2SFP Port 10/100/1000Mbps
Web Smart Ethernet Switch

DN-80201

DN-80211-1

DN-80221-1

Manual

DN-80201 • DN-80211-1 • DN-80221-1

Table of Contents

Chapter 1 Product Introduction

Congratulations on 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 8/16/24 port + 2SFP 10/100/1000Mbps Managed Ethernet Switch provides seamless network connection. It integrates 10/100/1000Mbps Ethernet network capabilities, and can be configured by web based interface. Including administrator, port management, VLAN setting, port statistics, trunking, QoS setting, security filter, configuration/ backup/recovery, log out, and so on.

1.2 Features (8 port)

- 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 Console port management
- Supports IEEE802.3x flow control for Full-duplex Mode and back pressure for Half-duplex Mode
- 8K entry MAC address table with auto-learning and auto-aging
- Supports WEB management interface
- LED indicators for monitoring power, link, activity and speed

1.2.1 Features (16 port)

- Comply with IEEE802.3, IEEE802.3u, IEEE802.3ab, IEEE802.3x, IEEE802.3z, EEE802.3ad standards
- Supports IEEE802.3x flow control for Full-duplex Mode and back pressure for Half-duplex Mode
- Supports MAC address auto-learning and auto-aging
- Store and forward mode operates
- Support SNMP/RMON/TELENT
- Supports IEEE802.1Q VLAN,4K VLAN Table
- Support IEEE802.1p Priority Queues
- Support ACL Function, 1.5K-entry ALC table
- Support Storm Control
- Support QoS, Port Mirroring, Link Aggregation Protocol
- LED indicators for monitoring power, link/activity
- Web-based Management Support
- Internal power adapter supply

1.2.2 Features (24 port)

- Comply with IEEE802.3, IEEE802.3u, IEEE802.3ab, IEEE802.3x, IEEE802.3z, EEE802.3ad standards
- Supports IEEE802.3x flow control for Full-duplex Mode and back pressure for Half-duplex Mode
- Supports MAC address auto-learning and auto-aging
- Store and forward mode operates
- Support SNMP/RMON/TELENT
- Supports IEEE802.1Q VLAN,4K VLAN Table
- Support IEEE802.1p Priority Queues
- Support ACL Function, 1.5K-entry ALC table
- Support Storm Control
- Support 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 (8 port)

1.3.1 Front Panel (8 port)

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.

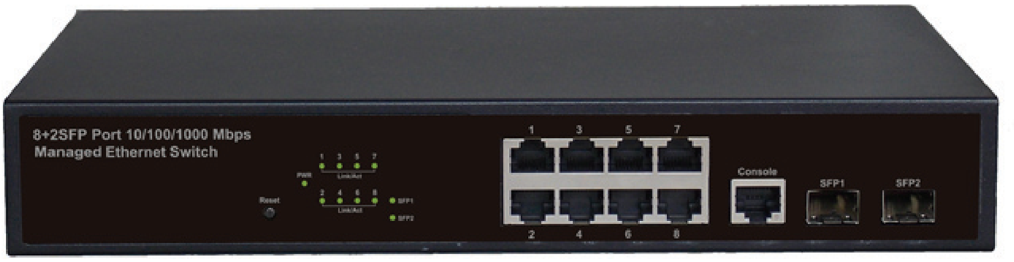


Figure 1 - Front Panel

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

Designed to connect to devices with a bandwidth of 10Mbps, 100Mbps or 1000Mbps. Each has a corresponding 10/100/1000Mbps LED.

SFP ports (SFP1, SFP2):

Designed to install SFP module and connect to devices with a bandwidth of 1000Mbps. Each has a corresponding 1000Mbps LED.

Console port (Console):

Designed to connect with 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.

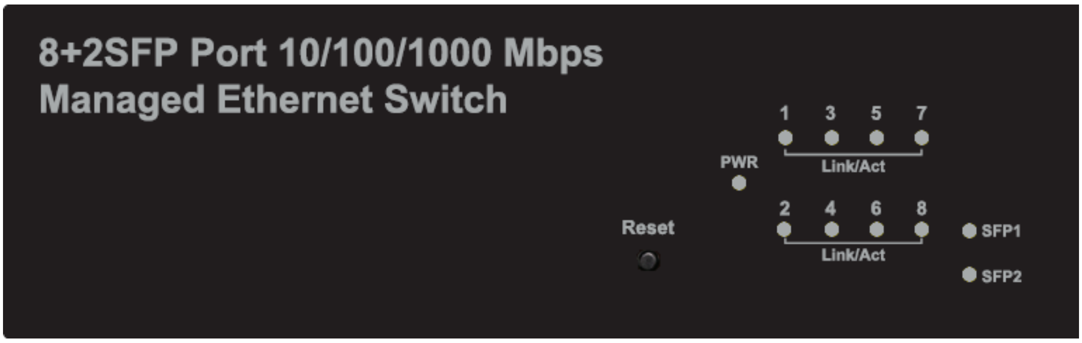


Figure 2 - LED Indicators

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	No device is connected to the port
	1000Mbps: Green	Flashing	Sending or receiving data
SFP1 SFP2	Green	On	A device is connected to the port
		Off	No device is connected to the port
		Flashing	Sending or receiving data

1.3.2 Rear Panel (8 port)

The rear panel of the Switch contains AC power connector shown as below.

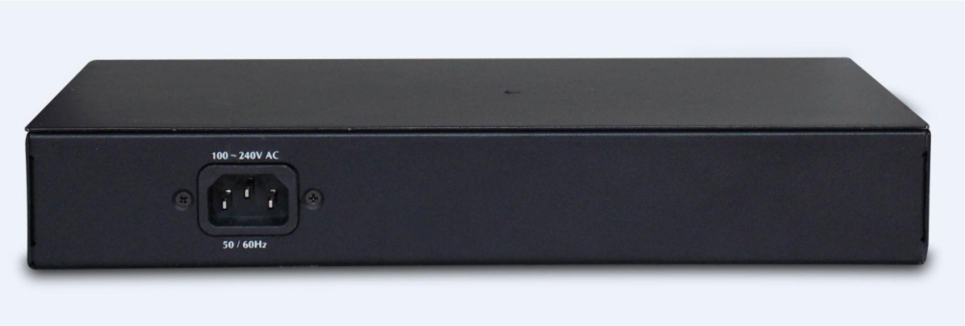


Figure 3 - Rear Panel

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

1.3.3 External Component Description (16 port)

1.3.4 Front Panel (16 port)

The front panel of the Switch consists of 16 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.

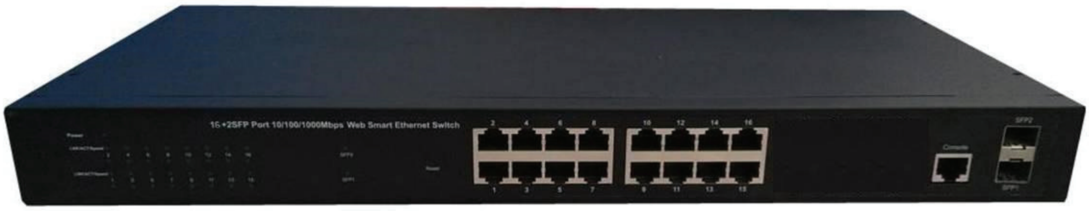


Figure 1 - Front Panel

10/100/1000Mbps RJ-45 ports (1~16):
Design 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):
Design to install the SFP module and connect to the device with a bandwidth of 1000Mbps. Each has a corresponding 1000Mbps LED.

Console port (Console):
Design 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.

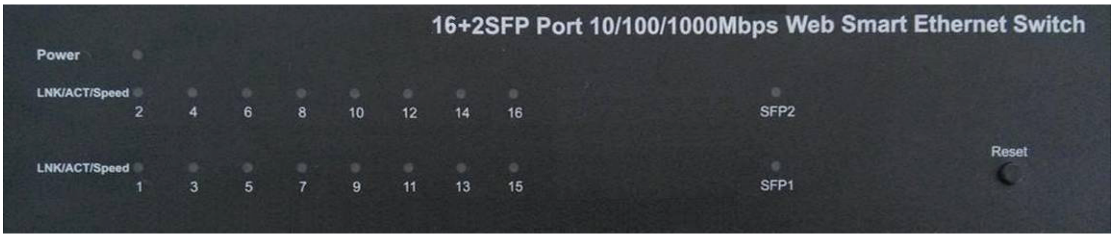


Figure 2 - LED Indicators

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

<table>
<tr><th>LED</th><th>COLOR</th><th>STATUS</th><th>STATUS DESCRIPTION</th></tr>
<tr><td rowspan="2">Power</td><td rowspan="2">Red</td><td>On</td><td>Power On</td></tr>
<tr><td>Off</td><td>Power Off</td></tr>
<tr><td rowspan="4">LNK/ACT/
Speed
(1~16)</td><td rowspan="2">10/100Mbps:
Orange</td><td>On</td><td>A device is connected to the port</td></tr>
<tr><td rowspan="2">Off</td><td rowspan="2">No device is connected to the port</td></tr>
<tr><td rowspan="2">1000Mbps:
Green</td></tr>
<tr><td>Flashing</td><td>Sending or receiving data</td></tr>
<tr><td rowspan="3">SFP1
SFP2</td><td rowspan="3">Green</td><td>On</td><td>A device is connected to the port</td></tr>
<tr><td>Off</td><td>No device is connected to the port</td></tr>
<tr><td>Flashing</td><td>Sending or receiving data</td></tr>
</table>

1.3.5 Rear Panel (16 port)

The rear panel of the Switch contains AC power connector shown as below.

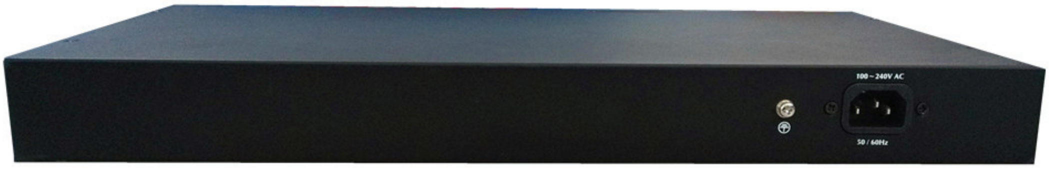


Figure 3 - Rear Panel

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

Grounding Terminal:
The Switch already comes with Lightning Protection Mechanism. You can also ground the Switch through the PE (Protecting Earth) cable of AC cord or with Ground Cable.

1.3.6 External Component Description (24 port)

1.3.7 Front Panel (24 port)

The front panel of the Switch consists of 24 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.

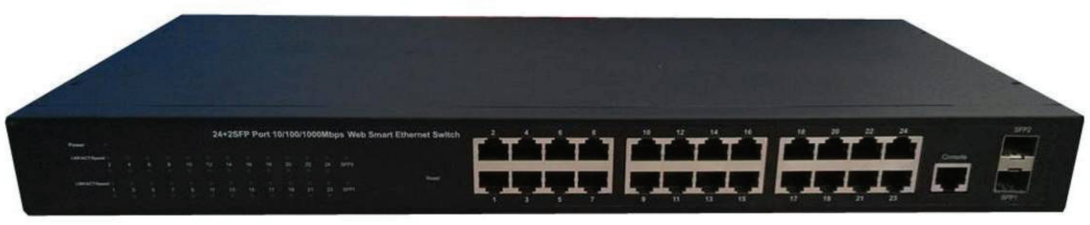


Figure 1 - Front Panel

10/100/1000Mbps RJ-45 ports (1~24):
Design 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):
Design to install the SFP module and connect to the device with a bandwidth of 1000Mbps. Each has a corresponding 1000Mbps LED.

Console port (Console):
Design 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.

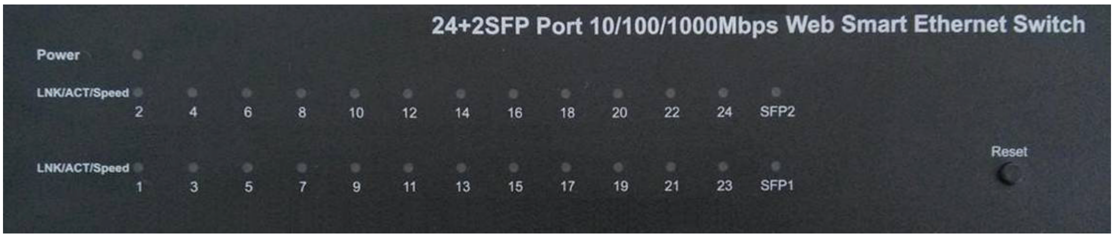

24+2SFP Port 10/100/1000Mbps Web Smart Ethernet Switch
Power
LNK/ACT/Speed
2 4 6 8 10 12 14 16 18 20 22 24 SFP2
LNK/ACT/Speed
1 3 5 7 9 11 13 15 17 19 21 23 SFP1
Reset

Figure 2 - LED Indicators

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

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

1.3.8 Rear Panel (24 port)

The rear panel of the Switch contains AC power connector and one marker shown as below.

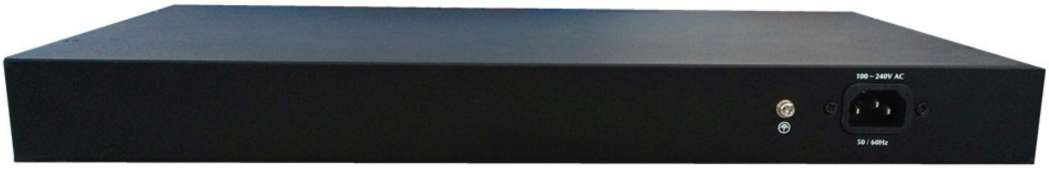


Figure 3 - Rear Panel

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

Grounding Terminal:
The Switch already comes with Lightning Protection Mechanism. You can also ground the Switch through the PE (Protecting Earth) cable of AC cord or with Ground Cable.

1.4 Package Contents (8 port)

Before installing the Switch, make sure that the following "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

1.4.1 Package Contents (16 port)

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

1.4.2 Package Contents (24 port)

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 that the cabinet has enough back up for the weight of the Switch and its accessories.

2.1.1 Desktop Installation (8 port)

Sometimes users are not equipped with the 19-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 19-inch Cabinet (8 port)

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, 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.

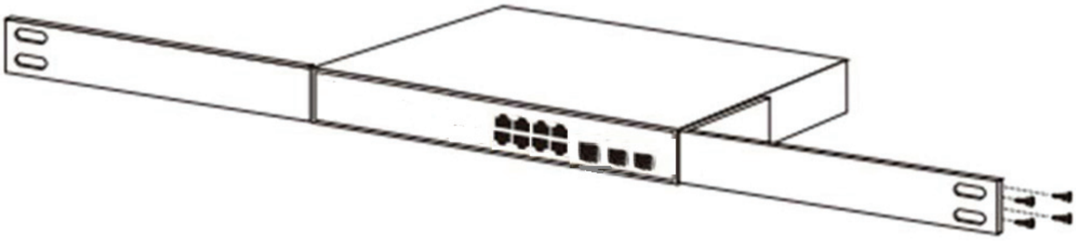


Figure 4 - Bracket Installation

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

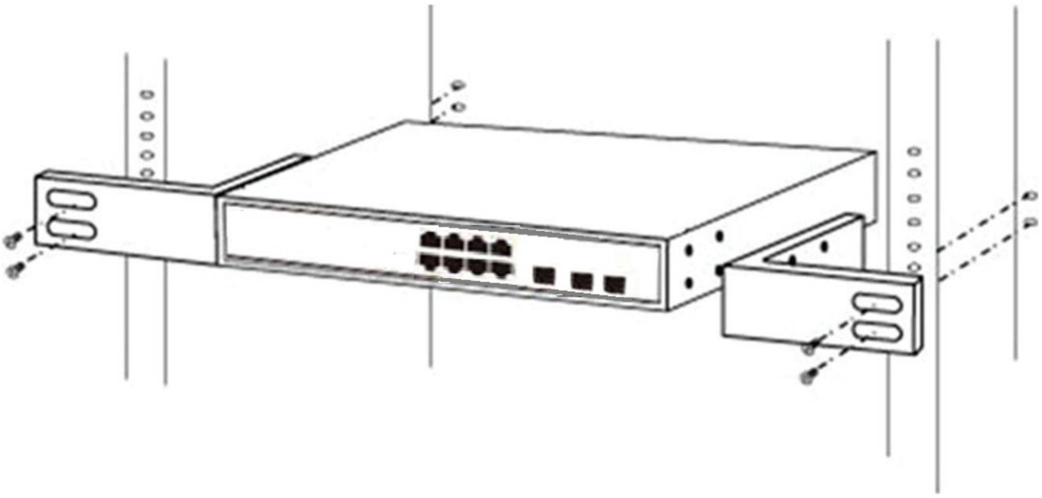


Figure 5 - Rack Installation

2.1.3 Power on the Switch (8 port)

The Switch is powered by 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.

2.1.4 Desktop Installation (16 port)

Sometimes users are not equipped with the 19-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.

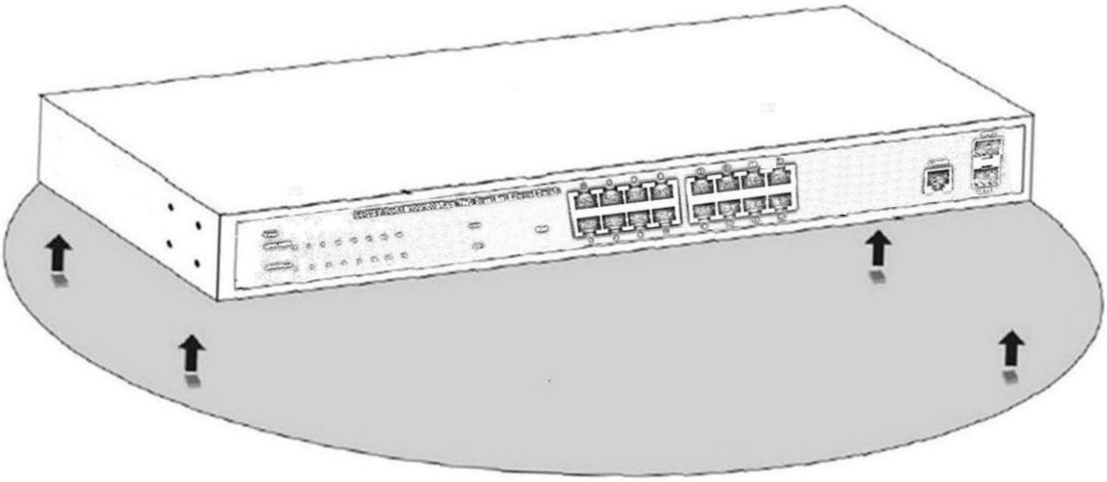


Figure 4 - Desktop Installation

2.1.5 Rack-mountable Installation in 19-inch Cabinet (16 port)

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, please follow these steps:

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

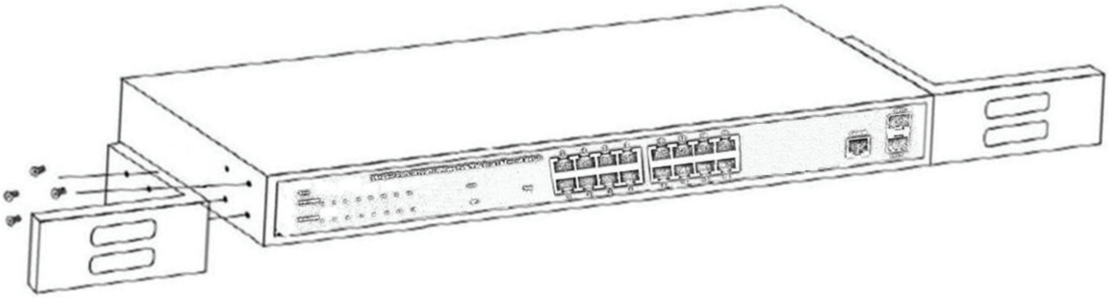


Figure 5 - Bracket Installation

d. Use the screws provided with the equipment rack to mount the Switch on the rack and tighten it.

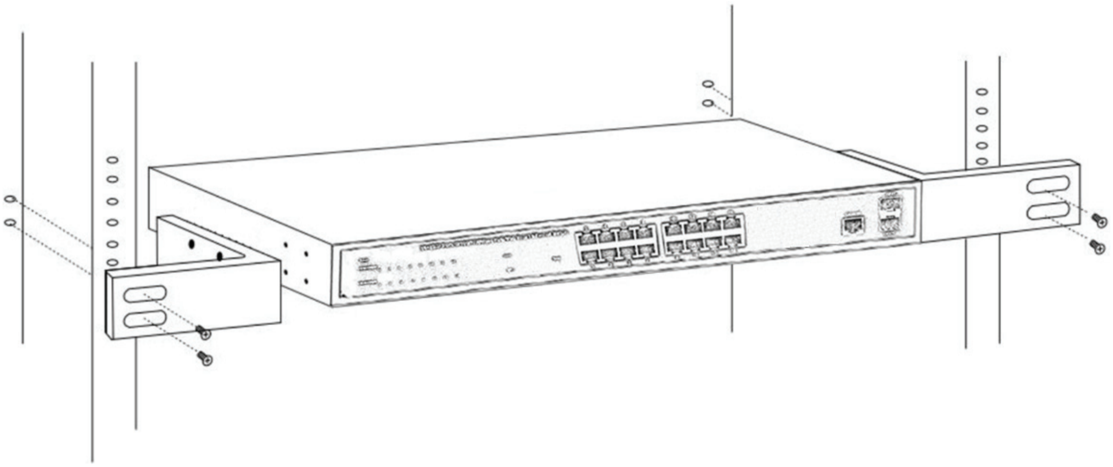


Figure 6 - Rack Installation

2.1.6 Power on the Switch (16 port)

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.

2.1.7 Desktop Installation (24 port)

Sometimes users are not equipped with the 19-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.

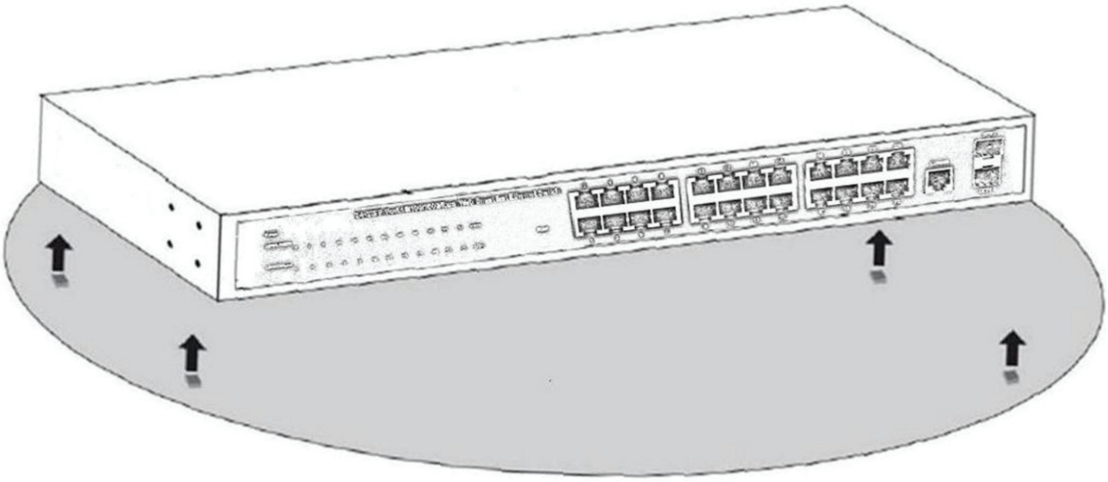


Figure 4 - Desktop Installation

2.1.8 Rack-mountable Installation in 19-inch Cabinet (24 port)

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, please follow these steps:

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

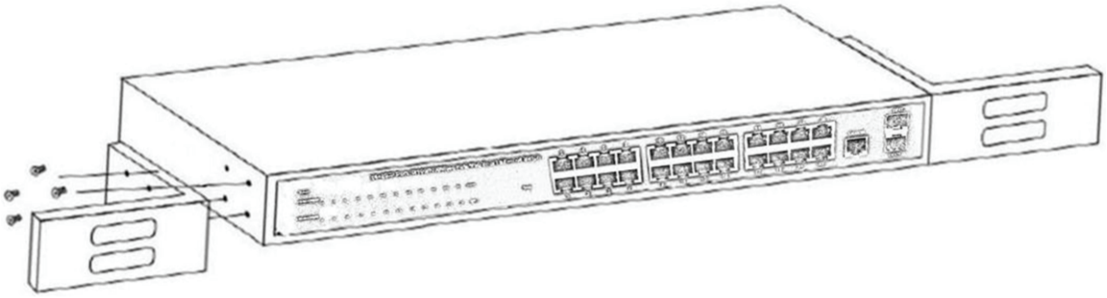


Figure 5 - Bracket Installation

f. Use the screws provided with the equipment rack to mount the Switch on the rack and tighten it.

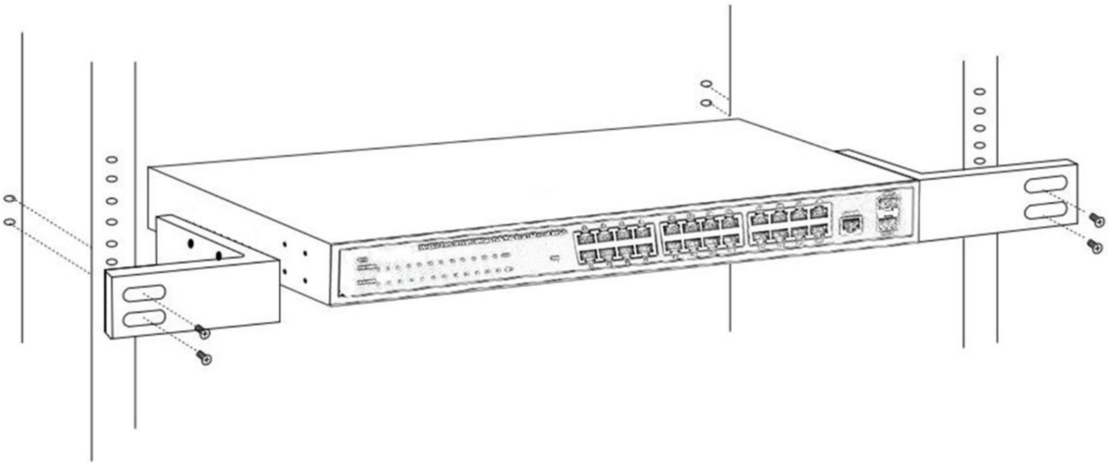


Figure 6 - Rack Installation

2.1.9 Power on the Switch (24 port)

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 (8 port)

3.1 Switch to End Node (8 port)

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.

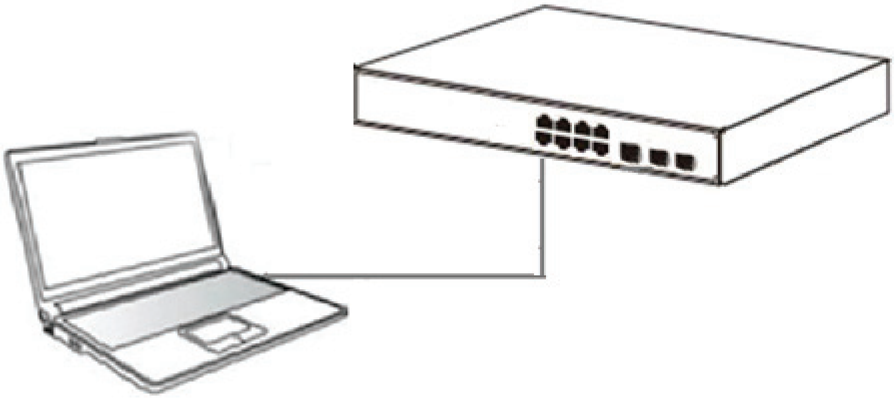


Figure 6 - PC Connect

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 (8 port)

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.

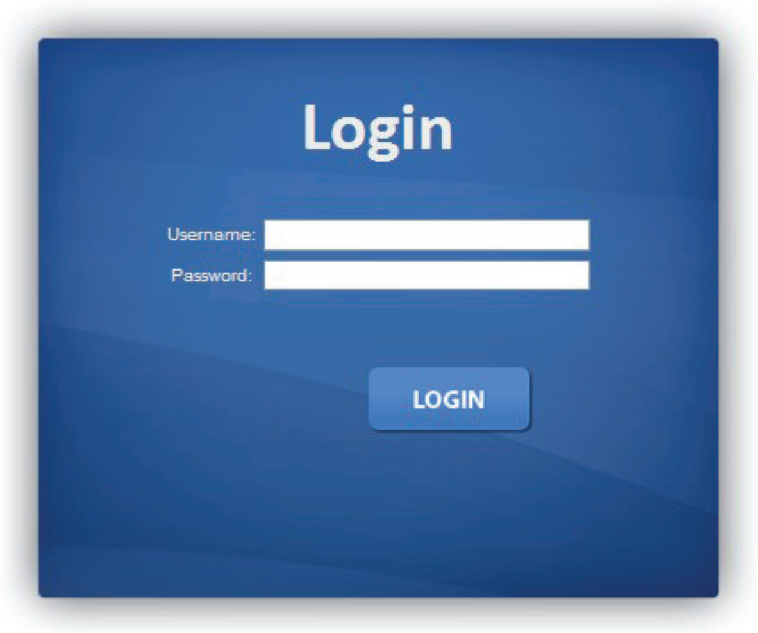
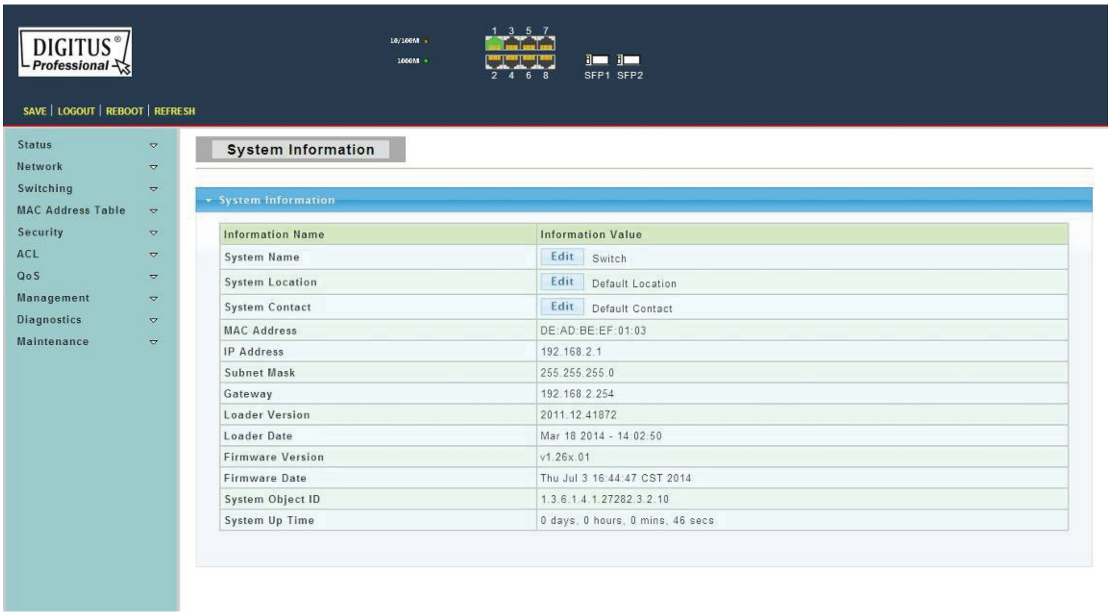


Figure 7 - Login Window

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.



Information Name	Information Value
System Name	Edit Switch
System Location	Edit Default Location
System Contact	Edit Default Contact
MAC Address	DE:AD:BE:EF:01:03
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Gateway	192.168.2.254
Loader Version	2011.12.41872
Loader Date	Mar 18 2014 - 14:02:50
Firmware Version	v1.26x.01
Firmware Date	Thu Jul 3 16:44:47 CST 2014
System Object ID	1.3.6.1.4.1.27282.3.2.10
System Up Time	0 days, 0 hours, 0 mins, 46 secs

Figure 8 - Configuration Window

Chapter 3 How to Login the Switch   (16 port)

3.3 Switch to End Node (16 port)

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.

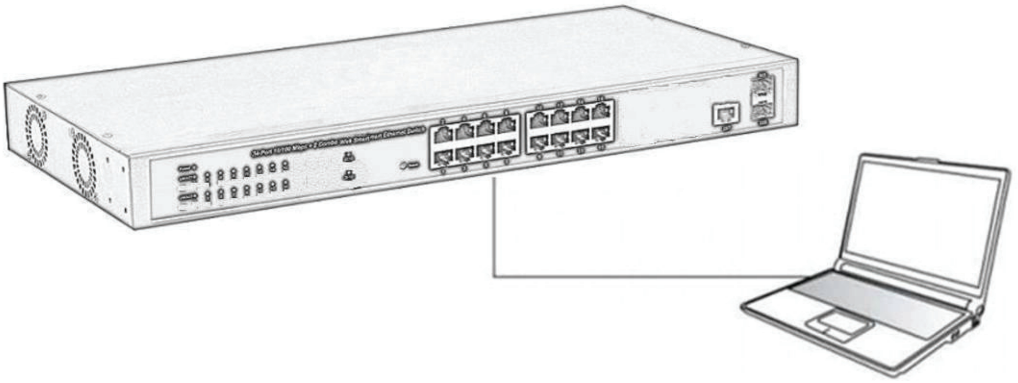


Figure 7 - PC Connect

Please refer to the LED Indicator Specification.The LINK/ACT/Speed LEDs for each port lights on when the link is available.

3.4 How to Login the Switch (16 port)

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:

6. Connect the Switch with the computer NIC interface.
7. Power on the Switch.
8. 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.
9. Open the browser, and enter ***http://192.168.2.1*** and then press "Enter". The Switch login window appears, as shown below.

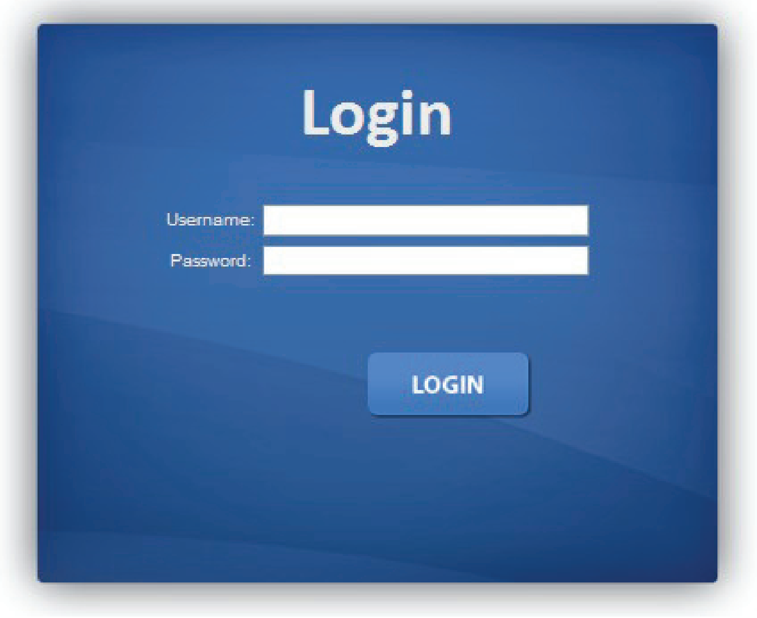
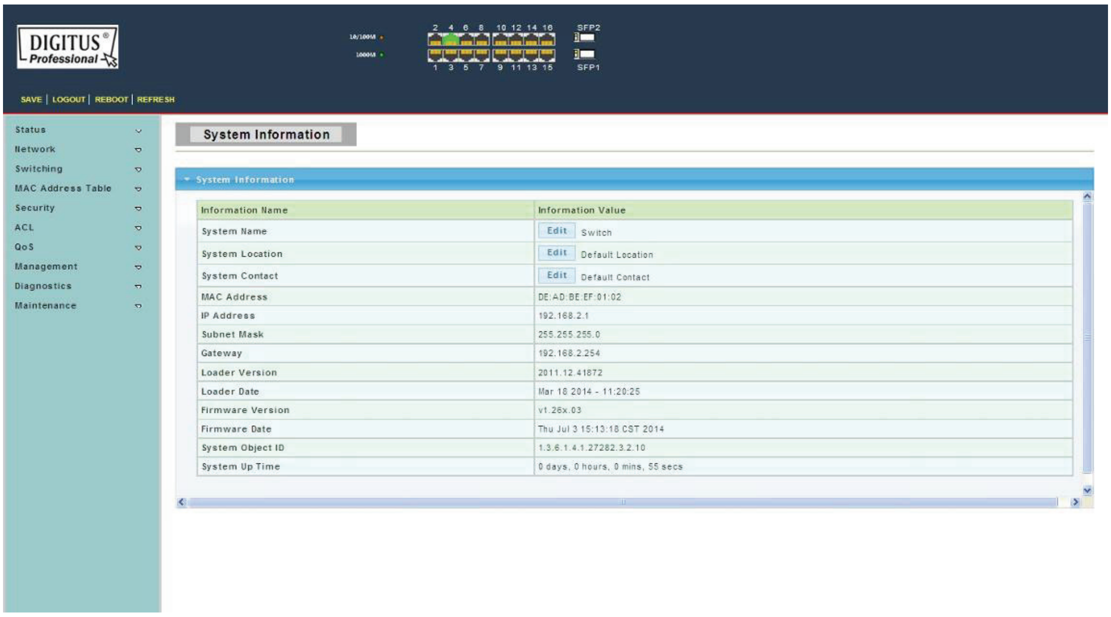


Figure 8 - Login Window

10. 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.



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	2011.12.41872
Loader Date	Mar 18 2014 - 11:20:25
Firmware Version	v1.26x.03
Firmware Date	Thu Jul 3 15:13:18 CST 2014
System Object ID	1.3.6.1.4.1.27282.3.2.10
System Up Time	0 days, 0 hours, 0 mins, 55 secs

Figure 9 - Configuration Window

Chapter 3 How to Login the Switch (24 port)

3.5 Switch to End Node (24 port)

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.

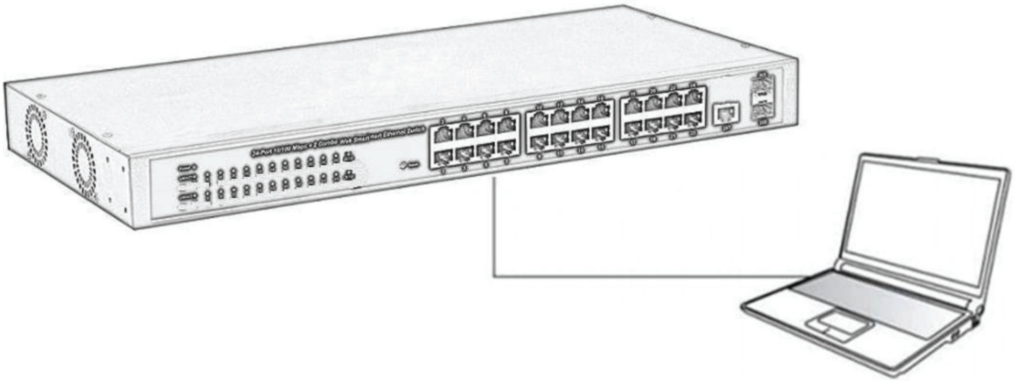


Figure 7 - PC Connect

Please refer to the LED Indicator Specification.The LINK/ACT/Speed LEDs for each port lights on when the link is available.

