

24-PORT POE+ WEB-MANAGED GIGABIT
ETHERNET SWITCH WITH 2 SFP PORTS
USER MANUAL
MODEL 560559



INT-560559-UM-0116-1

1 TABLE OF CONTENTS

2	Product Introduction	4
2.1	Product Overview.....	4
2.2	Features.....	4
2.3	Specifications	5
2.4	External Component Description.....	6
2.4.1	Front Panel	6
2.4.2	Rear Panel.....	8
2.5	Package Contents.....	8
3	Installing and Connecting the Switch	9
3.1	Installation.....	9
3.1.1	Desktop Installation.....	9
3.1.2	Rack-mountable Installation in 19-inch Cabinet.....	10
3.1.3	Power on the Switch	11
4	Connection to the Switch	12
4.1	Connecting Computer.....	12
4.2	How to Login to the Switch	12
5	Switch Configuration	14
5.1	Status.....	14
5.1.1	System Information	14
5.1.2	Logging Message	15
5.1.3	Port	16
5.1.4	Link Aggregation.....	18
5.1.5	LLDP Statistics.....	19
5.1.6	IGMP Snooping Statistics	20
5.2	Network.....	21
5.2.1	IP Address	21
5.2.2	Time Settings	22
5.3	Switching	24
5.3.1	Port Setting.....	24
5.3.2	Error Disabled.....	26
5.3.3	Traffic Mirroring	27

5.3.4	Link Aggregation.....	28
5.3.5	VLAN Management	32
5.3.6	Multicast.....	37
5.3.7	Jumbo Frame	44
5.4	Mac Address Table	50
5.5	Security.....	53
5.6	ACL.....	70
5.7	QoS	73
5.8	Management.....	82
5.9	Diagnostics	96
5.10	Maintenance	99

2 PRODUCT INTRODUCTION

Congratulations on your purchase of the 24-Port PoE+ Web-Managed PoE+ Gigabit Ethernet Switch. Before you install and use this product, read this manual carefully for a full understanding of its functions.

2.1 PRODUCT OVERVIEW

The Web-Managed Gigabit Ethernet Switch provides a seamless network connection. It integrates 1000 Mbps Gigabit Ethernet, 100Mbps Fast Ethernet and 10Mbps Ethernet network capabilities in a highly flexible package. With 24 10/100/1000 Mbps Auto-Negotiation RJ45 ports, all ports support Auto MDI/MDIX function. The switch is a low-cost, easy-to-use, high-performance upgrade from your old network to a 1000 Mbps Gigabit network, essential in helping solve network bottlenecks that frequently develop as more advanced computer users and newer applications continue to demand greater network resources. For efficient management, the switch is equipped with a remote Web interface. The switch can be programmed for advanced switch management functions, such as Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, Security, Access Control, MAC Address Table, LLDP, Diagnostics, RMON and Maintenance. Its PoE ports can automatically detect and supply power to IEEE802.3at compliant Powered Devices (PD), such as Wireless Access Points, network cameras or Voice over IP phones.

2.2 FEATURES

- Provides power and data connection for up to 24 PoE network devices
- Save installation cost by delivering data and power over existing network cables
- IEEE 802.3at/af-compliant RJ45 PoE/PoE+ output ports
- PoE power budget of 240 watts
- Power output up to 30 watts per port
- Supports IEEE 802.3at and IEEE 802.3af-compliant PoE devices (wireless access points, VoIP phones, IP cameras)
- Supports IEEE 802.3at/af detection and short circuit, overload and high-voltage protection
- Supports SNMP management
- Two small form-factor pluggable GBIC module slots (SFP)
- Supports VLAN (tag-based and port-based)
- Provides IEEE 802.1x port-based security
- Supports link aggregation (trunking)
- Supports port mirroring
- Supports jumbo frames up to 9 kBytes

- Supports Rapid Spanning Tree/Spanning Tree protocol
- Broadcast storm control with multicast packet rate settings
- Supports two types of QoS: port-based and DSCP
- LEDs for power, link/activity and PoE
- Includes 19" rackmount brackets

2.3 SPECIFICATIONS

Standards

- IEEE 802.1d (Spanning Tree Protocol)
- IEEE 802.1p (Traffic Prioritization)
- IEEE 802.1q (VLAN Tagging)
- IEEE 802.1w (Rapid Spanning Tree Protocol)
- IEEE 802.3 (10Base-T Ethernet)
- IEEE 802.3ab (Twisted Pair Gigabit Ethernet)
- IEEE 802.3ad (Link Aggregation Control Protocol LACP)
- IEEE 802.3af (Power over Ethernet 802.3at Type 1)
- IEEE 802.3at (Power over Ethernet 802.3at Type 2)
- IEEE 802.3u (100Base-TX Fast Ethernet)
- IEEE 802.3x (flow control, for full duplex mode)

Power

- Input: 90 – 260 V AC, 50 – 60 Hz
- Power consumption: 260 watts (maximum)

Environmental

- Metal housing
- Dimensions: 440 (W) x 220 (L) x 44 (H) mm (17.3 x 8.7 x 1.7 in.)
- Weight: 3.1 kg (6.8 lbs.)
- Operating temperature: 0 – 45°C (32 – 113°F)
- Operating humidity: 10 – 90% RH, non-condensing
- Storage temperature: -20 – 90°C (-4 – 194°F)

Package Contents

- 24-Port Gigabit Ethernet PoE+ Web-Managed Switch with 2 SFP Ports
- Power cable
- User manual

2.4 EXTERNAL COMPONENT DESCRIPTION

2.4.1 Front Panel

The front panel of the Switch consists of 24 x 10/100/1000 Mbps 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.



10/100/1000 Mbps RJ-45 ports (1~24):

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

SFP ports (SFP1, SFP2):

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

Console port (Console):

Designed to connect with the serial port of a computer or terminal for monitoring and configuring the Switch.

Reset button (Reset):

To restore the system factory default settings, press the reset button for 5 seconds while the device is powered on.

LED indicators:

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



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
LINK/ACT/Speed (1~24)	10/100 Mbps: Amber	On	A device is connected to the port
	1000 Mbps: Green	Off	No device is connected to the port
		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
POE	Orange	On	An IEEE 802.3af/at compliant powered device (PD) is connected to the port, and the PoE Switch supplies power successfully.
		Off	No powered device is connected to the port.
		Flashing	There may be a short circuit or PoE power overload. Disconnect the device from this port immediately.

2.4.2 Rear Panel

**AC Power Connector:**

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

Grounding Terminal:

Ground the switch through the PE cable on the AC cord or with a separate ground wire.

2.5 PACKAGE CONTENTS

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

- 24-Port Gigabit Ethernet PoE+ Web-Managed Switch with 2 SFP Ports
- Power cable
- Quick Installation Guide
- User manual (on CD)
- Four rubber feet, two mounting ears and eight screws

3 INSTALLING AND CONNECTING THE SWITCH

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

3.1 INSTALLATION

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

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

3.1.1 Desktop Installation

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

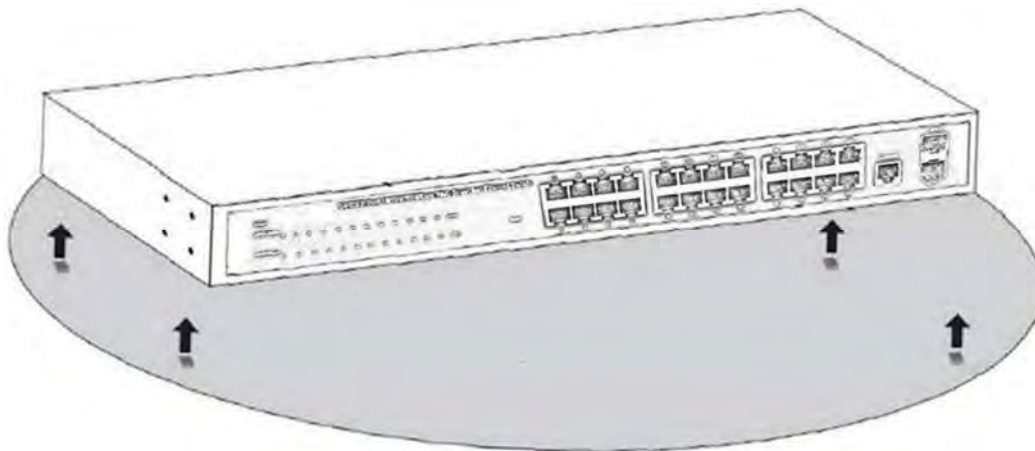


Figure 4 - Desktop Installation

3.1.2 Rack-mountable Installation in 19-inch Cabinet

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

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

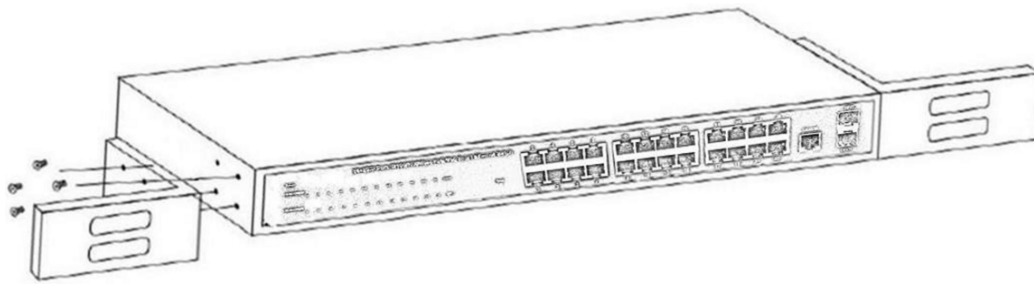


Figure 5 - Bracket Installation

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

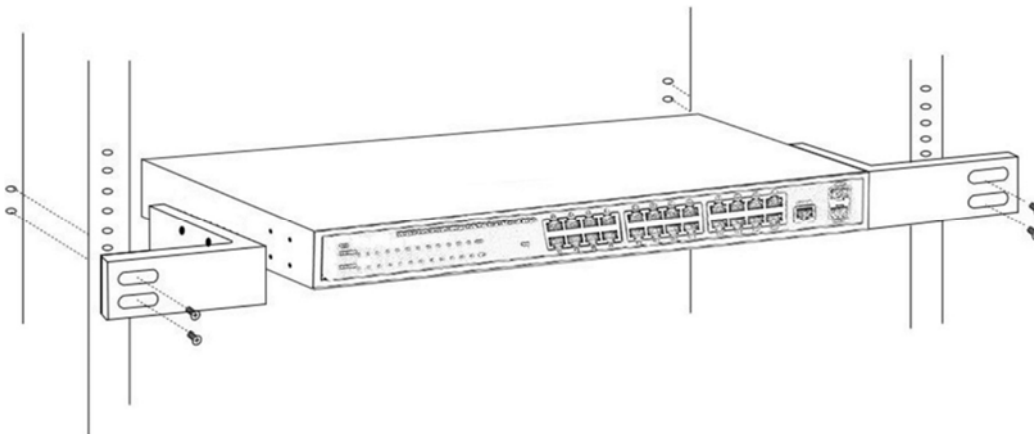


Figure 6 - Rack Installation

3.1.3 Power on the Switch

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

AC Electrical Outlet:

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

AC Power Cord Connection:

Connect the AC power connector on the back panel of the switch to an external receptacle with the included power cord, then check that the power indicator is ON. When it is ON, it indicates the power connection is okay.

4 CONNECTION TO THE SWITCH

4.1 CONNECTING COMPUTER

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

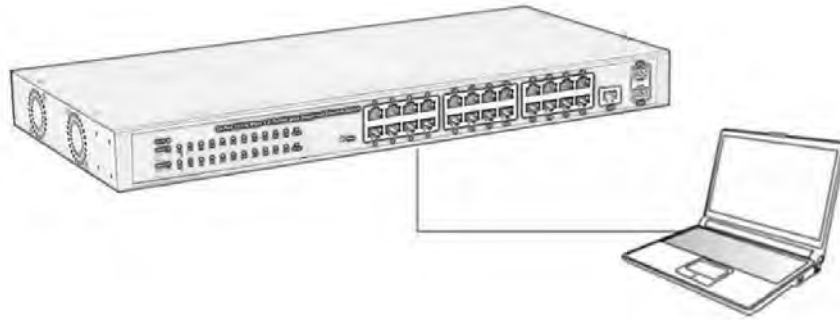


Figure 7 - PC Connect

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

4.2 HOW TO LOGIN TO THE SWITCH

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

Parameter	Default Value
Default IP address	192.168.2.1
Default Username	admin
Default Password	admin

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

1. Connect the switch with the computer NIC interface.
2. Power on the switch.
3. Check whether the IP address of the computer is within this network segment: 192.168.2.xxx ("xxx" range is 2-254); for example, 192.168.2.100.

4. Open the browser, and go to the URL <http://192.168.2.1>. The switch login window appears, as shown below.

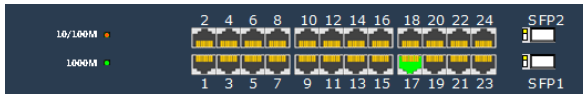


5. Enter the Username and Password (the factory default Username is **admin** and Password is **admin**), and then click “LOGIN” to log in to the switch configuration window as below.



5 SWITCH CONFIGURATION

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



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 (port 17 in the example above), 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.

5.1 STATUS

5.1.1 System Information

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

Information Name	Information Value
System Name	Edit Switch
System Location	Edit Default Location
System Contact	Edit Default Contact
MAC Address	DE:AD:BE:EF:01:02
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Gateway	192.168.2.254
Loader Version	2011.12.41872
Loader Date	Mar 18 2014 - 11:20:25
Firmware Version	V182M_1.26.X_26P_D150303-INTELLINET
Firmware Date	Tue Mar 3 10:19:22 CST 2015
System Object ID	1.3.6.1.4.1.27282.3.2.10
System Up Time	0 days, 6 hours, 47 mins, 13 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, e.g., "ServerRoom".

System Contact: System contact of the switch, e.g., the system administrator.

5.1.2 Logging Message

The Intellinet 24-Port Gigabit Ethernet PoE+ Web-Managed Switch is equipped with an extensive logging function. You can define the type of events you wish the switch to log, the level of detail and the target destination for the log.

The screenshot shows the web interface of the Intellinet switch. On the left is a navigation menu with categories like Status, Network, Switching, Security, ACL, QoS, Management, Diagnostics, and Maintenance. The 'Logging Message' option is selected under the Status category.

The main content area is titled 'Logging Filter Select' and contains three dropdown menus: Target (set to 'buffered'), Severity (set to 'Select Levels'), and Category (set to 'Select Categories'). Below these is a 'View' button.

Below the filter section, there are two expandable panels:

- Logging Information:** A table showing configuration details.

Information Name	Information Name
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:	7
- Logging Message:** A section with 'Clear' and 'Refresh' buttons, a pagination control showing '1' of 1 entries, and a table of log messages.

No.	Timestamp	Category	Severity	Message
1	Jan 01 11:06:11	STP	info	Port 17 STP port state is set to Forwarding

Target:

- **Buffered:** The Log information is stored in the RAM. All messages are lost when the switch loses power or is being restarted.
- **Flash:** Log information is stored in the FLASH memory and will be available after a system restart.

Severity: In a network there are events occurring constantly, and the Intellinet switch can log a great deal of these at runtime. With the severity filter you can define the threshold at which point an event is considered “log worthy”. “Emerg” only logs events which are considered an “Emergency”. That is the kind of event that would get a system administrator out of bed at 4 o’clock in the morning. “Debug” on the other hand is the polar opposite. In this mode there is nothing the switch considered unimportant. Choose whichever level is right for you.

