



## LNP-2804GN-SFP-T

**28-Port Industrial Gigabit PoE+ Managed Ethernet Switches,  
with 24\*10/100/1000Tx, and 4\* Gigabit Combo Ports  
(4\*10/100/1000Tx RJ45, 4\*100/1000 SFP Slots); EOT: -40°C to 75°C**



Version 1.1

## User Manual



## **© Copyright 2018 Antaira Technologies, LLC**

All Rights Reserved

This document contains information, which is protected by copyright. Reproduction, adaptation or translation without prior permission is prohibited, except as allowed under the copyright laws.

## **Trademark Information**

Antaira is a registered trademark of Antaira Technologies, LLC, Microsoft Windows and the Windows logo are the trademarks of Microsoft Corp. NetWare is the registered trademark of Novell Inc. WMM and WPA are the registered trademarks of Wi-Fi Alliance. All other brand and product names are trademarks or registered trademarks of their respective owners.

**Notice:** Copyrights © 2018 by Antaira Technologies, LLC. All rights reserved. Reproduction, adaptation, or translation without prior permission of Antaira Technologies, LLC is prohibited, except as allowed under the copyright laws.

## **Disclaimer**

Antaira Technologies, LLC provides this manual without warranty of any kind, expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Antaira Technologies, LLC may make improvements and/or changes to the product and/or specifications of the product described in this manual, without prior notice. Antaira Technologies, LLC will not be liable for any technical inaccuracies or typographical errors found in this guide. Changes are periodically made to the information contained herein and will be incorporated into later versions of the manual. The information contained is subject to change without prior notice.

## **FCC Warning**

This equipment has been tested and found to comply with the limits for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. It may cause harmful interference to radio communications if the equipment is not installed and used in accordance with the instructions. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

**Caution:** Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

## **CE Mark Warning**

This is a Class-A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

## **Industrial Ethernet Switches**

Industrial Grade Gigabit PoE Managed Ethernet Switches

User Manual

Version 1.1 (July 2018)

This manual supports the following models:

- LNP-2804GN-SFP-T

This document is the current official release manual. Please check our website ([www.antaira.com](http://www.antaira.com)) for any updated manual or contact us by e-mail ([support@antaira.com](mailto:support@antaira.com)).

## Table of Contents

<b>1. Introduction .....</b>	<b>8</b>
1.1 Product Overview .....	8
1.2 Product Software Features .....	8
1.3 Product Hardware Features .....	9
1.4 Package Contents .....	9
1.5 Safety Precaution .....	9
<b>2. Hardware Description .....</b>	<b>10</b>
2.1 Physical Dimensions.....	10
2.2 Front Panel.....	11
2.3 Back Panel .....	11
2.4 LED Indicators .....	11
2.5 Reset Button.....	13
2.6 Ethernet Ports.....	13
2.7 Cabling .....	14
2.8 Wiring the Power Inputs.....	14
2.9 Wiring a Relay Contact .....	15
<b>3. Mounting Installation .....</b>	<b>16</b>
3.1 Rack-Mounting .....	16
<b>4. Web Management.....</b>	<b>17</b>
4.1 Log In .....	17
4.2 Recommended Practices.....	17
4.3 Changing Default Password .....	17
4.4 Monitoring.....	18
4.5 Device Information.....	18
4.6 Logging Message .....	19
4.7 Port Monitoring .....	20

4.8	Link Aggregation.....	21
4.9	LLDP Statistics .....	22
4.10	IGMP/MLD Statistics.....	23
4.11	System .....	25
4.12	IP Settings .....	25
4.13	IPv6 Settings .....	26
4.14	DHCP Client Option 82.....	27
4.15	DHCP Auto Provision .....	28
4.16	Management VLAN .....	30
4.17	System Time.....	31
4.18	L2 Switching .....	33
4.19	Port Configuration.....	33
4.20	Port Mirror .....	34
4.21	Link Aggregation.....	35
4.22	802.1Q VLAN .....	39
4.23	Q-in-Q.....	42
4.24	GARP .....	44
4.25	802.3az EEE.....	46
4.26	Multicast .....	47
4.27	Jumbo Frame .....	53
4.28	Spanning Tree.....	54
4.28.1	ERPS.....	61
4.29	X-Ring .....	62
4.31	Loopback Detection.....	64
4.31.1	L3 Switching .....	66
4.31.2	SNAT.....	66
4.31.3	DNAT.....	68

4.31.4 Routing .....	69
4.32 MAC Address Table.....	70
4.33 Static MAC .....	70
4.34 MAC Aging Time .....	71
4.35 Dynamic Forwarding Table .....	72
4.36 Security .....	73
4.37 Storm Control .....	73
4.38 Port Security.....	75
4.39 Protected Ports.....	75
4.40 DoS Prevention .....	76
4.41 Applications .....	80
4.42 802.1x.....	83
4.43 IP Security .....	85
4.44 QoS .....	86
4.45 General.....	86
4.46 QoS Basic Mode.....	94
4.47 Rate Limit .....	96
4.48 Management.....	98
4.49 LLDP .....	98
4.50 SNMP .....	103
4.51 Power Over Ethernet.....	106
4.53 DHCP Server.....	109
4.54 SMTP Client .....	115
4.55 RMON .....	118
4.56 Diagnostics.....	122
4.57 Cable Diagnostics.....	122
4.58 Ping Test .....	123

4.59 IPv6 Ping Test .....	125
4.60 System Log .....	126
4.61 DDM .....	129
4.62 LED Indication .....	130
4.63 Tools.....	131
4.64 Backup Manager .....	131
4.65 Upgrade Manager.....	132
4.66 Dual Image .....	133
4.67 Save Configuration .....	134
4.68 User Account .....	134
4.69 Reset System .....	135
4.71 Reboot Device .....	136
<b>5. Command Line Interface Management .....</b>	<b>136</b>
5.1 About CLI Management.....	136
<b>6. Technical Specifications .....</b>	<b>151</b>

# 1. Introduction

All Antaira industrial managed switches come with a pre-installed “user-friendly” web console interface, which allows users to easily configure and manage the units, whether one is using a serial console and command line interface (CLI) commands like Telnet, SSH, HTTP (Web GUI) or simple network management protocols (SNMP).

## 1.1 Product Overview

**Antaira Technologies’ LNP-2804GN-SFP-T** is a 28-port industrial Gigabit PoE+ managed Ethernet switch embedded with 24\*10/100/1000Tx Ethernet ports that support IEEE802.3at/af for a maximum of 30W/port and 4\*100/1000 SFP slots for combo RJ45/Fiber connections. The LNP-2804GN-SFP-T is a fully manageable Layer 3 Ethernet switch that is pre-loaded with a user-friendly web management console design. It supports Source NATs, Destination NATs, and Static Routing. It also has network redundancy function using ERPS, X-Ring (ultra-high-speed recovery time < 20 ms), RSTP/STP (802.1w/1D), MSTP. The advanced network filtering and security functions, such as IGMP, VLAN, QoS, SNMP, port lock, RMON, and 802.1X/HTTPS/SSH/SSL increase determinism and improve network management for remote SCADA systems or control networks.

The LNP-2804GN-SFP-T is IP30 rated and rack mount design with extended temperature range (EOT: -40°C to 75°C). It also provides high EFT and ESD protection for industrial networking applications, such as power/utility, water wastewater, oil/gas/mining, factory automation, security surveillance, ITS and any other outdoor or harsh environment applications.

## 1.2 Product Software Features

- NAT/Routing
  - Source NAT, Destination NAT, and Static Routing
- Network Redundancy
  - ERPS (ITU-T G.8032 Open Standard Protocol), X-Ring (ultra-high-speed recovery time < 20 ms), RSTP/STP (802.1w/1D), MSTP for network redundancy
- Network Management
  - Web UI based management, SNMP v1/v2/v3, serial console
  - QoS, traffic classification QoS, COS, bandwidth control for Ingress and Egress, broadcast storm control, DiffServ
  - IEEE802.1q VLAN tagging, port-based VLAN support
  - IGMP snooping v1/v2
  - Supports IPv4/IPv6, RMON, MIB II, port mirroring, event syslog, DNS, NTP/SNTP, HTTPS, SSH/SSL, TFTP
- Port Configuration
  - Status, statistics, mirroring, rate limiting, event syslog
- Event Handling
  - Fault Alarm Relay Output
- Software Upgrade via TFTP and HTTP



## 1.3 Product Hardware Features

- System Interface and Performance
  - Embedded 24\*10/100/1000Tx (PSE 30W/Port) RJ45 Ports and 4\*100/1000 SFP slots for combo RJ45/Fiber
  - Store-and-forward switching architecture
  - 8k MAC address table
- Power Input
  - DC 46~57V redundant with a 4-pin terminal block
  - 2 alarm relay output
- Operating Temperature
  - Extended operating temperature models: -40°C to 75°C
- Case/Installation
  - IP30 protection metal housing
  - Rack mount design

## 1.4 Package Contents

- 1 - LNP-2804GN-SFP-T
- 1 - Quick installation guide
- 1 - Rack Mount Kit
- 1 - RJ45 to DB9 Serial Console cable

## 1.5 Safety Precaution

**Attention:** If the DC voltage is supplied by an external circuit, please use a protection device on the power supply input. The industrial Ethernet switch's hardware specs, ports, cabling information, and wiring installation will be described within this user manual.

## 2. Hardware Description

### 2.1 Physical Dimensions

Figure 2.1, below, shows the physical dimensions of Antaira's LNP-2804GN-SFP-T series: 28-Port Industrial Gigabit PoE+ Managed Ethernet Switches with 24\*10/100/1000Tx, and 4\* Gigabit Combo Ports (4\*10/100/1000Tx RJ45, 4\*100/1000 SFP Slots).

(W x D x H) is **438mm x 259.2mm x 43.6mm**

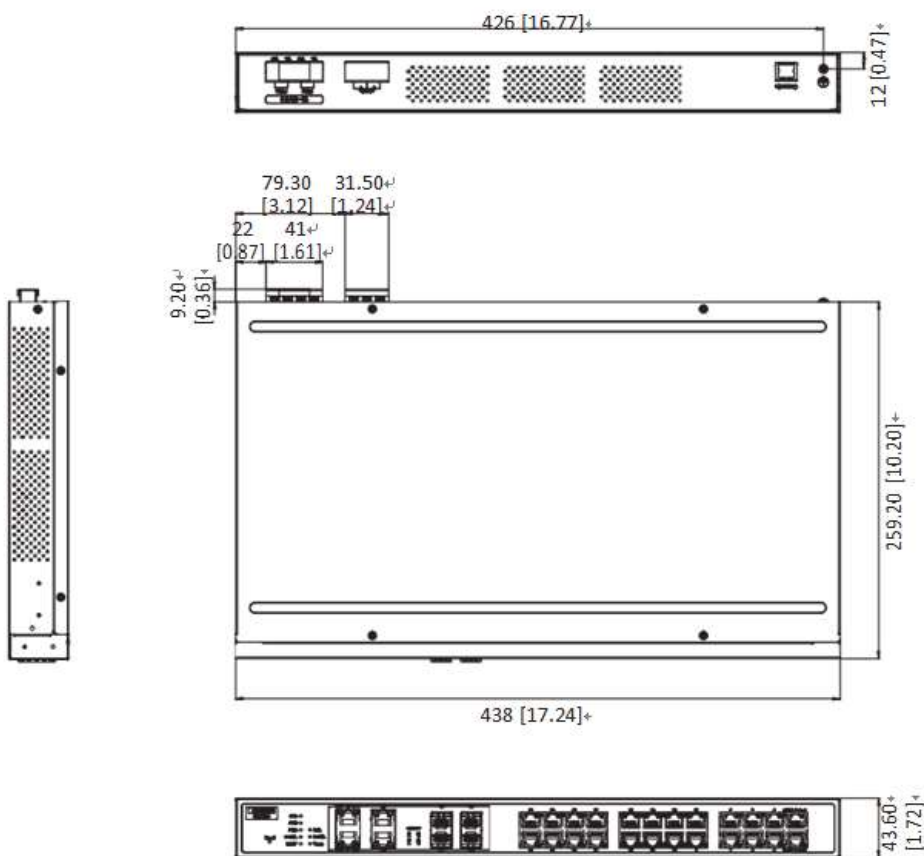


Figure 2.1

## 2.2 Front Panel

The front panel of the LNP-2804GN-SFP-T series industrial gigabit PoE+ managed Ethernet switch is shown below in *Figure 2.2*.

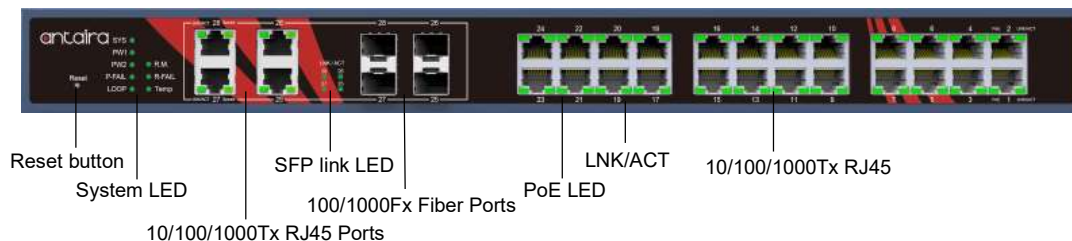


Figure 2.2

## 2.3 Back Panel

*Figure 2.3*, below, shows the back panel of the LNP-2804GN-SFP-T switch that is equipped with one 4-pin terminal block connector for dual DC power inputs 46~57VDC.

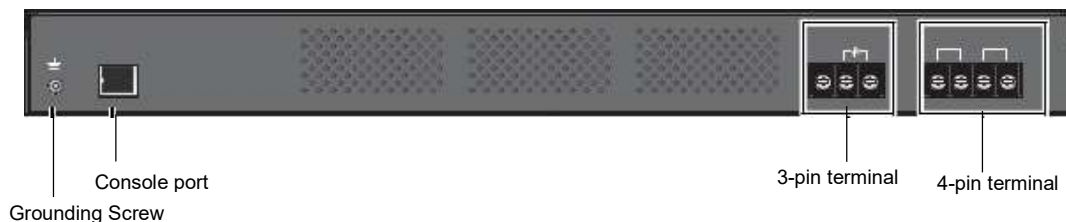


Figure 2.3

## 2.4 LED Indicators

There are LED light indicators located on the front panel of the industrial Ethernet switch that display the power status and network status. Each LED indicator has a different color and has its own specific meaning, see below in *Table 2.1*.

LED	Color	Description	
SYS	Green	On	System is operating normally
		Off	System is powered down / system crash / operation initiating
PWR1	Green	On	Power input 1 is active
		Off	Power input 1 is inactive
PWR2	Green	On	Power input 2 is active
		Off	Power input 2 is inactive
P-FAIL	Red	On	When PW1 or PW2 is disconnected, the LED is on.

		Off	When PW1 and PW2 is connected, the LED is off.
LOOP Detection	Red	On	When loop detected, the LED is on.
		Off	No loop detected
R. M. (Ring Master)	Green	On	An active switch within the ring is a designated ring master
		Off	No ring master determined in current ring
Ring Fail	Red	On	A ring port within the ring loop is identified as having a ring ID within a second ring loop
		Off	No ring ports having a ring ID within a secondary ring loop are detected
Temp	Red	On	IC sensor detects a temperature range exceeding set temperature range
		Off	IC sensor detects normal operating temperature
SFP LED	Green	On	SFP or GBIC plug-in and link up
		Blink	Packet transmit and receive
		Off	SFP or GBIC plug-out or link down
PoE (Left LED) (PoE Ports)	Green	On	Connect to PD and supply power
		Blink	Not applicable
		Off	Disconnect from PD
LNK/ACT (Right LED) (PoE Ports)	Green	On	Current link speed is 1000M
		Blink	Packet transmit and receive
		Off	No link
	Amber	On	Current link speed is 100/10M
		Blink	Packet transmit and receive
		Off	No link
LNK/ACT (Left LED) (Combo Ports)	Green	On	Link
		Off	No link
LNK/ACT (Right LED) (Combo Ports)	Green	On	Current link speed is 1000M
		Blink	Packet transmit and receive
		Off	No link
	Amber	On	Current link speed is 100/10M
		Blink	Packet transmit and receive
		Off	No link

Table 2.1

## 2.5 Reset Button

There is a 'Reset' button located on the front panel of the industrial Ethernet switch that helps users to reboot or restore default by pressing the button for different seconds. Please refer to *Table 2.2* for the timing and function.

Seconds	Function
3	System reboot
5	Reset configuration to factory default

Table 2.2

## 2.6 Ethernet Ports

### ■ RJ-45 Ports

**RJ-45 Ports (Auto MDI/MDIX):** The RJ-45 ports are auto-sensing for 10Base-T, 100Base-TX, or 1000Base-T connections. Auto MDI means that the switch can connect to another switch or workstation without changing the straight-through or crossover cabling. See the figures below for straight-through and crossover cabling schematics.

### ■ RJ-45 Pin Assignment

The following figures show the cabling schematics for straight-through and crossover cables:

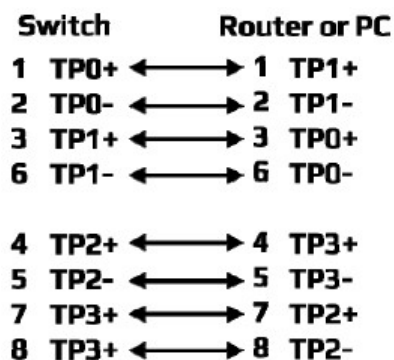


Figure 2.4  
Straight-Through Cables Schematic

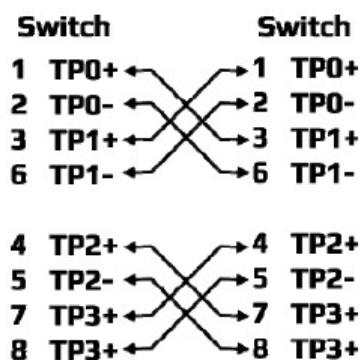
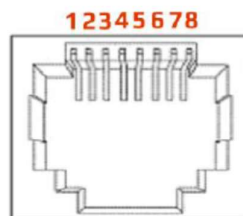


Figure 2.5  
Crossover Cables Schematic

The following figures show the 10,100, and 1000 Ethernet RJ45 pin outs.

Pin	Label
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-



## 2.7 Cabling

Use the four twisted-pair, category 5e, or the above cabling for the RJ-45 port connections. The cable between the switch and the link partner (switch, hub, workstation, etc.) must be less than 100 meters (328 ft.) in length.

## 2.8 Wiring the Power Inputs

There are two power inputs for normal and redundant power configurations. The power input 2 is used for wiring a redundant power configuration. See the following for terminal block connector views.

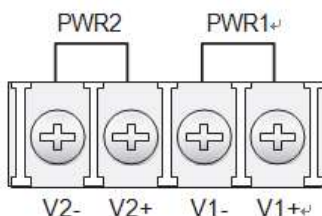


Figure 2.6 Terminal Receptor: Power Input Contacts

To wire the power inputs:

1. Make sure the power is not connected to the switch or the power converter before proceeding.
2. Insert a small flat-bladed screwdriver in the V1+/V1- wire-clamp screws, and loosen the screws.
3. Insert the negative/positive DC wires into the V+/V- terminals of PW1. If setting up power redundancy, connect PW2 in the same manner.
4. Tighten the wire-clamp screws to secure the DC wires in place.

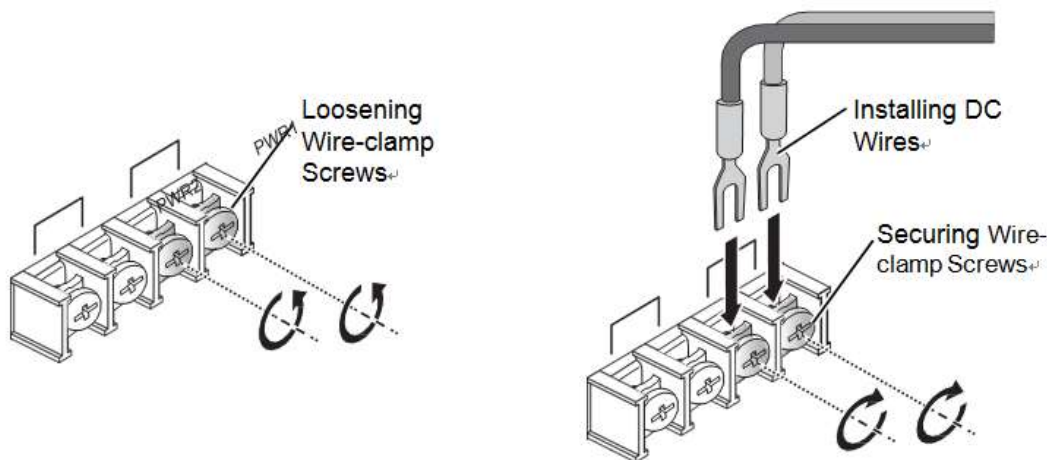


Figure 2.7 Installing DC Wires in a Terminal Block

## 2.9 Wiring a Relay Contact

The following section details the wiring of the relay output. The wires are installed onto the fixed terminal block located on the back of the switch.

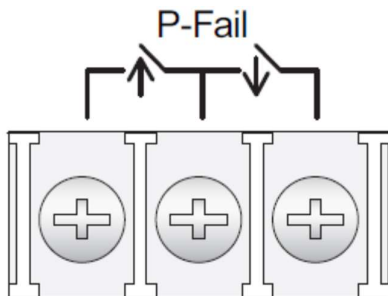


Figure 2.8 - Wiring the Fault Alarm Contact

The fixed terminal block includes a total of six pins: two for PWR1, two for PWR2 and two for a fault circuit.

---

**Note** • The wire gauge for the terminal block should range between 12 ~ 24AWG

---

## 3. Mounting Installation

### 3.1 Rack-Mounting

1. Align the rack mount brackets with the holes on the switch.
2. Secure the rack mount brackets with the provided screws.
3. Align the switch with the posts on the rack cabinet.
4. Secure the switch with the provided screws.



Figure 2.9 Installing the Switch



## 4. Web Management

### 4.1 Log In

To access the login window, connect the device to the network; see “Connecting the Switch to Ethernet Ports”. Once the switch is installed and connected, power on the switch; see the following procedures in Figure 4.1 to log into your switch. When the switch is first installed, the default network configuration is set to DHCP enabled. You will need to make sure your network environment supports the switch setup before connecting it to the network.

1. Launch your web browser on a computer.
2. In the browser's address bar, type in the switch's default IP address (192.168.1.254). The login screen displays.
3. Enter the default user name and password (admin/admin) to log into the management interface. You can change the default password after you have successfully logged in.
4. Click **Login** to enter the management interface.

The image shows a web-based login form with a light yellow background. It contains two text input fields: the top one is labeled "Username" and the bottom one is labeled "Password". Below the password field is a blue button with the text "Login" in white.

Figure 4.1

### 4.2 Recommended Practices

Antaira recommends creating a best practices policy for securing your network. This type of policy could be as simple as verifying that secure passwords have been used in place of default passwords but may also include other measures to maintain the security of the network.

### 4.3 Changing Default Password

In keeping with good management and security practices, it is recommended that you change the default password as soon as the device is functioning and setup correctly. The following details the necessary steps to change the default password.

To change the password:

1. Navigate to **Tools > User Account**.
2. From the User drop-down menu, select the Admin (default) account.
3. In the **User Name** field, enter admin for this account. It is not necessary to change the user name, however, a change in the default settings increases the security settings.
4. In the **Password** field, type in the new password. Re-type the same password in the **Retype Password** field.
5. Click **Apply** to change the current account settings.

The screenshot shows a web-based configuration window titled "Add/Edit User". It features several input fields and dropdown menus:
 

- User Name:** A text input field containing "Input name".
- Password Type:** A dropdown menu currently set to "Clear Text".
- Password:** A text input field containing "Input password".
- Retype Password:** A text input field containing "Input password".
- Privilege Type:** A dropdown menu currently set to "Admin".

 An "Apply" button is located at the bottom center of the form.

Figure 4.2

After saving all the desired settings, perform a system save (**Tools > Save Configuration**). The changes are saved.

## 4.4 Monitoring

## 4.5 Device Information

The Device Information menu lists information pertaining to the system, such as System Name, System Location, MAC Address, Firmware Version, and more. The information is for review only. To modify the device information, see the respective item within the user interface.

To access this page, click **Monitoring > Device Information**.

The screenshot shows a table titled "Device Information" with the following data:

Information Name	Information Value
System Name	Switch
System Location	Default
System Contact	Default
MAC Address	7C:CB:0D:01:FF:DB
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Gateway	192.168.1.1
Loader Version	1.0.0.48895
Loader Date	Sep 21 2016 - 14:16:09
Firmware Version	1.00.00
Firmware Date	Jul 25 2017 - 16:26:09
Build Version	D060626S03535
System OID	1.3.6.1.4.1.38477.311.1.81
System Up Time	0 days, 0 hours, 3 mins, 10 secs

Figure 4.3

The following table describes the items in Figure 4.3.

Item	Description
System Name	Click <b>Switch</b> to enter the system name: up to 128 alphanumeric characters (default is Switch).
System Location	Click <b>Default</b> to enter the location: up to 256 alphanumeric characters (default is Default).
System Contact	Click <b>Default</b> to enter the contact person: up to 128 alphanumeric characters (default is Default).
MAC Address	Displays the MAC address of the switch.
IP Address	Displays the assigned IP address of the switch.
Subnet Mask	Displays the assigned subnet mask of the switch.
Gateway	Displays the assigned gateway of the switch.
Loader Version	Displays the current loader version of the switch.
Loader Date	Displays the current loader build date of the switch.
Firmware Version	Displays the current firmware version of the switch.
Firmware Date	Displays the current firmware build date of the switch.
Build Version	Displays the current firmware build version of the switch.
System Object ID	Displays the base object ID of the switch.
System Up Time	Displays the time since the last switch reboot.

## 4.6 Logging Message

The Logging Message Filter page allows you to enable the display of the logging message filter. To access this page, click **Monitoring > Logging Message**.

Figure 4.4

The following table describes the functions in Figure 4.4.

Function	Description
----------	-------------

Target	Click the drop-down menu to select a target to store the log messages. Buffered: Store log messages in RAM. All log messages are cleared after system reboot. File: Store log messages in a file.
Severity	The setting allows you to designate a severity level for the Logging Message Filter function. Click the drop-down menu to select the severity level target setting. The level options are: <ul style="list-style-type: none"> <li>● emerg: Indicates system is unusable. It is the highest level of severity.</li> <li>● alert: Indicates action must be taken immediately.</li> <li>● crit: Indicates critical conditions.</li> <li>● error: Indicates error conditions.</li> <li>● warning: Indicates warning conditions.</li> <li>● notice: Indicates normal but significant conditions.</li> <li>● info: Indicates informational messages.</li> <li>● debug: Indicates debug-level messages.</li> </ul>
Category	Click the drop-down menu to select the category level target setting.
View	Click <b>View</b> to display all Logging Information and Logging Message Information.
Refresh	Click <b>Refresh</b> to update the screen.
Clear buffered messages	Click <b>Clear buffered messages</b> to clear the logging buffer history list.
The ensuing table for <b>Logging Information</b> table settings are informational only: Target, Severity and Category. The ensuing table for <b>Logging Message</b> table settings are informational only: No., Time Stamp, Category, Severity and Message.	

## 4.7 Port Monitoring

Port Network Monitor is a bandwidth and network monitoring tool for the purpose of capturing network traffic and measuring of network throughput. The monitoring functionality includes listing of port statistics as well as port utilization.

