

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

USER MANUAL

MODEL 560917

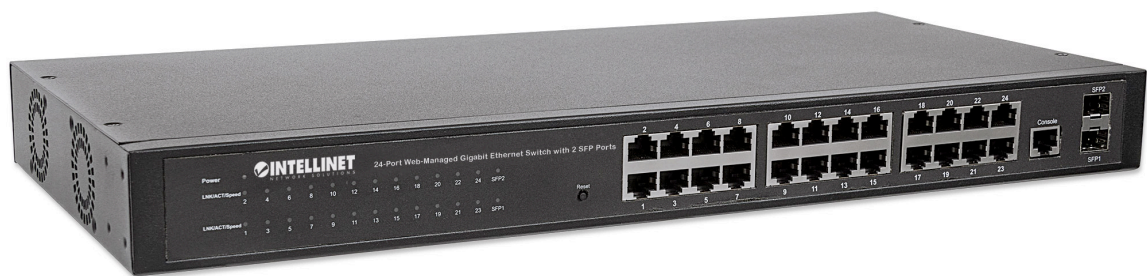


Table of Contents

Chapter 1 Product Introduction	4
1.1 Product Overview.....	4
1.2 Features.....	4
1.3 External Component Description	5
1.3.1 Front Panel.....	5
1.3.2 Rear Panel	6
1.4 Package Contents	7
Chapter 2 Installing and Connecting the Switch	8
2.1 Installation.....	8
2.1.1 Desktop Installation	8
2.1.2 Rack-mountable Installation in 19-inch Cabinet	9
2.1.3 Power on the Switch	9
Chapter 3 How to Login the Switch	11
3.1 Switch to End Node	11
3.2 How to Login the Switch.....	11
Chapter 4 Switch Configuration	13
4.1 Status.....	13
4.1.1 System Information.....	13
4.1.2 IP Configuration	14
4.1.3 User Configuration	14
4.1.4 Time Settings.....	15
4.1.5 Log Management	16
4.1.6 SNMP Management.....	18
4.2 Port Management	23
4.2.1 Port Configuration.....	23
4.2.2 Port Counters	23
4.2.3 Bandwidth Utilization	24
4.2.4 Port Mirroring	24
4.2.5 Jumbo Frame	25
4.2.6 Port Error Disabled Configuration.....	25
4.2.7 Port Error Disabled Status.....	26
4.3 Link Aggregation.....	26
4.3.1 LAG Setting.....	26
4.3.2 LAG Management	26
4.3.3 LAG Port Setting.....	27
4.3.4 LACP Setting	27
4.3.5 LACP Port Setting	28
4.3.6 LAG Status	28
4.4 VLAN.....	29
4.4.1 Create VLAN	29
4.4.2 Interface Settings	29
4.4.3 Port to VLAN	30

4.4.4 Port VLAN Membership	31
4.4.5 Protocol VLAN Group Setting	31
4.4.6 Protocol VLAN Port Setting	32
4.5 Spanning Tree.....	32
4.5.1 STP Global Setting	32
4.5.2 STP Port Setting.....	33
4.5.3 CIST Instance Setting.....	34
4.5.4 CIST Port Setting	35
4.5.5 MST Instance Setting	35
4.5.6 MST Port Setting	36
4.5.7 STP Statistics	36
4.6 Multicast.....	37
4.6.1 Properties.....	37
4.6.2 IGMP Snooping	37
4.6.3 IGMP Snooping Statistics	40
4.6.4 Multicast Throttling Setting	41
4.6.5 Multicast Filter	41
4.7 QoS.....	43
4.7.1 General.....	43
4.7.2 QoS Basic Mode	45
4.7.3 QoS Advanced Mode.....	46
4.7.4 Rate Limit	50
4.8 Security.....	52
4.8.1 Storm Control.....	52
4.8.2 802.1X	53
4.8.3 DHCP Snooping	55
4.8.4 Port Security.....	59
4.8.5 AAA	60
4.8.6 Tacacs+ Server	63
4.8.7 Radius server.....	64
4.8.8 Access.....	64
4.9 Access Control List.....	67
4.9.1 MAC-Based ACL.....	67
4.9.2 MAC-Based ACE	67
4.9.3 IPv4-Based ACL.....	68
4.9.4 IPv4-Based ACE	68
4.9.5 ACL Binding	69
4.10 MAC Address Table	70
4.10.1 Static MAC Setting	70
4.10.2 MAC Filtering	70
4.10.3 Dynamic Address Setting	71
4.10.4 Dynamic Learn	71
4.10.5 RMA Setting	72
4.11 LLDP	72

4.11.1 LLDP Global Setting	72
4.11.2 LLDP Port Setting.....	73
4.11.3 LLDP Local Device.....	73
4.11.4 LLDP Remote Device	74
4.11.5 MED Network Policy	74
4.11.6 MED Port Setting.....	75
4.11.7 LLDP Overloading	75
4.11.8 LLDP Statistics	76
4.12 Diagnostics	77
4.12.1 System Status.....	77
4.12.2 Ping Test.....	77
4.13 RMON	78
4.13.1 RMON Statistics	78
4.13.2 RMON Event.....	78
4.13.3 RMON Event Log	78
4.13.4 RMON Alarm	79
4.13.5 RMON History	79
4.13.6 RMON History Log.....	80
4.14 Maintenance	80
4.14.1 Factory Default.....	80
4.14.2 Reboot Switch	81
4.14.3 Backup Manager	81
4.14.4 Upgrade Manager	82
4.14.5 Configuration Manager	83
4.14.6 Enable Password	84

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.

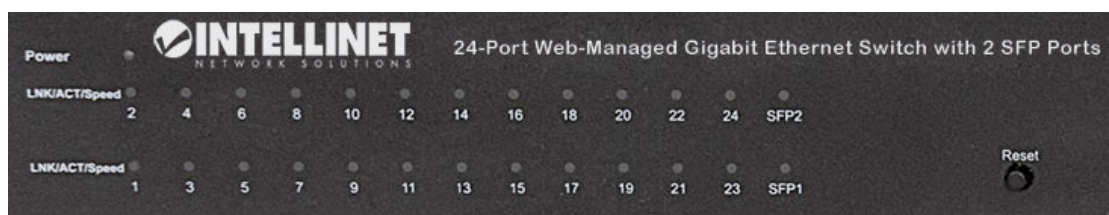


Figure 2 - LED Indicators

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
		Off	A device is disconnected to the port
	1000Mbps: Green	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.

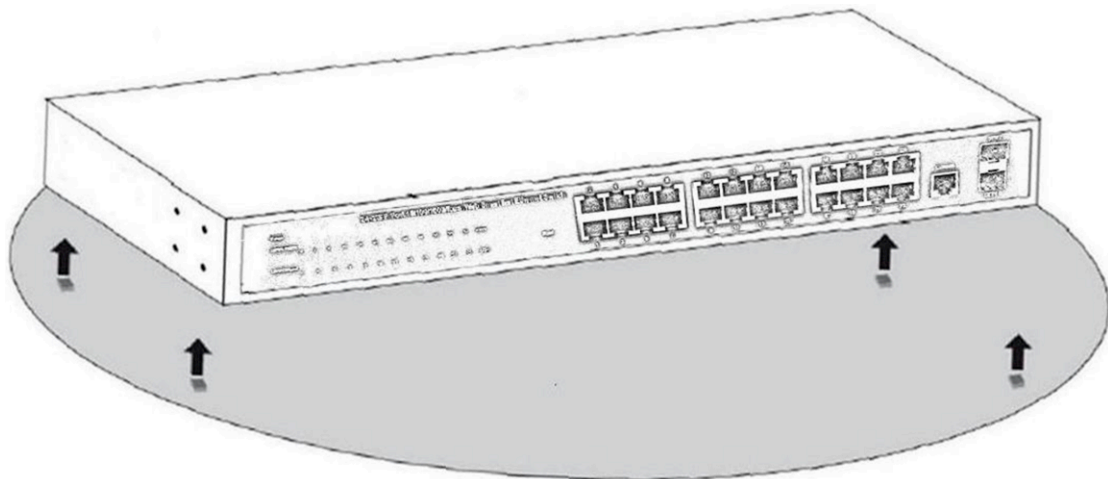


Figure 4 - Desktop Installation

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.

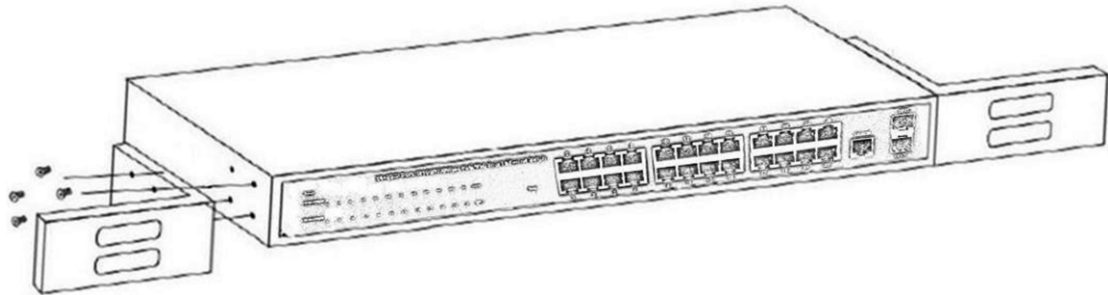


Figure 5 - Bracket Installation

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

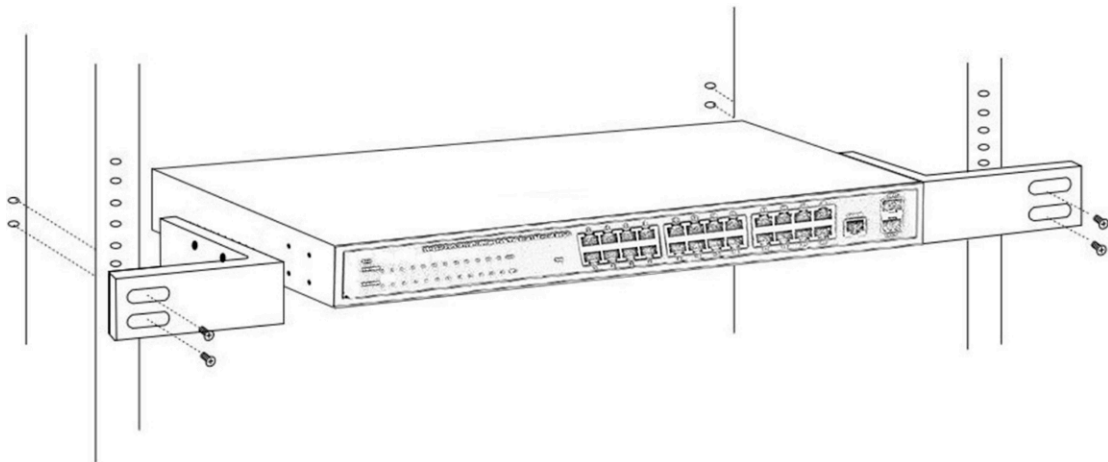


Figure 6 - Rack Installation

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.

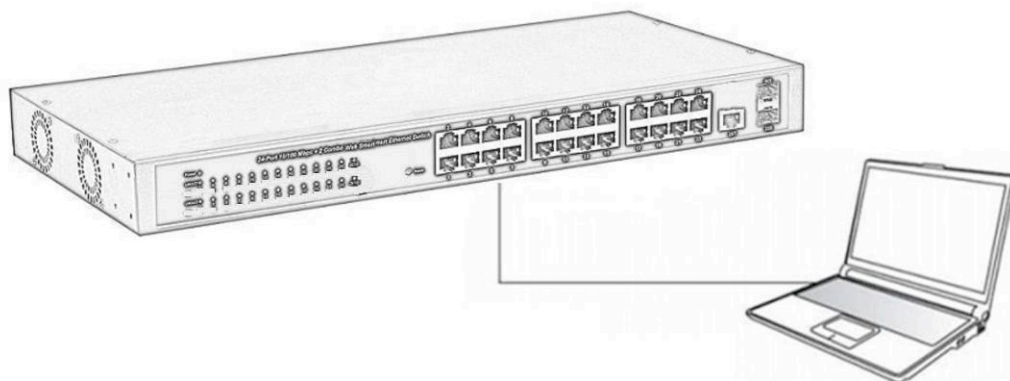


Figure 7 - PC Connect

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

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.



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.

24-Port Web-Managed Gigabit Ethernet Switch with 2 SFP Ports

[SAVE](#) | [LOGOUT](#) | [REBOOT](#) | [REFRESH](#)

10/100M 1000M

- Status
- Network
- Switching
- MAC Address Table
- Security
- ACL
- QoS
- Management
- Diagnostics
- Maintenance

System Information

System Information

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	2011.12.4.1872
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 m ins, 34 secs

Figure 9 - Configuration Window

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.

The screenshot displays the Web UI for a 24-Port Web-Managed Gigabit Ethernet Switch with 2 SFP Ports. The top navigation bar includes links for SAVE, LOGOUT, REBOOT, and REFRESH. A status bar shows the switch's link status for 10/100M and 1000M ports, along with a port status indicator showing 24 ports (1-24) and two SFP ports (SFP1, SFP2). The left sidebar contains a configuration menu with options: Status, Network, Switching, MAC Address Table, Security, ACL, QoS, Management, Diagnostics, and Maintenance. The main content area is titled "System Information" and displays a table of system information.

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	2011.12.4.1872
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.

SAVE | LOGOUT | REBOOT | REFRESH

System Information

Information Name	Information Value
System Name	Switch
System Description	Default Location
System Contact	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	2011.12.4.1872
Loader Date	Mar 18 2014 - 11:20:25
Firmware Version	v1.0b140721
Firmware Date	Wed Jul 23 11:16:23 CST 2014
System Object ID	1.3.6.1.4.1.10456.1.1539
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.

SAVE | LOGOUT | REBOOT | REFRESH

IP Address

IP Address Setting

Mode	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Gateway	192.168.2.254

Apply

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.

- ℓ Static: Enable static IP address.
- ℓ 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.

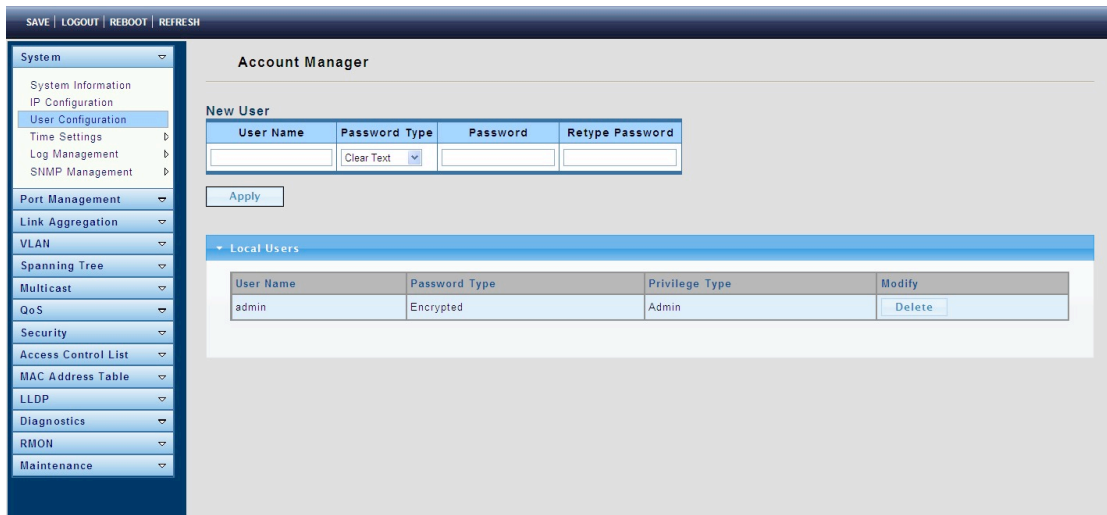
Subnet Mask: If static mode is enabled, enter a subnet mask in this field.

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.

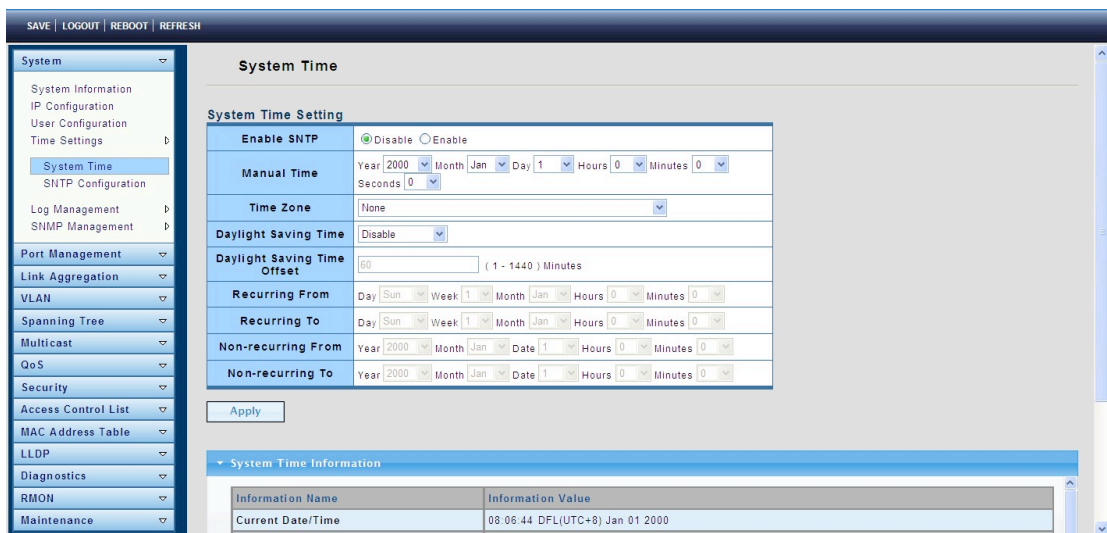


4.1.4 Time Settings

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.



4.1.4.2 SNTP Configuration

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

SAVE | LOGOUT | REBOOT | REFRESH

System

System Information
IP Configuration
User Configuration
Time Settings
System Time
SNTP Configuration
Log Management
SNMP Management

Port Management
Link Aggregation
VLAN
Spanning Tree
Multicast
QoS
Security
Access Control List
MAC Address Table
LLDP
Diagnostics
RMON
Maintenance

SNTP Server Settings

SNTP Server Settings

SNTP/NTP Server Address (X.X.X.X or Hostname)

Server Port (1 - 65535 | Default: 123)

Apply

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.