The screenshot shows the 'Severity' selection dialog. It has a title bar 'Severity' and a dropdown menu 'Select Levels'. Below the dropdown are checkboxes for different severity levels: Emerg (checked), Alert, Crit, Error, Warning, Notice, Info, and Debug.

Category: Select what type of events the switch should log, for instance port related events, or events belong to the ACL Access Control List.

5.1.3 Port

The Port configuration page displays port summary and status information.

5.1.3.1 Port Counters

This page displays standard counters of network traffic using modes like Interface, EtherLike and RMON. Interfaces and EtherLike 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: Select any of the 24 RJ45 Gigabit Ethernet Ports (GE), 2 SFP ports, or 8 Link Aggregation Groups (LAG).

Mode: Select the filter you wish to apply to the displayed results.

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

Status

System Information

Logging Message

Port

Port Counters

Port Error Disabled

Bandwidth Utilization

Link Aggregation

LLDP Statistics

IGMP Snooping Statistics

Network

Switching

MAC Address Table

Security

ACL

QoS

Management

Diagnostics

Maintenance

Port Counters

Port MIB Counters Settings

Port	Mode
GE1	☒ All ☐ Interface ☐ Etherlike ☐ RMON

GE1 mib Counters

Clear

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
dot3StatsSingleCollisionFrames	0
dot3StatsMultipleCollisionFrames	0
dot3StatsDeferredTransmissions	0
dot3StatsLateCollisions	0
dot3StatsExcessiveCollisions	0
dot3StatsFrameTooLongs	0
dot3StatsSymbolErrors	0

5.1.3.2 Port Error Disabled

Some protocols such as BPDU Guard, Loop back and UDLD can disable ports to protect the rest of the network, for instance if the switch detects that one of the attached network interface cards is malfunctioning and flooding the network with error packets.

Ideally, you want this screen to look as shown below.

The screenshot shows the 'Port Error Disabled Status' page. On the left is a navigation menu with categories: Status, Network, Switching, MAC Address Table, Security, ACL, QoS, Management, Diagnostics, and Maintenance. Under 'Status', there are links for System Information, Logging Message, Port, Port Counters, Port Error Disabled (highlighted), and Bandwidth Utilization. Under 'Network', there are links for Link Aggregation, LLDP Statistics, and IGMP Snooping Statistics. The main content area has a title 'Port Error Disabled Status' and a sub-header 'Port Error Disabled Status'. Below this is a table with three columns: Port Name, Error Disabled Reason, and Time Left (Seconds). The table is currently empty.

5.1.3.3 Bandwidth Utilization

This page displays the TX (transmit) and RX (receive) bandwidth utilization for each port.



5.1.4 Link Aggregation

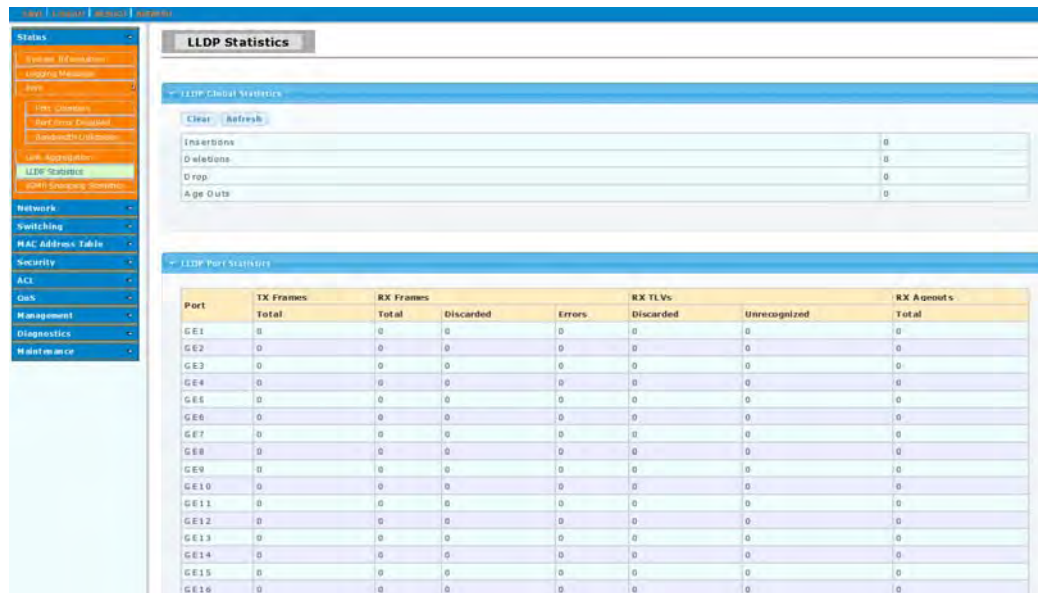
Link aggregation is a method of using multiple Ethernet ports in parallel to increase throughput beyond what a single connection could sustain, and to provide redundancy in case one of the links should fail. As this is essentially a grouping of ports into one logical unit, we call them Link Aggregation Groups, or “LAG” for short. Any LAG that is currently defined will be shown on this screen. The configuration of the LAG will be addressed later in the section “Switching”.



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		

5.1.5 LLDP Statistics

The Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, principally wired Ethernet. The LLDP statistics page displays an overall summary and per-port information for LLDP frames transmitted and received on the switch.



The screenshot shows the 'LLDP Statistics' page. On the left is a navigation menu with categories like Status, Network, Switching, MAC Address Table, Security, and Management. The main content area is titled 'LLDP Statistics' and contains two sections: 'LLDP Global Statistics' and 'LLDP Port Statistics'.

LLDP Global Statistics: This section has 'Clear' and 'Refresh' buttons and a table with the following data:

Insertions	Deletions	Drops	Age Outs
0	0	0	0

LLDP Port Statistics: This section contains a table with the following data:

Port	TX Frames		RX Frames		Errors	RX TLVs		RX Agnouts
	Total	Discarded	Total	Discarded		Discarded	Unrecognized	
GE1	0	0	0	0	0	0	0	0
GE2	0	0	0	0	0	0	0	0
GE3	0	0	0	0	0	0	0	0
GE4	0	0	0	0	0	0	0	0
GE5	0	0	0	0	0	0	0	0
GE6	0	0	0	0	0	0	0	0
GE7	0	0	0	0	0	0	0	0
GE8	0	0	0	0	0	0	0	0
GE9	0	0	0	0	0	0	0	0
GE10	0	0	0	0	0	0	0	0
GE11	0	0	0	0	0	0	0	0
GE12	0	0	0	0	0	0	0	0
GE13	0	0	0	0	0	0	0	0
GE14	0	0	0	0	0	0	0	0
GE15	0	0	0	0	0	0	0	0
GE16	0	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.

5.1.6 IGMP Snooping Statistics

The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships. IGMP is an integral part of IP multicast. IGMP can be used for one-to-many networking applications such as online streaming video and gaming, and allows more efficient use of resources when supporting these types of applications.

This page displays the IGMP statistics information, also referred to as 'Snooping Statistics'.



Statistics Packets	Counter
Total RX	128
Valid RX	3
Invalid RX	125
Other RX	0
Leave RX	0
Report RX	0
General Query RX	0
Special Group Query RX	0
Special Group & Source Query RX	0
Leave TX	0
Report TX	0
General Query TX	0
Special Group Query TX	0
Special Group & Source Query TX	0

5.2 NETWORK

Use the Network page to configure settings for the switch network interface and set up the time related settings.

5.2.1 IP Address

Define the IP address of the switch here.



The screenshot shows the 'IP Address' configuration page. On the left is a navigation menu with options: Status, Network, IP Address (selected), Time Settings, Switching, MAC Address Table, Security, ACL, QoS, Management, Diagnostics, and Maintenance. The main content area is titled 'IP Address' and contains the 'IP Address Setting' section. This section has a 'Mode' dropdown set to 'Static' (with 'DHCP' also visible). Below are three input fields: 'IP Address' (192.168.2.1), 'Subnet Mask' (255.255.255.0), and 'Gateway' (192.168.2.254). An 'Apply' button is located below these fields. At the bottom, the 'IP Information' section displays the current settings in a table:

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

Mode: Select the mode of network connection.

- Static: Define the IP address manually. The IP address, subnet mask and gateway address must be provided.
- DHCP: obtain IP information from a DHCP server on the network.

Note that you have multiple of these switches installed in your network, you must assign a unique IP address to each of them, even if you don't plan on using any of the smart features of the switch. As a reminder, the default IP address of this switch is 192.168.2.1.

5.2.2 Time Settings

5.2.2.1 System Time

For the switch to accurately flag messages with the correct date and time stamp, the switch's system time must be set up first. Set "Enable SNTP" to "Disabled" if you do not want to sync the switch system time with an external time server, but rather want to configure it manually.

The screenshot shows the 'System Time' configuration page. On the left is a navigation menu with categories: Status, Network, Switching, MAC Address Table, Security, ACL, QoS, Management, Diagnostics, and Maintenance. Under 'Network', 'Time Settings' is selected, showing 'System Time' and 'SNTP Settings'. The main content area is titled 'System Time' and contains a 'System Time Setting' form. This form includes:

- 'Enable SNTP' with radio buttons for 'Disabled' (selected) and 'Enabled'.
- 'Manual Time' with dropdowns for Year (2000), Month (1), Day (1), Hours (0), and Minutes (0).
- 'Time Zone' set to 'None'.
- 'Daylight Saving Time' set to 'Disabled'.
- 'Daylight Saving Time Offset' set to '(0)' minutes.
- 'Recurring From' and 'Recurring To' with date and time dropdowns.
- 'Non-recurring From' and 'Non-recurring To' with date and time dropdowns.

 Below the form is an 'Apply' button. Underneath is a 'System Time Informations' section containing a table with the following data:

Information Name	Information Value
Current Date/Time	08:26:22 DFL(UTC+8) Jan 04 2000
Enable SNTP	Disabled
Time Zone	UTC+8
Daylight Saving Time	Disabled
Daylight Saving Time Offset	
From	
To	

5.2.2.2 SNTP Settings

If you wish to synchronize the switch system time with an external time server, also referred to as an NTP or SNTP server, then you can provide the IP address or host name of said server on this screen. Unless you know it to be different, it is recommend to leave the server port as '123'. If you have a NTP server in your LAN, then you can utilize that too, of course.

The screenshot shows the 'SNTP Server Settings' configuration page. The left navigation menu is the same as in the previous screenshot, with 'SNTP Settings' selected under 'Time Settings'. The main content area is titled 'SNTP Server Settings' and contains a form with:

- 'SNTP/NTP Server Address' with a text input field and a hint '(X.X.X.X or Hostname)'.
- 'Server Port' with a text input field containing '123' and a hint '(1 - 65535 | Default : 123)'.

 Below the form is an 'Apply' button. Underneath is an 'SNTP Server Informations' section containing a table with the following data:

Information Name	Information Value
SNTP/NTP Server Address	
Server Port	0

5.3 SWITCHING

5.3.1 Port Setting

On this screen you can configure basic aspects of each of the ports.

Port Setting

Port Select	Enabled	Speed	Duplex	Flow Control
Select Ports	☒ Enabled ☐ Disabled	Auto	Auto	☐ Enabled ☒ Disabled
Fiber Ports	☒ Enabled ☐ Disabled	Auto-1000	Full	☐ Enabled ☒ Disabled

Apply

Port Status

Port	Description	Enable State	Link Status	Speed	Duplex	FlowCtrl Config	FlowCtrl Status
GE1	Edit	Enabled	Disabled	Auto	Auto	Disabled	Disabled
GE2	Edit	Enabled	Disabled	Auto	Auto	Disabled	Disabled
GE3	Edit	Enabled	Disabled	Auto	Auto	Disabled	Disabled
GE4	Edit	Enabled	Disabled	Auto	Auto	Disabled	Disabled
GE5	Edit	Enabled	Disabled	Auto	Auto	Disabled	Disabled
GE6	Edit	Enabled	Disabled	Auto	Auto	Disabled	Disabled
GE7	Edit	Enabled	Disabled	Auto	Auto	Disabled	Disabled
GE8	Edit	Enabled	Disabled	Auto	Auto	Disabled	Disabled
GE9	Edit	Enabled	Disabled	Auto	Auto	Disabled	Disabled
GE10	Edit	Enabled	Disabled	Auto	Auto	Disabled	Disabled
GE11	Edit	Enabled	Disabled	Auto	Auto	Disabled	Disabled
GE12	Edit	Enabled	Disabled	Auto	Auto	Disabled	Disabled
GE13	Edit	Enabled	Disabled	Auto	Auto	Disabled	Disabled
GE14	Edit	Enabled	Disabled	Auto	Auto	Disabled	Disabled
GE15	Edit	Enabled	Disabled	Auto	Auto	Disabled	Disabled

Port Select:

Select one or multiple ports to configure.

Enabled:

Enable or disable the port. Disabling the power will also cut off power to any connected PoE powered device.

Enabled

☒ Enabled ☐ Disabled

Speed:

Typically you set to speed to “Auto,” which stands for auto-negotiation. In this mode the connection will be made at the fastest possible speed. In very rare cases, however, this auto-negotiation can fail, and you need to manually adjust the speed to whatever the connecting device is capable of.

Speed

Auto

Auto-10M

Auto-100M

Auto-1000M

Auto-10/100M

10M

100M

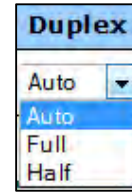
1000M

Duplex:

In a full duplex system, both parties can communicate to the other simultaneously.

An example of a full-duplex device is a telephone; the parties at both ends of a call can speak and be heard by the other party simultaneously. In networking terms, full duplex allows receiving and transmitting of data at the same time, whereas half duplex does not. If the telephone is an example for full duplex, then a push-to-talk

CB radio or 'walkie-talkie' represents half duplex. The switch can either receive or send data, but it can never happen simultaneously. Unless you have any specific reason not to do so, this should be left in "Auto" mode.

**Flow Control:**

IEEE 802.3x flow control is the process of managing the rate of data transmission between two nodes, i.E. the switch and a connected network client, to prevent a fast sender from

overwhelming a slow receiver. It provides a mechanism for the

receiver to control the transmission speed, so that the receiving node is not overwhelmed with data from transmitting node. That sounds like it is a good thing, and it is, but why then is the option by default set to "disabled" you might ask. The short answer is: Because you normally don't need it, and because it can in very rare circumstances have a negative impact on the overall performance in your network. The TCP protocol already provides its own flow control mechanism, allowing a sender to throttle back the speed if the receiver is having problems keeping up.



5.3.2 Error Disabled

This page allows you to define the parameters for the automatic port disable function.

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

Apply

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
ACL	Disabled
Port Security Violation	Disabled
DHCP rate limit	Disabled
ARP rate limit	Disabled

Recovery Interval: The switch will automatically re-enable ports that have been previously disabled, after the recovery interval time has elapsed.

BPDU Guard: BPDUs are sent out as multicast frames to which only other layer 2 switches or bridges are listening. If any loops (multiple possible paths between switches) are found in the network topology, the switches will co-operate to disable a port or ports to ensure that there are no loops.

Flood: The network can get overwhelmed by a large amount of unicast packets that can literally flood the entire network and can consume sufficient network resources so as to render the network unable to transport normal traffic.

ACL/Port Security Violation: Security related threads that violate the Access Control List settings can be caught by the switch, and drastic measures can be taken, namely disable the port from which the packets originate.

DHCP/ARP Rate Limit: Ports are disabled that exceed the DHCP request and ARP rate limits.

5.3.3 Traffic Mirroring

Port mirroring is the ability of a network switch to send a copy of network packets seen on a switch port or ports to a network-monitoring device connected to another switch port, i.e., a computer equipped with a packet sniffer utility.

