IS230-10GP

Industrial Ethernet Layer 2 Switch

Allied Telesis
AT-IS230-10GP
SFP 10
10R
9R
SFP 9
STATUS
SYS
MASTER
PWR 1
PWR 2
FAULT
PORT 1-8 9R-10R
RESET
CONSOLE
RS-232
LINK
ACT
PD ON
PoE plus
DC24-48V
V1+V1-
V2+V2-
4411

Web User Guide

613-002603 Rev. C

Acknowledgments
Intel and Pentium are trademarks of Intel Corporation.
Microsoft Windows and MS-DOS are registered trademarks of Microsoft Corp.
All other product names or trademarks are properties of their respective owners.

www.alliedtelesis.com
Please verify specifications before quoting. This guide is intended for reference purposes only.
All product specifications are subject to change without notice.

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis, Inc. has been advised of, known, or should have known, the possibility of such damages.

Table of Contents

List of Figures

List of Tables

Preface

This guide contains the hardware installation instructions for the IS230-10GP Industrial Managed Switch. The preface contains the following sections:

Safety Symbols Used in this Document

This document uses the following conventions.

Note
Notes provide additional information.

Caution
Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

Warning
Warnings inform you that performing or omitting a specific action may result in bodily injury.

Warning
Laser warnings inform you that an eye or skin hazard exists due to the presence of a Class 1 laser device.

Warning
Warnings inform you of hot surfaces.

Contacting Allied Telesis

If you need assistance with this product, you may contact Allied Telesis technical support by going to the Support & Services section of the Allied Telesis web site at **www.alliedtelesis.com/support**. You can find links for the following services on this page:

- ❒ 24/7 Online Support — Enter our interactive support center to search for answers to your product questions in our knowledge database, to check support tickets, to learn about RMAs, and to contact Allied Telesis technical experts.
- ❒ USA and EMEA phone support — Select the phone number that best fits your location and customer type.
- ❒ Hardware warranty information — Learn about Allied Telesis warranties and register your product online.
- ❒ Replacement Services — Submit a Return Merchandise Authorization (RMA) request via our interactive support center.
- ❒ Documentation — View the most recent installation and user guides, software release notes, white papers, and data sheets for your products.
- ❒ Software Downloads — Download the latest software releases for your managed products.

For sales or corporate information, go to **www.alliedtelesis.com/purchase** and select your region.

Chapter 1

Configuration Utility

This chapter contains the following sections:

First Time Setup

Overview

The Industrial Ethernet Managed Switch is a configurable device that facilitates the interconnection of Ethernet devices on an Ethernet network. This includes computers, operator interfaces, I/O, controllers, RTUs, PLCs, other switches/hubs or any device that supports the standard IEEE 802.3 protocol.

This switch has all the capabilities of a store and forward Ethernet switch plus advanced management features such as SNMP, RSTP and port mirroring. This manual details how to configure the various management parameters in this easy to use switch.

Introduction

To take full advantage of all the features and resources available from the switch, it must be configured for your network.

The switch implements Rapid Spanning Tree Protocol (RSTP) and Simple Network Management Protocol (SNMP) to provide most of the services offered by the switch. Rapid Spanning Tree Protocol allows managed switches to communicate with each other to ensure that there exists only one active route between each pair of network nodes and provides automatic fail-over to the next available redundant route. A brief explanation of how RSTP works is given in the Spanning Tree section.

The switch is capable of communicating with other SNMP capable devices on the network to exchange management information. This statistical/derived information from the network is saved in the Management Information Base (MIB) of the switch. The MIB is divided into several different information storage groups. These groups will be elaborated in detail in the Management and SNMP information section of this document. The switch implements Internet Group Management Protocol (IGMP) to optimize the flow of multicast traffic on your network.

The switch supports both port-based and tag-based Virtual LANs for flexible integration with VLAN-aware networks with support for VLAN-unaware devices.

Administrative Interface Access

A management session with the switch may be connected via the local Console port or a over network connection to any of the switch's Ethernet ports.

Note
The Console port on the front panel connects to a terminal interface via the RS232/USB port or over the network using telnet or Secure Shell (SSH).

There are several administrative interfaces to the switch:

1. The graphical web interface is accessible via the switch's built-in web server. Both HTTP and secure HTTPS with SSL are supported over an Ethernet connection.

Note
This is the recommended method for managing the switch.

2. Command Line Interface (CLI) can be used to read/write most settings. This interface may be used with an Ethernet connection (recommended) or the Console port.
3. The terminal interface via the RS232/USB port (Console port) or over the network using telnet or Secure Shell (SSH). This interface uses the CLI administrative interface only.
4. The SNMP interface can be used to read/write many settings and is available within the Web and CLI administrative interfaces.

Default User Name and Password

When logging into any of the administrative interfaces for the first time, use the default username and password. They are:

Username: ***manager***
Password: ***friend***.

Note
Both the user name and password are case sensitive.

Allied Telesis recommends that you change to a new password when you initially configure the switch.

❐ If you are using the graphical web interface, go to “Change Default Password” on page 28.

❐ If you are using the CLI interface, refer to the commands in the Security chapter of the IS230-10GP Reference Guide.

Using the Graphical (Web) Interface

The graphical interface is provided via a web server in the switch and can be accessed via a web browser such as Opera, Mozilla, or Internet Explorer.

Note
JavaScript must be supported and enabled in your browser for the graphical interface to work correctly.

HTTP and HTTPS (secure HTTP) are supported for access to the web server. By default, both protocols are enabled. Either or both may be disabled to secure the switch. (See the Remote Access Security topic in this section.)

To access the graphical interface, enter a URL like HTTP://192.168.1.1 in your browser's address bar. Replace “http” with “https” to use secure http and replace “192.168.1.1” with your switch's IP address if you've changed it from the factory default.

The web server in the switch uses a signed security certificate. When you access the server via https, you may see a warning dialog indicating that the certificate was signed by an unknown authority. This is expected and to avoid this message in the future you can choose to install the certificate on your computer.

Note
This manual describes and depicts the web user interface in detail. The terminal interface is not specifically shown but is basically the same.

Configuring the Switch for Network Access

To control and monitor the switch via the network, it must be configured with basic network settings, including an IP address and subnet mask. Refer to the quick start guide in Section 1 for how to initially access your switch.

To configure the switch for network access, select [Add Menu Address Here] to reach the System Settings menu. The settings in this menu control the switch's general network configuration.

❒ DHCP Enabled/Disabled: The switch can automatically obtain an IP address from a server using the Dynamic Host Configuration Protocol (DHCP). This can speed up initial set up, as the network administrator does not have to find an open IP address.

❒ IP Address and subnet mask configuration: The IP address for the switch can be changed to a user-defined address along with a customized subnet mask to separate subnets.

Note
Advanced users can set the IP address to 0.0.0.0 to disable the use of an IP address for additional security. However, any features requiring an IP address (i.e., web interface, etc.) will no longer be available.

❒ Default Gateway Selection: A Gateway Address is chosen to be the address of a router that connects two different networks. This can be an IP address or a Fully Qualified Domain Name (FQDN) such as “domainname.org”.

❒ NTP Server: The IP address or domain name of an NTP (Network Time Protocol) server from which the switch may retrieve the current time at startup. Please note that using a domain name requires that at least one domain name server be configured.

Configuring the Ethernet Ports

The switch comes with default port settings that should allow you to connect to the Ethernet Ports with out any necessary configuration. Should there be a need to change the name of the ports, negotiation settings or flow control settings, you can do this in the Port Configuration menu. Access this menu by selecting Setup from the Main menu, and then selecting Main Settings.

- Port Name: Each port in the managed switch can be identified with a custom name. Specify a name for each port here.
- Admin: Ports can be enabled or disabled in the managed switch. For ports that are disabled, they are virtually non-existent (not visible in terms of switch operation or spanning tree algorithm). Choose to enable or disable a port by selecting Enabled or Disabled, respectively.
- Negotiation: All copper ports and gigabit fiber ports in the managed switch are capable of autonegotiation such that the fastest bandwidth is selected. Choose to enable auto-negotiation or use fixed settings. 100Mbps Fiber ports are Fixed speed only.
- Speed/Duplex/Flow Control: The managed switch accepts three local area network Ethernet Standards. The first standard, 10BASE-T, runs 10Mbps with twisted pair Ethernet cable between network interfaces. The second local area network standard is 100BASE-T, which runs at 100Mbps over the same twisted pair Ethernet cable. Lastly, there is 100BASE-F, which enables fast Ethernet (100Mbps) over fiber.

These options are available:

- 10h–10 Mbps, Half Duplex
- 10f –10 Mbps, Full Duplex
- 100h–100 Mbps, Half Duplex
- 100f –100 Mbps, Full Duplex
- 1000f–1000 Mbps, Full Duplex

The gigabit combination ports have two rows, a standard row of check boxes and a row labeled “SFP” with radio buttons. The SFP setting independently sets the speed at which a transceiver will operate if one is plugged in. Otherwise, the switch will use the fixed Ethernet port and the corresponding settings for it.

Note
When 100f is selected for the SFP port, the corresponding fixed Ethernet jack will be disabled unless it is changed back to 1000F.

Command Line Interface Configuration

Introduction to Command-Line Interface (CLI)

The command-line interface (CLI) is constructed with an eye toward automation of CLI-based configuration. The interaction is modeled on that used in many Internet protocols such as Telnet, FTP, and SMTP. After each command is entered and processed, the switch will issue a reply that consists of a numeric status code and a human-readable explanation of the status.

The general format of commands is:

```
section parameter [value]
```

where:

- section is used to group parameters.
- parameter will specify the parameter within the section. For example, the network section will have parameters for DHCP, IP address, subnet mask, and default gateway.
- value is the new value of the parameter. If value is omitted, the current value is displayed.

Please note that new values will not take effect until explicitly committed.

Sections and parameter names are case sensitive (e.g., “Network” is not the same as “network”).

Note
Any commands in the CLI Commands section of this chapter, with the exception of the global commands, must be prefaced with the name of the section they are in. For example, to change the IP address of the switch, you would type:

```
network address <newIP>
```

Accessing the CLI

To access the CLI interface, establish Ethernet or serial connectivity to the switch.

To connect by Ethernet, open a command prompt window and type:

```
telnet <switchip> (where <switchip> is the IP address of the switch)
```

At the login prompt, type ***manager*** for the username and ***friend*** for the default password. The switch will respond with “Managed switch configuration CLI ready”.

Web Browser Configuration

The switch has an HTML based user interface embedded in the flash memory. The interface offers an easy to use means to manage basic and advanced switch functions. The interface allows for local or remote switch configuration anywhere on the network.

The interface is designed for use with Internet Explorer (6.0), Chrome, Firefox.

Default Network Configuration

When the switch is first installed, its management configuration parameters are set to pre-assigned default values. The default network configuration parameters are:

- Static IP address: 192.168.1.1
- Subnet Mask 255.255.255
- Gateway 192.168.1.254
- DNS Server 1: 168.95.1.1
- DNS Server 2: 168.95.192.1

The default User Name is ***manager*** and the default password is ***friend***. Both the user name and password are case sensitive.

Log In

To start a network management session, perform the following procedure:

1. Connect one of the Ethernet ports on the switch to an existing network.
2. Connect your computer console to the same local area network (LAN) that is connected to the IS230-10GP switch.
3. If you choose to use the Web management interface, perform the following steps:
   a. Launch your web browser on the PC.
   b. In the browser's URL address bar, type the switch's default IP address (192.168.1.1).

   The login screen displays.

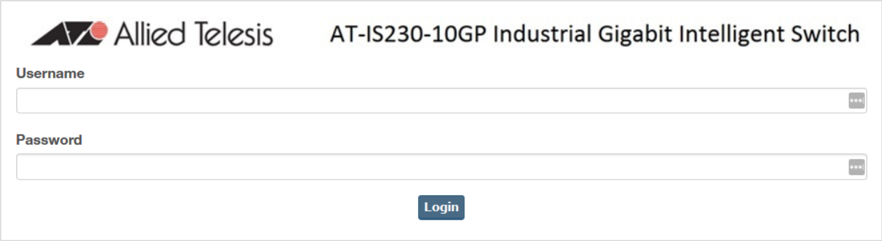
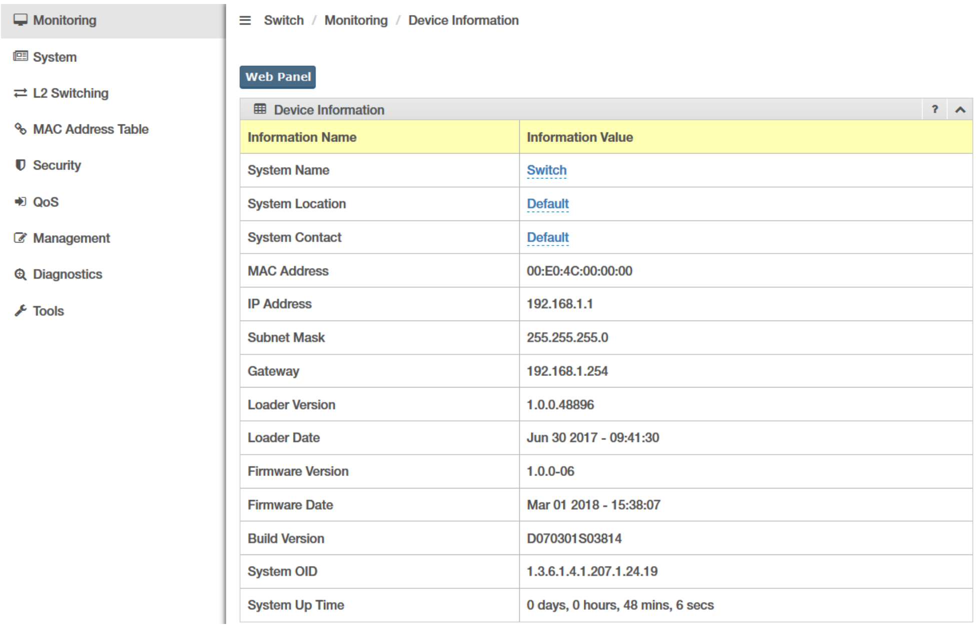


Figure 1. Login Screen

   c. Enter the default username (***manager***) and password (***friend***). Both the user name and password are case sensitive.
   d. Click **Login** on the login screen to log in.

The main web interface window - **Monitor > Device Information** - is displayed with the management menu selections on the left-hand side of the screen - refer to Figure 2. For the definition of the fields in this window, refer to “Device Information” on page 32.



Information Name	Information Value
System Name	Switch
System Location	Default
System Contact	Default
MAC Address	00:E0:4C:00:00:00
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
Loader Version	1.0.0.48896
Loader Date	Jun 30 2017 - 09:41:30
Firmware Version	1.0.0-06
Firmware Date	Mar 01 2018 - 15:38:07
Build Version	D070301S03814
System OID	1.3.6.1.4.1.207.1.24.19
System Up Time	0 days, 0 hours, 48 mins, 6 secs

Figure 2. Initial Web Window - Monitor > Device Information

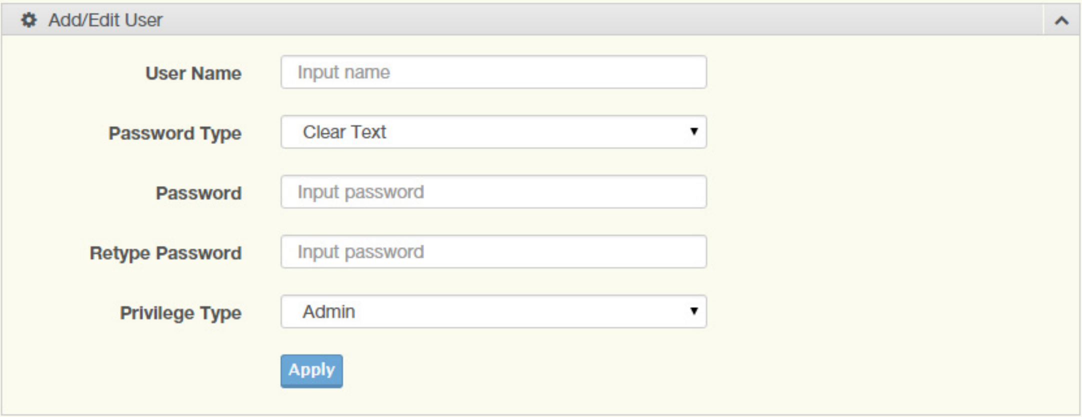
Change Default Password

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 procedure details the necessary steps to change an existing password:

1. Navigate to **Tools** > **User Account**.

   The Add/Edit User window displays. For more information about the fields in the window, refer to “User Account” on page 161.



User Name	Input name
Password Type	Clear Text
Password	Input password
Retype Password	Input password
Privilege Type	Admin

Figure 3. Switch > Tools > User Account - Add/Edit User Window

2. Enter a **User Name**. The User Name is case sensitive.
   a. Enter an existing User Name if you are only changing the password for that User Name.
   b. Enter a new User Name if you are creating a new User Name and Password combination.

   Note
   It is not necessary to change the user name every time along with a new password entry. However, when you define a new user name/ password combination and delete a previously used combination, security is increased. (Refer to Step 7 below.) This action is recommended when changing the Default User Name/Password.

3. From the Password Type drop-down menu, select **Clear Text**, **Encrypted** or **No Password**.
4. In the **Password** field, type in the new password. The password is case sensitive.
5. Enter the identical password in the **Retype Password** field.
6. Click **Apply** to add the current account settings.

   If a new User Name has been defined, a new line is displayed along with other user names in the Local Users table shown just below the **Apply** button.

7. If you choose to delete a user name and password combination, click **Delete** in the Modify column of the Local Users table.

   The user name/password combination will be removed from the configuration.

   Note
   This action is recommended when changing the Default User Name/ Password.

8. After saving all the desired settings, perform a system save (**Tools** > **Save Configuration**).

   The changes are saved.

Chapter 2

Managing Switch

This chapter describes the contents of the IS230-10GP management windows and contains the following sections:

Monitoring

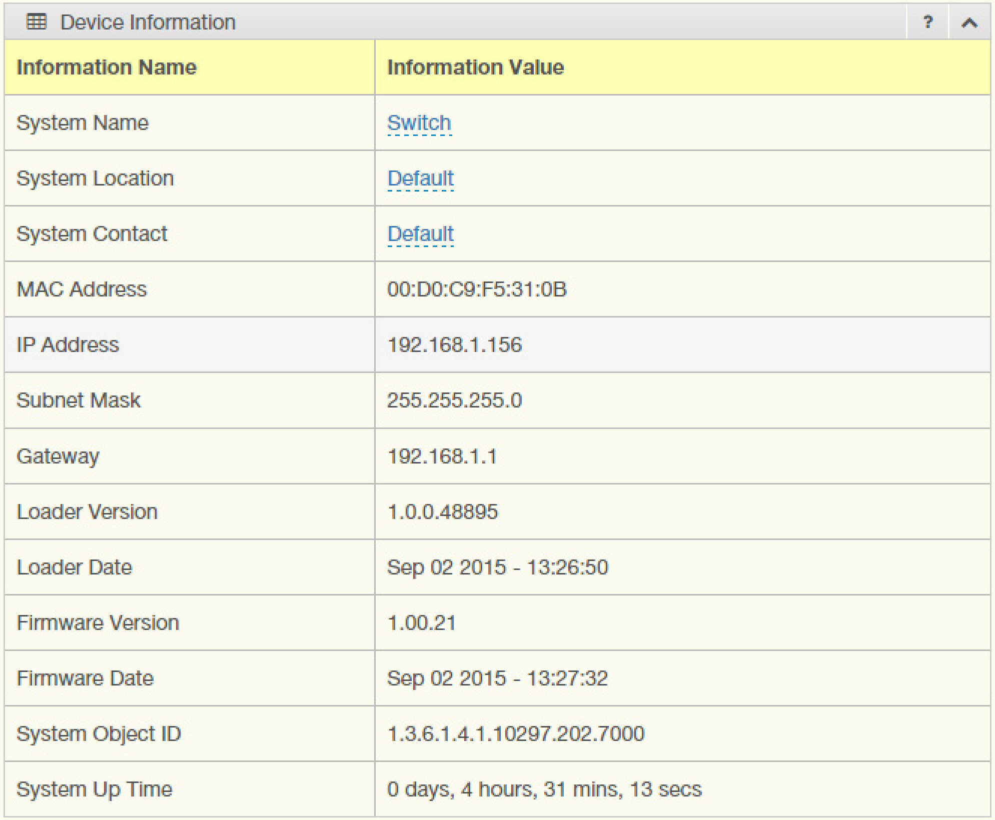
This section includes the following topics:

- ❐ “Device Information”
- ❐ “Logging Message” on page 33
- ❐ “Port Monitoring” on page 34
- ❐ “Link Aggregation” on page 36
- ❐ “LLDP Statistics” on page 36
- ❐ “IGMP Statistics” on page 38
- ❐ “MLD Statistics” on page 39

Device Information

The Device Information menu lists information, such as: System Name, System Location, MAC Address, Firmware version, and more, pertaining to the system. 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**.



Information Name	Information Value
System Name	Switch
System Location	Default
System Contact	Default
MAC Address	00:D0:C9:F5:31:0B
IP Address	192.168.1.156
Subnet Mask	255.255.255.0
Gateway	192.168.1.1
Loader Version	1.0.0.48895
Loader Date	Sep 02 2015 - 13:26:50
Firmware Version	1.00.21
Firmware Date	Sep 02 2015 - 13:27:32
System Object ID	1.3.6.1.4.1.10297.202.7000
System Up Time	0 days, 4 hours, 31 mins, 13 secs

Figure 4. Monitoring > Device Information

The following table describes the items in Figure 4.

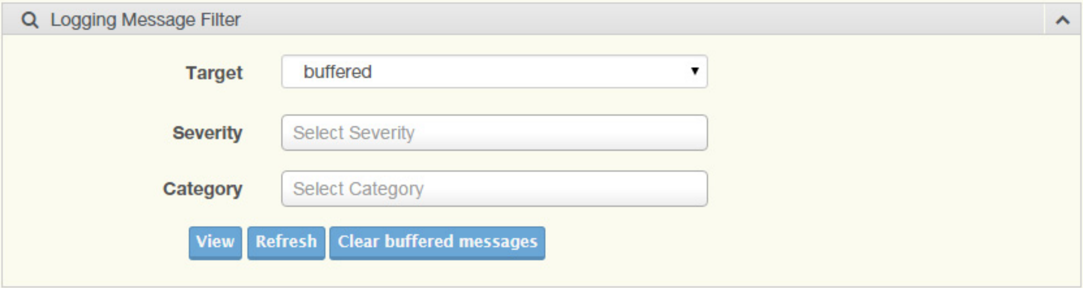
Table 1. Device Information

Item	Description
System Name	Click **Switch** to enter the system name: up to 128 alphanumeric characters (default is Switch).
System Location	Click **Default** to enter the location: up to 256 alphanumeric characters (default is Default).
System Contact	Click **Default** 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.
System Object ID	Displays the base object ID of the switch.
System Up Time	Displays the time since the last switch reboot.

Logging Message

The Logging Message Filter page allows you to enable the display of logging message filter.

To access this page, click **Monitoring** > **Logging Message**.



Logging Message Filter

Target: buffered

Severity: Select Severity

Category: Select Category

Figure 5. Monitoring > Logging Message

The following table describes the items in Figure 5.

Table 2. Logging Message

Item	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: • emerg: Indicates system is unusable. It is the highest level of severity. • alert: Indicates action must be taken immediately. • crit: Indicates critical conditions. • error: Indicates error conditions. • warning: Indicates warning conditions. • notice: Indicates normal but significant conditions. • info: Indicates informational messages. • debug: Indicates debug-level messages.
Category	Click the drop-down menu to select the category level target setting.
View	Click **View** to display all Logging Information and Logging Message information.
Refresh	Click **Refresh** to update the screen.
Clear buffered messages	Click **Clear buffered messages** to clear the logging buffer history list.

The **Logging Information** settings in the ensuing table are informational only: Target, Severity and Category.

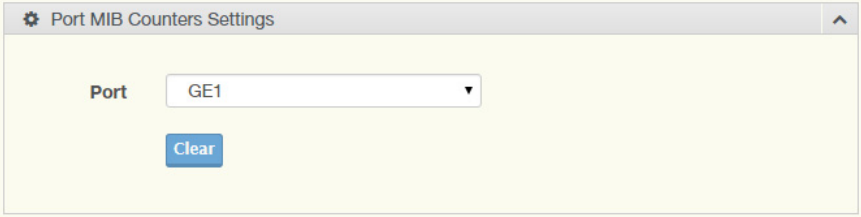
The **Logging Message** settings in the ensuing table are informational only: No., Time Stamp, Category, Severity and Message.

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**.



Port: GE1

Figure 6. Monitoring > Port Monitoring > Port Statistics

The following table describes the items in Figure 6.

Table 3. Port Statistic

Item	Description
Port	Click the drop-down menu to select a port and its captured statistical setting values.
Clear	Click **Clear** to clear the counter selections.

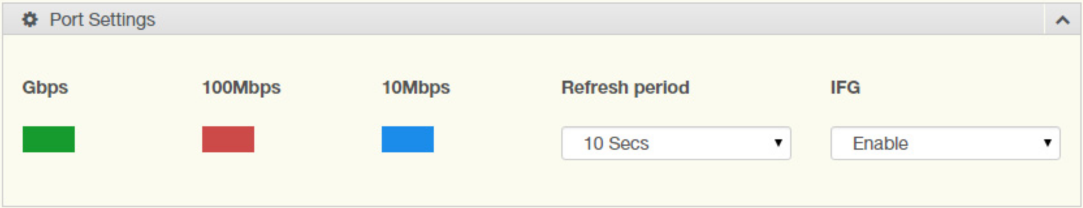
The **IF MIB Counters** settings in the ensuing table are informational only: ifInOctets, ifInUcastPkts, ifInNUcastPkts, ifInDiscards, ifOutOctets, ifOutUcastPkts, ifOutNUcastPkts, ifOutDiscards, ifInMulticastPkts, ifInBroadcastPkts, ifOutMulticastPkts and ifOutBroadcastPkts.

The **Ether-Like MIB Counters** settings in the ensuing table are informational only: dot3StatsAlignmentErrors, dot3StatsFCSErrors, dot3StatsSingleCollisionFrames, dot3StatsMultipleCollisionFrames, dot3StatsDeferredTransmissions, dot3StatsLateCollisions, dot3StatsExcessiveCollisions, dot3StatsFrameTooLongs, dot3StatsSymbolErrors, dot3ControlInUnknownOpcodes, dot3InPauseFrames and dot3OutPauseFrames.

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

Port Utilization

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



Port Settings

Gbps	100Mbps	10Mbps	Refresh period	IFG
🟩	🟥	🟦	10 Secs	Enable

Figure 7. Monitoring > Port Monitoring > Port Utilization

The following table describes the items in Figure 7 on page 36.

Table 4. Port Utilization

Item	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.

Link Aggregation

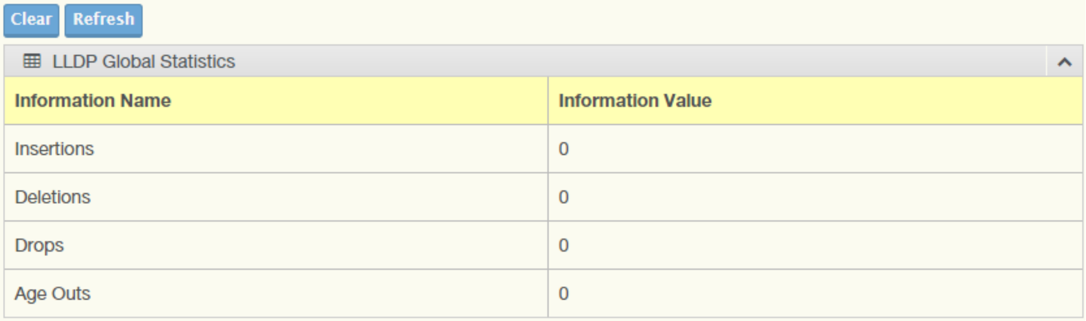
The Link Aggregation function provides LAG information for each trunk. It displays membership status, link state and membership type for each port. To access this page, click **Monitoring** > **Link Aggregation**.

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

LLDP Statistics

The LLDP Statistics page displays the LLDP statistics.

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



LLDP Global Statistics

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

Figure 8. Monitoring > LLDP Statistics

The following table describes the items in Figure 8.

Table 5. LLDP Statistics

Item	Description
Clear	Click **Clear** to reset LLDP Statistics of all the interfaces.
Refresh	Click **Refresh** to update the data on the screen with the present state of the data in the switch.

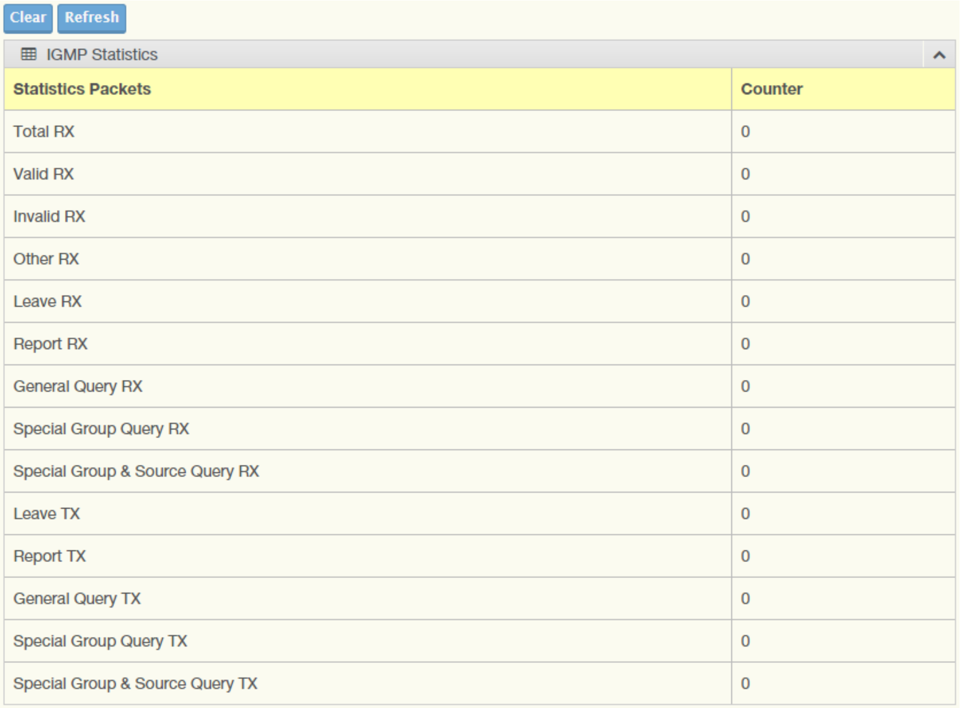
The fields in the **LLDP Global Statistics** table are for information only: Insertions, Deletions, Drops and Age Outs.

The fields in the **LLDP Port Statistics** table are for information only: Port, TX Frames (Total), RX Frames (Total, Discarded and Errors), RX TLVs (Discarded and Unrecognized) and RX Ageouts (Total).

IGMP Statistics

The IGMP Statistics page displays the IGMP statistics.

To access this page, click **Monitoring** > **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 9. Monitoring > IGMP Statistics

The following table describes the items in Figure 9.

Table 6. IGMP Statistics

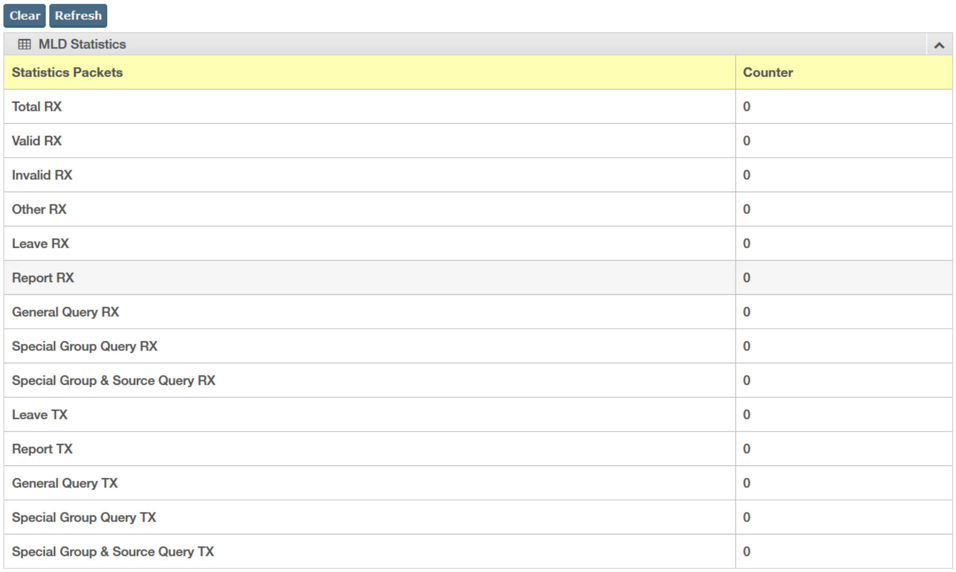
Item	Description
Clear	Click **Clear** to refresh IGMP Statistics of all the interfaces.
Refresh	Click **Refresh** to update the data on the screen with the present state of the data in the switch.

The **IGMP Statistics** settings in the ensuing table are informational only: Total RX, Valid RX, Invalid RX, Other RX, Leave RX, Report RX, General Query RX, Special Group Query RX, Special Group & Source Query RX, Leave TX, Report TX, General Query TX, Special Group Query TX and Special Group & Source Query TX.

MLD Statistics

The MLD Statistics function displays statistical package information for IP multicasting.

To access this page, click **Monitoring** > **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

Figure 10. Monitoring > MLD Statistics

The following table describes the items in Figure 10.

Table 7. MLD Statistics

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

The **MLD Statistics** settings in the ensuing table are informational only:

Total RX, Valid RX, Invalid RX, Other RX, Leave RX, Report RX, General Query RX, Special Group Query RX, Special Group & Source Query RX, Leave TX, Report TX, General Query TX, Special Group Query TX and Special Group & Source Query TX.

System

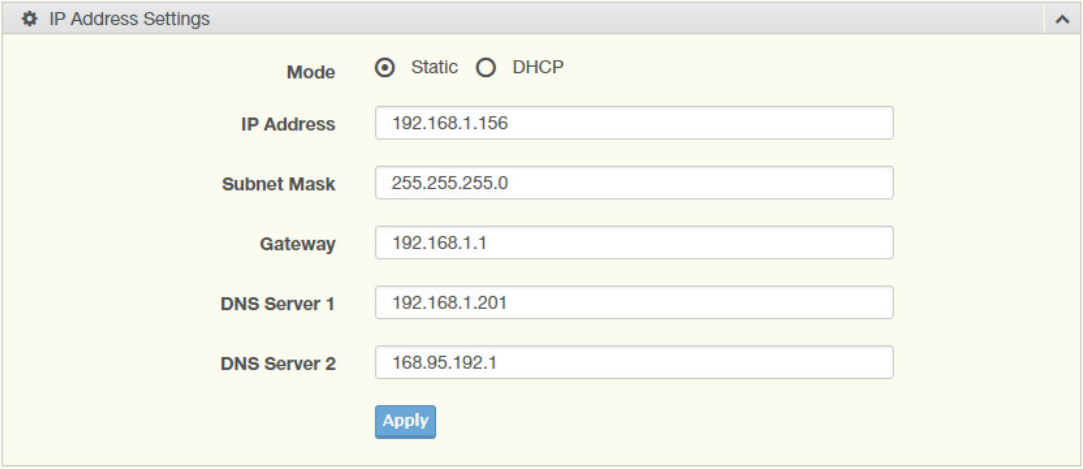
This section includes the following topics:

- “IP Settings”
- “IPv6 Settings” on page 41
- “DHCP Client Option 82” on page 42
- “DHCP Auto Provision” on page 43
- “Management VLAN” on page 43
- “System Time” on page 44
- “Network Port” on page 45

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**.



IP Address Settings

Mode	● Static ○ DHCP
IP Address	192.168.1.156
Subnet Mask	255.255.255.0
Gateway	192.168.1.1
DNS Server 1	192.168.1.201
DNS Server 2	168.95.192.1

Figure 11. System > IP Settings

The following table describes the items in Figure 11.

Table 8. IP Settings

Item	Description
Mode	Click the radio button to select the IP Address Setting mode: Static, DHCP, or BOOTP.
IP Address	Enter a value to specify the IP address of the interface. The default is 192.168.1.1.
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 192.168.1.254.

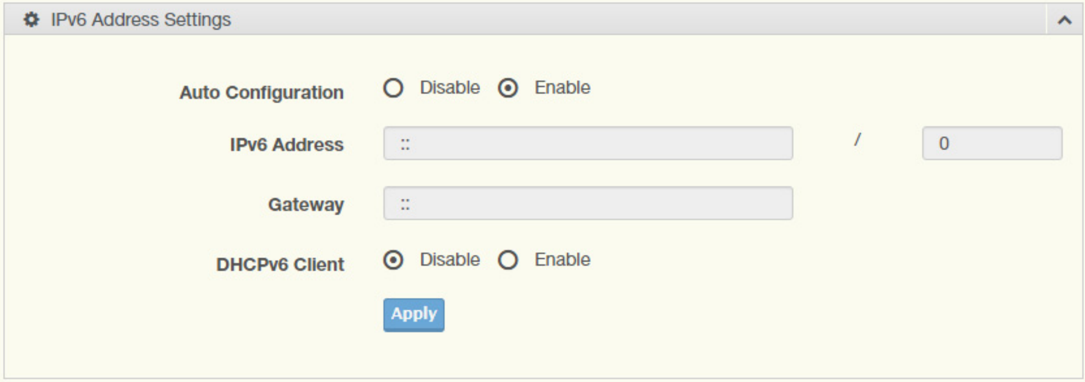
Table 8. IP Settings (Continued)

Item	Description
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 **Apply** to save the values and update the screen.