3.6 How to Login the Switch (24 port)

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:

11. Connect the Switch with the computer NIC interface.
12. Power on the Switch.
13. 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.
14. Open the browser, and enter ***http://192.168.2.1*** and then press "Enter". The Switch login window appears, as shown below.

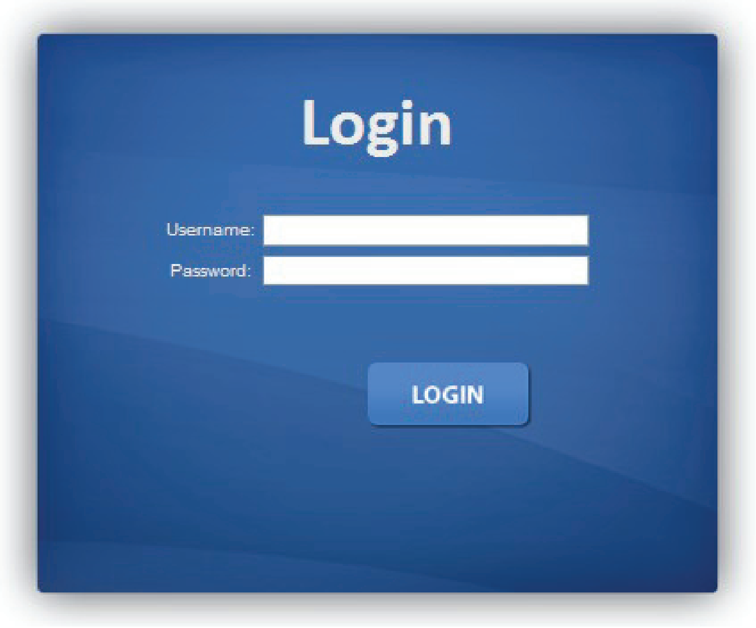
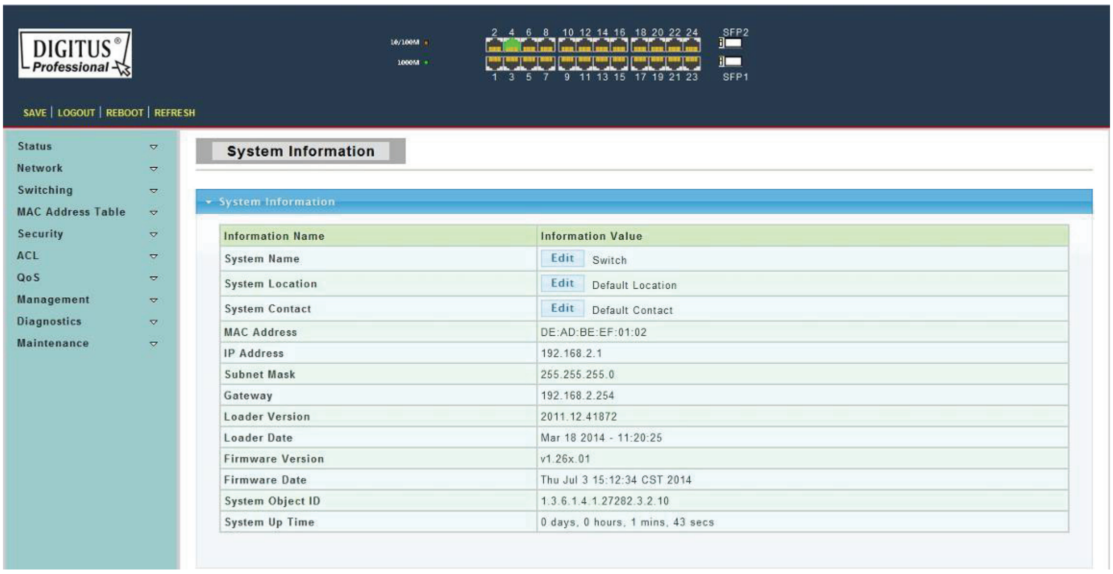


Figure 8 - Login Window

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



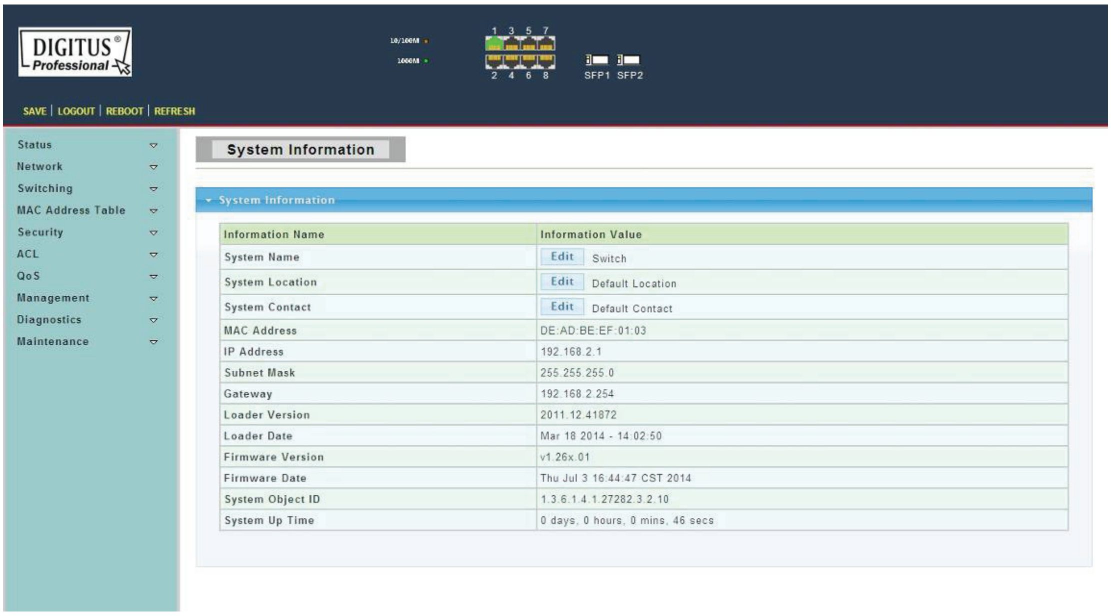
Information Name	Information Value
System Name	Edit Switch
System Location	Edit Default Location
System Contact	Edit Default Contact
MAC Address	DE:AD:BE:EF:01:02
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Gateway	192.168.2.254
Loader Version	2011.12.41872
Loader Date	Mar 18 2014 - 11:20:25
Firmware Version	v1.26x.01
Firmware Date	Thu Jul 3 15:12:34 CST 2014
System Object ID	1.3.6.1.4.1.27282.3.2.10
System Up Time	0 days, 0 hours, 1 mins, 43 secs

Figure 9 - Configuration Window

Chapter 4 Switch Configuration

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



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:01:03
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Gateway	192.168.2.254
Loader Version	2011.12.41872
Loader Date	Mar 18 2014 - 14:02:50
Firmware Version	v1.26x.01
Firmware Date	Thu Jul 3 16:44:47 CST 2014
System Object ID	1.3.6.1.4.1.27282.3.2.10
System Up Time	0 days, 0 hours, 0 mins, 46 secs

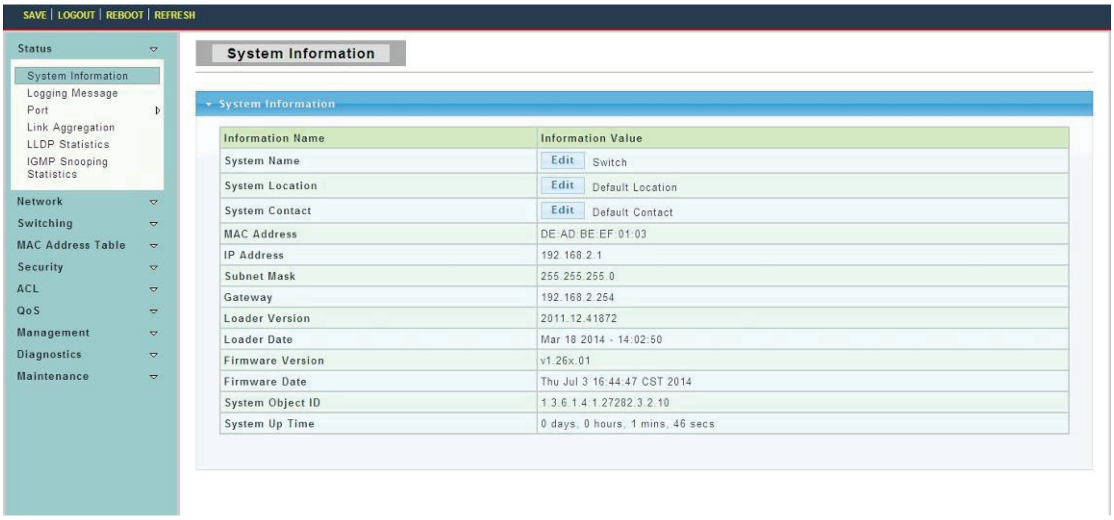
4.1 Status

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 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:01:03
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Gateway	192.168.2.254
Loader Version	2011.12.41872
Loader Date	Mar 18 2014 - 14:02:50
Firmware Version	v1.26x.01
Firmware Date	Thu Jul 3 16:44:47 CST 2014
System Object ID	1.3.6.1.4.1.27282.3.2.10
System Up Time	0 days, 0 hours, 1 mins, 46 secs

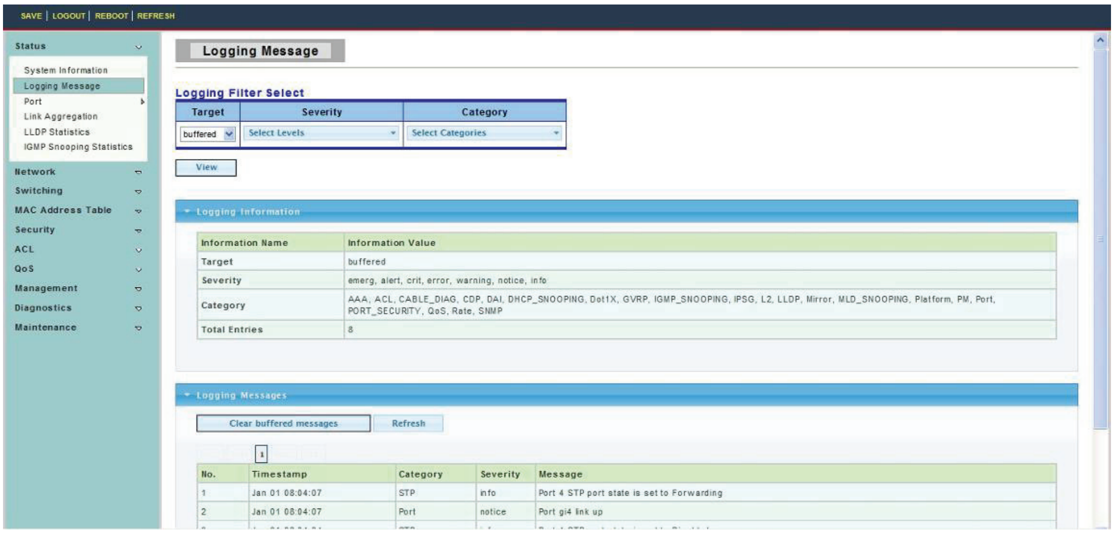
System Name: System name of the switch. This name will also use as CLI prefix of each line. (“Switch>” or “Switch#”).

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**



Logging Filter Select

Target	Severity	Category
buffered	Select Levels	Select Categories

Logging Information

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	8

Logging Messages

No.	Timestamp	Category	Severity	Message
1	Jan 01 08:04:07	STP	info	Port 4 STP port state is set to Forwarding
2	Jan 01 08:04:07	Port	notice	Port gi4 link up

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

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

Severity: Select severity to filter log messages.

Category: Select category to filter log messages.

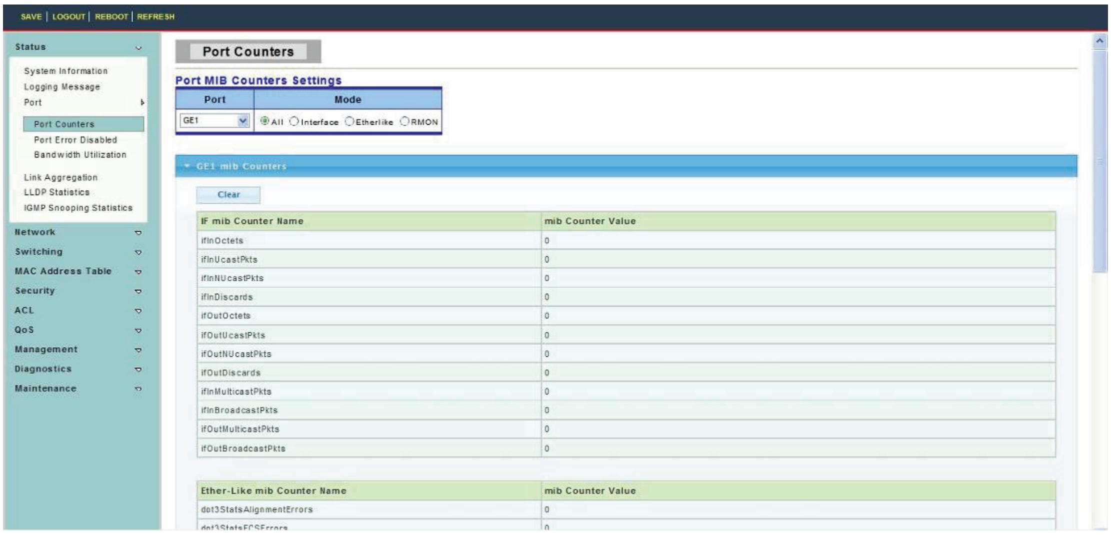
4.1.3 Port

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 form 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.



Port Counters

Port MIB Counters Settings

Port	Mode
GE1	● All ○ Interface ○ Etherlike ○ RMON

GE1 mib Counters

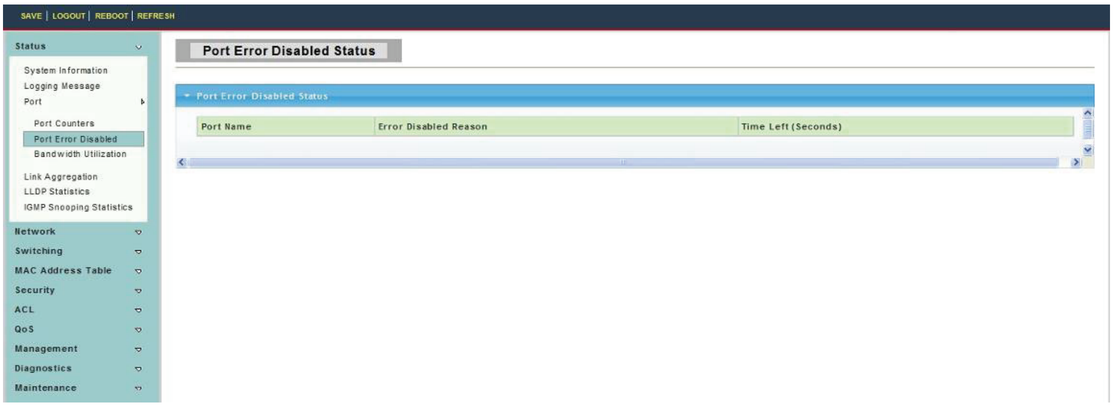
IF mib Counter Name	mib Counter Value
ifInOctets	0
ifInUcastPkts	0
ifInNUcastPkts	0
ifInDiscards	0
ifOutOctets	0
ifOutUcastPkts	0
ifOutNUcastPkts	0
ifOutDiscards	0
ifInMulticastPkts	0
ifInBroadcastPkts	0
ifOutMulticastPkts	0
ifOutBroadcastPkts	0

Ether-Like mib Counter Name	mib Counter Value
dot3StatsAlignmentErrors	0
dot3StatsFCSErrors	0

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.



Port Error Disabled Status

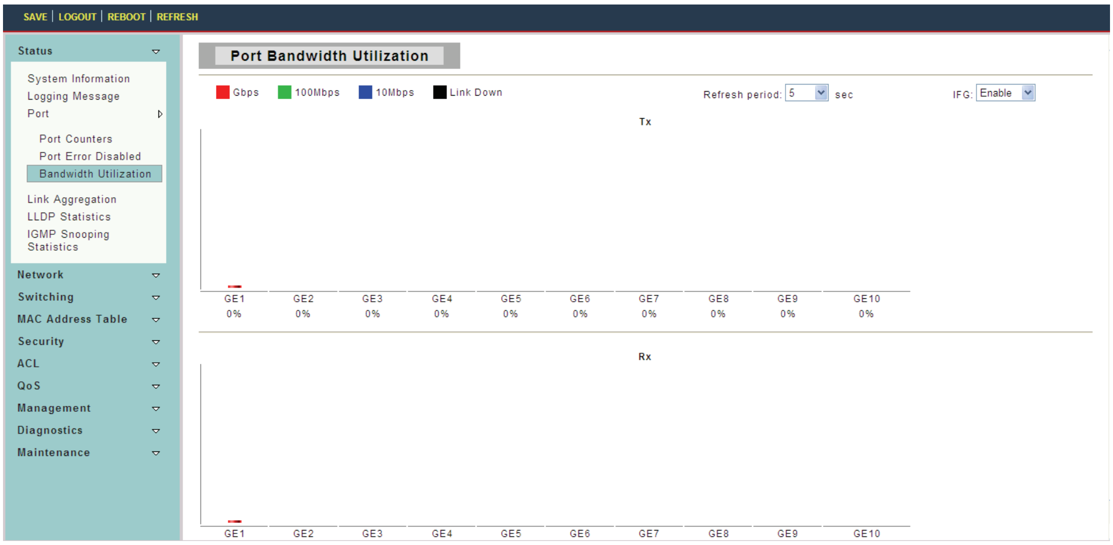
Port Error Disabled Status

Port Name	Error Disabled Reason	Time Left (Seconds)

4.1.3.3 Bandwidth Utilization

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

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



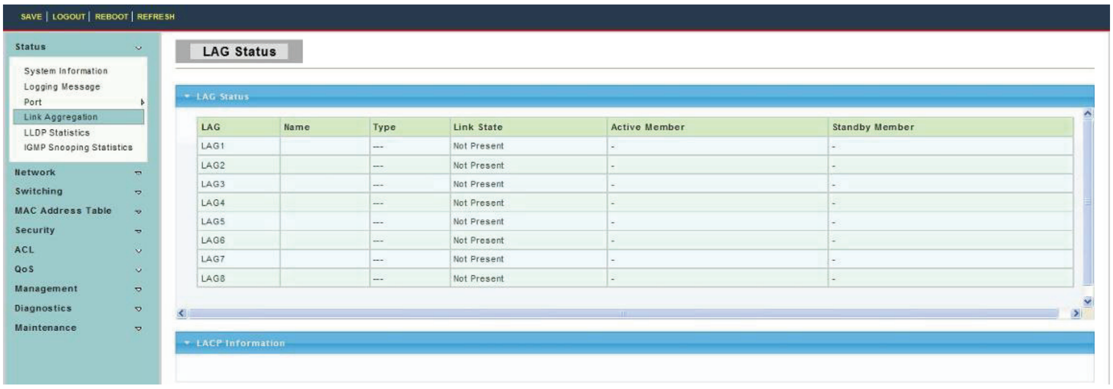
Refresh period: 5 sec

IFG: Enable

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 Status

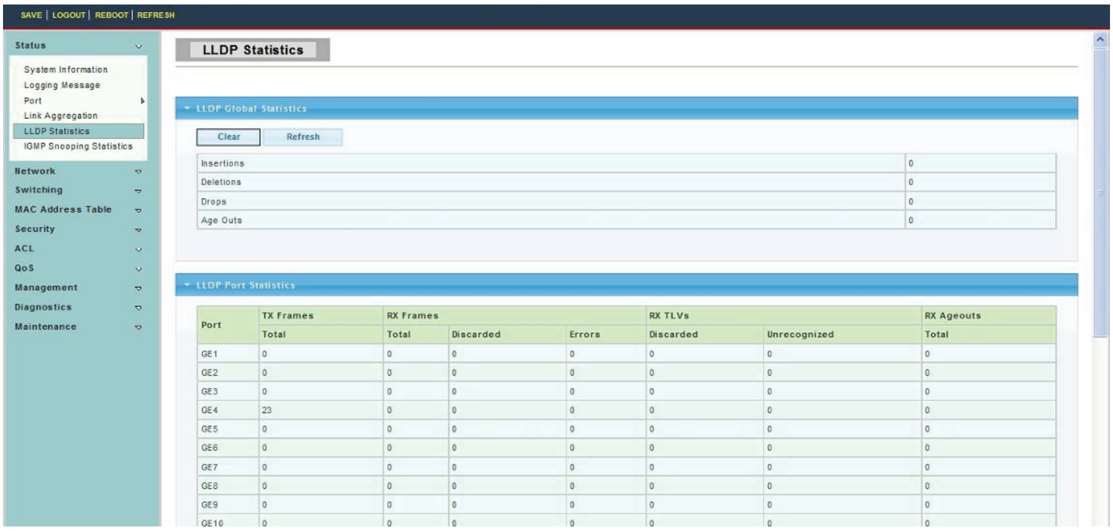
LAG	Name	Type	Link State	Active Member	Standby Member
LAG1		---	Not Present	-	-
LAG2		---	Not Present	-	-
LAG3		---	Not Present	-	-
LAG4		---	Not Present	-	-
LAG5		---	Not Present	-	-
LAG6		---	Not Present	-	-
LAG7		---	Not Present	-	-
LAG8		---	Not Present	-	-

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

4.1.5 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.



LLDP 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	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	23	0	0	0	0	0	0
GE5	0	0	0	0	0	0	0
GE6	0	0	0	0	0	0	0
GE7	0	0	0	0	0	0	0
GE8	0	0	0	0	0	0	0
GE9	0	0	0	0	0	0	0
GE10	0	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.

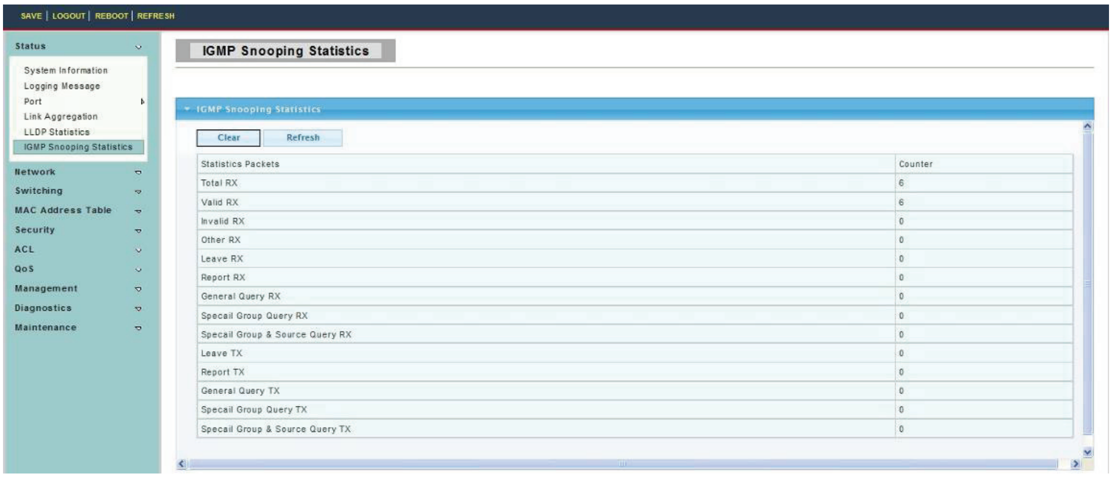
Drops: The number of times the complete set of information advertised by MSAP could not be entered into tables associated with the remote systems because of insufficient resources.

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.



IGMP Snooping Statistics

IGMP Snooping 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
Specail Group Query RX	0
Specail Group & Source Query RX	0
Leave TX	0
Report TX	0
General Query TX	0
Specail Group Query TX	0
Specail Group & Source Query TX	0

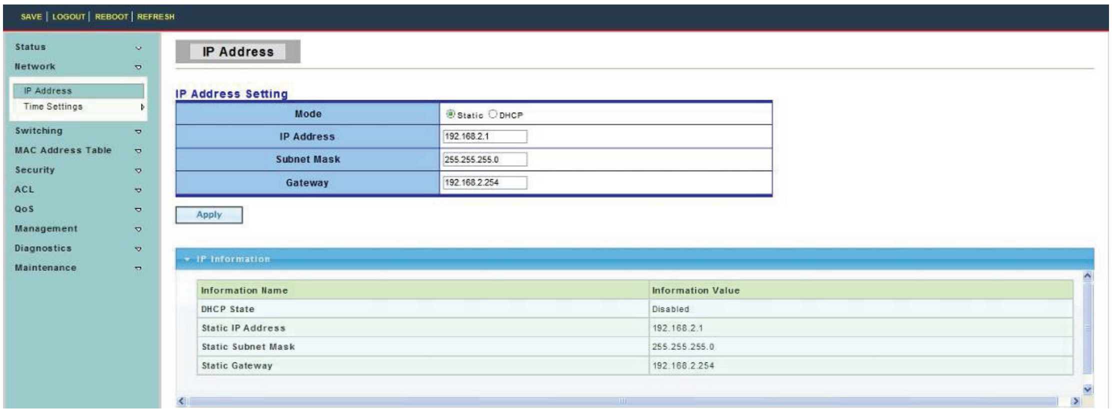
4.2 Network

Use the Network page to configure settings for the switch´s network interface.

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.



IP Address

IP Address Setting

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

IP Information

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

Mode: Select the mode of network connection.

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

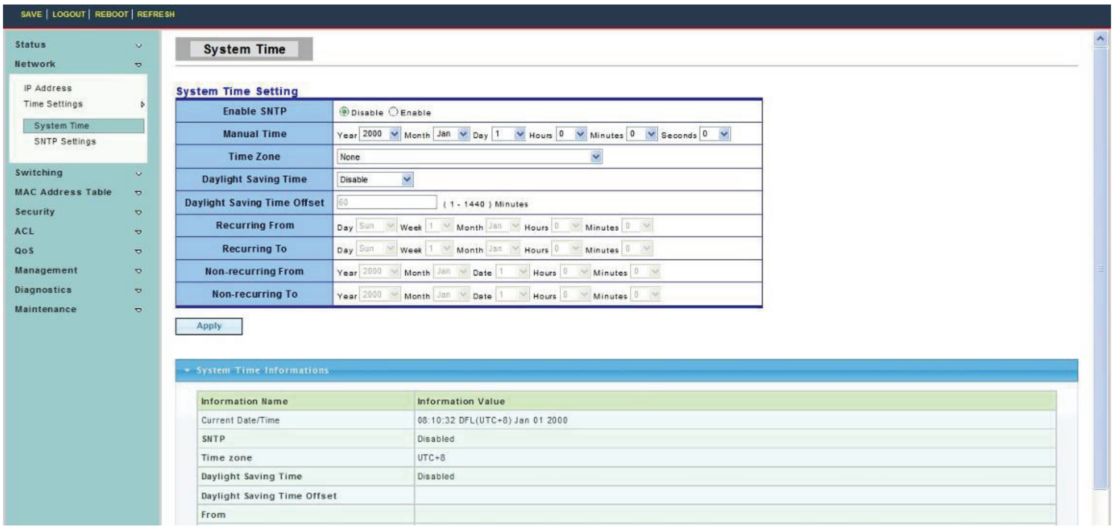
IP Address: If static mode is enabled, enter IP address in this field.
Subnet Mask: If static mode is enabled, enter subnet mask in this field.
Gateway: If static mode is enabled, enter gateway address in this field.

4.2.2 Time Settings

4.2.2.1 System Time

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

This page allow user to enable / disable the SNTP (Simple Network Time Protocol), set the time manually, adjust the time zone and enable or disable the daylight saving
it.



System Time

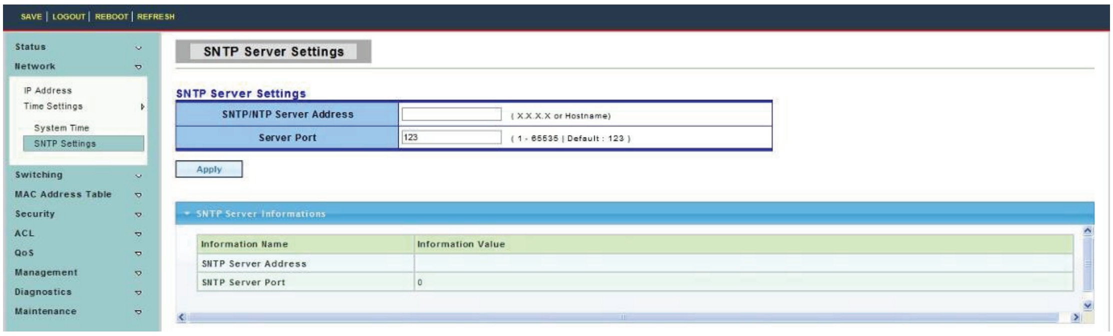
System Time Setting

Enable SNTP	● Disable ○ Enable
Manual Time	Year 2000 Month Jan Day 1 Hours 0 Minutes 0 Seconds 0
Time Zone	None
Daylight Saving Time	Disable
Daylight Saving Time Offset	60 (1 - 1440) Minutes
Recurring From	Day Sun Week 1 Month Jan Hours 0 Minutes 0
Recurring To	Day Sun Week 1 Month Jan Hours 0 Minutes 0
Non-recurring From	Year 2000 Month Jan Date 1 Hours 0 Minutes 0
Non-recurring To	Year 2000 Month Jan Date 1 Hours 0 Minutes 0

Information Name	Information Value
Current Date/Time	08:10:32 DFL(UTC+8) Jan 01 2000
SNTP	Disabled
Time zone	UTC+8
Daylight Saving Time	Disabled
Daylight Saving Time Offset	
From	

4.2.2.2 SNTP Settings

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



SNTP Server Settings

SNTP Server Settings

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

Information Name	Information Value
SNTP Server Address	
SNTP Server Port	0

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

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

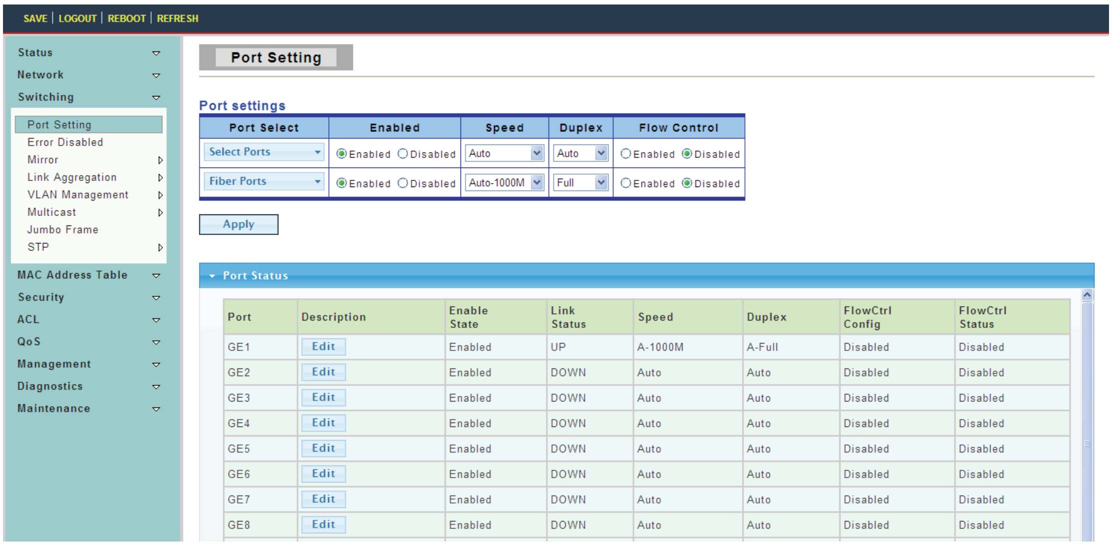
4.3 Switching

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

This page allow user to configure the port status, port speed and duplex mode.



Port settings

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

Port	Description	Enable State	Link Status	Speed	Duplex	FlowCtrl Config	FlowCtrl Status
GE1	Edit	Enabled	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.

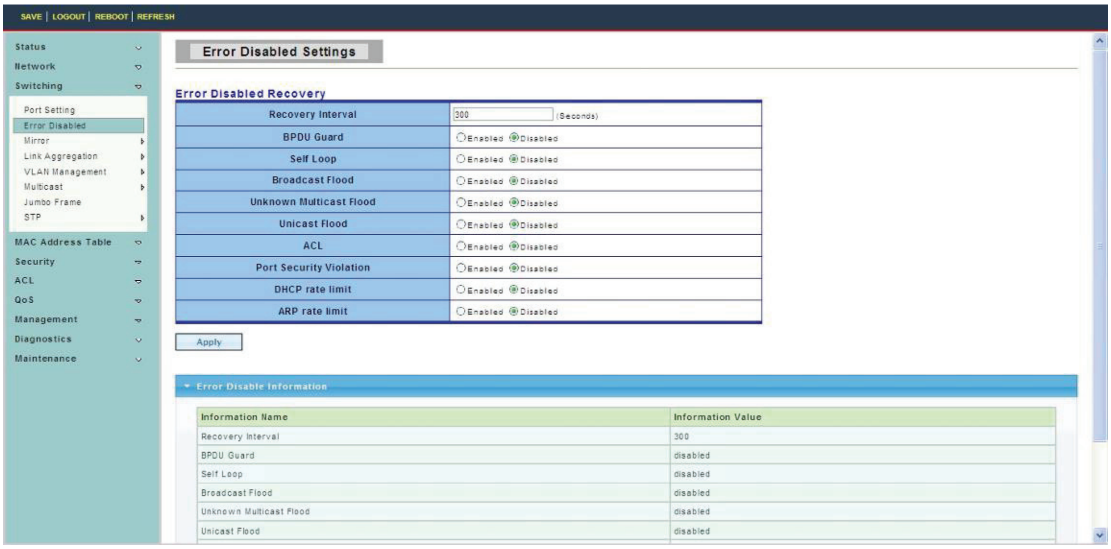
- Auto: Auto duplex with all capabilities.
- Full: Auto speed with full duplex ability only.
- Half: Auto speed with half duplex ability only.

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**



Error Disabled Settings

Error Disabled Recovery

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

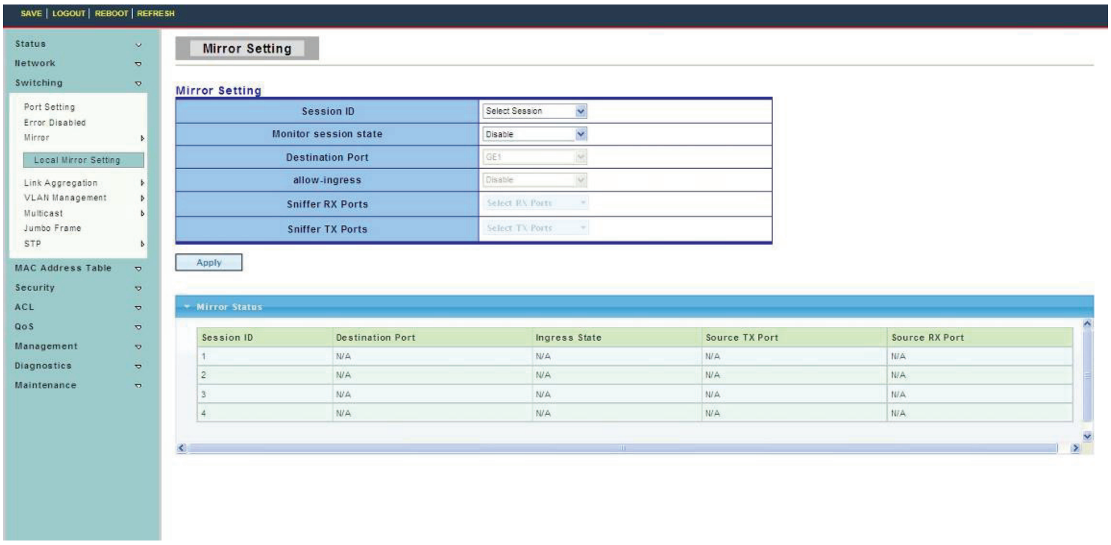
Error Disable Information

Information Name	Information Value
Recovery Interval	300
BPDU Guard	disabled
Self Loop	disabled
Broadcast Flood	disabled
Unknown Multicast Flood	disabled
Unicast Flood	disabled

4.3.3 Mirror

To display Local Mirror Setting web page, click **Switching > Mirror > Local Mirror Setting**

Port mirroring is copy the TX/RX data flow from the source port to the aiming port, commonly used in port mirroring.



Mirror Setting

Mirror Setting

Session ID	Select Session
Monitor session state	Disable
Destination Port	GE1
allow-ingress	Disable
Sniffer RX Ports	Select RX Ports
Sniffer TX Ports	Select TX Ports

Mirror Status

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

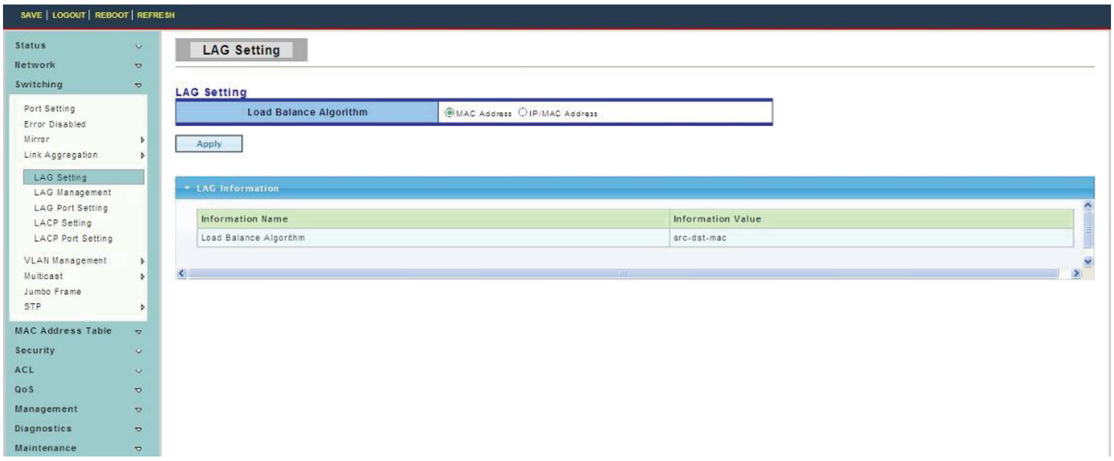
4.3.4 Link Aggregation

Link aggregation combine multiple Ethernet ports together to form a logical port, it supports 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.



LAG Setting

LAG Setting

Load Balance Algorithm	● MAC Address ○ IP/MAC Address

Apply

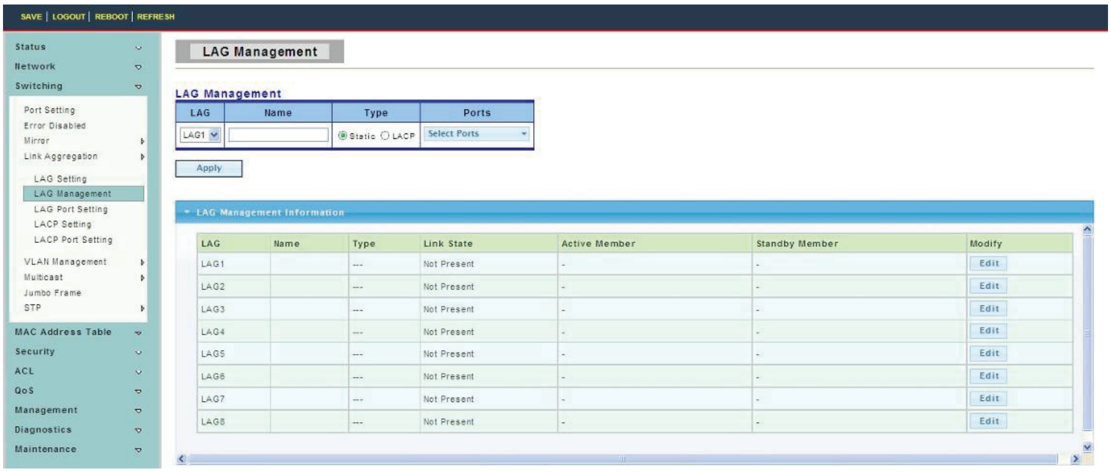
LAG Information

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

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, ports aggregation type and select member ports.



