comnet
Communication Networks

INSTALLATION AND OPERATION MANUAL

CNGE28FX4TX24MS(2,POE2/48)

Layer 2 Industrially Hardened Managed Ethernet Switch All Gigabit 24 TX with PoE+ and 4 Combo Ports

This manual serves the following ComNet Model Numbers:

CNGE28FX4TX24MS2
CNGE28FX4TX24MSPOE2/48

The ComNet CNGE28FX4TX24MS(2,POE2/48) Layer 2 Managed 28 Port Ethernet Switch supports twenty-four 10/100/1000 BASE-TX ports and four 10/100/1000 BASE-TX or 100/1000 BASE-FX SFP Combo ports of Ethernet data. PoE+ power is available for distribution across all 24 BASE-TX ports. The four combination ports are 10/100/1000TX or 100/1000FX SFP configurable for fiber type (multimode or single-mode), connector type and distance. Dual 48 VDC input power design ensures vital network capabilities with minimum downtime. Utilizing RSTP/STP (802.1w/1D) MSTP, and X-Ring redundant ring topologies, a network recovery time of <20 ms is provided for protection from network faults or temporary interruptions. The switch is optically (100/1000BASE-FX) and electrically compatible with any IEEE 802.3 compliant Ethernet device and are hardened for use in harsh operating environments.

Contents

Regulatory Compliance Statement

Product(s) associated with this publication complies/comply with all applicable regulations. Please refer to the Technical Specifications section for more details.

Warranty

ComNet warrants that all ComNet products are free from defects in material and workmanship for a specified warranty period from the invoice date for the life of the installation. ComNet will repair or replace products found by ComNet to be defective within this warranty period, with shipment expenses apportioned by ComNet and the distributor. This warranty does not cover product modifications or repairs done by persons other than ComNet-approved personnel, and this warranty does not apply to ComNet products that are misused, abused, improperly installed, or damaged by accidents.

Please refer to the Technical Specifications section for the actual warranty period(s) of the product(s) associated with this publication.

Disclaimer

Information in this publication is intended to be accurate. ComNet shall not be responsible for its use or infringements on third-parties as a result of its use. There may occasionally be unintentional errors on this publication. ComNet reserves the right to revise the contents of this publication without notice.

Note. The PoE port may be considered SELV circuits, if:

» Not likely to require connection to an Ethernet network with outside plant routing including campus environment; and

» The installation instructions clearly state that the ITE is to be connected only to PoE Networks without routing to the outside plant.

Safety Indications

» The equipment can only be accessed by a service person or users who have been instructed.

» The equipment should be installed in the location that needs a tool or lock and key, or other means of security, and controlled by a person of authority.

Federal Communication Commission Interference Statement

For further certification information, please go to www.comnet.net

Declaration of Conformity

CE

This product has passed the CE test for environmental specifications when shielded cables are used for external wiring. We recommend the use of shielded cables. Please contact your local supplier for ordering information.

This product has passed the CE test for environmental specifications. Test conditions for passing included the equipment being operated within an industrial enclosure. In order to protect the product from being damaged by ESD (Electrostatic Discharge) and EMI leakage, we strongly recommend the use of CE-compliant industrial enclosure products.

FCC Class A

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

Safety Instructions

Read these safety instructions carefully.

- » Keep this user manual for later reference.
- » Disconnect this equipment from any AC outlet before cleaning. Use damp cloth. Do not use liquid or spray detergents for cleaning.
- » For plug-in equipment, the power outlet socket must be located near the equipment and must be easily accessible.
- » Keep this equipment away from humidity.
- » Put this equipment on a stable surface during installation. Dropping it or letting it fall may cause damage.
- » The openings on the enclosure allow for air convection. Protect the equipment from over-heating. DO NOT COVER THE OPENINGS.
- » Make sure the voltage of the power source is correct before connecting the equipment to the power outlet.
- » Position the power cord so that people cannot step on it. Do not place anything over the power cord.
- » All cautions and warning on the equipment should be noted.
- » If the equipment is not used for a long time, disconnect it from the power source to avoid damage by transient over voltage.
- » Never pour any liquid into an opening. This may cause fire or electrical shock.
- » Never open the equipment. For safety reasons, the equipment should be opened only by qualified service personnel.
- » If one of the following situations arises, get the equipment checked by service personnel:
  - › The power cord or plug is damaged.
  - › Liquid has penetrated into the equipment.
  - › The equipment has been exposed to moisture.
  - › The equipment does not work well, or you cannot get it to work according to the user manual
  - › The equipment has been dropped and damaged.
  - › The equipment has obvious signs of breakage.
- » PoE requirements: The equipment is to be connected only to PoE networks without routing to the outside plant.
- » Do not leave this equipment in an environment where the storage temperature may go below -40°C (-40°F) or above 75°C (167°F) this could damage the equipment. The equipment should be in a controlled environment.

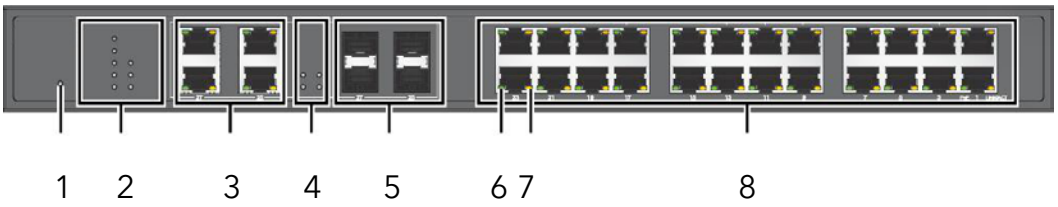
1.0 Product Overview

1.1 Specifications

Specifications	Description	
Interface	I/O Port	24 x 10/100/1000BaseT(X) + 4 x 10/100/1000Base-T(X) or 4 x 100/1000Base-X SFP Port
	Power Connector	4-pin screw terminal
	Relay Connector	3-pin screw terminal
Physical	Enclosure	Metal Shell
	Protection Class	IP30
	Installation	Rack mounting
	Dimensions (W x H x D)	438.0 x 43.6 x 259.2mm
LED Display	System LED	SYS, PWR1, PWR2, P-Fail, Loop detection, R.M., Ring Fail, Temp
	Port LED	Speed, Link, Activity, PoE (only for CNGE28FX4TX24MSPOE2/48)
Environment	Operating Temperature	-40°C ~ 75°C (-40°F ~ 167°F)
	Storage Temperature	-40°C ~ 85°C (-40°F ~ 185°F)
	Ambient Relative Humidity	10 ~ 95% (non-condensing)
Switch Properties	MAC Address	8K-entry
	Switching Bandwidth	56 Gbps
Power	Power Consumption	CNGE28FX4TX24MS2: 20W @ 24V CNGE28FX4TX24MSPOE2/48: 20W @ 48V (before PoE Load)
	Power Input	CNGE28FX4TX24MS2: 12 - 48 VDC CNGE28FX4TX24MSPOE2/48: 48 VDC (46 - 57 VDC) for PoE system (53 - 57 VDC is recommended for PoE+ devices)
Certifications	Safety	IEC EN60950, EN61010
	EMC	CE, FCC
	EMI	EN55022 Class A
	EMS	EN 61000-4-2 (ESD) Level 3 EN 61000-4-3 (RS) Level 3 EN 61000-4-4 (EFT) Level 3 EN 61000-4-5 (Surge) Level 3 EN 61000-4-6 (CS) Level 3 EN 61000-4-8 (Magnetic Field) Level 3
	Shock	IEC 60068-2-27
	Freefall	IEC 60068-2-32
	Vibration	IEC 60068-2-6
	Railway Track Side	EN 50121-4

1.2. Hardware Views

1.2.1 Front View



Front View

No.	Item	Description
1	Reset button	Button allows for system soft reset or factory default reset.
2	System LED panel	See "System LED Panel" on page 4 for further details.
3	ETH port	RJ45 ports x 4
4	SFP LEDs	SFP link activity LEDs
5	ETH port	Fiber ports x 4
6	PoE LED	Orange: 100M Green: 1G
7	LNK/ACT LED	Link activity LED
8	ETH port	RJ45 ports x 24

System LED Panel

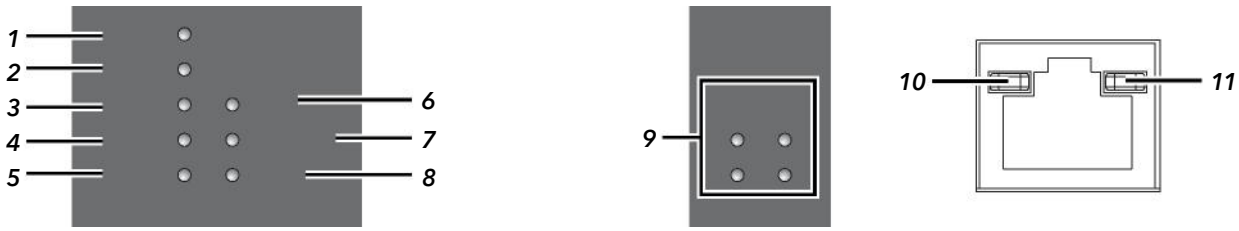


Figure 1-2. System LED Panel Table 1-3. System LED Panel

Table 1-3. System LED Panel (Continued)

No.	LED Name	LED Color	Description
1	SYS	Solid Green	System is operating normally
		Off	System is powered down / system crash / operation initiating.
2	PWR	Solid green	Powered up
		Off	Powered down or not installed
3	PWR2	Solid Green	Powered Up
		Off	Powered down or not installed
4	P-FAIL	Solid Red	PWR1 or PWR2 is disconnected
		Off	PWR1 or PWR2 connected
5	LOOP	Solid Red	Loop detected
		Off	No loop detected
6	R.M.	Solid Green	Switch is Ring Master
7	Ring Fail		
8	Temp		
SFP			
9	SFP LED	Solid Green	SFP plug-in and link up
		Blink Green	Packet transmit/receive
		Off	SFP unplugged or link down
RJ45			
10	PoE	Solid Green	Connected to power supply and able to act as PSE
		Off	Disconnected from power supply and unable to act as PSE
11	LNK/ACT	Solid green	Current link speed is 1000M.
		Blink green	Packet transmit and receive.
		Off	No link.
		Solid amber	Current link speed is 100/10M.
		Blink amber	Packet transmit and receive.
		Off	No link.

1.2.2 Rear View

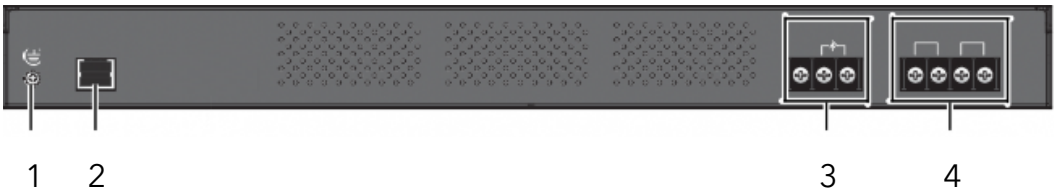


Figure 1-3. Rear View

Table 1-4. Rear View

No.	Item	Description
1	Ground terminal	Screw terminal used to ground chassis.
2	Console serial port	Console cable port to COM port (DB9 male) on computer to RS232 managed switch (RJ45 female).
3	P-Fail block	Connect cabling for alarm wiring.
4	Power block	Connect cabling for power wiring.

1.3 Dimensions

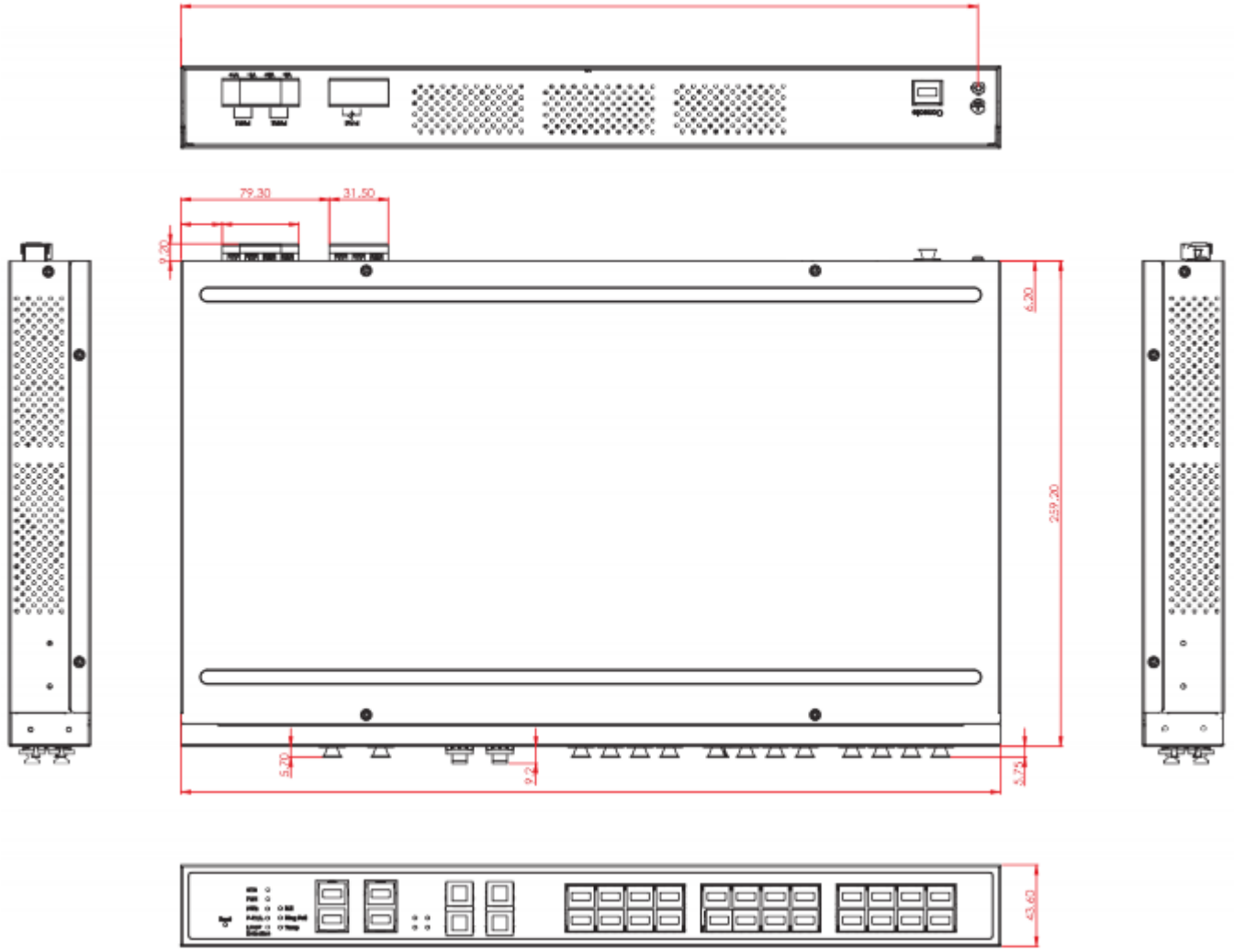


Figure 1-4. CNGE28FX4TX24MSPOE2/48 Dimensions

1.4. Packing List

The product package you have received should contain the following items. If any of them are not included or are damaged, please contact your local vendor for support.

» 1 × Industrial Ethernet Switch
» 1 × Rack Mount Kit
» 1 × Quick Start Guide
» 1 × Serial Console Cable

2.0 Installation Guidelines

2.1. Warnings

Warning: Before working on equipment that is connected to power lines, remove any jewelry (including rings, necklaces, and watches). Metal objects can heat up when connected to power and ground, which can cause serious burns or weld the metal object to the terminals.

- Exposure to chemicals can degrade the sealing properties of materials used in the sealed relay device.
- It is not recommended to work on the system or connect or disconnect cables during periods of lightning activity.
- Before performing any of the following procedures, disconnect the power source from the DC circuit.
- Read the installation instructions before connecting the system to its power source.
- This unit is intended for installation in restricted access areas. A restricted access area is defined as an area that can be accessed only through the use of a special tool, lock and key, or other means of security.
- The device must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor.
- This unit may have more than one power supply connection. All connections must be removed to de-energize the unit.
- If the switch is to be installed in a hazardous location, ensure that the DC power source is located away from the vicinity of the switch.
- The installation of the equipment must comply with all national and local electrical codes.
- Explosion Hazard - The area must be known to be nonhazardous before servicing or replacing any components.
- ***Airflow Around The Switch Must Be Unrestricted.*** To Prevent The Switch From Overheating, There Must Be The Following Minimum Clearances:
  - Top and Bottom: 2.0 in (50.8 mm)
  - Sides: 2.0 in (50.8 mm)
  - Front: 2.0 in (50.8 mm)

2.2. Installation Guidelines

- » The following guidelines are provided to optimize the device performance. Review the guidelines before installing the device.
- » Make sure cabling is away from sources of electrical noise. Radios, power lines, and fluorescent lighting fixtures can interference with the device performance.
- » Make sure the cabling is positioned away from equipment that can damage the cables.
- » Operating environment is within the ranges listed range, see “Specifications” on page 1.
- » Relative humidity around the switch does not exceed 95 percent (non-condensing).
- » Altitude at the installation site is not higher than 10,000 feet.
- » In 10/100 and 10/100/1000 fixed port devices, the cable length from the switch to connected devices can not exceed 100 meters (328 feet).
- » Make sure airflow around the switch and respective vents is unrestricted. Without proper airflow the switch can overheat. To prevent performance degradation and damage to the switch, make sure there is clearance at the top and bottom and around the exhaust vents.