### Port Statistics

To access this page, click **Monitoring > Port Monitoring > Port Statistics**.



Figure 4.5 Monitoring > Port Monitoring > Port Statistics

The following table describes the functions in Figure 4.5.

Function	Description
----------	-------------

Port	Click the drop-down menu to select a port and its captured statistical setting values.
Clear	Click <b>Clear</b> to clear the counter selections.

The ensuing list for **IF MIB Counters** settings are informational only: ifInOctets, ifInUcastPkts, ifInNUcastPkts, ifInDiscards, ifOutOctets, ifOutUcastPkts, ifOutNUcastPkts, ifOutDiscards, ifInMulticastPkts, ifInBroadcastPkts, ifOutMulticastPkts, and ifOutBroadcastPkts.

The ensuing list for **Ether-Like MIB Counters** settings are informational only: dot3StatsAlignmentErrors, dot3StatsFCSErrors, dot3StatsSingleCollisionFrames, dot3StatsMultipleCollisionFrames, dot3StatsDeferredTransmissions, dot3StatsLateCollisions, dot3StatsExcessiveCollisions, dot3StatsFrameTooLongs, dot3StatsSymbolErrors, dot3ControllnUnknownOpCodes, dot3InPauseFrames, and dot3OutPauseFrames.

The ensuing list for **Rmon MIB Counters** settings are informational only: etherStatsDropEvents, etherStatsOctets, etherStatsPkts, etherStatsBroadcastPkts, etherStatsMulticastPkts, etherStatsCRCAAlignErrors, etherStatsUnderSizePkts, etherStatsOverSizePkts, etherStatsFragments, etherStatsJabbers, etherStatsCollisions, etherStatsPkts64Octets, etherStatsPkts65to127Octets, etherStatsPkts128to255Octets, etherStatsPkts256to511Octets, etherStatsPkts512to1023Octets, and etherStatsPkts1024to1518Octets.

### Port Utilization

To access this page, click **Monitoring > Port Monitoring > Port Utilization**.

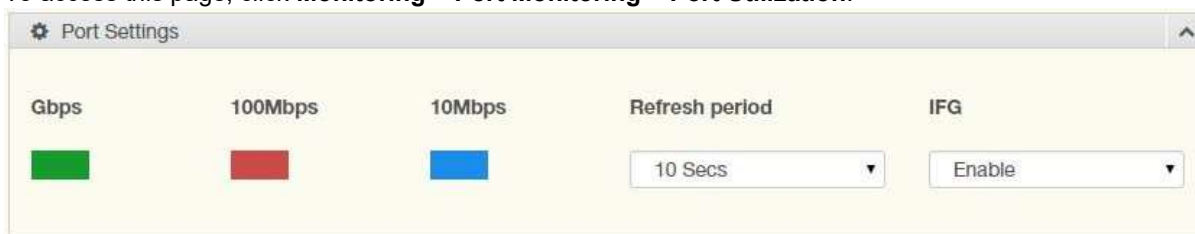


Figure 4.6

The following table describes the functions in the previous figure.

Function	Description
Refresh period	Click the drop-down menu to select and designate a period (second intervals) to refresh the information (TX and RX) listings.
IFG	Click the drop-down menu to enable or disable the Interframe Gap (IFG) statistic

## 4.8 Link Aggregation

The Link Aggregation function provides LAG information for each trunk. It displays membership status, link state, and membership type for each port.

To access this page, click **Monitoring > Link Aggregation**.

The ensuing table for **Link Aggregation Group Status** settings are informational only: LAG, Name, Type, Link State, Active Member, and Standby Member.

The ensuing table for **LACP Information** settings are informational only: LAG, Port, PartnerSysId, PnKey, AtKey, Sel, Mux, Receiv, PrdTx, AtState, and PnState.

## 4.9 LLDP Statistics

The LLDP Statistics page displays the LLDP statistics.

To access this page, click **Monitoring > LLDP Statistics**.

Information Name	Information Value
Insertions	0
Deletions	0
Drops	0
Age Outs	0

Figure 4.7

The ensuing table for **LLDP Global Statistics** settings are informational only: Insertions, Deletions, Drops, and Age Outs.

Function	Description
Clear	Click <b>Clear</b> to reset LLDP Statistics of all the interfaces.
Refresh	Click <b>Refresh</b> to update the data on the screen with the present state of the data in the switch.

The ensuing table for **LLDP Port Statistics** settings are informational only: Port, TX Frames (Total), RX Frames (Total, Discarded and Errors), RX TLVs (Discarded and Unrecognized) and RX Ageouts (Total).

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

## 4.10 IGMP/MLD Statistics

The IGMP Statistics function displays statistical package information for IP multicasting. To access this page, click **Monitoring > IGMP Statistics**.

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

Figure 4.8 Monitoring > IGMP Statistics

The following table describes the function in Figure 4.8.

Function	Description
Clear	Click <b>Clear</b> to refresh IGMP Statistics of all the interfaces.
Refresh	Click <b>Refresh</b> to update the data on the screen with the present state of the data in the switch.

The MLD Statistics function displays statistical package information for IP multicasting. To access this page, click **Monitoring > MLD Statistics**.

<span>Clear</span> <span>Refresh</span>	
MLD Statistics	
Statistics Packets	Counter
Total RX	0
Valid RX	0
Invalid RX	0
Other RX	0
Leave RX	0
Report RX	0
General Query RX	0
Special Group Query RX	0
Special Group & Source Query RX	0
Leave TX	0
Report TX	0
General Query TX	0
Special Group Query TX	0
Special Group & Source Query TX	0

The following table describes the items in the previous figure.

Item	Description
Clear	Click <b>Clear</b> to refresh MLD Statistics of all the interfaces.
Refresh	Click <b>Refresh</b> to update the data on the screen with the present state of the data in the switch.



## 4.11 System

### 4.12 IP Settings

The IP Settings menu allows you to select a static or DHCP network configuration. The Static displays the configurable settings for the static option. To access this page, click **System > IP Settings**.

Figure 4.9 System > IP Settings

The following table describes the items in the previous figure.

Item	Description
Mode	Click the radio button to select the IP Address Setting mode: Static or DHCP.
IP Address	Enter a value to specify the IP address of the interface. The default is 192.168.1.254.
Subnet Mask	Enter a value to specify the IP subnet mask for the interface. The default is 255.255.255.0.
Gateway	Enter a value to specify the default gateway for the interface. The default is 192.168.1.1.
DNS Server 1	Enter a value to specify the DNS server 1 for the interface. The default is 168.95.1.1.
DNS Server 2	Enter a value to specify the DNS server 2 for the interface. The default is 168.95.192.1.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **IP Address Information** settings are informational only: DHCP State, Static IP Address, Static Subnet Mask, Static Gateway, Static DNS Server 1 and Static DNS Server 2.

IP Address Information	
Information Name	Information Value
DHCP State	Disabled
Static IP Address	192.168.1.230
Static Subnet Mask	255.255.255.0
Static Gateway	192.168.1.254
Static DNS Server 1	168.95.1.1
Static DNS Server 2	168.95.192.1

## 4.13 IPv6 Settings

To access this page, click **System > IPv6 Settings**.

Figure 4.10 System > IPv6 Settings

The following table describes the items in the previous figure.

Item	Description
Auto Configuration	Select the radio button to enable or disable the IPv6.
IPv6 Address	Enter the IPv6 address for the system.
Gateway	Enter the gateway address for the system.
DHCPv6 Client	Enter the DHCPv6 address for the system.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **IPv6 Information** settings are informational only: Auto Configuration, IPv6 In Use Address, IPv6 In Use Router, IPv6 Static Address, IPv6 Static Router and DHCPv6 Client.

IPv6 Information	
Information Name	Information Value
Auto Configuration	Enabled
IPv6 Link Local Address	fe80::2e0:4cff:fe00:0 / 64
IPv6 In Use Address	fe80::2e0:4cff:fe00:0 / 64
IPv6 In Use Router	::
IPv6 Static Address	:: / 0
IPv6 Static Router	::
DHCPv6 Client	Disabled

## 4.14 DHCP Client Option 82

The DHCP Client Option 82 configurable Circuit ID and Remote ID feature enhances validation security by allowing you to select naming choices sub-options. You can select a switch configured hostname or specify an ASCII test string for the remote ID. You can also configure an ASCII text string to override the circuit ID.

To access this page, click **System > DHCP Client Option 82**.

**Mode**  Enabled  Disabled

**Circuit ID Format** String

**Circuit ID String** Input string

**Circuit ID Hex** Input HEX string

**Circuit ID User-Define** Input user-defined string

**Remote ID Format** String

**Remote ID String** Input string

**Remote ID Hex** Input HEX string

**Remote ID User-Define** Input user-defined string

Apply

Figure 4.11 System > DHCP Client Option 82

The following table describes the items in the previous figure.

Item	Description
Mode	Click the radio button to enable or disable the DHCP Client Option 82 mode.
Circuit ID Format	Click the drop-down menu to set the ID format: String, Hex, User Definition.
Circuit ID String	Enter the string ID of the corresponding class.
Circuit ID Hex	Enter the hex string of the corresponding class.
Circuit ID User-Define	Enter the user definition of the corresponding class.
Remote ID Format	Click the drop-down menu to set the Remote ID format: String, Hex, User Definition.
Remote ID String	Enter the remote string ID of the corresponding class.
Remote ID Hex	Enter the remote hex string of the corresponding class.
Remote ID UserDefine	Enter the remote user definition of the corresponding class.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **DHCP Client Option 82 Information** table settings are informational only: Status, Circuit ID Format, Circuit ID String, Circuit ID Hex, Circuit ID User-Define, Remote ID Format, Remote ID String, Remote ID Hex, and Remote ID User-Define.

DHCP Client Option 82 Information	
Information Name	Information Value
Status	Disabled
Circuit ID Format	String
Circuit ID String	
Circuit ID Hex	
Circuit ID User-Define	
Remote ID Format	String
Remote ID String	
Remote ID Hex	
Remote ID User-Define	

## 4.15 DHCP Auto Provision

The DHCP Auto Provision feature allows you to load configurations using a server with DHCP options. Through the remote connection, the switch obtains information from a configuration file available through the TFTP server.

To access this page, click **System > DHCP Auto Provision**.

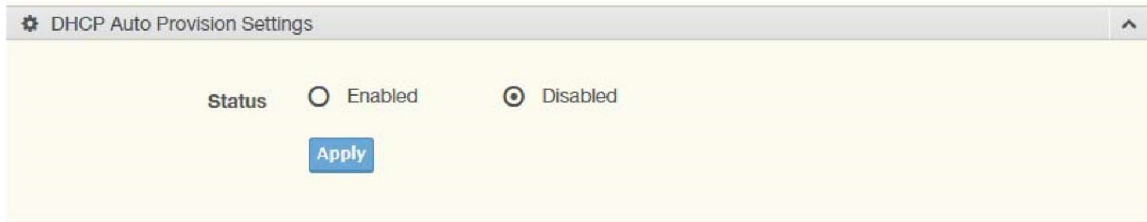


Figure 4.12 System > DHCP Auto Provision

The following table describes the items in the previous figure.

Item	Description
Status	Select the radio button to enable or disable the DHCP Auto Provisioning Setting.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **DHCP Auto Provision Information** settings are informational only: Status.

DHCP Auto Provision Information	
Information Name	Information Value
Status	Disabled

## 4.16 Management VLAN

By default, the VLAN is the management VLAN providing communication with the switch management interface.

To access this page, click **System > Management VLAN**.



Figure 4.13 System > Management VLAN

The following table describes the items in the previous figure.

Item	Description
Management VLAN	Click the drop-down menu to select a defined VLAN.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Management VLAN State** are informational only: Management VLAN.

Management VLAN State	
Config Name	Config Value
Management VLAN	1

## 4.17 System Time

To access this page, click **System > System Time**.

The screenshot shows the 'System Time Settings' page. At the top, there is a title bar with a gear icon and the text 'System Time Settings'. Below this, the 'Enable SNTP' section has two radio buttons: 'Disabled' (selected) and 'Enabled'. The 'SNTP/NTP Server Address' field contains 'input sntp server' with a placeholder '(X.X.X.X or Hostname)'. The 'SNTP Port' field contains '123' with a placeholder '(1 - 65535 | Default : 123)'. The 'Manual Time' section includes dropdowns for Year (2000), Month (Jan), Day (1), Hour (0), Minute (0), and Second (0). The 'Time Zone' dropdown is set to 'None'. The 'Daylight Saving Time' dropdown is set to 'Disable'. The 'Daylight Saving Time Offset' is a slider set to '60' with a range of '(1 - 1440) Minutes'. The 'Recurring From' section has dropdowns for Weekday (Sun), Week (1), and Month (Jan), with Hour (0) and Minute (0) below. The 'Recurring To' section has identical dropdowns. The 'Non-Recurring From' section has Year (2000), Month (Jan), Date (1), Hour (Hour), and Minute (0). The 'Non-Recurring To' section has Year (2000), Month (Jan), Date (1), Hour (0), and Minute (0). An 'Apply' button is located at the bottom left.

Figure 4.14 System > System Time

The following table describes the items in the previous figure.

Item	Description
Enable SNTP	Click the radio button to enable or disable the SNTP.
SNTP/NTP Server Address	Enter the address of the SNTP server. This is a text string of up to 64 characters containing the encoded unicast IP address or hostname of a SNTP server. Unicast SNTP requests will be sent to this address. If this address is a DNS hostname, then that hostname should be resolved into an IP address each time a SNTP request is sent to it.
SNTP Port	Enter the port on the server to which SNTP requests are to be sent. Allowed range is 1 to 65535 (default: 123).
Manual Time	Click the drop-down menus to set local date and time of the system.
Time Zone	Click the drop-down menu to select a system time zone.
Daylight Saving Time	Click the drop-down menu to enable or disable the daylight-saving time settings.
Daylight Saving Time Offset	Enter the offsetting variable in seconds to adjust for daylight saving time.
Recurring From	Click the drop-down menu to designate the start date and time for daylight saving time.
Recurring To	Click the drop-down menu to designate the end date and time for daylight saving time.
Non-Recurring From	Click the drop-down menu to designate a start date and time for a non-recurring daylight-saving time event.
Non-Recurring To	Click the drop-down menu to designate the end date and time for a non-recurring daylight-saving time event.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **System Time Information** settings are informational only: Current Date/Time, SNTP, SNTP Server Address, SNTP Server Port, Time zone, Daylight Saving Time, Daylight Saving Time Offset, From, and To.

System Time Information	
Information Name	Information Value
Current Date/Time	08:31:08 DFL(GMT+8) Jan 01 2000
SNTP	Disabled
SNTP Server Address	
SNTP Server Port	123
Time zone	GMT+8
Daylight Saving Time	Disabled
Daylight Saving Time Offset	
From	
To	



## 4.18 L2 Switching

### 4.19 Port Configuration

Port Configuration describes how to use the user interface to configure LAN ports on the switch.

To access this page, click **L2 Switching > Port Configuration**.

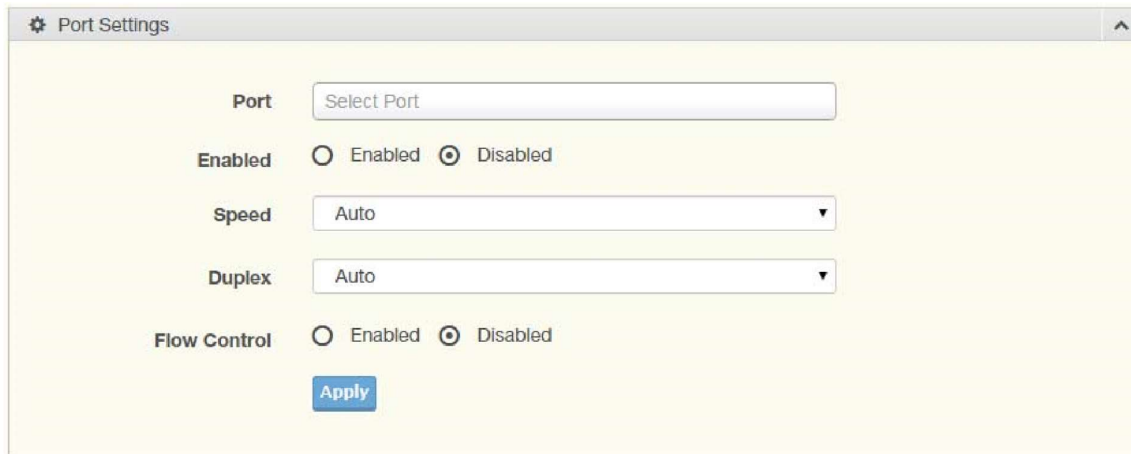


Figure 4.15 L2 Switching > Port Configuration

The following table describes the items in the previous figure.

Item	Description
Port	Click the drop-down menu to select the port for the L2 Switch setting.
Enabled	Click the radio-button to enable or disable the Port Setting function.
Speed	Click the drop-down menu to select the port speed: Auto, Auto-10M, Auto100M, Auto-1000M, Auto-10/100M, 10M, 100M, or 1000M.
Duplex	Click the drop-down menu to select the duplex setting: Half or Full.
Flow Control	Click the radio button to enable or disable the flow control function.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Port Status** settings are informational only: Port, **Edit** (click to enter description), Enable State, Link Status, Speed, Duplex, FlowCtrl Config, and FlowCtrl Status.

Port	Description	Enable State	Link Status	Speed	Duplex	FlowCtrl Config	FlowCtrl Status
GE1	<a href="#">Edit</a>	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE2	<a href="#">Edit</a>	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE3	<a href="#">Edit</a>	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE4	<a href="#">Edit</a>	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE5	<a href="#">Edit</a>	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE6	<a href="#">Edit</a>	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE7	<a href="#">Edit</a>	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE8	<a href="#">Edit</a>	Enabled	DOWN	Auto	Auto	Disabled	Disabled

## 4.20 Port Mirror

Port mirroring function allows the sending of a copy of network packets seen on one switch port to a network monitoring connection on another switch port. Port mirroring can be used to analyze and debug data, diagnose errors on a network, or to mirror either inbound or outbound traffic (or both).

There are no preset values in the Port Mirror. The displayed values do not represent the actual setting values.

To access this page, click **L2 Switching > Port Mirror**.

Figure 4.16 L2 Switching > Port Mirror

The following table describes the items in the previous figure.

Item	Description
Session ID	Click the drop-down menu to select a port mirroring session from the list. The number of sessions allowed is platform specific.
Monitor session state	Click the drop-down menu to enable or disable the session mode for a selected session ID.
Destination Port	Click the drop-down menu to select the destination port and receive all the traffic from configured mirrored port(s).
Allow-ingress	Click the drop-down menu to enable or disable the Allow-ingress function.
Sniffer RX Ports	Enter the variable to define the RX port.
Sniffer TX Ports	Enter the variable to define the TX port.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Mirror Status** settings are informational only: Session ID, Destination Port, Ingress State, Source TX Port and Source RX Port.

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

## 4.21 Link Aggregation

Link Aggregation is a method for combining multiple network connections in parallel in order to increase throughput beyond the capability of a single connection, and to provide redundancy in case one of the links should fail.

### Load Balance

The Load Balancing page allows you to select between a MAC Address or IP/MAC Address algorithm for the even distribution of IP traffic across two or more links.

To access this page, click **L2 Switching > Link Aggregation > Load Balance**.

Figure 4.17 L2 Switching > Link Aggregation > Load Balance

The following table describes the items in the previous figure.

Item	Description
Load Balance Algorithm	Select the radio button to select the Load Balance Setting: MAC Address or IP/MAC Address.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Load Balance Information** settings are informational only: Load Balance Algorithm.

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

### LAG Management

Link aggregation is also known as trunking. It is a feature available on the Ethernet gateway and is used with Layer 2 Bridging. Link aggregation allows for the logical merging of multiple ports into a single link.

To access this page, click **L2 Switching > Link Aggregation > LAG Management**.

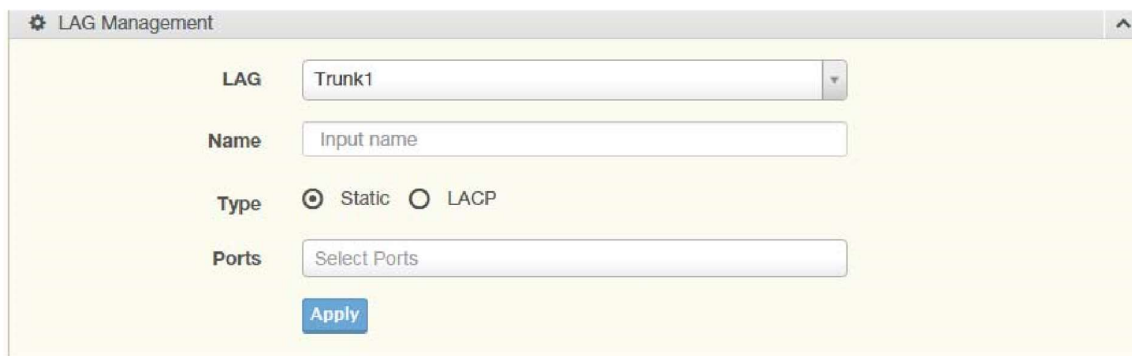


Figure 4.18 L2 Switching > Link Aggregation > LAG Management

The following table describes the items in the previous figure.

Item	Description
LAG	Click the drop-down menu to select the designated trunk group: Trunk 1 ~ 8.
Name	Enter an entry to specify the LAG name.
Type	Click the radio button to specify the type mode: Static or LACP.
Ports	Click the drop-down menu to select designated ports: GE1-28.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **LAG Management Information** settings are informational only: LAG, Name, Type, Link State, Active Member, Standby Member, **Edit** (click to modify the settings) and **Clear** (click to load default settings).

LAG	Name	Type	Link State	Active Member	Standby Member	Modify
Trunk1		---	Not Present	-	-	Edit Clear
Trunk2		---	Not Present	-	-	Edit Clear
Trunk3		---	Not Present	-	-	Edit Clear
Trunk4		---	Not Present	-	-	Edit Clear
Trunk5		---	Not Present	-	-	Edit Clear
Trunk6		---	Not Present	-	-	Edit Clear
Trunk7		---	Not Present	-	-	Edit Clear
Trunk8		---	Not Present	-	-	Edit Clear

### LAG Port Settings

The LAG Port Settings page allows you to enable or disable, set LAG status, speed and flow control functions.

In this example, we will configure a LAG between the following switches:

To access this page, click **L2 Switching > Link Aggregation > LAG Port Settings**.

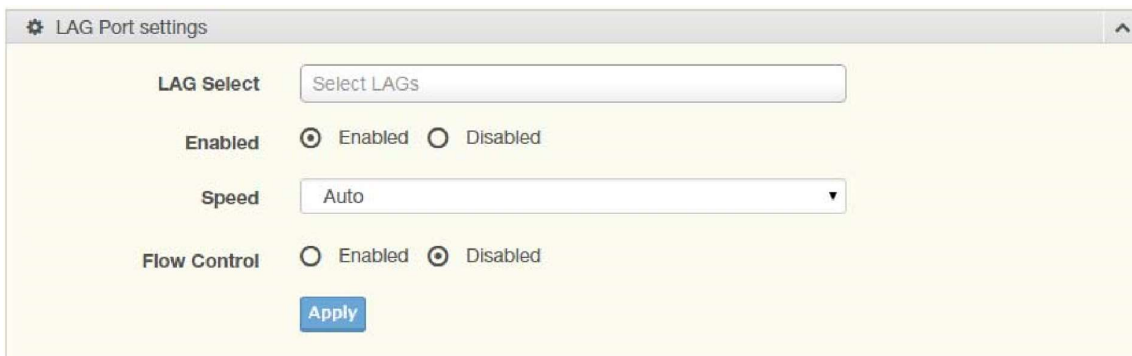


Figure 4.19 L2 Switching > Link Aggregation > LAG Port Settings

The following table describes the items in the previous figure.

Item	Description
LAG Select	Click the drop-down menu to select a predefined LAG trunk definition: LAG 1-8.
Enabled	Click the radio button to enable or disable the LAG Port.
Speed	Click the drop-down menu to select the port speed: Auto, Auto-10M, Auto100M, Auto-1000M, Auto-10/100M, 10M, 100M, or 1000M.
Flow Control	Click the radio button to enable or disable the Flow Control for the LAG Port.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **LAG Port Status** settings are informational only: LAG, Description, Port Type, Enable State, Link Status, Speed, Duplex, FlowCtrl Config, and FlowCtrl Status.

LAG	Description	Port Type	Enable State	Link Status	Speed	Duplex	FlowCtrl Config	FlowCtrl Status
Trunk1			Enabled		Auto	Auto	Disabled	Disabled
Trunk2			Enabled		Auto	Auto	Disabled	Disabled
Trunk3			Enabled		Auto	Auto	Disabled	Disabled
Trunk4			Enabled		Auto	Auto	Disabled	Disabled
Trunk5			Enabled		Auto	Auto	Disabled	Disabled
Trunk6			Enabled		Auto	Auto	Disabled	Disabled
Trunk7			Enabled		Auto	Auto	Disabled	Disabled
Trunk8			Enabled		Auto	Auto	Disabled	Disabled

### LACP Priority Settings

The LACP Priority Settings page allows you to configure the system priority for LACP.

To access this page, click **L2 Switching > Link Aggregation > LACP Priority Settings**.



Figure 4.20 L2 Switching > Link Aggregation > LACP Priority Settings

The following table describes the items in the previous figure.

Item	Description
System Priority	Enter the value (1-65535) to designate the LACP system priority.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **LACP Information** settings are informational only: System Priority.

LACP Priority Information	
Information Name	Information Value
System Priority	32768

### LACP Port Settings

Link Aggregation Control Protocol (LACP) provides a method to control the bundling of several physical ports together to form a single logical channel. By configuring the LACP function, the switch can negotiate an automatic bundling of links by sending LACP packets to the peer device (also implementing LACP).

To access this page, click **L2 Switching > Link Aggregation > LACP Port Settings**.

Figure 4.21 L2 Switching > Link Aggregation > LACP Port Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Select a port for the LACP Port Settings. The listed available settings are: GE1-GE28. However, the available settings are dependent on the connected LACP device and may not be listed as displayed in the current figure.
Priority	Enter a variable (1 to 65535) to assign a priority to the defined port selection.
Timeout	Click the radio button to select a long or short timeout period.
Mode	Click the radio button to select the setting mode: Active or Passive. <ul style="list-style-type: none"> <li>Active: Enables LACP unconditionally.</li> <li>Passive: Enables LACP only when an LACP device is detected (default state).</li> </ul>
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **LACP Port Information** settings are informational only: Port Name, Priority, Timeout, and Mode.

Port Name	Priority	Timeout	Mode
GE1	1	Long	Passive
GE2	1	Long	Passive
GE3	1	Long	Passive
GE4	1	Long	Passive
GE5	1	Long	Passive
GE6	1	Long	Passive

## 4.22 802.1Q VLAN

The 802.1Q VLAN feature allows for a single VLAN to support multiple VLANs. With the 802.1Q feature you can preserve VLAN IDs and segregate different VLAN traffic.

The 802.1Q VLAN tag feature encapsulates the 802.1Q VLAN tagging within another 802.1Q VLAN tag. The outer tag is assigned following the AP group, while the inner VLAN ID is assigned dynamically by the AAA server.

### VLAN Management

The management of VLANs is available through the VLAN Settings page. Through this page you can add or delete VLAN listings and add a prefix name to an added entry.

#### 802.1Q VLAN > VLAN Management.

Figure 4.22 L2 Switching > 802.1Q VLAN > VLAN Management

The following table describes the items in the previous figure.