Mirror Setting

Session ID	Select Session
Monitor session state	Disabled
Destination Port	GE1
allow Ingress	Disabled
Sniffer RX Ports	LAN0, RSP0, RSP1, RSP2, RSP3, RSP4, RSP5, RSP6, RSP7, RSP8, RSP9, RSP10, RSP11, RSP12, RSP13, RSP14, RSP15, RSP16, RSP17, RSP18, RSP19, RSP20, RSP21, RSP22, RSP23, RSP24, RSP25, RSP26, RSP27, RSP28, RSP29, RSP30, RSP31, RSP32, RSP33, RSP34, RSP35, RSP36, RSP37, RSP38, RSP39, RSP40, RSP41, RSP42, RSP43, RSP44, RSP45, RSP46, RSP47, RSP48, RSP49, RSP50, RSP51, RSP52, RSP53, RSP54, RSP55, RSP56, RSP57, RSP58, RSP59, RSP60, RSP61, RSP62, RSP63, RSP64, RSP65, RSP66, RSP67, RSP68, RSP69, RSP70, RSP71, RSP72, RSP73, RSP74, RSP75, RSP76, RSP77, RSP78, RSP79, RSP80, RSP81, RSP82, RSP83, RSP84, RSP85, RSP86, RSP87, RSP88, RSP89, RSP90, RSP91, RSP92, RSP93, RSP94, RSP95, RSP96, RSP97, RSP98, RSP99
Sniffer TX Ports	LAN0, RSP0, RSP1, RSP2, RSP3, RSP4, RSP5, RSP6, RSP7, RSP8, RSP9, RSP10, RSP11, RSP12, RSP13, RSP14, RSP15, RSP16, RSP17, RSP18, RSP19, RSP20, RSP21, RSP22, RSP23, RSP24, RSP25, RSP26, RSP27, RSP28, RSP29, RSP30, RSP31, RSP32, RSP33, RSP34, RSP35, RSP36, RSP37, RSP38, RSP39, RSP40, RSP41, RSP42, RSP43, RSP44, RSP45, RSP46, RSP47, RSP48, RSP49, RSP50, RSP51, RSP52, RSP53, RSP54, RSP55, RSP56, RSP57, RSP58, RSP59, RSP60, RSP61, RSP62, RSP63, RSP64, RSP65, RSP66, RSP67, RSP68, RSP69, RSP70, RSP71, RSP72, RSP73, RSP74, RSP75, RSP76, RSP77, RSP78, RSP79, RSP80, RSP81, RSP82, RSP83, RSP84, RSP85, RSP86, RSP87, RSP88, RSP89, RSP90, RSP91, RSP92, RSP93, RSP94, RSP95, RSP96, RSP97, RSP98, RSP99

Apply

Mirror Status

Session ID	Destination Port	Ingress State	Sniffer TX Ports	Sniffer RX Ports
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

Session ID: The Intellinet switch supports up to 4 session IDs.

Monitor Session State: Disables or enables port mirroring for this session.

Destination Port: The port to which the mirrored packets are sent, which is the port to which you connect your network monitoring station. This port will no longer function as a regular port, and it cannot be assigned to any LAG or VLAN group.

Allow-Ingress: Enable or Disable ingress traffic forwarding. An example for ingress traffic is the information returned by a web site to the local user's request. Egress, on the other hand, would be the request by the local user to the web site. Simply speaking, from the standpoint of your network, ingress traffic can be consider incoming or inbound traffic, whereas egress traffic is outgoing or outbound traffic.

Sniffer RX/TX Ports: Defines the source ports from which traffic will be mirrored.

TX Ports: Only traffic transmitted originating from these ports will be mirrored to the destination port.

RX Port: Only traffic received by these ports will be mirrored to the destination port.

5.3.4 Link Aggregation

5.3.4.1 LAG Setting

Besides providing a higher speed connection to another port by grouping ports together into a logical unit, Link Aggregation (LAG) also provides a load balancing feature. On this screen you define whether LAG that is depended on the MAC address or IP/MAC address.

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

5.3.4.2 LAG Management

This page is used to set up LAG groups. You can create up to 8 different LAG groups, each can have up to 8 member ports. Each LAG can be given a custom name, and you must select the ports for the LAG.

LAG	Name	Type	Port
LAG1		☒ Static ☐ LACP	Select Ports

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

As for the type, there are two choices: Static and LACP.

Static: All configuration settings must be set up manually exactly the same way on the participating LAG device, i.e., the other Intellinet 24 Port PoE+ Web Managed Gigabit Switch. There is no problem with doing this of course. Even the static method provides link redundancy, should one or more of the links in the trunk fail. However, if media converters are used, it can happen that the link on the switch#1 is up, but the connection to the switch#2 at the other end is interrupted, for example because of a cable malfunction. In this case, switch#1 keeps sending data via this connection, because on this end there are no interruptions. The data transfer is therefore interrupted.

LACP: Link Aggregation Control Protocol (LACP) allows the dynamic exchange of information with regard to the link aggregation between the two members of said aggregation. It allows for the automatic detection of links in an LAG group when connected to another LACP-compliant Switch. Both switch#1 and switch#2 need to be set to the same mode for this to work. The data between the two switches is packetized in Link Aggregation Control Protocol Data Units (LACDUs). Should any of these packets fail to arrive, for instance due to an interruption one side of the media converter, the switches will quickly remove the LAG group port causing the problem from the LAG group. No data is lost.

5.3.4.3 LAG Port Setting

On this page you define additional settings for the LAG groups.

LAG Port Setting

LAG Select	Enabled	Speed	Flow Control
Select LAGs	☒ Enabled ☐ Disabled	Auto	☐ Enabled ☒ Disabled

Apply

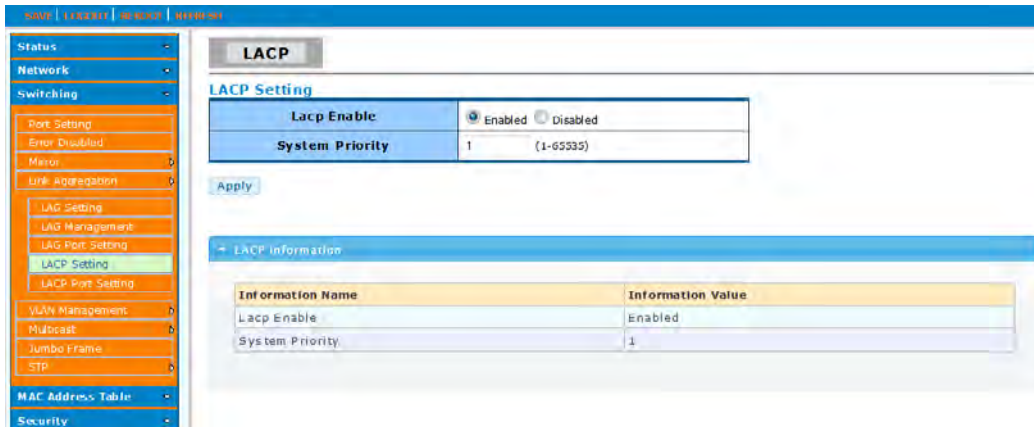
LAG Port Status

LAG	Description	Port Type	Enable State	Link Status	Speed	Duplex	FlowCtrl Config	FlowCtrl Status
LAG 1			Enabled		Auto	Auto	Disabled	Disabled
LAG 2			Enabled		Auto	Auto	Disabled	Disabled
LAG 3			Enabled		Auto	Auto	Disabled	Disabled
LAG 4			Enabled		Auto	Auto	Disabled	Disabled
LAG 5			Enabled		Auto	Auto	Disabled	Disabled
LAG 6			Enabled		Auto	Auto	Disabled	Disabled
LAG 7			Enabled		Auto	Auto	Disabled	Disabled
LAG 8			Enabled		Auto	Auto	Disabled	Disabled

You can enable or disable the entire group, set the speed to manual values from 10 to 1000 Mbps, or auto, and you can enable or disable flow control.

5.3.4.4 LACP Setting

This page is used to configure the system LACP system priority, which determines which switch (switch #1 or switch #2) in an LACP link controls port priorities. If both switches are set to the default value “1,” then the LACP system ID (MAC address of the switch) determines which of the switches is in charge. Other than that, the switch with the lowest system priority number is in control.



LACP

LACP Setting

LACP Enable	☒ Enabled ☐ Disabled
System Priority	1 (1-65535)

Apply

LACP Information

Information Name	Information Value
LACP Enable	Enabled
System Priority	1

5.3.4.5 LACP Port Setting

This page is used to set the priority for the LACP member ports. While the system priority defines, which switch is in charge in the LACP setup, the port priority is used to determine, how the ports in the LACP group are used, based on which port priority. The lowest number value has the highest priority, and if all are left at default, then the actual port number defines the priority.

Home | Config | Monitor | Advanced

Status

Network

Switching

Port Setting

Error Disabled

Monitor

Link Aggregation

LAG Setting

LAG Management

LAG Port Setting

LACP Setting

LACP Port Setting

VLAN Management

Multicast

Trunked Frame

STP

MAC Address Table

Security

ACL

QoS

Management

Diagnostics

Maintenance

LACP Port Setting

LACP Port Setting

Port Select	System Priority	Timeout
Select Ports	1 (1-65535)	☒ long ☐ short

Apply

LACP Port Information

	System 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
GE11	1	long

5.3.5 VLAN Management

5.3.5.1 Create VLAN

This page allows adding, deleting or editing the switch's 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: This is the ID for the new VLAN.

VLAN Action: Add or delete the VLAN.

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

Below is a real-world example:

VLAN Table			
VLAN ID	VLAN Name	VLAN Type	Modify
1	default	Default	Edit
2	accounting0002	Static	Edit Delete
3	sales0003	Static	Edit Delete

5.3.5.2 Interface Settings

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

Interface Settings

Edit Interface Setting

Port Select	Interface VLAN Mode	PVID	Accepted Type	Ingress Filtering	Uplink	TPID
Select Ports	Hybrid Access Trunk Tunnel	1 (1 - 4094)	All Tagged Untagged	Enabled Disabled	Enabled Disabled	0x0100

Apply

Port VLAN Status

Port	Interface VLAN Mode	PVID	Accepted Type	Ingress Filtering	Uplink	TPID
GE1	Trunk	1	All	Enabled	Disabled	0x0100
GE2	Trunk	1	All	Enabled	Disabled	0x0100
GE3	Trunk	1	All	Enabled	Disabled	0x0100
GE4	Trunk	1	All	Enabled	Disabled	0x0100
GE5	Trunk	1	All	Enabled	Disabled	0x0100
GE6	Trunk	1	All	Enabled	Disabled	0x0100
GE7	Trunk	1	All	Enabled	Disabled	0x0100
GE8	Trunk	1	All	Enabled	Disabled	0x0100
GE9	Trunk	1	All	Enabled	Disabled	0x0100
GE10	Trunk	1	All	Enabled	Disabled	0x0100
GE11	Trunk	1	All	Enabled	Disabled	0x0100
GE12	Trunk	1	All	Enabled	Disabled	0x0100
GE13	Trunk	1	All	Enabled	Disabled	0x0100
GE14	Trunk	1	All	Enabled	Disabled	0x0100
GE15	Trunk	1	All	Enabled	Disabled	0x0100
GE16	Trunk	1	All	Enabled	Disabled	0x0100

Port Select : Select one or multiple ports to configure.

Interface VLAN Mode: VLAN port mode

Hybrid: Port hybrid model.

Access: Port hybrid model.

Trunk: Port hybrid model.

Tunnel: Port hybrid model.

PVID: VLAN ID for the selected ports.

Accepted Type: Port accepted type.

All: Accept tagged and untagged frames.

Tag Only: Only accept tagged frame.

Untag Only: Only accept untagged frame.

Ingress Filtering: Choose filter port open and close.

Uplink: Select port Uplink open or close.

5.3.5.3 Port to VLAN

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

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

Port	Interface	VLAN Mode	Membership	PVID
GE1	Trunk		Forbidden Excluded Tagged Untagged	1
GE2	Trunk		Forbidden Excluded Tagged Untagged	1
GE3	Trunk		Forbidden Excluded Tagged Untagged	1
GE4	Trunk		Forbidden Excluded Tagged Untagged	1
GE5	Trunk		Forbidden Excluded Tagged Untagged	1
GE6	Trunk		Forbidden Excluded Tagged Untagged	1
GE7	Trunk		Forbidden Excluded Tagged Untagged	1
GE8	Trunk		Forbidden Excluded Tagged Untagged	1
GE9	Trunk		Forbidden Excluded Tagged Untagged	1
GE10	Trunk		Forbidden Excluded Tagged Untagged	1
GE11	Trunk		Forbidden Excluded Tagged Untagged	1
GE12	Trunk		Forbidden Excluded Tagged Untagged	1
GE13	Trunk		Forbidden Excluded Tagged Untagged	1
GE14	Trunk		Forbidden Excluded Tagged Untagged	1
GE15	Trunk		Forbidden Excluded Tagged Untagged	1
GE16	Trunk		Forbidden Excluded Tagged Untagged	1

5.3.5.4 Port VLAN Membership

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

Port	Mode	Administrative VLANs	Operational VLANs	Modify
GE1	Trunk	1UP	1UP	Edit
GE2	Trunk	1UP	1UP	Edit
GE3	Trunk	1UP	1UP	Edit
GE4	Trunk	1UP	1UP	Edit
GE5	Trunk	1UP	1UP	Edit
GE6	Trunk	1UP	1UP	Edit
GE7	Trunk	1UP	1UP	Edit
GE8	Trunk	1UP	1UP	Edit
GE9	Trunk	1UP	1UP	Edit
GE10	Trunk	1UP	1UP	Edit
GE11	Trunk	1UP	1UP	Edit
GE12	Trunk	1UP	1UP	Edit
GE13	Trunk	1UP	1UP	Edit
GE14	Trunk	1UP	1UP	Edit
GE15	Trunk	1UP	1UP	Edit
GE16	Trunk	1UP	1UP	Edit
GE17	Trunk	1UP	1UP	Edit
GE18	Trunk	1UP	1UP	Edit

5.3.5.5 Protocol VLAN Group Setting

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

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

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

Add

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_LL_C_Other: packet type is 802.3 packet with LLC other header.

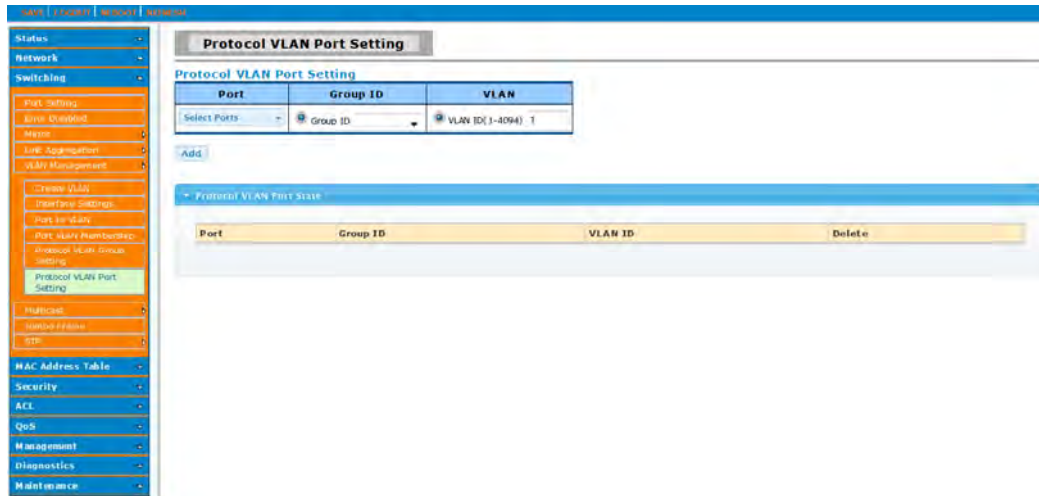
RFC_1042: packet type is RFC 1042 packet.