2.3. Environment and Enclosure Guidelines

Review these environmental and enclosure guidelines before installation:

This equipment is intended for use in a Pollution Degree 2 industrial environment, in over-voltage Category II applications (as defined in IEC publication 60664-1), at altitudes up to 9842 ft (3 km) without derating.

This equipment is considered Group 1, Class A industrial equipment, according to IEC/ CISPR Publication 11. Without appropriate precautions, there may be potential difficulties ensuring electromagnetic compatibility in other environments due to conducted as well as radiated disturbance.

This equipment is supplied as open-type equipment. It must be mounted within an enclosure that is suitably designed for those specific environmental conditions that will be present and appropriately designed to prevent personal injury resulting from accessibility to live parts. The enclosure must have suitable flame-retardant properties to prevent or minimize the spread of flame, complying with a flame-spread rating of 5VA, V2, V1, V0 (or equivalent) if nonmetallic. The interior of the enclosure must be accessible only by the use of a tool. Subsequent sections of this publication might contain additional information regarding specific enclosure-type ratings that are required to comply with certain product safety certifications.

2.3.1 Connecting Hardware

In this instruction, it will explain how to find a proper location for your Modbus Gateways, and how to connect to the network, hock up the power cable, and connect to the managed Ethernet switch.

2.4. Verifying Switch Operation

Before installing the device in a rack or on a wall, power on the switch to verify that the switch passes the power-on self-test (POST). To connect the cabling to the power source see “Power Supply Installation” on page 15.

At startup (POST), the System LED blinks green, while the remaining LEDs are a solidy green. Once the switch passes POST self-test, the System LED turns green. The other LEDs turn off and return to their operating status. If the switch fails POST, the System LED switches to an amber state.

After a successful self-test, power down the switch and disconnect the power cabling. The switch is now ready for installation on its final location.

2.5. Installing the Switch

2.5.1 Rack-Mounting

1. Align the rack mount brackets with the holes on the switch.
2. Secure the rack mount brackets with the provided screws.

Figure 2-1. Installing the Rack Mount Brackets

3. Align the switch with the posts on the rack cabinet.
4. Secure the switch with the provided screws.

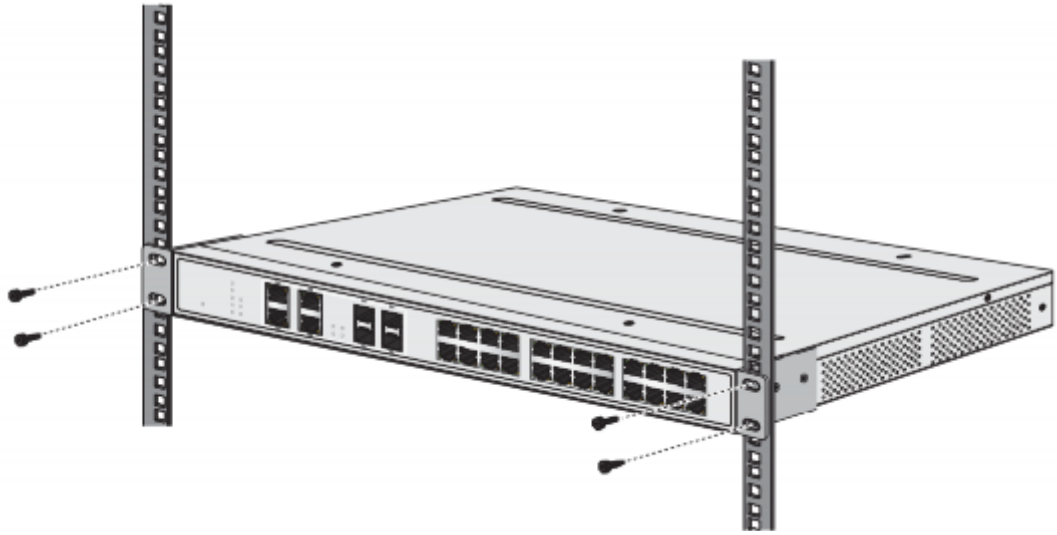


Figure 2-2. Installing the Switch

2.6. Installing and Removing SFP Modules

Up to two fiber optic ports are available (dependent on model) for use in the switch. Refer to the technical specifications for details.

The Gigabit Ethernet ports on the switch are 100/1000Base SFP Fiber ports, which require using the 100M or 1G mini-GBIC fiber transceivers to work properly. ComNet provides completed transceiver models for different distance requirement.

The concept behind the LC port and cable is quite straight forward. Suppose that you are connecting devices I and II; contrary to electrical signals, optical signals do not require a circuit in order to transmit data. Consequently, one of the optical lines is used to transmit data from device I to device II, and the other optical line is used transmit data from device II to device I, for full-duplex transmission.

Remember to connect the Tx (transmit) port of device I to the Rx (receive) port of device II, and the Rx (receive) port of device I to the Tx (transmit) port of device II. If you make your own cable, we suggest labeling the two sides of the same line with the same letter (A-to-A and B-to-B, or A1-to-A2 and B1-to-B2).

2.6.1 Installing SFP Modules

To connect the fiber transceiver and LC cable, use the following guidelines:

1. Remove the dust plug from the fiber optic slot chosen for the SFP transceiver.

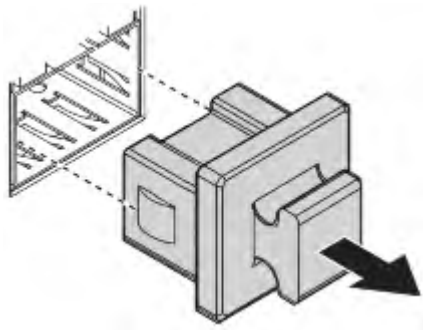


Figure 2-3. Removing the Dust Plug from an SFP Slot

Do not remove the dust plug from the SFP slot if you are not installing the transceiver at this time. The dust plug protects hardware from dust contamination.

2. Position the SFP transceiver with the handle on top, see the following figure.
3. Locate the triangular marking in the slot and align it with the bottom of the transceiver.
4. Insert the SFP transceiver into the slot until it clicks into place.
5. Make sure the module is seated correctly before sliding the module into the slot. A click sounds when it is locked in place.

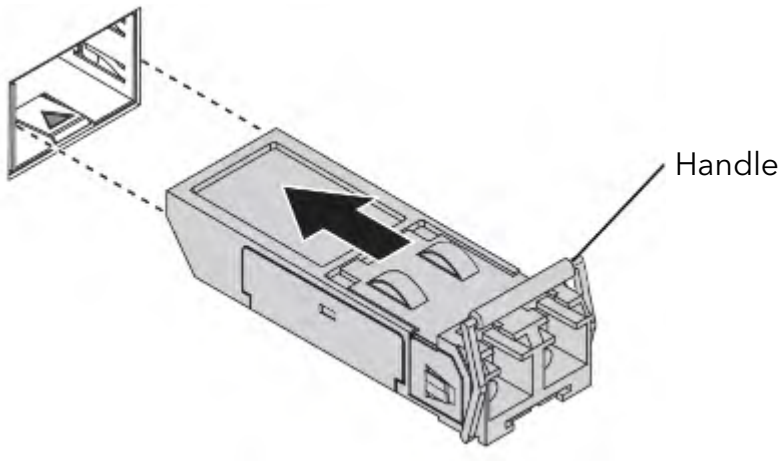


Figure 2-4. Installing an SFP Transceiver

If you are attaching fiber optic cables to the transceiver, continue with the following step. Otherwise, repeat the previous steps to install the remaining SFP transceivers in the device.

6. Remove the protective plug from the SFP transceiver.

Do not remove the dust plug from the transceiver if you are not installing the fiber optic cable at this time. The dust plug protects hardware from dust contamination.

7. Insert the fiber cable into the transceiver. The connector snaps into place and locks.

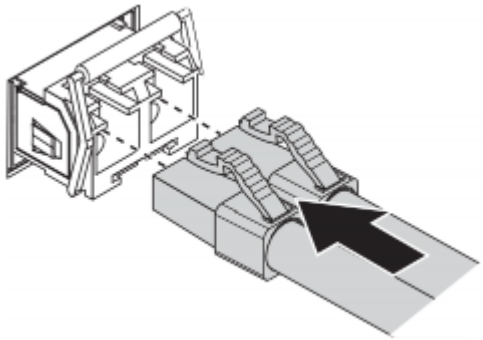


Figure 2-5. Attaching a Fiber Optic Cable to a Transceiver

8. Repeat the previous procedures to install any additional SFP transceivers in the switch. The fiber port is now setup.

2.6.2 Removing SFP Modules

To disconnect an LC connector, use the following guidelines:

1. Press down and hold the locking clips on the upper side of the optic cable.

2. Pull the optic cable out to release it from the transceiver.

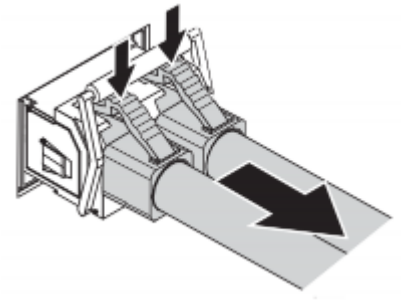


Figure 2-6. Removing a Fiber Optic Cable to a Transceiver

3. Hold the handle on the transceiver and pull the transceiver out of the slot.

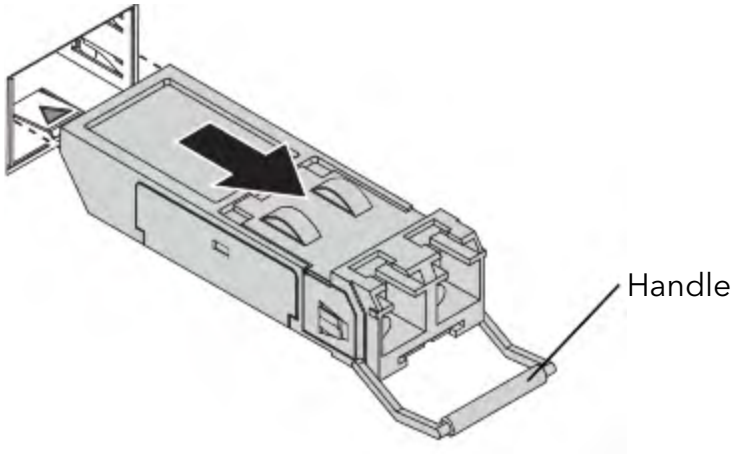


Figure 2-7. Removing an SFP Transceiver

Replace the dust plug on the slot if you are not installing a transceiver. The dust plug protects hardware from dust contamination.

2.7. Connecting the Switch to Ethernet Ports

2.7.1 RJ45 Ethernet Cable Wiring

For RJ45 connectors, data-quality, twisted pair cabling (rated CAT5 or better) is recommended. The connector bodies on the RJ45 Ethernet ports are metallic and connected to the GND terminal. For best performance, use shielded cabling. Shielded cabling may be used to provide further protection.

Table 2-1. RJ45 Ethernet Wiring for Reference

Straight-thru Cable Wiring		Cross-over Cable Wiring	
Pin 1	Pin 1	Pin 1	Pin 3
Pin 2	Pin 2	Pin 2	Pin 6
Pin 3	Pin 3	Pin 3	Pin 1
Pin 6	Pin 6	Pin 6	Pin 2

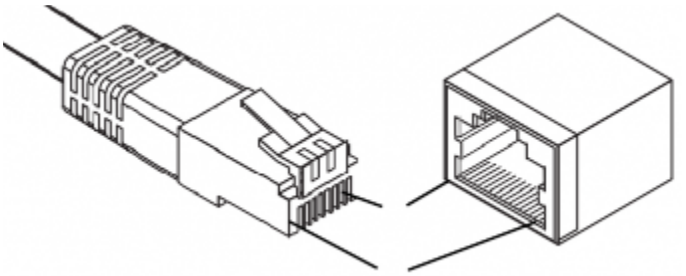


Figure 2-8. Ethernet Plug & Connector Pin Position

Maximum cable length: 100 meters (328 ft) for 10/100/1000Base-T

2.8. Connecting the Switch to Console Port

The industrial switch supports a secondary means of management. By connecting the RJ45 to RS232 serial cable between a COM port on your PC (9-pin D-sub female) and the switch's RJ45 (RJ45) port, a wired connection for management can be established.

To terminal or PC To console port

Figure 2-9. Serial Console Cable

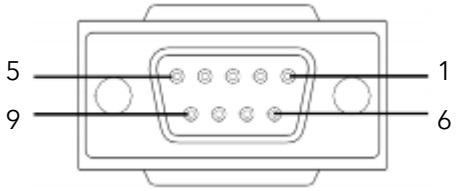


Figure 2-10. DB 9 Pin Position

Table 2-2. Pin Assignment

DB9 Connector	RJ45 Connector
NC	1 Orange/White
NC	2 Orange
2	3 Green/White
NC	4 Blue
5	5 Blue/White
3	6 Green
NC	7 Brown/White
NC	8 Brown

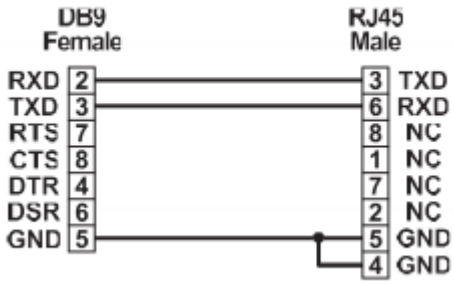


Figure 2-11. Pin Assignment

2.9. Power Supply Installation

2.9.1 Overview

Power down and disconnect the power cord before servicing or wiring the switch.

» Do not disconnect modules or cabling unless the power is first switched off.

» The device only supports the voltage outlined in the type plate. Do not use any other power components except those specifically designated for the switch device.

» Disconnect the power cord before installation or cable wiring.

The switches can be powered by using the same DC source used to power other devices. A DC voltage range of 12 to 48 VDC (Non PoE) or 48 VDC (PoE) must be applied between the V1+ terminal and the V1- terminal (PW1), see the following illustrations. A Class 2 power supply is required to maintain a UL60950 panel listing. The chassis ground screw terminal should be tied to the panel or chassis ground. A redundant power configuration is supported through a secondary power supply unit to reduce network down time as a result of power loss.

Dual power inputs are supported and allow you to connect a backup power source.

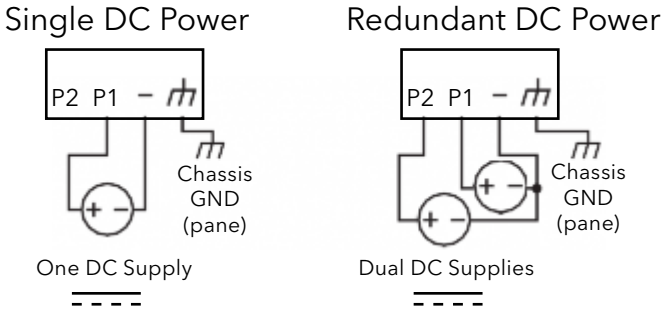


Figure 2-12. Power Wiring for Managed Ethernet Switch

2.9.2 Considerations

Take into consideration the following guidelines before wiring the device:

» The Terminal Block (CN1) is suitable for 12-24 AWG (3.31-0.205 mm^2). Torque value 7 lb/in.

» The cross sectional area of the earthing conductors shall be at least 3.331 mm^2.

» Calculate the maximum possible current for each power and common wire. Make sure the power draw is within limits of local electrical code regulations.

» For best practices, route wiring for power and devices on separate paths.

» Do not bundle together wiring with similar electrical characteristics.

» Make sure to separate input and output wiring.

» Label all wiring and cabling to the various devices for more effective management and servicing.

Routing communications and power wiring through the same conduit may cause signal interference. To avoid interference and signal degradation, route power and communications wires through separate conduits.