Item	Description
VLAN Action	Click the radio button to add or delete the VLAN entry shown in the previous field.
VLAN List	Enter the name of the VLAN entry to setup.
VLAN Name Prefix	Enter the prefix to be used by the VLAN list entry in the previous field.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **VLAN Table** settings are informational only: VLAN ID, VLAN Name, VLAN Type, and **Edit** (click to enter VLAN name).

VLAN ID	VLAN Name	VLAN Type	Modify
1	default	Default	Edit

Showing 1 to 1 of 1 VLANs

### PVID Settings

The PVID Settings page allows you to designate a PVID for a selected port, define the accepted type, and enable/disable the ingress filtering.

To access this page, click **L2 Switching > 802.1Q VLAN > PVID Settings**.

Figure 4.23 L2 Switching > 802.1Q VLAN > PVID Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Click the drop-down menu to select a port and edit its settings: GE1-GE28, or Trunk1 - Trunk8.
PVID	Enter the VLAN ID you want assigned to untagged or priority tagged frames received on this port. The value ranges 1 to 4094. The default is 1.
Accepted Type	Click the radio button to specify which frames to forward. <b>Tag Only:</b> discards any untagged or priority tagged frames. <b>Untag Only:</b> discards any tagged frames. <b>All:</b> accepts all untagged and tagged frames. Whichever you select, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN standard. The default is All.
Ingress Filtering	Click the radio button to specify how you want the port to handle tagged frames. If you enable Ingress Filtering, a tagged frame will be discarded if this port is not a member of the VLAN identified by the VLAN ID in the tag. If you select Disabled, all tagged frames will be accepted. The default is Disabled.
Apply	Click <b>Apply</b> to save the values and update the screen.



The ensuing table for **Port VLAN Status** settings are informational only: Port, Interface VLAN Mode, PVID, Accept Frame Type, and Ingress Filtering.

Port	Interface VLAN Mode	PVID	Accept Frame Type	Ingress Filtering
GE1	Hybrid	1	ALL	Enabled
GE2	Hybrid	1	ALL	Enabled
GE3	Hybrid	1	ALL	Enabled
GE4	Hybrid	1	ALL	Enabled

### Port to VLAN

The Port to VLAN page allows you to add a port to a VLAN and select the related parameters.

#### 802.1Q VLAN > Port to VLAN.

VLAN ID :

Port	Interface VLAN Mode	Membership	PVID
GE1	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	YES
GE2	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	YES
GE3	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	YES
GE4	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	YES
GE5	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	YES
GE6	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	YES
GE7	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	YES
GE8	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	YES
GE9	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	YES
GE10	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	YES
Trunk1	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	YES
Trunk2	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	YES
Trunk3	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	YES
Trunk4	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	YES
Trunk5	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	YES
Trunk6	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	YES
Trunk7	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	YES
Trunk8	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	YES

Figure 4.24 L2 Switching > 802.1Q VLAN > Port to VLAN

The following table describes the items in the previous figure.

Item	Description
Port	Displays the assigned port to the entry.
Interface VLAN Mode	Displays the assigned mode to the listed VLAN port. Hybrid: Port hybrid model. Access: Port hybrid model. Trunk: Port hybrid model. Tunnel: Port hybrid model.
Membership	Displays the assigned membership status of the port entry. Options include Forbidden, Excluded Tagged, or Untagged.
Apply	Click <b>Apply</b> to save the values and update the screen.

### Port-VLAN Mapping

To access this page, click **L2 Switching > 802.1Q VLAN > Port-VLAN Mapping**.

The ensuing table for **Port-VLAN Mapping Table** settings are informational only: Port, Mode, Administrative VLANs and Operational VLANs.

Port	Mode	Administrative VLANs	Operational VLANs
GE1	Hybrid	1UP	1UP
GE2	Hybrid	1UP	1UP
GE3	Hybrid	1UP	1UP
GE4	Hybrid	1UP	1UP

## 4.23 Q-in-Q

Q-in-Q is commonly referred as VLAN stacking in which VLANs are nested by adding two tags to each frame instead of one. Network service provider and users both can use VLANs and make it possible to have more than the 4,094 separate VLANs allowed by 802.1Q.

There are three ways in which a machine can be connected to a network carrying double tagged 802.1ad traffic:

- via an untagged port, where both inner and outer VLANs are handled by the switch or switches (so the attached machine sees ordinary Ethernet frames);
- via a single-tagged (tunnel) port, where the outer VLAN only is handled by the switch (so the attached machine sees single-tagged 802.1Q VLAN frames); or
- via a double-tagged (trunk) port, where both inner and outer VLANs are handled by the attached machine (which sees double-tagged 802.1ad VLAN frames).

### Global Settings

The Global Settings page allows you to set the outer VLAN Ethertype setting. To access this page, click **L2 Switching > Q-in-Q > Global Settings**.



Figure 4.25 L2 Switching > Q-in-Q > Global Settings

The following table describes the items in the previous figure.

Item	Description
Outer VLAN Ethertype	Enter the outer VLAN handled by the switch giving the attached machine a single-tagged 802.1Q VLAN frame.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **QinQ Global Information** settings are informational only: Outer VLAN Ethtype.

Information Name	Information Value
Outer VLAN Ethtype	0x9100

## Port Settings

The Port Settings page allows you to define the outer PVID and outer mode for a selected port.

### Q-in-Q > Port Settings.

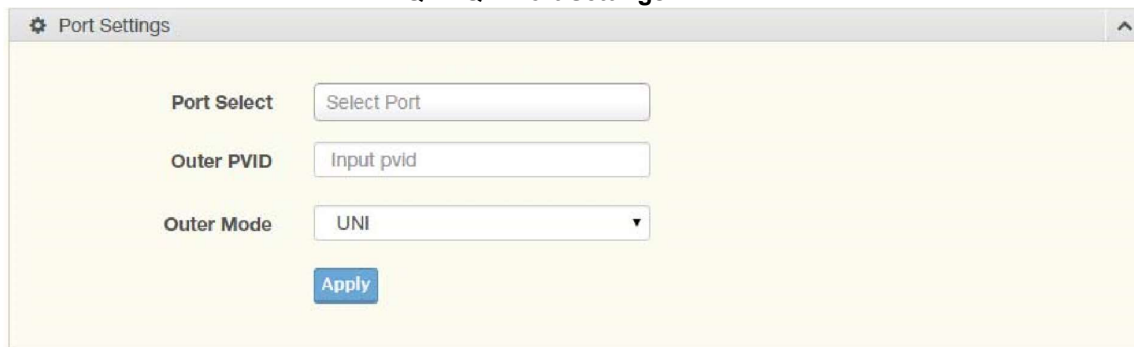


Figure 4.26 L2 Switching > Q-in-Q > Port Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Enter the switch port (part of VLAN configuration) to configure the selection as a tunnel port.
Outer PVID	Enter the Port VLAN ID (PVID) to assign the native VLAN ID. All untagged traffic coming in or out of the 802.1Q port is forwarded based on the PVID value

Outer Mode	<p>Click the drop-down menu to select between UNI or NNI role.</p> <ul style="list-style-type: none"> <li>UNI: Selects a user-network interface which specifies communication between the specified user and a specified network.</li> <li>NNI: Selects a network-to-network interface which specifies communication between two specified networks.</li> </ul>
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **QinQ Port Information** settings are informational only: Port, Outer PVID, and Outer Mode.

Port	Outer PVID	Outer Mode
GE1	1	UNI
GE2	1	UNI
GE3	1	UNI
GE4	1	UNI
GE5	1	NNI

## 4.24 GARP

The Generic Attribute Registration Protocol (GARP) is a local area network (LAN) protocol. The protocol defines procedures for the registration and de-registration of attributes (network identifiers or addresses) by end stations and switches with each other.

### GARP Settings

To access this page, click **L2 Switching > GARP > GARP Settings**.

**GARP Settings**

**Join Time**  Sec. (6-600)

**Leave Time**  Sec. (12-3000)

**Leave All Time**  Sec. (12-12000)

**Note** Join Time \* 2 < Leave Time < Leave All Time

**Apply**

Figure 4.27 L2 Switching > GARP > GARP Settings

The following table describes the items in the previous figure.

Item	Description
Join Time	Enter a value to specify the time between the transmission of GARP PDUs registering (or re-registering) membership for a VLAN or multicast group in centiseconds. Enter a number between 6 and 600. An instance of this timer exists for each GARP participant for each port.
Leave Time	Enter a value to specify the time to wait after receiving an unregister request for a VLAN or multicast group before deleting the associated entry in centiseconds. This allows time for another station to assert registration for the same attribute in order to maintain uninterrupted service. Enter a number between 12 and 3,000. An instance of this timer exists for each GARP participant for each port.
Leave All Time	Enter a value to specify the Leave All Time controls how frequently Leave All PDUs are generated. A Leave All PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. The Leave All Period Timer is set to a random value in the range of Leave All Time to 1.5*Leave All Time. The timer is specified in centiseconds. Enter a number between 12 and 12,000. An instance of this timer exists for each GARP participant for each port.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **GARP Information** settings are informational only: Join Time, Leave Time and Leave All Time.

GARP Information	
Information Name	Information Value
Join Time	10
Leave Time	30
Leave All Time	240

## GVRP Settings

The GVRP Settings page allows you to enable or disable the GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) Protocol which facilitates control of virtual local area networks (VLANs) within a larger network.

To access this page, click **L2 Switching > GARP > GVRP Settings**.



Figure 4.28 L2 Switching > GARP > GVRP Settings

The following table describes the items in the previous figure.

Item	Description
Status	Click to enable or disable the GARP VLAN Registration Protocol administrative mode for the switch. The factory default is Disable.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **GVRP Information** settings are informational only: GVRP.

## 4.25 802.3az EEE

The 802.3az Energy Efficient Ethernet (EEE) innovative green feature reduces energy consumption through intelligent functionality:

- Traffic detection — Energy Efficient Ethernet (EEE) compliance
- Inactive link detection — Inactive link detection function automatically reduces power usage when inactive links or devices are detected.

To access this page, click **L2 Switching > 802.3az EEE**.



Figure 4.29 L2 Switching > 802.3az EEE

The following table describes the items in the previous figure.

Item	Description
Port Select	Enter the port to setup the EEE function.
State	Click <b>Enabled</b> or <b>Disabled</b> to set the state mode of the port select setting.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **EEE Enable Status** settings are informational only: Port and EEE State.

EEE Port Status	
Port	EEE State
GE1	Disabled
GE2	Disabled
GE3	Disabled

## 4.26 Multicast

Multicast forwarding allows a single packet to be forwarded to multiple destinations. The service is based on an L2 switch receiving a single packet addressed to a specific Multicast address. Multicast forwarding creates copies of the packet and transmits the packets to the relevant ports.

### Multicast Filtering

The Multicast Filtering page allows for the definition of action settings when an unknown multicast request is received. The options include: Drop, Flood, or Router Port.

To access this page, click **L2 Switching > Multicast > Multicast Filtering**.

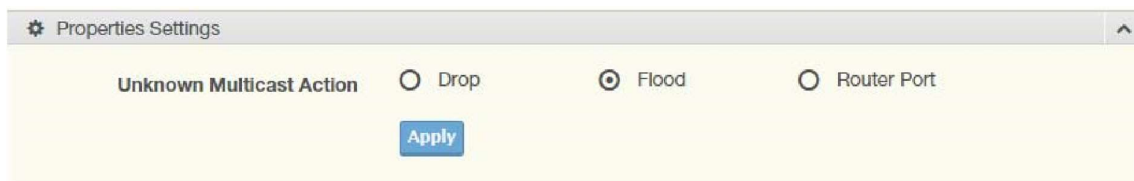


Figure 4.30 L2 Switching > Multicast > Multicast Filtering

The following table describes the items in the previous figure.

Item	Description
Unknown Multicast Action	Select the configuration protocol: Drop, Flood, or Router Port, to apply for any unknown multicast event.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Properties Information** settings are informational only: Unknown Multicast Action.

Properties Information	
Information Name	Information Value
Unknown Multicast Action	Flood

### IGMP Snooping

IGMP Snooping is defined as the process of listening to Internet Group Management Protocol (IGMP) network traffic. IGMP Snooping allows a network switch to listen in on the IGMP conversation between hosts and routers, and maintain a map of which links need which IP multicast streams. Multicasts can be filtered from the links, which do not need them in turn controlling which ports receive specific multicast traffic.

### IGMP Settings

To access this page, click **L2 Switching > Multicast > IGMP Snooping > IGMP Settings**.



Figure 4.31 L2 Switching > Multicast > IGMP Snooping > IGMP Settings

The following table describes the items in the previous figure.

Item	Description
IGMP Snooping State	Select <b>Enable</b> or <b>Disable</b> to designate the IGMP Snooping State.
IGMP Snooping Version	Select designated IGMP Snooping Version: V2 or V3.
IGMP Snooping Report Suppression	Select <b>Enable</b> or <b>Disable</b> to setup the report suppression for IGMP Snooping.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **IGMP Snooping Information** settings are informational only: IGMP Snooping State, IGMP Snooping Version, and IGMP Snooping V2 Report Suppression.

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

The ensuing table for **IGMP Snooping Table** settings are informational only: Entry No., VLAN ID, IGMP Snooping Operation State, Router Ports Auto Learn, Query Robustness, Query Interval (sec.), Query Max Response Interval (sec.), Last Member Query count, Last Member Query Interval (sec), Immediate Leave, and **Edit** (click to modify the settings).

Entry No.	VLAN ID	IGMP Snooping Operation State	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 Querier

IGMP Querier allows snooping to function by creating the tables for snooping. General queries must be unconditionally forwarded by all switches involved in IGMP snooping.

To access this page, click **L2 Switching > Multicast > IGMP Snooping > IGMP Querier**.



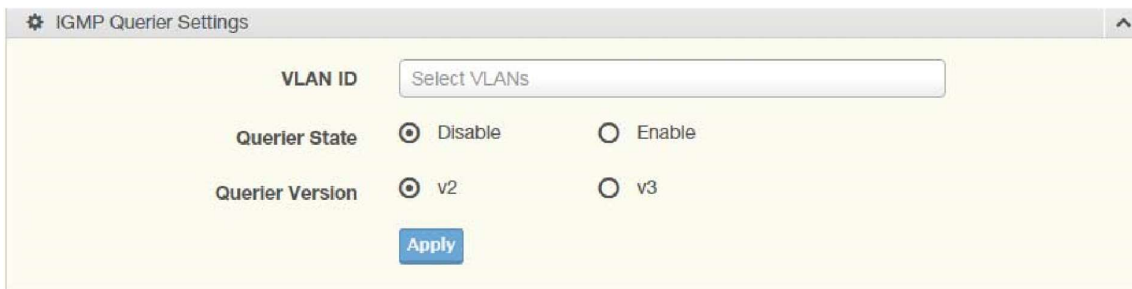


Figure 4.32 L2 Switching > Multicast > IGMP Snooping > IGMP Querier

The following table describes the items in the previous figure.

Item	Description
VLAN ID	Select the VLAN ID to define the local IGMP querier.
Querier State	Select <b>Disable</b> or <b>Enable</b> to configure the VLAN ID (IGMP Querier).
Querier Version	Select the querier version (V2 or V3) designated to the selected VLAN ID.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **IGMP Querier Status** settings are informational only: VLAN ID, Querier State, Querier Status, Querier Version, and Querier IP.

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

### IGMP Static Groups

To access this page, click **L2 Switching > Multicast > IGMP Snooping > IGMP Static Groups**.



Figure 4.33 L2 Switching > Multicast > IGMP Snooping > IGMP Static Groups

The following table describes the items in the previous figure.

Item	Description
VLAN ID	Select the VLAN ID to define IGMP static group.
Group IP Address	Enter the IP address assigned to the VLAN ID.
Member Ports	Enter the port numbers to associate with the static group.
Add	Click <b>Add</b> to add an IGMP group.

The ensuing table for **IGMP Static Groups Status** settings are informational only: VLAN ID, Group IP Address, Member Ports, and Modify.

IGMP Static Groups Status			
VLAN ID	Group IP Address	Member Ports	Modify

### Multicast Groups

To access this page, click **L2 Switching > Multicast > IGMP Snooping > Multicast Groups**.

The ensuing table for **Multicast Groups** settings are informational only: VLAN ID, Group IP Address, Member Ports, Type, and Life (Sec).

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

### Router Ports

To access this page, click **L2 Switching > Multicast > IGMP Snooping > Router Ports**.

The ensuing table for **Router Ports** settings are informational only: VLAN ID, Port, and Expiry Time (Sec).

Router Ports		
VLAN ID	Port	Expiry Time (Sec)

### MLD Snooping

The MLD Snooping page allows you to select the snooping status (enable or disable), the version (V1 or V2), and the enabling/disabling of the report suppression for the MLD querier, which sends out periodic general MLD queries and are forwarded through all ports in the VLAN.

### MLD Settings

To access this page, click **L2 Switching > Multicast > MLD Snooping > MLD Settings**.

**MLD Snooping Settings**

MLD Snooping State     Enable     Disable

MLD Snooping Version     v1     v2

MLD Snooping Report Suppression     Enable     Disable

Figure 4.34 L2 Switching > Multicast > MLD Snooping > MLD Settings

The following table describes the items in the previous figure.

Item	Description
MLD Snooping State	Select <b>Enable</b> or <b>Disable</b> to setup the MLD Snooping State.
MLD Snooping Version	Select the querier version (V1 or V2) designated to the MLD Snooping
MLD Snooping Report Suppression	Select <b>Enable</b> or <b>Disable</b> to designate the status of the report suppression
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **MLD Snooping Information** settings are informational only: MLD Snooping State, MLD Snooping Version, and MLD Snooping V2 Report Suppression.

Information Name	Information Value
MLD Snooping State	Disable
MLD Snooping Version	v1
MLD Snooping V2 Report Suppression	Enable

The ensuing table for **MLD Snooping Table** settings are informational only: Entry No., VLAN ID, MLD Snooping Operation State, Router Ports Auto Learn, Query Robustness, Query Interval (sec.), Query Max Response Interval (sec.), Last Member Query Count, Last Member Query Interval (sec), Immediate Leave, and **Edit** (click to modify the settings).

Entry No.	VLAN ID	MLD Snooping Operation State	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

### MLD Querier

The MLD Querier page allows you to select and enable/disable the MLD querier and define the version (IGMPv1 or IGMPv2) when enabled.

To access this page, click **L2 Switching > Multicast > MLD Snooping > MLD Querier**.

Figure 4.35 L2 Switching > Multicast > MLD Snooping > MLD Querier

The following table describes the items in the previous figure.

Item	Description
VLAN ID	Enter the VLAN ID to configure.
Querier State	Select <b>Enable</b> or <b>Disable</b> status on the selected VLAN. Enable: Enable IGMP Querier Election. Disable: Disable IGMP Querier Election.
Querier Version	Select the querier version (IGMPV1 or IGMPV2) designated to the MLD Querier function.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **MLD Querier Status** settings are informational only: VLAN ID, Querier State, Querier Status, Querier Version, and Querier IP.

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

### MLD Static Group

The MLD Static Group page allows you to configure specified ports as static member ports.

To access this page, click **L2 Switching > Multicast > MLD Snooping > MLD Static Group**.

Figure 4.36 L2 Switching > Multicast > MLD Snooping > MLD Static Group

The following table describes the items in the previous figure.

Item	Description
VLAN ID	Enter the VLAN ID to define the local MLD Static Group.
Group IP Address	Enter the IP address associated with the static group.
Member Ports	Enter the ports designated with the static group.
Add	Click <b>Add</b> to add a MLD static group.

The ensuing table for **MLD Static Groups Status** settings are informational only: VLAN ID, Group IP Address, Member Ports, and Modify.

MLD Static Groups Status			
VLAN ID	Group IP Address	Member Ports	Modify

### Multicast Groups

To access this page, click **L2 Switching > Multicast > MLD Snooping > Multicast Groups**. The ensuing table for **Multicast Groups** settings are informational only: ID, Group IP Address, Member Ports, Type, and Life (Sec).

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

### Router Ports

To access this page, click **L2 Switching > Multicast > MLD Snooping > Router Ports**. The ensuing table for **Router Ports** settings are informational only: VLAN ID, Port, and Expiry Time (Sec).

Router Ports		
VLAN ID	Port	Expiry Time (Sec)

## 4.27 Jumbo Frame

Jumbo frames are frames larger than the standard Ethernet frame size of 1518 bytes. The Jumbo Frame function allows the configuration of Ethernet frame size. To access this page, click **L2 Switching > Jumbo Frame**.

Figure 4.37 L2 Switching > Jumbo Frame

The following table describes the items in the previous figure.

Item	Description
Jumbo Frame (Bytes)	Enter the variable in bytes (1518 to 9216) to define the jumbo frame size.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Jumbo Frame Config** settings are informational only: Jumbo Frame (Bytes).

Jumbo Frame Config	
Information Name	Information Value
Jumbo Frame (Bytes)	1522

## 4.28 Spanning Tree

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

### STP Global Settings

The STP Global Settings page allows you to set the STP status, select the configuration for a BPDU packet, choose the path overhead, force version, and set the configuration revision range.

To access this page, click **L2 Switching > Spanning Tree > STP Global Settings**.

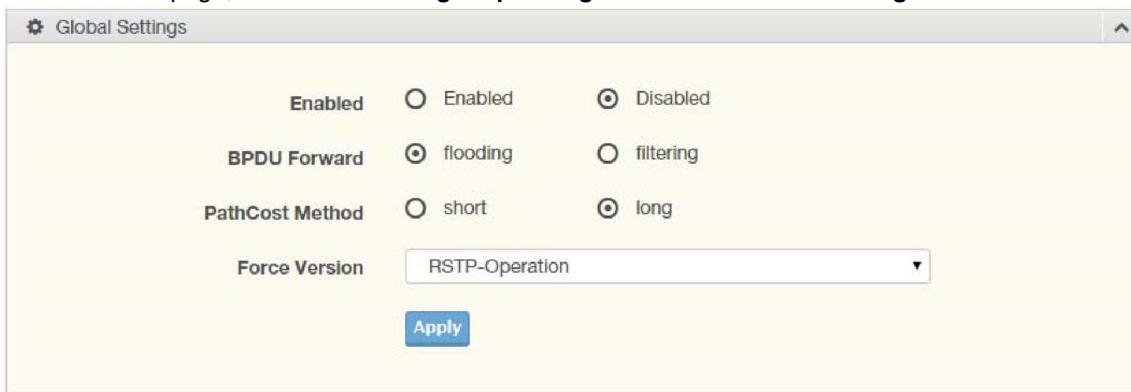


Figure 4.38 L2 Switching > Spanning Tree > STP Global Settings

The following table describes the items in the previous figure.

Item	Description
Enabled	Click the radio-button to enable or disable the STP status.
BPDU Forward	Select <b>flooding</b> or <b>filtering</b> to designate the type of BPDU packet.
PathCost Method	Select short or long to define the method used for path cost calculations.
Force Version	Click the drop-down menu to select the operating mode for STP. <ul style="list-style-type: none"> <li>● STP-Compatible: 802.1D STP operation.</li> <li>● RSTP-Operation: 802.1w operation.</li> <li>● MSTP-Operation: 802.1s operation.</li> </ul>
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **STP Information** settings are informational only: STP, BPDU Forward, PathCost Method, and Force Version.

STP Information	
Information Name	Information Value
STP	Disabled
BPDU Forward	flooding
PathCost Method	long
Force Version	RSTP-Operation

## STP Port Settings

The STP Port Settings page allows you to configure the ports for the setting, port's contribution, configured edge port, and set the status of the BPDU filter.

To access this page, click **L2 Switching > Spanning Tree > STP Port Settings**.

Figure 4.39 L2 Switching > Spanning Tree > STP Port Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Select the port list to specify the ports that apply to this setting.
Admin Enable	Select <b>Enabled</b> or <b>Disabled</b> to setup the admin profile for the STP port.
Path Cost (0 = Auto)	Set the port's cost contribution. For a root port, the root path cost for the bridge. (0 means Auto).
Edge Port	Click the drop-down menu to set the edge port configuration. <ul style="list-style-type: none"> <li>• No: Force to false state (as link to a bridge).</li> <li>• Yes: Force to true state (as link to a host).</li> </ul>
P2P MAC	Click the drop-down menu to set the Point-to-Point port configuration. <ul style="list-style-type: none"> <li>• No: Force to false state</li> <li>• Yes: Force to true state</li> </ul>
Migrate	Click the check box to enable the migrate function. Forces the port to use the new MST/RST BPDUs, requiring the switch to test on the LAN segment for the presence of legacy devices, which are not able to understand the new BPDU formats.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **STP Port Status** settings are informational only: Port, Admin Enable, Path Cost, Edge Port, and P2P MAC.

Port	Admin Enable	Path Cost	Edge Port	P2P MAC
GE1	Enable	0	No	No
GE2	Enable	0	No	No
GE3	Enable	0	No	No
GE4	Enable	0	No	No

## STP Bridge Settings

The STP Bridge Settings page allows you to configure the priority, forward delay, maximum age, Tx hold count, and the hello time for the bridge.

To access this page, click **L2 Switching > Spanning Tree > STP Bridge Settings**.

Figure 4.40 L2 Switching > Spanning Tree > STP Bridge Settings

The following table describes the items in the previous figure.

Item	Description
Priority	Click the drop-down menu to select the STP bridge priority.
Forward Delay	Enter the variable (4 to 30) to set the forward delay for STP bridge settings.
Max Age	Enter the variable (6 to 40) to set the Max Age for STP bridge settings.
Tx Hold Count	Enter the variable (1 to 10) to designate the TX hold count for STP bridge settings.
Hello Time	Enter the variable (1 to 10) to designate the Hello Time for STP bridge settings.
Apply	Click <b>Apply</b> to save the values and update the screen.



The ensuing table for **STP Bridge Information** settings are informational only: Priority, Forward Delay, Max Age, Tx Hold Count, and Hello Time.

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

The ensuing table for **STP Bridge Status** settings are informational only: Bridge Identifier, Designated Root Bridge, Root Path Cost, Designated Bridge, Root Port, and Last Topology Change.

STP Bridge Status	
Information Name	Information Value
Bridge Identifier	32768/ 0/00:E0:4C:00:00:00
Designated Root Bridge	0/ 0/00:00:00:00:00:00
Root Path Cost	0
Designated Bridge	0/ 0/00:00:00:00:00:00
Root Port	0 / 0
Last Topology Change	0

### STP Port Advanced Settings

The STP Port Advanced Settings page allows you to select the port list to apply this setting.

To access this page, click **L2 Switching > Spanning Tree > STP Port Advanced Settings**.

The screenshot shows a configuration window titled "STP Port Advanced Settings". Inside the window, there are two main settings: "Port Select" with a text input field containing "Select Ports" and a button to the right, and "Priority" with a dropdown menu currently showing "128". Below these settings is a blue "Apply" button.

Figure 4.41 L2 Switching > Spanning Tree > STP Port Advanced Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Select the port to designate the STP settings.
Priority	Click the drop-down menu to designate a priority.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **STP Port Status** settings are informational only: Port, Identifier (Priority / Port Id), Path Cost Conf/Oper, Designated Root Bridge, Root Path Cost, Designated Bridge, Edge Port Conf/Oper, P2P MAC Conf/Oper, Port Role, and Port State.

