



**8 + 2SFP Port 10/100/1000Mbps
Managed Ethernet Switch**

User's Manual

Table of Contents

Chapter 1 Product Introduction	3
1.1 Product Overview	3
1.2 Features.....	3
1.3 External Component Description	3
1.3.1 Front Panel.....	3
1.3.2 Rear Panel	5
1.4 Package Contents	5
Chapter 2 Installing and Connecting the Switch.....	6
2.1 Installation.....	6
2.1.1 Desktop Installation.....	6
2.1.2 Rack-mountable Installation in 19-inch Cabinet	6
2.1.3 Power on the Switch	7
2.2 Connect Computer (NIC) to the Switch.....	7
Chapter 3 How to Login the Switch	8
3.1 Switch to End Node	8
3.2 How to Login the Switch.....	8
Chapter 4 Switch Configuration.....	10
4.1 Status.....	10
4.1.1 System Information	10
4.1.2 Logging Message.....	11
4.1.3 Port.....	11
4.1.4 Link Aggregation	13
4.1.5 LLDP Statistics	13
4.1.6 IGMP Snooping Statistics.....	14
4.2 Network.....	15
4.2.1 IP Address	15
4.2.2 Time Settings	15
4.3 Switching	16
4.3.1 Port Setting.....	16
4.3.2 Error Disabled	17
4.3.3 Mirror	18
4.3.4 Link Aggregation	18
4.3.5 Vlan Management.....	21
4.3.6 Multicast	25
4.3.7 Jumbo Frame	30
4.3.8 STP	30
4.4 Mac Address Table	34
4.4.1 Static Mac Setting	34
4.4.2 MAC Filtering	35
4.4.3 Dynamic Address Setting.....	35
4.4.4 Dynamic Learned.....	36

4.4.5 RMA MAC Address	36
4.5 Security.....	36
4.5.1 Storm Control	36
4.5.2 802.1X.....	37
4.5.3 DHCP Snooping.....	39
4.5.4 Port Security.....	43
4.5.5 AAA	44
4.5.6 Tacacs+ Server	47
4.5.7 Radius server	47
4.5.8 Access	48
4.6 ACL.....	51
4.6.1 MAC-Based ACL.....	51
4.6.2 MAC-Based ACE.....	51
4.6.3 IPv4-Based ACL.....	51
4.6.4 IPv4-Based ACE	52
4.6.5 ACL Binding.....	52
4.7 QoS.....	53
4.7.1 General.....	53
4.7.2 QoS Basic Mode	55
4.7.3 QoS Advanced Mode	56
4.7.4 Rate Limit	59
4.8 Management.....	60
4.8.1 LLDP	60
4.8.2 SNMP	64
4.8.3 RMON	68
4.9 Diagnostics	70
4.9.1 System Status	70
4.9.2 Ping Test.....	70
4.9.3 Logging Setting	71
4.9.4 Factory Default.....	72
4.9.5 Reboot Switch	72
4.10 Maintenance	73
4.10.1 Backup Manager.....	73
4.10.2 Upgrade Manager	74
4.10.3 Configuration Manager	74
4.10.4 Account Manager	75
4.10.5 Enable Password	76

Chapter 1 Product Introduction

Congratulations on your purchasing of the Web Smart Ethernet Switch. Before you install and use this product, please read this manual carefully for full exploiting the functions of this product.

1.1 Product Overview

The 8 port + 2SFP 10/100/1000Mbps Managed Ethernet Switch provides the seamless network connection. It integrates 10/100/1000Mbps Ethernet network capabilities. The Web Smart Ethernet Switch, and can be configured by web based interface. Including administrator, port management, VLAN setting, each port statistics, trunking setting, QoS setting, security filter, configuration/ backup/recovery, log out, and so on.

The switch is easy to install and use. It requires no configuration and installation. It is a great selection for office network.

1.2 Features

- Complies with IEEE802.3, IEEE 802.3u, IEEE 802.3ab standards
- 8 x 10/100/1000Mbps Auto-Negotiation RJ45 ports supporting Auto-MDI/MDIX
- Support the Console port management
- Supports IEEE802.3x flow control for Full-duplex Mode and back pressure for Half-duplex Mode
- 8K entry MAC address table of the Managed Ethernet Switch with auto-learning and auto-aging
- Supports WEB management interface
- LED indicators for monitoring power, link, activity and speed
- Internal power adapter supply

1.3 External Component Description

1.3.1 Front Panel

The front panel of the Switch consists of 8 x 10/100/1000Mbps RJ-45 ports, 2 x SFP ports, 1 x Console port, 1 x Reset button and a series of LED indicators as shown as below.



Figure 1 - Front Panel

10/100/1000Mbps RJ-45 ports (1~8):

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 down 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.

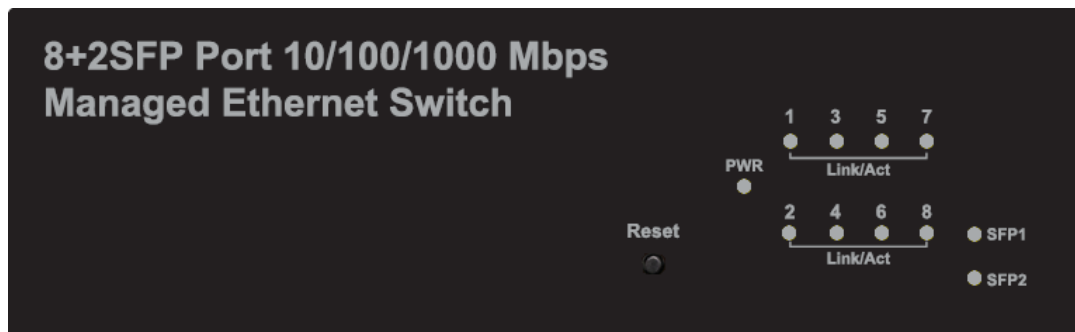


Figure 2 - LED Indicators

The following chart shows the LED indicators of the Switch along with explanation of each indicator.

LED	COLOR	STATUS	STATUS DESCRIPTION
Power	Green	On	Power On
		Off	Power Off
LNK/ACT/ Speed (1~8)	10/100Mbps: Orange	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 contains AC power connector and one marker shown as below.



Figure 3 - Rear Panel

AC Power Connector:

Power is supplied through an external AC power adapter. It supports AC 100~240V, 50~60Hz.

1.4 Package Contents

Before installing the Switch, make sure that the following the "packing list" listed OK. If any part is lost and damaged, please contact your local agent immediately. In addition, make sure that you have the tools install switches and cables by your hands.

- One Web Smart Ethernet Switch
- Four rubber feet, two mounting ears and eights screws
- One AC power cord
- One User Manual

Chapter 2 Installing and Connecting the Switch

This part describes how to install your Web Smart Ethernet Switch and make connections to it. Please read the following topics and perform the procedures in the order being presented.

2.1 Installation

Please follow the following instructions in avoid of incorrect installation causing device damage and security threat.

- Put the Switch on stable place or desktop in case of falling damage.
- 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, do not open the Switch's shell even in power failure.
- Make sure that there is proper heat dissipation from and adequate ventilation around the Switch.
- Make sure the cabinet to enough back up the weight of the Switch and its accessories.

2.1.1 Desktop Installation

Sometimes users are not equipped with the 11-inch standard cabinet. So when installing the Switch on a desktop, please attach these cushioning rubber feet provided on the bottom at each corner of the Switch in case of the external vibration. Allow adequate space for ventilation between the device and the objects around it.

2.1.2 Rack-mountable Installation in 11-inch Cabinet

The Switch can be mounted in an EIA standard-sized, 11-inch rack, which can be placed in a wiring closet with other equipment. To install the Switch, please 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 4 - Bracket Installation

- b. use the screws provided with the equipment rack to mount the Switch on the rack and tighten it.

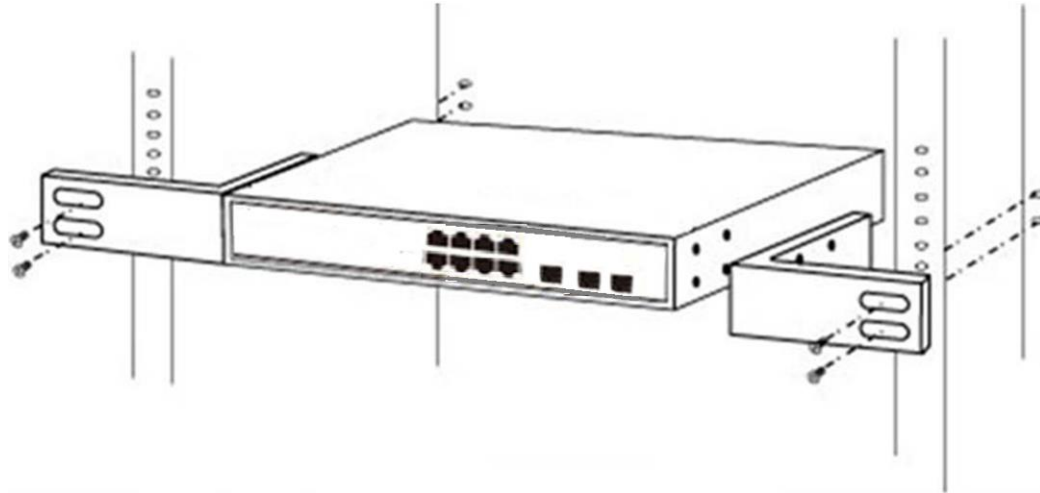


Figure 5 - Rack Installation

2.1.3 Power on the Switch

The Switch is powered on by the AC 100-240V 50/60Hz internal high-performance power supply. Please follow the next tips to connect:

AC Electrical Outlet:

It is recommended to use single-phase three-wire receptacle with neutral outlet or multifunctional computer professional receptacle. Please make sure to connect the metal ground connector to the grounding source on the outlet.

AC Power Cord Connection:

Connect the AC power connector in the back panel of the Switch to external receptacle with the included power cord, and check the power indicator is ON or not. When it is ON, it indicates the power connection is OK.

2.2 Connect Computer (NIC) to the Switch

Please insert the NIC into the computer, after installing network card driver, please connect one end of the twisted pair to RJ-45 jack of your computer, the other end will be connected to any RJ-45 port of the Switch, the distance between Switch and computer is around 100 meters. Once the connection is OK and the devices are power on normally, the LINK/ACT/Speed status indicator lights corresponding ports of the Switch.

Chapter 3 How to Login the Switch

3.1 Switch to End Node

Use standard Cat.5/5e 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 is connected.

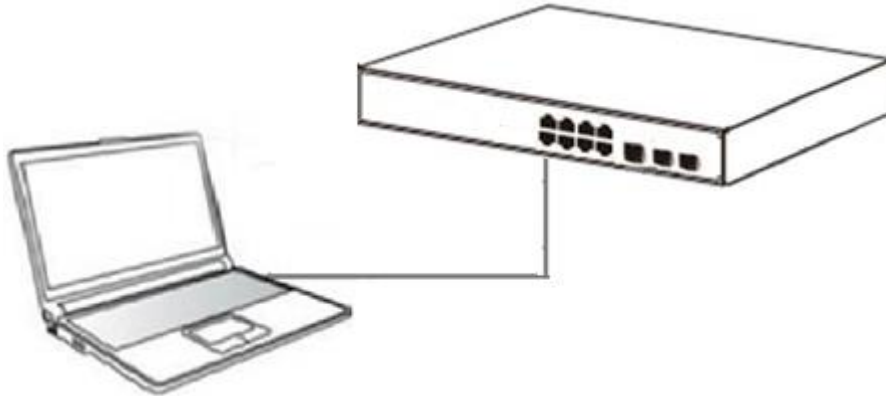


Figure 6 - PC Connect

Please refer to the [LED Indicator Specification](#). The LINK/ACT/Speed LEDs for each port lights on 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 user name	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" ranges 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 7 - 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.

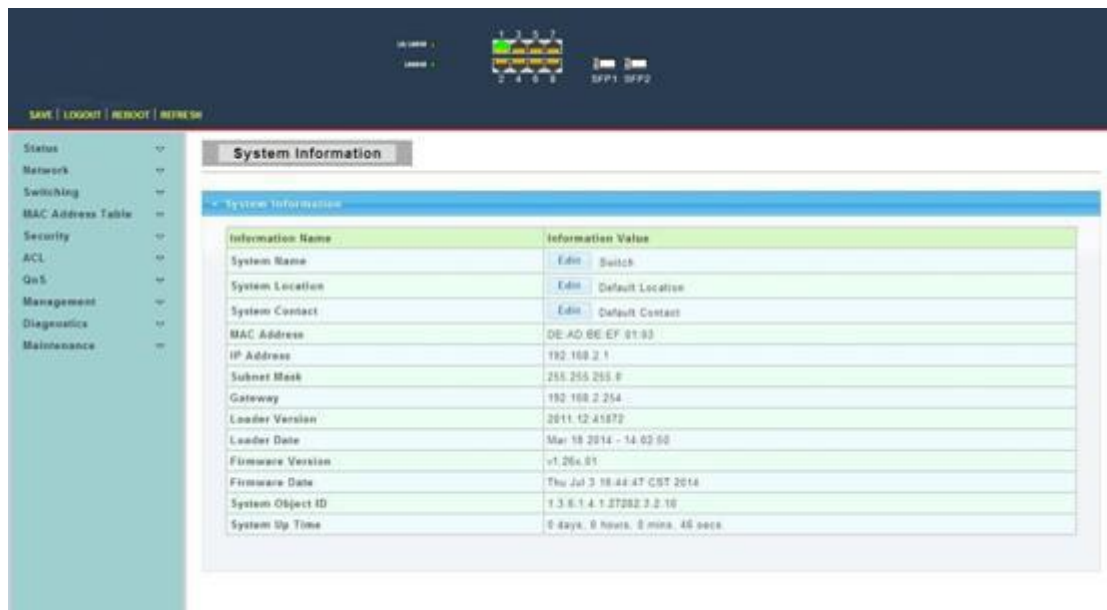
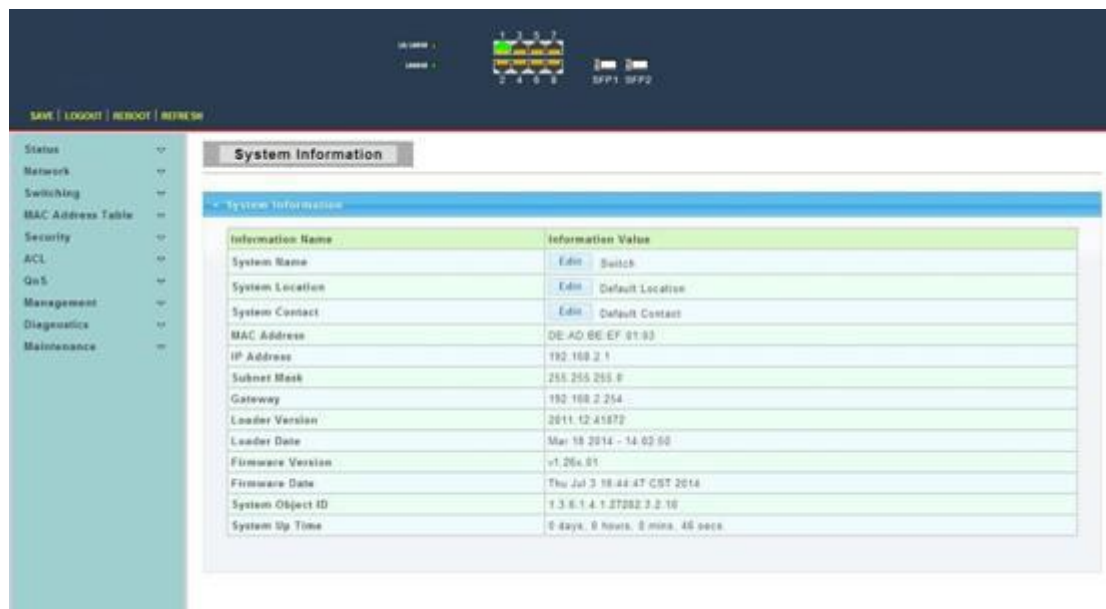


Figure 8 - Configuration Window

Chapter 4 Switch Configuration

The Web Smart Ethernet Switch Managed switch software provides rich layer 2 functionality for switches in your networks. This chapter describes how to use Web-based management interface (Web UI) to this switch 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.



4.1 Status

Use the Status pages to view system information and status.

4.1.1 System Information

To display System Information web page, click **Status > System Information**

This page allow user to configure System related information and browse some system information such as MAC address, IP address, firmware version, loader version etc.



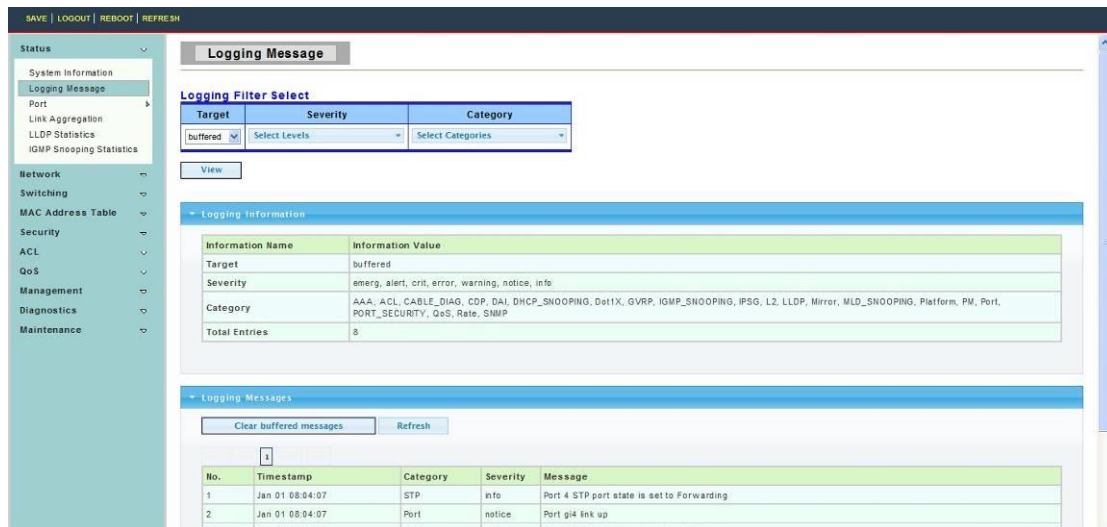
System Name: System name of the switch. This name will also use as CLI prefix of each line. (“Switch>” or “Switch#”).

System Location: System location of the switch.

System Contact: System contact of the switch.

4.1.2 Logging Message

To display Logging Message web page, click **Status > Logging Message**



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

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

Severity: Select severity to filter log messages.

Category: Select category to filter log messages.

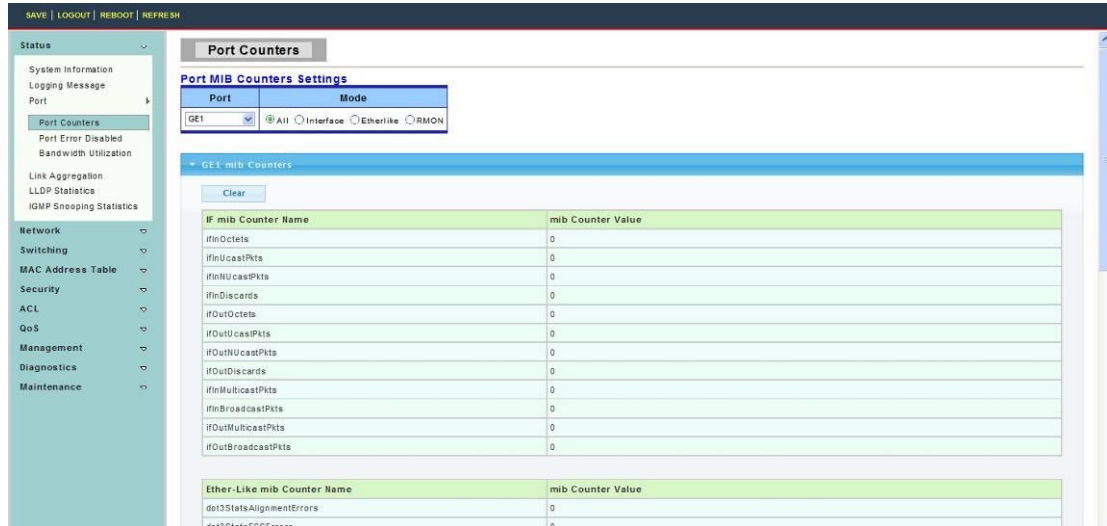
4.1.3 Port

The Port configuration page displays port summary and status information.

4.1.3.1 Port Counters

To display Port Counters web page, click **Status > Port > Port Counters**

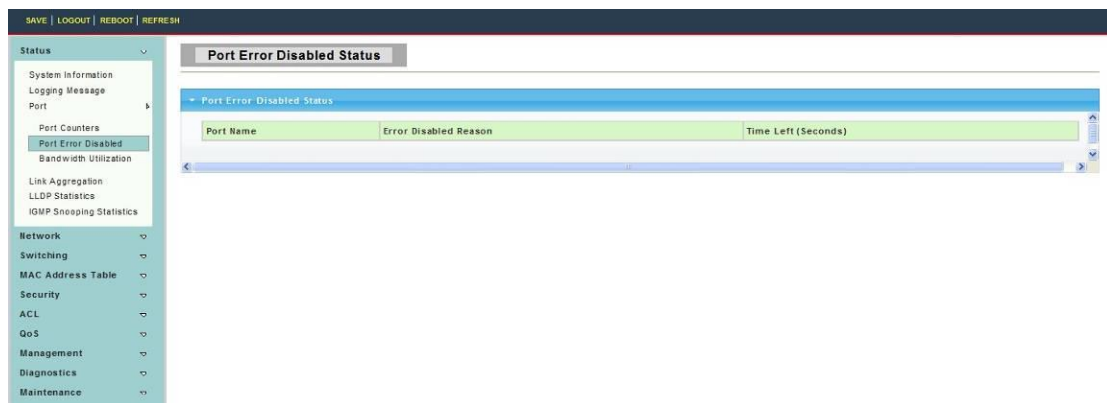
This page displays standard counters on network traffic from the Interfaces, Ethernet-like and RMON MIB. Interfaces and Ethernet-like counters display errors on the traffic passing through each port. RMON counters provide a total count of different frame types and sizes passing through each port.



4.1.3.2 Port Error Disabled

To display Port Error Disabled web page, click **Status > Port > Port Error Disabled**

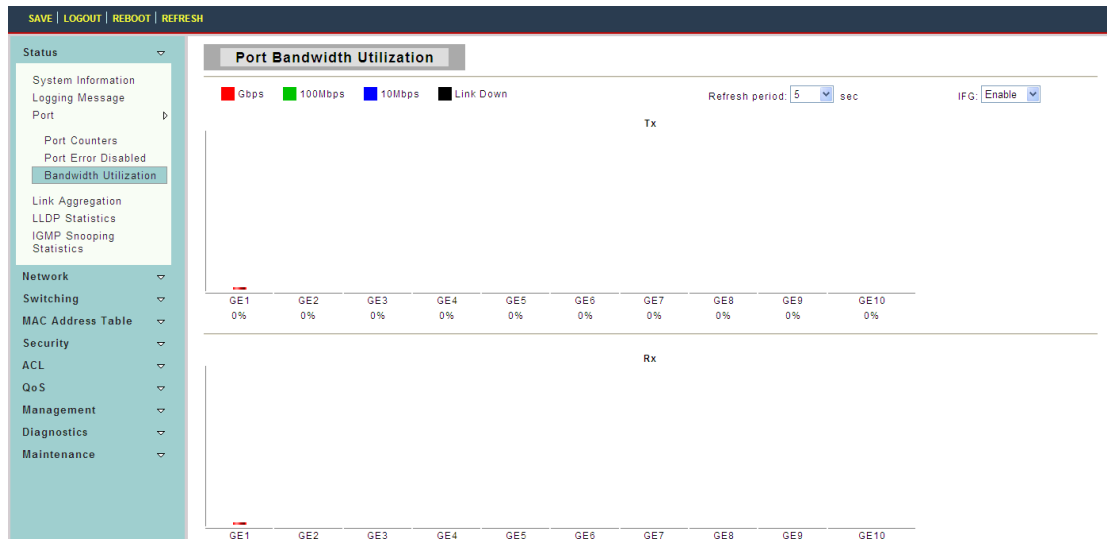
This page allow user to browse ports which disabled by some protocols such as BPDU Guard, Loop back and UDLD. The “Recovery” button will enable those error disabled ports.



4.1.3.3 Bandwidth Utilization

To display Bandwidth Utilization web page, click **Status > Port > Bandwidth Utilization**

This page is used to visual display switch each port TX and RX bandwidth utilization.



4.1.4 Link Aggregation

To display Link Aggregation web page, click **Status > Link Aggregation**

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

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

LAG: LAG ID.

Name: LAG Name.

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

4.1.5 LLDP Statistics

To display LLDP Statistics status, click **Status > LLDP Statistics**

The Link Layer Discovery Protocol (LLDP) Statistics page displays summary and per-port information for LLDP frames transmitted and received on the switch.

The screenshot shows the LLDP Statistics page with a left-hand navigation menu and a main content area. The main content area is divided into two sections: LLDP Global Statistics and LLDP Port Statistics.

LLDP Global Statistics

Insertions	0
Deletions	0
Drops	0
Age Outs	0

LLDP Port Statistics

Port	TX Frames		RX Frames		RX TLVs		RX Ageouts
	Total		Total	Discarded	Discarded	Unrecognized	Total
GE1	0		0	0	0	0	0
GE2	0		0	0	0	0	0
GE3	0		0	0	0	0	0
GE4	23		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

Insertions: The number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) has been inserted into tables associated with the remote systems.

Deletions: The number of times the complete set of information advertised by MSAP has been deleted from tables associated with the remote systems.

Drops: The number of times the complete set of information advertised by MSAP could not be entered into tables associated with the remote systems because of insufficient resources.

Age Outs: The number of times the complete set of information advertised by MSAP has been deleted from tables associated with the remote systems because the information timeliness interval has expired.

4.1.6 IGMP Snooping Statistics

To display IGMP Snooping Statistics web page, click **Status > IGMP Snooping Statistics**

This page is used to display IGMP Snooping statistics information.

The screenshot shows the IGMP Snooping Statistics page with a left-hand navigation menu and a main content area. The main content area is titled IGMP Snooping Statistics and contains a table of statistics.

Statistics Packets	Counter
Total RX	6
Valid RX	6
Invalid RX	0
Other RX	0
Leave RX	0
Report RX	0
General Query RX	0
Specall Group Query RX	0
Specall Group & Source Query RX	0
Leave TX	0
Report TX	0
General Query TX	0
Specall Group Query TX	0
Specall Group & Source Query TX	0

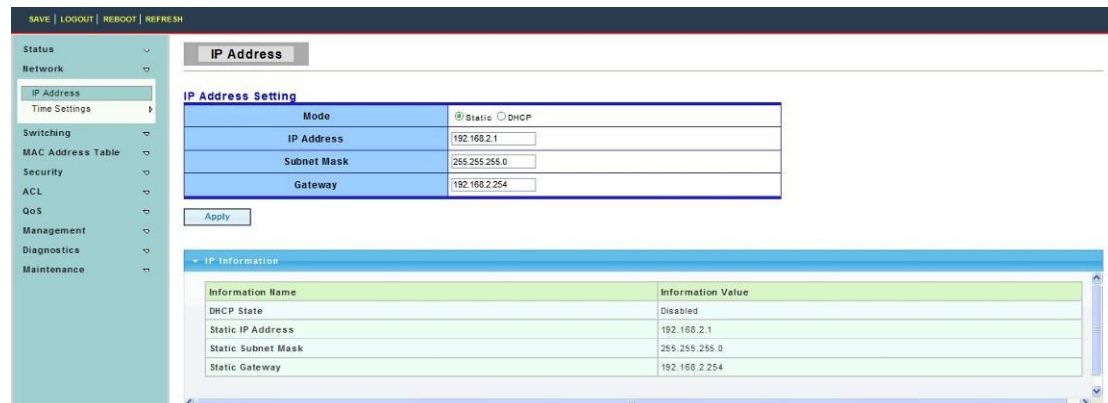
4.2 Network

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

4.2.1 IP Address

To display IP Address web page, click **Network > IP Address**

This page allow user to edit IP address,Subnet Mask and Gateway.