SAVE | LOGOUT | REBOOT | REFRESH

System

System Information
IP Configuration
User Configuration
Time Settings
Log Management
Logging Service
Local Logging
Remote Syslog
Logging Message
SNMP Management

Port Management
Link Aggregation
VLAN
Spanning Tree
Multicast
QoS
Security
Access Control List
MAC Address Table
LLDP
Diagnostics
RMON

Logging Service

Logging Service Settings

Logging Service Enabled Disabled

Apply

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**.

The screenshot shows the 'Local Logging' configuration page. On the left is a navigation menu with categories like System, Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, Security, Access Control List, MAC Address Table, LLDP, Diagnostics, and RMON. The main content area is titled 'Local Logging' and contains a 'Local Logging Setting' section with two dropdown menus: 'Target' (set to 'Select Targets') and 'Severity' (set to 'Select Levels'). Below these is an 'Apply' button. A 'Local Logging Setting Status' section contains a table with the following data:

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

Target: Select the target to store log messages.

- ℓ RAM: Store log messages in RAM disk. All log messages will disappear after system reboot.
- ℓ 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**.

The screenshot shows the 'Remote Syslog' configuration page. On the left is the same navigation menu as in the previous screenshot. The main content area is titled 'Remote Logging' and contains a 'Remote Logging Setting' section with four fields: 'Server Address' (empty), 'Server Port' (514), 'Severity' (set to 'Select Levels'), and 'Facility' (set to 'local0'). Below these is an 'Apply' button. A 'Remote Logging Setting Status' section contains a table with the following columns: Status, Server Info, Severity, Facility, and Action.

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**.

The screenshot shows the 'Logging Message' configuration page. The left sidebar contains a navigation menu with categories like System, Port Management, VLAN, and Security. The main content area is titled 'Logging Message' and includes a 'Logging Filter Select' section with three dropdown menus: 'Target' (set to 'Buffered'), 'Severity' (set to 'Select Levels'), and 'Category' (set to 'Select Categories'). Below the filters is a 'View' button. The 'Logging Information' section contains a table with the following data:

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

At the bottom of the page, there are two buttons: 'Clear buffered messages' and 'Refresh'.

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

- ℓ RAM: Logs store in the RAM disk.
- ℓ 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**.

The screenshot shows the 'SNMP Setting' configuration page. The left sidebar contains a navigation menu with categories like System, Port Management, VLAN, and Security. The main content area is titled 'SNMP Setting' and includes a 'SNMP Global Setting' section with a 'State' dropdown menu set to 'Disabled'. Below this is an 'SNMP Information' section containing a table with the following data:

Information Name	Information Value
SNMP	Disabled

State: SNMP daemon state.

- ℓ Enabled: Enable SNMP daemon.
- ℓ 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.

The screenshot shows the 'SNMP View' configuration page. On the left is a navigation menu with categories like System, Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, and QoS. The main content area is titled 'SNMP View' and contains two sections:

- View Table Setting:** A table with columns 'View Name', 'Subtree OID', 'Subtree OID Mask', and 'View Type'. The 'Subtree OID Mask' is set to 'All'. There are radio buttons for 'Include' (selected) and 'Exclude'. An 'Add' button is below the table.
- View Table Status:** A table with columns 'View Name', 'Subtree OID', 'OID Mask', 'View Type', and 'Action'. It contains one entry: 'All' with Subtree OID '.1', OID Mask 'All', View Type 'Include', and a 'Delete' button.

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.

The screenshot shows the 'SNMP Access Group' configuration page. On the left is a navigation menu. The main content area is titled 'SNMP Access Group' and contains two sections:

- Access Group Setting:** A table with columns 'Group Name', 'Security Model', 'Security Level', 'Read View Name', 'Write View Name', and 'Notify View Name'. The 'Security Model' is set to 'v1', 'Security Level' to 'Inauth', 'Read View Name' to 'All', 'Write View Name' to 'None', and 'Notify View Name' to 'None'. An 'Add' button is below the table.
- Access Group Status:** A table with columns 'Group Name', 'Security Model', 'Security Level', 'Read View Name', 'Write View Name', 'Notify View Name', and 'Action'. It is currently empty.

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.

The screenshot shows the 'SNMP Community' configuration page. The left sidebar contains a navigation menu with categories like System, Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, and QoS. The main content area is titled 'SNMP Community' and includes a 'Community Setting' table and a 'Community Status' table.

Community Setting

Community Name	Community Mode	Group Name	View Name	Access Right
<input type="text"/>	Basic	<input type="text"/>	All	ro

Community Status

Community Name	Group Name	View Name	Access Right	Action
public		All	rw	<input type="button" value="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.

The screenshot shows the 'SNMP User Table' configuration page. The left sidebar is the same as in the previous screenshot. The main content area is titled 'SNMP User Table' and includes a 'User Setting' table and a 'User Status' table.

User Setting

User Name	Group	Privilege Mode	Authentication Protocol	Authentication Password	Encryption Protocol	Encryption Key
<input type="text"/>	<input type="text"/>	noauth	None	<input type="text"/>	None	<input type="text"/>

User Status

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

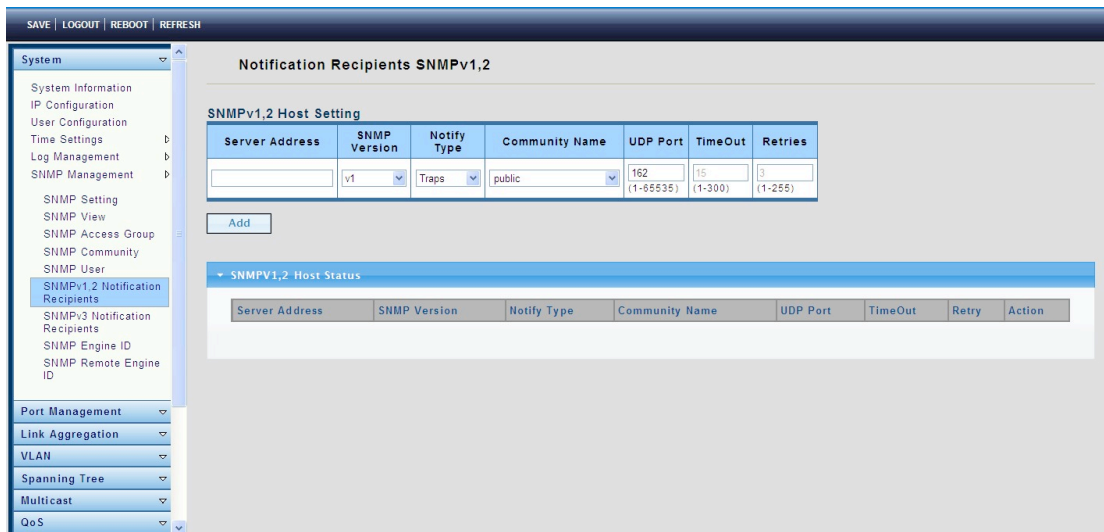
4.1.6.6 SNMPv1,2 Notification Recipients

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

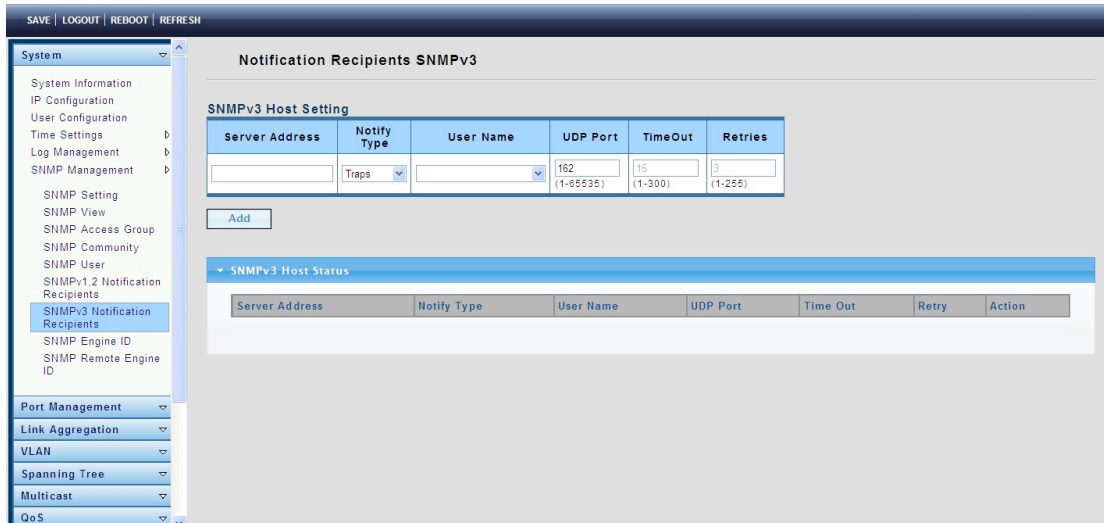
attributes of the notifications.



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.



4.1.6.8 SNMP Engine ID

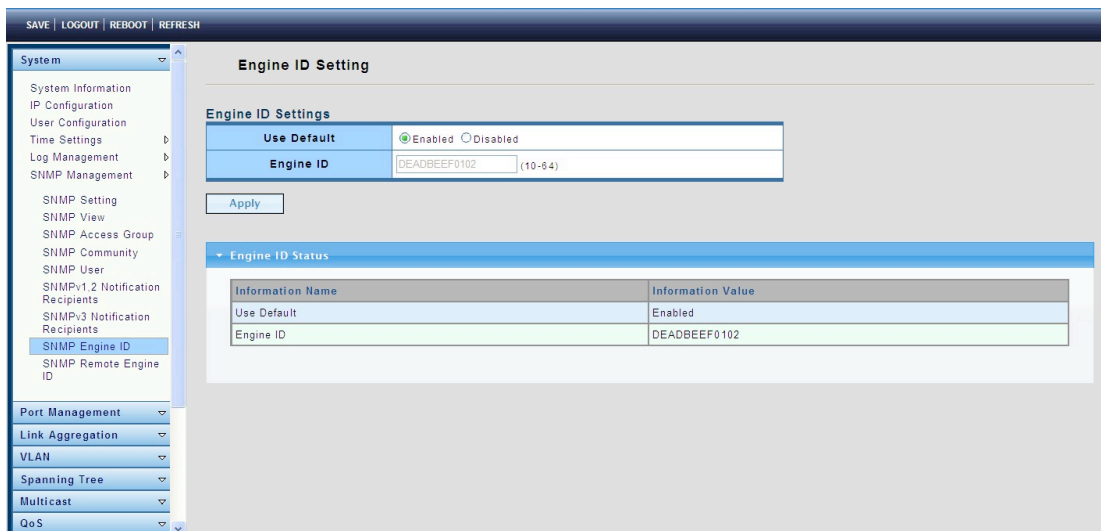
The Engine ID is used by SNMPv3 entities to uniquely identify them. An SNMP agent is considered an authoritative SNMP engine. This means that the agent responds to incoming messages (Get, GetNext, GetBulk, Set) and sends trap messages to a manager. The agent's local information is encapsulated in fields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



Use Default: Select the Use Default enable or disable.

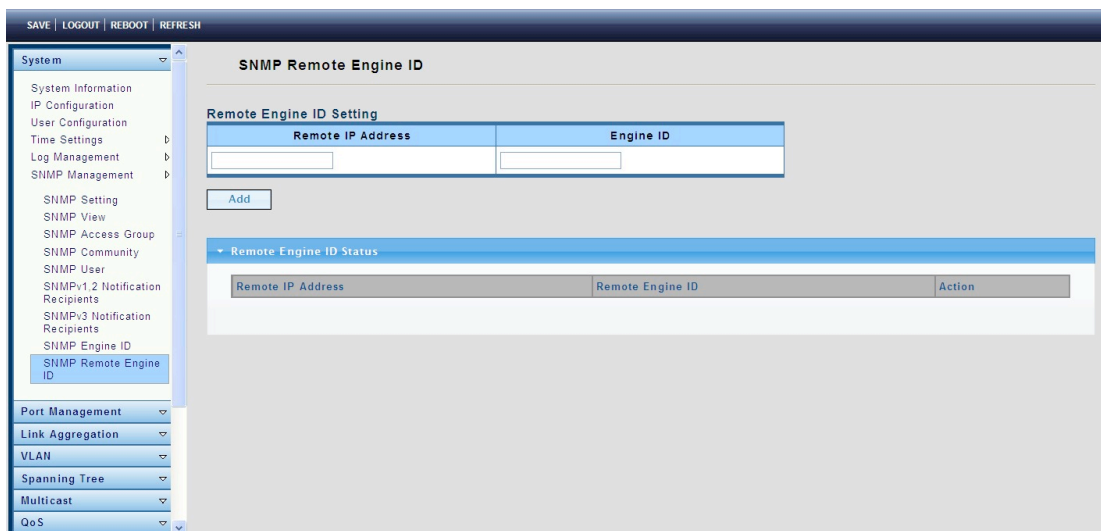
Engine ID: Enter the local device engine ID. The field value is a hexadecimal string (range: 10 - 64). Each byte in the hexadecimal character strings is represented by two hexadecimal digits.

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.



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.

The screenshot shows the 'Port Setting' configuration page. On the left is a navigation menu with categories like System, Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, Security, Access Control List, MAC Address Table, LLDP, Diagnostics, RMON, and Maintenance. The main content area is titled 'Port Setting' and contains 'Port Settings' and 'Port Status' sections.

Port Settings

Port Select	Enabled	Speed	Duplex	Flow Control
Select Ports	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	Auto	Auto	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Fiber Ports	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	Auto-1000M	Full	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Apply

Port Status

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.

The screenshot shows the 'Port Counters' configuration page. The navigation menu is similar to the previous page. The main content area is titled 'Port Counters' and contains 'Port MIB Counters Settings' and 'GE1 MIB Counters' sections.

Port MIB Counters Settings

Port	Mode
GE1	<input checked="" type="radio"/> All <input type="radio"/> Interface <input type="radio"/> Ethernetlike <input type="radio"/> RMON

Clear

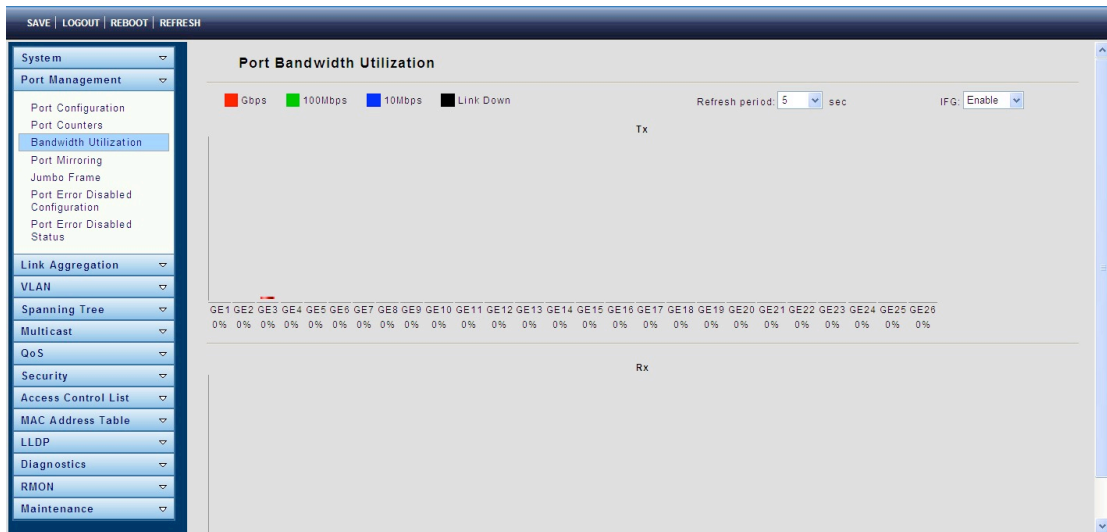
GE1 MIB Counters

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**.

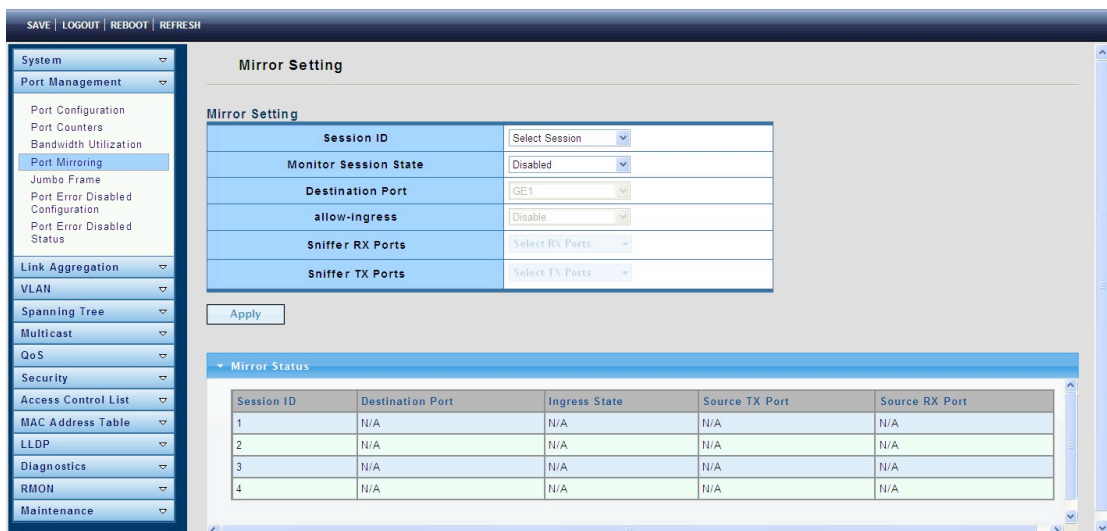
This page displays and lets you switch each port's TX and RX bandwidth utilization.