Port	Identifier (Priority / Port Id)	Path Cost Conf/Oper	Designated Root Bridge	Root Path Cost	Designated Bridge	Edge Port Conf/Oper	P2P MAC Conf/Oper	Port Role	Port State
GE1	128 / 1	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	No / No	Disabled	Disabled
GE2	128 / 2	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	No / No	Disabled	Disabled
GE3	128 / 3	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	No / No	Disabled	Disabled

### MST Config Identification

The MST Config Identification page allows you to configure the identification setting name and the identification range.

To access this page, click **L2 Switching > Spanning Tree > MST Config Identification**.

Figure 4.42 L2 Switching > Spanning Tree > MST Config Identification

The following table describes the items in the previous figure.

Item	Description
Configuration Name	Enter the identifier used to identify the configuration currently being used. It may be up to 32 characters.
Revision Level	Enter the identifier for the Revision Configuration, range: 0 to 65535 (default: 0).
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **MST Configuration Identification Information** settings are informational only: Configuration Name and Revision Level.

Information Name	Information Value
Configuration Name	
Revision Level	0

### MST Instance ID Settings

The MST Instance ID Settings page allows you to edit the MSTI ID and VID List settings. To access this page, click **L2 Switching > Spanning Tree > MST Instance ID Settings**.



Figure 4.43 L2 Switching > Spanning Tree > MST Instance ID Settings

The following table describes the items in the previous figure.

Item	Description
MSTI ID	Enter the MST instance ID (0-15).
VID List	Enter the pre-configured VID list.
Move	Click <b>Move</b> to save the values and update the screen.

The ensuing table for **MST Instance ID Information** settings are informational only: MSTI ID and VID List.

MST Instance ID Information	
MSTI ID	VID List
0	1-4094

### MST Instance Priority Settings

The MST Instance Priority Settings allows you to specify the MST instance and the bridge priority in that instance.

To access this page, click **L2 Switching > Spanning Tree > MST Instance Priority Settings**.



Figure 4.44 L2 Switching > Spanning Tree > MST Instance Priority Settings

The following table describes the items in the previous figure.

Item	Description
MSTI ID	Click the drop-down menu to specify the MST instance.
Priority	Click the drop-down menu to set the bridge priority in the specified MST instance
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **MST Instance Priority Information** settings are informational only: MSTI ID, Priority, and Action.

MST Instance Priority Information		
MSTI ID	Priority	Action

### MST Instance Info

To access this page, click **L2 Switching > Spanning Tree > MST Instance Info**.

The ensuing table for **STP Bridge Status** settings are informational only: Bridge Identifier, Designated Root Bridge, Root Path Cost, Designated Bridge, Root Port, and TCNLast Topology Change.

STP Bridge Status	
Information Name	Information Value
Bridge Identifier	32768/ 0/00:E0:4C:00:00:00
Designated Root Bridge	0/ 0/00:00:00:00:00:00
Root Path Cost	0
Designated Bridge	0/ 0/00:00:00:00:00:00
Root Port	0 / 0
Last Topology Change	0

The ensuing table for **STP Port Status** settings are informational only: Port, Identifier (Priority / Port Id), Path Cost Conf/Oper, Designated Root Bridge, Root Path Cost, Designated Bridge, Edge Port Conf/Oper, P2P MAC Conf/Oper, Port Role, and Port State.

STP Port Status									
Port	Identifier (Priority / Port Id)	Path Cost Conf/Oper	Designated Root Bridge	Root Path Cost	Designated Bridge	Edge Port Conf/Oper	P2P MAC Conf/Oper	Port Role	Port State
GE1	128 / 1	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	No / No	Disabled	Disabled
GE2	128 / 2	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	No / No	Disabled	Disabled
GE3	128 / 3	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	No / No	Disabled	Disabled

### STP Statistics

To access this page, click **L2 Switching > Spanning Tree > STP Statistics**.

The ensuing table for **STP Statistics** settings are informational only: Port, Configuration BPDUs Received, TCN BPDUs Received, Configuration BPDUs Transmitted, and TCN BPDUs Transmitted.

STP Statistics				
Port	Configuration BPDUs Received	TCN BPDUs Received	Configuration BPDUs Transmitted	TCN BPDUs Transmitted
GE1	0	0	0	0
GE2	0	0	0	0
GE3	0	0	0	0

## 4.28.1 ERPS

The ERPS (Ethernet Ring Protection Switching) is an open standard protocol defined in ITU-T G.8032. ERPS provides protection for Ethernet traffic in a ring topology, while preventing loops within the ring. Loops are prevented by blocking traffic on either a user-configured link (RPL) or a failed link.

### ERPS Settings

The ERPS Settings allow you to Enable or Disable the state of the ERPS settings. To access this page, click **L2 Switching > ERPS > ERPS Settings**.



Figure 4.44.1 L2 Switching > ERPS > ERPS Settings

The following table describes the items in the previous figure.

Item	Description
State	Select <b>Enabled</b> or <b>Disabled</b> to setup the ERPS mode.
Apply	Click <b>Apply</b> to save the values and update the screen.

Information	
Information Name	Information Value
ERPS State	Disabled

The ensuing table for **Information** settings are informational only: ERPS State.

### ERPS Groups

The ERPS Groups page allows you to select the function and role for each device and the connected ports. You can select the RPL (Ring Protection Link), MEL (Maintenance Entity Level), and Inclusion VLAN. To access this page, click **L2 Switching > ERPS > ERPS Groups**.



Figure 4.44.2 L2 Switching > ERPS > ERPS Groups

The following table describes the items in the previous figure.

Item	Description
Ring ID	Enter a number within the range of 1 to 255 to identify a given ERPS group.
Role	Click the drop-down menu to select the ring role.
East Link	Click the drop-down menu to define the port designation.
RPL	Check RPL box to set the East Link as the RPL.
West Link	Click the drop-down menu to define the port designation.
RPL	Check RPL box to set the West Link as the RPL.
MEL	Click the drop-down menu to select the MEL (0 to 7).
Inclusion VLAN	Click the drop-down menu to select the inclusion VLAN.

The ensuing table for **Information** settings are informational only: Ring ID, Role, State, East Link, West Link, MEL, VLAN, and **Delete** (click to delete the desired Ring ID).

Information							
Ring ID	Role	State	East Link	West Link	MEL	VLAN	Delete

## 4.29 X-Ring

The X-Ring function provides an improvement over Spanning Tree and Rapid Spanning Tree and a rapid auto recovery in the event that the network suffers a corrupt or broken link and prevents network loops.

### X-Ring Settings

The X-Ring Settings allows you to enable or disable the state of the X-Ring settings. To access this page, click **L2 Switching > X-Ring > X-Ring Settings**.



Figure 4.45 L2 Switching > X-Ring > X-Ring Settings

The following table describes the items in the previous figure.

Item	Description
State	Select <b>Enabled</b> or <b>Disabled</b> to setup the X-Ring mode.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Information** settings are informational only: X-Ring State.

Information	
Information Name	Information Value
X-Ring State	Enabled

### X-Ring Groups

The X-Ring Groups page allows you to select the function and role for each device and the connected ports.

To access this page, click **L2 Switching > X-Ring > X-Ring Groups**.

Ring ID	Role	Port 1	Port 2	
1-255	Basic	GE1	GE1	Add

Figure 4.46 L2 Switching > X-Ring > X-Ring Groups

The following table describes the items in the previous figure.

Item	Description
Ring ID	Enter a number within the range of 1 to 255 to identify a given X-Ring group.
Role	Click the drop-down menu to select the ring role.
Port 1	Click the drop-down menu to define the port designation.
Port 2	Click the drop-down menu to define the port designation.
Add	Click <b>Add</b> to save the values and update the screen.

The ensuing table for **Information** settings are informational only: Ring ID, Role, Port 1, Port 2, and **Delete** (click to delete the desired Ring ID).

Information				
Ring ID	Role	Port 1	Port 2	Delete

## 4.31 Loopback Detection

The Loopback Detection function is used to detect looped links. By sending detection frames and then checking to see if the frames returned to any port on the device, the function is used to detect loops.

### Global Settings

The Global Settings page allows you to configure the state (enabled or disabled) of the function, select the interval at which frames are transmitted and the delay before recovery. To access this page, click **L2 Switching > Loopback Detection > Global Settings**.



Figure 4.50 L2 Switching > Loopback Detection > Global Settings



The following table describes the items in the previous figure.

Item	Description
State	Select <b>Enabled</b> or <b>Disabled</b> to setup the loopback mode.
Interval	Enter the variable in seconds (1 to 32767) to set the interval at which frames are transmitted.
Recover Time	Enter the variable in seconds (60 to 1000000) to define the delay before recovery.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Loopback Detection Global Information** settings are informational only: State, Interval, and Recover Time.

Loopback Detection Global Information	
Information Name	Information Value
State	Disabled
Interval	1
Recover Time	60

### Port Settings

The Port Settings page allows you to select ports that are detected by the loopback detection function and configure their status (enabled or disabled).

To access this page, click **L2 Switching > Loopback Detection > Port Settings**.



Figure 4.51 L2 Switching > Loopback Detection > Port Settings

The following table describes the items in the previous figure.

**Table 4-1.** L2 Switching > Loopback Detection > Port Settings

Item	Description
Port Select	Enter the port to define the local loopback detection setting.
Enabled	Select <b>Enabled</b> or <b>Disabled</b> to setup the Loopback Detection function.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Loopback Detection Port Information** settings are informational only: Port, Enable State, and Loop Status.

Loopback Detection Port Information		
Port	State	Loop Status
GE1	Disabled	Normal
GE2	Disabled	Normal
GE3	Disabled	Normal
GE4	Disabled	Normal

### 4.31.1 L3 Switching

### 4.31.2 SNAT

The SNAT (Source NAT) function is a many-to-one static translation. SNAT translates an entire private network to a single public destination address.

#### Global Settings

To access this page, click **L3 Switching > SNAT > Global Settings**.

Figure 4.51.1 SNAT > Global Settings

The following table describes the items in the previous figure.

Item	Description
Interface	Click the drop-down menu to select the interface.
Auto Mode	Auto Mode builds the return path for packets sent from a translated source. Specifically, SNAT without Auto Mode only guarantees that packets can reach out with a translated IP but does not imply that replies can be sent back correspondingly. Select <b>Enabled</b> or <b>Disabled</b> to setup the auto mode.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **SNAT Global settings** are informational only: VLAN and Auto Mode.

Global Information	
Information Name	Information Value
VLAN	1
Auto Mode	Disabled

### Entry Settings

The Entry Settings allow you to enter a source (private) network to be translated to a single source (public) destination IP address.

To access this page, click **L3 Switching > SNAT > Entry Settings**.

Figure 4.51.2 SNAT > Entry Settings

The following table describes the items in the previous figure.

Item	Description
Interface	Click the drop-down menu to select the Vlan interface.
Original Source IP Address	Input the original source IP address.
Original Source IP Mask	Input the original source IP netmask.
New Source IP Address	Input a new source IP address.
Add	Click <b>Add</b> to save the values and update the screen.

The ensuing table for **SNAT Entry settings** are information only: Original Source IP Address, Original Source IP Mask, New Source IP Address, Action.

Original Source IP Address	Original Source IP Mask	New Source IP address	Action
----------------------------	-------------------------	-----------------------	--------

### 4.31.3 DNAT

DNAT (Destination NAT) is a one-to-one static translation that is done on incoming packets.

DNAT translates a public destination address to a private address. To access this page, click **L3**

**Switching > DNAT.**

Figure 4.51.3 DNAT > Entry Settings

The following table describes the items in the previous figure.

Item	Description
Interface	Click the drop-down menu to select the interface.
Original Destination IP Address	Input the original destination IP address.
New Destination IP Address	Input the new destination IP address.
Apply	Click <b>Add</b> to save the values and update the screen.

The ensuing table for **DNAT Entry Settings** are informational only: Original Destination IP Address, New Destination IP Address, Action.

Original Destination IP Address	New Destination IP address	Action
---------------------------------	----------------------------	--------

### 4.31.4 Routing

The Routing function allows you to statically route an entire network to a relative gateway.  
 To access this page, click **L3 Switching > Routing**.

Figure 4.51.4 Routing > Routing Settings

The following table describes the items in the previous figure.

Item	Description
Interface	Click the drop-down menu to select the interface.
Destination IP Address	Input the destination IP address.
Destination IP Mask	Input the destination netmask.
Gateway	Input the Gateway IP address.
Add	Click <b>Add</b> to save the values and update the screen.

The ensuing table for **Routing Information** are informational only: Destination IP Address, Destination IP Mask, Gateway IP Address, Action.

Destination IP Address	Destination IP Mask	Gateway IP address	Action
------------------------	---------------------	--------------------	--------

## 4.32 MAC Address Table

The MAC Address Table provides access to the Static MAC Settings, MAC Aging Time, and Dynamic Forwarding.

## 4.33 Static MAC

The Static MAC page allows you to configure the address for forwarding of packets, the VLAN ID of the listed MAC address and the designated Port.

To access this page, click **MAC Address Table -> Static Mac**



The screenshot shows a web interface window titled "Static MAC Settings". It contains three configuration fields: "MAC Address" with the value "00:00:00:00:00:00", "VLAN" with a dropdown menu set to "default", and "Port" with a dropdown menu set to "GE1". Below these fields is a blue "Apply" button.

Figure 4.52 MAC Address Table > Static MAC

The following table describes the items in the previous figure.

**Table 4-2.** MAC Address Table > Static MAC

Item	Description
MAC Address	Enter the MAC address to which packets are statically forwarded.
VLAN	Click the drop-down menu to select the VLAN ID number of the VLAN for which the MAC address is residing.
Port	Click the drop-down menu to select the port number.
Apply	Click Apply to save the values and update the screen.

The ensuing table for Static MAC Status settings are informational only: No., MAC Address, VLAN, Port, and **Delete** (click to delete the desired MAC address).

Static MAC Status				
No.	MAC Address	VLAN	Port	Delete
1	00:E0:4C:00:00:00	default(1)	CPU	

## 4.34 MAC Aging Time

The MAC Aging Time page allows you to set the MAC address of the aging time to study. To access this page, click **MAC Address Table > MAC Aging Time**.

The screenshot shows a web interface titled "Dynamic Address Settings". It features a text input field for "Aging Time" containing the value "300". To the right of the input field, the text "(Range: 10 - 630)" is displayed. Below the input field is a blue "Apply" button.

*Figure 4.53* MAC Address Table > MAC Aging Time

The following table describes the items in the previous figure.

Item	Description
Aging Time	Enter the variable (10 to 630) to define the time required for aging.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Dynamic Address Status** settings are informational only: Aging time.

Dynamic Address Status	
Information Name	Information Value
Aging Time	300

## 4.35 Dynamic Forwarding Table

The Dynamic Forwarding function allows you to configure an address table, which contain the following:

- The port each hardware address is associated with
- The VLAN to show or clear dynamic MAC entries
- The MAC address selection

To access this page, click **MAC Address Table > Dynamic Forwarding Table**.

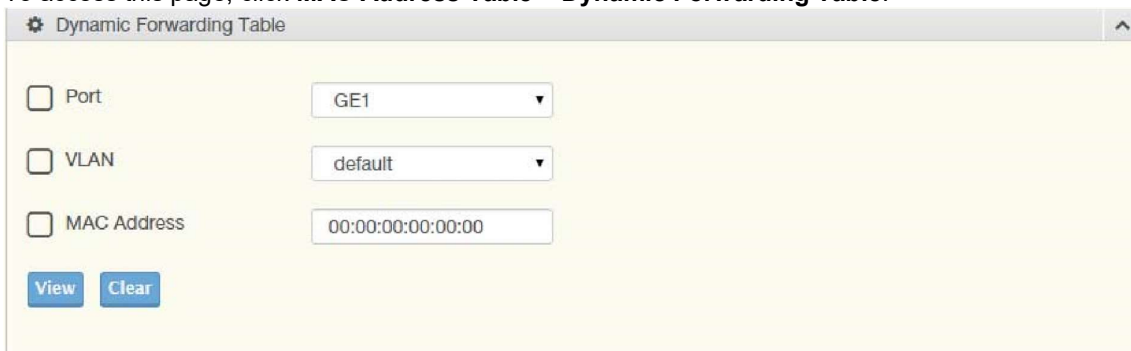


Figure 4.54 MAC Address Table > Dynamic Forwarding Table

The following table describes the items in the previous figure.

Item	Description
Port	Click the drop-down menu to select the port number to show or clear dynamic MAC entries. If a port, VLAN or MAC address is not selected, the whole dynamic MAC table is displayed or cleared.
VLAN	Click the drop-down menu to select the VLAN to show or clear dynamic MAC entries.
MAC Address	Enter the MAC address to show or clear dynamic MAC entries. If a port, VLAN or MAC address is not selected, the whole dynamic MAC table is displayed or cleared.
View	Click <b>View</b> to display the MAC address information.
Clear	Click <b>Clear</b> to clear the MAC Address Information table.

The ensuing table for **MAC Address Information** settings are informational only: MAC Address, VLAN, Type, Port and **Add to Static MAC** (click to add the MAC address to static MAC address list).

MAC Address	VLAN	Type	Port	
00:13:20:67:D5:D8	default(1)	Dynamic	GE26	Add to Static MAC
08:74:02:2B:BE:29	default(1)	Dynamic	GE26	Add to Static MAC
10:6F:3F:E7:B0:2A	default(1)	Dynamic	GE26	Add to Static MAC
14:AB:C5:68:96:6A	default(1)	Dvnamic	GE26	Add to Static MAC



## 4.36 Security

The Security function allows for the configuration of Storm Control, Port Security, Protected Ports, DoS Prevention, Applications, 802.1x, and IP Security.

## 4.37 Storm Control

The Storm Control page allows you to setup the units and Preamble/IFG to manage the occurrence of packet flooding on the LAN and consequent traffic to prevent the degrading of network performance.

### Global Settings

To access this page, click **Security > Storm Control > Global Settings**.

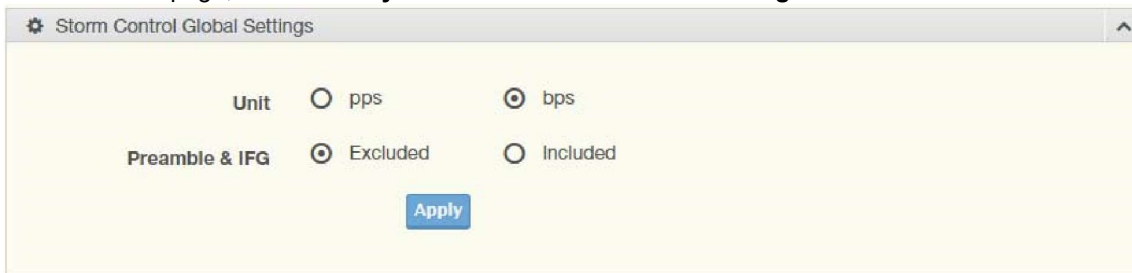


Figure 4.55 Security > Storm Control > Global Settings

The following table describes the items in the previous figure.

Item	Description
Unit	Select <b>pps</b> or <b>bps</b> control units for the Storm Control function.
Preamble & IFG	Select <b>Excluded</b> or <b>Included</b> to setup the Storm Control Global settings. Excluded: exclude preamble & IFG (20 bytes) when count ingress storm control rate. Included: include preamble & IFG (20 bytes) when count ingress storm control rate.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Storm Control Global Information** settings are informational only: Unit and Preamble & IFG.

Storm Control Global Information	
Information Name	Information Value
Unit	bps
Preamble & IFG	Excluded

### Port Settings

The Port Settings page allows you to configure the port and the type of storm control association along with the value of the storm rate for the selected port.

To access this page, click **Security > Storm Control > Port Settings**.

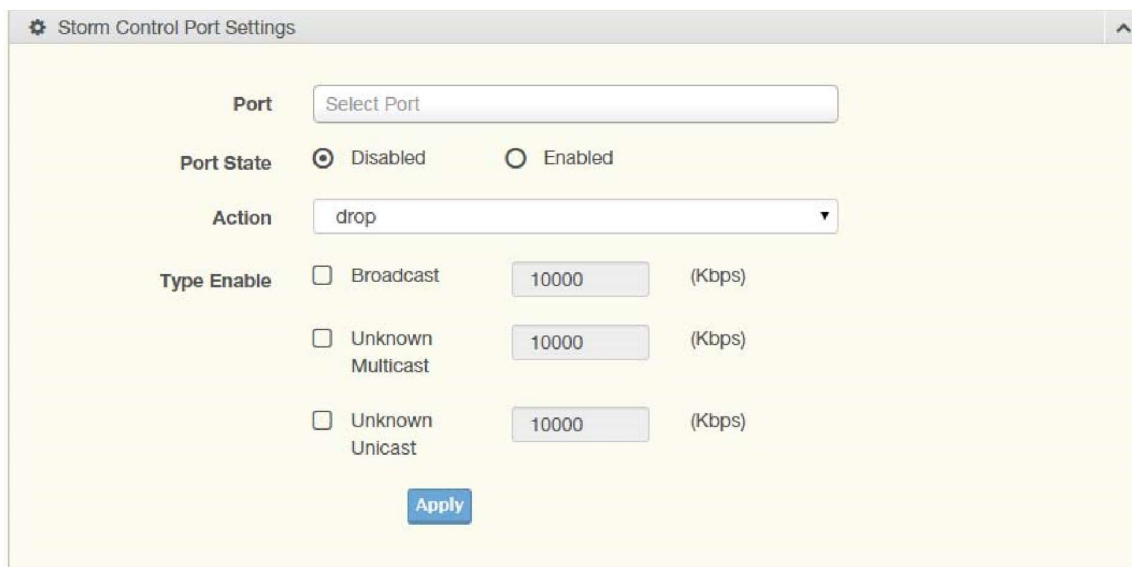


Figure 4.56 Security > Storm Control > Port Settings

The following table describes the items in the previous figure.

Item	Description
Port	Enter the port number to designate the local port for the Storm Control function.
Port State	Select <b>Disabled</b> or <b>Enabled</b> to define the port state
Action	Click the drop-down menu to select the type of action to designate for the selected port during a Storm Control incident. The options are Drop and Shutdown.
Type Enable	Click the radio button to enable Broadcast, Unknown Multicast, or Unknown Unicast. <ul style="list-style-type: none"> <li>● Broadcast: Select the variable in Kbps to define the broadcast bandwidth.</li> <li>● Unknown Multicast: Select the variable in Kbps to define the multicast setting.</li> <li>● Broadcast: Select the variable in Kbps to define the unknown unicast setting.</li> </ul>
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Storm Control Port Information** settings are informational only: Port, Port State, Broadcast (Kbps), Unknown Multicast (Kbps), Unknown Unicast (Kbps) and Action.

Port	Port State	Broadcast (Kbps)	Unknown Multicast (Kbps)	Unknown Unicast (Kbps)	Action
GE1	Disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE2	Disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE3	Disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE4	Disabled	Off (10000)	Off (10000)	Off (10000)	Drop

## 4.38 Port Security

The Port Security page allows you to configure port isolation behavior. To access this page, click **Security > Port Security**.

Figure 4.57 Security > Port Security

The following table describes the items in the previous figure.

Item	Description
Port Select	Enter a single port or multiple port numbers to configure.
Enabled	Select <b>Enabled</b> or <b>Disabled</b> to define the selected Port.
FDB Learn Limit (0-64)	Enter the variable (0 to 64) to set the learn limit for the FDB setting.
Violation MAC Notification	Select <b>Enabled</b> or <b>Disabled</b> to define the selected Port.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Port Security Information** settings are informational only: Port, Enabled, FDB Learn Limit, and Violation MAC Notification.

Port Security Information			
Port	Enabled	FDB Learn Limit	Violation MAC Notification
GE1	Disabled	0	Disabled
GE2	Disabled	0	Disabled
GE3	Disabled	0	Disabled
GE4	Disabled	0	Disabled
GE5	Disabled	0	Disabled
GE6	Disabled	0	Disabled
GE7	Disabled	0	Disabled

## 4.39 Protected Ports

The Protected Port page allows you to configure a single port or multiple ports as a protected or unprotected type.

To access this page, click **Security > Protected Ports**.



Figure 4.58 Security > Protected Ports

The following table describes the items in the previous figure.

Item	Description
Port List	Enter the port number to designate for the Protected Port setting.
Port Type	Select <b>Unprotected</b> or <b>Protected</b> to define the port type.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Protected Ports Status** settings are informational only: Protected Ports and Unprotected Ports.

Protected Ports Status	
Protected Type	Port List
Protected Ports	
Unprotected Ports	all

## 4.40 DoS Prevention

The DoS Prevention page allows you to setup (enabled or disabled) the denial of service.

### DoS Global Settings

The DoS Global Settings page allows you to configure (enabled or disabled) the setting for each function.

To access this page, click **Security > DoS Prevention > DoS Global Settings**.

⚙ DoS Global Settings ^

DMAC = SMAC	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
LAND	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
UDP Blat	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
TCP Blat	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
POD	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
IPv6 Min Fragment	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
	Bytes <input style="width: 80px;" type="text" value="1240"/>	(0-65535)
ICMP Fragments	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
IPv4 Ping Max Size	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
IPv6 Ping Max Size	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Ping Max Size Setting	Bytes <input style="width: 80px;" type="text" value="512"/>	(0-65535)
Smurf Attack	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
	Netmask Length <input style="width: 80px;" type="text" value="0"/>	(0-32)
TCP Min Hdr Size	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
	Byte <input style="width: 80px;" type="text" value="20"/>	(0-31)
TCP-SYN(SPORT<1024)	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Null Scan Attack	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
X-Mas Scan Attack	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
TCP SYN-FIN Attack	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
TCP SYN-RST Attack	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
TCP Fragment (Offset = 1)	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled

Figure 4.59 Security > DoS Prevention > DoS Global Settings

The following table describes the items in the previous figure.

Item	Description
DMAC = SMAC	Click <b>Enabled</b> or <b>Disabled</b> to define DMAC-SMAC for the DoS Global settings.
LAND	Click <b>Enabled</b> or <b>Disabled</b> to define LAND for the DoS Global settings.
UDP Blat	Click <b>Enabled</b> or <b>Disabled</b> to define UDP Blat for the DoS Global settings.
TCP Blat	Click <b>Enabled</b> or <b>Disabled</b> to define TCP Blat for the DoS Global settings.
POD	Click <b>Enabled</b> or <b>Disabled</b> to define POD for the DoS Global settings.
IPv6 Min Fragment	Click <b>Enabled</b> or <b>Disabled</b> to define minimum fragment size for the IPv6 protocol. Enter the variable in bytes (0 to 65535) to set the minimum fragment size when the function is enabled.
ICMP Fragments	Click <b>Enabled</b> or <b>Disabled</b> to define the ICMP Fragments function.
IPv4 Ping Max Size	Click <b>Enabled</b> or <b>Disabled</b> to set the maximum ping size for the IPv4 protocol.
IPv6 Ping Max Size	Click <b>Enabled</b> or <b>Disabled</b> to set a maximum ping size for the IPv6 protocol.
Ping Max Size Setting	Enter the variable in bytes (0 to 65535) to set the maximum ping size.
Smurf Attack	Click <b>Enabled</b> or <b>Disabled</b> to set the Smurf Attack function.
TCP Min Hdr Size	Click <b>Enabled</b> or <b>Disabled</b> to set the minimum header size. Enter the variable in bytes (0 to 31) to set the minimum header size.
TCP-SYN (SPORT < 1024)	Click <b>Enabled</b> or <b>Disabled</b> to set the TCP synchronization function (sport < 1021).
Null Scan Attack	Click <b>Enabled</b> or <b>Disabled</b> to set the Null Scan Attack function.
X-Mas Scan Attack	Click <b>Enabled</b> or <b>Disabled</b> to set the X-Mas Scan function.
TCP SYN-FIN Attack	Click <b>Enabled</b> or <b>Disabled</b> to set the TCP synchronization termination attack function.
TCP SYN-RST Attack	Click <b>Enabled</b> or <b>Disabled</b> to set the TCP synchronization reset attack function.
TCP Fragment	(Offset Click <b>Enabled</b> or <b>Disabled</b> to set the TCP fragment function (offset =1).
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **DoS Global Information** settings are informational only: DMAC = SMAC, Land Attack, UDP Blat, TCP Blat, POD (Ping of Death), IPv6 Min Fragment Size, ICMP Fragment Packets, IPv4 Ping Max Packet Size, IPv6 Ping Max Packet Size, Smurf Attack, TCP Min Header Length, TCP Syn (SPORT < 1024), Null Scan Attack, X-Mas Scan Attack, TCP SYN-FIN Attack, TCP SYN-RST Attack, and TCP Fragment (Offset = 1).