2.9.3 Grounding the Device

- » Do not disconnect modules or cabling unless the power is first switched off. The device only supports the voltage outlined in the type plate. Do not use any other power components except those specifically designated for the switch device.
- » Before connecting the device properly ground the device. Lack of a proper grounding setup may result in a safety risk and could be hazardous.
- » Do not service equipment or cables during periods of lightning activity.
- » Do not service any components unless qualified and authorized to do so.
- » Do not block air ventilation holes.

Electromagnetic Interference (EMI) affects the transmission performance of a device. By properly grounding the device to earth ground through a drain wire, you can setup the best possible noise immunity and emissions.

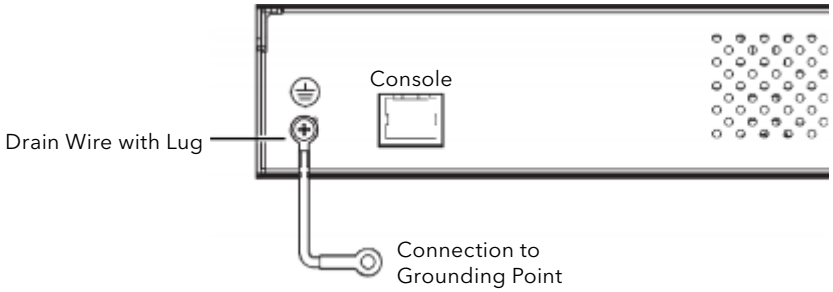


Figure 2-13. Grounding Connection

By connecting the ground terminal by drain wire to earth ground the switch and chassis can be ground.

Before applying power to the grounded switch, it is advisable to use a volt meter to ensure there is no voltage difference between the power supply's negative output terminal and the grounding point on the switch.

2.9.4 Wiring a Relay Contact

The following section details the wiring of the relay output. The terminal block on the managed Ethernet switch is wired and then installed onto the terminal receptor located on the managed Ethernet switch.

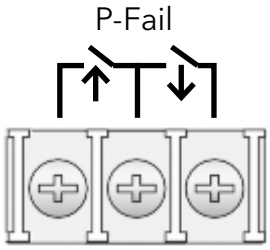


Figure 2-14. Terminal Receptor: Relay Contact

The terminal receptor includes a total of three pins.

2.9.5 Wiring the Power Inputs

» Do not disconnect modules or cabling unless the power is first switched off. The device only supports the voltage outlined in the type plate. Do not use any other power components except those specifically designated for the switch device.

Power down and disconnect the power cord before servicing or wiring the switch.

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

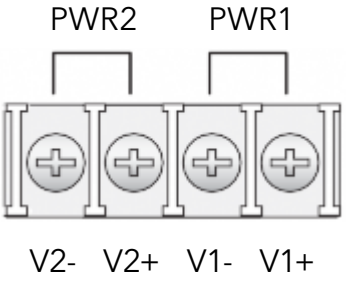


Figure 2-15. Terminal Receptor: Power Input Contacts

To wire the power inputs:

Make sure the power is not connected to the switch or the power converter before proceeding.

1. Insert a small flat-bladed screwdriver in the V1+/V1- wire-clamp screws, and loosen the screws.
2. Insert the negative/positive DC wires into the V+/V- terminals of PW1. If setting up power redundancy, connect PW2 in the same manner.
3. Tighten the wire-clamp screws to secure the DC wires in place.

Figure 2-16. Installing DC Wires in a Terminal Block

2.10. Reset Button

Reset configuration to factory default

Press and hold Reset button for 5 seconds.

System reboot

Press and hold Reset button for 2 seconds.

Do NOT power off the Ethernet switch when loading default settings.

3.0 Setup

3.1. First Time Setup

3.1.1 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.

3.1.2 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 failover 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.

3.1.3 Administrative Interface Access

There are several administrative interfaces to the switch:

1. A graphical web interface accessible via the switch's built-in web server. Both HTTP and secure HTTPS with SSL are supported.

This is the recommended method for managing the switch.

2. A terminal interface via the RS232/USB port or over the network using telnet or Secure Shell (SSH).

3. An SNMP interface can be used to read/write many settings.

4. Command Line Interface (CLI) can be used to read/write most settings. Initial setup must be done using an Ethernet connection (recommended) or the serial port.

3.1.4 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.

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://192.168.10.1 in your browser's address bar. Replace "http" with "https" to use secure http and replace "192.168.10.1" 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.

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

3.1.5 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.

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.

3.1.6 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

On managed switches with gigabit combination ports, those ports with 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.

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

3.2. Command Line Interface Configuration

3.2.1 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").

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>

3.2.2 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 "cli" for the username and "admin" for the password. The switch will respond with "Managed switch configuration CLI ready".

3.3. 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].

3.3.1 Preparing for Web Configuration

The interface requires the installation and connection of the switch to the existing network. A PC also connected to the network is required to connect to the switch and access the interface through a web browser. The required networking information is provided as follows:

- » IP address: 192.168.10.1
- » Subnet mask: 255.255.255.0
- » Default gateway: 192.168.10.254
- » User name: admin
- » Password: admin

3.3.2 System Login

Once the switch is installed and connected, power on the switch. The following information guides you through the logging in process.

1. Launch your web browser on the PC.
2. In the browser's address bar, type the switch's default IP address (192.168.10.1). The login screen displays.
3. Enter the user default name and password (admin / admin).
4. Click OK on the login screen to log in. The main interface displays.

4.0. Switch Management

4.1. Log In

To access the login window, connect the device to the network, see “Connecting the Switch to Ethernet Ports” on page 13. Once the switch is installed and connected, power on the switch see the following procedures to log into your switch.

When the switch is first installed, the default network configuration is set to DHCP enabled. You will need to make sure your network environment supports the switch setup before connecting it to the network.

1. Launch your web browser on a computer.
2. In the browser’s address bar type in the switch’s default IP address (192.168.10.1). The login screen displays.
3. Enter the default user name and password (admin/admin) to log into the management interface. You can change the default password after you have successfully logged in.
4. Click Login to enter the management interface.

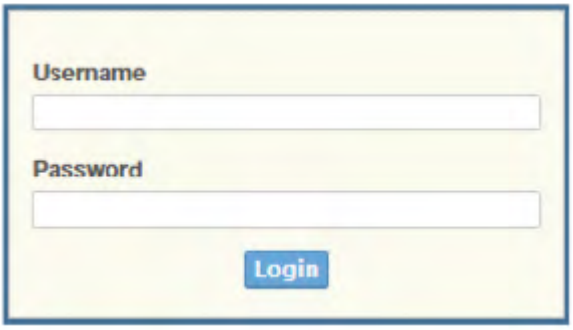


Figure 4-1. Login Screen

4.2. Recommended Practices

One of the easiest things to do to help increase the security posture of the network infrastructure is to implement a policy and standard for secure management. This practice is an easy way to maintain a healthy and secure network.

After you have performed the basic configurations on your switches, the following is a recommendation which is considered best practice policy.

4.2.1 Changing Default Password

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

To change the password:

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

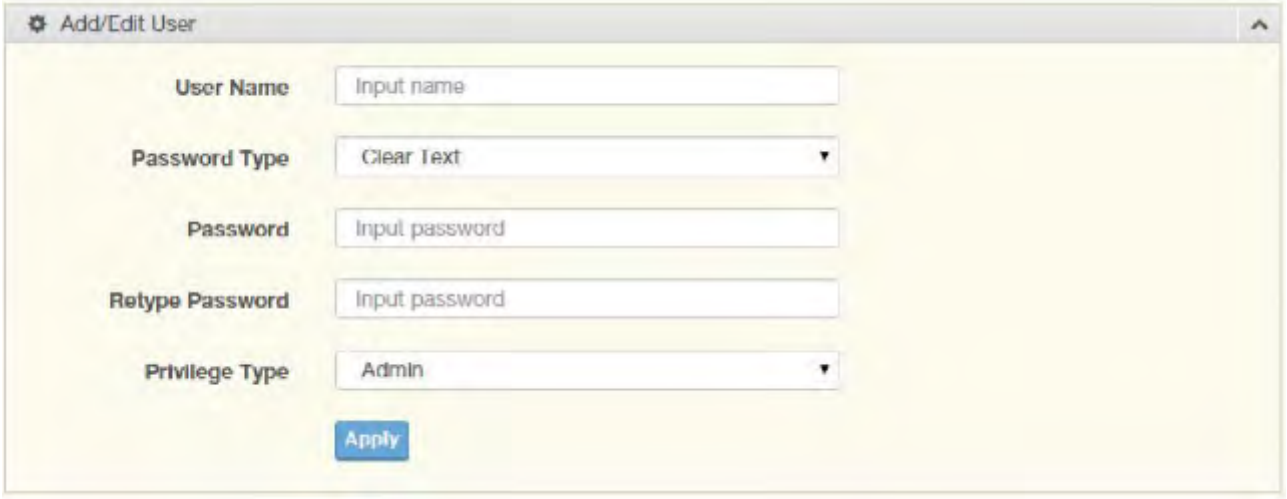


Figure 4-2. Changing a Default Password

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

4.3. Monitoring

4.3.1 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.

Figure 4-3. Monitoring > Device Information

Table 4-1. Monitoring > 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.

4.3.2 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.

Figure 4-4. Monitoring > Logging Message

Table 4-2. Monitoring > 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 ensuing table for Logging Information table settings are informational only: Target, Severity and Category.

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

4.3.3 Port Monitoring

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

Port Statistics

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

Figure 4-5. Monitoring > Port Monitoring > Port Statistics

Table 4-3. Monitoring > Port Monitoring > Port Statistics

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 ensuing table for IF MIB Counters settings are informational only: ifInOctets, ifInUcast-Pkts, ifInNUcastPkts, ifInDiscards, ifOutOctets, ifOutUcastPkts, ifOutNUcastPkts, ifOutDis-cards, ifInMulticastPkts, ifInBroadcastPkts, ifOutMulticastPkts and ifOutBroadcastPkts.

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

The ensuing table for Rmon MIB Counters settings are informational only: etherStats-DropEvents, etherStatsOctets, etherStatsPkts, etherStatsBroadcastPkts, etherStatsMulti-castPkts, 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.

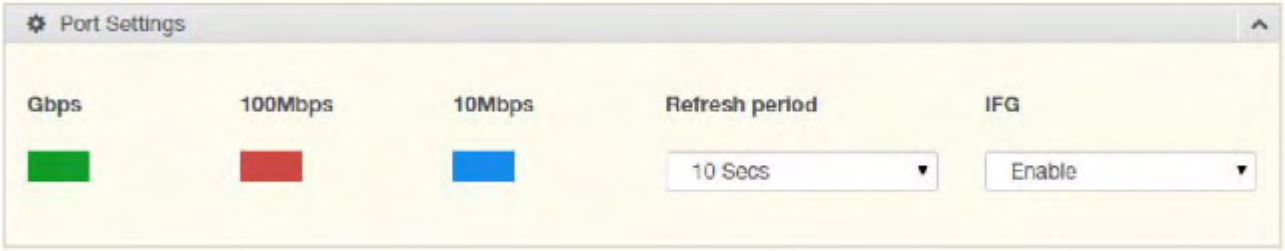


Figure 4-6. Monitoring > Port Monitoring > Port Utilization

Table 4-4. Monitoring > Port Monitoring > 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.

4.3.4 Link Aggregation

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

To access this page, click Monitoring > Link Aggregation.

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

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

4.3.5 LLDP Statistics

The LLDP Statistics page displays the LLDP statistics.

To access this page, click Monitoring > LLDP Statistics.

Figure 4-7. Monitoring > LLDP Statistics

Table 4-5. Monitoring > LLDP Statistics

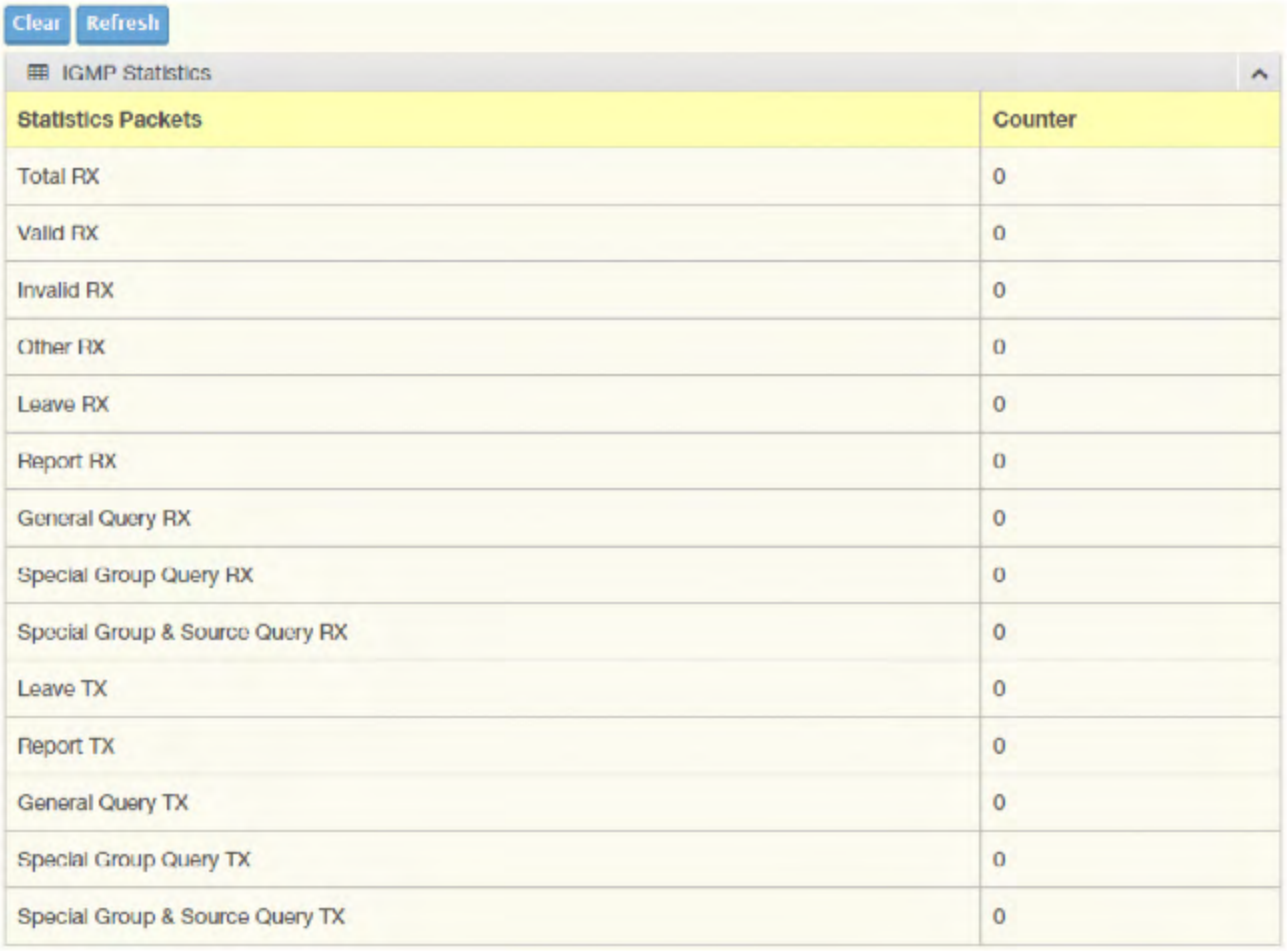
Item	Description
Clear	Click Clear to reset LLDP Statistics of all the interfaces.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

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

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

4.3.6 IGMP Statistics

The IGMP Statistics function displays statistical package information for IP multicasting. 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 4-8. Monitoring > IGMP Statistics

Table 4-6. Monitoring > 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 ensuing table for IGMP Statistics settings 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.

4.4. System

4.4.1 IP Settings

The IP Settings menu allows you to select a static or DHCP network configuration. The Static displays the configurable settings for the static option.

To access this page, click System > IP Settings.