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

5.3.5.6 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.



The screenshot shows the 'Protocol VLAN Port Setting' web page. On the left is a sidebar menu with categories like Status, Network, Switching, and others. Under 'Switching', 'VLAN Management' is expanded, showing options like Create VLAN, Port Settings, and Protocol VLAN Port Setting. The main content area has a title bar 'Protocol VLAN Port Setting'. Below it is a table with three columns: 'Port', 'Group ID', and 'VLAN'. The 'Port' column has a 'Select Ports' dropdown. The 'Group ID' column has a radio button and a dropdown menu. The 'VLAN' column has a radio button and a dropdown menu. Below the table is an 'Add' button. At the bottom, there is a section titled 'Protocol VLAN Port Settings' with a table for adding new settings. This table has columns for 'Port', 'Group ID', 'VLAN ID', and a 'Delete' button.

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.

5.3.6 Multicast

5.3.6.1 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

Apply

Properties Information

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

5.3.6.2 IGMP Snooping

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

IGMP Setting

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

IGMP Snooping

IGMP Snooping

IGMP Snooping Status	☒ Enabled ☐ Disabled
IGMP Snooping Version	☒ v2 ☐ v3
IGMP Snooping Report Suppression	☒ Enabled ☐ Disabled

Apply

IGMP Snooping Information

Information Name	Information Value
IGMP Snooping Status	Enabled
IGMP Snooping Version	v2
IGMP Snooping Report Suppression	Enabled

IGMP Snooping Table

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 the IGMP Snooping enable or disable.

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

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

IGMP Snooping Querier Setting

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

VLAN ID	Querier State	Querier Status	Querier Version	Querier IP
1	Disabled	None/Querier	v2	...

VLAN ID: Select the VLANs to configure.

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

Enable: Enable IGMP Querier Election.

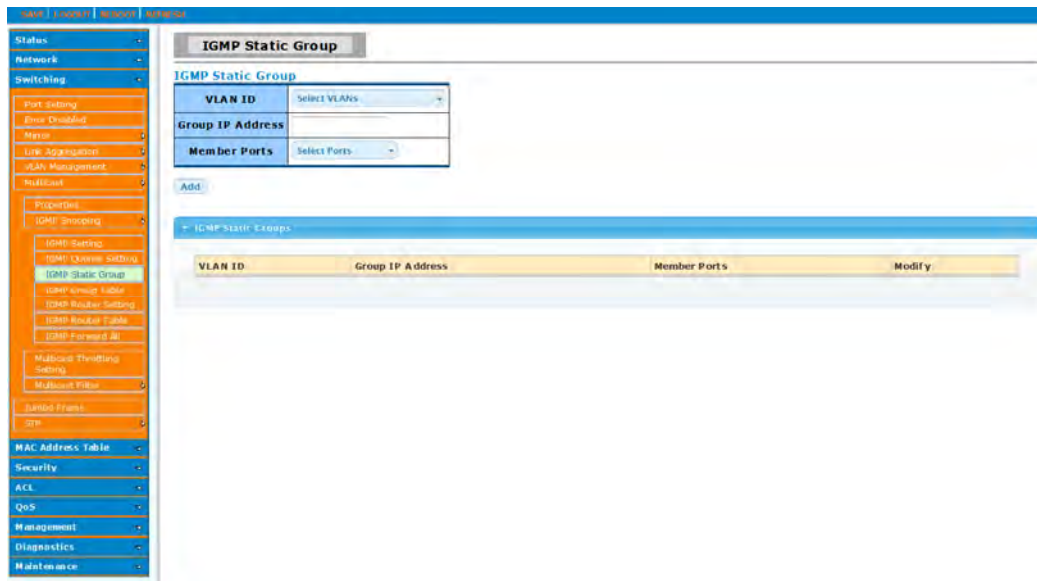
Disable: Disable IGMP Querier Election.

Version:Select the Querier Version,IGMPv2 or IGMPv3

IGMP Static Group

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

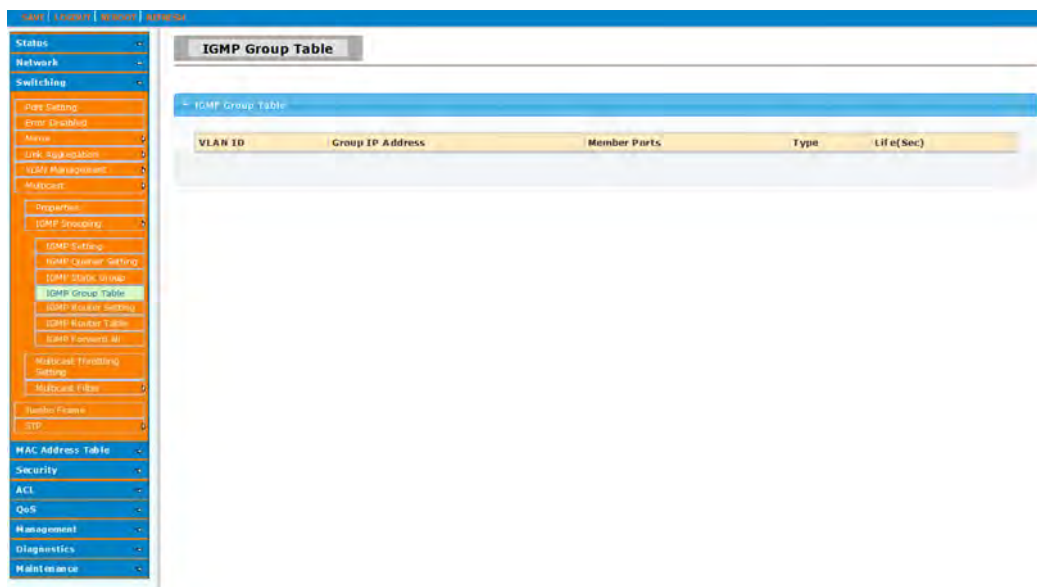
This page is used to configure specified ports as static member ports.



IGMP Group Table

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

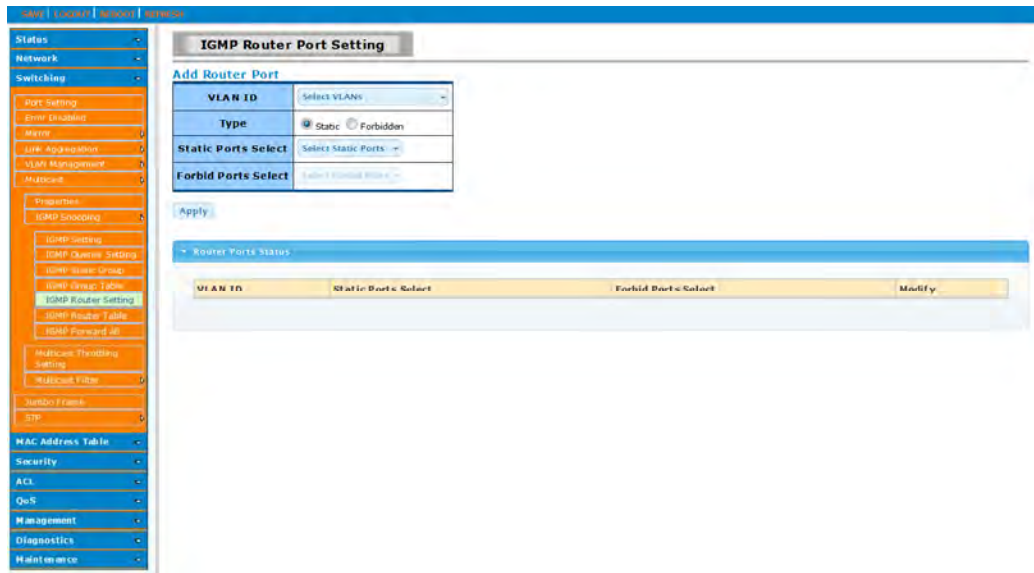
This page is used to display IGMP Group Table statistics information.



IGMP 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 ☐ Forbidden
Static Ports Select	Select Static Ports
Forbidden Ports Select	Select Forbidden Ports

Apply

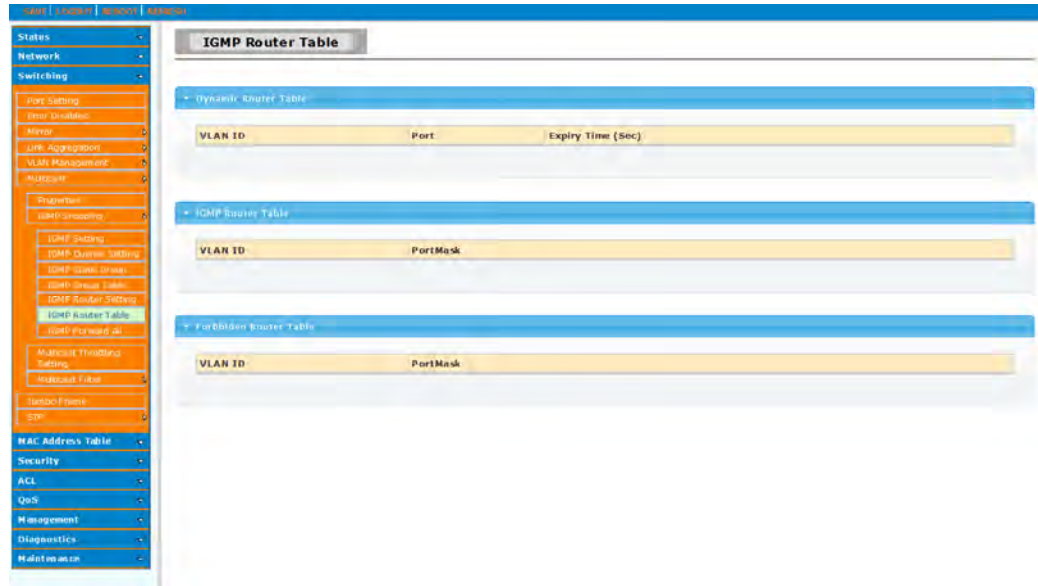
Router Ports Status

VLAN ID	Static Ports Select	Forbidden Ports Select	Modify

IGMP Router Table

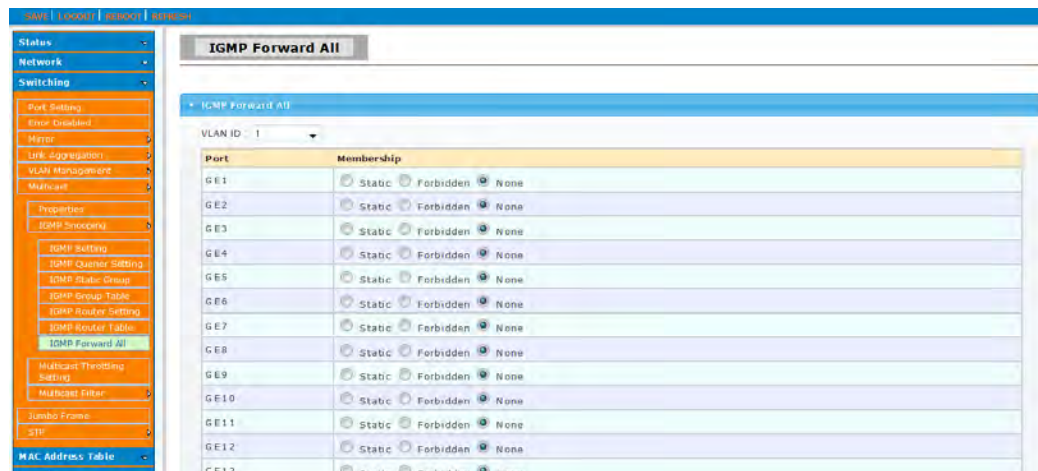
To display IGMP Router Table web page, click **Switching > Multicast > IGMP Snooping > IGMP Router Table**

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



IGMP Forward All

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



5.3.6.3 Multicast Port Max-Groups

To display Multicast Port Max-Groups web page, click **Switching > Multicast > Multicast Port Max-Groups**

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

Multicast Port Max-Groups

Max groups and action Setting

Ip Type	Port Select	Max Groups	Action
IPv4	Select Ports	256 (0-256)	☒ Deny ☐ Replace

Apply

IGMP Port Max Groups Information

Port	Max Groups	Action
GE1	256	Deny
GE2	256	Deny
GE3	256	Deny
GE4	256	Deny
GE5	256	Deny
GE6	256	Deny
GE7	256	Deny
GE8	256	Deny
GE9	256	Deny
GE10	256	Deny
GE11	256	Deny
GE12	256	Deny
GE13	256	Deny
GE14	256	Deny

Multicast Filter

This page allow user to Create filter instance.

Multicast Profile Setting

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

Ip Type	Profile Index	Group from	Group to	Action
IPv4	1			☒ Permit ☐ Deny

Add

Index	Ip Type	Group from	Group to	Action	Modify
-------	---------	------------	----------	--------	--------

Multicast Profile Setting

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

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

Port Select	Filter Profile ID
Select Ports	

Apply

Port	Filter Profile ID	Action
------	-------------------	--------

5.3.7 Jumbo Frame

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

Information Name	Information Value
Jumbo Frame (Bytes)	1522

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

STP

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

STP Global Setting

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

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 enabled/disabled on the Switch.

BPDU Forward: Choose BPDU packets is a flood or filtering

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

Force Version: Select the operating mode of STP.

STP-Compatible: 802.1D STP operation.

RSTP-Operation: 802.1w operation.

MSTP-Operation: 802.1s operation.

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

STP Port Setting

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

Apply

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
GE11	Enable	0	No	No	No	Yes
GE12	Enable	0	No	No	No	Yes
GE13	Enable	0	No	No	No	Yes
GE14	Enable	0	No	No	No	Yes
GE15	Enable	0	No	No	No	Yes
GE16	Enable	0	No	No	No	Yes
GE17	Enable	0	No	No	No	Yes
GE18	Enable	0	No	No	No	Yes
GE19	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).

CIST Instance Setting

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

CIST Instance Setting

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

Apply

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 BPDU transmission rate.

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

CIST Port Setting

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

CIST Port Setting

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

Apply

CIST Port Status

Port	Identifier (Priority / Port ID)	External Path Cost	Internal Path Cost	Designated Root Bridge	External Root Cost	Regional Root Bridge	Internal Root Cost	Designated Bridge	Internal Path Cost	Edge Port Conf/Oper	P2P MAC Conf/Oper	Port Role	Port State
GE1	128 / 1	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabled	Disabled
GE2	128 / 2	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabled	Disabled
GE3	128 / 3	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabled	Disabled
GE4	128 / 4	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabled	Disabled
GE5	128 / 5	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabled	Disabled
GE6	128 / 6	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabled	Disabled
GE7	128 / 7	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabled	Disabled
GE8	128 / 8	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabled	Disabled
GE9	128 / 9	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / No	Disabled	Disabled
GE10	128 / 10	0 / 20000	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	20000	No / No	Auto / Yes	Disabled	Forwarding

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`)

MST Instance Setting

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

MST Instance Setting

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

Apply

MST Instance Setting Information

MSTI	Status	VLAN List	VLAN Count	Priority
1				

MST Instance Status

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

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

VLAN List: Set the VLAN List.