LAG Management

LAG Management

LAG	Name	Type	Ports
LAG1		● Static ○ LACP	Select Ports

Apply

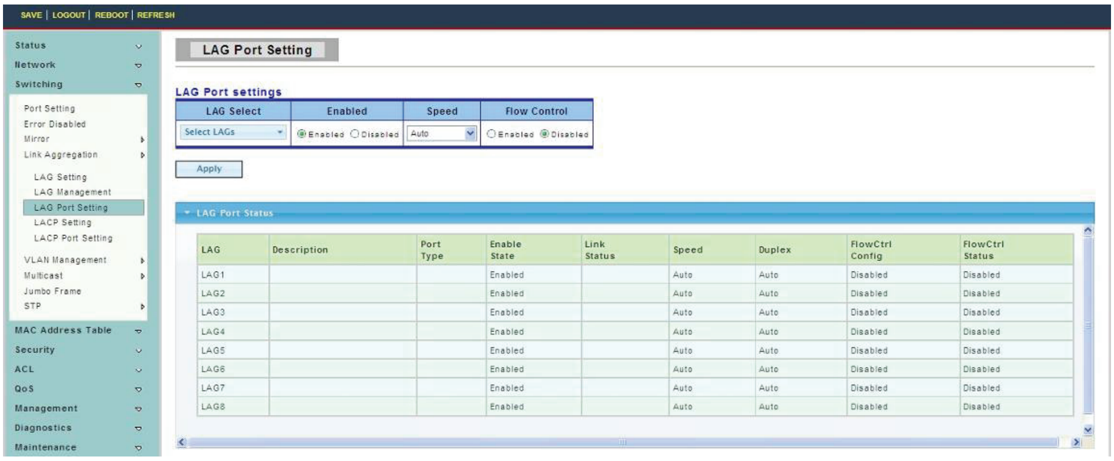
LAG Management Information

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

4.3.4.3 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 flow control function.



LAG Port settings

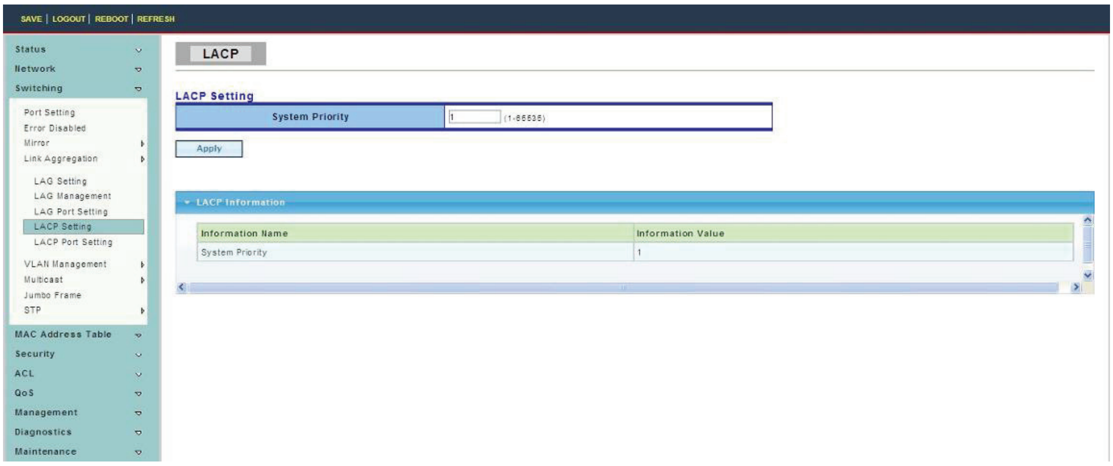
LAG Select	Enabled	Speed	Flow Control
Select LAGs	● Enabled ○ Disabled	Auto	○ Enabled ● Disabled

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

4.3.4.4 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.



LACP Setting

System Priority	1 (1-65535)

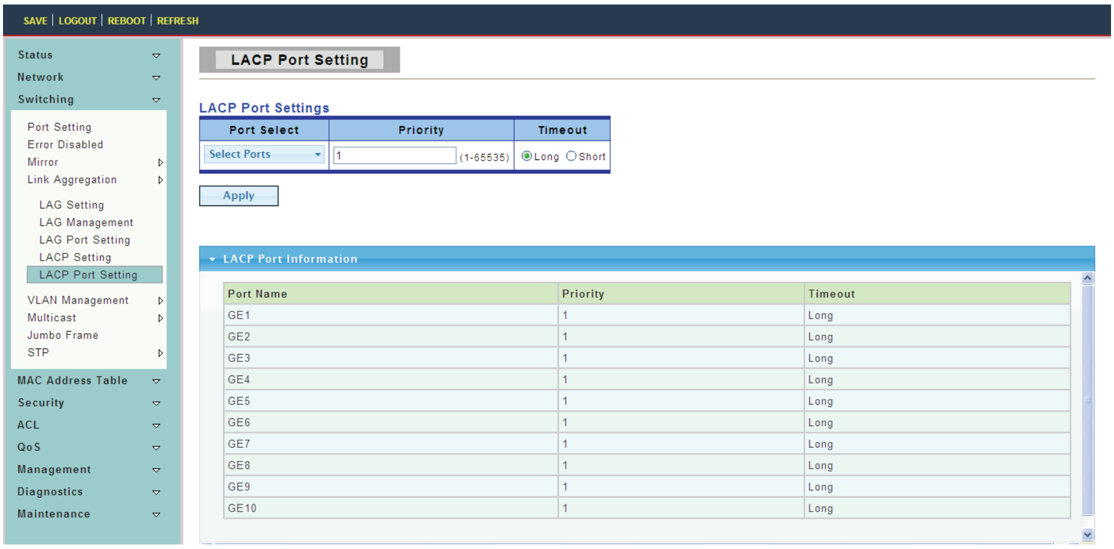
Information Name	Information Value
System Priority	1

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)	● Long ○ Short

LACP Port Information

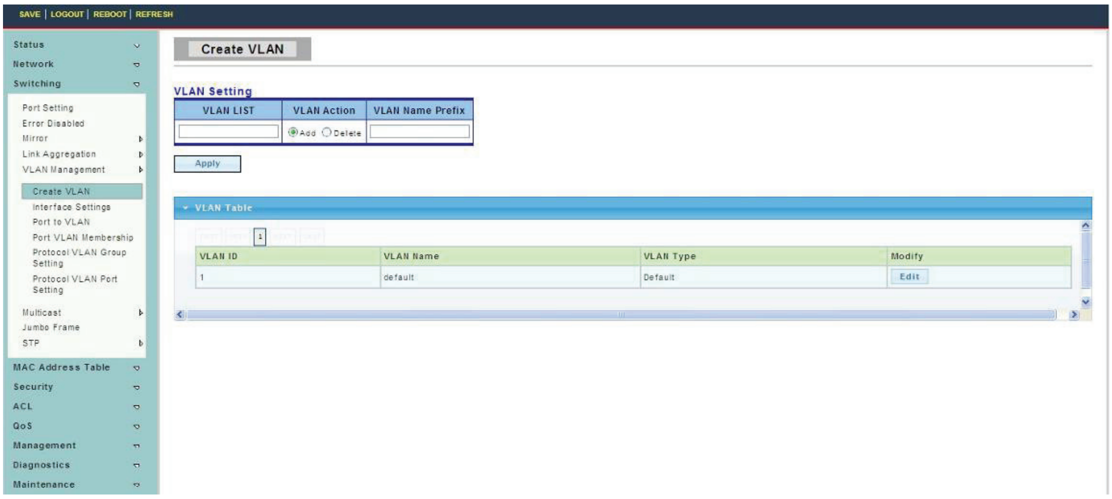
Port Name	Priority	Timeout
GE1	1	Long
GE2	1	Long
GE3	1	Long
GE4	1	Long
GE5	1	Long
GE6	1	Long
GE7	1	Long
GE8	1	Long
GE9	1	Long
GE10	1	Long

4.3.5 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
	● Add ○ Delete	

VLAN Table

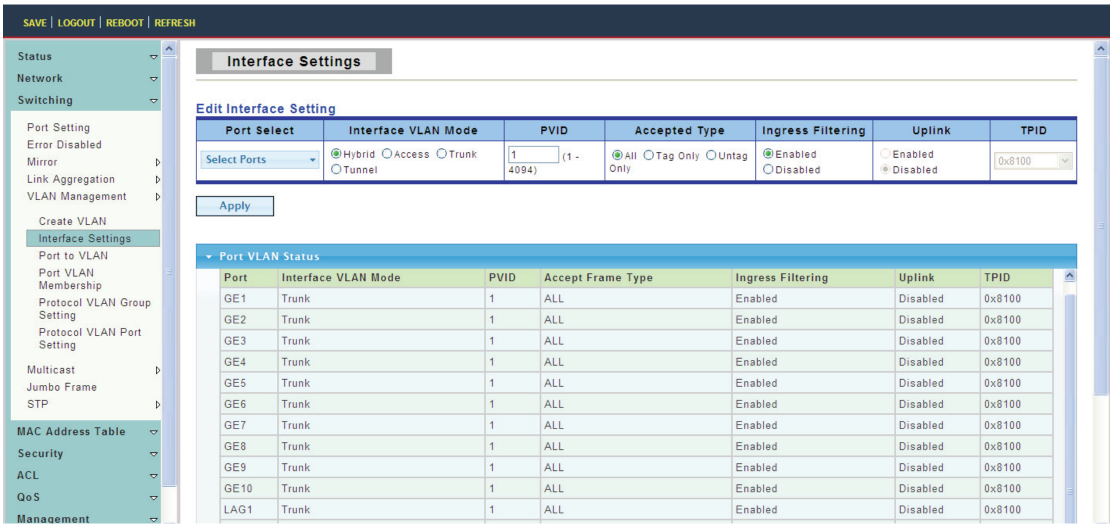
VLAN ID	VLAN Name	VLAN Type	Modify
1	default	Default	Edit

VLAN LIST: VLAN LIST for the new VLAN.
VLAN Action: Add or delete VLAN.
VLAN Name Prefix: VLAN Name Prefix for the new VLAN.

4.3.5.2 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, the port VLAN ID and whether the port should have a tag.



Edit Interface Setting

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

Port VLAN Status

Port	Interface VLAN Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
GE1	Trunk	1	ALL	Enabled	Disabled	0x8100
GE2	Trunk	1	ALL	Enabled	Disabled	0x8100
GE3	Trunk	1	ALL	Enabled	Disabled	0x8100
GE4	Trunk	1	ALL	Enabled	Disabled	0x8100
GE5	Trunk	1	ALL	Enabled	Disabled	0x8100
GE6	Trunk	1	ALL	Enabled	Disabled	0x8100
GE7	Trunk	1	ALL	Enabled	Disabled	0x8100
GE8	Trunk	1	ALL	Enabled	Disabled	0x8100
GE9	Trunk	1	ALL	Enabled	Disabled	0x8100
GE10	Trunk	1	ALL	Enabled	Disabled	0x8100
LAG1	Trunk	1	ALL	Enabled	Disabled	0x8100

Port Select : Select one or multiple ports to configure.

Interface VLAN Mode: VLAN port mode

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.

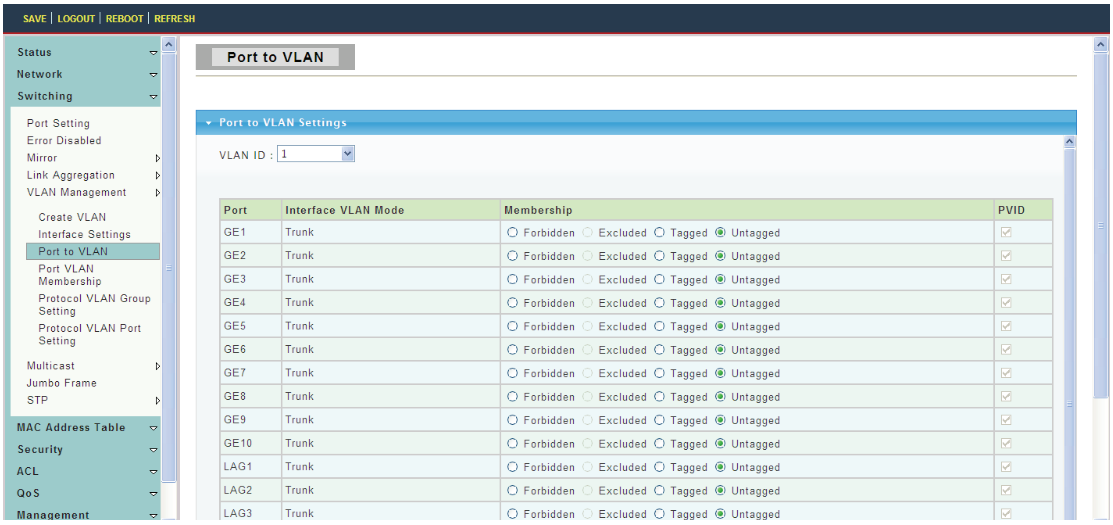
Ingress Filtering: Choose filter port open and close.

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**

Select the port's different behaviors when it works under the VLAN.



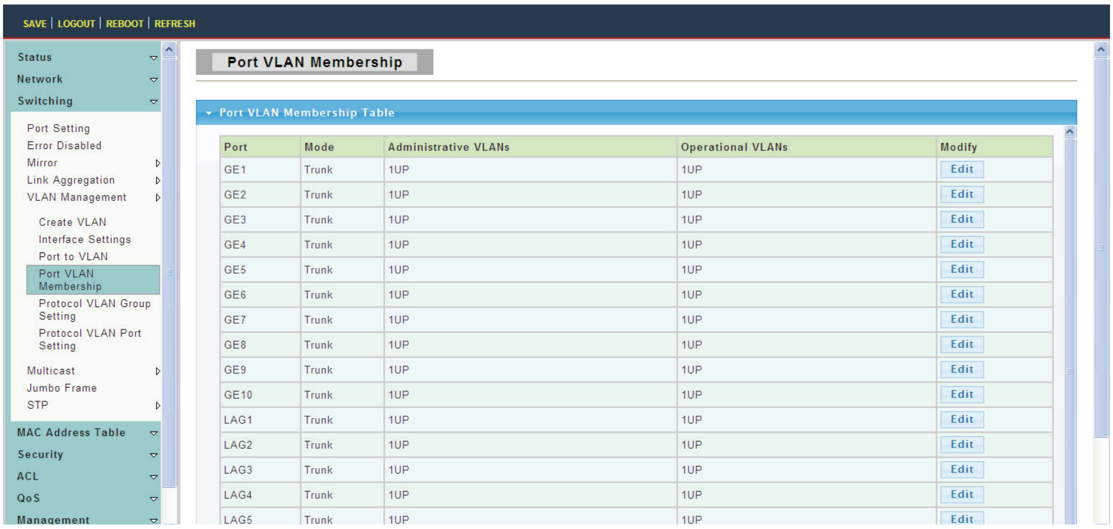
Port to VLAN Settings

VLAN ID : 1

Port	Interface VLAN Mode	Membership	PVID
GE1	Trunk	○ Forbidden ○ Excluded ○ Tagged ● Untagged	☑
GE2	Trunk	○ Forbidden ○ Excluded ○ Tagged ● Untagged	☑
GE3	Trunk	○ Forbidden ○ Excluded ○ Tagged ● Untagged	☑
GE4	Trunk	○ Forbidden ○ Excluded ○ Tagged ● Untagged	☑
GE5	Trunk	○ Forbidden ○ Excluded ○ Tagged ● Untagged	☑
GE6	Trunk	○ Forbidden ○ Excluded ○ Tagged ● Untagged	☑
GE7	Trunk	○ Forbidden ○ Excluded ○ Tagged ● Untagged	☑
GE8	Trunk	○ Forbidden ○ Excluded ○ Tagged ● Untagged	☑
GE9	Trunk	○ Forbidden ○ Excluded ○ Tagged ● Untagged	☑
GE10	Trunk	○ Forbidden ○ Excluded ○ Tagged ● Untagged	☑
LAG1	Trunk	○ Forbidden ○ Excluded ○ Tagged ● Untagged	☑
LAG2	Trunk	○ Forbidden ○ Excluded ○ Tagged ● Untagged	☑
LAG3	Trunk	○ Forbidden ○ Excluded ○ Tagged ● Untagged	☑

4.3.5.4 Port VLAN Membership

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



Port VLAN Membership

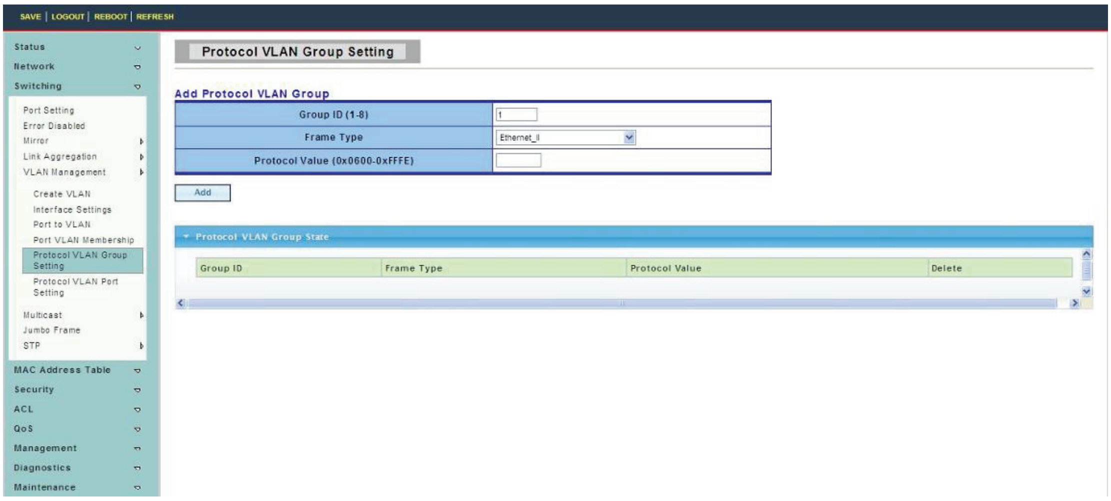
Port VLAN Membership Table

Port	Mode	Administrative VLANs	Operational VLANs	Modify
GE1	Trunk	1UP	1UP	Edit
GE2	Trunk	1UP	1UP	Edit
GE3	Trunk	1UP	1UP	Edit
GE4	Trunk	1UP	1UP	Edit
GE5	Trunk	1UP	1UP	Edit
GE6	Trunk	1UP	1UP	Edit
GE7	Trunk	1UP	1UP	Edit
GE8	Trunk	1UP	1UP	Edit
GE9	Trunk	1UP	1UP	Edit
GE10	Trunk	1UP	1UP	Edit
LAG1	Trunk	1UP	1UP	Edit
LAG2	Trunk	1UP	1UP	Edit
LAG3	Trunk	1UP	1UP	Edit
LAG4	Trunk	1UP	1UP	Edit
LAG5	Trunk	1UP	1UP	Edit

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 sets the same type as a group and transmit it in the specific VLAN.



Protocol VLAN Group Setting

Add Protocol VLAN Group

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

Protocol VLAN Group State

Group ID	Frame Type	Protocol Value	Delete

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

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.

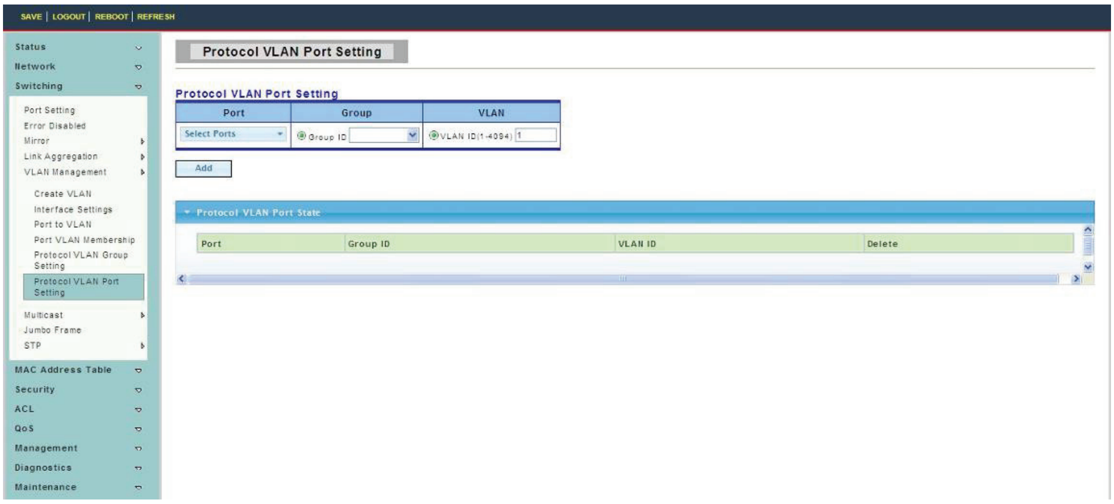
- Ethernet_II: packet type is Ethernet version 2.
- IEEE802.3_LLC_Other: packet type is 802.3 packet with LLC other header.
- RFC_1042: packet type is RFC 1042 packet.

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

4.3.5.6 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.



Protocol VLAN Port Setting

Protocol VLAN Port Setting

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

Protocol VLAN Port State

Port	Group ID	VLAN ID	Delete

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.

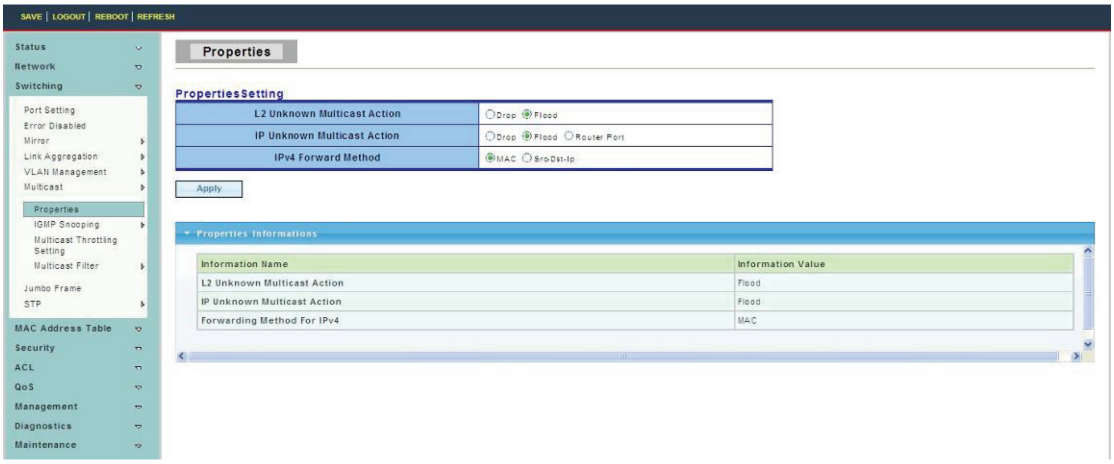
VLAN: Click the corresponding radio button to select a previously configured VLAN ID or VLAN Name.

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.



Properties

PropertiesSetting

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

Properties Informations

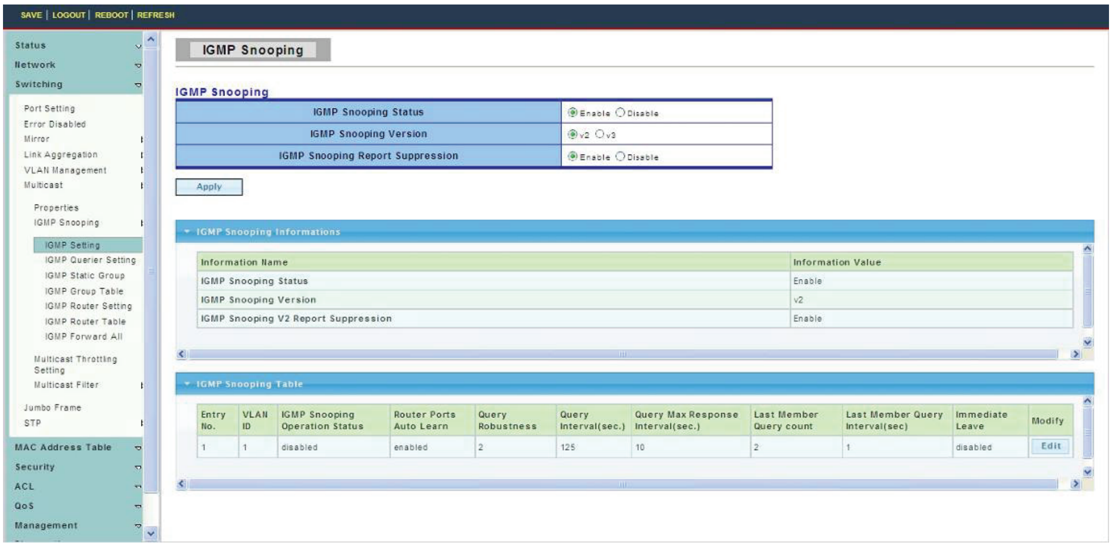
Information Name	Information Value
L2 Unknown Multicast Action	Flood
IP Unknown Multicast Action	Flood
Forwarding Method For IPv4	MAC

4.3.6.2 IGMP Snooping

Use the Switching pages to configure settings for the switch network interface.

1. IGMP Setting

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



IGMP Snooping

IGMP Snooping

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

IGMP Snooping Informations

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

IGMP Snooping Table

Entry No.	VLAN ID	IGMP Snooping Operation Status	Router Ports Auto Learn	Query Robustness	Query Interval(sec.)	Query Max Response Interval(sec.)	Last Member Query count	Last Member Query Interval(sec)	Immediate Leave	Modify
1	1	disabled	enabled	2	125	10	2	1	disabled	Edit

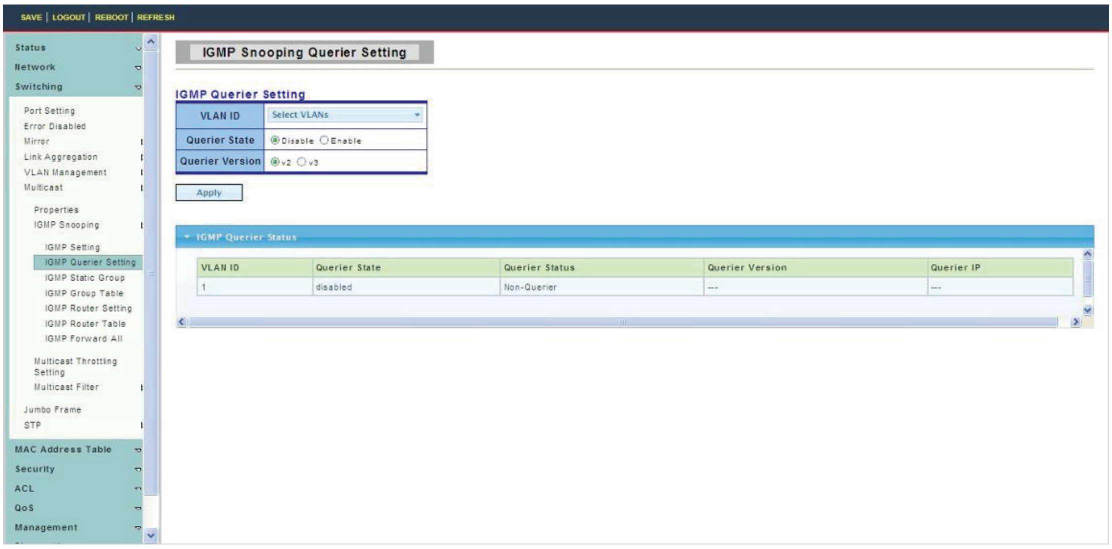
IGMP Snooping: Select IGMP Snooping enable or disable.

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

IGMP Snooping Report Suppression: Select 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**



IGMP Snooping Querier Setting

IGMP Querier Setting

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

IGMP Querier Status

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

VLAN ID: Select the VLANs to configure.

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

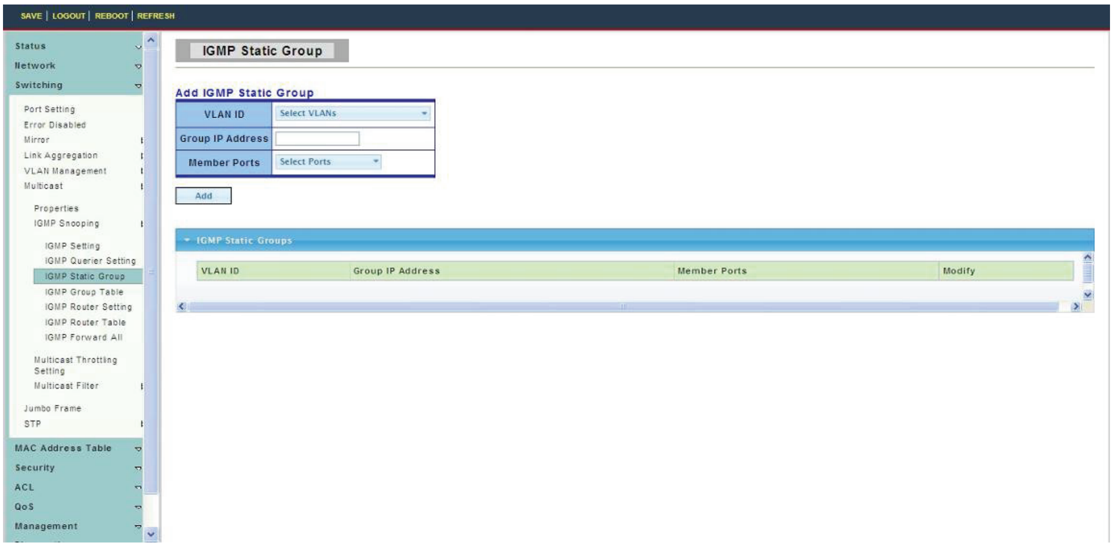
- Enable: Enable IGMP Querier Election.
- Disable: Disable IGMP Querier Election.

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.



IGMP Static Group

Add IGMP Static Group

VLAN ID	Select VLANs
Group IP Address	
Member Ports	Select Ports

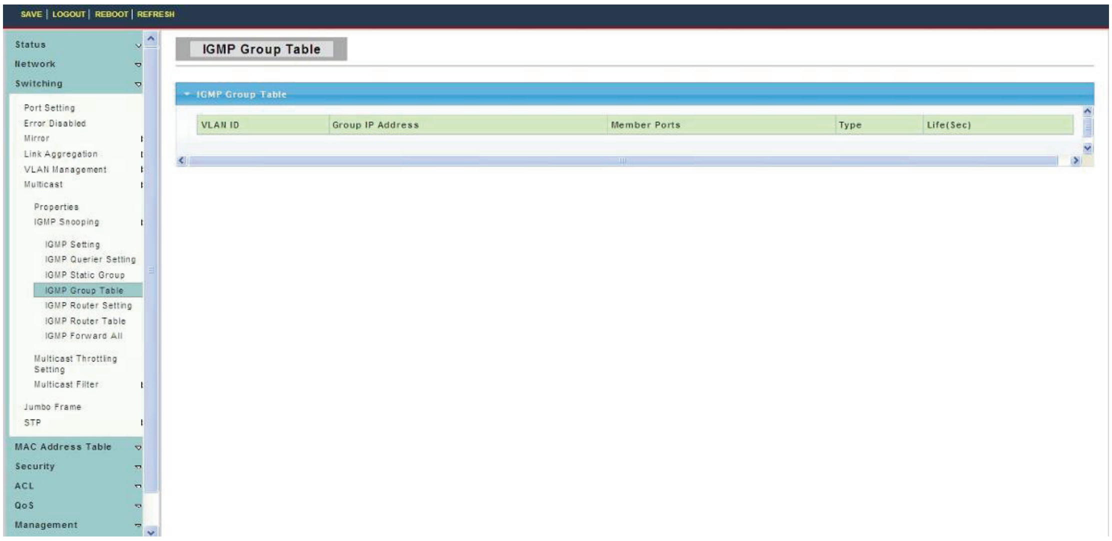
IGMP Static Groups

VLAN ID	Group IP Address	Member Ports	Modify

4. 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.



IGMP Group Table

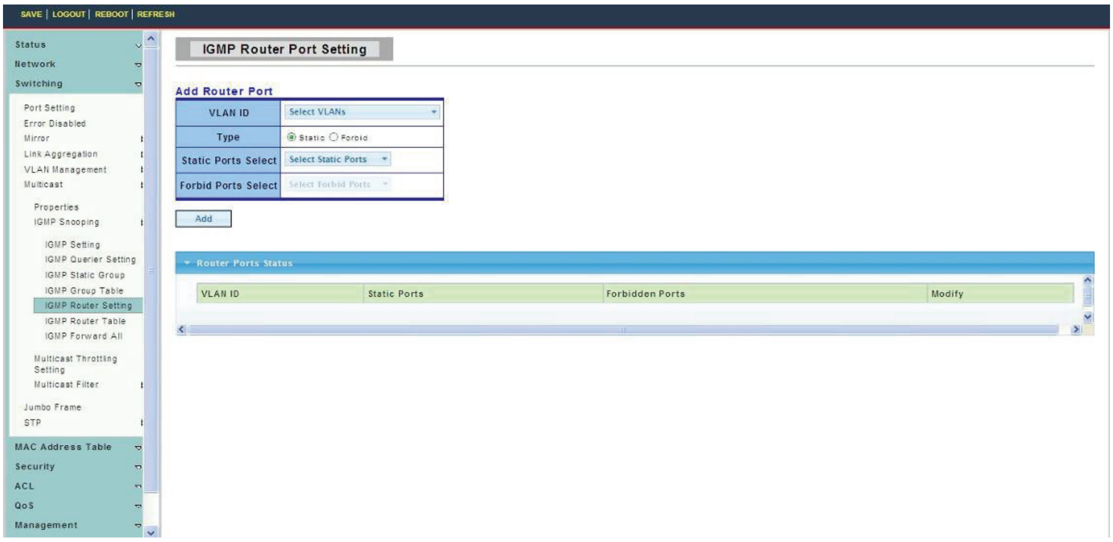
IGMP Group Table

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

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.



IGMP Router Port Setting

Add Router Port

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

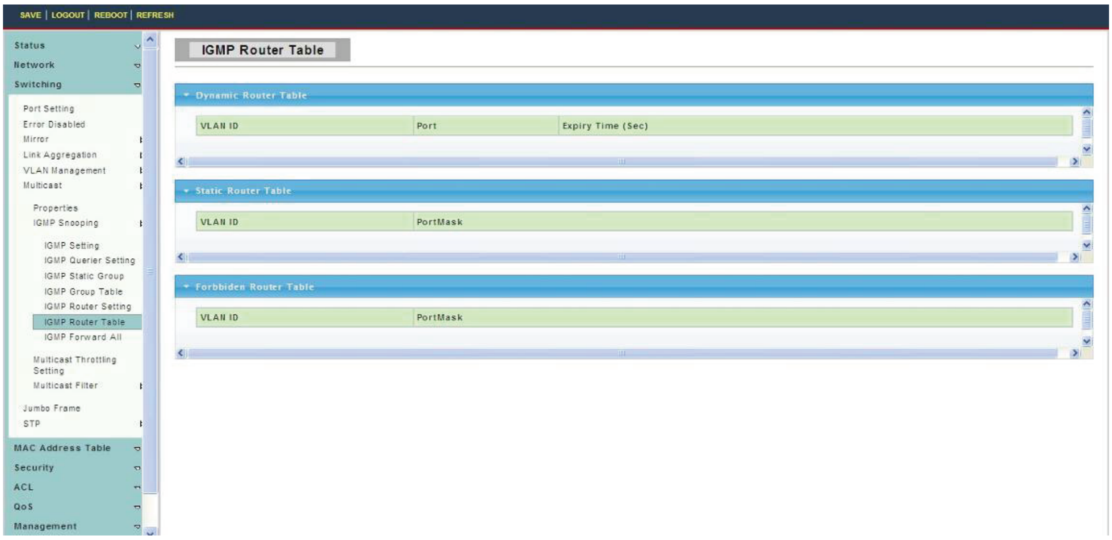
Router Ports Status

VLAN ID	Static Ports	Forbidden Ports	Modify

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.



