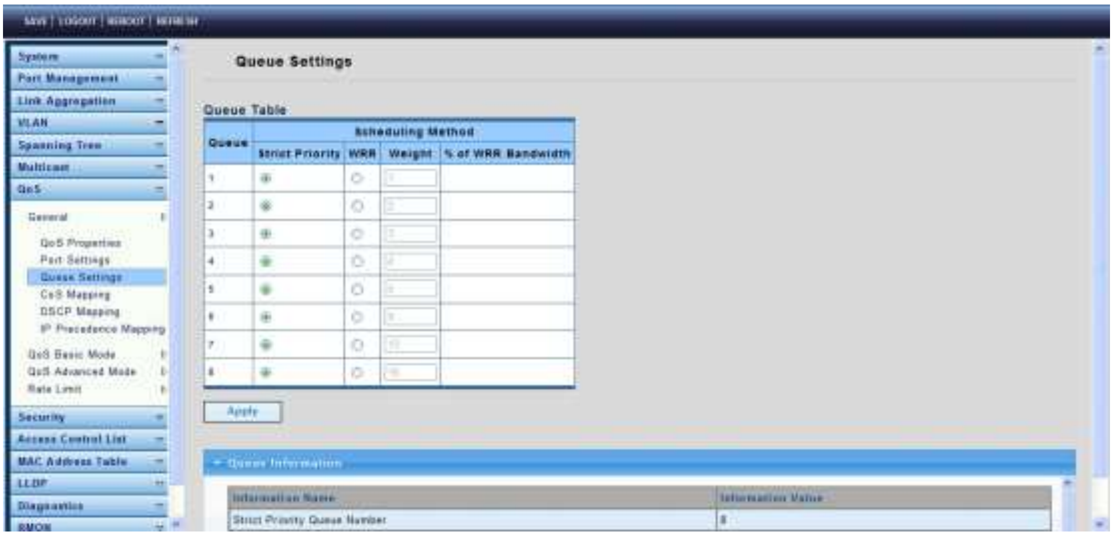
QoS Port Status

Port	CoS Value	Remark CoS	Remark DSCP	Remark IP Precedence
GE1	0	Disabled	Disabled	Disabled
GE2	0	Disabled	Disabled	Disabled
GE3	0	Disabled	Disabled	Disabled
GE4	0	Disabled	Disabled	Disabled
GE5	0	Disabled	Disabled	Disabled
GE6	0	Disabled	Disabled	Disabled
GE7	0	Disabled	Disabled	Disabled
GE8	0	Disabled	Disabled	Disabled
GE9	0	Disabled	Disabled	Disabled
GE10	0	Disabled	Disabled	Disabled
GE11	0	Disabled	Disabled	Disabled

4.7.1.3 Queue Settings

To display the Queue Setting page, click **QoS > General > Queue Settings.**

This page allows you to set the QoS queue scheduling methods.



Queue Settings

Queue Table

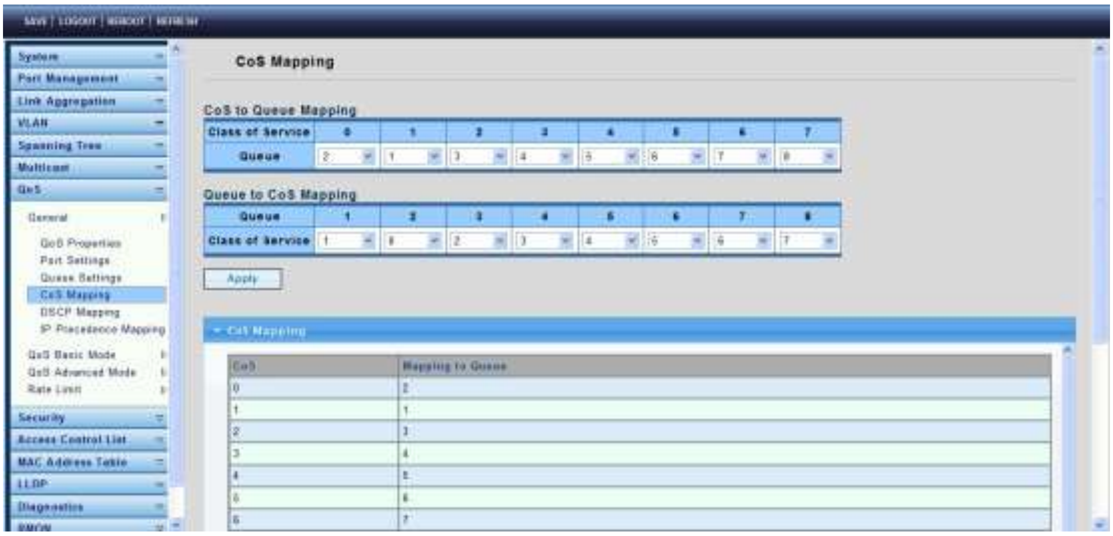
Queue	Scheduling Method			
	Strict Priority	WRR	Weight	% of WRR Bandwidth
1	●	○	1	
2	●	○	2	
3	●	○	3	
4	●	○	4	
5	●	○	5	
6	●	○	6	
7	●	○	[illegible]	
8	●	○	[illegible]	

Information Name	Information Value
Strict Priority Queue Number	8

4.7.1.4 COS Mapping

To display the COS Mapping page, click **QoS > General > COS Mapping.**

The page allows you to apply COS Mapping.



CoS Mapping

CoS to Queue Mapping

Class of Service	0	1	2	3	4	5	6	7
Queue	2	1	3	4	5	6	7	8

Queue to CoS Mapping

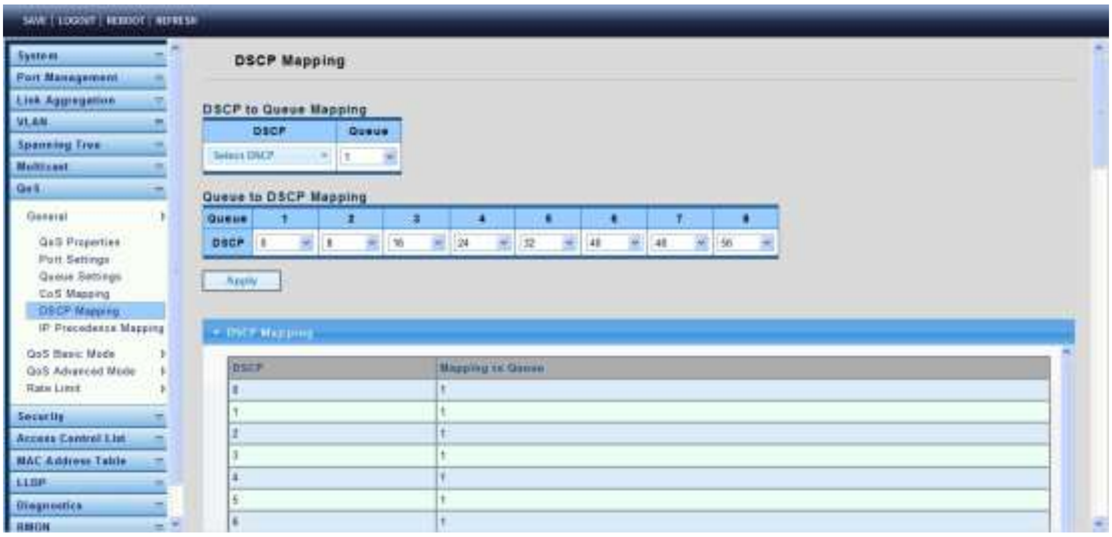
Queue	1	2	3	4	5	6	7	8
Class of Service	1	0	2	3	4	5	6	7

CoS	Mapping to Queue
0	2
1	1
2	3
3	4
4	5
5	6
6	7

4.7.1.5 DSCP Mapping

To display the DSCP Mapping page, click **QoS > General > DSCP Mapping.**

The page allows you to set DSCP Mapping.



DSCP Mapping

DSCP to Queue Mapping

DSCP	Queue
Select DSCP	1

Queue to DSCP Mapping

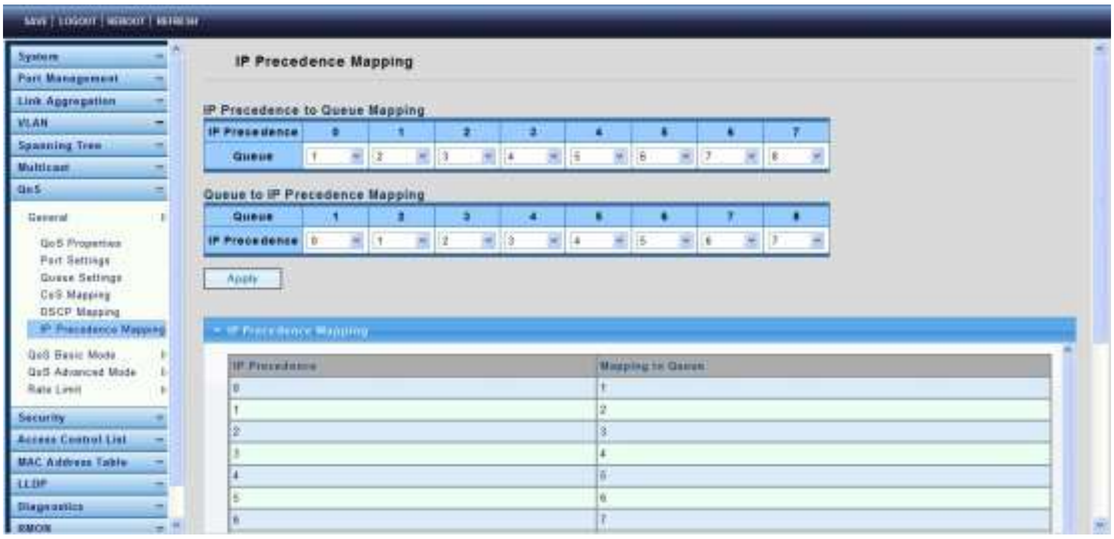
Queue	1	2	3	4	5	6	7	8
DSCP	0	8	16	24	32	40	48	56

DSCP	Mapping to Queue
0	1
1	1
2	1
3	1
4	1
5	1
6	1

4.7.1.6 IP Precedence Mapping

To display the IP Precedence Mapping page, click **QoS > General > IP Precedence Mapping.**

The page allows you to set IP Precedence Mapping.



IP Precedence Mapping

IP Precedence to Queue Mapping

IP Precedence	0	1	2	3	4	5	6	7
Queue	1	2	3	4	5	6	7	8

Queue to IP Precedence Mapping

Queue	1	2	3	4	5	6	7	8
IP Precedence	0	1	2	3	4	5	6	7

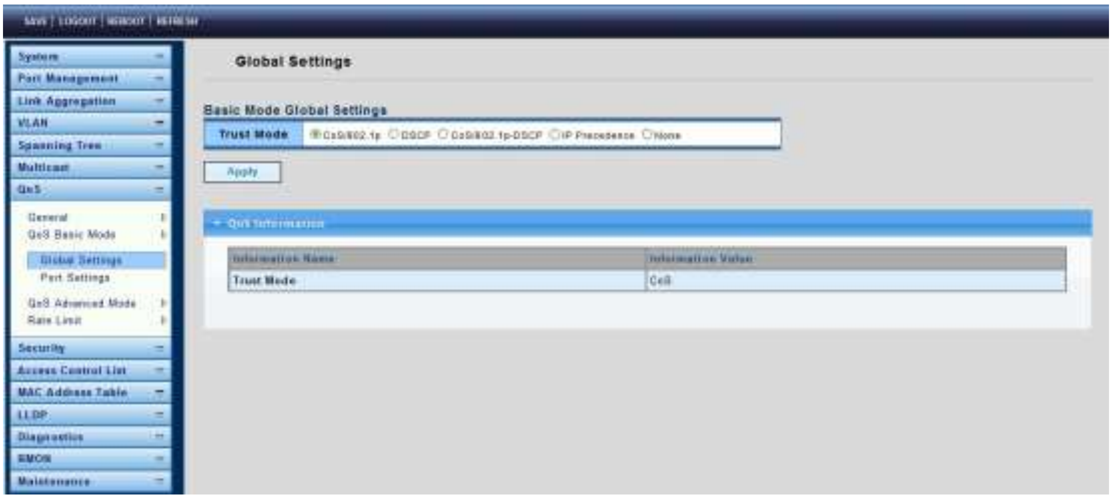
IP Precedence	Mapping to Queue
0	1
1	2
2	3
3	4
4	5
5	6
6	7

4.7.2 QoS Basic Mode

4.7.2.1 Global Settings

To display the Global Settings page, click **QoS > QoS Basic Mode > Global Settings.**

This page allows you to set the QoS for trust mode on basic mode global settings.



Global Settings

Basic Mode Global Settings

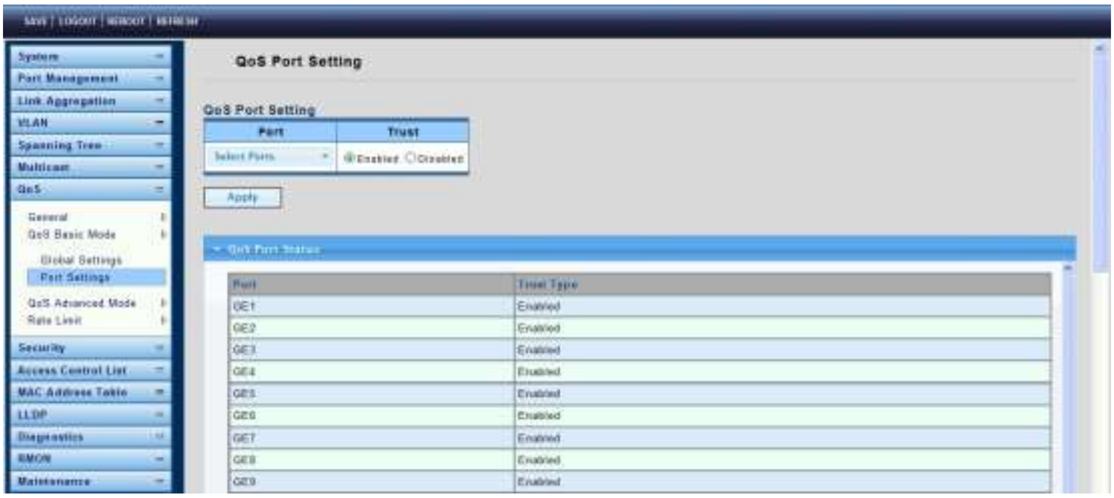
Trust Mode: ● CoS/802.1p ○ DSCP ○ CoS/802.1p-DSCP ○ IP Precedence ○ None

Information Name	Information Value
Trust Mode	CoS

4.7.2.2 Port Settings

To display the Port Settings page, click **QoS > QoS Basic Mode > Port Settings.**

This page allows you to revise QoS Port Setting selections.



QoS Port Setting

QoS Port Setting

Port	Trust
Select Ports	● Enabled ○ Disabled

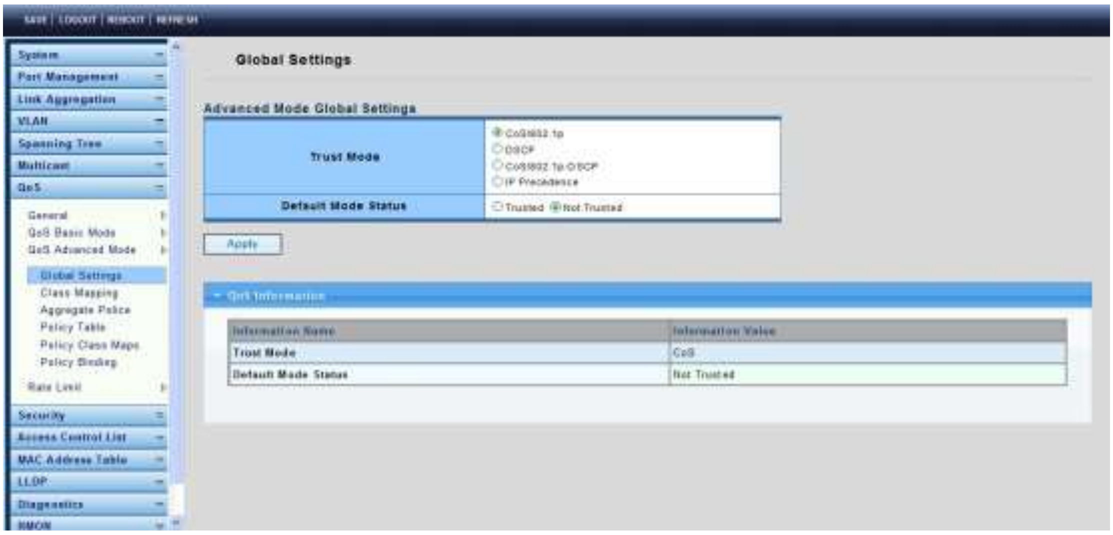
Port	Trust Type
GE1	Enabled
GE2	Enabled
GE3	Enabled
GE4	Enabled
GE5	Enabled
GE6	Enabled
GE7	Enabled
GE8	Enabled
GE9	Enabled

4.7.3 QoS Advanced Mode

4.7.3.1 Global Settings

To display the Global Settings page, click **QoS > QoS Advanced Mode > Global Settings.**

This page allows you to set the default QoS mode state under advanced mode global settings trust mode.



Global Settings

Advanced Mode Global Settings

Trust Mode	● CoS/802.1p ○ DSCP ○ CoS/802.1p-DSCP ○ IP Precedence
Default Mode Status	○ Trusted ● Not Trusted

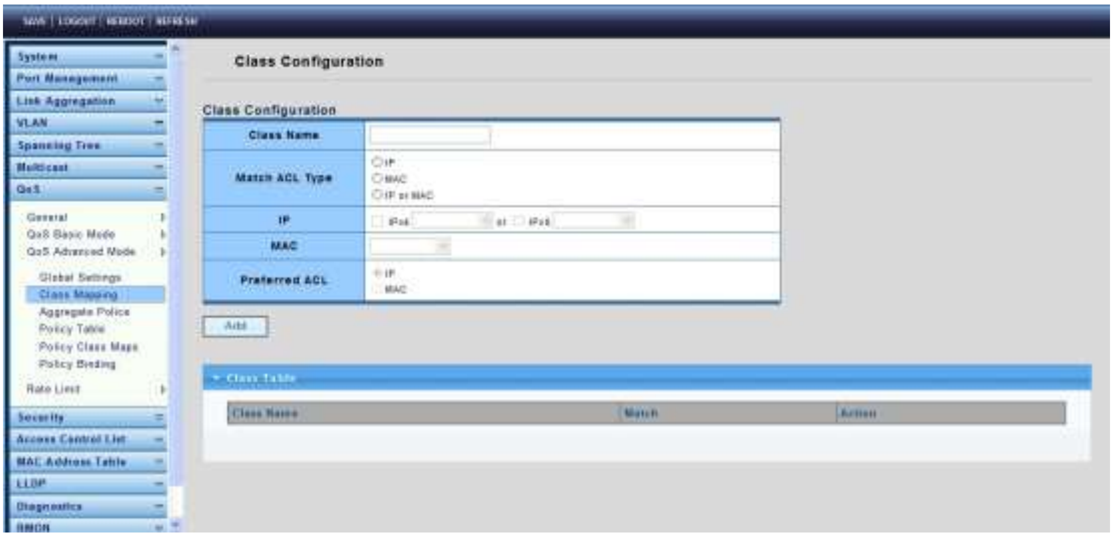
QoS Information

Information Name	Information Value
Trust Mode	CoS
Default Mode Status	Not Trusted

4.7.3.2 Class Mapping

To display the Class Mapping page, click **QoS > QoS Advanced Mode > Class Mapping.**

This page allows you to create a QoS class, which is used to link the ACL.



Class Configuration

Class Configuration

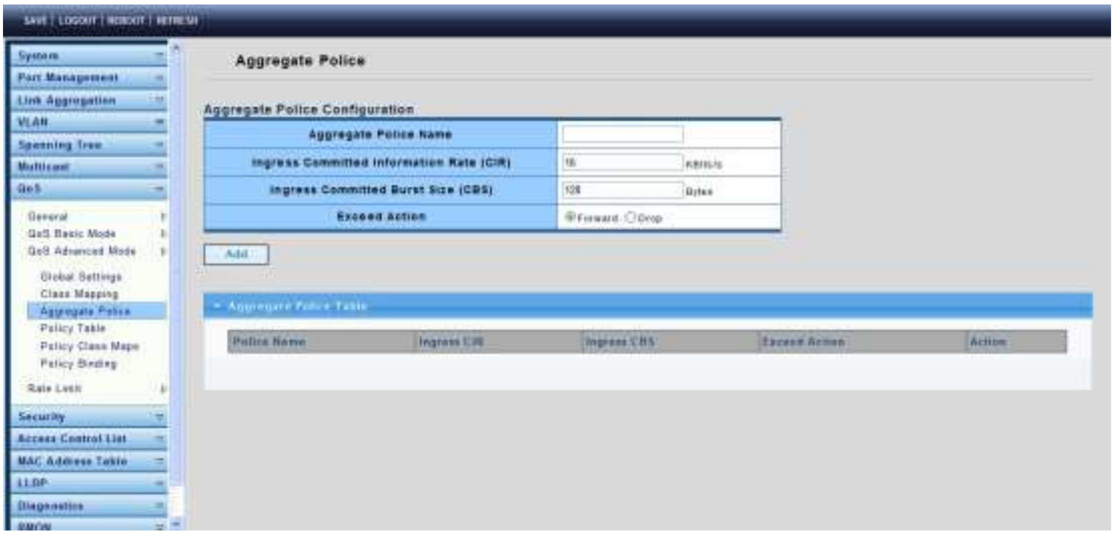
Class Name	
Match ACL Type	○ IP ○ MAC ○ IP or MAC
IP	□ IPv4 or □ IPv6
MAC	
Preferred ACL	● IP ○ MAC

Class Table

Class Name	Match	Action

4.7.3.3 Aggregate Police

To display the Aggregate Police page, click **QoS > QoS Advanced Mode > Aggregate Police.**



Aggregate Police

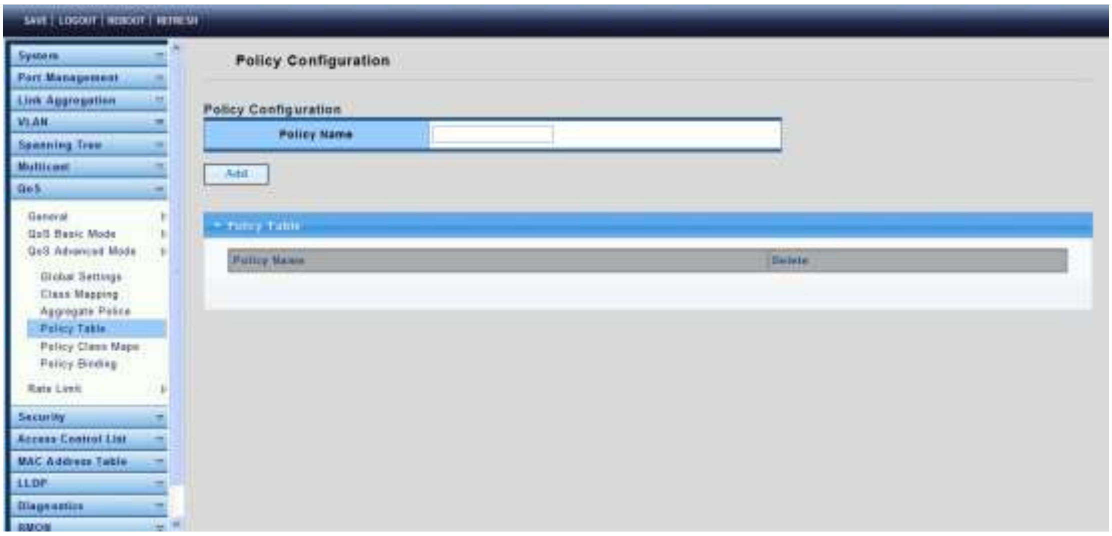
Aggregate Police Configuration

Aggregate Police Name	
Ingress Committed Information Rate (CIR)	16 Kbits/s
Ingress Committed Burst Size (CBS)	128 Bytes
Exceed Action	● Forward ○ Drop

Police Name	Ingress CIR	Ingress CBS	Exceed Action	Action

4.7.3.4 Policy Table

To display the Policy Table page, click **QoS > QoS Advanced Mode > Policy Table.** This page allows you to establish your Policy Configuration and edit the Policy Name.