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

IPv6 Settings

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



IPv6 Address Settings

Auto Configuration ○ Disable ● Enable

IPv6 Address :: / 0

Gateway ::

DHCPv6 Client ● Disable ○ Enable

Figure 12. System > IPv6 Settings

The following table describes the items in Figure 12.

Table 9. IPv6 Settings

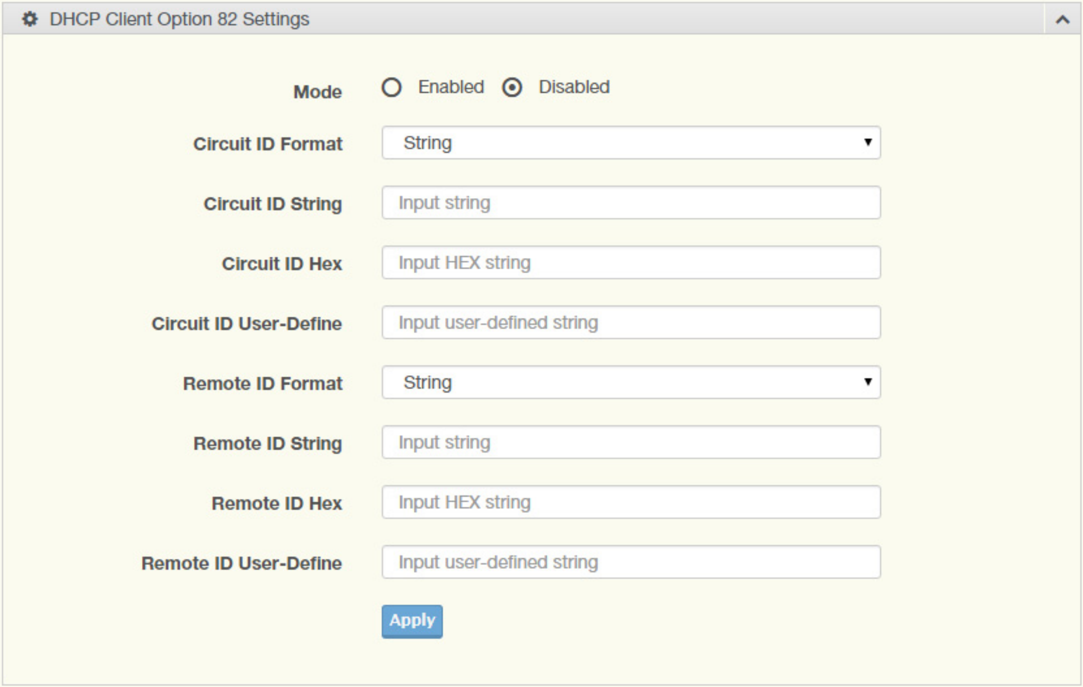
Item	Description
Auto Configuration	Select the radio button to enable or disable the IPv6.
IPv6 Address	Enter the IPv6 address for the system.
Gateway	Enter the gateway address for the system.
DHCPv6 Client	Enter the DHCPv6 address for the system.
Apply	Click **Apply** to save the values and update the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

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

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 suboptions. 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**.



DHCP Client Option 82 Settings

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

Figure 13. System > DHCP Client Option 82

The following table describes the items in Figure 13.

Table 10. DHCP Client Option 82

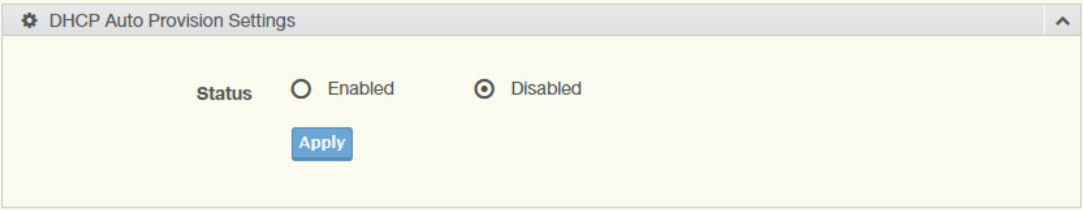
Item	Description
Mode	Click the radio button to enable or disable the DHCP Client Option 82 mode.
Circuit ID Format	Click the drop-down menu to set the ID format: String, Hex, User Definition.
Circuit ID String	Enter the string ID of the corresponding class.
Circuit ID Hex	Enter the hex string of the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

The **DHCP Client Option 82 Information** settings in the ensuing table 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 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**.



DHCP Auto Provision Settings

Status ○ Enabled ● Disabled

Figure 14. System > DHCP Auto Provision

The following table describes the items in Figure 14.

Table 11. DHCP Auto Provision

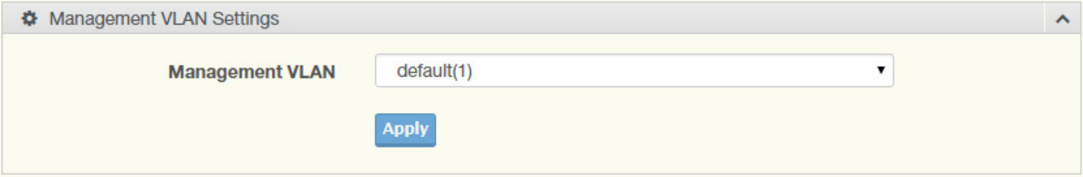
Item	Description
Status	Select the radio button to enable or disable the DHCP Auto Provisioning Setting.
Apply	Click **Apply** to save the values and update the screen.

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

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**.



Management VLAN Settings

Management VLAN: default(1)

Figure 15. System > Management VLAN

The following table describes the items in Figure 15.

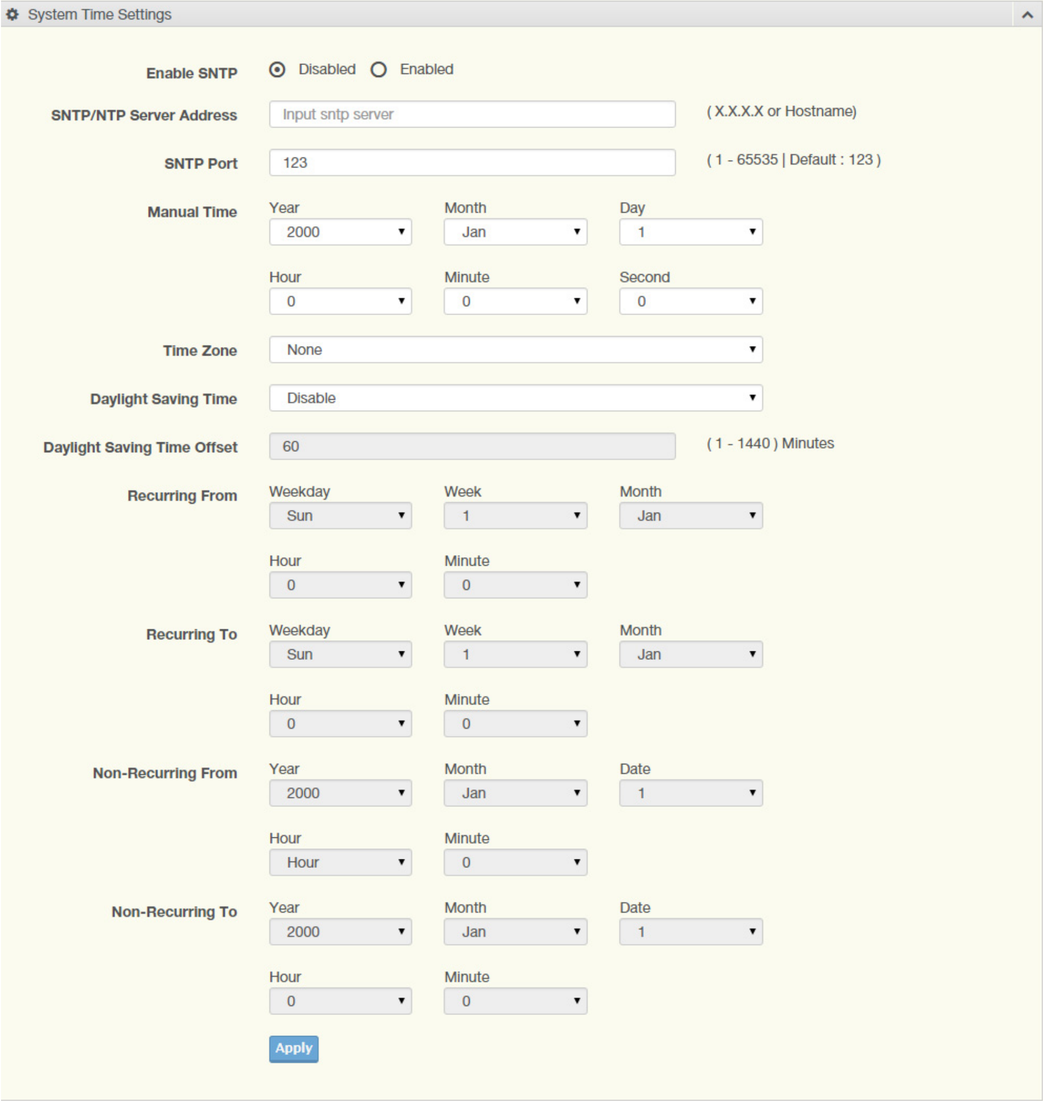
Table 12. Management VLAN

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

The **Management VLAN State** in the ensuing table is informational only: Management VLAN.

System Time

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



System Time Settings

Enable SNTP ● Disabled ○ Enabled

SNTP/NTP Server Address: Input sntp server (X.X.X.X or Hostname)

SNTP Port: 123 (1 - 65535 | Default : 123)

Manual Time: Year 2000, Month Jan, Day 1; Hour 0, Minute 0, Second 0

Time Zone: None

Daylight Saving Time: Disable

Daylight Saving Time Offset: 60 (1 - 1440) Minutes

Recurring From: Weekday Sun, Week 1, Month Jan; Hour 0, Minute 0

Recurring To: Weekday Sun, Week 1, Month Jan; Hour 0, Minute 0

Non-Recurring From: Year 2000, Month Jan, Date 1; Hour Hour, Minute 0

Non-Recurring To: Year 2000, Month Jan, Date 1; Hour 0, Minute 0

Figure 16. System > System Time

The following table describes the items in Figure 16.

Table 13. System Time

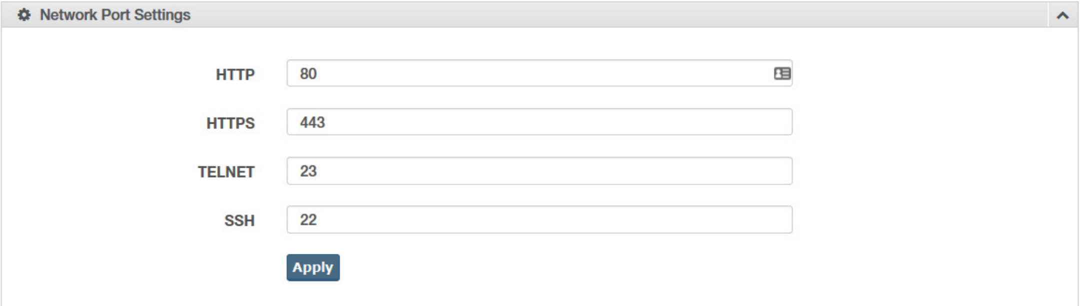
Item	Description
Enable SNTP	Click the radio button to enable or disable the SNTP.
SNTP/FNTServer Address	Enter the address of the SNTP server. This is a text string of up to 64 characters containing the encoded unicast IP address or hostname of a SNTP server. Unicast SNTP requests will be sent to this 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 **Apply** to save the values and update the screen.

The **System Time Information** settings in the ensuing table 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.

Network Port

The Network Port 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 **System > Network Port**.



HTTP: 80

HTTPS: 443

TELNET: 23

SSH: 22

Figure 17. System > Network Port

The following table describes the items in Figure 17 on page 45.

Table 14. Network Port Settings

Item	Description
HTTP	Enter the HTTP Port address
HTTPS	Enter the HTTPS Port address
TELNET	Enter the TELNET Port address
SSH	Enter the SSH Port address
Apply	Click **Apply** to save the values and update the screen.

The **Network Port Information** settings in the ensuing table are informational only: Protocol Name and Port Value.

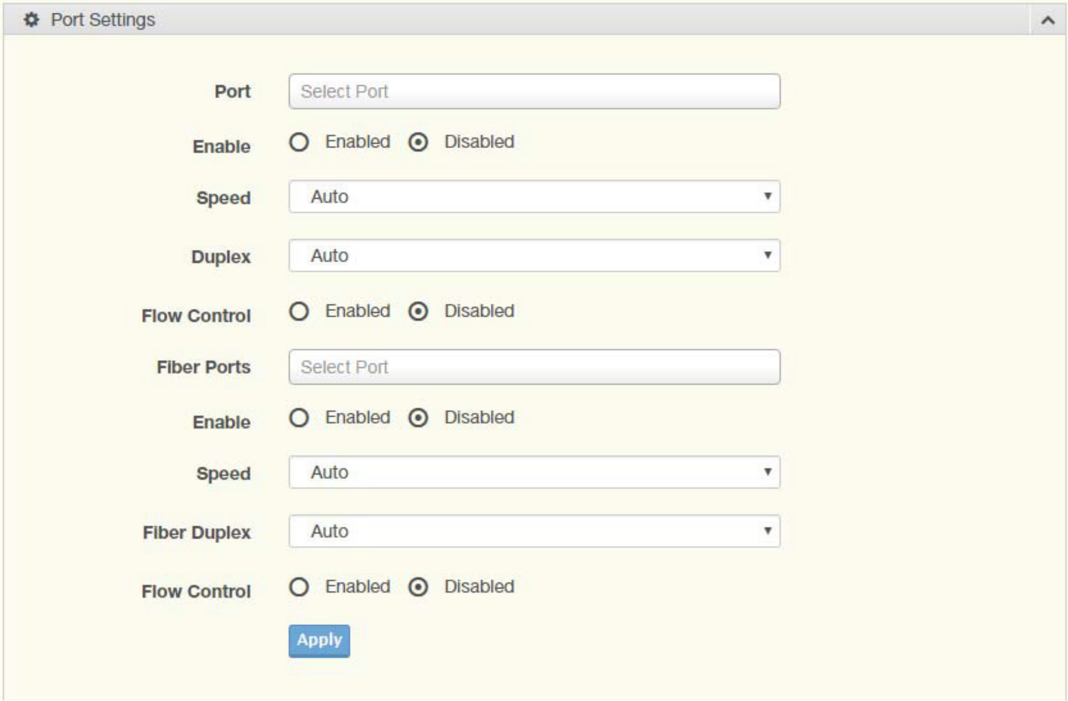
L2 Switching

This section includes the following topics:

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**.



Port Settings

Port: Select Port

Enable: ○ Enabled ◉ Disabled

Speed: Auto

Duplex: Auto

Flow Control: ○ Enabled ◉ Disabled

Fiber Ports: Select Port

Enable: ○ Enabled ◉ Disabled

Speed: Auto

Fiber Duplex: Auto

Flow Control: ○ Enabled ◉ Disabled

Apply

Figure 18. L2 Switching > Port Configuration

The following table describes the items in Figure 18.

Table 15. L2 Switching Port Configuration

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

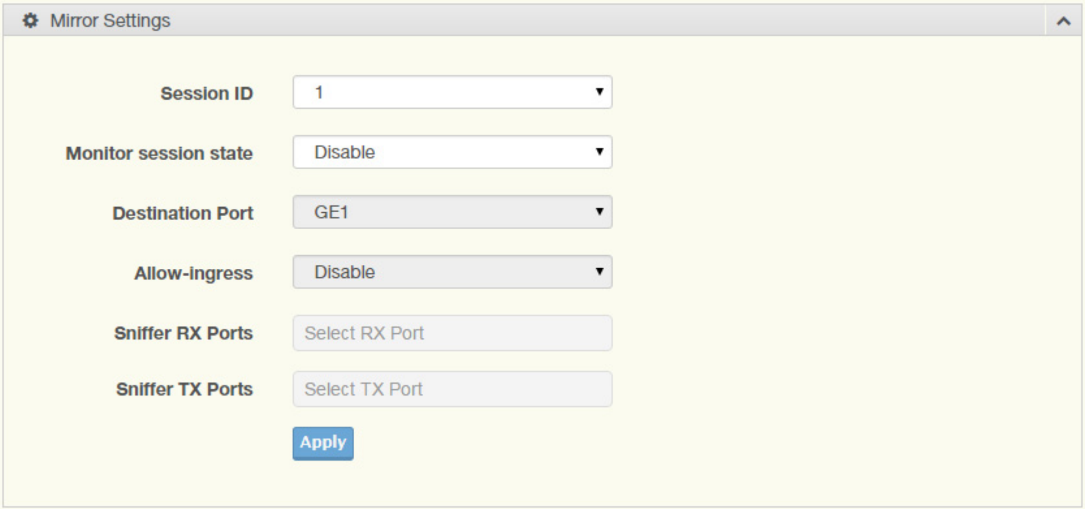
The **Port Status** settings in the ensuing table are informational only: Port, **Edit** (click to enter description), Enable State, Link Status, Speed, Duplex, FlowCtrl Config and FlowCtrl Status.

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 or 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**.



Mirror Settings

Session ID: 1

Monitor session state: Disable

Destination Port: GE1

Allow-ingress: Disable

Sniffer RX Ports: Select RX Port

Sniffer TX Ports: Select TX Port

Figure 19. L2 Switching > Port Mirror

The following table describes the items in Figure 19.

Table 16. Port Mirror

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 **Apply** to save the values and update the screen.

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

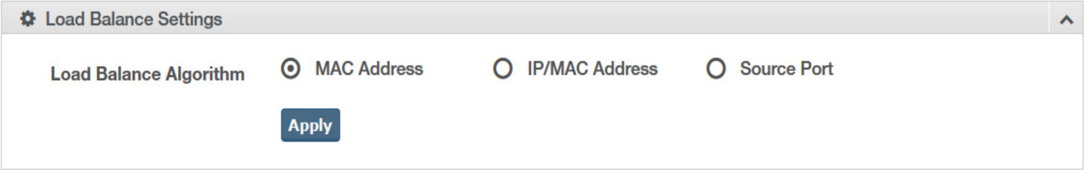
Link Aggregation

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**.



Load Balance Settings

Load Balance Algorithm ● MAC Address ○ IP/MAC Address ○ Source Port

Figure 20. L2 Switching > Link Aggregation > Load Balance

The following table describes the items in Figure 20.

Table 17. Load Balance

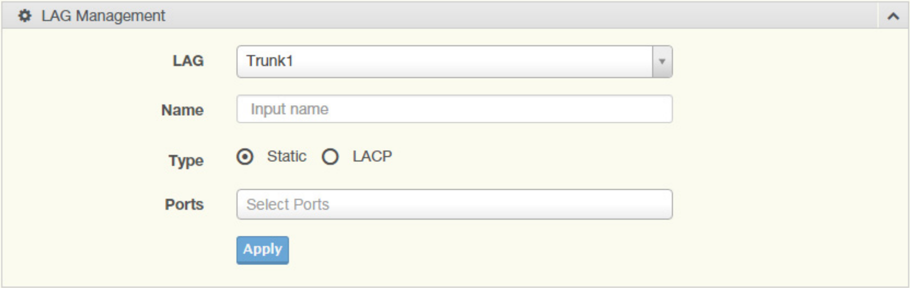
Item	Description
Load Balance Algorithm	Select the radio button to select the Load Balance Setting: MAC Address, IP/MAC Address or Source Port.
Apply	Click **Apply** to save the values and update the screen.

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

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**.



LAG Management

LAG: Trunk1

Name: Input name

Type: ● Static ○ LACP

Ports: Select Ports

Figure 21. L2 Switching > Link Aggregation > LAG Management

The following table describes the items in Figure 21.

Table 18. LAG Management

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: Port1-10.
Apply	Click **Apply** to save the values and update the screen.

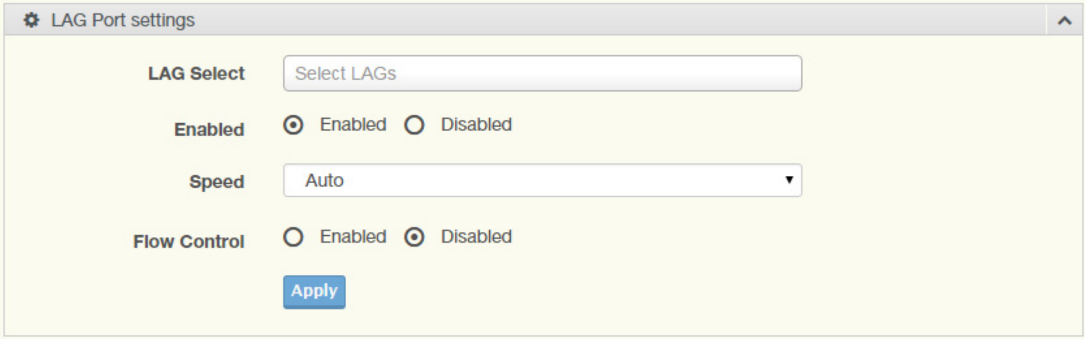
The **LAG Management Information** settings in the ensuing table are informational only: LAG, Name, Type, Link State, Active Member, Standby Member, **Edit** (click to modify the settings) and **Clear** (click to load default settings).

LAG 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**.



LAG Port settings

LAG Select: Select LAGs

Enabled: ● Enabled ○ Disabled

Speed: Auto

Flow Control: ○ Enabled ● Disabled

Apply

Figure 22. L2 Switching > Link Aggregation > LAG Port Settings

The following table describes the items in Figure 22.

Table 19. LAG Port Settings

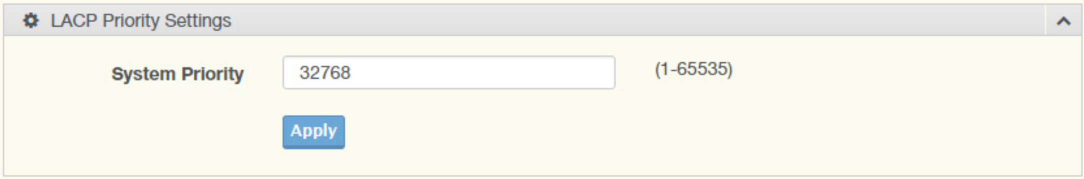
Item	Description
LAG Select	Click the drop-down menu to select a predefined LAG trunk definition: LAG 1-8.
Enabled	Click the radio button to enable or disable the LAG Port.
Speed	Click the drop-down menu to select the port speed: Auto, Auto-10M, Auto-100M, Auto-1000M, Auto-10/100M, 10M, 100M, or 1000M.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

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

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**.



LACP Priority Settings

System Priority: 32768 (1-65535)

Figure 23. L2 Switching > Link Aggregation > LACP Priority Settings

The following table describes the items in Figure 23.

Table 20. LACP Priority Settings

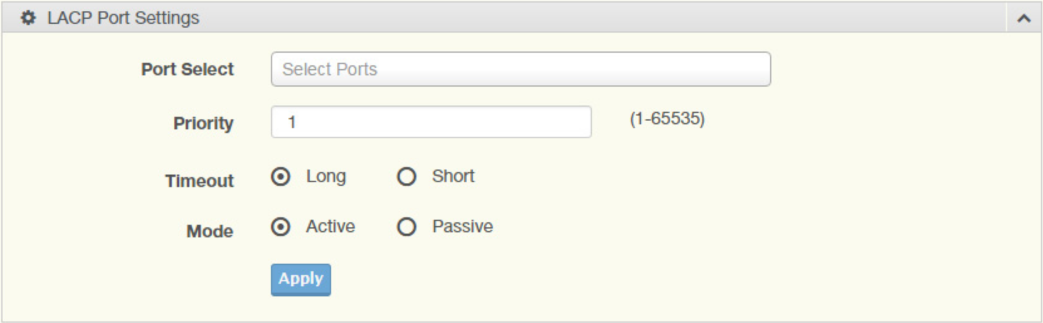
Item	Description
System Priority	Enter the value (1-65535) to designate the LACP system priority.
Apply	Click **Apply** to save the values and update the screen.

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

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**.


LACP Port Settings

Port Select: Select Ports

Priority: 1 (1-65535)

Timeout: ● Long ○ Short

Mode: ● Active ○ Passive

Figure 24. L2 Switching > Link Aggregation > LACP Port Settings

The following table describes the items in Figure 24.

Table 21. LACP Port Settings

Item	Description
Port Select	Select a port for the LACP Port Settings. The listed available settings are: Port1-10. 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. • Active: Enables LACP unconditionally. • Passive: Enables LACP only when an LACP device is detected (default state).
Apply	Click **Apply** to save the values and update the screen.

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

802.1Q VLAN

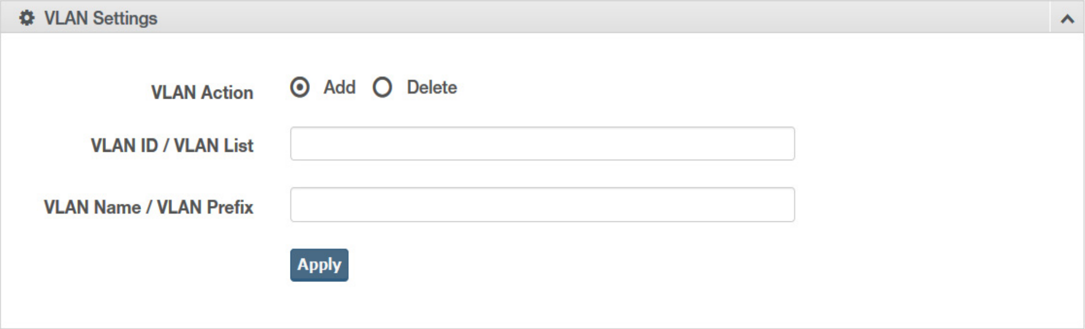
The 802.1Q VLAN feature allows for a single VLAN to support multiple VLANs. With the 802.1Q feature you can preserve VLAN IDs and segregate different VLAN traffic.

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.

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



VLAN Settings

VLAN Action ● Add ○ Delete

VLAN ID / VLAN List

VLAN Name / VLAN Prefix

Figure 25. L2 Switching > 802.1Q VLAN > VLAN Management

The following table describes the items in Figure 25:

Table 22. VLAN Management

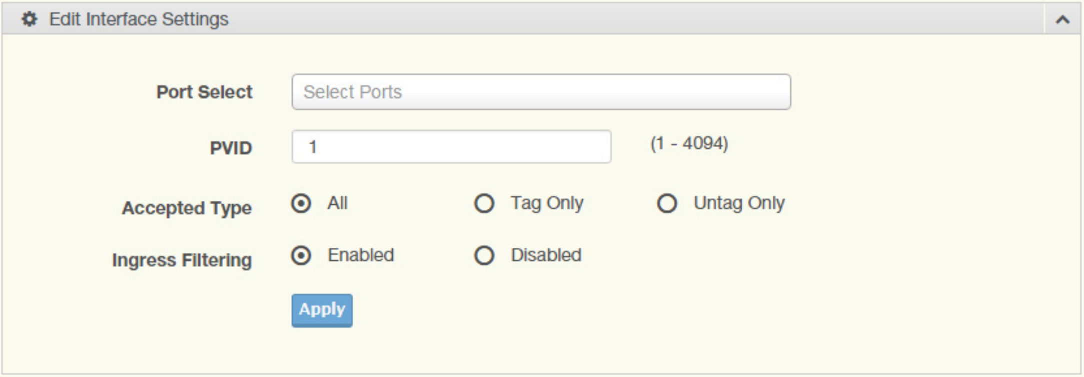
Item	Description
VLAN Action	Click the radio button to add or delete the VLAN entry shown in the previous field.
VLAN ID / VLAN list	Enter the name of the VLAN entry to setup.
VLAN Name VLAN Prefix	Enter the prefix to be used by the VLAN list entry in the previous field.
Apply	Click **Apply** to save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

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

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**.



Edit Interface Settings

Port Select: Select Ports

PVID: 1 (1 - 4094)

Accepted Type: ● All ○ Tag Only ○ Untag Only

Ingress Filtering: ● Enabled ○ Disabled

Figure 26. L2 Switching > 802.1Q VLAN > PVID Settings

The following table describes the items in Figure 26.

Table 23. PVID Settings

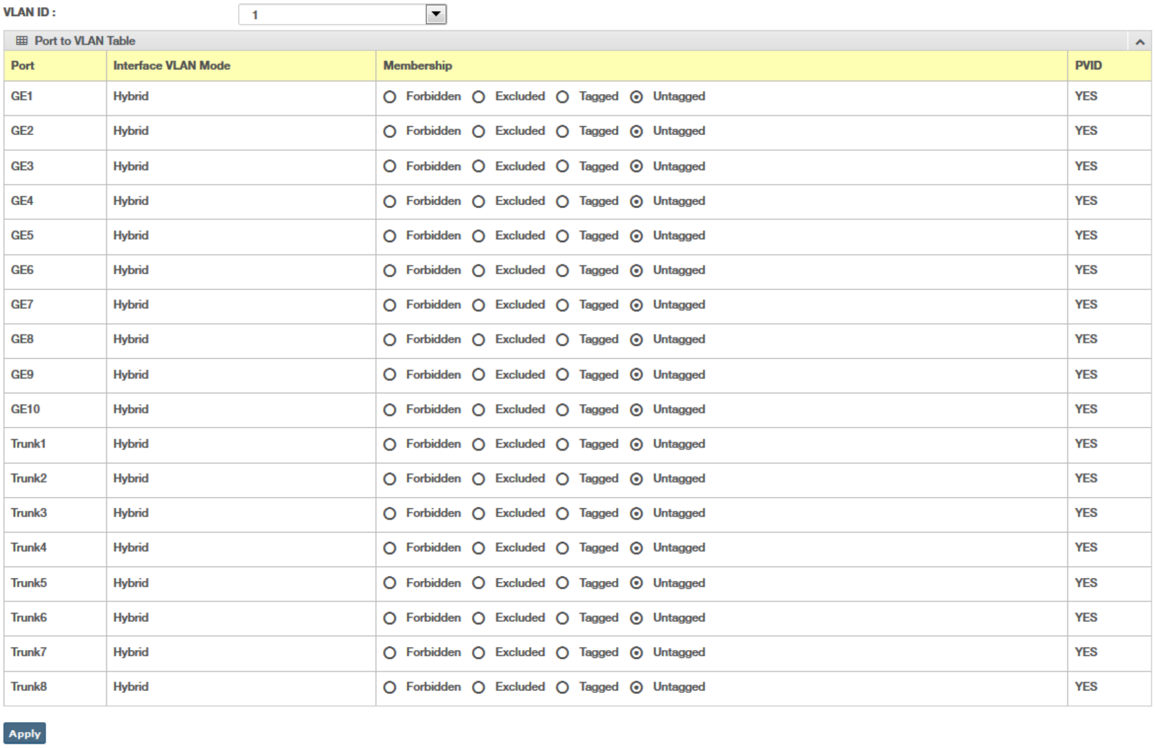
Item	Description
Port Select	Click the drop-down menu to select a port and edit its settings: FE1-FE8, GE1-GE2, or Trunk1 - Trunk8.
PVID	Enter the VLAN ID you want assigned to untagged or priority tagged frames received on this port. The value ranges 1 to 4094. The default is 1.
Accepted Type	Click the radio button to specify which frames to forward. Tag Only discards any untagged or priority tagged frames. Untag Only discards any tagged frames. All 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 **Apply** to save the values and update the screen.

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

Port to VLAN

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

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



VLAN ID : 1

Port to VLAN Table

Port	Interface VLAN Mode	Membership	PVID
GE1	Hybrid	○ Forbidden ○ Excluded ○ Tagged ◉ Untagged	YES
GE2	Hybrid	○ Forbidden ○ Excluded ○ Tagged ◉ Untagged	YES
GE3	Hybrid	○ Forbidden ○ Excluded ○ Tagged ◉ Untagged	YES
GE4	Hybrid	○ Forbidden ○ Excluded ○ Tagged ◉ Untagged	YES
GE5	Hybrid	○ Forbidden ○ Excluded ○ Tagged ◉ Untagged	YES
GE6	Hybrid	○ Forbidden ○ Excluded ○ Tagged ◉ Untagged	YES
GE7	Hybrid	○ Forbidden ○ Excluded ○ Tagged ◉ Untagged	YES
GE8	Hybrid	○ Forbidden ○ Excluded ○ Tagged ◉ Untagged	YES
GE9	Hybrid	○ Forbidden ○ Excluded ○ Tagged ◉ Untagged	YES
GE10	Hybrid	○ Forbidden ○ Excluded ○ Tagged ◉ Untagged	YES
Trunk1	Hybrid	○ Forbidden ○ Excluded ○ Tagged ◉ Untagged	YES
Trunk2	Hybrid	○ Forbidden ○ Excluded ○ Tagged ◉ Untagged	YES
Trunk3	Hybrid	○ Forbidden ○ Excluded ○ Tagged ◉ Untagged	YES
Trunk4	Hybrid	○ Forbidden ○ Excluded ○ Tagged ◉ Untagged	YES
Trunk5	Hybrid	○ Forbidden ○ Excluded ○ Tagged ◉ Untagged	YES
Trunk6	Hybrid	○ Forbidden ○ Excluded ○ Tagged ◉ Untagged	YES
Trunk7	Hybrid	○ Forbidden ○ Excluded ○ Tagged ◉ Untagged	YES
Trunk8	Hybrid	○ Forbidden ○ Excluded ○ Tagged ◉ Untagged	YES

Figure 27. L2 Switching > 802.1Q VLAN > Port to VLAN

The following table describes the items in Figure 27.

Table 24. Port to VLAN

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 **Apply** to save the values and update the screen.

Port-VLAN Mapping

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

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 makes it possible to have more than the 4094 separate VLANs allowed by 802.1Q.

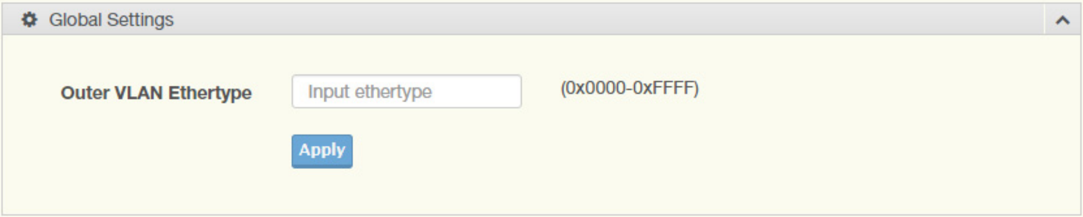
There are three ways in which a machine can be connected to a network carrying double-tagged 802.1ad traffic:

- ❐ via a 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**.



Global Settings

Outer VLAN Ethertype: Input ethertype (0x0000-0xFFFF)

Figure 28. L2 Switching > Q-in-Q > Global Settings

The following table describes the items in Figure 28.

Table 25. Q-in-Q Global Settings

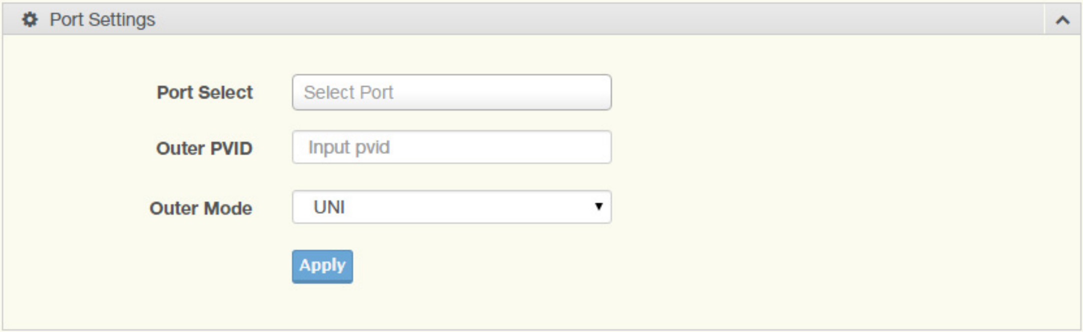
Item	Description
Outer VLAN Ethertype	Enter the outer VLAN handled by the switch giving the attached machine a single-tagged 802.1Q VLAN frame.
Apply	Click **Apply** to save the values and update the screen.

The **QinQ Global Information** settings in the ensuing table are informational only: Outer VLAN Ethertype.

Port Settings

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

To access this page, click **L2 Switching** > **Q-in-Q** > **Port Settings**.



Port Settings

Port Select: Select Port

Outer PVID: Input pvid

Outer Mode: UNI

Figure 29. L2 Switching > Q-in-Q > Port Settings

The following table describes the items in Figure 29.

Table 26. Q-in-Q Port Settings

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 assigned 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	Click the drop-down menu to select between UNI or NNI role. • UNI: Selects a user-network interface which specifies communication between the specified user and a specified network. • NNI: Selects a network-to-network interface which specifies communication between two specified networks.
Apply	Click **Apply** to save the values and update the screen.

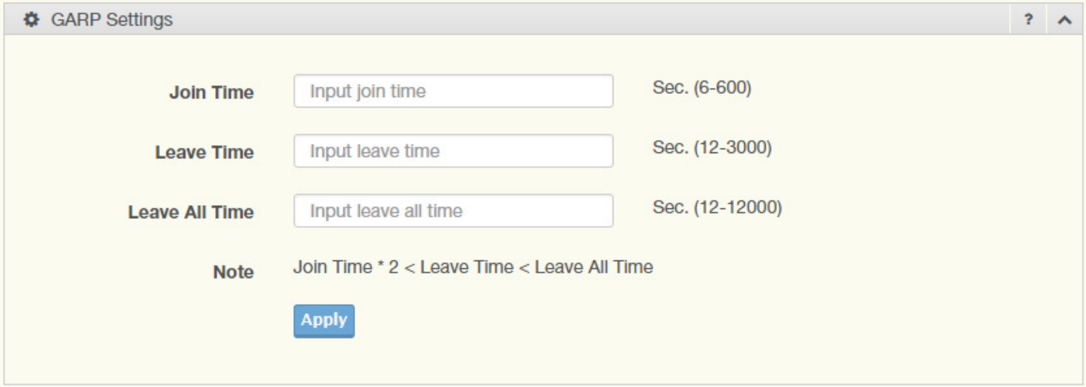
The **QinQ Port Information** settings in the ensuing table are informational only: Port, Outer PVID and Outer Mode.