IGMP Router Table

Dynamic Router Table

VLAN ID	Port	Expiry Time (Sec)

Static Router Table

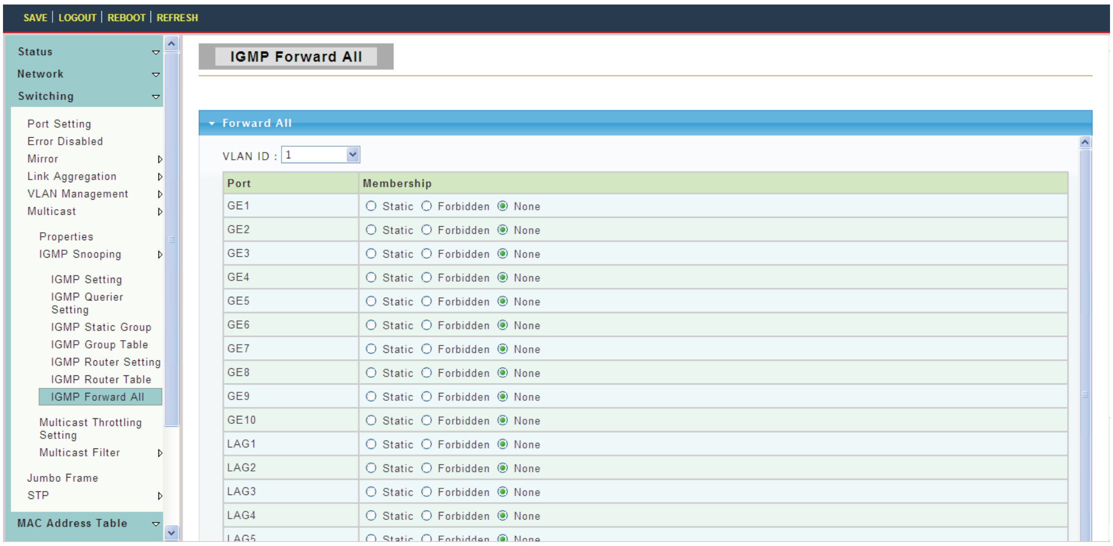
VLAN ID	PortMask

Forbidden Router Table

VLAN ID	PortMask

7. IGMP Forward All

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



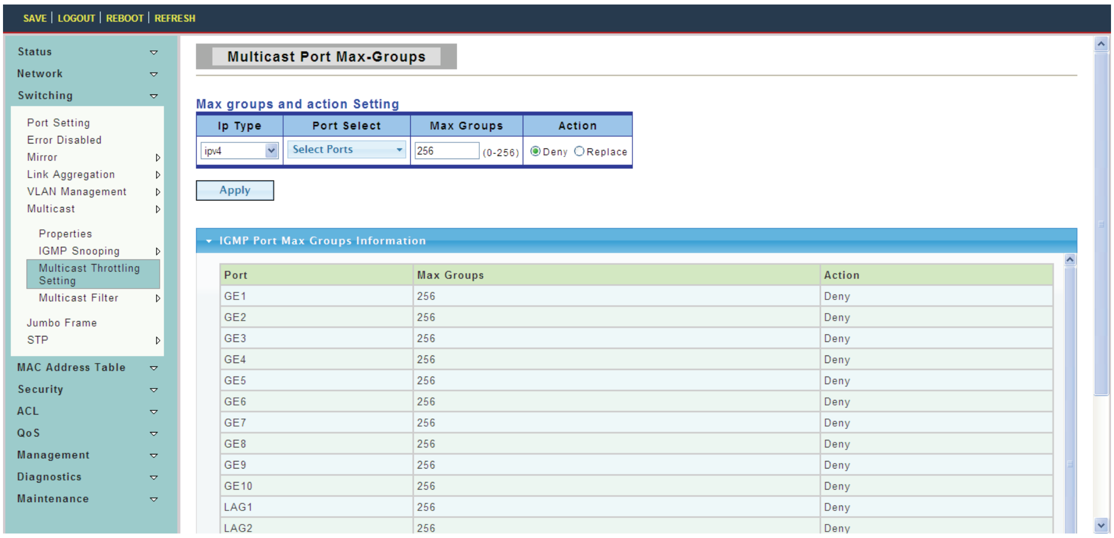
VLAN ID : 1

Port	Membership
GE1	○ Static ○ Forbidden ● None
GE2	○ Static ○ Forbidden ● None
GE3	○ Static ○ Forbidden ● None
GE4	○ Static ○ Forbidden ● None
GE5	○ Static ○ Forbidden ● None
GE6	○ Static ○ Forbidden ● None
GE7	○ Static ○ Forbidden ● None
GE8	○ Static ○ Forbidden ● None
GE9	○ Static ○ Forbidden ● None
GE10	○ Static ○ Forbidden ● None
LAG1	○ Static ○ Forbidden ● None
LAG2	○ Static ○ Forbidden ● None
LAG3	○ Static ○ Forbidden ● None
LAG4	○ Static ○ Forbidden ● None
LAG5	○ Static ○ Forbidden ● None

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
ipv4	Select Ports	256 (0-256)	● Deny ○ Replace

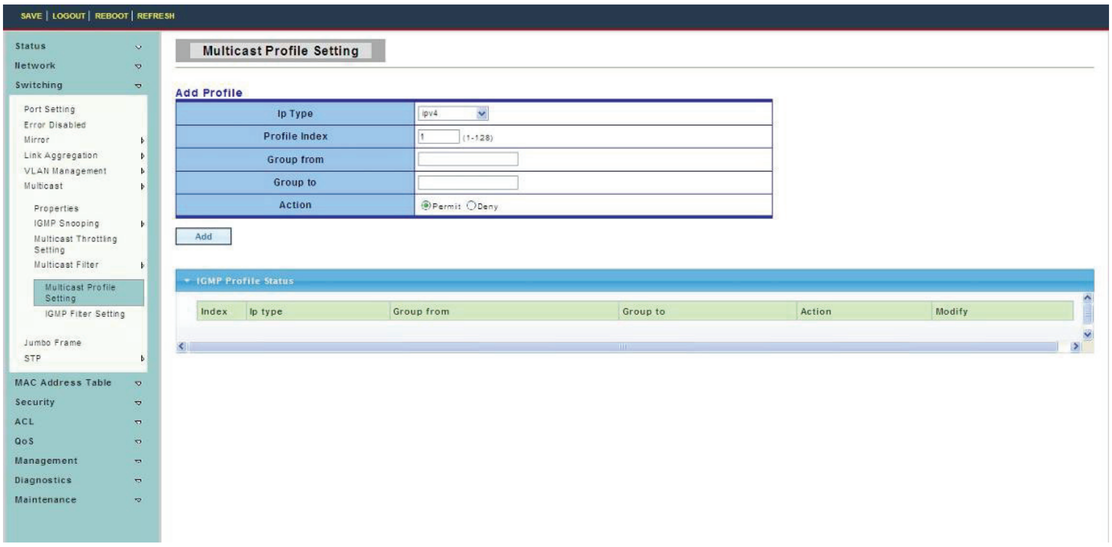
Port	Max Groups	Action
GE1	256	Deny
GE2	256	Deny
GE3	256	Deny
GE4	256	Deny
GE5	256	Deny
GE6	256	Deny
GE7	256	Deny
GE8	256	Deny
GE9	256	Deny
GE10	256	Deny
LAG1	256	Deny
LAG2	256	Deny

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	ipv4
Profile Index	1 (1-128)
Group from	
Group to	
Action	● Permit ○ Deny

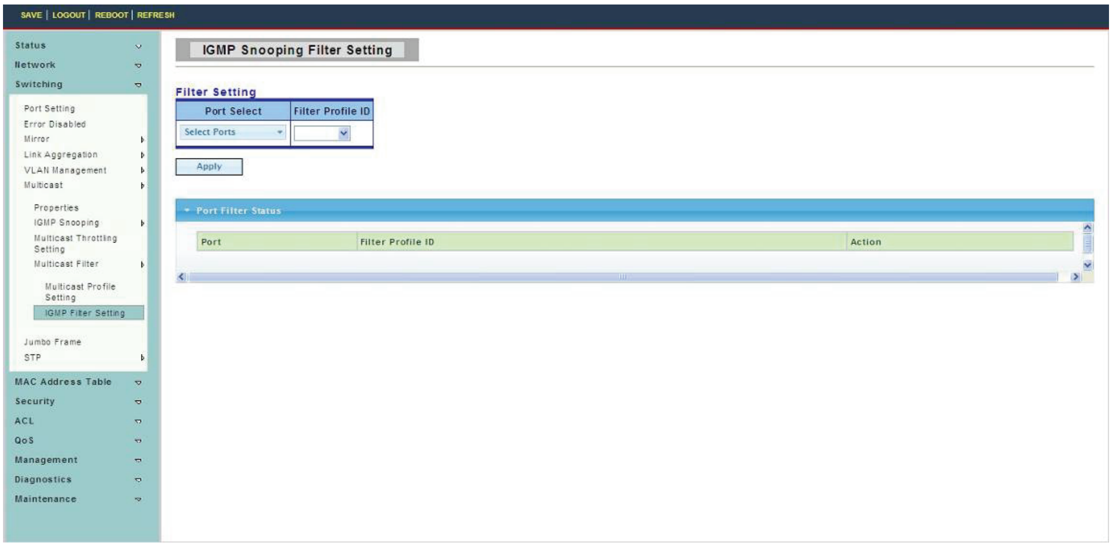
IGMP Profile Status

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 the port to bind to that instance.



IGMP Snooping Filter Setting

Filter Setting

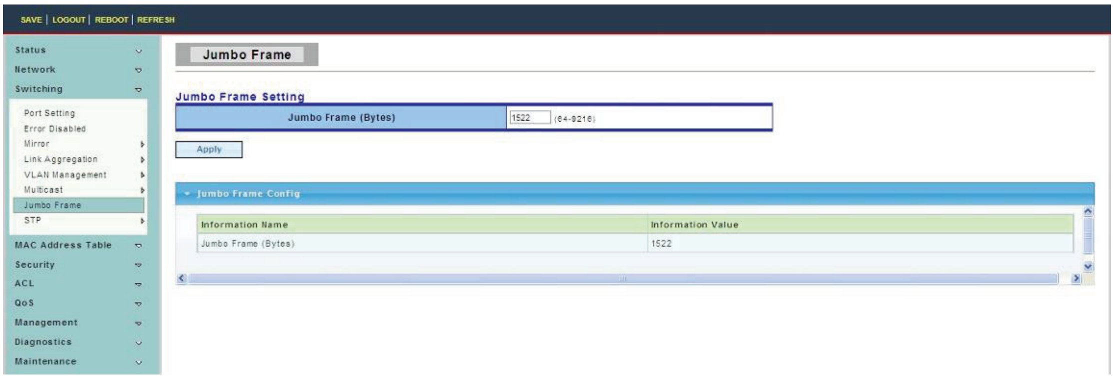
Port Select	Filter Profile ID
Select Ports	

Port Filter Status

Port	Filter Profile ID	Action

4.3.7 Jumbo Frame

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



Jumbo Frame

Jumbo Frame Setting

Jumbo Frame (Bytes)	1522 (64-9216)

Jumbo Frame Config

Information Name	Information Value
Jumbo Frame (Bytes)	1522

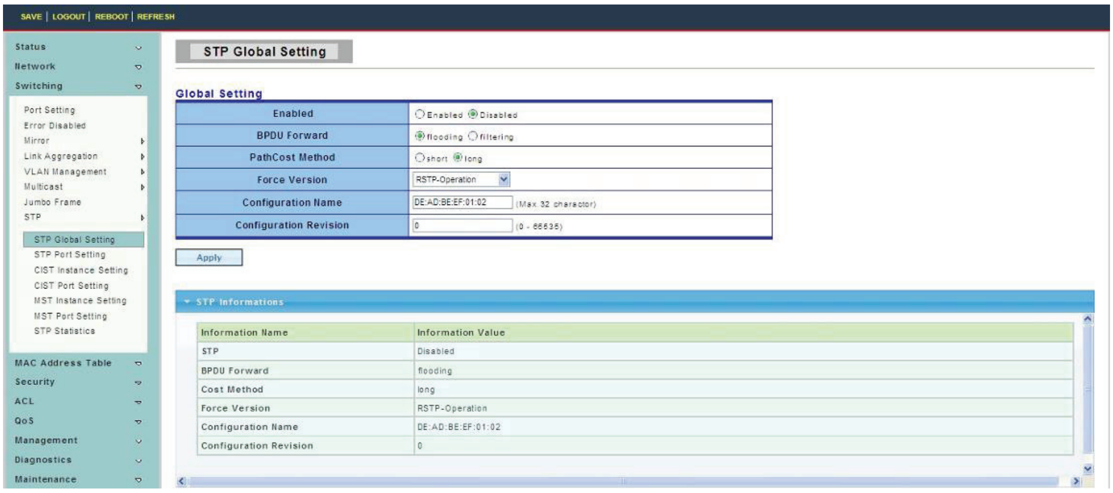
Jumbo Frame: Jumbo frame size. The valid range is 0 bytes – 9216 bytes.

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**



STP Global Setting

Global Setting

Enabled	○ Enabled ● Disabled
BPDU Forward	● flooding ○ filtering
PathCost Method	○ short ● long
Force Version	RSTP-Operation
Configuration Name	DE:AD:BE:EF:01:02 (Max 32 charector)
Configuration Revision	0 (0 - 65535)

STP Informations

Information Name	Information Value
STP	Disabled
BPDU Forward	flooding
Cost Method	long
Force Version	RSTP-Operation
Configuration Name	DE:AD:BE:EF:01:02
Configuration Revision	0

Enabled: Set the STP status to be enable/disable on the Switch.

BPDU Forward: Choose BPDU packets is a flood or filtering

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

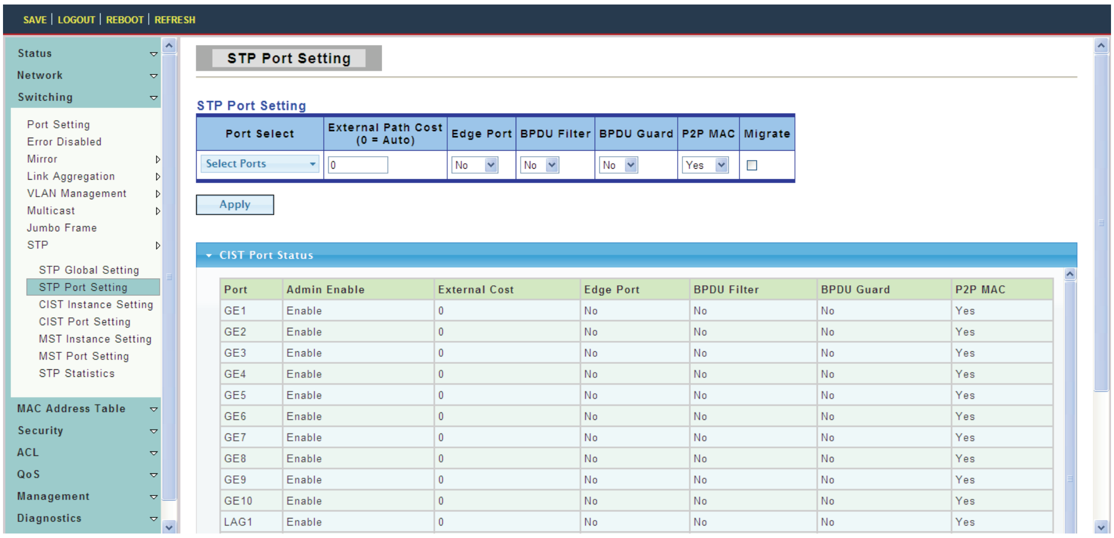
Force Version: Select the operating mode of STP.

- 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**



STP Port Setting

STP Port Setting

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

CIST Port Status

Port	Admin Enable	External Cost	Edge Port	BPDU Filter	BPDU Guard	P2P MAC
GE1	Enable	0	No	No	No	Yes
GE2	Enable	0	No	No	No	Yes
GE3	Enable	0	No	No	No	Yes
GE4	Enable	0	No	No	No	Yes
GE5	Enable	0	No	No	No	Yes
GE6	Enable	0	No	No	No	Yes
GE7	Enable	0	No	No	No	Yes
GE8	Enable	0	No	No	No	Yes
GE9	Enable	0	No	No	No	Yes
GE10	Enable	0	No	No	No	Yes
LAG1	Enable	0	No	No	No	Yes

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

External Path Cost: set the port’s contribution, when it is the Root Port, 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.

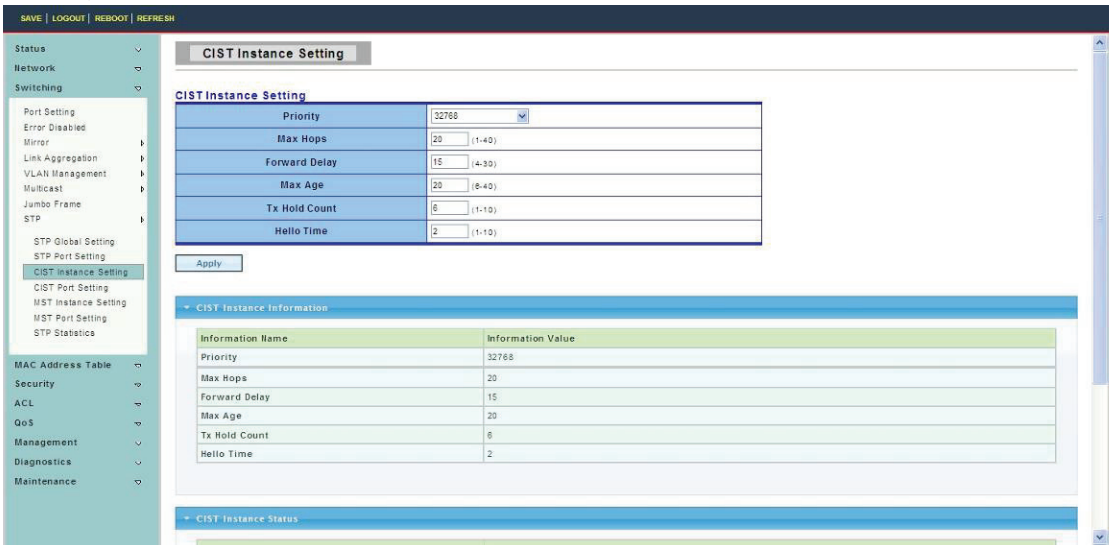
P2P MAC: Set the Point-to-Point port configuration.

- 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**



CIST Instance Setting

CIST Instance Setting

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

CIST Instance Information

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.

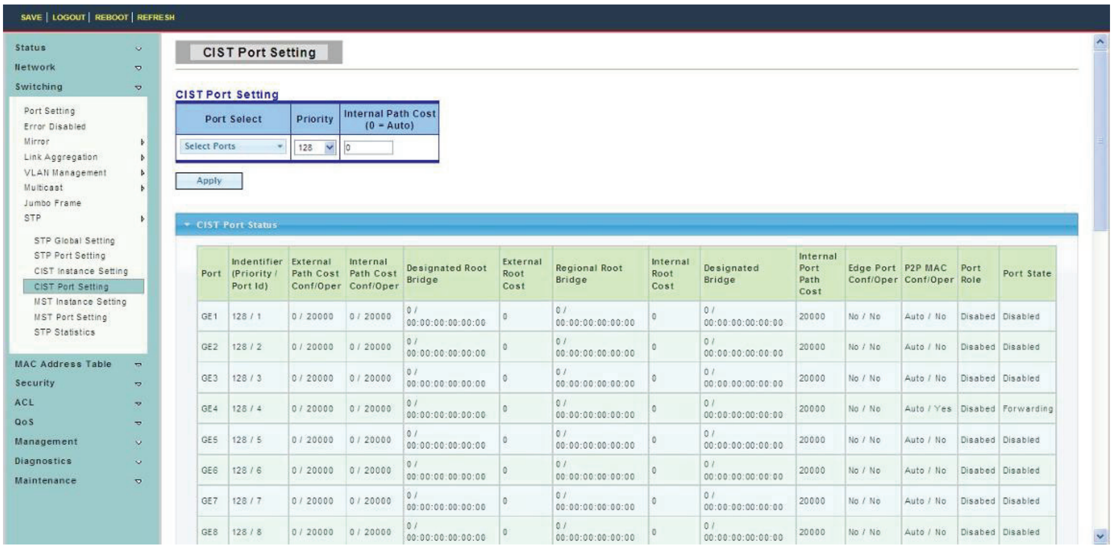
Max Age: Set the time any switch should wait before trying to change the STP topology after unhearing Hello BPDU.

Tx Hold Count: Set the Transmit Hold Count used to limit BPDIU 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

CIST Port Status

Port	Indentifier (Priority / Port Id)	External Path Cost Conf/Oper	Internal Path Cost Conf/Oper	Designated Root Bridge	External Root Cost	Regional Root Bridge	Internal Root Cost	Designated Bridge	Internal Port Path Cost	Edge Port Conf/Oper	P2P MAC Conf/Oper	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	Disabed	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	Disabed	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	Disabed	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	Disabed	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	Disabed	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	Disabed	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	Disabed	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	Disabed	Disabled

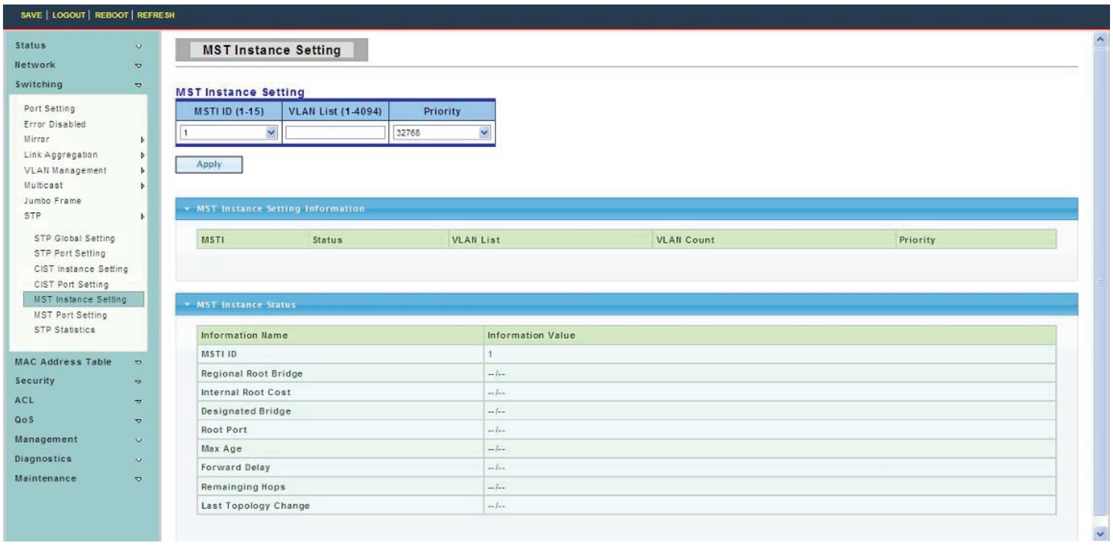
Port Select : Select the port list to specify which ports should apply this setting.

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

MST Instance Setting

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

MST Instance Setting Information

MSTI	Status	VLAN List	VLAN Count	Priority

MST Instance Status

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

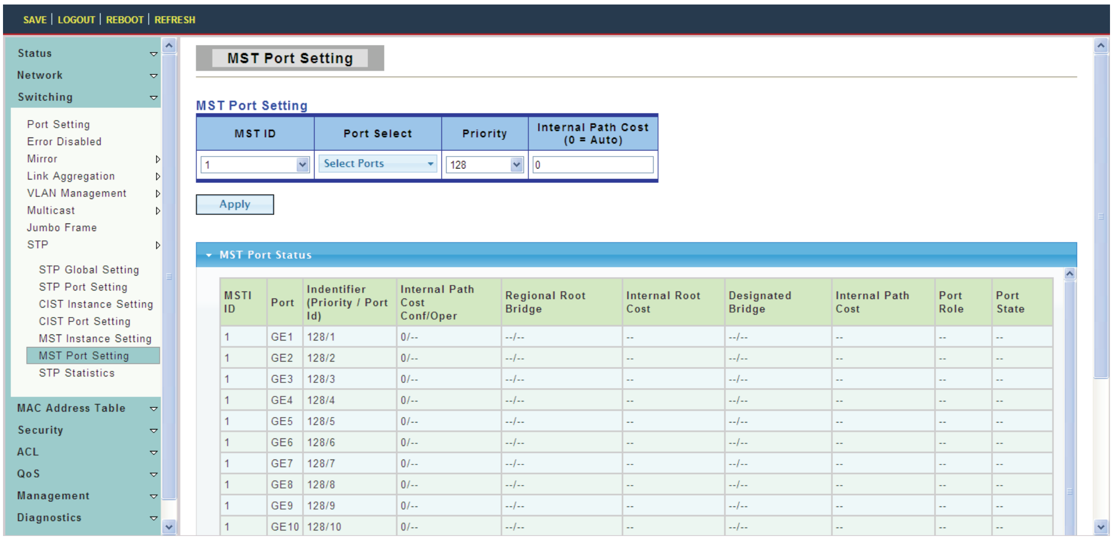
MSTI ID: Set the MSTI ID to specify the MST instance.

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 Port Setting

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

MST Port Status

MSTI ID	Port	Indentifier (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.

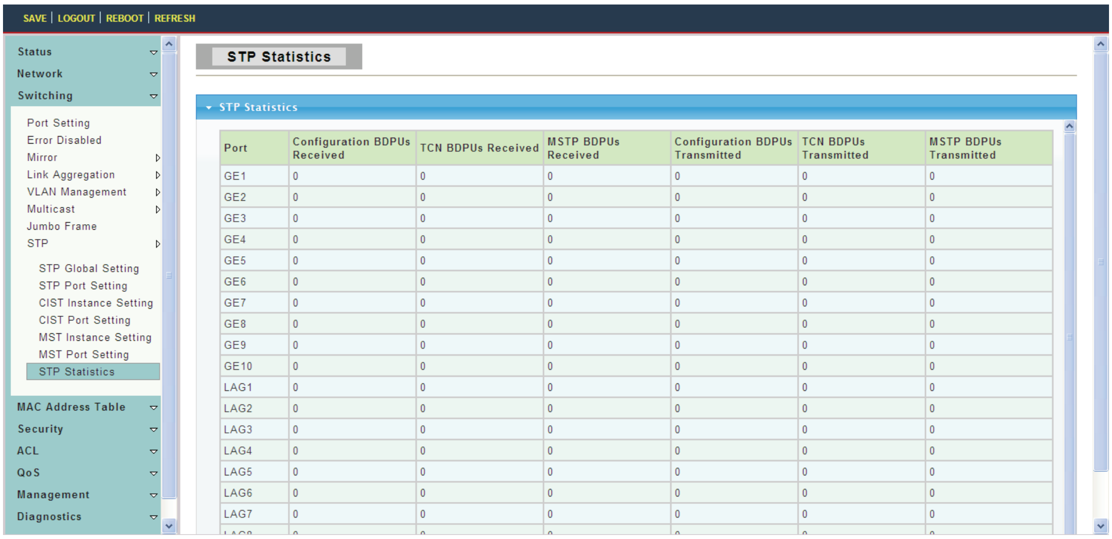
Port Select: Select the port list to specify which ports should apply this setting.

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

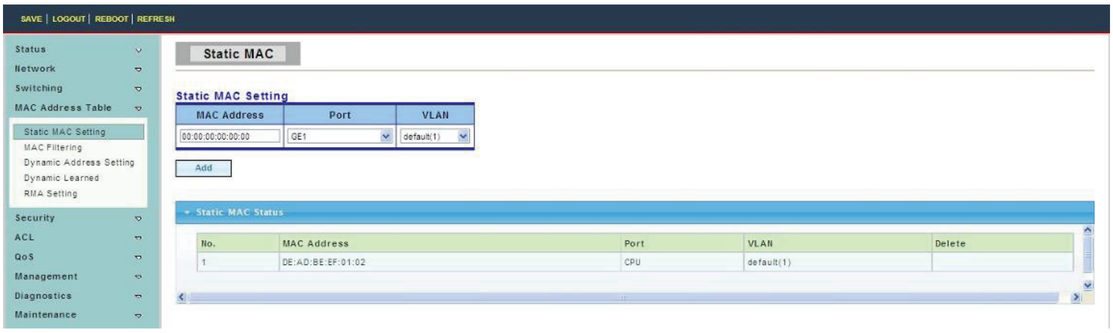
STP Statistics

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
LAG8	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**



Static MAC

Static MAC Setting

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

Static MAC Status

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

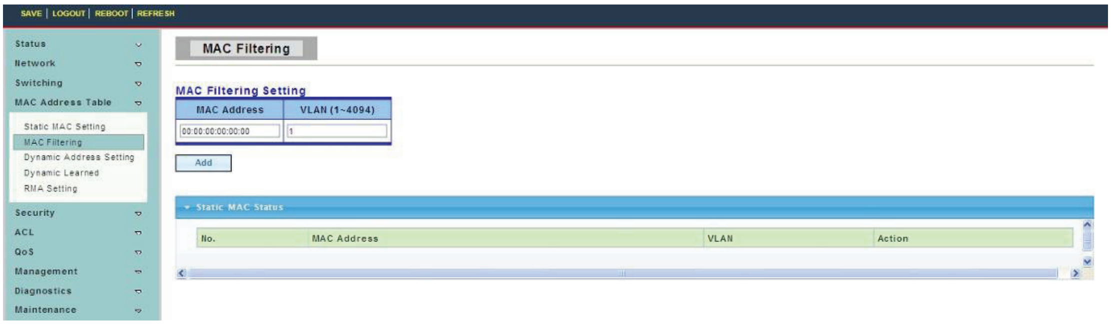
MAC Address: The MAC address to which packets will be statically forwarded. If type is unicast, enter unicast MAC address in this field; if type is multicast, enter multicast MAC address in this field.

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

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

4.4.2 MAC Filtering

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



MAC Filtering

MAC Filtering Setting

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

Static MAC Status

No.	MAC Address	VLAN	Action

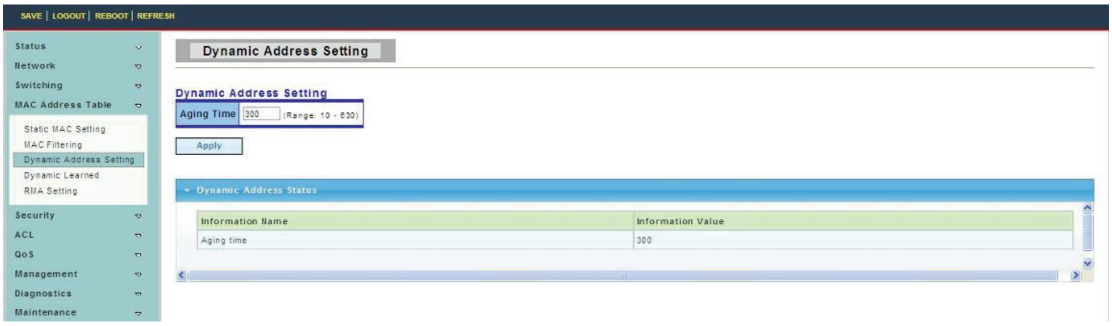
MAC Address: The MAC address to which packets will be filtered. This must be a unicast MAC address.

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

4.4.3 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



Dynamic Address Setting

Dynamic Address Setting

Aging Time 300 (Range: 10 - 630)

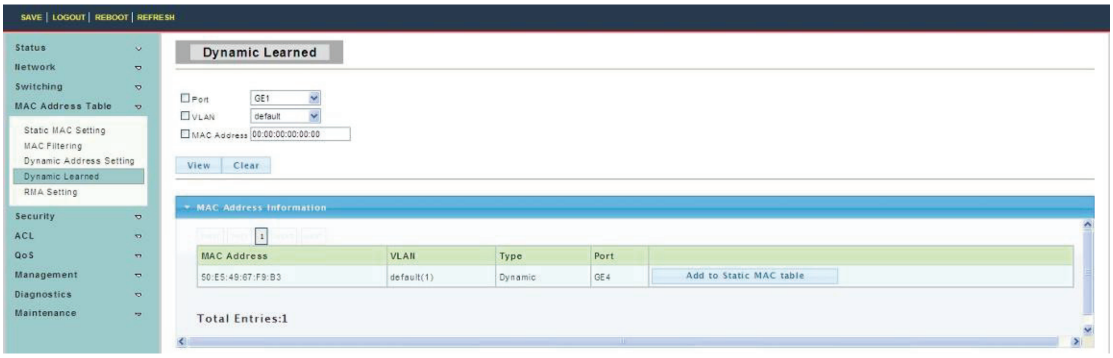
Dynamic Address Status

Information Name	Information Value
Aging time	300

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**



Dynamic Learned

□ Port GE1

□ VLAN default

□ MAC Address 00:00:00:00:00:00

MAC Address Information

MAC Address	VLAN	Type	Port	
50:E5:49:67:F9:B3	default(1)	Dynamic	GE4	Add to Static MAC table

Total Entries:1

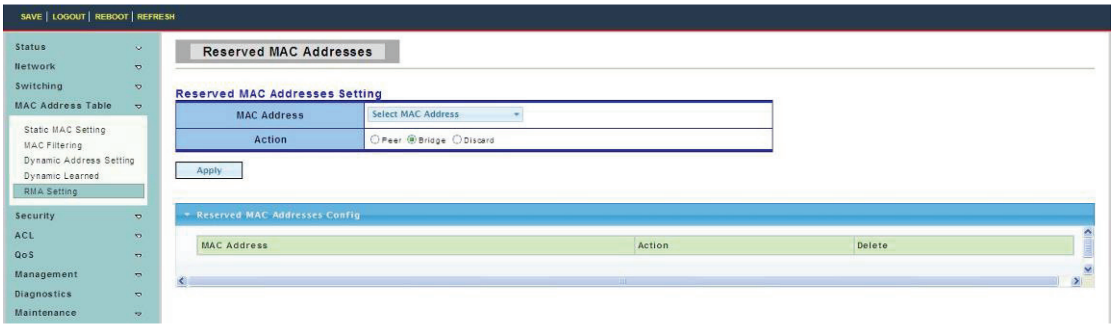
Port: Select the port number to show or clear dynamic MAC entries. If not select any port, VLAN and MAC address, the whole dynamic MAC table will be displayed or cleared.

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**



Reserved MAC Addresses

Reserved MAC Addresses Setting

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

Reserved MAC Addresses Config

MAC Address	Action	Delete

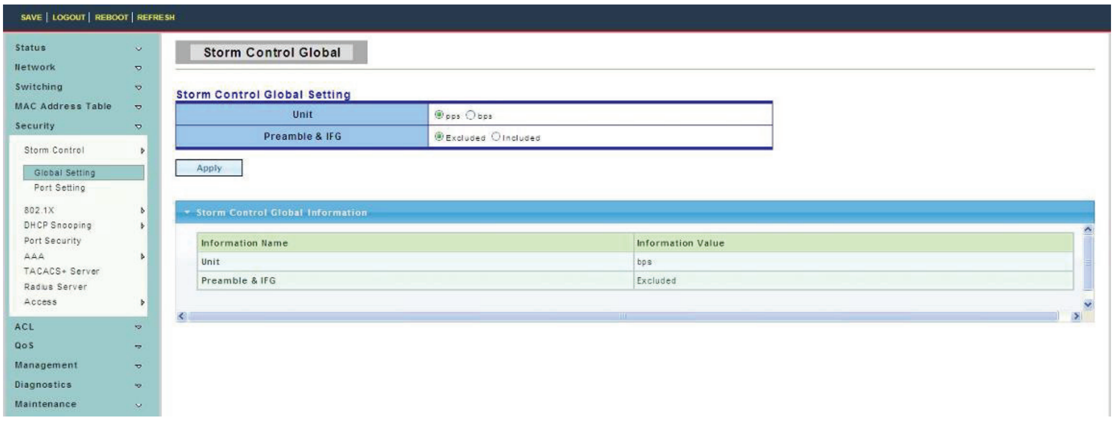
4.5 Security

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**



Storm Control Global

Storm Control Global Setting

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

Storm Control Global Information

Information Name	Information Value
Unit	bps
Preamble & IFG	Excluded

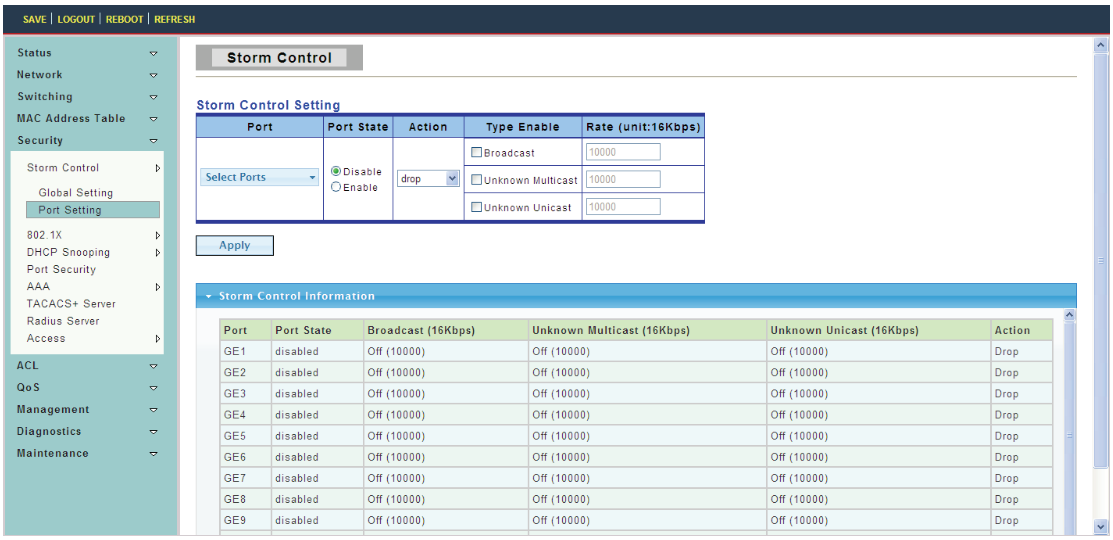
Unit: Choose storm control unit is pps or bps

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**



Storm Control

Storm Control Setting

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

Apply

Storm Control Information

Port	Port State	Broadcast (16Kbps)	Unknown Multicast (16Kbps)	Unknown Unicast (16Kbps)	Action
GE1	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE2	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE3	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE4	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE5	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE6	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE7	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE8	disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE9	disabled	Off (10000)	Off (10000)	Off (10000)	Drop

Port: Select the ports.

Type Enable: Select the type of storm control.

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

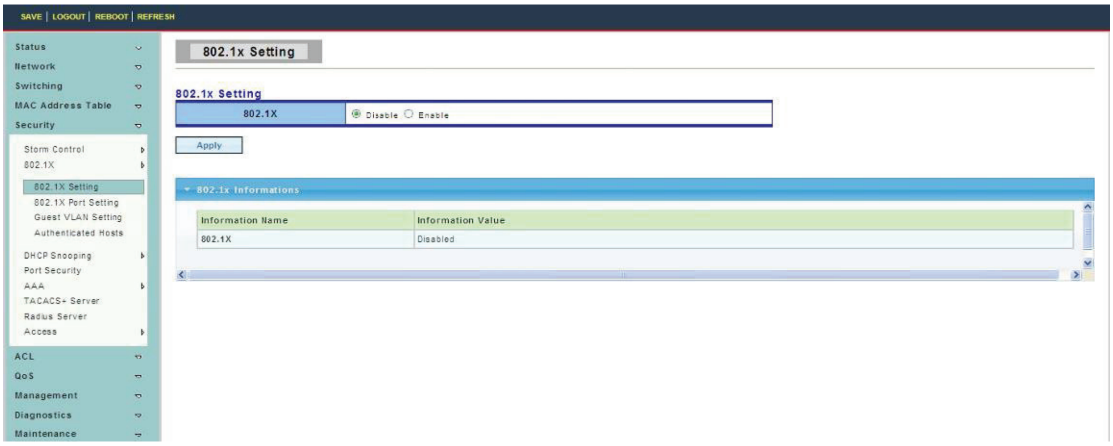
Rate: Value of storm control rate, Unit: pps (packet per-second) or Kbps (Kbits per-second) depends on global mode setting. The range is from 0 to 1000000.

4.5.2 802.1X

802.1x is based on the Client/Server access control and authentication protocol. It can restrict unauthorized users or devices to connect the access port via LAN/WLAN. Before getting permission from the switch, 802.1x will check the users or devices that connect with the switch ports. EAPoL data are transmitted between device and switch, when the device is allowed to access; all data 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 Setting

802.1x Setting

802.1X: ● Disable ○ Enable

Apply

802.1x Informations

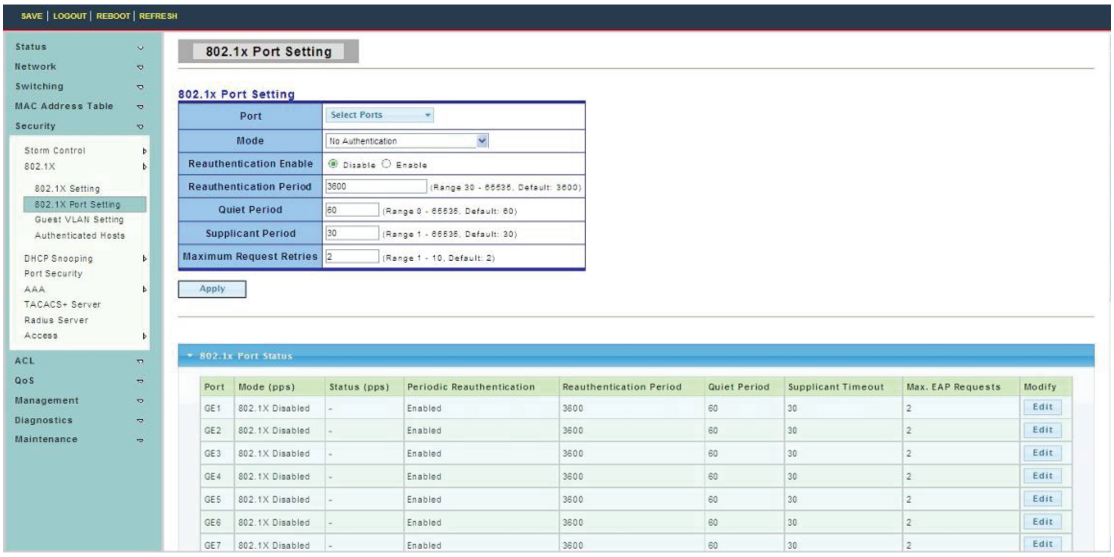
Information Name	Information Value
802.1X	Disabled

802.1X: Set the 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**



802.1x Port Setting

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

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 Disabled	-	Enabled	3600	60	30	2	Edit
GE3	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE4	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE5	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE6	802.1X Disabled	-	Enabled	3600	60	30	2	Edit
GE7	802.1X Disabled	-	Enabled	3600	60	30	2	Edit

Port: Select the ports to configure their authentication mode.