Policy Configuration

Policy Configuration

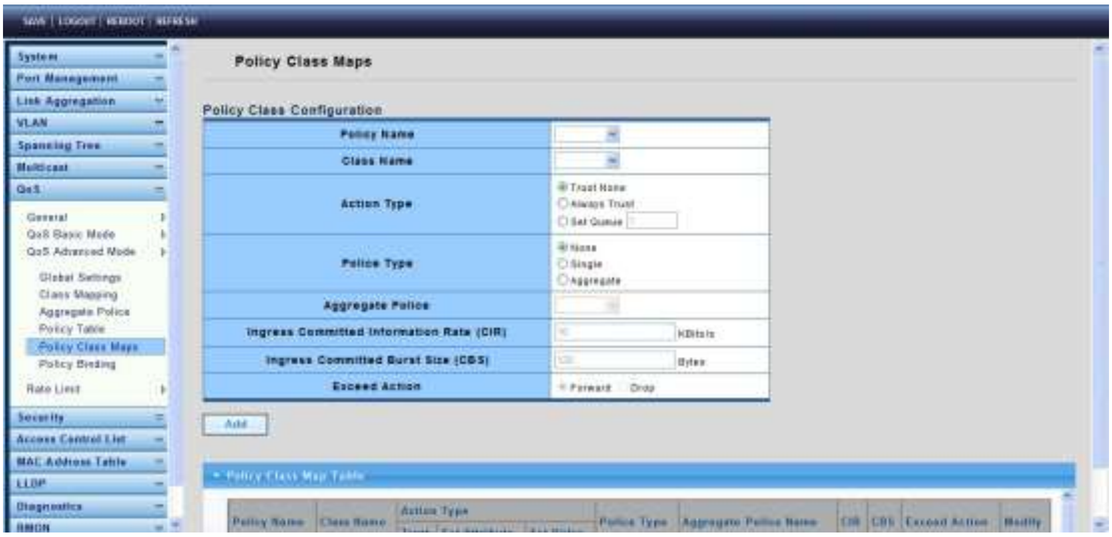
Policy Name	

Policy Name	Delete

4.7.3.5 Policy Class Maps

One or more class maps can be added to a policy. A class map defines the type of packets that are considered to belong to the same traffic flow.

To display the Policy Class Maps page, click **QoS > QoS Advanced Mode > Policy Class Maps.**



Policy Class Maps

Policy Class Configuration

Policy Name	
Class Name	
Action Type	● Trust None ○ Always Trust ○ Set Queue
Police Type	● None ○ Single ○ Aggregate
Aggregate Police	
Ingress Committed Information Rate (CIR)	KBits/s
Ingress Committed Burst Size (CBS)	Bytes
Exceed Action	● Forward ○ Drop

Policy Name	Class Name	Action Type	Police Type	Aggregate Police Name	CIR	CBS	Exceed Action	Modify

Policy Name: Displays the policy to which the class map is being added.

Class Name: Select an existing class map to be associated with the policy. Class maps are created on the Class Mapping page.

Action Type: Select the action regarding the ingress CoS/802.1p and/or DSCP value of all the matching packets.

Police Type: Available in Layer 2 system mode only. Select the policer type for the policy.

Aggregate Policer: Available in Layer 2 system mode only. If Police Type is Aggregate, select a previously defined (in the Aggregate Policer page) aggregate policer.

Ingress Committed Information Rate (CIR): Enter the CIR in kbps. See a description of this on the Bandwidth page.

Ingress Committed Burst Size (CBS): Enter the CBS in bytes. See a description of this on the Bandwidth page.

Exceed Action: Select the action assigned to incoming packets exceeding the CIR.

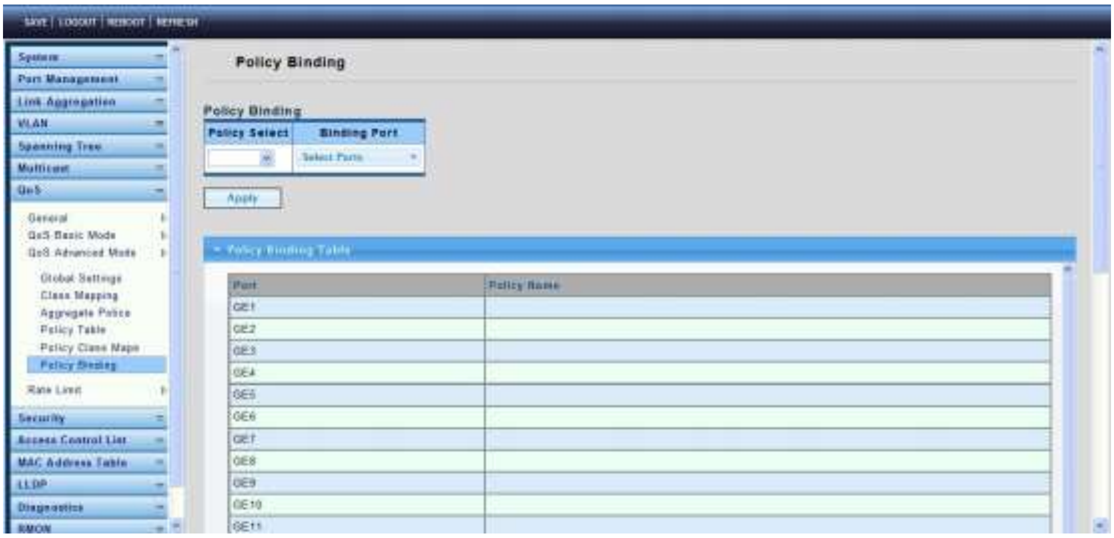
4.7.3.6 Policy Binding

The Policy Binding page shows which policy profile is bound and to which port. When a policy profile is bound to a specific port, it is active on that port. Only one policy profile can be configured on a single port, but a single policy can be bound to more than one port.

When a policy is bound to a port, it filters and applies QoS to ingress traffic that belongs to the flows defined in the policy. The policy does not apply to traffic egress to the same port.

To edit a policy, it must first be removed (unbound) from all those ports to which it is bound.

To display the Policy Binding page, click **QoS > QoS Advanced Mode > Policy Binding.**



Policy Binding

Policy Binding

Policy Select	Binding Port
	Select Ports

Policy Binding Table

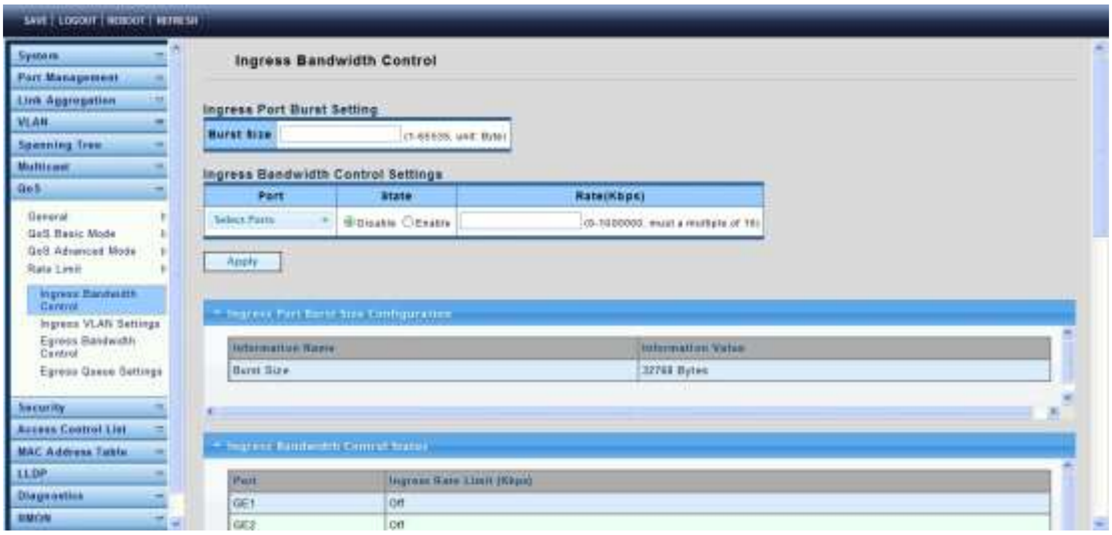
Port	Policy Name
GE1	
GE2	
GE3	
GE4	
GE5	
GE6	
GE7	
GE8	
GE9	
GE10	
GE11	

4.7.4 Rate Limit

4.7.4.1 Ingress Bandwidth Control

To display the Ingress Bandwidth Control page, click **QoS > Rate Limit > Ingress Bandwidth Control.**

This page allows you to set the ingress bandwidth control.



Ingress Bandwidth Control

Ingress Port Burst Setting

Burst Size: (1-65535, unit: Byte)

Ingress Bandwidth Control Settings

Port	State	Rate(Kbps)
Select Ports	● Disable ○ Enable	(0-1000000, must a multiple of 16)

Ingress Port Burst Size Configuration

Information Name	Information Value
Burst Size	32768 Bytes

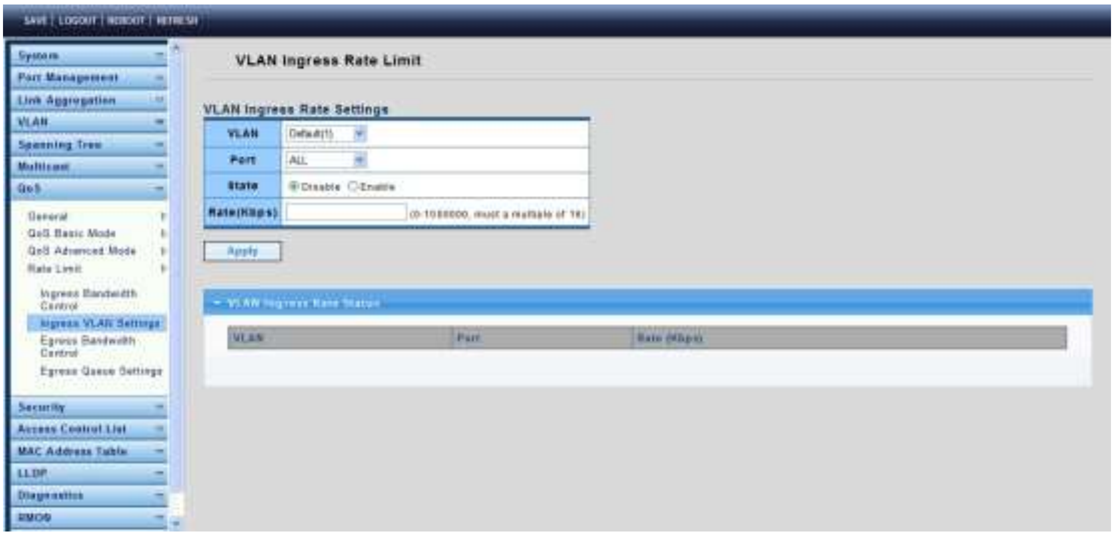
Ingress Bandwidth Control Status

Port	Ingress Rate Limit (Kbps)
GE1	Off
GE2	Off

4.7.4.2 Ingress VLAN Settings

To display the Ingress VLAN Settings page, click **QoS > Rate Limit > Ingress VLAN Settings.**

This page is used to set the bandwidth of the VLAN entry control**.**



VLAN Ingress Rate Limit

VLAN Ingress Rate Settings

VLAN	Default(1)
Port	ALL
State	● Disable ○ Enable
Rate(Kbps)	(0-1000000, must a multiple of 16)

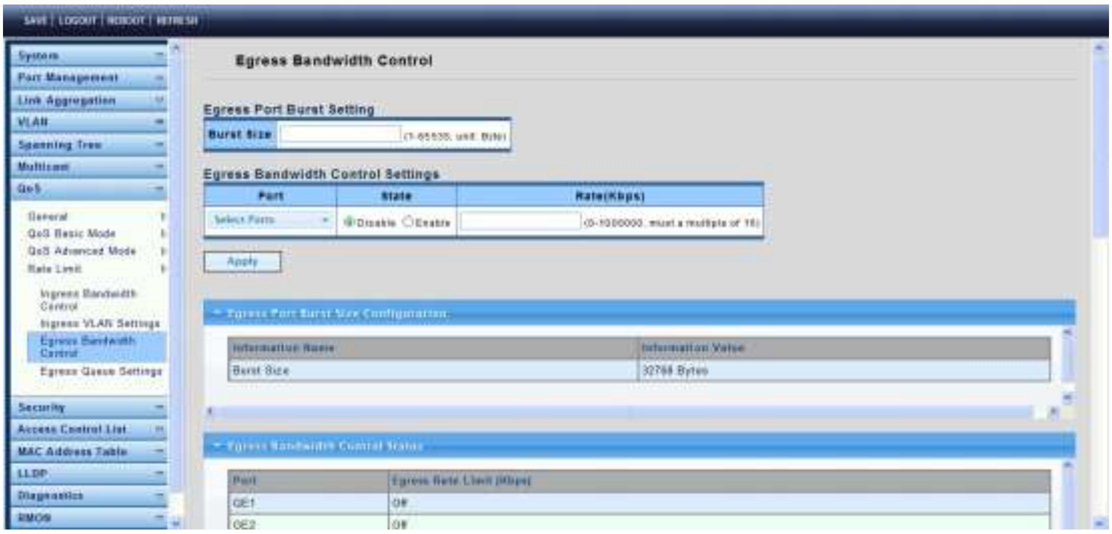
VLAN Ingress Rate Status

VLAN	Port	Rate (Kbps)

4.7.4.3 Egress Bandwidth Control

To display the Egress Port Settings page, click **QoS > Rate Limit > Egress Bandwidth Control.**

This page is used to set the egress bandwidth control.



Egress Bandwidth Control

Egress Port Burst Setting

Burst Size	(1-65535, unit: Byte)

Egress Bandwidth Control Settings

Port	State	Rate(Kbps)
Select Ports	● Disable ○ Enable	(0-1000000, must a multiple of 16)

Egress Port Burst Size Configuration

Information Name	Information Value
Burst Size	32768 Bytes

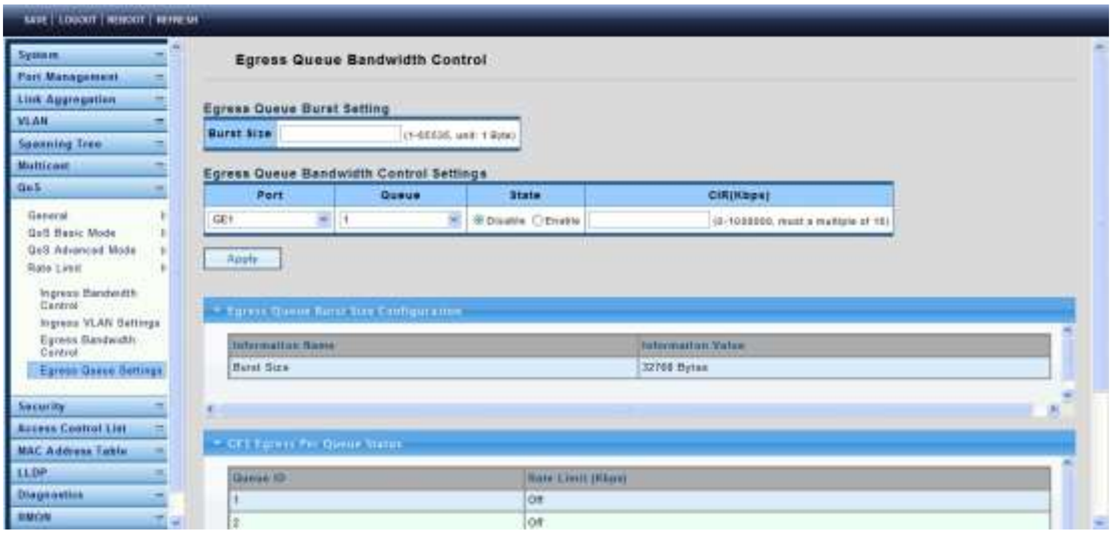
Egress Bandwidth Control Status

Port	Egress Rate Limit (Kbps)
GE1	Off
GE2	Off

4.7.4.4 Egress Queue Settings

To display the Egress Queue Settings page, click **QoS > Rate Limit > Egress Queue Settings.**

The page is used to set the egress bandwidth parameters.



Egress Queue Bandwidth Control

Egress Queue Burst Setting

Burst Size: (1-65535, unit: 1 Byte)

Egress Queue Bandwidth Control Settings

Port	Queue	State	CIR(Kbps)
GE1	1	● Disable ○ Enable	(0-1000000, must a multiple of 16)

Egress Queue Burst Size Configuration

Information Name	Information Value
Burst Size	32768 Bytes

GE1 Egress Per Queue Status

Queue ID	Rate Limit (Kbps)
1	Off
2	Off

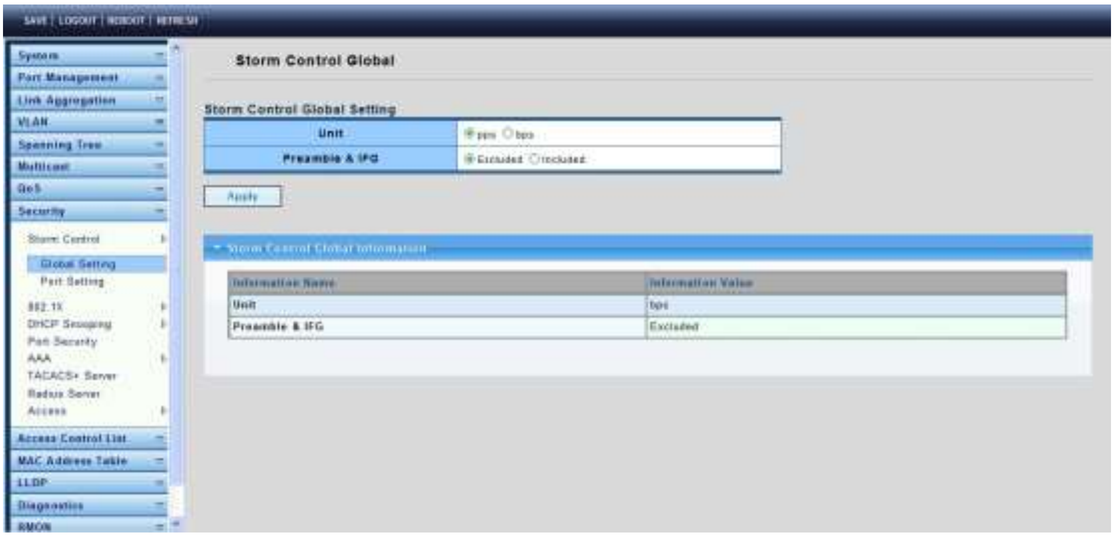
4.8 Security

Use the Security pages to configure settings for the switch’s security features.

4.8.1 Storm Control

4.8.1.1 Global Setting

To display the Global Setting page, click **Security > Storm Control > Global Setting.**



Storm Control Global

Storm Control Global Setting

Unit	● pps ○ bps
Preamble & IFG	● Excluded ○ Included

Storm Control Global Information

Information Name	Information Value
Unit	bps
Preamble & IFG	Excluded

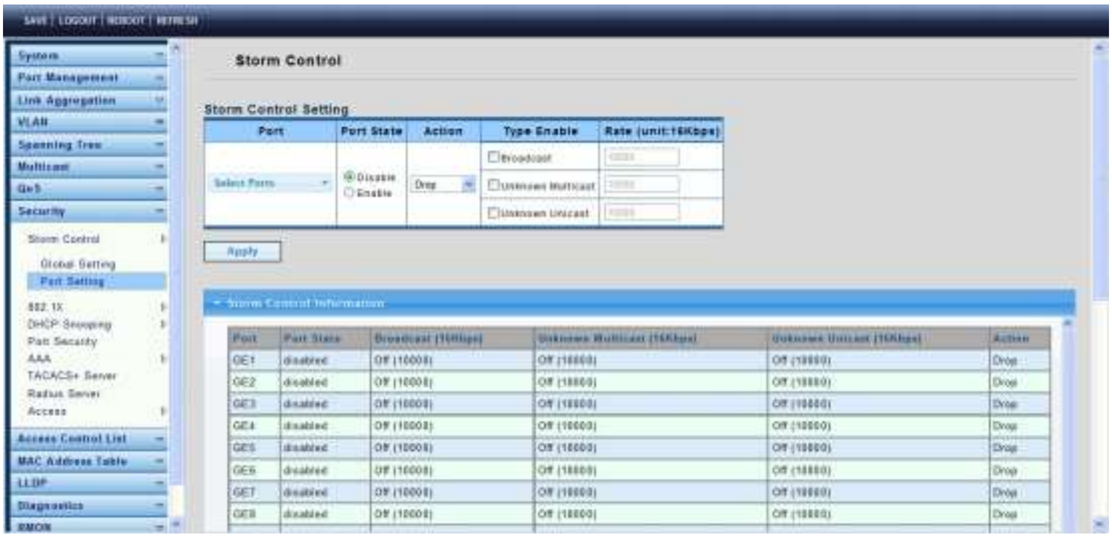
Unit: Choose a storm control unit: pps or bps.

Preamble & IFG: Choose to include or exclude Preamble & IFG (20 bytes).

- Excluded: exclude preamble & IFG (20 bytes) when count ingress storm control rate.
- Included: include preamble & IFG (20 bytes) when count ingress storm control rate.

4.8.1.2 Port Setting

To display the Port Setting page, click **Security > Storm Control > Port Setting.**



Storm Control

Storm Control Setting

Port	Port State	Action	Type Enable	Rate (unit:16Kbps)
Select Ports	● Disable ○ Enable	Drop	□ Broadcast	10000
			□ Unknown Multicast	10000
			□ Unknown Unicast	10000

Apply

Storm Control Information

Port	Port State	Broadcast (16Kbps)	Unknown Multicast (16Kbps)	Unknown Unicast (16Kbps)	Action
GE1	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE2	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE3	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE4	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE5	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE6	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE7	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE8	disabled	Off (10000)	Off (10000)	Off (10000)	Drop

Port: Select the setting ports.

Type Enable: Select the type of storm control.

- Broadcast: Broadcast packet.
- Unknown Multicast: Unknown multicast packet State.
- Unknown Unicast: Unknown unicast packet.

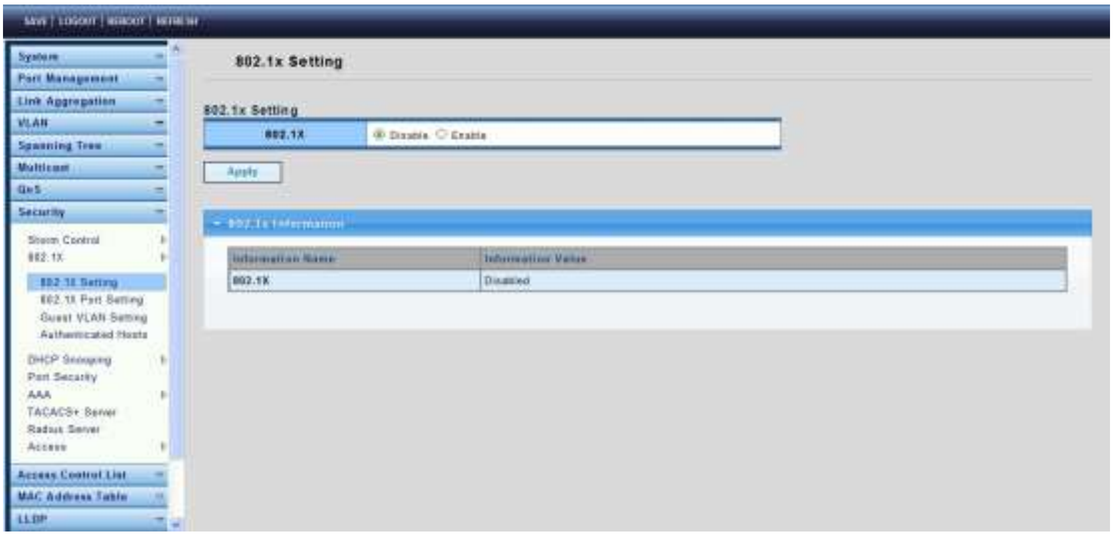
Rate: Value of the storm control rate. Unit: pps (packet per-second) or Kbps (Kbits per-second) depends on global mode setting. The range is from 0 to 1000000.