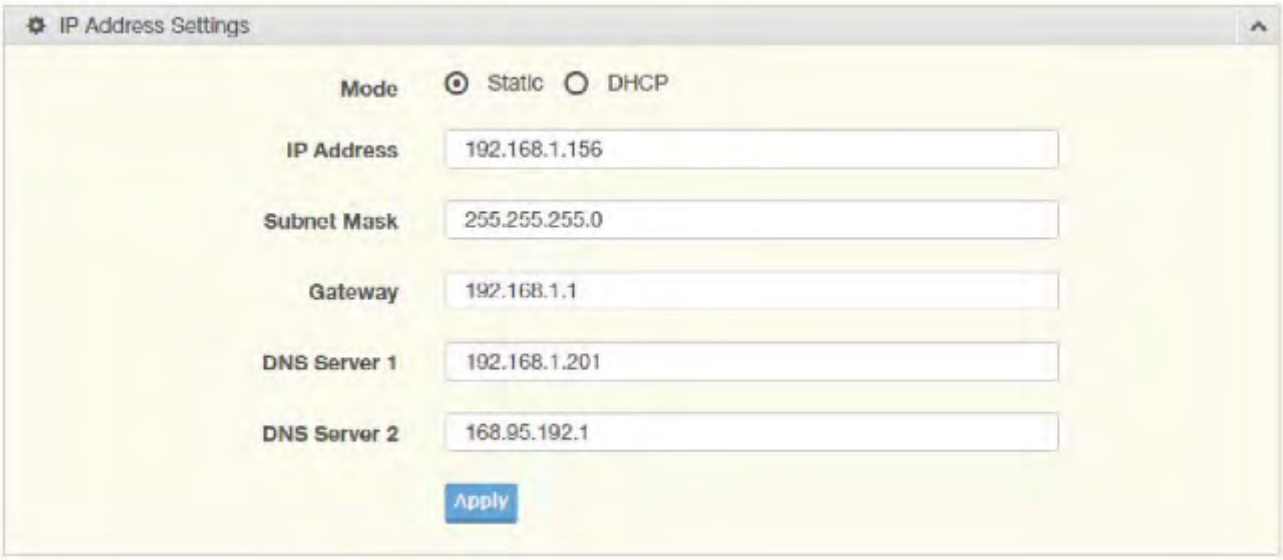


Figure 4-9. System > IP Settings

Table 4-7. System > IP Settings

Item	Description
Mode	Click the radio button to select the IP Address Setting mode: Static or DHCP.
IP Address	Enter a value to specify the IP address of the interface. The default is 192.168.10.1.
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.
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 ensuing table for IP Address Information settings are informational only: DHCP State, Static IP Address, Static Subnet Mask, Static Gateway, Static DNS Server 1 and Static DNS Server 2.

4.4.2 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.

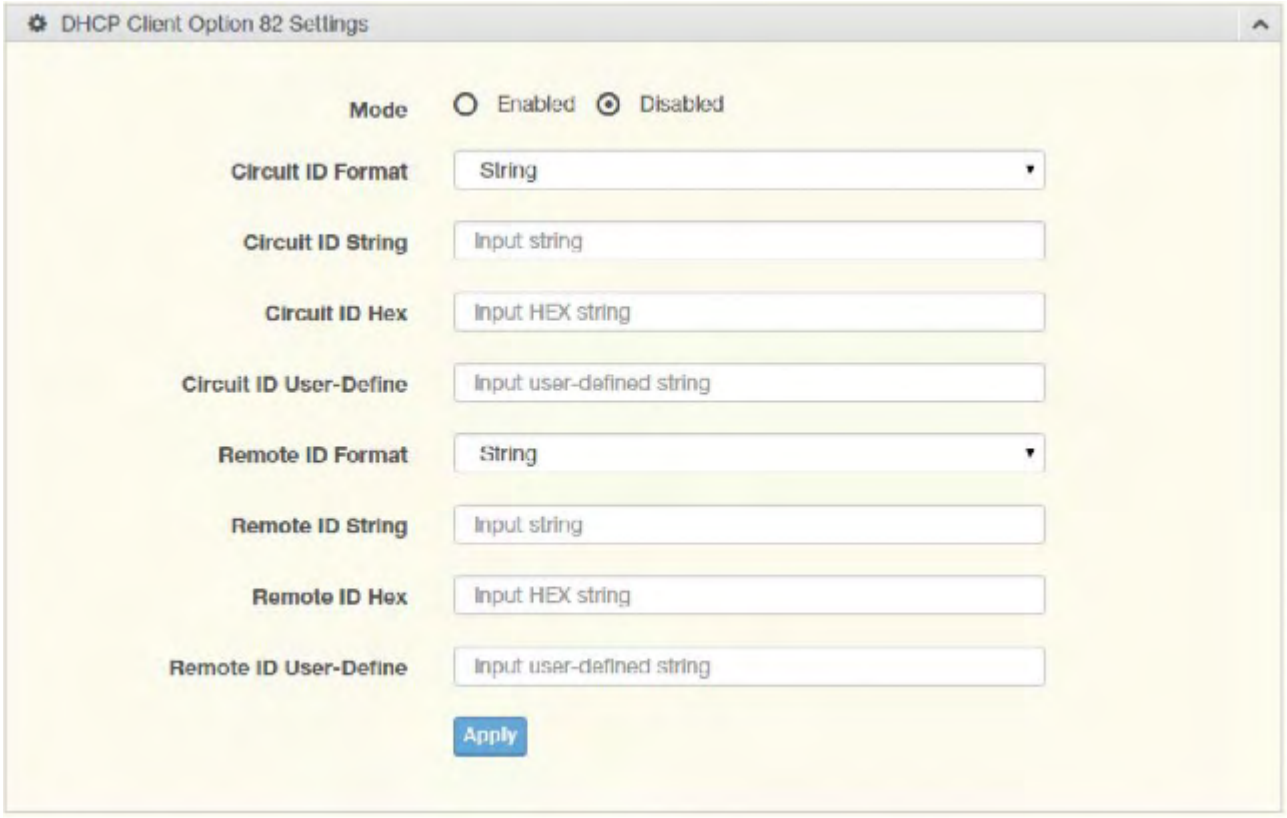


Figure 4-10. System > DHCP Client Option 82

Table 4-8. System > 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 ensuing table for DHCP Client Option 82 Information table settings are informational only: Status, Circuit ID Format, Circuit ID String, Circuit ID Hex, Circuit ID User-Define, Remote ID Format, Remote ID String, Remote ID Hex and Remote ID User-Define.

4.4.3 DHCP Auto Provision

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

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

Figure 4-11. System > DHCP Auto Provision

Table 4-9. System > 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 ensuing table for DHCP Auto Provision Information settings are informational only: Status

4.4.4 IPv6 Settings

To access this page, click System > IPv6 Settings.

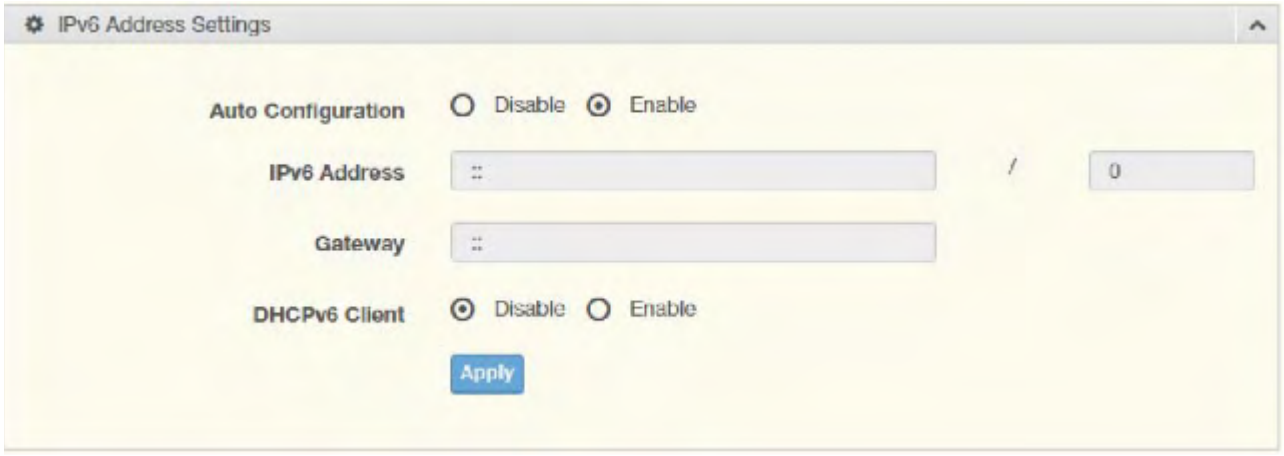


Figure 4-12. System > IPv6 Settings

Table 4-10. System > 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 ensuing table for IPv6 Information settings are informational only: Auto Configuration, IPv6 In Use Address, IPv6 In Use Router, IPv6 Static Address, IPv6 Static Router and DHCPv6 Client.

4.4.5 Management VLAN

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

To access this page, click System > Management VLAN.

Figure 4-13. System > Management VLAN

Table 4-11. System > 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 ensuing table for Management VLAN State are informational only: Management VLAN.

4.4.6 System Time

To access this page, click System > System Time.

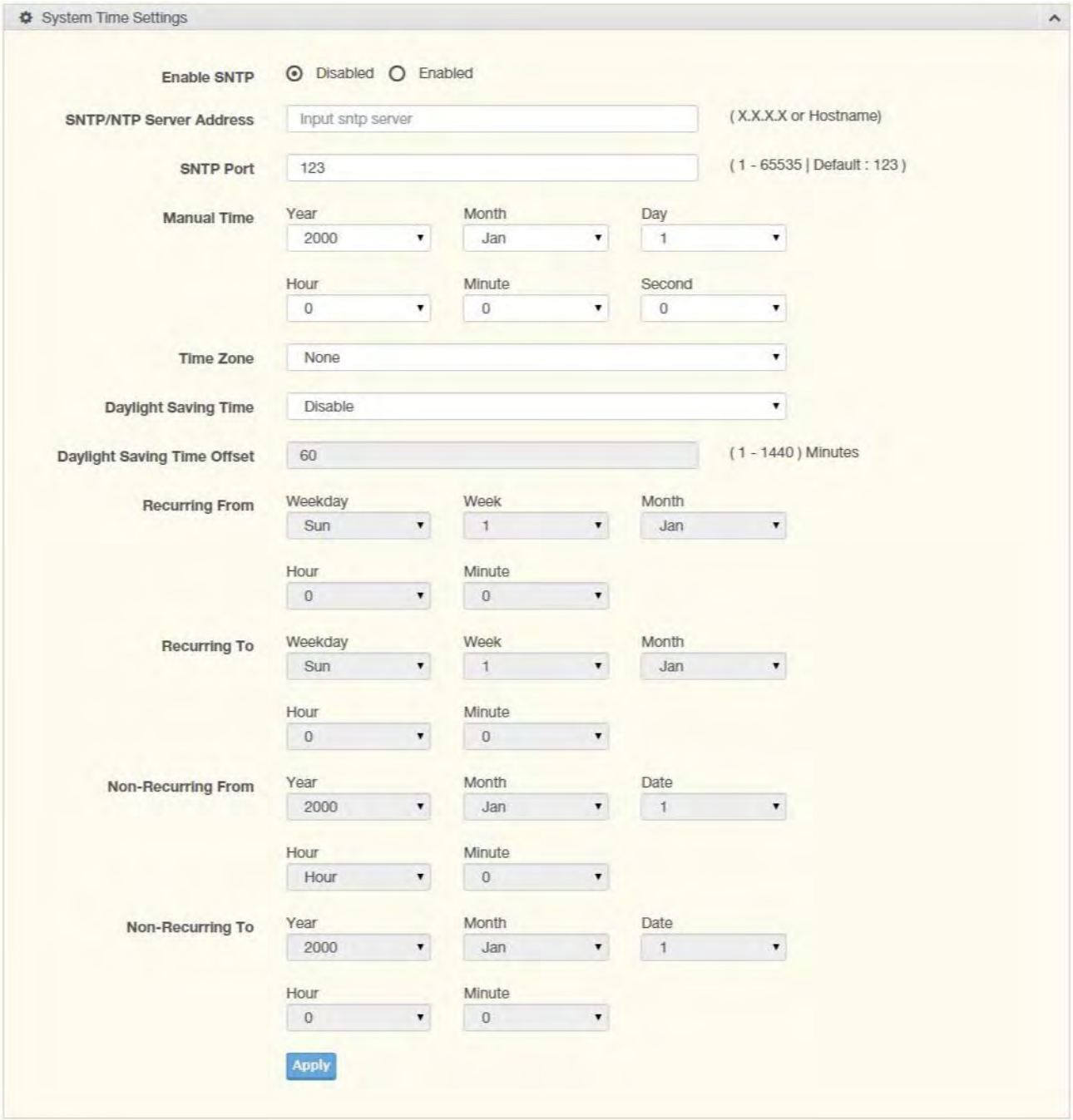


Figure 4-14. System > System Time

Table 4-12. System > System Time

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

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

4.5. L2 Switching

4.5.1 Port Configuration

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

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

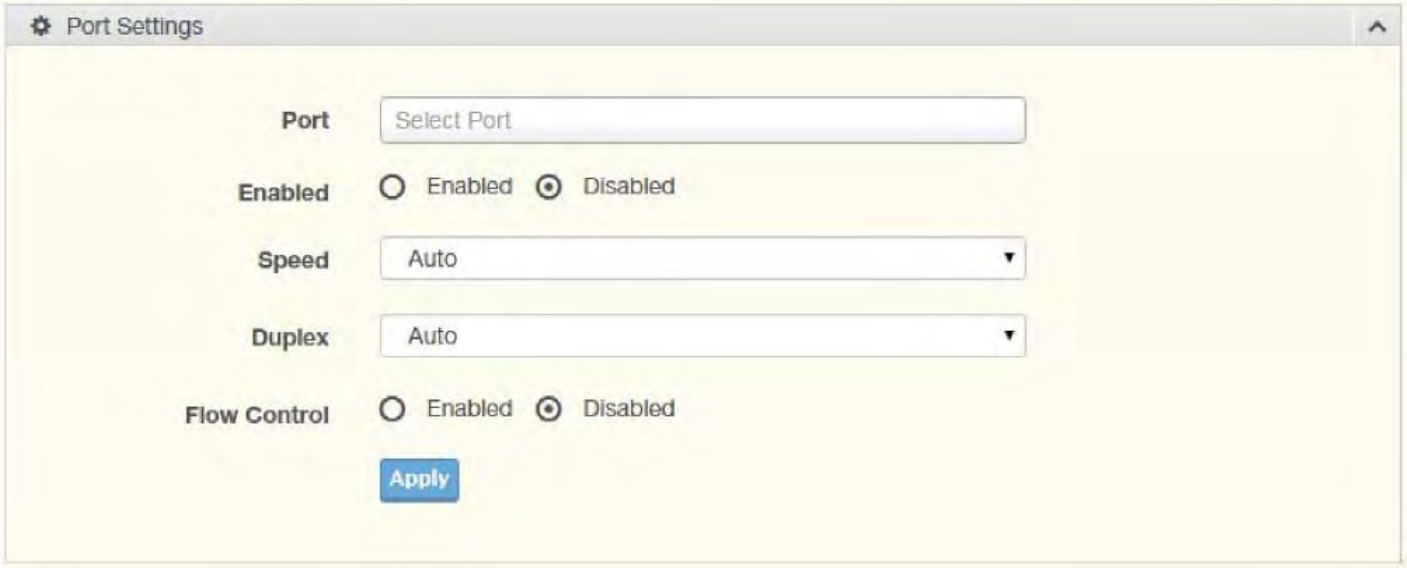


Figure 4-15. L2 Switching > Port Configuration

Table 4-13. 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: 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 ensuing table for Port Status settings are informational only: Port, Edit (click to enter description), Enable State, Link Status, Speed, Duplex, FlowCtrl Config and FlowCtrl Status.

4.5.2 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.