DoS Global Information	
Information Name	Information Value
DMAC = SMAC	Enabled
Land Attack	Enabled
UDP Blat	Enabled
TCP Blat	Enabled
POD (Ping of Death)	Enabled
IPv6 Min Fragment Size	Enabled (1240 Bytes)
ICMP Fragment Packets	Enabled
IPv4 Ping Max Packet Size	Enabled (512 Bytes)
IPv6 Ping Max Packet Size	Enabled (512 Bytes)
Smurf Attack	Enabled (Netmask Length: 0)
TCP Min Header Length	Enabled (20 Bytes)
TCP Syn (SPORT < 1024)	Enabled
Null Scan Attack	Enabled
X-Mas Scan Attack	Enabled
TCP SYN-FIN Attack	Enabled
TCP SYN-RST Attack	Enabled
TCP Fragment (Offset = 1)	Enabled

### DoS Port Settings

The DoS Port Settings page allow you to configure DoS security (enabled or disabled) for the selected port.

To access this page, click **Security > DoS Prevention > DoS Port Settings**.

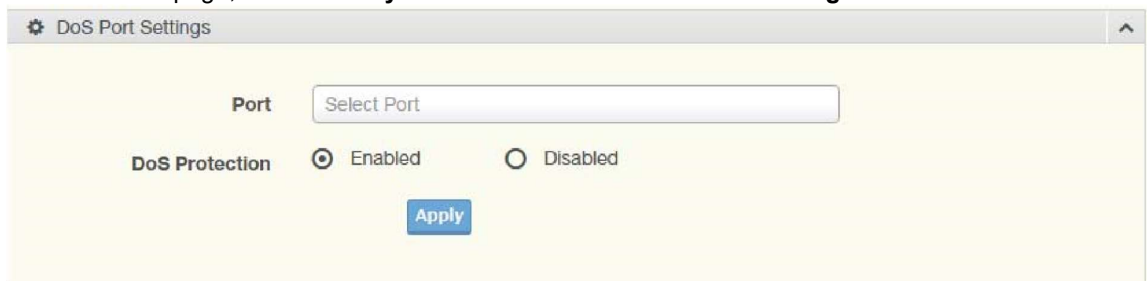


Figure 4.60 Security > DoS Prevention > DoS Port Settings

The following table describes the items in the previous figure.

Item	Description
Port	Select the port to configure for the DoS prevention function.
DoS Protection	Click <b>Enabled</b> or <b>Disabled</b> to set the DoS Port security function state.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **DoS Port Status** settings are informational only: Port and DoS Protection.

DoS Port Status	
Port	DoS Protection
GE1	Disabled
GE2	Disabled
GE3	Disabled
GE4	Disabled
GE5	Disabled

## 4.41 Applications

The Applications function allows you to configure various types of AAA lists.

### TELNET

The TELNET page allows you to combine all kinds of AAA lists with the Telnet line. To access this page, click **Security > Applications > TELNET**.



Figure 4.61 Security > Applications > TELNET

The following table describes the items in the previous figure.

Item	Description
Telnet Service	Click <b>Enabled</b> or <b>Disabled</b> to set remote access through the Telnet Service function.
Apply	Click <b>Apply</b> to save the values and update the screen.
Disconnect	Click <b>Disconnect</b> to disable the current Telnet service.



The ensuing table for **Telnet Information** settings are informational only: Telnet Service and Current Telnet Sessions Count.

Telnet Information	
Information Name	Information Value
Telnet Service	Enabled
Current Telnet Sessions Count	0

## SSH

Secure Shell (SSH) is a protocol providing secure (encrypted) management connection to a remote device.

To access this page, click **Security > Applications > SSH**.



Figure 4.62 Security > Applications > SSH

The following table describes the items in the previous figure.

Item	Description
SSH Service	Click <b>Enabled</b> or <b>Disabled</b> to set up Ethernet encapsulation (remote access) through the Secure Shell (SSH) function.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **SSH Information** settings are informational only: SSH.

SSH Information	
Information Name	Information Value
SSH	Disabled

## HTTP

The HTTP page allows you to combine all kinds of AAA lists to the HTTP line. Attempts to access the switch's Web UI from HTTP are first authenticated.

To access this page, click **Security > Applications > HTTP**.

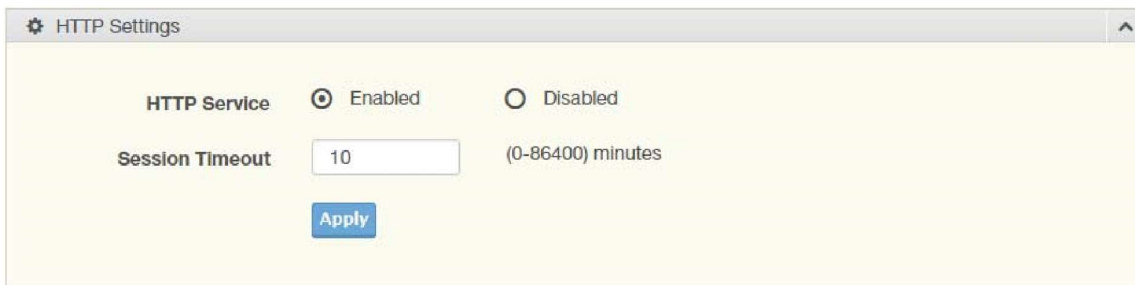


Figure 4.63 Security > Applications > HTTP

The following table describes the items in the previous figure.

Item	Description
HTTP Service	Click <b>Enabled</b> or <b>Disabled</b> to set up Ethernet encapsulation (remote access) through HTTP function.
Session Timeout	Enter the variable in minutes (0 to 86400) to define the timeout period for the HTTP session.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **HTTP Information** settings are informational only: HTTP Service and Session Timeout.

HTTP Information	
Information Name	Information Value
HTTP Service	Enabled
Session Timeout	10

## HTTPS

The HTTPS page allows you to combine all kinds of AAA lists on the HTTPS line. Attempts to access the switch's Web UI from HTTPS are first authenticated. To access this page, click **Security > Applications > HTTPS**.

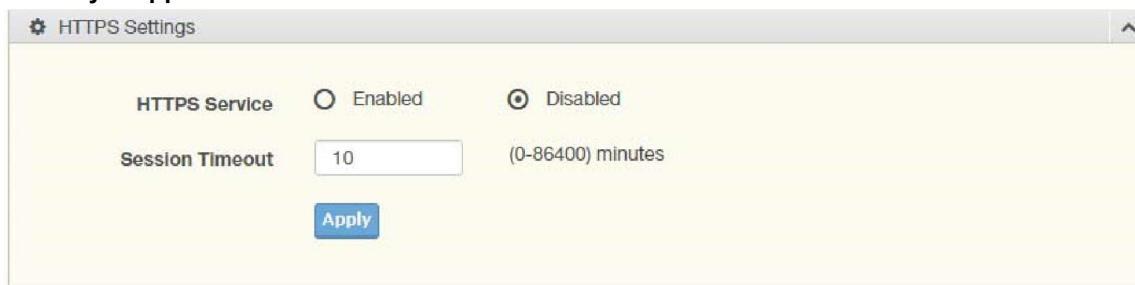


Figure 4.64 Security > Applications > HTTPS

The following table describes the items in the previous figure.

Item	Description
HTTPS Service	Click <b>Enabled</b> or <b>Disabled</b> to set up Ethernet encapsulation over HTTPS.
Session Timeout	Enter the variable in minutes (0 to 86400) to define the timeout period for the HTTP session.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **HTTPS Information** settings are informational only: HTTPS Service and Session Timeout.

HTTPS Information	
Information Name	Information Value
HTTPS Service	Disabled
Session Timeout	10

## 4.42 802.1x

The 802.1x function provides port-based authentication to prevent unauthorized devices (clients) from gaining access to the network.

### 802.1x Settings

The 802.1x Settings page allows you to set the state (enabled or disabled) for the selected IP server address, port, accounting port, and associated password including a reauthentication period.

To access this page, click **Security > 802.1x > 802.1x Settings**.

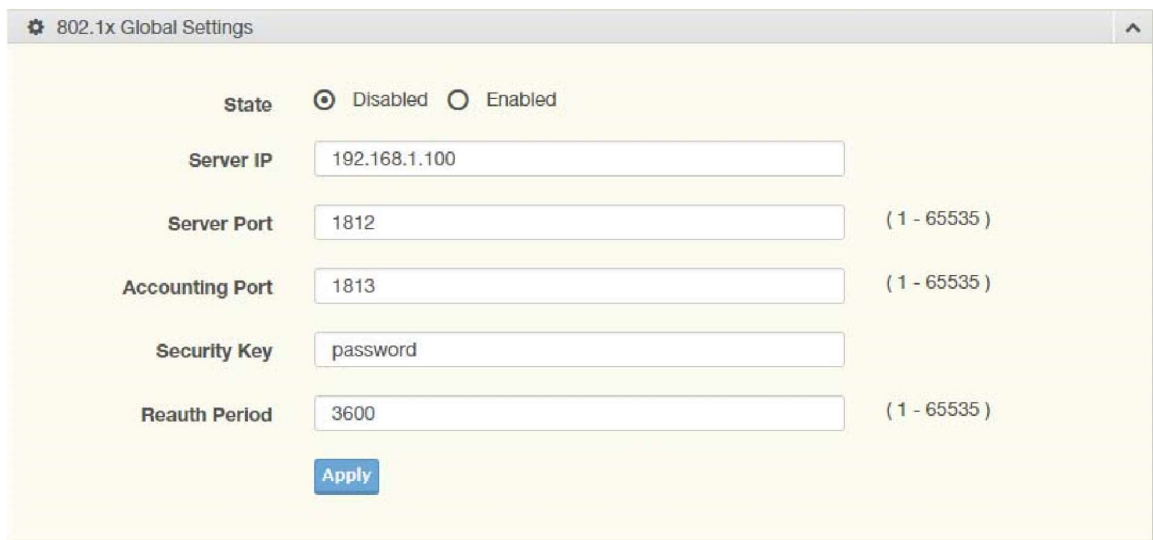


Figure 4.65 Security > 802.1x > 802.1x Settings

The following table describes the items in the previous figure.

Item	Description
State	Click <b>Enabled</b> or <b>Disabled</b> to set up 802.1x Setting function.
Server IP	Enter the IP address of the local server providing authentication function.
Server Port	Enter the port number (1 to 65535) assigned to the listed Server IP.
Accounting Port	Enter the port number (1 to 65535) assigned to the listed server IP configured to provide authorization and authentication for network access.
Security Key	Enter the variable to define the network security key used in authentication.
Reauth Period	Enter the variable in seconds to define the period of time between authentication attempts.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **802.1x Information** settings are informational only: 802.1x State, Server IP, Server Port, Accounting Port, Security Key and Reauth Period.

802.1x Information	
Information Name	Information Value
802.1xState	Disabled
Server IP	192.168.1.100
Server Port	1812
Accounting Port	1813
Security Key	password
Reauth Period	3600

### 802.1x Port Configuration

The 802.1x Port Configuration page allows you to identify the authorization state for a port by using a MAC or Port authentication base.

To access this page, click **Security > 802.1x > 802.1x Port Configuration**.

Figure 4.66 Security > 802.1x > 802.1x Port Configuration

The following table describes the items in the previous figure.

Item	Description
Authentication based	Click <b>Port</b> or <b>Mac</b> to designate the type of configuration for the 802.1x Port setting.
Port Select	Enter the port number associated with the configuration setting.
State	Click <b>Authorize</b> or <b>Disabled</b> to define the listed port's state mode.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **802.1x Port Authorization** settings are informational only: Port and Port State.



802.1x Port Authorization	
Port	802.1x Port Authorization
GE1	Disabled
GE2	Disabled
GE3	Disabled
GE4	Disabled
GE5	Disabled

## 4.43 IP Security

This section provides a means to configure the IP Security settings.

### Global Settings

The Global Settings page allows you to set the IP Security status (enabled or disabled). To access this page, click **Security > IP Security > Global Settings**.



Figure 4.67 Security > IP Security > Global Settings

The following table describes the items in the previous figure.

Item	Description
Status	Click <b>Enabled</b> or <b>Disabled</b> to define the global setting for the IP security function.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **IP Security Status** settings are informational only: IP Security.

IP Security Status	
Information Name	Information Value
IP Security	Disabled

## Entry Settings

Once the Global Setting is enabled, use the Entry Settings to define an IP Security entry.

### Security > IP Security > Entry Settings.

Figure 4.68 Security > IP Security > Entry Settings

The following table describes the items in the previous figure.

Item	Description
IP Address	Enter the source IP address to apply the IP Security function.
IP Mask	Enter the IP address for use in masking the previous IP Address.
Services	Enter the type of services to associate with the entry setting.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **IP Security Entry Information** settings are informational only: IP Address, IP Mask, Services and Action.

IP Security Entry Information			
IP Address	IP Mask	Service	Action

## 4.44 QoS

The QoS function allows you to configure settings for the switch QoS interface and how the switch connects to a remote server to get services.

## 4.45 General

Traditionally, networks operate on a best-effort delivery basis, all traffic has equal priority and an

equal chance of being delivered in a timely manner. When there is congestion, all traffic has an equal chance of being dropped.

The QoS feature can be configured for congestion-management and congestion-avoidance to specifically manage the priority of the traffic delivery. Implementing QoS in the network makes performance predictable and bandwidth utilization much more effective.

The QoS implementation is based on the prioritization values in Layer 2 frames.

### QoS Properties

The QoS Properties allows you to set the QoS mode.

To access this page, click **QoS > General > QoS Properties**.



Figure 4.69 QoS > General > QoS Properties

The following table describes the items in the previous figure.

Item	Description
QoS Mode	Select <b>Disabled</b> or <b>Basic</b> to setup the QoS function.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **QoS Global Information** settings are informational only: QoS Mode.

QoS Global Information	
Information Name	Information Value
QoS Mode	Disabled

### QoS Settings

Once the QoS function is enabled, you can configure the available settings. To access this page, click **QoS > General > QoS Settings**.

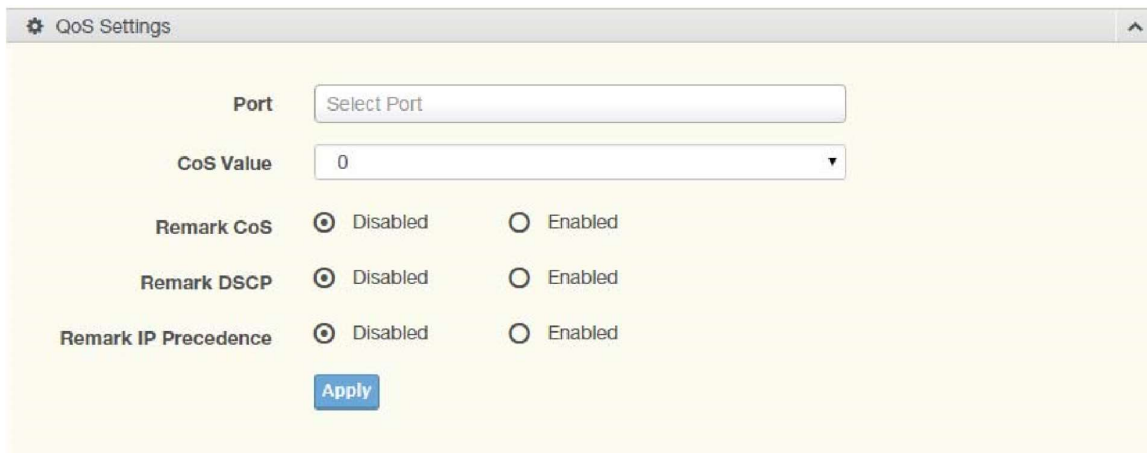


Figure 4.70 QoS > General > QoS Settings

The following table describes the items in the previous figure.

Item	Description
Port	Enter the port number to associate with the QoS setting.
CoS Value	Click the drop-down menu to designate the Class of Service (CoS) value (0 to 7) for the Port entry.
Remark CoS	Click <b>Disabled</b> or <b>Enabled</b> to setup the Remark CoS function. When enabled the LAN (preassigned priority values) is marked at Layer 2 boundary to CoS values.
Remark DSCP	Click <b>Disabled</b> or <b>Enabled</b> to setup the DSCP remark option for the QoS function.
Remark IP Precedence	Click <b>Disabled</b> or <b>Enabled</b> to setup the Remark IP Precedence for the QoS function.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **QoS Status** settings are informational only: Port, CoS value, Remark CoS, Remark DSCP and Remark IP Precedence.

QoS Status				
Port	CoS Value	Remark CoS	Remark DSCP	Remark IP Precedence
GE1	0	Disabled	Disabled	Disabled
GE2	0	Disabled	Disabled	Disabled
GE3	0	Disabled	Disabled	Disabled
GE4	0	Disabled	Disabled	Disabled

### Queue Scheduling

The switch supports eight CoS queues for each egress port. For each of the eight queues, two types of scheduling can be configured: Strict Priority and Weighted Round Robin (WRR). Strict Priority scheduling is based on the priority of queues. Packets in a high-priority queue are always sent first and packets in a low-priority queue are only sent after all the high priority queues are empty.

Weighted Round Robin (WRR) scheduling is based on the user priority specification to indicate



the importance (weight) of the queue relative to the other CoS queues. WRR scheduling prevents low-priority queues from being completely ignored during periods of high priority traffic. The WRR scheduler sends some packets from each queue in turn.

**QoS > General > QoS Scheduling.**

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

Figure 4.71 QoS > General > QoS Scheduling

The following table describes the items in the previous figure.

Item	Description
Queue	Queue entry for egress port.
Strict	Select Strict to assign the scheduling designation to the selected queue.
WRR	Select WRR to assign the scheduling designation to the selected queue.
Weight	Enter a queue priority (weight) relative to the defined entries (WRR only).
% of WRR Bandwidth	Displays the allotted bandwidth for the queue entry in percentage values.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Queue Information** settings are informational only: Strict Priority Queue Number.

Information Name	Information Value
Strict Priority Queue Number	8

### CoS Mapping

The CoS Mapping allows you to apply CoS mapping.

To access this page, click **QoS > General > CoS Mapping**.

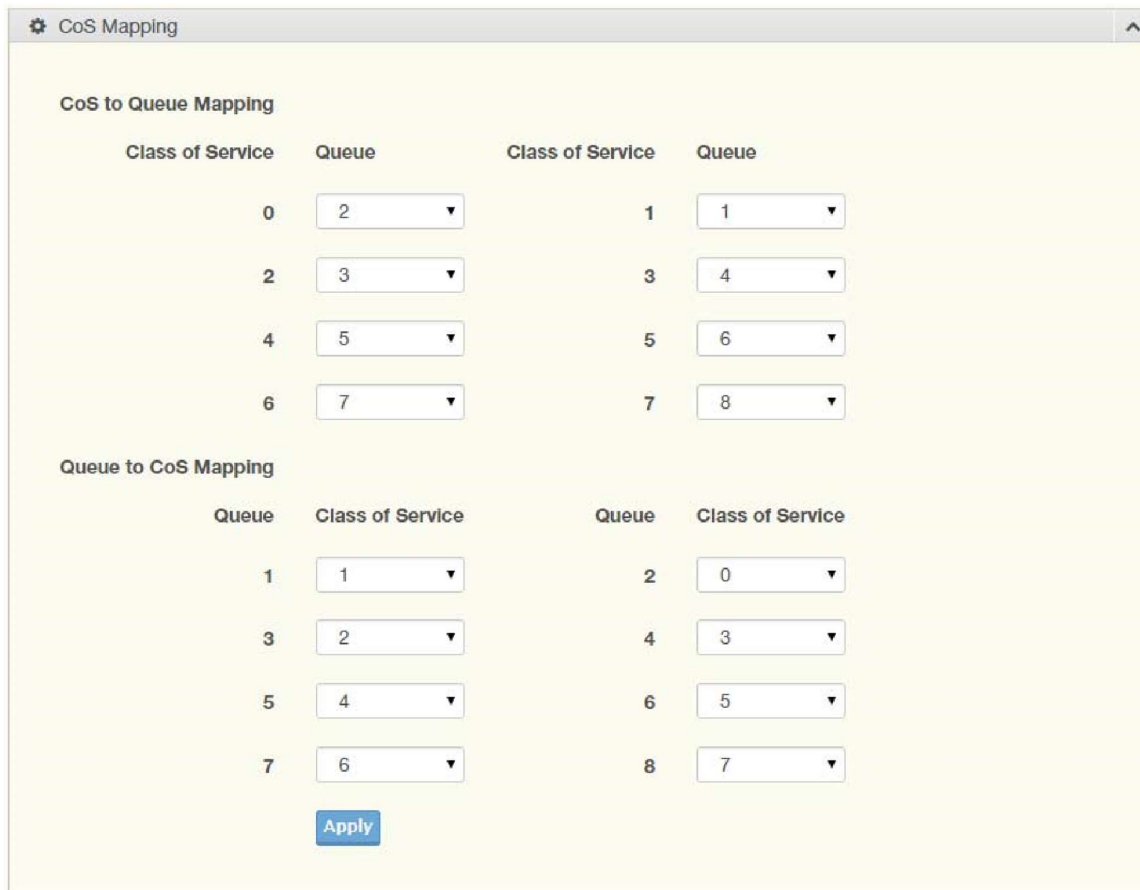


Figure 4.72 QoS > General > CoS Mapping

The following table describes the items in the previous figure.

Item	Description
CoS to Queue Mapping	
Class of Service	Displays the CoS for the queue entry
Queue	Click the drop-down menu to select the queue priority for selected CoS
Queue to CoS Mapping	
Queue	Displays the queue entry for CoS mapping.
Class of Service	Click the drop-down menu to select the CoS type
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **CoS Mapping Information** settings are informational only: CoS and Mapping to Queue.

CoS Mapping Information	
CoS	Mapping to Queue
0	2
1	1
2	3
3	4
4	5

The ensuing table for **Queue Mapping Information** settings are informational only: Queue and Mapping to CoS.

Queue Mapping Information	
Queue	Mapping to CoS
1	1
2	0
3	2
4	3

### **DSCP Mapping**

The DSCP to Queue mapping function maps queue values in incoming packets to a DSCP value that QoS uses internally to represent the priority of the traffic. The following table shows the DSCP to Queue map.

If these values are not appropriate for your network, you need to modify them.

**QoS > General > DSCP Mapping.**

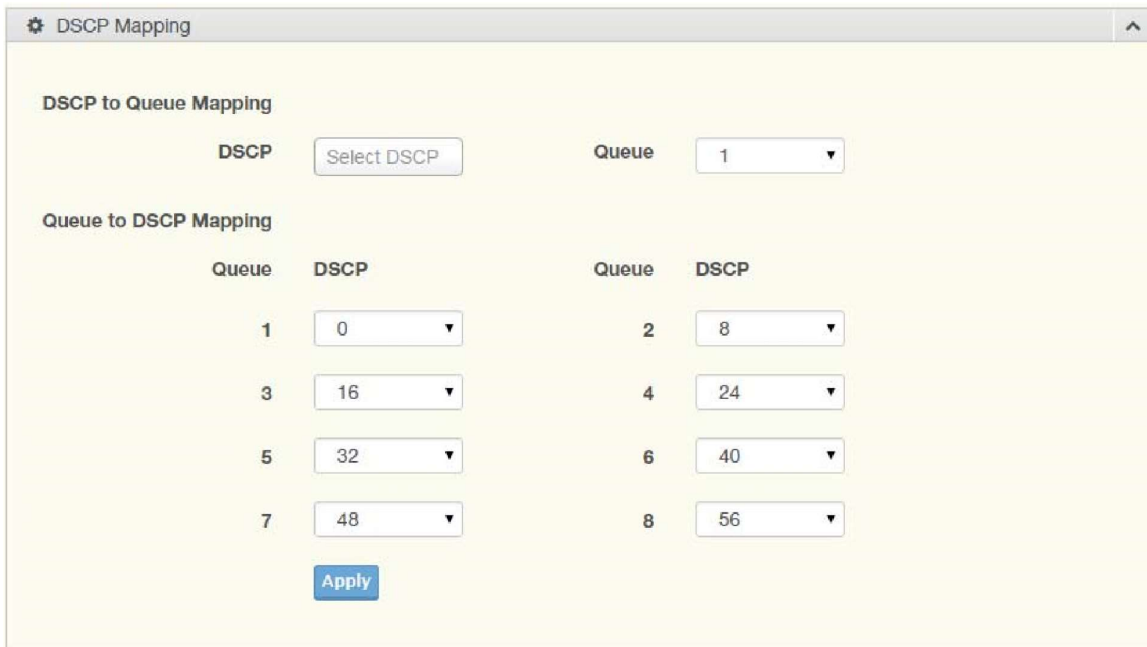


Figure 4.73 QoS > General > DSCP Mapping

The following table describes the items in the previous figure.

Item	Description
<b>DSCP to Queue Mapping</b>	
DSCP	Enter the DSCP entry to define the precedence values.
Queue	Click the drop-down menu to select the queue designation for the DSCP value.
<b>Queue to DSCP Mapping</b>	
Queue	Displays the queue value for the DSCP map.
DSCP	Enter the DSCP entry to define the precedence values.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **DSCP Mapping Information** settings are informational only: DSCP and Mapping to Queue.

DSCP Mapping Information	
DSCP	Mapping to Queue
0	1
1	1
2	1
3	1
4	1

The ensuing table for **Queue Mapping Information** settings are informational only: Queue and Mapping to DSCP.

Queue Mapping Information	
Queue	Mapping to DSCP
1	0
2	8
3	16

### IP Precedence Mapping

The IP Precedence Mapping allows you to set IP Precedence mapping.

To access this page, click **QoS > General > IP Precedence Mapping**.

⚙ IP Precedence Mapping ^

**IP Precedence to Queue Mapping**

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

**Queue to IP Precedence Mapping**

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

Figure 4.74 QoS > General > IP Precedence Mapping

The following table describes the items in the previous figure.

Item	Description
IP Precedence to Queue Mapping	
IP Precedence	Displays the IP precedence value for the queue map.
Queue	Click the drop-down menu to map a queue value to the selected IP precedence.
Queue to IP Precedence Mapping	
Queue	Displays the queue entry for mapping IP precedence values.
IP Precedence	Click the drop-down menu to map an IP precedence value to the selected queue.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **IP Precedence Mapping Information** settings are informational only: IP Precedence and Mapping to Queue.

IP Precedence Mapping Information	
IP Precedence	Mapping to Queue
0	1
1	2
2	3

The ensuing table for **Queue Mapping Information** settings are informational only: Queue and Mapping to IP Precedence.