4.8.2 802.1X

802.1x is based on the Client/Server access control and authentication protocol. It can restrict any unauthorized users or devices trying to connect to the access port of the LAN/WLAN. Before getting the mission from the switch or LAN, the 802.1x will check the users or devices that connect with the switch ports. Before the devices or users pass the "test," it only accepts the EAPoL data connected with the switch; but after it passes, the ordinary data all can be transmitted through Ethernet ports.

4.8.2.1 802.1X Setting

To display the 802.1X Setting page, click **Security > 802.1X > 802.1X Setting.**



802.1x Setting

802.1x Setting

802.1X	● Disable ○ Enable

Apply

802.1x Information

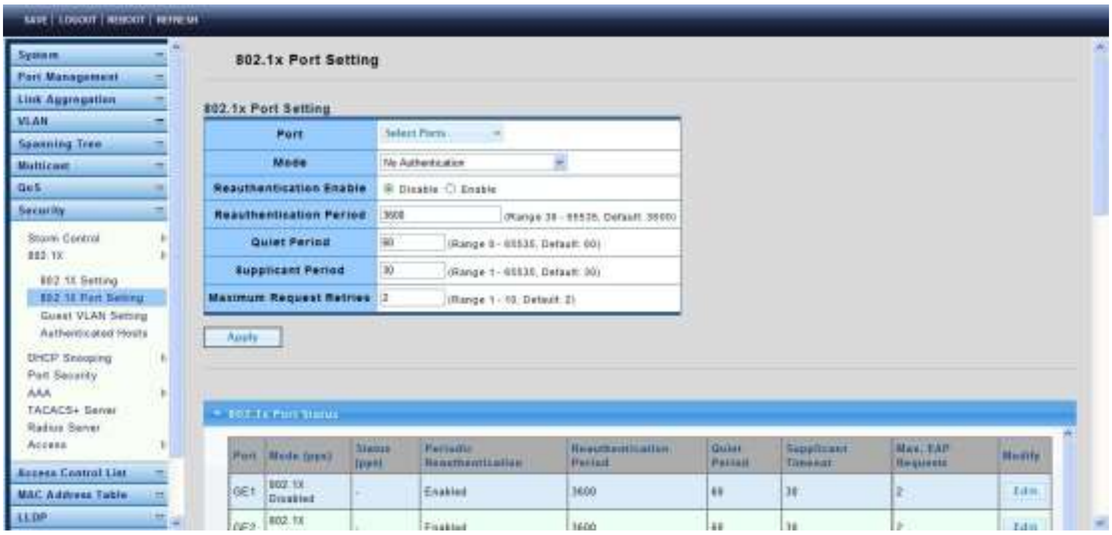
Information Name	Information Value
802.1X	Disabled

802.1X: Set the enabling status of 802.1X functionality.

- Enable: Enable 802.1X.
- Disable: Disable 802.1X.

4.8.2.2 802.1X Port Setting

To display the 802.1X Port Setting page, click **Security > 802.1X > 802.1X Port S etting.**



802.1x Port Setting

802.1x Port Setting

Port	Select Ports
Mode	No Authentication
Reauthentication Enable	● Disable ○ Enable
Reauthentication Period	3600 (Range 30 - 65535, Default: 3600)
Quiet Period	60 (Range 0 - 65535, Default: 60)
Supplicant Period	30 (Range 1 - 65535, Default: 30)
Maximum Request Retries	2 (Range 1 - 10, Default: 2)

802.1x Port Status

Port	Mode (oper)	Status (oper)	Periodic Reauthentication	Reauthentication Period	Quiet Period	Supplicant Timeout	Max. EAP Requests	Modify
GE1	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE2	802.1X	-	Enabled	3600	60	30	2	Edit

Port: Select the ports to configure their authentication mode.

Mode: The authentication mode.

- Force Unauthorized: Force this port to be unconditional unauthorized.
- Force Authorized: Force this port to be unconditional authorized.
- Authentication: 802.1X authentication.
- No Authentication: 802.1X disabled.

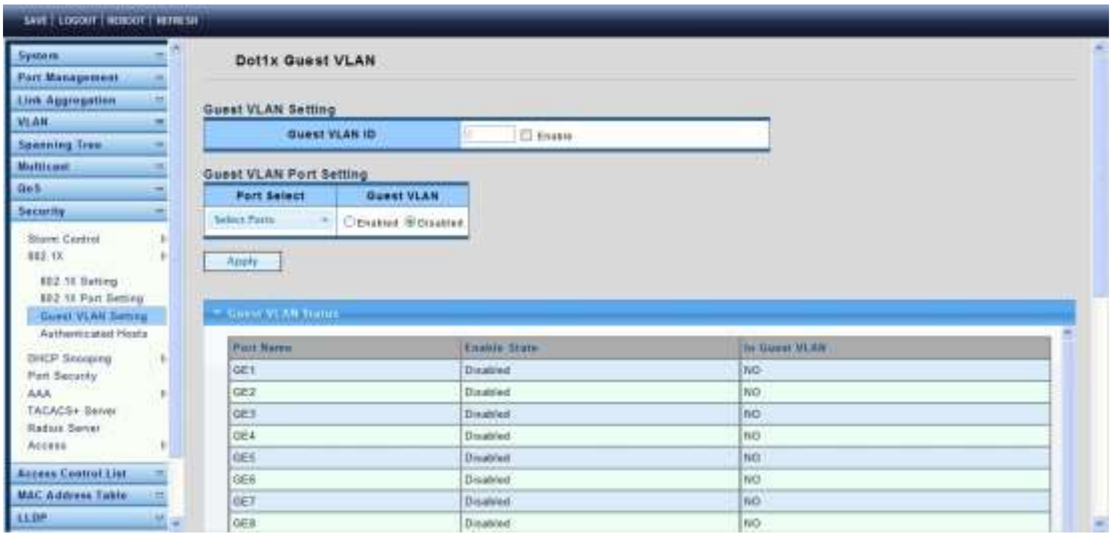
Reauthentication Enable: Set the enabling status of 802.1X reauthentication.
Reauthentication Period: Set the reauthentication period of 802.1X if reauthentication is enabled.

4.8.2.3 Guest VLAN Setting

Guest VLAN provides access to services that do not require the subscribing devices or ports to be 802.1x or MAC-based authenticated and authorized.

An unauthenticated VLAN is a VLAN that allows access by both authorized and unauthorized devices or ports. You can configure one or more VLANs to be unauthenticated in Creating VLANs.

To display the Guest VLAN Setting page, click **Security > 802.1X > Guest VLAN Setting.**



Dot1x Guest VLAN

Guest VLAN Setting

Guest VLAN ID: □ Enable

Guest VLAN Port Setting

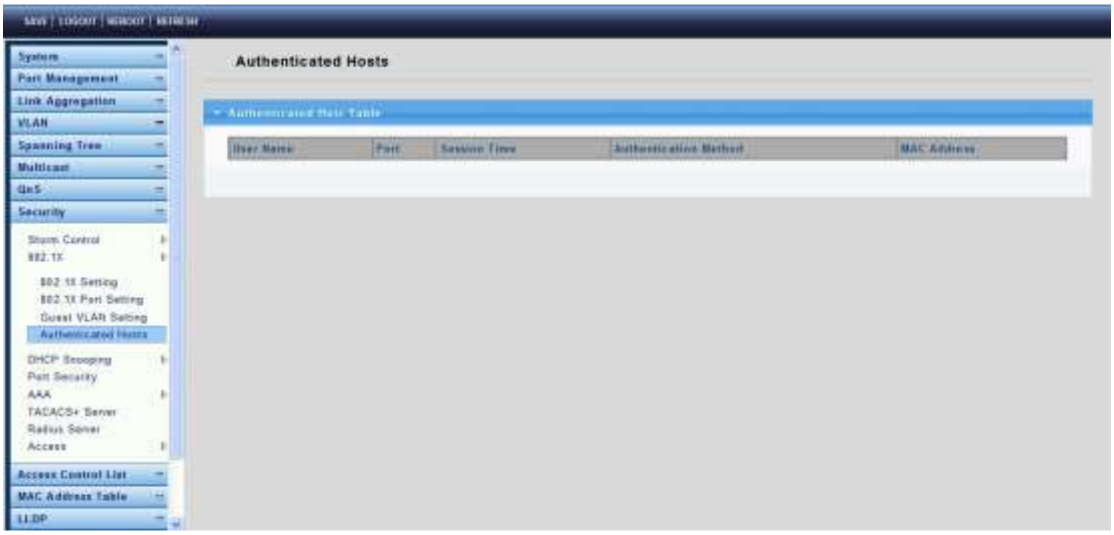
Port Select	Guest VLAN
Select Ports	○ Enabled ● Disabled

Guest VLAN Status

Port Name	Enable State	In Guest VLAN
GE1	Disabled	NO
GE2	Disabled	NO
GE3	Disabled	NO
GE4	Disabled	NO
GE5	Disabled	NO
GE6	Disabled	NO
GE7	Disabled	NO
GE8	Disabled	NO

4.8.2.4 Authenticated Hosts

To display the Authenticated Hosts page, click **Security > 802.1X > Authenticated Hosts.**



Authenticated Hosts

Authenticated Host Table

User Name	Port	Session Time	Authentication Method	MAC Address

User Name: Supplicant names that were authenticated on each port.

Port: Number of the port.

Session Time (DD:HH:MM:SS): Amount of time that the supplicant was logged on the port.

Authentication Method: Method by which the last session was authenticated.

The options are:

- None: No authentication is applied; it is automatically authorized.
- RADIUS: Supplicant was authenticated by a RADIUS server.

MAC Address: Displays the supplicant MAC address.

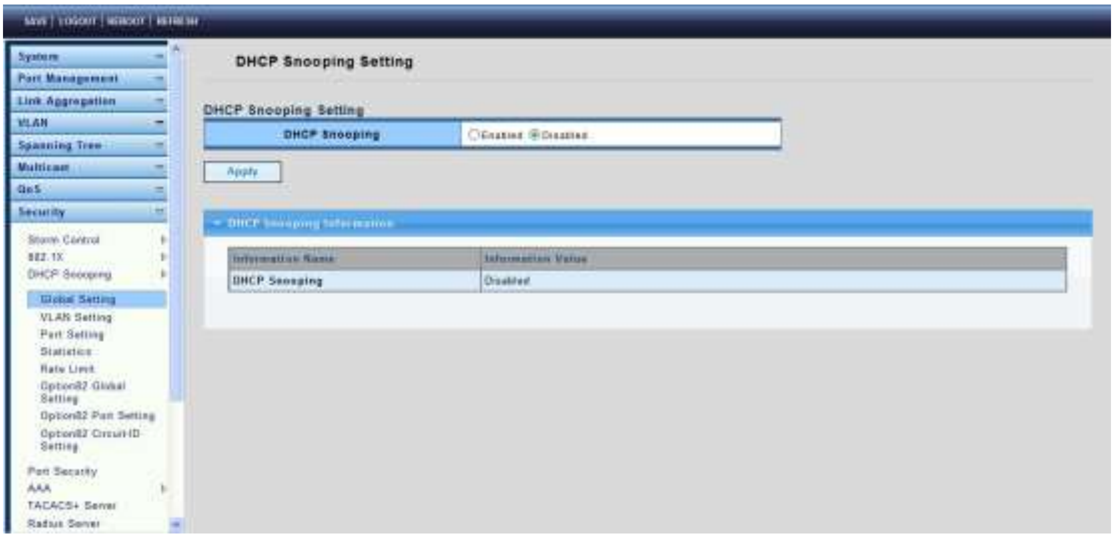
4.8.3 DHCP Snooping

When the switch opens DHCP Snooping, it will snoop DHCP messages and receive DHCP requests, and abstract and record the IP address and MAC address from the DHCP ACK message. DHCP Snooping admits one physical port setting as a creditable port or discreditable port. Creditable ports can receive and forward the DHCP offer message; whereas, the discreditable port will lose the DHCP offer message. In so doing, the switch can pick out the fake DHCP server and make sure that the client gets legal IP addresses from the DHCP server.

4.8.3.1 Global Setting

To display the Global Setting page, click **Security > DHCP Snooping > Global Setting.**

This page is used to open the DHCP Snooping function.



DHCP Snooping Setting

DHCP Snooping Setting

DHCP Snooping	○ Enabled ● Disabled

DHCP Snooping Information

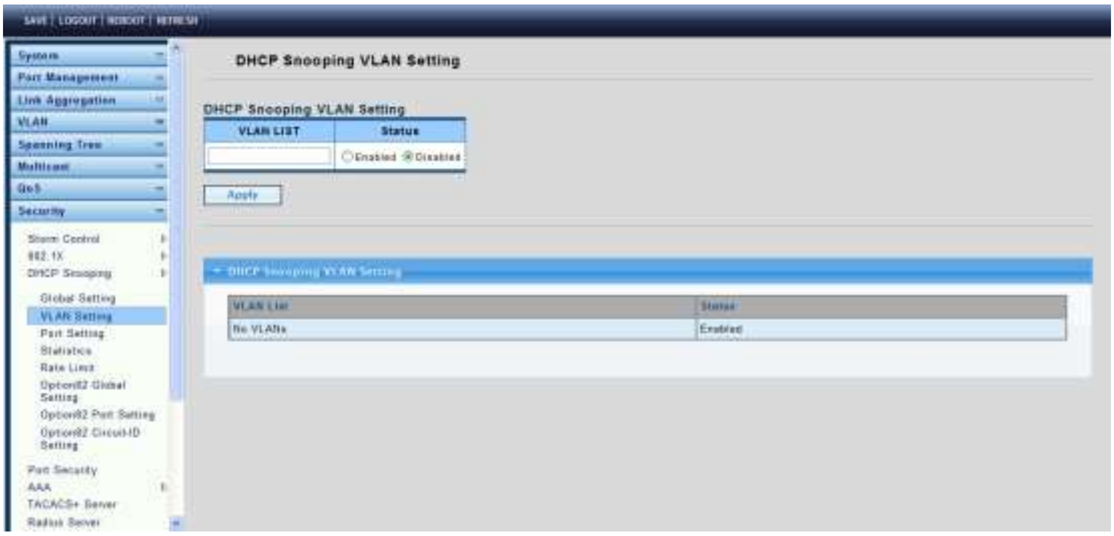
Information Name	Information Value
DHCP Snooping	Disabled

DHCP Snooping: Enable or disable the DHCP Snooping function.

4.8.3.2 VLAN Setting

To display the VLAN Setting page, click **Security > DHCP Snooping > VLAN Setting.**

This page allows you to configure the DHCP Snooping VLAN, enable status on a VLAN, and move the VLAN from the Available VLANs list to the Enabled VLANs list.



DHCP Snooping VLAN Setting

DHCP Snooping VLAN Setting

VLAN LIST	Status
	○ Enabled ● Disabled

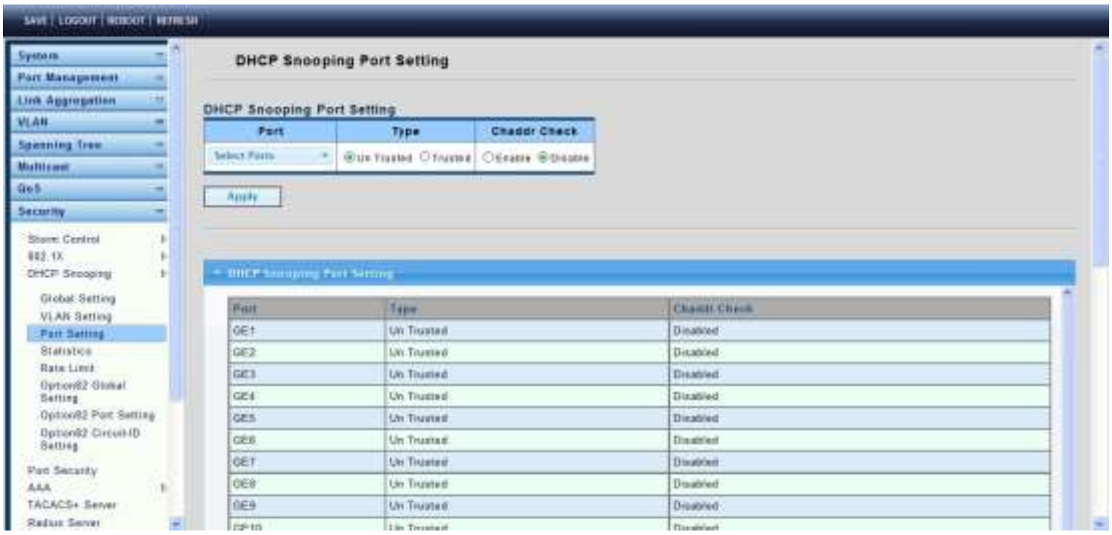
DHCP Snooping VLAN Setting

VLAN List	Status
No VLANs	Enabled

4.8.3.3 Port Setting

To display the Port Setting page, click **Security > DHCP Snooping > Port Setting.**

This page allows you to configure a specific port as a DHCP Snooping trust port.



DHCP Snooping Port Setting

DHCP Snooping Port Setting

Port	Type	Chaddr Check
Select Ports	● Un Trusted ○ Trusted	○ Enable ● Disable

Apply

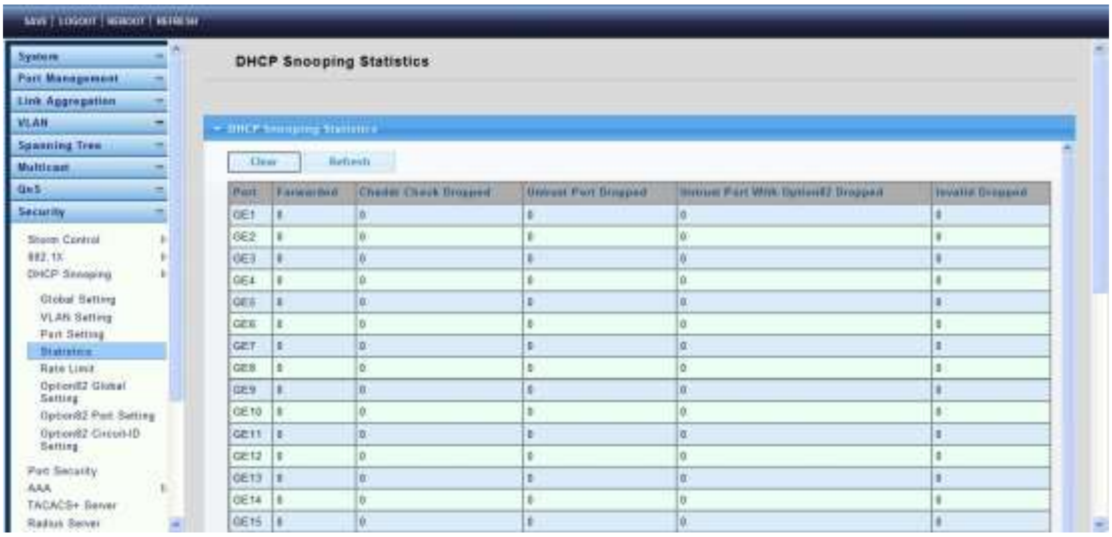
DHCP Snooping Port Setting

Port	Type	Chaddr Check
GE1	Un Trusted	Disabled
GE2	Un Trusted	Disabled
GE3	Un Trusted	Disabled
GE4	Un Trusted	Disabled
GE5	Un Trusted	Disabled
GE6	Un Trusted	Disabled
GE7	Un Trusted	Disabled
GE8	Un Trusted	Disabled
GE9	Un Trusted	Disabled
GE10	Un Trusted	Disabled

4.8.3.4 Statistics

To display the Statistics page, click **Security > DHCP Snooping > Statistics.**

This page presents statistics of each port and DHCP Snooping state information.



DHCP Snooping Statistics

DHCP Snooping Statistics

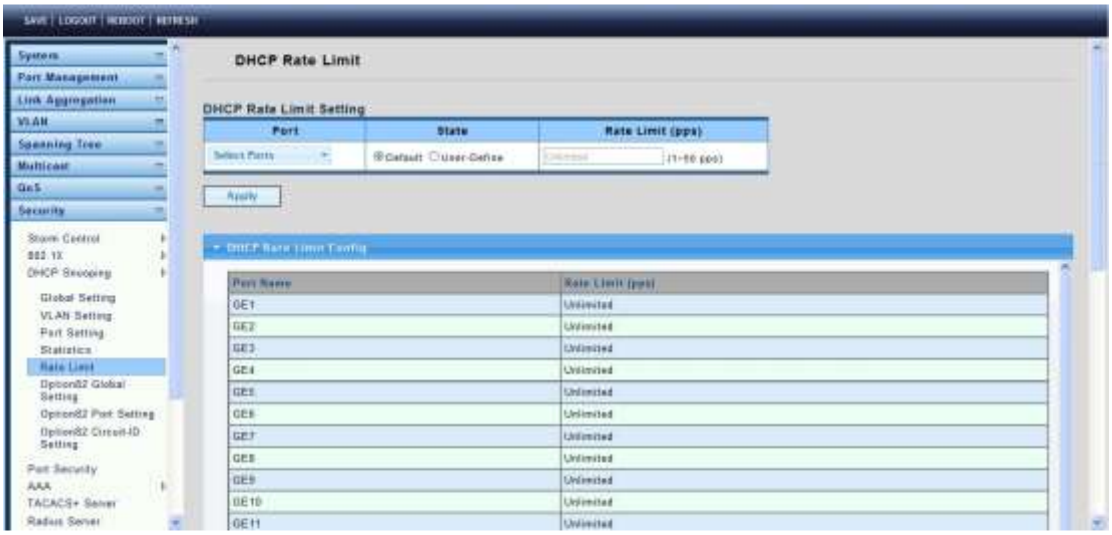
Clear Refresh

Port	Forwarded	Chaddr Check Dropped	Untrust Port Dropped	Untrust Port With Option82 Dropped	Invalid Dropped
GE1	0	0	0	0	0
GE2	0	0	0	0	0
GE3	0	0	0	0	0
GE4	0	0	0	0	0
GE5	0	0	0	0	0
GE6	0	0	0	0	0
GE7	0	0	0	0	0
GE8	0	0	0	0	0
GE9	0	0	0	0	0
GE10	0	0	0	0	0
GE11	0	0	0	0	0
GE12	0	0	0	0	0
GE13	0	0	0	0	0
GE14	0	0	0	0	0
GE15	0	0	0	0	0

4.8.3.5 Rate Limit

To display the Rate Limit page, click **Security > DHCP Snooping > Rate Limit.**

This page allows you to set DHCP Rate Limit for each port and restrict the Internet speed.