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

MST Port Setting

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

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

Apply

MST ID	Port	Identifier (Priority / Port ID)	Internal Path Cost	Regional Root Bridge	Internal Root Cost	Designated Bridge	Internal Path Cost	Port Role	Port State
1	GE 1	128/1	0/...	...	...	...	...	...	...
1	GE 2	128/2	0/...	...	...	...	...	...	...
1	GE 3	128/3	0/...	...	...	...	...	...	...
1	GE 4	128/4	0/...	...	...	...	...	...	...
1	GE 5	128/5	0/...	...	...	...	...	...	...
1	GE 6	128/6	0/...	...	...	...	...	...	...
1	GE 7	128/7	0/...	...	...	...	...	...	...
1	GE 8	128/8	0/...	...	...	...	...	...	...
1	GE 9	128/9	0/...	...	...	...	...	...	...
1	GE 10	128/10	0/...	...	...	...	...	...	...
1	GE 11	128/11	0/...	...	...	...	...	...	...
1	GE 12	128/12	0/...	...	...	...	...	...	...
1	GE 13	128/13	0/...	...	...	...	...	...	...
1	GE 14	128/14	0/...	...	...	...	...	...	...
1	GE 15	128/15	0/...	...	...	...	...	...	...
1	GE 16	128/16	0/...	...	...	...	...	...	...
1	GE 17	128/17	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')

STP Statistics

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

Save Logout | Logout | Register

Status

Network

Switching

Port Setting

Error Disabled

Monitor

Link Aggregation

VLAN Management

Multicast

Jumbo Frame

STP

STP Global Setting

STP Port Setting

IST Instance Setting

IST Port Setting

MST Instance Setting

MST Port Setting

STP Statistics

MAC Address Table

Security

ACL

QoS

Management

Diagnostics

Maintenance

STP Statistics

STP Statistics

Port	Configuration BDPUs Received	TCH BDPUs Received	MSTP BDPUs Received	Configuration BDPUs Transmitted	TCH BDPUs Transmitted	MSTP BDPUs Transmitted
GE1	0	0	0	0	0	0
GE2	0	0	0	0	0	0
GE3	0	0	0	0	0	0
GE4	0	0	0	0	0	0
GE5	0	0	0	0	0	0
GE6	0	0	0	0	0	0
GE7	0	0	0	0	0	0
GE8	0	0	0	0	0	0
GE9	0	0	0	0	0	0
GE10	0	0	0	0	0	0
GE11	0	0	0	0	0	0
GE12	0	0	0	0	0	0
GE13	0	0	0	0	0	0
GE14	0	0	0	0	0	0
GE15	0	0	0	0	0	0
GE16	0	0	0	0	0	0
GE17	0	0	0	0	0	0
GE18	0	0	0	0	0	0
GE19	0	0	0	0	0	0
GE20	0	0	0	0	0	0
GE21	0	0	0	0	0	0
GE22	0	0	0	0	0	0
GE23	0	0	0	0	0	0
GE24	0	0	0	0	0	0

5.4 MAC ADDRESS TABLE

Static Mac Setting

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

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

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

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

MAC Filtering

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

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

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

Dynamic Address Setting

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

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

Aging Time: Set the time needed for aging

Dynamic Learned

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

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

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

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

RMA MAC Address

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

[Home](#)
[Logout](#)
[Reset](#)
[Help](#)

Status

Network

Switching

MAC Address Table

Static MAC Setting

MAC Filtering

Dynamic Address Setting

Dynamic Learned

RMV Setting

Security

ACL

QoS

Management

Diagnosis

Maintenance

Reserved MAC Addresses

Reserved MAC Addresses Setting

MAC Address

Select MAC Address

Action

☐ Peer
 ☒ Bridge
 ☐ Discard

Apply

Reserved MAC Addresses Table

MAC Address	Action	Delete

5.5 SECURITY

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

Storm Control

Global Setting

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

Information Name	Information Value
Unit	pps
Preamble & IFG	Excluded

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

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

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

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

Port Setting

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

Port: Select the setting ports.

Type Enable: Select the type of storm control.

Broadcast: Broadcast packet.

Unknown Multicast: Unknown multicast packet State.

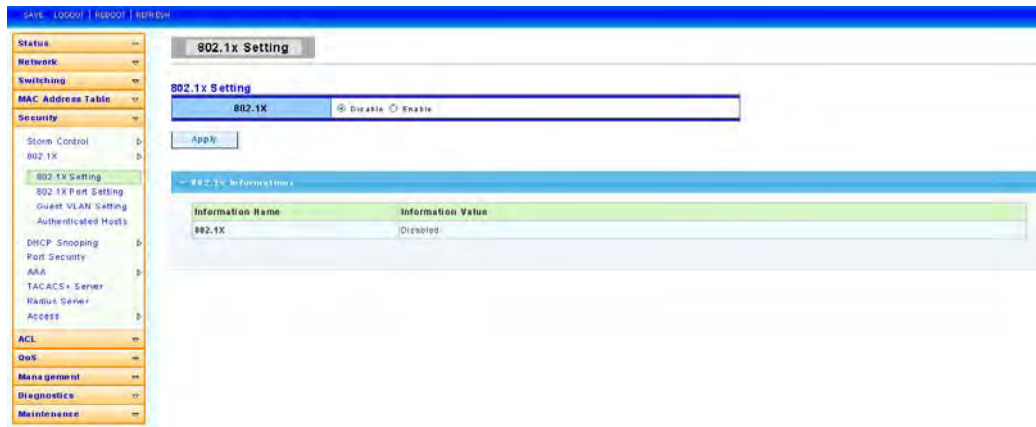
Unknown Unicast: Unknown unicast packet.

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

802.1X

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

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



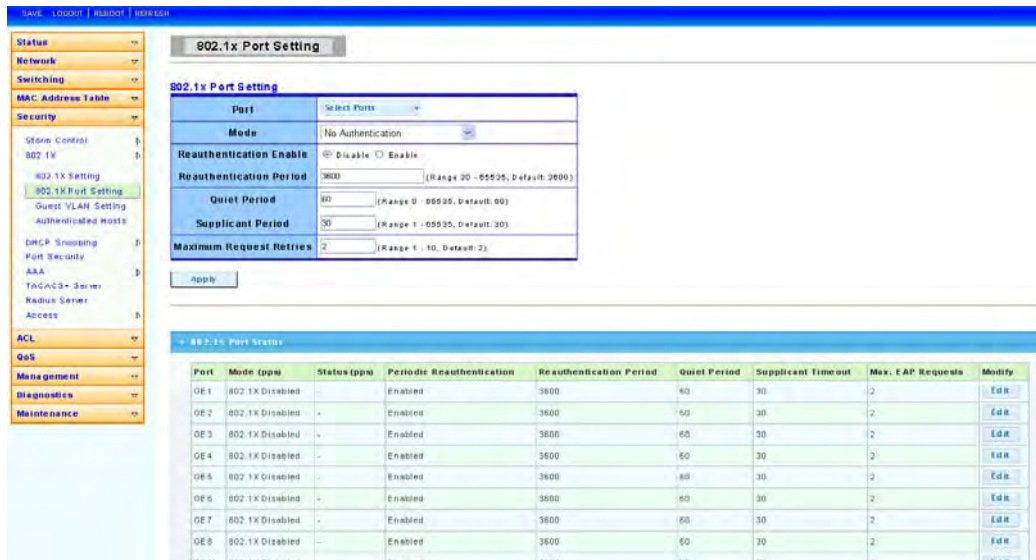
802.1X: Set the enabling status of 802.1X functionality.

Enable: Enable 802.1X.

Disable: Disable 802.1X.

802.1X Port Setting

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



Port: Select the ports to configure their authentication mode.

Mode: The authentication mode.

Force Unauthorized: Force this port to be unconditional unauthorized.

Force Authorized: Force this port to be unconditional authorized.

Authentication: 802.1X authentication.

No Authentication:802.1X disabled.

Reauthentication Enable: Set the enabling status of802.1X reauthentication.

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

Guest VLAN Setting

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

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
GE10	Disabled	NO
GE11	Disabled	NO
GE12	Disabled	NO
GE13	Disabled	NO
GE14	Disabled	NO
GE15	Disabled	NO

Authenticated Hosts

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

User Name	Port	Session Time	Authentication Method	MAC Address
-----------	------	--------------	-----------------------	-------------

DHCP Snooping

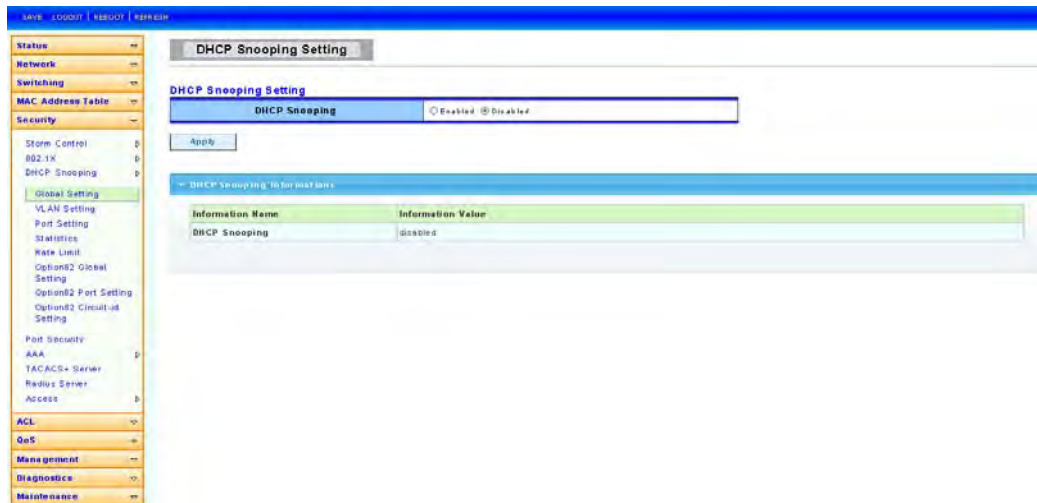
When the switch opens DHCP-Snooping, it will snoop DHCP message and receive DHCP Request and abstract and record the IP address and MAC address from DHCP ACK message. Besides, DHCP-Snooping admits one physical port setting as creditable port or discreditable ports. Creditable

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.

Global Setting

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

This page is used to open DHCP Snooping function

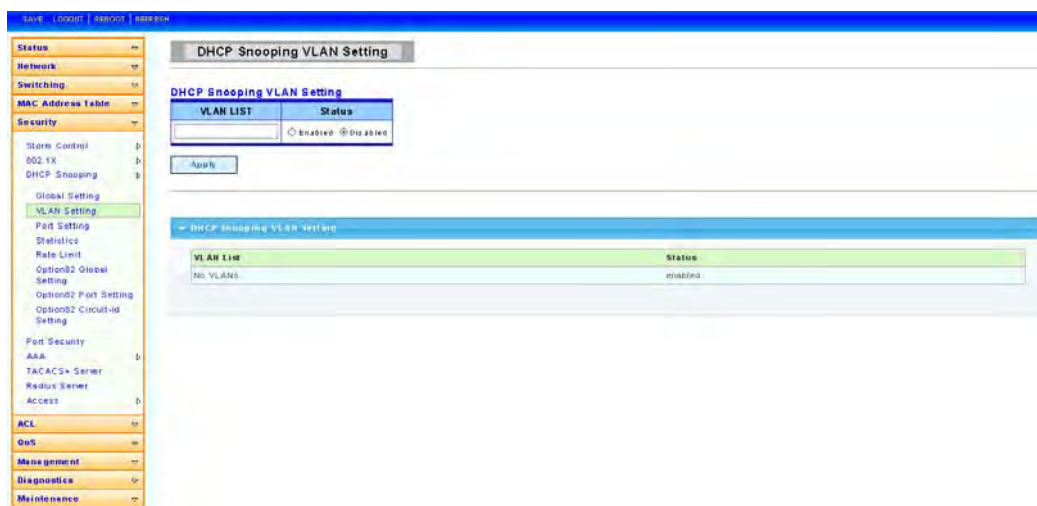


DHCP Snooping: enable or disable DHCP Snooping function

VLAN Setting

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

Specific VLAN starts DHCP Snooping



Port Setting

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

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

DHCP Snooping Port Setting

Port	Type	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
GE11	Un Trusted	disabled
GE12	Un Trusted	disabled
GE13	Un Trusted	disabled
GE14	Un Trusted	disabled
GE15	Un Trusted	disabled
GE16	Un Trusted	disabled
GE17	Un Trusted	disabled

Statistics

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

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

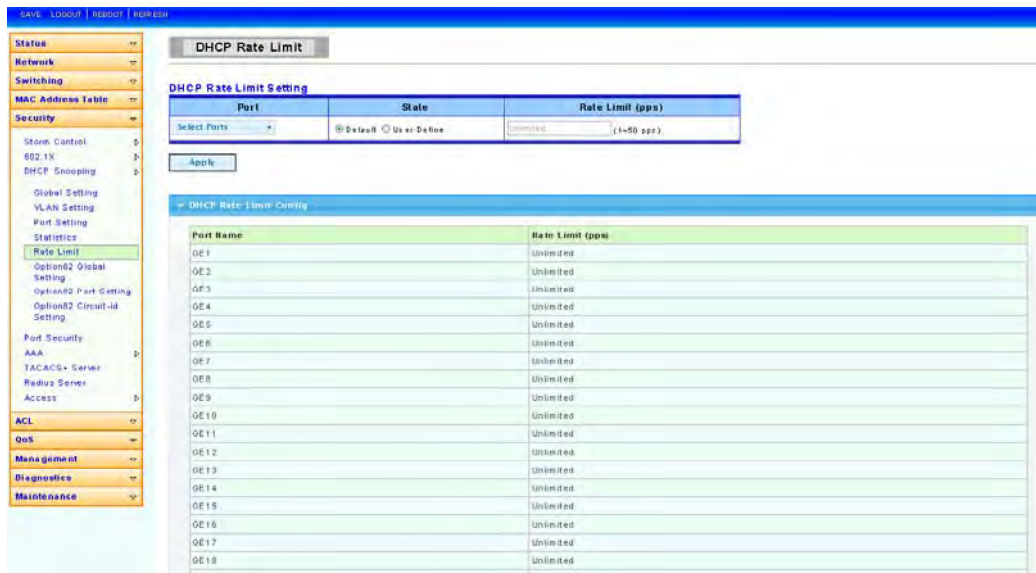
DHCP Snooping Statistics

Clear Refresh

Port	Forwarded	Chaddr Check Dropped	Untrust Port Dropped	Untrust Port With Option82 Dropped	Invalid Dropped
GE1	0	0	0	0	0
GE2	0	0	0	0	0
GE3	0	0	0	0	0
GE4	0	0	0	0	0
GE5	0	0	0	0	0
GE6	0	0	0	0	0
GE7	0	0	0	0	0
GE8	0	0	0	0	0
GE9	0	0	0	0	0
GE10	0	0	0	0	0
GE11	0	0	0	0	0
GE12	0	0	0	0	0
GE13	0	0	0	0	0
GE14	0	0	0	0	0
GE15	0	0	0	0	0
GE16	0	0	0	0	0
GE17	0	0	0	0	0
GE18	0	0	0	0	0
GE19	0	0	0	0	0
GE20	0	0	0	0	0
GE21	0	0	0	0	0
GE22	0	0	0	0	0
GE23	0	0	0	0	0

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)