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

Mode: Select the mode of network connection.

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

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

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

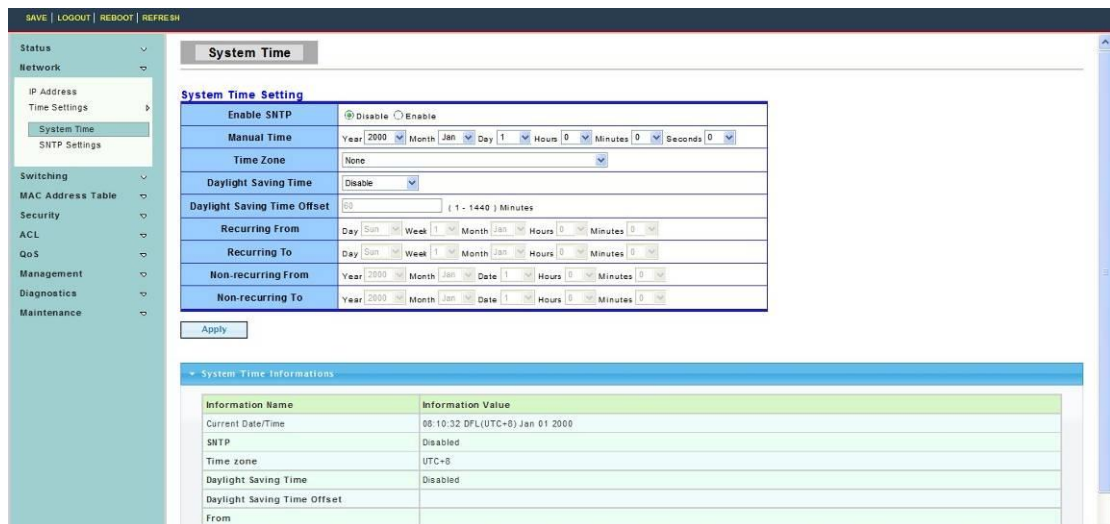
Gateway: If static mode is enabled, enter gateway address in this field.

4.2.2 Time Settings

4.2.2.1 System Time

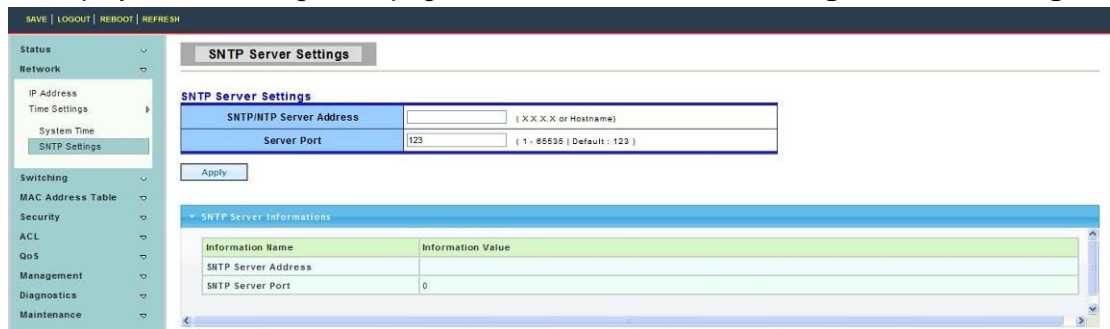
To display System Time web page, click **Network > Time Settings > System Time**

System time setting,that is set time zone,time servicer,get the time and daylight sav ing time automatically.



4.2.2.2 SNTP Settings

To display SNTP Settings web page, click **Network > Time Settings > SNTP Settings**



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

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

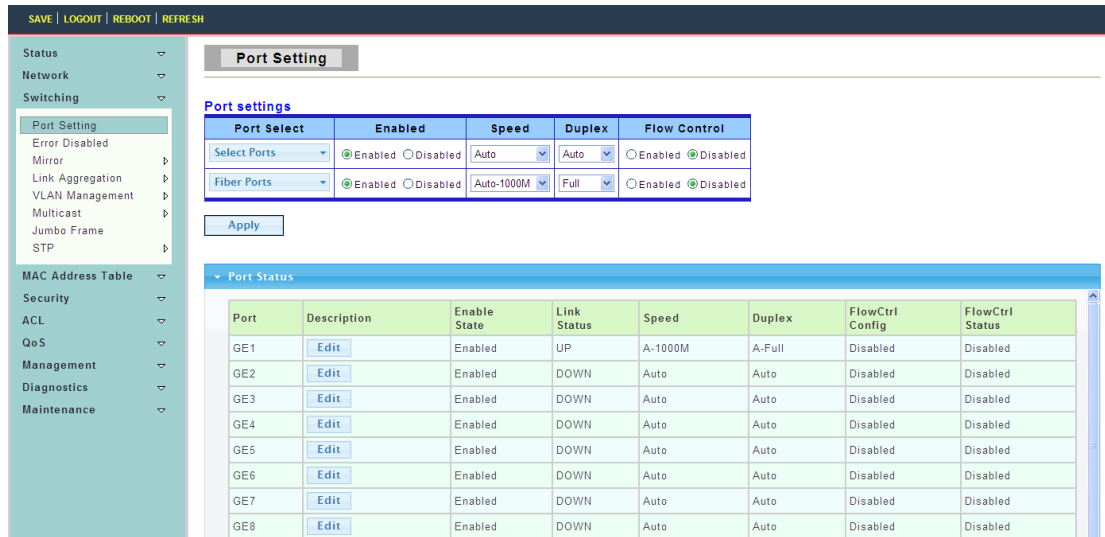
4.3 Switching

Use the Switching pages to configure settings for the switch ports, trunk, layer 2 protocols and other switch features.

4.3.1 Port Setting

To display Port Setting web page, click **Switching > Port Setting**

Port Setting, that is set ports status, speed, duplex mode and fluid control function.



Port Setting

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	UP	A-1000M	A-Full	Disabled	Disabled
GE2	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE3	Edit	Enabled	DOWN	Auto	Auto	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
GE8	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled

Port Select: Select one or multiple ports to configure.

Enabled: Port admin state.

- Enabled: Enable the port.
- Disabled: Disable the port.

Speed: Port speed capabilities.

- Auto: Auto speed with all capabilities.
- Auto-10M: Auto speed with 10M ability only.
- Auto-100M: Auto speed with 100M ability only.
- Auto-1000M: Auto speed with 1000M ability only.
- Auto-10M/100M: Auto speed with 10M/100M abilities.
- 10M: Force speed with 10M ability.
- 100M: Force speed with 100M ability.
- 1000M: Force speed with 1000M ability.

Duplex: Port duplex capabilities.

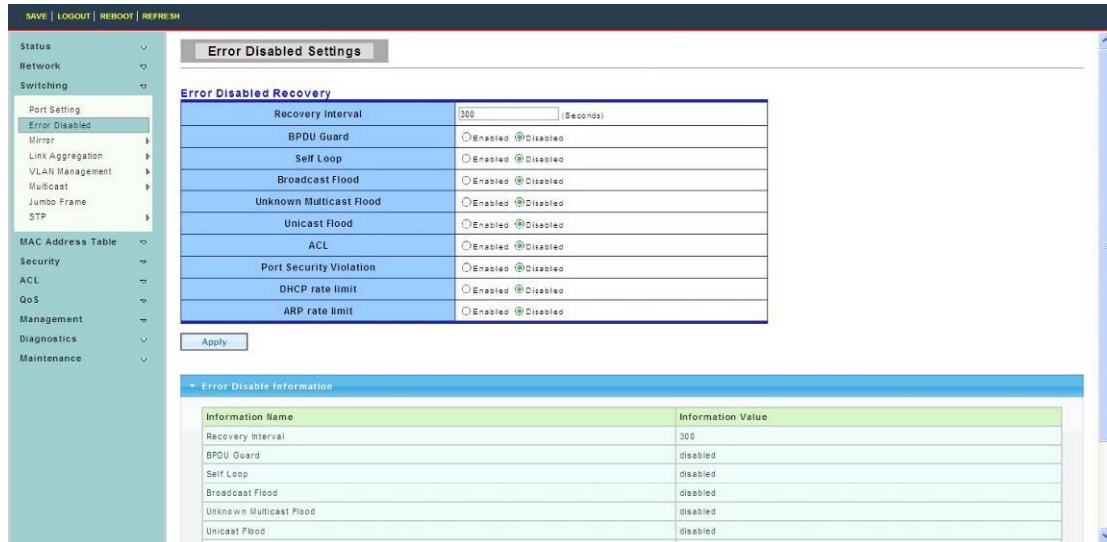
- Auto: Auto duplex with all capabilities.
- Full: Auto speed with full duplex ability only.
- Half: Auto speed with half duplex ability only.

Flow Control: Port flow control.

- Enable: Enable flow control ability.
- Disabled: Disable flow control ability.

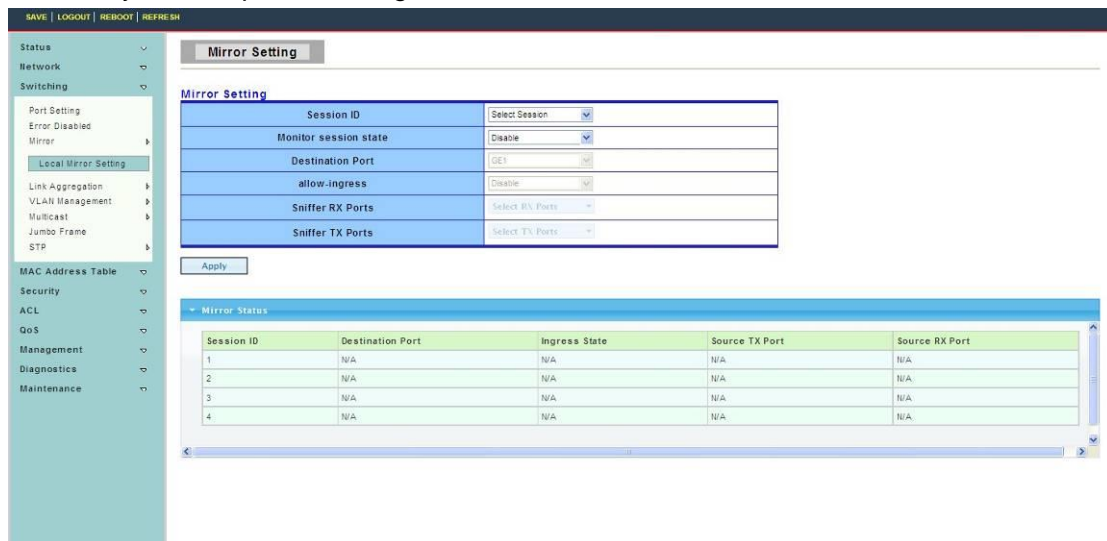
4.3.2 Error Disabled

To display Error Disabled web page, click **Switching > Error Disabled**



4.3.3 Mirror

To display Local Mirror Setting web page,click **Switching > Mirror > Local Mirror Setting**
 Port mirroring,that is copy the TX/RX data flow from the source port to the aiming port, commonly used in port mirroring.



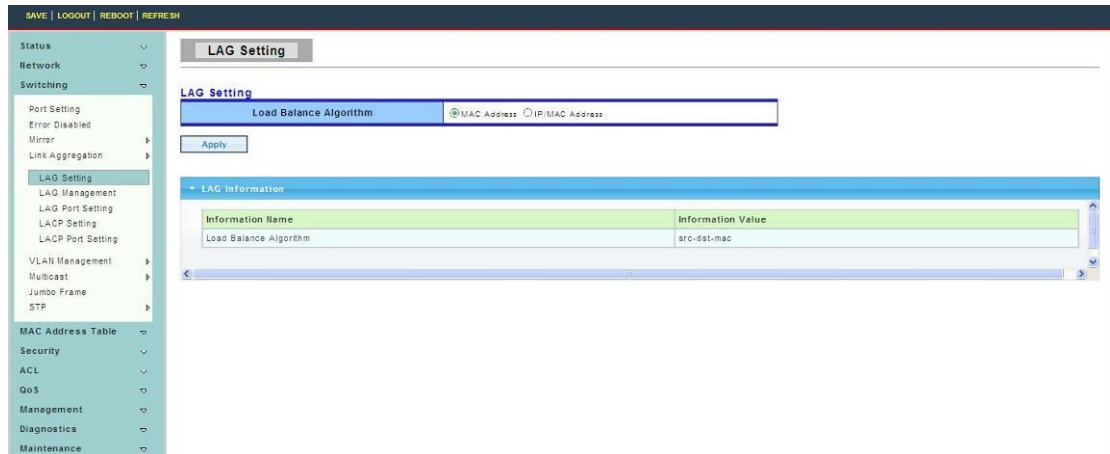
4.3.4 Link Aggregation

Link aggregation,that is multiple Ethernet ports together to form a logical port,it sup ports static allocation or LACP.

4.3.4.1 LAG Setting

To display LAG Setting web page, click **Switching > Link Aggregation > LAG Setting**

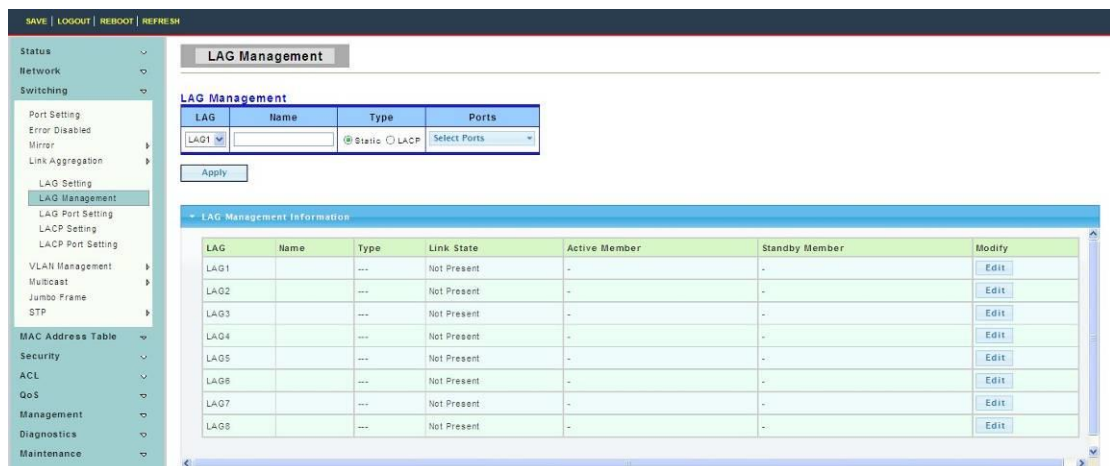
This page allow user to configure Ports aggregation rules that is depended on MAC Address or IP/MAC Address.



4.3.4.2 LAG Management

To display LAG Management web page, click **Switching > Link Aggregation > LAG Management**

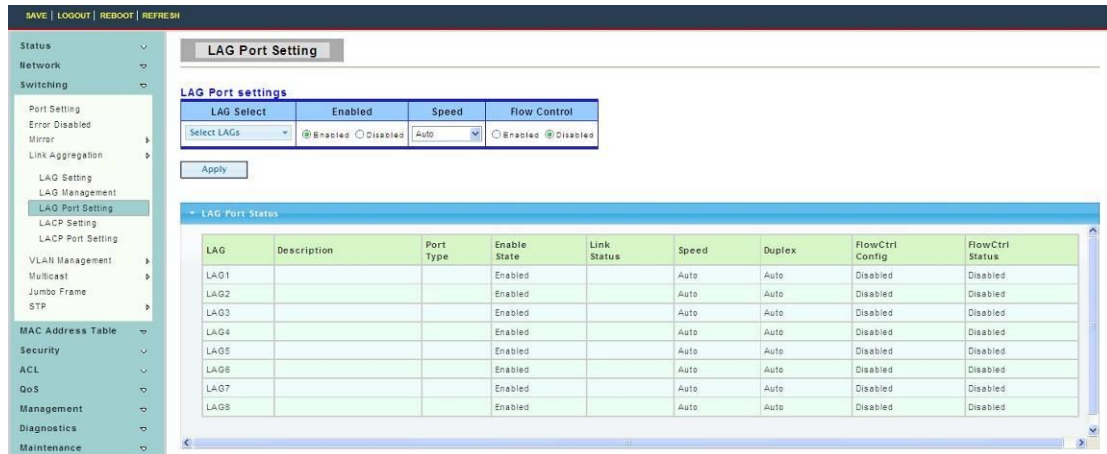
This page is used to create new LAG, configure ports aggregation type, and select member ports.



4.3.4.3 LAG Port Setting

To display LAG Port setting web page, click **Switching > Link Aggregation > LAG Port Setting**

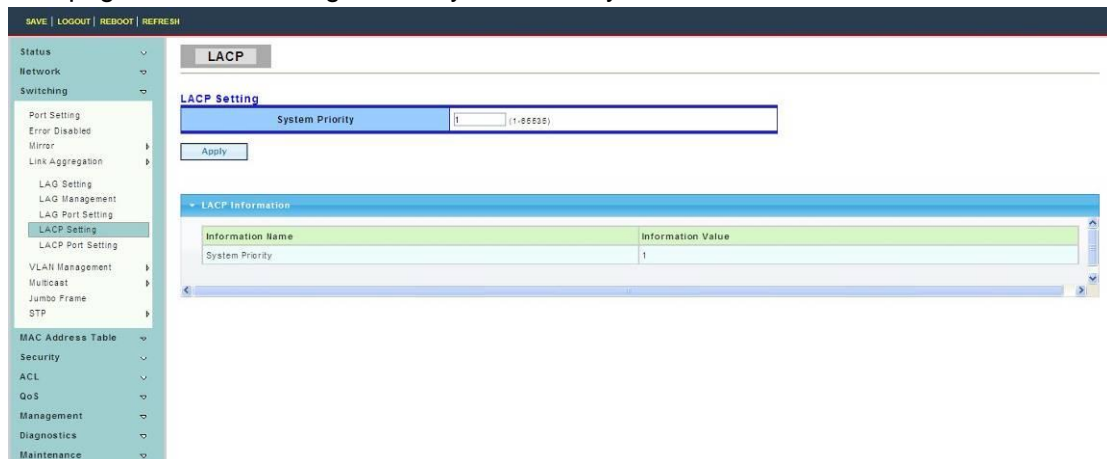
This page is used to set LAG status, speed and fluid control function.



4.3.4.4 LACP Setting

To display LACP Setting web page, click **Switching > Link Aggregation > LACP Setting**

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



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

4.3.4.5 LACP Port Setting

To display LACP Port Setting web page, click **Switching > Link Aggregation > LACP Port Setting**

This page is used to set LACP member ports.

LACP Port Setting

LACP Port Settings

Port Select	Priority	Timeout
Select Ports	1 (1-65535)	<input checked="" type="radio"/> Long <input type="radio"/> 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

4.3.5 VLAN Management

4.3.5.1 Create VLAN

To display Create VLAN web page, click **Switching > VLAN Management > Create VLAN**

This page allow user to add, delete or edit VLAN settings.

Create VLAN

VLAN Setting

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

Apply

VLAN Table

VLAN ID	VLAN Name	VLAN Type	Modify
1	default	Default	Edit

VLAN LIST: VLAN LIST for the new VLAN.

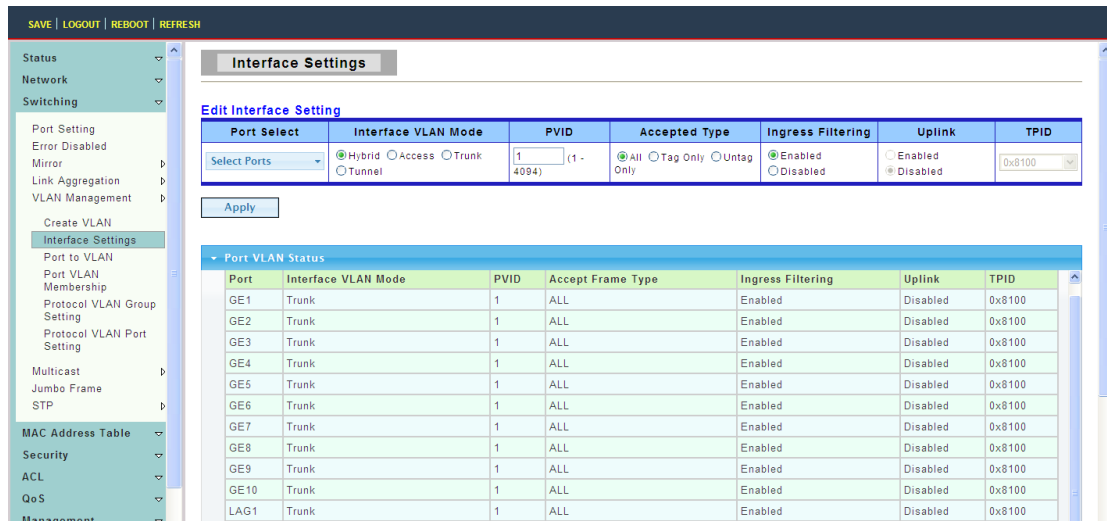
VLAN Action: Add or delete VLAN.

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

4.3.5.2 Interface Settings

To display VLAN Interface Settings web page, **click Switching > VLAN Management > Interface Settings**

This page allows the user to set the port type of vlan, common have access and trunk, dot1q - tunnel three modes and native VLAN choose whether the port TX,RX should have a tag.



Port Select : Select one or multiple ports to configure.

Interface VLAN Mode: VLAN port mode

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

PVID: VLAN ID for the selected ports.

Accepted Type: Port accepted type.

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

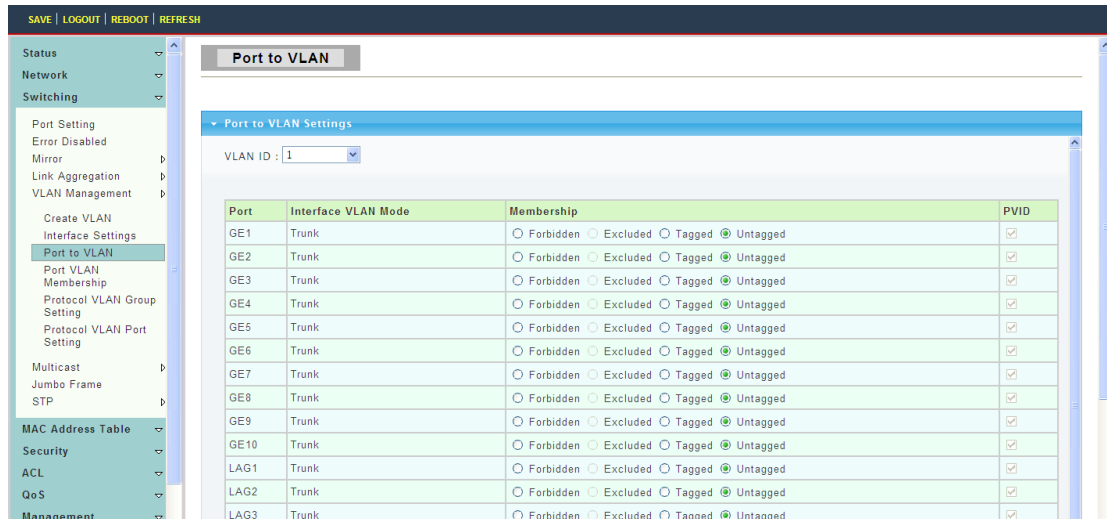
Ingress Filtering: Choose filter port open and close.

Uplink: Select port Uplink open or close.

4.3.5.3 Port to VLAN

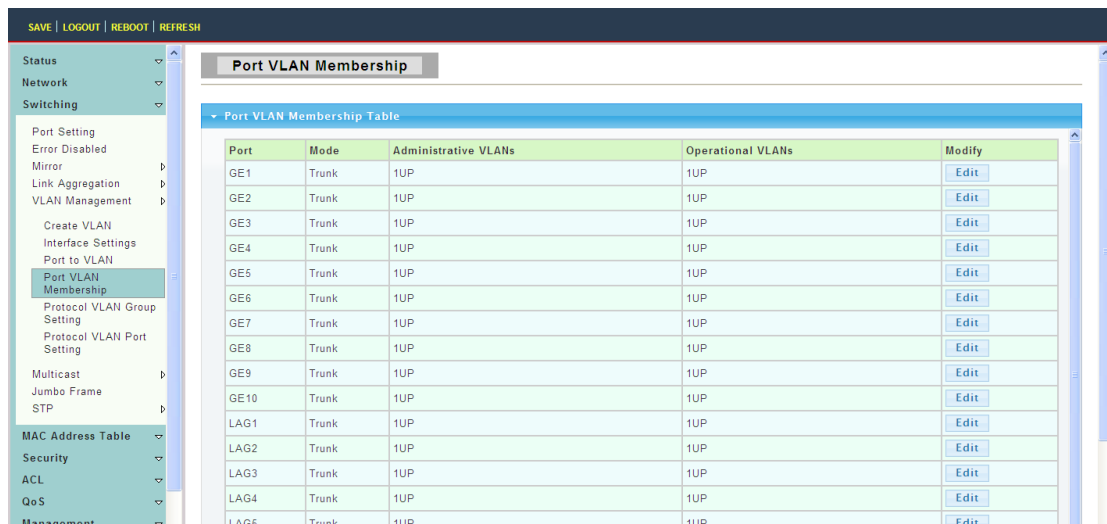
To display Port to VLAN web page, **click Switching > VLAN Management > Port to VLAN**

Make port add to VLAN ,select the port's different behaviors when it works under the VLAN.



4.3.5.4 Port VLAN Membership

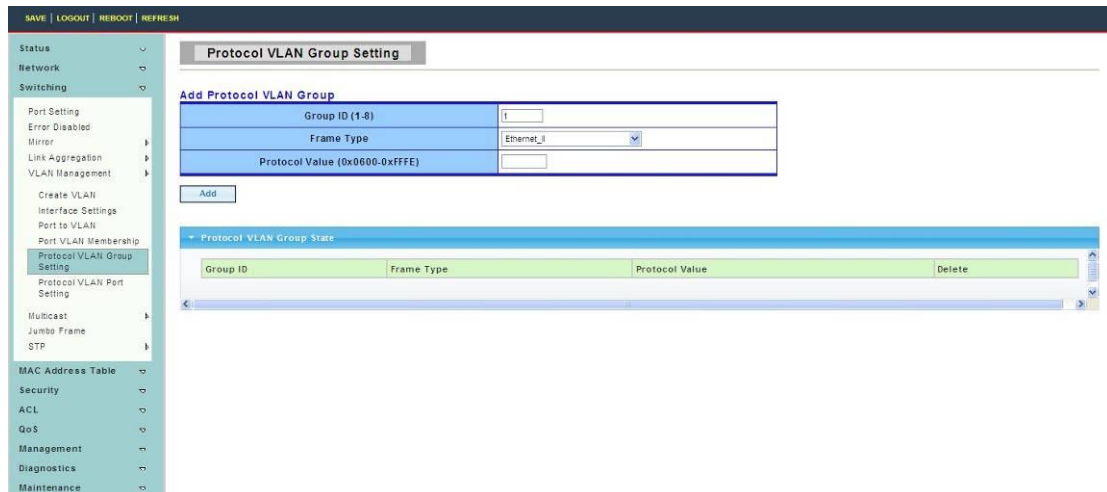
To display Port VLAN Membership web page, click **Switching > VLAN Management > Port VLAN Membership**



4.3.5.5 Protocol VLAN Group Setting

To display Protocol VLAN Group Setting web page, click **Switching > VLAN > Protocol VLAN Group Setting**

The VLAN group setting, that is sets the same type message as a group and transmit it in the specific VLAN.