DHCP Rate Limit

DHCP Rate Limit Setting

Port	State	Rate Limit (pps)
Select Ports	● Default ○ User-Define	Unlimited (1-50 pps)

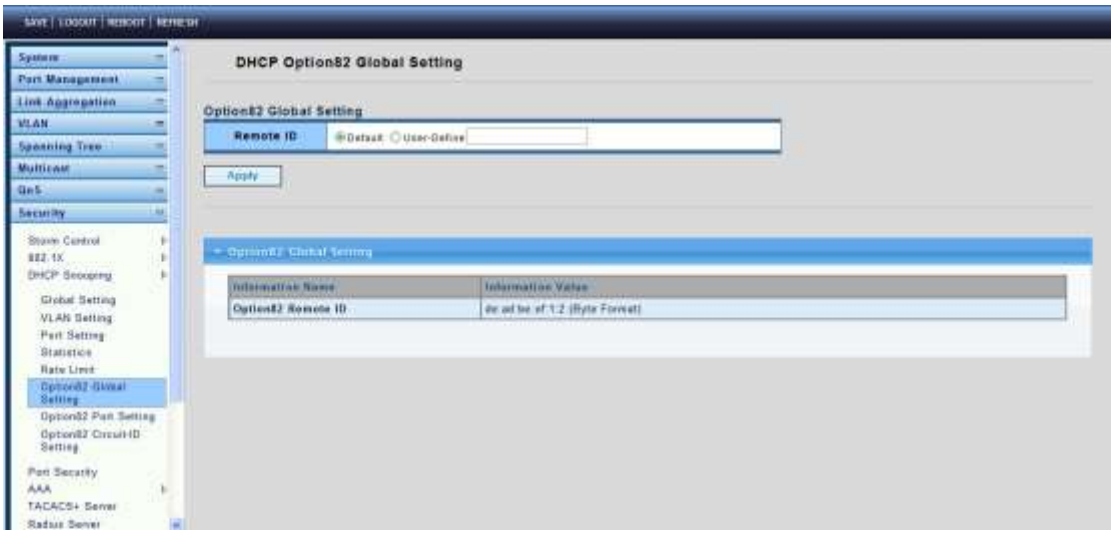
DHCP Rate Limit Config

Port Name	Rate Limit (pps)
GE1	Unlimited
GE2	Unlimited
GE3	Unlimited
GE4	Unlimited
GE5	Unlimited
GE6	Unlimited
GE7	Unlimited
GE8	Unlimited
GE9	Unlimited
GE10	Unlimited
GE11	Unlimited

4.8.3.6 Option82 Global Setting

To display the Option82 Global Setting page, click **Security > DHCP Snooping > Option82 Global Setting.**

This page is used to configure DHCP Snooping support Option82 strategy.



DHCP Option82 Global Setting

Option82 Global Setting

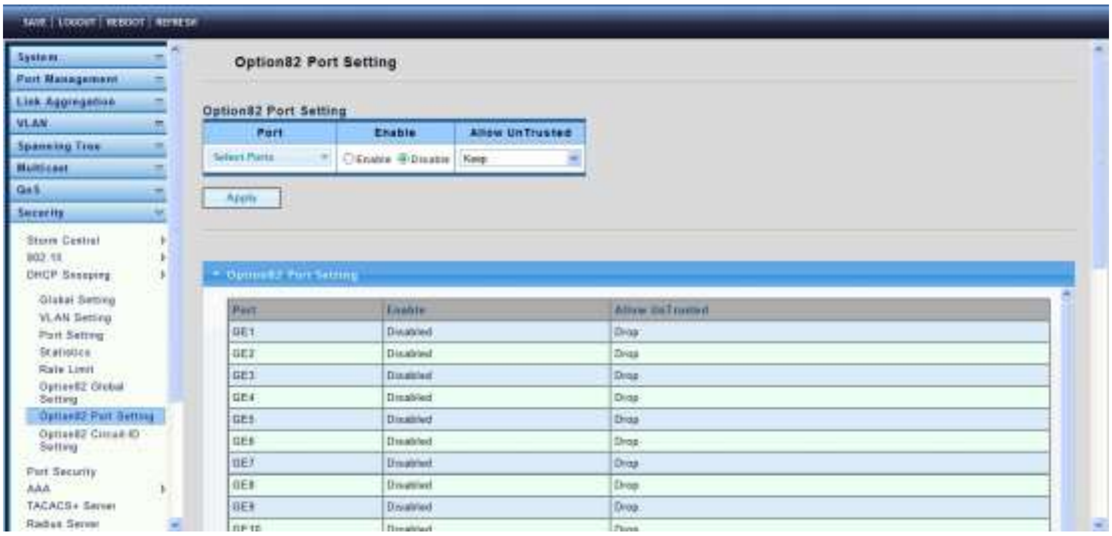
Remote ID: ● Default ○ User-Define

Option82 Global Setting

Information Name	Information Value
Option82 Remote ID	de ad be ef 1:2 (Byte Format)

4.8.3.7 Option82 Port Setting

To display the Option82 Port Setting page, click **Security > DHCP Snooping > Option82 Port Setting.**



Option82 Port Setting

Option82 Port Setting

Port	Enable	Allow UnTrusted
Select Ports	○ Enable ● Disable	Keep

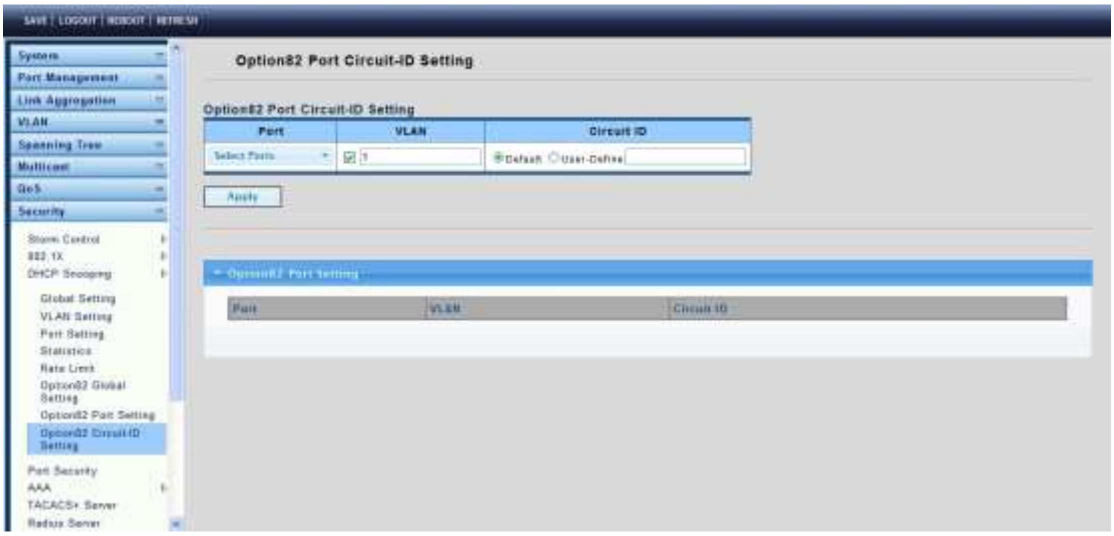
Option82 Port Setting

Port	Enable	Allow UnTrusted
GE1	Disabled	Drop
GE2	Disabled	Drop
GE3	Disabled	Drop
GE4	Disabled	Drop
GE5	Disabled	Drop
GE6	Disabled	Drop
GE7	Disabled	Drop
GE8	Disabled	Drop
GE9	Disabled	Drop
GE10	Disabled	Drop

4.8.3.8 Option82 Circuit-ID Setting

To display the Option82 Circuit-ID Setting page, click **Security > DHCP Snooping > Option82 Circuit-ID Setting.**

This page allows you to edit the circuit ID content in the Option82 settings.



Option82 Port Circuit-ID Setting

Option82 Port Circuit-ID Setting

Port	VLAN	Circuit ID
Select Ports	☑ 1	● Default ○ User-Define

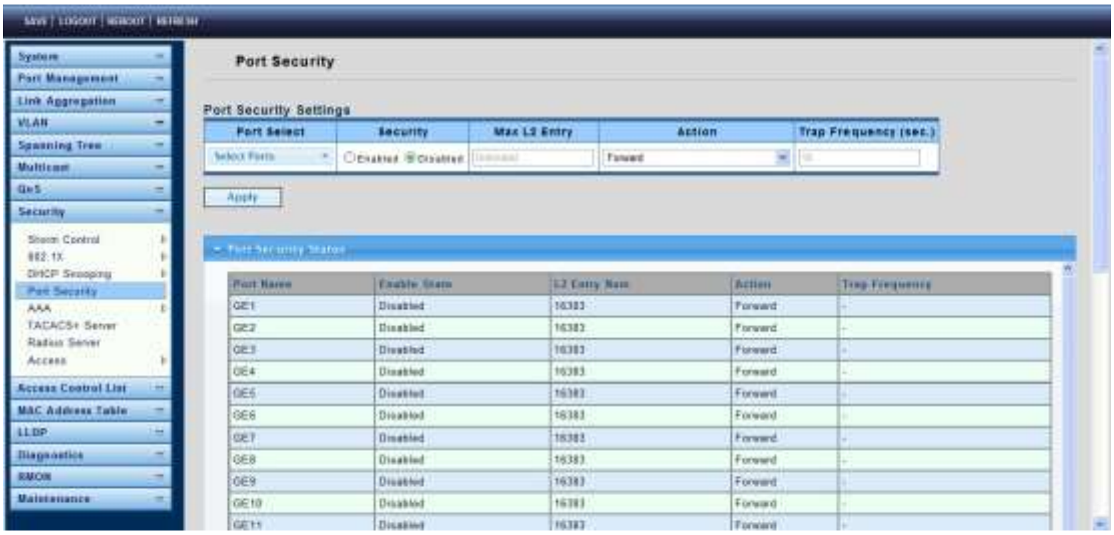
Option82 Port Setting

Port	VLAN	Circuit ID

4.8.4 Port Security

To display the Port Security page, click **Security > Port Security.**

Port Security allows the determination of port isolation and specific behavior.



Port Security

Port Security Settings

Port Select	Security	Max L2 Entry	Action	Trap Frequency (sec.)
Select Ports	○Enabled ●Disabled	Unlimited	Forward	10

Port Name	Enable State	L2 Entry Num	Action	Trap Frequency
GE1	Disabled	16383	Forward	-
GE2	Disabled	16383	Forward	-
GE3	Disabled	16383	Forward	-
GE4	Disabled	16383	Forward	-
GE5	Disabled	16383	Forward	-
GE6	Disabled	16383	Forward	-
GE7	Disabled	16383	Forward	-
GE8	Disabled	16383	Forward	-
GE9	Disabled	16383	Forward	-
GE10	Disabled	16383	Forward	-
GE11	Disabled	16383	Forward	-

Port Select: Select one or multiple ports to configure.

Security: Port security function. It limits how many MAC addresses can be recognized by a port and blocks new ones once the limit is reached.

- Enable: Enable port security function.
- Disable: Disable port security function.

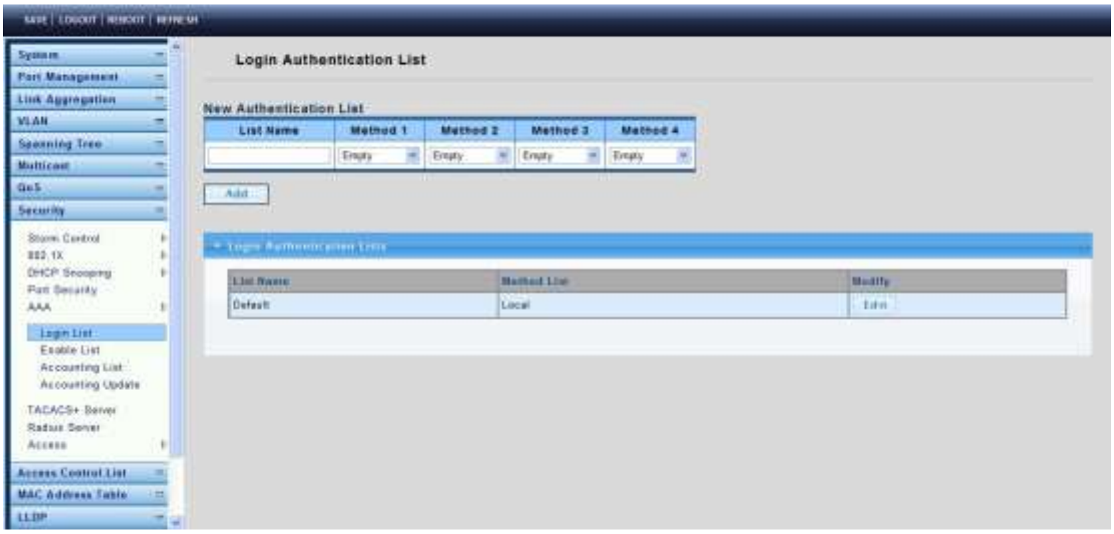
Max L2 Entry: The total number of MAC addresses that can be recognized by a port.

4.8.5 AAA

4.8.5.1 Login List

To display the Login List page, click **Security > AAA > Login List.**

This page allows you to add, edit and delete Login Authentication List settings (the “default” list cannot be deleted). The items in this list will authenticate login users by the incorporated methods. If the first method fails, it will try to use the next priority method to authenticate.



Login Authentication List

New Authentication List

List Name	Method 1	Method 2	Method 3	Method 4
	Empty	Empty	Empty	Empty

List Name	Method List	Modify
Default	Local	Edit

List Name: New Login Authentication List name. This name should be different from other existing lists.

Method 1: Select the first priority method for login authentication.

- Local: Use local accounts database to authenticate.
- Tacacs+: Use remote TACACS+ server to authenticate.
- Radius: Use remote Radius server to authenticate. Not supported now, it will besupported in the future.
- Enable: Use local enable password to authenticate.

Method 2: Select the second priority method for login authentication.

- Local: Use local accounts database to authenticate.
- Tacacs+: Use remote TACACS+ server to authenticate.
- Radius: Use remote Radius server to authenticate. Not supported now, it will be supported in the future.
- Enable: Use local enable password to authenticate.

Method 3: Select the third priority method for login authentication.

- Local: Use local accounts database to authenticate.
- Tacacs+: Use remote TACACS+ server to authenticate.
- Radius: Use remote Radius server to authenticate. Not supported now, it will besupported in the future.
- Enable: Use local enable password to authenticate.

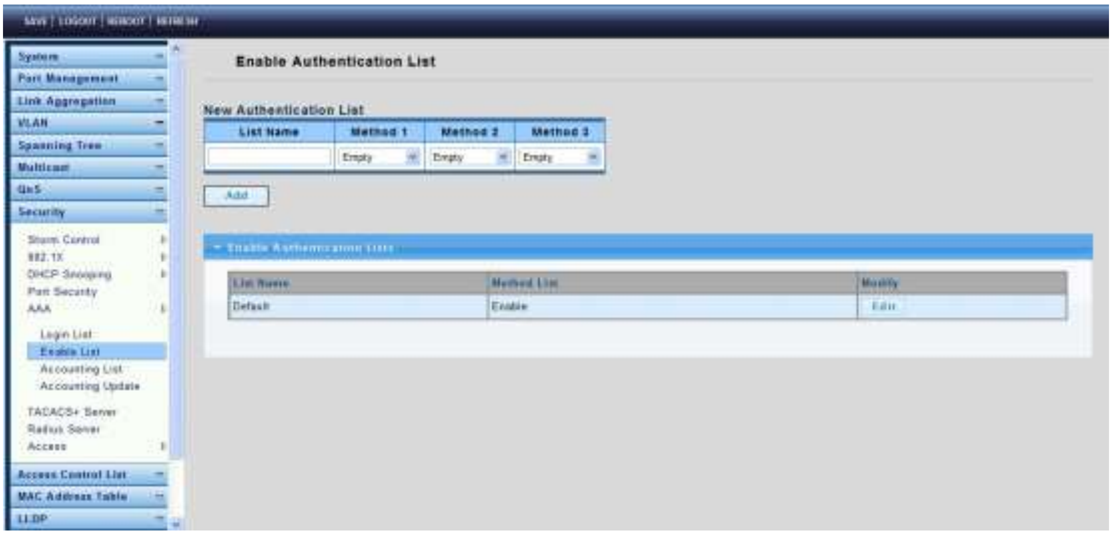
Method 4: Select the fourth priority method for login authentication.

- Local: Use local accounts database to authenticate
- Tacacs+: Use remote TACACS+ server to authenticate.
- Radius: Use remote Radius server to authenticate. Not supported now, it will besupported in the future.
- Enable: Use local enable password to authenticate.

4.8.5.2 Enable List

To display the Login List page, click **Security > AAA > Enable List.**

This page allows you to add, edit or delete Enable Authentication List settings (the “default” list cannot be deleted). The line attached to this list will authenticate a user issuing the “enable” command by methods in this list. If the first method fails, it will try to use the next priority method to authenticate.



Enable Authentication List

New Authentication List

List Name	Method 1	Method 2	Method 3
	Empty	Empty	Empty

Enable Authentication Lists

List Name	Method List	Modify
Default	Enable	Edit

List Name: New Enable Authentication List name. This name should be. different from other existing lists.

Method 1: Select the first priority method for enable authentication.

- Enable: Use local enable password to authenticate
- Tacacs+: Use remote TACACS+ server to authenticate.
- Radius: Use remote Radius server to authenticate. Not supported now, it will besupported in the future.

Method 2: Select the second priority method for enable authentication.

- Enable: Use local enable password to authenticate
- Tacacs+: Use remote TACACS+ server to authenticate.
- Radius: Use remote Radius server to authenticate. Not supported now, it will besupported in the future.

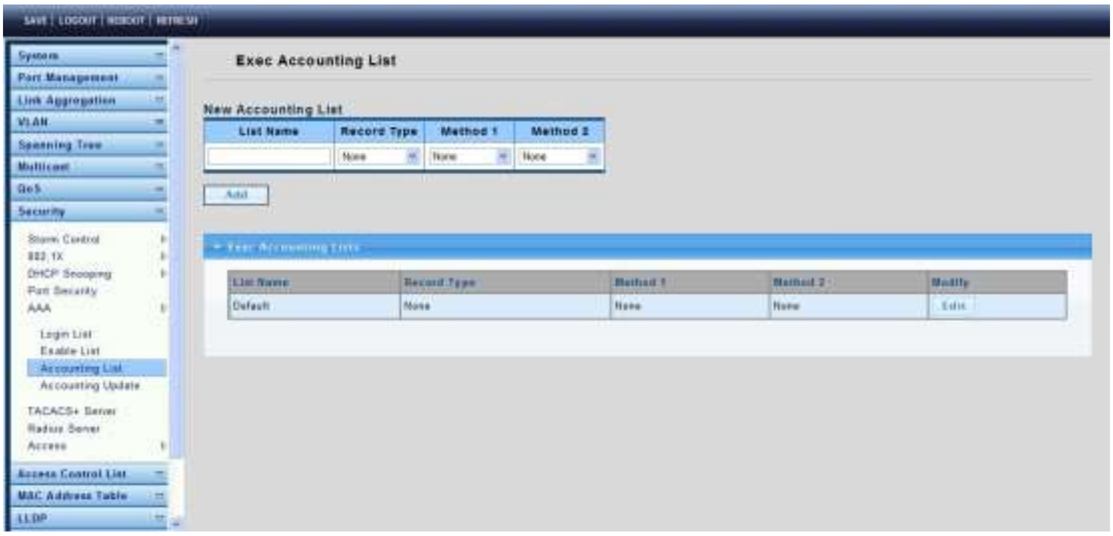
Method 3: Select the third priority method for enable authentication.

- Enable: Use local enable password to authenticate.
- Tacacs+: Use remote TACACS+ server to authenticate.
- Radius: Use remote Radius server to authenticate. Not supported now, it will besupported in the future.

4.8.5.3 Accounting List

To display the Accounting List page, click **Security > AAA > Accounting List.**

This page allows you to add, edit or delete accounting list settings (the “default” list cannot be deleted). The line attached to this list will account for users entering the CLI shell by methods in this list. If the first method fails, it will try to use the next priority method for accounting.



Exec Accounting List

New Accounting List

List Name	Record Type	Method 1	Method 2
	None	None	None

List Name	Record Type	Method 1	Method 2	Modify
Default	None	None	None	Edit

List Name: New Accounting List name. This name should be different from other existing lists.

Record Type: Select the accounting record type.

- none: No accounting.
- start-stop: Record start and stop without waiting.
- stop-only: Record stop when service terminates.

Method 1: Select the first priority method for exec accounting.

- Tacacs+: Use remote TACACS+ server to accounting.

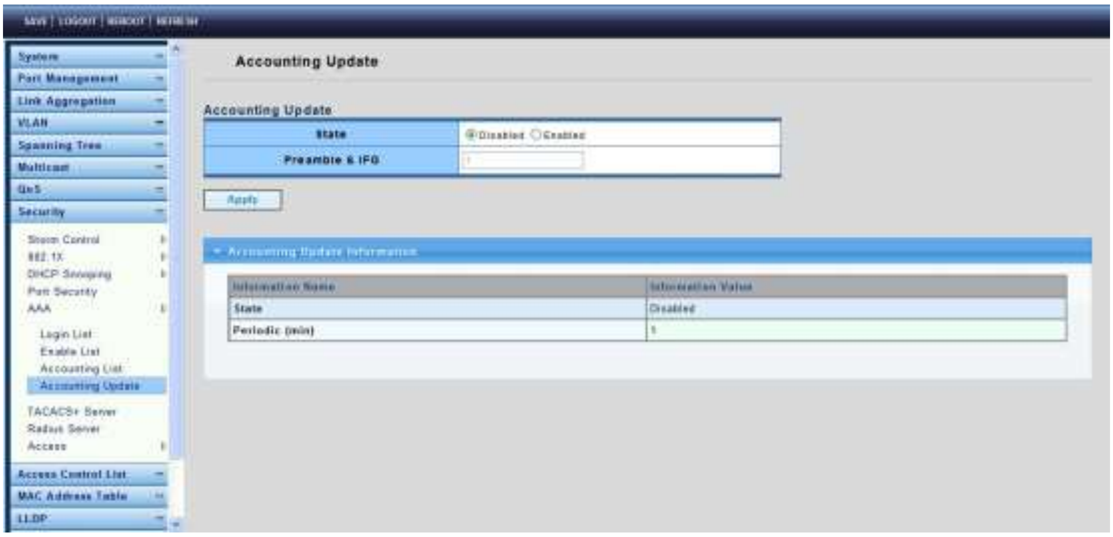
- Radius: Use remote Radius server to accounting. Not supported now, it will besupported in the future.

Method 2: Select the second priority method for exec accounting.

- Tacacs+: Use remote TACACS+ server to accounting.
- Radius: Use remote Radius server to accounting. Not supported now, it will besupported in the future.

4.8.5.4 Accounting Update

To display the Accounting Update page, click **Security > AAA > Accounting Update.**



Accounting Update

Accounting Update

State	● Disabled ○ Enabled
Preamble & IFG	1

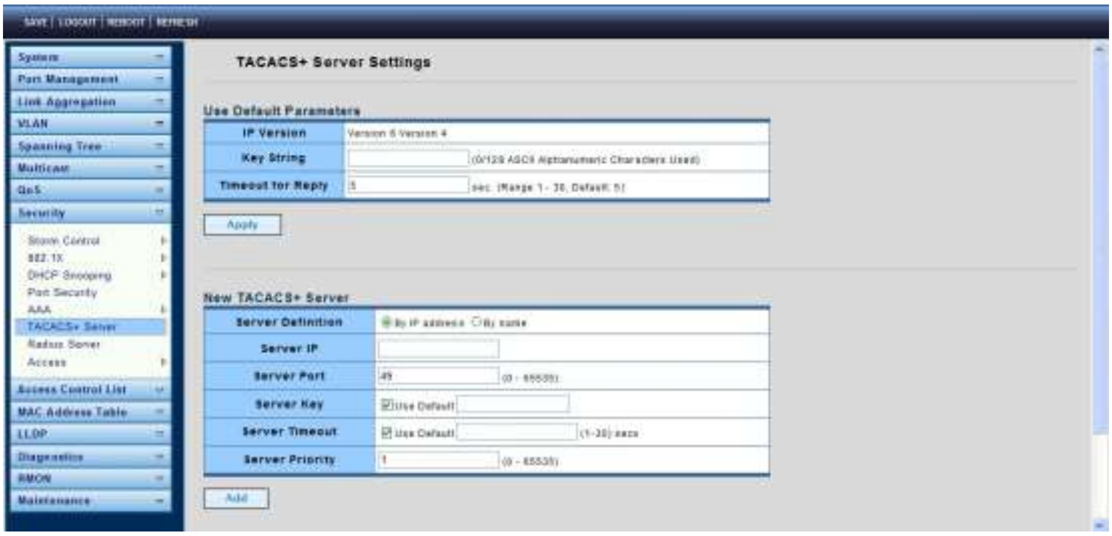
Accounting Update Information

Information Name	Information Value
State	Disabled
Periodic (min)	1

4.8.6 Tacacs+ Server

To display the Tacacs+ server page, click **Security > AAA >Tacacs+ Server.**

This page allows you to add, edit or delete TACACS+ Server settings.