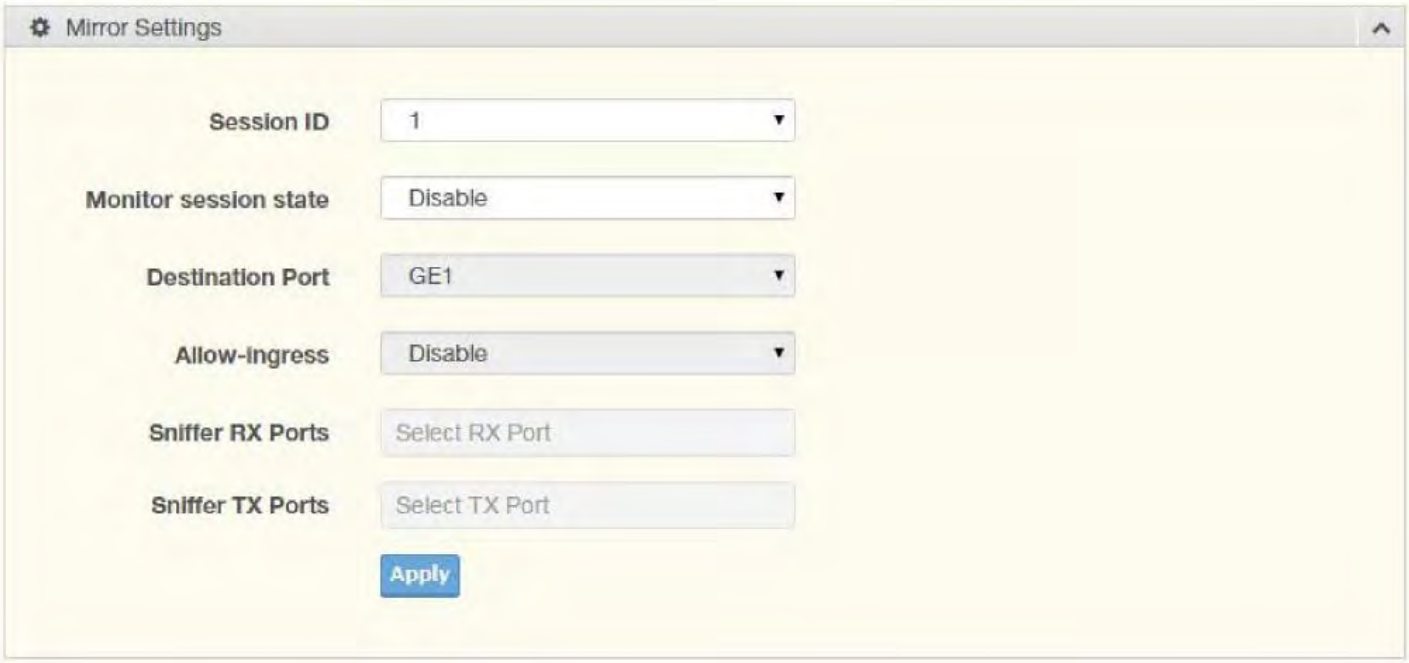


Figure 4-16. L2 Switching > Port Mirror

Table 4-14. L2 Switching > 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 ensuing table for Mirror Status settings are informational only: Session ID, Destination Port, Ingress State, Source TX Port and Source RX Port.

4.5.3 Link Aggregation

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

Load Balance

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

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

Figure 4-17. L2 Switching > Link Aggregation > Load Balance

Table 4-15. L2 Switching > Link Aggregation > Load Balance

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

The ensuing table for Load Balance Information settings 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.

Figure 4-18. L2 Switching > Link Aggregation > LAG Management

Table 4-16. L2 Switching > Link Aggregation > 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: FE1-8 or GE1-2.
Apply	Click Apply to save the values and update the screen.

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

LAG Port Settings

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

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

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

Figure 4-19. L2 Switching > Link Aggregation > LAG Port Settings

Table 4-17. L2 Switching > Link Aggregation > 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 ensuing table for LAG Port Status settings are informational only: LAG, Description, Port Type, Enable State, Link Status, Speed, Duplex, FlowCtrl Config and FlowCtrl Status.

LACP Priority Settings

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

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

Figure 4-20. L2 Switching > Link Aggregation > LACP Priority Settings

Table 4-18. L2 Switching > Link Aggregation > 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 ensuing table for LACP Information settings 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.

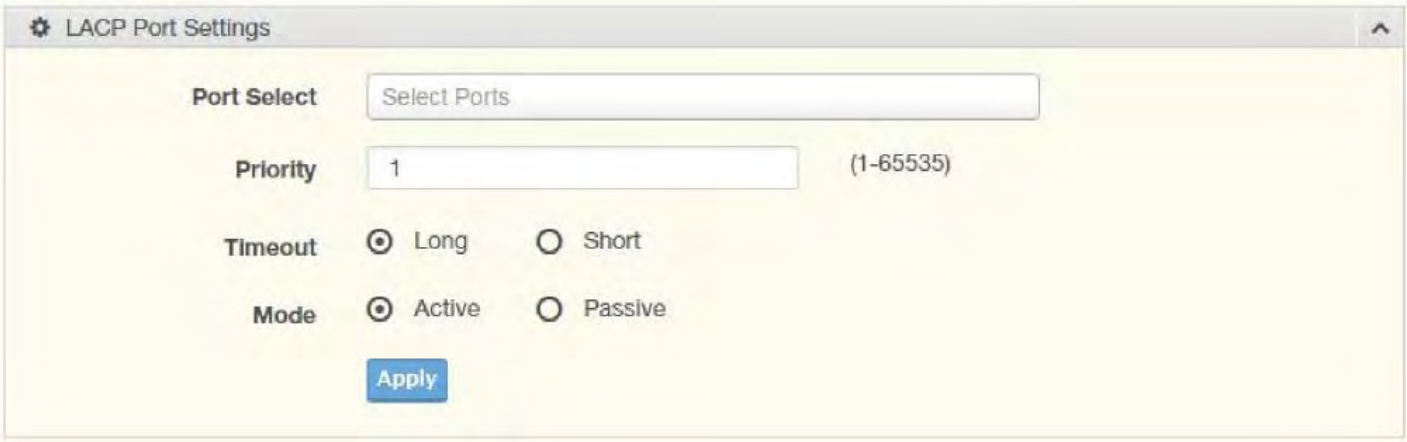


Figure 4-21. L2 Switching > Link Aggregation > LACP Port Settings

Table 4-19. L2 Switching > Link Aggregation > LACP Port Settings

Item	Description
Port Select	Select a port for the LACP Port Settings. The listed available settings are: FE1-FE8, GE1-GE2. 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 ensuing table for LACP Port Information settings are informational only: Port Name, Priority, Timeout and Mode.

4.5.4 802.1Q 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.

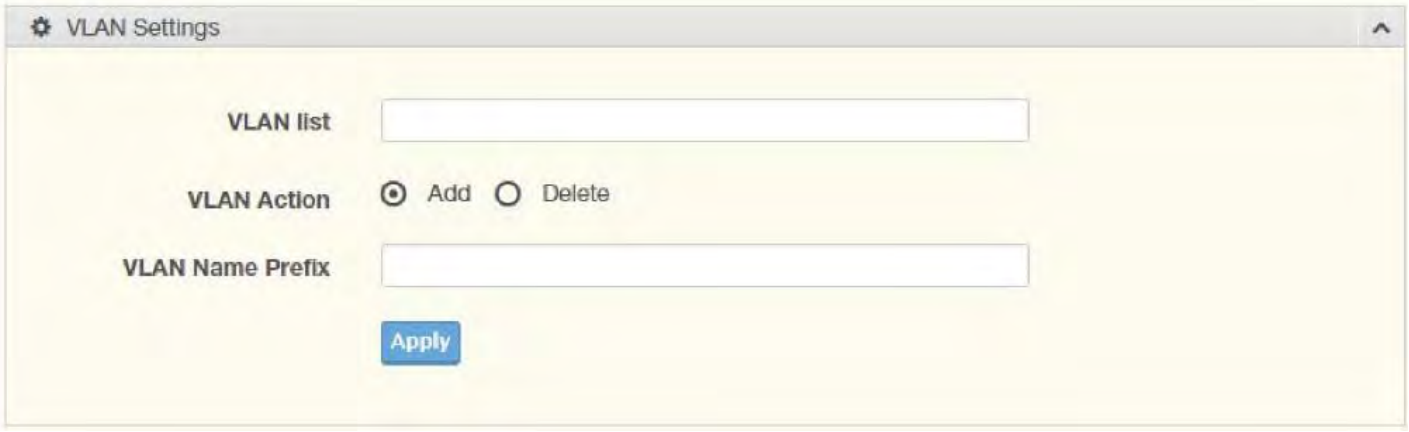


Figure 4-22. L2 Switching > 802.1Q VLAN > VLAN Management

Table 4-20. L2 Switching > 802.1Q VLAN > VLAN Management

Item	Description
VLAN list	Enter the name of the VLAN entry to setup.
VLAN Action	Click the radio button to add or delete the VLAN entry shown in the previous field.
VLAN Name 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 ensuing table for VLAN Table settings 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.

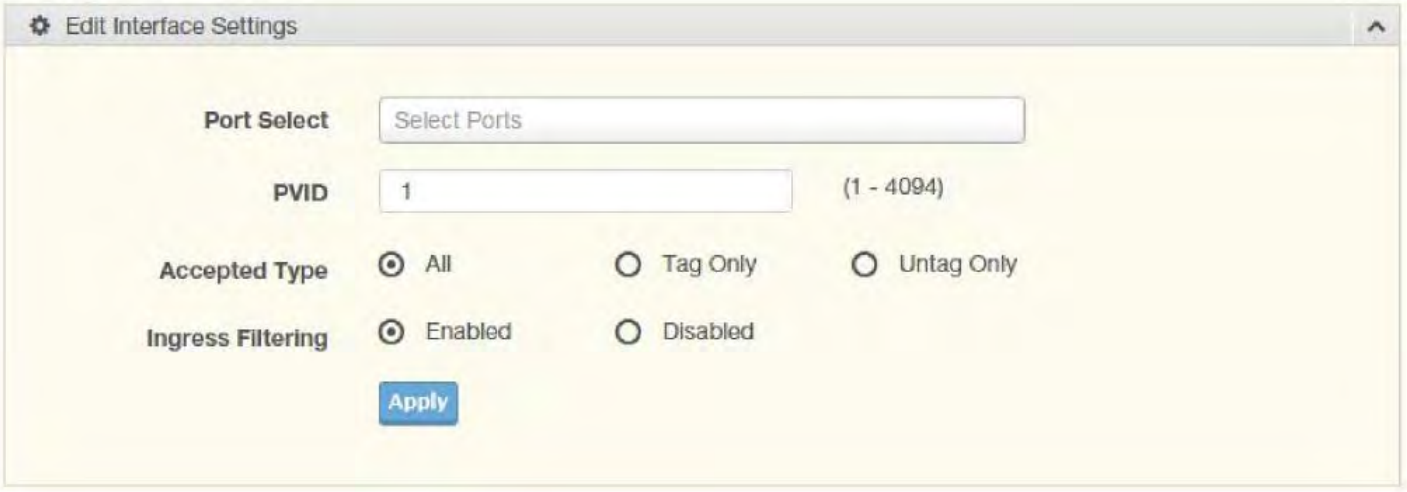


Figure 4-23. L2 Switching > 802.1Q VLAN > PVID Settings

Table 4-21. L2 Switching > 802.1Q VLAN > 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 ensuing table for Port VLAN Status settings 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

Apply

Figure 4-24. L2 Switching > 802.1Q VLAN > Port to VLAN

Table 4-22. L2 Switching > 802.1Q VLAN > 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

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

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

4.5.5 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.

Figure 4-25. L2 Switching > Q-in-Q > Global Settings

Table 4-23. L2 Switching > 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 ensuing table for QinQ Global Information settings 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.

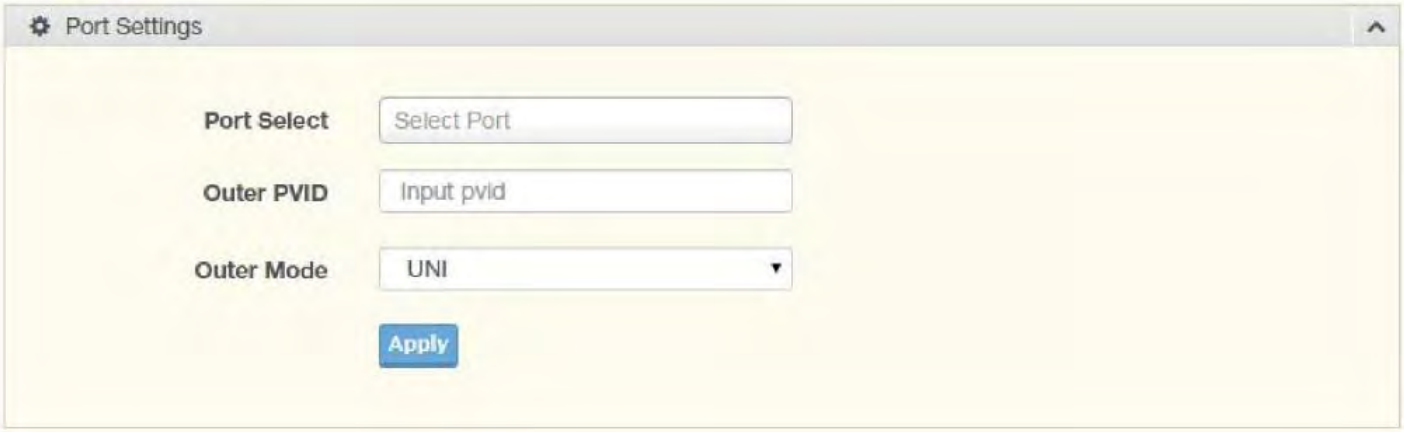


Figure 4-26. L2 Switching > Q-in-Q > Port Settings

Table 4-24. L2 Switching > 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 ensuing table for QinQ Port Information settings are informational only: Port, Outer PVID and Outer Mode.

4.5.6 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.

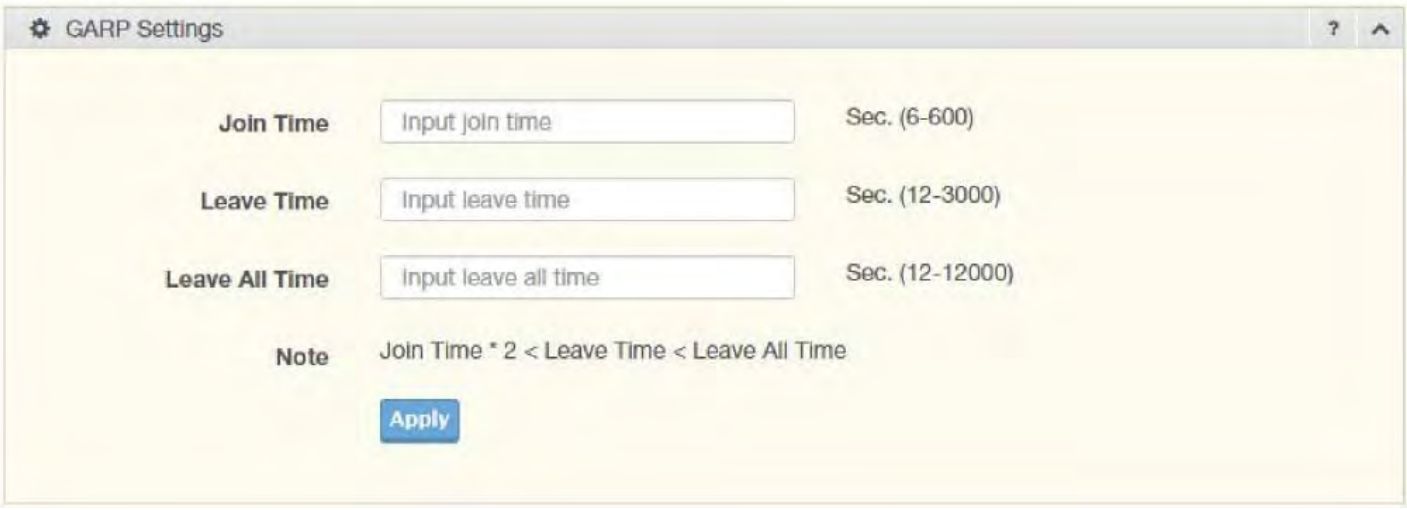


Figure 4-27. L2 Switching > GARP > GARP Settings

Table 4-25. L2 Switching > GARP > 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 ensuing table for GARP Information settings 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.

Figure 4-28. L2 Switching > GARP > GVRP Settings

Table 4-26. L2 Switching > GARP > 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 ensuing table for GVRP Information settings are informational only: GVRP.

4.5.7 802.3az EEE

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

» Traffic detection – Energy Efficient Ethernet (EEE) compliance

» Inactive link detection

Inactive link detection function automatically reduces power usage when inactive links or devices are detected.

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

Figure 4-29. L2 Switching > 802.3az EEE

Table 4-27. L2 Switching > 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 ensuing table for EEE Enable Status settings are informational only: Port and EEE State.

4.5.8 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.

Figure 4-30. L2 Switching > Multicast > Multicast Filtering

Table 4-28. L2 Switching > Multicast > 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 ensuing table for Properties Information settings 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.

Figure 4-31. L2 Switching > Multicast > IGMP Snooping > IGMP Settings

Table 4-29. L2 Switching > Multicast > IGMP Snooping > 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 ensuing table for IGMP Snooping Information settings are informational only: IGMP Snooping State, IGMP Snooping Version and IGMP Snooping V2 Report Suppression.

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

IGMP Querier

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

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

Figure 4-32. L2 Switching > Multicast > IGMP Snooping > IGMP Querier

Table 4-30. L2 Switching > Multicast > IGMP Snooping > 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 ensuing table for IGMP Querier Status settings 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.

Figure 4-33. L2 Switching > Multicast > IGMP Snooping > IGMP Static Groups

Table 4-31. L2 Switching > Multicast > IGMP Snooping > 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 ensuing table for IGMP Static Groups Status settings 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 ensuing table for Multicast Groups settings 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 ensuing table for Router Ports settings are informational only: VLAN ID, Port and Expiry Time (Sec).