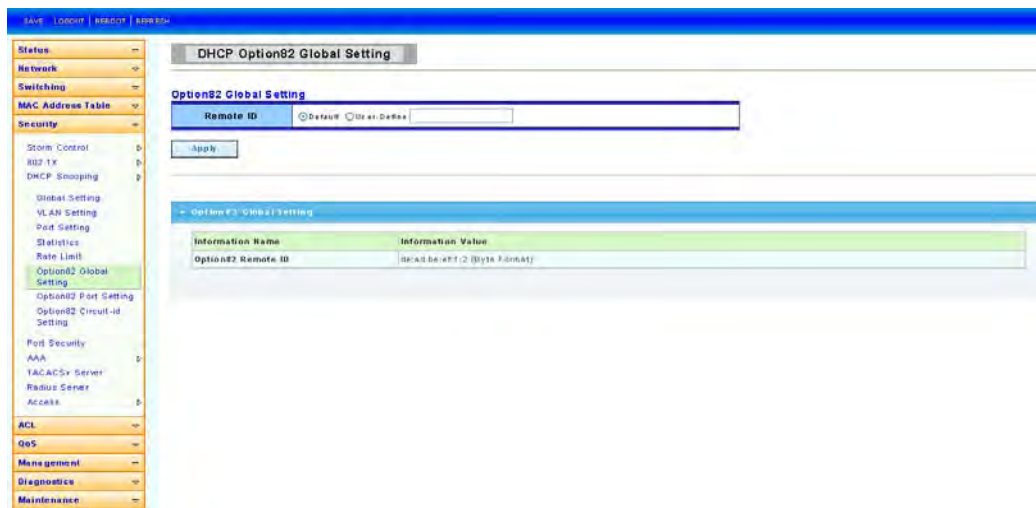
DHCP Rate Limit Setting

Port Name	Rate Limit (pps)
GE1	Unlimited
GE2	Unlimited
GE3	Unlimited
GE4	Unlimited
GE5	Unlimited
GE6	Unlimited
GE7	Unlimited
GE8	Unlimited
GE9	Unlimited
GE10	Unlimited
GE11	Unlimited
GE12	Unlimited
GE13	Unlimited
GE14	Unlimited
GE15	Unlimited
GE16	Unlimited
GE17	Unlimited
GE18	Unlimited

Option82 Global Setting

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

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



DHCP Option82 Global Setting

Option82 Global Setting

Remote ID
☒ Default ☐ User Define

Option82 Global Setting

Information Name	Information Value
Option82 Remote ID	Default (2 Byte Format)

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

Port	Enable	Allow Untrusted
Select Ports	☐ Enable ☐ Disable	Keep

Apply

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
GE11	disabled	Drop
GE12	disabled	Drop
GE13	disabled	Drop
GE14	disabled	Drop
GE15	disabled	Drop
GE16	disabled	Drop
GE17	disabled	Drop

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

Port	Vlan	Circuit ID
Select Ports	1	☐ Default ☐ User-Defined

Apply

Option82 Port Circuit-ID Setting

Port	VLAN	Circuit ID
------	------	------------

Port Security

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

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

Port Security Settings

Port Select	Security	Max L2 Entry	Action	Trap Frequency (sec.)
Select Ports: -	☐ Enabled ☒ Disabled	Default	Forward	☒ 60

Apply

Port Security Status

Port Name	Enable State	L2 Entry Num	Action	Trap Frequency
GE 1	Disabled	16383	Forward	60
GE 2	Disabled	16383	Forward	60
GE 3	Disabled	16383	Forward	60
GE 4	Disabled	16383	Forward	60
GE 5	Disabled	16383	Forward	60
GE 6	Disabled	16383	Forward	60
GE 7	Disabled	16383	Forward	60
GE 8	Disabled	16383	Forward	60
GE 9	Disabled	16383	Forward	60
GE 10	Disabled	16383	Forward	60
GE 11	Disabled	16383	Forward	60
GE 12	Disabled	16383	Forward	60
GE 13	Disabled	16383	Forward	60
GE 14	Disabled	16383	Forward	60
GE 15	Disabled	16383	Forward	60
GE 16	Disabled	16383	Forward	60
GE 17	Disabled	16383	Forward	60
GE 18	Disabled	16383	Forward	60

Port Select: Select one or multipleports to configure.

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

Enable: Enable port security function.

Disable: Disable port security function.

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

AAA

Login List

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

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

The screenshot shows a web management interface for a switch. On the left is a navigation menu with categories: Status, Network, Switching, MAC Address Table, Security, ACL, QoS, Management, Diagnostics, and Maintenance. The 'Security' category is expanded, showing sub-items: Storm Control, 802.1X, DHCP Snooping, Port Security, AAA, Login List (selected), Enable List, Accounting List, Accounting Update, TACACS+ Server, Radius Server, and Access. The main content area is titled 'Login Authentication List'. It contains a 'New Authentication List' section with a table for defining a new list:

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

Below this table is an 'Add' button. Further down is a section titled 'Login Authentication List' containing a table of existing 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 besupported 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 besupported 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 besupported 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 besupported in the future.

Enable: Use local enable password to authenticate

Enable List

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

This page allow user to add, editor 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.

List Name	Method 1	Method 2	Method 3
	Empty	Empty	Empty

Add

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 besupported 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 besupported 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.

Accounting List

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

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

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.

Accounting Update

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

The screenshot shows the 'Accounting Update' configuration page. On the left is a navigation menu with options: Status, Network, Switching, MAC Address Table, Security, Storm Control, 802.1X, DHCP Snooping, Port Security, AAA, Login List, Enable List, Accounting List, Accounting Update (highlighted), TACACS+ Server, Radius Server, Access, ACL, QoS, Management, Diagnostics, and Maintenance. The main content area has a title bar 'Accounting Update' and a 'State' section with radio buttons for 'Disabled' (selected) and 'Enabled'. Below this is an 'Apply' button. A section titled 'Accounting Update Information' contains a table with two columns: 'Information Name' and 'Information Value'. The table has two rows: 'State' with value 'disabled' and 'Periodic (min)' with value '1'.

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.

The screenshot shows the 'Tacacs+ server settings' configuration page. On the left is the same navigation menu as the previous page, with 'Tacacs+ Server' highlighted. The main content area has a title bar 'Tacacs+ server settings'. It contains two main sections: 'Use Default Parameters' and 'New Tacacs+ Server'. The 'Use Default Parameters' section has fields for 'IP Version' (set to 'Version 8 Version 4'), 'Key String' (with a hint '(0-128 ASCII Alphanumeric Character Used)'), and 'Timeout for Reply' (set to '5' with a hint 'sec. (Range 1-30, Default: 5)'). There is an 'Apply' button below. The 'New Tacacs+ Server' section has a 'Server Definition' section with radio buttons for 'By IP address' (selected) and 'By name'. Below this are fields for 'Server IP', 'Server Port' (set to '49' with a hint '(0 - 65535)'), 'Server Key' (with a hint 'Use a Default'), 'Server Timeout' (with a hint 'Use a Default' and '(1-30) sec'), and 'Server Priority' (set to '1' with a hint '(0 - 55535)'). There is an 'Add' button below. At the bottom, there is a table titled 'TACACS+ Servers' with columns: IP Address, Port, Key, Timeout, Priority, and Modify.

Radius server

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

This page is used to set about radius server.

The screenshot shows the 'Radius server settings' page. On the left is a navigation menu with categories like Status, Network, Switching, MAC Address Table, Security, Storm Control, 802.1X, DHCP Snooping, Port Security, AAA, TACACS+ Server, Radius Server, Access, ACL, QoS, Management, Diagnostics, and Maintenance. The 'Radius Server' option is highlighted. The main content area is titled 'Radius server settings' and contains two sections: 'Use Default Parameters' and 'New Radius Server'.

Use Default Parameters

IP Version	Version 0 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	(0128 ASCII Alphabetic Character (8x4))

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 a Default (0 - 85535)
Timeout for Reply	☒ Use a Default (1-30) sec
Retries	☒ Use a Default (1 - 10)
Server Priority	1 (0 - 65535)
Dead Time	0 (0 - 2000)
Usage Type	☐ Login ☐ 802.1X ☐ All

Add

Access

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.

The screenshot shows the 'Console Settings' page. The navigation menu on the left is the same as in the previous screenshot, but the 'Access' option is highlighted. The main content area is titled 'Console Settings' and contains a table for configuring console settings and a section for console information.

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.

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.

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.

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.

The screenshot shows the 'HTTP Settings' page. On the left is a navigation menu with categories like Status, Network, Switching, MAC Address Table, Security, and others. The 'Security' category is expanded, showing sub-items like Storm Control, QoS, DHCP Snooping, Port Security, AAA, TACACS+ Server, Radius Server, Access, Console, Telnet, HTTP, and HTTPS. The 'HTTP Settings' section has two main fields: 'HTTP Service' with radio buttons for 'Enabled' (selected) and 'Disabled', and 'Login Authentication List' with a dropdown menu showing 'default'. Below these is a 'Session Timeout' field set to '10' minutes. An 'Apply' button is at the bottom of the settings section. Below the settings is an 'HTTP Information' table.

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, WEBUI will logout automatically. 0 minutes means never timeout.

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 Service: ☐ Enabled ☒ Disabled

Login Authentication List: default

Session Timeout: 10 (0-60400) minutes

Apply

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.

5.6 ACL

MAC-Based ACL

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

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

ACL Name: Enter ACL name in this field.

MAC-Based ACE

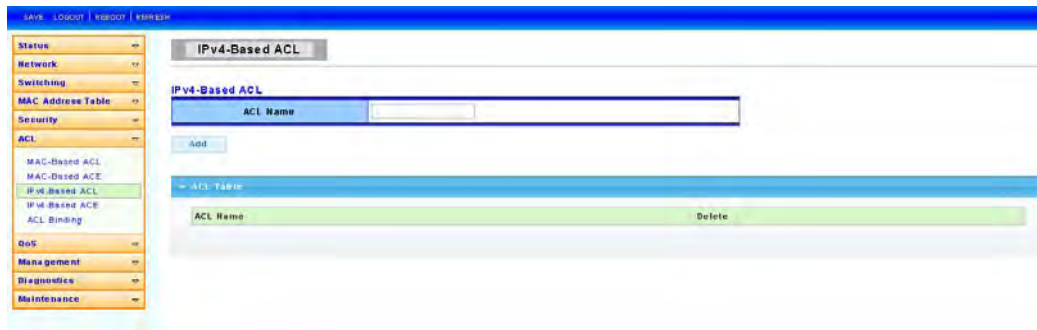
To display MAC-Based ACE web page, click **ACL > MAC-Based ACE**

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

IPv4-Based ACL

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

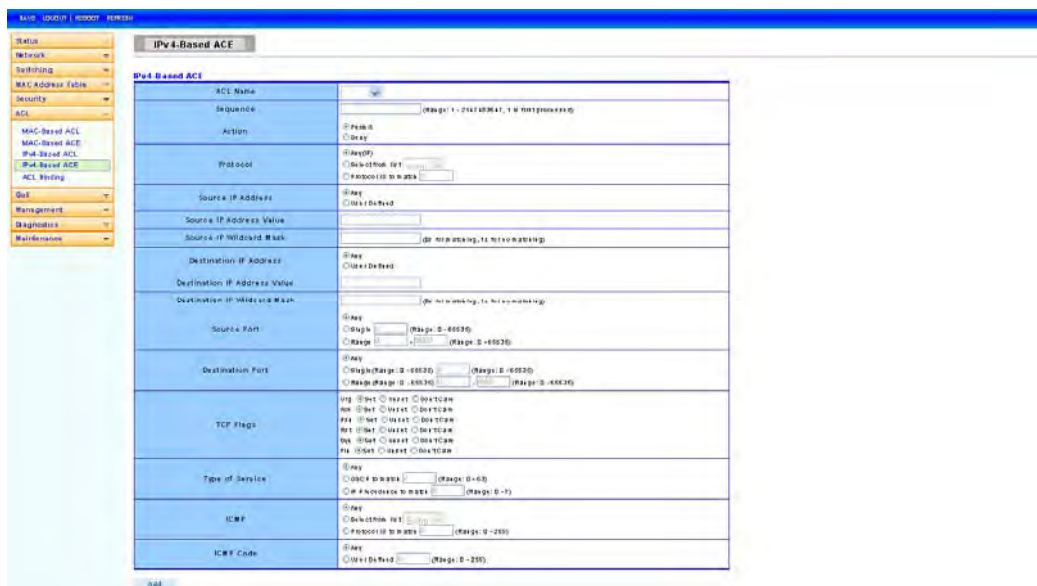
This page allow user to set name for IPv4-Based ACL.



IPv4-Based 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.



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.

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

Status

Network

Switching

MAC Address Table

Security

ACL

QoS

Management

Diagnostics

Maintenance

MAC-Based ACL

MAC-Based ACE

IPv4-Based ACL

IPv4-Based ACE

ACL Binding

ACL Binding

ACL Binding

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

Apply

ACL Binding Table

Port	MAC ACL	IPv4 ACL	IPv6 ACL	Modify
------	---------	----------	----------	--------

5.7 QoS

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

General

QoS Properties

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

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

Port Settings

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

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

Port	CoS Value	Remark CoS	Remark DSCP	Remark IP Precedence
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
GE11	0	disabled	disabled	disabled
GE12	0	disabled	disabled	disabled
GE13	0	disabled	disabled	disabled
GE14	0	disabled	disabled	disabled
GE15	0	disabled	disabled	disabled

Queue Settings

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

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

Queue	Strict Priority	WRR	Weight	% of WRR Bandwidth
1	☐	☐		
2	☐	☐		
3	☐	☐		
4	☐	☐		
5	☐	☐		
6	☐	☐		
7	☐	☐		
8	☐	☐		

Apply

Information Name	Information Value
Strict Priority Queue Number	8

CoS Mapping

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

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

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

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

Apply

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

Queue Mapping to CoS

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

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

QoS Basic Mode

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.

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.

Port	Trust Type
GE1	enabled
GE2	enabled
GE3	enabled
GE4	enabled
GE5	enabled
GE6	enabled
GE7	enabled
GE8	enabled
GE9	enabled
GE10	enabled
GE11	enabled
GE12	enabled
GE13	enabled

QoS Advanced Mode

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.

SAVE | LOGOUT | REBOOT | REFRESH

Global Settings

Advanced Mode Global Settings

Trust Mode

☒ CoS/802.1p
☐ DSCP
☐ CoS/802.1p-DSCP
☐ IP Precedence

Default Mode Status

☐ Trusted ☒ Not Trusted

Apply

Dev Informations

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

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.

SAVE | LOGOUT | REBOOT | REFRESH

Class Configuration

Class Configuration

Class Name

Match ACL Type

☐ IP
☐ MAC
☐ IP or MAC

IP

IPv4 or IPv6

MAC

Preferred ACL

☐ IP
☐ MAC

Add

Class Table

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

Aggregate Policer

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

The screenshot shows the 'Aggregate Policer' configuration page. On the left is a navigation menu with categories: Status, Network, Switching, MAC Address Table, Security, ACL, QoS, Management, Diagnostics, and Maintenance. The 'QoS' category is expanded, showing sub-items: General, QoS Basic Mode, QoS Advanced Mode, Global Settings, Class Mapping, Aggregate Policer (selected), Policy Table, Policy Class Maps, Policy Binding, and Rate Limit. The main content area is titled 'Aggregate Policer' and contains an 'Aggregate Policer Configuration' section with the following fields:

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

Below the configuration fields is an 'Add' button. At the bottom, there is an 'Aggregate Policer Table' section with a table header:

Policer Name	Ingress CIR	Ingress CBS	Exceed Action	Action
--------------	-------------	-------------	---------------	--------

Policy Table

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

The screenshot shows the 'Policy Configuration' page. The navigation menu on the left is the same as in the previous screenshot, but 'Policy Table' is now selected under the 'QoS' category. The main content area is titled 'Policy Configuration' and contains a 'Policy Name' field with an 'Add' button below it. Below this is a 'Policy Table' section with a table header:

Policy Name	Delete
-------------	--------

Policy Class Maps

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

The screenshot shows the 'Policy Class Maps' configuration page. On the left is a navigation menu with categories: Status, Network, Switching, MAC Address Table, Security, ACL, QoS, Management, Diagnostics, and Maintenance. Under QoS, there are sub-items: General, QoS Basic Mode, QoS Advanced Mode, Global Settings, Class Mapping, Aggregate Policer, Policy Table, Policy Class Maps (highlighted), Policy Binding, and Rate Limit. The main content area is titled 'Policy Class Configuration' and contains a form with the following fields:

- Policy Name: [Dropdown]
- Class Name: [Dropdown]
- Action Type:
 - ☐ Trust None
 - ☐ Always Trust
 - ☐ Set Queue []
- Policer Type:
 - ☐ None
 - ☐ Single
 - ☐ Aggregate
- Aggregate Policer: [Dropdown]
- Ingress Committed Information Rate (CIR): [] KBits/s
- Ingress Committed Burst Size (CBS): [] Bytes
- Exceed Action: ☐ Forward ☐ Drop

Below the form is an 'Add' button. At the bottom, there is a 'Policy Class Map Table' with the following columns: Policy Name, Class Name, Action Type (Trust, Set Attribute, Set Value), Policer Type, Aggregate Policer Name, CIR, CBS, Exceed Action, and Modify.