TACACS+ Server Settings

Use Default Parameters

IP Version	Version 6 Version 4
Key String	(0/128 ASCII Alphanumeric Characters Used)
Timeout for Reply	5 sec. (Range 1 - 30, Default: 5)

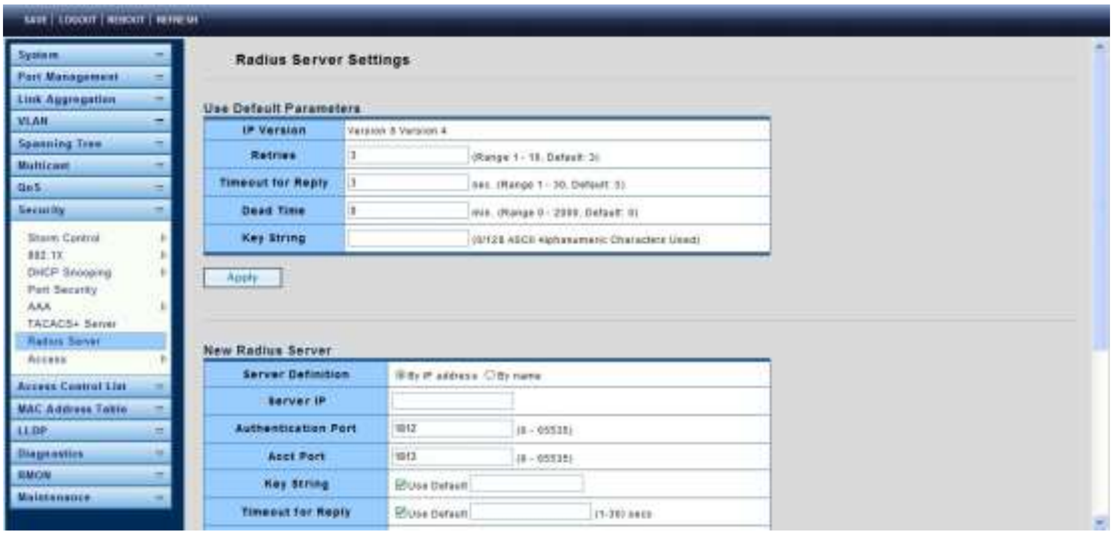
New TACACS+ Server

Server Definition	● By IP address ○ By name
Server IP	
Server Port	49 (0 - 65535)
Server Key	☑ Use Default
Server Timeout	☑ Use Default (1-30) secs
Server Priority	1 (0 - 65535)

4.8.7 Radius Server

To display the Radius Server page, click **Security > AAA > Radius Server.**

This page is used for radius server settings.



Radius Server Settings

Use Default Parameters

IP Version	Version 6 Version 4
Retries	3 (Range 1 - 10, Default: 3)
Timeout for Reply	3 sec. (Range 1 - 30, Default: 3)
Dead Time	0 min. (Range 0 - 2000, Default: 0)
Key String	(0/128 ASCII Alphanumeric Characters Used)

New Radius Server

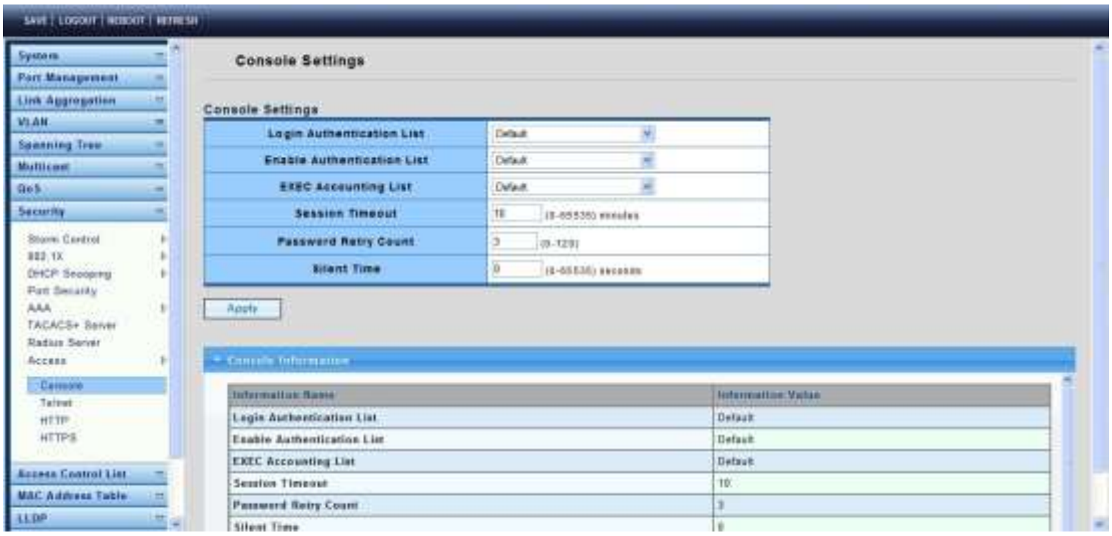
Server Definition	● By IP address ○ By name
Server IP	
Authentication Port	1812 (0 - 65535)
Acct Port	1813 (0 - 65535)
Key String	☑ Use Default
Timeout for Reply	☑ Use Default (1-30) secs

4.8.8 Access

4.8.8.1 Console

To display the Console page, click **Security > Access > Console.**

This page allows you to combine all kinds of AAA lists on the console line. Attempts to access the switch from a console will be authenticated, authorized and accounted for by AAA lists combined here.



Console Settings

Console Settings

Login Authentication List	Default
Enable Authentication List	Default
EXEC Accounting List	Default
Session Timeout	10 (0-65535) minutes
Password Retry Count	3 (0-120)
Silent Time	0 (0-65535) seconds

Information Name	Information Value
Login Authentication List	Default
Enable Authentication List	Default
EXEC Accounting List	Default
Session Timeout	10
Password Retry Count	3
Silent Time	0

Login Authentication List: Select one of the Login Authentication Lists configured on the Login List page.

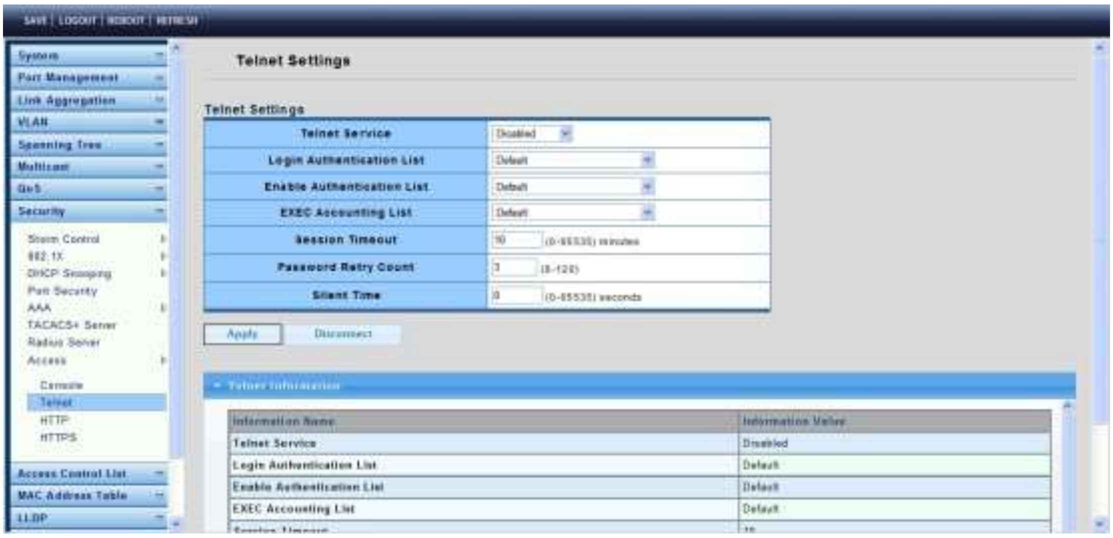
Enable Authentication List: Select one of the Enable Authentication Lists configured on the Enable List page.

EXEC Authorization List: Select one of the EXEC authorization lists configured on the EXEC List page.
Commands Authorization List: Select one of the commands authorization lists configured on the Commands List page.
EXEC Accounting List: Select one of the EXEC accounting lists configured on the Accounting List page.
Session Timeout: Set the session timeout minutes for user access CLI from console line. If a user does not respond before the session times out, CLI will log out automatically. 0 minutes means “Never timeout.”

4.8.8.2 Telnet

To display the Telnet page, click **Security > Access > Telnet.**

This page allows you to combine all kinds of AAA lists with the Telnet line. Attempts to access the switch from Telnet will be authenticated, authorized and accounted for by AAA lists combined here.



Telnet Settings

Telnet Settings

Telnet Service	Disabled
Login Authentication List	Default
Enable Authentication List	Default
EXEC Accounting List	Default
Session Timeout	10 (0-65535) minutes
Password Retry Count	3 (0-120)
Silent Time	0 (0-65535) seconds

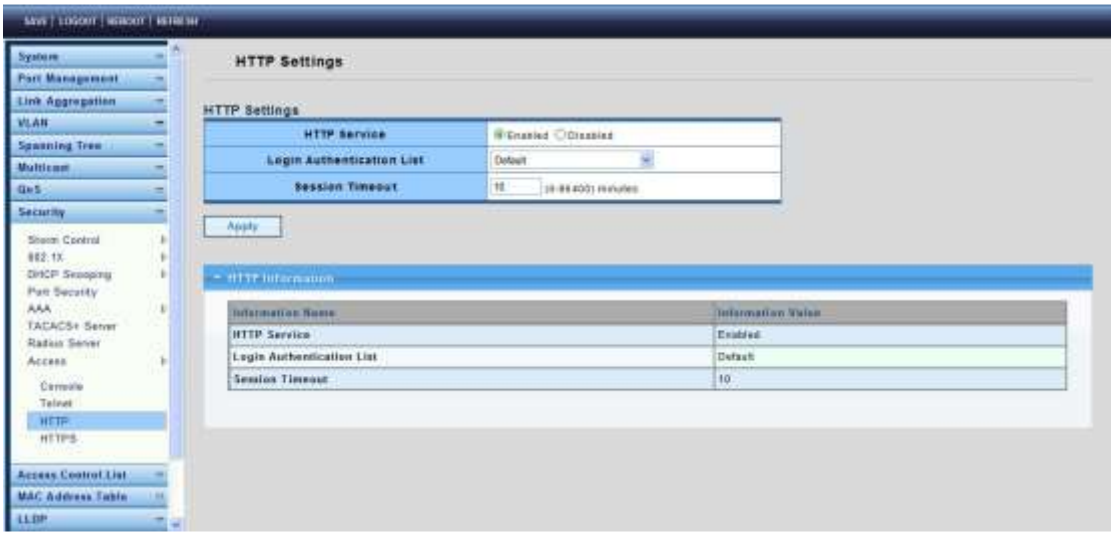
Information Name	Information Value
Telnet Service	Disabled
Login Authentication List	Default
Enable Authentication List	Default
EXEC Accounting List	Default
Session Timeout	10

Telnet Service: Set to disable or enable.
Login Authentication List: Select one of the Login Authentication Lists configured on the Login List page.
Enable Authentication List: Select one of the Enable Authentication Lists configured on the Enable List page.
EXEC Authorization List: Select one of the EXEC Authorization Lists configured on the EXEC List page.
Commands Authorization List: Select one of the Commands Authorization Lists configured on the Commands List page.
EXEC Accounting List: Select one of the EXEC Accounting Lists configured on the Accounting List page.
Session Timeout: Set the session timeout minutes for user access to CLI from the Telnet line. If a user does not respond before the session times out, CLI will log out automatically.

4.8.8.3 HTTP

To display the HTTP page, click **Security > Access > http.**

This page allows you to combine all kinds of AAA lists to the HTTP line. Attempts to access the switch’s Web UI from HTTP will be authenticated by AAA lists combined here.



HTTP Settings

HTTP Settings

HTTP Service	● Enabled ○ Disabled
Login Authentication List	Default
Session Timeout	10 (0-86400) minutes

HTTP Information

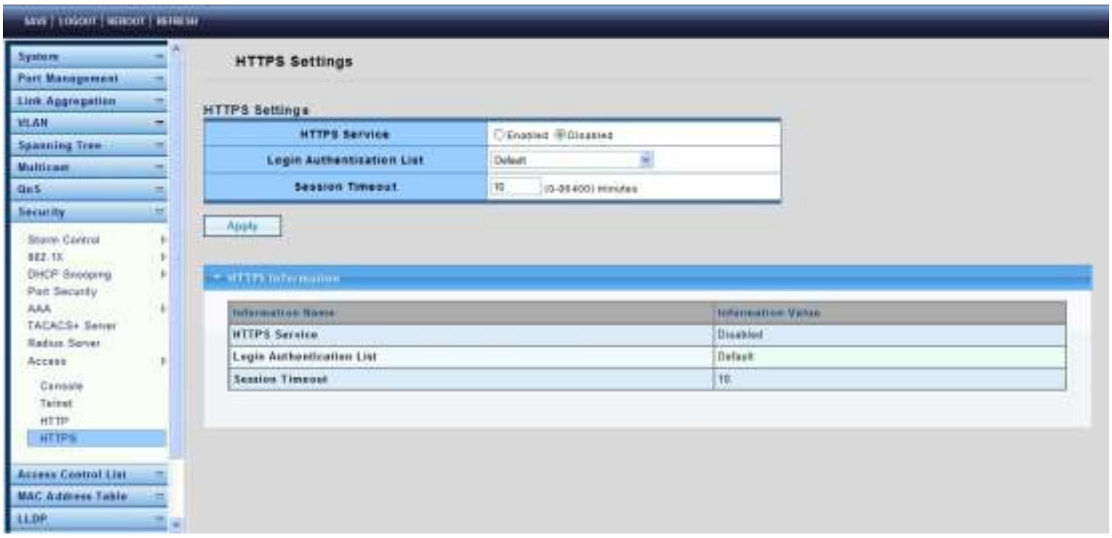
Information Name	Information Value
HTTP Service	Enabled
Login Authentication List	Default
Session Timeout	10

HTTP Server: Set to disable or enable.
Login Authentication List: Select one of the login authentication lists we configured in “Login List” page.
Session Timeout: Set session timeout minutes for user access WEB from HTTP protocol. If user does not response after session timeout minute, WEBUI will logout automatically. 0 minutes means “Never timeout.”

4.8.8.4 HTTPS

To display the HTTPS page, click **Security > Access > HTTPS.**

This page allows you to combine all kinds of AAA lists on the HTTPS line. Attempts to access the switch’s Web UI from HTTPS will be authenticated by AAA lists combined here.



HTTPS Settings

HTTPS Settings

HTTPS Service	○ Enabled ● Disabled
Login Authentication List	Default
Session Timeout	10 (0-86400) minutes

HTTPS Information

Information Name	Information Value
HTTPS Service	Disabled
Login Authentication List	Default
Session Timeout	10

HTTPS Server: Set to disable or enable.

Login Authentication List: Select one of the Login Authentication Lists configured on the Login List page.

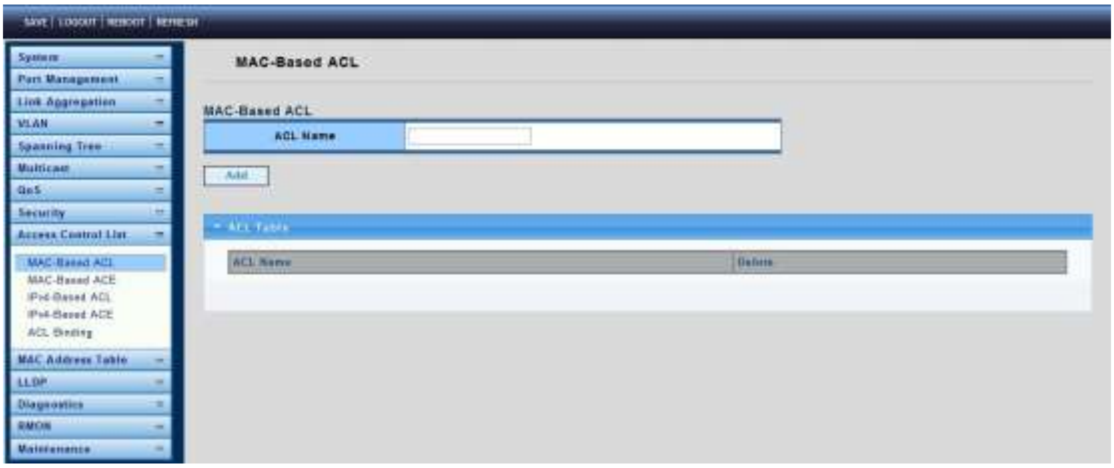
Session Timeout: Set the session timeout minutes for user access via the HTTPS protocol. If a user does not respond before the session times out, Web UI will log out automatically. 0 minutes means “Never timeout.”

4.9 Access Control List

4.9.1 MAC-Based ACL

To display the MAC-Based ACL page, click **Access Control List > MAC-Based ACL.**

This page allows you to set a name for MAC-Based ACL.



MAC-Based ACL

MAC-Based ACL

ACL Name	

ACL Table

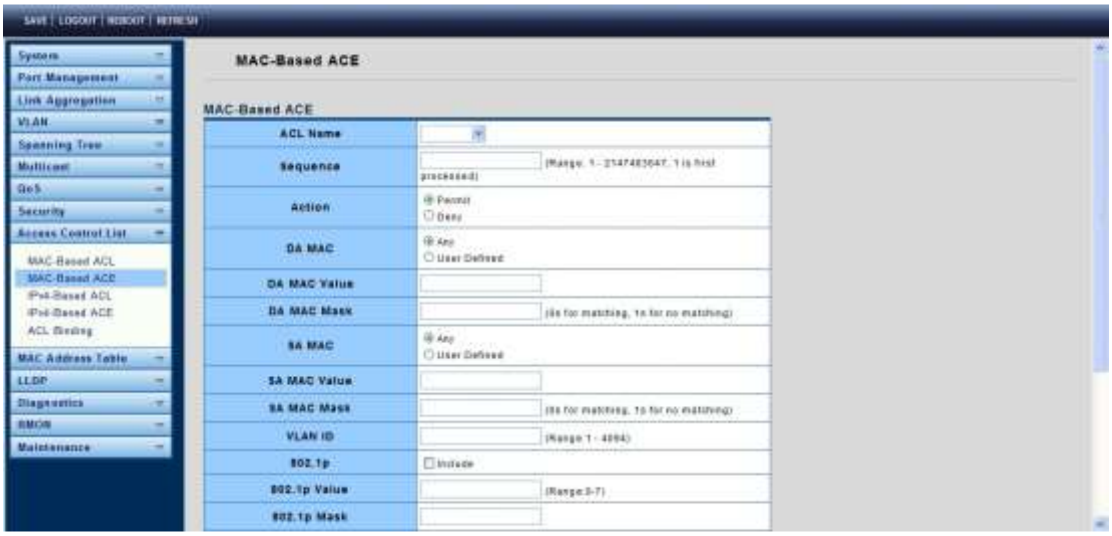
ACL Name	Delete

ACL Name: Enter an ACL name in this field.

4.9.2 MAC-Based ACE

To display the MAC-Based ACE page, click **Access Control List > MAC-Based ACE.**

This page allows you to set the Based-on-MAC-address Expanding ACL List, matching corresponding MACs and setting the ports as drop or forward.



MAC-Based ACE

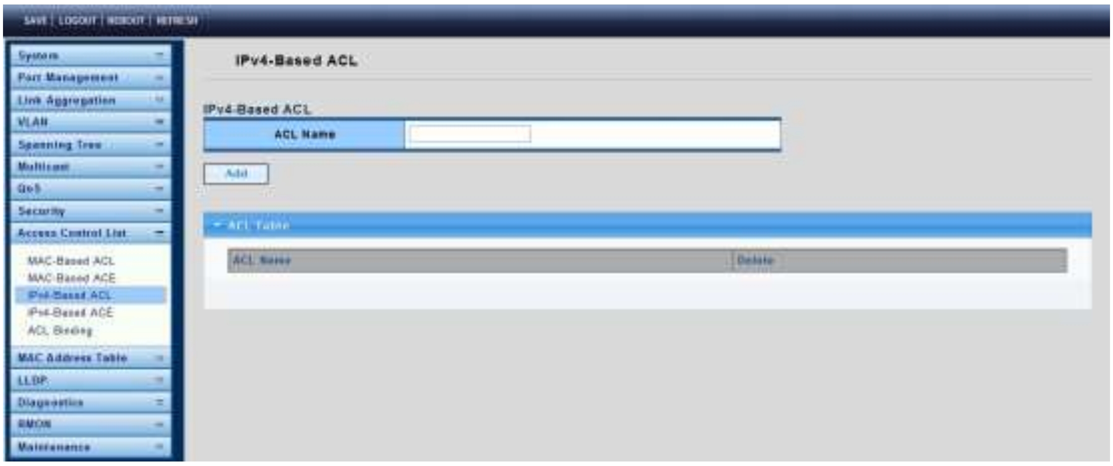
MAC-Based ACE

ACL Name	
Sequence	(Range: 1 - 2147483647, 1 is first processed)
Action	● Permit ○ Deny
DA MAC	● Any ○ User Defined
DA MAC Value	
DA MAC Mask	(0s for matching, 1s for no matching)
SA MAC	● Any ○ User Defined
SA MAC Value	
SA MAC Mask	(0s for matching, 1s for no matching)
VLAN ID	(Range 1 - 4094)
802.1p	□ Include
802.1p Value	(Range:0-7)
802.1p Mask	

4.9.3 IPv4-Based ACL

To display the IPv4-Based ACL page, click **Access Control List > IPv4-Based ACL.**

This page allows you to set a name for IPv4-Based ACL.



IPv4-Based ACL

IPv4-Based ACL

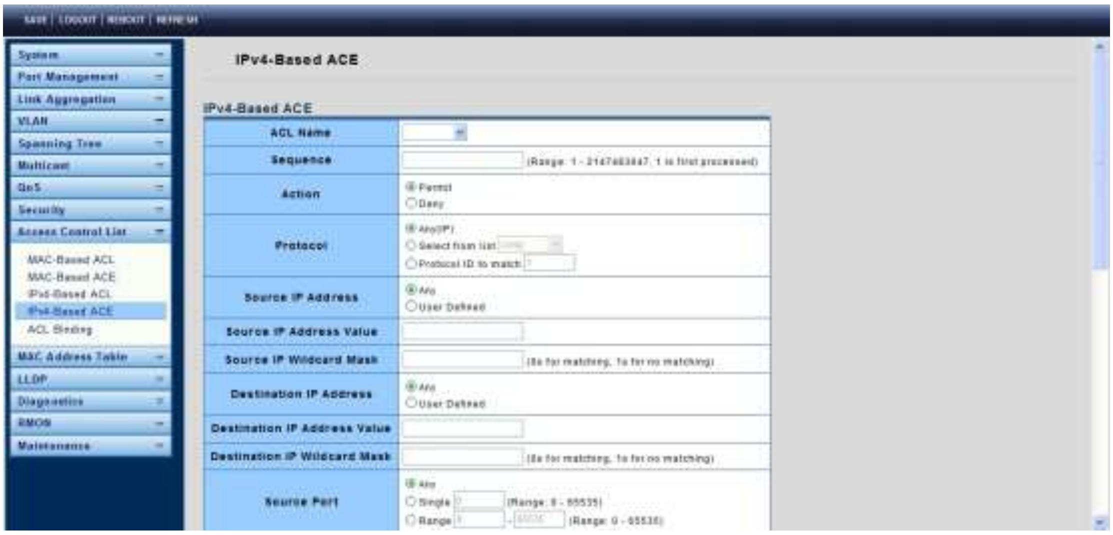
ACL Name	

ACL Name	Delete

4.9.4 IPv4-Based ACE

To display the IPv4-Based ACE page, click **Access Control List > IPv4-Based ACE.**

This page allows you to set Based-on-IPv4 expanding ACL Peer Guardian and matching corresponding IP and setting the port as drop or forward.