Mode: The authentication mode.

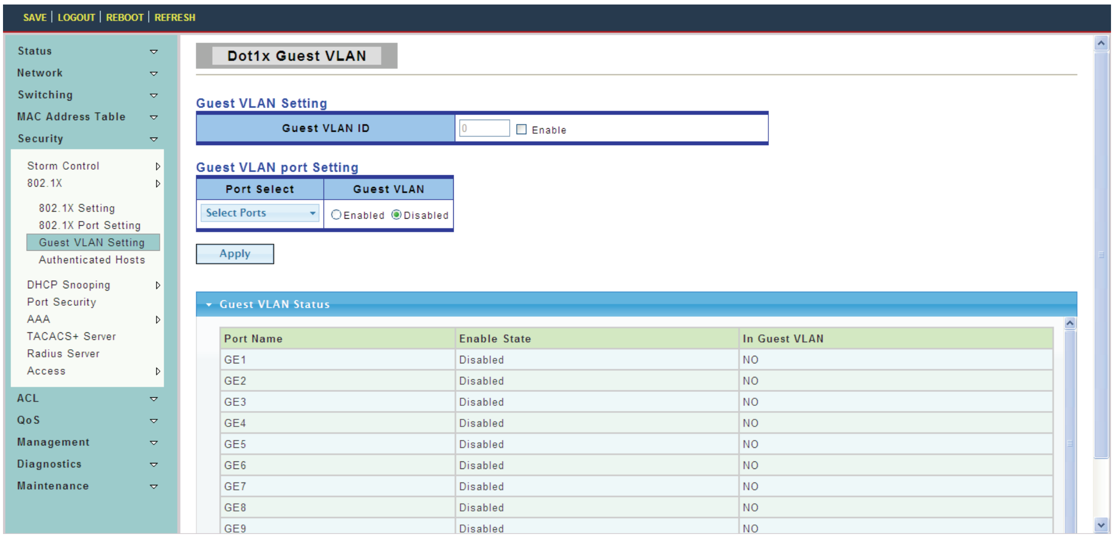
- Force Unauthorized: Force this port to be unconditional unauthorized.
- Force Authorized: Force this port to be unconditional authorized.
- Authentication: 802.1X authentication.
- No Authentication:802.1X disabled.

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

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

4.5.5.1 Guest VLAN Setting

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



Dot1x Guest VLAN

Guest VLAN Setting

Guest VLAN ID	0 □ Enable

Guest VLAN port Setting

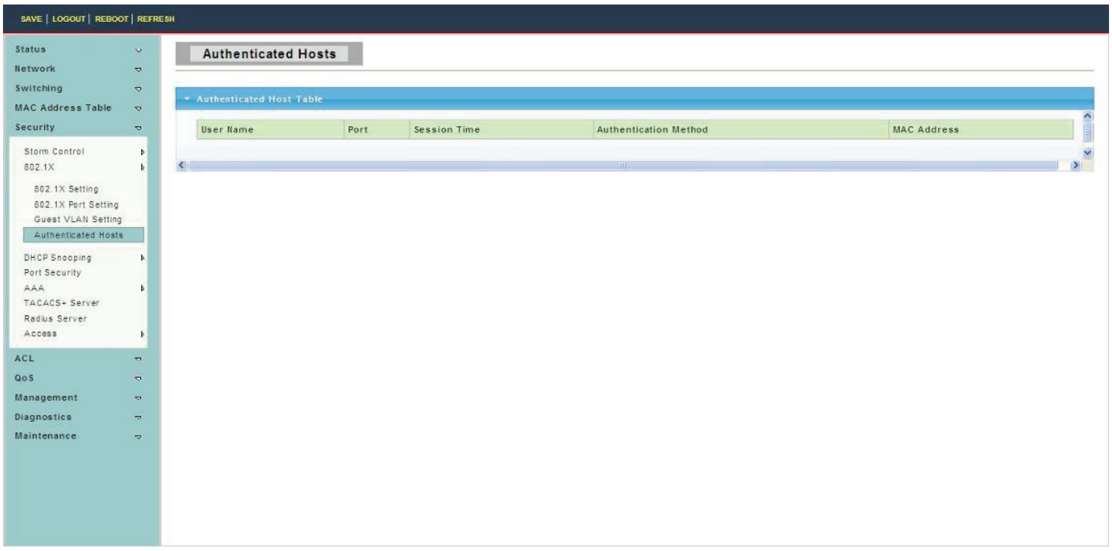
Port Select	Guest VLAN
Select Ports	○ Enabled ● Disabled

Guest VLAN Status

Port Name	Enable State	In Guest VLAN
GE1	Disabled	NO
GE2	Disabled	NO
GE3	Disabled	NO
GE4	Disabled	NO
GE5	Disabled	NO
GE6	Disabled	NO
GE7	Disabled	NO
GE8	Disabled	NO
GE9	Disabled	NO

4.3.5.1 Authenticated Hosts

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



Authenticated Hosts

Authenticated Host Table

User Name	Port	Session Time	Authentication Method	MAC Address

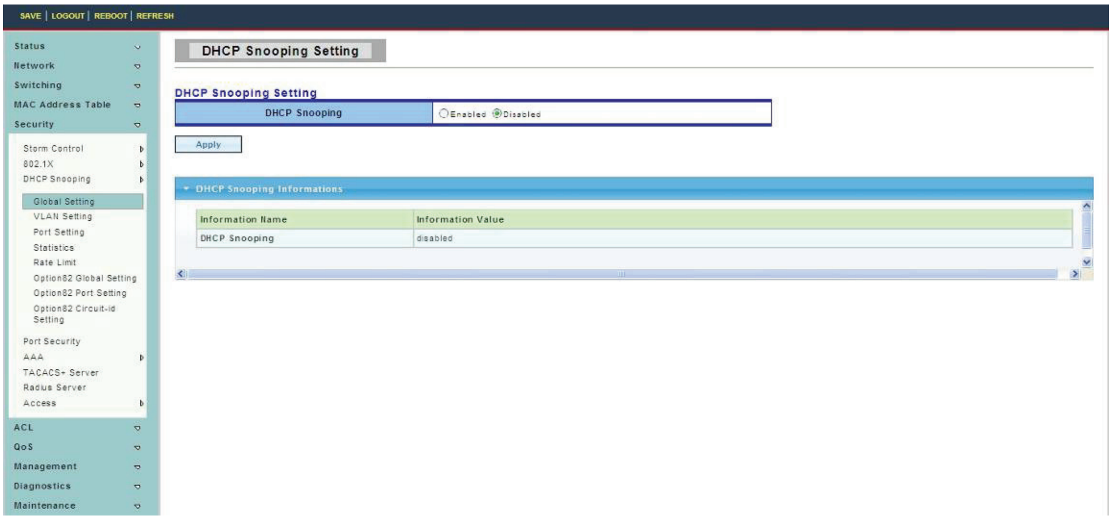
4.5.3 DHCP Snooping

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 Setting

DHCP Snooping	○Enabled ●Disabled

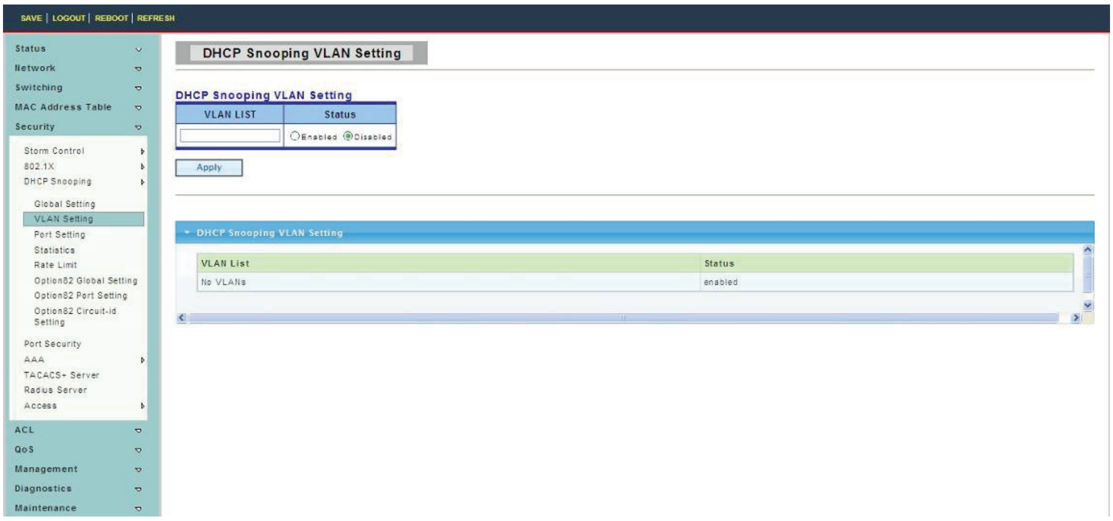
DHCP Snooping Informations

Information Name	Information Value
DHCP Snooping	disabled

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**



DHCP Snooping VLAN Setting

VLAN LIST	Status
	○Enabled ●Disabled

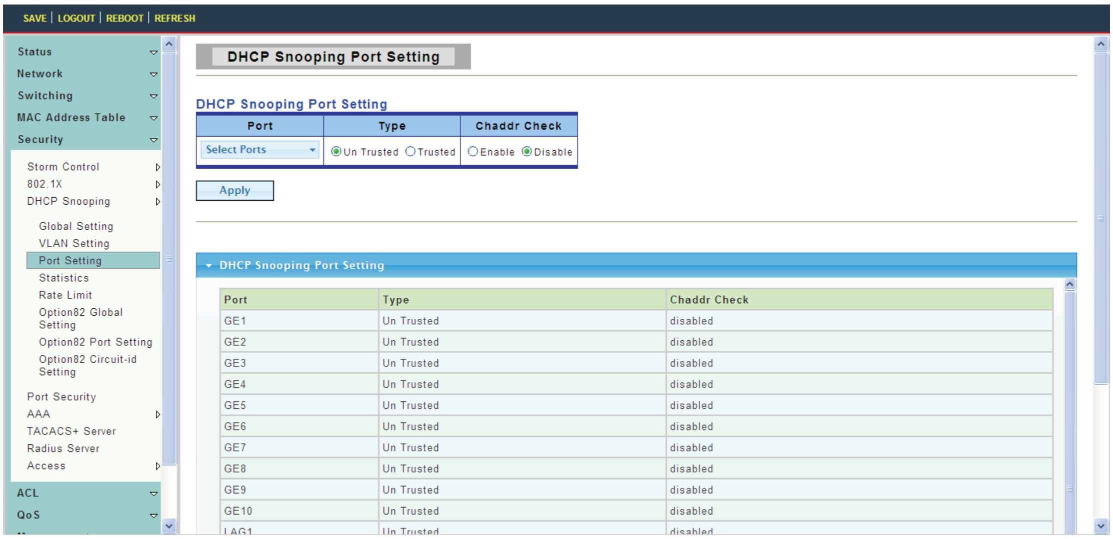
DHCP Snooping VLAN Setting

VLAN List	Status
No VLANs	enabled

4.5.3.3 Port Setting

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

This page allow user to configure the specific port as DHCP Snooping trust port.



DHCP Snooping Port Setting

DHCP Snooping Port Setting

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

Apply

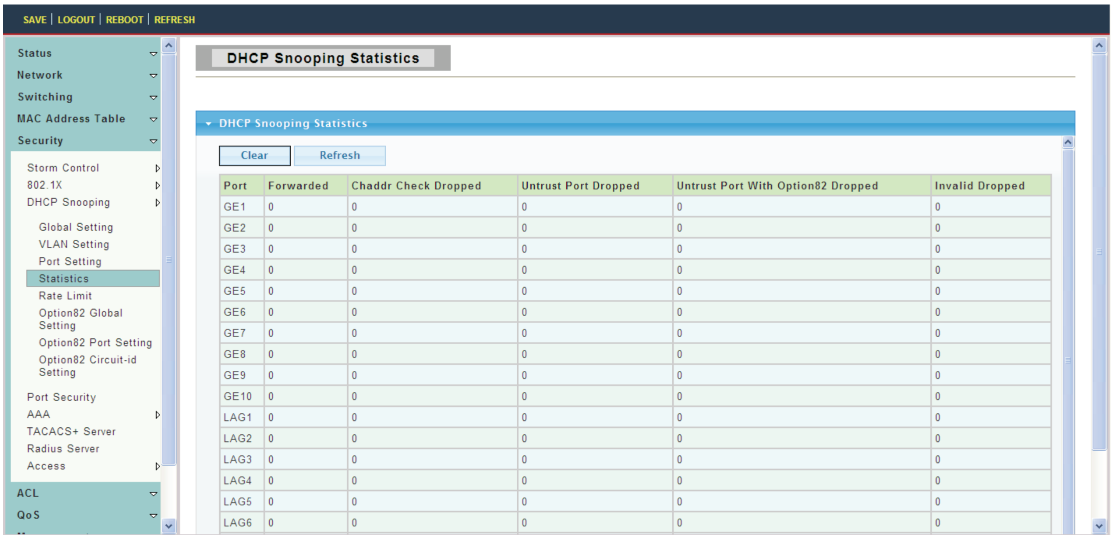
DHCP Snooping Port Setting

Port	Type	Chaddr Check
GE1	Un Trusted	disabled
GE2	Un Trusted	disabled
GE3	Un Trusted	disabled
GE4	Un Trusted	disabled
GE5	Un Trusted	disabled
GE6	Un Trusted	disabled
GE7	Un Trusted	disabled
GE8	Un Trusted	disabled
GE9	Un Trusted	disabled
GE10	Un Trusted	disabled
LAG1	Un Trusted	disabled

4.5.3.4 Statistics

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

This page shows statistics of each port´s DHCP Snooping state information.



DHCP Snooping Statistics

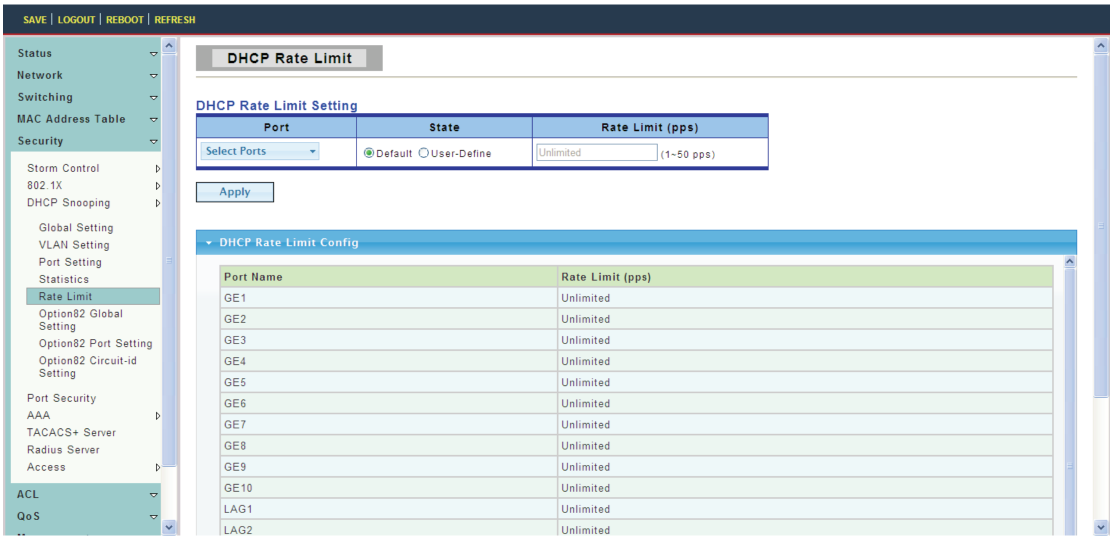
DHCP Snooping Statistics

Clear Refresh

Port	Forwarded	Chaddr Check Dropped	Untrust Port Dropped	Untrust Port With Option82 Dropped	Invalid Dropped
GE1	0	0	0	0	0
GE2	0	0	0	0	0
GE3	0	0	0	0	0
GE4	0	0	0	0	0
GE5	0	0	0	0	0
GE6	0	0	0	0	0
GE7	0	0	0	0	0
GE8	0	0	0	0	0
GE9	0	0	0	0	0
GE10	0	0	0	0	0
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**



DHCP Rate Limit

DHCP Rate Limit Setting

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

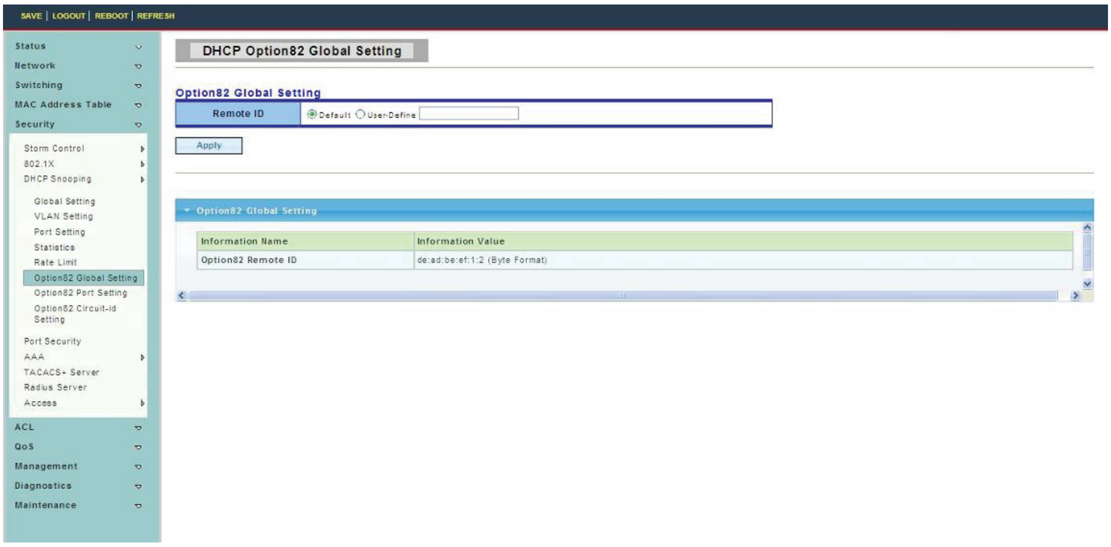
DHCP Rate Limit Config

Port Name	Rate Limit (pps)
GE1	Unlimited
GE2	Unlimited
GE3	Unlimited
GE4	Unlimited
GE5	Unlimited
GE6	Unlimited
GE7	Unlimited
GE8	Unlimited
GE9	Unlimited
GE10	Unlimited
LAG1	Unlimited
LAG2	Unlimited

4.5.3.6 DHCP Option82 Global Setting

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

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



DHCP Option82 Global Setting

Option82 Global Setting

Remote ID: ● Default ○ User-Define

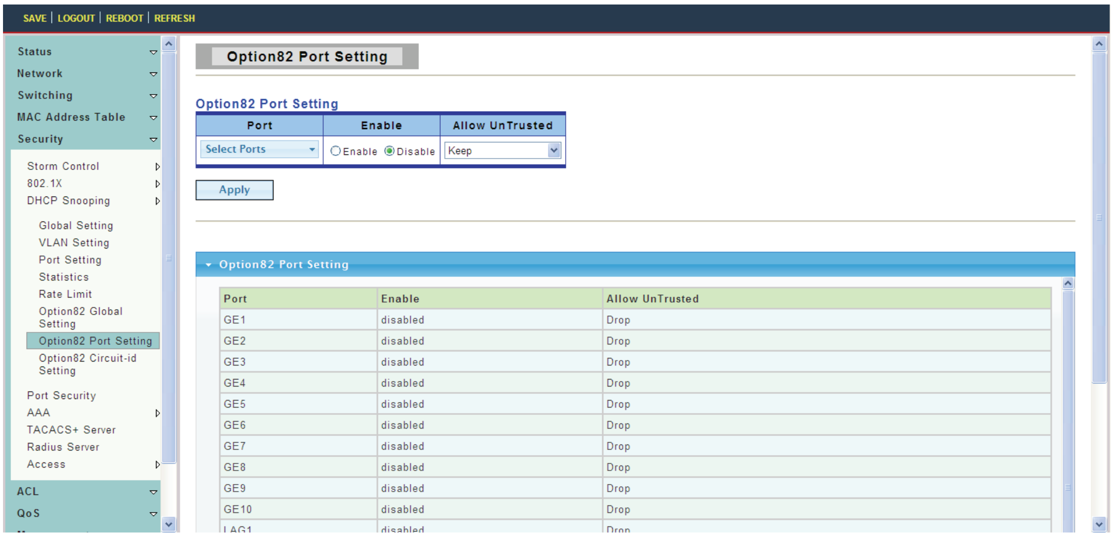
Option82 Global Setting

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

4.5.3.7 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.



Option82 Port Setting

Option82 Port Setting

Port	Enable	Allow UnTrusted
Select Ports	○Enable ●Disable	Keep

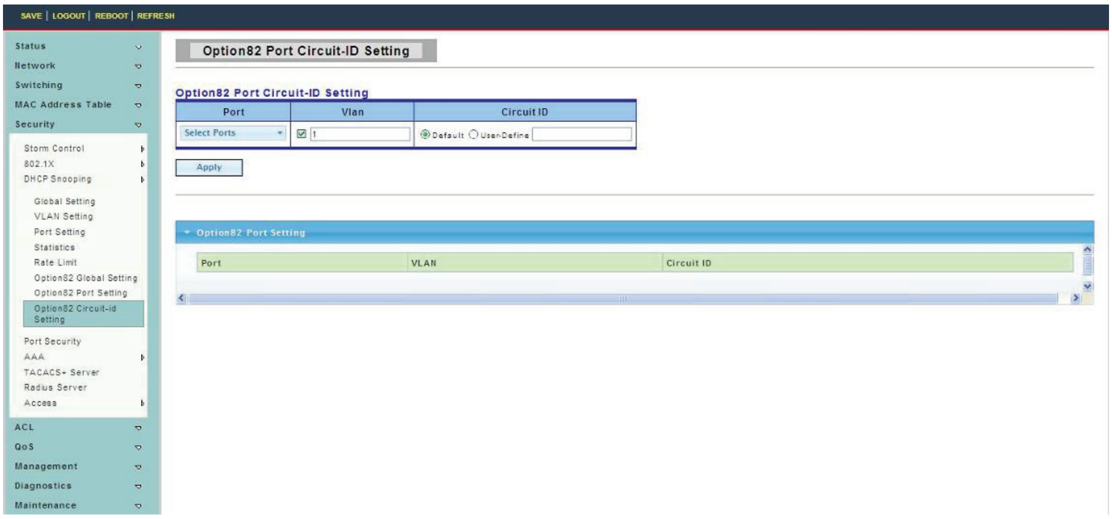
Option82 Port Setting

Port	Enable	Allow UnTrusted
GE1	disabled	Drop
GE2	disabled	Drop
GE3	disabled	Drop
GE4	disabled	Drop
GE5	disabled	Drop
GE6	disabled	Drop
GE7	disabled	Drop
GE8	disabled	Drop
GE9	disabled	Drop
GE10	disabled	Drop
LAG1	disabled	Drop

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.



Option82 Port Circuit-ID Setting

Option82 Port Circuit-ID Setting

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

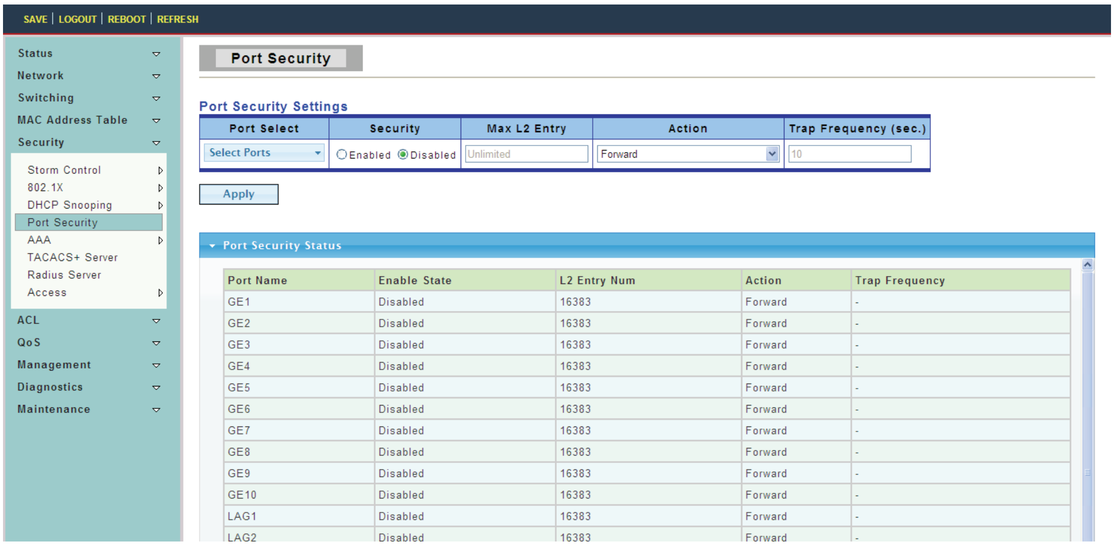
Option82 Port Setting

Port	VLAN	Circuit ID

4.5.4 Port Security

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

Ports Security can set port isolation and specific behavior.



Port Security

Port Security Settings

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

Port Security Status

Port Name	Enable State	L2 Entry Num	Action	Trap Frequency
GE1	Disabled	16383	Forward	-
GE2	Disabled	16383	Forward	-
GE3	Disabled	16383	Forward	-
GE4	Disabled	16383	Forward	-
GE5	Disabled	16383	Forward	-
GE6	Disabled	16383	Forward	-
GE7	Disabled	16383	Forward	-
GE8	Disabled	16383	Forward	-
GE9	Disabled	16383	Forward	-
GE10	Disabled	16383	Forward	-
LAG1	Disabled	16383	Forward	-
LAG2	Disabled	16383	Forward	-

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.

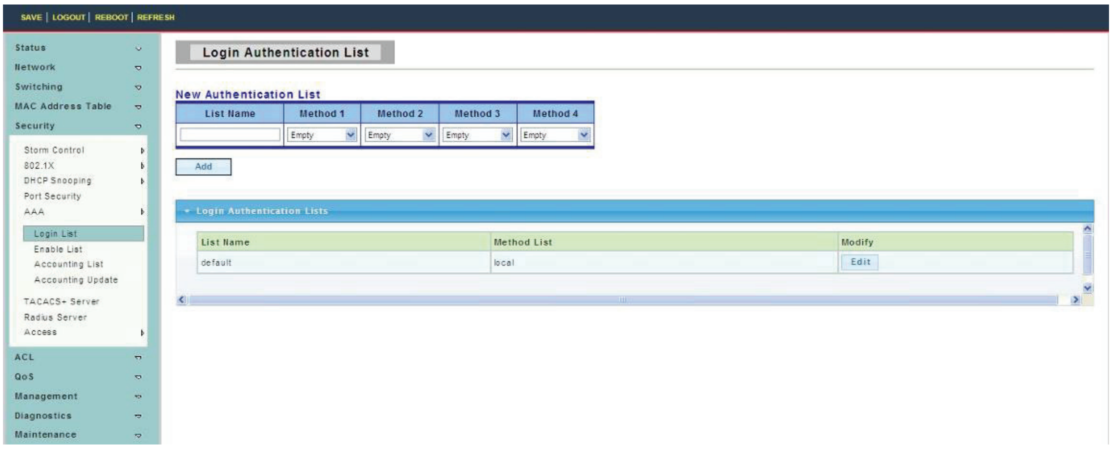
Max L2 Entry: The total number of MAC addresses entry, which can be learned by a port.

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 or 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.



Login Authentication List

New Authentication List

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

Login Authentication Lists

List Name	Method List	Modify
default	local	Edit

List Name:

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

Method 1: Select 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.

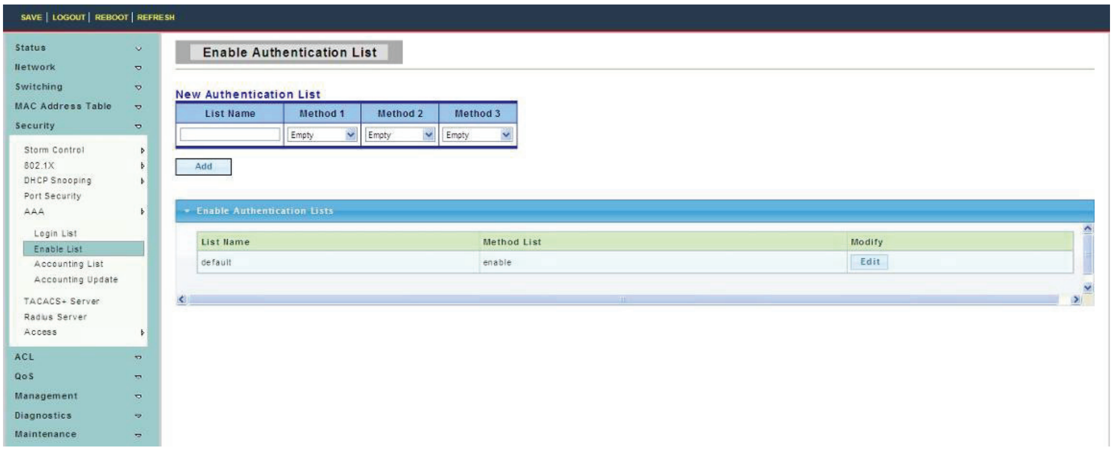
Method 4: Select forth priority of login authentication method.

- 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 allow 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 issuing 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.



Enable Authentication List

New Authentication List

List Name	Method 1	Method 2	Method 3
	Empty	Empty	Empty

Enable Authentication Lists

List Name	Method List	Modify
default	enable	Edit

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

Method 1: Select 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.

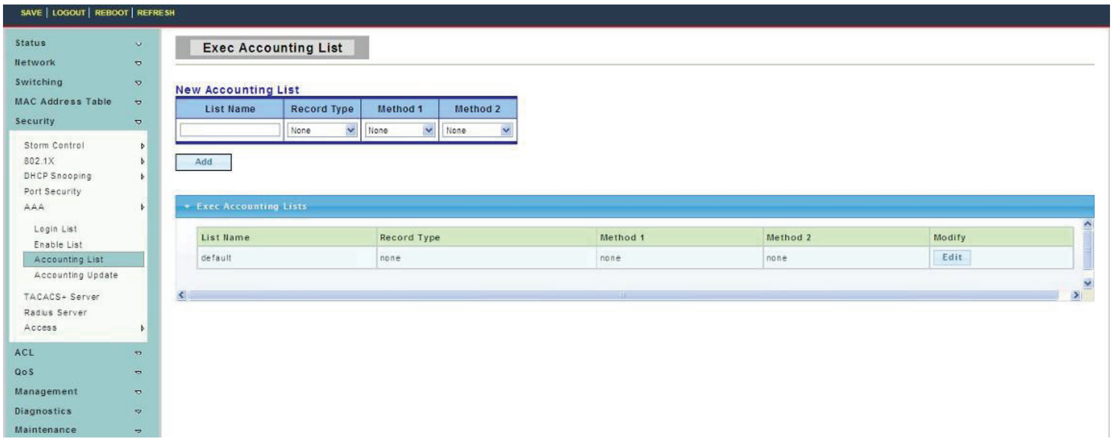
Method 3: Select third priority of enable authentication method.

- 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 allow user to add, edit or delete accounting list settings (The “default” list cannot be deleted.). The line combined to this list will accounting user who entering CLI shell by methods in this list. If the first method is failed, it will try to use the next priority method to accounting if it exists.



Exec Accounting List

New Accounting List

List Name	Record Type	Method 1	Method 2
	None	None	None

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 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.

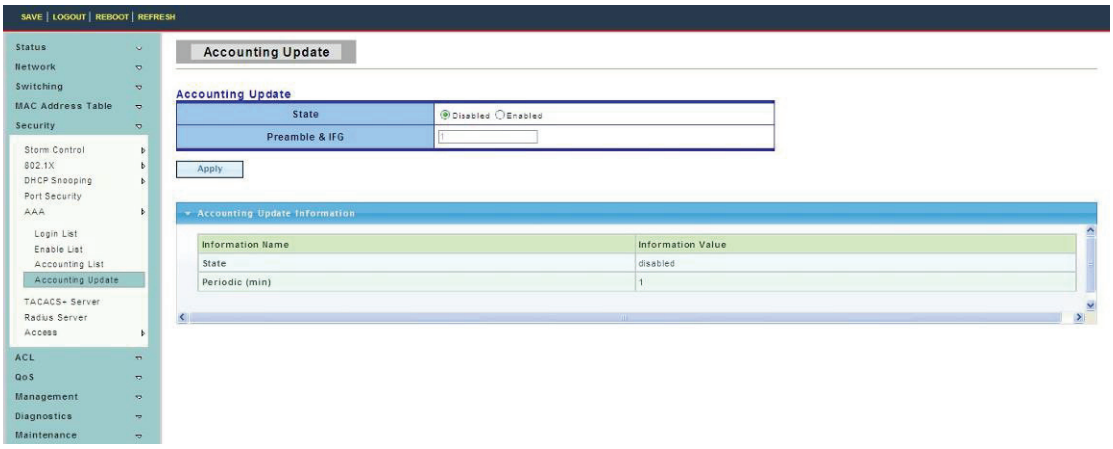
- Tacacs+: Use remote TACACS+ server to accounting.
- Radius: Use remote Radius server to accounting. Not supported now, it will be supported in the future.

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**



Accounting Update

Accounting Update

State	● Disabled ○ Enabled
Preamble & IFG	1

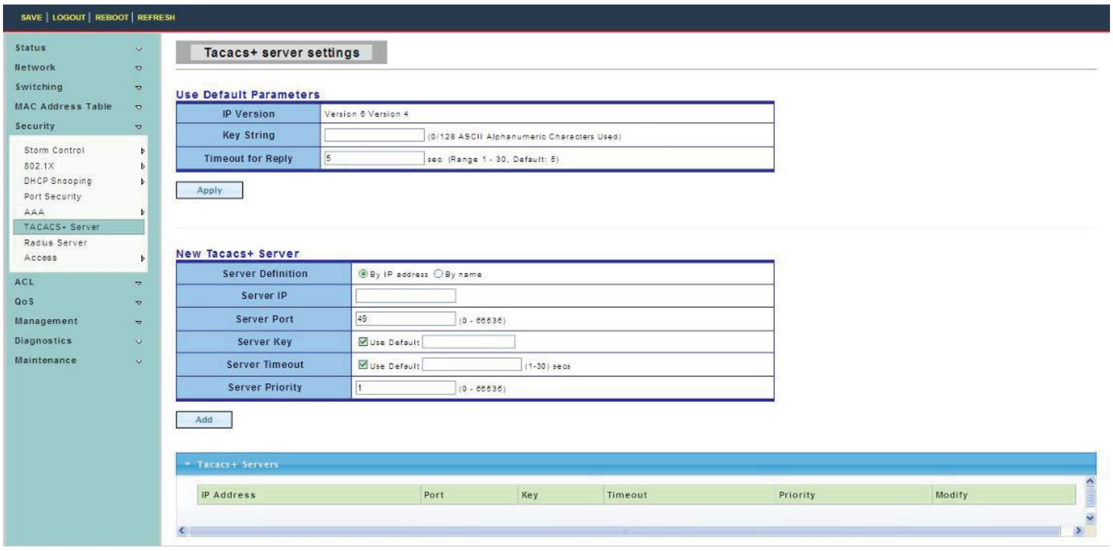
Accounting Update Information

Information Name	Information Value
State	disabled
Periodic (min)	1

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.



Tacacs+ server settings

Use Default Parameters

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

New Tacacs+ Server

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

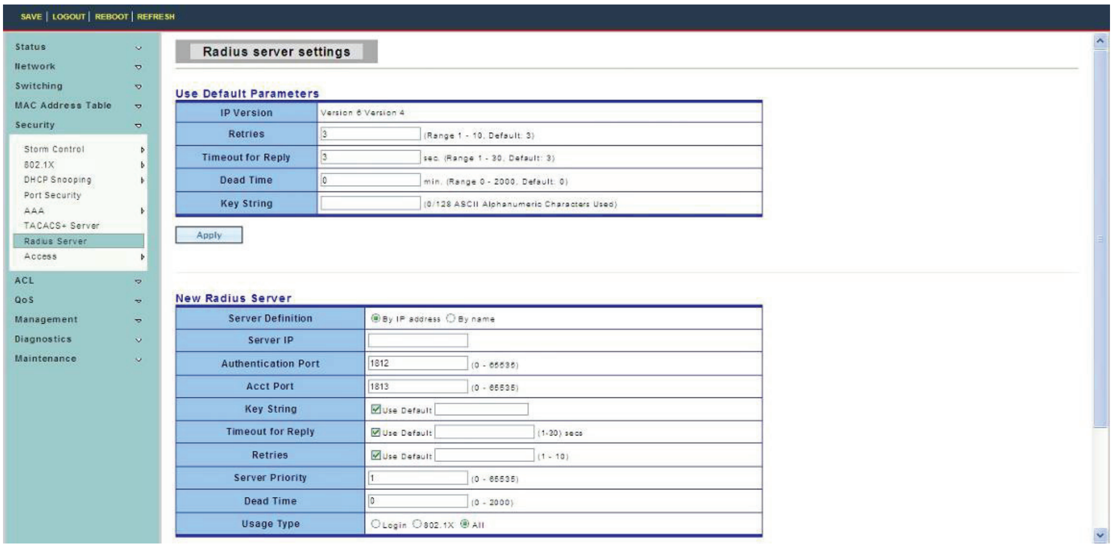
Tacacs+ Servers

IP Address	Port	Key	Timeout	Priority	Modify

4.5.7 Radius server

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

This page is used to set up radius server.



Radius server settings

Use Default Parameters

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

Apply

New Radius Server

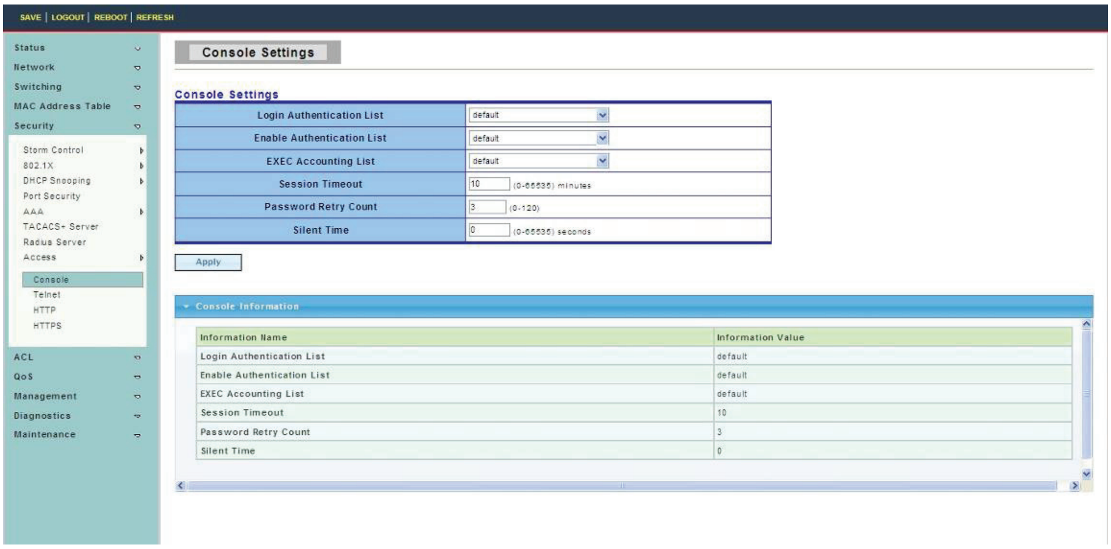
Server Definition	● By IP address ○ By name
Server IP	
Authentication Port	1812 (0 - 65535)
Acct Port	1813 (0 - 65535)
Key String	☑ Use Default
Timeout for Reply	☑ Use Default (1-30) secs
Retries	☑ Use Default (1 - 10)
Server Priority	1 (0 - 65535)
Dead Time	0 (0 - 2000)
Usage Type	○ Login ○ 802.1X ● All

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.