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

Group Name: This is used to identify the new Protocol VLAN group.Type an alphanumeric string of up to 16 characters.

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

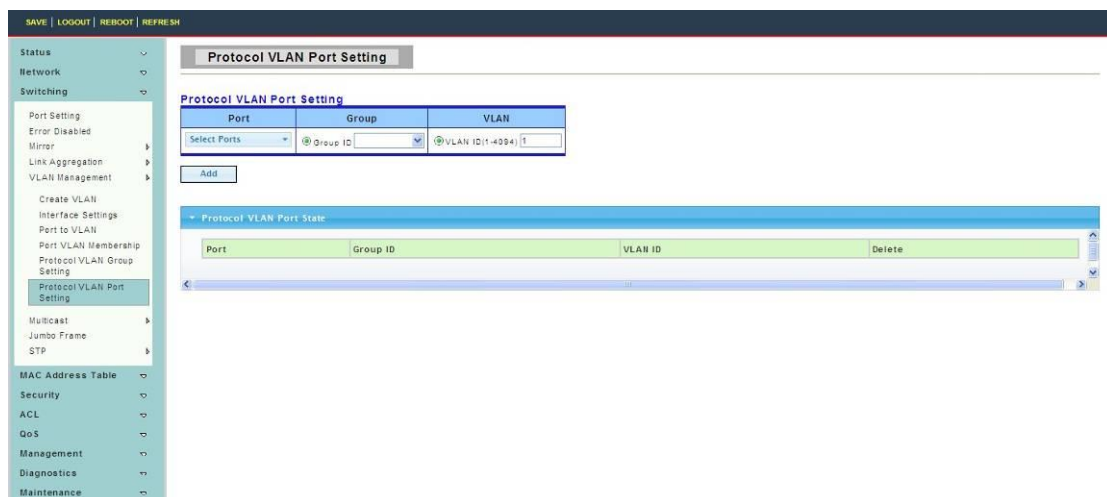
- Ethernet_II: packet type is Ethernet version 2.
- IEEE802.3_LL_C_Other: packet type is 802.3 packet with LLC other header.
- RFC_1042: packet type is RFC 1042 packet.

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

4.3.5.6 Protocol VLAN Port Setting

To display Protocol VLAN Port Setting web page, click **Switching> VLAN> Protocol VLAN Port Setting**

This page is used to divide the port into groups and map it to the VLAN.



Port: Select the specified ports you wish to configure by selecting the port in this list.

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

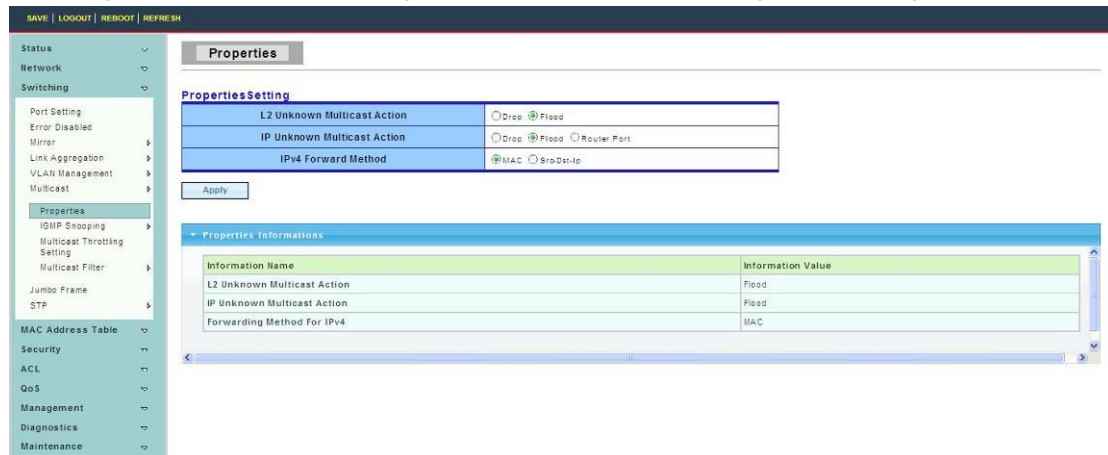
VLAN :Click the corresponding radio button to select a previously configured VLAN ID or VLAN Name.

4.3.6 Multicast

4.3.6.1 Properties

To display Properties web page, click **Switching > Multicast > Properties**

This page is used to Set message behavior and IPv4 message forwarding rules.

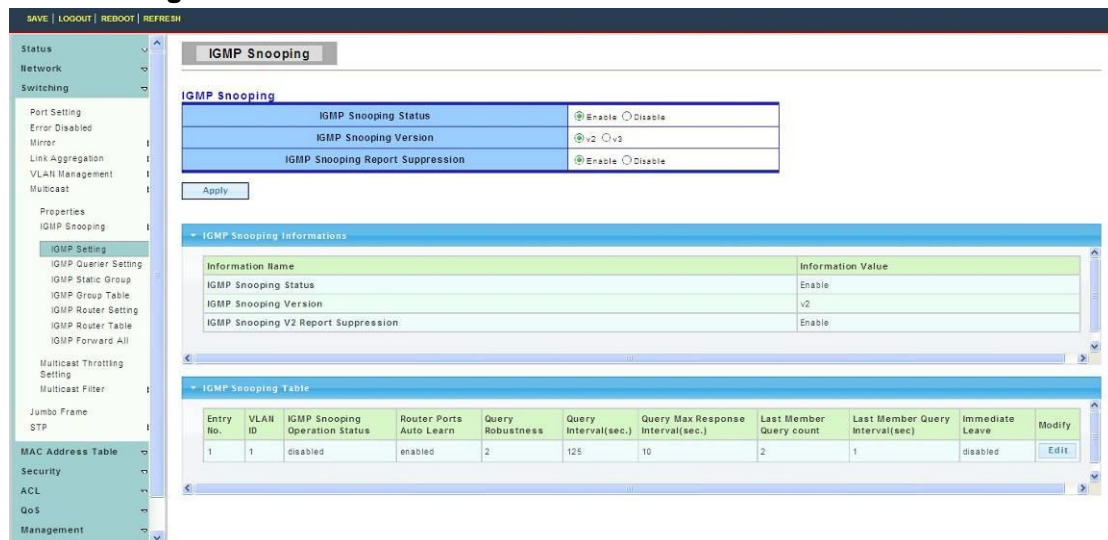


4.3.6.2 IGMP Snooping

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

1. IGMP Setting

To display IGMP Setting web page, click **Switching > Multicast > IGMP Snooping > IGMP Setting**



IGMP Snooping: Select the IGMP Snooping enable or disable.

IGMP Snooping Version: Select the IGMP Snooping Version,IGMPv2 or IGMPv3.

IGMP Snooping Report Suppression:Select the IGMP Snooping Report Suppression enable or disable.

2. IGMP Snooping Querier Setting

To display IGMP Snooping Querier Setting web page, click **Switching > Multicast >**

IGMP Snooping > IGMP Snooping Querier Setting



VLAN ID: Select the VLANs to configure.

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

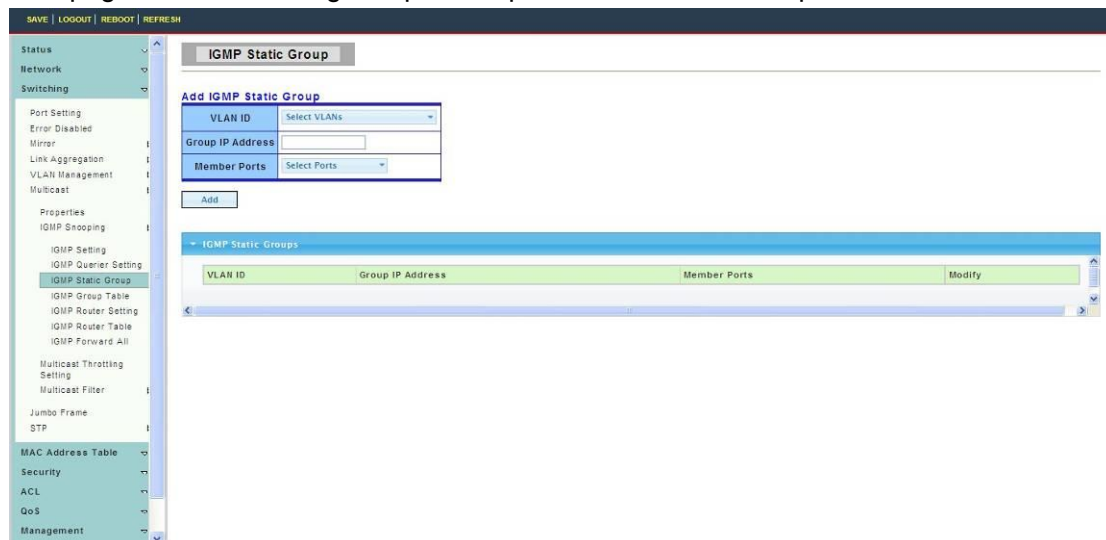
- Enable: Enable IGMP Querier Election.
- Disable: Disable IGMP Querier Election.

Version: Select the Querier Version, IGMPv2 or IGMPv3

3. IGMP Static Group

To display IGMP Static Setting web page, click **Switching > Multicast > IGMP Snooping > IGMP Static Group**

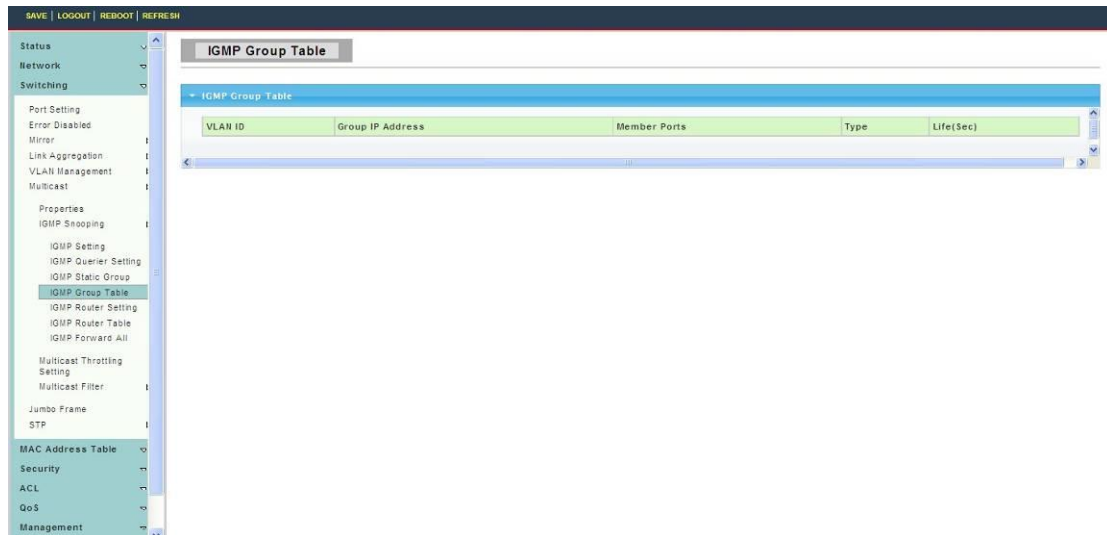
This page is used to configure specified ports as static member ports.



4. IGMP Group Table

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

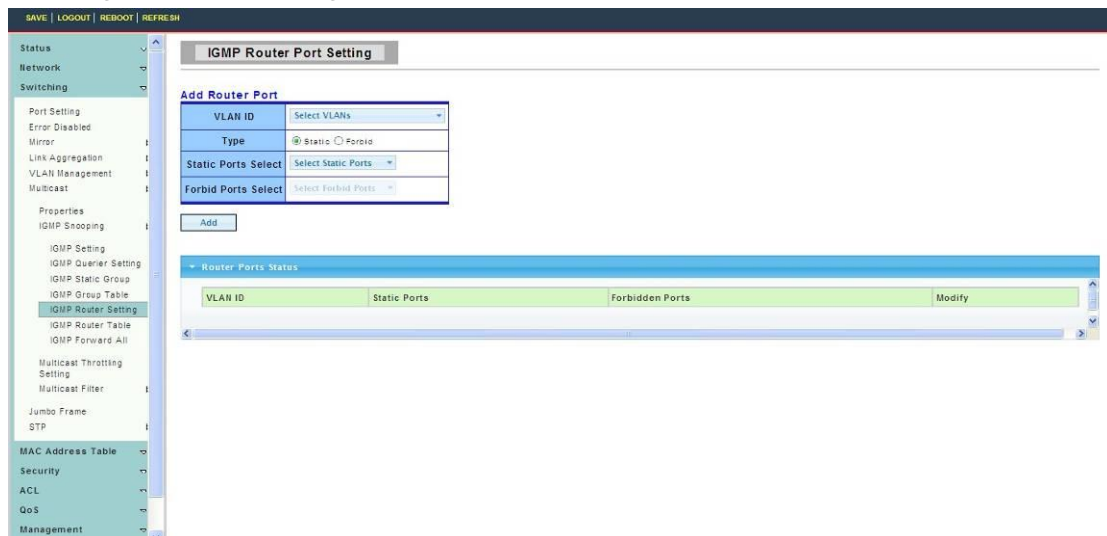
This page is used to display IGMP Group Table statistics information.



5. IGMP Router Port Setting

To display IGMP Router Port Setting web page, click **Switching > Multicast > IGMP Snooping > IGMP Router Port Setting**

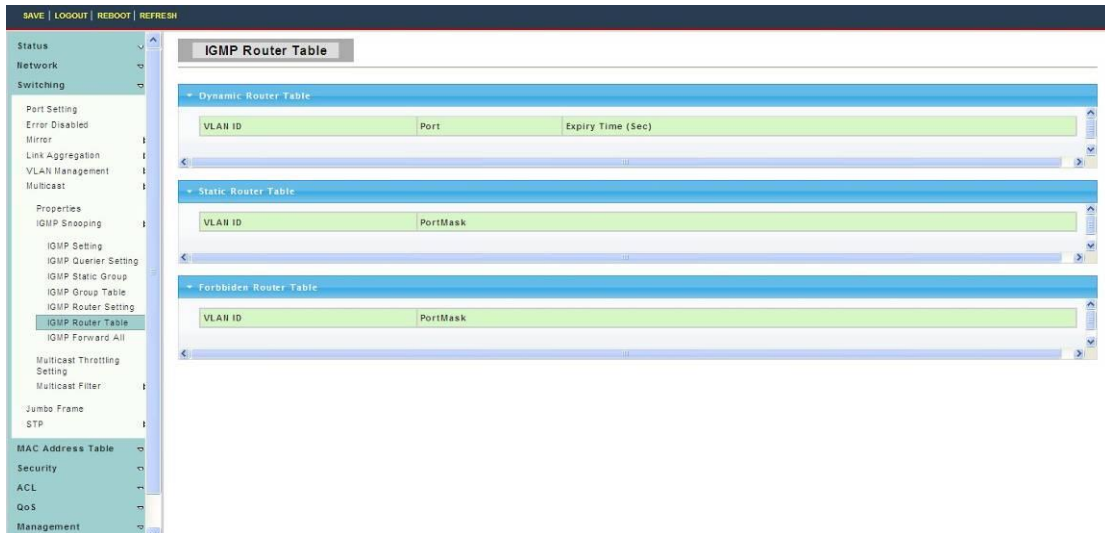
This page is used to configure specified ports as static route ports.



6. IGMP Router Table

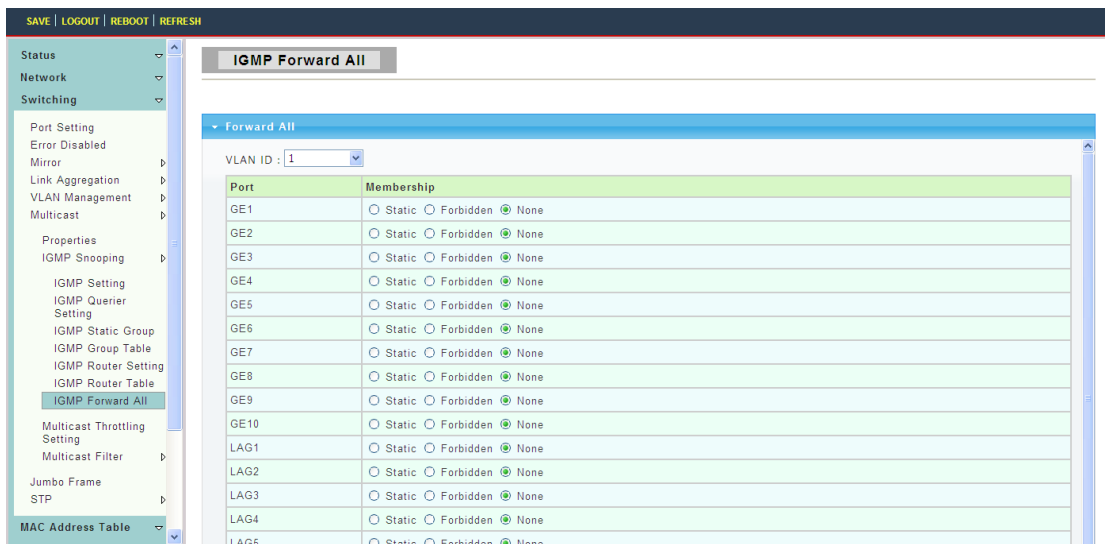
To display IGMP Router Table web page, click **Switching > Multicast > IGMP Snooping > IGMP Router Table**

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



7. IGMP Forward All

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



4.3.6.3 Multicast Throttling Setting

To display Multicast Throttling Setting web page, click **Switching > Multicast > Multicast Throttling Setting**

This page is used to Limit the port can join one of the biggest Multicast instance.

Max groups and action Setting

Ip Type	Port Select	Max Groups	Action
ip4	Select Ports	256 (0-256)	<input checked="" type="radio"/> Deny <input type="radio"/> Replace

IGMP Port Max Groups Information

Port	Max Groups	Action
GE1	256	Deny
GE2	256	Deny
GE3	256	Deny
GE4	256	Deny
GE5	256	Deny
GE6	256	Deny
GE7	256	Deny
GE8	256	Deny
GE9	256	Deny
GE10	256	Deny
LAG1	256	Deny
LAG2	256	Deny

4.3.6.4 Multicast Filter

This page allow user to Create filter instance.

1.Multicast Profile Setting

To display Multicast Profile Setting web page, click **Switching > Multicast > Multicast Filter > Multicast Profile Setting**

Multicast Profile Setting

Add Profile

Ip Type	ip4
Profile Index	1 (1-128)
Group from	
Group to	
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny

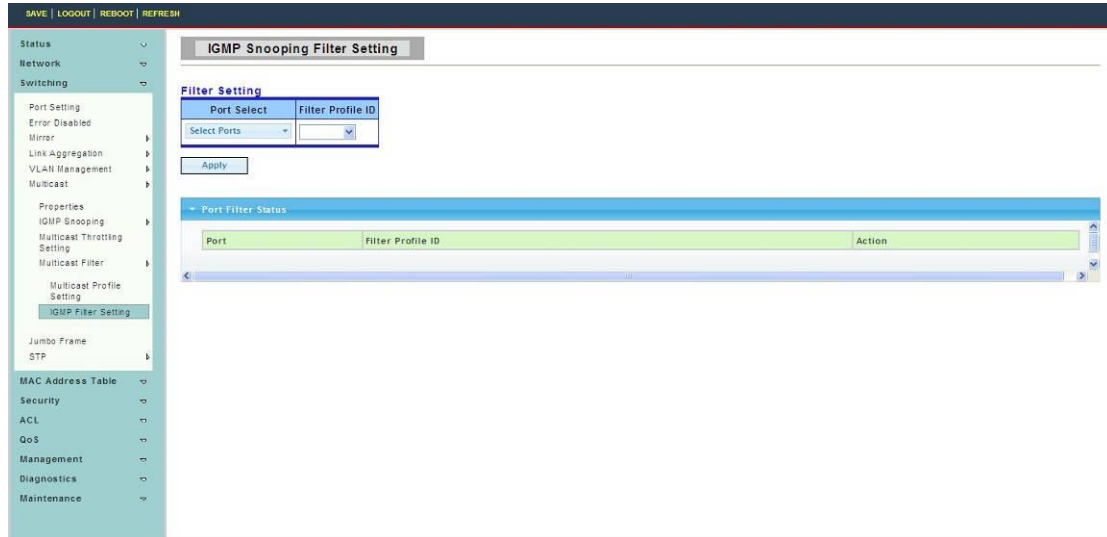
IGMP Profile Status

Index	Ip type	Group from	Group to	Action	Modify

2.Multicast Profile Setting

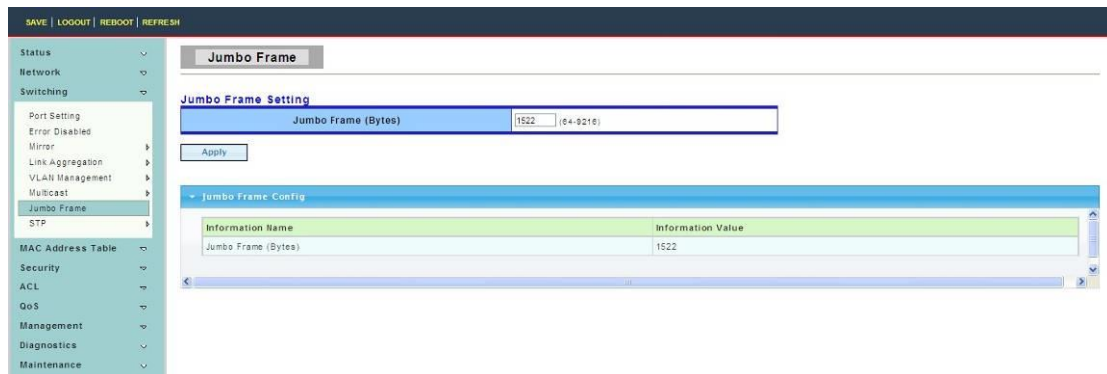
To display IGMP Filter Setting web page, click **Switching > Multicast > Multicast Filter > IGMP Filter Setting**

This page is used to Filter on the port to bind to that instance.



4.3.7 Jumbo Frame

To display Jumbo Frame web page, click **Switching > Jumbo Frame**



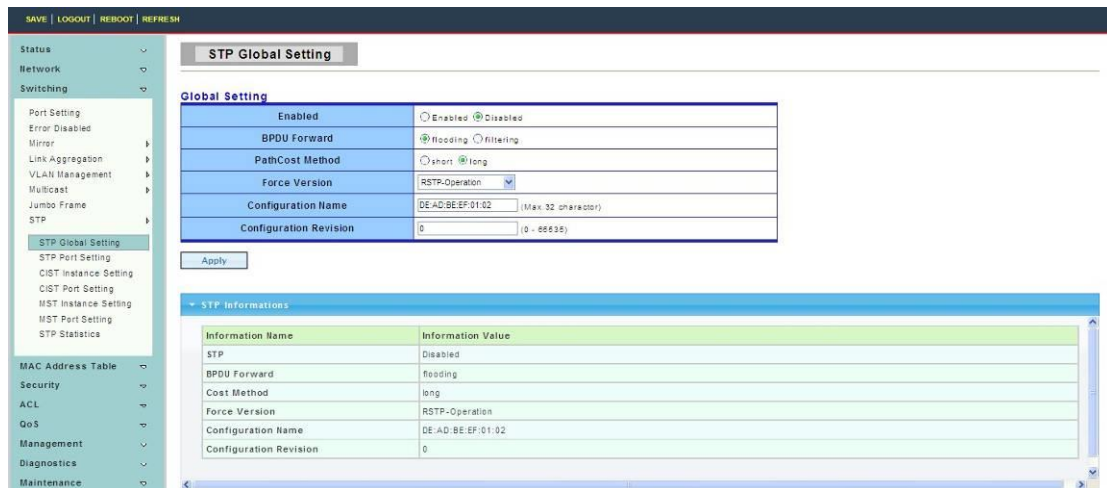
Jumbo Frame: Jumbo frame size. The valid range is 0 bytes – 9216 bytes.

4.3.8 STP

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

4.3.8.1 STP Global Setting

To display STP Global Setting web page, click **Switching > STP > 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

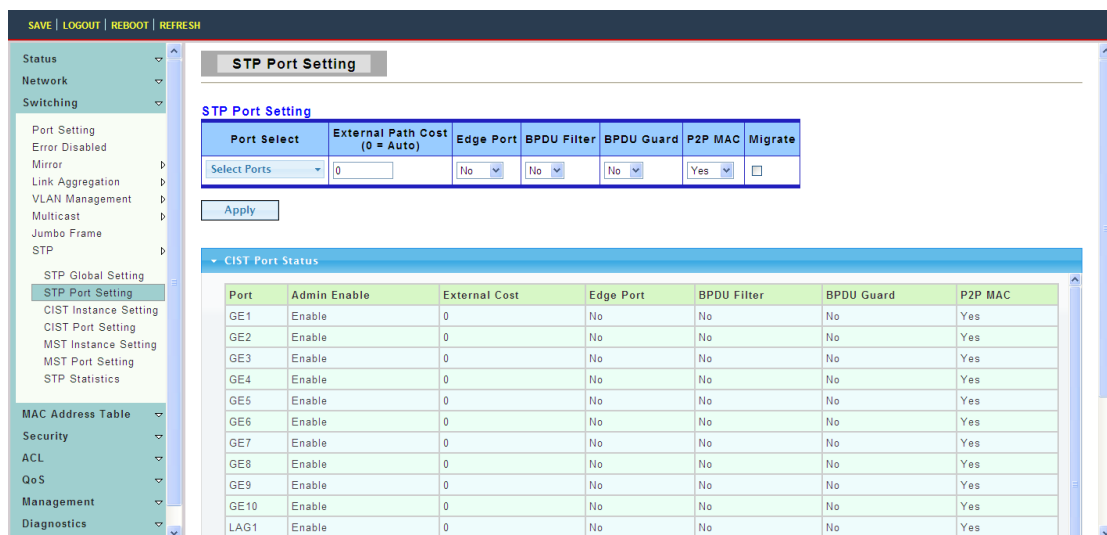
Force Version: Select the operating mode of STP.

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

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

4.3.8.2 STP Port Setting

To display STP Port Setting web page, click **Switching > STP > 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, to the Root Path Cost for the Bridge. (0 means `Auto`).

Edge Port: Set the edge port configuration.

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

BPDU Filter: Set the BPDU Filter configuration.

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

To avoid transmitting BPDU from the specified ports.

BPDU Guard : Set the BPDU Guard configuration.

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

To drop directly the received BPDU from the specified ports.