MLD Snooping

The MLD Snooping page allows you to select the snooping status (enable or disable), the version (v1 or v2) and the enabling/disabling of the report suppression for the MLD querier, which sends out periodic general MLD queries and are forwarded through all ports in the VLAN.

MLD Settings

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

Figure 4-34. L2 Switching > Multicast > MLD Snooping > MLD Settings

Table 4-32. L2 Switching > Multicast > MLD Snooping > 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 ensuing table for MLD Snooping Information settings are informational only: MLD Snooping State, MLD Snooping Version and MLD Snooping V2 Report Suppression.

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

MLD Querier

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

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

Figure 4-35. L2 Switching > Multicast > MLD Snooping > MLD Querier

Table 4-33. L2 Switching > Multicast > MLD Snooping > 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 ensuing table for MLD Querier Status settings are informational only: VLAN ID, Querier State, Querier Status, Querier Version and Querier IP.

MLD Static Group

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

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

Figure 4-36. L2 Switching > Multicast > MLD Snooping > MLD Static Group

Table 4-34. L2 Switching > Multicast > MLD Snooping > 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 ensuing table for MLD Static Groups Status settings 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.

The ensuing table for Multicast Groups settings 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.

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

4.5.9 Jumbo Frame

Jumbo frames are frames larger than the standard Ethernet frame size of 1518 bytes. The Jumbo Frame function allows the configuration of Ethernet frame size.

To access this page, click L2 Switching > Jumbo Frame.

Figure 4-37. L2 Switching > Jumbo Frame

Table 4-35. L2 Switching > 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 ensuing table for Jumbo Frame Config settings are informational only: Jumbo Frame (Bytes).

4.5.10 Spanning Tree

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

STP Global Settings

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

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

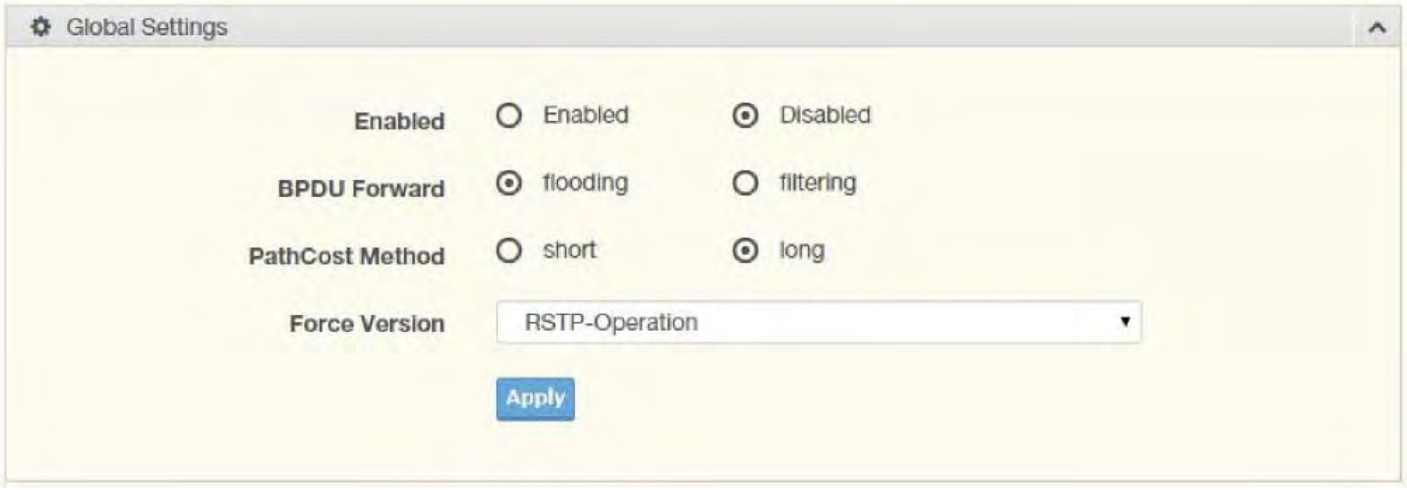


Figure 4-38. L2 Switching > Spanning Tree > STP Global Settings

Table 4-36. L2 Switching > Spanning Tree > 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.
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 ensuing table for STP Information settings are informational only: STP, BPDU Forward, 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.

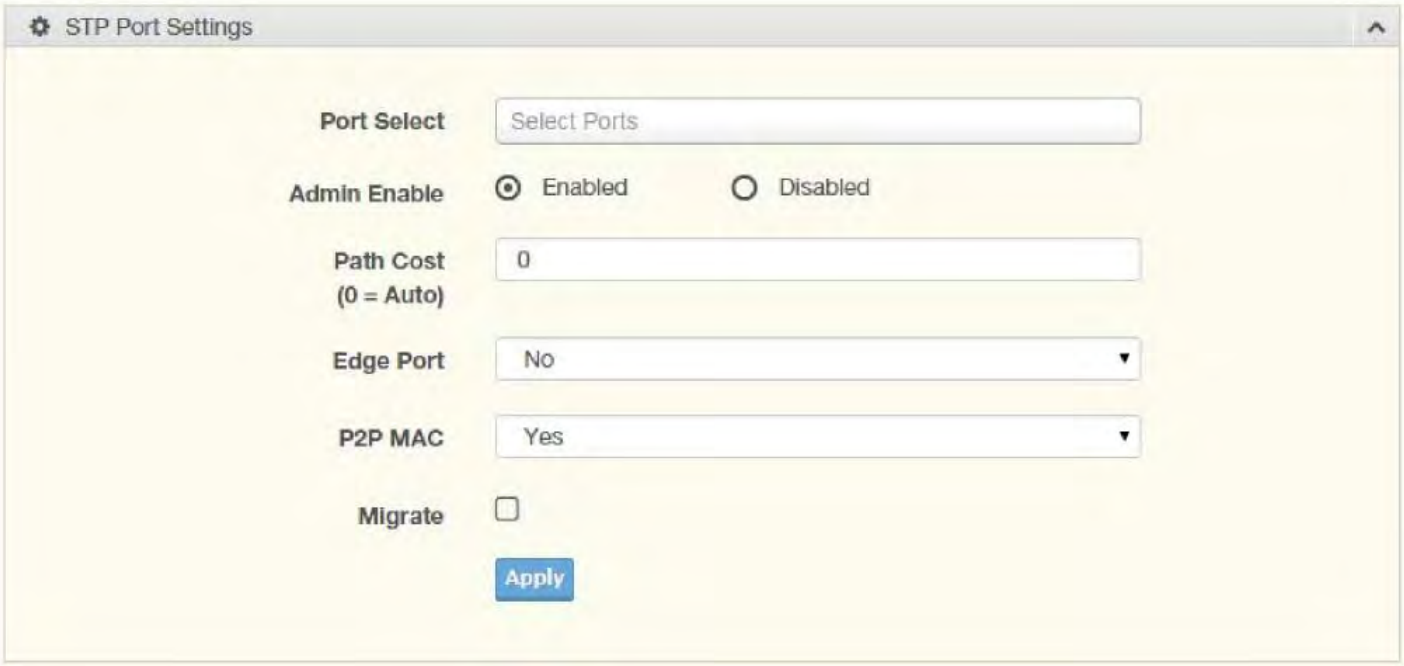


Figure 4-39. L2 Switching > Spanning Tree > STP Port Settings

Table 4-37. L2 Switching > Spanning Tree > STP Port Settings

Item	Description
Port Select	Select the port list to specify the ports that apply to this setting.
Admin Enable	Select Enabled or Disabled to setup the admin profile for the STP port.
Path Cost (0 = Auto)	Set the port's cost contribution. For a root port, the root path cost for the bridge. (0 means Auto).
Edge Port	Click the drop-down menu to set the edge port configuration. 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 ensuing table for STP Port Status settings are informational only: Port, Admin 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.

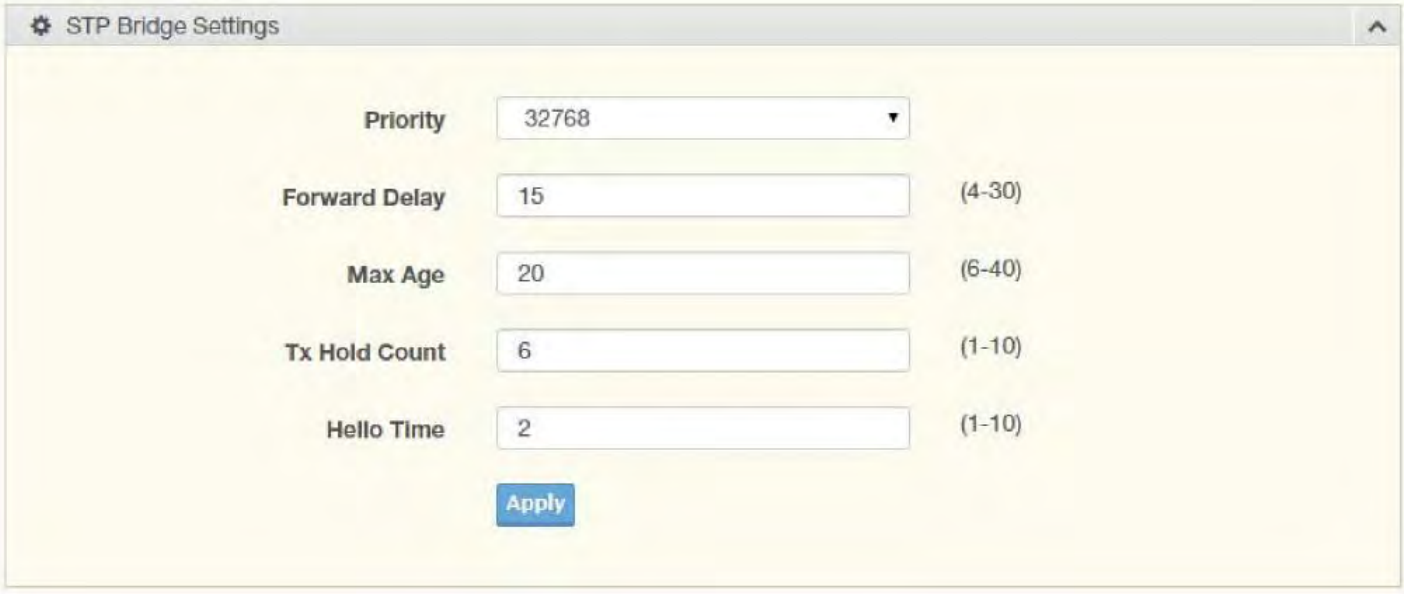


Figure 4-40. L2 Switching > Spanning Tree > STP Bridge Settings

Table 4-38. L2 Switching > Spanning Tree > 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 ensuing table for STP Bridge Information settings are informational only: Priority, Forward Delay, Max Age, Tx Hold Count and Hello Time.

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

STP 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.

Figure 4-41. L2 Switching > Spanning Tree > STP Port Advanced Settings

Table 4-39. L2 Switching > Spanning Tree > 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 ensuing table for STP Port Status settings are informational only: Port, Identifier (Priority / Port Id), Path Cost Conf/Oper, Designated Root Bridge, Root Path Cost, Designated Bridge, Edge Port Conf/Oper, P2P MAC Conf/Oper, Port Role and Port State.

MST Config Identification

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

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

Figure 4-42. L2 Switching > Spanning Tree > MST Config Identification

Table 4-40. L2 Switching > Spanning Tree > 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 ensuing table for MST Configuration Identification Information settings 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.

Figure 4-43. L2 Switching > Spanning Tree > MST Instance ID Settings

Table 4-41. L2 Switching > Spanning Tree > 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 ensuing table for MST Instance ID Information settings 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.

Figure 4-44. L2 Switching > Spanning Tree > MST Instance Priority Settings

Table 4-42. L2 Switching > Spanning Tree > 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 ensuing table for MST Instance Priority Information settings are informational only: MSTI ID, Priority and Action.

MST Instance Info

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

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

The ensuing table for STP Port Status settings are informational only: Port, Identifier

(Priority / Port Id), Path Cost Conf/Oper, Designated Root Bridge, Root Path Cost, Designated Bridge, Edge Port Conf/Oper, P2P MAC Conf/Oper, Port Role and Port State.

STP Statistics

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

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

4.5.11 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.

Figure 4-45. L2 Switching > X-Ring Elite > X-Ring Elite Settings

Table 4-43. L2 Switching > X-Ring Elite > 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 ensuing table for Information settings 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.

Figure 4-46. L2 Switching > X-Ring Elite > X-Ring Elite Groups

Table 4-44. L2 Switching > X-Ring Elite > 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 ensuing table for Information settings are informational only: Ring ID, Role, Port 1, Port 2 and Delete (click to delete the desired Ring ID).

4.5.12 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.

Figure 4-47. L2 Switching > X-Ring Pro > X-Ring Pro Settings

Table 4-45. L2 Switching > X-Ring Pro > 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 ensuing table for Information settings 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.

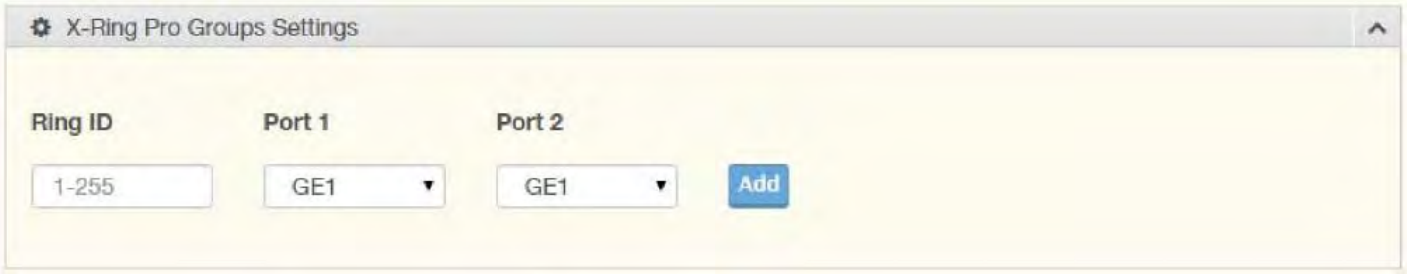


Figure 4-48. L2 Switching > X-Ring Pro > X-Ring Pro Groups > X-Ring Pro Groups Settings

Table 4-46. L2 Switching > X-Ring Pro > X-Ring Pro Groups > 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.

Figure 4-49. L2 Switching > X-Ring Pro > X-Ring Pro Groups > Couple Setting

Table 4-47. L2 Switching > X-Ring Pro > X-Ring Pro Groups > Couple Setting

Item	Description
Couple Ring ID	Enter a number to specifies a ranging from 1 to 255 to identify a given XRing 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 ensuing table for Information settings 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).

4.5.13 Loopback Detection

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

Global Settings

The Global Settings page allows you to configure the state (enabled or disabled) of the function, select the interval at which frames are transmitted and the delay before recovery.

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

Figure 4-50. L2 Switching > Loopback Detection > Global Settings

Table 4-48. L2 Switching > 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 ensuing table for Loopback Detection Global Information settings 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 4-51. L2 Switching > Loopback Detection > Port Settings

Table 4-49. L2 Switching > 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 ensuing table for Loopback Detection Port Information settings are informational only: Port, Enable State and Loop Status.

4.6. MAC Address Table

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

4.6.1 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.

Figure 4-52. MAC Address Table > Static MAC

Table 4-50. MAC Address Table > Static MAC

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

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

4.6.2 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.

Figure 4-53. MAC Address Table > MAC Aging Time

Table 4-51. MAC Address Table > 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 ensuing table for Dynamic Address Status settings are informational only: Aging time.

4.6.3 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.