IPv4-Based ACE

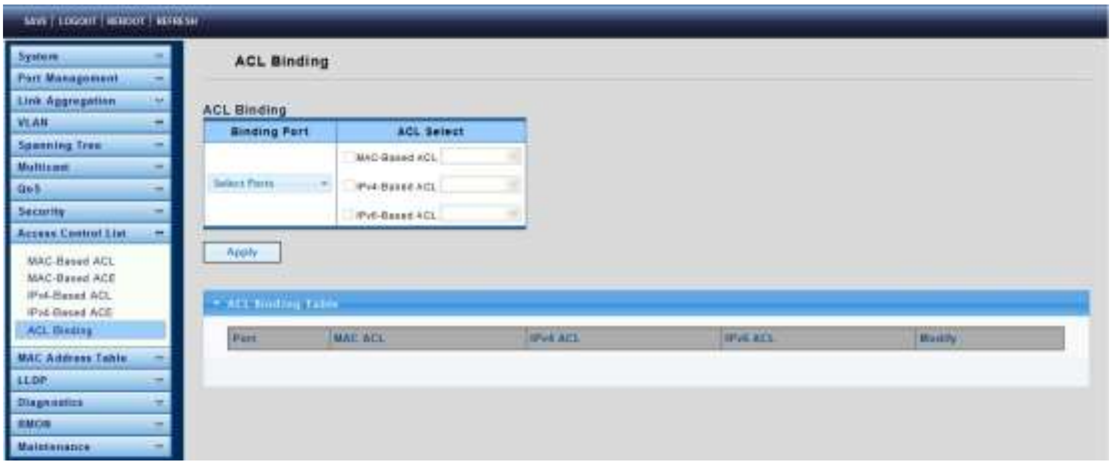
IPv4-Based ACE

ACL Name	
Sequence	(Range: 1 - 2147483647, 1 is first processed)
Action	● Permit ○ Deny
Protocol	● Any(IP) ○ Select from list ○ Protocol ID to match
Source IP Address	● Any ○ User Defined
Source IP Address Value	
Source IP Wildcard Mask	(0s for matching, 1s for no matching)
Destination IP Address	● Any ○ User Defined
Destination IP Address Value	
Destination IP Wildcard Mask	(0s for matching, 1s for no matching)
Source Port	● Any ○ Single (Range: 0 - 65535) ○ Range - (Range: 0 - 65535)

4.9.5 ACL Binding

To display the ACL Binding page, click **Access Control List > ACL Binding.**

This page allows you to establish Binding in accordance with ACL rules.



ACL Binding

ACL Binding

Binding Port	ACL Select
Select Ports	□ MAC-Based ACL □ IPv4-Based ACL □ IPv6-Based ACL

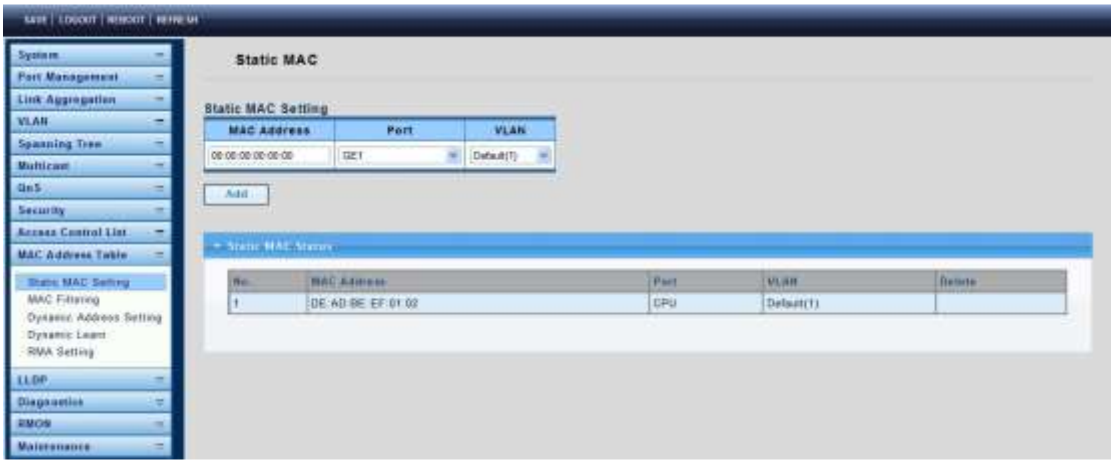
ACL Binding Table

Port	MAC ACL	IPv4 ACL	IPv6 ACL	Modify

4.10 MAC Address Table

4.10.1 Static MAC Setting

To display the Static Mac Setting page, click **Mac Address Table > Static Mac Setting.**



Static MAC

Static MAC Setting

MAC Address	Port	VLAN
00:00:00:00:00:00	GE1	Default(1)

Static MAC Status

No.	MAC Address	Port	VLAN	Delete
1	DE:AD:BE:EF:01:02	CPU	Default(1)	

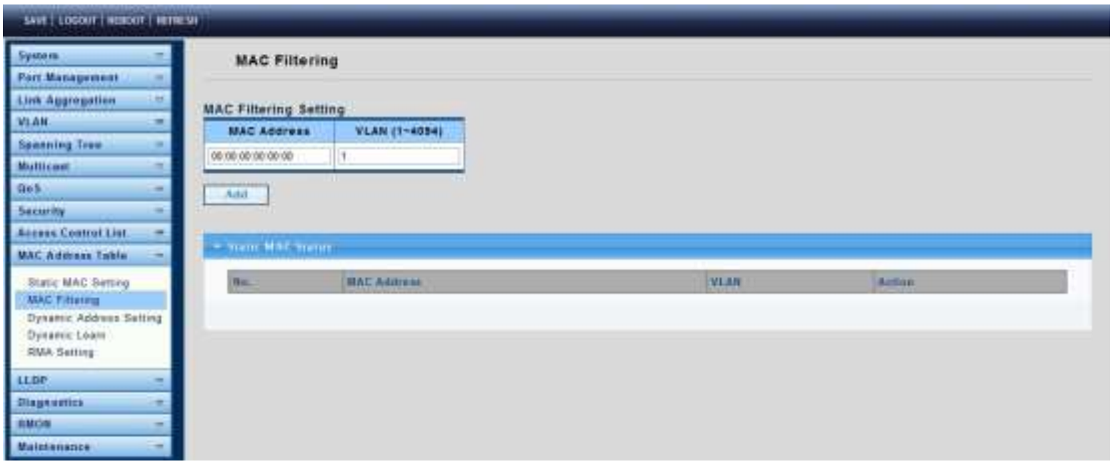
MAC Address: The MAC address to which packets will be statically forwarded. If Type is unicast, enter unicast MAC address in this field; If Type is multicast, enter multicast MAC address in this field.

Port: If Type is unicast, select the port number of the MAC entry; If Type is multicast, select the port list of the MAC entry.

VLAN: The VLAN ID number of the VLAN on which the above MAC address resides.

4.10.2 MAC Filtering

To display the MAC Filtering page, click **Mac Address Table > MAC Filtering.**



MAC Filtering

MAC Filtering Setting

MAC Address	VLAN (1~4094)
00:00:00:00:00:00	1

Static MAC Status

No.	MAC Address	VLAN	Action

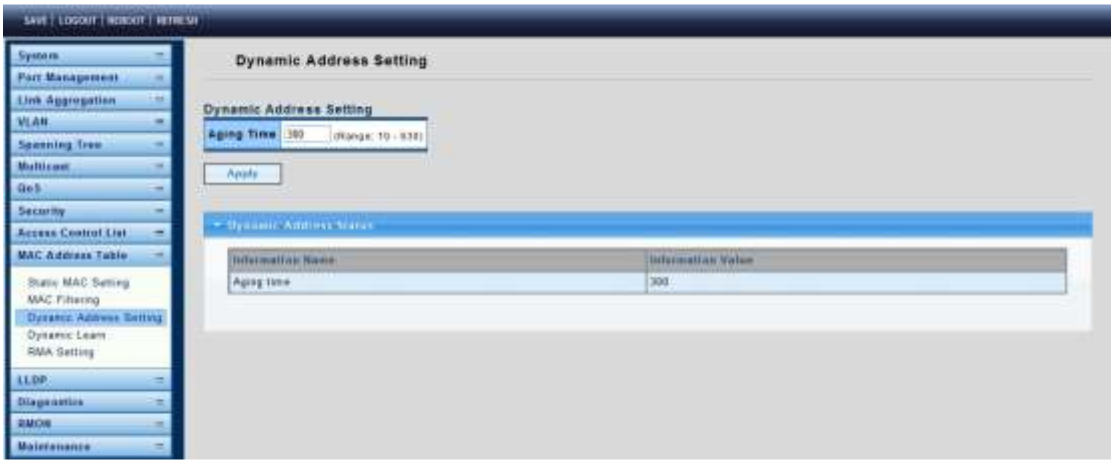
MAC Address: The MAC address to which packets will be filtered. This must be a unicast MAC address.

VLAN: The VLAN ID number of the VLAN on which the above MAC address resides.

4.10.3 Dynamic Address Setting

To display the Dynamic Address Setting page, click **Mac Address Table > Dynamic Address Setting.**

This page is used to set the MAC address of the aging time to study.



Dynamic Address Setting

Dynamic Address Setting

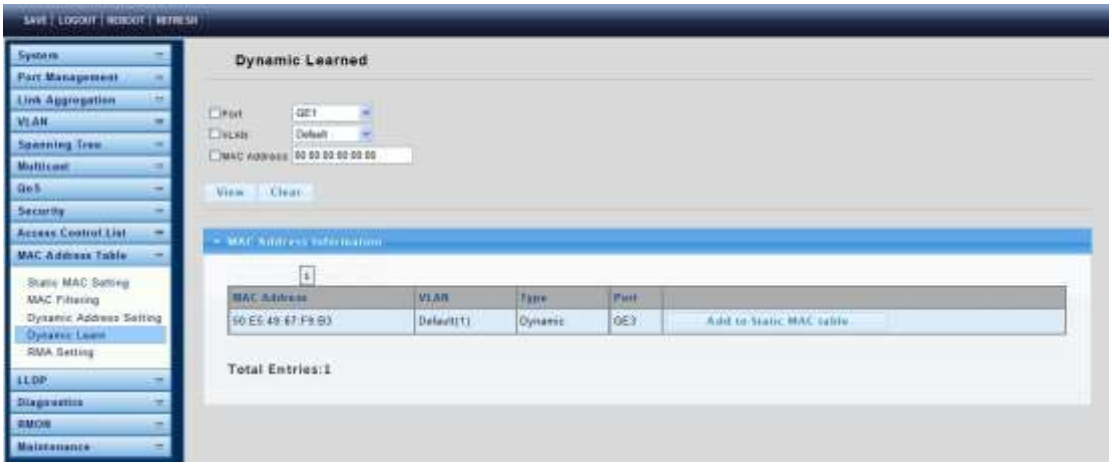
Aging Time: 300 (Range: 10 - 630)

Information Name	Information Value
Aging time	300

Aging Time: Set the time needed for aging.

4.10.4 Dynamic Learn

To display the Dynamic Learn page, click **Mac Address Table > Dynamic Learn.**



Dynamic Learned

□ Port: GE1
□ VLAN: Default
□ MAC Address: 00:00:00:00:00:00

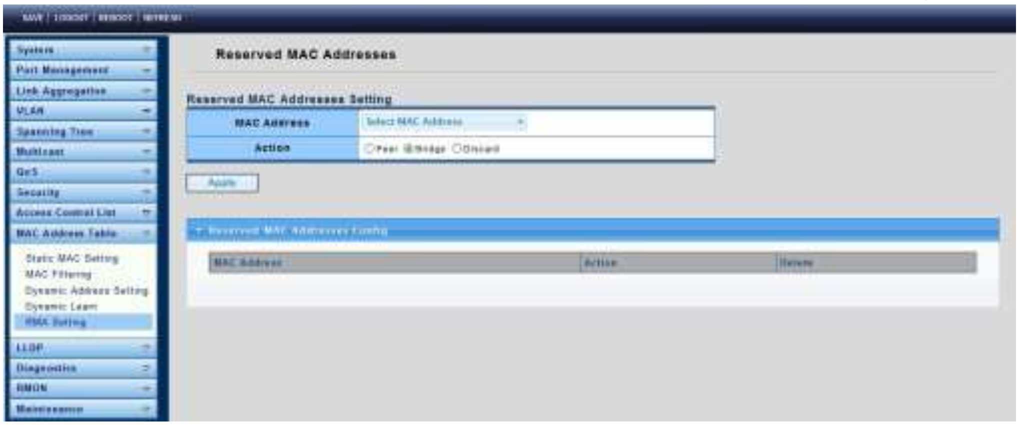
MAC Address	VLAN	Type	Port	
50:E5:49:67:F9:B3	Default(1)	Dynamic	GE3	Add to Static MAC table

Total Entries:1

Port: Select the port number to show or clear dynamic MAC entries. If not selecting any port, VLAN or MAC address, the whole dynamic MAC table will be displayed or cleared.
VLAN: Select the VLAN to show or clear dynamic MAC entries. If not selecting any port, VLAN or MAC address, the whole dynamic MAC table will be displayed or cleared.
MAC Address: Select the MAC address to show or clear dynamic MAC entries. If not selecting any port, VLAN or MAC address, the whole dynamic MAC table will be displayed or cleared.

4.10.5 RMA Setting

To display the RMA Setting page, click **Mac Address Table > RMA Setting.**



Reserved MAC Addresses

Reserved MAC Addresses Setting

MAC Address	Select MAC Address
Action	○Peer ●Bridge ○Discard

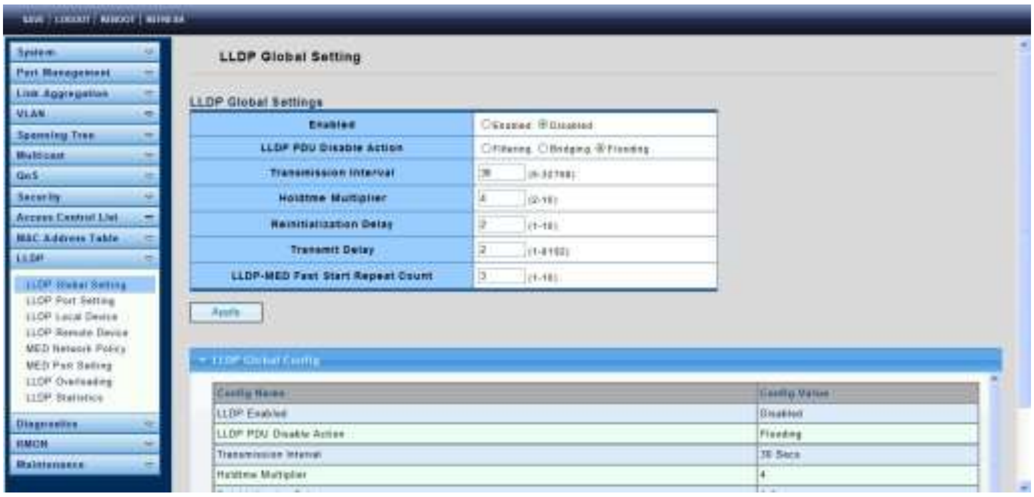
MAC Address	Action	Delete

4.11 LLDP

LLDP is a one-way protocol; there are no request/response sequences. Information is advertised by stations implementing the transmit function, and is received and processed by stations implementing the receive function.

4.11.1 LLDP Global Setting

To display the LLDP Global Settings page, click **LLDP > LLDP Global Setting.**



LLDP Global Setting

LLDP Global Settings

Enabled	○Enabled ●Disabled
LLDP PDU Disable Action	○Filtering ○Bridging ●Flooding
Transmission Interval	30 (5-32768)
Holdtime Multiplier	4 (2-10)
Reinitialization Delay	2 (1-10)
Transmit Delay	2 (1-8192)
LLDP-MED Fast Start Repeat Count	3 (1-10)

Config Name	Config Value
LLDP Enabled	Disabled
LLDP PDU Disable Action	Flooding
Transmission Interval	30 Secs
Holdtime Multiplier	4

Enabled: Enable/Disable the LLDP protocol on this switch.

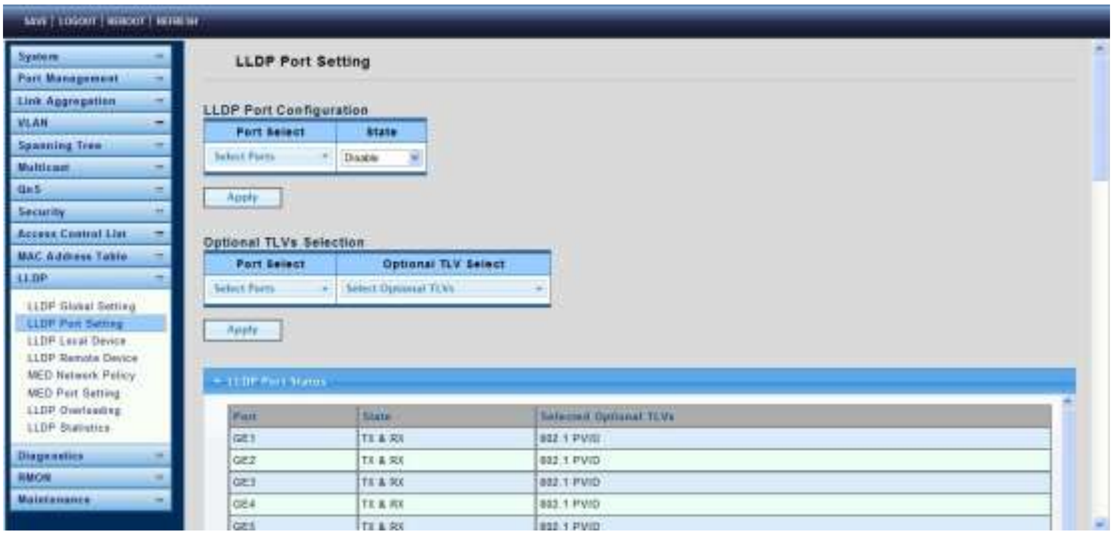
Transmission Interval: Select the interval at which frames are transmitted. The default is 30 seconds, and the valid range is 5-32768 seconds.

Holdtime Multiplier: Select the multiplier onthe transmit interval to assign to TTL (range 2-10, default = 4).

Reinitialization Delay: Select the delay before a re-initialization (range 1-10 seconds, default = 2).

4.11.2 LLDP Port Setting

To display the LLDP Port Settings page, click **LLDP > LLDP Port Setting.**



LLDP Port Setting

LLDP Port Configuration

Port Select	State
Select Ports	Disable

Optional TLVs Selection

Port Select	Optional TLV Select
Select Ports	Select Optional TLVs

Port	State	Selected Optional TLVs
GE1	TX & RX	802.1 PVID
GE2	TX & RX	802.1 PVID
GE3	TX & RX	802.1 PVID
GE4	TX & RX	802.1 PVID
GE5	TX & RX	802.1 PVID

Port Select: Select a specific port or all ports to configure transmission state.

State: Select the transmission state of the LLDP port interface.

- Disable: Disable the transmission of LLDP PDUs.
- RX Only: Receive LLDP PDUs only.
- TX Only: Transmit LLDP PDUs only.
- TX And RX: Transmit and receive LLDP PDUs both Select specified port or all port configure transmission state.

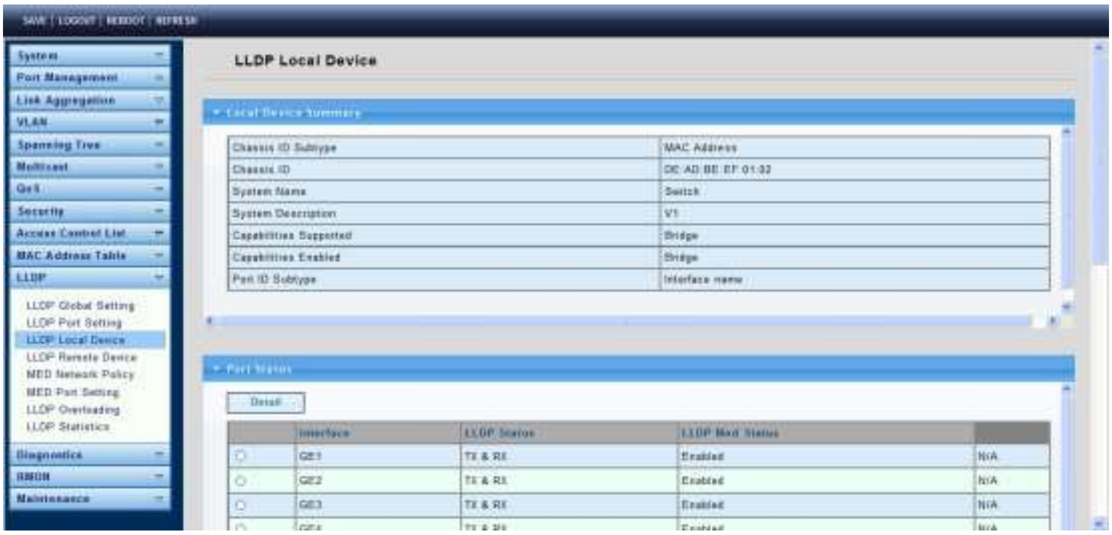
Port Select: Select specific ports.

Optional TLV Select: Select Optional TLVs.

4.11.3 LLDP Local Device

To display the LLDP Local Device page, click **LLDP > LLDP Local Device.**

Use the LLDP Local Device page to view information about devices on the network for which the switch has received LLDP information.



LLDP Local Device

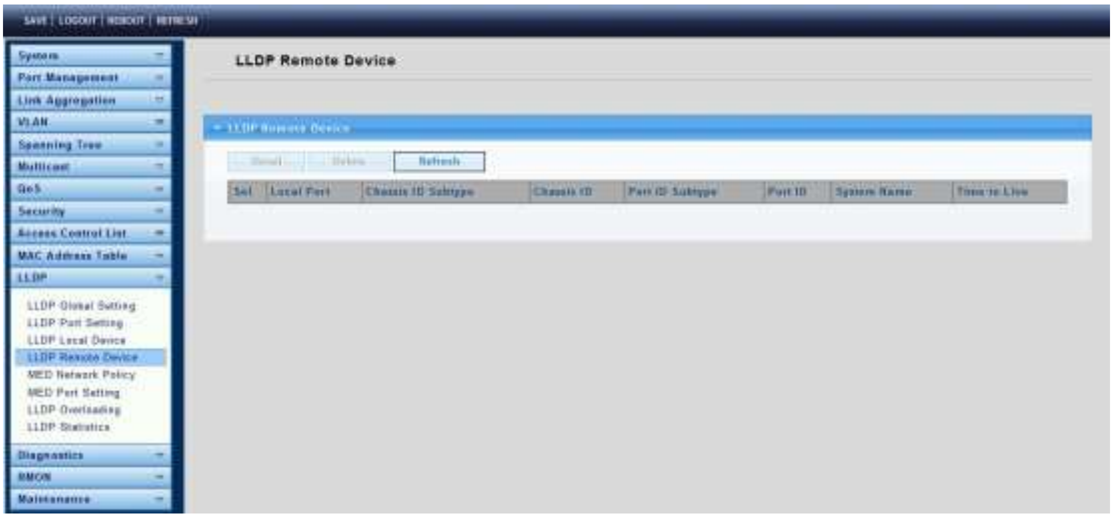
Chassis ID Subtype	MAC Address
Chassis ID	DE:AD:BE:EF:01:02
System Name	Switch
System Description	V1
Capabilities Supported	Bridge
Capabilities Enabled	Bridge
Port ID Subtype	Interface name

	Interface	LLDP Status	LLDP Med Status	
○	GE1	TX & RX	Enabled	N/A
○	GE2	TX & RX	Enabled	N/A
○	GE3	TX & RX	Enabled	N/A
○	GE4	TX & RX	Enabled	N/A

4.11.4 LLDP Remote Device

To display the LLDP Remote Device page, click **LLDP > LLDP Remote Device.**

Use the LLDP Remote Device page to view information about remote devices for which the switch has received LLDP information.