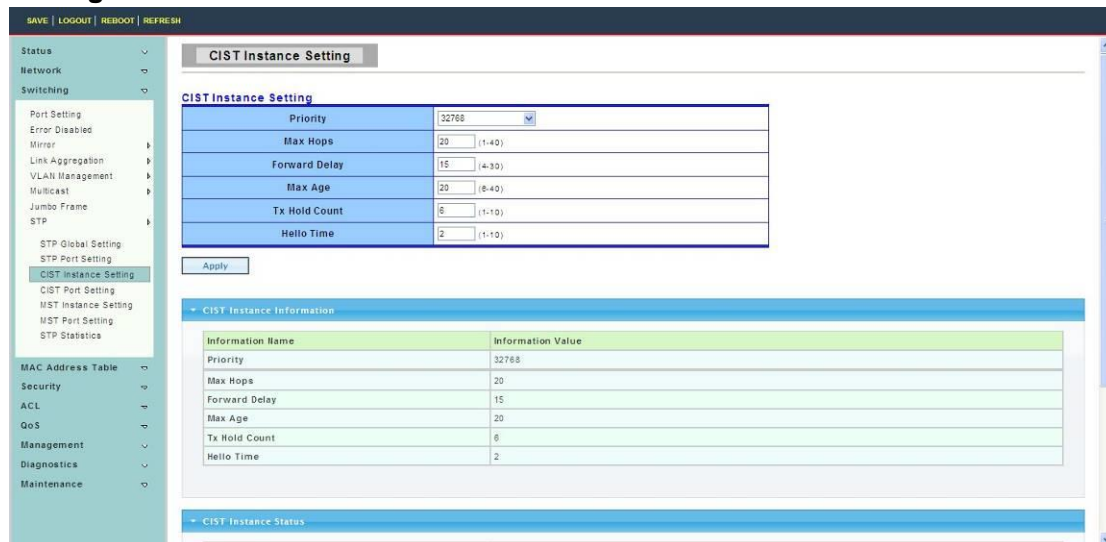
P2P MAC: Set the Point-to-Point port configuration.

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

Migrate: Force 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).

4.3.8.3 CIST Instance Setting

To display CIST Instance Setting web page, click **Switching > STP > CIST Instance Setting**



The screenshot shows the 'CIST Instance Setting' web page. On the left is a navigation menu with categories like Status, Network, Switching, MAC Address Table, Security, ACL, QoS, Management, Diagnostics, and Maintenance. The main content area is titled 'CIST Instance Setting' and contains a table with the following settings:

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 this table is an 'Apply' button. Further down is a section titled 'CIST Instance Information' which contains a table with the following data:

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

At the bottom, there is a section for 'CIST Instance Status' which is currently empty.

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.

4.3.8.4 CIST Port Setting

To display CIST Port Setting web page, click **Switching > STP > CIST Port Setting**

CIST Port Setting

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

Apply

CIST Port Status

Port	Identifier (Priority / Port ID)	External Path Cost Conf/Oper	Internal Path Cost Conf/Oper	Designated Root Bridge	External Root Cost	Regional Root Bridge	Internal Root Cost	Designated Bridge	Internal Path Cost	Edge Port Conf/Oper	P2P MAC Conf/Oper	Port Role	Port State
GE1	128 / 1	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabled	Disabled
GE2	128 / 2	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabled	Disabled
GE3	128 / 3	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabled	Disabled
GE4	128 / 4	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / Yes	Disabled	Forwarding
GE5	128 / 5	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabled	Disabled
GE6	128 / 6	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabled	Disabled
GE7	128 / 7	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabled	Disabled
GE8	128 / 8	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabled	Disabled

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`)

4.3.8.5 MST Instance Setting

To display MST Instance Setting web page, click **Switching > STP > MST Instance Setting**

MST Instance Setting

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

Apply

MST Instance Setting Information

MSTI	Status	VLAN List	VLAN Count	Priority
1				

MST Instance Status

Information Name	Information Value
MSTI ID	1
Regional Root Bridge	--/--
Internal Root Cost	--/--
Designated Bridge	--/--
Root Port	--/--
Max Age	--/--
Forward Delay	--/--
Remaining Hops	--/--
Last Topology Change	--/--

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.

4.3.8.6 MST Port Setting

To display MST Port Setting web page, click **Switching > STP > MST Port Setting**

MST Port Setting

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

Apply

MST Port Status

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/--	--/--	--	--/--	--	--	--
1	GE10	128/10	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`)

4.3.8.7 STP Statistics

To display STP Statistics web page, click **Switching > STP > STP Statistics**

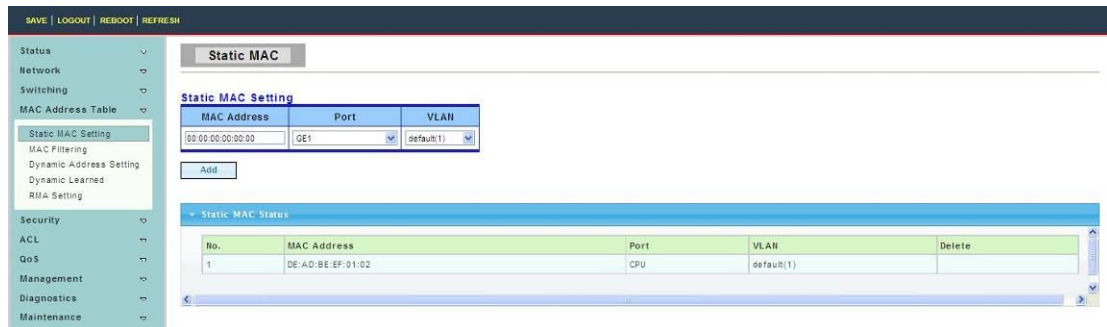
STP Statistics

Port	Configuration BDPUs Received	TCN BDPUs Received	MSTP BDPUs Received	Configuration BDPUs Transmitted	TCN BDPUs Transmitted	MSTP BDPUs Transmitted
GE1	0	0	0	0	0	0
GE2	0	0	0	0	0	0
GE3	0	0	0	0	0	0
GE4	0	0	0	0	0	0
GE5	0	0	0	0	0	0
GE6	0	0	0	0	0	0
GE7	0	0	0	0	0	0
GE8	0	0	0	0	0	0
GE9	0	0	0	0	0	0
GE10	0	0	0	0	0	0
LAG1	0	0	0	0	0	0
LAG2	0	0	0	0	0	0
LAG3	0	0	0	0	0	0
LAG4	0	0	0	0	0	0
LAG5	0	0	0	0	0	0
LAG6	0	0	0	0	0	0
LAG7	0	0	0	0	0	0

4.4 Mac Address Table

4.4.1 Static Mac Setting

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



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.

4.4.2 MAC Filtering

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



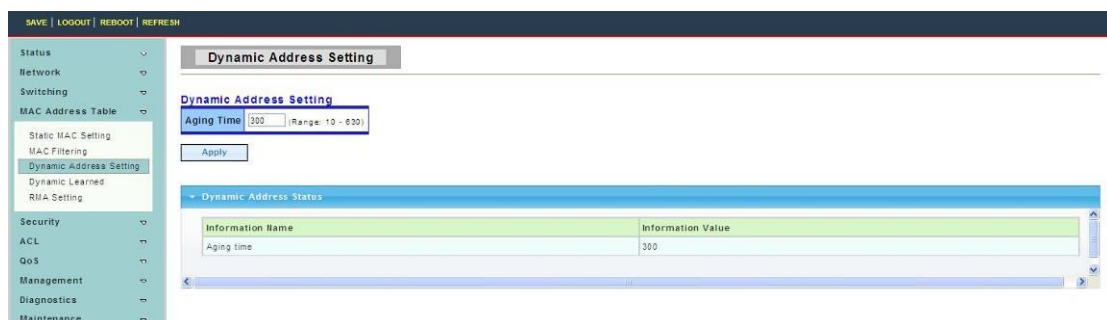
MAC Address: The MAC address to which packets will be filtered. This must be a unicast MAC address.

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

4.4.3 Dynamic Address Setting

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

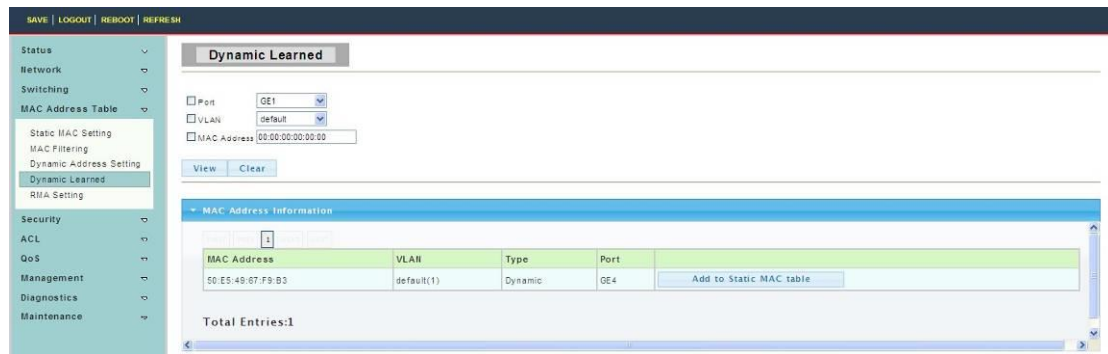
This page is used to set the MAC address of the aging time to study



Aging Time: Set the time needed for aging

4.4.4 Dynamic Learned

To display Dynamic Learned web page, click **Mac Address Table > Dynamic Learned**



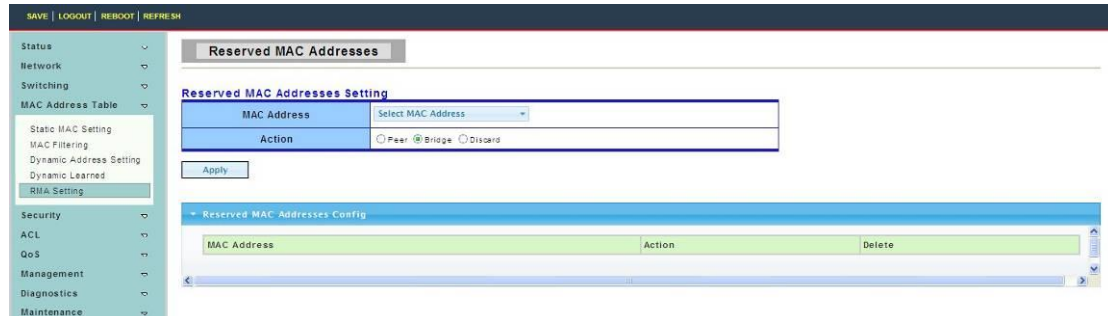
Port: Select the port number to show or clear dynamic MAC entries. If not select any port, VLAN and MAC address, the whole dynamic MAC table will be displayed or cleared.

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

4.4.5 RMA MAC Address

To display RMA MAC Address web page, click **Mac Address Table > RMA MAC Address**



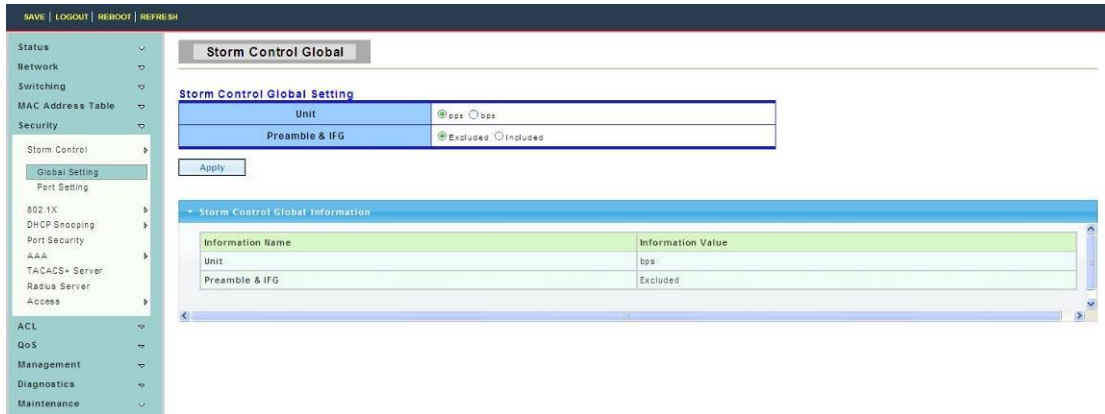
4.5 Security

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

4.5.1 Storm Control

4.3.5.1 Global Setting

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



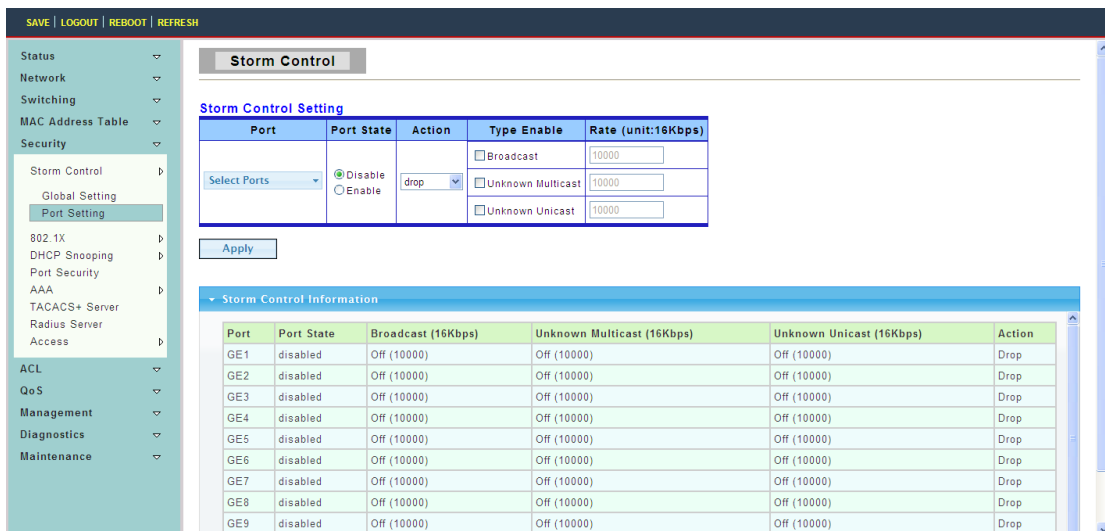
Unit: Choose to storm control unit is the pps or bps

Preamble & IFG: Select the rate calculates w/o preamble & IFG (20 bytes).

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

4.3.5.2 Port Setting

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



Port: Select the setting ports.

Type Enable: Select the type of storm control.

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

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

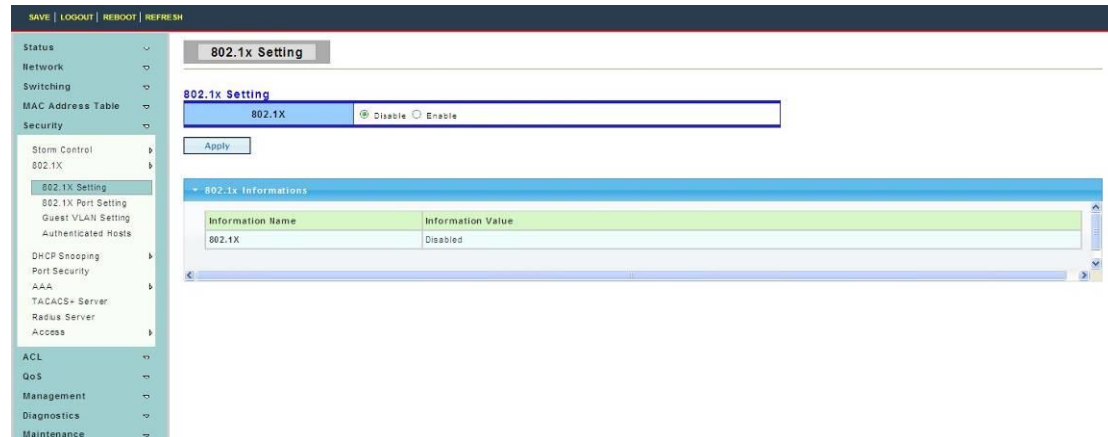
4.5.2 802.1X

802.1x is based on the Client/Server access control and authentication protocol. It can restrict the unauthorized users or devices to connect the access port visit 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 exam, it

only accept the EAPoL data connect with the switch; but after it passes it, the ordinary data all can be transmitted through Ethernet ports.

4.5.2.1 802.1X Setting

To display 802.1X Setting web page, click **Security > 802.1X > 802.1X Setting**

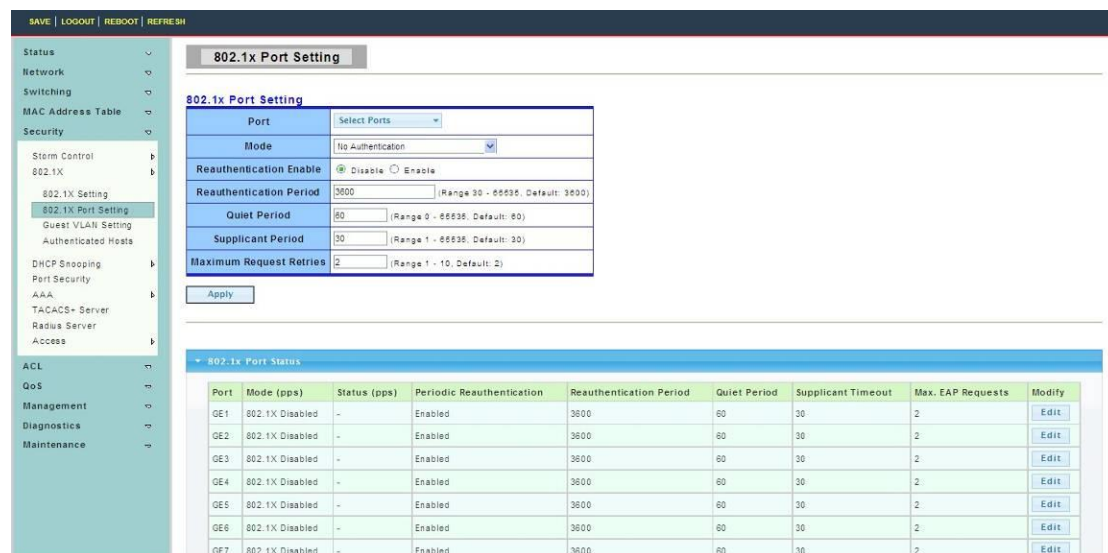


802.1X: Set the enabling status of 802.1X functionality.

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

4.5.2.2 802.1X Port Setting

To display 802.1X Port Setting web page, click **Security > 802.1X > 802.1X Port Setting**



Port: Select the ports to configure their authentication mode.

Mode: The authentication mode.

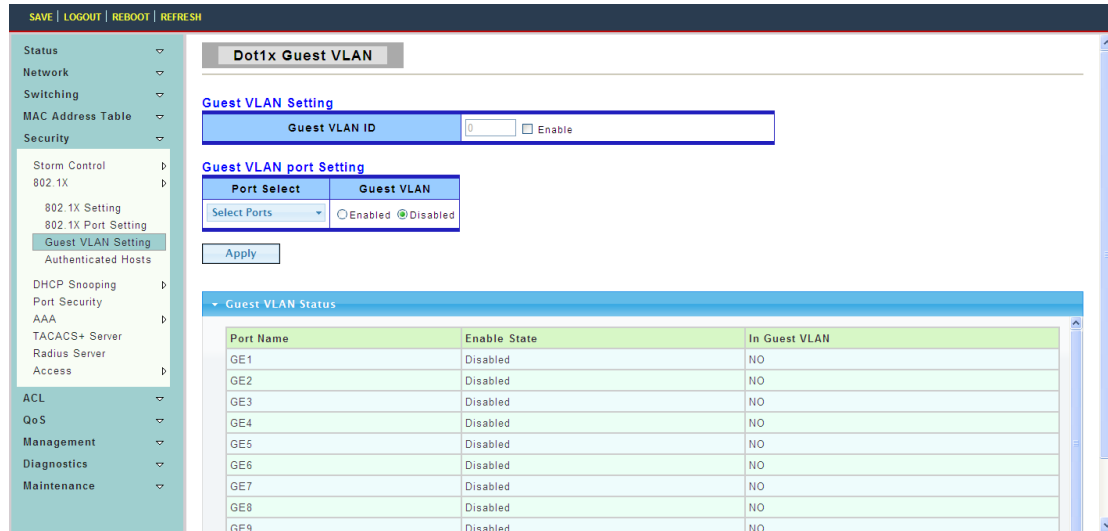
- Force Unauthorized: Force this port to be unconditional unauthorized.
- Force Authorized: Force this port to be unconditional authorized.
- Authentication: 802.1X authentication.
- No Authentication: 802.1X disabled.

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

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

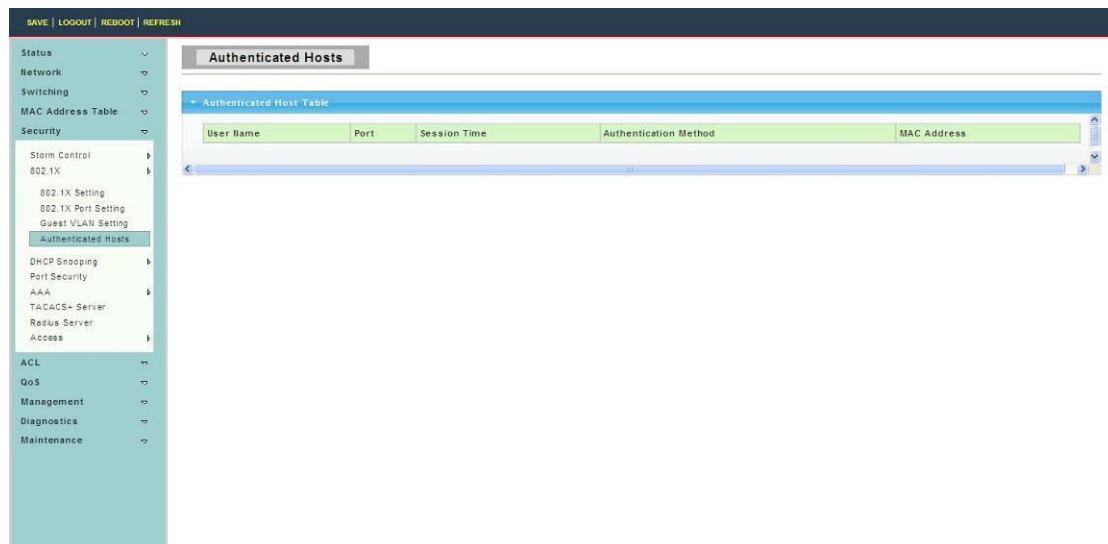
4.5.5.1 Guest VLAN Setting

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



4.3.5.1 Authenticated Hosts

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



4.5.3 DHCP Snooping

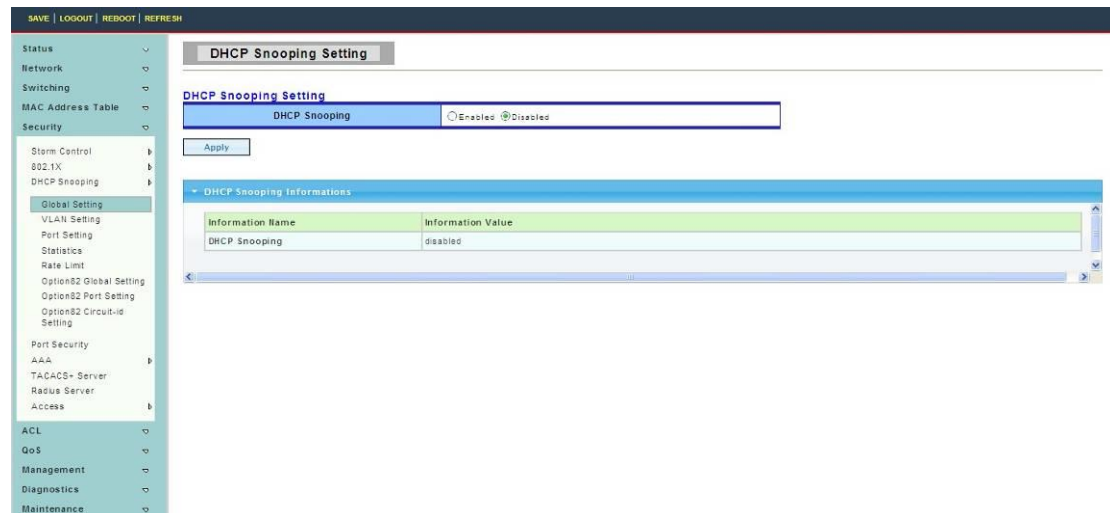
When the switch opens DHCP-Snooping, it will snoop DHCP message and receive DHCP Request and abstract and record the IP address and MAC address from DHCP ACK message. Besides, DHCP-Snooping admits one physical port setting as creditable port or discreditable ports. Creditable ports can receive and forward the DHCP Offer message, on the contrary, the discreditable port will lose the DHCP Offer message. In that way, the

switch can pick out the fake DHCP Server and make sure that the client gets legal IP address from DHCP Server.

4.5.3.1 Global Setting

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

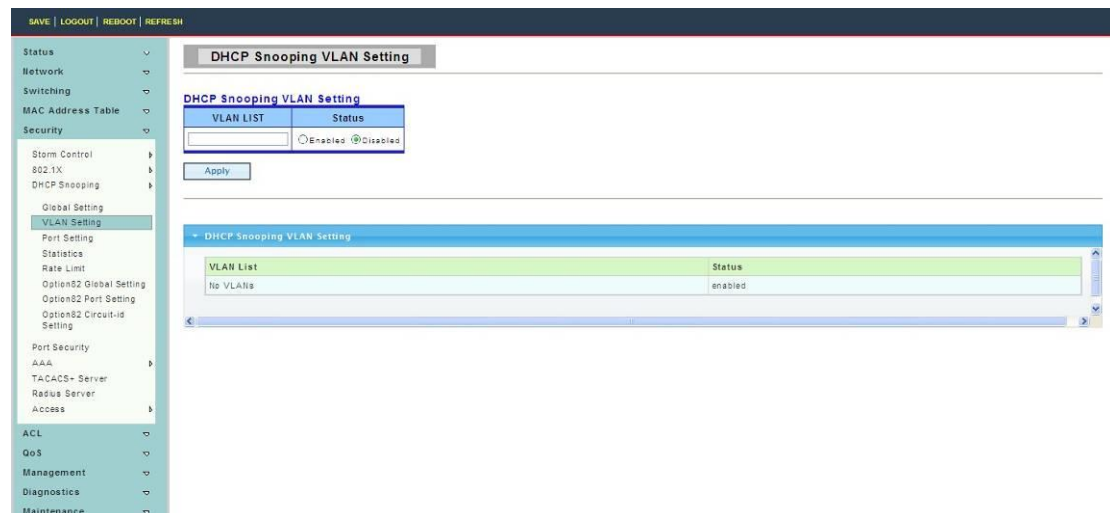
This page is used to open DHCP Snooping function



DHCP Snooping: enable or disable DHCP Snooping function

4.5.3.2 VLAN Setting

To display VLAN Setting web page, click **Security > DHCP Snooping > VLAN Setting**
Specific VLAN starts DHCP Snooping



4.5.3.3 Port Setting

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

This page allow user to make the specific port is configured for DHCP Snooping trust port.