4.2.4 Port Mirroring

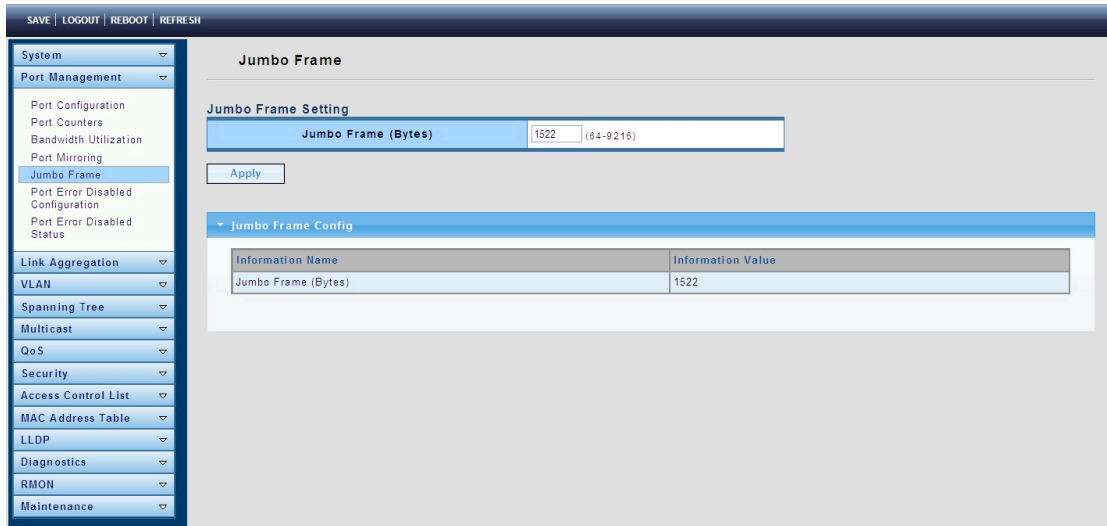
To display the Port Mirroring page, click **Port Management > Port Mirroring**.

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



4.2.5 Jumbo Frame

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

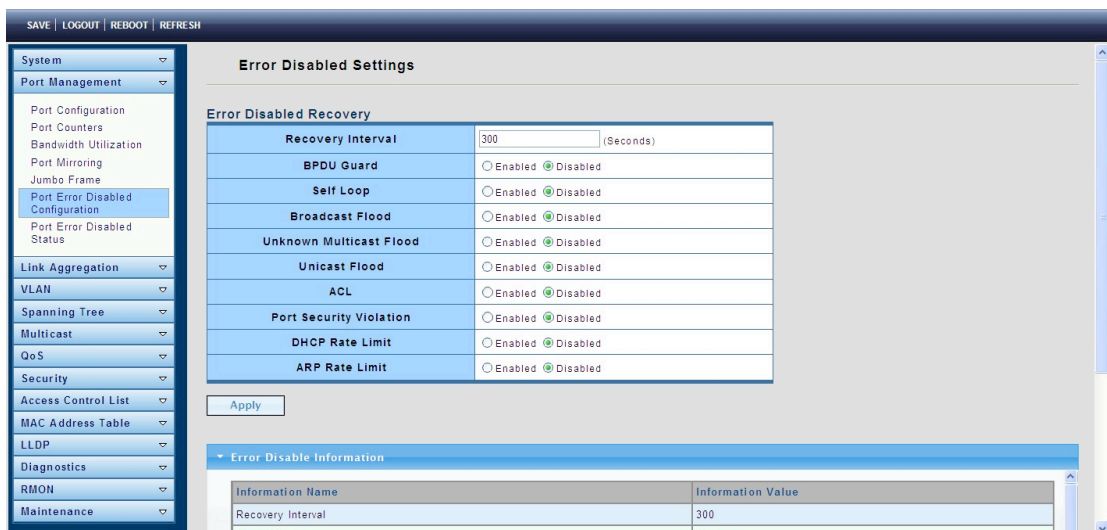


Jumbo Frame: The valid size range is 64 bytes – 9216 bytes.

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.



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.

The screenshot shows the 'Port Error Disabled Status' page. At the top, there are navigation links: SAVE | LOGOUT | REBOOT | REFRESH. On the left is a sidebar menu with categories: System, Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, Security, Access Control List, MAC Address Table, LLDP, Diagnostics, RMON, and Maintenance. Under 'Port Management', the following items are listed: Port Configuration, Port Counters, Bandwidth Utilization, Port Mirroring, Jumbo Frame, Port Error Disabled Configuration, and Port Error Disabled Status (which is selected). The main content area is titled 'Port Error Disabled Status' and contains a table with the following columns: Port Name, Error Disabled Reason, and Time Left (Seconds). The table is currently empty.

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.

The screenshot shows the 'LAG Setting' page. At the top, there are navigation links: SAVE | LOGOUT | REBOOT | REFRESH. On the left is a sidebar menu with categories: System, Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, Security, Access Control List, MAC Address Table, LLDP, Diagnostics, RMON, and Maintenance. Under 'Link Aggregation', the following items are listed: LAG Setting (which is selected), LAG Management, LAG Port Setting, LACP Setting, LACP Port Setting, and LAG Status. The main content area is titled 'LAG Setting' and contains a 'Load Balance Algorithm' section with radio buttons for 'MAC Address' (selected) and 'IP/MAC Address'. Below this is an 'Apply' button. Underneath is a section titled 'LAG Information' containing a table with the following columns: Information Name and Information Value. The table has one row: Load Balance Algorithm with the value 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.

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.

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.

SAVE | LOGOUT | REBOOT | REFRESH

System
Port Management
Link Aggregation
LAG Setting
LAG Management
LAG Port Setting
LACP Setting
LACP Port Setting
LAG Status
VLAN
Spanning Tree
Multicast
QoS
Security
Access Control List
MAC Address Table
LLDP
Diagnostics
RMON
Maintenance

LACP

LACP Setting

LACP Enable Enable Disable

System Priority (1-85535)

Apply

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.

SAVE | LOGOUT | REBOOT | REFRESH

System
Port Management
Link Aggregation
LAG Setting
LAG Management
LAG Port Setting
LACP Setting
LACP Port Setting
LAG Status
VLAN
Spanning Tree
Multicast
QoS
Security
Access Control List
MAC Address Table
LLDP
Diagnostics
RMON
Maintenance

LACP Port Setting

LACP Port Settings

Port Select **Priority** (1-85535) **Timeout** Long Short

Apply

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.

SAVE | LOGOUT | REBOOT | REFRESH

System
Port Management
Link Aggregation
LAG Setting
LAG Management
LAG Port Setting
LACP Setting
LACP Port Setting
LAG Status
VLAN
Spanning Tree
Multicast
QoS
Security
Access Control List
MAC Address Table
LLDP
Diagnostics
RMON
Maintenance

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	-	-

LACP Information

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.

SAVE | LOGOUT | REBOOT | REFRESH

System
Port Management
Link Aggregation
VLAN
Create VLAN
Interface Settings
Port to VLAN
Port VLAN Membership
Protocol VLAN Group Setting
Protocol VLAN Port Setting
Spanning Tree
Multicast
QoS
Security
Access Control List
MAC Address Table
LLDP
Diagnostics
RMON
Maintenance

Create VLAN

VLAN Setting

VLAN LIST	VLAN Action	VLAN Name Prefix
<input type="text"/>	<input checked="" type="radio"/> Add <input type="radio"/> Delete	<input type="text"/>

Apply

VLAN Table

VLAN ID	VLAN Name	VLAN Type	Modify
1	Default	Default	Edit

VLAN LIST: VLAN list for the new VLAN.

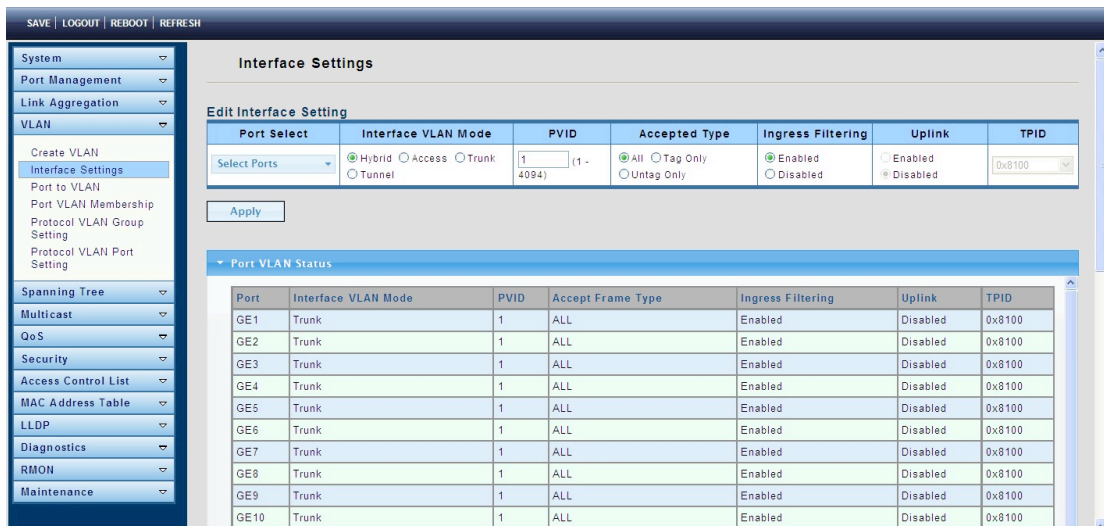
VLAN Action: Add or delete VLAN.

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.



Port Select: Select one or multiple ports to configure.

Interface VLAN Mode: VLAN port mode.

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

PVID: VLAN ID for the selected ports.

Accepted Type: Port accepted type.

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

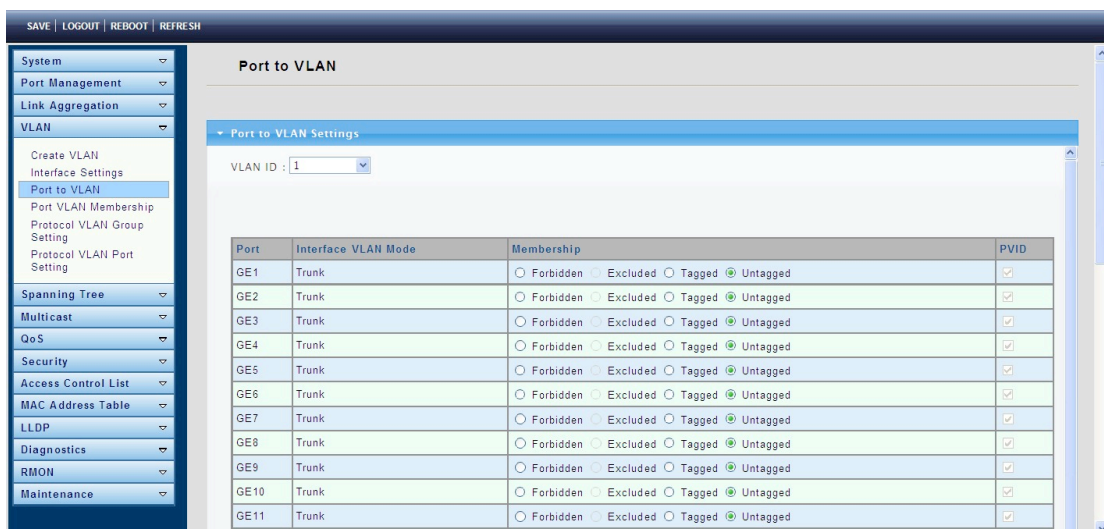
Ingress Filtering: Choose filter port open and close.

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.



4.4.4 Port VLAN Membership

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

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.

Add Protocol VLAN Group

Group ID (1-8)	<input type="text" value="1"/>
Frame Type	<input type="text" value="Ethernet_II"/>
Protocol Value (0x0600-0xFFFFE)	<input type="text"/>

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.

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

Protocol Value (0x0600-0xFFFFE): 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.

SAVE | LOGOUT | REBOOT | REFRESH

System
Port Management
Link Aggregation
VLAN
Spanning Tree
Multicast
QoS
Security
Access Control List
MAC Address Table
LLDP
Diagnostics
RMON
Maintenance

Protocol VLAN Port Setting

Port	Group	VLAN
Select Ports	<input type="radio"/> Group ID	<input type="radio"/> VLAN ID(1-4094) 1

Add

Protocol VLAN Port State

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.

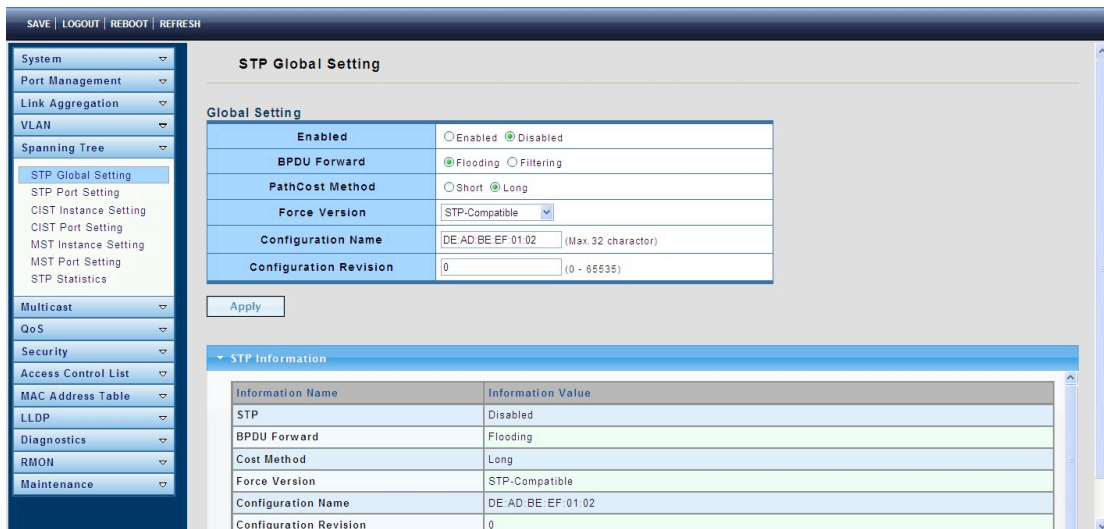
VLAN: Click the corresponding radio button to select a previously configured VLAN ID or VLAN Name.

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**.



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.

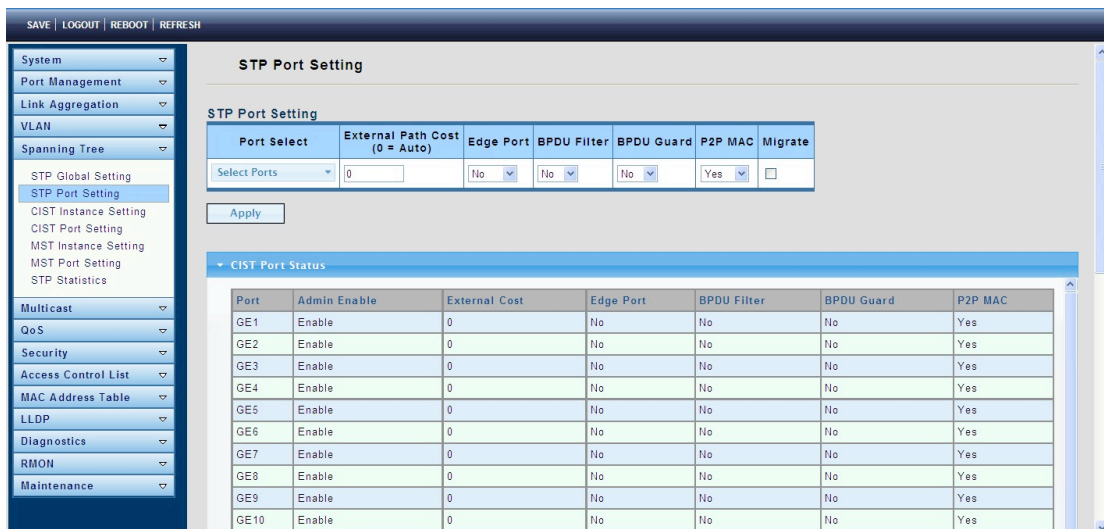
Force Version: Select the operating mode of STP.

- ℓ STP-Compatible: 802.1D STP operation.
- ℓ RSTP-Operation: 802.1w operation.
- ℓ 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**.



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.

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

BPDU Filter: Set the BPDU Filter configuration.

- ℓ No: Disable BPDU filter function.

ℓ Yes: Enable BPDU filter function.

To avoid transmitting BPDU from the specified ports.

BPDU Guard: Set the BPDU Guard configuration.

ℓ No: Disable BPDU guard function.

ℓ Yes: Enable BPDU filter function.

To drop directly the received BPDU from the specified ports.

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

ℓ No: Force to false state.

ℓ 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**.

The screenshot displays the 'CIST Instance Setting' page in a web management interface. The left sidebar contains a navigation menu with categories like System, Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, Security, Access Control List, MAC Address Table, LLDP, Diagnostics, RMON, and Maintenance. The 'Spanning Tree' category is expanded, showing sub-items like STP Global Setting, STP Port Setting, CIST Instance Setting (selected), CIST Port Setting, MST Instance Setting, MST Port Setting, and STP Statistics.

The main content area is titled 'CIST Instance Setting' and contains a table of configuration parameters:

Parameter	Value	Range
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)

Below the configuration table is an 'Apply' button and a section titled 'CIST Instance Information' which contains a table summarizing the current values:

Information Name	Information Value
Priority	32768
Max Hops	20
Forward Delay	15
Max Age	20
Tx Hold Count	6
Hello Time	2

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.

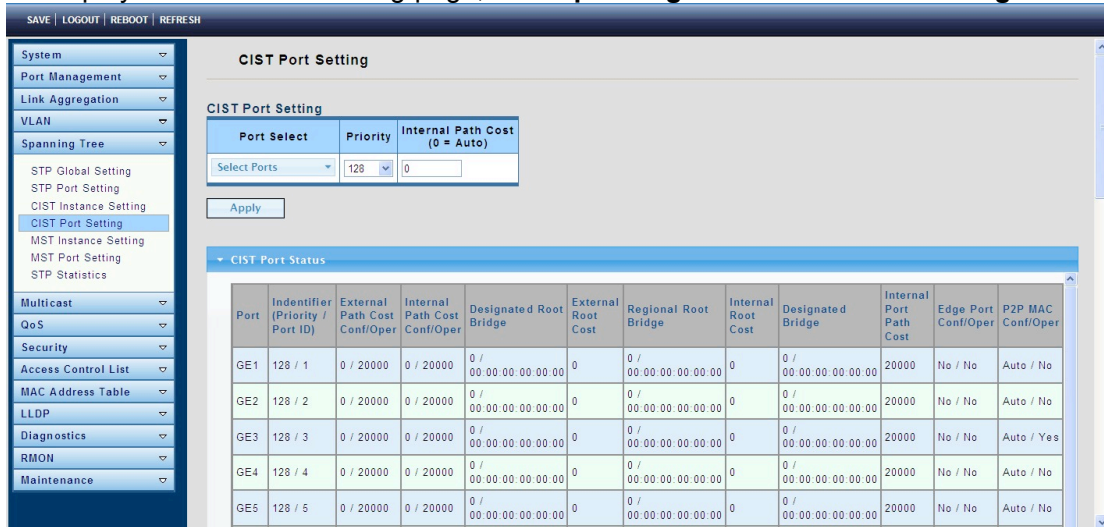
Max Age: Set the time any switch should wait before trying to change the STP topology after unhearing Hello BPDU.