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	Input join time	Sec. (6-600)
Leave Time	Input leave time	Sec. (12-3000)
Leave All Time	Input leave all time	Sec. (12-12000)
Note	Join Time * 2 < Leave Time < Leave All Time	

Figure 30. L2 Switching > GARP > GARP Settings

The following table describes the items in Figure 30.

Table 27. GARP Settings

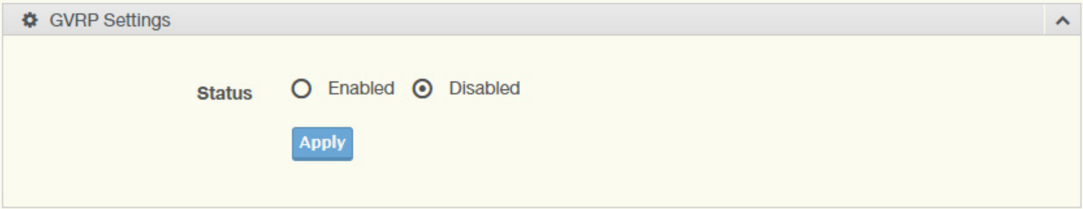
Item	Description
Join Time	Enter a value to specify the time between the transmission of GARP PDUs registering (or re-registering) membership for a VLAN or multicast group in centiseconds. Enter a number between 6 and 600. An instance of this timer exists for each GARP participant for each port.
Leave 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 3000. 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 LeaveAll 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 LeaveAllTime to 1.5*LeaveAllTime. The timer is specified in centiseconds. Enter a number between 12 and 12000. An instance of this timer exists for each GARP participant for each port.
Apply	Click **Apply** to save the values and update the screen.

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

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**.



GVRP Settings

Status ○ Enabled ● Disabled

Figure 31. L2 Switching > GARP > GVRP Settings

The following table describes the items in Figure 31.

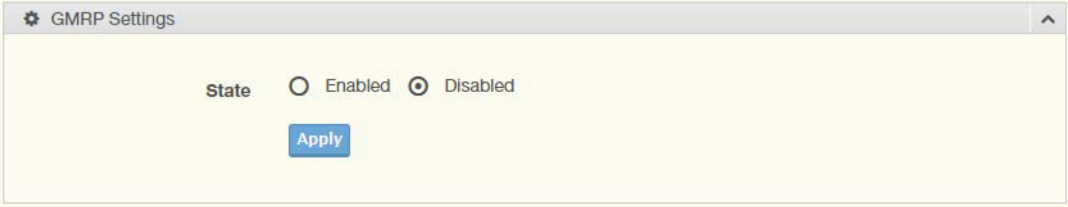
Table 28. GVRP Settings

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 **Apply** to save the values and update the screen.

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

GMRP Settings

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



GMRP Settings

State ○ Enabled ● Disabled

Figure 32. L2 Switching > GARP > GMRP Settings

The following table describes the items in Figure 32.

Table 29. GMRP Settings

Item	Description
Status	Click to enable or disable the GMRP mode for the switch. The factory default is Disable.
Apply	Click **Apply** to save the values and update the screen.

The **GMRP Information** settings in the ensuing table are informational only: GMRP.

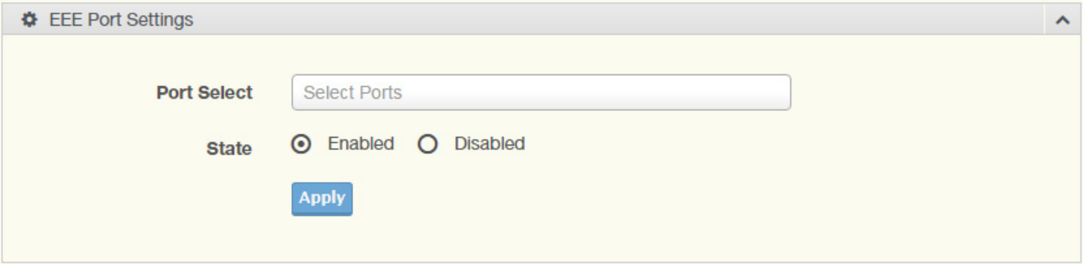
802.3az EEE

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**.



EEE Port Settings

Port Select: Select Ports

State: ● Enabled ○ Disabled

Figure 33. L2 Switching > 802.3az EEE

The following table describes the items in Figure 33.

Table 30. 802.3az EEE

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

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

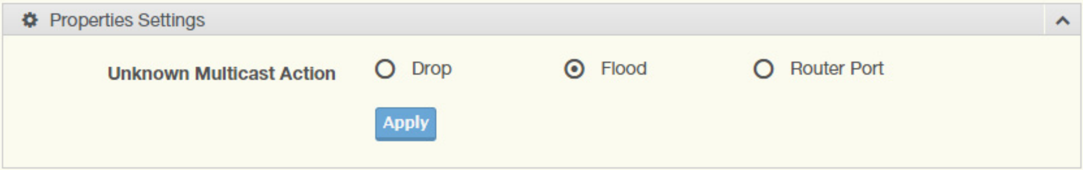
Multicast

Multicast forwarding allows a single packet to be forwarded to multiple destinations. The service is based on 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**.



Properties Settings

Unknown Multicast Action ○ Drop ● Flood ○ Router Port

Figure 34. L2 Switching > Multicast > Multicast Filtering

The following table describes the items in Figure 34.

Table 31. Multicast Filtering

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

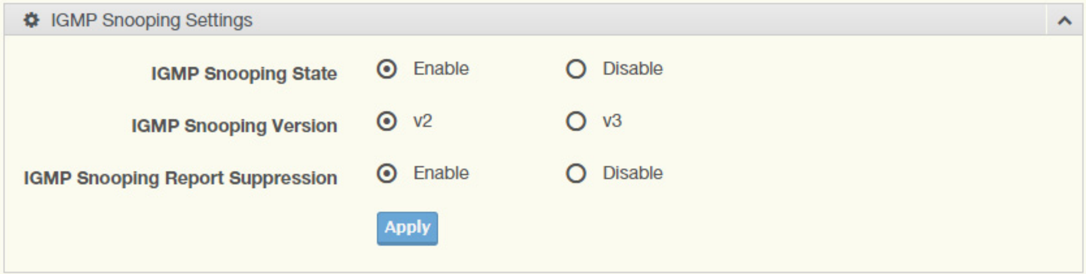
The **Properties Information** settings in the ensuing table are informational only: Unknown Multicast Action.

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**.



IGMP Snooping Settings

IGMP Snooping State ● Enable ○ Disable

IGMP Snooping Version ● v2 ○ v3

IGMP Snooping Report Suppression ● Enable ○ Disable

Figure 35. L2 Switching > Multicast > IGMP Snooping > IGMP Settings

The following table describes the items in Figure 35.

Table 32. IGMP Settings

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

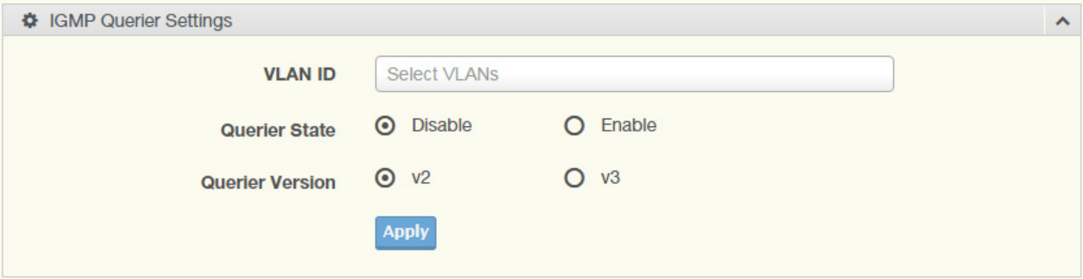
The **IGMP Snooping Information** settings in the ensuing table are informational only: IGMP Snooping State, IGMP Snooping Version and IGMP Snooping V2 Report Suppression.

The **IGMP Snooping Table** settings in the ensuing table 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).

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**.



IGMP Querier Settings

VLAN ID: Select VLANs

Querier State: ● Disable ○ Enable

Querier Version: ● v2 ○ v3

Figure 36. L2 Switching > Multicast > IGMP Snooping > IGMP Querier

The following table describes the items in Figure 36.

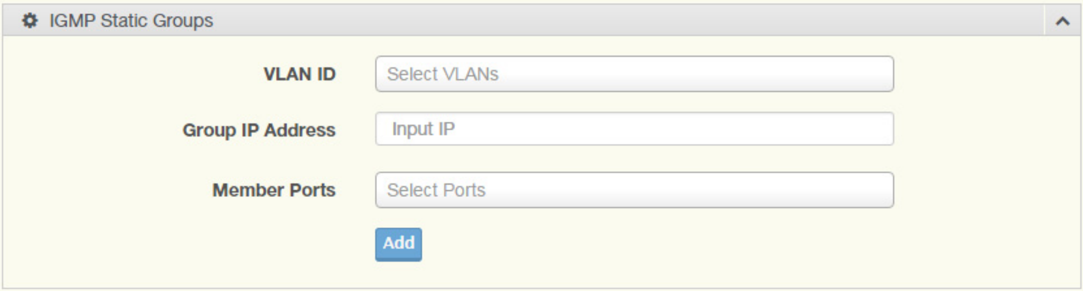
Table 33. IGMP Querier

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

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

IGMP Static Groups

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



IGMP Static Groups

VLAN ID: Select VLANs

Group IP Address: Input IP

Member Ports: Select Ports

Figure 37. L2 Switching > Multicast > IGMP Snooping > IGMP Static Groups

The following table describes the items in Figure 37.

Table 34. IGMP Static Groups

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 **Add** to add an IGMP group.

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

Multicast Groups

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

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

Router Ports

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

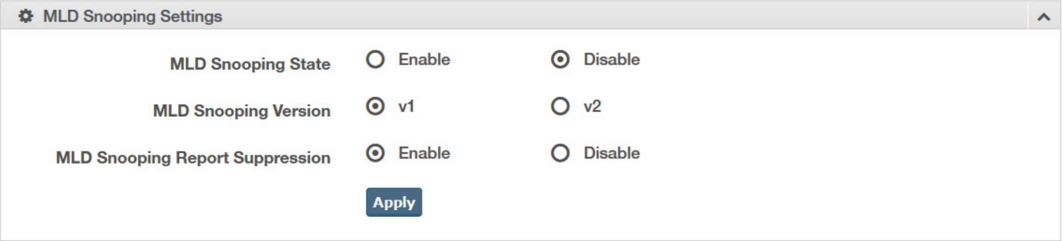
The **Router Ports** settings in the ensuing table are informational only: VLAN ID, Port and Expiry Time (Sec).

MLD Snooping

The MLD Snooping 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 the **MLD Snooping Settings** 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 38. L2 Switching > Multicast > MLD Snooping > MLD Settings

The following table describes the items in Figure 38 on page 65.

Table 35. MLD Settings

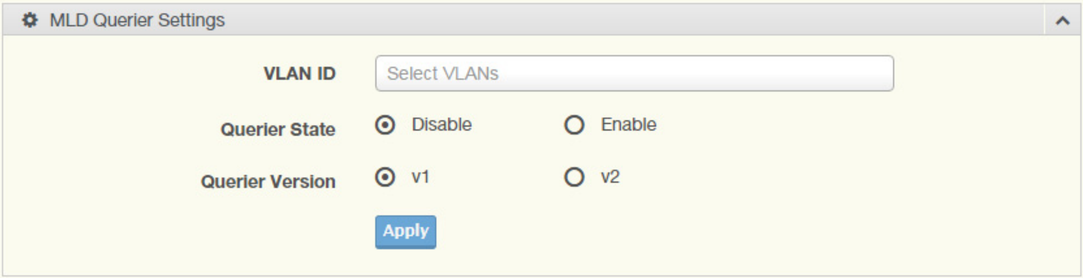
Item	Description
MLD Snooping State	Select **Enable** or **Disable** to setup the MLD Snooping State.
MLD Snooping Version	Select the querier version (V1 or V2) designated to the MLD Snooping Version.
MLD Snooping Report Suppression	Select **Enable** or **Disable** to designate the status of the report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

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

The **MLD Snooping Table** settings in the ensuing table 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).

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**.



MLD Querier Settings

VLAN ID: Select VLANs

Querier State: ● Disable ○ Enable

Querier Version: ● v1 ○ v2

Figure 39. L2 Switching > Multicast > MLD Snooping > MLD Querier

The following table describes the items in Figure 39.

Table 36. MLD Querier

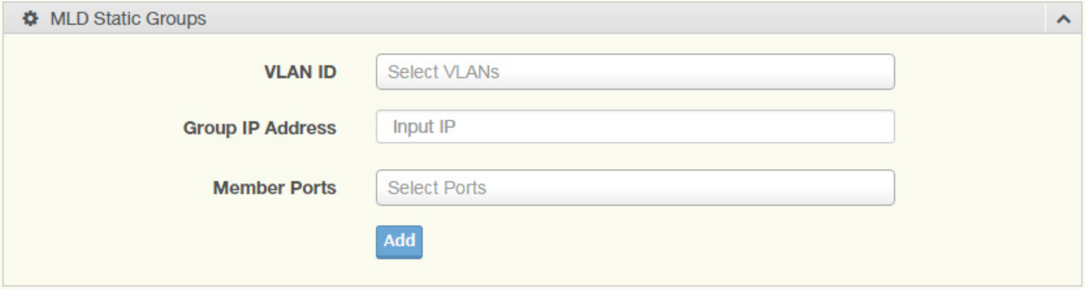
Item	Description
VLAN ID	Enter the VLAN ID to configure.
Querier State	Select **Enable** or **Disable** status on the selected VLAN. • Enable: Enable IGMP Querier Election. • Disable: Disable IGMP Querier Election.
Querier Version	Select the querier version (IGMPV1 or IGMPV2) designated to the MLD Querier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

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

MLD Static Groups

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

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



MLD Static Groups

VLAN ID: Select VLANs

Group IP Address: Input IP

Member Ports: Select Ports

Figure 40. L2 Switching > Multicast > MLD Snooping > MLD Static Groups

The following table describes the items in Figure 40.

Table 37. MLD Static Group

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 **Add** to add a MLD static group.

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

Multicast Groups

To access this page, click **L2 Switching** > **Multicast** > **MLD Snooping** > **Multicast Groups**. This page is informational only.

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

Router Ports

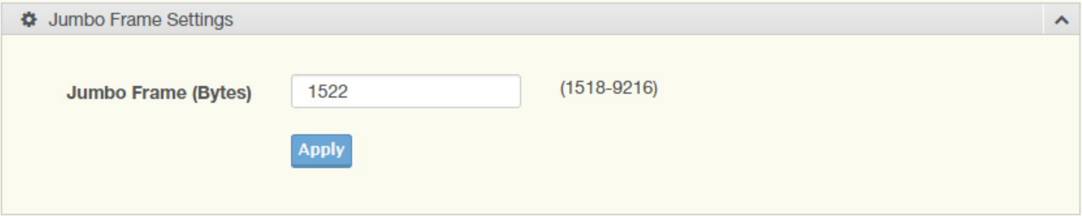
To access this page, click **L2 Switching** > **Multicast** > **MLD Snooping** > **Router Ports**. This page is informational only.

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

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**.



Jumbo Frame Settings

Jumbo Frame (Bytes): 1522 (1518-9216)

Figure 41. L2 Switching > Jumbo Frame

The following table describes the items in Figure 41.

Table 38. Jumbo Frame

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

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

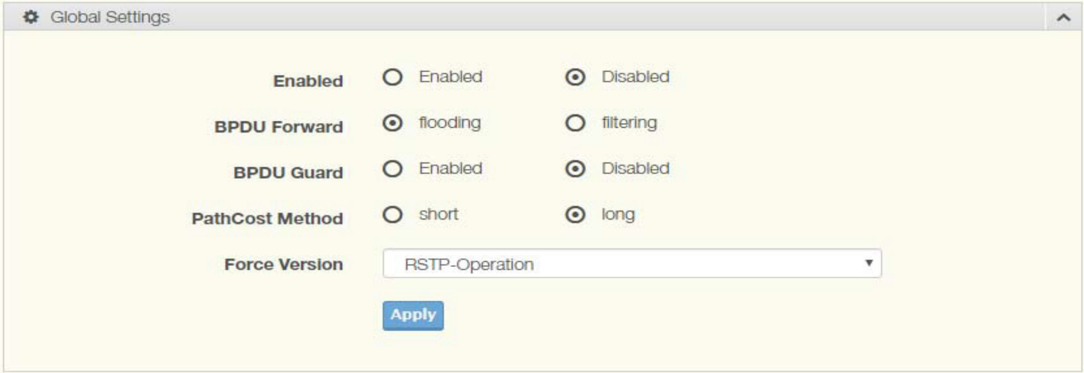
Spanning Tree

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**.



Global Settings

Enabled	○ Enabled	● Disabled
BPDU Forward	● flooding	○ filtering
BPDU Guard	○ Enabled	● Disabled
PathCost Method	○ short	● long
Force Version	RSTP-Operation	

Figure 42. L2 Switching > Spanning Tree > STP Global Settings

The following table describes the items in Figure 42 on page 68.

Table 39. STP Global Settings

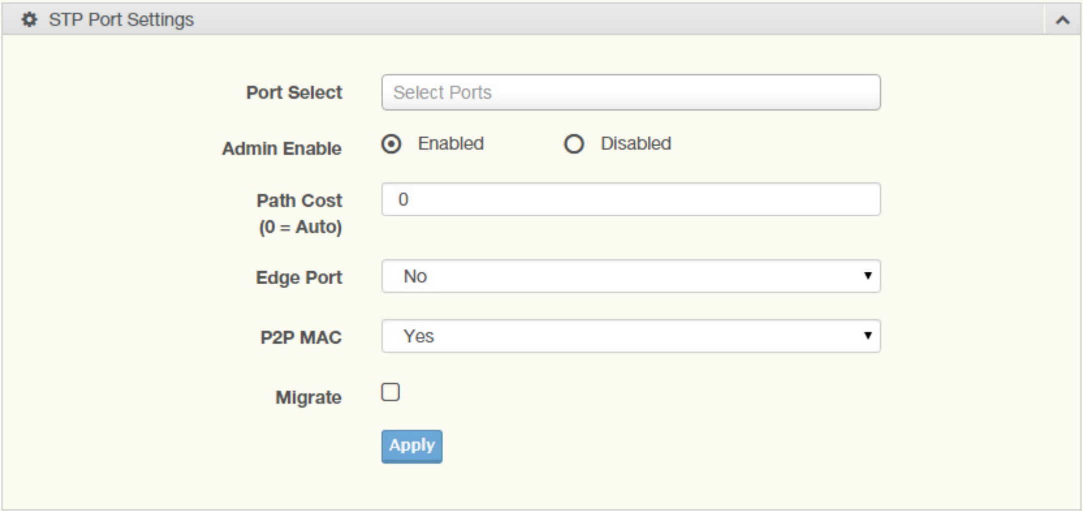
Item	Description
Enabled	Click the radio-button to enable or disable the STP status.
BPDU Forward	Select **flooding** or **filtering** to designate the type of BPDU packet.
BPDU Guard	Click the radio-button to enable or disable the BPDU guard. When enabled, BPDU Guard can disable edge ports that receive BPDU packets. This prevents a new device from entering the existing STP topology. Thus devices that were originally not a part of STP are not allowed to influence the STP topology
PathCost Method	Select short or long to define the method of used for path cost calculations.
Force Version	Click the drop-down menu to select the operating mode for STP. • STP-Compatible: 802.1D STP operation. • RSTP-Operation: 802.1w operation. • MSTP-Operation: 802.1s operation.
Apply	Click **Apply** to save the values and update the screen.

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

STP Port Settings

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

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



STP Port Settings

Port Select	Select Ports
Admin Enable	● Enabled ○ Disabled
Path Cost (0 = Auto)	0
Edge Port	No
P2P MAC	Yes
Migrate	□

Figure 43. L2 Switching > Spanning Tree > STP Port Settings

The following table describes the items in Figure 43.

Table 40. STP Port Settings

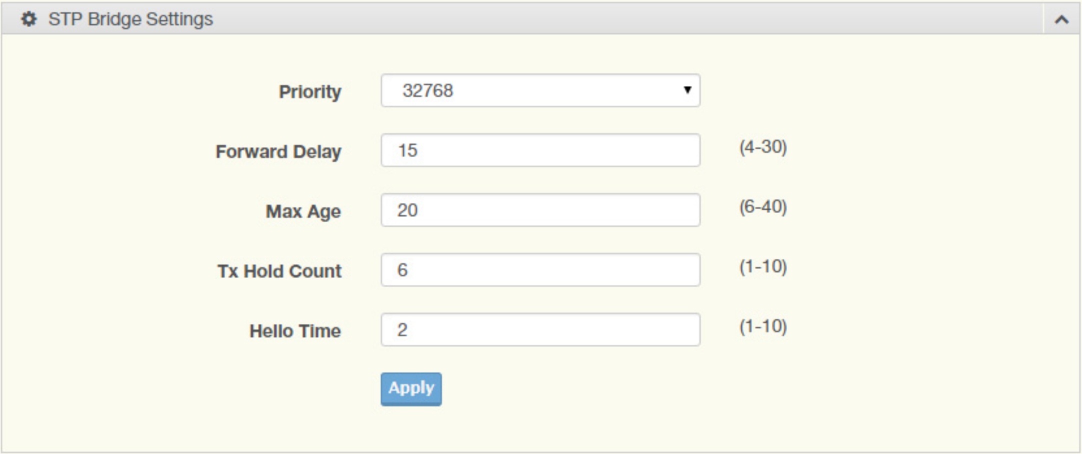
Item	Description
Port Select	Select the port list to specify the ports that apply to this setting.
Enable	Select **Enabled** or **Disabled** to setup the profile for the STP port.
Path Cost (0 = Auto)	Set the port's cost contribution. For a root port, the root path cost for the bridge. (0 means Auto).
Edge Port	Click the drop-down menu to set the edge port configuration. • No: Force to false state (as link to a bridge). • Yes: Force to true state (as link to a host).
P2P MAC	Click the drop-down menu to set the Point-to-Point port configuration. • No: Force to false state. • Yes: Force to true state.
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 **Apply** to save the values and update the screen.

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

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**.



STP Bridge Settings

Priority: 32768 ▾

Forward Delay: 15 (4-30)

Max Age: 20 (6-40)

Tx Hold Count: 6 (1-10)

Hello Time: 2 (1-10)

Figure 44. L2 Switching > Spanning Tree > STP Bridge Settings

The following table describes the items in Figure 44.

Table 41. STP Bridge Settings

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 **Apply** to save the values and update the screen.

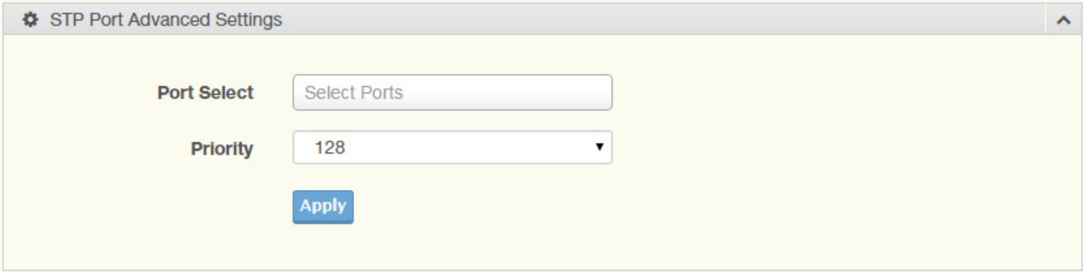
The **STP Bridge Information** settings in the ensuing table are informational only: Priority, Forward Delay, Max Age, Tx Hold Count and Hello Time.

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

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**.


STP Port Advanced Settings

Port Select: Select Ports

Priority: 128

Figure 45. L2 Switching > Spanning Tree > STP Port Advanced Settings

The following table describes the items in Figure 45.

Table 42. STP Port Advanced Settings

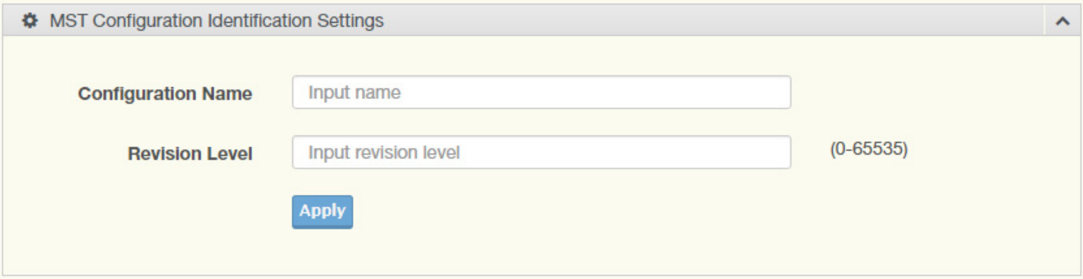
Item	Description
Port Select	Select the port to designate the STP settings.
Priority	Click the drop-down menu to designate a priority.
Apply	Click **Apply** to save the values and update the screen.

The **STP Port Status** settings in the ensuing table 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.

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**.



MST Configuration Identification Settings

Configuration Name: Input name

Revision Level: Input revision level (0-65535)

Figure 46. L2 Switching > Spanning Tree > MST Config Identification

The following table describes the items in Figure 46.

Table 43. MST Config Identification

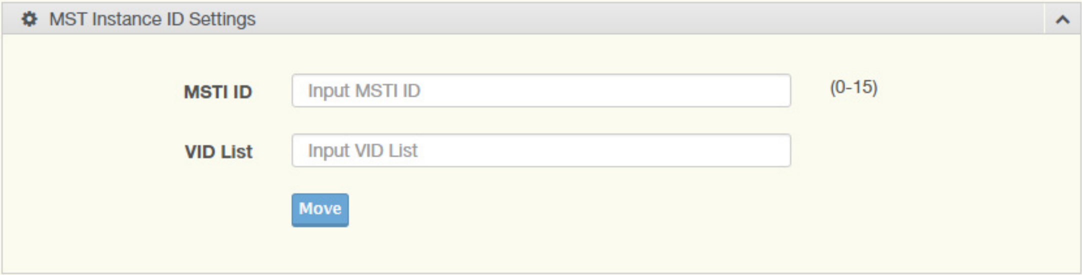
Item	Description
Configuration Name	Enter the identifier used to identify the configuration currently being used. It may be up to 32 characters.
Revision Level	Enter the identifier for the Revision Configuration, range: 0 to 65535 (default: 0).
Apply	Click **Apply** to save the values and update the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

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

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**.



MST Instance ID Settings

MSTI ID: Input MSTI ID (0-15)

VID List: Input VID List

Figure 47. L2 Switching > Spanning Tree > MST Instance ID Settings

The following table describes the items in Figure 47 on page 73.

Table 44. MST Instance ID Settings

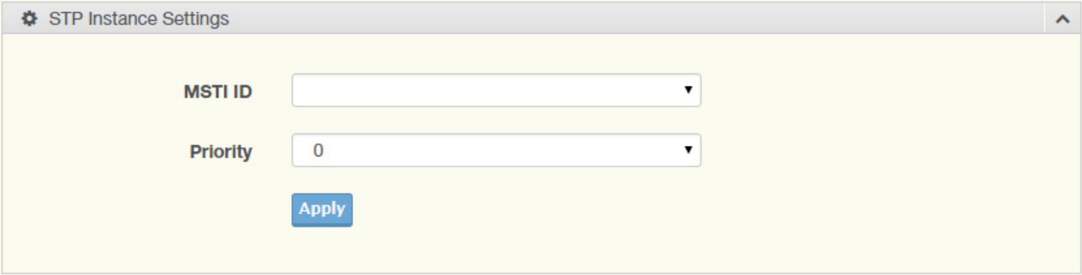
Item	Description
MSTI ID	Enter the MST instance ID (0-15).
VID List	Enter the pre-configured VID list.
Move	Click **Move** to save the values and update the screen.

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

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**.



STP Instance Settings

MSTI ID:

Priority: 0

Figure 48. L2 Switching > Spanning Tree > MST Instance Priority Settings

The following table describes the items in Figure 48.

Table 45. MST Instance Priority Settings

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

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

MST Instance Info

To access this page, click **L2 Switching** > **Spanning Tree** > **MST Instance Info**. The tables in this window are informational only.

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

The **STP Port Status** settings in the ensuing table 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 Statistics

To access this page, click **L2 Switching** > **Spanning Tree** > **STP Statistics**. This window is informational only.

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

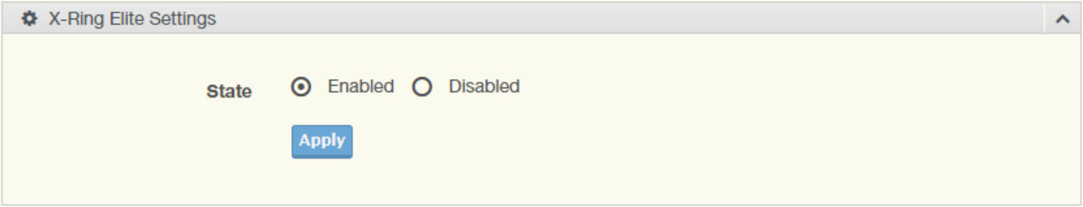
X-Ring Elite

The X-Ring Elite 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 Elite Settings

The X-Ring Elite Settings allows you to enable or disable the state of the X-Ring settings.

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



State ● Enabled ○ Disabled

Figure 49. L2 Switching > X-Ring Elite > X-Ring Elite Settings

The following table describes the items in Figure 49.

Table 46. X-Ring Elite Settings

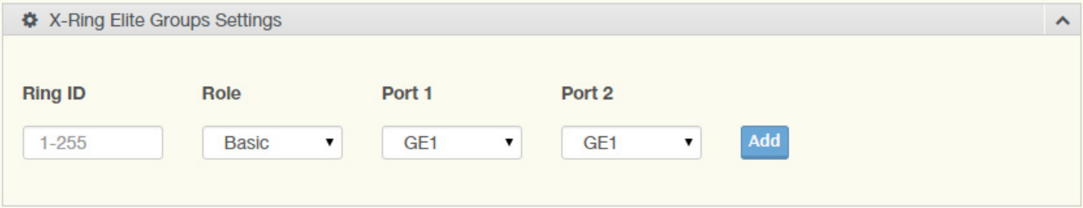
Item	Description
State	Select **Enabled** or **Disabled** to setup the X-Ring Elite mode.
Apply	Click **Apply** to save the values and update the screen.

The **Information** settings in the ensuing table are informational only: X-Ring Elite State.

X-Ring Elite Groups

The X-Ring Elite 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 Elite** > **X-Ring Elite Groups**.



X-Ring Elite Groups Settings

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

Figure 50. L2 Switching > X-Ring Elite > X-Ring Elite Groups

The following table describes the items in Figure 50.

Table 47. X-Ring Elite Groups

Item	Description
Ring ID	Enter a number to specifies a ranging from 1 to 255 to identify a given X-Ring Elite 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 **Add** to save the values and update the screen.

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

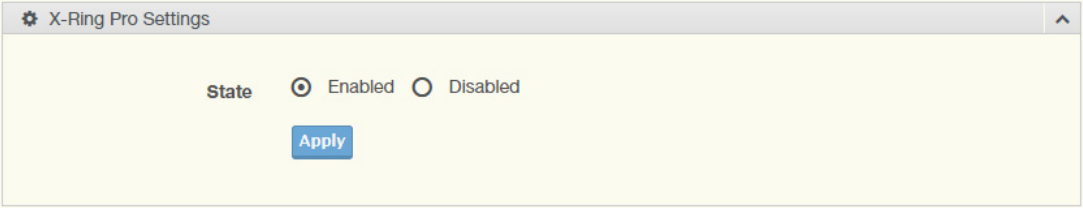
X-Ring Pro

The X-Ring Pro 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 Pro Settings

The X-Ring Pro Settings page allows you to configure the status (enabled or disabled) of the function.

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



X-Ring Pro Settings

State ● Enabled ○ Disabled

Apply

Figure 51. L2 Switching > X-Ring Pro > X-Ring Pro Settings

The following table describes the items in Figure 51 on page 76.

Table 48. X-Ring Pro Settings

Item	Description
State	Select **Enabled** or **Disabled** to setup the X-Ring Pro mode.
Apply	Click **Apply** to save the values and update the screen.

The **Information** settings in the ensuing table are informational only: X-Ring Pro State.

X-Ring Pro Groups

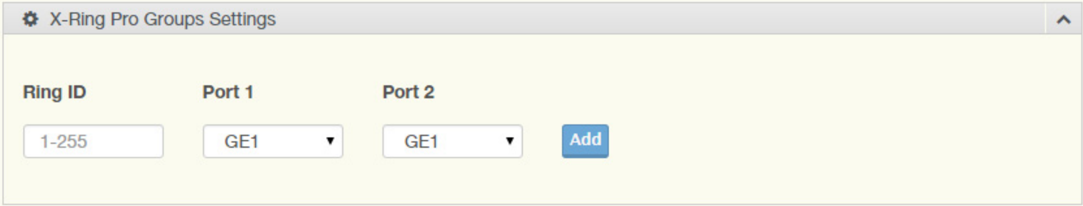
The X-Ring Pro Groups page allows you to select the function and role for each ring ID and its connected ports.

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

The X-Ring Pro Groups page has four configuration areas:

- "X-Ring Pro Groups Settings"
- "Chain Settings" on page 78
- "Couple Settings" on page 78
- "Pair Settings" on page 79
- "RPair Settings" on page 80

X-Ring Pro Groups Settings


X-Ring Pro Groups Settings

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

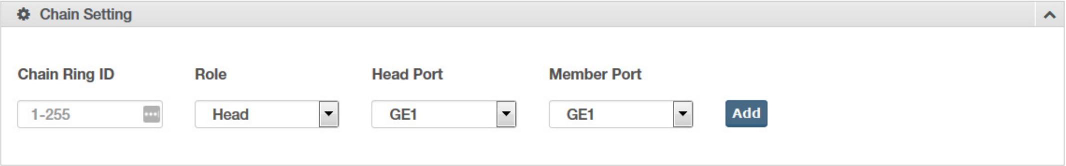
Figure 52. L2 Switching > X-Ring Pro > X-Ring Pro Groups > X-Ring Pro Groups Settings

The following table describes the items in Figure 52.

Table 49. X-Ring Pro Groups Settings

Item	Description
Ring ID	Enter a number to specifies a ranging from 1 to 255 to identify a given X-Ring Pro group.
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 **Add** to save the values and update the screen.

Chain Settings



Chain Setting

Chain Ring ID: 1-255
Role: Head
Head Port: GE1
Member Port: GE1

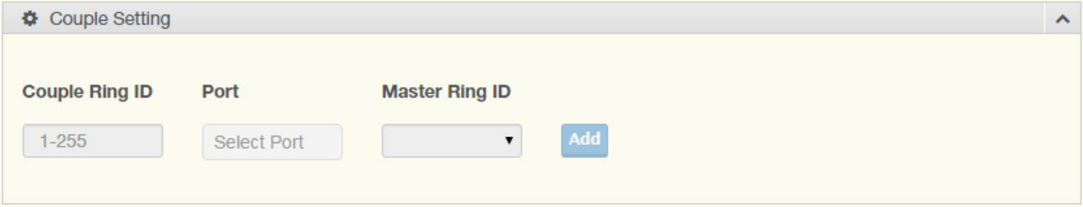
Figure 53. L2 Switching > X-Ring Pro > X-Ring Pro Groups > Chain Setting

The following table describes the items in Figure 53.

Table 50. Chain Setting

Item	Description
Chain Ring ID	Enter a number to specifies a ranging from 1 to 255 to identify a given X-Ring group.
Role	Click the drop-down menu to designate the Role.
Head Port	Click the drop-down menu to designate the head port.
Member Port	Click the drop-down menu to designate the member port.
Add	Click **Add** to save the values and update the screen.

Couple Settings



Couple Setting

Couple Ring ID: 1-255
Port: Select Port
Master Ring ID:

Figure 54. L2 Switching > X-Ring Pro > X-Ring Pro Groups > Couple Setting

The following table describes the items in Figure 54.

Table 51. Couple Setting

Item	Description
Couple Ring ID	Enter a number to specifies a ranging from 1 to 255 to identify a given X-Ring group.
Port	Enter the port to assign to define the couple setting.
Master Ring ID	Click the drop-down menu to designate the master ring.
Add	Click **Add** to save the values and update the screen.

The **Information** settings in the ensuing table are informational only: Ring ID, Mode, Operation State, Port 1, Forwarding State, Port 2, Forwarding State and **Delete** (click to delete the desired Ring ID).