DHCP Snooping Port Setting

Port: Type: Un Trusted Trusted Chaddr Check: Enable Disable

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
LAG1	Un Trusted	disabled

4.5.3.4 Statistics

To display Statistics web page, click **Security > DHCP Snooping > Statistics**

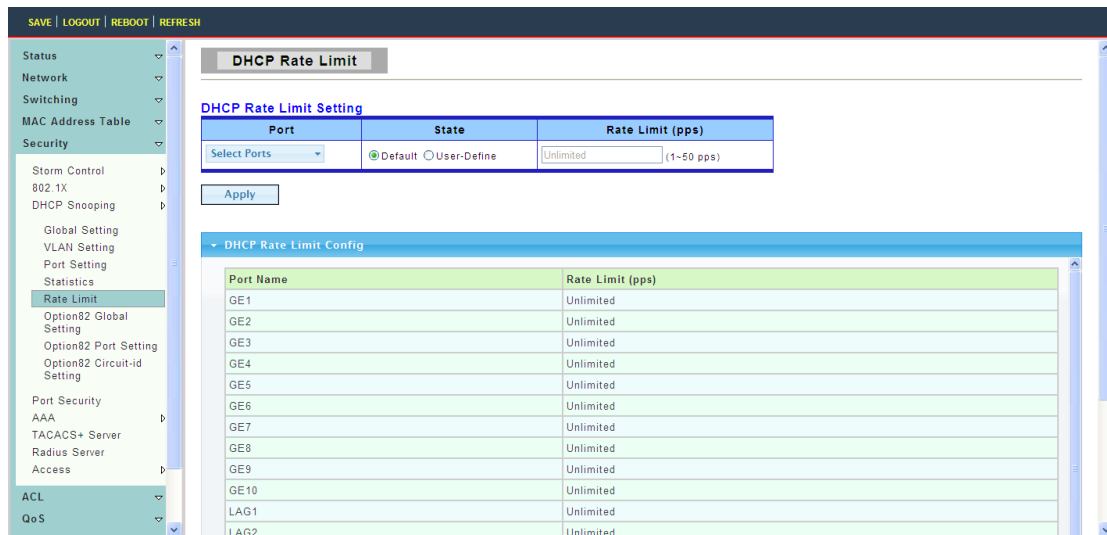
This page statistics of each port of DHCP Snooping state information.

DHCP Snooping Statistics

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
LAG1	0	0	0	0	0
LAG2	0	0	0	0	0
LAG3	0	0	0	0	0
LAG4	0	0	0	0	0
LAG5	0	0	0	0	0
LAG6	0	0	0	0	0

4.5.3.5 Rate Limit

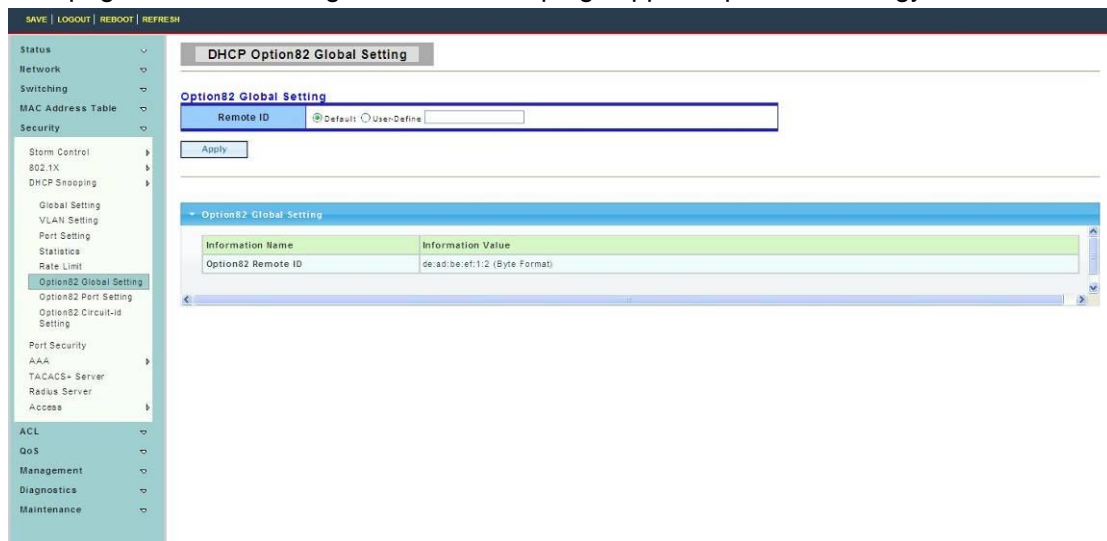
To display Rate Limit web page, click **Security > DHCP Snooping > Rate Limit**



4.5.3.6 Option82 Global Setting

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

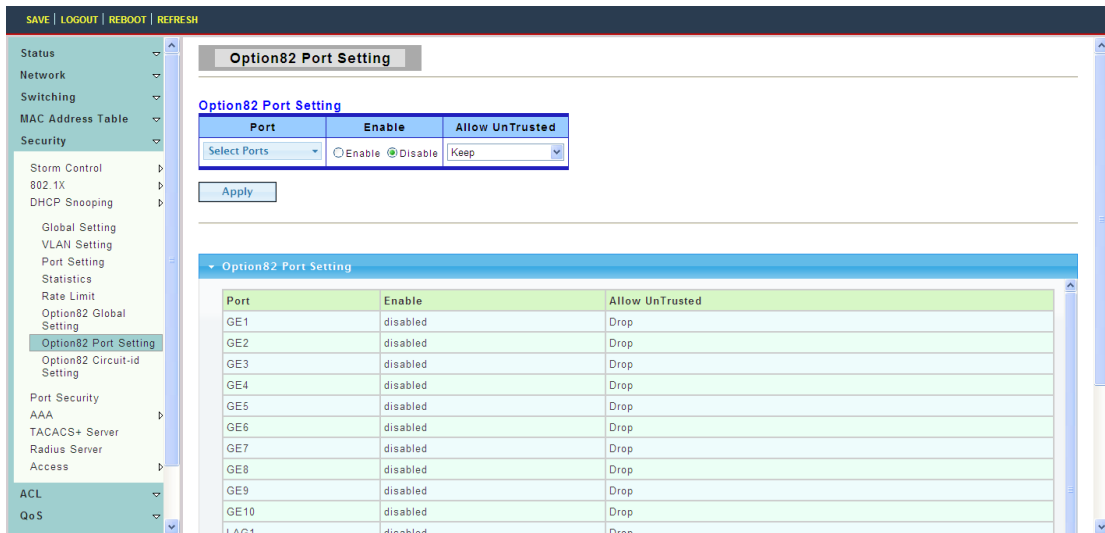
This page is used to configure DHCP Snooping support Option82 strategy.



4.5.3.7 Option82 Port Setting

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

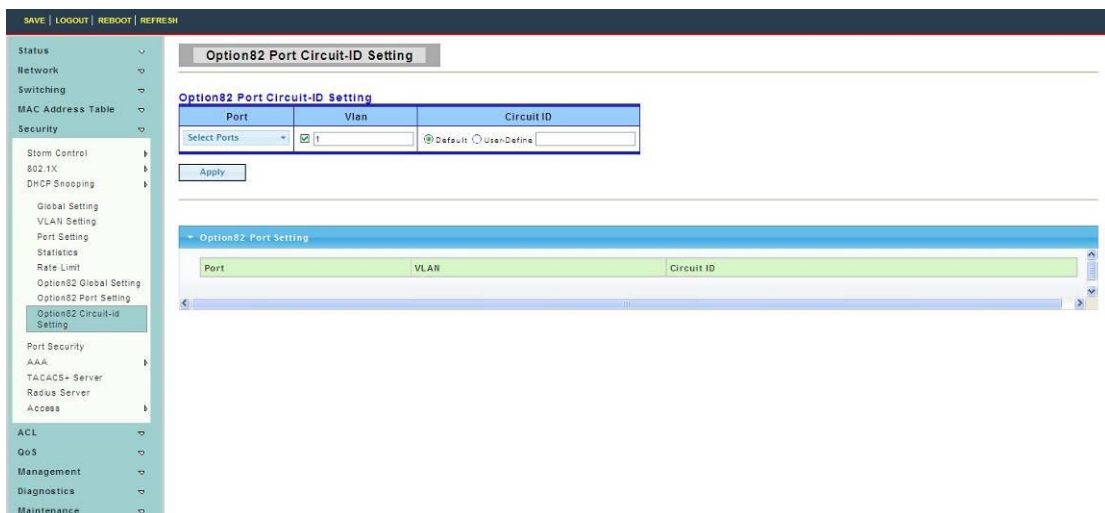
To the specified port configuration of receiving containing Option 82 options request packet port handling strategy.



4.5.3.8 Option82 Circuit-ID Setting

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

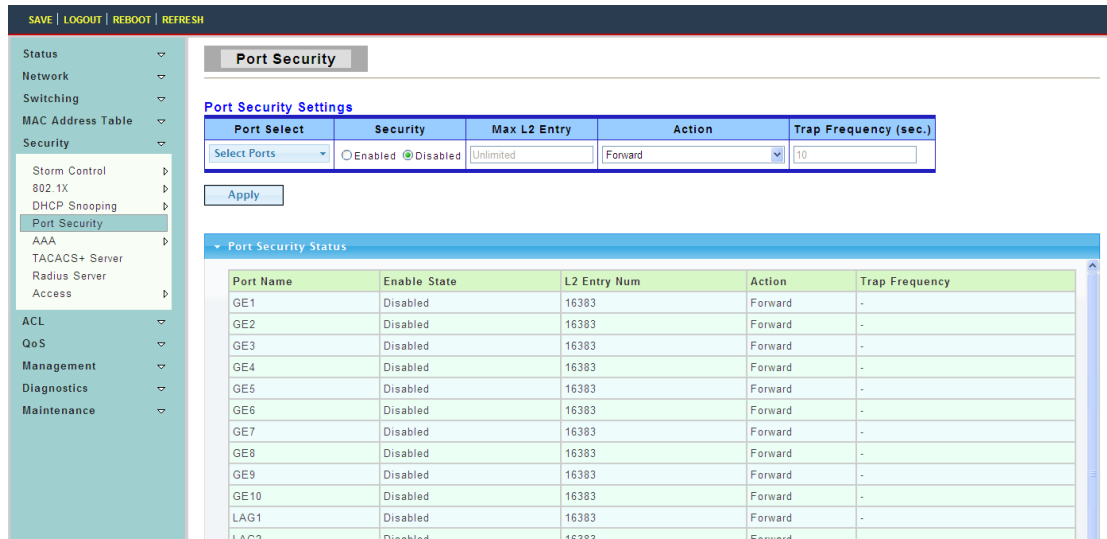
This page allow user to edit circuit ID content in the option82.



4.5.4 Port Security

To display Port Security web page, click **Security> Port Security**

Ports Security, it can set port isolation and specific behavior.



Port Select: Select one or multiple ports to configure.

Security: Port security function. It constraint how many MAC addresses can be learned by a port and drop new one when reach the limitation.

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

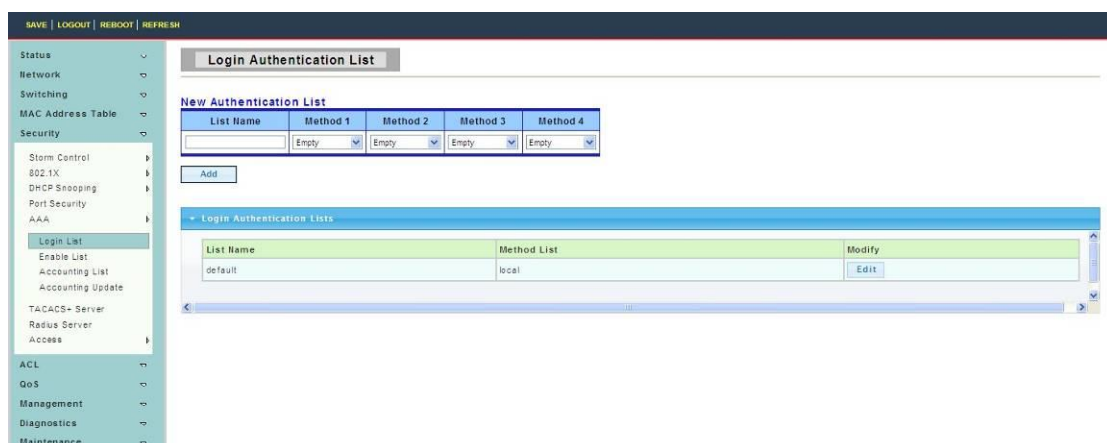
Max L2 Entry: The total number of MAC addresses entry which can be learn by a port.

4.5.5 AAA

4.5.5.1 Login List

To display Login List web page, click **Security > AAA > Login List**

This page allow user to add, edit delete login authentication list settings (The “default” list cannot be deleted.).The line combined to this list will authenticate login user by methods in this list. If the first method is failed, it will try to use the next priority method to authenticate if it exists.



List Name: New login authentication list name. This name should be different from other existing lists.

Method 1: Select first priority of login authentication method.

- Local: Use local accounts database to authenticate.

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

- Enable: Use local enable password to authenticate.

Method 2: Select second priority of login authentication method.

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

- Enable: Use local enable password to authenticate.

Method 3: Select third priority of login authentication method.

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

- Enable: Use local enable password to authenticate.

Method 4: Select fourth priority of login authentication method.

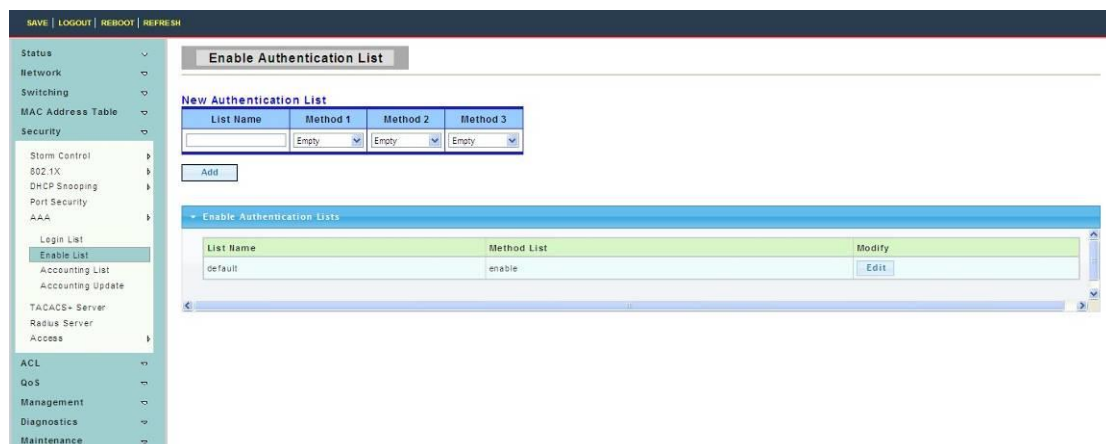
- Local: Use local accounts database to authenticate
- Tacacs+: Use remote TACACS+ server to authenticate.
- Radius: Use remote Radius server to authenticate. Not supported now, it will be supported in the future.

- Enable: Use local enable password to authenticate

4.5.5.2 Enable List

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

This page allows user to add, edit or delete enable authentication list settings (The “default” list cannot be deleted.). The line combined to this list will authenticate user who issues the ‘enable’ command by methods in this list. If the first method is failed, it will try to use the next priority method to authenticate if it exists.



List Name: New enable authentication list name. This name should be different from other existing lists.

Method 1: Select first priority of enable authentication method.

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

Method 2: Select second priority of enable authentication method.

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

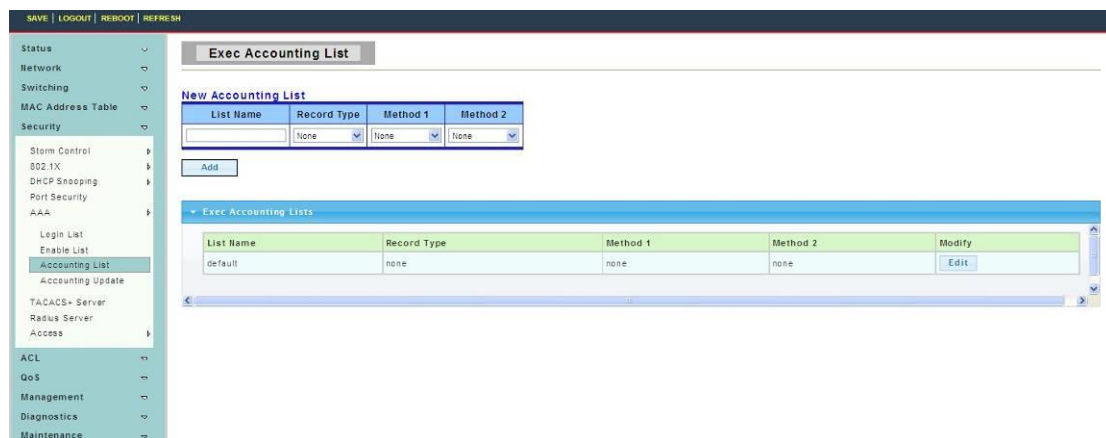
Method 3: Select third priority of enable authentication method.

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

4.5.5.3 Accounting List

To display Accounting List web page, click **Security> AAA > Accounting List**

This page allows user to add, edit or delete accounting list settings (The “default” list cannot be deleted.). The line combined to this list will account user who enters CLI shell by methods in this list. If the first method fails, it will try to use the next priority method to account if it exists.



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

Record Type: Select accounting record type.

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

Method 1: Select first priority of exec accounting method.

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

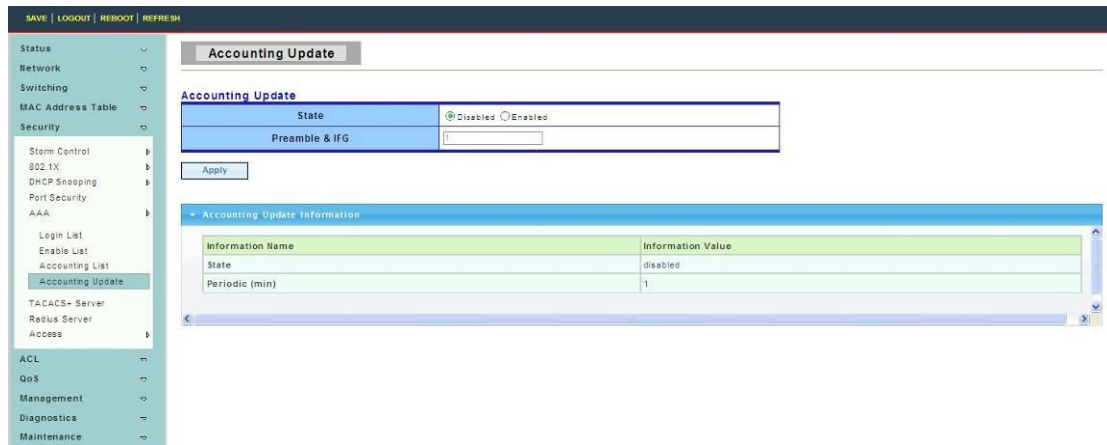
Method 2: Select second priority of exec accounting method.

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

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

4.5.5.4 Accounting Update

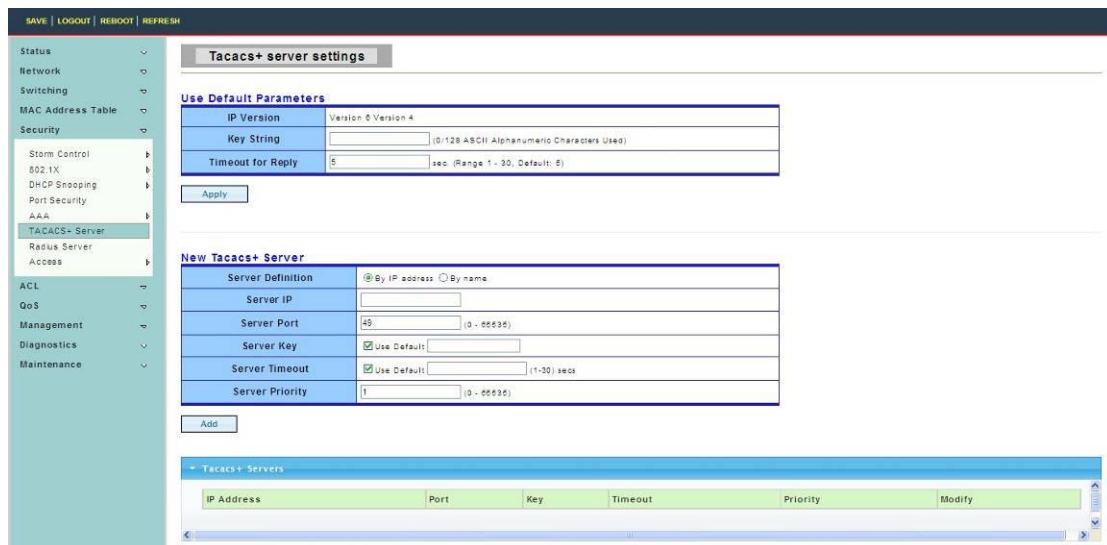
To display Accounting Update web page, click **Security> AAA > Accounting Update**



4.5.6 Tacacs+ Server

To display Tacacs+ server web page, click **Security> AAA > Tacacs+ server**

This page allow user to add, edit or delete TACACS+ server settings.



4.5.7 Radius server

To display Radius server web page, click **Security > AAA > Radius server**

This page is used to set about radius server.

4.5.8 Access

4.5.8.1 Console

To display Console web page, click **Security > Access > Console**

This page allow user to combine all kinds of AAA lists to console line. The user accesses switch from console will be authenticated, authorized and accounted by AAA lists we combined here.

Login Authentication List: Select one of the login authentication lists we configured in “Login List” page.

Enable Authentication List: Select one of the enable authentication lists we configured in “Enable List” page.

EXEC Authorization List: Select one of the EXEC authorization lists we configured in “EXEC List” page.

Commands Authorization List: Select one of the commands authorization lists we configured in “Commands List” page.

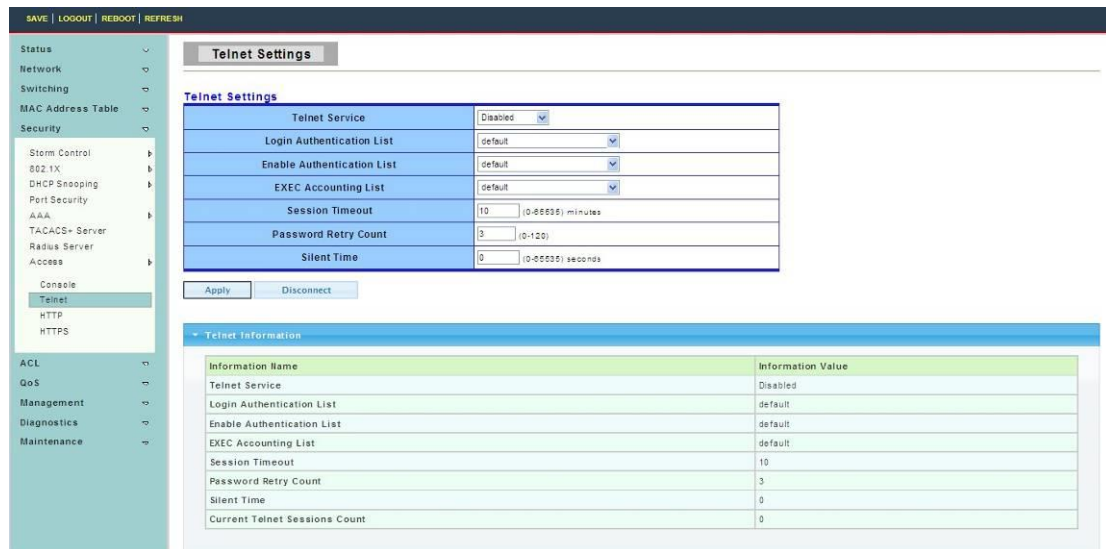
EXEC Accounting List: Select one of the EXEC accounting lists we configured in “Accounting List” page.

Session Timeout: Set session timeout minutes for user access CLI from console line. If user does not response after session timeout minute, CLI will logout automatically. 0 minutes means never timeout.

4.5.8.2 Telnet

To display Telnet web page, click **Security > Access > Telnet**

This page allow user to combine all kinds of AAA lists to telnet line. The user accesses switch from telnet will be authenticated, authorized and accounted by AAA lists we combined here.



Telnet Service: Set remote service disable or enable

Login Authentication List: Select one of the login authentication lists we configured in “Login List” page.

Enable Authentication List: Select one of the enable authentication lists we configured in “Enable List” page.

EXEC Authorization List: Select one of the EXEC authorization lists we configured in “EXEC List” page.

Commands Authorization List: Select one of the commands authorization lists we configured in “Commands List” page.

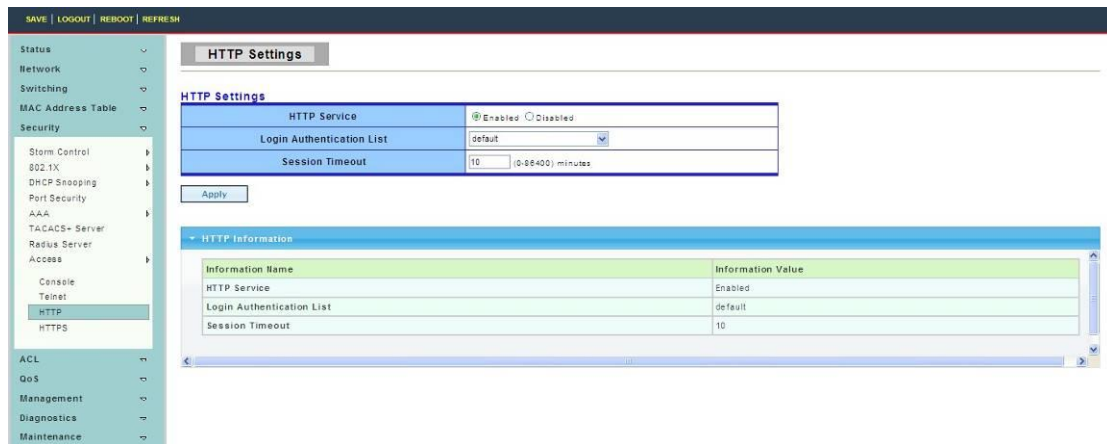
EXEC Accounting List: Select one of the EXEC accounting lists we configured in “Accounting List” page.

Session Timeout: Set session timeout minutes for user access CLI from telnet line. If user does not response after session timeout minute, CLI will logout automatically.

4.5.8.3 HTTP

To display HTTP web page, click **Security > Access > HTTP**

This page allow user to combine all kinds of AAA lists to HTTP line. The user accesses switch WEBUI from HTTP will be authenticated by AAA lists we combined here.



HTTP Server: set HTTP Server disable or enable.

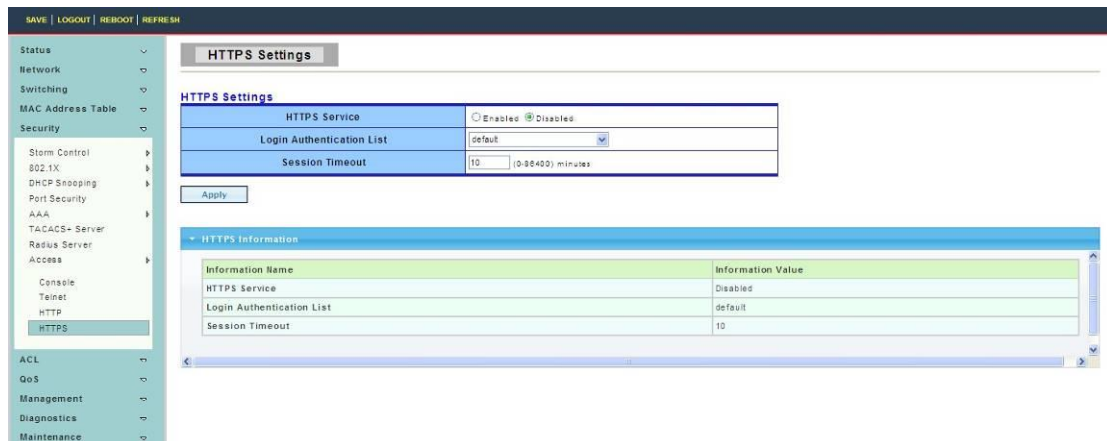
Login Authentication List: Select one of the login authentication lists we configured in “Login List” page.