Tx Hold Count: Set the Transmit Hold Count used to limit BPDU 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**.



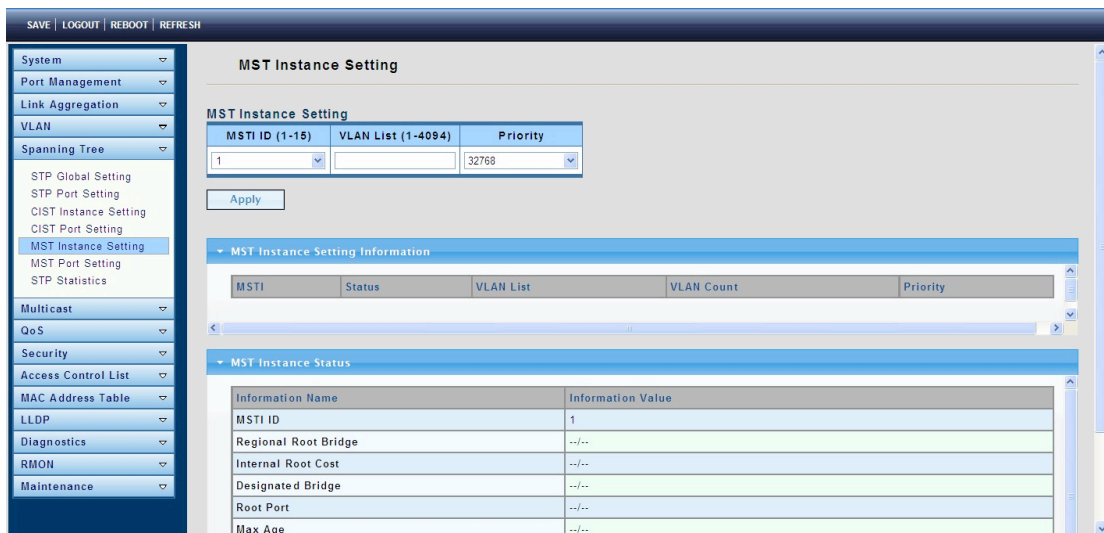
Port Select : Select the port list to specify which ports should apply this setting.

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**.



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**.

The screenshot shows the 'MST Port Setting' configuration page. At the top, there are navigation links: SAVE, LOGOUT, REBOOT, and REFRESH. On the left is a sidebar menu with categories like System, Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, Security, Access Control List, MAC Address Table, LLDP, Diagnostics, RMON, and Maintenance. The 'Spanning Tree' menu is expanded, showing options like STP Global Setting, STP Port Setting, CIST Instance Setting, CIST Port Setting, MST Instance Setting, MST Port Setting (selected), and STP Statistics.

The main content area is titled 'MST Port Setting'. It contains a configuration form with the following fields:

- MST ID:** A dropdown menu set to '1'.
- Port Select:** A dropdown menu set to 'Select Ports'.
- Priority:** A dropdown menu set to '128'.
- Internal Path Cost (0 = Auto):** A text input field set to '0'.

Below the form is an 'Apply' button. Underneath is a section titled 'MST Port Status' which contains a table with the following data:

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.

The screenshot shows the 'STP Statistics' page. It features the same sidebar menu as the previous page, with 'STP Statistics' selected under the 'Spanning Tree' category.

The main content area is titled 'STP Statistics' and contains a table with the following data:

Port	Configuration BPDUs Received	TCN BPDUs Received	MSTP BPDUs Received	Configuration BPDUs Transmitted	TCN BPDUs Transmitted	MSTP BPDUs 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.

The screenshot shows the 'Properties' configuration page for Multicast. The left sidebar contains a navigation menu with 'Multicast' expanded to 'Properties'. The main content area is titled 'Properties' and contains the following settings:

- L2 Unknown Multicast Action:** Radio buttons for Drop and Flood (selected).
- IP Unknown Multicast Action:** Radio buttons for Drop, Flood (selected), and Router Port.
- IPv4 Forward Method:** Radio buttons for MAC (selected) and Src-Dst-Ip.

Below the settings is an 'Apply' button. Under the 'Properties Information' section, there is a table:

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**.

The screenshot shows the 'IGMP Snooping' configuration page, specifically the 'IGMP Setting' sub-page. The left sidebar shows 'Multicast' expanded to 'IGMP Snooping' and then 'IGMP Setting'. The main content area is titled 'IGMP Snooping' and contains the following settings:

- IGMP Snooping Status:** Radio buttons for Enable (selected) and Disable.
- IGMP Snooping Version:** Radio buttons for v2 (selected) and v3.
- IGMP Snooping Report Suppression:** Radio buttons for Enable (selected) and Disable.

Below the settings is an 'Apply' button. Under the 'IGMP Snooping Information' section, there is a table:

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

At the bottom, there is an 'IGMP Snooping Table' with the following columns: 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, and 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**.

VLAN ID: Select the VLANs to configure.

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

- ℳ Enable: Enable IGMP Querier Election.
- ℳ 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.

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.

The screenshot shows the 'IGMP Group Table' page. At the top, there are navigation links: SAVE, LOGOUT, REBOOT, and REFRESH. On the left is a sidebar menu with categories: System, Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, Security, and Access Control List. Under Multicast, the following options are listed: Properties, IGMP Snooping, IGMP Setting, IGMP Querier Setting, IGMP Static Group, IGMP Group Table (highlighted), IGMP Router Setting, IGMP Router Table, IGMP Forward All, IGMP Snooping Statistics, Multicast Throttling Setting, and Multicast Filter. The main content area is titled 'IGMP Group Table' and contains a table with the following columns: VLAN ID, Group IP Address, Member Ports, Type, and Life(Sec). The table is currently empty.

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.

The screenshot shows the 'IGMP Router Port Setting' page. At the top, there are navigation links: SAVE, LOGOUT, REBOOT, and REFRESH. On the left is a sidebar menu with categories: System, Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, Security, and Access Control List. Under Multicast, the following options are listed: Properties, IGMP Snooping, IGMP Setting, IGMP Querier Setting, IGMP Static Group, IGMP Group Table, IGMP Router Setting (highlighted), IGMP Router Table, IGMP Forward All, IGMP Snooping Statistics, Multicast Throttling Setting, and Multicast Filter. The main content area is titled 'IGMP Router Port Setting' and contains a form for 'Add Router Port'. The form has the following fields: VLAN ID (with a 'Select VLANs' dropdown), Type (with radio buttons for 'Static' and 'Forbid'), Static Ports Select (with a 'Select Static Ports' dropdown), and Forbid Ports Select (with a 'Select Forbid Ports' dropdown). Below the form is an 'Add' button. Below the form is a table titled 'Router Ports Status' with the following columns: VLAN ID, Static Ports, Forbidden Ports, and Modify. The table is currently empty.

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.

4.6.2.7 IGMP Forward All

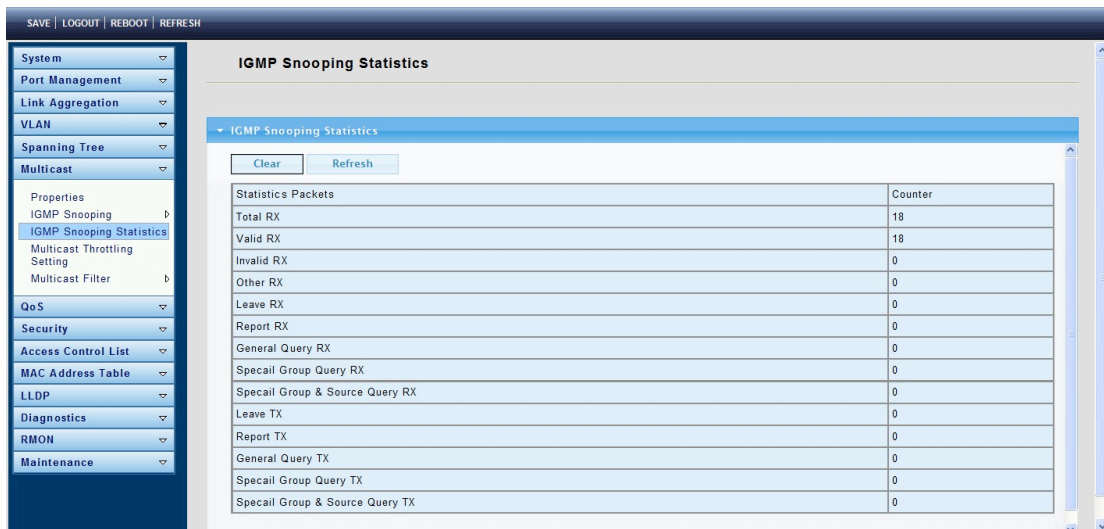
To display IGMP Forward All web page, click **Multicast > IGMP Snooping > IGMP Forward All**

Port	Membership
GE1	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE2	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE3	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE4	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE5	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE6	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE7	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE8	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE9	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE10	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE11	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE12	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE13	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE14	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None

4.6.3 IGMP Snooping Statistics

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

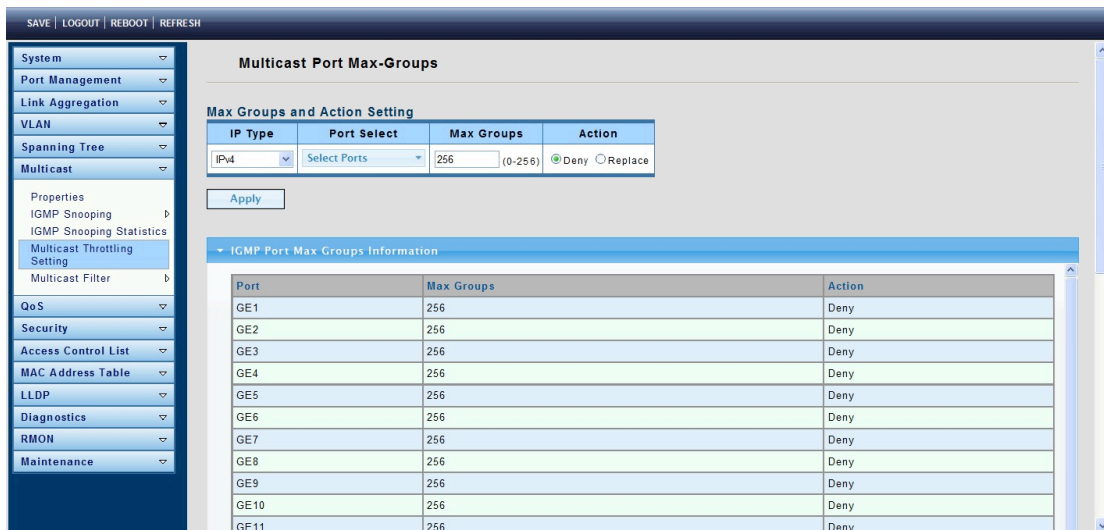
This page is used to display IGMP Snooping statistics information.



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.

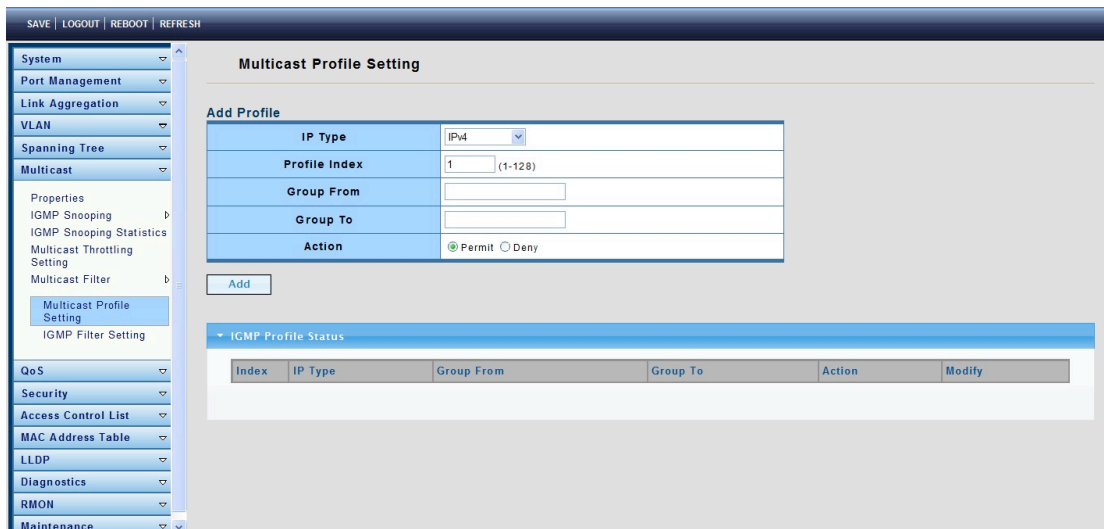


4.6.5 Multicast Filter

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.

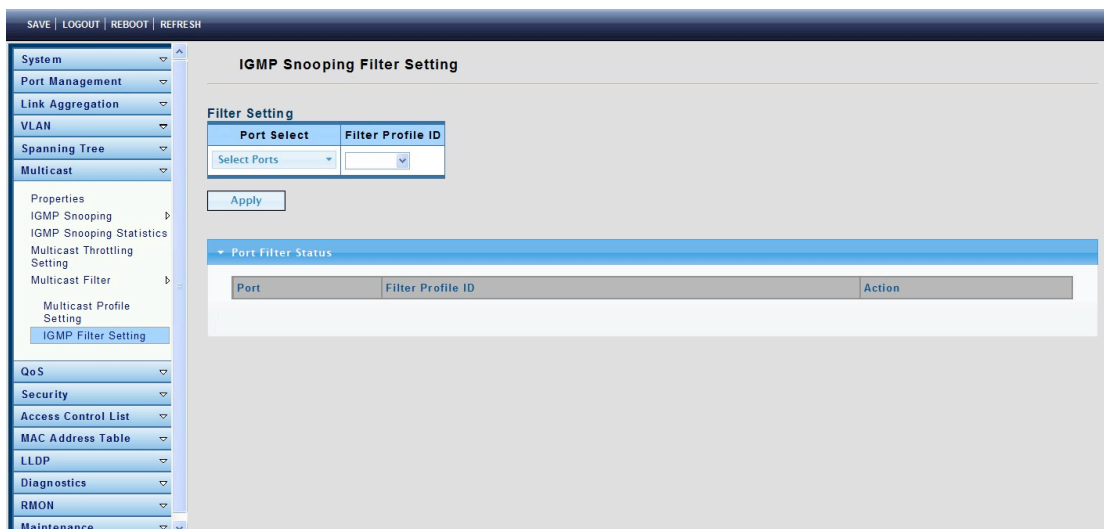
To display the Multicast Profile Setting page, click **Multicast > Multicast Filter > Multicast Profile Setting**.



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.



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.

The screenshot shows the 'QoS Global Setting' page. At the top, there are navigation links: SAVE, LOGOUT, REBOOT, REFRESH. A left sidebar contains a menu with categories like System, Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, Security, Access Control List, MAC Address Table, LLDP, Diagnostics, and RMON. Under the QoS category, 'QoS Properties' is selected. The main content area is titled 'QoS Global Setting' and contains a 'QoS Mode' section with three radio buttons: 'Disable' (checked), 'Basic', and 'Advanced'. Below this is an 'Apply' button. A 'QoS Information' table is displayed below, with the following data:

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.

The screenshot shows the 'QoS Port Settings' page. At the top, there are navigation links: SAVE, LOGOUT, REBOOT, REFRESH. A left sidebar contains a menu with categories like System, Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, Security, Access Control List, MAC Address Table, LLDP, Diagnostics, and RMON. Under the QoS category, 'Port Settings' is selected. The main content area is titled 'QoS Port Settings' and contains a 'QoS Port Settings' section with a 'Port' dropdown, a 'CoS Value' dropdown (set to 0), and radio buttons for 'Remark CoS', 'Remark DSCP', and 'Remark IP Precedence' (all set to 'Disable'). Below this is an 'Apply' button. A 'QoS Port Status' table is displayed below, with the following data:

Port	CoS Value	Remark Co S	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.

The screenshot shows the 'Queue Settings' page. On the left is a navigation menu with categories like System, Port Management, VLAN, QoS, Security, etc. The main content area is titled 'Queue Settings' and contains a 'Queue Table' with the following data:

Queue	Scheduling Method			
	Strict Priority	WRR	Weight	% of WRR Bandwidth
1	<input checked="" type="checkbox"/>	<input type="radio"/>	1	
2	<input checked="" type="checkbox"/>	<input type="radio"/>	2	
3	<input checked="" type="checkbox"/>	<input type="radio"/>	3	
4	<input checked="" type="checkbox"/>	<input type="radio"/>	4	
5	<input checked="" type="checkbox"/>	<input type="radio"/>	5	
6	<input checked="" type="checkbox"/>	<input type="radio"/>	9	
7	<input checked="" type="checkbox"/>	<input type="radio"/>	13	
8	<input checked="" type="checkbox"/>	<input type="radio"/>	15	

Below the table is an 'Apply' button. At the bottom, the 'Queue Information' section shows a table with 'Information Name' and 'Information Value':

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.

The screenshot shows the 'CoS Mapping' page. It features two mapping tables and an 'Apply' button.

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

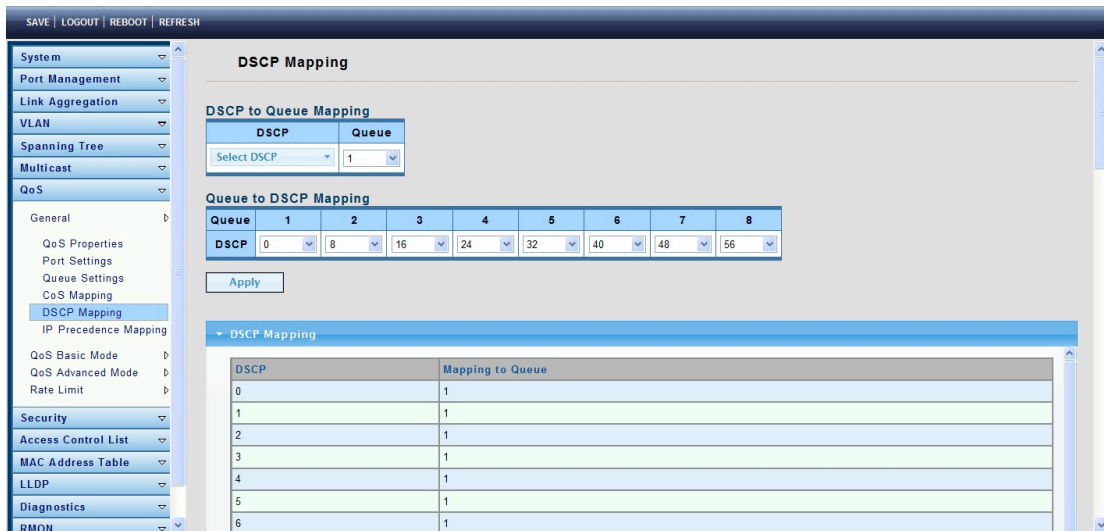
Below these is an 'Apply' button and a 'CoS Mapping' table:

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**.