Console Settings

Console Settings

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

Apply

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

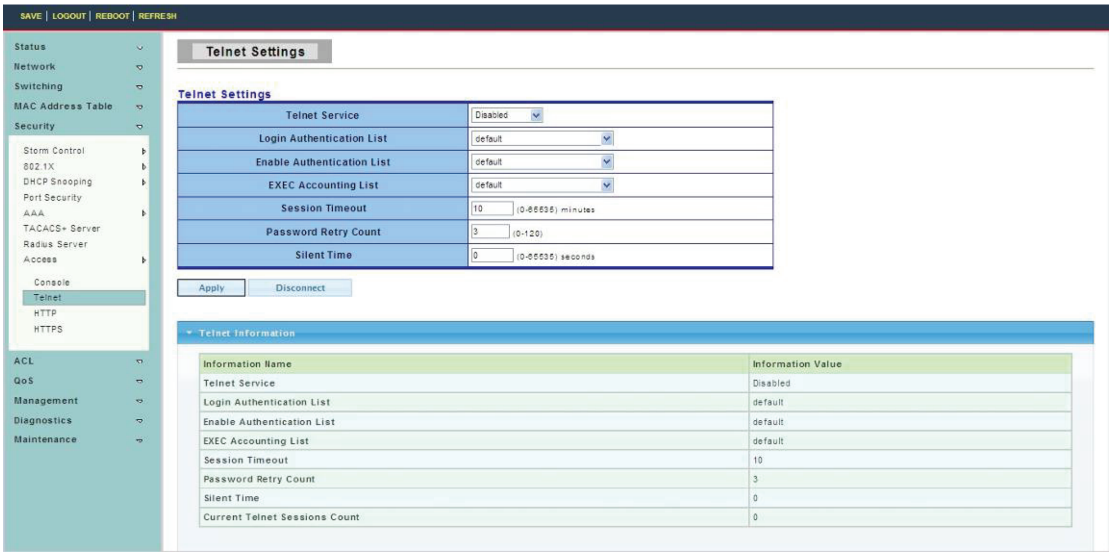
Login Authentication List: Select one of the login authentication lists we configured in “Login List” page.
Enable Authentication List: Select one of the enable authentication lists we configured in “Enable List” page.
EXEC Authorization List: Select one of the EXEC authorization lists we configured 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 Settings

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

Telnet Information

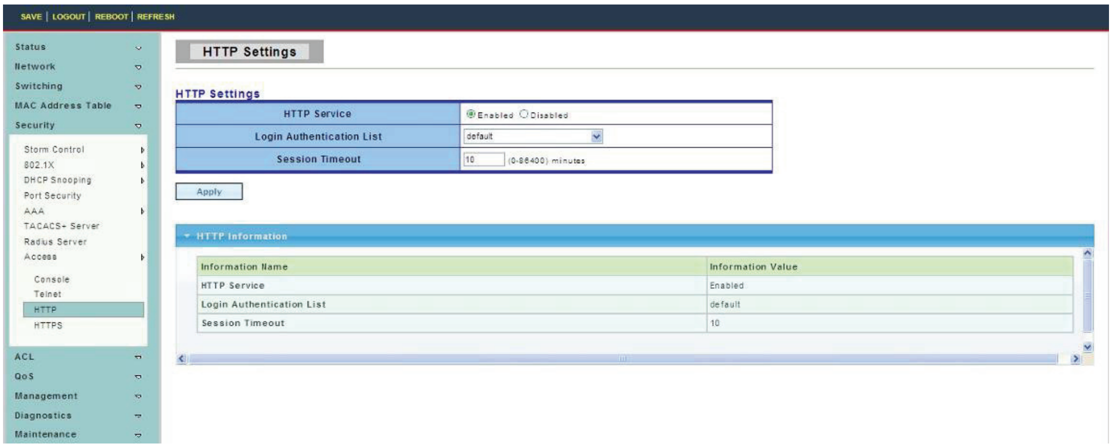
Information Name	Information Value
Telnet Service	Disabled
Login Authentication List	default
Enable Authentication List	default
EXEC Accounting List	default
Session Timeout	10
Password Retry Count	3
Silent Time	0
Current Telnet Sessions Count	0

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 Settings

HTTP Settings

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

HTTP Information

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

HTTP Server：set HTTP Server disable or enable.

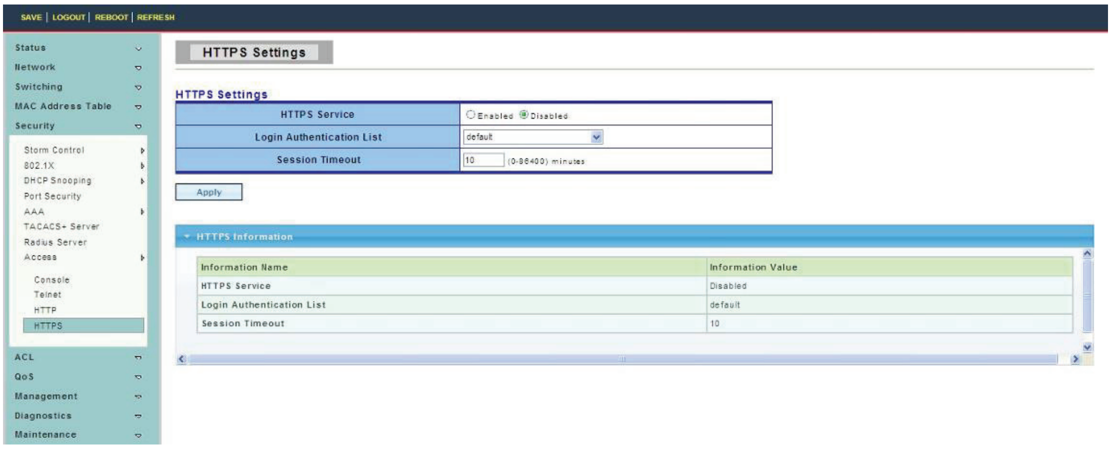
Login Authentication List: Select one of the login authentication lists we configured in “Login List” page.

Session Timeout: Set session timeout minutes for user access WEB from HTTP protocol. If user does not response after session timeout minute, WEB UI 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 Settings

HTTPS Settings

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

HTTPS Information

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

HTTPS Server: Set HTTPS Server disable or enable.

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

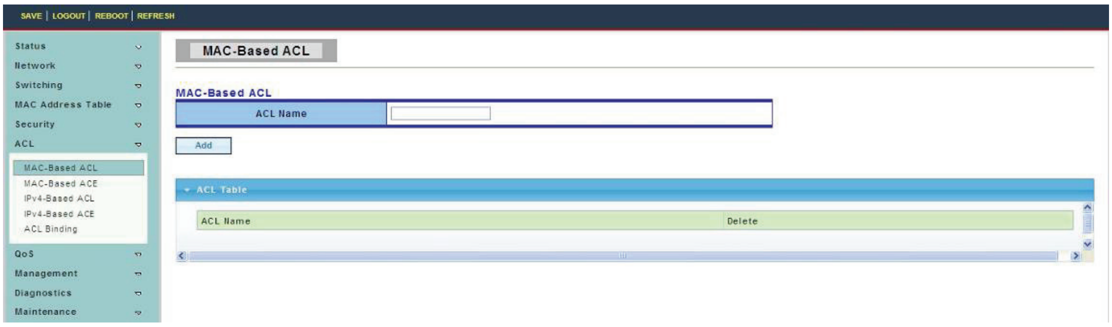
Session Timeout: Set session timeout minutes for user access WEB from HTTPS protocol. If user does not response after session timeout minute, WEBUI will logout automatically. 0 minutes means never timeout.

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.



MAC-Based ACL

MAC-Based ACL

ACL Name	

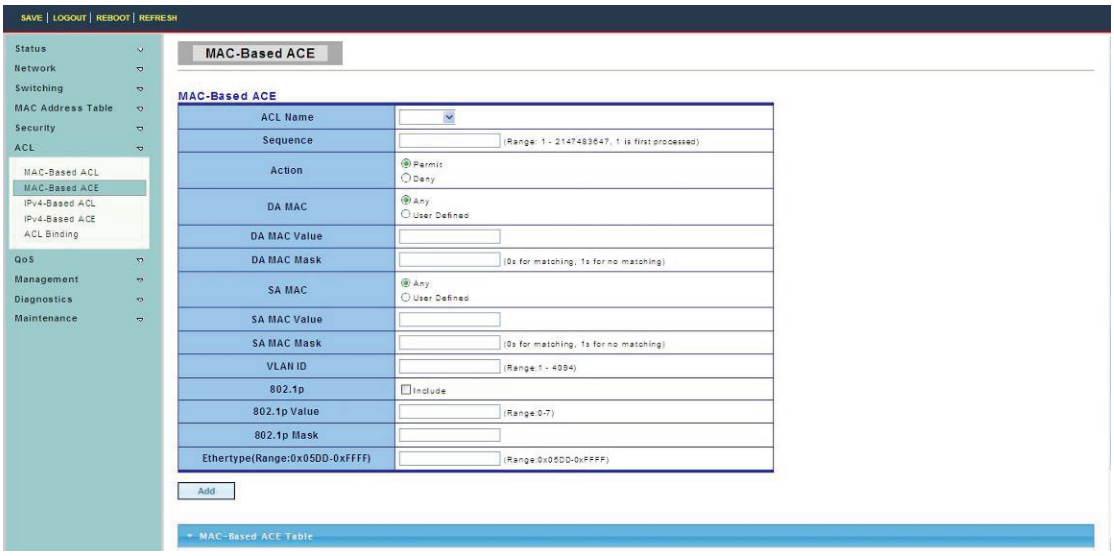
ACL Name	Delete

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.



MAC-Based ACE

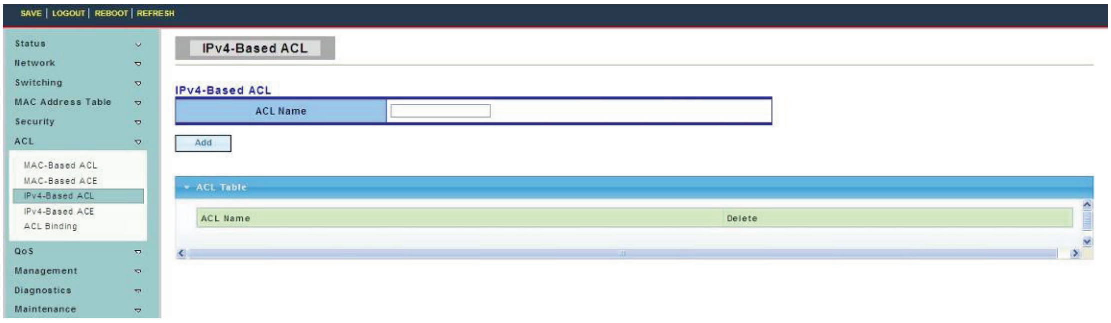
MAC-Based ACE

ACL Name	
Sequence	(Range: 1 - 2147483647, 1 is first processed)
Action	● Permit ○ Deny
DA MAC	● Any ○ User Defined
DA MAC Value	
DA MAC Mask	(0s for matching, 1s for no matching)
SA MAC	● Any ○ User Defined
SA MAC Value	
SA MAC Mask	(0s for matching, 1s for no matching)
VLAN ID	(Range:1 - 4094)
802.1p	□ Include
802.1p Value	(Range:0-7)
802.1p Mask	
Ethertype(Range:0x05DD-0xFFFF)	(Range:0x05DD-0xFFFF)

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.



IPv4-Based ACL

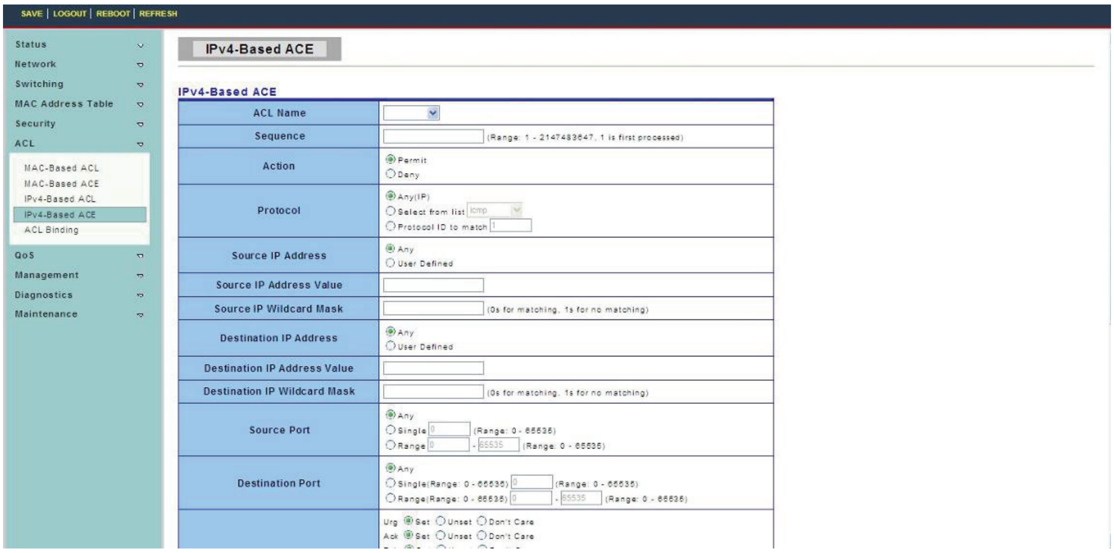
ACL Name	

ACL Name	Delete

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.



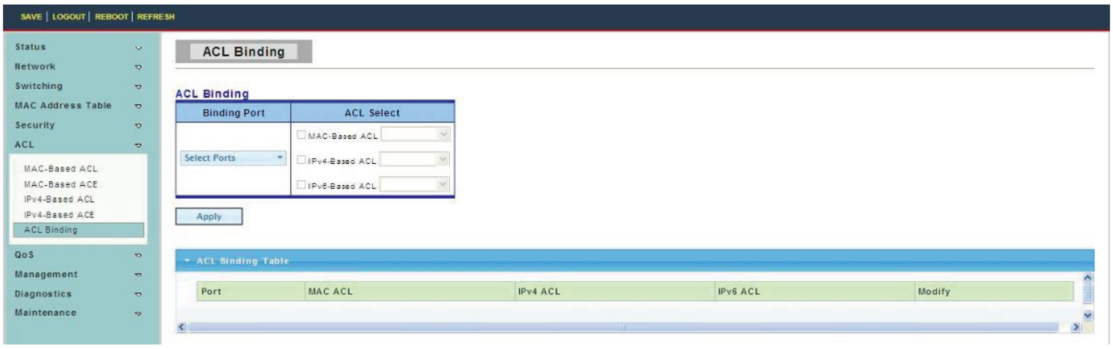
IPv4-Based ACE

ACL Name	
Sequence	(Range: 1 - 2147483647, 1 is first processed)
Action	● Permit ○ Deny
Protocol	● Any(IP) ○ Select from list icmp ○ Protocol ID to match 1
Source IP Address	● Any ○ User Defined
Source IP Address Value	
Source IP Wildcard Mask	(0s for matching, 1s for no matching)
Destination IP Address	● Any ○ User Defined
Destination IP Address Value	
Destination IP Wildcard Mask	(0s for matching, 1s for no matching)
Source Port	● Any ○ Single 0 (Range: 0 - 65535) ○ Range 0 - 65535 (Range: 0 - 65535)
Destination Port	● Any ○ Single(Range: 0 - 65535) 0 (Range: 0 - 65535) ○ Range(Range: 0 - 65535) 0 - 65535 (Range: 0 - 65535)
	Urg ● Set ○ Unset ○ Don't Care Ack ● Set ○ Unset ○ Don't Care

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.



ACL Binding

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

Port	MAC ACL	IPv4 ACL	IPv6 ACL	Modify

4.7 QoS

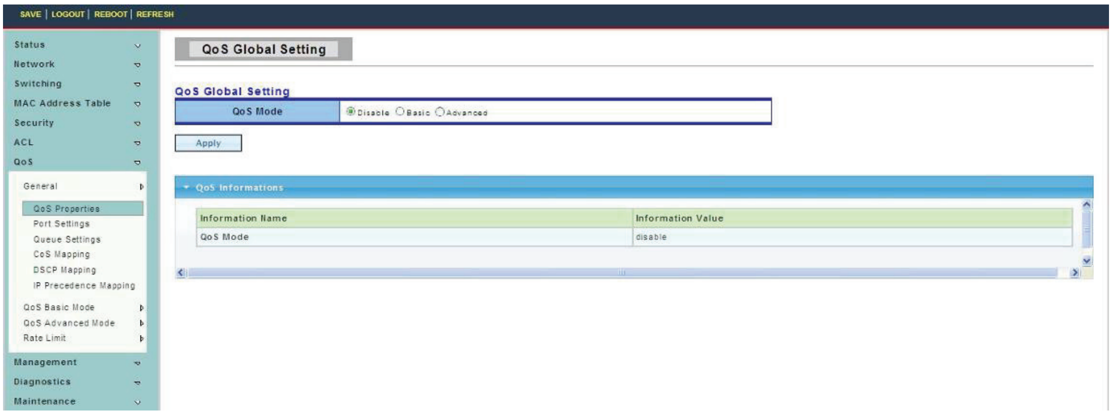
Use the QoS pages to configure settings for the switch QoS interface.

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, basic or advanced.



QoS Global Setting

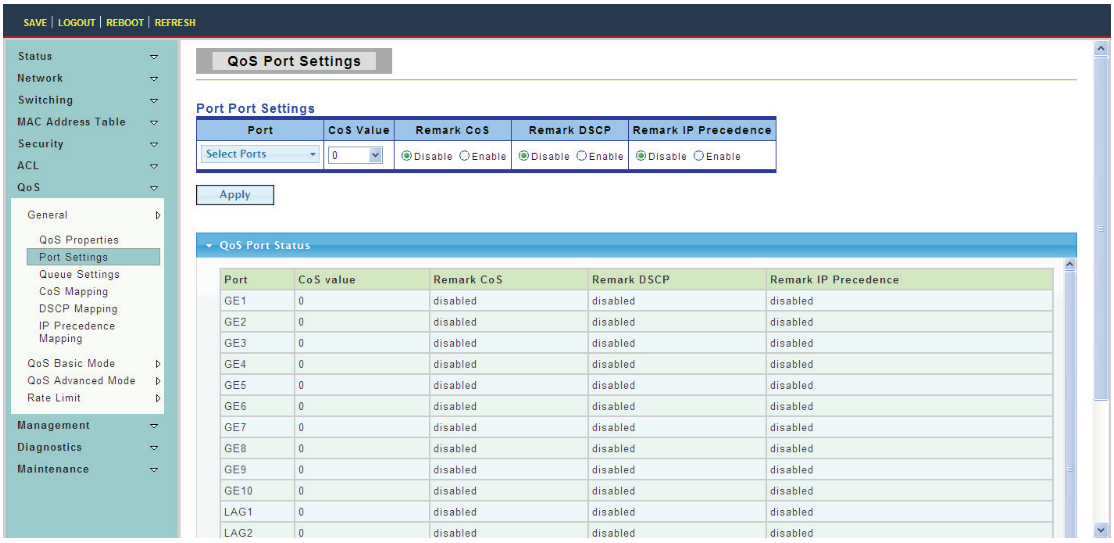
QoS Mode: ● Disable ○ Basic ○ Advanced

Information Name	Information Value
QoS Mode	disable

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 Port Settings

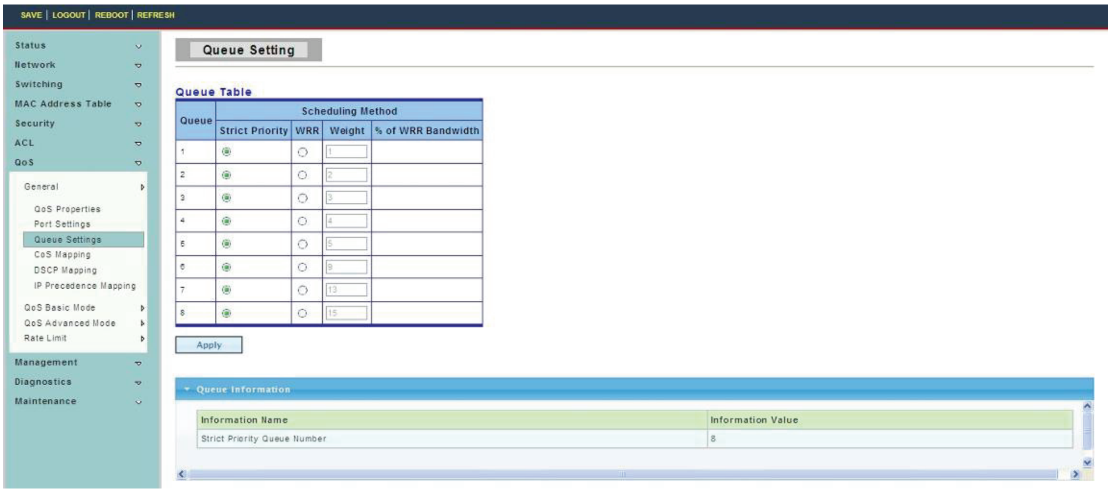
Port	CoS Value	Remark CoS	Remark DSCP	Remark IP Precedence
Select Ports	0	● Disable ○ Enable	● Disable ○ Enable	● Disable ○ Enable

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 the QoS instance queue scheduling model.



Queue Table

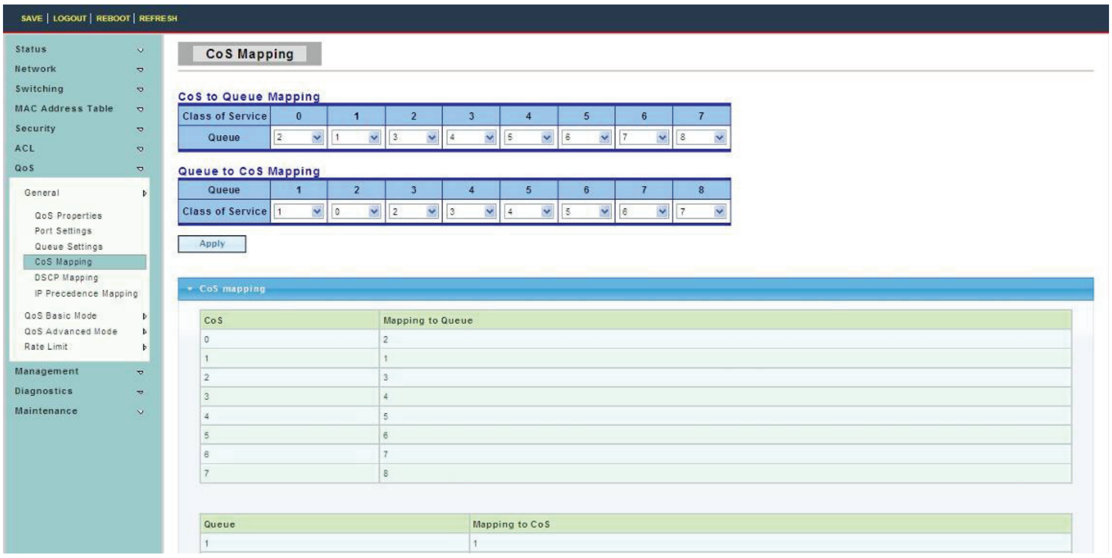
Queue	Scheduling Method			
	Strict Priority	WRR	Weight	% of WRR Bandwidth
1	●	○	1	
2	●	○	2	
3	●	○	3	
4	●	○	4	
5	●	○	5	
6	●	○	9	
7	●	○	13	
8	●	○	15	

Information Name	Information Value
Strict Priority Queue Number	8

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.



CoS to Queue Mapping

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

Queue to CoS Mapping

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

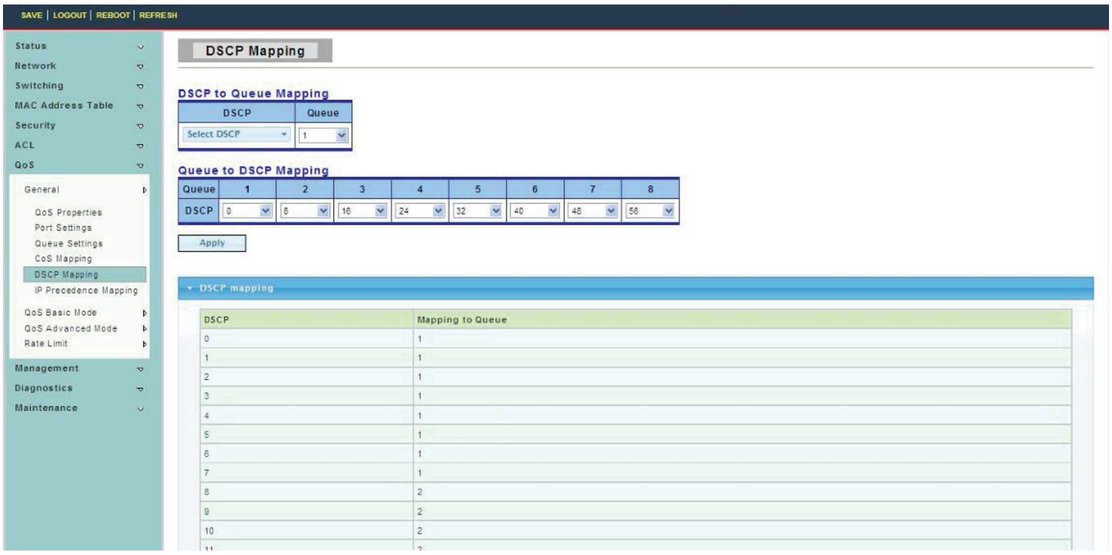
CoS	Mapping to Queue
0	2
1	1
2	3
3	4
4	5
5	6
6	7
7	8

Queue	Mapping to CoS
1	1

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.



DSCP Mapping

DSCP to Queue Mapping

DSCP	Queue
Select DSCP	1

Queue to DSCP Mapping

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

Apply

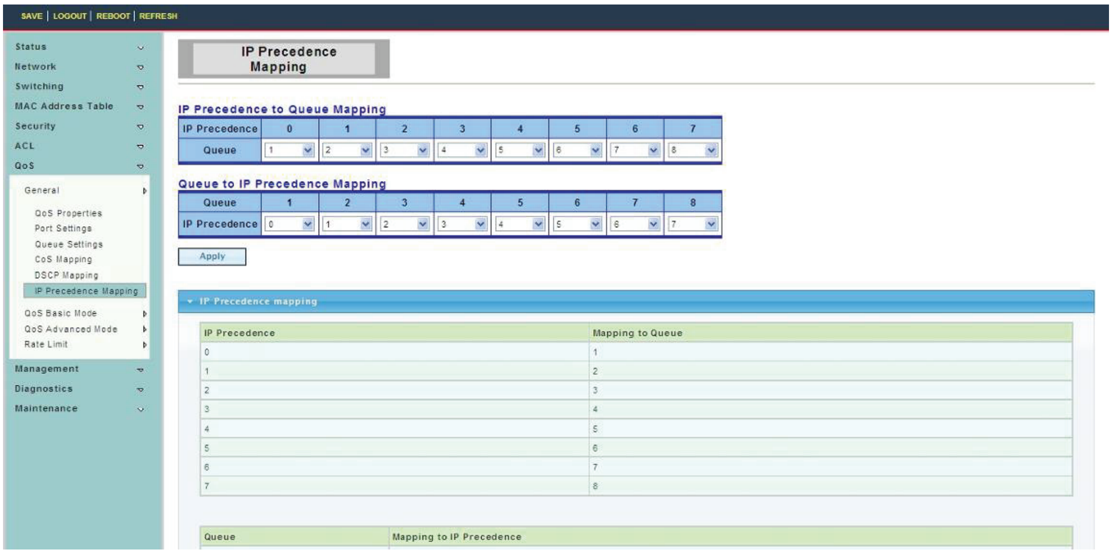
DSCP mapping

DSCP	Mapping to Queue
0	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	2
9	2
10	2
11	2

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.



IP Precedence Mapping

IP Precedence to Queue Mapping

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

Queue to IP Precedence Mapping

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

Apply

IP Precedence mapping

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

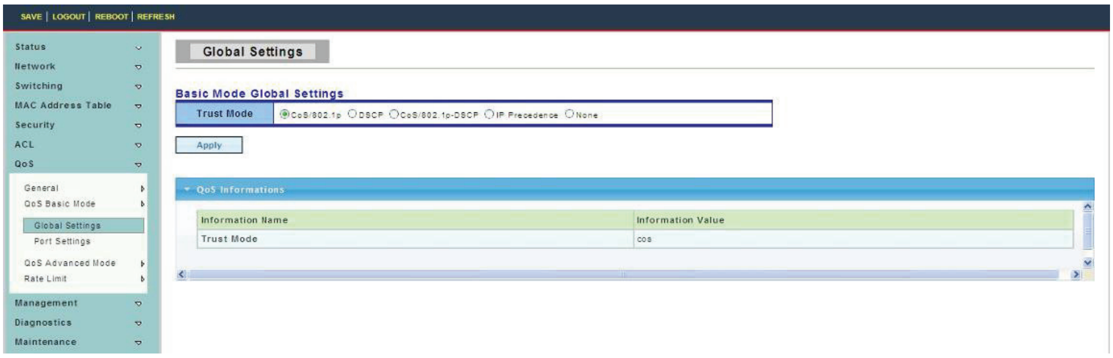
Queue	Mapping to IP Precedence

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.



Basic Mode Global Settings

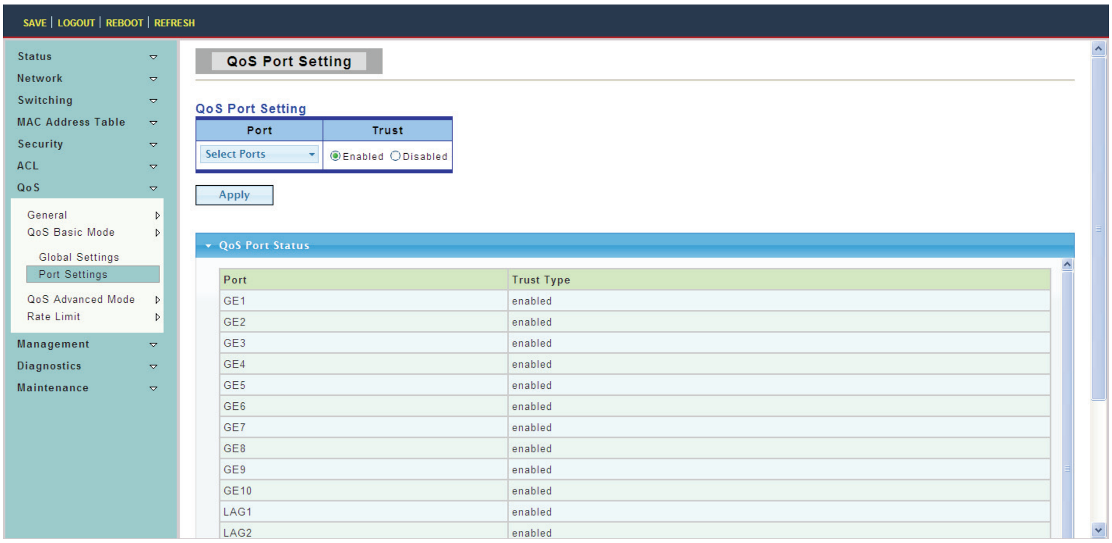
Trust Mode ● CoS/802.1p ○ DSCP ○ CoS/802.1p-DSCP ○ IP Precedence ○ None

Information Name	Information Value
Trust Mode	cos

4.7.2.2 Port Settings

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

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



QoS Port Setting

Port	Trust
Select Ports	● Enabled ○ Disabled

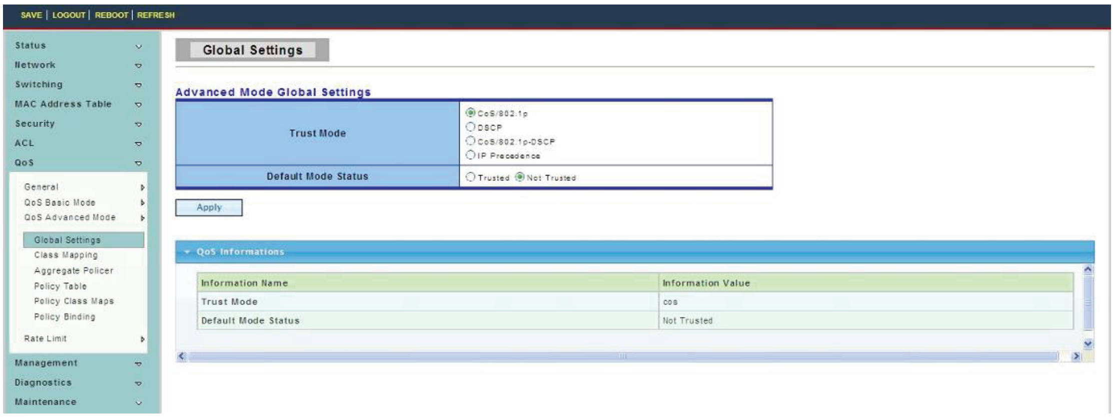
Port	Trust Type
GE1	enabled
GE2	enabled
GE3	enabled
GE4	enabled
GE5	enabled
GE6	enabled
GE7	enabled
GE8	enabled
GE9	enabled
GE10	enabled
LAG1	enabled
LAG2	enabled

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.



Global Settings

Advanced Mode Global Settings

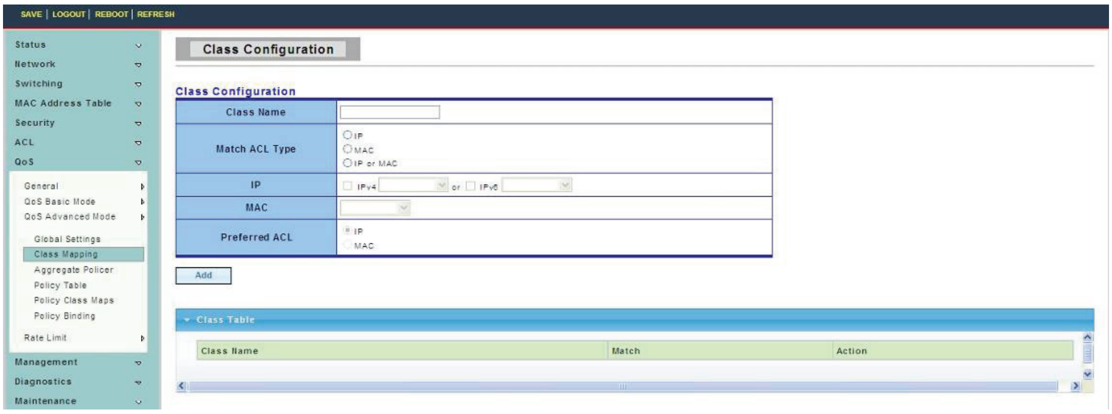
Trust Mode	● CoS/802.1p ○ DSCP ○ CoS/802.1p-DSCP ○ IP Precedence
Default Mode Status	○ Trusted ● Not Trusted

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

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.