Queue Mapping Information	
Queue	Mapping to IP Precedence
1	0
2	1
3	2
4	3

## 4.46 QoS Basic Mode

Quality of Service (QoS) allows giving preferential treatment to certain types of traffic at the expense of others. Without QoS, the switch offers best-effort service to each packet, regardless of the packet contents or size sending the packets without any assurance of reliability, delay bounds, or throughput.

QoS mode supports two modes: 802.1p and DSCP.

### Global Settings

The Global Settings page allows you to configure the trust mode to a port selection.

To access this page, click **QoS > QoS Basic Mode > Global Settings**. The function is only available when **QoS Properties** is set to **Basic**.



Figure 4.75 QoS > QoS Basic Mode > Global Settings

The following table describes the items in the previous figure.

Item	Description
Trust Mode	Click the drop-down menu to select the trust state of the QoS basic mode.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **QoS Information** settings are informational only: Trust Mode.

QoS Global Information	
Information Name	Information Value
QoS Mode	Disabled

### Port Settings

The Port Settings page allows you to define a trust state (enabled or disabled) to a listed port.

To access this page, click **QoS > QoS Basic Mode > Port Settings**.



Figure 4.76 QoS > QoS Basic Mode > Port Settings

The following table describes the items in the previous figure.

Item	Description
Port	Enter the port number for the QoS basic mode setting.
Trust State	Select <b>Enabled</b> or <b>Disabled</b> to set the port's trust state status.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **QoS Port Status** settings are informational only: Port and Trust State.

QoS Global Information	
Information Name	Information Value
QoS Mode	Disabled

## 4.47 Rate Limit

Rate Limit features control on a per port basis. Bandwidth control is supported for the following: Ingress Bandwidth Control, Egress Bandwidth Control, and Egress Queue.

### Ingress Bandwidth Control

The Ingress Bandwidth Control page allows you to configure the bandwidth control for a listed port.

To access this page, click **QoS > Rate Limit > Ingress Bandwidth Control**.

Figure 4.77 QoS > Rate Limit > Ingress Bandwidth Control

The following table describes the items in the previous figure.

Item	Description
Port	Enter the port number for the rate limit setup.
State	Select <b>Disabled</b> or <b>Enabled</b> to set the port's state status.
Rate (Kbps)	Enter the value in Kbps (16 to 1000000) to set as the bandwidth rate for the selected port.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Ingress Bandwidth Control Status** settings are informational only: Port and Ingress Rate Limit (Kbps).

QoS Global Information	
Information Name	Information Value
QoS Mode	Disabled



## Egress Bandwidth Control

The Egress Bandwidth Control page allows you to set the egress bandwidth control for a listed port.

To access this page, click **QoS > Rate Limit > Egress Bandwidth Control**.

Figure 4.78 QoS > Rate Limit > Egress Bandwidth Control

The following table describes the items in the previous figure.

Item	Description
Port	Enter the port number to set the Egress Bandwidth Control.
State	Select <b>Disabled</b> or <b>Enabled</b> to set the Egress Bandwidth Control state.
Rate (Kbps)	Enter the value in Kbps (16 to 1000000) to set the Egress Bandwidth rate.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Egress Bandwidth Control Status** settings are informational only: Port and Egress Rate Limit (Kbps).

QoS Global Information	
Information Name	Information Value
QoS Mode	Disabled

## Egress Queue

The Egress Queue page allows you to set the egress bandwidth parameters. To access this page, click **QoS > Rate Limit > Egress Queue**.

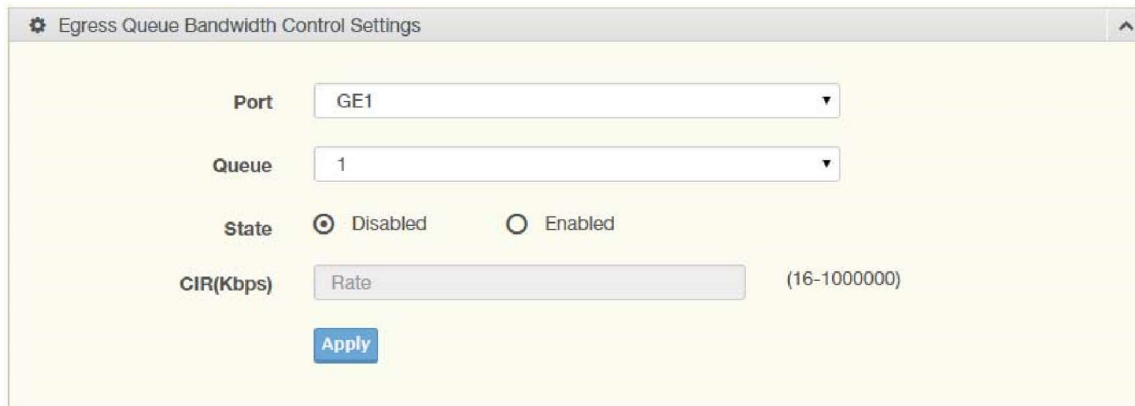


Figure 4.79 QoS > Rate Limit > Egress Queue

The following table describes the items in the previous figure.

Item	Description
Port	Click the drop-down menu to select the port to define the Egress queue.
Queue	Click the drop-down menu to set the queue order for the Egress setting.
State	Click <b>Disabled</b> or <b>Enabled</b> to set the Egress queue state.
CIR (Kbps)	Enter the value in Kbps (16 to 1000000) to set the CIR rate for the Egress queue.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **GE1 Egress Per Queue Status** settings are informational only: Queue Id and Egress Rate Limit (Kbps).

QoS Global Information	
Information Name	Information Value
QoS Mode	Disabled

## 4.48 Management

### 4.49 LLDP

LLDP is a one-way protocol without request/response sequences. Information is advertised by stations implementing the transmit function, and is received and processed by stations implementing the receive function.

#### LLDP System Settings

The LLDP System Settings allows you to configure the status (enabled or disabled) for the protocol, set the interval for frame transmission, set the hold time multiplier, and the re-initialization delay.

To access this page, click **Management > LLDP > LLDP System Settings**.

Figure 4.80 Management > LLDP > LLDP System Settings

The following table describes the items in the previous figure.

Item	Description
Enabled	Click <b>Enabled</b> or <b>Disabled</b> to set the Global Settings state.
LLDP PDU Disable Action	Click to select the LLDP PDU handling action when LLDP is globally disabled. Options include: Filtered, Bridged, or Flooded.
Transmission Interval	Select the interval at which frames are transmitted. The default is 30 seconds, and the valid range is 5 to 32767 seconds.
Holdtime Multiplier	Select the multiplier on the transmit interval to assign to TTL.
Reinitialization Delay	Select the delay length before re-initialization.
Transmit Delay	Select the delay after an LLDP frame is sent.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **LLDP Global Config** settings are informational only: LLDP Enabled, LLDP PDU Disable Action, Transmission Interval, Holdtime Multiplier, Reinitialization Delay and Transmit Delay.

LLDP Global Config	
Config Name	Config Value
LLDP Enabled	Disabled
LLDP PDU Disable Action	Flooding
Transmission Interval	30 Secs
Holdtime Multiplier	4
Reinitialization Delay	2 Secs
Transmit Delay	2 Secs

### LLDP Port Settings

The LLDP Port Settings page allows you to configure the state (enabled or disabled) of the selected port.

To access this page, click **Management > LLDP > LLDP Port Settings**.



Figure 4.81 Management > LLDP > LLDP Port Settings > LLDP Port Configuration

The following table describes the items in the previous figure.

Item	Description
Port Select	Enter the port number associated with the LLDP setting.
State	Click the drop-down menu to select the LLDP port state.
Apply	Click <b>Apply</b> to save the values and update the screen.



Figure 4.82 Management > LLDP > LLDP Port Settings > Optional TLVs Selection

The following table describes the items in the previous figure.

Item	Description
Port Select	Enter the port number associated with the TLV (optional) selection.
Optional TLV Select	<p>Click the drop-down menu to select the LLDP optional TLVs to be carried (multiple selections are allowed).</p> <ul style="list-style-type: none"> <li>● System Name: To include system name TLV in LLDP frames.</li> <li>● Port Description: To include port description TLV in LLDP frames.</li> <li>● System Description: To include system description TLV in LLDP frames.</li> <li>● System Capability: To include system capability TLV in LLDP frames.</li> <li>● 802.3 MAC-PHY: To include MAC/PHY TLV in LLDP frames.</li> <li>● 802.3 Link Aggregation: To include link aggregation TLV in LLDP frames.</li> </ul>

	<ul style="list-style-type: none"> <li>802.3 Maximum Frame Size: To include maximum frame size TLV in LLDP frames.</li> <li>Management Address: To include management address TLV in LLDP frames.</li> <li>802.1 PVID: To include port VLAN ID TLV in LLDP frames.</li> </ul>
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **LLDP Port Status** settings are informational only: Port, State and Selected Optional TLVs.

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

**VLAN Name TLV VLAN Selection**

Port Select

VLAN Select

Figure 4.83 Management > LLDP > LLDP Port Settings > VLAN Name TLV VLAN Selection

The following table describes the items in the previous figure.

Item	Description
Port Select	Enter the port number to associated with the TLV selection.
VLAN Select	Select the VLAN Name ID to be carried out (multiple selection is allowed).
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **LLDP Port VLAN TLV Status** settings are informational only: Port and Selected VLAN.

LLDP Port VLAN TLV Status	
Port	Selected VLAN
GE1	
GE2	
GE3	

### LLDP Local Device Info

The LLDP Local Device Info page allows you to view information regarding network devices, providing that the switch has already obtained LLDP information on the devices.

To access this page, click **Management > LLDP > LLDP Local Device Info**.

The ensuing table for **Local Device Summary** settings are informational only: Chassis ID Subtype, Chassis ID, System Name, System Description, Capabilities Supported, Capabilities Enabled, and Port ID Subtype.

Local Device Summary	
Information Name	Information Value
Chassis ID Subtype	MAC Address
Chassis ID	00:E0:4C:00:00:00
System Name	Switch
System Description	switch
Capabilities Supported	Bridge
Capabilities Enabled	Bridge
Port ID Subtype	Interface name

The ensuing table for **Port Status** settings are informational only: Port, Selected VLAN, and **Detail** (click the radio box and click **Detail** to displays the details).

Port Status		
Detail	Port	Selected VLAN
<input type="radio"/>	GE1	TX & RX
<input type="radio"/>	GE2	TX & RX
<input type="radio"/>	GE3	TX & RX
<input type="radio"/>	GE4	TX & RX

### LLDP Remote Device Info

The LLDP Remote Device Info page allows you to view information about remote devices, LLDP information must be available on the switch.

To access this page, click **Management > LLDP > LLDP Remote Device Info**.

Remote Device Info							
<input type="button" value="Detail"/> <input type="button" value="Delete"/> <input type="button" value="Refresh"/>							
Sel	Local Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	System Name	Time to Live

Figure 4.84 Management > LLDP > LLDP Remote Device Info

The following table describes the items in the previous figure.

Item	Description
Detail	Click to display the device details.
Delete	Click to delete the selected devices.
Refresh	Click to refresh the remote device information list.

## LLDP Overloading

To access this page, click **Management > LLDP > LLDP Overloading**.

The ensuing table for **LLDP Overloading** settings are informational only: Port, Total (Bytes), Left to Send (Bytes), Status, and Status (Mandatory TLVs, 802.3 TLVs, Optional TLVs and 802.1 TLVs).

Port	Total (Bytes)	Left to Send (Bytes)	Status	Status			
				Mandatory TLVs	802.3 TLVs	Optional TLVs	802.1 TLVs
GE1	29	1459	Not Overloading	21(Transmitted)			8(Transmitted)
GE2	29	1459	Not Overloading	21(Transmitted)			8(Transmitted)
GE3	29	1459	Not Overloading	21(Transmitted)			8(Transmitted)

## 4.50 SNMP

Simple Network Management Protocol (SNMP) is a protocol to facilitate the monitoring and exchange of management information between network devices. Through SNMP, the health of the network or status of a particular device can be determined.

### SNMP Settings

The SNMP Settings page allows you to set the SNMP daemon state (enabled or disabled). To access this page, click **Management > SNMP > SNMP Settings**.

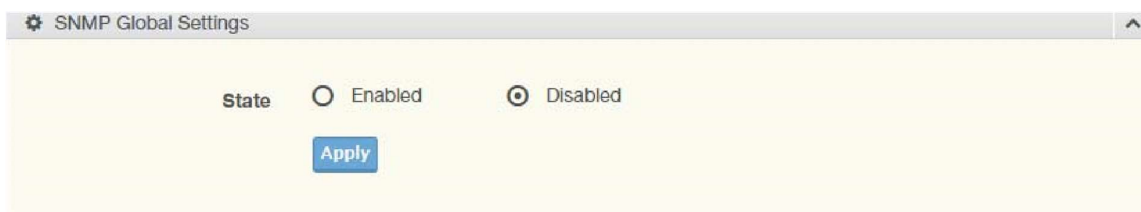


Figure 4.85 Management > SNMP > SNMP Settings

The following table describes the items in the previous figure.

Item	Description
State	Click <b>Enabled</b> or <b>Disabled</b> to define the SNMP daemon.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **SNMP Information** settings are informational only: SNMP.

Information Name	Information Value
SNMP	Enabled

### SNMP Community

The SNMP Community page provides configuration options for the community.

SNMP v1 and SNMP v2c use the group name (Community Name) certification. Its role is similar to the password function. If SNMP v1 and SNMP v2c are used, you can go directly from the configuration settings to this page to configure the SNMP community.

To access this page, click **Management > SNMP > SNMP Community**.

*Figure 4.86 Management > SNMP > SNMP Community*

The following table describes the items in the previous figure.

Item	Description
Community Name	Enter a community name (up to 20 characters).
Access Right	Click the radio box to specify the access level (read only or read write).
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Community Status** settings are informational only: No., Community Name, Access Right, and **Delete** (click to delete the desired community name).

No.	Community Name	Access Right	Action
1	public	read-only	Delete
2	private	read-write	Delete

## SNMP User Settings

The SNMP User Settings page allows you to create SNMP groups. The users have the same level of security and access control permissions as defined by the group settings.

To access this page, click **Management > SNMP > SNMP User Settings**.



Figure 4.87 Management > SNMP > SNMP User Settings

The following table describes the items in the previous figure.

Item	Description
User Name	Enter a user name (up to 32 characters) to create an SNMP profile.
Access Right	Click <b>read-only</b> or <b>read-write</b> to define the access right for the profile.
Encrypted	Click the option to set the encrypted option for the user setting.
Auth-Protocol	Click the drop-down menu to select the authentication level: MD5 or SHA. The field requires a user password. <ul style="list-style-type: none"> <li>• MD5: specify HMAC-MD5-96 authentication level</li> <li>• SHA: specify HMAC-SHA authentication protocol</li> </ul>
Password	Enter the characters to define the password associated with the authentication protocol.
Priv-Protocol	Click the drop-down menu to select an authorization protocol: none or DES. The field requires a user password. <ul style="list-style-type: none"> <li>• None: no authorization protocol in use</li> <li>• DES: specify 56-bit encryption in use</li> </ul>
Password	Enter the characters to define the password associated with the authorization protocol.
Add	Click <b>Add</b> to save the values and update the screen.

The ensuing table for **User Status** settings are informational only: User Name, Access Right, Auth-Protocol, Priv-Protocol and **Delete** (click to delete the desired user name).

User Status				
User Name	Access Right	Auth-Protocol	Priv-Protocol	Action

## SNMP Trap

The SNMP Trap page allows you to set the IP address of the node and the SNMP credentials corresponding to the version that is included in the trap message.

To access this page, click **Management > SNMP > SNMP Trap**.

Figure 4.88 Management > SNMP > SNMP Trap

The following table describes the items in the previous figure.

Item	Description
IP Address	Enter the IP address to designate the SNMP trap host.
Community Name	Click the drop-down menu to select a defined community name.
Version	Click the drop-down menu to designate the SNMP version credentials (v1 or v2c).
Add	Click <b>Add</b> to save the values and update the screen.

The ensuing table for **Trap Host Status** settings are informational only: No., IP Address, Community Name, Version and **Delete** (click to delete the desired IP address).

No.	IP Address	Community Name	Version	Action
-----	------------	----------------	---------	--------

## 4.51 Power Over Ethernet

Power Over Ethernet is the function supplying power to Powered Devices (PD) through the switch in the event that AC power is not readily available. Power over Ethernet can be used for the following areas:

- Surveillance devices
- I/O sensors for security requirements
- Wireless access points

### PoE System Settings

The PoE System Settings page allows you to configure the overload disconnect and the

maximum available wattage.

To access this page, click **Management > Power Over Ethernet > PoE System Settings**.

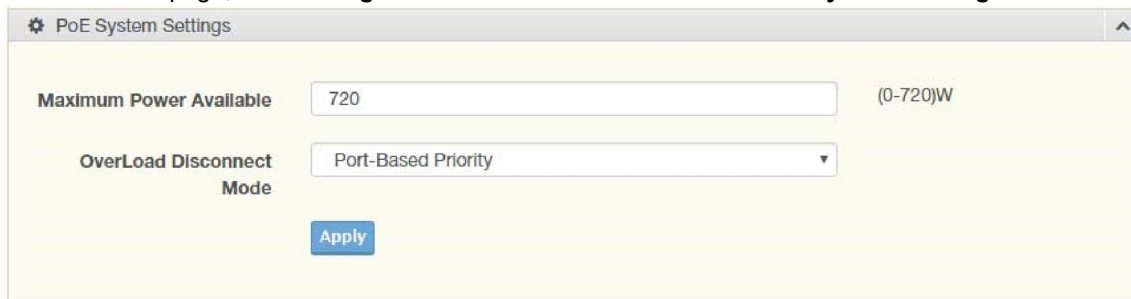


Figure 4.89 Management > Power Over Ethernet > PoE System Settings

The following table describes the items in the previous figure.

Item	Description
Maximum Power Available	Select the value in Watts to set the maximum available power.
OverLoad Disconnect Mode	Click the drop-down menu to designate the overload mode: Overload Port First Port-Based Priority
Apply	Click <b>Apply</b> to save the values and update the screen

The ensuing table for **PoE System Information** settings are informational only: Firmware Version, Maximum Power Available, Actual Power Consumption, and Overload Disconnect Type.

PoE System Information	
Information Name	Information Value
Firmware Version	1607
Maximum Power Available	740.0 W
Actual Power Consumption	1.9 W
OverLoad Disconnect TYPE	Port-Based Priority

### PoE Port Settings

The PoE Port Settings page allows you to configure the port status, its power limitations, legacy mode status, and power limit settings.

To access this page, click **Management > Power Over Ethernet > PoE Port Settings**.

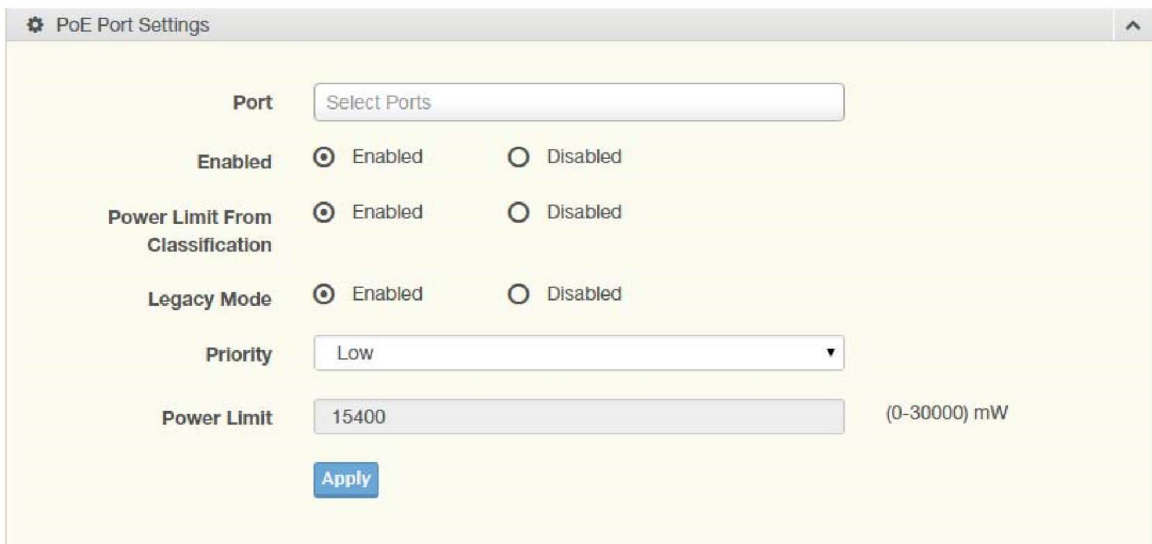


Figure 4.90 Management > Power Over Ethernet > PoE Port Settings

The following table describes the items in the previous figure.

Item	Description
Port	Click the drop-down menu to select a PoE port.
Enabled	Select <b>Enabled</b> or <b>Disabled</b> to designate the PoE port function by ports.
Power Limit From Classification	Select <b>Enabled</b> or <b>Disabled</b> to designate the power limit classification.
Legacy Mode	Select <b>Enabled</b> or <b>Disabled</b> to designate the legacy mode option for the port.
Priority	Click the drop-down menu to configure the power supply priority: <b>Critical, Low, Medium, or High</b> . Default is <b>Low</b> .
Power Limit	Enter a number to set the port power current limitation to be given to the Powered Device (PD)
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **PoE Information** settings are informational only: Port, Enable State, Power Limit From Classification, Priority, Legacy and Power Limit (W).

Port	Switch State	Power Limit From Classification	Priority	Legacy Mode	Power Limit(W)
GE1	Enabled	Disabled	Low	Disabled	30.000
GE2	Enabled	Disabled	Low	Disabled	30.000
GE3	Enabled	Disabled	Low	Disabled	30.000

### PoE Port Status

To access this page, click **Management > Power Over Ethernet > PoE Port Status**. The ensuing table for **PoE Port Status** settings are informational only: Port, Current (mA), Voltage (V), Power (W), and Temp. (°C).

Port	Current (mA)	Voltage (V)	Power (W)	Temp. °C
GE23	39	50.013(V)	1.900(W)	35.000(°C)

## 4.53 DHCP Server

The Dynamic Host Configuration Protocol (DHCP) is a network protocol enabling a server to automatically assign an IP address to a computer from a defined range of numbers configured for a given network.

### Status Settings

The Status Settings page allows you to configure the DHCP server mode (enabled or disabled). To access this page, click **Management > DHCP Server > Status Settings**.



Figure 4.92 Management > DHCP Server > Status Settings

The following table describes the items in the previous figure.

Item	Description
DHCP Server	Select <b>Enable</b> or <b>Disable</b> to designate the DHCP server function type. When a new DHCP server mode is selected, the switch requires a system restart for the new mode to take effect.
Apply	Click <b>Apply</b> to save the values and update the screen.
Restart	Click <b>Restart</b> to have the switch perform a system restart function. In the event that the IP settings are changed, the DHCP server must be restarted for the IP settings to take effect.

The ensuing table for **Status Information** settings are informational only: DHCP Server Service.

Information Name	Information Value
DHCP Server Service	Disabled

## Global Settings

The Global Settings page allows you to configure the global settings for the DHCP function. To access this page, click **Management > DHCP Server > Global Settings**.

Figure 4.93 Management > DHCP Server > Global Settings

The following table describes the items in the previous figure.

Item	Description
Lease Time	Type in the value designating the lease time (60 - 864000) in seconds for each setting lease.
Low IP Address	Type in the value designating the lowest range in the IP address pool.
High IP Address	Type in the value designating the highest range in the IP address pool.
Subnet Mask	Type in the value designating the subnet mask for the IP address pool.
Gateway	Type in the value designating the gateway for the IP address pool.
DNS	Type in the value designating the DNS for the IP address pool.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Global Information** settings are informational only: Lease Time, Low IP Address, High IP Address, Subnet Mask, Gateway, DNS, and **Clear** (click to clear IP pool).

Global Information	
Information Name	Information Value
Lease time	86400 sec
Low IP Address	0.0.0.0
High IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
DNS	0.0.0.0
Clear IP Pool	<input type="button" value="Clear"/>

## Port Settings

The Port Settings page allows you to configure selected ports for the DHCP function.

To access this page, click **Management > DHCP Server > Port Settings**.

Figure 4.94 Management > DHCP Server > Port Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Click the drop-down menu to select a pre-defined port to configure. The sub options are designated for the selected port.
Low IP Address	Type in the value designating the lowest range in the IP address pool.
High IP Address	Type in the value designating the highest range in the IP address pool.
Subnet Mask	Type in the value designating the subnet mask for the IP address pool.
Gateway	Type in the value designating the gateway for the IP address pool.
DNS	Type in the value designating the DNS for the IP address pool.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Port Information** settings are informational only: Port, Low IP Address, High IP Address, Subnet Mask, Gateway, DNS, **Edit** (click to modify the settings), and **Clear** (click to clear the settings).

Port Information						
Port	Low IP Address	High IP Address	Subnet Mask	Gateway	DNS	Modify
GE1	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Edit Clear
GE2	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Edit Clear
GE3	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Edit Clear

## VLAN Settings

The VLAN Settings page allows you to configure VLAN function.

To access this page, click **Management > DHCP Server > VLAN Settings**.

The screenshot shows the 'VLAN Settings' configuration interface. At the top, there is a gear icon and the title 'VLAN Settings'. Below the title, the 'Entry' is set to '1' in a dropdown menu. The 'VLAN ID' field is labeled 'Input VLAN ID' and has a range of '(1-4094)'. Below this are several input fields: 'Low IP Address' (Input low IP), 'High IP Address' (Input high IP), 'Subnet Mask' (Input subnet mask), 'Gateway' (Input gateway), and 'DNS' (Input DNS). At the bottom of the form is a blue 'Apply' button.



The following table describes the items in the previous figure.

Item	Description
Entry	Click the drop-down menu to select a pre-defined entry to configure.
VLAN ID	Type in the value designating the ID (1 - 4094)
Low IP Address	Type in the value designating the highest range in the IP address pool.
High IP Address	Type in the value designating the lowest range in the IP address pool.
Subnet Mask	Type in the value designating the subnet mask for the IP address pool.
Gateway	Type in the value designating the gateway for the IP address pool.
DNS	Type in the value designating the DNS for the IP address pool.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Port Information** settings are informational only: Entry, VLAN ID, Low IP Address, High IP Address, Subnet Mask, Gateway, DNS, **Edit** (click to modify the settings), and **Clear** (click to clear the settings).

Entry Information	
Information Name	Information Value
Entry ID	1
VLAN ID	0
Low IP Address	0.0.0.0
High IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
DNS	0.0.0.0
Modify	<input type="button" value="Edit"/> <input type="button" value="Clear"/>

## Option 82 Settings

The Option 82 Settings, also known as the DHCP relay agent information option, provides information about the network location of a DHCP client. In turn, the DHCP server uses the information to implement IP addresses or other parameters for the client.

To access this page, click **Management > DHCP Server > Option 82 Settings**.

Figure 4.95 Management > DHCP Server > Option 82 Settings

The following table describes the items in the previous figure.

Item	Description
Entry	Click the drop-down menu to select an entry for the Option 82 setting.
Circuit ID Format	Click the drop-down menu to select the format of the circuit ID: string or hex.
Circuit ID Content	Enter the circuit ID string on the switch on which the request was received.
Remote ID Format	Click the drop-down menu to select the format of the remote ID: string or hex.
Remote ID Content	Enter the remote ID string of the host.
Low IP Address	Type in the value designating the lowest range in the IP address pool.
High IP Address	Type in the value designating the highest range in the IP address pool.
Subnet Mask	Type in the value designating the subnet mask for the IP address pool.
Gateway	Type in the value designating the gateway for the IP address pool.
DNS	Type in the value designating the DNS for the IP address pool.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Entry Information** settings are informational only: **Entry** (click the dropdown menu to select an entry), Entry ID, Circuit ID Format, Circuit ID Content, Remote ID Format, Remote ID Content, Low IP Address, High IP Address, Subnet Mask, Gateway, DNS, **Edit** (click to modify the settings), and **Clear** (click to clear the settings).