Pair Settings

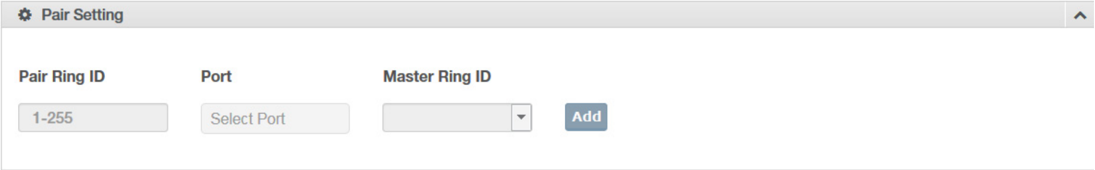


Figure 55. L2 Switching > X-Ring Pro > X-Ring Pro Groups > Pair Setting

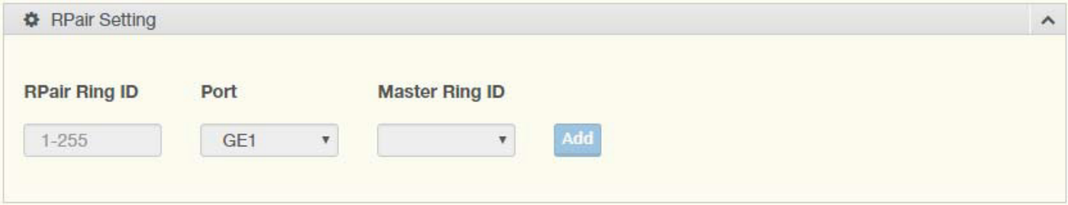
The following table describes the items in Figure 55.

Table 52. Pair Setting

Item	Description
Pair Ring ID	Enter a number to specifies a ranging from 1 to 255 to identify a given X-Ring group.
Port	Enter the port to assign to define the couple setting.
Master Ring ID	Click the drop-down menu to designate the master ring.
Add	Click **Add** to save the values and update the screen.

The **Pair** settings in the ensuing table for are informational only: Ring ID, Port, Master Ring ID and **Add**.

RPair Settings



RPair Ring ID	Port	Master Ring ID
1-255	GE1	

Figure 56. L2 Switching > X-Ring Pro > X-Ring Pro Groups > RPair Setting

The following table describes the items in Figure 55.

Table 53. RPair Setting

Item	Description
RPair Ring ID	Enter a number to specifies a ranging from 1 to 255 to identify a given X-Ring group.
Port	Enter the port to assign to define the couple setting.
Master Ring ID	Click the drop-down menu to designate the master ring.
Add	Click **Add** to save the values and update the screen.

The **RPair** settings in the ensuing table for are informational only: Ring ID, Port, Master Ring ID and **Add**.

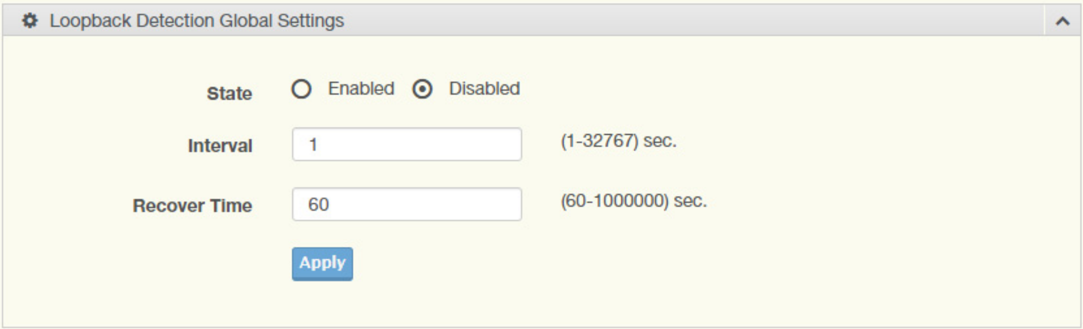
Loopback Detection

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**.



State ○ Enabled ● Disabled

Interval 1 (1-32767) sec.

Recover Time 60 (60-1000000) sec.

Figure 57. L2 Switching > Loopback Detection > Global Settings

The following table describes the items in Figure 57 on page 80.

Table 54. Loopback Detection Global Settings

Item	Description
State	Select **Enabled** or **Disabled** 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 **Apply** to save the values and update the screen.

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

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**.

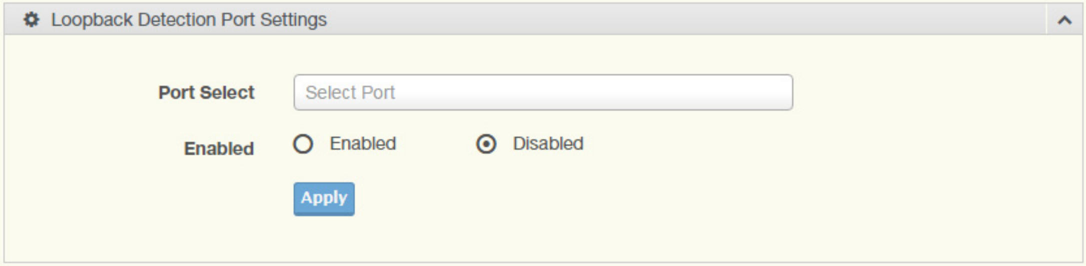


Figure 58. L2 Switching > Loopback Detection > Port Settings

The following table describes the items in Figure 58.

Table 55. Loopback Detection Port Settings

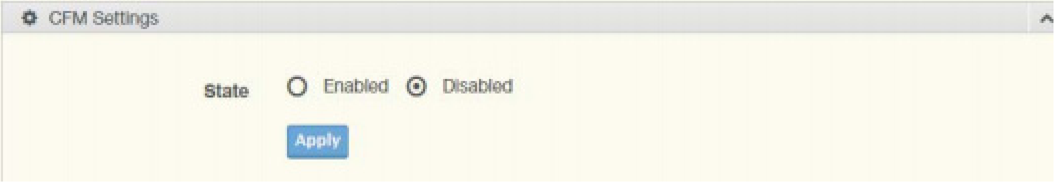
Item	Description
Port Select	Enter the port to define the local loopback detection setting.
Enabled	Select **Enabled** or **Disabled** to setup the Loopback Detection function.
Apply	Click **Apply** to save the values and update the screen.

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

Ethernet CFM

CFM Settings

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



State ○ Enabled ◉ Disabled

Figure 59. L2 Switching > CFM > CFM Settings

The following table describes the items in Figure 62.

Table 56. CFM Settings

Item	Description
State	Select **Enabled** or **Disabled** to enable CFM settings.
Apply	Click **Apply** to save the values and update the screen.

The **CFM** setting in the ensuing table are informational only: CFM State.

ME Groups

To access this page, click **L2 Switching** > **CFM** > **ME Groups**.

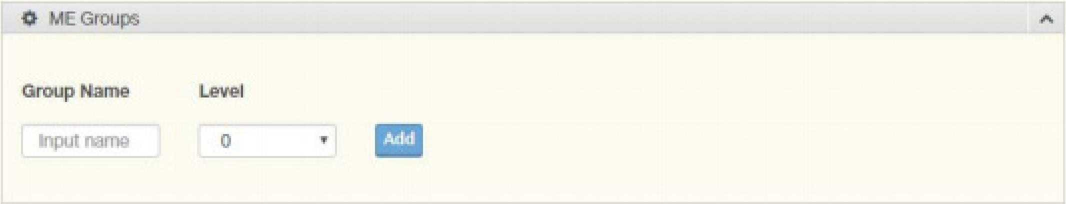


Figure 60. L2 Switching > CFM > ME Groups

The following table describes the items in Figure 60.

Table 57. ME Groups

Item	Description
Group Name	Enter the name for ME group.
Level	Click the drop down menu to select the ME group level.
Add	Click **Add** to add the values and update the screen.

The **ME Groups** setting in the ensuing table are informational only: Group, Level and Delete (click **Delete** to delete the desired ME group).

ME Settings

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

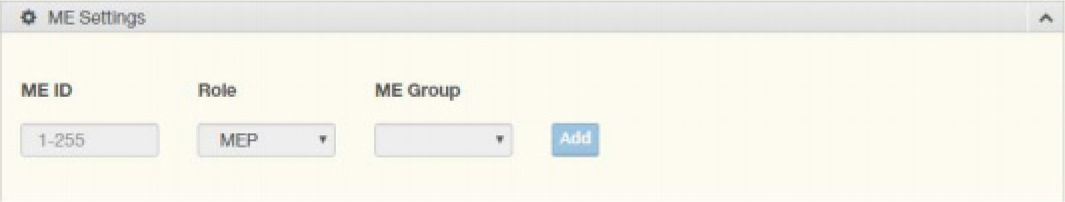


Figure 61. L2 Switching > CFM > ME Settings

The following table describes the items in Figure 61.

Table 58. ME Settings

Item	Description
ME ID	Enter the value to set the ME ID.
Role	Click the drop down menu to select the role. Options include: MEP, MIP, or TRCP.
ME Group	Click the drop down menu to select the ME Group.
Add	Click **Add** to add the values and update the screen.

The **ME** settings in the ensuing table are informational only: ME ID, Role, ME Group, MEG Level and Delete (click **Delete** to delete the desired ME ID).

ERPS Configuration

The International Telecommunication Union (ITU)-T G.8032 Ethernet Ring Protection Switching (ERPS) prevents loops on a per-VLAN basis with networks that are wired in a simple ring topology, and multiple ring and ladder topologies. G.8032 offers a rapid detection and recovery time if a link or node fails (in the order of 50 ms, depending on configuration).

ERPS Settings

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

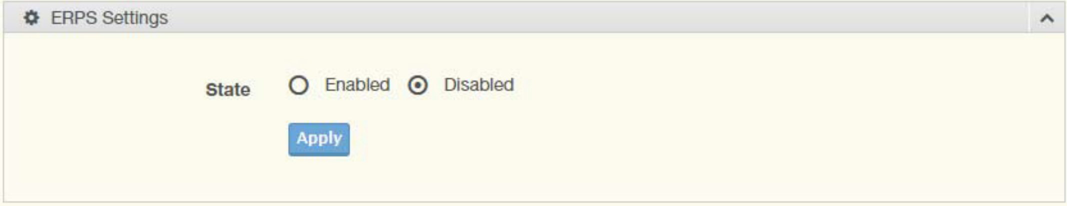


Figure 62. L2 Switching > ERPS > ERPS Settings

The following table describes the items in Figure 62.

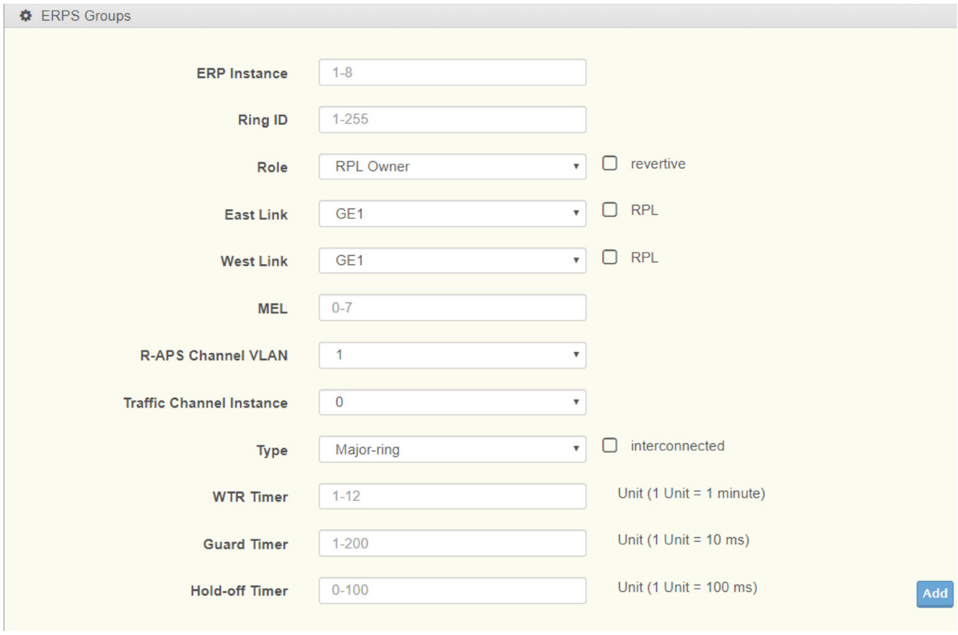
Table 59. ERPS Settings

Item	Description
State	Select **Enabled** to set up the ERPS function.
Apply	Click **Apply** to save the values and update the screen.

The **ERPS** setting in the ensuing table are informational only: State.

ERPS Groups

To access this page, click **L2 Switching** > **ERPS** > **ERPS Groups**.



ERPS Groups

ERP Instance: 1-8

Ring ID: 1-255

Role: RPL Owner ▾ □ revertive

East Link: GE1 ▾ □ RPL

West Link: GE1 ▾ □ RPL

MEL: 0-7

R-APS Channel VLAN: 1 ▾

Traffic Channel Instance: 0 ▾

Type: Major-ring ▾ □ interconnected

WTR Timer: 1-12 Unit (1 Unit = 1 minute)

Guard Timer: 1-200 Unit (1 Unit = 10 ms)

Hold-off Timer: 0-100 Unit (1 Unit = 100 ms)

Figure 63. L2 Switching > ERPS > ERPS Groups

The following table describes the items in Figure 63.

Table 60. ERPS Groups

Item	Description
ERP Instance	Enter the value to set the ERP instance.
Ring ID	Enter the value to set the ring ID.
Role	Click the drop down menu to select the role. Options include: RPL Owner, RPL Neighbor or Other.
East Link	Enter the port to define the east link.
RPL	Check the check box to enable RPL.
West Link	Enter the port to define the west link.
RPL	Check the check box to enable RPL.
MEL	Enter the value to set minimum equipment list.
R-APS Channel VLAN	Click the drop-down menu to select the VLAN.

Table 60. ERPS Groups

Item	Description
Traffic Channel Instance	Click the drop-down menu to select the channel instance.
Type	Click the drop-down menu to select the ERP group type.
WTR Timer	Enter the value to set WTR timer.
Guard Timer	Enter the value to set guard timer.
Hold-off Timer	Enter the value to set hold-off timer.
Add	Click **Apply** to save the values and update the screen.

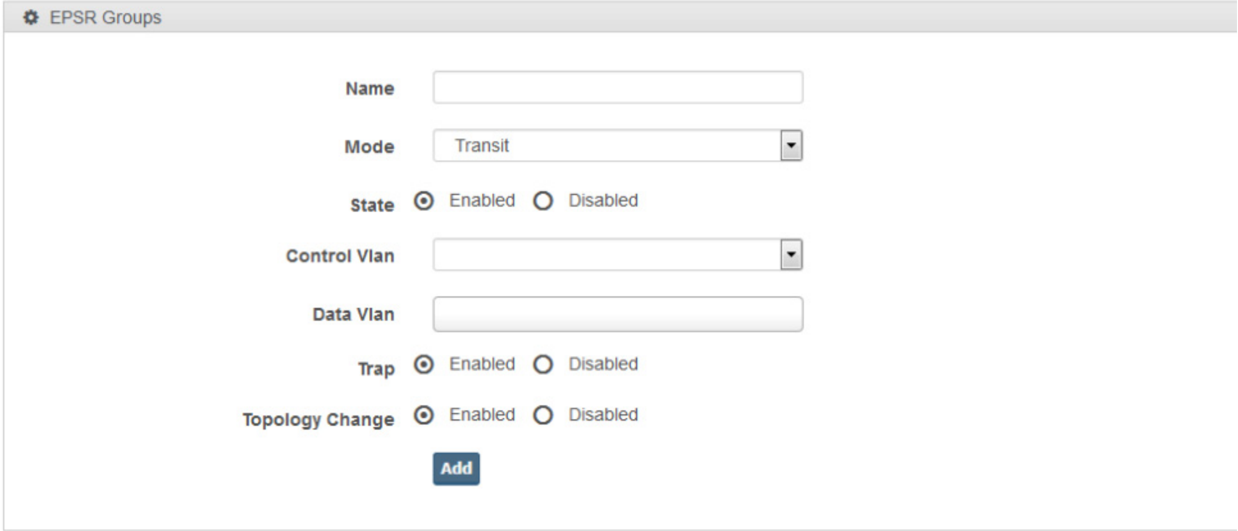
The **ERPS** Groups in the ensuing table are informational only: ERP Instance, Ring ID, Role, East Link, West Link, MEL, R-APS Channel VLAN, Traffic Channel Instance, Type, WTR Timer, Guard Timer, Hold-off Timer.

EPSR Transit

Ethernet Protection Switched Ring is a protection system that prevents loops within Ethernet ring-based topologies. EPSR offers rapid detection and failover recovery rates of less than 50 milliseconds, a rate that is equivalent to that provided by circuit-switched equipment.

EPSR Groups

To access this page, click **L2 Switching** > **EPSR** > **EPSR Groups**.



EPSR Groups

Name

Mode: Transit

State: ● Enabled ○ Disabled

Control Vlan

Data Vlan

Trap: ● Enabled ○ Disabled

Topology Change: ● Enabled ○ Disabled

Figure 64. L2 Switching > EPSR > EPSR Groups

The following table describes the items in Figure 64.

Table 61. EPSR Groups

Item	Description
Name	Enter the EPSR domain name. Use alphanumeric characters only.
Mode	Select the Transit mode from the pull down menu.
State	Select **Enabled** to set up the EPSR function.
Control Vlan	Select the Vlan ID to be set as the control Vlan that carries control messages from the pull down menu.
Data Vlan	Enter the data Vlan that normally carries data.
Trap	Select **Enabled** to send an SNMP trap when the status of the EPSR domain changes.
Topology Change	If the topology of the G.8032 sub ring is changed due to a failure or other reason, select **Enabled** to notify the change the EPSR ring.
Add	Click **Add** to add the values and update the screen.

The **EPSR** setting in the ensuing table are informational only: State.

MAC Address Table

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

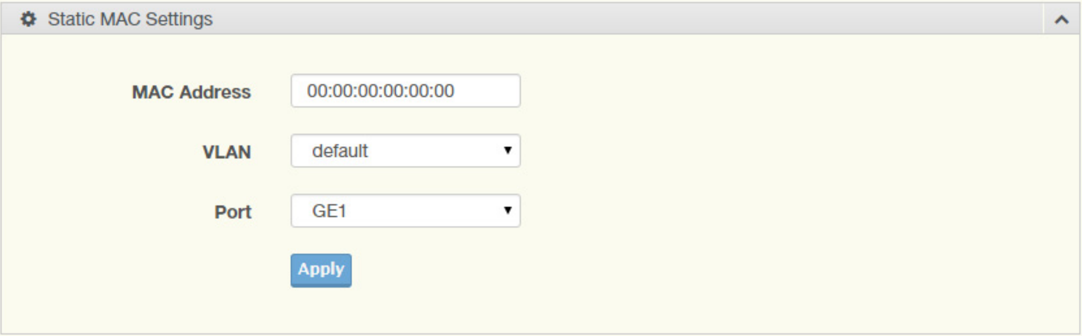
This section includes the following topics:

- "Static MAC"
- "MAC Aging Time" on page 88
- "Dynamic Forwarding Table" on page 88

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**.


Static MAC Settings

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

VLAN default

Port GE1

Figure 65. MAC Address Table > Static MAC

The following table describes the items in Figure 65.

Table 62. Static MAC

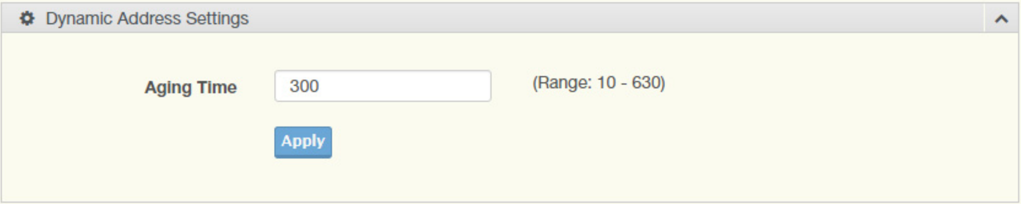
Item	Description
MAC Address	Enter the MAC address to which packets are statically forwarded.
VLAN	Click the drop-down menu to select the VLAN ID number of the VLAN for which the MAC address is residing.
Port	Click the drop-down menu to select the port number.
Apply	Click **Apply** to save the values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

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

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**.



Dynamic Address Settings

Aging Time: 300 (Range: 10 - 630)

Figure 66. MAC Address Table > MAC Aging Time

The following table describes the items in Figure 66.

Table 63. MAC Aging Time

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

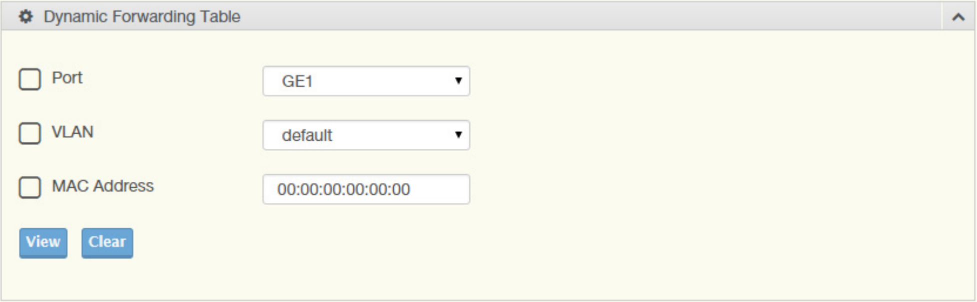
The **Dynamic Address Status** settings in the ensuing table are informational only: Aging time.

Dynamic Forwarding Table

The Dynamic Forwarding function allows you to configure an address tables, 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**.



Dynamic Forwarding Table

□ Port: GE1

□ VLAN: default

□ MAC Address: 00:00:00:00:00:00

Figure 67. MAC Address Table > Dynamic Forwarding Table

The following table describes the items in Figure 67.

Table 64. Dynamic Forwarding Table

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 **View** to display the MAC address information.
Clear	Click **Clear** to clear the MAC Address Information table.

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

Security

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

This section includes the following topics:

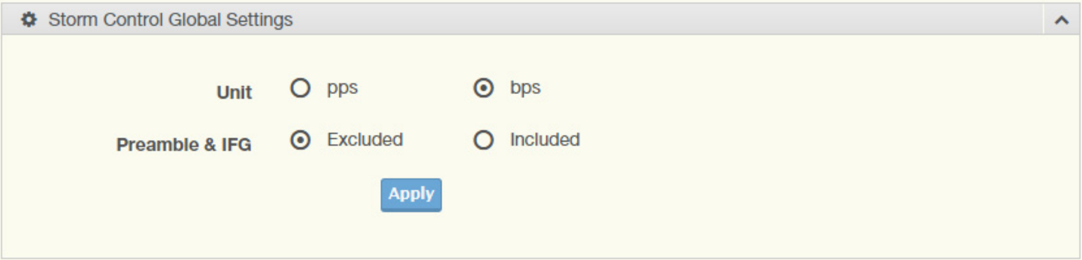
- “Storm Control”
- “Port Security” on page 92
- “Protected Ports” on page 93
- “DoS Prevention” on page 94
- “Applications” on page 96
- “802.1x” on page 99
- “IP Security” on page 101
- “Security Login” on page 102
- “Access Control List” on page 105
- “IP Source Guard” on page 108
- “DHCP Snooping” on page 109
- “ARP Spoofing” on page 111

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**.



Storm Control Global Settings

Unit ○ pps ● bps

Preamble & IFG ● Excluded ○ Included

Figure 68. Security > Storm Control > Global Settings

The following table describes the items in Figure 68.

Table 65. Storm Control Global Settings

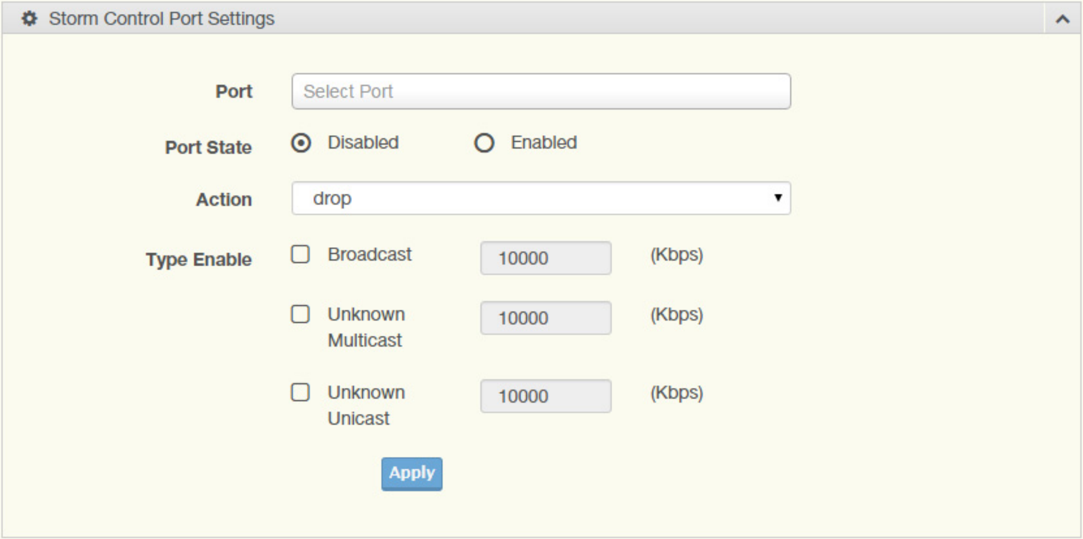
Item	Description
Unit	Select **pps** or **bps** control units for the Storm Control function.
Preamble & IFG	Select **Excluded** or **Included** to setup the Storm Control Global settings. • Excluded: exclude preamble & IFG (20 bytes) when count ingress storm control rate. • Included: include preamble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

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

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**.



Storm Control Port Settings

Port	Select Port		
Port State	● Disabled	○ Enabled	
Action	drop ▾		
Type Enable	□ Broadcast	10000	(Kbps)
	□ Unknown Multicast	10000	(Kbps)
	□ Unknown Unicast	10000	(Kbps)

Figure 69. Security > Storm Control > Port Settings

The following table describes the items in Figure 69.

Table 66. Storm Control Port Settings

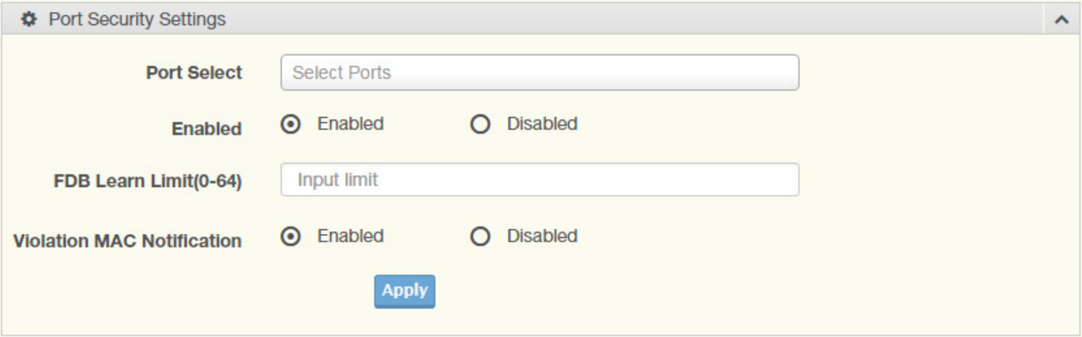
Item	Description
Port	Enter the port number to designate the local port for the Storm Control function.
Port State	Select **Disabled** or **Enabled** to define the port state
Action	Click the drop-down menu to select the type of action to designate for the selected port during a Storm Control incident. The options are Drop and Shutdown.
Type Enable	Click the radio button to enable Broadcast, Unknown Multicast, or Unknown Unicast. • Broadcast: Select the variable in Kbps to define the broadcast bandwidth. • Unknown Multicast: Select the variable in Kbps to define the multicast setting. • Broadcast: Select the variable in Kbps to define the unknown unicast setting.
Apply	Click **Apply** to save the values and update the screen.

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

Port Security

The Port Security page allows you to configure port isolation behavior.

To access this page, click **Security** > **Port Security**.



Port Security Settings

Port Select	Select Ports
Enabled	● Enabled ○ Disabled
FDB Learn Limit(0-64)	Input limit
Violation MAC Notification	● Enabled ○ Disabled

Figure 70. Security > Port Security

The following table describes the items in Figure 70.

Table 67. Port Security

Item	Description
Port Select	Enter a single or multiple port numbers to configure.
Enabled	Select **Enabled** or **Disabled** 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 **Enabled** or **Disabled** to define the selected Port.
Apply	Click **Apply** to save the values and update the screen.

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

Protected Ports

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

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

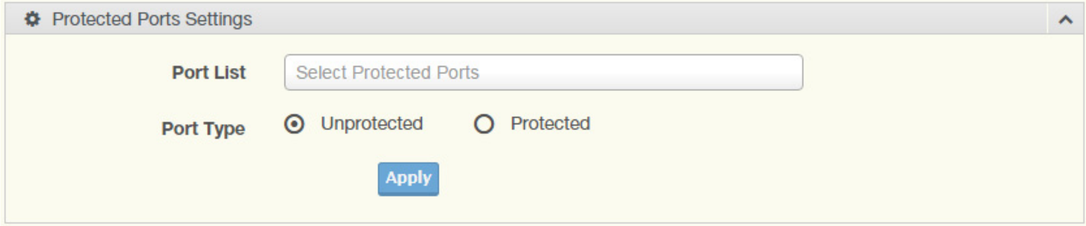


Figure 71. Security > Protected Ports

The following table describes the items in Figure 71 on page 93.

Table 68. Protected Ports

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

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

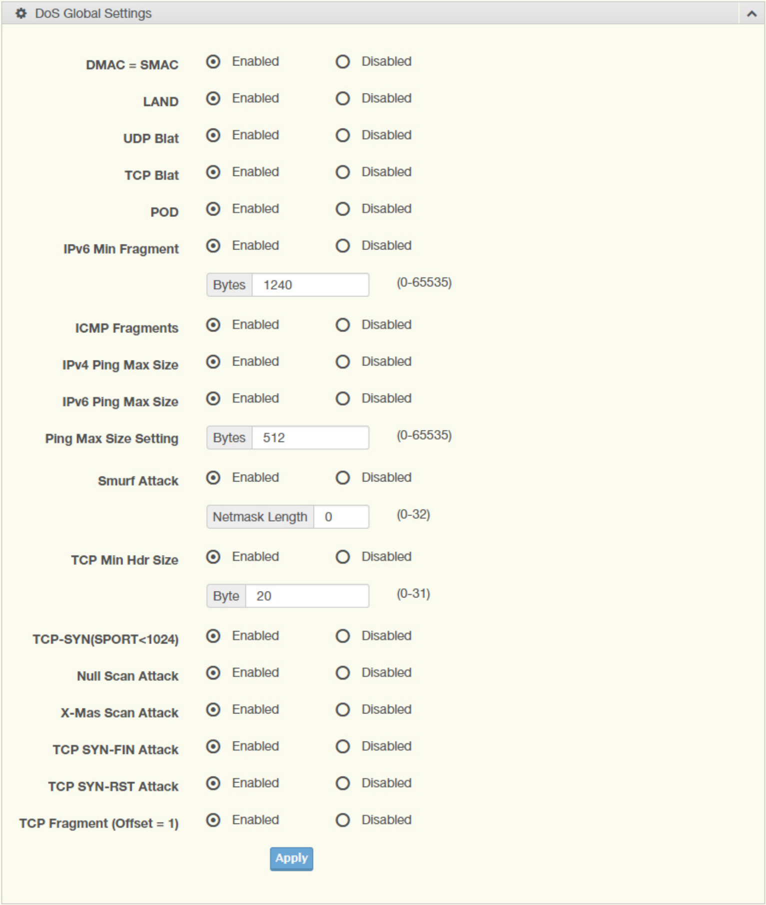
DoS Prevention

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	● Enabled	○ Disabled
LAND	● Enabled	○ Disabled
UDP Blat	● Enabled	○ Disabled
TCP Blat	● Enabled	○ Disabled
POD	● Enabled	○ Disabled
IPv6 Min Fragment	● Enabled	○ Disabled
	Bytes 1240	(0-65535)
ICMP Fragments	● Enabled	○ Disabled
IPv4 Ping Max Size	● Enabled	○ Disabled
IPv6 Ping Max Size	● Enabled	○ Disabled
Ping Max Size Setting	Bytes 512	(0-65535)
Smurf Attack	● Enabled	○ Disabled
	Netmask Length 0	(0-32)
TCP Min Hdr Size	● Enabled	○ Disabled
	Byte 20	(0-31)
TCP-SYN(SPORT<1024)	● Enabled	○ Disabled
Null Scan Attack	● Enabled	○ Disabled
X-Mas Scan Attack	● Enabled	○ Disabled
TCP SYN-FIN Attack	● Enabled	○ Disabled
TCP SYN-RST Attack	● Enabled	○ Disabled
TCP Fragment (Offset = 1)	● Enabled	○ Disabled

Figure 72. Security > DoS Prevention > DoS Global Settings

The following table describes the items in Figure 72 on page 94.

Table 69. DoS Global Settings

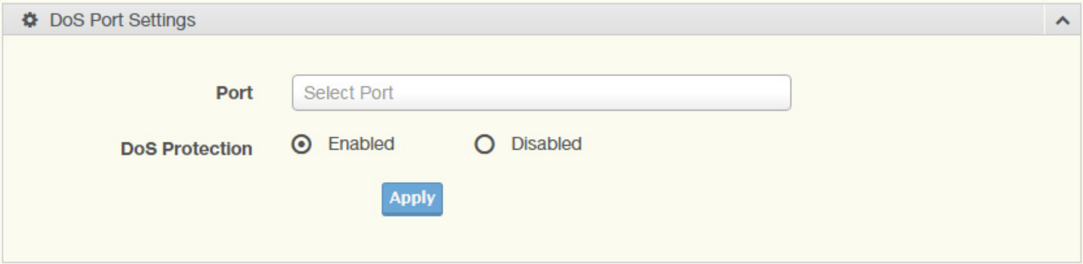
Item	Description
DMAC = SMAC	Click **Enabled** or **Disabled** to define DMAC-SMAC for the DoS Global settings.
LAND	Click **Enabled** or **Disabled** to define LAND for the DoS Global settings.
UDP Blat	Click **Enabled** or **Disabled** to define UDP Blat for the DoS Global settings.
TCP Blat	Click **Enabled** or **Disabled** to define TCP Blat for the DoS Global settings.
POD	Click **Enabled** or **Disabled** to define POD for the DoS Global settings.
IPv6 Min Fragment	Click **Enabled** or **Disabled** 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 **Enabled** or **Disabled** to define the ICMP Fragments function.
IPv4 Ping Max Size	Click **Enabled** or **Disabled** to set the maximum ping size for the IPv4 protocol.
IPv6 Ping Max Size	Click **Enabled** or **Disabled** 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 **Enabled** or **Disabled** to set the Smurf Attack function.
TCP Min Hdr Size	Click **Enabled** or **Disabled** 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 **Enabled** or **Disabled** to set the TCP synchronization function (sport < 1021).
Null Scan Attack	Click **Enabled** or **Disabled** to set the Null Scan Attack function.
X-Mas Scan Attack	Click **Enabled** or **Disabled** to set the X-Mas Scan function.
TCP SYN-FIN Attack	Click **Enabled** or **Disabled** to set the TCP synchronization termination attack function.
TCP SYN-RST Attack	Click **Enabled** or **Disabled** to set the TCP synchronization reset attack function.
TCP Fragment (Offset = 1)	Click **Enabled** or **Disabled** to set the TCP fragment function (offset =1).
Apply	Click **Apply** to save the values and update the screen.

The **DoS Global Information** settings in the ensuing table 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 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**.



DoS Port Settings

Port: Select Port

DoS Protection ● Enabled ○ Disabled

Figure 73. Security > DoS Prevention > DoS Port Settings

The following table describes the items in Figure 73.

Table 70. DoS Port Settings

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

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

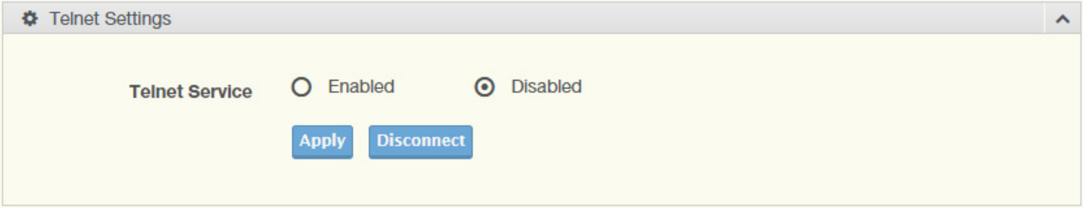
Applications

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**.



Telnet Settings

Telnet Service ○ Enabled ● Disabled

Figure 74. Security > Applications > TELNET

The following table describes the items in Figure 74 on page 96.

Table 71. TELNET

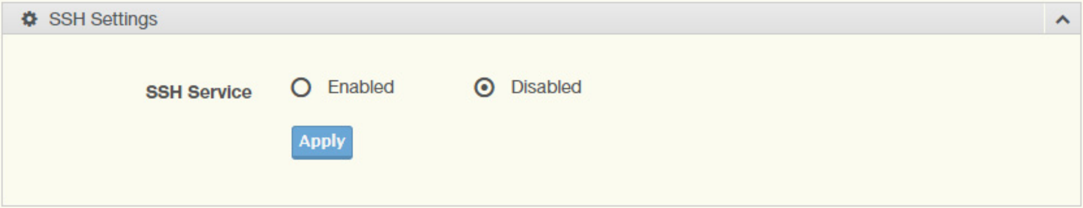
Item	Description
Telnet Service	Click **Enabled** or **Disabled** to set remote access through the Telnet Service function.
Apply	Click **Apply** to save the values and update the screen.
Disconnect	Click **Disconnect** to disable the current Telnet service.

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

SSH

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

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



SSH Settings

SSH Service ○ Enabled ● Disabled

Figure 75. Security > Applications > SSH

The following table describes the items in Figure 75.