Session Timeout: Set session timeout minutes for user access WEB from HTTP protocol. If user does not response after session timeout minutes minute, WEBUI will logout automatically. 0 minutes means never timeout.

4.5.8.4 HTTPS

To display HTTPS web page, click **Security > Access > HTTPS**

This page allow user to combine all kinds of AAA lists to HTTPS line. The user accesses switch WEBUI from HTTPS will be authenticated by AAA lists we combined here.



HTTPS Server: Set HTTPS Server 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 HTTPS protocol. If user does not response after session timeout minute, WEBUI will logout automatically. 0 minutes means never timeout.

4.6 ACL

4.6.1 MAC-Based ACL

To display MAC-Based ACL web page, click **ACL > MAC-Based ACL**

This page allow user to set name for MAC-Based ACL.

ACL Name: Enter ACL name in this field.

4.6.2 MAC-Based ACE

To display MAC-Based ACE web page, click **ACL > MAC-Based ACE**

This page allow user to set Based on MAC address expanding ACL list, matching corresponding MAC and setting the ports as drop or forward.

4.6.3 IPv4-Based ACL

To display IPv4-Based ACL web page, click **ACL > IPv4-Based ACL**

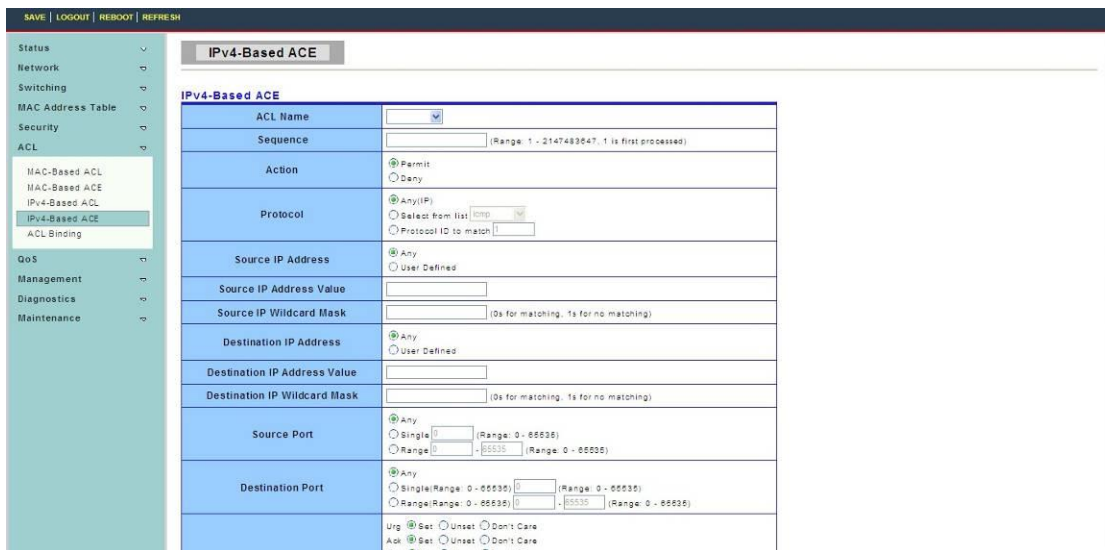
This page allow user to set name for IPv4-Based ACL.



4.6.4 IPv4-Based ACE

To display IPv4-Based ACE web page, click **ACL > IPv4-Based ACE**

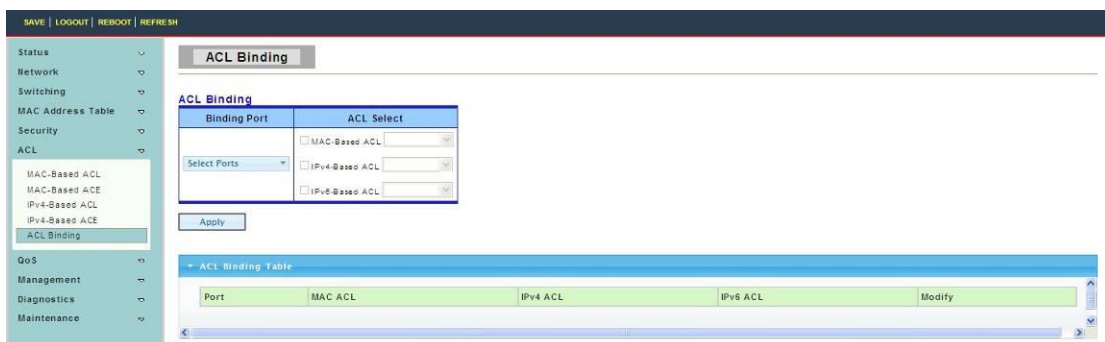
This page allow user to set Based on IPv4 expanding ACL Peer Guardian and matching corresponding IP and setting the port as drop or forward.



4.6.5 ACL Binding

To display ACL Binding web page, click **ACL > ACL Binding**

This page allow user to Bounding with accordingly ACL rules, port bounding ACL rules.



4.7 QoS

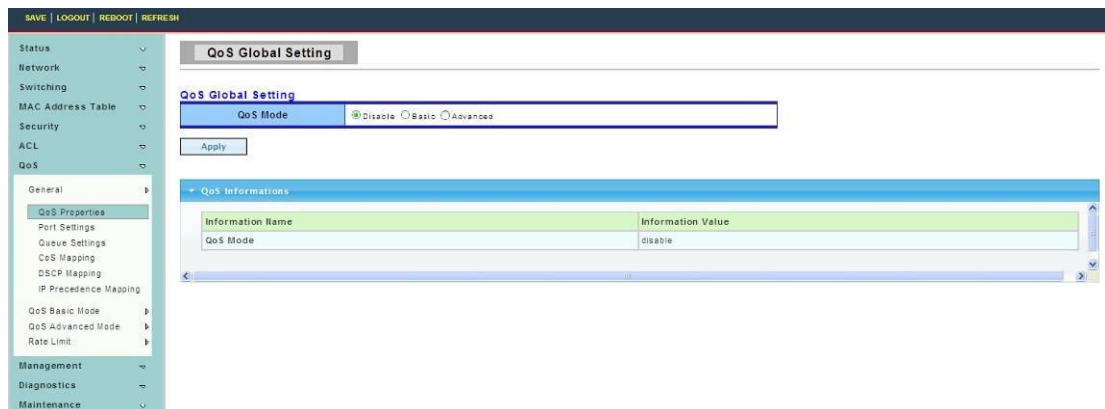
Use the QoS pages to configure settings for the switch QoS interface and how the switch connects to a remote server to get services.

4.7.1 General

4.7.1.1 QoS Properties

To display QoS properties web page, click **QoS > General > QoS properties**

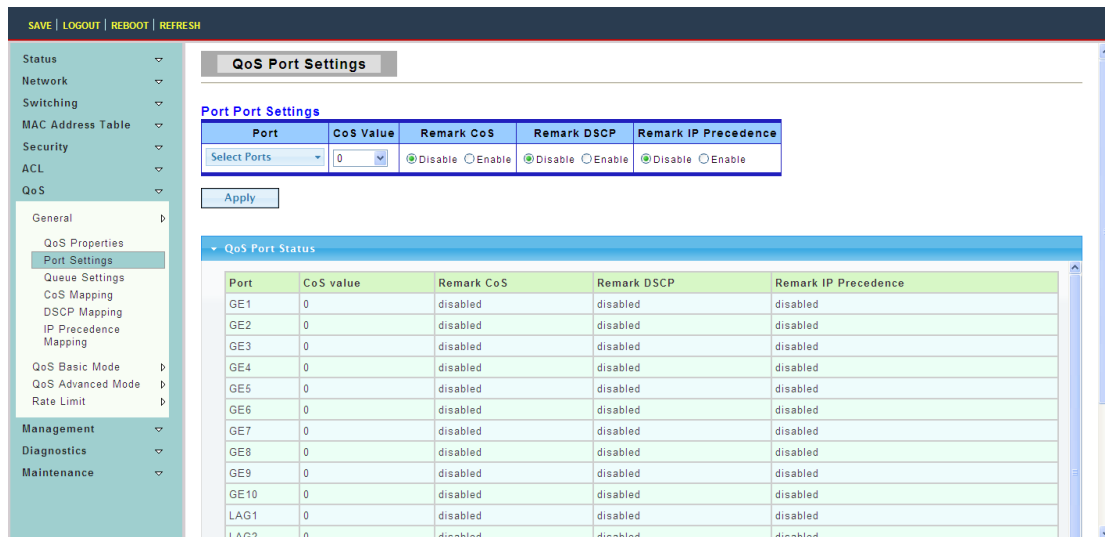
This page allow user to set QoS mode such basic or advanced.



4.7.1.2 Port Settings

To display Port Settings web page, click **QoS > General > Port Settings**

This page is used to give the QoS instance port configuration.

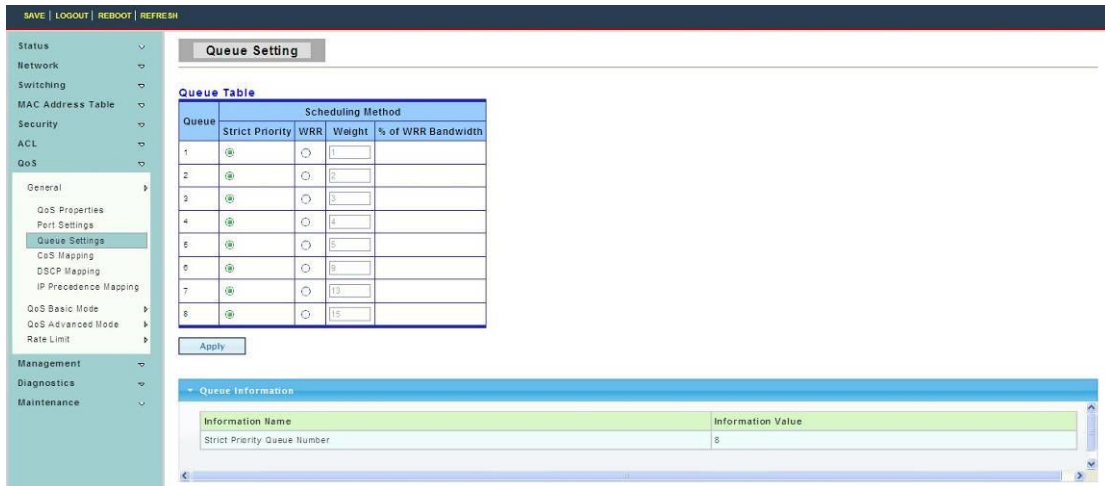


Port	CoS value	Remark CoS	Remark DSCP	Remark IP Precedence
GE1	0	disabled	disabled	disabled
GE2	0	disabled	disabled	disabled
GE3	0	disabled	disabled	disabled
GE4	0	disabled	disabled	disabled
GE5	0	disabled	disabled	disabled
GE6	0	disabled	disabled	disabled
GE7	0	disabled	disabled	disabled
GE8	0	disabled	disabled	disabled
GE9	0	disabled	disabled	disabled
GE10	0	disabled	disabled	disabled
LAG1	0	disabled	disabled	disabled
LAG2	0	disabled	disabled	disabled

4.7.1.3 Queue Settings

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

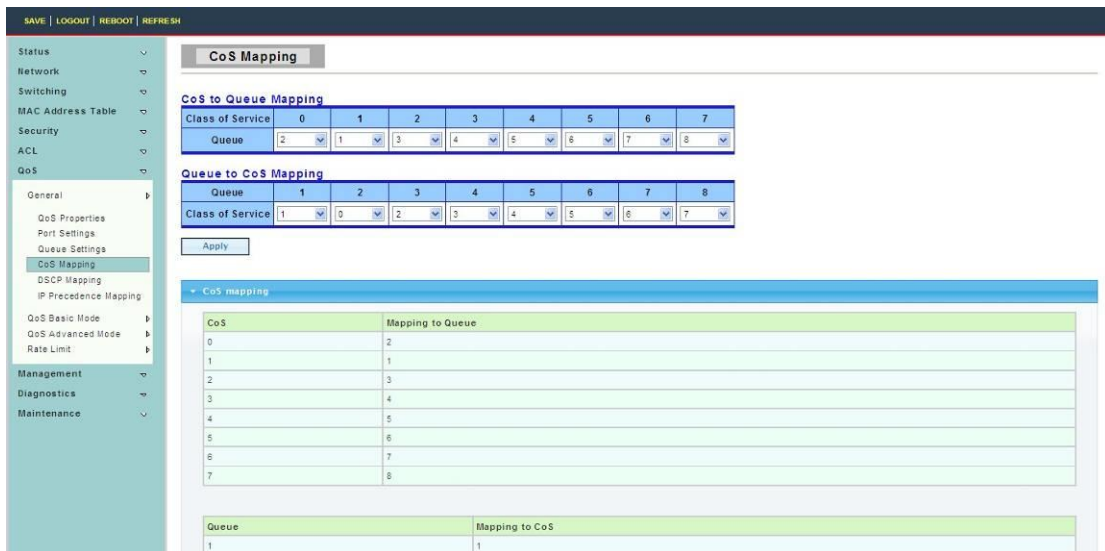
This page allow user to set Set the QoS instance queue scheduling model.



4.7.1.4 COS Mapping

To display COS Mapping web page, click **QoS > General > COS Mapping**

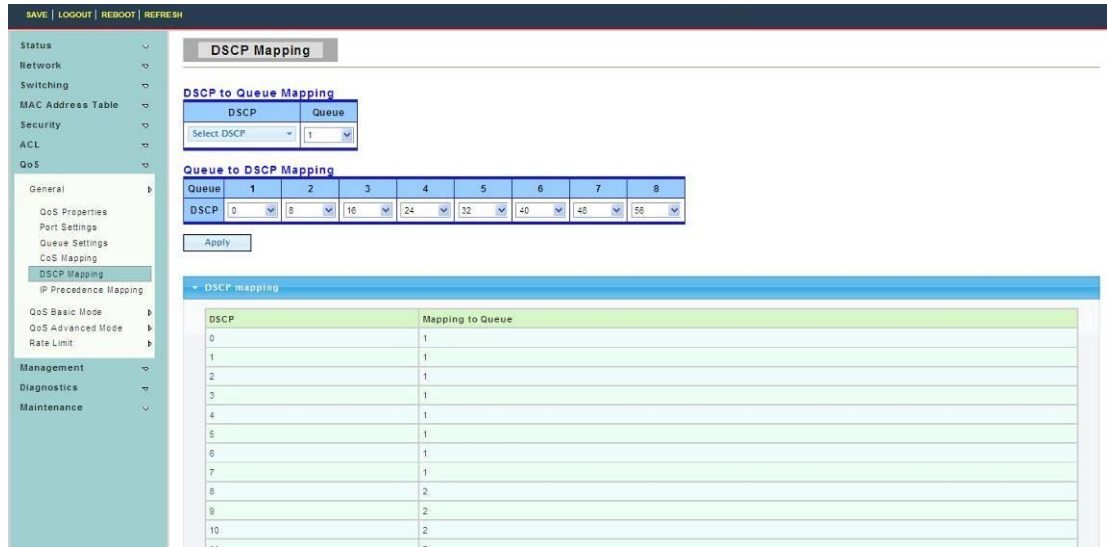
The page allow user to set QoS instance of COS Mapping.



4.7.1.5 DSCP Mapping

To display DSCP Mapping web page, click **QoS > General > DSCP Mapping**

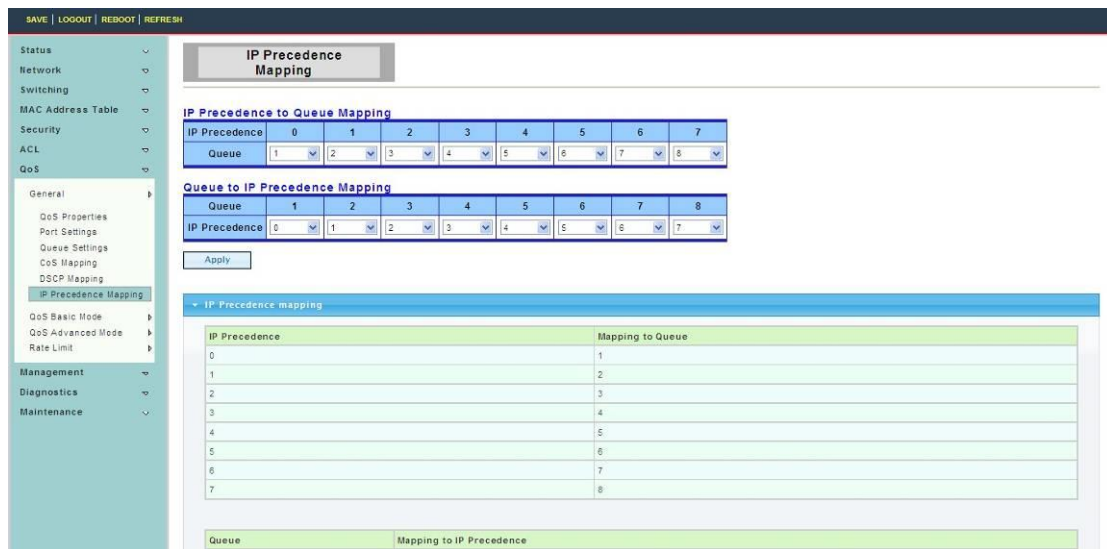
The page allow user to set QoS instance of DSCP Mapping.



4.7.1.5 IP Precedence Mapping

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

The page allow user to set QoS instance of IP Precedence Mapping.

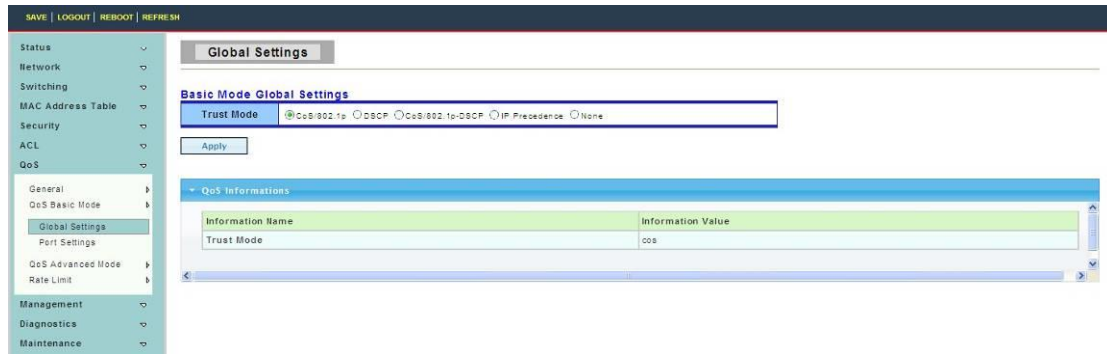


4.7.2 QoS Basic Mode

4.7.2.1 Global Settings

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

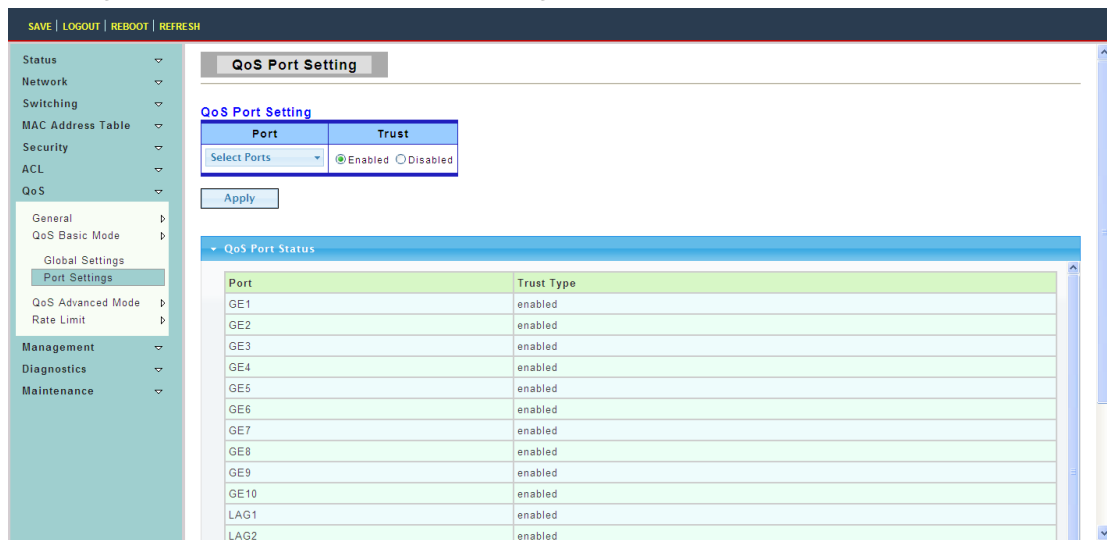
This page allow user to set QoS for trust mode on basic mode global settings.



4.7.2.2 Port Settings

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

This page allow user to set QoS port setting enabled or disabled.

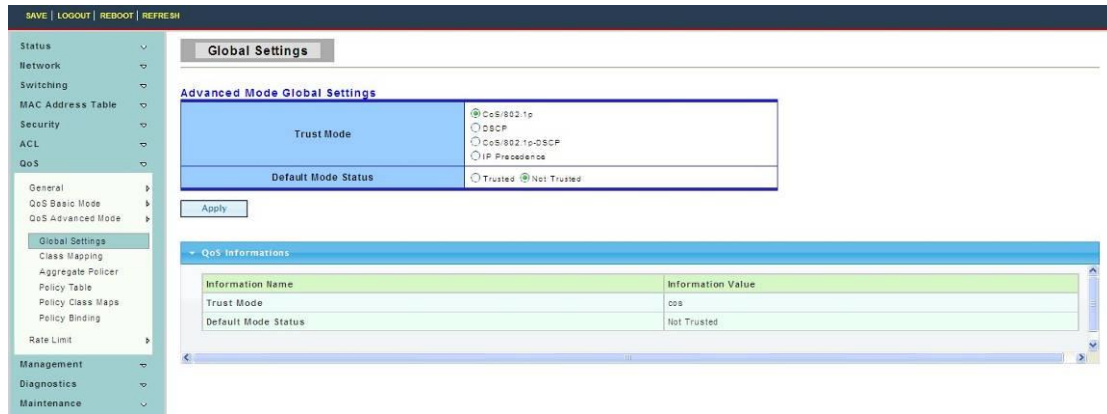


4.7.3 QoS Advanced Mode

4.7.3.1 Global Settings

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

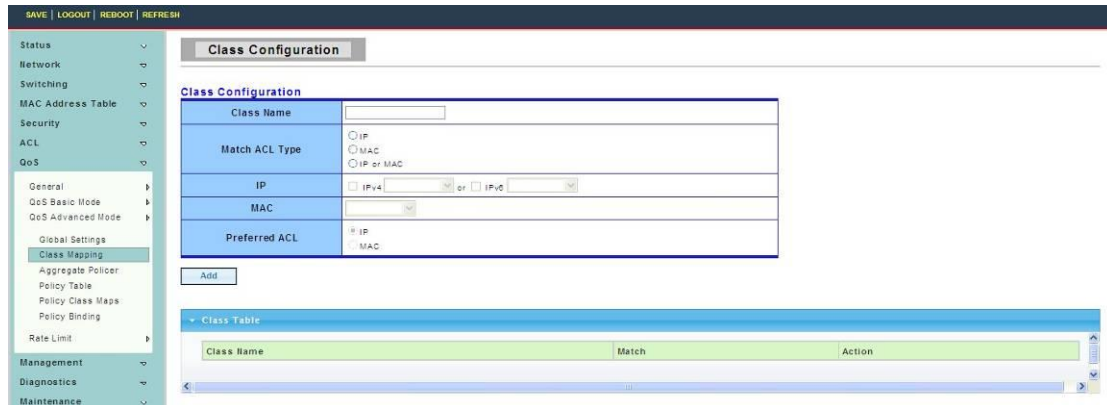
This page allow user to set the default QoS mode state under advanced mode global settings trust mode.



4.7.3.2 Class Mapping

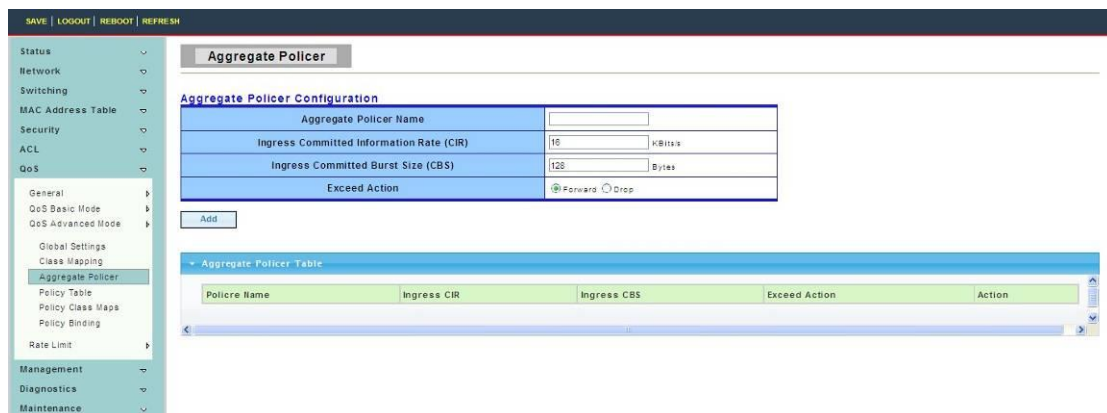
To display Class Mapping web page, click **QoS > QoS Advanced Mode > Class Mapping**

This page allow user to create a QoS class which is used to link the ACL.