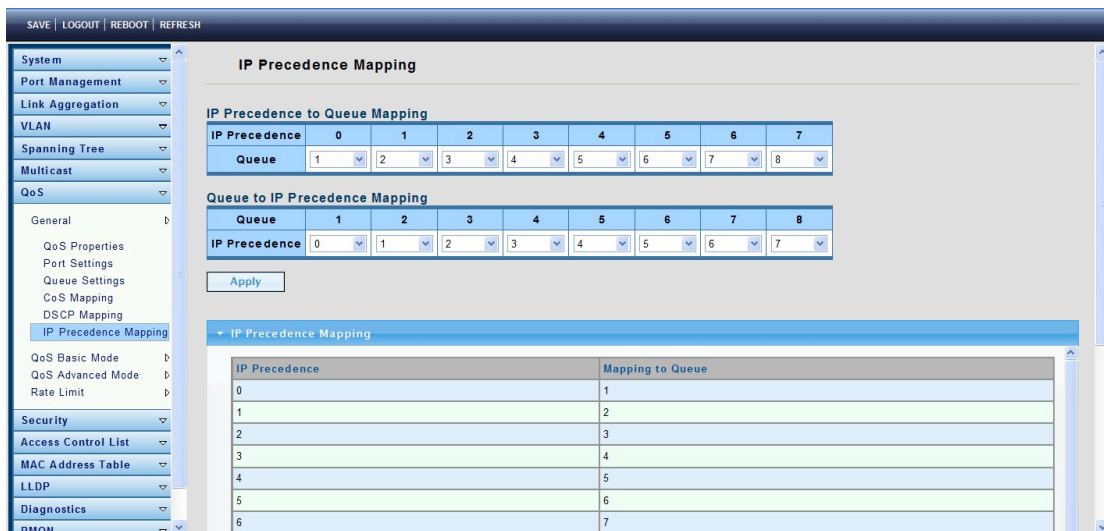
The page allows you to set DSCP Mapping.



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.



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.

SAVE | LOGOUT | REBOOT | REFRESH

System
Port Management
Link Aggregation
VLAN
Spanning Tree
Multicast
QoS
General
QoS Basic Mode
Global Settings
Port Settings
QoS Advanced Mode
Rate Limit
Security
Access Control List
MAC Address Table
LLDP
Diagnostics
RMON
Maintenance

Global Settings

Basic Mode Global Settings

Trust Mode CoS/802.1p DSCP CoS/802.1p-DSCP IP Precedence None

Apply

QoS Information

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.

SAVE | LOGOUT | REBOOT | REFRESH

System
Port Management
Link Aggregation
VLAN
Spanning Tree
Multicast
QoS
General
QoS Basic Mode
Global Settings
Port Settings
QoS Advanced Mode
Rate Limit
Security
Access Control List
MAC Address Table
LLDP
Diagnostics
RMON
Maintenance

QoS Port Setting

QoS Port Setting

Port **Trust** Enabled Disabled

Apply

QoS Port Status

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

Apply

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

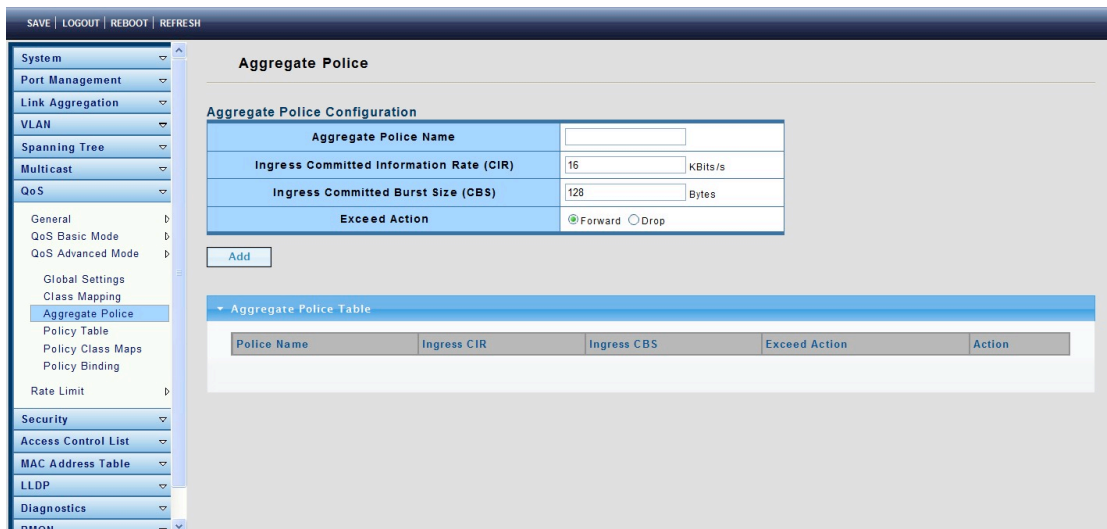
Add

Class Table

Class Name	Match	Action
------------	-------	--------

4.7.3.3 Aggregate Police

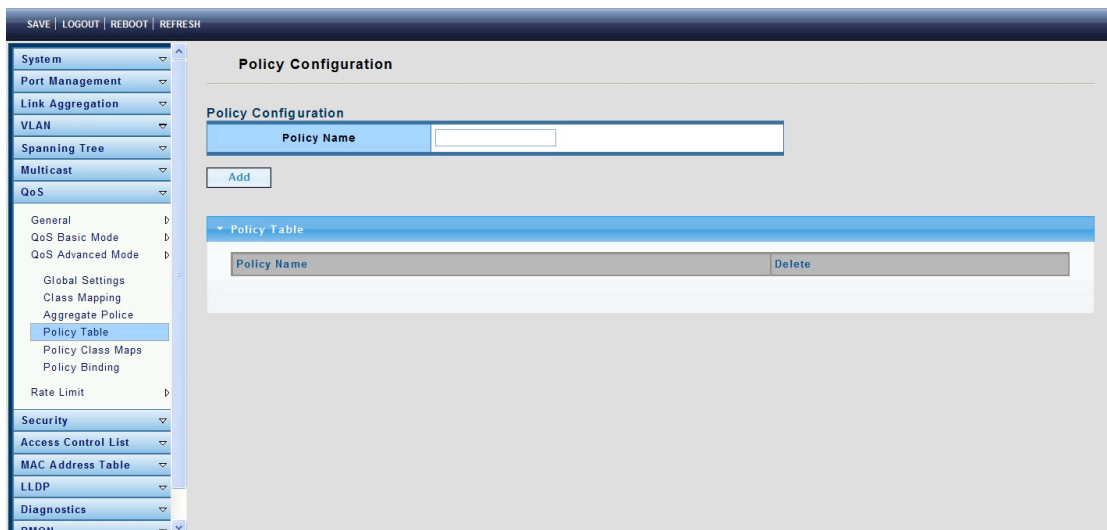
To display the Aggregate Police page, click **QoS > QoS Advanced Mode > Aggregate Police**.



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.



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**.

The screenshot shows the 'Policy Class Maps' configuration page. The left sidebar contains a navigation menu with categories like System, Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, Security, and Diagnostics. The main area is titled 'Policy Class Configuration' and contains several fields:

- Policy Name:** A dropdown menu.
- Class Name:** A dropdown menu.
- Action Type:** Radio buttons for 'Trust None' (selected), 'Always Trust', and 'Set Queue' with a text input field.
- Police Type:** Radio buttons for 'None' (selected), 'Single', and 'Aggregate'.
- Aggregate Police:** A dropdown menu.
- Ingress Committed Information Rate (CIR):** A text input field with '16' and 'KBits/s'.
- Ingress Committed Burst Size (CBS):** A text input field with '128' and 'Bytes'.
- Exceed Action:** Radio buttons for 'Forward' (selected) and 'Drop'.

Below the configuration fields is a table titled 'Policy Class Map Table' with columns: Policy Name, Class Name, Action Type, Police Type, Aggregate Police Name, CIR, CBS, Exceed Action, and 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.

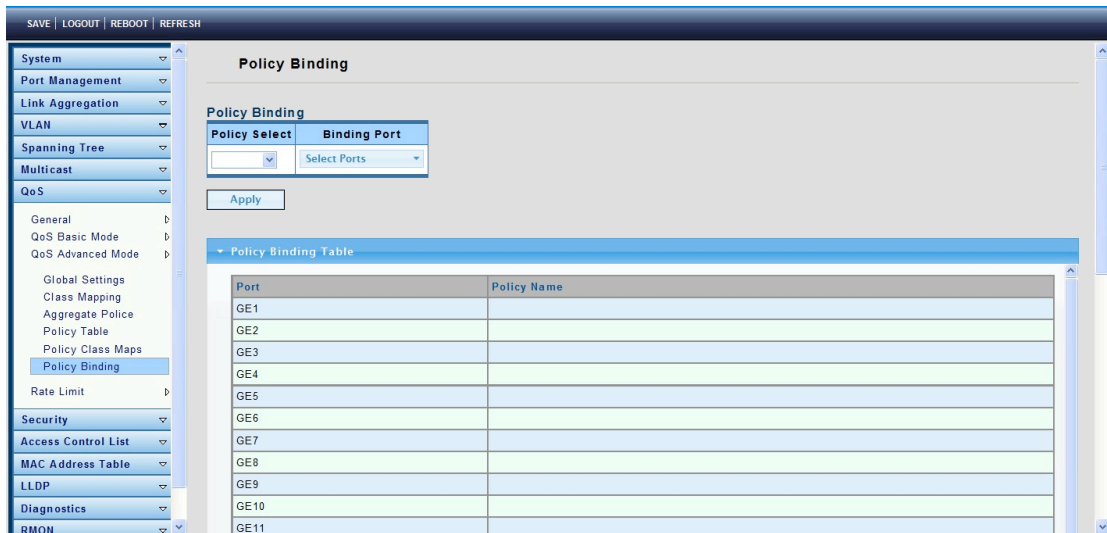
4.7.3.6 Policy Binding

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**.

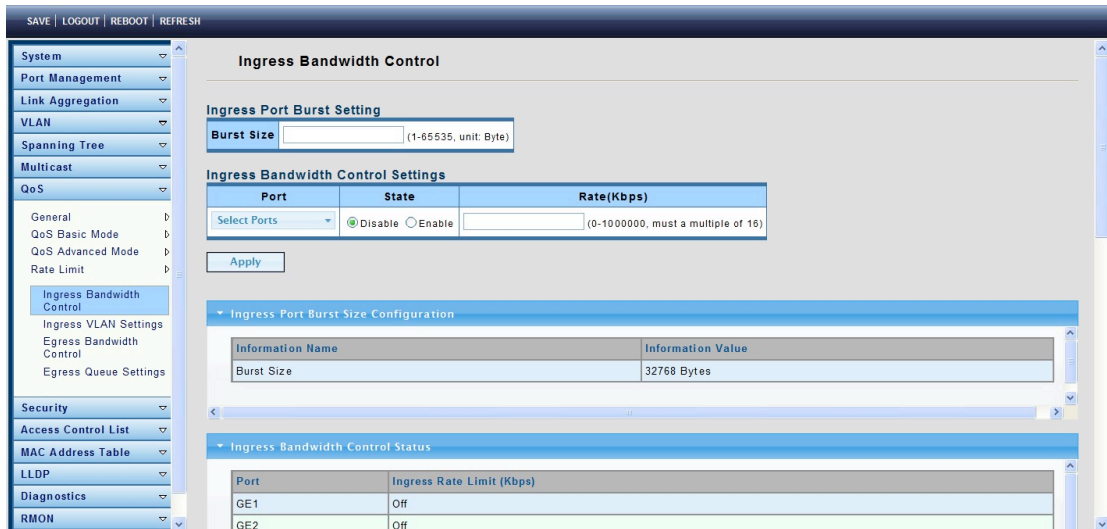


4.7.4 Rate Limit

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.



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.

The screenshot shows the 'VLAN Ingress Rate Limit' configuration page. The left sidebar contains a navigation menu with categories like System, Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, Security, and Diagnostics. The main content area is titled 'VLAN Ingress Rate Limit' and contains the following settings:

- 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.

The screenshot shows the 'Egress Bandwidth Control' configuration page. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Egress Bandwidth Control' and contains the following settings:

- Egress Port Burst Setting:**
 - Burst Size: [] (1-65535, unit: Byte)
- Egress Bandwidth Control Settings:**

Port	State	Rate(Kbps)
Select Ports	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	[] (0-1000000, must a multiple of 16)
- Egress Port Burst Size Configuration:**

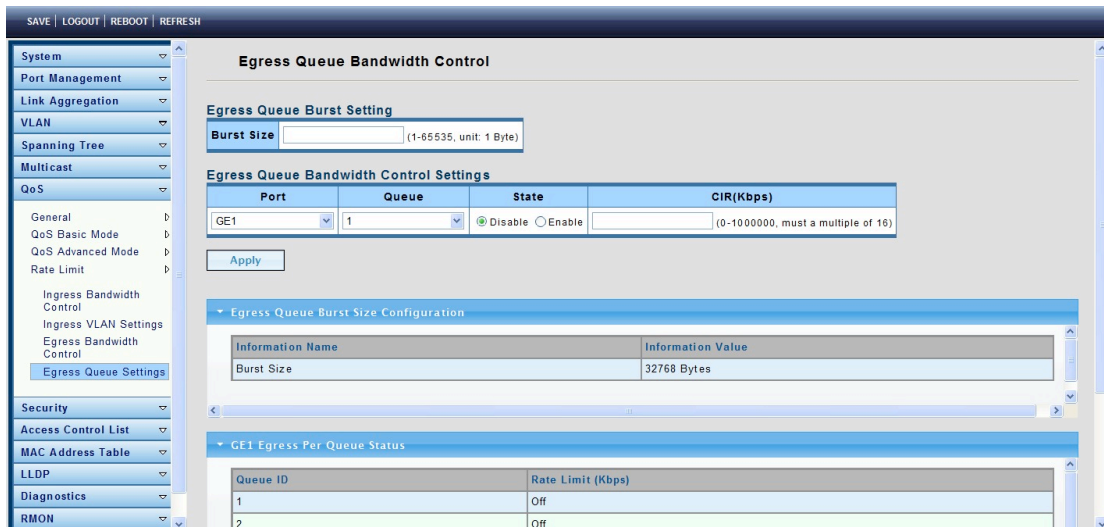
Information Name	Information Value
Burst Size	32768 Bytes
- Egress Bandwidth Control Status:**

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.



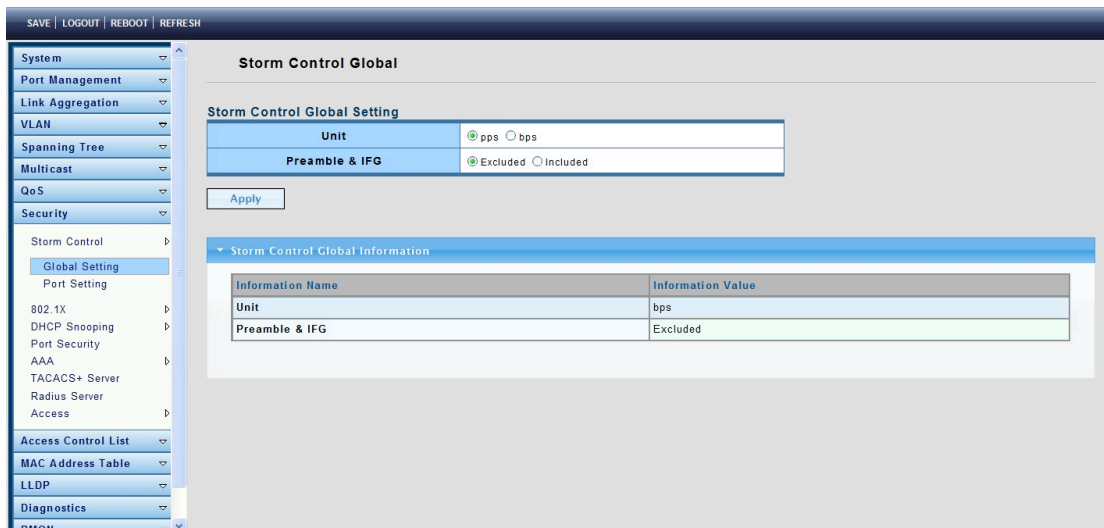
4.8 Security

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**.



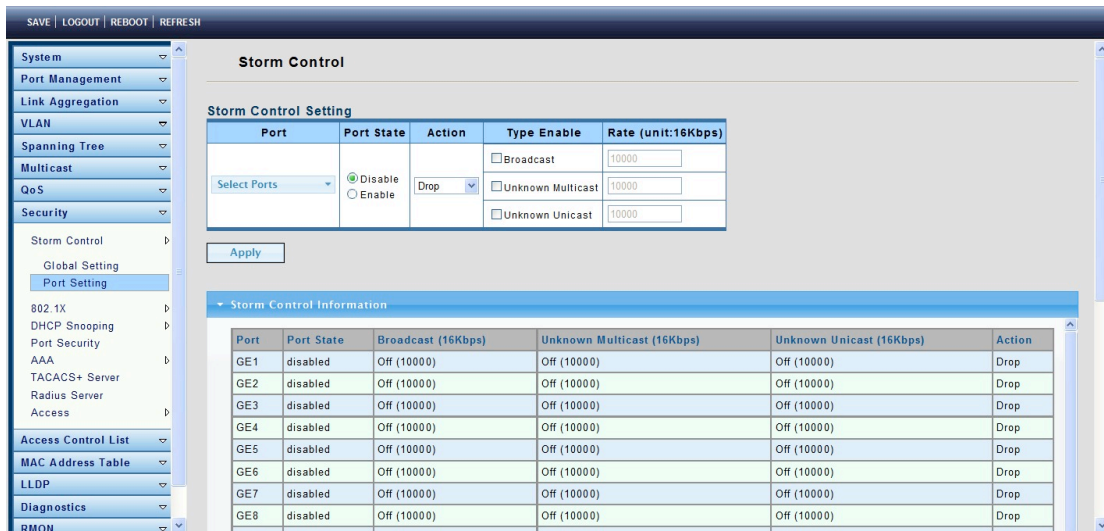
Unit: Choose a storm control unit: pps or bps.