Table 72. SSH

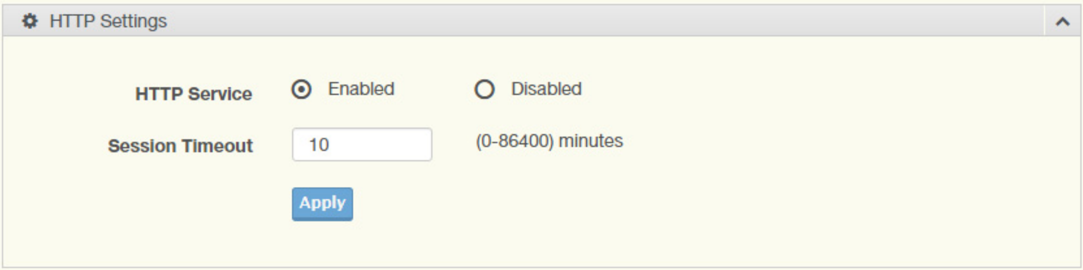
Item	Description
SSH Service	Click **Enabled** or **Disabled** to set up Ethernet encapsulation (remote access) through the Secure Shell (SSH) function.
Apply	Click **Apply** to save the values and update the screen.

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

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**.



HTTP Settings

HTTP Service ● Enabled ○ Disabled

Session Timeout 10 (0-86400) minutes

Apply

Figure 76. Security > Applications > HTTP

The following table describes the items in Figure 76.

Table 73. HTTP

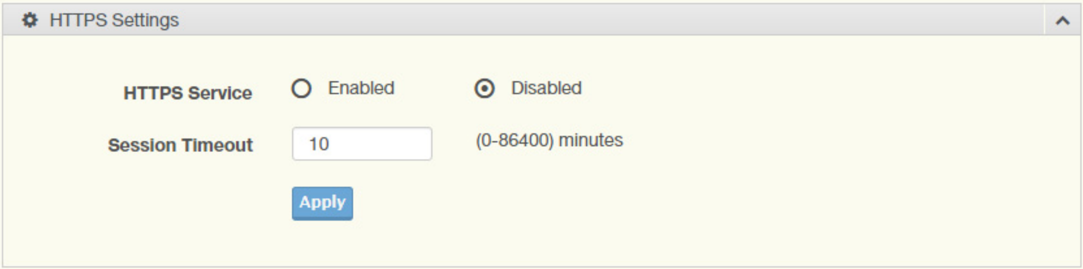
Item	Description
HTTP Service	Click **Enabled** or **Disabled** to set up Ethernet encapsulation (remote access) through HTTP function.
Session Timeout	Enter the variable in minutes (0 to 86400) to define the timeout period for the HTTP session.
Apply	Click **Apply** to save the values and update the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

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

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**.



HTTPS Settings

HTTPS Service ○ Enabled ● Disabled

Session Timeout 10 (0-86400) minutes

Apply

Figure 77. Security > Applications > HTTPS

The following table describes the items in Figure 77 on page 98.

Table 74. HTTPS

Item	Description
HTTPS Service	Click **Enabled** or **Disabled** 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 **Apply** to save the values and update the screen.

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

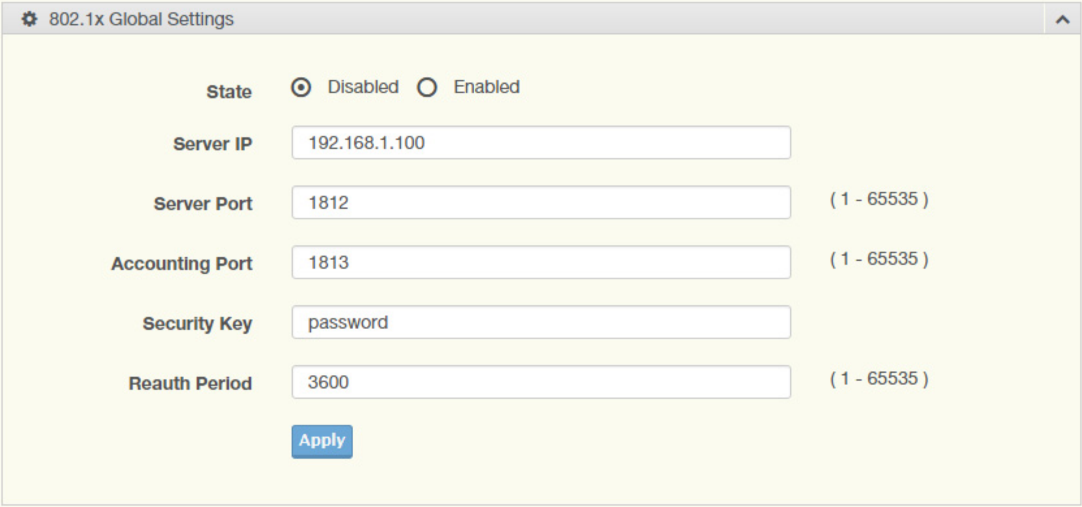
802.1x

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**.



802.1x Global Settings

State ● Disabled ○ Enabled

Server IP: 192.168.1.100

Server Port: 1812 (1 - 65535)

Accounting Port: 1813 (1 - 65535)

Security Key: password

Reauth Period: 3600 (1 - 65535)

Figure 78. Security > 802.1x > 802.1x Settings

The following table describes the items in Figure 78.

Table 75. 802.1X Settings

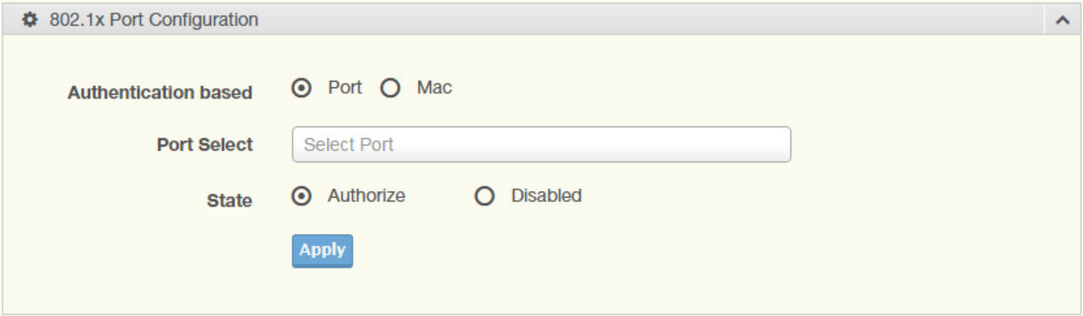
Item	Description
State	Click **Enabled** or **Disabled** to set up 802.1x Setting function.
Server IP	Enter the IP address of the local server providing authentication function.
Server Port	Enter the port number (1 to 65535) assigned to the listed Server IP.
Accounting Port	Enter the port number (1 to 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 **Apply** to save the values and update the screen.

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

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**.



802.1x Port Configuration

Authentication based ● Port ○ Mac

Port Select: Select Port

State ● Authorize ○ Disabled

Figure 79. Security > 802.1x > 802.1x Port Configuration

The following table describes the items in Figure 79.

Table 76. 802.1x Port Configuration

Item	Description
Authentication based	Click **Port** or **Mac** 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 **Authorize** or **Disabled** to define the listed port's state mode.
Apply	Click **Apply** to save the values and update the screen.

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

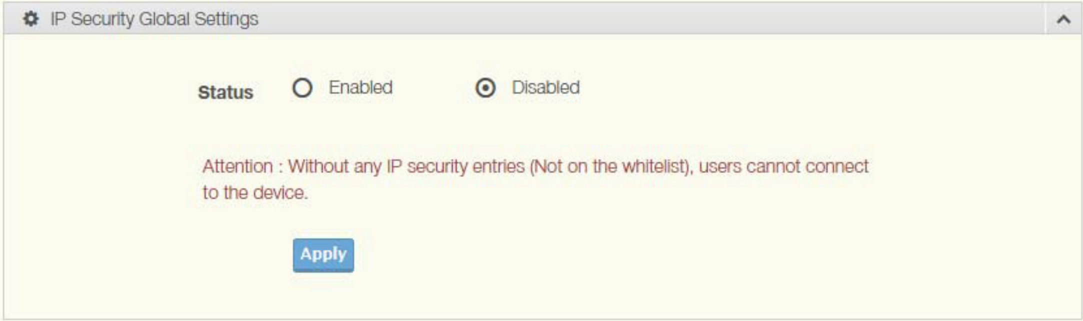
IP Security

This section provides you 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**.



Status ○ Enabled ● Disabled

Attention : Without any IP security entries (Not on the whitelist), users cannot connect to the device.

Figure 80. Security > IP Security > Global Settings

The following table describes the items in Figure 80.

Table 77. IP Security Global Settings

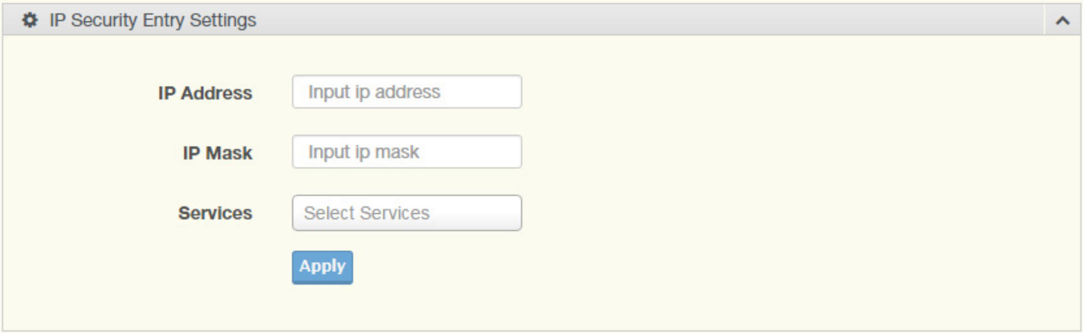
Item	Description
Status	Click **Enabled** or **Disabled** to define the global setting for the IP security function.
Apply	Click **Apply** to save the values and update the screen.

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

Entry Settings

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

To access this page, click **Security** > **IP Security** > **Entry Settings**.



IP Security Entry Settings

IP Address: Input ip address

IP Mask: Input ip mask

Services: Select Services

Figure 81. Security > IP Security > Entry Settings

The following table describes the items in Figure 81 on page 102.

Table 78. IP Security Entry Settings

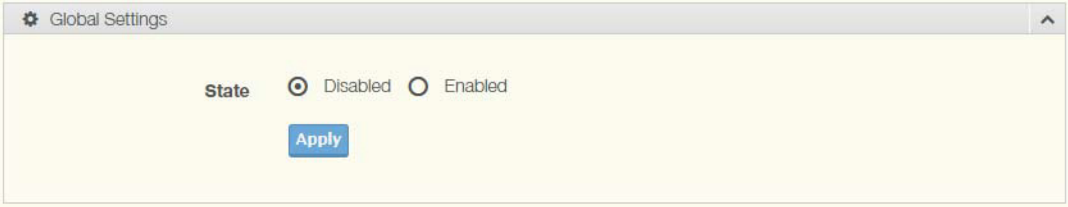
Item	Description
IP Address	Enter the source IP address to apply the IP Security function.
IP Mask	Enter the IP address for use in masking the previous IP Address.
Services	Enter the type of services to associate with the entry setting.
Apply	Click **Apply** to save the values and update the screen.

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

Security Login

Global Settings

This function provides a means to enable or disable the global security settings for the system.
To access this page, click **Security** > **Security Login** > **Global Settings**.



Global Settings

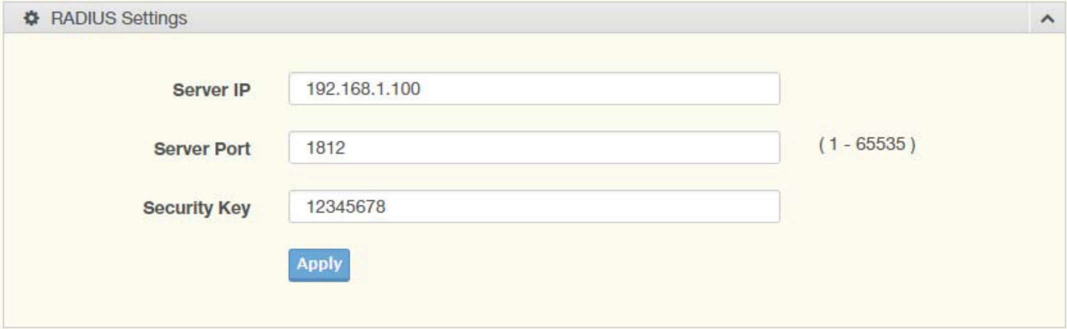
State: ● Disabled ○ Enabled

Figure 82. Security > Security Login > Global Settings

The following table describes the items in Figure 82.

Table 79. Global Settings

Item	Description
State	Click **Enabled** or **Disabled** to set up security login global setting status.
Apply	Click **Apply** to save the values and update the screen.



RADIUS Settings

Server IP: 192.168.1.100

Server Port: 1812 (1 - 65535)

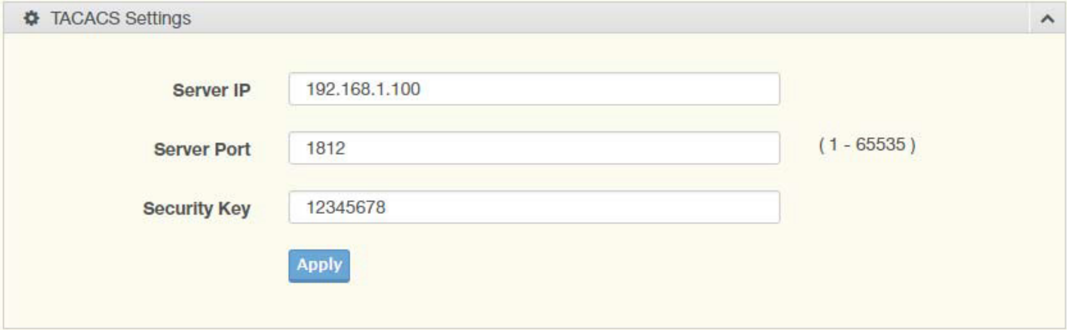
Security Key: 12345678

Figure 83. Security > Security Login > Global Settings > RADIUS Settings

The following table describes the items in Figure 83 on page 103.

Table 80. RADIUS Settings

Item	Description
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.
Security Key	Enter the variable to define the network security key used in authentication.
Apply	Click **Apply** to save the values and update the screen.



TACACS Settings

Server IP: 192.168.1.100

Server Port: 1812 (1 - 65535)

Security Key: 12345678

Figure 84. Security > Security Login > Global Settings > TACACS Settings

The following table describes the items in Figure 84.

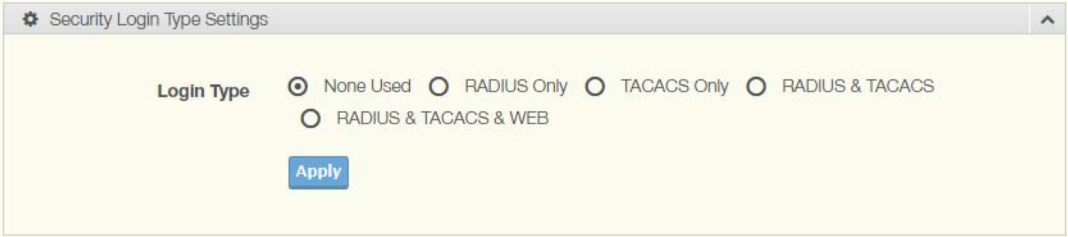
Table 81. TACACS Settings

Item	Description
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.
Security Key	Enter the variable to define the network security key used in authentication.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Global Information** settings are informational only: State, RADIUS Server IP, RADIUS Server Port, RADIUS Security Key, TACACS Server IP, TACACS Server Port and TACACS Security Key.

Access Control Settings

This function specifies the login authentication type for the system.
To access this page, click **Security** > **Security Login** > **Security Login Access Control Settings**.



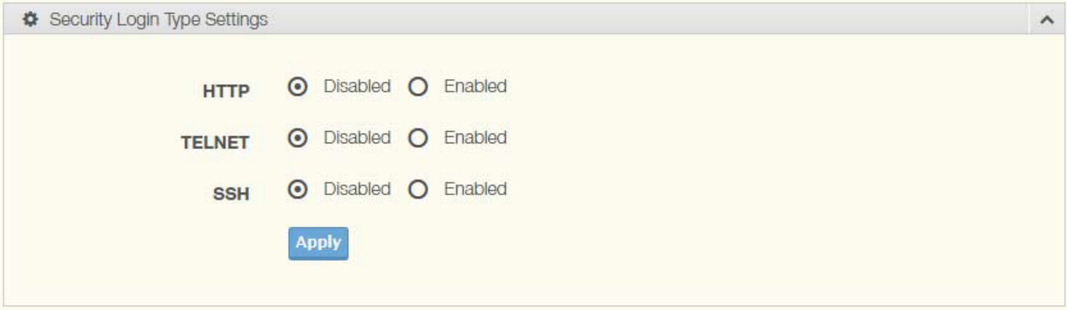
Login Type ● None Used ○ RADIUS Only ○ TACACS Only ○ RADIUS & TACACS ○ RADIUS & TACACS & WEB

Figure 85. Security > Security Login > Access Control Settings

The following table describes the items in Figure 85.

Table 82. Access Control Settings

Item	Description
Login Type	Click to select the login type. Options include: None Used, RADIUS Only, TACACS Only, RADIUS & TACACS or RADIUS & TACACS & WEB.
Apply	Click **Apply** to save the values and update the screen.



Security Login Type Settings

HTTP ● Disabled ○ Enabled

TELNET ● Disabled ○ Enabled

SSH ● Disabled ○ Enabled

Figure 86. Security > Security Login > Access Control Settings > Security Login Type Settings

The following table describes the items in Figure 86.

Table 83. Security Login Type Settings

Item	Description
HTTP	Click **Enabled** or **Disabled** to set up HTTP.
TELNET	Click **Enabled** or **Disabled** to set up HTTPS.
SSH	Click **Enabled** or **Disabled** to set up SSH.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Access Control Information** settings are informational only: Login Type, HTTP, TELNET and SSH.

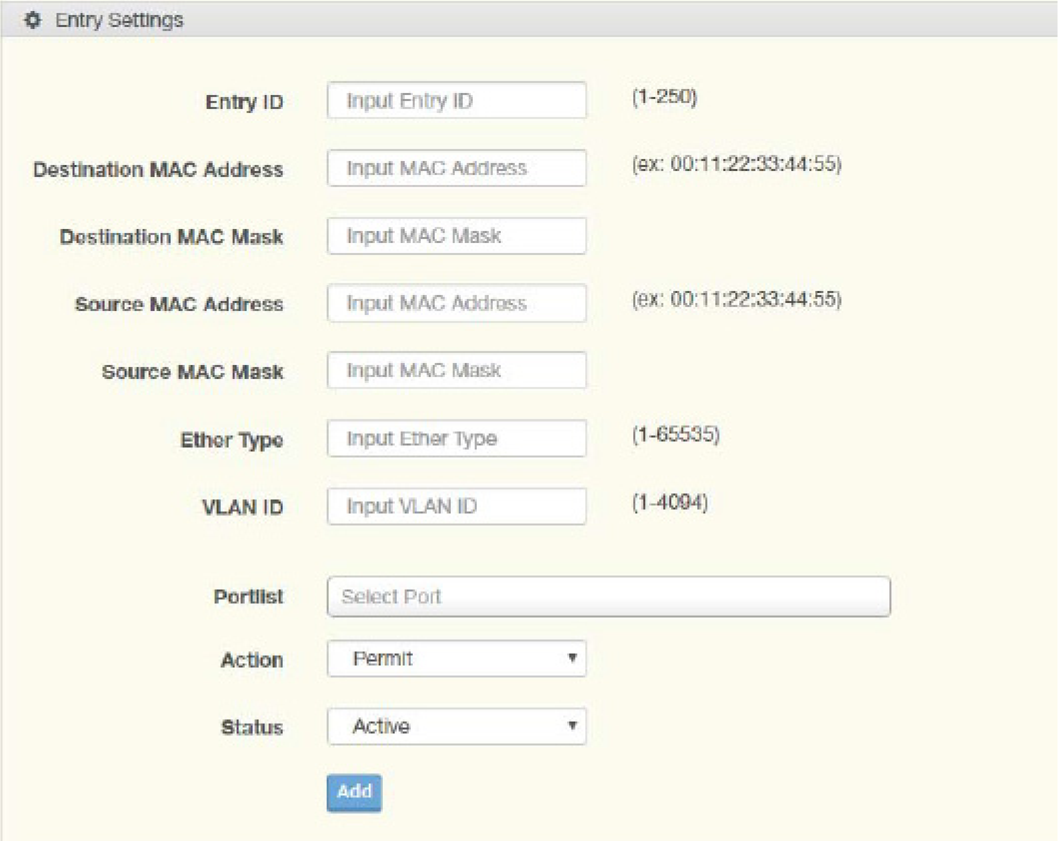
Access Control List

MAC ACL

Entry Settings

To access this page, click **Security** > **Access Control List** > **MAC ACL** >

Entry Settings.



⚙ Entry Settings

Entry ID	Input Entry ID	(1-250)
Destination MAC Address	Input MAC Address	(ex: 00:11:22:33:44:55)
Destination MAC Mask	Input MAC Mask	
Source MAC Address	Input MAC Address	(ex: 00:11:22:33:44:55)
Source MAC Mask	Input MAC Mask	
Ether Type	Input Ether Type	(1-65535)
VLAN ID	Input VLAN ID	(1-4094)
Portlist	Select Port	
Action	Permit ▾	
Status	Active ▾	

Figure 87. Security > Access Control List > MAC ACL > Entry Settings

The following table describes the items in Figure 87.

Table 84. MAC ACL Entry Settings

Item	Description
Entry ID	Type in the value designating the entry ID.
Destination MAC Address	Enter the MAC address to set destination MAC address.
Destination MAC Mask	Enter a value to specify the subnet mask for the destination MAC address.
Source MAC Address	Enter the MAC address to set source MAC address.
Source MAC Mask	Enter a value to specify the subnet mask for the source MAC address.
Ether Type	Enter a value to specify the DNS server for the interface.
VLAN ID	Type in the value designating the VLAN ID.
Portlist	Select the port to configure for the MAC ACL function.
Action	Click the drop down menu to select the MAC ACL action. Options include: Permit or Drop.
Status	Click the drop down menu to select the MAC ACL status. Options include: Active or Inactive.
Add	Click **add** to add a MAC ACL entry.

Entry List

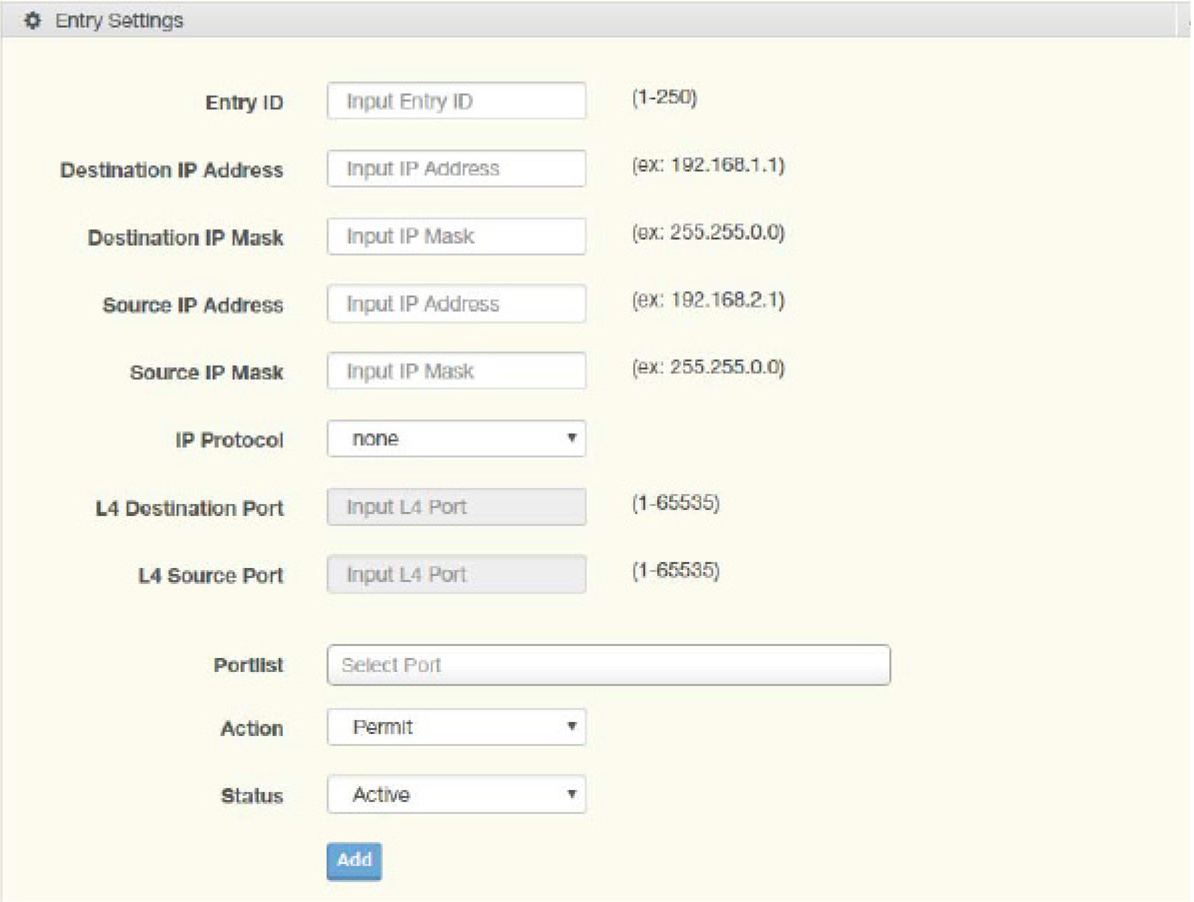
To access this page, click **Security** > **Access Control List** > **MAC ACL** > **Entry List**.

The ensuing table for **MAC ACL Information** settings are informational only: Entry ID, Summary, Portlist, Action, Status and Modify (Click **Edit** to edit the desired entry id or **Delete** to delete the desired entry id).

IP ACL

Entry Settings

To access this page, click **Security** > **Access Control List** > **IP ACL** > **Entry Settings**.



Entry Settings

Entry ID	Input Entry ID	(1-250)
Destination IP Address	Input IP Address	(ex: 192.168.1.1)
Destination IP Mask	Input IP Mask	(ex: 255.255.0.0)
Source IP Address	Input IP Address	(ex: 192.168.2.1)
Source IP Mask	Input IP Mask	(ex: 255.255.0.0)
IP Protocol	none ▾	
L4 Destination Port	Input L4 Port	(1-65535)
L4 Source Port	Input L4 Port	(1-65535)
Portlist	Select Port	
Action	Permit ▾	
Status	Active ▾	

Figure 88. Security > Access Control List > IP ACL > Entry Settings

The following table describes the items in Figure 88.

Table 85. IP ACL Entry Settings

Item	Description
Entry ID	Type in the value designating the entry ID.
Destination IP Address	Enter the IP address to set destination MAC address.
Destination IP Mask	Enter a value to specify the subnet mask for the destination IP address.
Source IP Address	Enter the MAC address to set source IP address.
Source IP Mask	Enter a value to specify the subnet mask for the source IP address.
IP Protocol	Click the drop down menu to select the IP protocol. Options include: none, ICMP, TCP or UDP.
L4 Destination Port	Enter a value to specify the L4 destination port.
L4 Source Port	Enter a value to specify the L4 source port.
Portlist	Select the port to configure for the IP ACL function.
Action	Click the drop down menu to select the IP ACL action. Options include: Permit or Drop.
Assign Queue	Click the drop down menu to select the queue. The function is only available when **Action** is **Assign Queue**.
Status	Click the drop down menu to select the IP ACL status. Options include: Active or Inactive.
Add	Click **add** to add a IP ACL entry.

Entry List

To access this page, click **Security** > **Access Control List** > **IP ACL** > **Entry List**.
The ensuing table for **IP ACL Information** settings are informational only: Entry ID, Summary, Portlist, Action, Status and Modify (Click **Edit** to edit the desired entry id or Delete to delete the desired entry id).

IP Source Guard

Global Settings

To access this page, click **Security** > **IP Source Guard** > **Global Settings**.

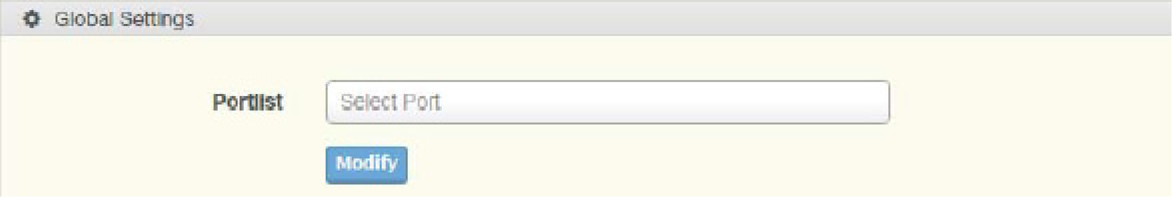


Figure 89. Security > IP Source Guard > Global Settings

The following table describes the items in Figure 89.

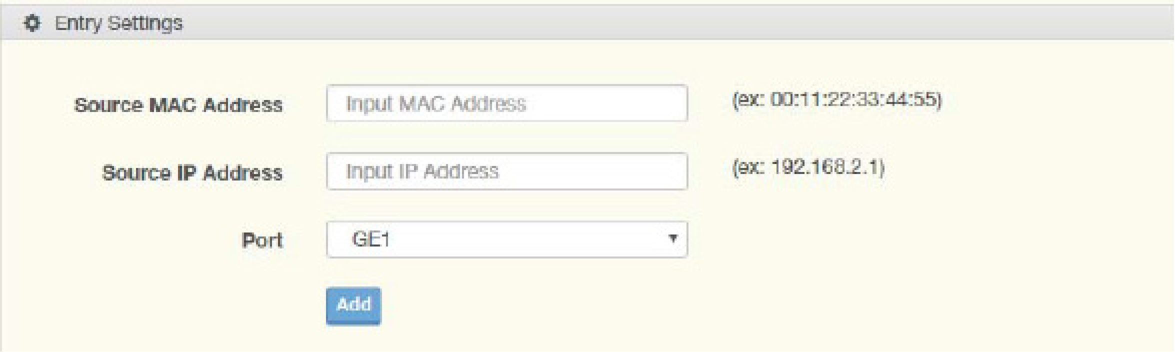
Table 86. IP Source Guard Global Settings

Item	Description
Portlist	Select the port to verify.
Action	Click **Modify** to save the values and update the screen.

The ensuing table for **Global Information** settings are informational only: Verify Ports.

Entry Settings

To access this page, click **Security** > **IP Source Guard** > **Entry Settings**.


Entry Settings

Source MAC Address: Input MAC Address (ex: 00:11:22:33:44:55)

Source IP Address: Input IP Address (ex: 192.168.2.1)

Port: GE1

Figure 90. Security > IP Source Guard > Entry Settings

The following table describes the items in Figure 90.

Table 87. IP Source Guard Entry Settings

Item	Description
Source MAC Address	Enter the MAC address to set source MAC address.
Source IP Address	Enter the IP address to set source IP address
Port	Select the port to configure for the IP source guard.
Add	Click **Add** to add an IP source guard.

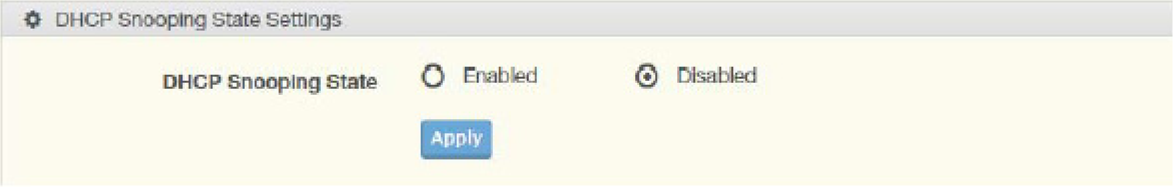
The ensuing table for **Entry Information** settings are informational only: Source MAC, Source IP, Port and Modify (Click **Delete** to delete the desired option).

DHCP Snooping

Global Settings

To access this page, click **Security** > **DHCP Snooping** > **Global**

Settings.



DHCP Snooping State Settings

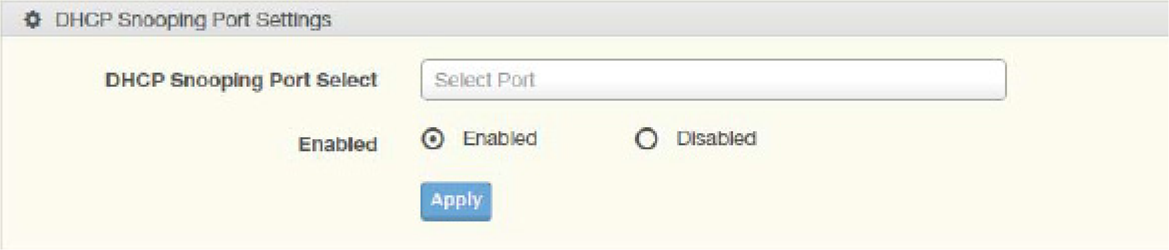
DHCP Snooping State ○ Enabled ◉ Disabled

Figure 91. Security > DHCP Snooping > Global Settings > DHCP Snooping State Settings

The following table describes the items in Figure 91.

Table 88. DHCP Snooping State Settings

Item	Description
DHCP Snooping State	Click Enabled or Disabled to set DHCP snooping state.
Apply	Click **Apply** to save the values and update the screen.



DHCP Snooping Port Settings

DHCP Snooping Port Select: Select Port

Enabled ◉ Enabled ○ Disabled

Figure 92. Security > DHCP Snooping > Global Settings > DHCP Snooping Port Settings

The following table describes the items in Figure 92.

Table 89. DHCP Snooping Port Settings

Item	Description
DHCP Snooping Port Select	Select the port to configure for the DHCP Snooping port.
Enabled	Click **Enabled** or **Disabled** to enable the DHCP Snooping port.
Apply	Click **Apply** to save the values and update the screen.

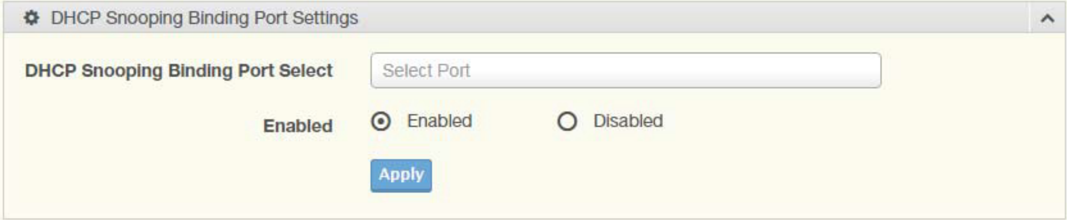

DHCP Snooping Binding Port Settings
DHCP Snooping Binding Port Select
Select Port
Enabled
● Enabled
○ Disabled
Apply

Figure 93. Security > DHCP Snooping > Global Settings > DHCP Snooping Binding Port Settings

The following table describes the items in Figure 92.

Table 90. DHCP Snooping Binding Port Settings

Item	Description
DHCP Snooping Binding Port Select	Select the port to configure for the DHCP Snooping binding port.
Enabled	Click **Enabled** or **Disabled** to enable the DHCP Snooping port.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **DHCP Snooping Information** settings are informational only: DHCP Snooping, DHCP Snooping Port and DHCP Snooping Binding Port.

Entry Settings

To access this page, click **Security** > **DHCP Snooping** > **Entry Settings**. The ensuing table for **IP Security Entry Information** settings are informational only: MAC Address, IP Address, Lease Time, VLAN Id and Port.

ARP Spoofing

To access this page, click **Security** > **ARP Spoofing**.

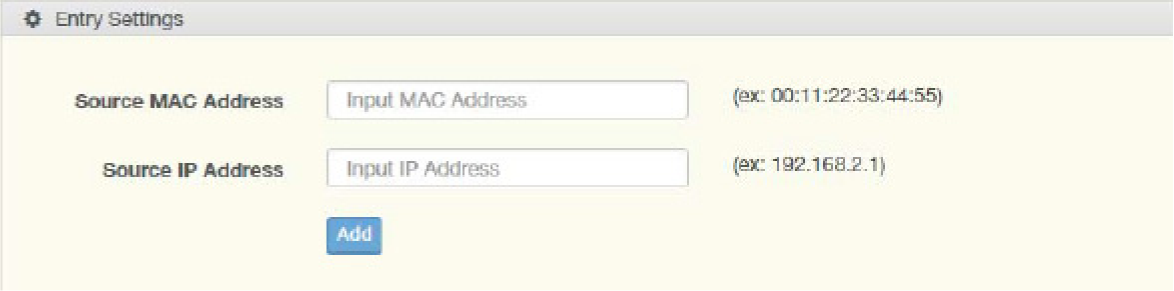


Figure 94. Security >ARP Spoofing

The following table describes the items in Figure 94.

Table 91. Security ARP Spoofing

Item	Description
Source MAC Address	Enter the MAC address to set source MAC address.
Source IP Address	Enter the IP addr3ess to set source IP address.
Add	Click **Add** to add an ARP spoofing.

The ensuing table for **Entry Information** settings are informational only: Source MAC, Source IP and Modify.

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.

This section includes the following topics:

- "General"
- "QoS Basic Mode" on page 119
- "Rate Limit" on page 120
- "Bandwidth Guarantee" on page 122

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.

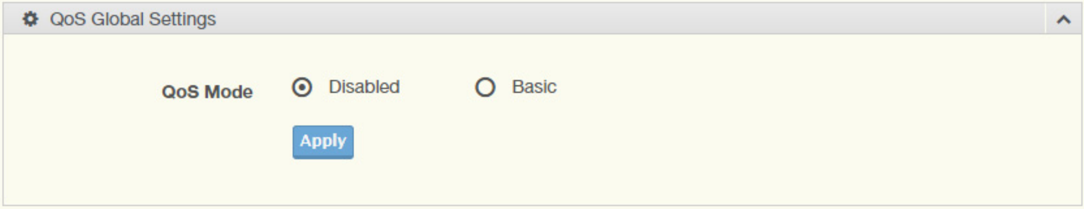
The QoS feature can be configured for congestion-management and congestion-avoidance to specifically manage the priority of the traffic delivery. Implementing QoS in the network makes performance predictable and bandwidth utilization much more effective.