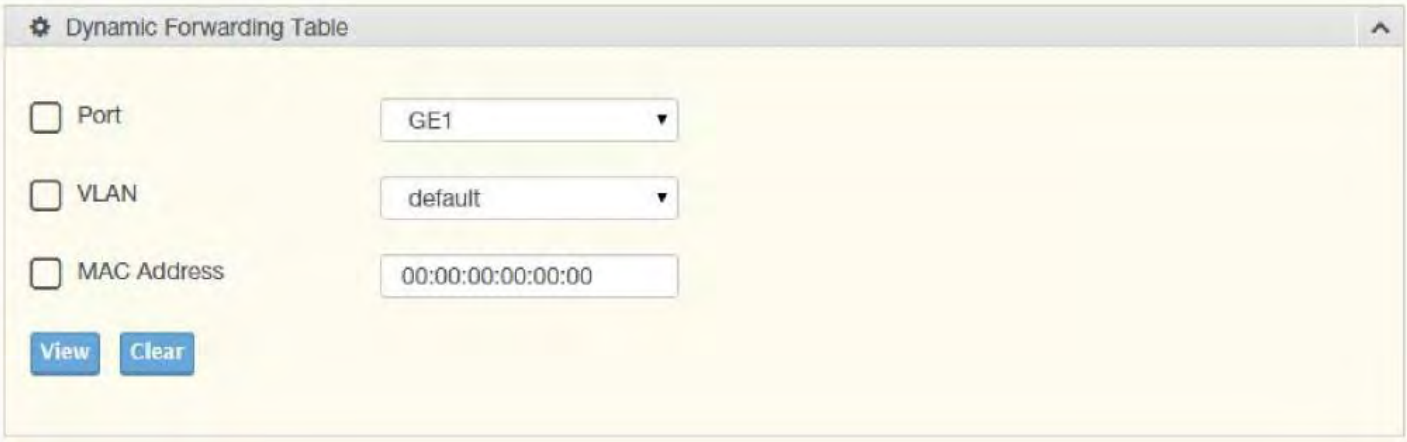


Figure 4-54. MAC Address Table > Dynamic Forwarding Table

Table 4-52. MAC Address Table > 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 ensuing table for MAC Address Information settings are informational only: MAC Address, VLAN, Type, Port and Add to Static MAC (click to add the MAC address to static MAC address list).

4.7. Security

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

4.7.1 Storm Control

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

Global Settings

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

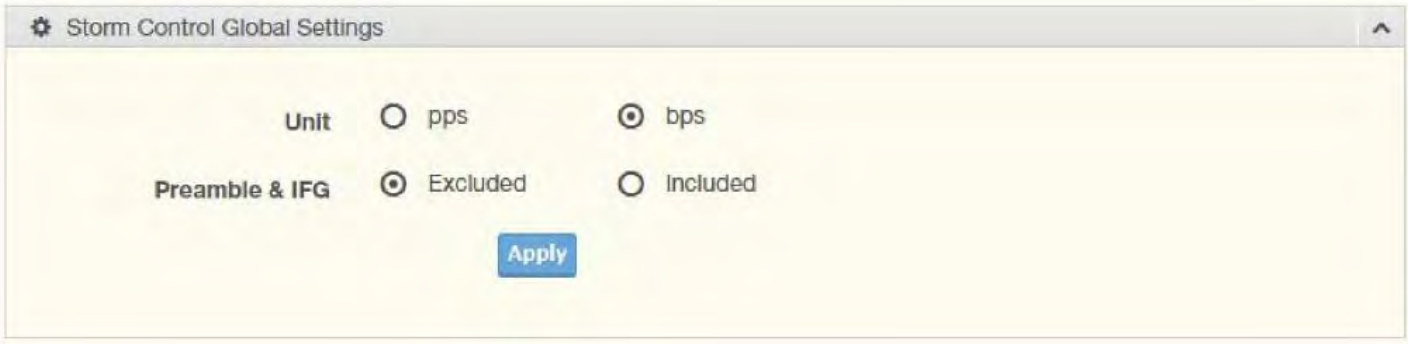


Figure 4-55. Security > Storm Control > Global Settings

Table 4-53. Security > 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.

Port Settings

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

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

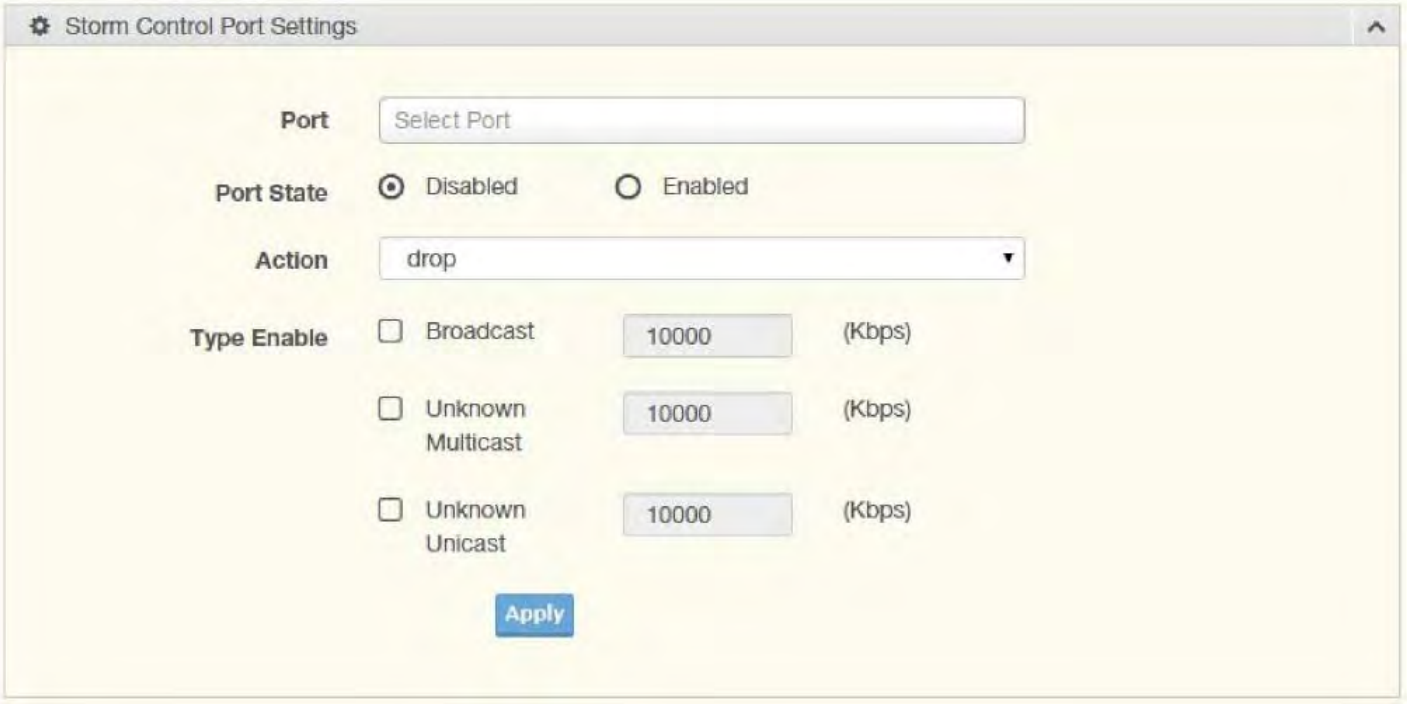


Figure 4-56. Security > Storm Control > Port Settings

Table 4-54. Security > 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 ensuing table for Storm Control Port Information settings are informational only: Port, Port State, Broadcast (Kbps), Unknown Multicast (Kbps), Unknown Unicast (Kbps) and Action.

4.7.2 Port Security

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

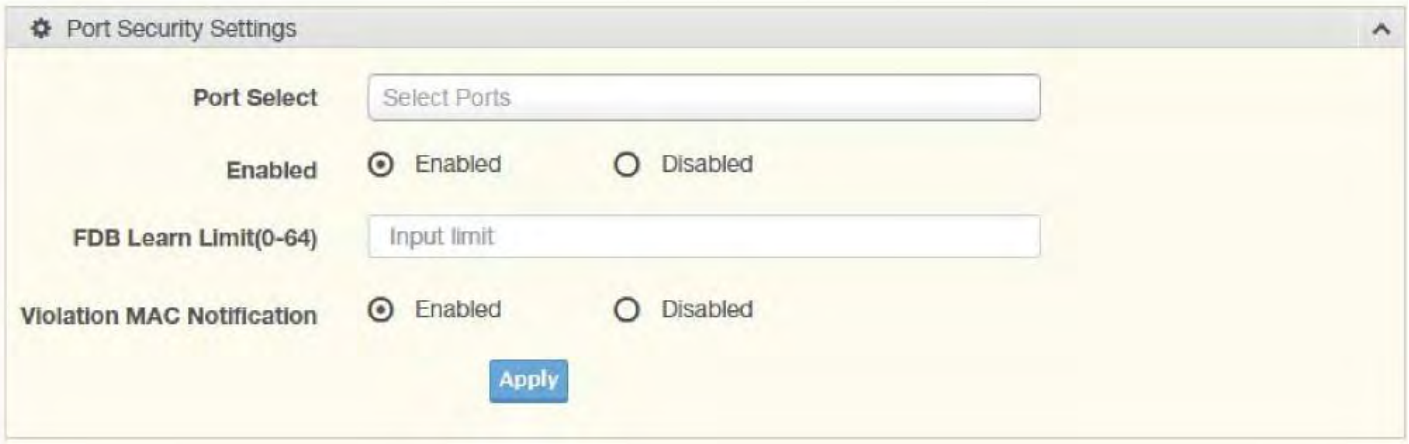


Figure 4-57. Security > Port Security

Table 4-55. Security > 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 ensuing table for Port Security Information settings are informational only: Port, Enabled, FDB Learn Limit and Violation MAC Notification.

4.7.3 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 4-58. Security > Protected Ports

Table 4-56. Security > 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 ensuing table for Protected Ports Status settings are informational only: Protected Ports and Unprotected Ports.

4.7.4 DoS Prevention

DoS Global Settings

The DoS Global Settings page allows you to enabled or disable the setting for each function.

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

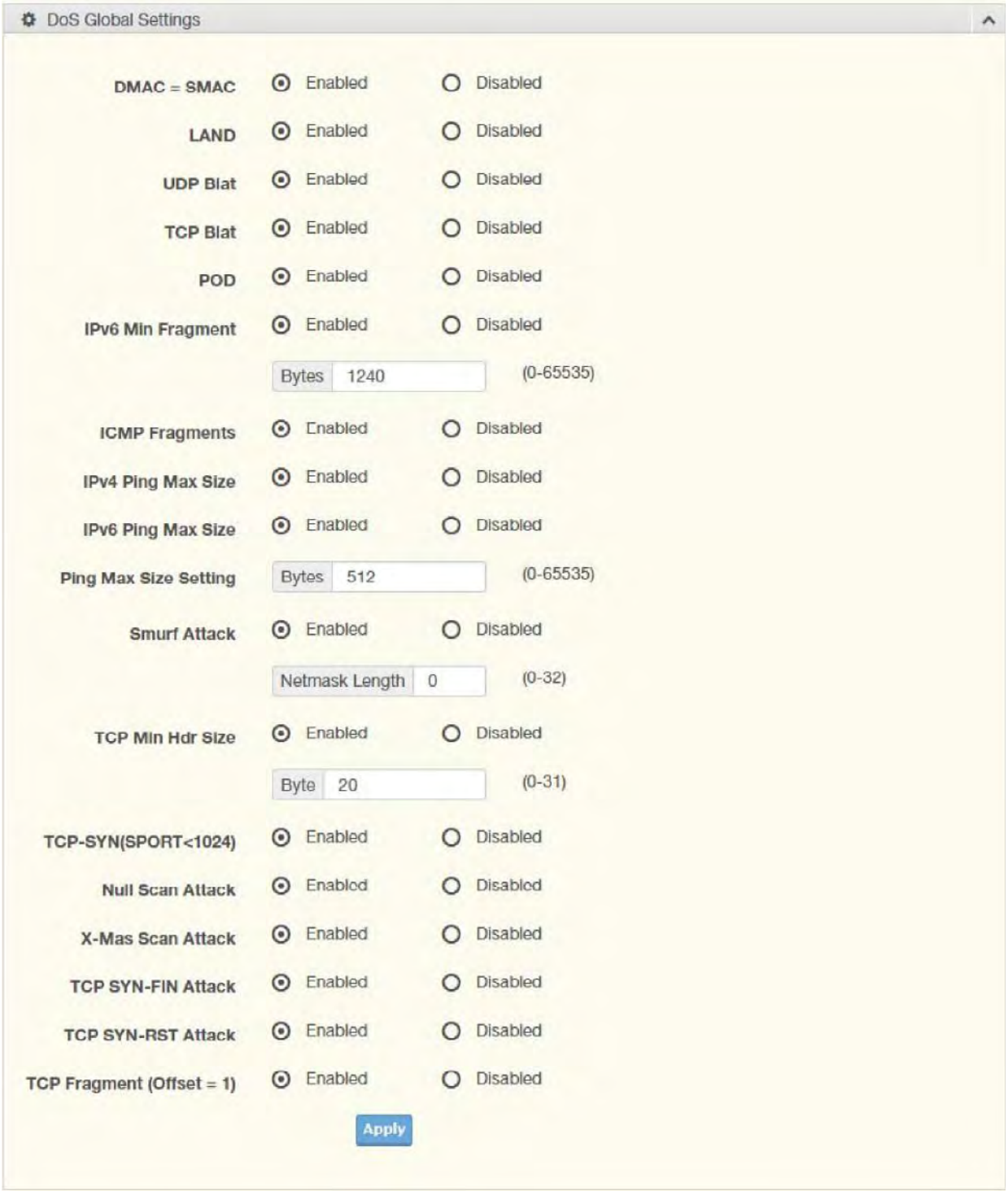


Figure 4-59. Security > DoS Prevention > DoS Global Settings

Table 4-57. Security > DoS Prevention > 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 ensuing table for DoS Global Information settings are informational only: DMAC = SMAC, Land Attack, UDP Blat, TCP Blat, POD (Ping of Death), IPv6 Min Fragment Size, ICMP Fragment Packets, IPv4 Ping Max Packet Size, IPv6 Ping Max Packet Size, Smurf Attack, TCP Min Header Length, TCP Syn (SPORT < 1024), Null Scan Attack, X-Mas Scan Attack, TCP SYN-FIN Attack, TCP SYN-RST Attack and TCP Fragment (Offset = 1).

DoS Port Settings

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

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

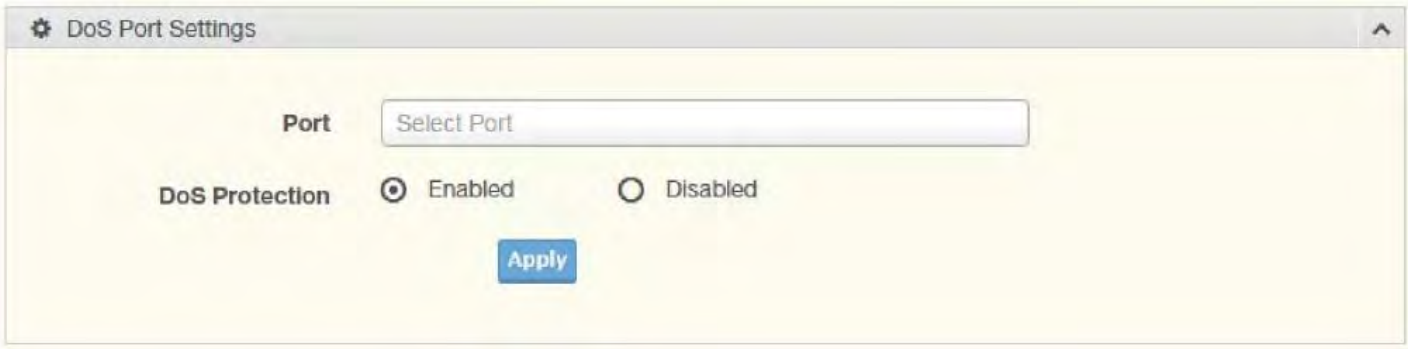


Figure 4-60. Security > DoS Prevention > DoS Port Settings

Table 4-58. Security > DoS Prevention > 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 ensuing table for DoS Port Status settings are informational only: Port and DoS Protection.

4.7.5 Applications

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

TELNET

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

Figure 4-61. Security > Applications > TELNET

Table 4-59. Security > Applications > 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 ensuing table for Telnet Information settings 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.

Figure 4-62. Security > Applications > SSH

Table 4-60. Security > Applications > 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 ensuing table for SSH Information settings 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.