Entry :

Entry Information	
Information Name	Information Value
Entry ID	1
Circuit ID Format	String
Circuit ID Content	
Remote ID Format	String
Remote ID Content	
Low IP Address	0.0.0.0
High IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
DNS	0.0.0.0
Modify	<input type="button" value="Edit"/> <input type="button" value="Clear"/>

### Lease Entry

To access this page, click **Management > DHCP Server > Lease Entry**.

The ensuing table for **Lease entry Table** settings are informational only: IP Address, Client Mac, Start Time, End Time, and Type.

IP Address	Client Mac	Start Time	End Time	Type
No Message				

## 4.54 SMTP Client

Simple Mail Transfer Protocol (SMTP) is a protocol to send e-mail messages between servers. SMTP is used to send messages from a mail client to a mail server. SMTP by default uses TCP Port 25.

### Global Settings

The Global Settings page allows you to set the active profile for the SMTP client. To access this page, click **Management > SMTP Client > Global Settings**.



Figure 4.96 Management > SMTP Client > Global Settings

The following table describes the items in the previous figure.

Item	Description
Active Profile	Click the drop-down menu to select the profile status (None, 1 or 2).
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **SMTP Information** settings are informational only: Active Profile Id.

SMTP Information	
Information Name	Information Value
Active Profile Id	None

### Profile Settings

The Profile Settings page allows you to select the server IP, the server port, and sender mail for the listed profile.

To access this page, click **Management > SMTP Client > Profile Settings**.



Figure 4.97 Management > SMTP Client > Profile Settings > Profile Settings

The following table describes the items in the previous figure.

Item	Description
Profile ID	Click the drop-down menu to select the identification type for the profile (1 or 2).
Server IP	Enter the IP address to designate the server host.
Server Port	Enter the port number to designate the port associated with the server IP address.

Sender Mail	Enter the email address of the sender client.
Apply	Click <b>Apply</b> to save the values and update the screen.



Figure 4.98 Management > SMTP Client > Profile Settings > Profile Target Mail Settings  
 The following table describes the items in the previous figure.

Item	Description
Profile ID	Click the drop-down menu to select the identification type for the profile (1 or 2).
Target Mail	Enter the email address of the target client.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Profile Information** settings are informational only: **Profile ID** (click the drop-down menu to select a profile ID), Server IP, Server Port, and Sender Mail Address.

Profile ID : <input type="text" value="1"/>		
Profile Information		
Information Name	Information Value	Delete
Profile ID	1	
Server IP	0.0.0.0	
Server Port	25	
Sender Mail Address		

### Sending Message

The Sending Message page allows you to setup the log message for use with the SMTP client. To access this page, click **Management > SMTP Client > Sending Message**.

Figure 4.99 Management > SMTP Client > Sending Message

The following table describes the items in the previous figure.

Item	Description
Title	Assign the title of the email. The maximum length is 20 characters (alphanumeric, symbols, dots, underlines, dashes, and spaces).
Content	Assign the content of the email. The maximum length is 64 characters (alphanumeric, symbols, dots, underlines, dashes, and spaces).
Apply	Click <b>Apply</b> to save the values and update the screen.

## 4.55 RMON

Remote monitoring (RMON) uses a client-server model to monitor/manage remote devices on a network.

### RMON Statistics

The RMON Statistics page allows you to view information regarding packet sizes and information for physical layer errors. The information displayed is according to the RMON standard. To access this page, click **Management > RMON > RMON Statistics**.

Figure 4.100 Management > RMON > Rmon Statistics

The following table describes the items in the previous figure.

Item	Description
Index	Enter an entry selection (1 to 65535) to display its statistical information.
Port	Enter the respective port number for the selected entry.
Owner	Enter the name of the owner of the RMON group.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Statistics Information** settings are informational only: Index, Port, Drop Events, Octets, Packets, Broadcast, Multicast, Owner, and **Delete** (click to delete the desired index).

### RMON History

The RMON History page allows you to configure the display of history entries.

To access this page, click **Management > RMON > RMON History**.

Figure 4.101 Management > RMON > RMON History

The following table describes the items in the previous figure.

Item	Description
Index	Enter the index entry (1 to 65535) to select the number of new history table entries.
Port	Select the specific port switch.
Buckets Requested	Enter the specific (1-50) number of samples to store.
Interval	Enter value in seconds (1 to 3600) to designate a specific interval time for the collection of samples.
Owner	Enter the name of the owner of the RMON history group.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **History Information** settings are informational only: Index, Port, Buckets Requested, Interval, Owner, and **Delete** (click to delete the desired index).

History Information					
Index	Port	Buckets Requested	Interval	Owner	Action

## RMON Alarm

The RMON Alarm page allows you to configure RMON statistics group and alarm groups.

To access this page, click **Management > RMON > RMON Alarm**.

Figure 4.102 Management > RMON > Rmon Alarm



The following table describes the items in the previous figure.

Item	Description
Index	Enter the index entry (1 to 65535) to define a specific Alarm Collection history entry.
Interval	Enter a value (1 to 2147483647) to define the interval value for the Alarm Collection history.
Variable	Enter the alarm variables to define the monitoring triggers.
Sample Type	Enter the variable sample type.
Rising Threshold	Enter the rising alarm threshold trigger.
Falling Threshold	Enter the falling alarm threshold trigger.
Rising Event Index	Enter the rising event index (1-65535) to define the alarm group.
Falling Event Index	Enter the falling event index (1-65535) to define the alarm group.
Owner	Enter the name of the owner of the RMON alarm group.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Alarm Information** settings are informational only: Index, Interval, Variable, Sample Type, Rising Threshold, Falling Threshold, Rising Event Index, Falling Event Index, Owner and **Delete** (click to delete the desired index).

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

## RMON Event

The RMON Event page is used to configure RMON event groups.

To access this page, click **Management > RMON > RMON Event**.

RMON Event Control Settings

Index:  (1-65535)

Description:

Type:

Community:

Owner:

Figure 4.103 Management > RMON > RMON Event

The following table describes the items in the previous figure.

Item	Description
Index	Enter the index entry (1 to 65535) to define a specific RMON event.
Description	Enter a value (1 to 2147483647) to define the interval value for the Alarm Collection history.
Type	Click the drop-down menu to define the event type: None, Log, SNMP Trap, Log, and Trap.
Community	Enter the community string to be passed for the specified event.
Owner	Enter the name of the owner of the RMON event.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Event Information** settings are informational only: Index, Description, Type, Community, Owner, and **Delete** (click to delete the desired index).

Index	Description	Type	Community	Owner	Action
-------	-------------	------	-----------	-------	--------

## 4.56 Diagnostics

Through the Diagnostics function, configuration of settings for the switch diagnostics is available.

## 4.57 Cable Diagnostics

The Cable Diagnostics page allows you to select the port for applying a copper test. To access this page, click **Diagnostics > Cable Diagnostics**.

Figure 4.104 Diagnostics > Cable Diagnostics

Item	Description
Port	Click the drop-down menu to select a pre-defined port for diagnostic testing. Gigabit ports are displayed with a channel A to D designation.
Copper Test	Click <b>Copper Test</b> to display the test result for the selected port.

The ensuing table for **Test Result** settings are informational only: Port, Channel A, Cable Length A, Channel B, Cable Length B, Channel C, Cable Length C, Channel D and Cable Length D.

Port	Channel A	Cable Length A	Channel B	Cable Length B	Channel C	Cable Length C	Channel D	Cable Length D
GE1	[Open]	1.75 (m)	[Open]	1.80 (m)	[Open]	1.76 (m)	[Open]	1.75 (m)

## 4.58 Ping Test

The Ping Test page allows you to configure the test log page.

To access this page, click **Diagnostics > Ping Test**.

Figure 4.105 Diagnostics > Ping Test

The following table describes the items in the previous figure.

Item	Description
IP Address	Enter the IP address or host name of the station to ping. The initial value is blank. The IP Address or host name you enter is not retained across a power cycle. Host names are composed of series of labels concatenated with periods. Each label must be between 1 and 63 characters long, maximum of 64 characters.
Count	Enter the number of echo requests to send. The default value is 4. The value ranges from 1 to 5. The count entered is not retained across a power cycle.
Interval (in sec)	Enter the interval between ping packets in seconds. The default value is 1. The value ranges from 1 to 5. The interval entered is not retained across a power cycle.
Size (in bytes)	Enter the size of ping packet. The default value is 56. The value ranges from 8 to 5120. The size entered is not retained across a power cycle.
Ping Results	<p>Display the reply format of ping.                      PING 172.17.8.254 (172.17.8.254): 56 data bytes</p> <p>--- 172.17.8.254 ping statistics ---                      4 packets transmitted, 0 packets received, 100% packet loss                      Or                      PING 172.17.8.93 (172.17.8.93): 56 data bytes                      64 bytes from 172.17.8.93: icmp_seq=0 ttl=128 time=0.0ms                      64 bytes from 172.17.8.93: icmp_seq=1 ttl=128 time=0.0ms                      64 bytes from 172.17.8.93: icmp_seq=2 ttl=128 time=0.ms                      64 bytes from 172.17.8.93: icmp_seq=3 ttl=128 time=0.0ms</p> <p>--- 172.17.8.93 ping statistics ---                      4 packets transmitted, 4 packets received, 0% packet loss                      round-trip min/avg/max = 0.0/0.0/0.0ms</p>
Apply	Click <b>Apply</b> to display ping result for the IP address.

## 4.59 IPv6 Ping Test

The IPv6 Ping Test page allows you to configure the Ping Test for IPv6. To access this page, click **Diagnostics > IPv6 Ping Test**.

IPv6 Ping Test

IPv6 Address  (XX:XX::XX:XX)

Count  ( 1 - 5 | Default : 4 )

Interval (in sec)  ( 1 - 5 | Default : 1 )

Size (in bytes)  ( 8 - 5120 | Default : 56 )

Ping Results

Figure 4.106 Diagnostics > IPv6 Ping Test

Item	Description
IPv6 Address	Enter the IP address or host name of the station you want the switch to ping. The initial value is blank. The IP Address or host name you enter is not retained across a power cycle. Host names are composed of a series of labels concatenated with dots. Each label must be between 1 and 63 characters long, and the entire hostname has a maximum of 64 characters.
Count	Enter the number of echo requests you want to send. The default value is 4. The value ranges from 1 to 5. The count you enter is not retained across a power cycle.
Interval (in sec)	Enter the interval between ping packets in seconds. The default value is 1. The value ranges from 1 to 5. The interval you enter is not retained across a power cycle.
Size (in bytes)	Enter the size of ping packet. The default value is 56. The value ranges from 8 to 5120. The size you enter is not retained across a power cycle.
Ping Results	<p>Display the reply format of ping.                      PING 2222::777 (2222::777): 56 data bytes</p> <p>--- 2222::777 ping statistics ---                      4 packets transmitted, 0 packets received, 100% packet loss                      Or                      PING 2222::717 (2222::717): 56 data bytes                      64 bytes from 2222::717: icmp6_seq=0 ttl=128 time=10.0ms                      64 bytes from 2222::717: icmp6_seq=1 ttl=128 time=0.0ms                      64 bytes from 2222::717: icmp6_seq=2 ttl=128 time=0.0ms                      64 bytes from 2222::717: icmp6_seq=3 ttl=128 time=0.0ms</p> <p>--- 2222::717 ping statistics ---                      4 packets transmitted, 4 packets received, 0% packet loss                      round-trip min/avg/max = 0.0/2.5/10.0ms</p>
Apply	Click <b>Apply</b> to display ping result for the IP address.

## 4.60 System Log

### Logging Service

The Logging Service page allows you to setup the logging services feature for the system log.

To access this page, click **Diagnostics > System Log > Logging Service**.

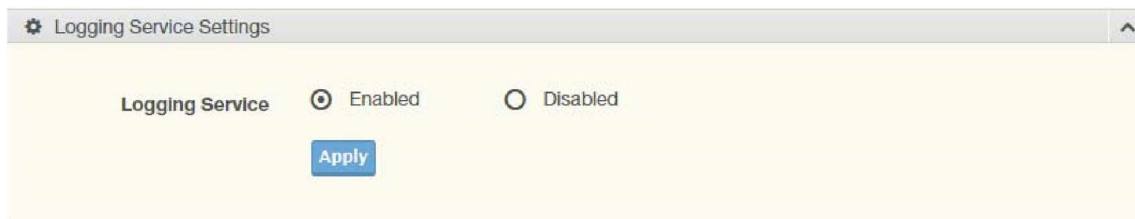


Figure 4.107 Diagnostics > System Log > Logging Service

The following table describes the items in the previous figure.

Item	Description
Logging Service	Click <b>Enabled</b> or <b>Disabled</b> to set the Logging Service status.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Logging Information** settings are informational only: Logging Service.

Logging Information	
Information Name	Information Value
Logging Service	enabled

### Local Logging

The Local Logging page allows you to designate a local target when the severity criteria is reached.

To access this page, click **Diagnostics > System Log > Local Logging**.



Figure 4.108 Diagnostics > System Log > Local Logging

The following table describes the items in the previous figure.

Item	Description
Target	Enter the local logging target.
Severity	<p>Click the drop-down menu to select the severity level for local log messages. The level options are:</p> <ul style="list-style-type: none"> <li>● emerg: Indicates system is unusable. It is the highest level of severity</li> <li>● alert: Indicates action must be taken immediately</li> <li>● crit: Indicates critical conditions</li> <li>● error: Indicates error conditions</li> <li>● warning: Indicates warning conditions</li> <li>● notice: Indicates normal but significant conditions</li> <li>● info: Indicates informational messages</li> <li>● debug: Indicates debug-level messages</li> </ul>
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Local Logging Settings Status** settings are informational only: Status, Target, Severity, and **Delete** (click to delete the desired target).

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

### System Log Server

The System Log Server page allows you to configure the log server.

To access this page, click **Diagnostics > System Log > System Log Server**.

The screenshot shows the 'Remote Logging Settings' configuration page. It contains the following fields and values:

- Server Address:** input server
- Server Port:** 514 (with a note '(1-65535)')
- Severity:** emerg (selected from a dropdown menu)
- Facility:** local0 (selected from a dropdown menu)
- Apply:** A blue button to save the settings.

Figure 4.109 Diagnostics > System Log > System Log Server

Item	Description
Server Address	Enter the IP address of the log server.
Server Port	Enter the Udp port number of the log server.
Severity	<p>Click the drop-down menu to select the severity level for local log messages. The default is emerg. The level options are:</p> <ul style="list-style-type: none"> <li>● emerg: Indicates system is unusable. It is the highest level of severity</li> <li>● alert: Indicates action must be taken immediately</li> <li>● crit: Indicates critical conditions</li> <li>● error: Indicates error conditions</li> <li>● warning: Indicates warning conditions</li> <li>● notice: Indicates normal but significant conditions</li> <li>● info: Indicates informational messages</li> <li>● debug: Indicates debug-level messages</li> </ul>
Facility	Click the drop-down menu to select facility to which the message refers.
Apply	Click <b>Apply</b> to save the values and update the screen.



The ensuing table for **Remote Logging Setting Status** settings are informational only: Status, Server Info, Severity, Facility and **Delete** (click to delete the desired server address).

Remote Logging Setting Status				
Status	Server Info	Severity	Facility	Action

## 4.61 DDM

The DDM page allows you to setup the diagnostic alarm status.

To access this page, click **Diagnostics > DDM**.



Figure 4.110 Diagnostics > DDM

The following table describes the items in the previous figure.

Item	Description
Diagnostic Alarm	Click the drop-down menu to designate the announcement method: Disabled, SysLog, E-mail, or SNMP.
Apply	Click <b>Apply</b> to save the values and update the screen.

The ensuing table for **Diagnostic Alarm Information** settings are informational only: Diagnostic Alarm.

Diagnostic Alarm Information	
Diagnostic Alarm Information	Diagnostic Alarm Information
Diagnostic Alarm	Disabled

DMI Info				
GE9	High Alarm	High Warning	Low Alarm	Low Warning
Temperature	95.000 °C <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	90.000 °C <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	-50.000 °C <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	-45.000 °C <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Voltage	3.500 V <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	3.450 V <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	3.100 V <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	3.150 V <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
TX Basis	100.000 mA <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	90.000 mA <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	6.000 mA <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	7.000 mA <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
TX Power	-1.000 dbm <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	-5.000 dbm <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	-35.000 dbm <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	-30.000 dbm <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
RX Power	-1.000 dbm <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	-5.000 dbm <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	-35.000 dbm <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	-30.000 dbm <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
<input type="button" value="Apply"/>				

Figure 4.111 Diagnostics > DDM

The following table describes the items in the previous figure.

Item	Description
High Alarm	Click <b>Enabled</b> or <b>Disabled</b> to set the alarm state.
High Warning	Click <b>Enabled</b> or <b>Disabled</b> to set the alarm state.
Low Alarm	Click <b>Enabled</b> or <b>Disabled</b> to set the alarm state.
Low Warning	Click <b>Enabled</b> or <b>Disabled</b> to set the alarm state.
Apply	Click <b>Apply</b> to save the values and update the screen.

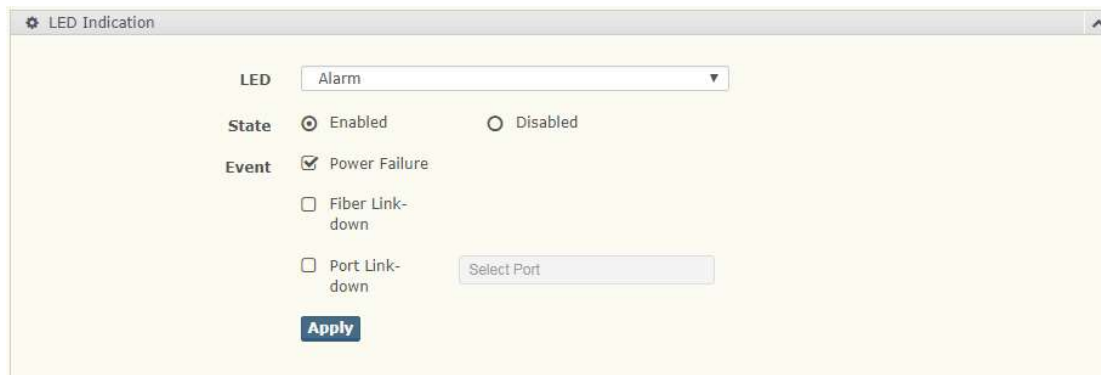
The ensuing table for **Vendor Info** settings are informational only: **Refresh** (click to reload the vendor information), Port, Connector, Speed, VendorName, VendorOui, VendorPn, VendorRev, VendorSn, and DateCode.

Vendor Info							
Port	Connector	Speed	VendorName	VendorPn	VendorRev	VendorSn	DateCode

## 4.62 LED Indication

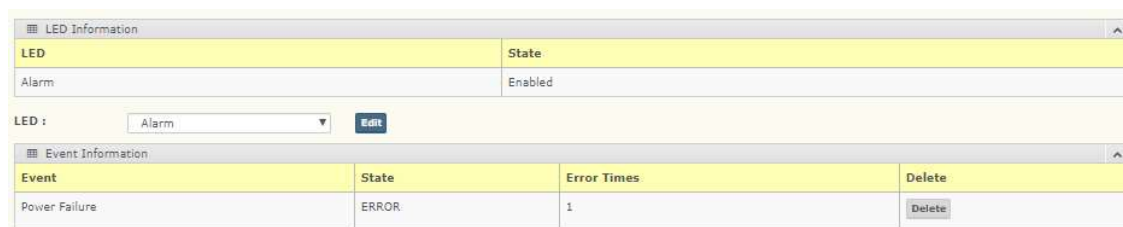
The LED Indication page allows you to setup the LED indication.

To access this page, click **Diagnostics > LED Indication**.



The following table describes the items in the previous figure.

Item	Description
LED	Alarm is selected by default.
State	Click <b>Enabled</b> or <b>Disabled</b> to set the alarm state.
Event	Click <b>Power Failure</b> , <b>Fiber Link down</b> , or <b>Port Link down</b> to set the alarm event.
Apply	Click <b>Apply</b> to save the values and update the screen.



## 4.63 Tools

## 4.64 Backup Manager

The Backup Manager page allows you to configure a remote TFTP sever or host file system in order to back up the firmware image or configuration file. To access this page, click **Tools > Backup Manager**.

Figure 4.113 Tools > Backup Manager

The following table describes the items in the previous figure.

Item	Description
Backup Method	Click the drop-down menu to select the backup method: TFTP or HTTP.
Server IP	Enter the IP address of the backup server.
Backup Type	Click a type to define the backup method: image, running configuration, startup configuration, flash log, or buffered log.
Image	Click the format for the image type: LNP-2804GN-SFP-T-x-xx-xx.hex (Active) or LNP-2804GN-SFP-T-x-xx-xx.hex (backup).
Backup	Click <b>Backup</b> to back up the settings.

## 4.65 Upgrade Manager

The Upgrade Manager page allows you to configure a remote TFTP sever or host file system in order to upload firmware upgrade images or configuration files. To access this page, click **Tools > Upgrade Manager**.

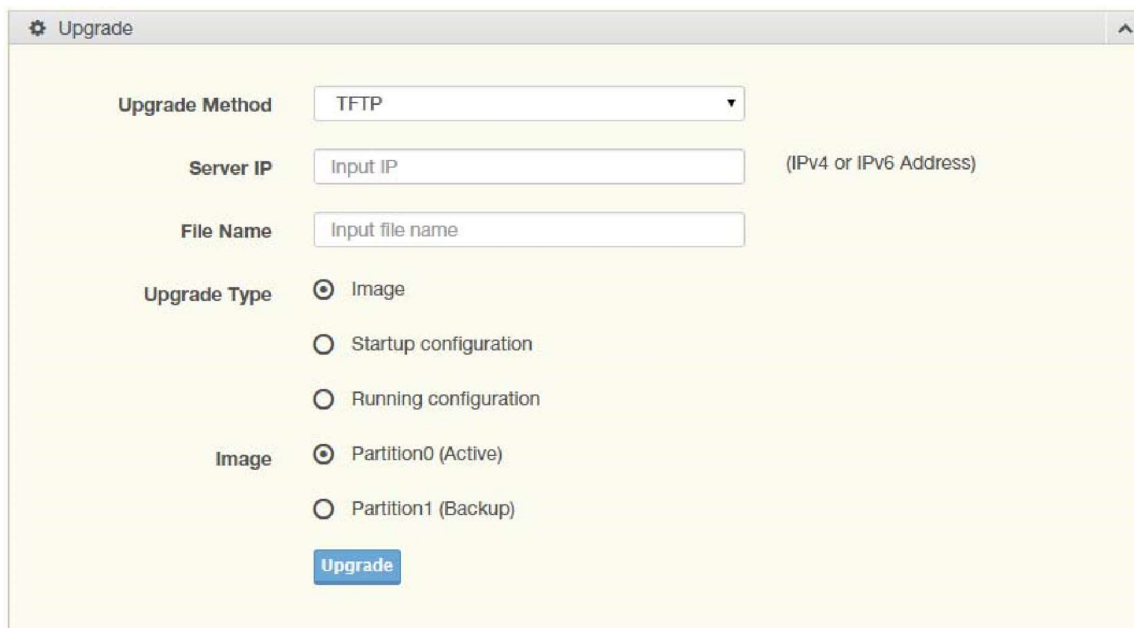


Figure 4.114 Tools > Upgrade Manager

The following table describes the items in the previous figure.

Item	Description
Upgrade Method	Click the drop-down menu to select the upgrade method: TFTP or HTTP.
Server IP	Enter the IP address of the upgrade server.
File Name	Enter the file name of the new firmware version.
Upgrade Type	Click a type to define the upgrade method: image, startup configuration, or running configuration.
Image	Click the format for the image type: LNP-2804GN-SFP-T-x-xx-xx.hex (Active) or LNP-2804GN-SFP-T-x-xx-xx.hex (backup).
Upgrade	Click <b>Upgrade</b> to upgrade to the current version.

## 4.66 Dual Image

The Dual Image page allows you to setup an active and backup partitions for firmware image redundancy.

To access this page, click **Tools > Dual Image**.



Figure 4.115 Tools > Dual Image

Item	Description
Active Image	Click the format for the image type: LNP-2804GN-SFP-T-x-xx-xx.hex (Active) or LNP-2804GN-SFP-T-x-xx-xx.hex (backup).
Save	Click <b>Save</b> to save and keep the new settings.

The ensuing table for **Image Information 0/1** settings are informational only: Flash Partition, Image Name, Image Size and Created Time.

Images Information 0	
<b>LNP-2804GN-SFP-T-1-00-02.hex</b>	<b>Active</b>
Flash Partition	0
Image Name	LNP-2804GN-SFP-T-1-00-02.hex
Image Version	1.00.02
Image Size	9139311 Bytes
Created Time	2017-06-21 10:31:24 UTC
Images Information 1	
<b>Partition1</b>	<b>Backup</b>
Flash Partition	1
Image Name	
Image Version	1.00.85_1220
Image Size	9757869 Bytes
Created Time	2016-12-20 14:49:14 UTC

## 4.67 Save Configuration

To access this page, click **Tools > Save Configuration**.

Click **Save Configuration to FLASH** to have configuration changes you have made to be saved across a system reboot. All changes submitted since the previous save or system reboot will be retained by the switch.

## 4.68 User Account

The User Account page allows you to setup a user and the related parameters. To access this page, click **Tools > User Account**.

Figure 4.116 Tools > User Account

The following table describes the items in the previous figure.

Item	Description
User Name	Enter the name of the new user entry.
Password Type	Click the drop-down menu to define the type of password: <b>Clear Text</b> , <b>Encrypted</b> , or <b>No Password</b> .
Password	Enter the character set for the define password type.
Retype Password	Retype the password entry to confirm the profile password.
Privilege Type	Click the drop-down menu to designate privilege authority for the user entry: <b>Admin</b> or <b>User</b> .
Apply	Click <b>Apply</b> to create a new user account.

The ensuing table for **Local Users** settings are informational only: User Name, Password Type, Privilege Type and **Delete** (click to delete the desired user account).

User Name	Password Type	Privilege Type	Modify
superuser	Encrypted		
root	Encrypted	Admin	Delete
test	Clear Text	User	Delete

## 4.69 Reset System

To access this page, click **Tools > Reset System**.

Click **Restore** to have all configuration parameters reset to their factory default values. All changes that have been made will be lost, even if you have issued a save. Reset settings take effect after a system reboot.

## 4.71 Reboot Device

To access this page, click **Tools > Reboot Device**.

Click **Reboot** to reboot the switch. Any configuration changes you have made since the last time you issued a save will be lost.

# 5. Command Line Interface Management

## 5.1 About CLI Management

Besides WEB-based management, LMP-1204G-SFP series also supports CLI management.

Users can use console or telnet to management switch by CLI.

### CLI Management by RS-232 Serial Console (115200, 8, none, 1, none)

Before configuring by an RS-232 serial console, use an RJ45 to DB9-F cable to connect the switches' RS-232 Console port to the PC's COM port.