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**.



QoS Global Settings

QoS Mode ● Disabled ○ Basic

Figure 95. QoS > General > QoS Properties

The following table describes the items in Figure 95.

Table 92. QoS Properties

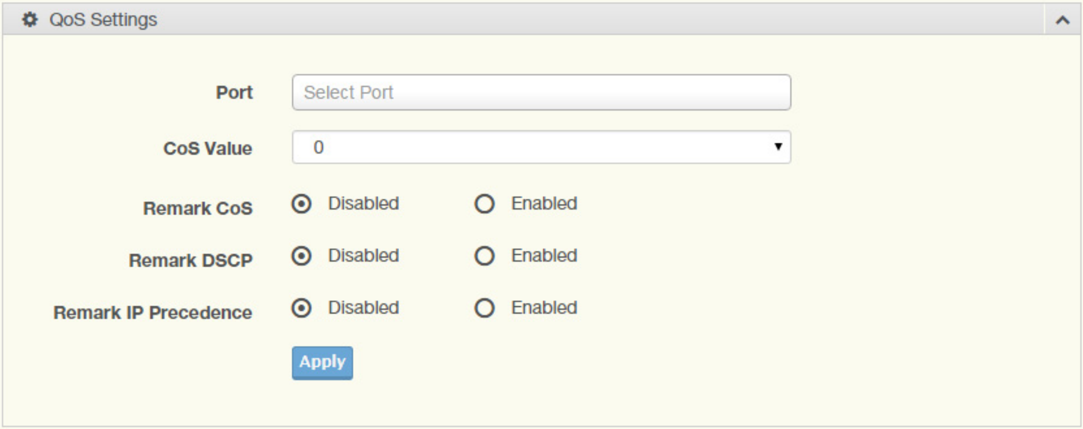
Item	Description
QoS Mode	Select **Disabled** or **Basic** to setup the QoS function.
Apply	Click **Apply** to save the values and update the screen.

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

QoS Settings

Once the QoS function is enabled, you can configure the available settings.

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



QoS Settings

Port: Select Port

CoS Value: 0

Remark CoS: ● Disabled ○ Enabled

Remark DSCP: ● Disabled ○ Enabled

Remark IP Precedence: ● Disabled ○ Enabled

Figure 96. QoS > General > QoS Settings

The following table describes the items in Figure 96.

Table 93. QoS Settings

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 **Disabled** or **Enabled** 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 **Disabled** or **Enabled** to setup the DSCP remark option for the QoS function.
Remark IP Precedence	Click **Disabled** or **Enabled** to setup the Remark IP Precedence for the QoS function.
Apply	Click **Apply** to save the values and update the screen.

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

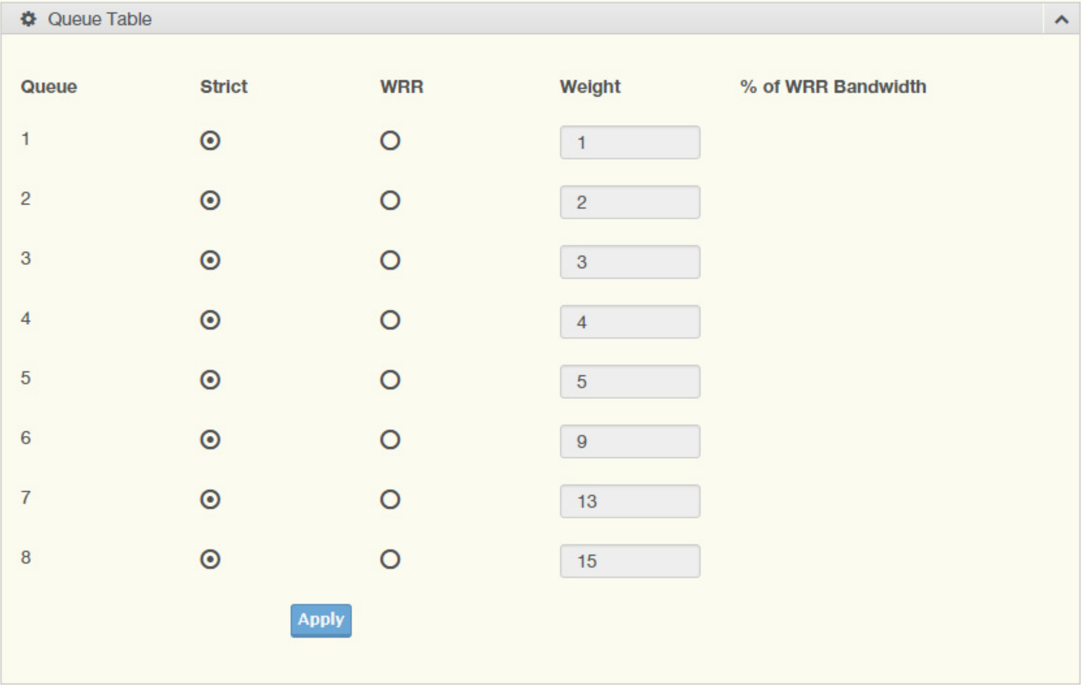
QoS Scheduling

The switch support 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 RoundRobin (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.

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



Queue Table

Queue	Strict	WRR	Weight	% of WRR Bandwidth
1	◉	○	1	
2	◉	○	2	
3	◉	○	3	
4	◉	○	4	
5	◉	○	5	
6	◉	○	9	
7	◉	○	13	
8	◉	○	15	

Figure 97. QoS > General > QoS Scheduling

The following table describes the items in Figure 97.

Table 94. QoS Scheduling

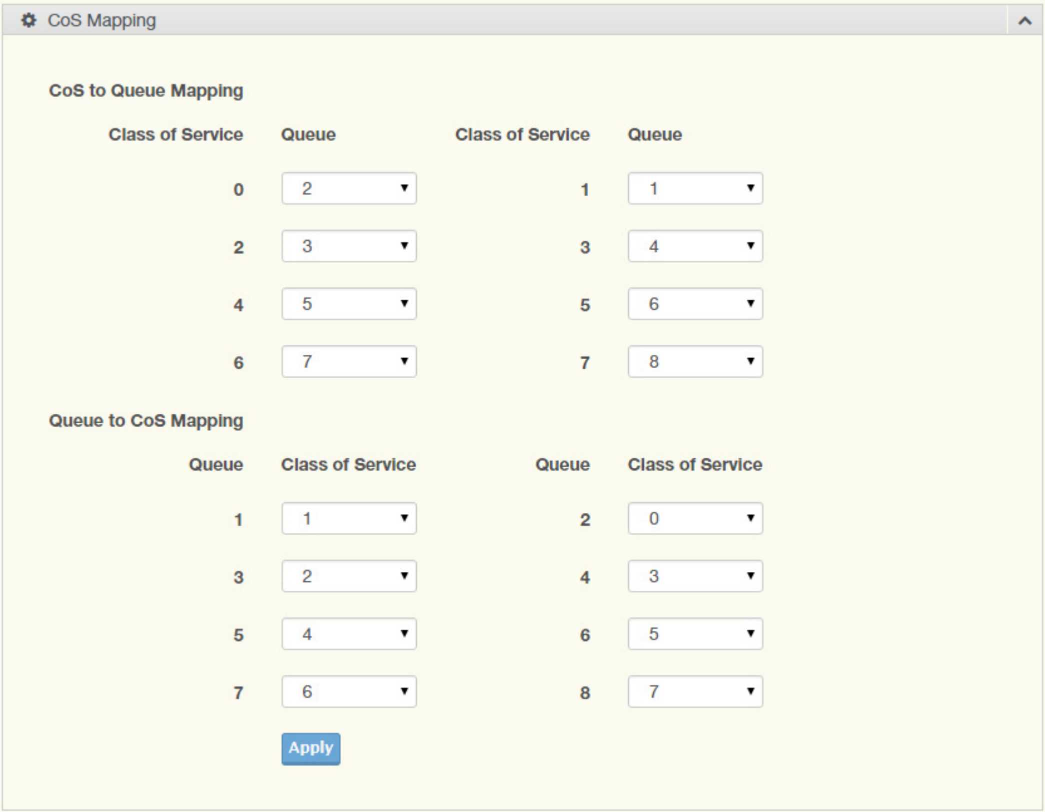
Item	Description
Queue	Queue entry for egress port.
Strict	Select Strict to assign the scheduling designation to the selected queue.
WRR	Select WRR to assign the scheduling designation to the selected queue.
Weight	Enter a queue priority (weight) relative to the defined entries (WRR only).
% of WRR Bandwidth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

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

CoS Mapping

The CoS Mapping allows you to apply CoS mapping.

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



CoS Mapping

CoS to Queue Mapping

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

Queue to CoS Mapping

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

Figure 98. QoS > General > CoS Mapping

The following table describes the items in Figure 98.

Table 95. CoS Mapping

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 **Apply** to save the values and update the screen.

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

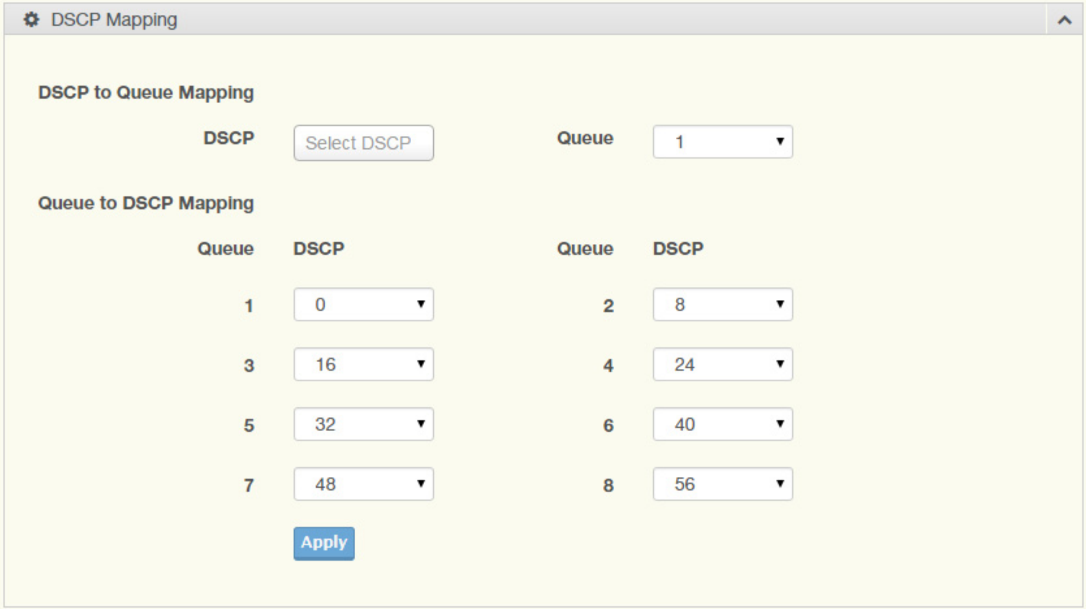
The **Queue Mapping Information** settings in the ensuing table are informational only: Queue and Mapping to CoS.

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.

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



DSCP Mapping

DSCP to Queue Mapping

DSCP: Select DSCP   Queue: 1

Queue to DSCP Mapping

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

Apply

Figure 99. QoS > General > DSCP Mapping

The following table describes the items in Figure 99.

Table 96. DSCP Mapping

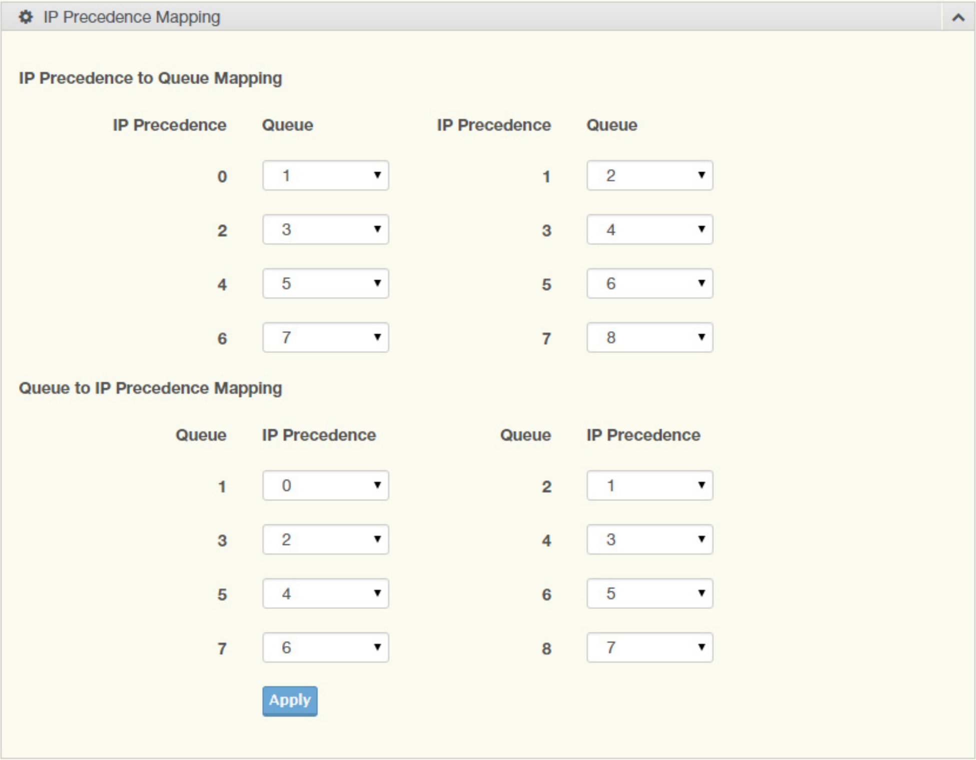
Item	Description
DSCP to Queue Mapping	
DSCP	Enter the DSCP entry to define the precedence values.
Queue	Click the drop-down menu to select the queue designation for the DSCP value.
Queue to DSCP Mapping	
Queue	Displays the queue value for the DSCP map.
DSCP	Enter the DSCP entry to define the precedence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

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

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

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 100. QoS > General > IP Precedence Mapping

The following table describes the items in Figure 100.

Table 97. IP Precedence Mapping

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 **Apply** to save the values and update the screen.

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

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

QoS Basic Mode

Quality of Service (QoS) allows to give 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.

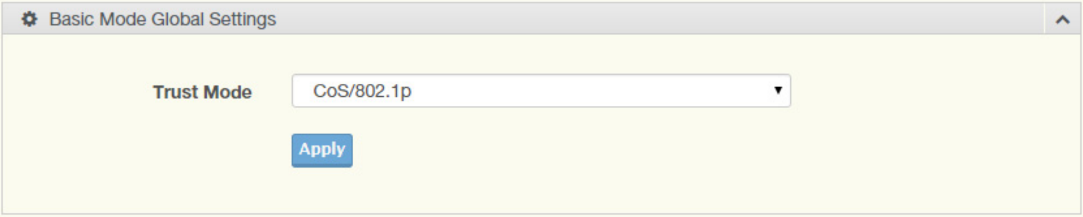
QoS mode supports two modes: 802.1p and DSCP.

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**.


Basic Mode Global Settings

Trust Mode: CoS/802.1p

Figure 101. QoS > QoS Basic Mode > Global Settings

The following table describes the items in Figure 101.

Table 98. QoS Basic Mode Global Settings

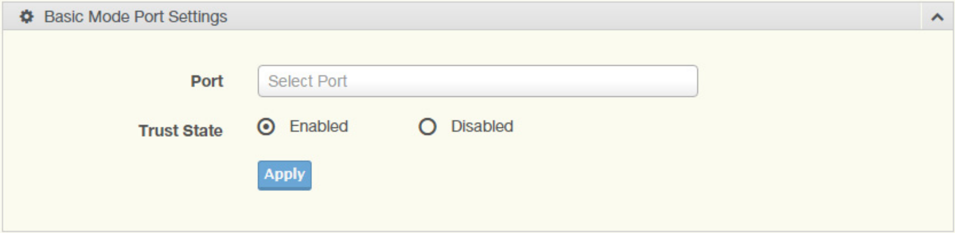
Item	Description
Trust Mode	Click the drop-down menu to select the trust state of the QoS basic mode.
Apply	Click **Apply** to save the values and update the screen.

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

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**.


Basic Mode Port Settings

Port: Select Port

Trust State: ● Enabled ○ Disabled

Figure 102. QoS > QoS Basic Mode > Port Settings

The following table describes the items in Figure 102 on page 119.

Table 99. QoS Basic Mode Port Settings

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

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

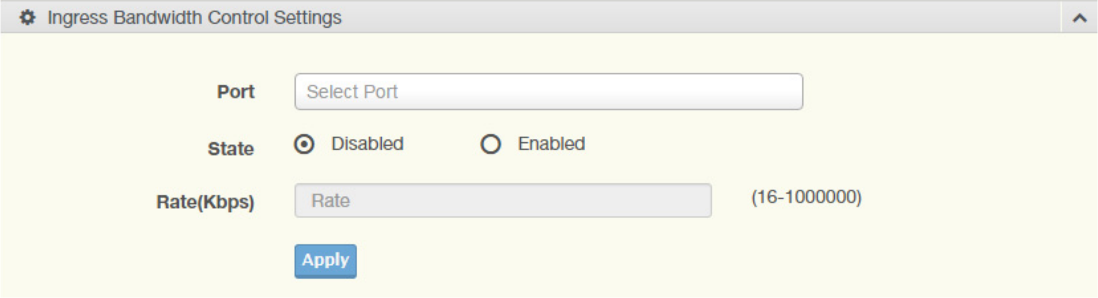
Rate Limit

Rate Limits 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**.



Ingress Bandwidth Control Settings

Port: Select Port

State: ● Disabled ○ Enabled

Rate(Kbps): Rate (16-1000000)

Figure 103. QoS > Rate Limit > Ingress Bandwidth Control

The following table describes the items in Figure 103.

Table 100. Ingress Bandwidth Control

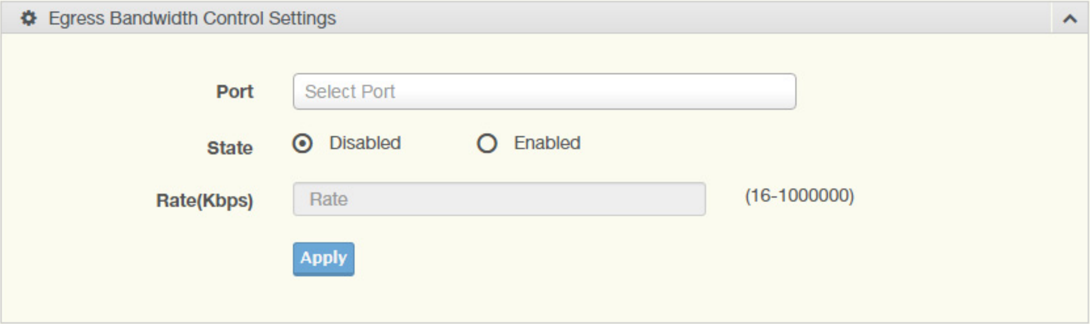
Item	Description
Port	Enter the port number for the rate limit setup.
State	Select **Disabled** or **Enabled** to set the port's state status.
Rate (Kbps)	Enter the value in Kbps (16 to 1000000) to set as the bandwidth rate for the selected port.
Apply	Click **Apply** to save the values and update the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

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

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**.



Egress Bandwidth Control Settings

Port: Select Port

State: ● Disabled ○ Enabled

Rate(Kbps): Rate (16-1000000)

Apply

Figure 104. QoS > Rate Limit > Egress Bandwidth Control

The following table describes the items in Figure 104.

Table 101. Egress Bandwidth Control

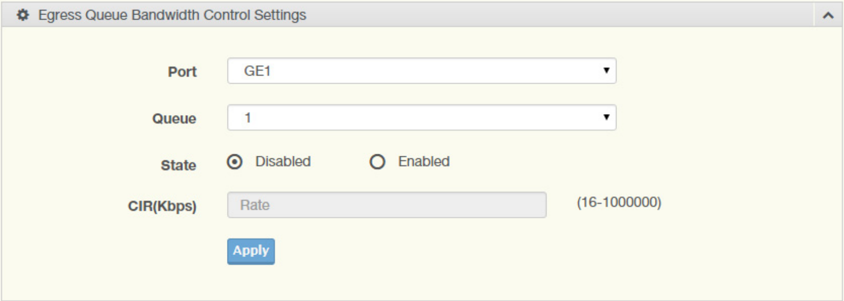
Item	Description
Port	Enter the port number to set the Egress Bandwidth Control.
State	Select **Disabled** or **Enabled** to set the Egress Bandwidth Control state.
Rate (Kbps)	Enter the value in Kbps (16 to 1000000) to set the Egress Bandwidth rate.
Apply	Click **Apply** to save the values and update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

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

Egress Queue

The Egress Queue page allows you to set the egress bandwidth parameters.

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



Egress Queue Bandwidth Control Settings

Port: GE1

Queue: 1

State: ● Disabled ○ Enabled

CIR(Kbps): Rate (16-1000000)

Apply

Figure 105. QoS > Rate Limit > Egress Queue

The following table describes the items in Figure 105 on page 121.

Table 102. Egress Queue

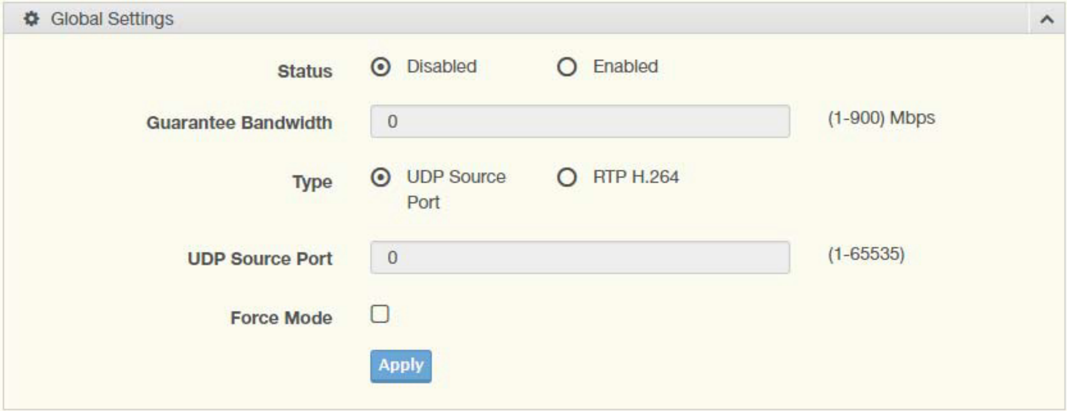
Item	Description
Port	Click the drop-down menu to select the port to define the Egress queue.
Queue	Click the drop-down menu to set the queue order for the Egress setting.
State	Click **Disabled** or **Enabled** to set the Egress queue state.
CIR (Kbps)	Enter the value in Kbps (16 to 1000000) to set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

The **FE1 Egress Per Queue Status** settings in the ensuing table are informational only: Queue Id and Egress Rate Limit (Kbps).

Bandwidth Guarantee

Global Settings

To access this page, click **QoS** > **Bandwidth Guarantee** > **Global Settings**.



Global Settings

Status ● Disabled ○ Enabled

Guarantee Bandwidth 0 (1-900) Mbps

Type ● UDP Source Port ○ RTP H.264

UDP Source Port 0 (1-65535)

Force Mode □

Figure 106. QoS > Bandwidth Guarantee > Global Settings

The following table describes the items in Figure 106.

Table 103. Global Settings

Item	Description
Status	Click **Disabled** or **Enabled** to set the guarantee bandwidth.
Guarantee Bandwidth	Enter the value for the guarantee bandwidth.
Type	Click **UDP Source Port** or **RTP H.264** to set the guarantee bandwidth type.
UDP Source Port	Enter the port number for the UDP source.
Force Mode	Click the check box to enable the force mode.
Apply	Click **Apply** to save the values and update the screen.

The **Ingress Bandwidth Control Status** settings in the ensuing table are informational only: Status, Guarantee Bandwidth, Guarantee Type, UDP Source Port and Force Mode.

Utilization

To access this page, click **QoS** > **Bandwidth Guarantee** > **Utilization**.

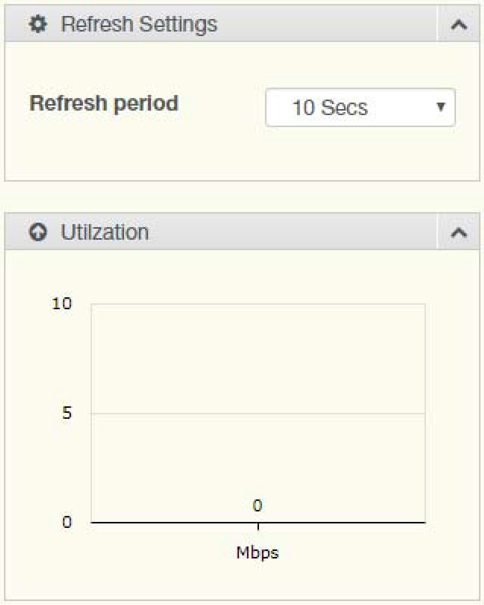


Figure 107. QoS > Bandwidth Guarantee > Utilization

The following table describes the items in Figure 107.

Table 104. Utilization

Item	Description
Refresh period	Click the drop-down menu to select refresh time.
Apply	Click **Apply** to save the values and update the screen.

Management

This section includes the following topics:

- “LLDP”
- “SNMP” on page 128
- “Power Over Ethernet” on page 132
- “TCP Modbus Settings”
- “DHCP Server” on page 134
- “SMTP Client” on page 141
- “RMON” on page 144
- “NTP Server” on page 147

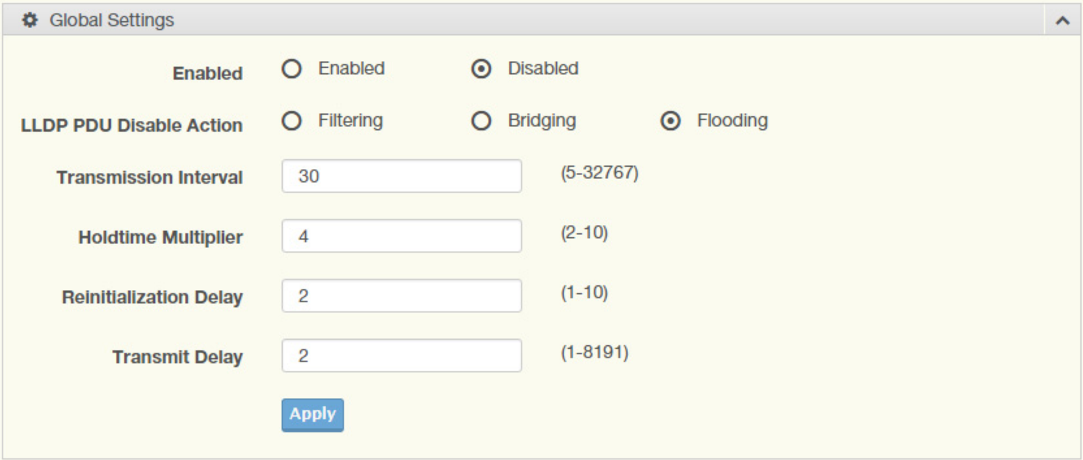
LLDP

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**.



Enabled	○ Enabled	● Disabled	
LLDP PDU Disable Action	○ Filtering	○ Bridging	● Flooding
Transmission Interval	30	(5-32767)	
Holdtime Multiplier	4	(2-10)	
Reinitialization Delay	2	(1-10)	
Transmit Delay	2	(1-8191)	

Figure 108. Management > LLDP > LLDP System Settings

The following table describes the items in Figure 108.

Table 105. LLDP System Settings

Item	Description
Enabled	Click **Enabled** or **Disabled** 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 32768 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 **Apply** to save the values and update the screen.

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

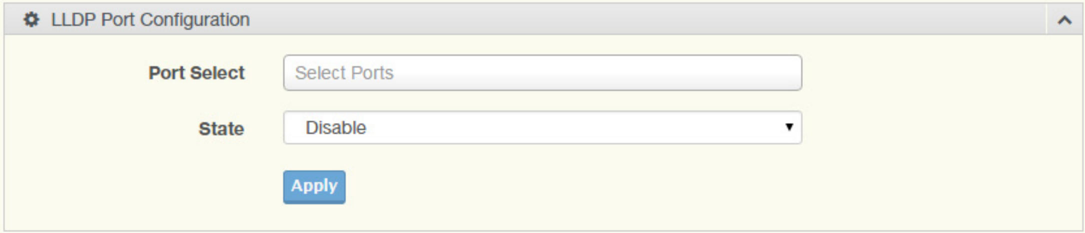
LLDP Port Settings

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**.

There are three regions on this page:

- LLDP Port Configuration
- Optional TLV Selection
- VLAN Name TLV VLAN Selection



LLDP Port Configuration

Port Select: Select Ports

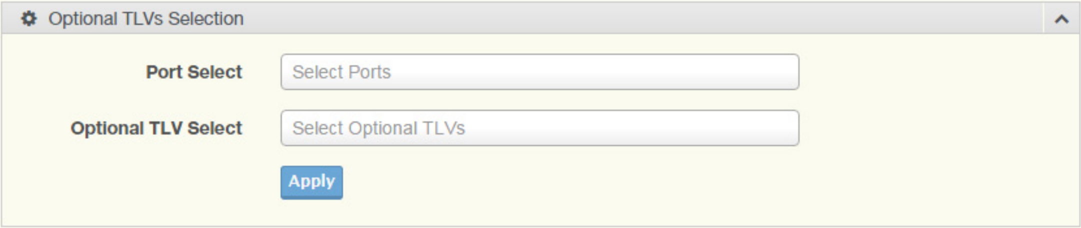
State: Disable

Figure 109. Management > LLDP > LLDP Port Settings > LLDP Port Configuration

The following table describes the items in Figure 109.

Table 106. LLDP Port Configuration

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 **Apply** to save the values and update the screen.



Optional TLVs Selection

Port Select: Select Ports

Optional TLV Select: Select Optional TLVs

Apply

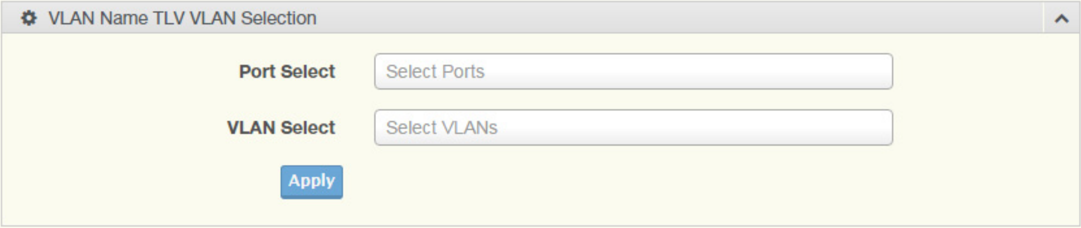
Figure 110. Management > LLDP > LLDP Port Settings > Optional TLVs Selection

The following table describes the items in Figure 110.

Table 107. Optional TLVs Selection

Item	Description
Port Select	Enter the port number associated with the TLV (optional) selection.
Optional TLV Select	Click the drop-down menu to select the LLDP optional TLVs to be carried (multiple selections are allowed). System Name: To include system name TLV in LLDP frames. Port Description: To include port description TLV in LLDP frames. □ System Description: To include system description TLV in LLDP frames. □ System Capability: To include system capability TLV in LLDP frames. □ 802.3 MAC-PHY: □ 802.3 Link Aggregation: □ 802.3 Maximum Frame Size: □ Management Address: □ 802.1 PVID:
Apply	Click **Apply** to save the values and update the screen.

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



VLAN Name TLV VLAN Selection

Port Select: Select Ports

VLAN Select: Select VLANs

Apply

Figure 111. Management > LLDP > LLDP Port Settings > VLAN Name TLV VLAN Selection

The following table describes the items in Figure 111 on page 126.

Table 108. VLAN Name TLV VLAN Selection

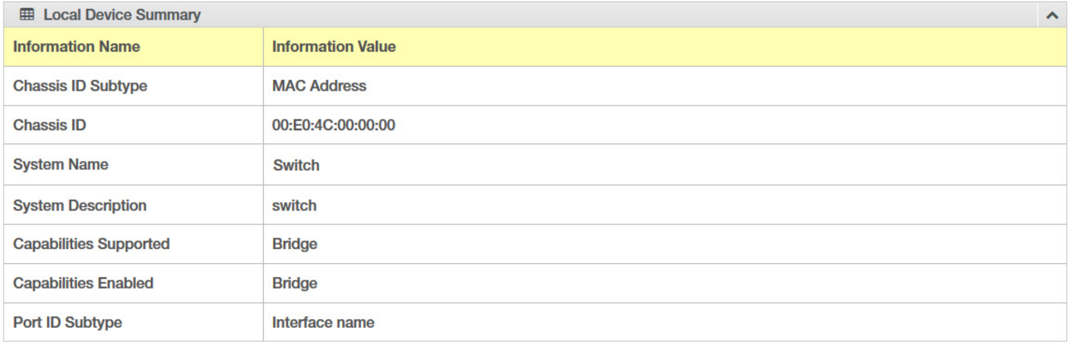
Item	Description
Port Select	Enter the port number to associated with the TLV selection.
VLAN Select	Select the VLAN Name ID to be carried out (multiple selection is allowed).
Apply	Click **Apply** to save the values and update the screen.

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

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**.



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

Figure 112. Management > LLDP > LLDP Local Device Info

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

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

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**.

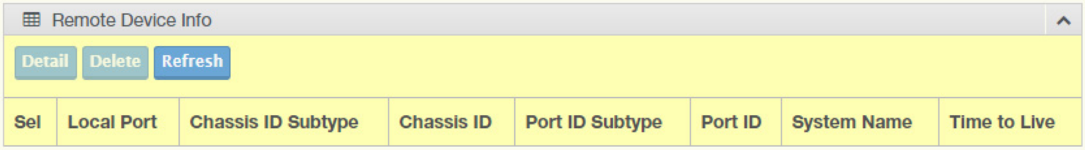


Figure 113. Management > LLDP > LLDP Remote Device Info

The following table describes the items in Figure 113.

Table 109. LLDP Remote Device Info

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.
Sel	Indicates that a device that is selected
Local Port	Indicates the local port connected to the remote device
Chassis ID Subtype	Indicates the Chassis ID Subtype
Chassis ID	Indicates the Chassis ID
Port ID Subtype	Indicates the Port ID Subtype
Port ID	Indicates the Port ID
System Name	Indicates the System ID
Time to Live	Indicates the Time to Live interval

LLDP Overloading

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

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

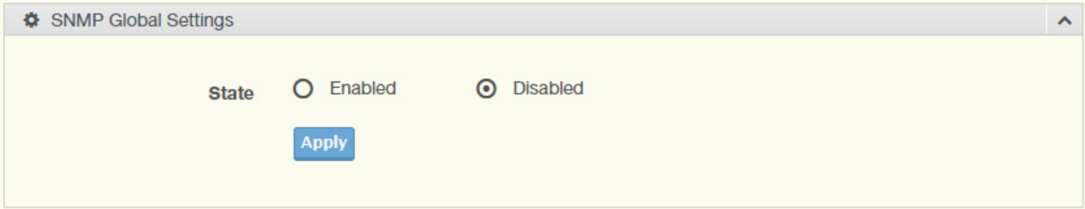
SNMP

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**.



SNMP Global Settings

State ○ Enabled ● Disabled

Figure 114. Management > SNMP > SNMP Settings

The following table describes the items in Figure 114.

Table 110. SNMP Settings

Item	Description
State	Click **Enabled** or **Disabled** to define the SNMP daemon.
Apply	Click **Apply** to save the values and update the screen.

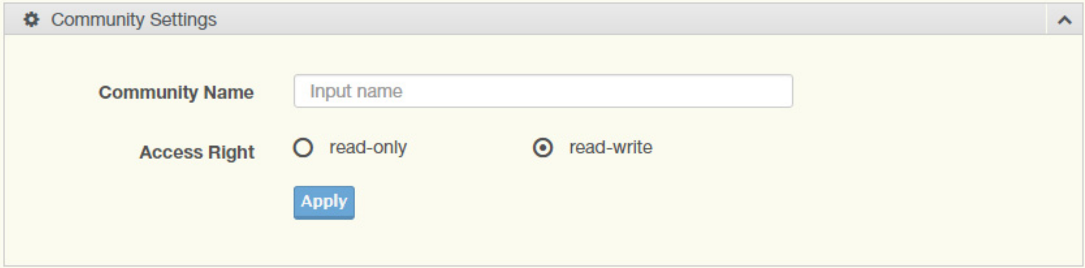
The **SNMP Information** settings in the ensuing table are informational only: SNMP.

SNMP Community

The SNMP Community page provides configuration options for the community.

SNMP v1 and SNMP v2c use the group name (Community Name) certification. It's 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**.



Community Settings

Community Name: Input name

Access Right ○ read-only ● read-write

Figure 115. Management > SNMP > SNMP Community

The following table describes the items in Figure 115.