Policy Binding

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

The screenshot shows the 'Policy Binding' configuration page. The navigation menu is the same as in the previous screenshot, with 'Policy Binding' highlighted under the QoS section. The main content area is titled 'Policy Binding' and contains a form with the following fields:

- Policy Select: [Dropdown]
- Binding Port: [Dropdown]

Below the form is an 'Apply' button. At the bottom, there is a 'Policy Binding Table' with the following columns: Port and Policy Name. The table lists ports from GE1 to GE15.

Rate Limit

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.

SAVE | LOGOUT | REBOOT | REFRESH

Status Network Switching MAC Address Table Security ACL QoS

General QoS Basic Mode QoS Advanced Mode Rate Limit Ingress Port Settings Ingress VLAN Settings Egress Port Settings Egress Queue Settings Management Diagnostics Maintenance

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)

Apply

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

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.

SAVE | LOGOUT | REBOOT | REFRESH

Status Network Switching MAC Address Table Security ACL QoS

General QoS Basic Mode QoS Advanced Mode Rate Limit Ingress Port Settings Ingress VLAN Settings Egress Port Settings Egress Queue Settings Management Diagnostics Maintenance

VLAN Ingress RateLimit

VLAN Ingress Rate Settings

VLAN: (default(1))

Port: ALL

State: ☐ Disable ☐ Enable

Rate(Kbps): (0-1000000, must a multiple of 16)

Apply

VLAN Ingress Rate Status

VLAN	Port	Rate (Kbps)
------	------	-------------

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.

SAVE | LOGOUT | REBOOT | REFRESH

Status

Network

Switching

MAC Address Table

Security

ACL

QoS

General

QoS Basic Mode

QoS Advanced Mode

Rate Limit

Ingress Port Settings

Ingress VLAN Settings

Egress Port Settings

Egress Queue Settings

Management

Diagnostics

Maintenance

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)

Apply

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

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.

SAVE | LOGOUT | REBOOT | REFRESH

Status

Network

Switching

MAC Address Table

Security

ACL

QoS

General

QoS Basic Mode

QoS Advanced Mode

Rate Limit

Ingress Port Settings

Ingress VLAN Settings

Egress Port Settings

Egress Queue Settings

Management

Diagnostics

Maintenance

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)

Apply

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

5.8 MANAGEMENT

POE

POE Global Setting

To display POE Global Setting web page, click **Management > POE > POE Global Setting**

This page is used to check POE Status, you can set Max Available Power here.

Global Setting	
Max Available Power	500 (0-900)Watt
System Operation Status	On
Main Power Consumption	0 (Watt)
Device Temperature	
Device #1	51(C)
Device #2	53(C)
Device #3	55(C)

MAX Available Power: Switch configuration can provide maximum power.

System Operation Status : display POE operation status on or off

Main Power Consumption: configure main power consumption

Device Temperature: display the temperature of device.

POE Port Setting

To display POE Global Setting web page, click **Management > POE > POE Port Setting**

This page allow user to configure POE setting.

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

Status

Network

Switching

MAC Address Table

Security

ACL

QoS

Management

POE

POE Global Setting

POE Port Setting

POE Delay Setting

LLDP

SNMP

RMON

Diagnostics

Maintenance

POE Port Setting

Port Select

Status

Priority

Power Budget

Select Ports

Enabled

Disabled

3-Low

2-Medium

1-Critical

30

(0-36)Watt

Apply

POE Port Status

Port	Status	Class	Priority	Power Consumption(Watt)	Power Budget(Watt)
GE1	enable	---	3	0.00	30
GE2	enable	---	3	0.00	30
GE3	enable	---	3	0.00	30
GE4	enable	---	3	0.00	30
GE5	enable	---	3	0.00	30
GE6	enable	---	3	0.00	30
GE7	enable	---	3	0.00	30
GE8	enable	---	3	0.00	30
GE9	enable	---	3	0.00	30
GE10	enable	---	3	0.00	30
GE11	enable	---	3	0.00	30
GE12	enable	---	3	0.00	30
GE13	enable	---	3	0.00	30
GE14	enable	---	3	0.00	30
GE15	enable	---	3	0.00	30

Port Select: Select specific ports.

Priority: Setting the priority of POE.

Critical

High

Low

Power Budget: POE port estimation can provide power.

POE Delay Setting

To display POE Global Setting web page, click **Management > POE > POE Delay Setting**

This page is for setting POE Power Delay.

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

Status

Network

Switching

MAC Address Table

Security

ACL

QoS

Management

POE

LLDP

SNMP

RMON

Diagnostics

Maintenance

POE Power Delay

POE Delay Setting

POE Delay Status

Port Select

Delay Mode

Delay Time

Select Ports

☒ Enabled
☐ Disabled

0 (0-300)Sec

Apply

POE Delay Status

Port	Delay Mode	Delay Time(Second)
GE1	disable	0
GE2	disable	0
GE3	disable	0
GE4	disable	0
GE5	disable	0
GE6	disable	0
GE7	disable	0
GE8	disable	0
GE9	disable	0
GE10	disable	0
GE11	disable	0
GE12	disable	0
GE13	disable	0
GE14	disable	0
GE15	disable	0

Port Select: Select specific ports.

Delay Mode: enable or disable delay mode.

Delay Time: Configuration delay time.

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.

LLDP Global Settings

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

SAVE | LOGOUT | REBOOT | REFRESH

Status

Network

Switching

MAC Address Table

Security

ACL

QoS

Management

POE

LLDP

SNMP

RMON

Diagnostics

Maintenance

LLDP Global Setting

LLDP Global Setting

LLDP Global Setting

Global Settings

LLDP Global Config

Enabled

☒ Enabled
☐ Disabled

LLDP PDU Disable Action

☐ Filtering
☐ Bridging
☒ Flooding

Transmission Interval

30 (5-32768)

Holdtime Multiplier

4 (2-10)

Reinitialization Delay

2 (1-10)

Transmit Delay

2 (1-6192)

LLDP-MED Fast Start Repeat Count

3 (1-10)

Apply

LLDP Global Config

Config Name	Config Value
LLDP Enabled	Enabled
LLDP PDU Disable Action	Flooding
Transmission Interval	30 Secs
Holdtime 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.

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

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

LLDP Port Settings

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

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

State: Select the transmission state of LLDP port interface.

Disable: Disable the transmission of LLDP PDUs.

RX Only: Receive LLDP PDUs only.

TX Only: Transmit LLDP PDUs only.

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

Port Select: Select specific ports.

Optional TLV Select: Select Optional TLVs.

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

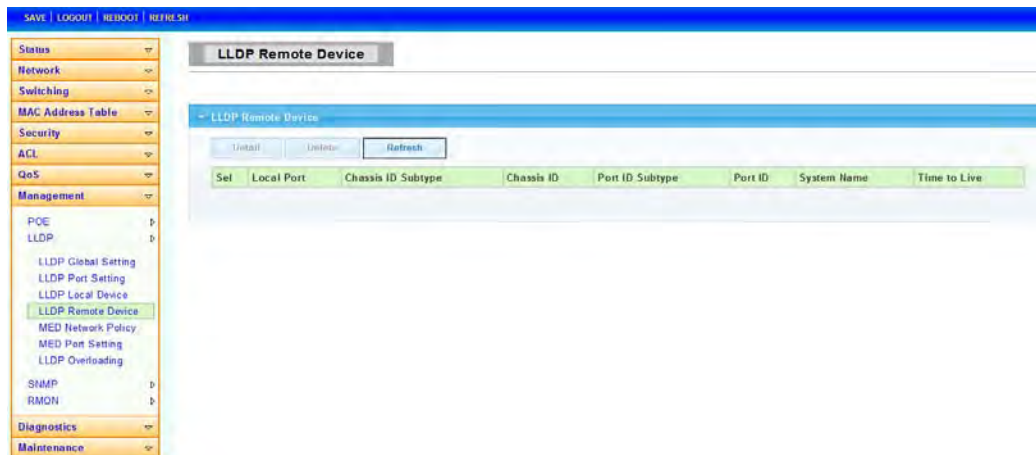
Port Status

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

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

Unlink Init Refresh

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

LLDP Network Policy

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

SAVE | LOGOUT | REBOOT | REFRESH

LLDP MED Network Policy Setting

Voice Auto Mode Configuration

LLDP MED Policy for Voice Application ☒ Auto ☐ Manual

Apply

Network Policy Configuration

Network Policy Number	1
Application	Voice
VLAN ID	1 (1-4096)
VLAN Tag	☒ Tagged ☐ Untagged
L2 Priority	0 (0-7)
DSCP Value	0 (0-63)

Apply

LLDP MED Network Policy Table

Delete

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

MED Port Setting

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

SAVE | LOGOUT | REBOOT | REFRESH

LLDP Port MED Setting

Port LLDP MED Configuration

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

Apply

LLDP MED Port Setting Table

Interface	LLDP MED Status	User Defined Network Policy		Location	Inventory
		Active	Application		
GE1	Enabled	Yes		No	No
GE2	Enabled	Yes		No	No
GE3	Enabled	Yes		No	No
GE4	Enabled	Yes		No	No
GE5	Enabled	Yes		No	No
GE6	Enabled	Yes		No	No
GE7	Enabled	Yes		No	No
GE8	Enabled	Yes		No	No
GE9	Enabled	Yes		No	No
GE10	Enabled	Yes		No	No
GE11	Enabled	Yes		No	No
GE12	Enabled	Yes		No	No
GE13	Enabled	Yes		No	No
GP14	Enabled	Yes		No	No

LLDP Overloading

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

SAVE LOGOUT REBOOT REFRESH												
Status	LLDP Port Overloading											
Network	LLDP Port Overloading Table											
Switching												
MAC Address Table												
Security												
ACL												
QoS												
Management												
POE												
LLDP												
LLDP Global Setting												
LLDP Port Setting												
LLDP Local Device												
LLDP Remote Device												
MED Network Policy												
MED Port Setting												
LLDP Overloading												
SNMP												
RMON												
Diagnostics												
Maintenance												

Interface	Total (Bytes)	Left to Send (Bytes)	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)	
GE10	63	1425	Not Overloading	22 (Transmitted)	9 (Transmitted)		10 (Transmitted)		14 (Transmitted)		8 (Transmitted)	
GE11	63	1425	Not Overloading	22 (Transmitted)	9 (Transmitted)		10 (Transmitted)		14 (Transmitted)		8 (Transmitted)	

SNMP

SNMP Setting

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

SAVE LOGOUT REBOOT REFRESH												
Status	SNMP Setting											
Network												
Switching												
MAC Address Table												
Security												
ACL												
QoS												
Management												
POE												
LLDP												
SNMP												
SNMP Setting												
SNMP View												
SNMP Access Group												
SNMP Community												
SNMP User												
SNMPv1.2 Notification Recipients												
SNMPv3 Notification Recipients												
SNMP Engine ID												
SNMP Remote Engine ID												
RMON												
Diagnostics												
Maintenance												

SNMP Global Setting	
State	☒ Disabled ☐ Enabled
Apply	

SNMP Informations	
Information Name	Information Value
SNMP	Disabled

State: SNMP daemon state

Enabled: Enable SNMP daemon

Disabled: Disable SNMP daemon

SNMP View

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

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

SAVE | LOGOUT | REBOOT | REFRESH

SNMP View

View Table Setting

View Name	Subtree OID	Subtree OID Mask	View Type
		all	☒ included ☐ excluded

[Add](#)

View Table Status

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

SNMP Access Group

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

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

SAVE | LOGOUT | REBOOT | REFRESH

SNMP Access Group

Access Group Setting

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

[Add](#)

Access Group Status

Group Name	Security Model	Security Level	Read View Name	Write View Name	Notify View Name	Action
v1	community	all	None	None	None	Delete

SNMP Community

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

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

The screenshot shows the 'SNMP Community' configuration page. On the left is a navigation menu with categories like Status, Network, Switching, MAC Address Table, Security, ACL, QoS, and Management. Under Management, there are sub-items for POE, LLDP, and SNMP. The SNMP section is expanded, showing options like SNMP Setting, SNMP View, SNMP Access Group, and SNMP Community (which is selected). The main content area has a 'SNMP Community' tab. Below it is a 'Community Setting' table with columns: Community Name, Community Mode, Group Name, View Name, and Access Right. The table contains one row with 'Basic' in Community Mode, 'all' in View Name, and 'rw' in Access Right. There is an 'Add' button below the table. Below the table is a 'Community Status' section with a table showing the status of the community. The table has columns: Community Name, Group Name, View Name, Access Right, and Action. It shows one entry with 'public' as the Community Name, 'all' as the View Name, 'rw' as the Access Right, and a 'Delete' button in the Action column.

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.

The screenshot shows the 'SNMP User Table' configuration page. On the left is the same navigation menu as in the previous screenshot. The 'SNMP User' option under the Management > SNMP section is selected. The main content area has a 'SNMP User Table' tab. Below it is a 'User Setting' table with columns: User Name, Group, Privilege Mode, Authentication Protocol, Authentication Password, Encryption Protocol, and Encryption Key. The table contains one row with 'noauth' in Privilege Mode, 'None' in Authentication Protocol, and 'None' in Encryption Protocol. There is an 'Add' button below the table. Below the table is a 'User Status' section with a table showing the status of the user. The table has columns: User Name, Group, Privilege Mode, Authentication Protocol, Encryption Protocol, Access Right, and Action. It shows one entry with 'noauth' as the Privilege Mode, 'None' as the Authentication Protocol, 'None' as the Encryption Protocol, and a 'Delete' button in the Action column.