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

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



Port: Select the setting ports.

Type Enable: Select the type of storm control.

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

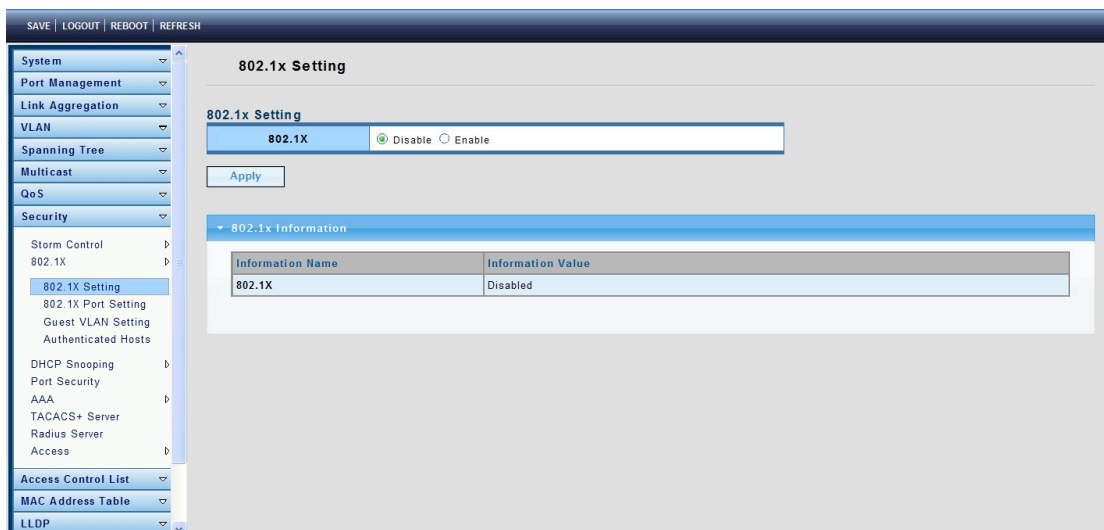
Rate: Value of the storm control rate. Unit: pps (packet per-second) or Kbps (Kbits per-second) depends on global mode setting. The range is from 0 to 100000.

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: Set the enabling status of 802.1X functionality.

- ℓ Enable: Enable 802.1X.
- ℓ 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 Setting**.

The screenshot displays the '802.1x Port Setting' configuration page. On the left is a navigation menu with 'Security' expanded to '802.1X Port Setting'. The main content area contains the following configuration fields:

- Port:** Select Ports (dropdown)
- Mode:** No Authentication (dropdown)
- 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)

Below the fields is an 'Apply' button. At the bottom, a table titled '802.1x Port Status' shows the current configuration for two ports:

Port	Mode (pps)	Status (pps)	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.

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

Reauthentication Enable: Set the enabling status of 802.1X reauthentication.

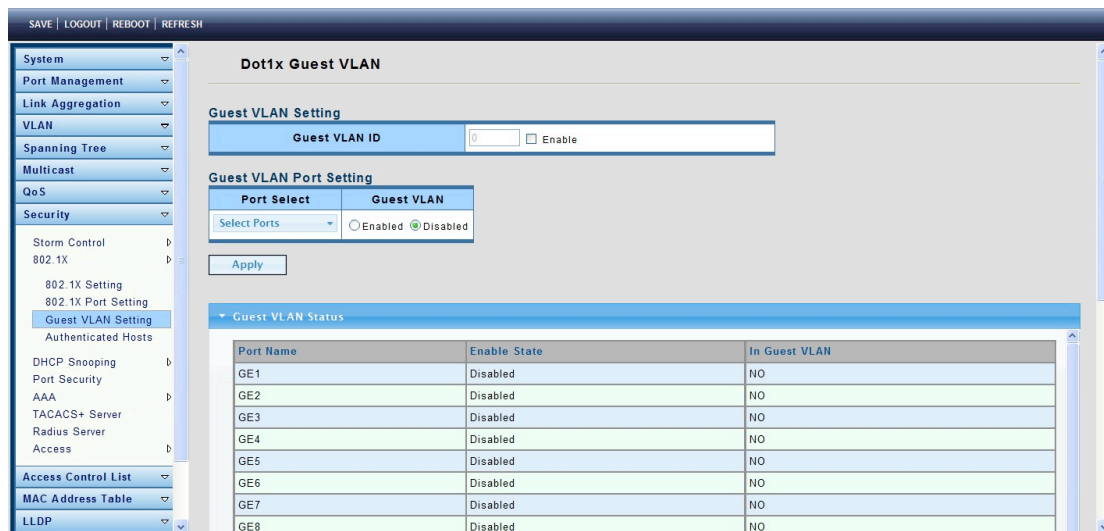
Reauthentication Period: Set the reauthentication period of 802.1X if reauthentication is enabled.

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.

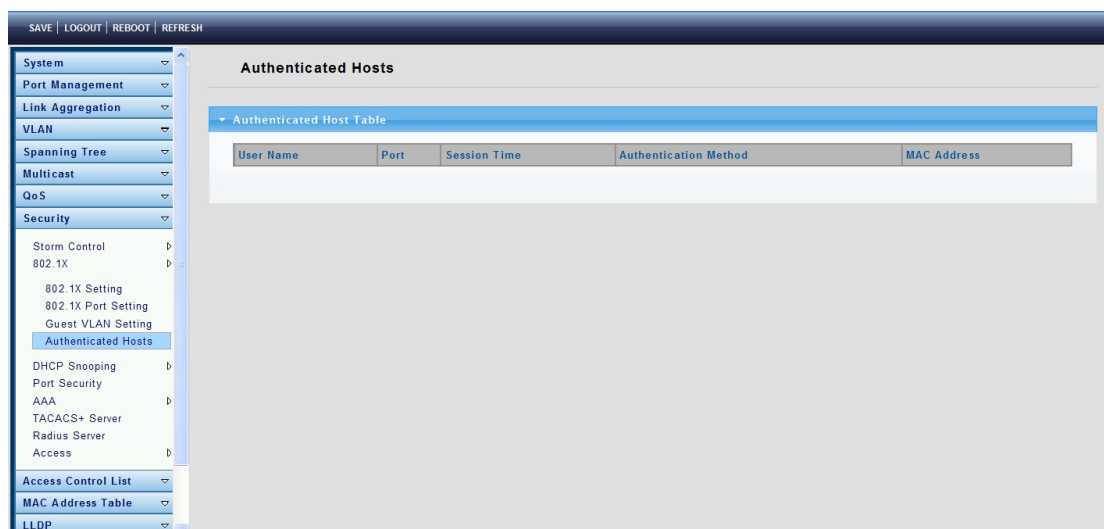
An unauthenticated VLAN is a VLAN that allows access by both authorized and unauthorized devices or ports. You can configure one or more VLANs to be unauthenticated in Creating VLANs.

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



4.8.2.4 Authenticated Hosts

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



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:

- ℓ None: No authentication is applied; it is automatically authorized.
- ℓ 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.

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.

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

Select Ports: Un Trusted Trusted Enable Disable

Apply

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

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.

The screenshot shows the 'DHCP Rate Limit' configuration page. At the top, there are navigation links: SAVE | LOGOUT | REBOOT | REFRESH. A left sidebar contains a menu with categories like System, Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, and Security. The Security menu is expanded, showing options like Storm Control, 802.1X, DHCP Snooping, and Rate Limit (which is selected). The main content area is titled 'DHCP Rate Limit' and contains a 'DHCP Rate Limit Setting' section with a 'Port' dropdown, a 'State' section with radio buttons for 'Default' (selected) and 'User-Define', and a 'Rate Limit (pps)' input field set to 'Unlimited'. Below this is an 'Apply' button. A 'DHCP Rate Limit Config' section contains a table with two columns: 'Port Name' and 'Rate Limit (pps)'. The table lists ports GE1 through GE11, all with 'Unlimited' rate limits.

Port	State	Rate Limit (pps)
Select Ports	<input checked="" type="radio"/> Default <input type="radio"/> User-Define	Unlimited (1-50 pps)

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**.

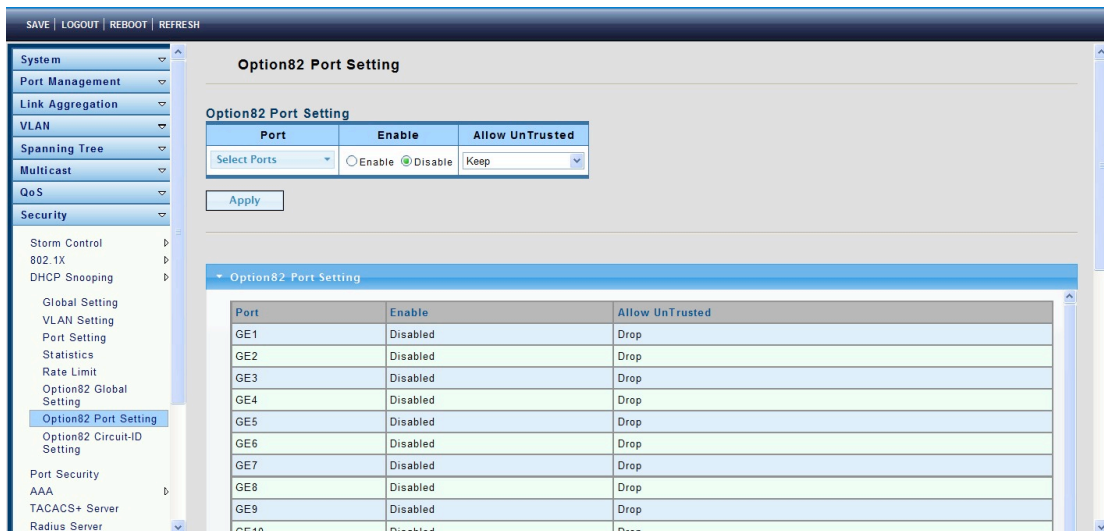
This page is used to configure DHCP Snooping support Option82 strategy.

The screenshot shows the 'DHCP Option82 Global Setting' configuration page. At the top, there are navigation links: SAVE | LOGOUT | REBOOT | REFRESH. A left sidebar contains a menu with categories like System, Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, and Security. The Security menu is expanded, showing options like Storm Control, 802.1X, DHCP Snooping, and Option82 Global Setting (which is selected). The main content area is titled 'DHCP Option82 Global Setting' and contains an 'Option82 Global Setting' section with a 'Remote ID' input field, a 'State' section with radio buttons for 'Default' (selected) and 'User-Define', and an 'Apply' button. Below this is an 'Option82 Global Setting' section containing a table with two columns: 'Information Name' and 'Information Value'. The table has one entry: 'Option82 Remote ID' with the value 'de.ad.be.ef.1.2 (Byte Format)'.

Information Name	Information Value
Option82 Remote ID	de.ad.be.ef.1.2 (Byte Format)

4.8.3.7 Option82 Port Setting

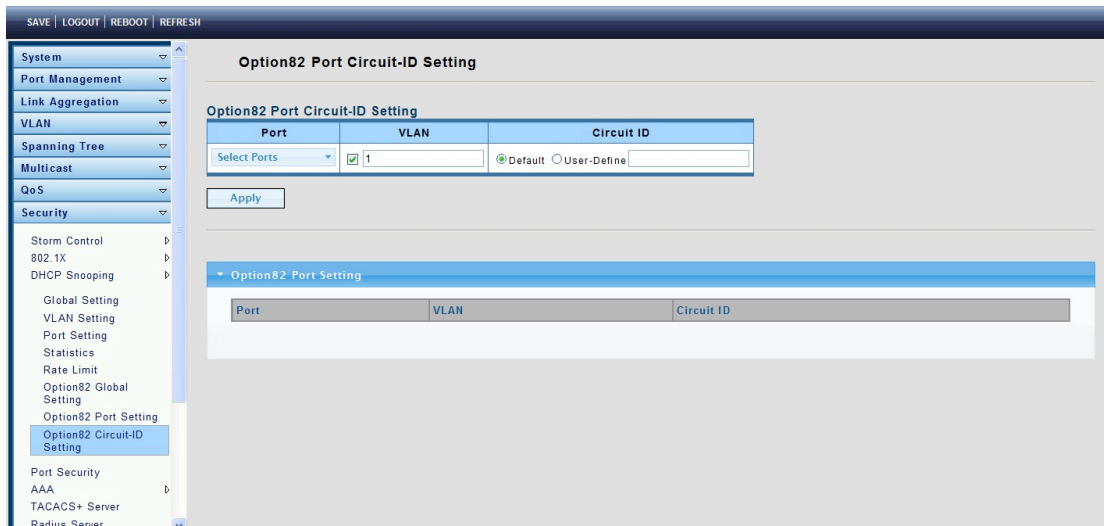
To display the Option82 Port Setting page, click **Security > DHCP Snooping > Option82 Port Setting**.



4.8.3.8 Option82 Circuit-ID Setting

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

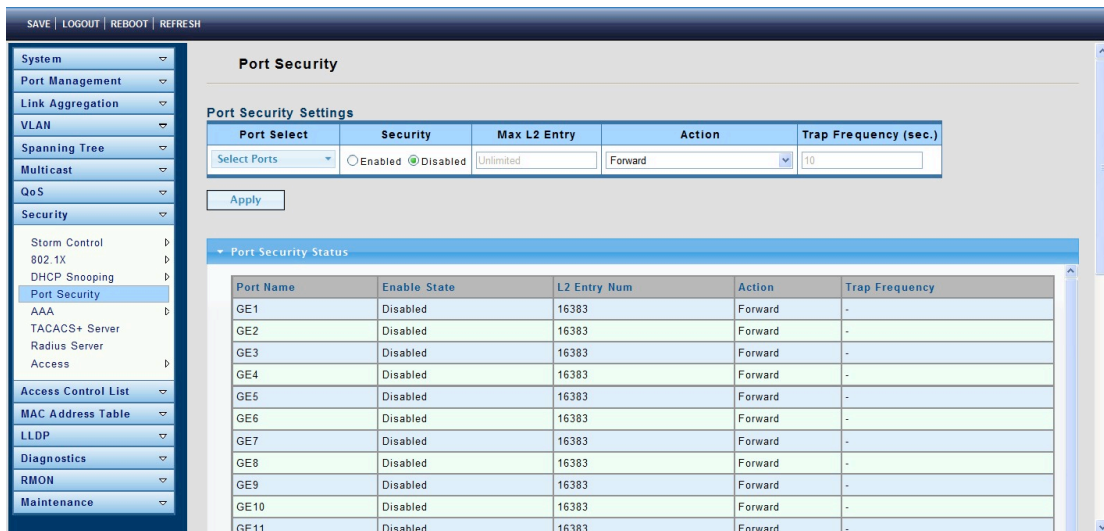
This page allows you to edit the circuit ID content in the Option82 settings.



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 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.

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

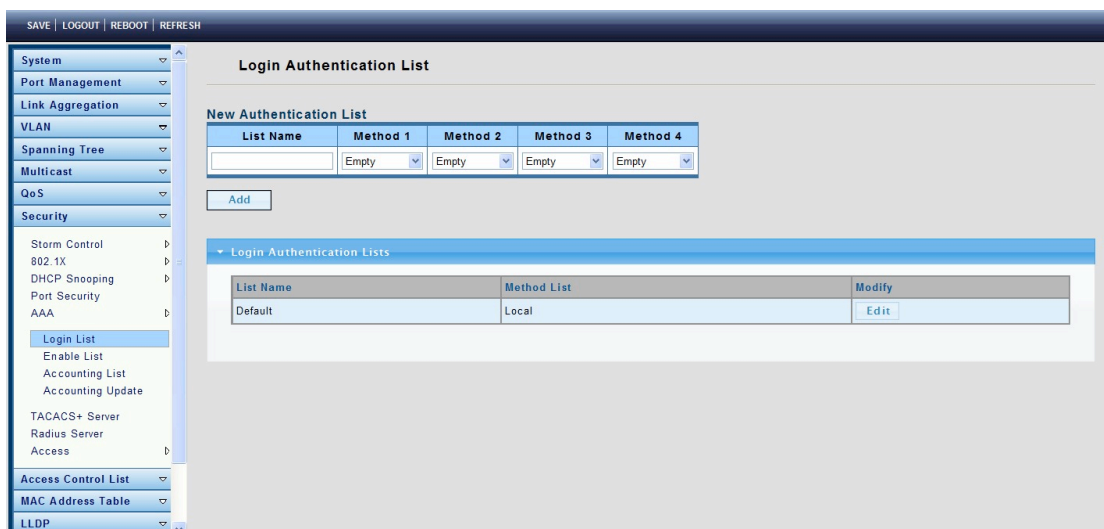
Max L2 Entry: The total number of MAC addresses that can be recognized by a port.

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.



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

Method 1: Select the first priority method 2 for login authentication.

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

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

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

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

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

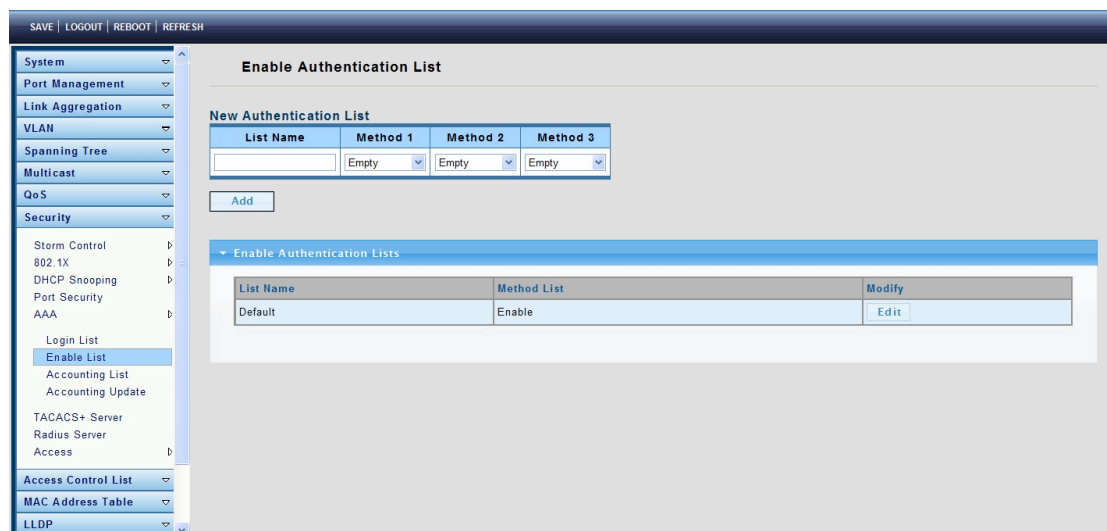
Method 4: Select the fourth priority method for login authentication.