Table 111. SNMP Community

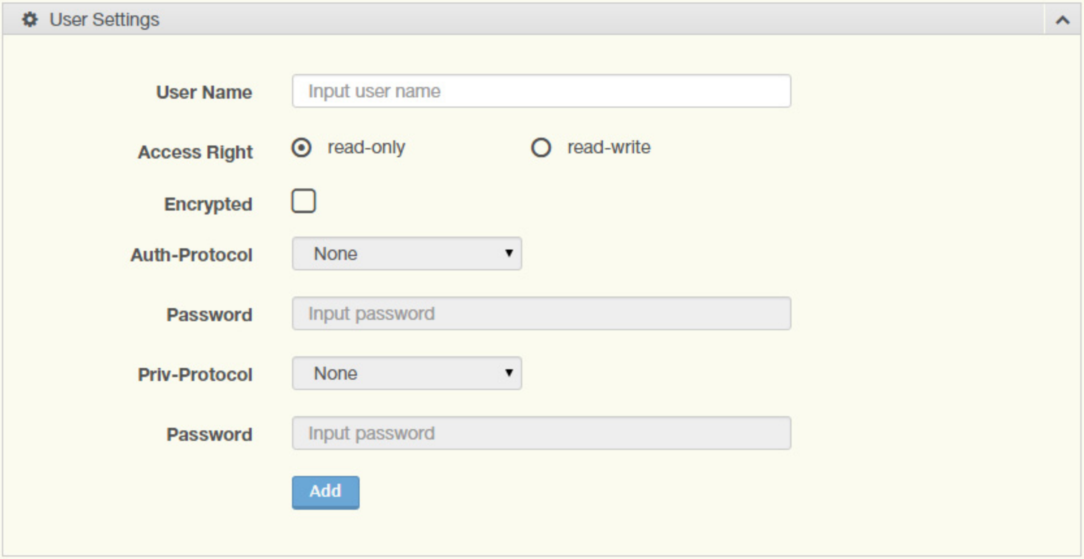
Item	Description
Community Name	Enter a community name (up to 20 characters).
Access Right	Click the radio box to specify the access level (read only or read write)
Apply	Click **Apply** to save the values and update the screen.

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

SNMPv3 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** > **SNMPv3 Settings**.



User Settings

User Name: Input user name

Access Right: ● read-only ○ read-write

Encrypted: □

Auth-Protocol: None

Password: Input password

Priv-Protocol: None

Password: Input password

Figure 116. Management > SNMP > SNMPv3 Settings

The following table describes the items in Figure 116.

Table 112. SNMP User Settings

Item	Description
User Name	Enter a user name (up to 32 characters) to create an SNMP profile.
Access Right	Click **read-only** or **read-write** 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. • MD5: specify HMAC-MD5-96 authentication level • SHA: specify HMAC-SHA authentication protocol
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. • None: no authorization protocol in use • DES: specify 56-bit encryption in use

Table 112. SNMP User Settings (Continued)

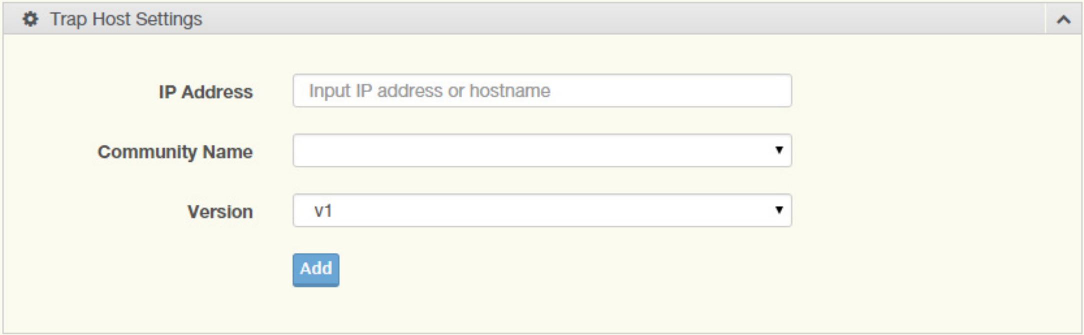
Item	Description
Password	Enter the characters to define the password associated with the authorization protocol.
Add	Click **Add** to save the values and update the screen.

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

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**.



Trap Host Settings

IP Address: Input IP address or hostname

Community Name:

Version: v1

Figure 117. Management > SNMP > SNMP Trap

The following table describes the items in Figure 117.

Table 113. SNMP Trap

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, v2c- trap, v2c - inform, v2c - trap or v2c - inform).
Add	Click **Add** to save the values and update the screen.

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

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.

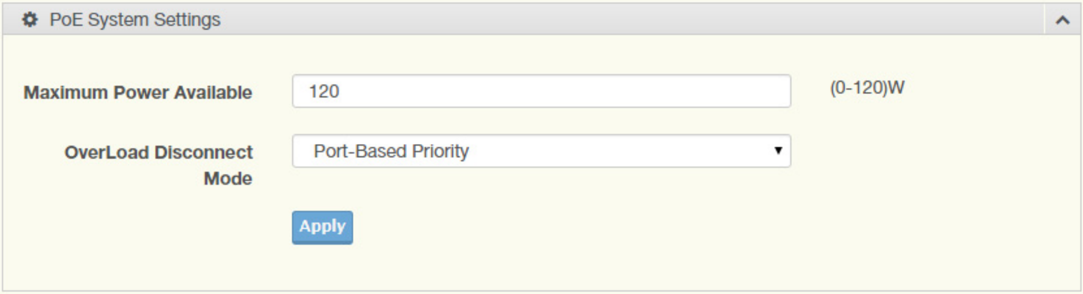
Power over Ethernet can be used for the following areas:

- ❐ 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**.



Maximum Power Available: 120 (0-120)W

OverLoad Disconnect Mode: Port-Based Priority

Figure 118. Management > Power Over Ethernet > PoE System Settings

The following table describes the items in Figure 118.

Table 114. PoE System Settings

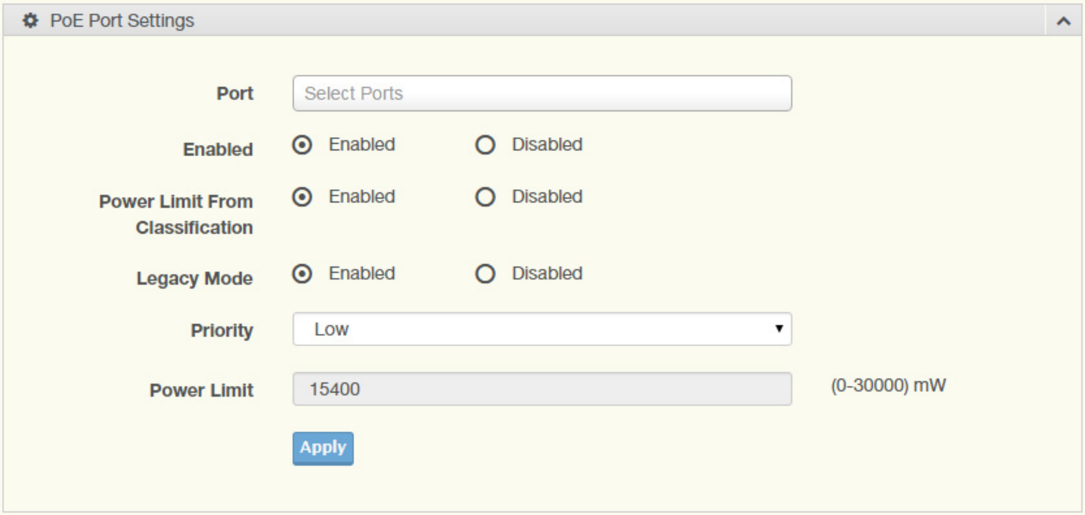
Item	Description
Maximum Power Available	Select the value in Watts to set the maximum available power.
OverLoad Disconnect Mode	Click the drop-down menu to designate the overload mode: • Overload Port First: • Port-Based Priority:
Apply	Click **Apply** to save the values and update the screen.

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

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**.



PoE Port Settings

Port	Select Ports	
Enabled	◉ Enabled	○ Disabled
Power Limit From Classification	◉ Enabled	○ Disabled
Legacy Mode	◉ Enabled	○ Disabled
Priority	Low ▾	
Power Limit	15400	(0-30000) mW

Figure 119. Management > Power Over Ethernet > PoE Port Settings

The following table describes the items in Figure 119.

Table 115. PoE Port Settings

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

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

PoE Port Status

To access this page, click **Management** > **Power Over Ethernet** > **PoE Port Status**. This window is informational only.

The **PoE Port Status** settings in the ensuing table are informational only: Port, Current (mA), Voltage (V), Power (W) and Temp. (°C).

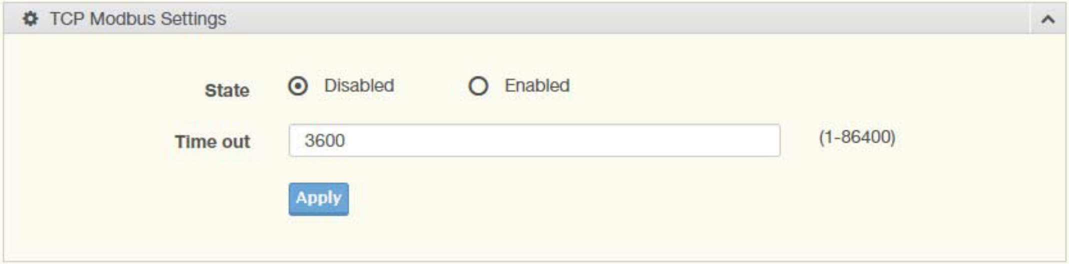
TCP Modbus Settings

The TCP Modbus function allows for client-server communication between a switch module (server) and a device in the networking running MODBUS client software (client).

TCP Modbus Settings

The TCP Modbus Settings page allows you to configure the modbus function.

To access this page, click **Management** > **TCP Modbus Settings** > **TCP Modbus Settings**.



TCP Modbus Settings

State ● Disabled ○ Enabled

Time out 3600 (1-86400)

Figure 120. Management > TCP Modbus Settings > TCP Modbus Settings

The following table describes the items in Figure 120.

Table 116. TCP Modbus Settings

Item	Description
State	Click **Disabled** or **Enabled** to set the TCP Modbus state.
Time out	Enter the value (1 to 86400) to define the timeout period between transport time.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **TCP Modbus Status** settings are informational only: TCP Modbus status and TCP Modbus time out.

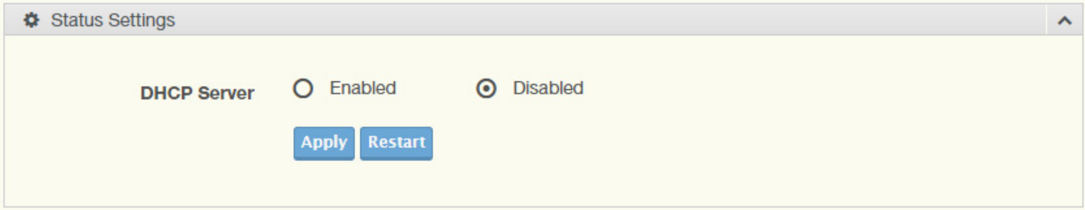
DHCP Server

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**.



DHCP Server ○ Enabled ● Disabled

Figure 121. Management > DHCP Server > Status Settings

The following table describes the items in Figure 121.

Table 117. Status Settings

Item	Description
DHCP Server	Select **Enable** or **Disable** 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 **Apply** to save the values and update the screen.
Restart	Click **Restart** 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 **Status Information** settings in the ensuing table are informational only: DHCP Server Service.

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**.

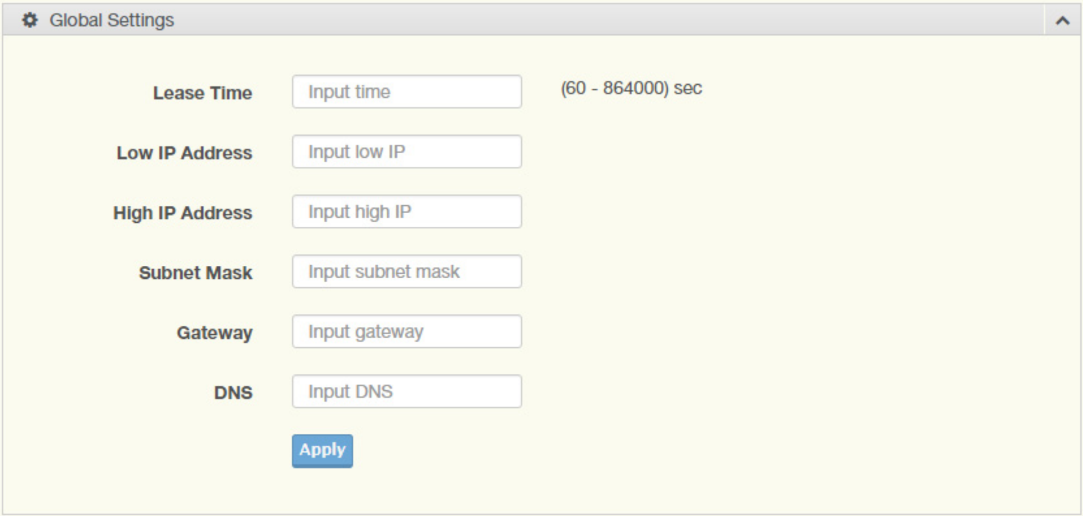


Figure 122. Management > DHCP Server > Global Settings

The following table describes the items in Figure 122.

Table 118. DHCP Server Global Settings

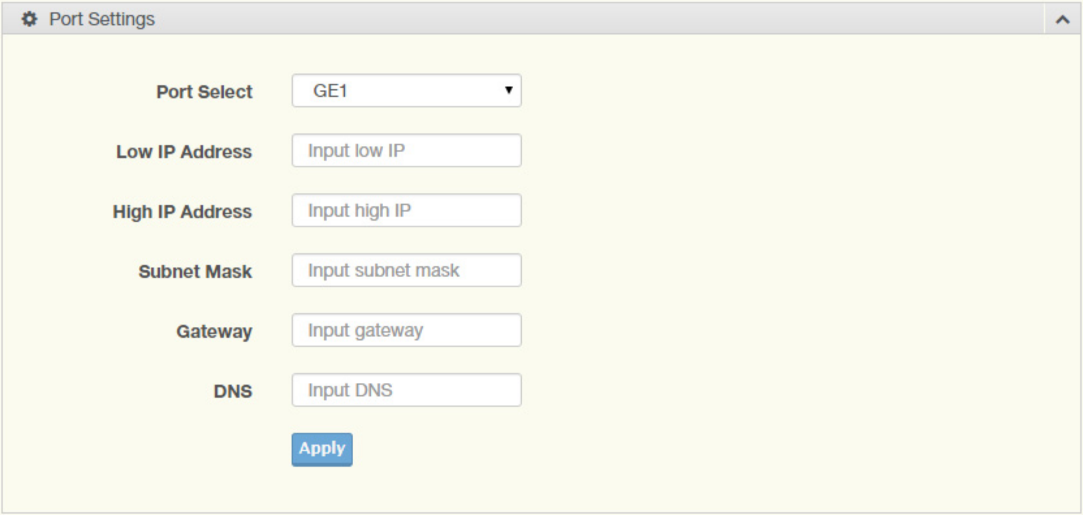
Item	Description
Lease Time	Type in the value designating the lease time (60 - 864000) in seconds for each setting lease.
Low IP Address	Type in the value designating the lowest range in the IP address pool.
High IP Address	Type in the value designating the highest range in the IP address pool.
Subnet 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 **Apply** to save the values and update the screen.

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

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**.



Port Settings

Port Select: GE1

Low IP Address: Input low IP

High IP Address: Input high IP

Subnet Mask: Input subnet mask

Gateway: Input gateway

DNS: Input DNS

Figure 123. Management > DHCP Server > Port Settings

The following table describes the items in Figure 123.

Table 119. DHCP Server Port Settings

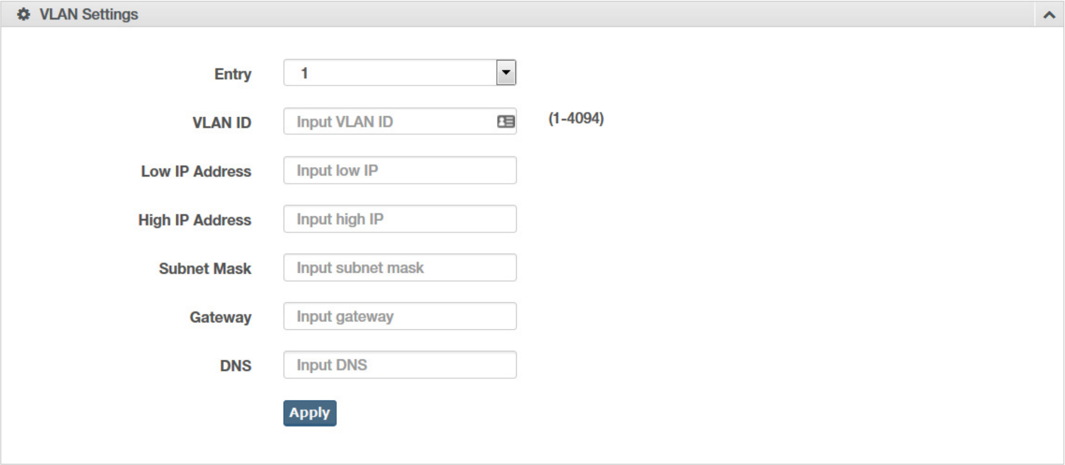
Item	Description
Port Select	Click the drop-down menu to select a pre-defined port to configure. The suboptions are designated for the selected port.
Low IP Address	Type in the value designating the lowest range in the IP address pool.
High IP Address	Type in the value designating the highest range in 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 **Apply** to save the values and update the screen.

The **Port Information** settings in the ensuing table 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).

VLAN Settings

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

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



VLAN Settings

Entry: 1

VLAN ID: Input VLAN ID (1-4094)

Low IP Address: Input low IP

High IP Address: Input high IP

Subnet Mask: Input subnet mask

Gateway: Input gateway

DNS: Input DNS

Figure 124. Management > DHCP Server > VLAN Settings

The following table describes the items in Figure 123.

Table 120. DHCP Server Port Settings

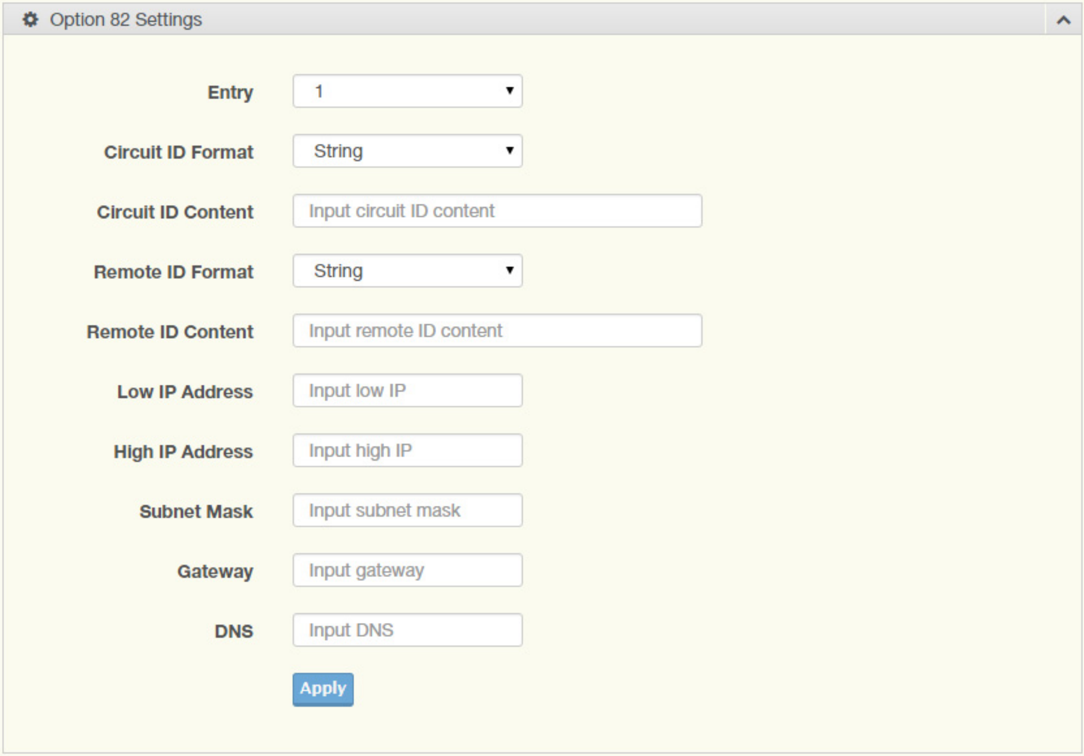
Item	Description
Entry ID	Select entry number from pull-down menu
VLAN ID	Input VLAN ID
Low IP Address	Input low IP address
High IP Address	Input high IP address
Subnet Mask	Input Subnet Mask
Gateway	Input Gateway address
DNS	Input DNS
Apply	Click **Apply** to save the values and update the screen.

The **VLAN** settings in the ensuing table are informational only: Entry ID, 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).

Option 82 Settings

The Option 82 Settings, also known as the DHCP relay agent information option, provide 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**.



Option 82 Settings

Entry	1
Circuit ID Format	String
Circuit ID Content	Input circuit ID content
Remote ID Format	String
Remote ID Content	Input remote ID content
Low IP Address	Input low IP
High IP Address	Input high IP
Subnet Mask	Input subnet mask
Gateway	Input gateway
DNS	Input DNS

Figure 125. Management > DHCP Server > Option 82 Settings

The following table describes the items in Figure 125.

Table 121. Option 82 Settings

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.

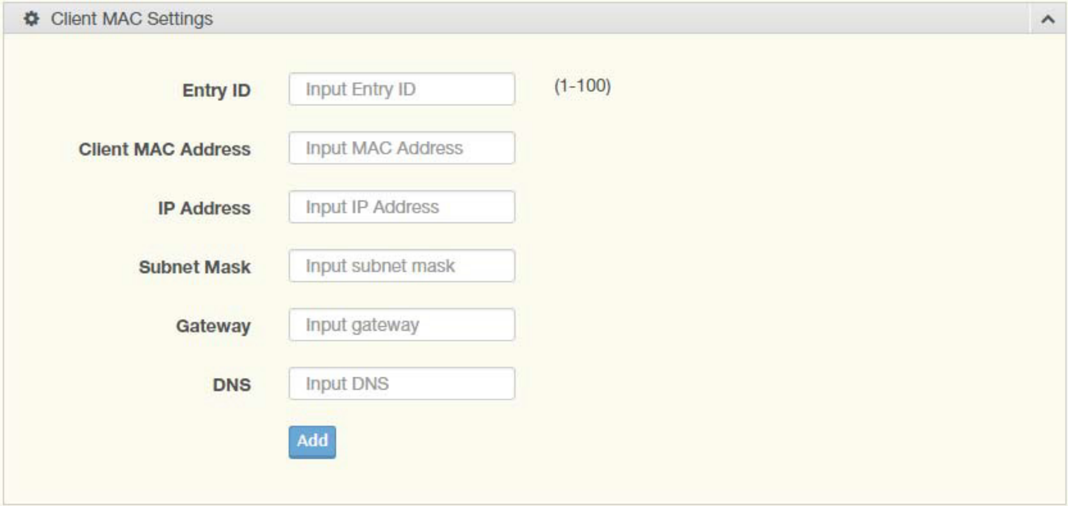
Table 121. Option 82 Settings (Continued)

Item	Description
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 **Apply** to save the values and update the screen.

The **Entry Information** settings in the ensuing table are informational only: **Entry** (click the drop-down 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).

Client MAC Settings

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



Client MAC Settings

Entry ID: Input Entry ID (1-100)

Client MAC Address: Input MAC Address

IP Address: Input IP Address

Subnet Mask: Input subnet mask

Gateway: Input gateway

DNS: Input DNS

Add

Figure 126. Management > DHCP Server > Client MAC Settings

The following table describes the items in Figure 126.

Table 122. Client MAC Settings

Item	Description
Entry ID	Type in the value designating the entry ID.
Client MAC Address	Enter the MAC address for the DHCP server.
IP Address	Enter a value to specify the IP address of the interface.
Subnet Mask	Enter a value to specify the IP subnet mask for the interface.
Gateway	Enter a value to specify the gateway for the interface.
DNS	Enter a value to specify the DNS server for the interface.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Client MAC Information** settings are informational only: Entry ID, Client MAC Address, IP Address, Subnet Mask and Modify (Click **Detail** to display the detail information of desired entry id or Delete to delete the desired entry id).

Lease Entry

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

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

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.

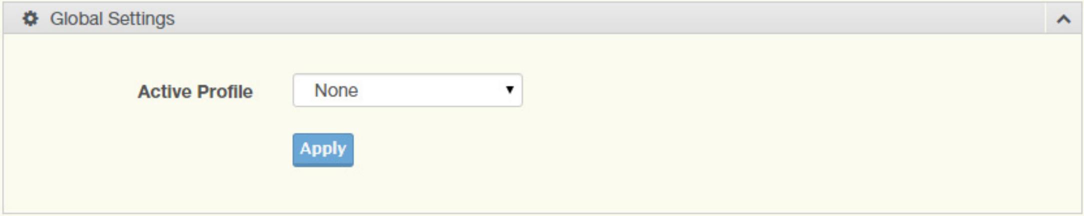


Figure 127. Management > SMTP Client > Global Settings

The following table describes the items in Figure 127.

Table 123. SMTP Client Global Settings

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

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

Profile Settings

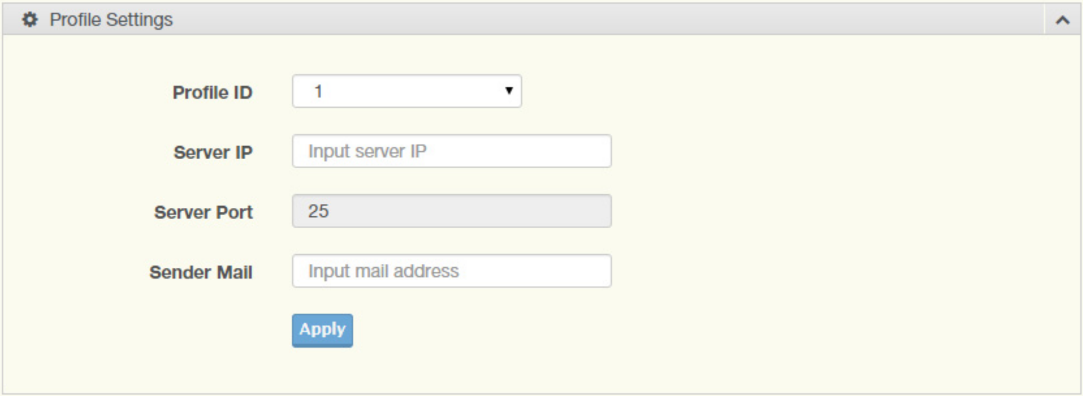
The Profile Settings page allows you to select the server IP, the server port, and sender mail address for the listed profile.

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

There are two regions on the Profile Settings page:

- ❐ Profile Settings
- ❐ Profile Target Mail Settings

Profile Settings Window



Profile Settings

Profile ID: 1

Server IP: Input server IP

Server Port: 25

Sender Mail: Input mail address

Figure 128. Management > SMTP Client > Profile Settings

The following table describes the items in Figure 128.

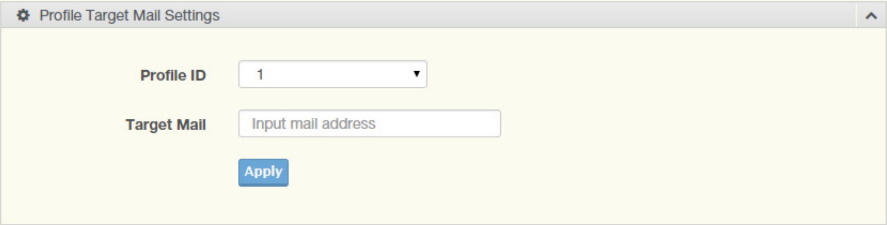
Table 124. SMTP Client Profile Settings

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 **Apply** to save the values and update the screen.

Profile Target Mail Settings Window

The Profile Target Mail Settings page allows you to select the Profile ID for the Target Mail (input mail address) for the listed profile.

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



Profile ID 1

Figure 129. Management > SMTP Client > Profile Settings > Profile Target Mail Settings

The following table describes the items in Figure 129.

Table 125. Profile Target Mail Settings

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 **Apply** to save the values and update the screen.

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

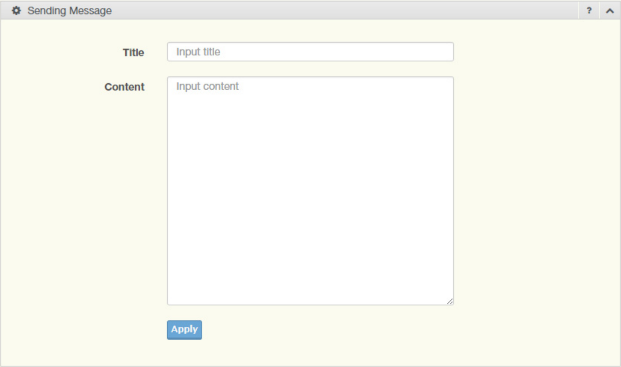


Figure 130. Management > SMTP Client > Sending Message

The following table describes the items in Figure 130 on page 143.

Table 126. Sending Message

Item	Description
Title	Assign the title of the email. The maximum length is 20 characters (alphanumeric, symbols (. (dot), _ (underline), - (dash line) and space).
Content	Assign the content of the email. The maximum length is 64 characters (alphanumeric, symbols (. (dot), _ (underline), - (dash line) and space).
Apply	Click **Apply** to save the values and update the screen.

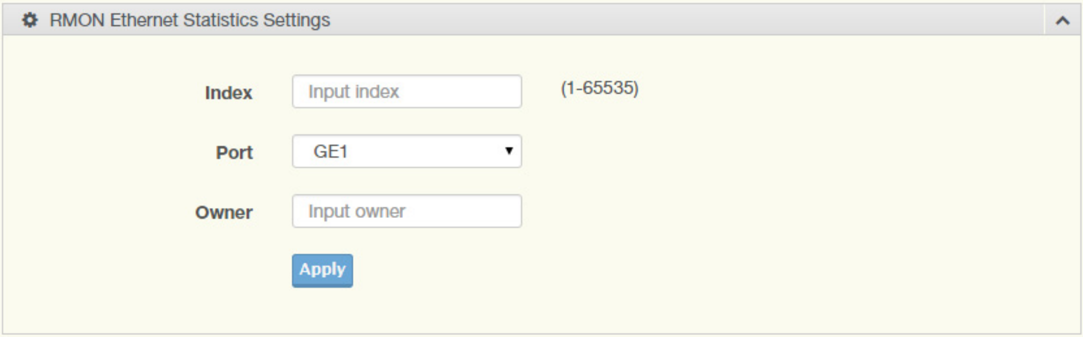
RMON

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**.



RMON Ethernet Statistics Settings

Index: Input index (1-65535)

Port: GE1

Owner: Input owner

Figure 131. Management > RMON > Rmon Statistics

The following table describes the items in Figure 131.

Table 127. Rmon Statistics

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 **Apply** to save the values and update the screen.

The **Statistics Information** settings in the ensuing table 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**.

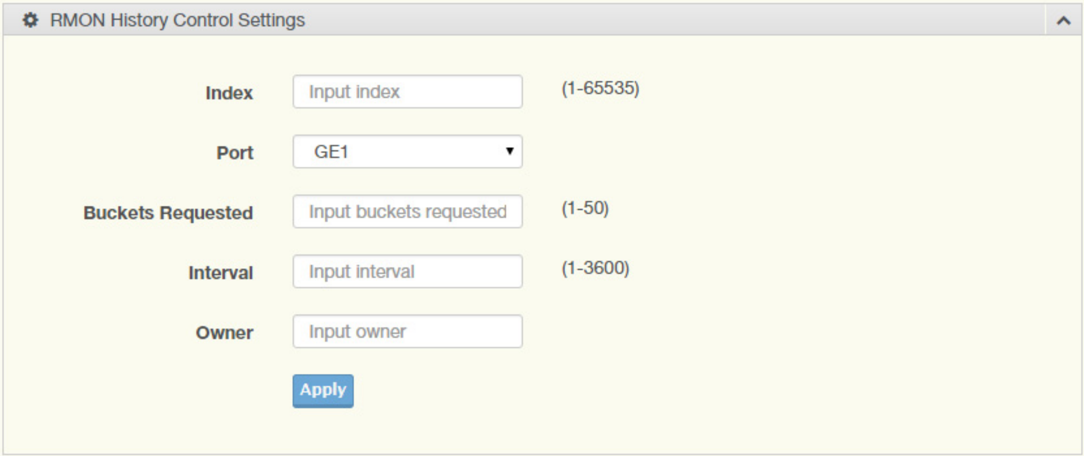


Figure 132. Management > RMON > RMON History

The following table describes the items in Figure 132.

Table 128. RMON History

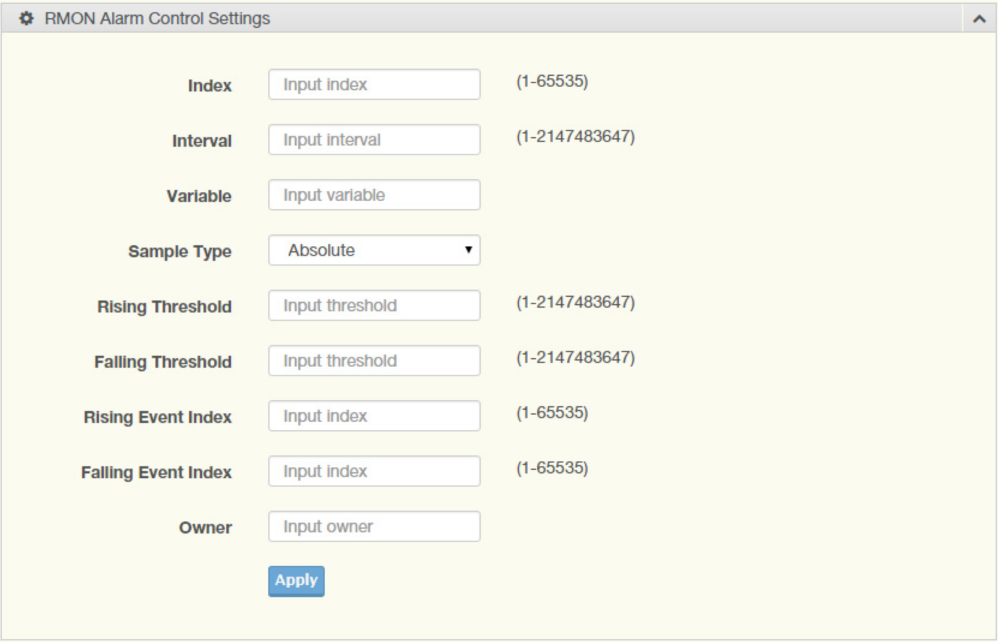
Item	Description
Index	Enter the index entry (1 to 65535) to select the number of new history table entries.
Port	Select the specific port switch.
Buckets Requested	Enter the specific (1-50) number of samples to store.
Interval	Enter value in seconds (1 to 3600) to designate a specific interval time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

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

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**.



⚙ RMON Alarm Control Settings

Index	Input index	(1-65535)
Interval	Input interval	(1-2147483647)
Variable	Input variable	
Sample Type	Absolute ▾	
Rising Threshold	Input threshold	(1-2147483647)
Falling Threshold	Input threshold	(1-2147483647)
Rising Event Index	Input index	(1-65535)
Falling Event Index	Input index	(1-65535)
Owner	Input owner	

Figure 133. Management > RMON > Rmon Alarm

The following table describes the items in Figure 133.

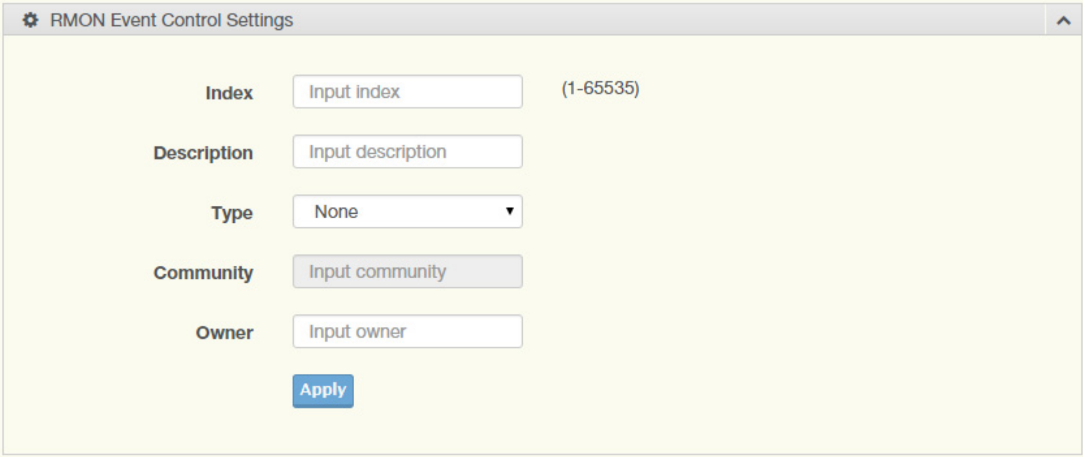
Table 129. Rmon Alarm

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 **Apply** to save the values and update the screen.

The **Alarm Information** settings in the ensuing table 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).

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: Input index (1-65535)

Description: Input description

Type: None

Community: Input community

Owner: Input owner

Figure 134. Management > RMON > RMON Event

The following table describes the items in Figure 134.