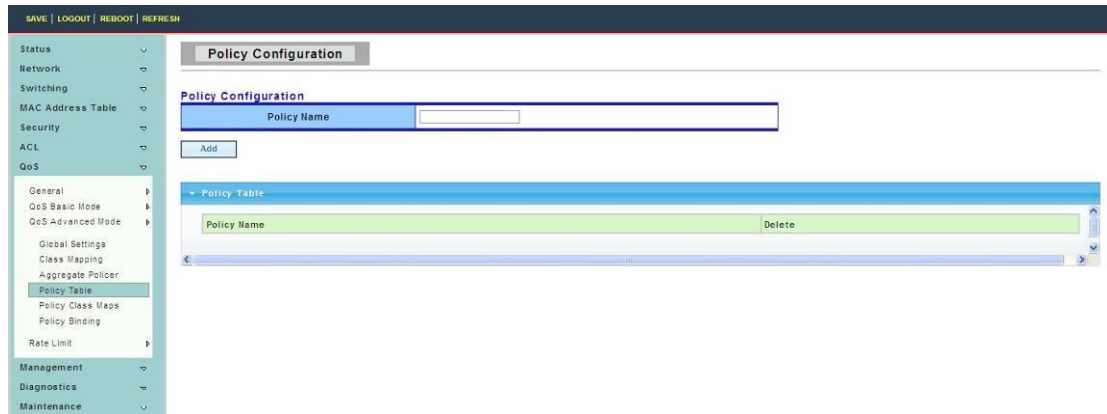
4.7.3.3 Aggregate Policier

To display Aggregate Policier web page, click **QoS > QoS Advanced Mode > Aggregate Policier**



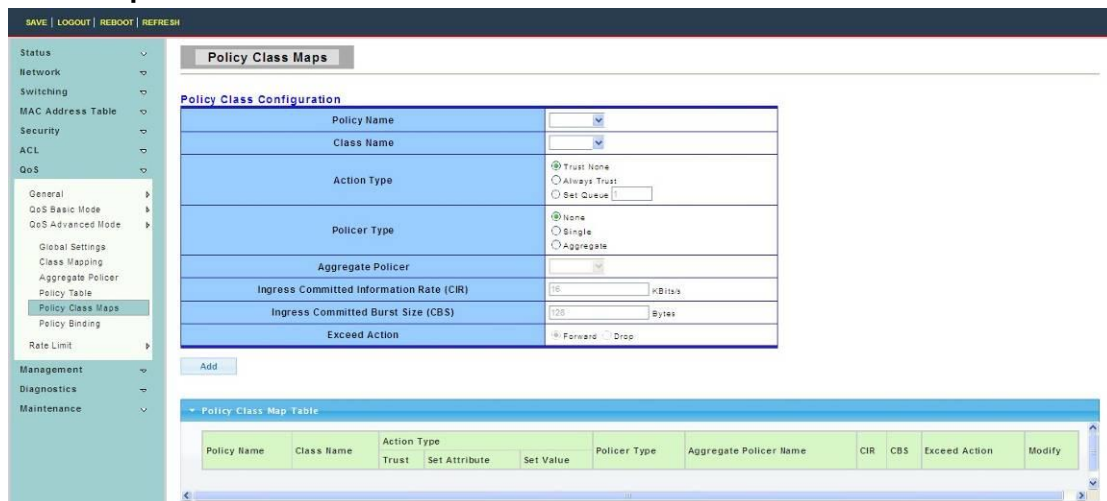
4.7.3.4 Policy Table

To display Policy Table web page, click **QoS > QoS Advanced Mode > Policy Table**



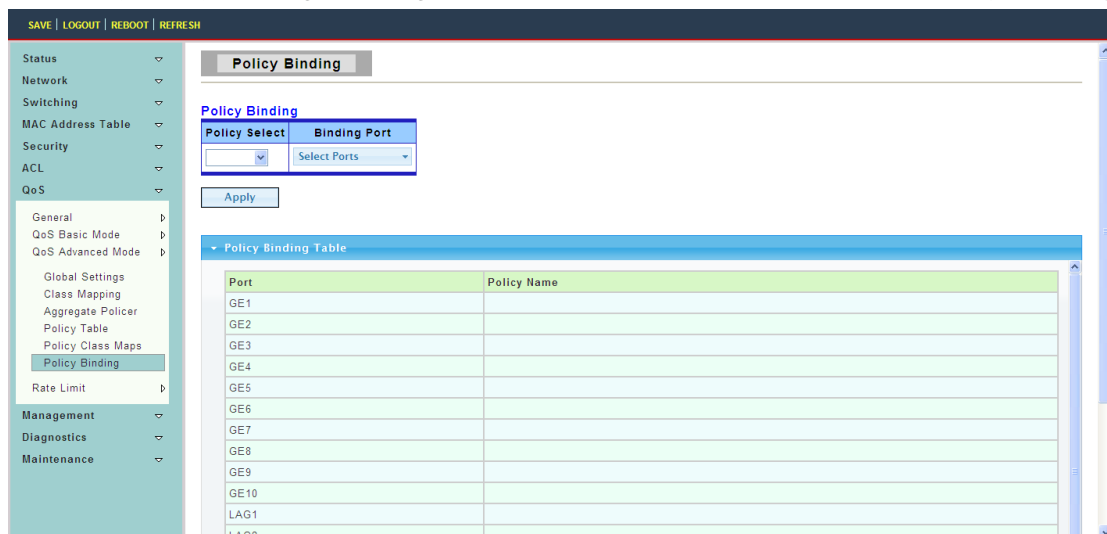
4.7.3.5 Policy Class Maps

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



4.7.3.6 Policy Binding

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



4.7.4 Rate Limit

4.7.4.1 Ingress Port Settings

To display Ingress Port Settings web page, click **QoS > Rate Limit > Ingress Port Settings**

This page allow user to set ingress port monitor.

4.7.4.2 Ingress VLAN Settings

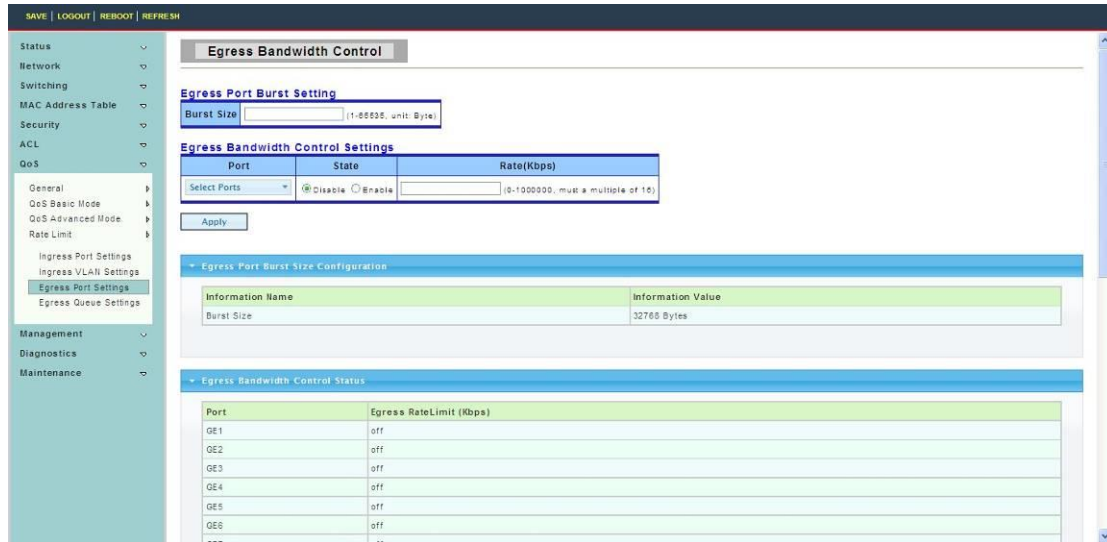
To display Ingress VLAN Settings web page, click **QoS > Rate Limit > Ingress VLAN Settings**

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

4.7.4.3 Egress Port Settings

To display Egress Port Settings web page, click **QoS > Rate Limit > Egress Port Settings**

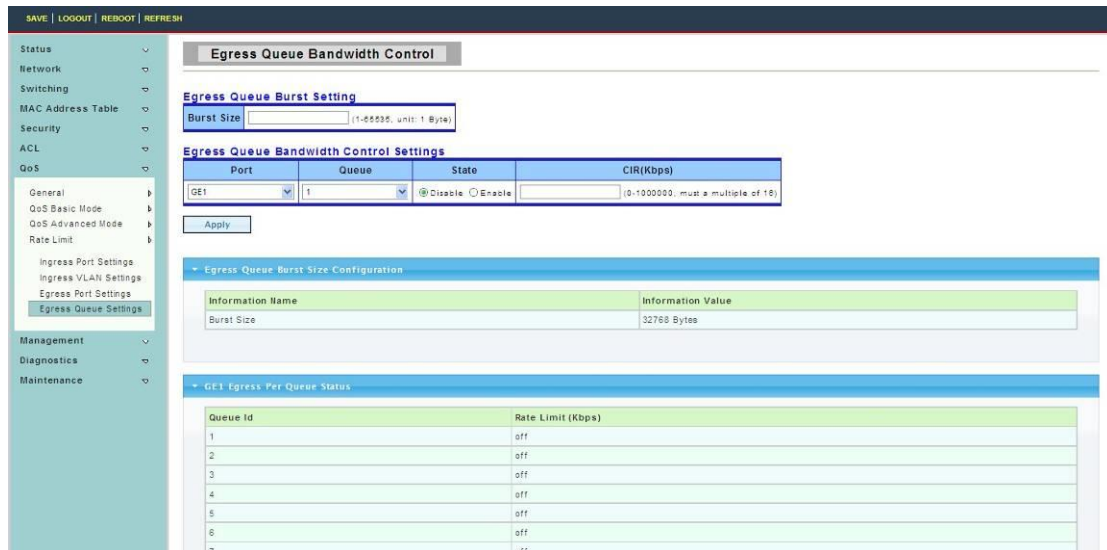
This page is used to set the egress port monitor.



4.7.4.4 Egress Queue Settings

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

The page is used to set the egress lined up bandwidth monitor.



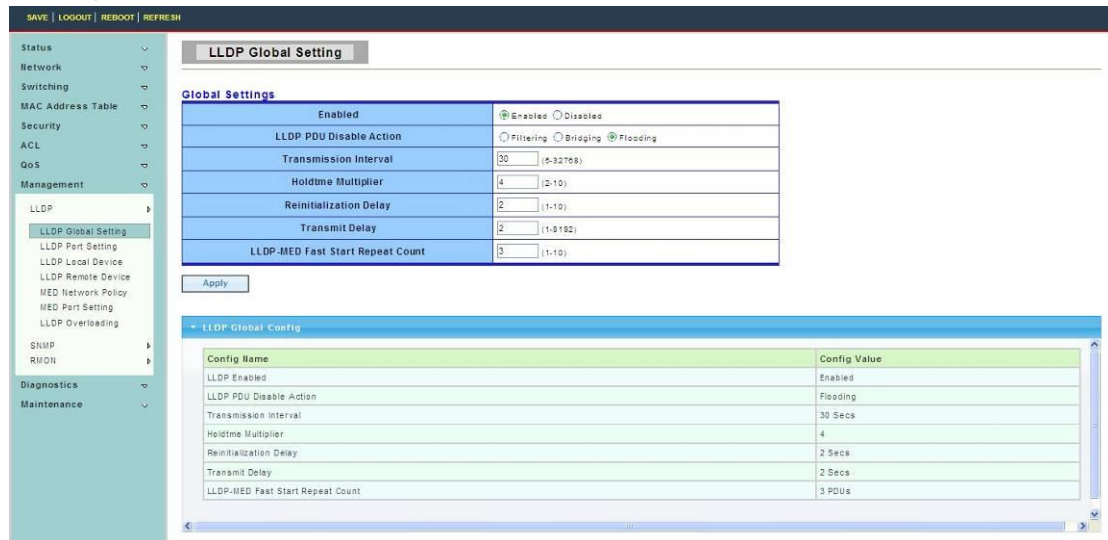
4.8 Management

4.8.1 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.

4.8.1.1 LLDP Global Settings

To display LLDP Global Settings web page, click **Management > LLDP > LLDP Global Settings**



Enabled: Enable/ Disable LLDP protocol on this switch.

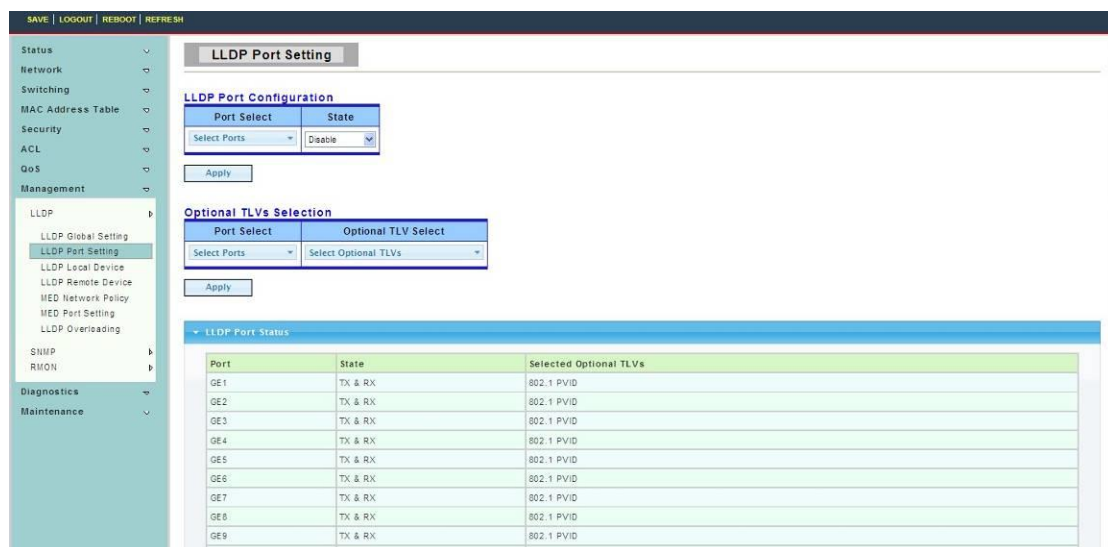
Transmission Interval: Select the interval at which frames are transmitted. The default is 30 seconds, and the valid range is 5–32768 seconds.

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).

4.8.1.2 LLDP Port Settings

To display LLDP Port Settings web page, click **Management > LLDP > LLDP Port Settings**



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

State: Select the transmission state of LLDP port interface.

- Disable: Disable the transmission of LLDP PDUs.

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

Port Select: Select specific ports.

Optional TLV Select: Select Optional TLVs.

4.8.1.3 LLDP Local Device

To display LLDP Local Device web page, click **Management > 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. It features a left-hand navigation menu with categories like Status, Network, Switching, and Management. The 'Management' menu is expanded to show 'LLDP Local Device'. The main content area is titled 'LLDP Local Device' and contains two sections:

- Local Device Summary:** A table with the following data:

Chassis ID Subtype	MAC Address
Chassis ID	DE:AD:BE:EF:01:02
System Name	Switch
System Description	
Capabilities Supported	Bridge
Capabilities Enabled	Bridge
Port ID Subtype	Interface name
- Port Status:** A table with columns: Interface, LLDP Status, and LLDP Med Status.

Interface	LLDP Status	LLDP Med Status
GE1	TX & RX	Enabled
GE2	TX & RX	Enabled
GE3	TX & RX	Enabled
GE4	TX & RX	Enabled
GE5	TX & RX	Enabled
GE6	TX & RX	Enabled
GE7	TX & RX	Enabled
GE8	TX & RX	Enabled

4.8.1.4 LLDP Remote Device

To display LLDP Remote Device web page, click **Management > 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. It features a left-hand navigation menu similar to the previous page. The 'Management' menu is expanded to show 'LLDP Remote Device'. The main content area is titled 'LLDP Remote Device' and contains a table of remote devices. Above the table are buttons for 'Detail', 'Delete', and 'Refresh'.

Sel	Local Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	System Name	Time to Live
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							

4.8.1.5 LLDP Network Policy

To display LLDP Network Policy web page, click **Management > LLDP > LLDP Network Policy**

LLDP MED Network Policy Setting

Voice Auto Mode Configuration

LLDP MED Policy for Voice Application Auto Manual

Apply

Network Policy Configuration

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)

Apply

LLDP MED Network Policy Table

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

4.8.1.6 MED Port Setting

To display MED Port Setting web page, click **Management > LLDP > MED Port Setting**

LLDP Port MED Setting

Port LLDP MED Configuration

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

Apply

LLDP MED Port Setting Table

Interface	LLDP MED Status	User Defined Network Policy		Location	Inventory
		Active	Application		
GE1	Enabled	Yes		No	No
GE2	Enabled	Yes		No	No
GE3	Enabled	Yes		No	No
GE4	Enabled	Yes		No	No
GE5	Enabled	Yes		No	No
GE6	Enabled	Yes		No	No
GE7	Enabled	Yes		No	No
GE8	Enabled	Yes		No	No
GE9	Enabled	Yes		No	No
GE10	Enabled	Yes		No	No

4.8.1.7 LLDP Overloading

To display LLDP Overloading web page, click **Management > LLDP > LLDP Overloading**

SAVE | LOGOUT | REBOOT | REFRESH

Status
Network
Switching
MAC Address Table
Security
ACL
QoS
Management
LLDP
SNMP
RMON

LLDP Port Overloading

LLDP Port Overloading Table

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

4.8.2 SNMP

4.8.2.1 SNMP Setting

To display SNMP Setting web page, click **Management > SNMP > SNMP Setting**

SAVE | LOGOUT | REBOOT | REFRESH

Status
Network
Switching
MAC Address Table
Security
ACL
QoS
Management
LLDP
SNMP
SNMP Setting
SNMP View
SNMP Access Group
SNMP Community
SNMP User
SNMPv1,2 Notification Recipients
SNMPv3 Notification Recipients
SNMP Engine ID
SNMP Remote Engine ID
RMON

SNMP Setting

SNMP Global Setting

State: Disabled Enabled

Apply

SNMP Informations

Information Name	Information Value
SNMP	Disabled

State: SNMP daemon state

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

4.8.2.2 SNMP View

To display SNMP View web page, click **Management > SNMP > SNMP View**

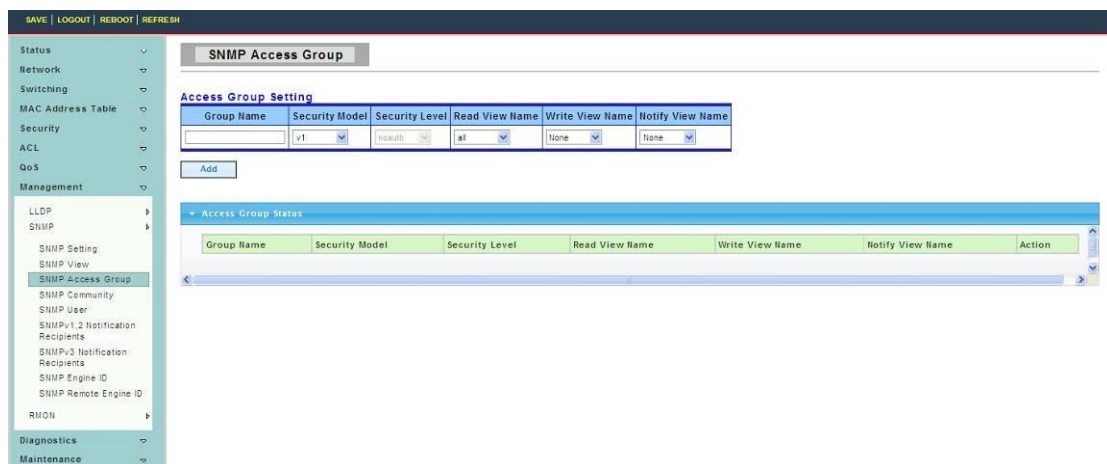
This page is used to configure SNMP view.Used in the SNMP message Management variables (OID) to describe the switch in the Management object,MIB (Management Information Base,Management Information Base) is a set of the monitoring network equipment Management variables.View is used to control variable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



4.8.2.3 SNMP Access Group

To display SNMP Access Group web page, click **Management > SNMP > SNMP Access Group**

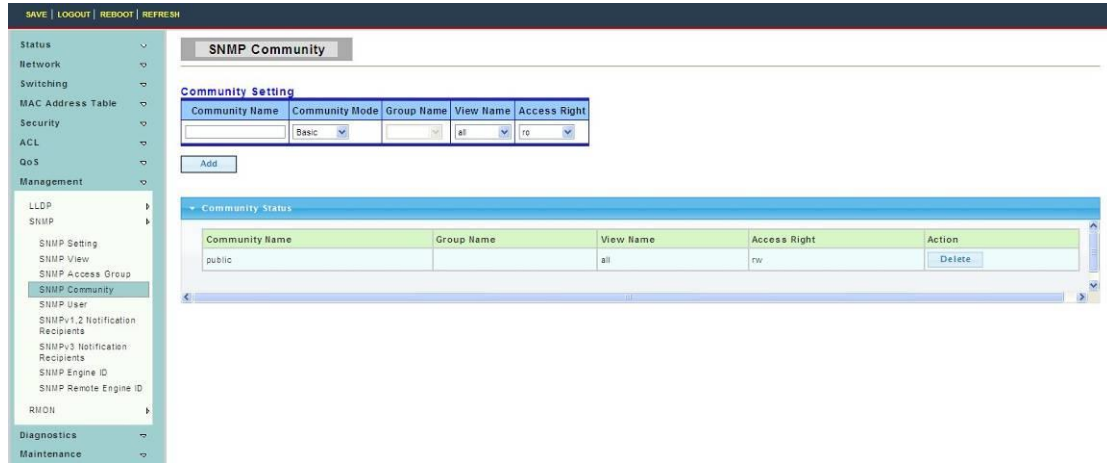
This page is used to configure SNMP group ,Within the group by the user read-only, only write, inform the view to achieve the goal of access control.



4.8.2.4 SNMP Community

To display SNMP Community web page, click **Management > SNMP > SNMP Community**

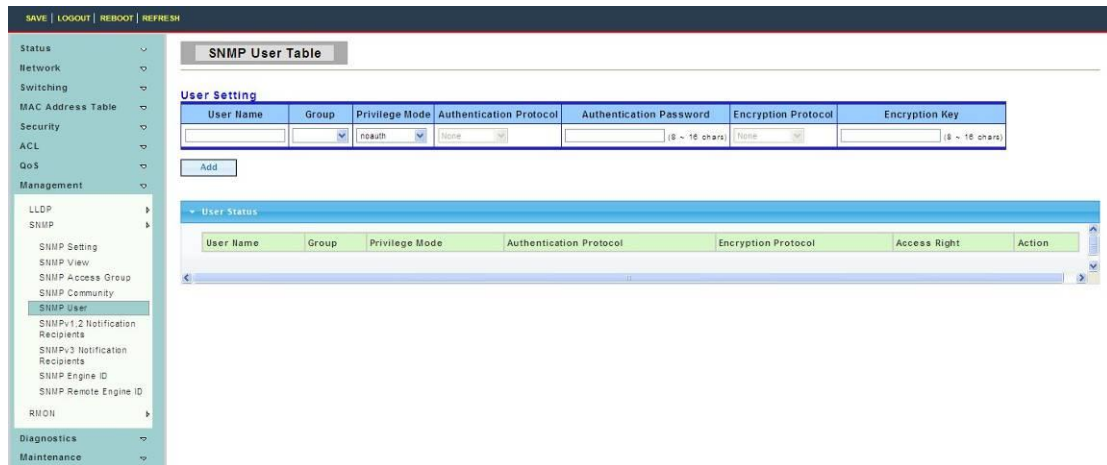
SNMP v1 and the SNMP v2c USES the group Name (Community Name) certification, the group has played a role similar to the password.If use SNMP v1 and SNMP v2c, after configuration view, can be directly on this page to configure SNMP community.



4.8.2.5 SNMP User

To display SNMP User web page, click **Management > SNMP > SNMP User**

This page is used to create SNMP user under the group, And the group with the same level of security and access control permissions.



4.8.2.6 SNMPv1,2 Notification Recipients

To display SNMPv1,2 Notification Recipients web page, click **Management > SNMP > SNMPv1,2 Notification Recipients**

The screenshot shows the 'Notification Recipients SNMPv1,2' configuration page. It includes a navigation menu on the left with categories like Status, Network, Switching, and Management. The main content area has a 'SNMPv1,2 Host Setting' table with columns for Server Address, SNMP Version, Notify Type, Community Name, UDP Port, TimeOut, and Retries. Below this is an 'Add' button and a 'SNMPv1,2 Host Status' table with columns for Server Address, SNMP Version, Notify Type, Community Name, UDP Port, TimeOut, Retry, and Action.

4.8.2.7 SNMPv3 Notification Recipients

To display SNMPv3 Notification Recipients web page, click **Management > SNMP > SNMPv3 Notification Recipients**

The screenshot shows the 'Notification Recipients SNMPv3' configuration page. It features a navigation menu on the left. The main content area has an 'SNMPv3 Host Setting' table with columns for Server Address, Notify Type, User Name, UDP Port, TimeOut, and Retries. Below this is an 'Add' button and a 'SNMPv3 Host Status' table with columns for Server Address, Notify Type, User Name, UDP Port, Time Out, Retry, and Action.

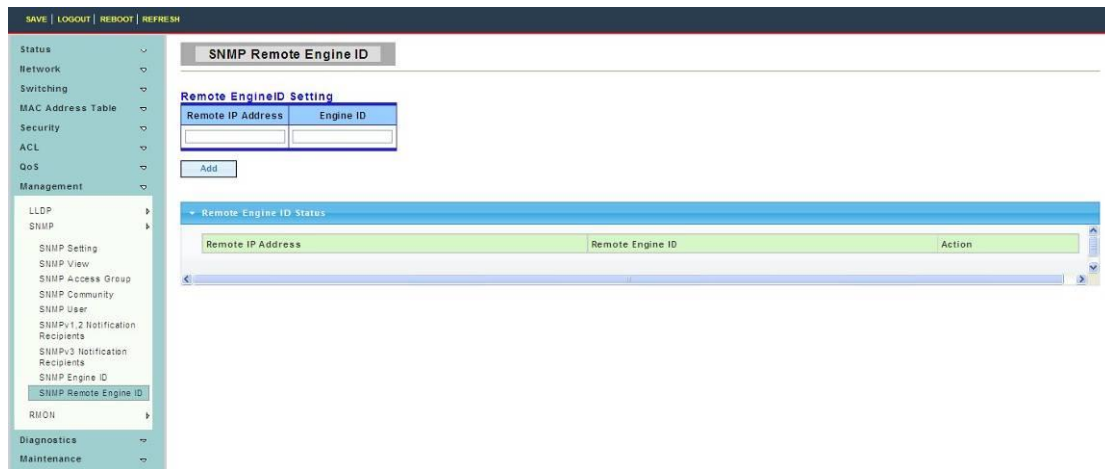
4.8.2.8 SNMP Engine ID

To display SNMP Engine ID web page, click **Management > SNMP > SNMP Engine ID**

The screenshot shows the 'Engine ID Setting' configuration page. It includes a navigation menu on the left. The main content area has an 'Engine ID Setting' section with a table for 'Engine ID Settings' containing 'Use Default' (radio buttons for Enabled/Disabled) and 'Engine ID' (text input field with value 'DEADBEEF0102'). Below this is an 'Apply' button and an 'Engine ID Status' table with columns for Information Name and Information Value, showing 'Use Default' as Enabled and 'Engine ID' as DEADBEEF0102.