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



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.

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

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

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

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

- ℓ Enable: Use local enable password to authenticate.
- ℓ Tacacs+: Use remote TACACS+ server to authenticate.
- ℓ Radius: Use remote Radius server to authenticate. Not supported now, it will be supported 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.

The screenshot shows the 'Exec Accounting List' configuration page. On the left is a navigation menu with categories like System, Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, Security, Access Control List, MAC Address Table, and LLDP. The 'Security' menu is expanded to show 'Accounting List' selected. The main content area is titled 'Exec Accounting List' and contains a 'New Accounting List' form with the following fields:

List Name	Record Type	Method 1	Method 2
<input type="text"/>	None	None	None

Below the form is an 'Add' button. Underneath is a table of existing 'Exec Accounting Lists':

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.

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

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

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

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

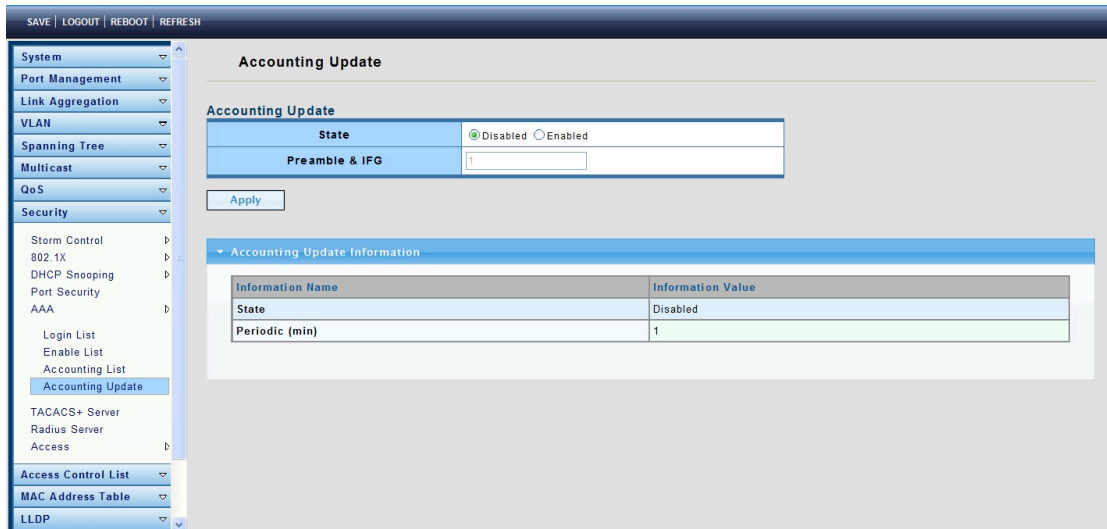
Method 2: Select the second priority method for exec accounting.

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

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

4.8.5.4 Accounting Update

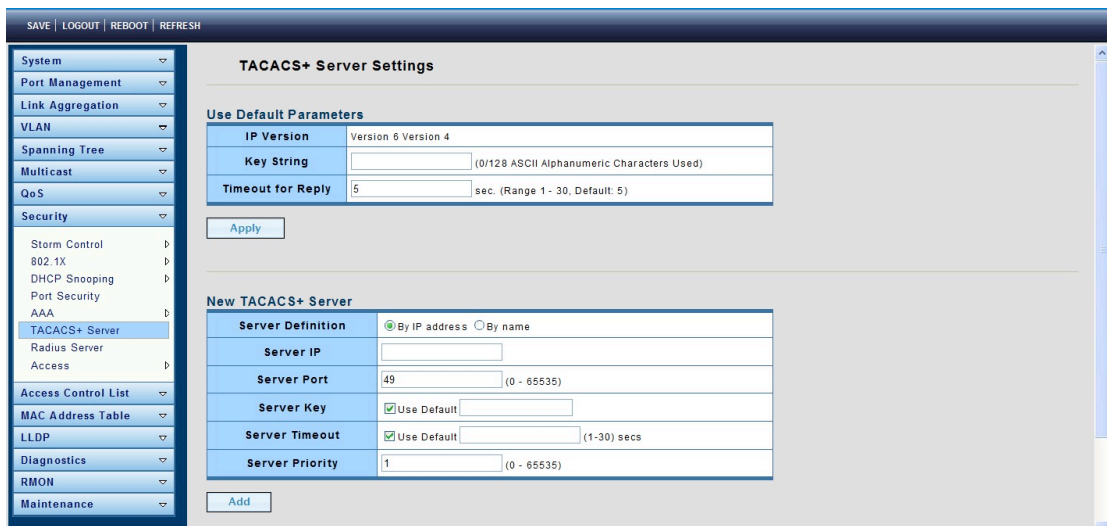
To display the Accounting Update page, click **Security > AAA > Accounting Update**.



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.



4.8.7 Radius Server

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

This page is used for radius server settings.

The screenshot shows the 'Radius Server Settings' page. The left navigation menu includes System, Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, Security, Storm Control, 802.1X, DHCP Snooping, Port Security, AAA, TACACS+ Server, Radius Server, Access, Access Control List, MAC Address Table, LLDP, Diagnostics, RMON, and Maintenance. The main content area is titled 'Radius Server Settings' and contains the following sections:

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	<input checked="" type="checkbox"/> Use Default
Timeout for Reply	<input checked="" type="checkbox"/> 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.

The screenshot shows the 'Console Settings' page. The left navigation menu includes System, Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, Security, Storm Control, 802.1X, DHCP Snooping, Port Security, AAA, TACACS+ Server, Radius Server, Access, Console, Telnet, HTTP, HTTPS, Access Control List, MAC Address Table, and LLDP. The main content area is titled 'Console Settings' and contains the following sections:

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

Console Information

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.

The screenshot shows the 'Telnet Settings' page. On the left is a navigation menu with categories like System, Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, Security, Console, Access Control List, MAC Address Table, and LLDP. The 'Security' menu is expanded to show 'Telnet'. The main content area is titled 'Telnet Settings' and contains a form with the following fields:

Field	Value
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

Below the form are 'Apply' and 'Disconnect' buttons. At the bottom, there is a 'Telnet Information' table:

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.

The screenshot shows the 'HTTP Settings' page. At the top, there are navigation links: SAVE, LOGOUT, REBOOT, and REFRESH. On the left is a navigation menu with categories like System, Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, Security, Access Control List, MAC Address Table, and LLDP. The 'Security' menu is expanded to show 'HTTP' and 'HTTPS'. The main content area is titled 'HTTP Settings' and contains a form with the following fields:

- HTTP Service:** Radio buttons for 'Enabled' (selected) and 'Disabled'.
- Login Authentication List:** A dropdown menu with 'Default' selected.
- Session Timeout:** A text input field containing '10' and a label '(0-86400) minutes'.

Below the form is an 'Apply' button. Underneath is a section titled 'HTTP Information' which contains a table with the following data:

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.

SAVE | LOGOUT | REBOOT | REFRESH

System
Port Management
Link Aggregation
VLAN
Spanning Tree
Multicast
QoS
Security
Storm Control
802.1X
DHCP Snooping
Port Security
AAA
TACACS+ Server
Radius Server
Access
Console
Telnet
HTTP
HTTPS
Access Control List
MAC Address Table
LLDP

HTTPS Settings

HTTPS Settings

HTTPS Service	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Login Authentication List	Default
Session Timeout	10 (0-86400) minutes

Apply

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.

SAVE | LOGOUT | REBOOT | REFRESH

System
Port Management
Link Aggregation
VLAN
Spanning Tree
Multicast
QoS
Security
Access Control List
MAC-Based ACL
MAC-Based ACE
IPv4-Based ACL
IPv4-Based ACE
ACL Binding
MAC Address Table
LLDP
Diagnostics
RMON
Maintenance

MAC-Based ACL

MAC-Based ACL

ACL Name

Add

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.

The screenshot shows the 'MAC-Based ACE' configuration page. The left sidebar contains a navigation menu with categories like System, Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, Security, and Access Control List. Under 'Access Control List', 'MAC-Based ACE' is selected. The main content area is titled 'MAC-Based ACE' and contains a table of configuration fields:

ACL Name	<input type="text"/>
Sequence	<input type="text"/> (Range: 1 - 2147483647, 1 is first processed)
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
DA MAC	<input checked="" type="radio"/> Any <input type="radio"/> User Defined
DA MAC Value	<input type="text"/>
DA MAC Mask	<input type="text"/> (0s for matching, 1s for no matching)
SA MAC	<input checked="" type="radio"/> Any <input type="radio"/> User Defined
SA MAC Value	<input type="text"/>
SA MAC Mask	<input type="text"/> (0s for matching, 1s for no matching)
VLAN ID	<input type="text"/> (Range: 1 - 4094)
802.1p	<input type="checkbox"/> Include
802.1p Value	<input type="text"/> (Range: 0-7)
802.1p Mask	<input type="text"/>

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.

The screenshot shows the 'IPv4-Based ACL' configuration page. The left sidebar is similar to the previous page, but 'IPv4-Based ACL' is selected under 'Access Control List'. The main content area is titled 'IPv4-Based ACL' and contains:

- An 'ACL Name' input field.
- An 'Add' button.
- An 'ACL Table' section with a table containing one entry:

ACL Name	Delete
<input type="text"/>	<input type="button" value="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.

SAVE | LOGOUT | REBOOT | REFRESH

- System
- Port Management
- Link Aggregation
- VLAN
- Spanning Tree
- Multicast
- QoS
- Security
- Access Control List
 - MAC-Based ACL
 - MAC-Based ACE
 - IPv4-Based ACL
 - IPv4-Based ACE
 - ACL Binding
- MAC Address Table
- LLDP
- Diagnostics
- RMON
- Maintenance

IPv4-Based ACE

IPv4-Based ACE

ACL Name	<input type="text"/>
Sequence	<input type="text"/> (Range: 1 - 2147483647, 1 is first processed)
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Protocol	<input checked="" type="radio"/> Any(IP) <input type="radio"/> Select from list <input type="text" value="icmp"/> <input type="radio"/> Protocol ID to match <input type="text" value="1"/>
Source IP Address	<input checked="" type="radio"/> Any <input type="radio"/> User Defined
Source IP Address Value	<input type="text"/>
Source IP Wildcard Mask	<input type="text"/> (0s for matching, 1s for no matching)
Destination IP Address	<input checked="" type="radio"/> Any <input type="radio"/> User Defined
Destination IP Address Value	<input type="text"/>
Destination IP Wildcard Mask	<input type="text"/> (0s for matching, 1s for no matching)
Source Port	<input checked="" type="radio"/> Any <input type="radio"/> Single <input type="text" value="0"/> (Range: 0 - 65535) <input type="radio"/> Range <input type="text" value="0"/> - <input type="text" value="65535"/> (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.

SAVE | LOGOUT | REBOOT | REFRESH

- System
- Port Management
- Link Aggregation
- VLAN
- Spanning Tree
- Multicast
- QoS
- Security
- Access Control List
 - MAC-Based ACL
 - MAC-Based ACE
 - IPv4-Based ACL
 - IPv4-Based ACE
 - ACL Binding
- MAC Address Table
- LLDP
- Diagnostics
- RMON
- Maintenance

ACL Binding

ACL Binding

Binding Port	ACL Select
Select Ports	<input type="checkbox"/> MAC-Based ACL <input type="text"/> <input type="checkbox"/> IPv4-Based ACL <input type="text"/> <input type="checkbox"/> IPv6-Based ACL <input type="text"/>

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**.

SAVE | LOGOUT | REBOOT | REFRESH

System
Port Management
Link Aggregation
VLAN
Spanning Tree
Multicast
QoS
Security
Access Control List
MAC Address Table
Static MAC Setting
MAC Filtering
Dynamic Address Setting
Dynamic Learn
RMA Setting
LLDP
Diagnostics
RMON
Maintenance

Static MAC

Static MAC Setting

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

Add

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**.

SAVE | LOGOUT | REBOOT | REFRESH

System
Port Management
Link Aggregation
VLAN
Spanning Tree
Multicast
QoS
Security
Access Control List
MAC Address Table
Static MAC Setting
MAC Filtering
Dynamic Address Setting
Dynamic Learn
RMA Setting
LLDP
Diagnostics
RMON
Maintenance

MAC Filtering

MAC Filtering Setting

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

Add

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.

SAVE | LOGOUT | REBOOT | REFRESH

Dynamic Address Setting

Dynamic Address Setting

Aging Time: 300 (Range: 10 - 630)

Apply

Dynamic Address Status

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**.

SAVE | LOGOUT | REBOOT | REFRESH

Dynamic Learned

Port: GE1

VLAN: Default

MAC Address: 00:00:00:00:00:00

View Clear

MAC Address Information

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

Total Entries:1

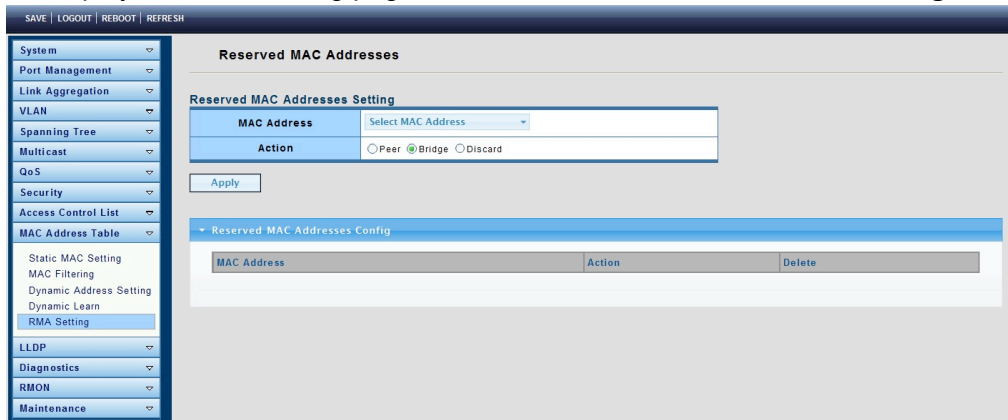
Port: Select the port number to show or clear dynamic MAC entries. If not selecting any port, VLAN or MAC address, the whole dynamic MAC table will be displayed or cleared.

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**.

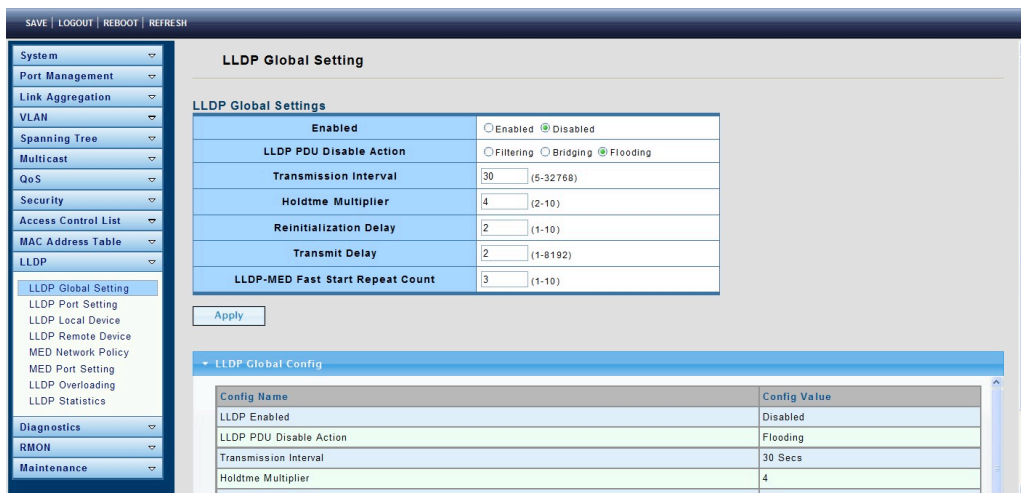


4.11 LLDP

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**.



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 on the 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**.

The screenshot shows the 'LLDP Port Setting' configuration page. On the left is a navigation menu with categories like System, Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, Security, Access Control List, MAC Address Table, LLDP, Diagnostics, RMON, and Maintenance. The LLDP section is expanded to show 'LLDP Port Setting'.

The main content area is titled 'LLDP Port Setting' and contains the following sections:

- LLDP Port Configuration:** A table with two columns: 'Port Select' (a dropdown menu) and 'State' (a dropdown menu with 'Disable' selected). Below this is an 'Apply' button.
- Optional TLVs Selection:** A table with two columns: 'Port Select' (a dropdown menu) and 'Optional TLV Select' (a dropdown menu). Below this is an 'Apply' button.
- LLDP Port Status:** A table showing the status of LLDP on various ports.

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.

- ℓ Disable: Disable the transmission of LLDP PDUs.
- ℓ RX Only: Receive LLDP PDUs only.
- ℓ TX Only: Transmit LLDP PDUs only.
- ℓ 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.

The screenshot shows the 'LLDP Local Device' configuration page. On the left is the same navigation menu as in the previous screenshot, with 'LLDP Local Device' selected.

The main content area is titled 'LLDP Local Device' and contains the following sections:

- Local Device Summary:** A table showing summary information for the local device.
- Port Status:** A table showing the status of LLDP on various ports.

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.

The screenshot shows the 'LLDP Remote Device' configuration page. At the top, there are navigation links: SAVE | LOGOUT | REBOOT | REFRESH. The left sidebar contains a menu with categories: System, Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, Security, Access Control List, MAC Address Table, LLDP, Diagnostics, RMON, and Maintenance. Under the LLDP category, the following items are listed: LLDP Global Setting, LLDP Port Setting, LLDP Local Device, LLDP Remote Device (highlighted), MED Network Policy, MED Port Setting, LLDP Overloading, and LLDP Statistics. The main content area is titled 'LLDP Remote Device' and features a sub-header 'LLDP Remote Device' with buttons for 'Detail', 'Delete', and 'Refresh'. Below this is a table with the following columns: Sel, Local Port, Chassis ID Subtype, Chassis ID, Port ID Subtype, Port ID, System Name, and Time to Live. The table is currently empty.