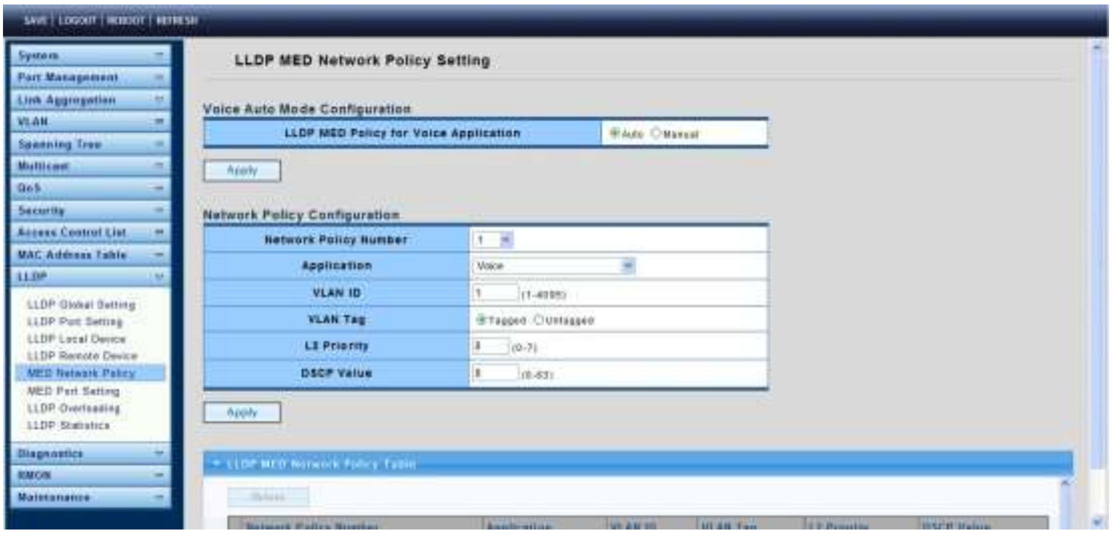


LLDP Remote Device

Sel	Local Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	System Name	Time to Live

4.11.5 MED Network Policy

To display the MED Network Policy page, click **LLDP > MED Network Policy.**



LLDP MED Network Policy Setting

Voice Auto Mode Configuration

LLDP MED Policy for Voice Application	● Auto ○ Manual

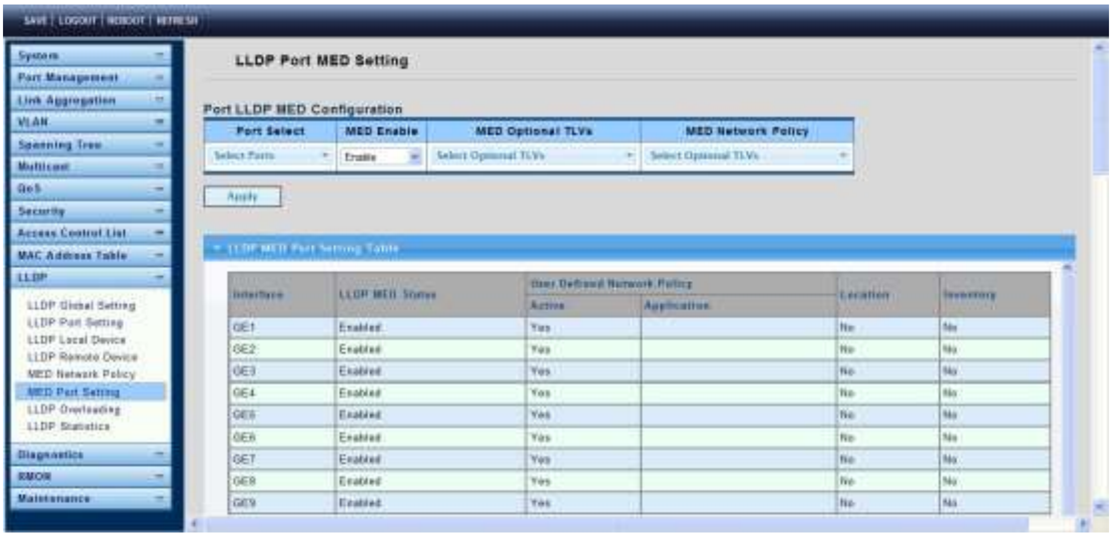
Network Policy Configuration

Network Policy Number	1
Application	Voice
VLAN ID	1 (1-4095)
VLAN Tag	● Tagged ○ Untagged
L2 Priority	3 (0-7)
DSCP Value	8 (0-63)

Network Policy Number	Application	VLAN ID	VLAN Tag	L2 Priority	DSCP Value

4.11.6 MED Port Setting

To display the MED Port Setting page, click **LLDP > MED Port Setting.**



LLDP Port MED Setting

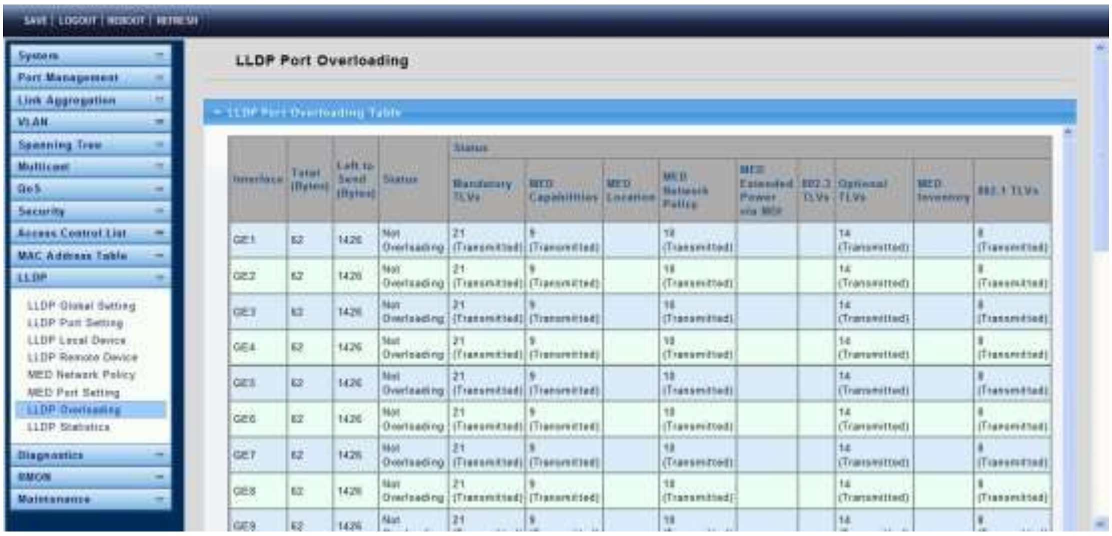
Port LLDP MED Configuration

Port Select	MED Enable	MED Optional TLVs	MED Network Policy
Select Ports	Enable	Select Optional TLVs	Select Optional TLVs

Interface	LLDP MED Status	User Defined Network Policy		Location	Inventory
		Active	Application		
GE1	Enabled	Yes		No	No
GE2	Enabled	Yes		No	No
GE3	Enabled	Yes		No	No
GE4	Enabled	Yes		No	No
GE5	Enabled	Yes		No	No
GE6	Enabled	Yes		No	No
GE7	Enabled	Yes		No	No
GE8	Enabled	Yes		No	No
GE9	Enabled	Yes		No	No

4.11.7 LLDP Overloading

To display the LLDP Overloading page, click **LLDP > LLDP Overloading.**



LLDP Port Overloading

Interface	Total (Bytes)	Left to Send (Bytes)	Status	Status								
				Mandatory TLVs	MED Capabilities	MED Location	MED Network Policy	MED Extended Power via MDI	802.3 TLVs	Optional TLVs	MED Inventory	802.1 TLVs
GE1	62	1426	Not Overloading	21 (Transmitted)	9 (Transmitted)		10 (Transmitted)			14 (Transmitted)		8 (Transmitted)
GE2	62	1426	Not Overloading	21 (Transmitted)	9 (Transmitted)		10 (Transmitted)			14 (Transmitted)		8 (Transmitted)
GE3	62	1426	Not Overloading	21 (Transmitted)	9 (Transmitted)		10 (Transmitted)			14 (Transmitted)		8 (Transmitted)
GE4	62	1426	Not Overloading	21 (Transmitted)	9 (Transmitted)		10 (Transmitted)			14 (Transmitted)		8 (Transmitted)
GE5	62	1426	Not Overloading	21 (Transmitted)	9 (Transmitted)		10 (Transmitted)			14 (Transmitted)		8 (Transmitted)
GE6	62	1426	Not Overloading	21 (Transmitted)	9 (Transmitted)		10 (Transmitted)			14 (Transmitted)		8 (Transmitted)
GE7	62	1426	Not Overloading	21 (Transmitted)	9 (Transmitted)		10 (Transmitted)			14 (Transmitted)		8 (Transmitted)
GE8	62	1426	Not Overloading	21 (Transmitted)	9 (Transmitted)		10 (Transmitted)			14 (Transmitted)		8 (Transmitted)
GE9	62	1426	Not	21	9		10			14		8

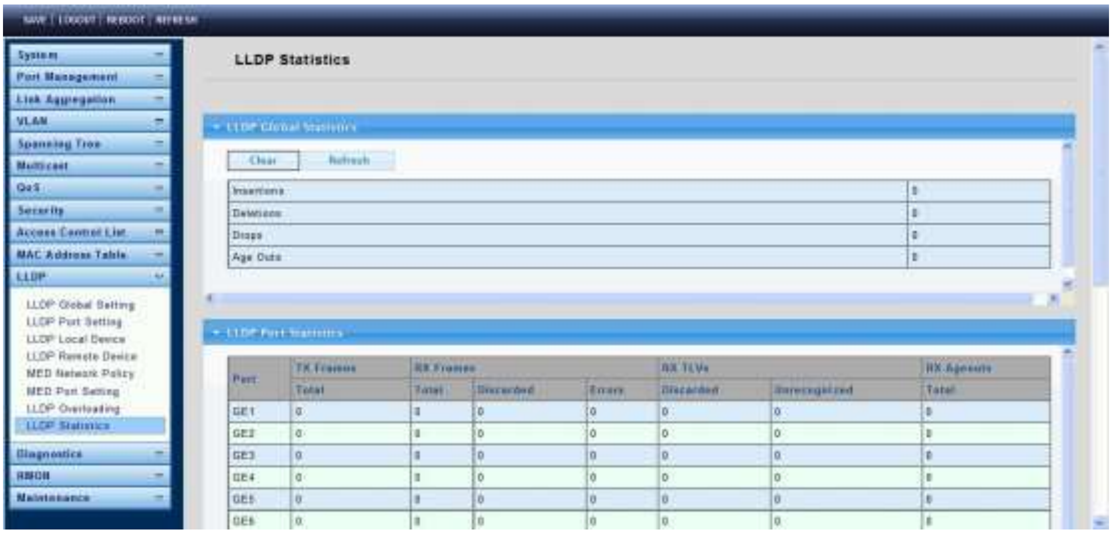
Total (Bytes): Total number of bytes of LLDP information in each packet.

Left to Send (Bytes): Total number of available bytes left for additional LLDP information in each packet.

Status: Whether TLVs are being transmitted or if they are overloaded.

4.11.8 LLDP Statistics

To display the LLDP Statistics page, click **LLDP > LLDP Statistics.**



Insertions	0
Deletions	0
Drops	0
Age Outs	0

Port	TX Frames	RX Frames			RX TLVs		RX Ageouts
	Total	Total	Discarded	Errors	Discarded	Unrecognized	Total
GE1	0	0	0	0	0	0	0
GE2	0	0	0	0	0	0	0
GE3	0	0	0	0	0	0	0
GE4	0	0	0	0	0	0	0
GE5	0	0	0	0	0	0	0
GE6	0	0	0	0	0	0	0

Tx Frames

Total: Number of transmitted frames.

Rx Frames

Total: Number of received frames.

Discarded: Total number of received frames that were discarded.

Errors: Total number of received frames with errors.

Rx TLVs

Discarded: Total number of received TLVs that were discarded.

Unrecognized: Neighbor's Information Deletion Count.

Rx Ageouts

Total: Number of neighbor ageouts on the interface.

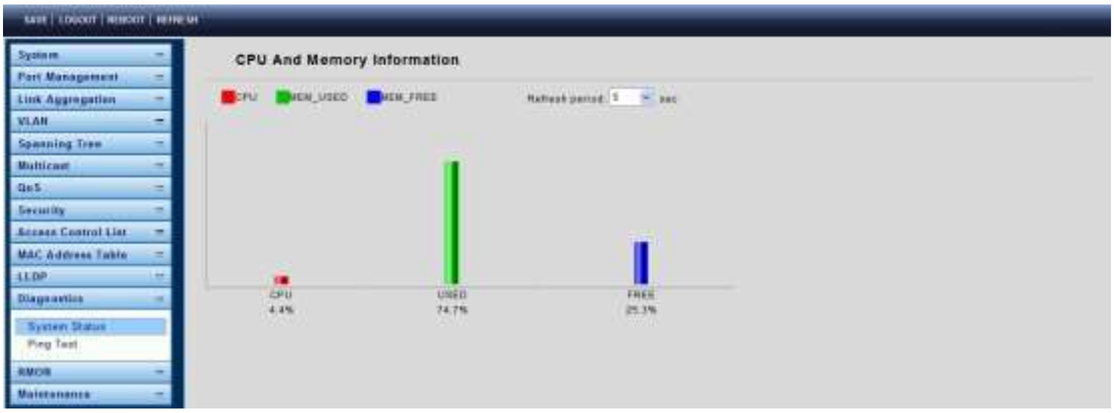
4.12 Diagnostics

Use the Diagnostics pages to configure settings for the switch diagnostics feature or operating diagnostic utilities.

4.12.1 System Status

To display the System Status Log page, click **Diagnostics > System Status.**

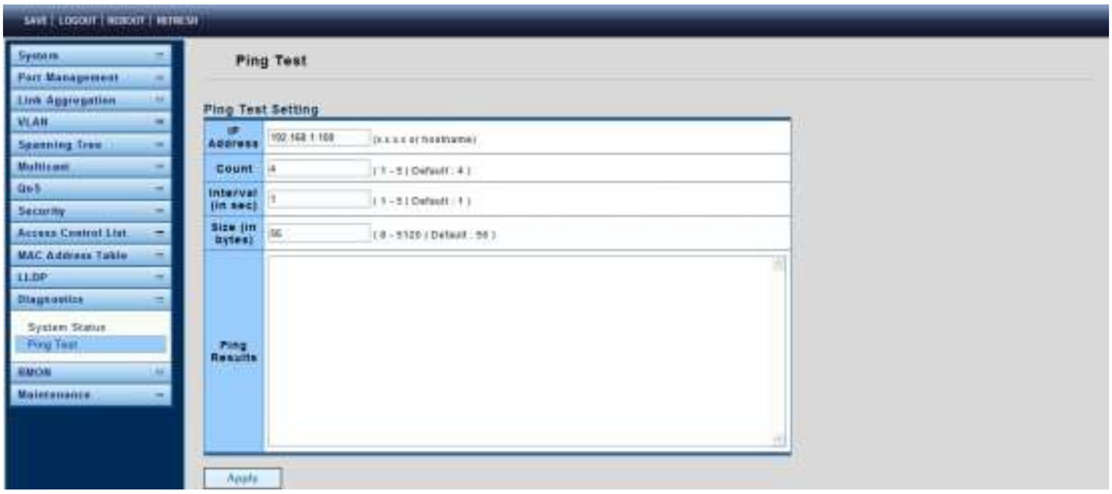
This page is used to display the state of the system operation, CPU resource utilization, used memory and free memory rate, and set the refresh time.



Refresh period: 5 sec

4.12.2 Ping Test

To display the Ping Test Log page, click **Diagnostics > Ping Test.**



Ping Test

Ping Test Setting

IP Address	192.168.1.100	(x.x.x.x or hostname)
Count	4	(1 - 5 | Default : 4)
Interval (in sec)	1	(1 - 5 | Default : 1)
Size (in bytes)	56	(8 - 5120 | Default : 56)
Ping Results		

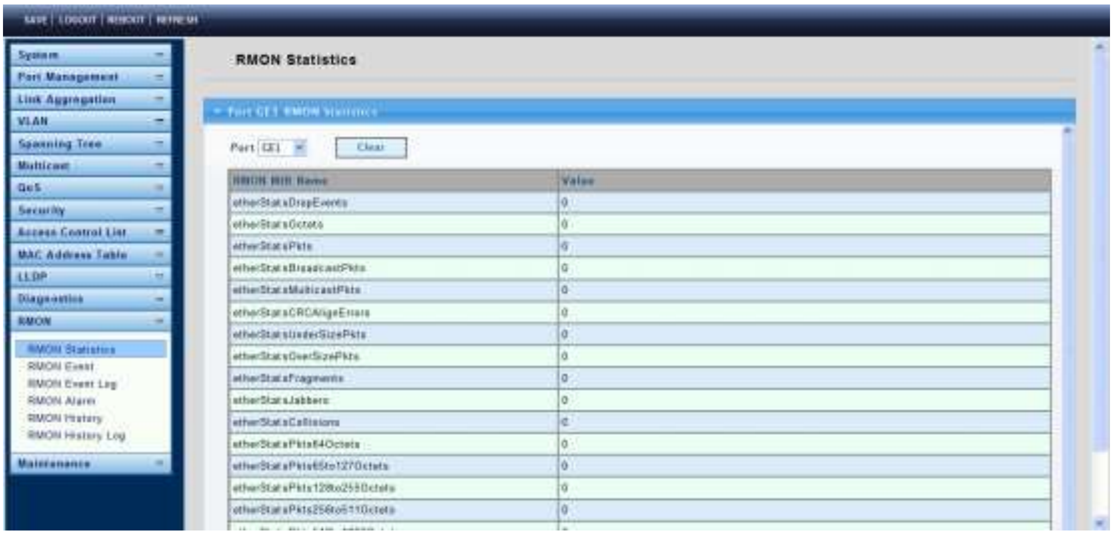
IP Address: The IP address of a ping target.
Count: How many times to send a ping request packet.
Interval: Time interval between each ping request packet.
Size: The size of a ping packet.
Ping Results: After a ping is finished, results will show in this field.

4.13 RMON

4.13.1 RMON Statistics

To display the RMON Statistics page, click **RMON > RMON Statistics.**

The Statistics page displays detailed information regarding packet sizes and information regarding physical layer errors. The information displayed is according to the RMON standard.



RMON Statistics

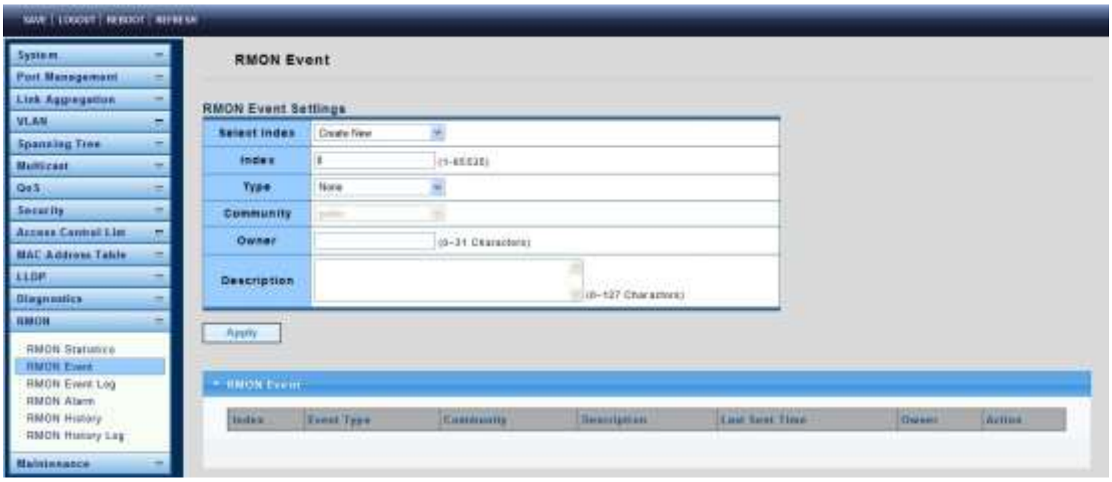
Port GE1

RMON MIB Name	Value
etherStatsDropEvents	0
etherStatsOctets	0
etherStatsPkts	0
etherStatsBroadcastPkts	0
etherStatsMulticastPkts	0
etherStatsCRCAlignErrors	0
etherStatsUnderSizePkts	0
etherStatsOverSizePkts	0
etherStatsFragments	0
etherStatsJabbers	0
etherStatsCollisions	0
etherStatsPkts64Octets	0
etherStatsPkts65to127Octets	0
etherStatsPkts128to255Octets	0
etherStatsPkts256to511Octets	0

4.13.2 RMON Event

To display the RMON Event page, click **RMON > RMON Event.**

This page is used to configure RMON event groups.



RMON Event

RMON Event Settings

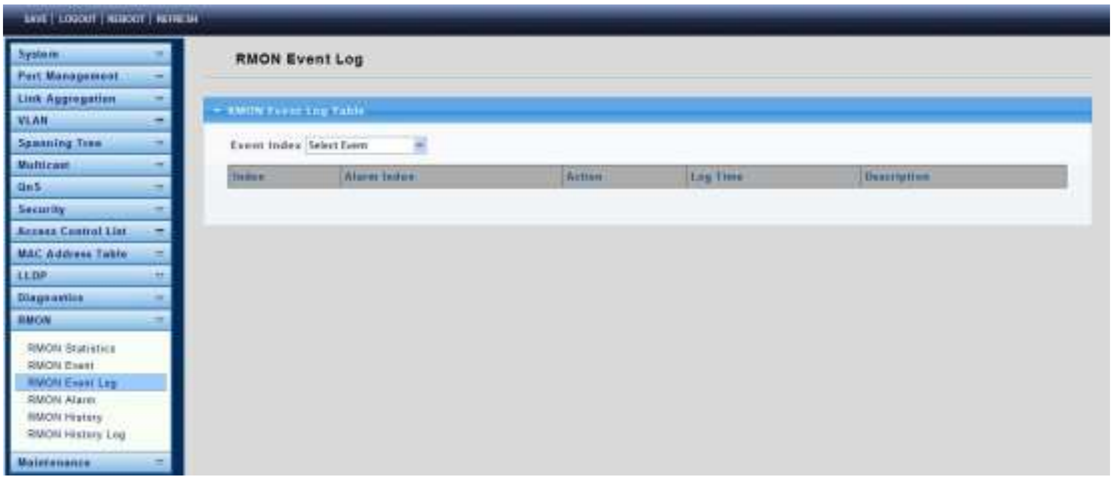
Select Index	Create New
Index	8 (1-65535)
Type	None
Community	public
Owner	(0-31 Characters)
Description	(0-127 Characters)

Index	Event Type	Community	Description	Last Sent Time	Owner	Action

4.13.3 RMON Event Log

To display the RMON Event Log page, click **RMON > RMON Event Log.**

The Event Log Table page displays the log of events (actions) that occurred. Two types of events can be logged: Log or Log and Trap. The action in the event is performed when the event is bound to an alarm (see the Alarms page) and the conditions of the alarm have occurred.