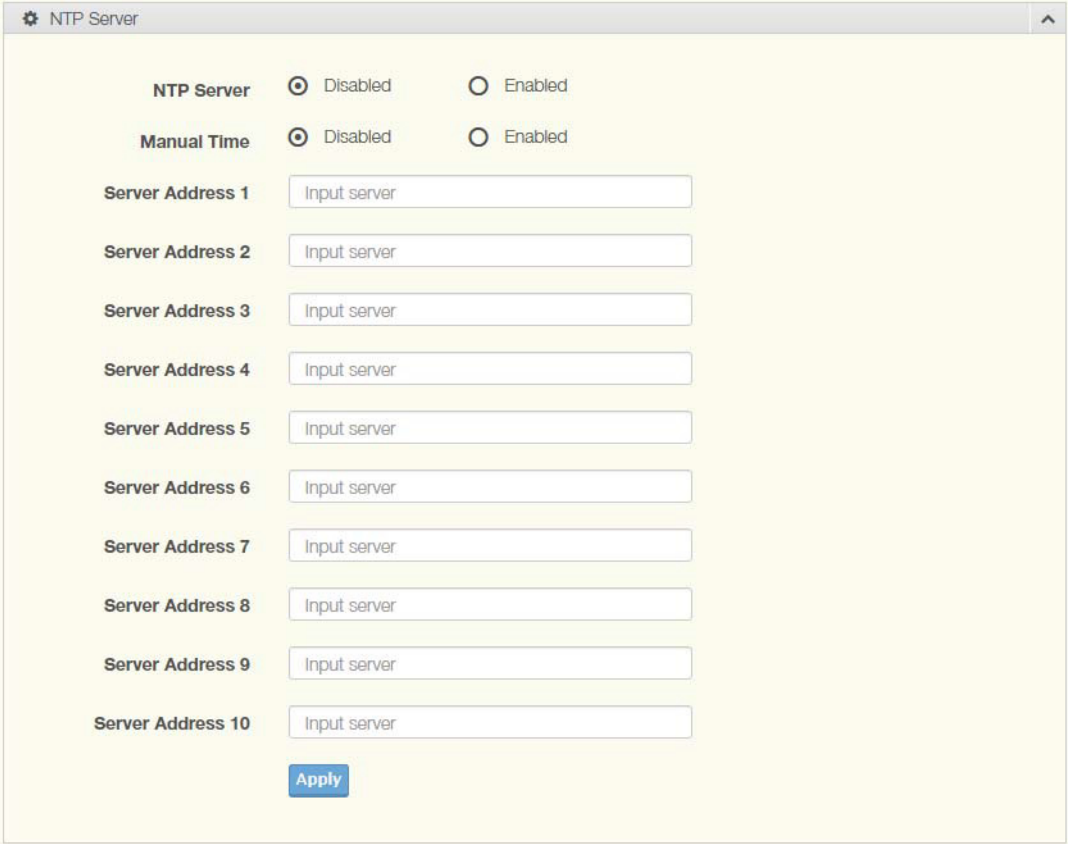
Table 130. RMON Event

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 **Apply** to save the values and update the screen.

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

NTP Server

To access this page, click **Management** > **NTP Server**.



NTP Server

NTP Server ● Disabled ○ Enabled

Manual Time ● Disabled ○ Enabled

Server Address 1 Input server

Server Address 2 Input server

Server Address 3 Input server

Server Address 4 Input server

Server Address 5 Input server

Server Address 6 Input server

Server Address 7 Input server

Server Address 8 Input server

Server Address 9 Input server

Server Address 10 Input server

Figure 135. Management > NTP Server

The following table describes the items in Figure 135.

Table 131. NTP Server

Item	Description
NTP Server	Click the radio button to enable or disable the NTP server function.
Manual Time	Click the radio button to enable or disable the manual time function.
Server Address 1 ~ Server Address 10	Enter the address of the NTP server. This is a text string of up to 64 characters containing the encoded unicast IP address or hostname of a NTP server.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **NTP Server Status** settings are informational only: INTP Server Status, Manual Time, Server AddressInformation Value, Server 1, Server 2, Server 3, Server 4, Server 5, Server 6, Server 7, Server 8, Server 9 and Server 10.

Diagnostics

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

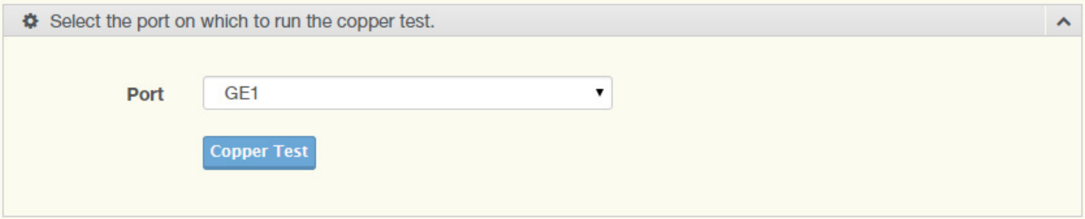
This section includes the following topics:

- ❐ “Cable Diagnostics”
- ❐ “Ping Test”
- ❐ “IPv6 Ping Test” on page 152
- ❐ “System Log” on page 153
- ❐ “DDM” on page 156
- ❐ “LED Indication” on page 157

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**.



Select the port on which to run the copper test.

Port: GE1

Figure 136. Diagnostics > Cable Diagnostics

The following table describes the items in Figure 136.

Table 132. Cable Diagnostics

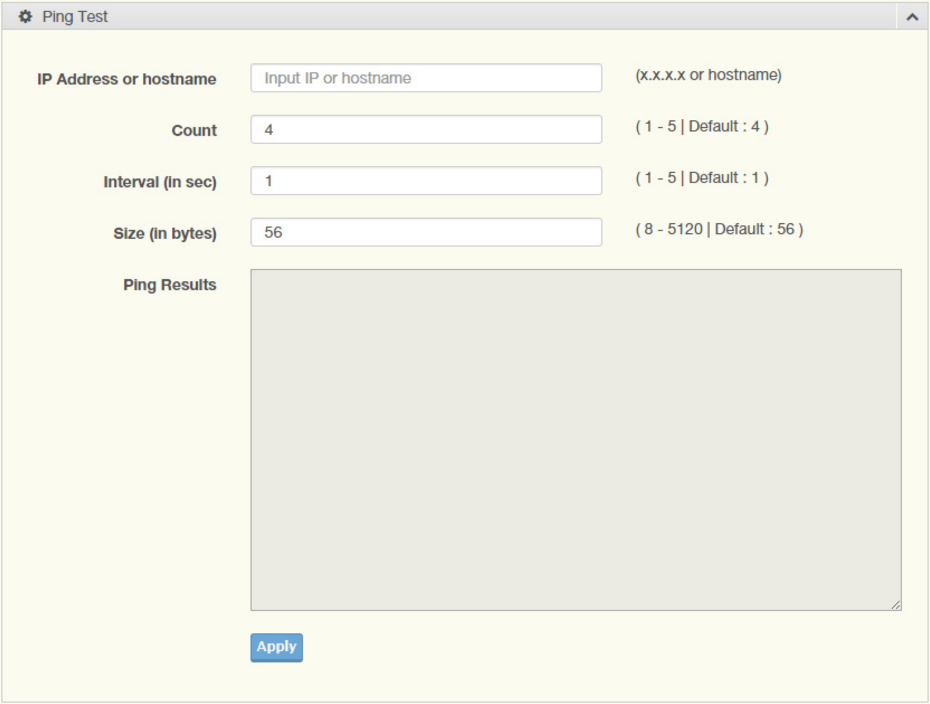
Item	Description
Port	Click the drop-down menu to select a pre-defined port for diagnostic testing. Giga ports are displayed with a channel A to D designation.
Copper Test	Click **Copper Test** to display the test result for the selected port.

The **Test Result** settings in the ensuing table 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.

Ping Test

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

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



IP Address or hostname: Input IP or hostname (x.x.x.x or hostname)

Count: 4 (1 - 5 | Default : 4)

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

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

Ping Results

Figure 137. Diagnostics > Ping Test

The following table describes the items in Figure 137.

Table 133. Ping Test

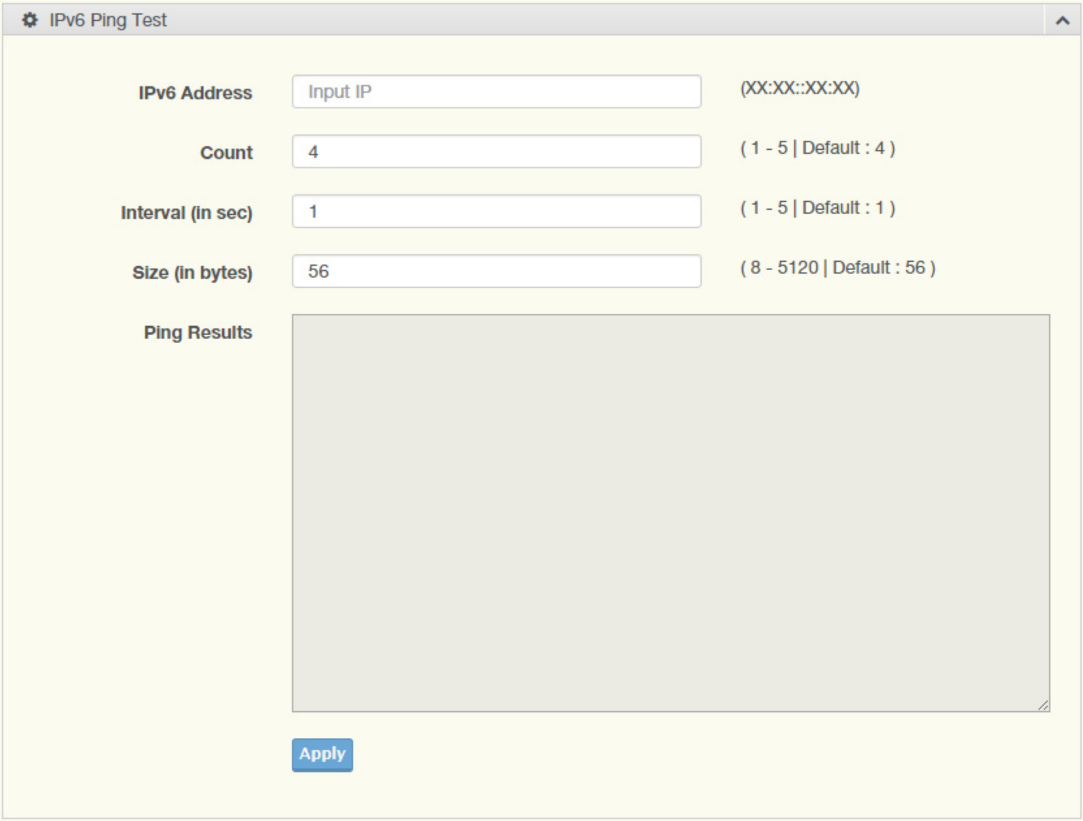
Item	Description
IP Address	Enter the IP address or host name of the station to ping. The initial value is blank. The IP Address or host name you enter is not retained across a power cycle. Host names are composed of series of labels concatenated with periods. Each label must be between 1 and 63 characters 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.

Table 133. Ping Test (Continued)

Item	Description
Ping Results	Display the reply format of ping. PING 172.17.8.254 (172.17.8.254): 56 data bytes --- 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=0.0 ms 64 bytes from 172.17.8.93: icmp_seq=1 ttl=128 time=0.0 ms 64 bytes from 172.17.8.93: icmp_seq=2 ttl=128 time=0.0 ms 64 bytes from 172.17.8.93: icmp_seq=3 ttl=128 time=0.0 ms --- 172.17.8.93 ping statistics --- 4 packets transmitted, 4 packets received, 0% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms
Apply	Click **Apply** to display ping result for the IP address.

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	Input IP	(XX:XX::XX:XX)
Count	4	(1 - 5 | Default : 4)
Interval (in sec)	1	(1 - 5 | Default : 1)
Size (in bytes)	56	(8 - 5120 | Default : 56)
Ping Results		

Figure 138. Diagnostics > IPv6 Ping Test

The following table describes the items in Figure 138.

Table 134. 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 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.

Table 134. IPv6 Ping Test (Continued)

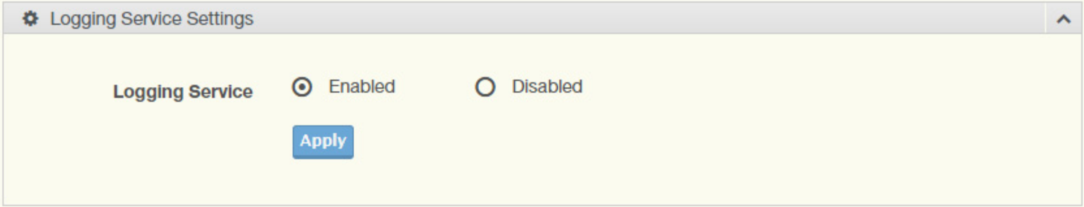
Item	Description
Ping Results	Display the reply format of ping. PING 2222::777 (2222::777): 56 data bytes --- 2222::777 ping statistics --- 4 packets transmitted, 0 packets received, 100% packet loss Or PING 2222::717 (2222::717): 56 data bytes 64 bytes from 2222::717: icmp6_seq=0 ttl=128 time=10.0 ms 64 bytes from 2222::717: icmp6_seq=1 ttl=128 time=0.0 ms 64 bytes from 2222::717: icmp6_seq=2 ttl=128 time=0.0 ms 64 bytes from 2222::717: icmp6_seq=3 ttl=128 time=0.0 ms --- 2222::717 ping statistics --- 4 packets transmitted, 4 packets received, 0% packet loss round-trip min/avg/max = 0.0/2.5/10.0 ms
Apply	Click **Apply** to display ping result for the IP address.

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**.



Logging Service Settings

Logging Service ● Enabled ○ Disabled

Figure 139. Diagnostics > System Log > Logging Service

The following table describes the items in Figure 139.

Table 135. Logging Service

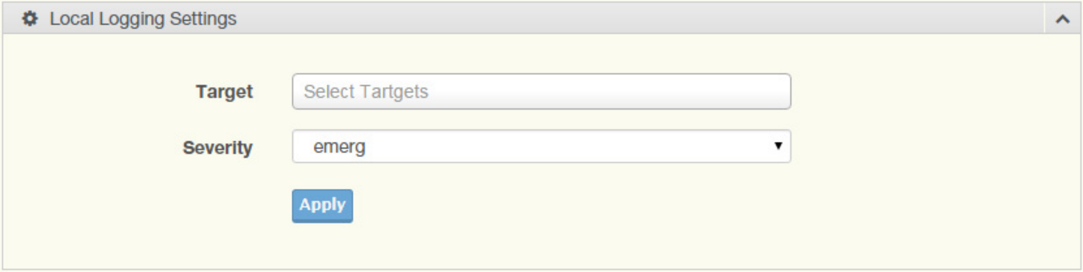
Item	Description
Logging Service	Click Enabled or Disabled to set the Logging Service status.
Apply	Click **Apply** to save the values and update the screen.

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

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**.



Local Logging Settings

Target: Select Tartgets

Severity: emerg

Figure 140. Diagnostics > System Log > Local Logging

The following table describes the items in Figure 140.

Table 136. Local Logging

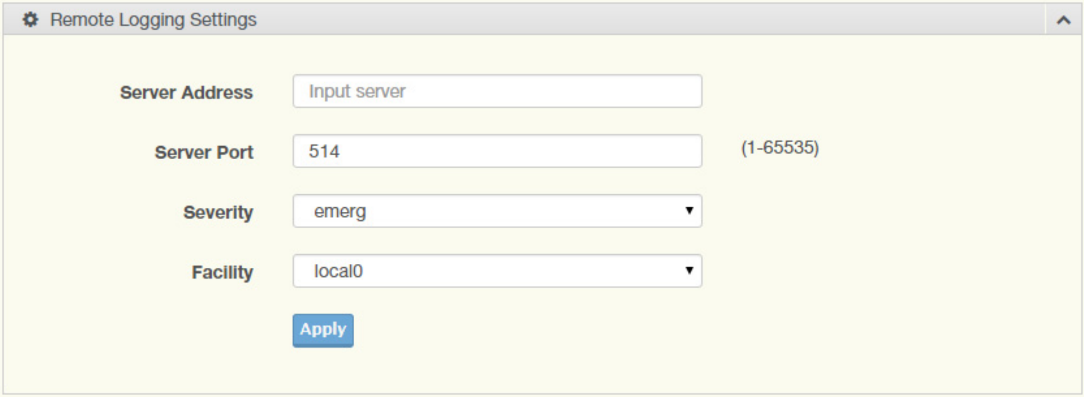
Item	Description
Target	Enter the local logging target.
Severity	Click the drop-down menu to select the severity level for local log messages. The level options are: • emerg: Indicates system is unusable. It is the highest level of severity • alert: Indicates action must be taken immediately • crit: Indicates critical conditions • error: Indicates error conditions • warning: Indicates warning conditions • notice: Indicates normal but significant conditions • info: Indicates informational messages • debug: Indicates debug-level messages
Apply	Click **Apply** to save the values and update the screen.

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

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**.



Server Address: Input server

Server Port: 514 (1-65535)

Severity: emerg

Facility: local0

Figure 141. Diagnostics > System Log > System Log Server

The following table describes the items in Figure 141.

Table 137. System Log Server

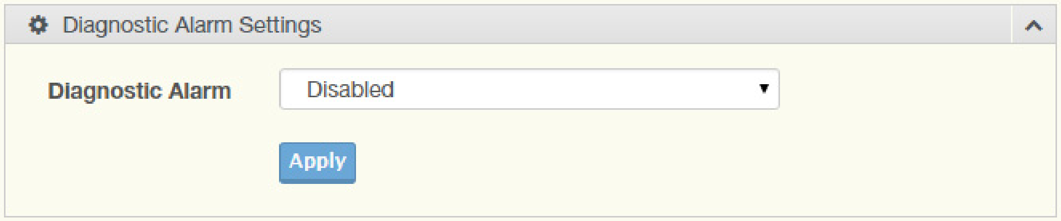
Item	Description
Server Address	Enter the IP address of the log server.
Server Port	Enter the Udp port number of the log server.
Severity	Click the drop-down menu to select the severity level for local log messages. The default is emerg. The level options are: • emerg: Indicates system is unusable. It is the highest level of severity • alert: Indicates action must be taken immediately • crit: Indicates critical conditions • error: Indicates error conditions • warning: Indicates warning conditions • notice: Indicates normal but significant conditions • info: Indicates informational messages • debug: Indicates debug-level messages
Facility	Click the drop-down menu to select facility to which the message refers.
Apply	Click **Apply** to save the values and update the screen.

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

DDM

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

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



Diagnostic Alarm Settings

Diagnostic Alarm: Disabled

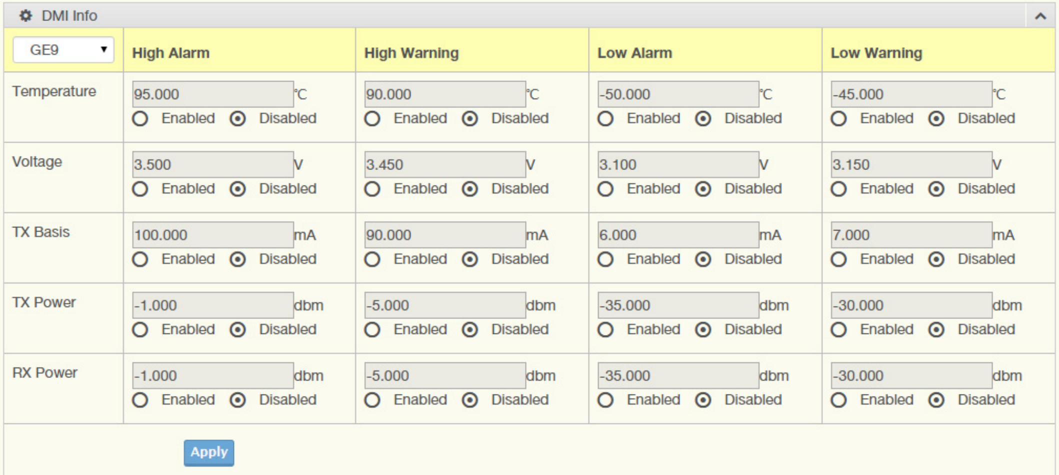
Figure 142. Diagnostics > DDM Alarm

The following table describes the items Figure 142.

Table 138. DDM Alarm

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

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



DMI Info

GE9	High Alarm	High Warning	Low Alarm	Low Warning
Temperature	95.000 °C ○ Enabled ● Disabled	90.000 °C ○ Enabled ● Disabled	-50.000 °C ○ Enabled ● Disabled	-45.000 °C ○ Enabled ● Disabled
Voltage	3.500 V ○ Enabled ● Disabled	3.450 V ○ Enabled ● Disabled	3.100 V ○ Enabled ● Disabled	3.150 V ○ Enabled ● Disabled
TX Basis	100.000 mA ○ Enabled ● Disabled	90.000 mA ○ Enabled ● Disabled	6.000 mA ○ Enabled ● Disabled	7.000 mA ○ Enabled ● Disabled
TX Power	-1.000 dbm ○ Enabled ● Disabled	-5.000 dbm ○ Enabled ● Disabled	-35.000 dbm ○ Enabled ● Disabled	-30.000 dbm ○ Enabled ● Disabled
RX Power	-1.000 dbm ○ Enabled ● Disabled	-5.000 dbm ○ Enabled ● Disabled	-35.000 dbm ○ Enabled ● Disabled	-30.000 dbm ○ Enabled ● Disabled

Figure 143. Diagnostics > DDM Alarm Info

The following table describes the items in Figure 143.

Table 139. DDM Alarm Info

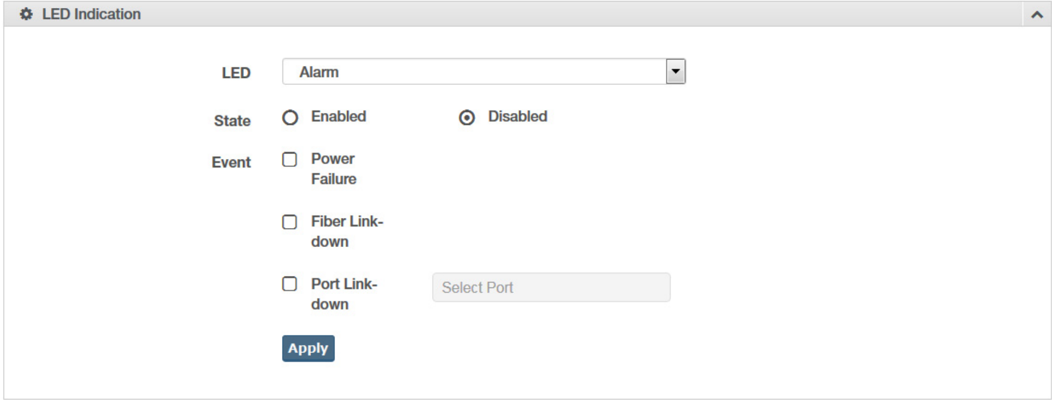
Item	Description
High Alarm	Click **Enabled** or **Disabled** to set the alarm state.
High Warning	Click **Enabled** or **Disabled** to set the alarm state.
Low Alarm	Click **Enabled** or **Disabled** to set the alarm state.
Low Warning	Click **Enabled** or **Disabled** to set the alarm state.
Apply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

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

LED Indication

The LED Indication page allows you to setup the diagnostic alarm status.

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



LED Indication

LED: Alarm

State: ○ Enabled ● Disabled

Event: □ Power Failure

□ Fiber Link-down

□ Port Link-down Select Port

Figure 144. Diagnostics > LED Indication

The following table describes the items Figure 144.

Table 140. DDM Alarm

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

The **LED Information** settings in the ensuing table are informational only: LED and State.

The **Event Information** settings in the ensuing table are informational only: Event, State, Error Times, Delete (Click on button to reset the event counter and LED) and **Refresh** (click to reload the vendor information).

Tools

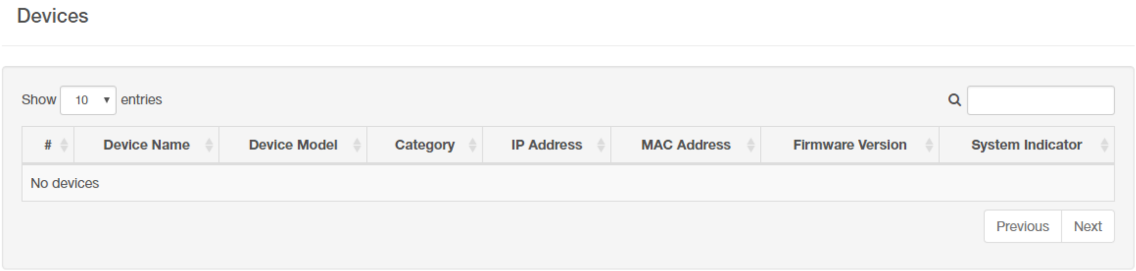
This section includes the following topics:

- ❒ “IXM”
- ❒ “Backup Manager” on page 159
- ❒ “Upgrade Manager” on page 160
- ❒ “Dual Image” on page 161
- ❒ “Save Configuration” on page 161
- ❒ “User Account” on page 161
- ❒ “N-Key” on page 162
- ❒ “Reset System” on page 163
- ❒ “Reboot Device” on page 163

IXM

The IXM tool is an industrial Ethernet switch solution to help the users deploy industrial Ethernet switch hardware by allowing users with multiple, managed Ethernet switches in the field to eliminate the need to individually connect to each device to configure it.

To access this page, click **Tools** > **IXM**.



Devices

Show 10 entries

#	Device Name	Device Model	Category	IP Address	MAC Address	Firmware Version	System Indicator
No devices							

Figure 145. Tools > IXM

The following table describes the items in Figure 145.

Table 141. IXM

Item	Description
Search Field	Enter criteria to search the IXM information.
#	Displays the reference to the device number.
Device Name	Displays the device name.
Device Model	Displays the device model type.
Category	Displays the device’s category type.
IP Address	Displays the device’s IP address.
MAC Address	Displays the device’s IP MAC address.
Firmware Version	Displays the device’s firmware version.
System Indicator	Displays the device’s system indicator.

Table 141. IXM (Continued)

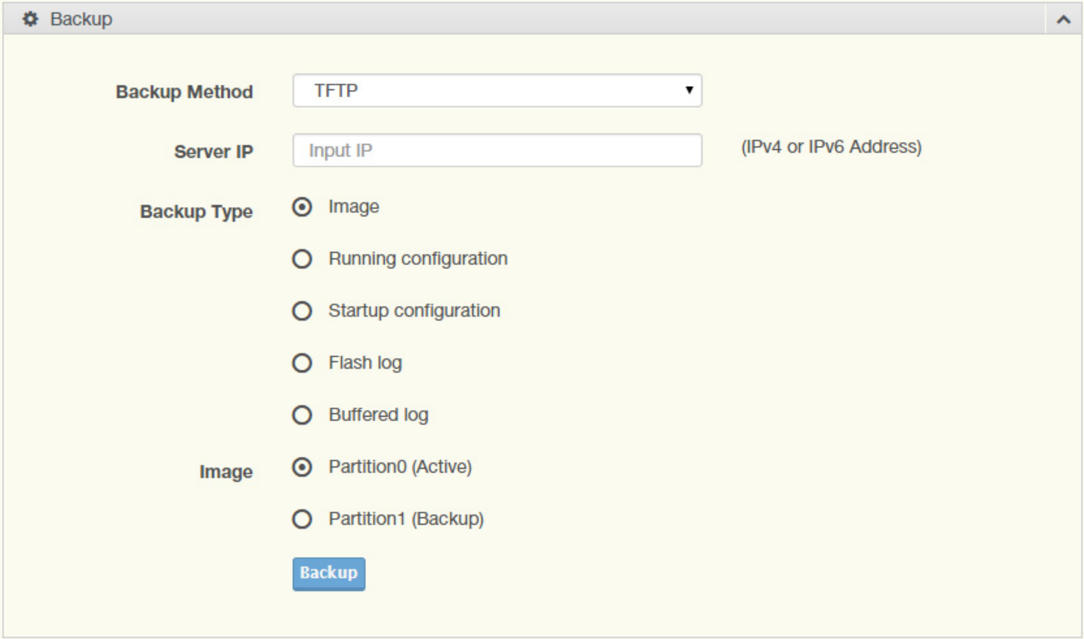
Item	Description
Previous	Click **Previous** to back to previous page.
Next	Click **Next** to go to next page.

Backup Manager

The Backup Manager page allows you to configure a remote TFTP sever or host file system in order to backup the firmware image or configuration file.

The following figures represent multiple supported devices. Some interface screens may represent specific device models.

To access this page, click **Tools** > **Backup Manager**.



Backup

Backup Method: TFTP

Server IP: Input IP (IPv4 or IPv6 Address)

Backup Type: ● Image ○ Running configuration ○ Startup configuration ○ Flash log ○ Buffered log

Image: ● Partition0 (Active) ○ Partition1 (Backup)

Figure 146. Tools > Backup Manager

The following table describes the items in Figure 146.

Table 142. Backup Manager

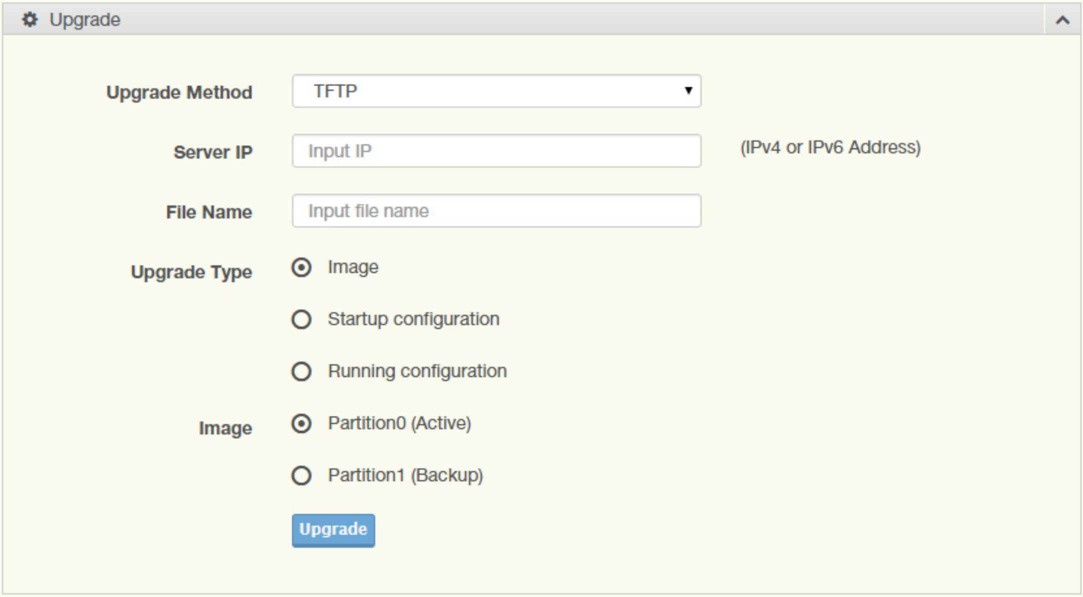
Item	Description
Backup Method	Click the drop-down menu to select the backup method: TFTP or HTTP.
Server IP	Enter the IP address of the backup server.
Backup Type	Click a type to define the backup method: image: running configuration, startup configuration, flash log, or buffered log.
Image	Click the format for the image type: 7710E_2C_1_00_13.bix (Active) or vmlinux.bix (backup).
Backup	Click **Backup** to backup the settings.

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.

The following figures represent multiple supported devices. Some interface screens may represent specific device models.

To access this page, click **Tools** > **Upgrade Manager**.



Upgrade

Upgrade Method: TFTP ▾

Server IP: Input IP (IPv4 or IPv6 Address)

File Name: Input file name

Upgrade Type: ● Image ○ Startup configuration ○ Running configuration

Image: ● Partition0 (Active) ○ Partition1 (Backup)

Figure 147. Tools > Upgrade Manager

The following table describes the items in Figure 147.

Table 143. Upgrade Manager

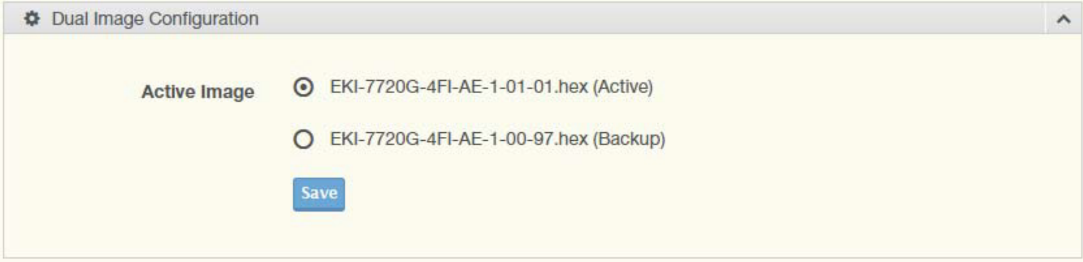
Item	Description
Upgrade Method	Click the drop-down menu to select the upgrade method: TFTP or HTTP.
Server IP	Enter the IP address of the upgrade server.
File Name	Enter the file name of the new firmware version.
Upgrade Type	Click a type to define the upgrade method: image, startup configuration, or running configuration.
Image	Click the format for the image type: 7710E_2C_1_00_13.bix (Active) or vmlinux.bix (backup).
Upgrade	Click **Upgrade** to upgrade to the current version.

Dual Image

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

The following figures represent multiple supported devices. Some interface screens may represent specific device models.

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



Dual Image Configuration

Active Image
● EKI-7720G-4FI-AE-1-01-01.hex (Active)
○ EKI-7720G-4FI-AE-1-00-97.hex (Backup)

Figure 148. Tools > Dual Image

The following table describes the items in Figure 148.

Table 144. Dual Image

Item	Description
Active Image	Click the format for the image type: Partition0 (Active) or Partition1 (backup).
Save	Click **Save** to save and keep the new settings.

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

Save Configuration

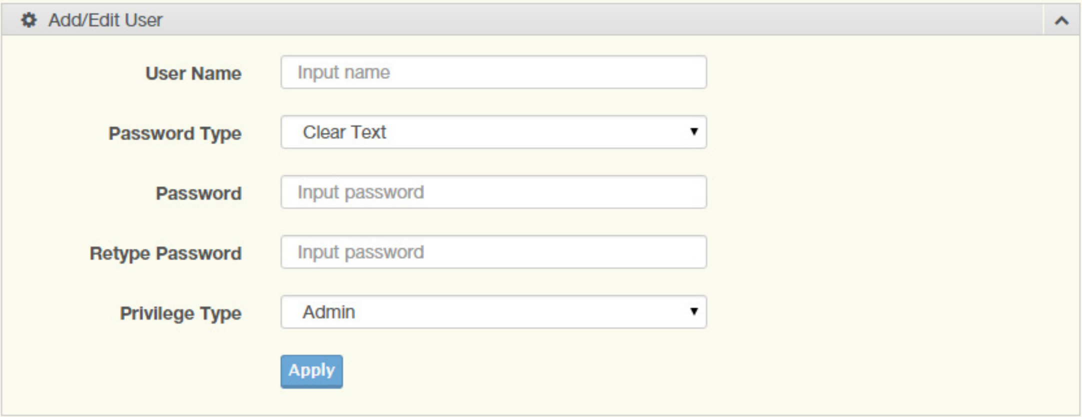
To access this page, click **Tools** > **Save Configuration**.

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

User Account

The User Account page allows you to setup a user and the related parameters. Use the fields in this window to change the default password.

To access this page, click **Tools** > **User Account**.



User Name: Input name

Password Type: Clear Text

Password: Input password

Retype Password: Input password

Privilege Type: Admin

Figure 149. Tools > User Account

The following table describes the items in Figure 149 on page 162.

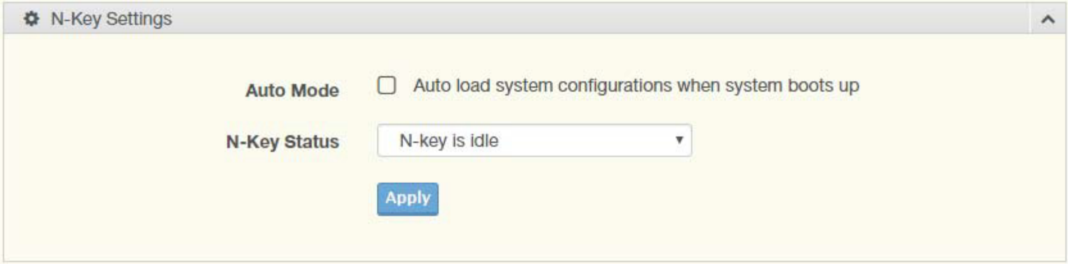
Table 145. User Account

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: **Clear Text**, **Encrypted** or **No Password**.
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: **Admin** or **User**.
Apply	Click **Apply** to create a new user account.

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

N-Key

To access this page, click **Tools** > **N-Key**.



Auto Mode: □ Auto load system configurations when system boots up

N-Key Status: N-key is idle

Figure 150. Tools > N-Key

The following table describes the items in Figure 150 on page 162.

Table 146. N-Key

Item	Description
Auto Mode	Click the option to set the auto mode for the N-Key status.
N-Key Status	Click the drop-down menu to select N-Key status.
Apply	Click **Apply** to create a new user account.

The ensuing table for **N-Key Information** settings are informational only: Auto Mode and N-Key Status.

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 made previously are lost, even if you issued a save.

Reset settings take effect after a system reboot.

Reboot Device

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

Click **Reboot** to reboot the switch. Any configuration changes that are not saved before rebooting are lost.

Appendix A

Troubleshooting

- ❐ Verify that the device is using the right power cord/adapter (DC 48V); please don't use a power adapter with DC output higher than 48V, or it may damage this device.
- ❐ Select the proper UTP/STP cable to construct the user network. Use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable for RJ-45 connections that depend on the connector type the device equipped: 100R Category 3, 4 or 5 cable for 10Mbps connections, 100R Category 5 cable for 100Mbps connections, or 100R Category 5e/above cable for 1000Mbps connections. Also ensure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).
- ❐ R = replacement letter for Ohm symbol.
- ❐ **Diagnosing LED Indicators:** To assist in identifying problems, the device can be easily monitored through panel indicators, which describe common problems the user may encounter and where the user can find possible solutions.
- ❐ If the power indicator does not light on when the power cord is plugged in, you may have a problem with power cord; check for loose power connections, power losses, or surges, at the power outlet. If you still cannot resolve the problem, contact a local dealer for assistance.
- ❐ If the LED indicators are normal and the connected cables are correct but the packets still cannot be transmitted, please check the user system's Ethernet devices' configuration or status.