4.11.5 MED Network Policy

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

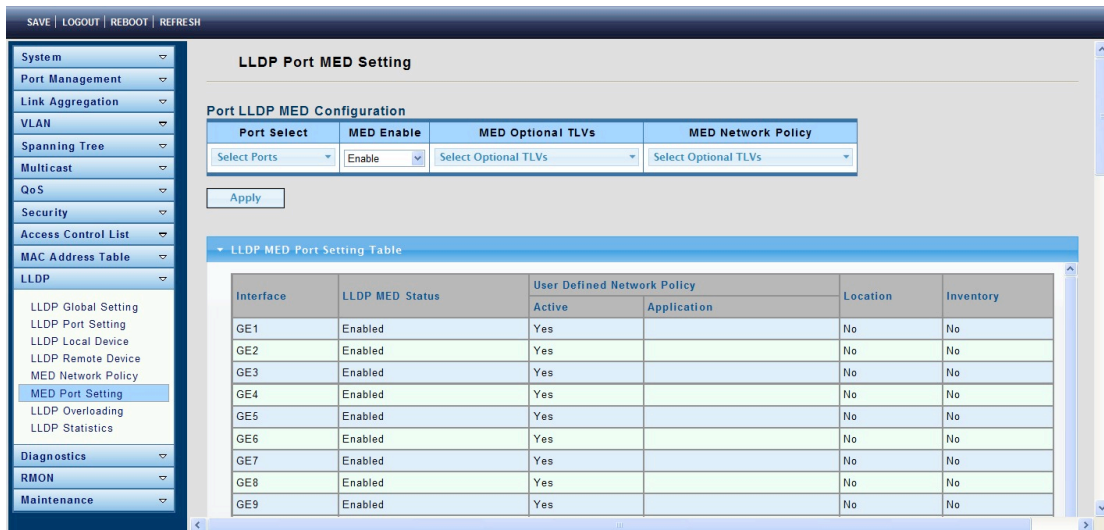
The screenshot shows the 'LLDP MED Network Policy Setting' configuration page. At the top, there are navigation links: SAVE | LOGOUT | REBOOT | REFRESH. The left sidebar contains a menu with categories: System, Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, Security, Access Control List, MAC Address Table, LLDP, Diagnostics, RMON, and Maintenance. Under the LLDP category, the following items are listed: LLDP Global Setting, LLDP Port Setting, LLDP Local Device, LLDP Remote Device, MED Network Policy (highlighted), MED Port Setting, LLDP Overloading, and LLDP Statistics. The main content area is titled 'LLDP MED Network Policy Setting' and features a sub-header 'Voice Auto Mode Configuration' with a section 'LLDP MED Policy for Voice Application' and radio buttons for 'Auto' (selected) and 'Manual'. Below this is an 'Apply' button. The next section is 'Network Policy Configuration' with a table of configuration fields:

Network Policy Number	1
Application	Voice
VLAN ID	1 (1-4095)
VLAN Tag	<input checked="" type="radio"/> Tagged <input type="radio"/> Untagged
L2 Priority	0 (0-7)
DSCP Value	0 (0-63)

 Below the table is an 'Apply' button. At the bottom, there is a section 'LLDP MED Network Policy Table' with a 'Delete' button and a table with the following columns: Network Policy Number, Application, VLAN ID, VLAN Tag, L2 Priority, and DSCP Value. The table is currently empty.

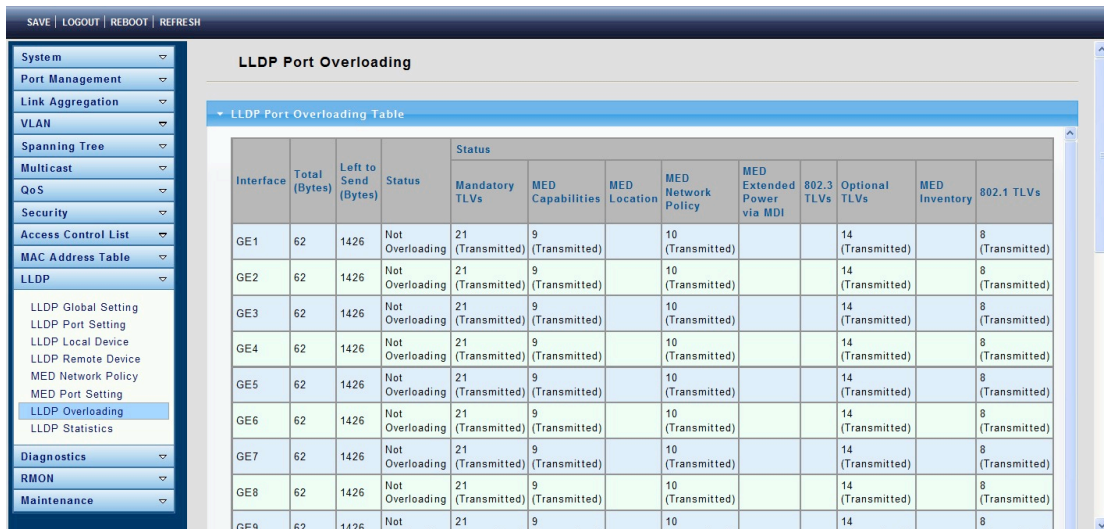
4.11.6 MED Port Setting

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



4.11.7 LLDP Overloading

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



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**.

The screenshot shows the LLDP Statistics page with the following data:

LLDP Global Statistics

Category	Value
Insertions	0
Deletions	0
Drops	0
Age Outs	0

LLDP Port Statistics

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.

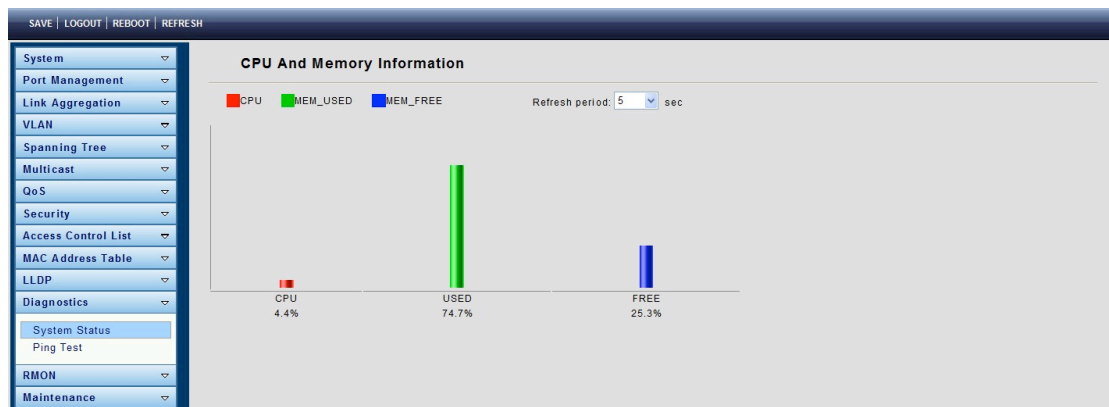
4.12 Diagnostics

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.



4.12.2 Ping Test

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

The screenshot shows the 'Ping Test' page. At the top, there are links for 'SAVE', 'LOGOUT', 'REBOOT', and 'REFRESH'. A navigation menu on the left lists various system settings, with 'Ping Test' selected. The main content area is titled 'Ping Test' and contains a 'Ping Test Setting' form with the following fields:

- 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 (0 - 5120 | Default: 56)

Below the settings is a large empty text area labeled 'Ping Results'. An 'Apply' button is located at the bottom of the form.

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.

SAVE | LOGOUT | REBOOT | REFRESH

System
Port Management
Link Aggregation
VLAN
Spanning Tree
Multicast
QoS
Security
Access Control List
MAC Address Table
LLDP
Diagnostics
RMON
RMON Statistics
RMON Event
RMON Event Log
RMON Alarm
RMON History
RMON History Log
Maintenance

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.

SAVE | LOGOUT | REBOOT | REFRESH

System
Port Management
Link Aggregation
VLAN
Spanning Tree
Multicast
QoS
Security
Access Control List
MAC Address Table
LLDP
Diagnostics
RMON
RMON Statistics
RMON Event
RMON Event Log
RMON Alarm
RMON History
RMON History Log
Maintenance

RMON Event

RMON Event Settings

Select Index: Create New

Index: 0 (1-65535)

Type: None

Community: public

Owner: (0-31 Characters)

Description: (0-127 Characters)

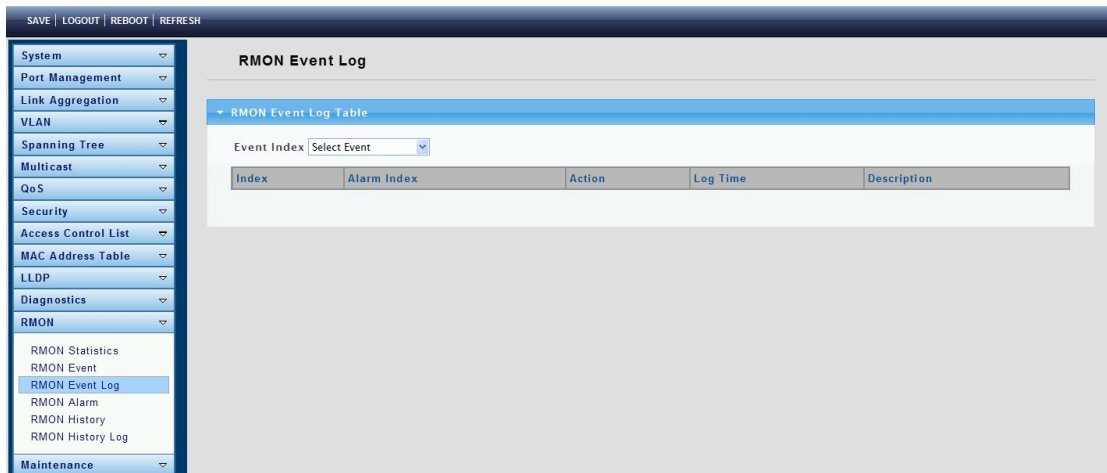
Index	Event Type	Community	Description	Last Sent Time	Owner	Action
-------	------------	-----------	-------------	----------------	-------	--------

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

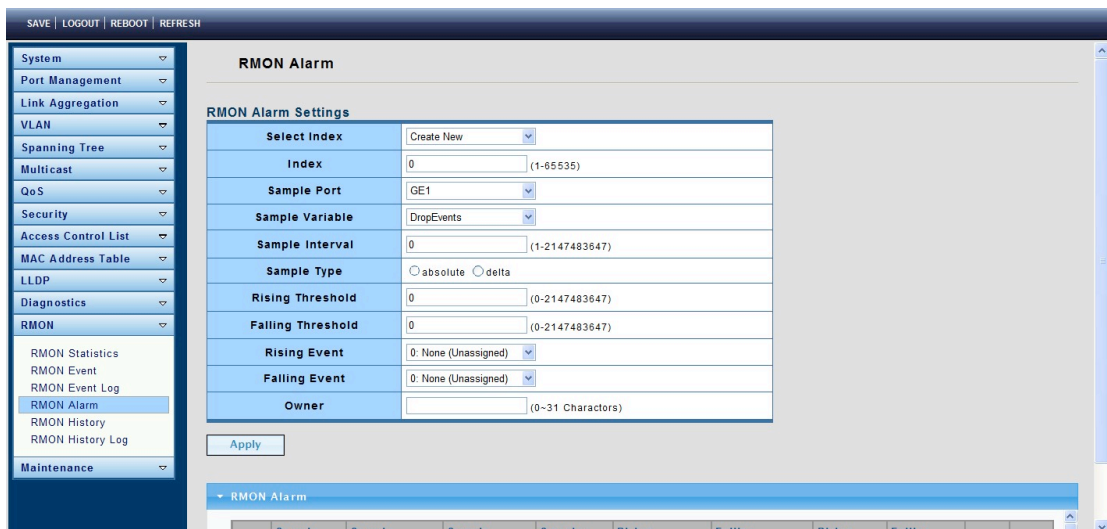
occurred.



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.



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.

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.

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.

SAVE | LOGOUT | REBOOT | REFRESH

System ▾
Port Management ▾
Link Aggregation ▾
VLAN ▾
Spanning Tree ▾
Multicast ▾
QoS ▾
Security ▾
Access Control List ▾
MAC Address Table ▾
LLDP ▾
Diagnostics ▾
RMON ▾
Maintenance ▾
 Factory Default
 Reboot Switch
Backup Manager
 Upgrade Manager
 Configuration Manager
 Enable Password

Backup Manager

Backup Manager

Backup Method	TFTP ▾
Server IP	<input type="text"/>
Backup Type	<input checked="" type="radio"/> Image <input type="radio"/> Startup configuration <input type="radio"/> Backup configuration <input type="radio"/> Flash log <input type="radio"/> Buffer log

SAVE | LOGOUT | REBOOT | REFRESH

System ▾
Port Management ▾
Link Aggregation ▾
VLAN ▾
Spanning Tree ▾
Multicast ▾
QoS ▾
Security ▾
Access Control List ▾
MAC Address Table ▾
LLDP ▾
Diagnostics ▾
RMON ▾
Maintenance ▾
 Factory Default
 Reboot Switch
Backup Manager
 Upgrade Manager
 Configuration Manager
 Enable Password

Backup Manager

Backup Manager

Backup Method	TFTP ▾
Server IP	<input type="text"/>
Backup Type	<input checked="" type="radio"/> Image <input type="radio"/> Startup configuration <input type="radio"/> Backup configuration <input type="radio"/> Flash log <input type="radio"/> Buffer log

Backup Method: Select a backup method.

- ℓ TFTP: Use TFTP to backup.
- ℓ 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.

SAVE | LOGOUT | REBOOT | REFRESH

System
Port Management
Link Aggregation
VLAN
Spanning Tree
Multicast
QoS
Security
Access Control List
MAC Address Table
LLDP
Diagnostics
RMON
Maintenance
Factory Default
Reboot Switch
Backup Manager
Upgrade Manager
Configuration Manager
Enable Password

Upgrade Manager

Upgrade Manager

Upgrade Method	TFTP
Server IP	
File Name	
Upgrade Type	<input checked="" type="radio"/> Image <input type="radio"/> Startup Configuration <input type="radio"/> Backup Configuration

Upgrade

SAVE | LOGOUT | REBOOT | REFRESH

System
Port Management
Link Aggregation
VLAN
Spanning Tree
Multicast
QoS
Security
Access Control List
MAC Address Table
LLDP
Diagnostics
RMON
Maintenance
Factory Default
Reboot Switch
Backup Manager
Upgrade Manager
Configuration Manager
Enable Password

Upgrade Manager

Upgrade Manager

Upgrade Method	HTTP
Upgrade Type	<input checked="" type="radio"/> Image <input type="radio"/> Startup Configuration <input type="radio"/> Backup Configuration
Browse file	<input type="text"/> 浏览...

Upgrade

Upgrade Method: Select the upgrade method.

- ℓ TFTP: Use TFTP to upgrade.
- ℓ 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.

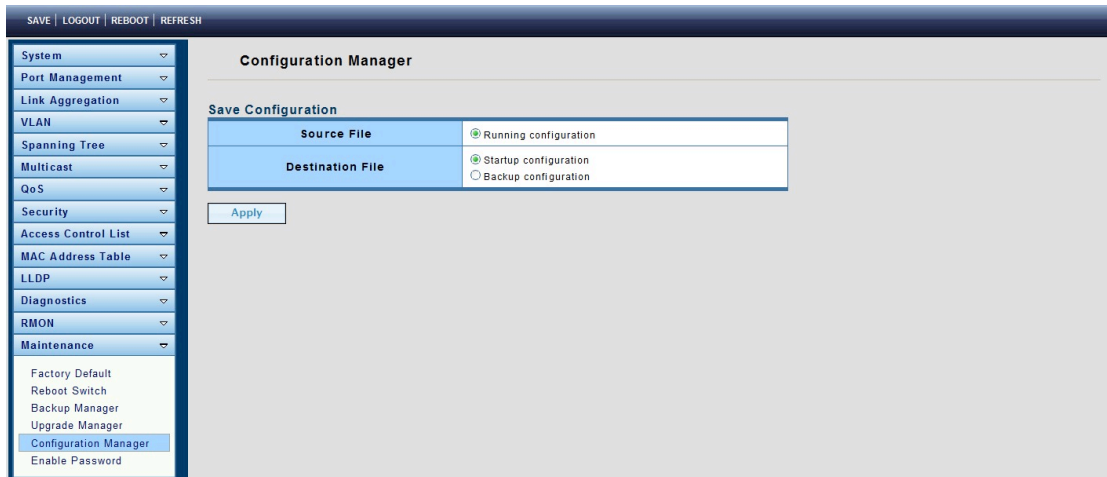
File Name: Firmware image or configuration file name on remote TFTP server. If the TFTP upgrade method is selected, the file name must be specified.

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

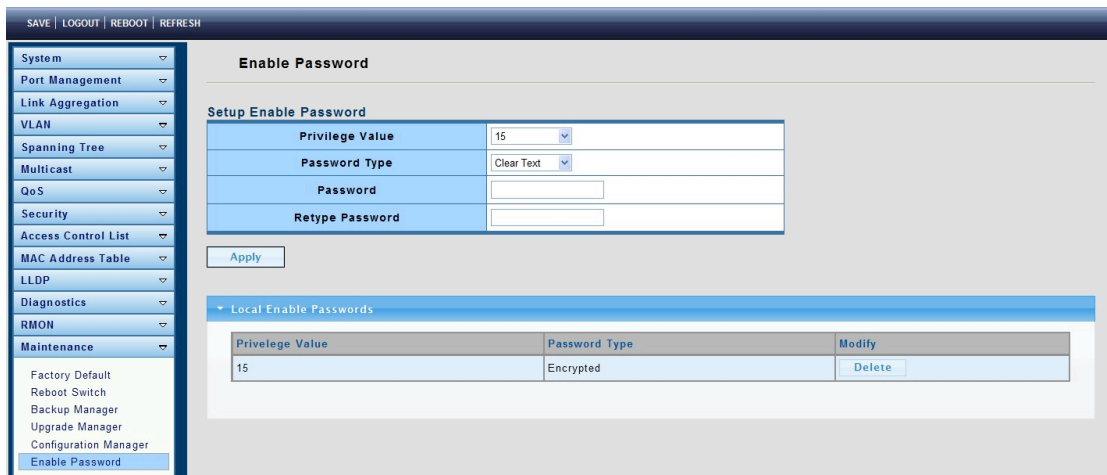
To display the Configuration Manager page, click **Maintenance > Configuration Manager**.



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.



Password Type: Select the password type for Enable Password.

- ℓ Clear Text: Password without encryption.
- ℓ 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.