Class Configuration

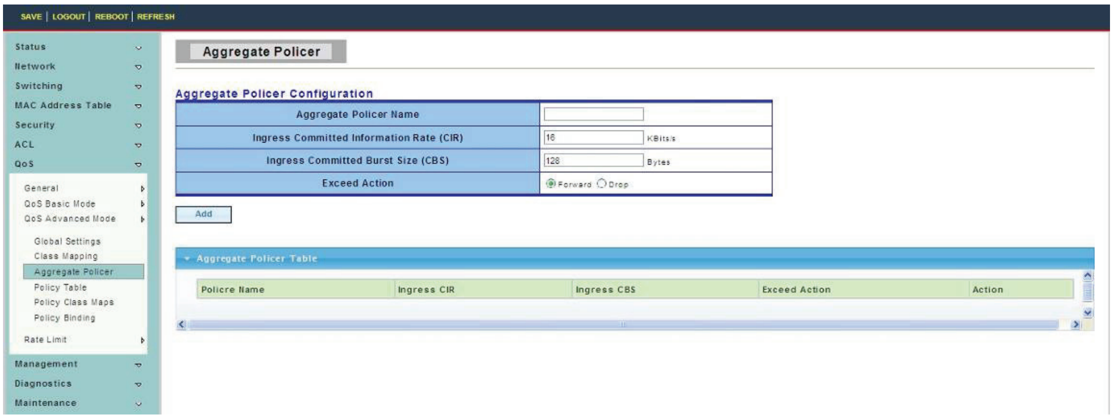
Class Configuration

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

Class Name	Match	Action

4.7.3.3 Aggregate Policer

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



Aggregate Policer

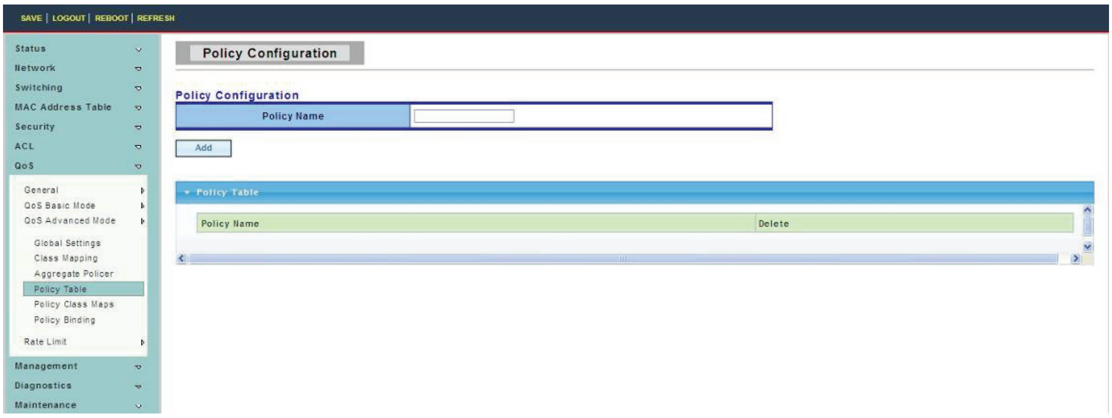
Aggregate Policer Configuration

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

Policre Name	Ingress CIR	Ingress CBS	Exceed Action	Action

4.7.3.4 Policy Table

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



Policy Configuration

Policy Configuration

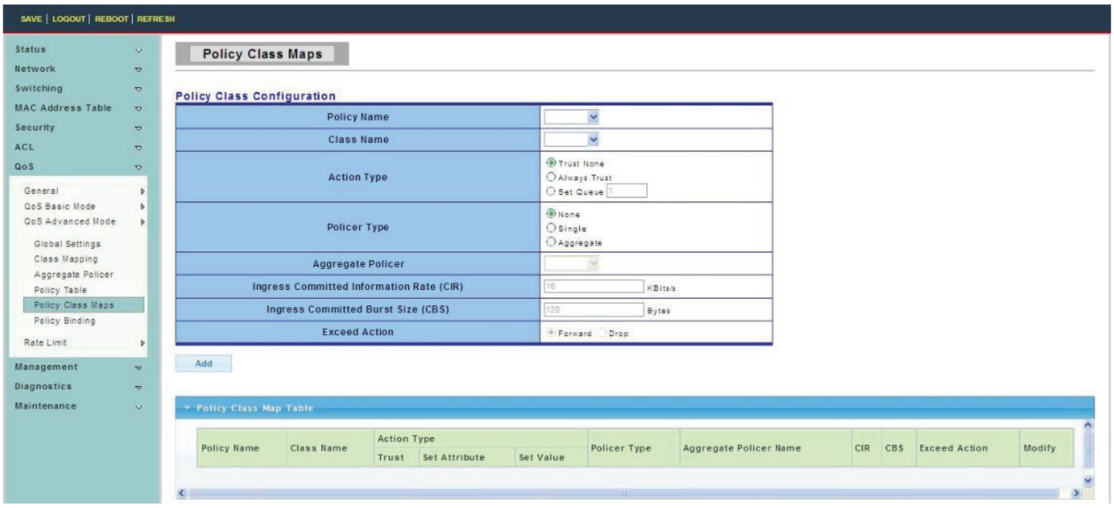
Policy Name	

Policy Table

Policy Name	Delete

4.7.3.5 Policy Class Maps

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



Policy Class Maps

Policy Class Configuration

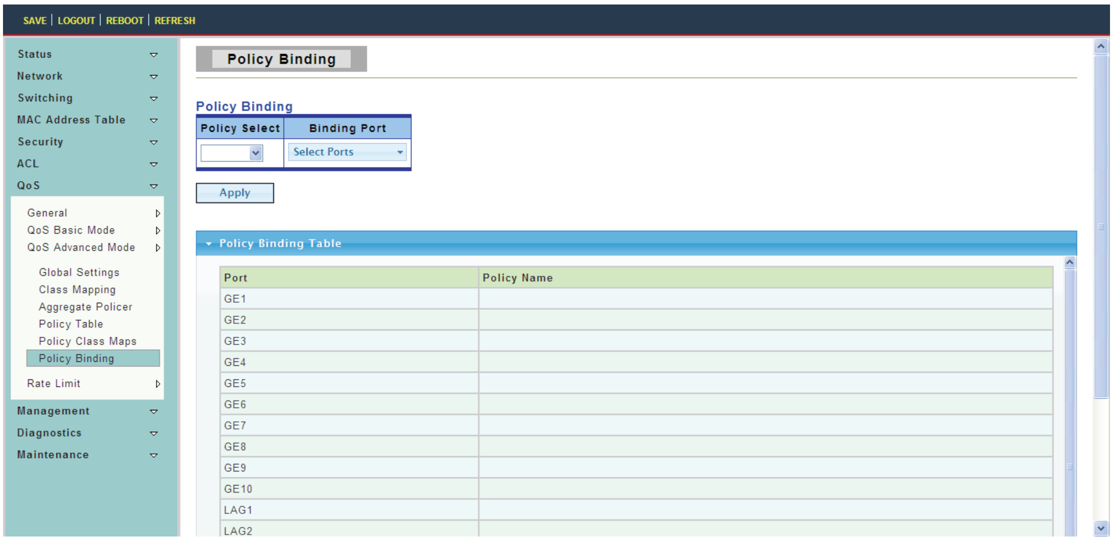
Policy Name	
Class Name	
Action Type	● Trust None ○ Always Trust ○ Set Queue 1
Policer Type	● None ○ Single ○ Aggregate
Aggregate Policer	
Ingress Committed Information Rate (CIR)	16 KBits/s
Ingress Committed Burst Size (CBS)	128 Bytes
Exceed Action	● Forward ○ Drop

Policy Class Map Table

Policy Name	Class Name	Action Type			Policer Type	Aggregate Policer Name	CIR	CBS	Exceed Action	Modify
		Trust	Set Attribute	Set Value						

4.7.3.6 Policy Binding

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



Policy Binding

Policy Binding

Policy Select	Binding Port
	Select Ports

Policy Binding Table

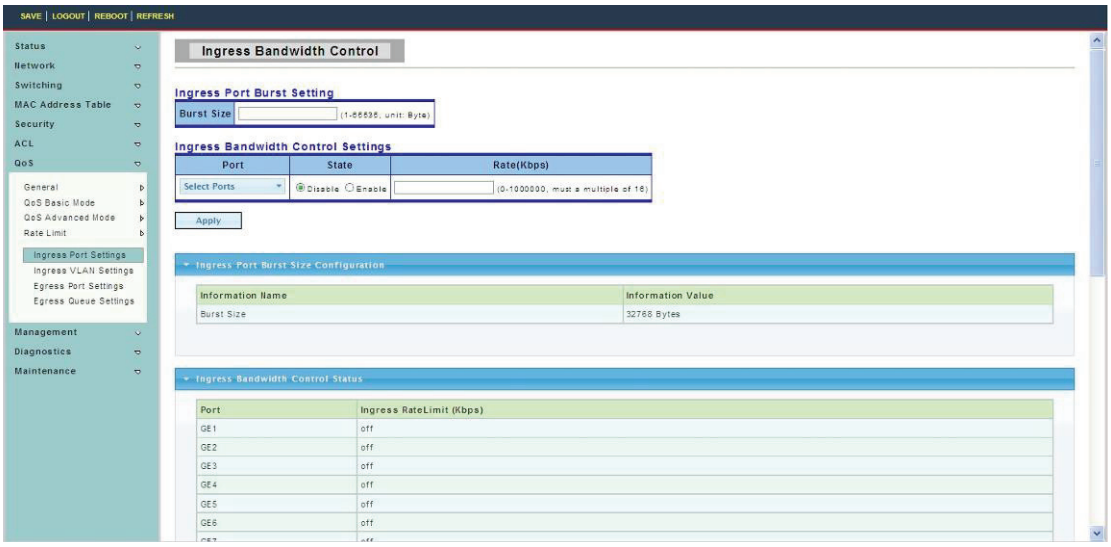
Port	Policy Name
GE1	
GE2	
GE3	
GE4	
GE5	
GE6	
GE7	
GE8	
GE9	
GE10	
LAG1	
LAG2	

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.



Ingress Bandwidth Control

Ingress Port Burst Setting

Burst Size (1-65535, unit: Byte)

Ingress Bandwidth Control Settings

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

Ingress Port Burst Size Configuration

Information Name	Information Value
Burst Size	32768 Bytes

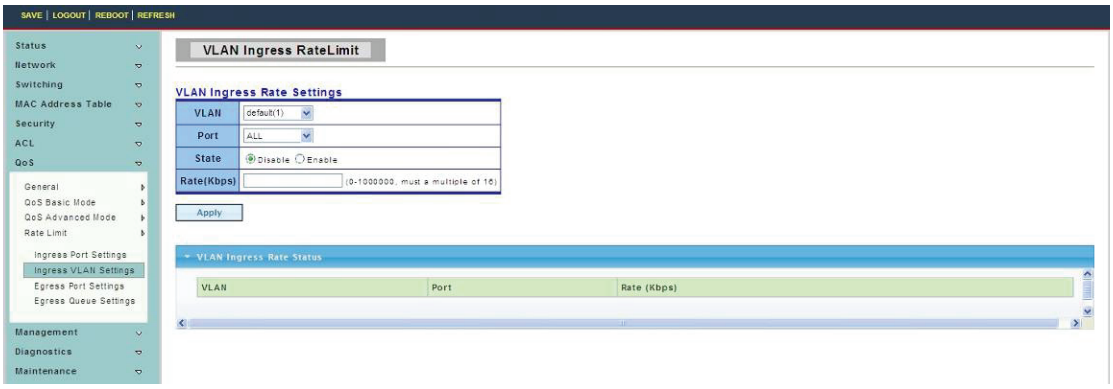
Ingress Bandwidth Control Status

Port	Ingress RateLimit (Kbps)
GE1	off
GE2	off
GE3	off
GE4	off
GE5	off
GE6	off
GE7	off

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**.**



VLAN Ingress RateLimit

VLAN Ingress Rate Settings

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

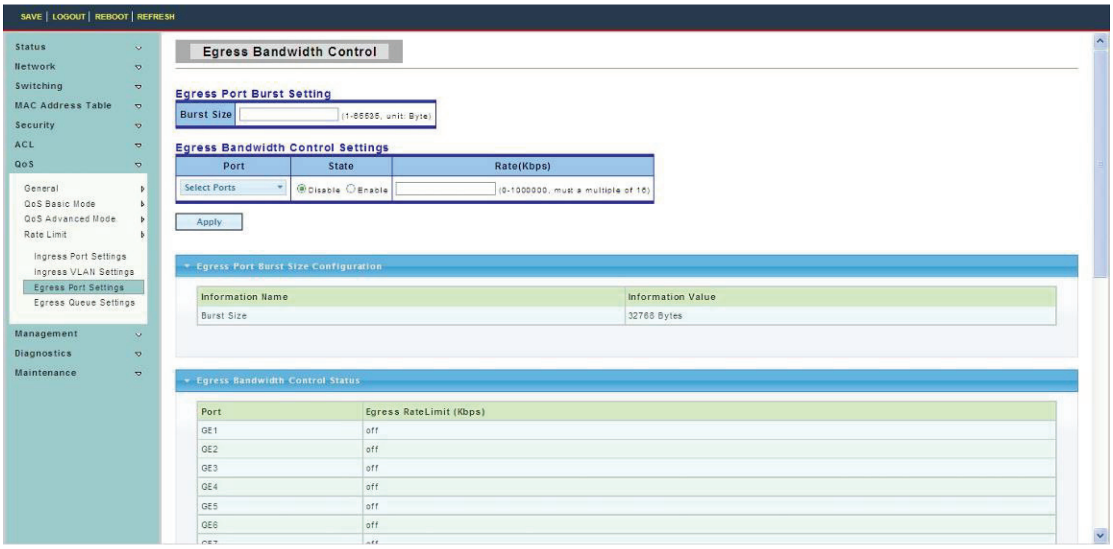
VLAN Ingress Rate Status

VLAN	Port	Rate (Kbps)

4.7.4.3 Egress 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.



Egress Bandwidth Control

Egress Port Burst Setting

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

Egress Bandwidth Control Settings

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

Egress Port Burst Size Configuration

Information Name	Information Value
Burst Size	32768 Bytes

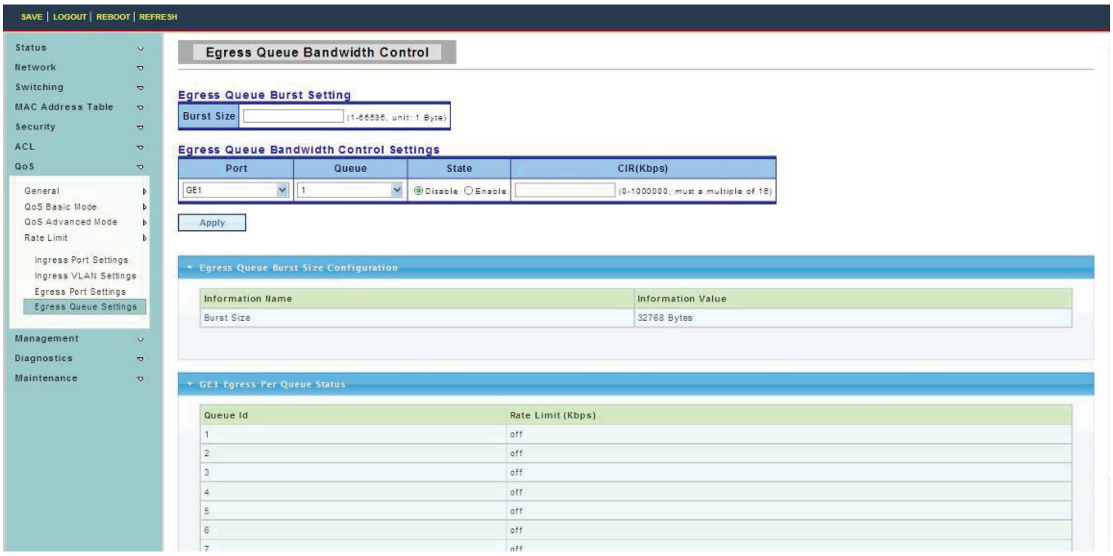
Egress Bandwidth Control Status

Port	Egress RateLimit (Kbps)
GE1	off
GE2	off
GE3	off
GE4	off
GE5	off
GE6	off
GE7	off

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.



Egress Queue Bandwidth Control

Egress Queue Burst Setting

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

Egress Queue Bandwidth Control Settings

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

Egress Queue Burst Size Configuration

Information Name	Information Value
Burst Size	32768 Bytes

GE1 Egress Per Queue Status

Queue Id	Rate Limit (Kbps)
1	off
2	off
3	off
4	off
5	off
6	off
7	off

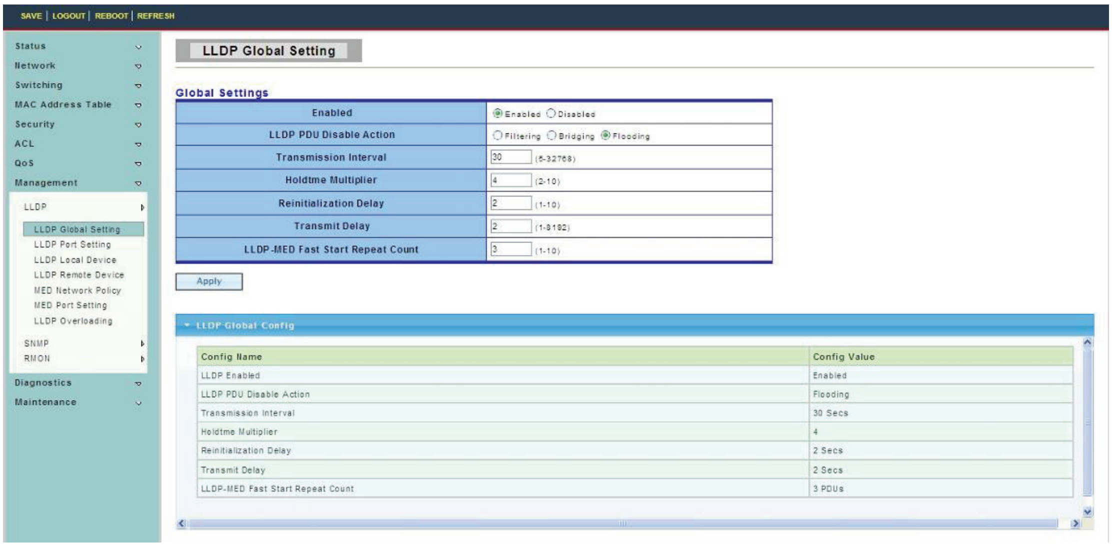
4.8 Management

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**



LLDP Global Setting

Global Settings

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

LLDP Global Config

Config Name	Config Value
LLDP Enabled	Enabled
LLDP PDU Disable Action	Flooding
Transmission Interval	30 Secs
Holdtme Multiplier	4
Reinitialization Delay	2 Secs
Transmit Delay	2 Secs
LLDP-MED Fast Start Repeat Count	3 PDUs

Enabled: Enable/ Disable LLDP protocol on this switch.

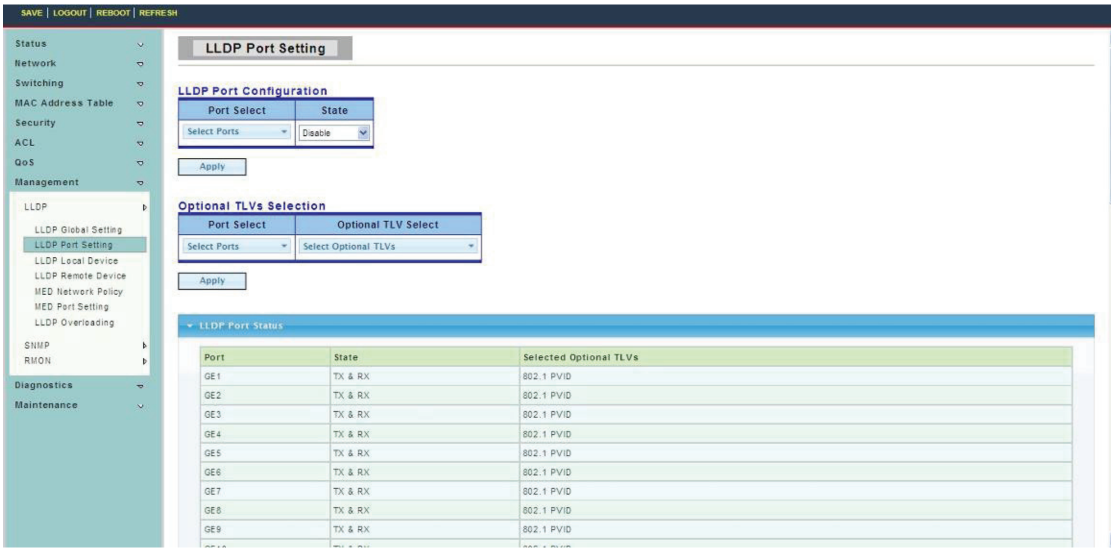
Transmission Interval: Select the interval at which frames are transmitted. The default is 30 seconds, and the valid range is 5–32768 seconds.

Hold time 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**



LLDP Port Setting

LLDP Port Configuration

Port Select	State
Select Ports	Disable

Optional TLVs Selection

Port Select	Optional TLV Select
Select Ports	Select Optional TLVs

LLDP Port Status

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
GE6	TX & RX	802.1 PVID
GE7	TX & RX	802.1 PVID
GE8	TX & RX	802.1 PVID
GE9	TX & RX	802.1 PVID

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.

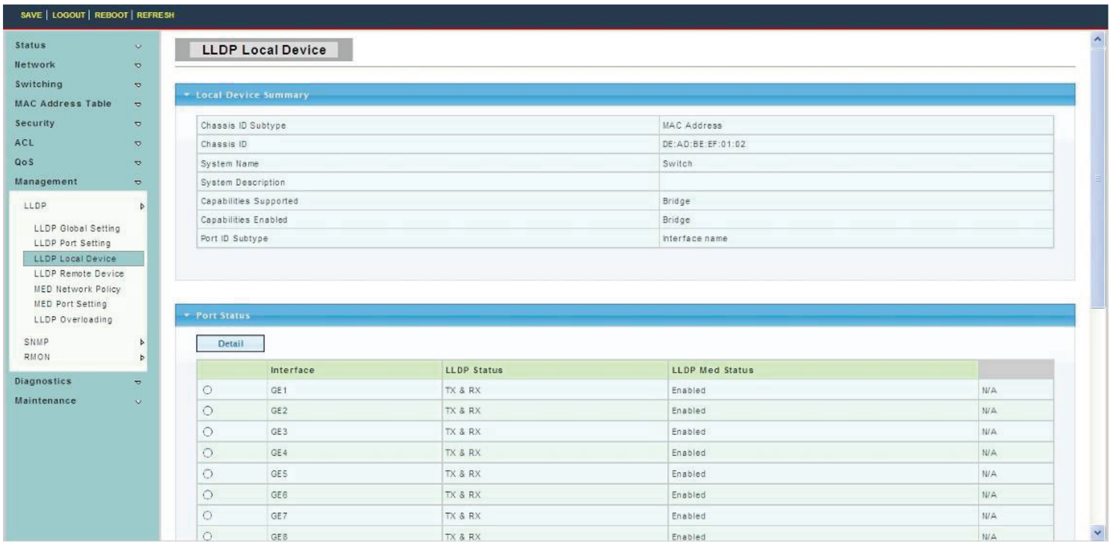
Port Select: Select specific ports.

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.



LLDP Local Device

Local Device Summary

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

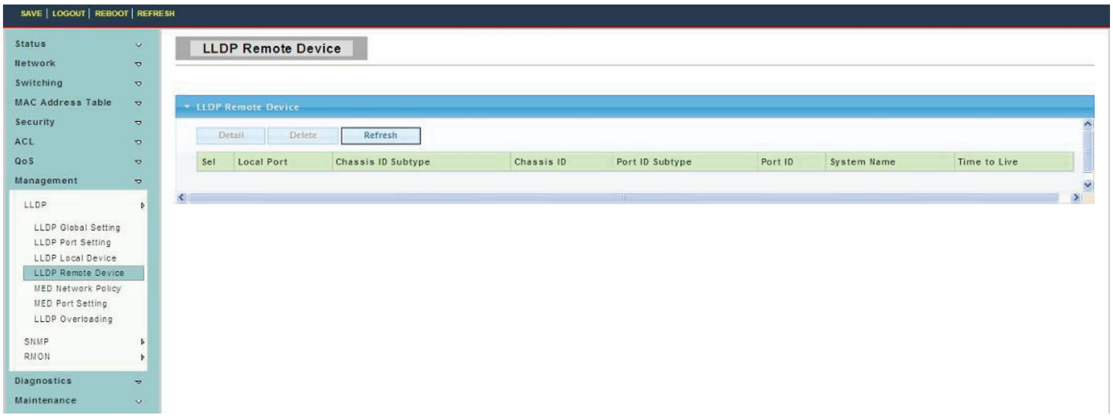
Port Status

	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
○	GE5	TX & RX	Enabled	N/A
○	GE6	TX & RX	Enabled	N/A
○	GE7	TX & RX	Enabled	N/A
○	GE8	TX & RX	Enabled	N/A

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.



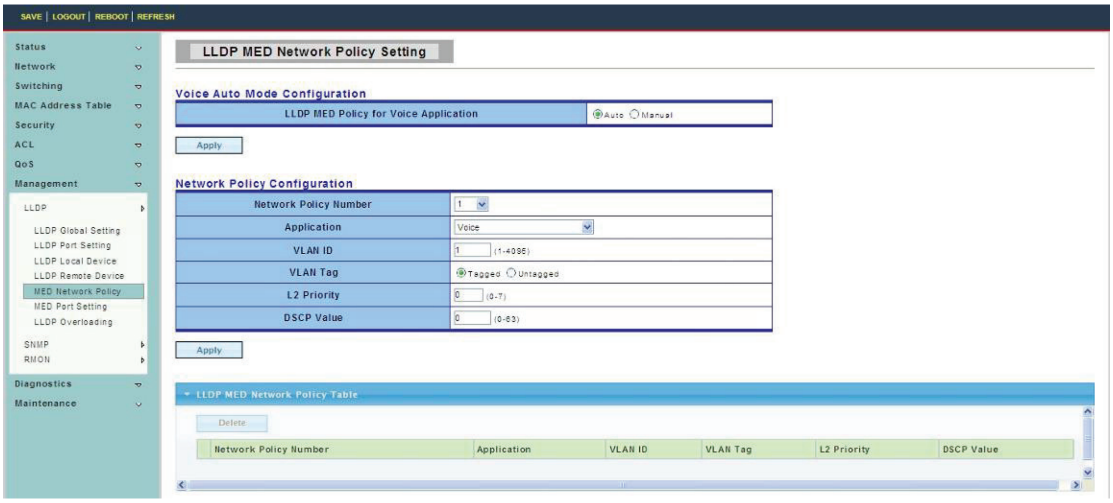
LLDP Remote Device

LLDP Remote Device

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

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

Network Policy Configuration

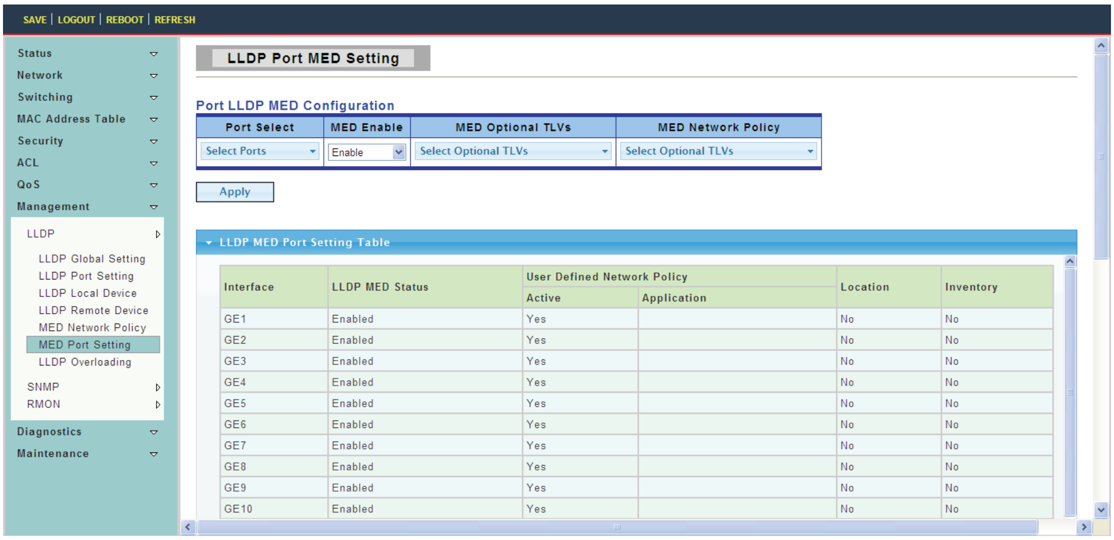
Network Policy Number	1
Application	Voice
VLAN ID	1 (1-4095)
VLAN Tag	● Tagged ○ Untagged
L2 Priority	0 (0-7)
DSCP Value	0 (0-63)

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

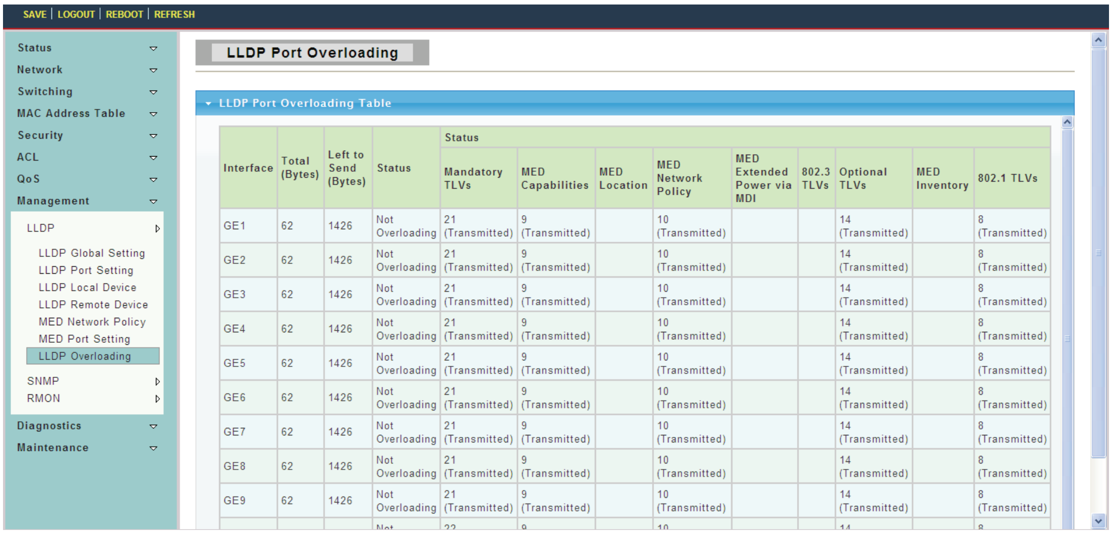
Port Select	MED Enable	MED Optional TLVs	MED Network Policy
Select Ports	Enable	Select Optional TLVs	Select Optional TLVs

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**



LLDP Port Overloading

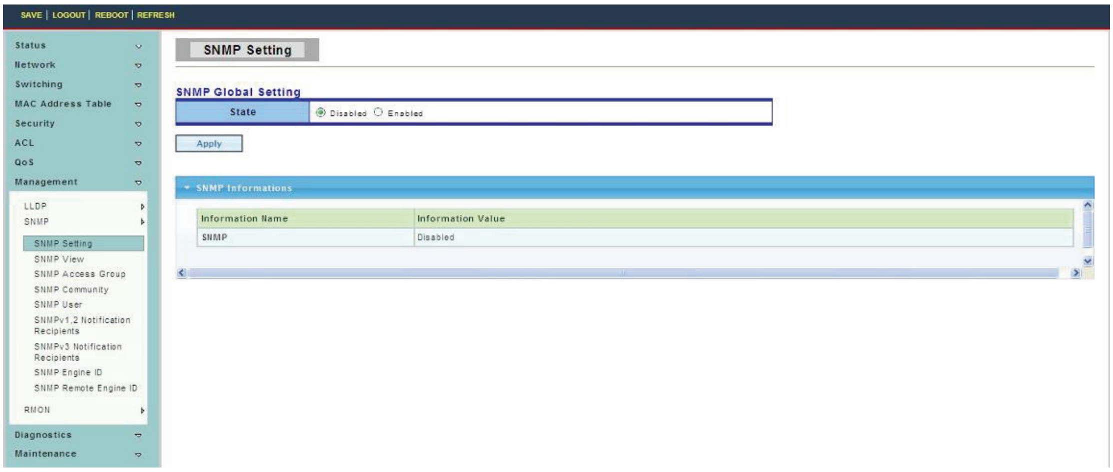
LLDP Port Overloading Table

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)
			Not	22	9		10			14		8

4.8.2 SNMP

4.8.2.1 SNMP Setting

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



SNMP Setting

SNMP Global Setting

State: ● Disabled ○ Enabled

SNMP Informations

Information Name	Information Value
SNMP	Disabled

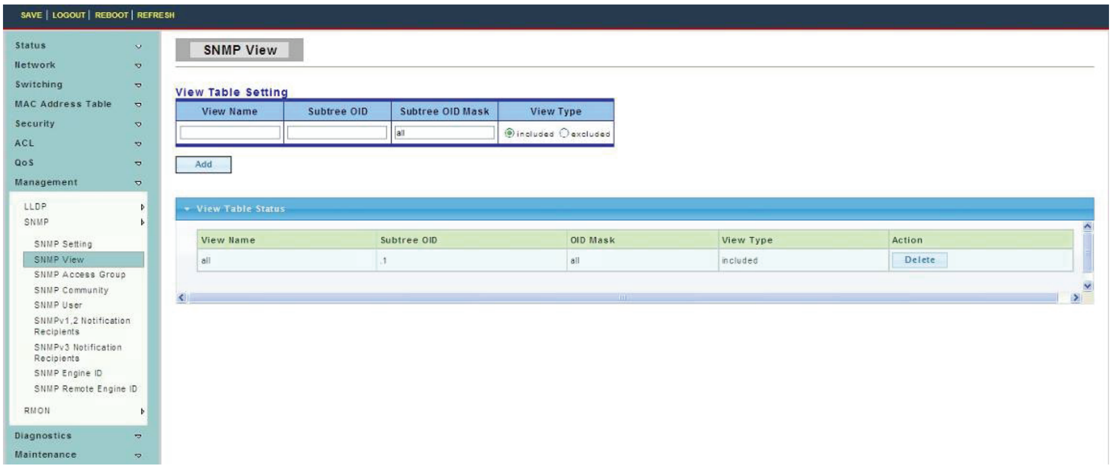
State: SNMP daemon state

- 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) is a set of monitoring network equipment Management variables. View is used to control, variable is how to be managed.



View Table Setting

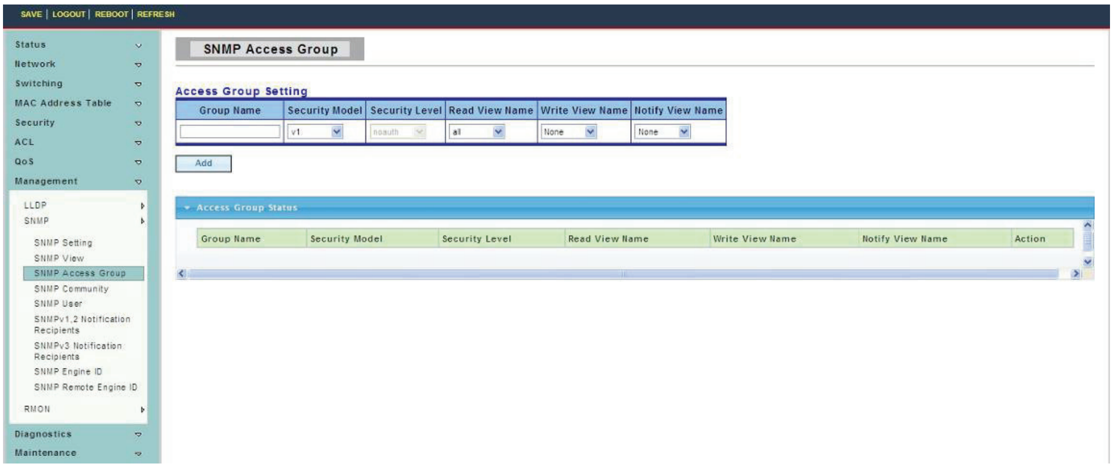
View Name	Subtree OID	Subtree OID Mask	View Type
		all	● included ○ excluded

View Name	Subtree OID	OID Mask	View Type	Action
all	.1	all	included	Delete

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 the user can set read-only or write only.



Access Group Setting

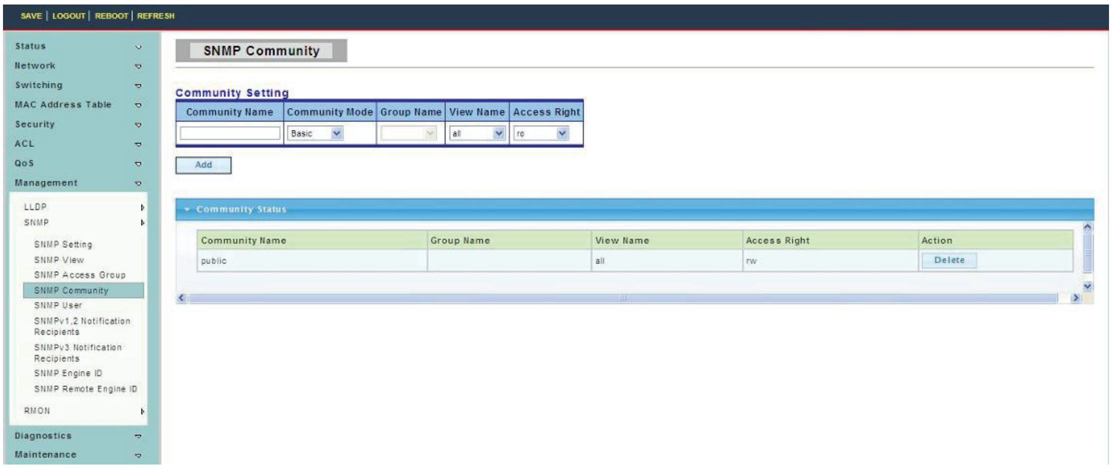
Group Name	Security Model	Security Level	Read View Name	Write View Name	Notify View Name
	v1	noauth	all	None	None

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

4.8.2.4 SNMP Community

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

SNMP v1 and SNMP v2c uses the group Name (Community Name) certification, which is similar to the password. If use SNMP v1 and SNMP v2c, after configuring SNMP view, the SNMP community can be directly configured.



SNMP Community

Community Setting

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

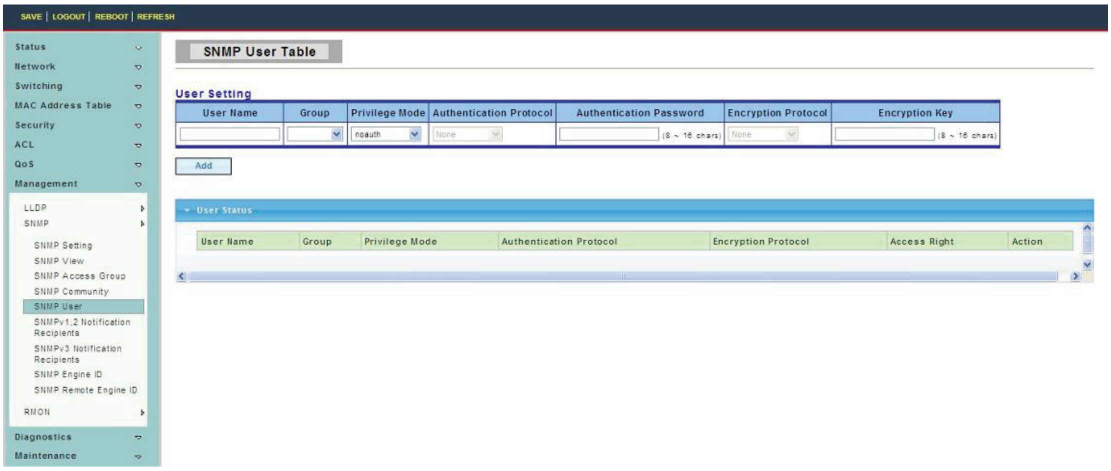
Community Status

Community Name	Group Name	View Name	Access Right	Action
public		all	rw	Delete

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.