4.8.2.9 SNMP Remote Engine ID

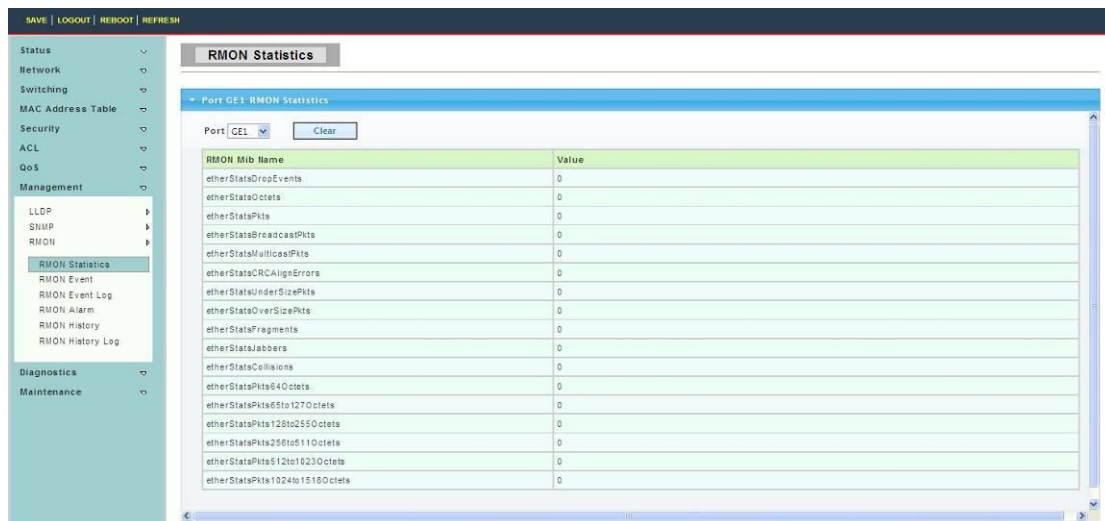
To display SNMP Remote Engine ID web page, click **Management > SNMP > SNMP Remote Engine ID**



4.8.3 RMON

4.8.3.1 RMON Statistics

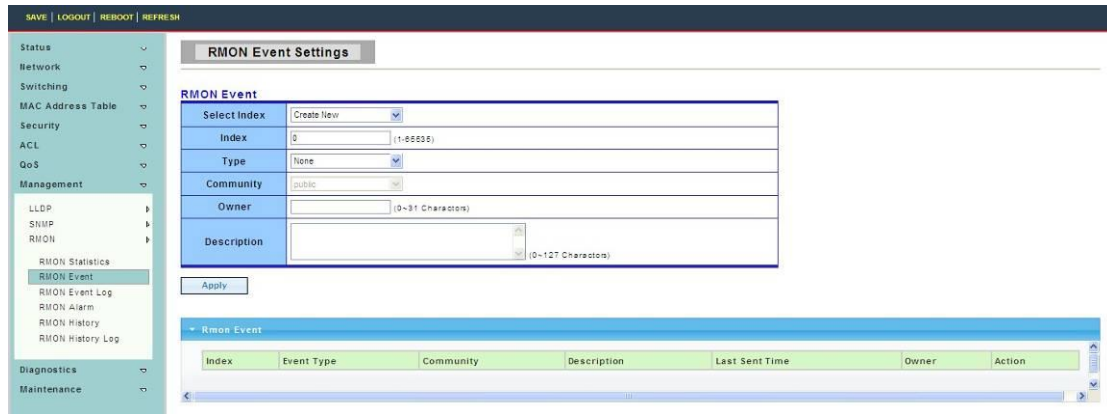
To display RMON Statistics web page, click **Management > RMON > RMON Statistics**



4.8.3.2 RMON Event

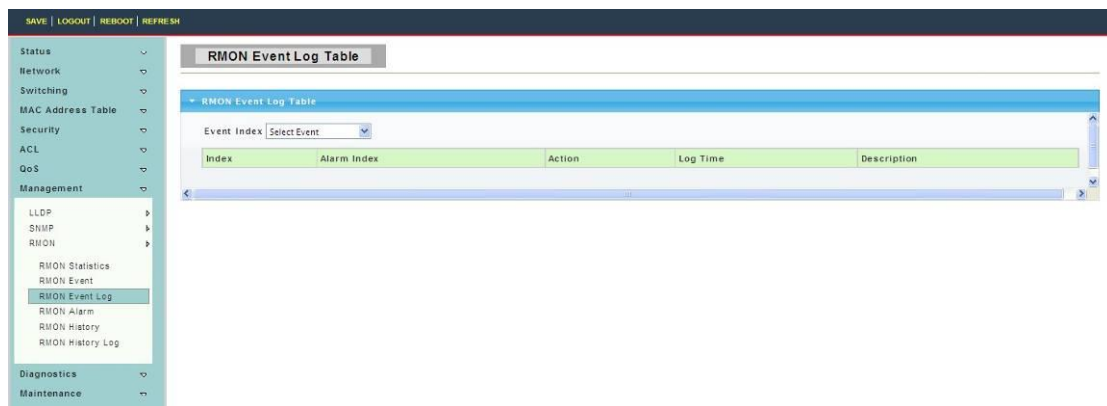
To display RMON Event web page, click **Management > RMON > RMON Event**

This page is used to configure RMON event group.



4.8.3.3 RMON Event Log

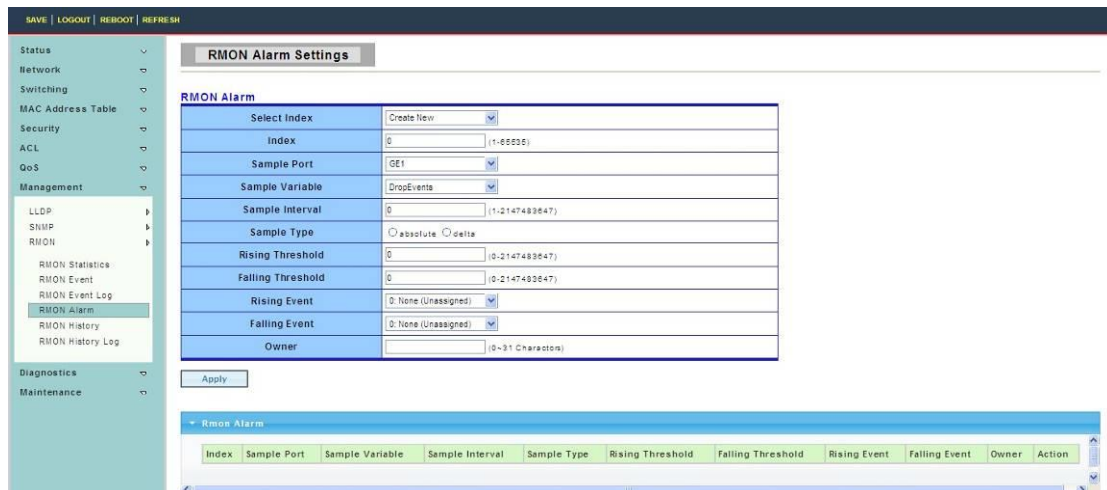
To display RMON Event Logweb page, click **Management > RMON > RMON Event Log**



4.8.3.4 RMON Alarm

To display RMON Alarm web page, click **Management > RMON > RMON Alarm**

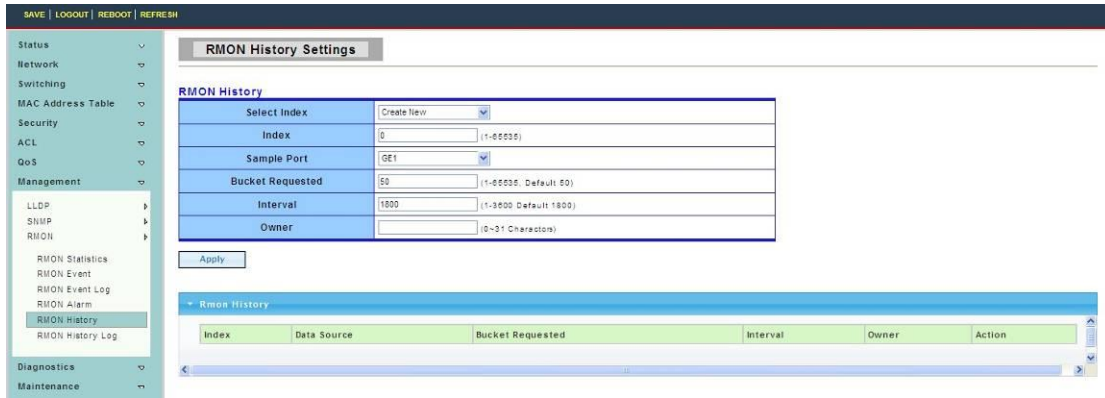
This page is used to configure RMON statistics group and alarm group.



4.8.3.5 RMON History

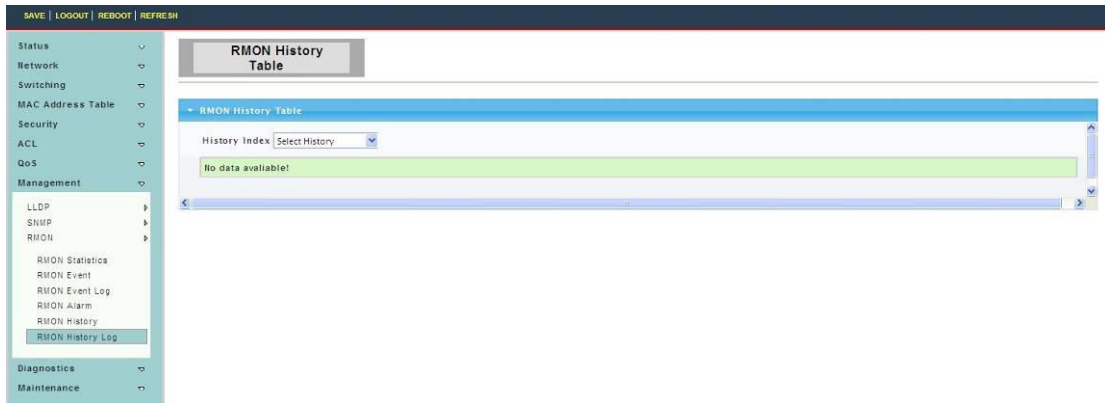
To display RMON History web page, click **Management > RMON > RMON History**

This page is used to configure the PMON history group.



4.8.3.6 RMON History Log

To display RMON History Log web page, click **Management > RMON > RMON History Log**

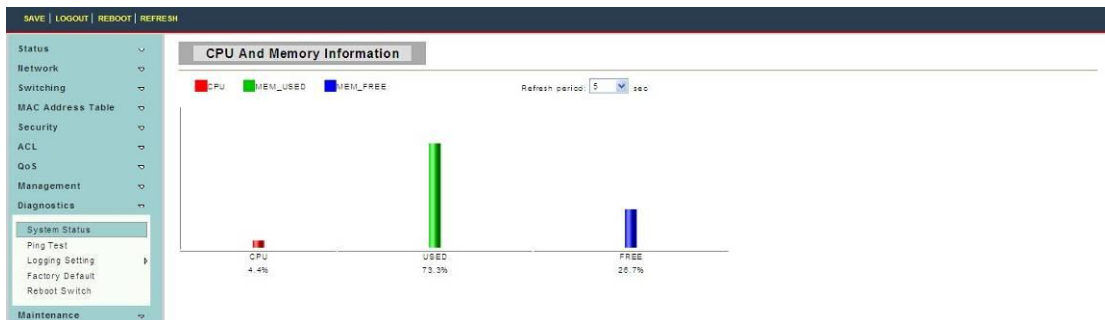


4.9 Diagnostics

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

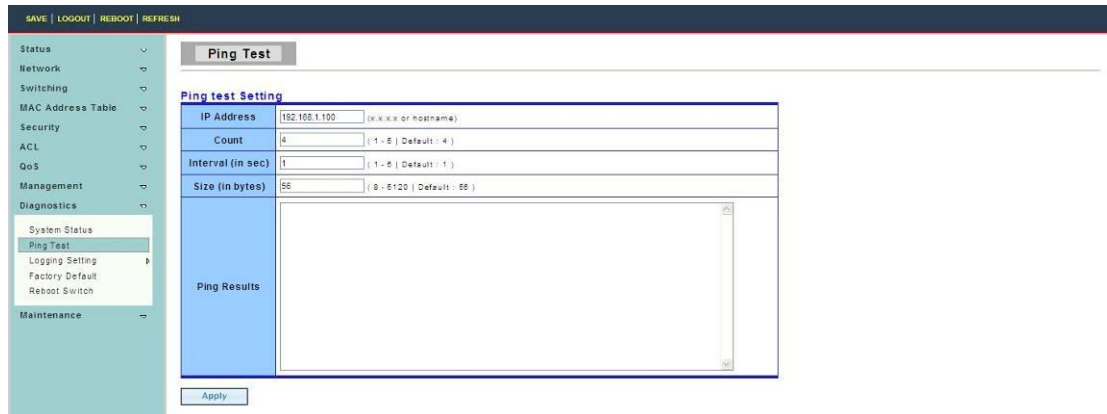
4.9.1 System Status

To display System Status Log web page, click **Diagnostics > System Status**



4.9.2 Ping Test

To display Ping Test Log web page, click **Diagnostics > Ping Test**



IP Address:The IP address of ping target.

Count: How many times to send ping request packet.

Interval: Time interval between each ping request packet.

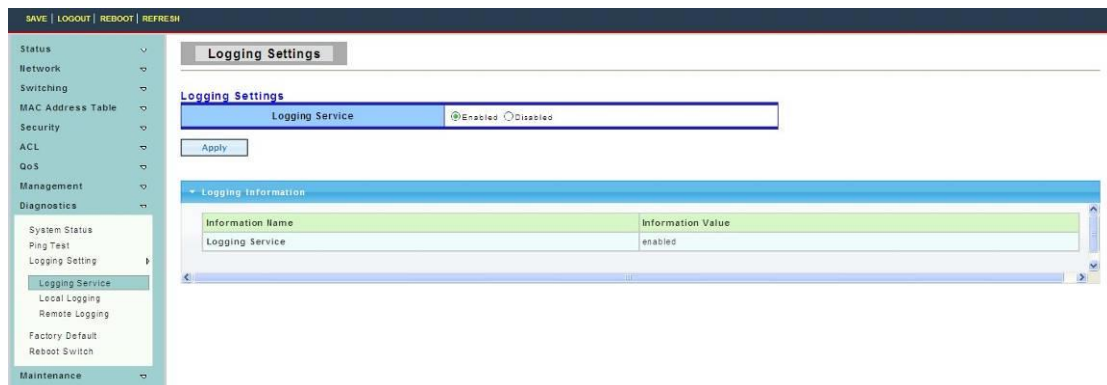
Size: The size of ping packet.

Ping Results: After ping finished, results will show in this field.

4.9.3 Logging Setting

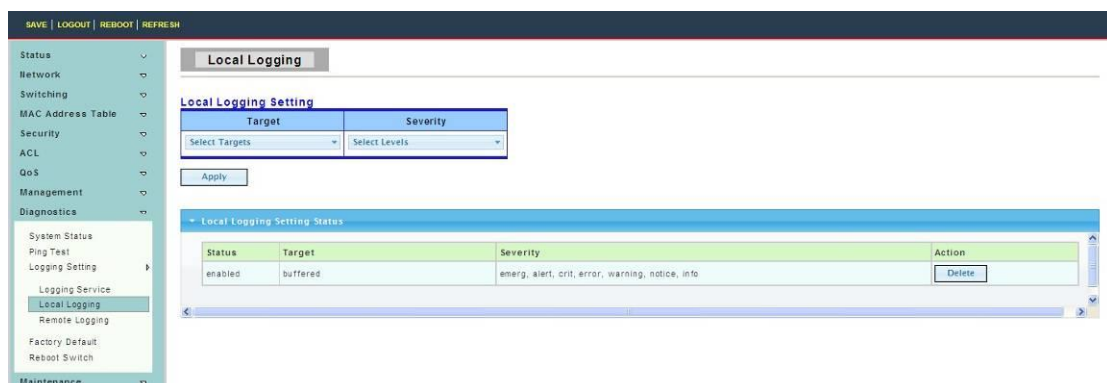
4.9.3.1 Logging Service

To display Logging Service web page, click **Diagnostics > Logging Setting > Logging Service**



4.9.3.2 Local Logging

To display Local Logging web page, click **Diagnostics > Logging Setting > Local Logging**



Target: Select the target to store log message

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

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

4.9.3.3 Remote Logging

To display Remote Logging web page, click **Diagnostics > Logging Setting > Remote Logging**



Server Address: The IP address of remote log server.

Server Port:The Port number of remote log server.

Severity: Select severity of log messages which will be sent.

4.9.4 Factory Default

To display Factory Default web page, click **Diagnostics > Factory Default**

This page allow user to restore switch to factory default by pushing “Restore” button.



4.9.5 Reboot Switch

To display Reboot Switch web page, click **Diagnostics > Reboot Switch**

This page allow user to reboot the switch by pushing “Reboot” button.



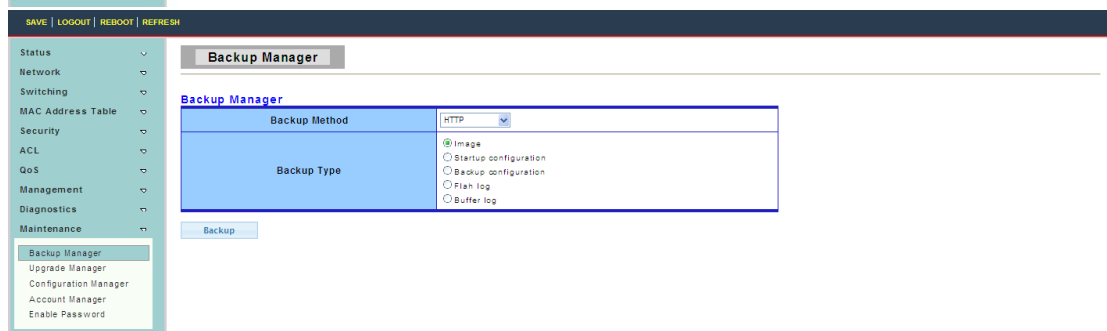
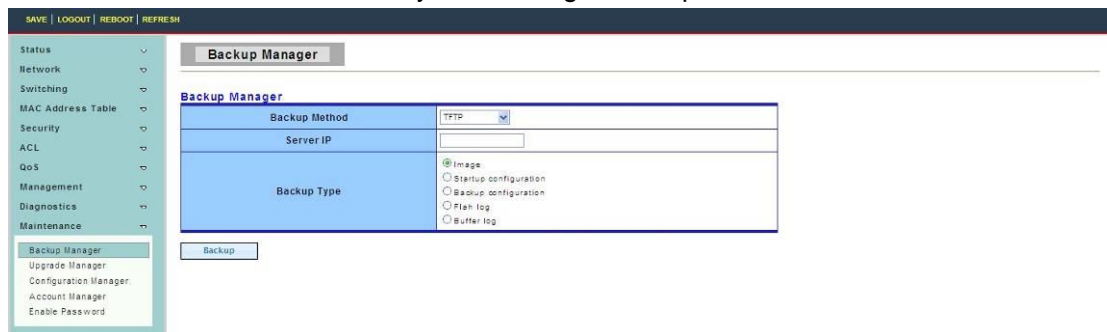
4.10 Maintenance

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

4.10.1 Backup Manager

To display Backup Manager web page, click **Maintenance > Backup Manager**

This page allow user to backup the firmware image or configuration file on the switch to remote TFTP server or host file system through HTTP protocol.



Backup Method: Select backup method

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

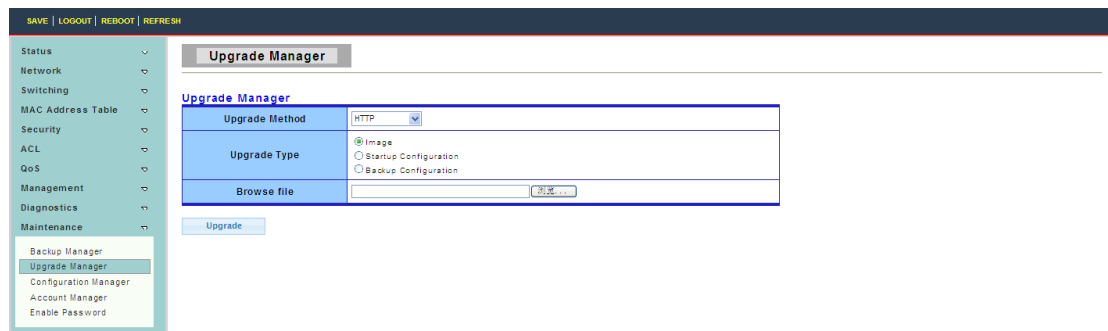
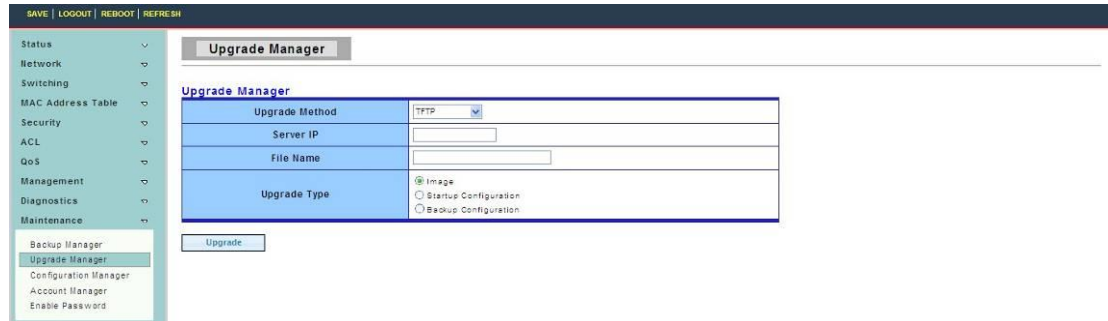
Server IP: IP address of the TFTP server. If the TFTP backup method is selected, the IP address of the TFTP server must be assigned.

Backup Type: Select Backup Type

4.10.2 Upgrade Manager

To display Upgrade Manager web page, click **Maintenance > Upgrade Manager**

This page allow user to upgrade new firmware image or configuration file to the switch from remote TFTP server or select file from web browser.



Upgrade Method: Select upgrade method

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

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

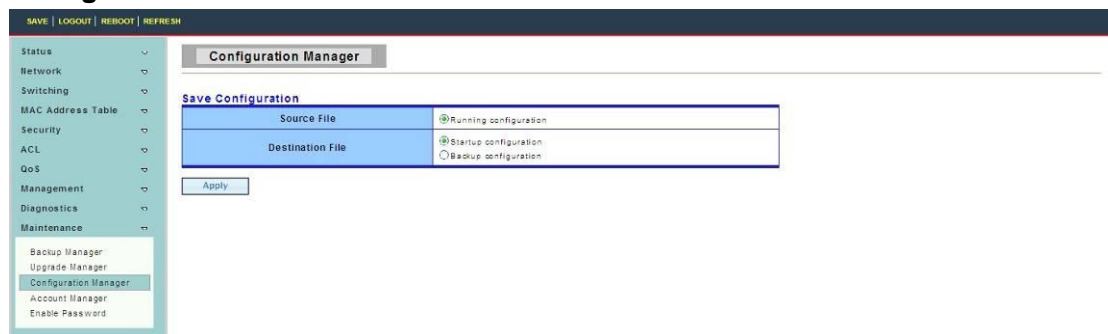
File Name: Firmware image or configuration file name on remote TFTP server. If the TFTP upgrade method is selected, the file name must be specified.

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

Upgrade Type: Select Backup Type

4.10.3 Configuration Manager

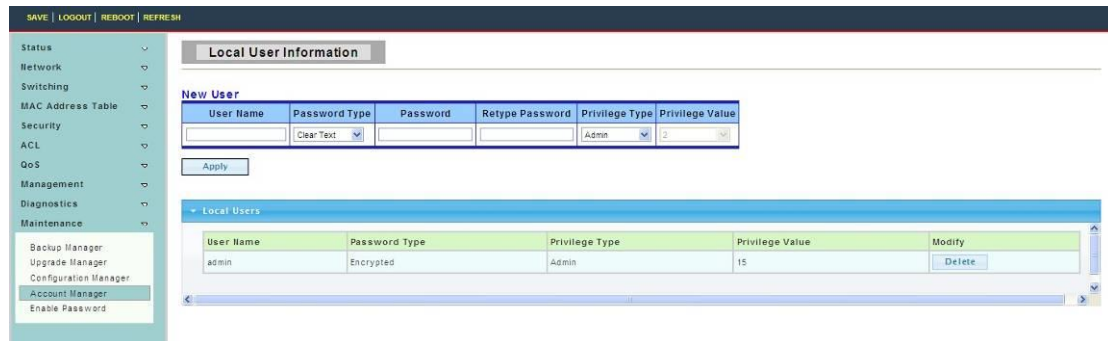
To display Configuration Manager web page, click **Maintenance > Configuration Manager**



4.10.4 Account Manager

To display Account Manager web page, click **Maintenance > Account Manager**

This page allow user to add or delete switch local user database for authenticating.



User Name: User name for new account.

Password Type: Select password type for new account.

- Clear Text: Password without encryption
- Encrypted: Password with encryption
- No Password: No password for the new account.

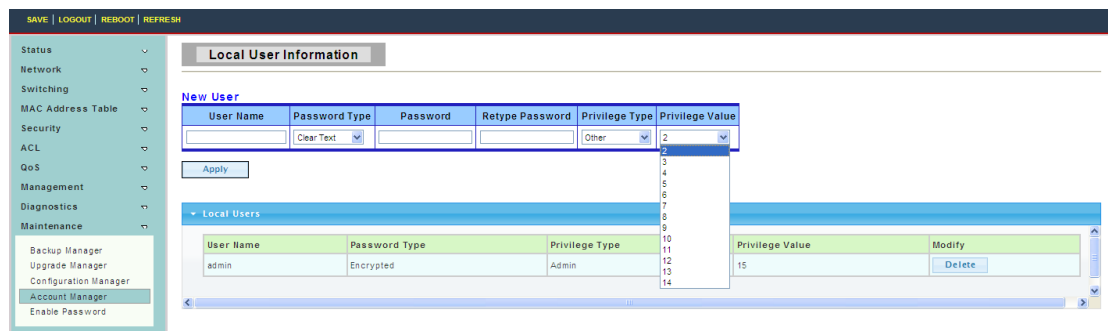
Password: If the password type is not “No Password”, the password must be specified.

Retype Password: Retype password to make sure the password is exactly you typed before in “Password” field.

Privilege Type: Select privilege level for new account.

- Admin: Allow to change switch settings.
- User: See switch settings only. Not allow to change it.

If AAA feature is enabled, we have one more privilege type to allow user adding privilege value for this account.



User Name: User name for new account.

Password Type: Select password type for new account.

- Clear Text: Password without encryption
- Encrypted: Password with encryption
- No Password: No password for the new account.

Password: If the password type is not “No Password”, the password must be specified.

Retype Password: Retype password to make sure the password is exactly you typed before in “Password” field.

Privilege Type: Select privilege level for new account.

- Admin: Allow to change switch settings.

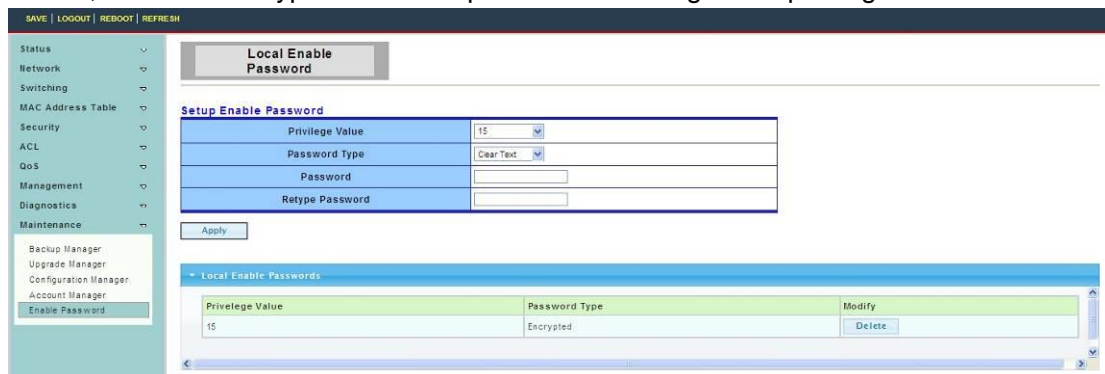
- User: See switch settings only. Not allow to change it.
- Other: Assign privilege level value in Privilege value field.

Privilege Value: If the account privilege type is “Other”, set the privilege level for this account here. The valid privilege level is from 2 to 14.

4.10.5 Enable Password

To display Enable Password web page, click **Maintenance > Enable Password**

This page allow user to modify the enable password. In command line interface, user can use “enable” command to change their privilege level to “Admin”. After “enable” command is issued, user need to type the enable password to change their privilege level.



Privilege Value	Password Type	Modify
15	Encrypted	Delete

Password Type: Select password type for enable password.

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

Password: Password string.

Retype Password: Retype password to make sure the password is exactly you typed before in “Password” field.