SNMPv1,2 Notifcation Recipients

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

SAVE | LOGOUT | REBOOT | REFRESH

Status

Network

Switching

MAC Address Table

Security

ACL

QoS

Management

POE

LLDP

SNMP

SNMP Setting

SNMP View

SNMP Access Group

SNMP Community

SNMP User

SNMPv1.2 Notification Recipients

SNMPv3 Notification Recipients

SNMP Engine ID

SNMP Remote Engine ID

RMON

Diagnostics

Maintenance

Notification Recipients SNMPv1.2

SNMPv1.2 Host Setting

Server Address	SNMP Version	Notify Type	Community Name	UDP Port	TimeOut	Retries
	v1	Traps	public	162	(1-65535)	10 (1-300) 3 (1-255)

Add

SNMPv1.2 Host Status

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

SNMPv3 Notification Recipients

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

SAVE | LOGOUT | REBOOT | REFRESH

Status

Network

Switching

MAC Address Table

Security

ACL

QoS

Management

POE

LLDP

SNMP

SNMP Setting

SNMP View

SNMP Access Group

SNMP Community

SNMP User

SNMPv1.2 Notification Recipients

SNMPv3 Notification Recipients

SNMP Engine ID

SNMP Remote Engine ID

RMON

Diagnostics

Maintenance

Notification Recipients SNMPv3

SNMPv3 Host Setting

Server Address	Notify Type	User Name	UDP Port	TimeOut	Retries
	Traps		162	(1-65535)	10 (1-300) 3 (1-255)

Add

SNMPv3 Host Status

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

SNMP Engine ID

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

SAVE | LOGOUT | REBOOT | REFRESH

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

Engine ID Setting

Engine ID Settings

Use Default	☒ Enabled ☐ Disabled
Engine ID	DEADBEEF0102 (10-54)

Apply

Engine ID Status

Information Name	Information Value
Use Default	Enabled
Engine ID	DEADBEEF0102

SNMP Remote Engine ID

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

SAVE | LOGOUT | REBOOT | REFRESH

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

SNMP Remote Engine ID

Remote EngineID Setting

Remote IP Address	Engine ID

Add

Remote Engine ID Status

Remote IP Address	Remote Engine ID	Action
-------------------	------------------	--------

RMON

RMON Statistics

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

SAVE LOGOUT REBOOT REFRESH																																					
Status Network Switching MAC Address Table Security ACL QoS Management POE LLDP SNMP RMON RMON Statistics RMON Event RMON Event Log RMON Alarm RMON History RMON History Log Diagnostics Maintenance	RMON Statistics Port GE1 RMON Statistics Port GE1 Clear <table> <tr> <th>RMON Mib Name</th><th>Value</th></tr> <tr><td>etherStatsDropEvents</td><td>0</td></tr> <tr><td>etherStatsOctets</td><td>0</td></tr> <tr><td>etherStatsPkts</td><td>0</td></tr> <tr><td>etherStatsBroadcastPkts</td><td>0</td></tr> <tr><td>etherStatsMulticastPkts</td><td>0</td></tr> <tr><td>etherStatsCRCAlignErrors</td><td>0</td></tr> <tr><td>etherStatsUnderSizePkts</td><td>0</td></tr> <tr><td>etherStatsOverSizePkts</td><td>0</td></tr> <tr><td>etherStatsFragments</td><td>0</td></tr> <tr><td>etherStatsJabbers</td><td>0</td></tr> <tr><td>etherStatsCollisions</td><td>0</td></tr> <tr><td>etherStatsPkts64Octets</td><td>0</td></tr> <tr><td>etherStatsPkts65to127Octets</td><td>0</td></tr> <tr><td>etherStatsPkts128to255Octets</td><td>0</td></tr> <tr><td>etherStatsPkts256to511Octets</td><td>0</td></tr> <tr><td>etherStatsPkts512to1023Octets</td><td>0</td></tr> <tr><td>etherStatsPkts1024to1518Octets</td><td>0</td></tr> </table>	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
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																																				

RMON Event

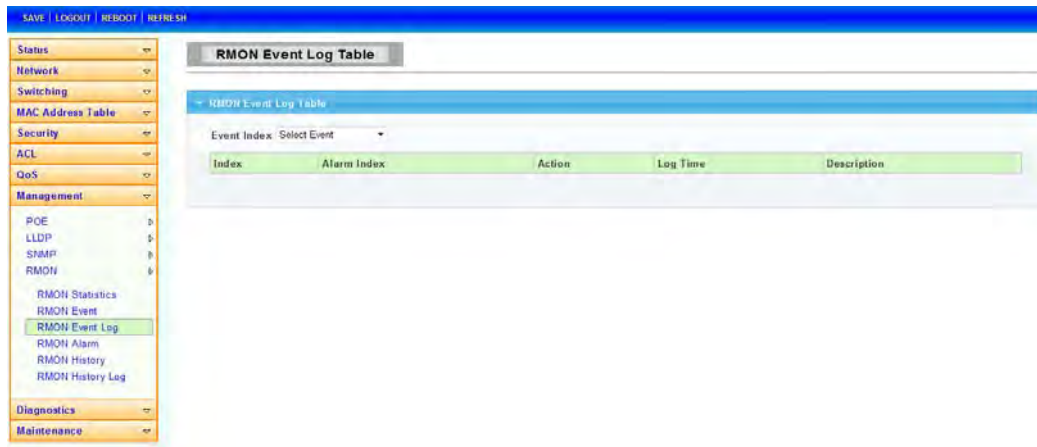
To display RMON Event web page, click **Management > RMON > RMON Event**

This page is used to configure RMON event group.

SAVE LOGOUT REBOOT REFRESH								
Status Network Switching MAC Address Table Security ACL QoS Management POE LLDP SNMP RMON RMON Statistics RMON Event RMON Event Log RMON Alarm RMON History RMON History Log Diagnostics Maintenance	RMON Event Settings RMON Event Select Index Create New Index 0 (1-5535) Type None Community public Owner (0-31 Characters) Description (0-127 Characters) Apply RMON Event <table> <tr> <th>Index</th><th>Event Type</th><th>Community</th><th>Description</th><th>Last Sent Time</th><th>Owner</th><th>Action</th></tr> </table>	Index	Event Type	Community	Description	Last Sent Time	Owner	Action
Index	Event Type	Community	Description	Last Sent Time	Owner	Action		

RMON Event Log

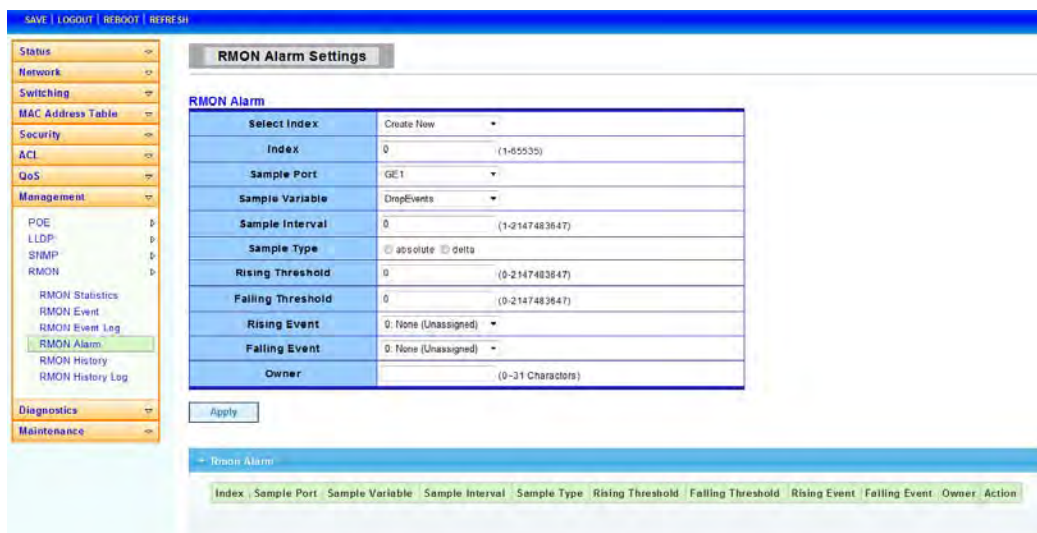
To display RMON Event Logweb page, click **Management > RMON > RMON Event Log**



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 History

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

This page is used to configure the PMON history group.

SAVE | LOGOUT | REBOOT | REFRESH

Status

Network

Switching

MAC Address Table

Security

ACL

QoS

Management

POE

LLDP

STAMP

RMON

RMON Statistics

RMON Event

RMON Event Log

RMON Alarm

RMON History

RMON History Log

Diagnostics

Maintenance

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)

Apply

RMON History

Index	Data Source	Bucket Requested	Interval	Owner	Action
-------	-------------	------------------	----------	-------	--------

RMON History Log

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

Log

SAVE | LOGOUT | REBOOT | REFRESH

Status

Network

Switching

MAC Address Table

Security

ACL

QoS

Management

POE

LLDP

STAMP

RMON

RMON Statistics

RMON Event

RMON Event Log

RMON Alarm

RMON History

RMON History Log

Diagnostics

Maintenance

RMON History Table

RMON History Table

History Index: Select History

No data available!

5.9 DIAGNOSTICS

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

System Status

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



Ping Test

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

Ping test Setting	
IP Address	192.168.1.100 (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

Apply

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.

Logging Setting

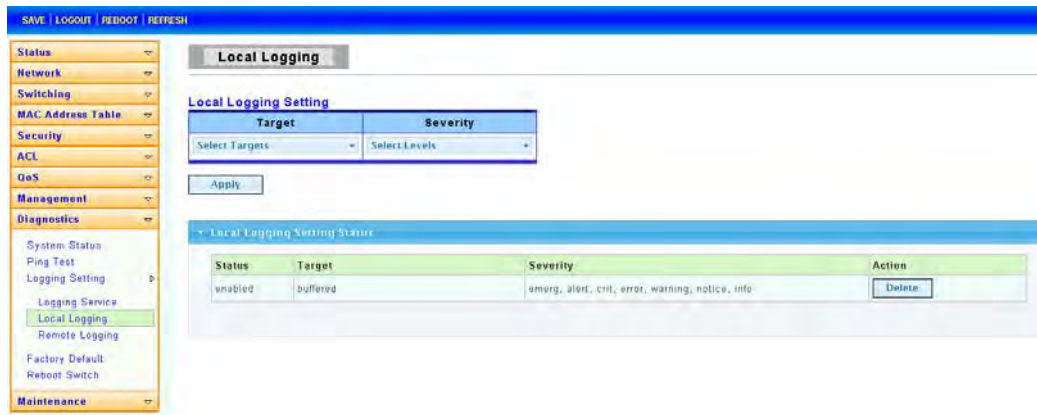
Logging Service

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



Local Logging

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



Target: Select the target to store log message

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

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

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

Remote Logging

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

The screenshot shows the 'Remote Logging' configuration page. On the left is a navigation menu with categories: Status, Network, Switching, MAC Address Table, Security, ACL, QoS, Management, Diagnostics, and Maintenance. The 'Diagnostics' category is expanded, showing options like System Status, Ping Test, Logging Setting, Local Logging, Remote Logging (highlighted), Factory Default, Reboot Switch, and Maintenance. The main content area has a 'Remote Logging' tab. Below it is the 'Remote Logging Setting' section with a table for configuration:

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

Below the table is an 'Apply' button. Further down is a 'Remote Logging Setting Status' section with a table showing the status of the logging settings:

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.

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.

The screenshot shows the 'Factory Default' configuration page. The navigation menu on the left is the same as in the previous screenshot, but 'Factory Default' is now highlighted under the 'Diagnostics' category. The main content area has a 'Factory Default' tab and a single 'Restore' button.

Reboot Switch

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

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



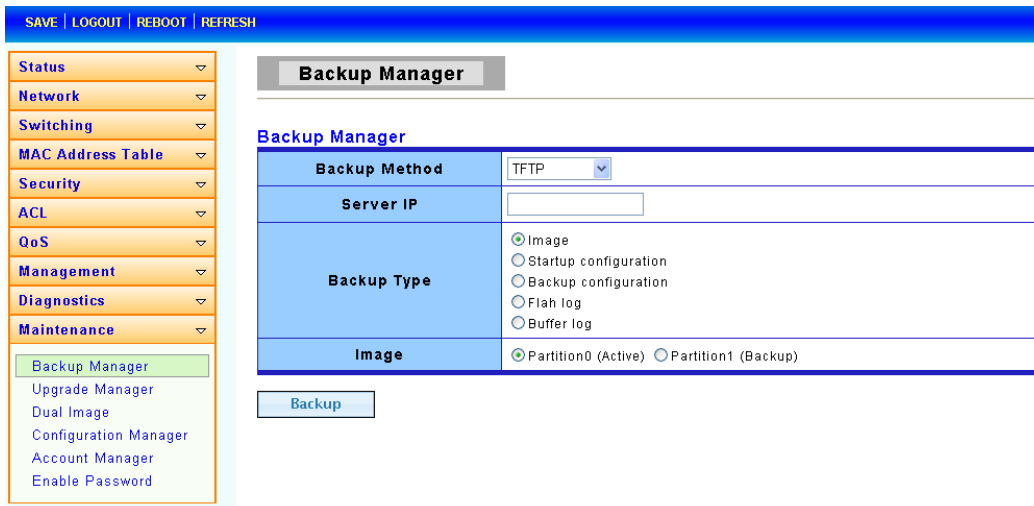
5.10 MAINTENANCE

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

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.



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

Status

Network

Switching

MAC Address Table

Security

ACL

QoS

Management

Diagnostics

Maintenance

Backup Manager

Upgrade Manager

Dual Image

Configuration Manager

Account Manager

Enable Password

Backup Manager

Backup Manager

Backup Method	HTTP
Backup Type	☒ Image ☐ Startup configuration ☐ Backup configuration ☐ Flash log ☐ Buffer log
Image	☒ Partition0 (Active) ☐ Partition1 (Backup)

Backup

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

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.

SAVE | LOGOUT | REBOOT | REFRESH

Status

Network

Switching

MAC Address Table

Security

ACL

QoS

Management

Diagnostics

Maintenance

Backup Manager

Upgrade Manager

Dual Image

Configuration Manager

Account Manager

Enable Password

Upgrade Manager

Upgrade Manager

Upgrade Method	TFTP
Server IP	
File Name	
Upgrade Type	☒ Image ☐ Startup Configuration ☐ Backup Configuration
Image	☐ (Active) ☒ (Backup)

Upgrade

SAVE | LOGOUT | REBOOT | REFRESH

Upgrade Manager

Upgrade Manager

Upgrade Method	HTTP
Upgrade Type	☒ Image ☐ Startup Configuration ☐ Backup Configuration
Image	☐ (Active) ☒ (Backup)
Browse file	浏览...

Upgrade

Upgrade Method: Select upgrade method

TFTP: Use TFTP to upgrade

HTTP: Use HTTP to upgrade

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

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

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

Upgrade Type: Select Backup Type

Dual Image

To display Dual Image web page, click **Maintenance > Dual Image**

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

Status

Network

Switching

MAC Address Table

Security

ACL

QoS

Management

Diagnostics

Maintenance

Backup Manager

Upgrade Manager

Dual Image

Configuration Manager

Account Manager

Enable Password

Dual Image

Dual Image Configuration

Active Image

☒ Partition0 (Active)
☐ Partition1 (Backup)

Apply

Images Information

Partition0

Active

Flash Partition

0

Image Name

Image Size

5679455 Bytes

Created Time

2014-03-18 13:26:37 UTC

Partition1

Backup

Flash Partition

1

Image Name

Image Size

131073 Bytes

Created Time

1970-01-01 00:00:00 UTC

Configuration Manager

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

SAVE | LOGOUT | REBOOT | REFRESH

Status

Network

Switching

MAC Address Table

Security

ACL

QoS

Management

Diagnostics

Maintenance

Backup Manager

Upgrade Manager

Dual Image

Configuration Manager

Account Manager

Enable Password

Configuration Manager

Save Configuration

Source File

☒ Running configuration

Destination File

☒ Startup configuration
☐ Backup configuration

Apply

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.

SAVE | LOGOUT | REBOOT | REFRESH

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

Backup Manager Upgrade Manager Dual Image Configuration Manager Account Manager Enable Password

Local User Information

New User

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

Apply

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.

SAVE | LOGOUT | REBOOT | REFRESH

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

Backup Manager Upgrade Manager Dual Image Configuration Manager Account Manager Enable Password

Local User Information

New User

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

Apply

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.

Enable Password

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

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

Privilege Value	Password Type	Modify
15	Encrypted	Delete

Password Type: Select password type for enable password.

Clear Text: Password without encryption

Encrypted: Password with encryption

Password: Password string.

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