Suggested product to connect via serial cable:

Hyperterminal – on older windows machines

Putty – Free download on the internet

A successful connection via the serial cable will look like this: (default username and password is {admin/admin})

```
User Access Verification
Username: admin
Password:

SWES> en

SWES# configure terminal
```

### CLI Management by Telnet

Users can use “TELNET” to configure the switches.

The default value is as below:

- IP Address: **192.168.1.254**
- Subnet Mask: **255.255.255.0**

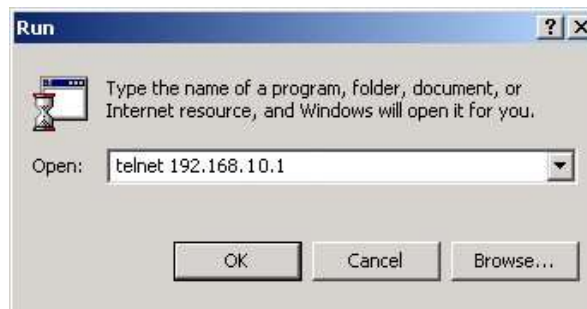


- Default Gateway: none
- User Name: **admin**
- Password: **admin**

Follow the steps below to access the console via Telnet.

**Step 1:**

Telnet to the IP address of the switch from the Windows “**Run**” command as below.



Note: Telnet may not be installed by default on some windows systems.

**Step 2:**

The Login screen will appear. Use the keyboard to enter the Username and Password, and then press “**Enter**”

```
User Access Verification
Username: admin
Password:

SWES> en

SWES# configure terminal
```

**Commander Groups**

Group	Command	Mode
System	hostname [Switch]	configure
	no hostname	configure
	system location [none]	configure
	system contact [none]	configure
	no system location	configure
	no system contact	configure
	show system uptime	configure

	show system mac	configure
	show system version firmware	configure
	show system version loader	configure
	admin username admin	configure
	admin password admin	configure
<b>IP</b>	boot host dhcp	configure
	ip address [ip_addr] [ip_mask]	configure
	ip default-gateway [ip_router]	configure
	ip name-server [ip_addr_string]	configure
	no boot host dhcp	configure
	no ip default-gateway	configure
	no ip name-server	configure
	show boot host dhcp	configure
	show ip address	configure
	show ip default-gateway	configure
	show ip name-server	configure
	show ip mode	configure
<b>Time</b>	ntp time update	configure
	ntp client timeserver [ip_addr_string]	configure
	clock set [hh:mm:ss] [day] [month] [year]	configure
	clock timezone [area] [city]	configure
	ntp client sync[minute   hour   day   month   year] [NUMBER]	configure
	no ntp client timeserver	configure
	no clock timezone	configure
<b>Time</b>	no ntp client sync[minute   hour   day   month   year] [NUMBER]	configure
	show ntp client timeserver	configure
	show clock timezone	configure
	show ntp client sync[minute   hour   day   month   year] [NUMBER]	configure
<b>Port</b>	speed [auto   10   100   1000] [full   half]	interface
	Duplex [auto   full   half]	interface
	flowcontrol <receive> [on   off   desired]	interface
	name [string]	interface
	shutdown	interface
	no speed	interface
	no duplex	interface
	no flowcontrol	interface

	no name	interface
	no shutdown	interface
	show speed	interface
	show duplex	interface
	show flow control	interface
	show name	interface
	show link rx	interface
	show link tx	interface
	show link summary	interface
<b>VLAN</b>	management vlan [vlan_id]	configure
	name [vlan_name]	vlan
	member [member_portlist] [<untag_portlist>]	vlan
	switchport pvid [vlan_id]	interface
	switchport filter [tagged   untagged]	interface
	no name	vlan
	no member	vlan
	no switchport pvid	interface
	no switchport filter	interface
	show name	vlan
	show member	vlan
	show switchport pvid	interface
show switchport filter	interface	
<b>PoE</b>	power inline never	interface
	keepalive ip [IP_Address]	interface
	keepalive time [Seconds]	interface
	schedule [monday~sunday] enable	interface
	schedule [monday~sunday] start time [Hour]	interface
	schedule [monday~sunday] end time [Hour]	interface
	no power inline never	interface
	no keepalive ip	interface
	no keepalive time	interface
	no schedule [monday~sunday] enable	interface
	no schedule [monday~sunday] start time	interface
	no schedule [monday~sunday] end time	interface
show power inline status	interface	
show keepalive ip	interface	

	show keepalive time	interface
	show schedule [monday~sunday] enable	interface
	show schedule [monday~sunday] start time	interface
	show schedule [monday~sunday] end time	interface
<b>STP</b>	spanning-tree mode [rstp   mst]	configure
	spanning-tree priority [priority_value]	configure
	spanning-tree forward-time [ forward time]	configure
	spanning-tree hello-time [hello_time]	configure
	spanning-tree max-age [max_age]	configure
	spanning-tree cost [link_cost_value]	interface
	spanning-tree port-priority [port_priority]	interface
	spanning-tree link-type [point-to-point   point-to-multiple]	interface
	spanning-tree auto-edge off	interface
	spanning-tree admin-edge on	interface
	spanning-tree stp disable	interface
	no spanning-tree mode	configure
	no spanning-tree priority	configure
	no spanning-tree forward-time	configure
	no spanning-tree hello-time	configure
	no spanning-tree max-age	configure
	no spanning-tree mst [instance_ID] priority	configure
	no spanning-tree cost	interface
	no spanning-tree port-priority	interface
	no spanning-tree link-type	interface
no spanning-tree auto-edge	interface	
no spanning-tree admin-edge	interface	
no spanning-tree stp	interface	
<b>STP</b>	show spanning-tree mode	configure
	show spanning-tree priority	configure
	show spanning-tree forward-time	configure
	show spanning-tree hello-time	configure
	show spanning-tree max-age	configure
	show spanning-tree cost	interface
	show spanning-tree port-priority	interface
	show spanning-tree link-type	interface
	show spanning-tree auto-edge	interface

	show spanning-tree admin-edge	interface
	show spanning-tree stp	interface
	spanning-tree mst [instance_ID] priority [priority]	configure
	spanning-tree mst name [NAME]	configure
	spanning-tree mst revision [REVISION]	configure
	spanning-tree mst instance [instance_ID] vlan [vlan_grp]	configure
	spanning-tree mst [instance_ID] cost [cost_value]	interface
	spanning-tree mst [instance_ID] port-priority [priority]	interface
	no spanning-tree mst name	configure
	no spanning-tree mst revision	configure
	no spanning-tree mst instance [instance_ID] vlan	configure
	no spanning-tree mst [instance_ID] cost	interface
	no spanning-tree mst [instance_ID] port-priority	interface
	show spanning-tree mst name	configure
	show spanning-tree mst revision	configure
	show spanning-tree mst instance [instance_ID] vlan	configure
	show spanning-tree mst [instance_ID] priority	configure
	show spanning-tree mst [instance_ID] cost	interface
	show spanning-tree mst [instance_ID] port-priority	interface
<b>Event</b>	event smtp power1 enable	configure
	event smtp power2 enable	configure
	event smtp cold-start enable	configure
	event smtp warm-start enable	configure
	event smtp authentication-failure enable	configure
	event smtp interface [INTERFACE_NAME] up	configure
	event smtp interface [INTERFACE_NAME] down	configure
	no event smtp power1	configure
	no event smtp power2	configure
	no event smtp cold-start	configure
	no event smtp warm-start	configure
	no event smtp authentication-failure	configure
	no event smtp interface [INTERFACE_NAME] up	configure
	no event smtp interface [INTERFACE_NAME] down	configure
	show event smtp power1	configure
	show event smtp power2	configure
	show event smtp cold-start	configure

	show event smtp warm-start	configure
	show event smtp authentication-failure	configure
	show event smtp interface [INTERFACE_NAME] up	configure
	show event smtp interface [INTERFACE_NAME] down	configure
	event syslog power1 enable	configure
	event syslog power2 enable	configure
	event syslog cold-start enable	configure
	event syslog warm-start enable	configure
	event syslog authentication-failure enable	configure
	event syslog interface [INTERFACE_NAME] up	configure
	event syslog interface [INTERFACE_NAME] down	configure
	no event syslog power1	configure
	no event syslog power2	configure
	no event syslog cold-start	configure
	no event syslog warm-start	configure
	no event syslog authentication-failure	configure
	no event syslog interface [INTERFACE_NAME] up	configure
	no event syslog interface [INTERFACE_NAME] down	configure
	show event syslog power1	configure
	show event syslog power2	configure
	show event syslog cold-start	configure
	show event syslog warm-start	configure
	show event syslog authentication-failure	configure
	show event syslog interface [INTERFACE_NAME] up	configure
	show event syslog interface [INTERFACE_NAME] down	configure
	event alarm power1 enable	configure
	event alarm power2 enable	configure
	event alarm interface [INTERFACE_NAME] down	configure
	no event alarm power1	configure
	no event alarm power2	configure
	no event alarm interface [INTERFACE_NAME] down	configure
	show event alarm power1	configure
	show event alarm power2	configure
	show event alarm interface [INTERFACE_NAME] down	configure
	event apply	configure
<b>SYSLOG</b>	syslog server [IP_address]	configure

	syslog mode [all   remote   local   usb]	configure
	no syslog server	configure
	no syslog mode	configure
	show syslog server	configure
	show syslog mode	configure
	show syslog log	configure
<b>SMTP</b>	smtp enable	configure
	smtp sender [E-MAIL_ADDR]	configure
	smtp subject [subject_text]	configure
	smtp server address [GMAIL_SMPT_SERVER]	configure
	smtp server port [GMAIL_SMPT_SERVER]	configure
	smtp authentication enable	configure
	smtp authentication username [GMAIL_ACCOUNT]	configure
	smtp authentication password [GMAIL_PASS]	configure
	smtp receive [1   2   3   4] [e-mail_address]	configure
	no smtp enable	configure
	no smtp sender	configure
	no smtp subject	configure
	no smtp server address	configure
	no smtp server port	configure
	no smtp authentication enable	configure
	no smtp authentication username	configure
	no smtp authentication password	configure
	no smtp receive [1   2   3   4]	configure
	show smtp state	configure
	show smtp sender	configure
	show smtp subject	configure
show smtp server address	configure	
show smtp server port	configure	
show smtp authentication enable	configure	
show smtp authentication username	configure	
show smtp receive [1   2   3   4]	configure	
<b>SNMP</b>	snmp server enable [<v1-v2c-only   v3-only>]	configure
	snmp server community [ro   rw] [community_name]	configure
	snmp server v3 level [admin  user] [auth   noauth   priv]	configure
	snmp server v3 auth [admin   user] [md5   sha] [PWD]	configure

	snmp server v3 encryption [admin   user] [des   aes] [PWD]	configure
	no snmp server enable	configure
	no snmp server community [ro   rw]	configure
	no snmp server v3 level [admin  user]	configure
	no snmp server v3 auth [admin   user]	configure
	no snmp server v3 encryption [admin   user]	configure
	show snmp server enable	configure
	show snmp server community [ro   rw]	configure
	show snmp server v3 level [admin  user]	configure
	show snmp server v3 auth [admin   user]	configure
	show snmp server v3 encryption [admin   user]	configure
	snmp trap enable	configure
	snmp trap host [DESTINATION_IP]	configure
	snmp trap version [1   2c   3] [traps   inform]	configure
	snmp trap community [trap_community_name]	configure
	snmp trap inform retry [retry_time]	configure
	snmp trap inform timeout [retry_interval]	configure
	snmp trap v3 user [user_ID]	configure
	snmp trap v3 level [auth   noauth   priv]	configure
	snmp trap v3 engine-ID [engineID]	configure
	snmp trap v3 auth [md5   sha] [PASSWORD]	configure
	snmp trap v3 encryption [des   aes] [PASSWORD]	configure
<b>SNMP</b>	no snmp trap enable	configure
	no snmp trap host	configure
	no snmp trap version	configure
	no snmp trap community	configure
	no snmp trap inform retry	configure
	no snmp trap inform timeout	configure
	no snmp trap v3 user	configure
	no snmp trap v3 level	configure
	no snmp trap v3 engine-ID	configure
	no snmp trap v3 auth	configure
	no snmp trap v3 encryption	configure
	show snmp trap enable	configure
	show snmp trap host	configure
	show snmp trap version	configure



	show snmp trap community	configure
	show snmp trap inform retry	configure
	show snmp trap inform timeout	configure
	show snmp trap v3 user	configure
	show snmp trap v3 level	configure
	show snmp trap v3 engine-ID	configure
	show snmp trap v3 auth	configure
	show snmp trap v3 encryption	configure
<b>FILE</b>	copy running-config startup-config	configure
	copy startup-config running-config	configure
<b>PORT MIRROR</b>	monitor enable	configure
	monitor source [rx   tx   both] [port_list]	configure
	monitor destination [dest_port_number]	configure
	no monitor enable	configure
	no monitor source	configure
	no monitor destination	configure
	show monitor enable	configure
	show monitor source	configure
show monitor destination	configure	
<b>QoS</b>	qos queue-schedule [strict   wrr]	configure
	qos map cos [priority_type] to tx-queue [queue]	configure
	qos map dscp [[priority_type] to tx-queue [[queue]	configure
	qos trust [cos   dscp]	interface
	qos default cos [cos_default_value]	interface
	no qos queue-schedule	configure
	no qos map cos [priority_type]	configure
	no qos map dscp [priority_type]	configure
	no qos trust	interface
	no qos default cos	interface
	show qos queue-schedule	configure
	show qos map cos [priority_type]	configure
	show qos map dscp [priority_type]	configure
	show qos trust	interface
show qos default cos	interface	
<b>IGMP</b>	igmp snooping enable	configure
	igmp snooping query max-respond-time [1...12]	configure

	igmp snooping query interval [1...3600]	configure
	igmp snooping last-member count [2...10]	configure
	igmp snooping last-member interval [60...300]	configure
	igmp snooping querier enable	configure
	igmp snooping fast-leave enable	interface
	no igmp snooping enable	configure
	no igmp snooping query max-respond-time	configure
	no igmp snooping query interval	configure
	no igmp snooping last-member count	configure
	no igmp snooping last-member interval	configure
	no igmp snooping querier	configure
	no igmp snooping fast-leave	interface
	show igmp snooping mdb	configure
	show igmp snooping all	configure
	show igmp snooping fast-leave	interface
<b>Trunk</b>	trunk group [group] [static   lacp] [interface_list]	configure
<b>DHCP Server/Relay</b>	dhcp service server	configure
	dhcp server included-address [IP_START] [IP_END]	configure
	dhcp server default-gateway [router_ip]	configure
	dhcp server name-server [dns_ip]	configure
	dhcp server lease [dhcp_lease_time]	configure
	dhcp server binding [bind_num][MAC] [bind_IP]	configure
	dhcp server port-binding [Port] [bind_IP]	configure
	dhcp service relay	configure
	dhcp relay server [server_number] [IP]	configure
	dhcp relay information option	configure
	dhcp relay information policy [replace   keep   drop]	configure
	dhcp relay untrust	interface
	no dhcp service server	configure
	no dhcp server included-address	configure
	no dhcp server default-gateway	configure
	no dhcp server name-server	configure
	no dhcp server lease	configure
	no dhcp server binding [bind_num]	configure
	no dhcp service relay	configure
	no dhcp relay server [server_number]	configure

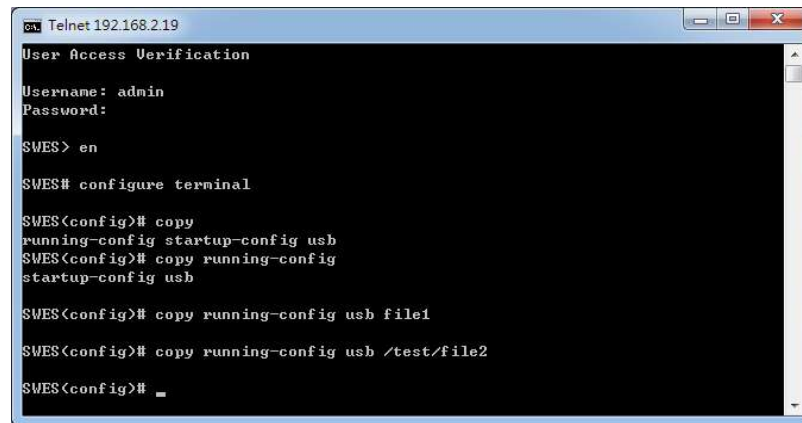
	no dhcp relay information option	configure
	no dhcp relay information policy [replace   keep   drop]	configure
	no dhcp relay untrust	configure
	show dhcp service	interface
	show dhcp server status	configure
	show dhcp server included-address	configure
	show dhcp server default-gateway	configure
	show dhcp server name-server	configure
	show dhcp server lease	configure
	show dhcp server binding [bind_num] [MAC] [bind_IP]	configure
	show dhcp relay enable	configure
	show dhcp relay server [server_number]	configure
	show dhcp relay information option	configure
	show dhcp relay information policy [replace   keep   drop]	configure
	show dhcp relay untrust	interface
<b>UPnP</b>	upnp enable	configure
	upnp advertisement interval [SEC]	configure
	no upnp enable	configure
	no upnp advertisement interval	configure
	show upnp enable	configure
	show upnp advertisement interval	configure
<b>802.1X</b>	dot1x enable	configure
	dot1x authentication server type [local   radius]	configure
	dot1x authentication server 1 ip [IP]	configure
	dot1x authentication server 1 port [PORT]	configure
	dot1x authentication server 1 share-key [KEY]	configure
	dot1x authentication server 2 ip [IP]	configure
	dot1x authentication server 2 port [PORT]	configure
	dot1x authentication server 2 share-key [KEY]	configure
	dot1x local-db [USER] [PASSWORD]	configure
	dot1x authenticator enable	interface
	dot1x reauthentication enable	interface
	dot1x reauthentication period [SEC]	interface
	no dot1x enable	configure
	no dot1x authentication server type	configure
	no dot1x authentication server 1 ip	configure

	no dot1x authentication server 1 port	configure
	no dot1x authentication server 1 share-key	configure
	no dot1x authentication server 2 ip	configure
	no dot1x authentication server 2 port	configure
	no dot1x authentication server 2 share-key	configure
	no dot1x local-db [USER] [PASSWORD]	configure
	no dot1x authenticator enable	interface
	no dot1x reauthentication enable	interface
	no dot1x reauthentication period	interface
	show dot1x enable	configure
	show dot1x authentication server type	configure
	show dot1x authentication server 1 ip	configure
	show dot1x authentication server 1 port	configure
	show dot1x authentication server 1 share-key	configure
	show dot1x authentication server 2 ip	configure
	show dot1x authentication server 2 port	configure
	show dot1x authentication server 2 share-key	configure
	show dot1x local-db [USER] [PASSWORD]	configure
	show dot1x brief	configure
	show dot1x server brief	configure
	show dot1x brief	interface
	show dot1x server brief	interface
	show dot1x authenticator enable	interface
	show dot1x reauthentication enable	interface
	show dot1x reauthentication period	interface
<b>IPv6</b>	ipv6 enable	configure
	ipv6 address add [IPV6_ADDR</PREFIX_LEN>]	configure
	ipv6 neighbor flush	configure
	ipv6 ping [IPV6_ADDR] [<size PKG_SIZ>   <repeat PKG_CNT>]	configure
	no ipv6 enable	configure
	no ipv6 address [IPV6_ADDR/PREFIX_LEN]	configure
	show ipv6 enable	configure
	show ipv6 address	configure
	show ipv6 neighbor	configure
<b>TFTP</b>	tftp upgrade	configure
	tftp server ip [IP_ADDRESS]	configure

	tftp file name [UPGRADE_FILE_NAME]	configure
--	------------------------------------	-----------

## Save and Load Configuration File to/from USB

1. CLI: enable → configure terminal → copy running-config usb (path)

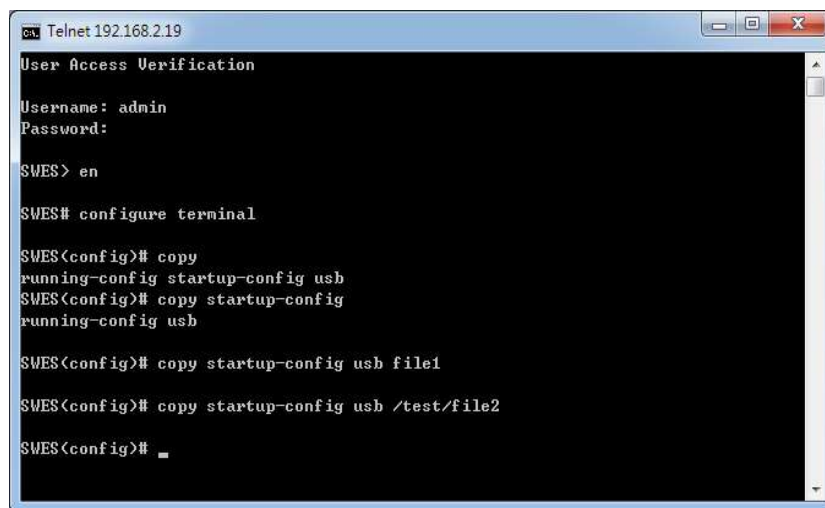


```
Telnet 192.168.2.19
User Access Verification
Username: admin
Password:
SWES> en
SWES# configure terminal
SWES(config)# copy
running-config startup-config usb
SWES(config)# copy running-config
startup-config usb
SWES(config)# copy running-config usb file1
SWES(config)# copy running-config usb /test/file2
SWES(config)# _
```

Fill in the folder and filename behind the “copy running-config usb” command.

Ex: file1, / folder /file2.

2. CLI: enable → configure terminal → copy startup-config usb (path)



```
Telnet 192.168.2.19
User Access Verification
Username: admin
Password:
SWES> en
SWES# configure terminal
SWES(config)# copy
running-config startup-config usb
SWES(config)# copy startup-config
running-config usb
SWES(config)# copy startup-config usb file1
SWES(config)# copy startup-config usb /test/file2
SWES(config)# _
```

Fill in the folder and filename behind the “copy startup-config usb” command.

Ex: file1, / folder /file2.

3. CLI: enable → configure terminal → copy usb startup-config (path)

```

Telnet 192.168.2.19
User Access Verification
Username: admin
Password:
SWES> en
SWES# configure terminal
SWES(config)# copy
running-config startup-config usb
SWES(config)# copy usb
startup-config firmware
SWES(config)# copy usb
startup-config destination file
firmware destination file
SWES(config)# copy usb startup-config file1
    
```

Fill in the folder and filename behind the “copy usb startup-config” command.

Ex: file1, / folder /file2.

### Upgrade via TFTP

- CLI: enable → configure terminal → tftp server ip [IP\_ADDRESS] → tftp file name [UPGRADE\_FILE\_NAME] → tftp upgrade

```

COM7:115200baud - Tera Term V1
File Edit Setup Control Window Help

Switch> enable
Switch# configure terminal
Switch(config)# tftp server ip 192.168.1.237
Switch(config)# tftp file name 240.dat
Switch(config)# tftp upgrade
    
```

peer	file	start time	progress	bytes
192.168.1.254	c240.dat	10.40.05	47%	3665920

240.dat to 192.168.1.254  
 File size: 7639040  
 3665920 Bytes sent 2291.20 Bytes/sec

Fill in the TFTP server IP and upgrade file name behind the “tftp server ip [IP\_ADDRESS]” and “tftp file name [UPGRADE\_FILE\_NAME]”

## 6. Technical Specifications

Table 6.1 has the technical specifications.

<b>Standards</b>	IEEE 802.3	10Base-T 10Mbit/s Ethernet
	IEEE 802.3u	100Base-Tx, 100Base-Fx, Fast Ethernet
	IEEE 802.3ab	1000Base-Tx Gigabit Ethernet
	IEEE 802.3z	Gigabit Fiber
	IEEE 802.3x	Flow Control for Full Duplex
	IEEE 802.3af	Power-over-Ethernet
	IEEE 802.3at	Power-over-Ethernet Plus (Enhanced)
	IEEE 802.3ad	Port Trunking with LACP
	IEEE 802.1d	STP (Spanning Tree Protocol)
	IEEE 802.1w	RSTP (Rapid Spanning Tree Protocol)
	IEEE 802.1s	MTP (Multiple Spanning Tree Protocol)
	IEEE 802.1q	Virtual LANs (VLAN)
	IEEE 802.1x	Port based Network Control, Authentication
	IEEE 802.1ad	Stacked VLAN, Q-in-Q
IEEE 802.1p	QoS/CoS Protocol for Traffic Prioritization	
<b>Switch</b>	Protocol	Web browser, Telnet, Serial console, TFTP, SNMPv1/v2c/v3, Port Speed/Duplex Configuration, IPv6, IEEE 802.1Q, GVRP, Port-based VLAN, X-Ring, 802.1w/D RSTP/STP, IP Access security, port security, DHCP client, Port and IP Binding, 802.1X Port Access Control
	Data Process	Store-and-Forward
	Packet Buffer	4.1 Mbits
	MAC Table	8k
	Jumbo Frame	9216bytes
	Flow Control	IGMP Snooping/Query for multicast group management, Port Trunking, Static/802.3ad, LACP Rate limit and storm control, IEEE 802.1p QoS CoS/TOS/ DSCP priority queuing, IEEE 802.3x flow control
VLAN Groups	1 ~ 4094	
<b>Port Interface</b>	Ethernet (RJ45) Port	24*10/100/1000BaseTx (PSE: 30W/Port, Max. total PoE budget: 685W) auto negotiation speed, Full/Half duplex mode, and auto MDI connection
	Fiber Connections	4*100/1000 Dual rate SFP fiber slots
	Serial Console Port	1*RS232 in RJ45 connector with console cable
<b>Mechanical Characteristics</b>	LED Indicator	Power Unit: P1 (Green), P2 (Green), fault(Green/Red) Ethernet port: Link/active(Green), 1000Mbps
	Housing	Metal IP30 protection

	Dimension	438 x 43.6 x 259.2 mm (W x H x D)
	Weight	Unit Weight: 8.37 lbs.
	Mounting	1U 19" Rack mount
<b>Power Requirements</b>	Input Voltage	46~57VDC Redundant Input
	Power Connection	4-pin terminal block
	Power Consumption	20 Watts for system
	Max. PoE Power Budget	685 Watts
<b>Environmental Limits</b>	Operating Temperature	EOT: -40°C to 75°C (-40°F to 167°F)
	Storage Temperature	-40°C ~ 85°C (-40°F ~ 185°F)
	Ambient Relative Humidity	10% to 95%, (non-condensing)
<b>Regulatory Approvals</b>	EMI	CE FCC EN55022 Class A
	EMS	IEC61000-4-2/3/4/5/6/8; IEC61000-6-2; IEC61000-6-4
	Stability Testing	IEC60068-2-32 (Free fall)
		IEC60068-2-27 (Shock)
		IEC60068-2-6 (Vibration)
	Safety	UL61010-1, UL61010-2-201
Compliance	EN50121-4	

*Table 6.1 - Technical Specifications*

**Antaira Customer Service and Support**

(Antaira US Headquarter) + 844-268-2472

(Antaira Europe Office) + 48-22-862-88-81

(Antaira Asia Office) + 886-2-2218-9733

**Please report any problems to Antaira:**

[www.antaira.com](http://www.antaira.com) / [support@antaira.com](mailto:support@antaira.com)

[www.antaira.eu](http://www.antaira.eu) / [info@antaira.eu](mailto:info@antaira.eu)

[www.antaira.com.tw](http://www.antaira.com.tw) / [info@antaira.com.tw](mailto:info@antaira.com.tw)

**Any changes to this material will be announced on the Antaira website.**