RMON Event Log

RMON Event Log Table

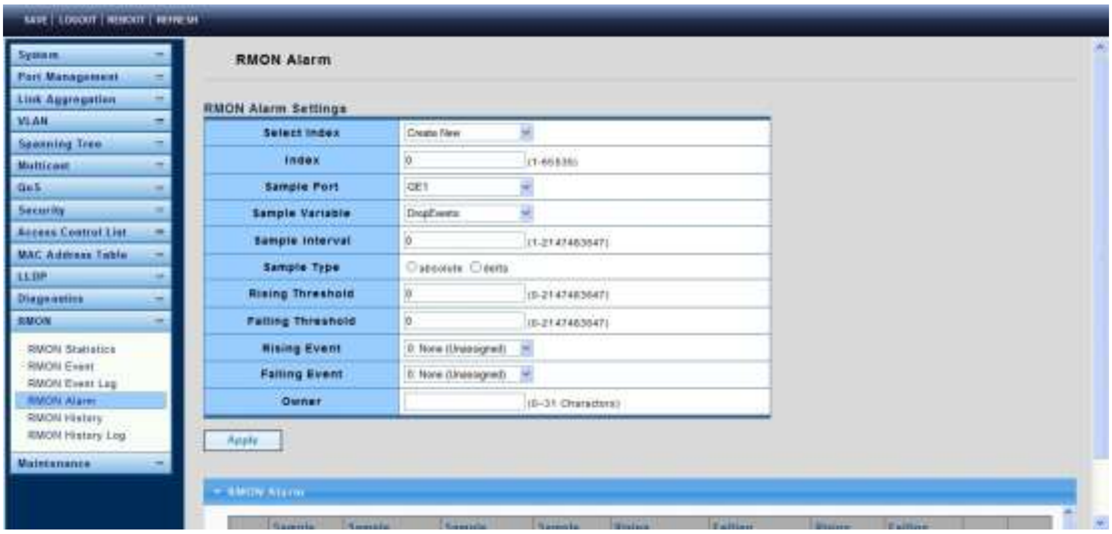
Event Index: Select Event

Index	Alarm Index	Action	Log Time	Description

4.13.4 RMON Alarm

To display the RMON Alarm page, click **RMON > RMON Alarm.**

This page is used to configure RMON statistics group and alarm groups.



RMON Alarm

RMON Alarm Settings

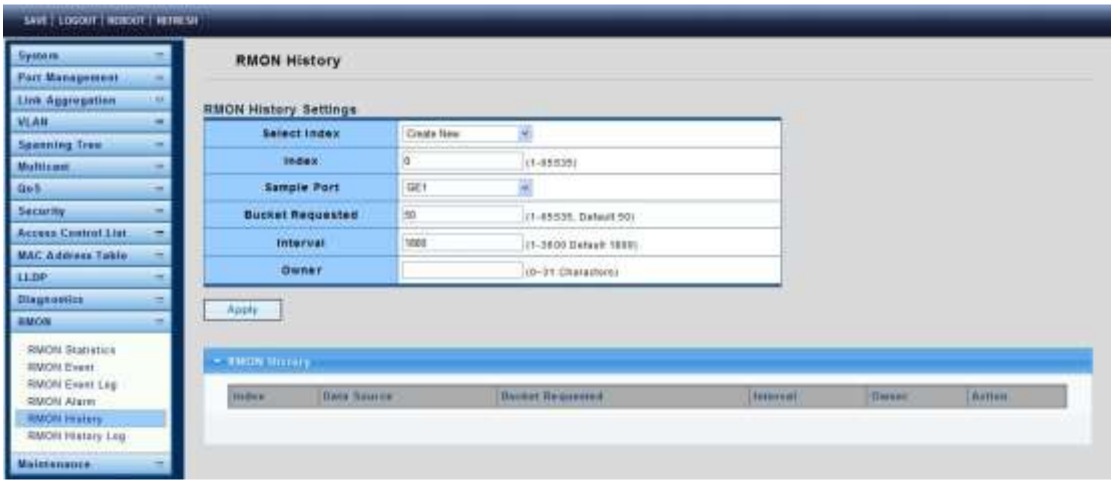
Select Index	Create New
Index	0 (1-65535)
Sample Port	GE1
Sample Variable	DropEvents
Sample Interval	0 (1-2147483647)
Sample Type	○ absolute ○ delta
Rising Threshold	0 (0-2147483647)
Falling Threshold	0 (0-2147483647)
Rising Event	0: None (Unassigned)
Falling Event	0: None (Unassigned)
Owner	(0-31 Characters)

RMON Alarm

4.13.5 RMON History

To display the RMON History page, click **RMON > RMON History.**

This page is used to configure the RMON history group.



RMON History

RMON History Settings

Select Index	Create New	
Index	0	(1-65535)
Sample Port	GE1	
Bucket Requested	50	(1-65535, Default 50)
Interval	1800	(1-3600 Default 1800)
Owner		(0~31 Characters)

RMON History

Index	Data Source	Bucket Requested	Interval	Owner	Action

Index: Displays the number of the new History Table entry.

Sample Port: Select the port of switch.

Bucket Requested: Enter the number of samples to store.

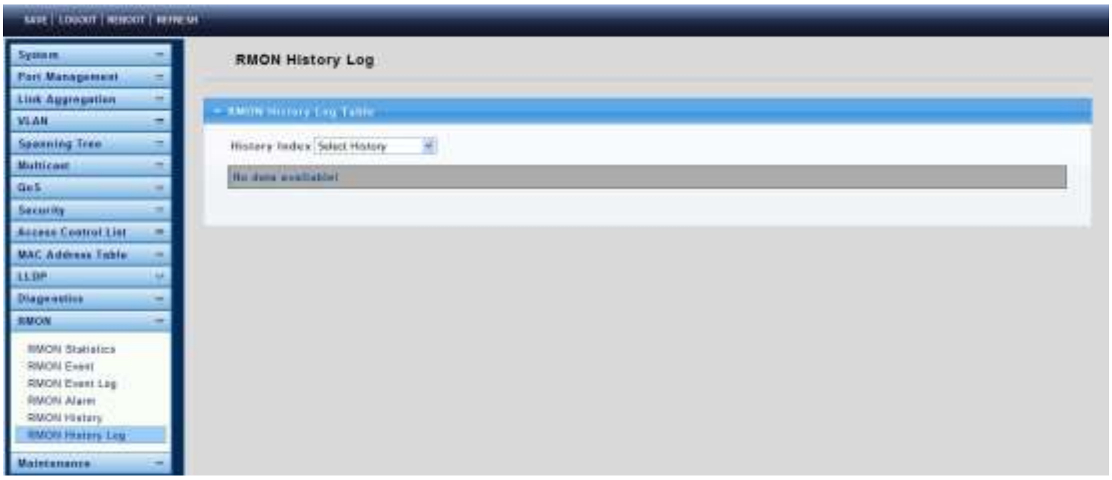
Interval: Enter the time in seconds that samples are collected from the ports. The field range is 1-3600.

Owner: Enter the RMON station or user that requested the RMON information.

4.13.6 RMON History Log

To display the RMON History Log page, click **RMON > RMON History Log.**

The RMON History Log Table page displays interface-specific statistical network samplings. The samples were configured in the History Control table described above.



RMON History Log

RMON History Log Table

History Index: Select History

No data available!

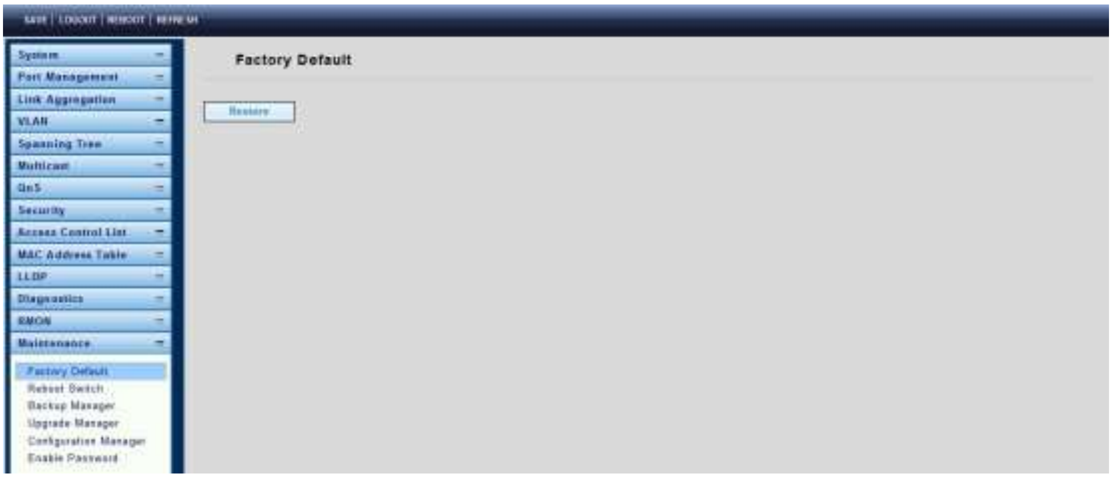
4.14 Maintenance

Use the Maintenance pages to configure settings for the switch network interface and how the switch connects to a remote server to get services.

4.14.1 Factory Default

To display the Factory Default page, click **Maintenance > Factory Default.**

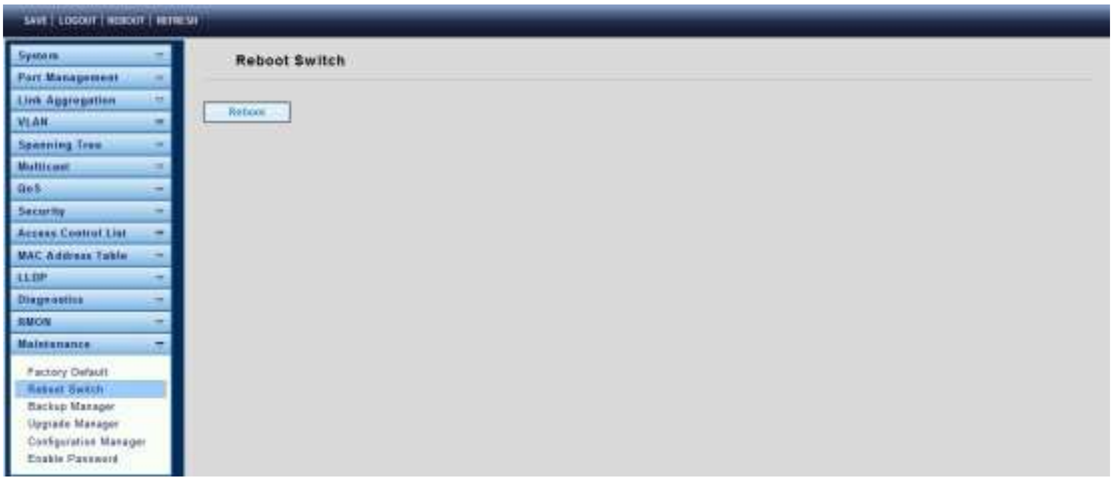
This page allows you to restore factory defaults by clicking the Restore button.



4.14.2 Reboot Switch

To display the Reboot Switch page, click **Maintenance > Reboot Switch.**

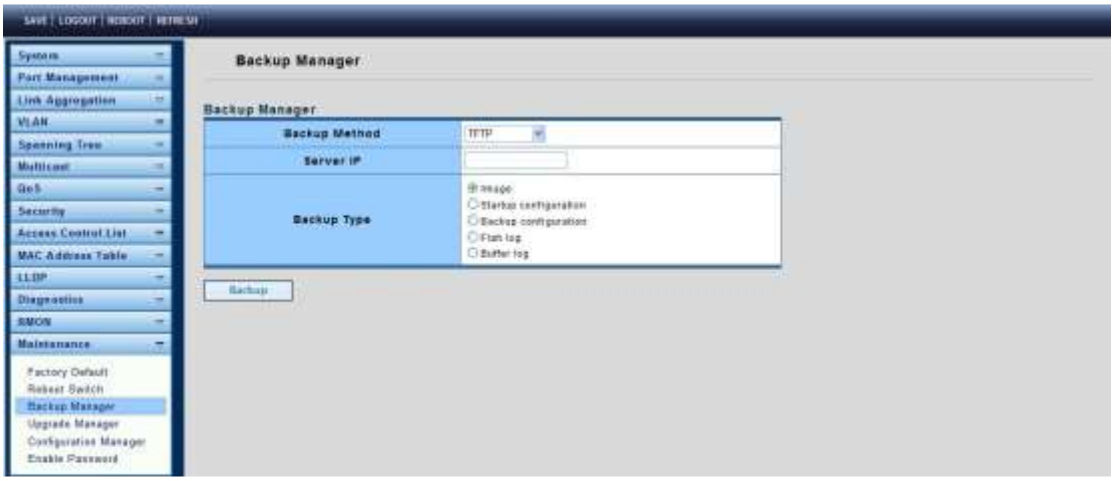
This page allows you to reboot the switch by clicking the Reboot button.



4.14.3 Backup Manager

To display the Backup Manager page, click **Maintenance > Backup Manager.**

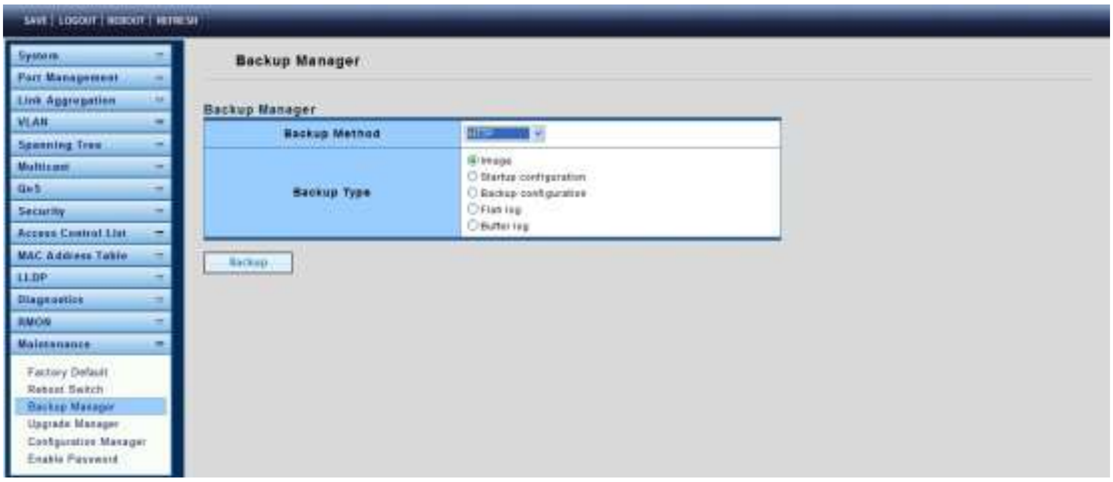
This page allows you to back up the firmware image or configuration file on the switch to a remote TFTP server or host file system via the HTTP protocol.



Backup Manager

Backup Manager

Backup Method	TFTP
Server IP	
Backup Type	● Image ○ Startup configuration ○ Backup configuration ○ Flash log ○ Buffer log



Backup Manager

Backup Manager

Backup Method	HTTP
Backup Type	● Image ○ Startup configuration ○ Backup configuration ○ Flash log ○ Buffer log

Backup Method: Select a backup method.

- TFTP: Use TFTP to backup.
- HTTP: Use HTTP to backup.

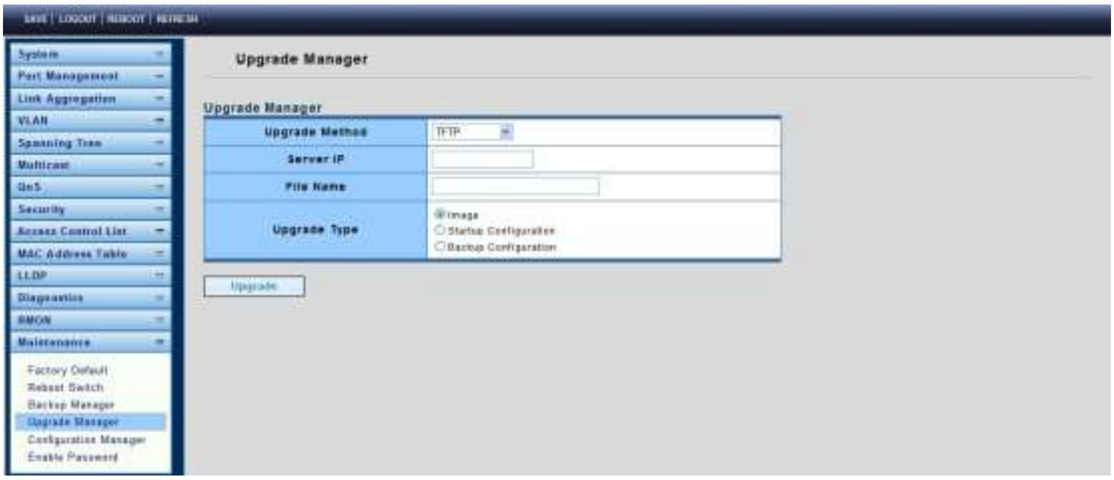
Server IP: IP address of the TFTP server. If the TFTP backup method is selected, the IP address of the TFTP server must be assigned.

Backup Type: Select Backup Type.

4.14.4 Upgrade Manager

To display the Upgrade Manager page, click **Maintenance > Upgrade Manager.**

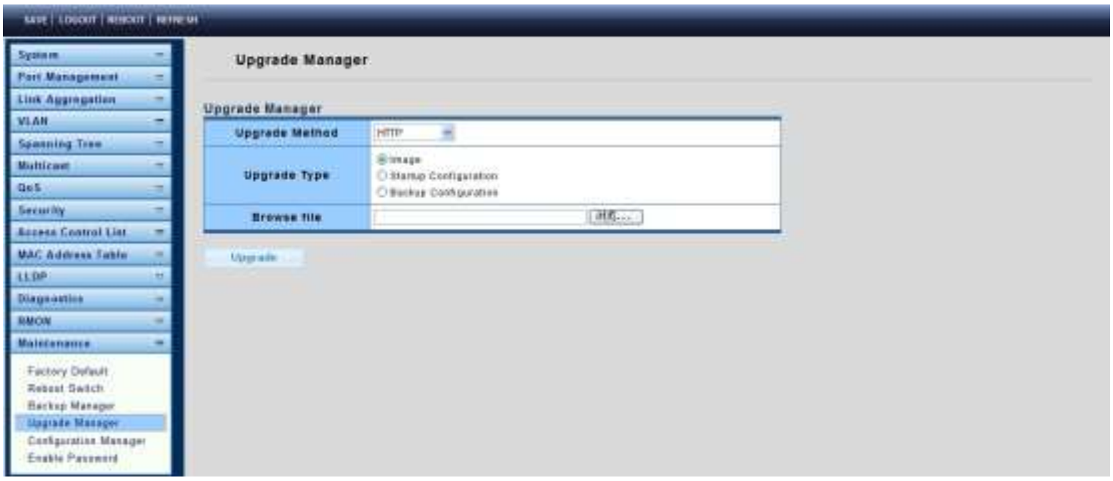
This page allows you to upgrade new firmware images or configuration files to the switch from a remote TFTP server or to select files using a Web browser.



Upgrade Manager

Upgrade Manager

Upgrade Method	TFTP
Server IP	
File Name	
Upgrade Type	● Image ○ Startup Configuration ○ Backup Configuration



Upgrade Manager

Upgrade Manager

Upgrade Method	HTTP
Upgrade Type	● Image ○ Startup Configuration ○ Backup Configuration
Browse file	

Upgrade Method: Select the upgrade method.

- TFTP: Use TFTP to upgrade.
- HTTP: Use HTTP to upgrade.

Server IP: IP address of the TFTP server. If the TFTP upgrade method is selected, the IP address of the TFTP server must be assigned.

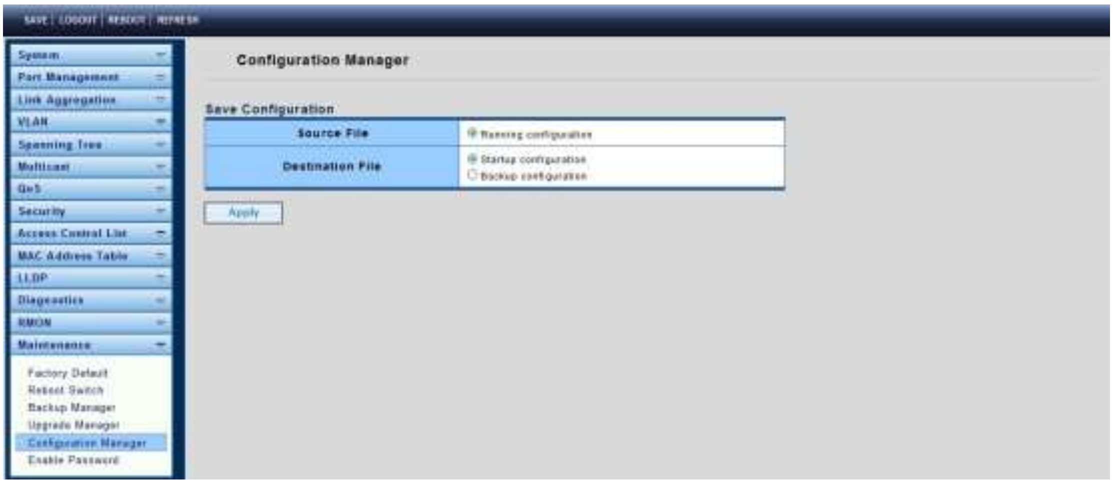
File Name: Firmware image or configuration file name on remote TFTP server. If the TFTP upgrade method is selected, the file name must be specified.

Browse file: If the HTTP upgrade method is selected, the browse file field allows you to select any file on the host operating system.

Upgrade Type: Select Backup Type.

4.14.5 Configuration Manager

To display the Configuration Manager page, click **Maintenance > Configuration Manager.**



Configuration Manager

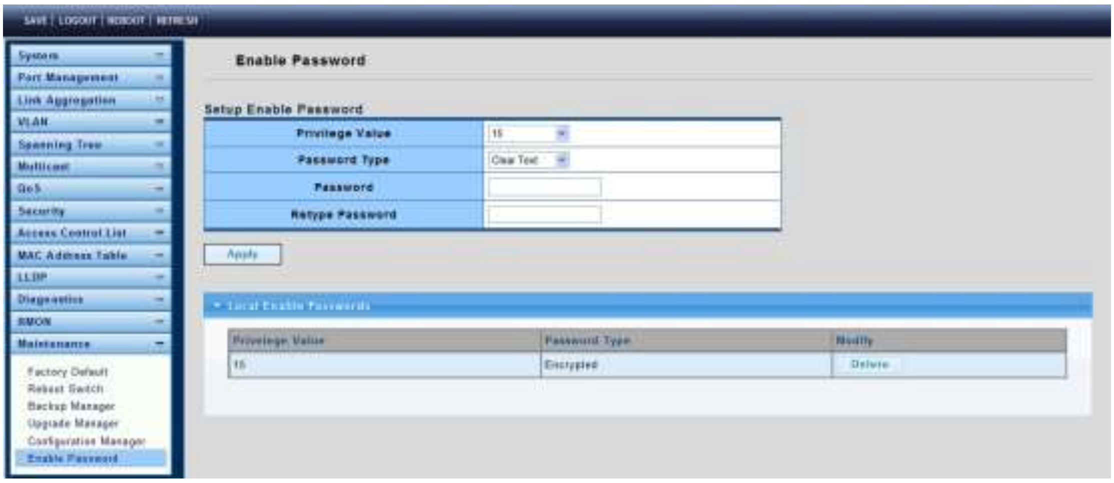
Save Configuration

Source File	● Running configuration
Destination File	● Startup configuration ○ Backup configuration

4.14.6 Enable Password

To display the Enable Password page, click **Maintenance > Enable Password.**

This page allows you to modify the enable password. In the command line interface, you can use “enable” to change the privilege level to “Admin.” After the “enable” command is issued, you need to enter the enable password to change the privilege level.



Enable Password

Setup Enable Password

Privilege Value	15
Password Type	Clear Text
Password	
Retype Password	

Local Enable Passwords

Privilege Value	Password Type	Modify
15	Encrypted	Delete

Password Type: Select the password type for Enable Password.

- Clear Text: Password without encryption.
- Encrypted: Password with encryption.

Password: Password string.

Retype Password: Re-enter the password to make sure the password is exactly what was entered in the “Password” field.