SNMP User Table

User Setting

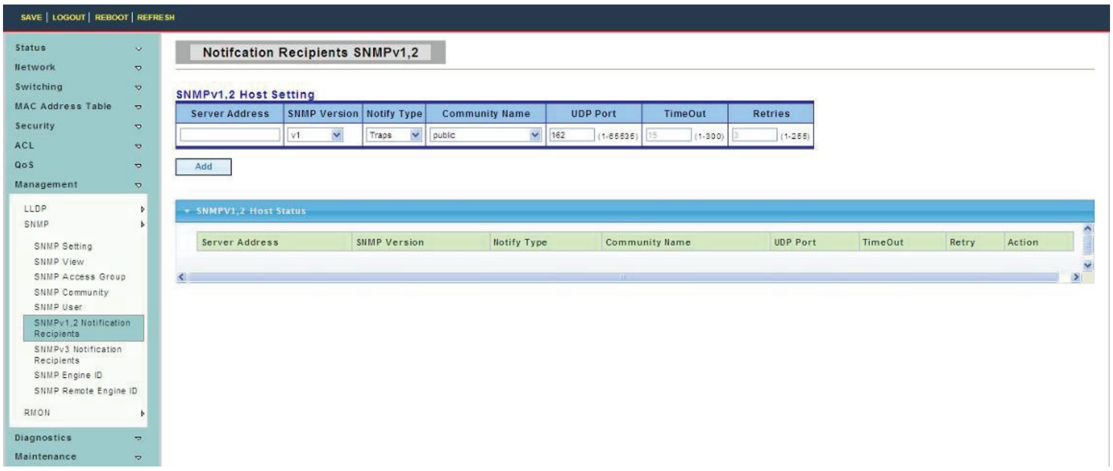
User Name	Group	Privilege Mode	Authentication Protocol	Authentication Password	Encryption Protocol	Encryption Key
		noauth	None	(8 ~ 16 chars)	None	(8 ~ 16 chars)

User Status

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

4.8.2.6 SNMPv1,2 Notification Recipients

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



Notifcation Recipients SNMPv1,2

SNMPv1,2 Host Setting

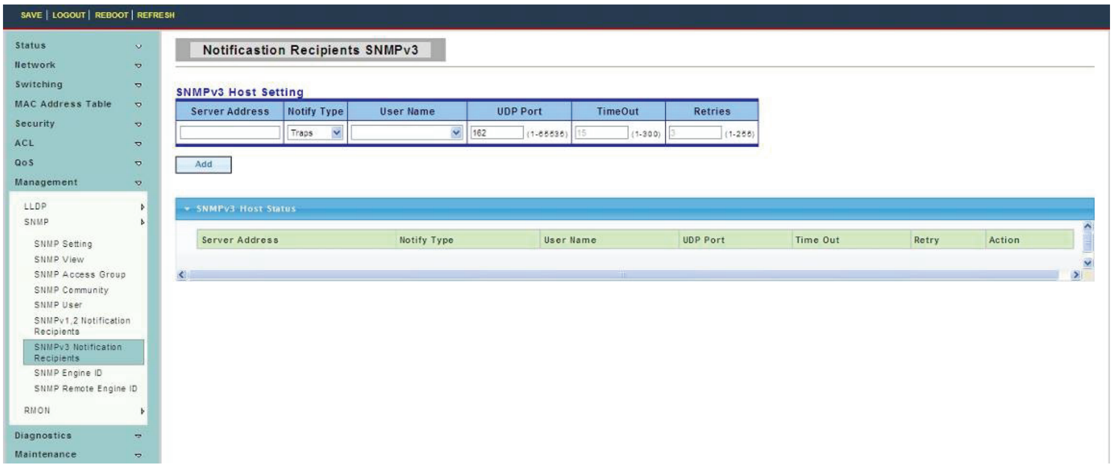
Server Address	SNMP Version	Notify Type	Community Name	UDP Port	TimeOut	Retries
	v1	Traps	public	162 (1-65535)	15 (1-300)	3 (1-255)

SNMPV1,2 Host Status

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

4.8.2.7 SNMPv3 Notification Recipients

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



Notificastion Recipients SNMPv3

SNMPv3 Host Setting

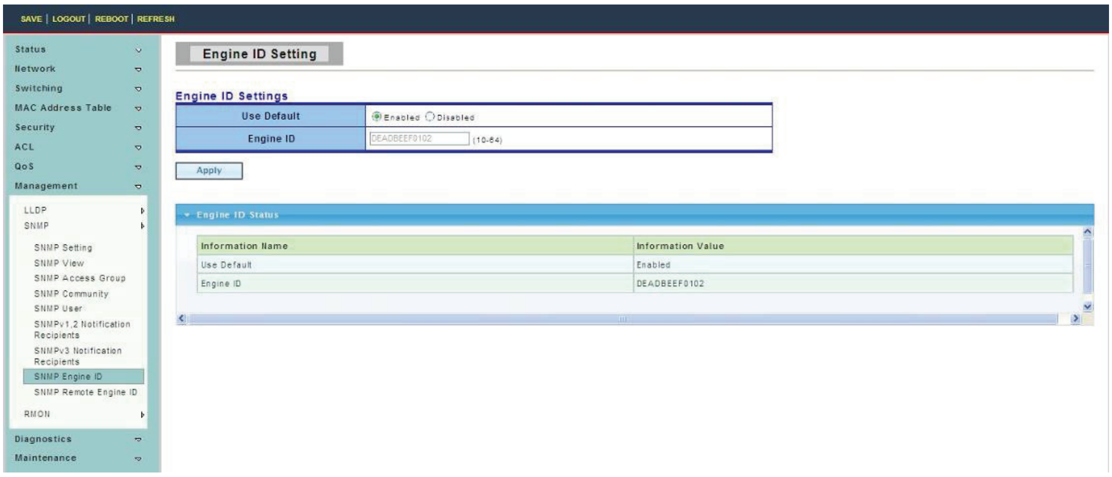
Server Address	Notify Type	User Name	UDP Port	TimeOut	Retries
	Traps		162 (1-65535)	15 (1-300)	3 (1-255)

SNMPv3 Host Status

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

4.8.2.8 SNMP Engine ID

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



Engine ID Setting

Engine ID Settings

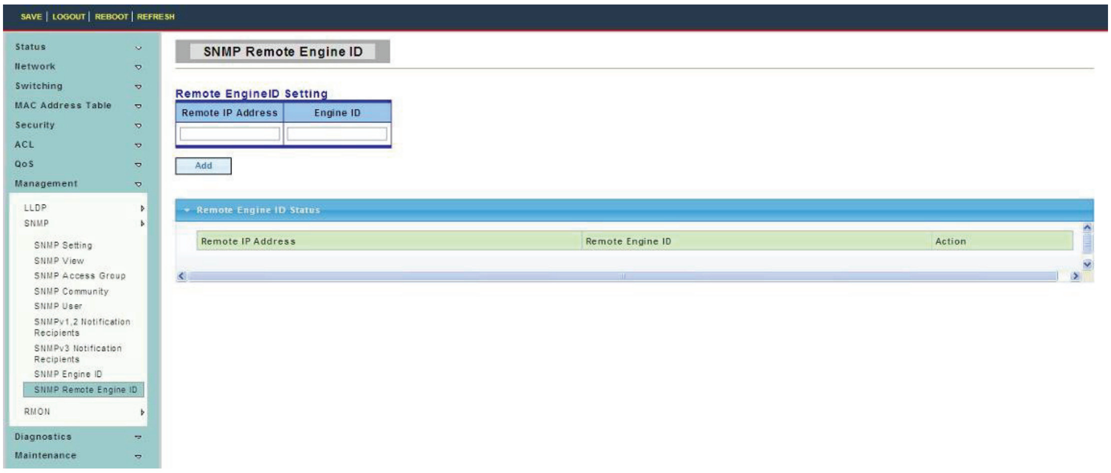
Use Default	● Enabled ○ Disabled
Engine ID	DEADBEEF0102 (10-64)

Engine ID Status

Information Name	Information Value
Use Default	Enabled
Engine ID	DEADBEEF0102

4.8.2.9 SNMP Remote Engine ID

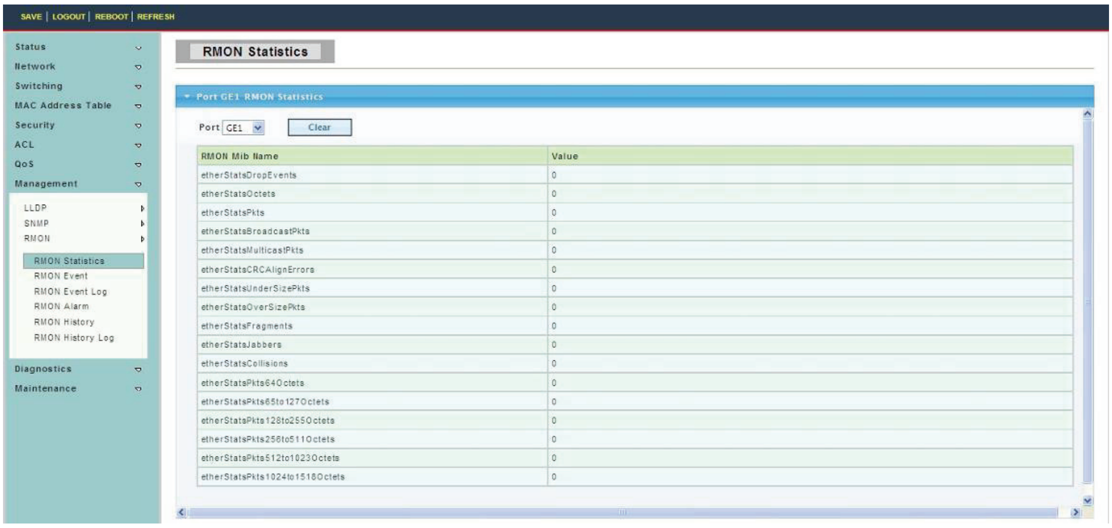
To display SNMP Remote Engine ID web page, click **Management > SNMP > SNMP Remote Engine ID**



4.8.3 RMON

4.8.3.1 RMON Statistics

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



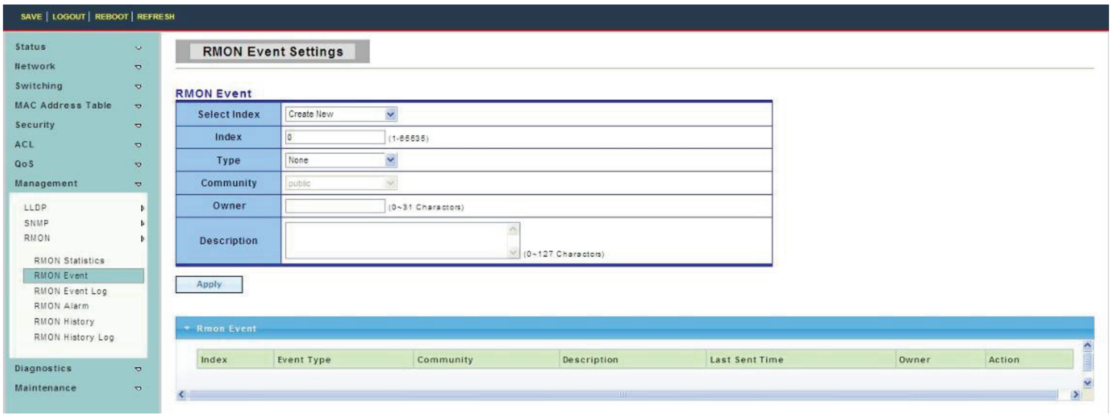
Port GE1

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
etherStatsPkts512to1023Octets	0
etherStatsPkts1024to1518Octets	0

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.



RMON Event Settings

RMON Event

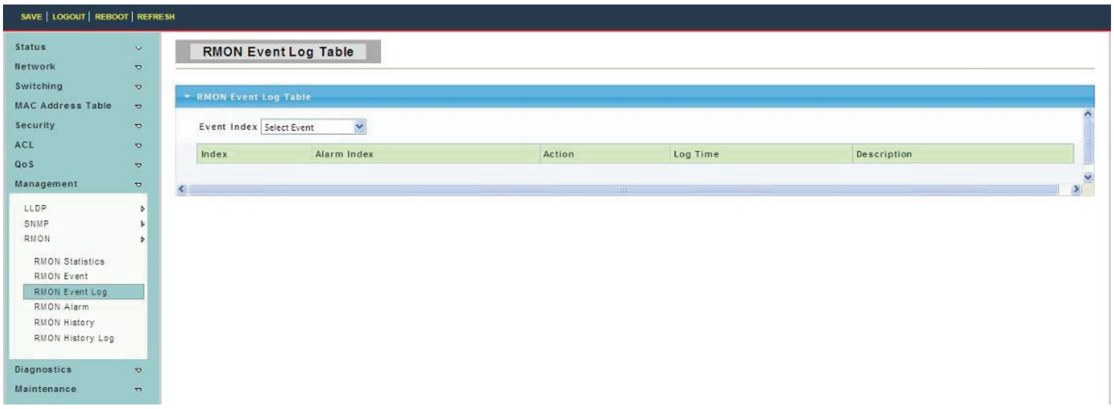
Select Index	Create New
Index	0 (1-65535)
Type	None
Community	public
Owner	(0~31 Characters)
Description	(0~127 Characters)

Rmon Event

Index	Event Type	Community	Description	Last Sent Time	Owner	Action

4.8.3.3 RMON Event Log

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



RMON Event Log Table

RMON Event Log Table

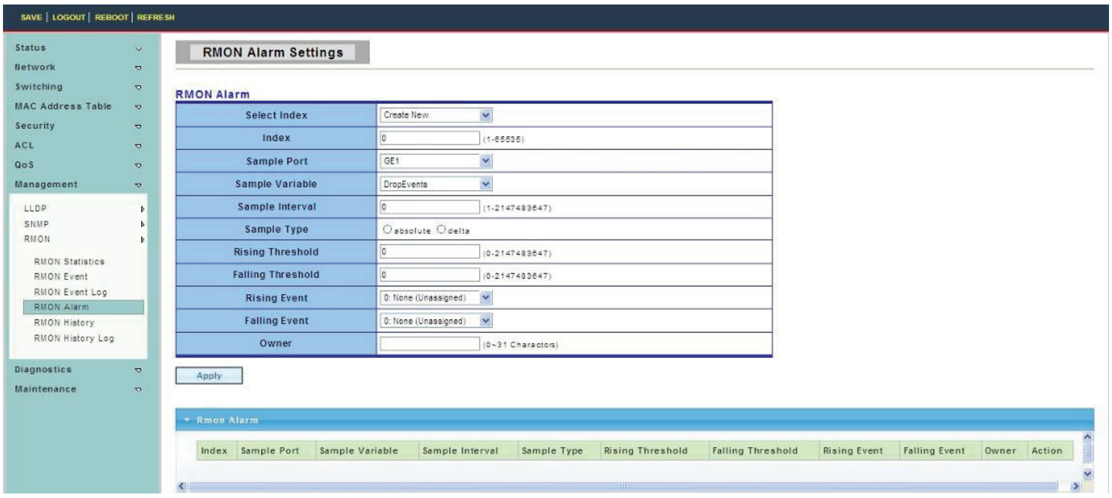
Event Index: Select Event

Index	Alarm Index	Action	Log Time	Description

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.



RMON Alarm Settings

RMON Alarm

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

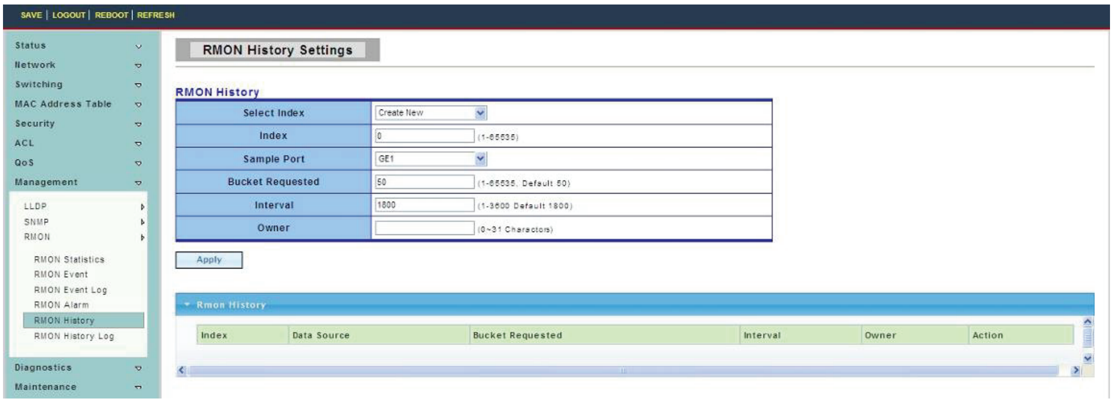
Rmon Alarm

Index	Sample Port	Sample Variable	Sample Interval	Sample Type	Rising Threshold	Falling Threshold	Rising Event	Falling Event	Owner	Action

4.8.3.5 RMON History

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

This page is used to configure the RMON history group.



RMON History Settings

RMON History

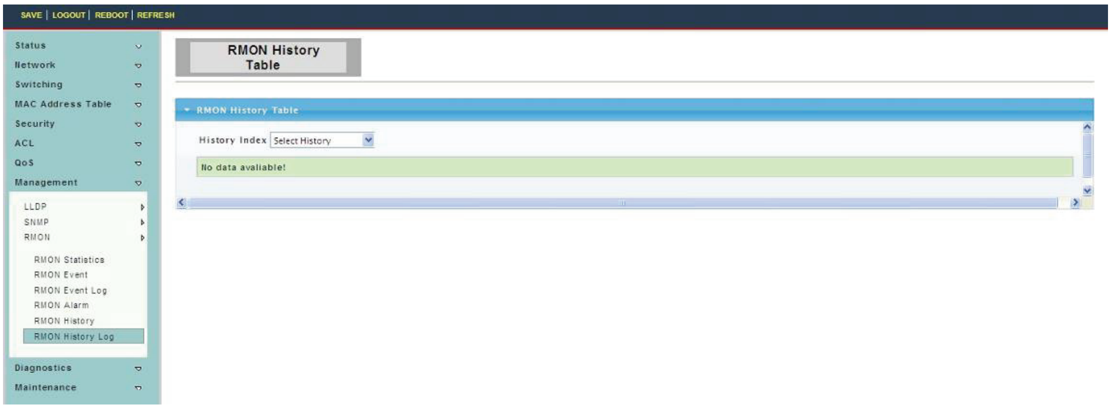
Select Index	Create New
Index	0 (1-65535)
Sample Port	GE1
Bucket Requested	50 (1-65535, Default 50)
Interval	1800 (1-3600 Default 1800)
Owner	(0~31 Characters)

Rmon History

Index	Data Source	Bucket Requested	Interval	Owner	Action

4.8.3.6 RMON History Log

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



RMON History Table

RMON History Table

History Index: Select History

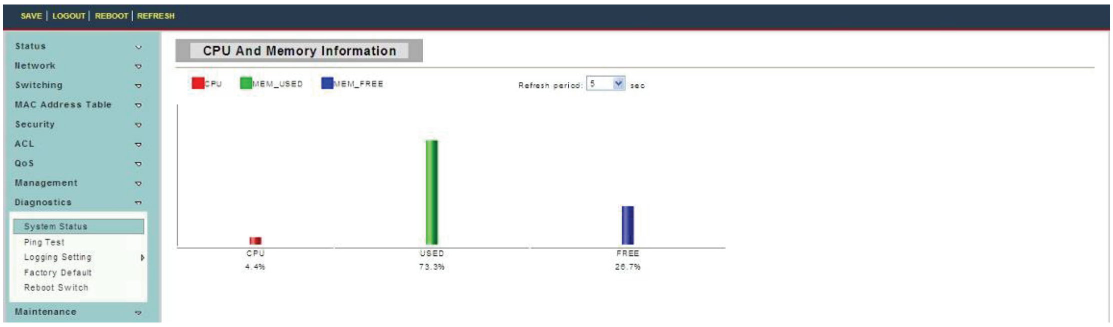
No data avaliable!

4.9 Diagnostics

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

4.9.1 System Status

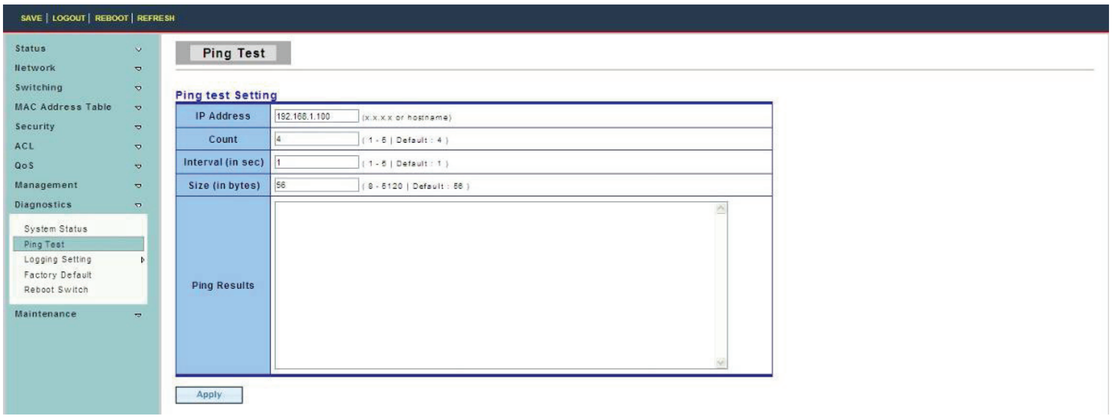
To display System Status Log web page, click **Diagnostics > System Status**



Refresh period: 5 sec

4.9.2 Ping Test

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



Ping Test

Ping test Setting

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

IP Address: The IP address of ping target.

Count: How many times to send ping request packet.

Interval: Time interval between each ping request packet.

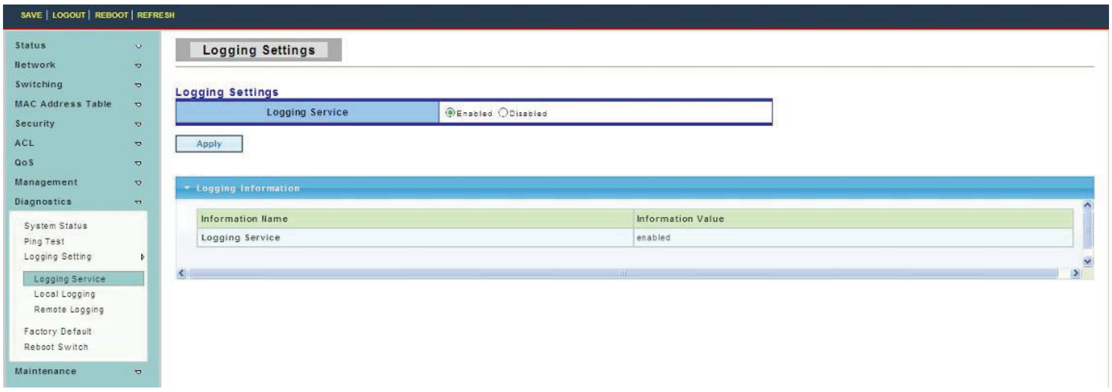
Size: The size of ping packet.

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**



Logging Settings

Logging Settings

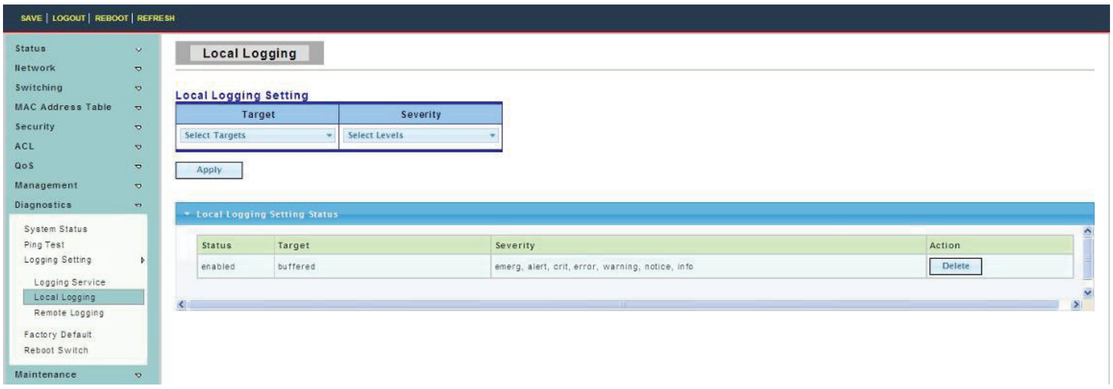
Logging Service: ● Enabled ○ Disabled

Logging Information

Information Name	Information Value
Logging Service	enabled

4.9.3.2 Local Logging

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



Local Logging

Local Logging Setting

Target	Severity
Select Targets	Select Levels

Local Logging Setting Status

Status	Target	Severity	Action
enabled	buffered	emerg, alert, crit, error, warning, notice, info	Delete

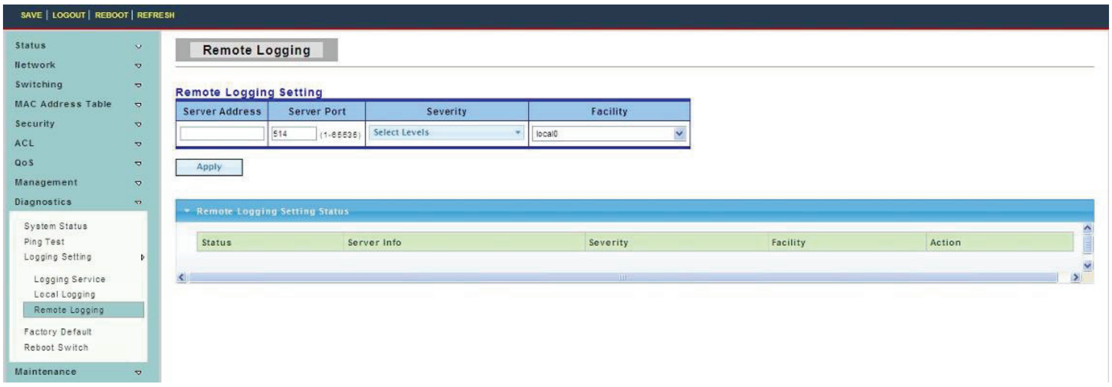
Target: Select the target to store log message

- 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**



Remote Logging

Remote Logging Setting

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

Remote Logging Setting Status

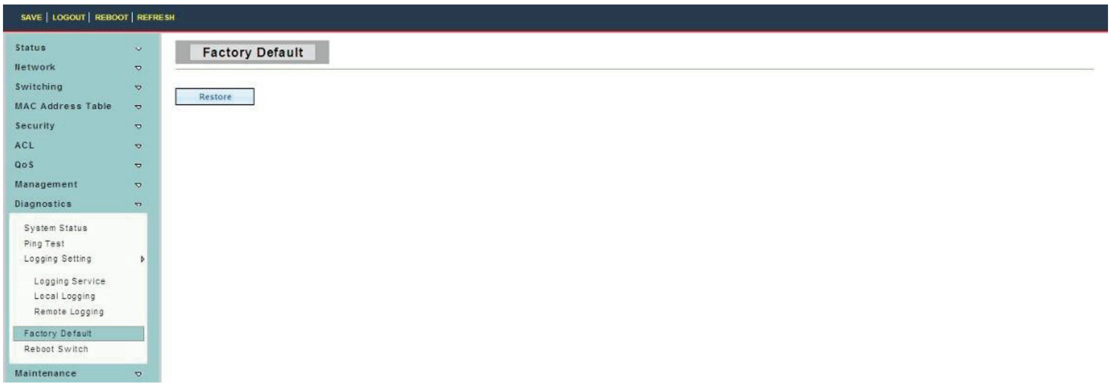
Status	Server Info	Severity	Facility	Action

Server Address: The IP address of 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**

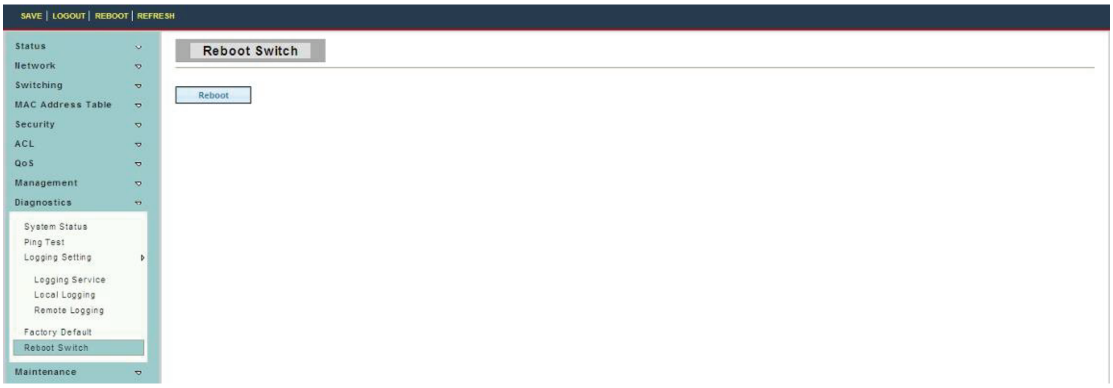
This page allow user to restore switch to factory default by pushing “Restore” button.



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.



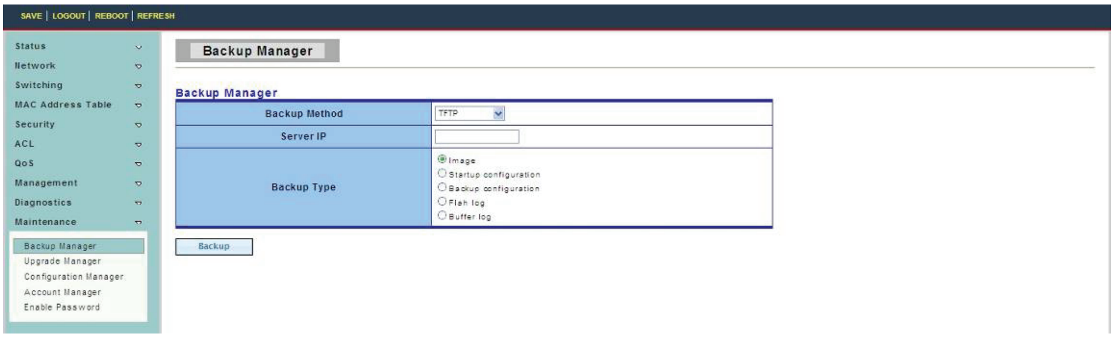
4.10 Maintenance

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

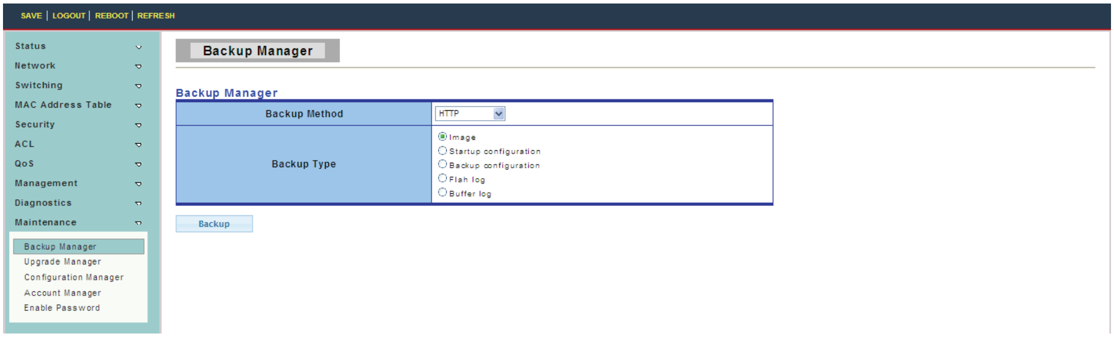
To display Backup Manager web page, click **Maintenance > Backup Manager**

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 Manager

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



Backup Manager

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

Backup Method: Select backup method

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

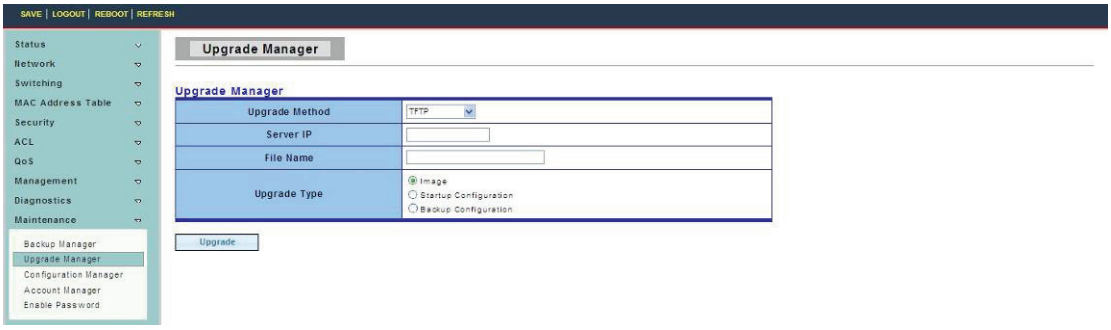
Server IP: IP address of the TFTP server. If the TFTP backup method is selected, the IP address of the TFTP server must be assigned.

Backup Type: Select Backup Type

4.10.2 Upgrade Manager

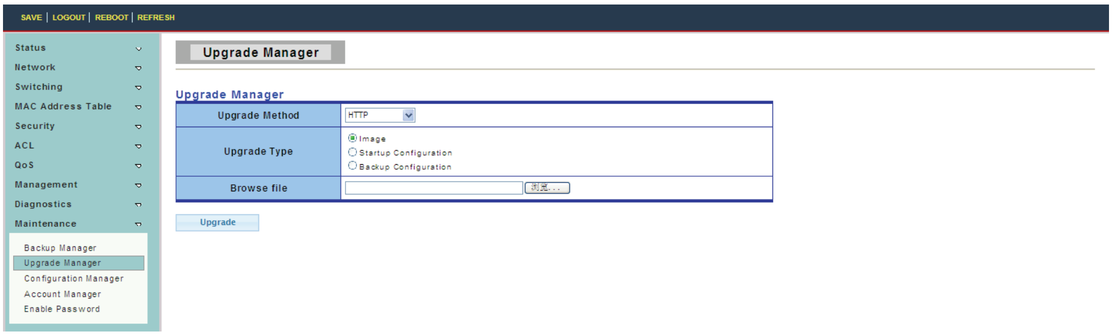
To display Upgrade Manager web page, click **Maintenance > Upgrade Manager**

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 Manager

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



Upgrade Manager

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

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.

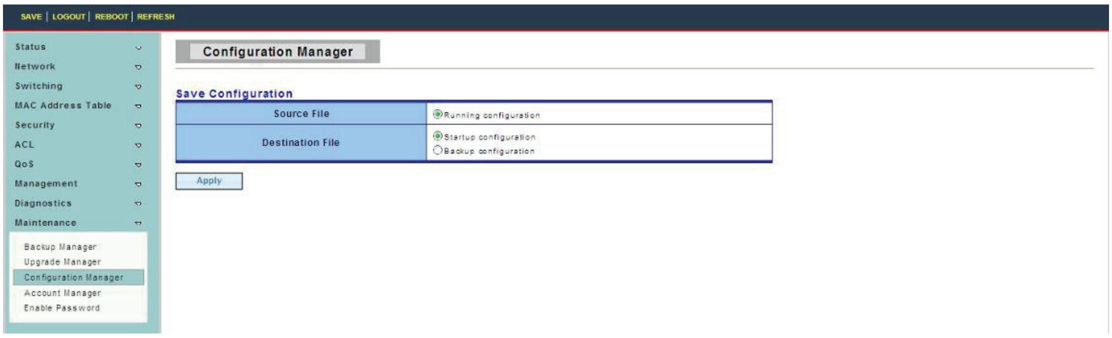
File Name: Firmware image or configuration file name on remote TFTP server. If the TFTP upgrade method is selected, the file name must be specified.

Browse file: If the HTTP upgrade method is selected, the browse file field allows 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**



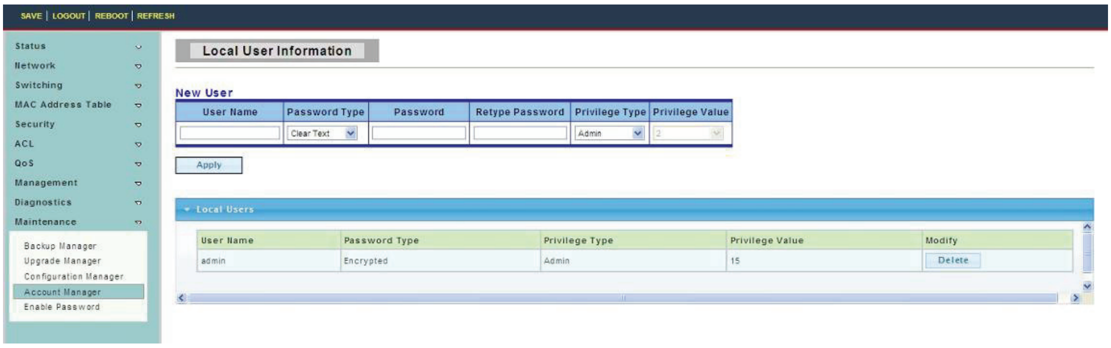
Save Configuration

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

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.



Local User Information

New User

User Name	Password Type	Password	Retype Password	Privilege Type	Privilege Value
	Clear Text			Admin	2

Local Users

User Name	Password Type	Privilege Type	Privilege Value	Modify
admin	Encrypted	Admin	15	Delete

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.

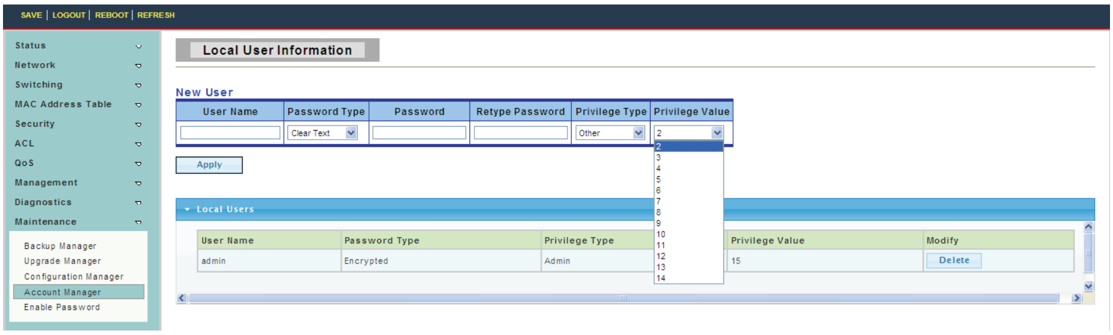
Password: If the password type is not “No Password”, the password must be specified.

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.



Local User Information

New User

User Name	Password Type	Password	Retype Password	Privilege Type	Privilege Value
	Clear Text			Other	2

Local Users

User Name	Password Type	Privilege Type	Privilege Value	Modify
admin	Encrypted	Admin	15	Delete

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.

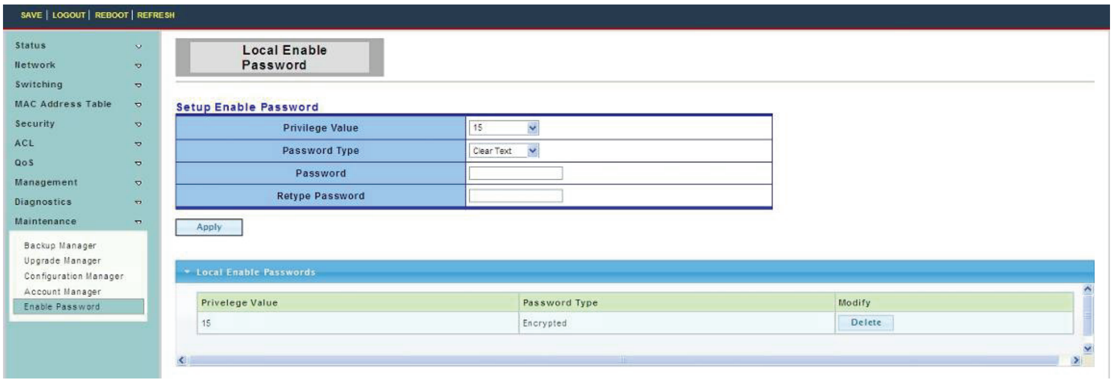
- Admin: Allow to change switch settings.
- User: See switch settings only. Not allow to change it.
- Other: Assign privilege level value in Privilege value field.

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.



Setup Enable Password

Privilege Value	15
Password Type	Clear Text
Password	
Retype Password	

Local Enable Passwords

Privelege 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.

Hinweis: Bei falscher Installation und unsachgemäßem Gebrauch im Wohnbereich kann das Gerät Störungen bei Rundfunkgeräten und anderen elektronischen Geräten verursachen. Ein sachgemäßer Gebrauch liegt vor, wenn das Gerät, soweit durchführbar, mit geschirmten Anschlusskabeln betrieben wird (bei Netzwerkprodukten zusätzlich geschirmter Kabel der Kategorie 5e und höher). Das Gerät wurde getestet und liegt innerhalb der Grenzen für Computerzubehör der Klasse A gemäß den Anforderungen nach EN 55022. Warnung: Dieses Produkt entspricht der Prüfklasse A –es kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen und dafür aufzukommen. Konformitätserklärung: Das Gerät erfüllt die EMV-Anforderungen nach EN 55022 Klasse A für ITE und EN 55024. Geräte mit externer oder eingebauter Spannungsversorgung erfüllen weiterhin die Anforderungen nach EN 61000-3-2 und EN 61000-3-3. Damit sind die grundlegenden Schutzanforderungen der EMV-Richtlinie 2004/108/EC erfüllt. Die CE-Konformität wurde nachgewiesen. Die entsprechenden Erklärungen sind beim Hersteller hinterlegt.

www.assmann.com
ASSMANN Electronic GmbH
Auf dem Schüffel 3
58513 Lüdenscheid
Germany