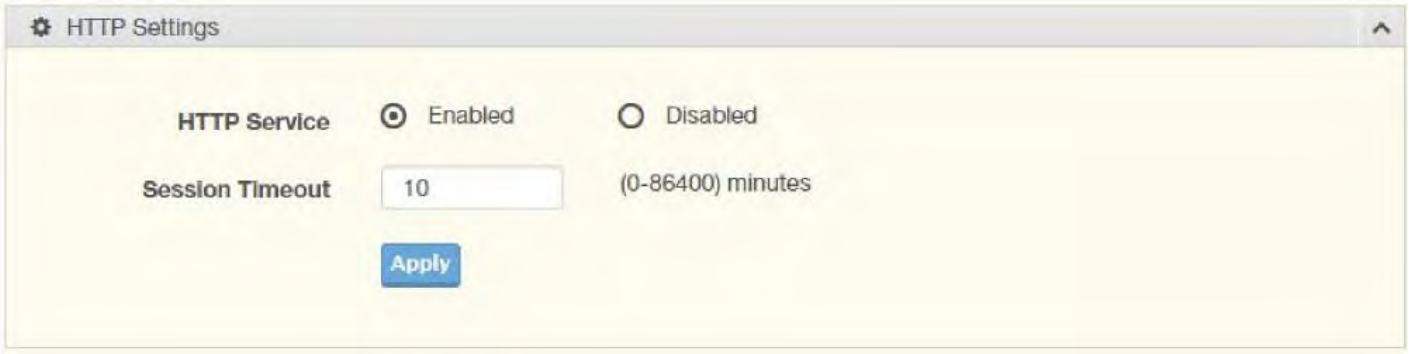


Figure 4-63. Security > Applications > HTTP

Table 4-61. Security > Applications > 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 ensuing table for HTTP Information settings 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.

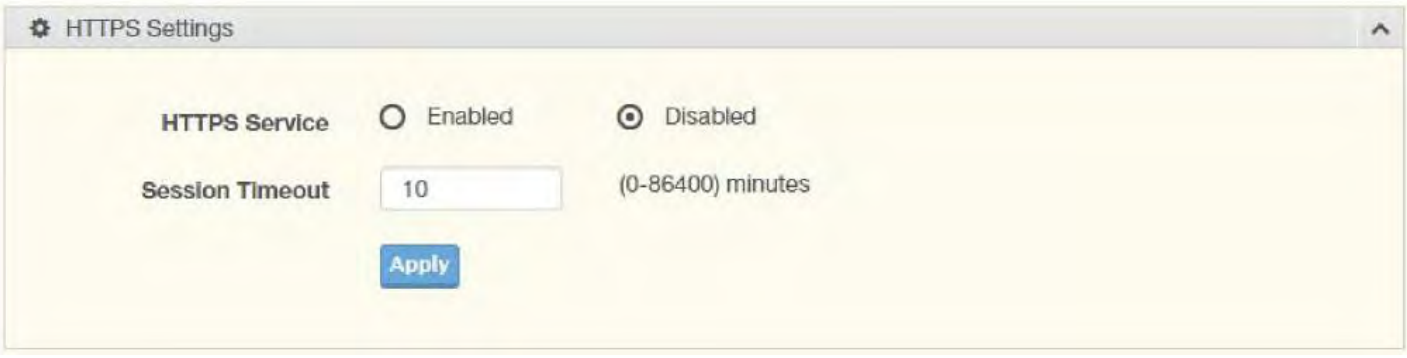


Figure 4-64. Security > Applications > HTTPS

Table 4-62. Security > Applications > 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 ensuing table for HTTPS Information settings are informational only: HTTPS Service and Session Timeout.

4.7.6 802.1x

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

802.1x Settings

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

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

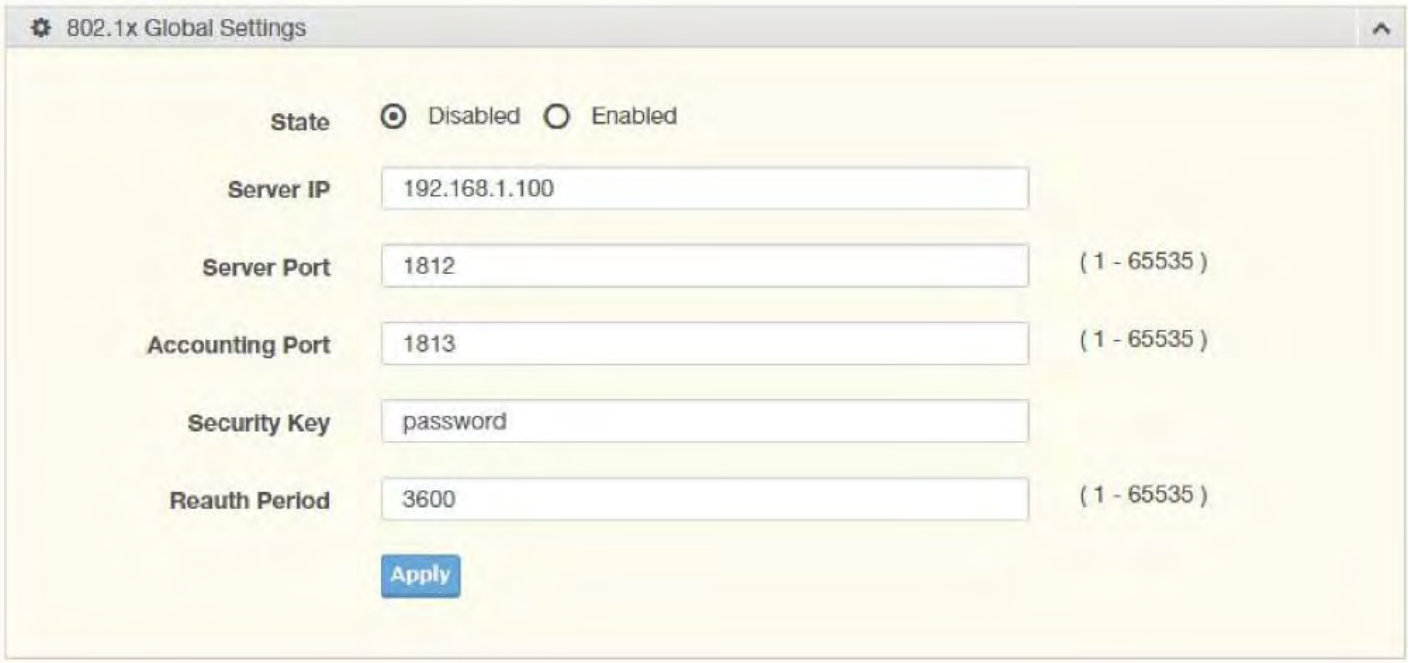


Figure 4-65. Security > 802.1x > 802.1x Settings

Table 4-63. Security > 802.1x > 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.

802.1x Port Configuration

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

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

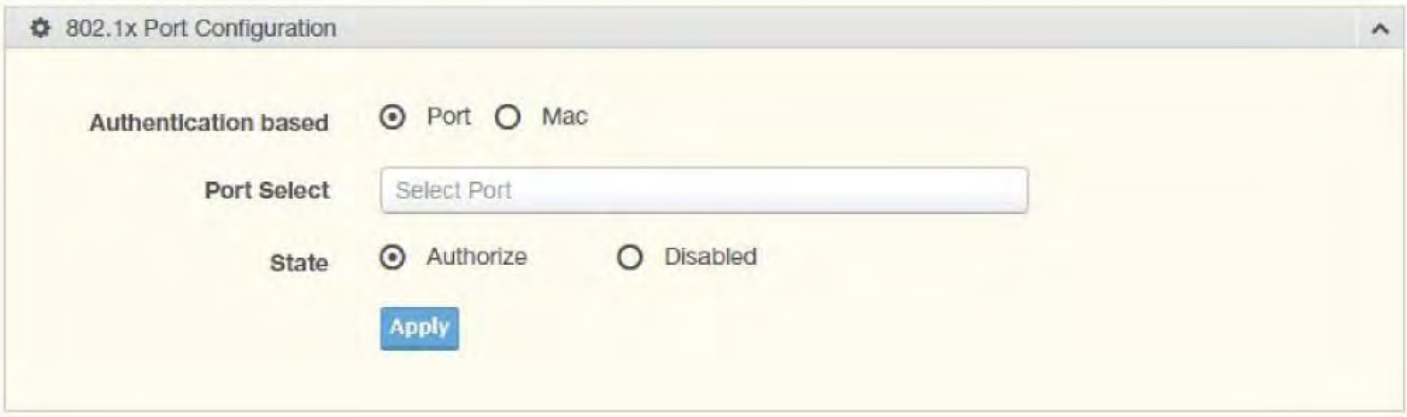


Figure 4-66. Security > 802.1x > 802.1x Port Configuration

Table 4-64. Security > 802.1x > 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 ensuing table for 802.1x Port Authorization settings are informational only: Port and Port State.

4.7.7 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.

Figure 4-67. Security > IP Security > Global Settings

Table 4-65. Security > 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 ensuing table for IP Security Status settings 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.

Figure 4-68. Security > IP Security > Entry Settings

Table 4-66. Security > 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 ensuing table for IP Security Entry Information settings are informational only: IP Address, IP Mask, Services and Action.

4.8. QoS

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

4.8.1 General

Traditionally, networks operate on a best-effort delivery basis, all traffic has equal priority and an equal chance of being delivered in a timely manner. When there is congestion, all traffic has an equal chance of being dropped.

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

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

QoS Properties

The QoS Properties allows you to set the QoS mode.

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

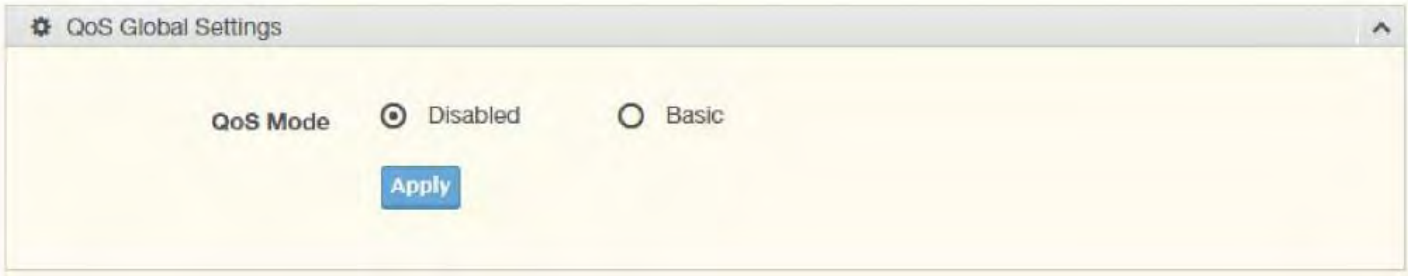


Figure 4-69. QoS > General > QoS Properties

Table 4-67. QoS > General > 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.

QoS Settings

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

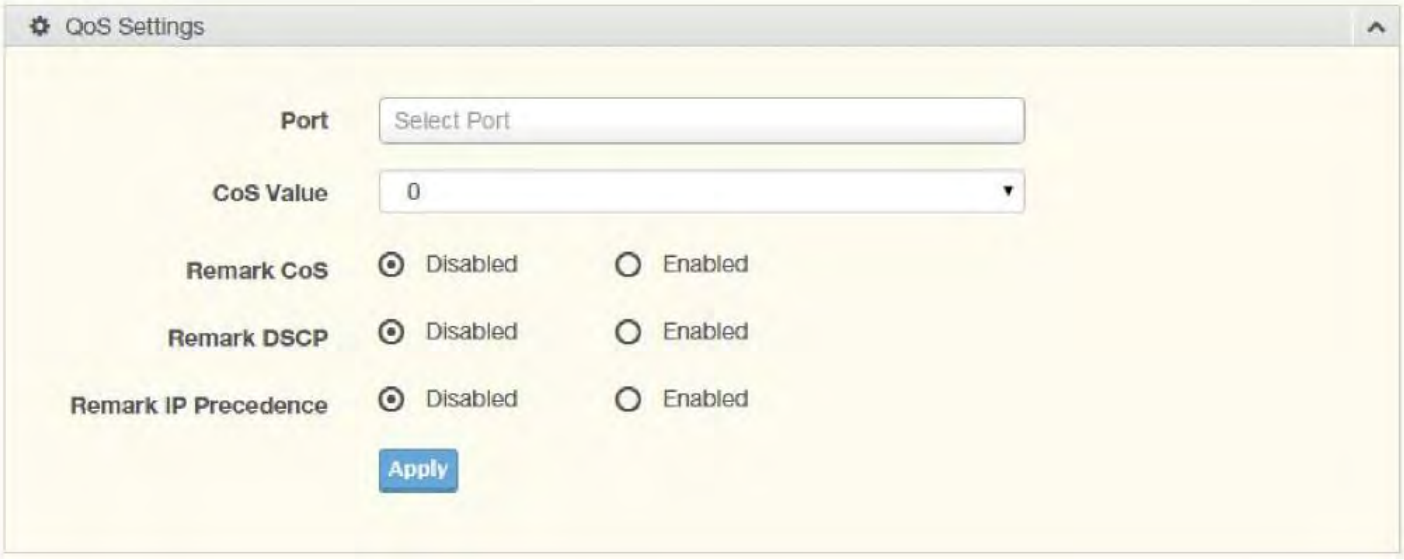


Figure 4-70. QoS > General > QoS Settings

Table 4-68. QoS > General > 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 ensuing table for QoS Status settings are informational only: Port, CoS value, Remark CoS, Remark DSCP and Remark IP Precedence.

Queue 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.

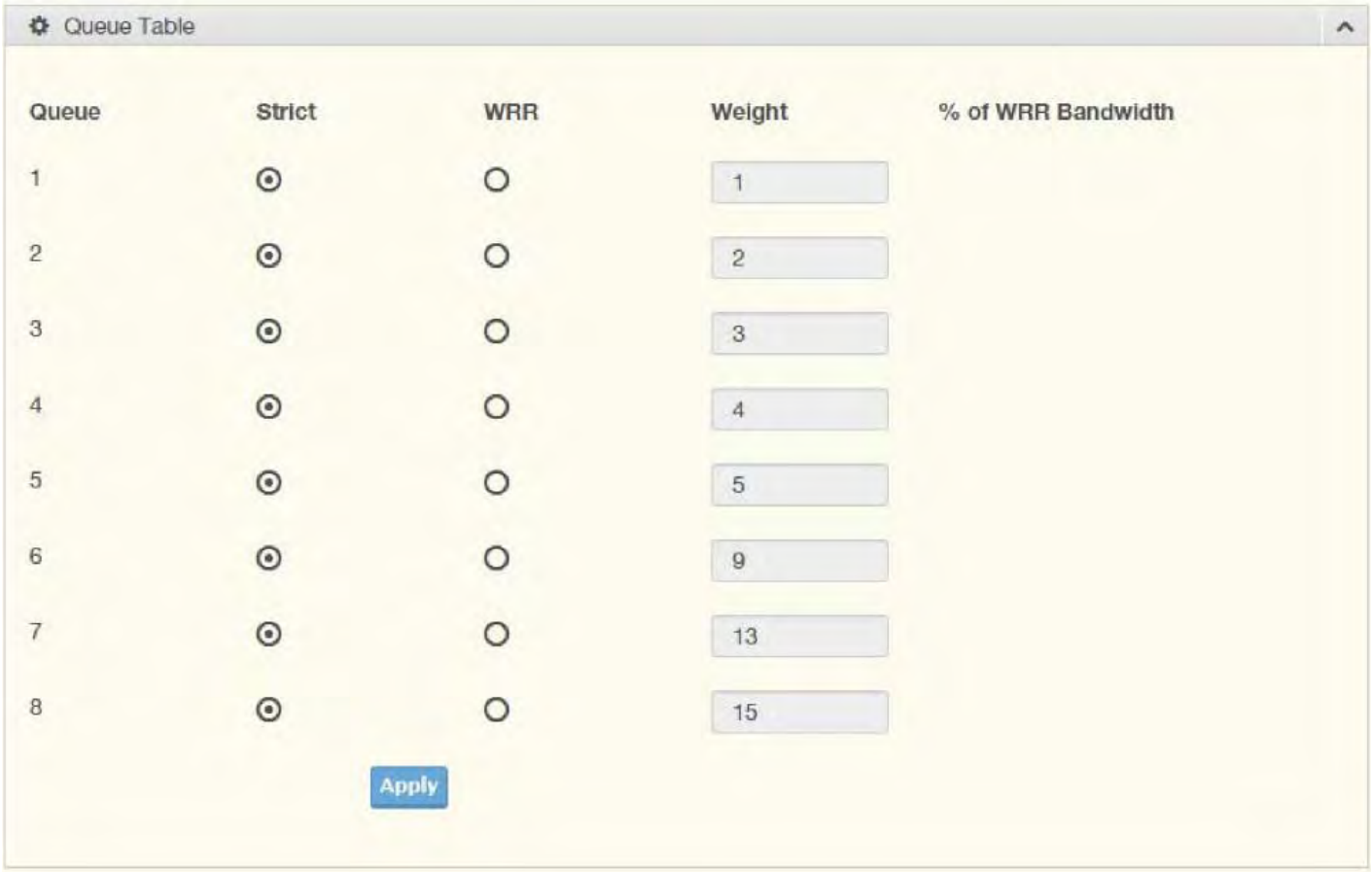


Figure 4-71. QoS > General > QoS Scheduling

Table 4-69. QoS > General > 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 ensuing table for Queue Information settings 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.

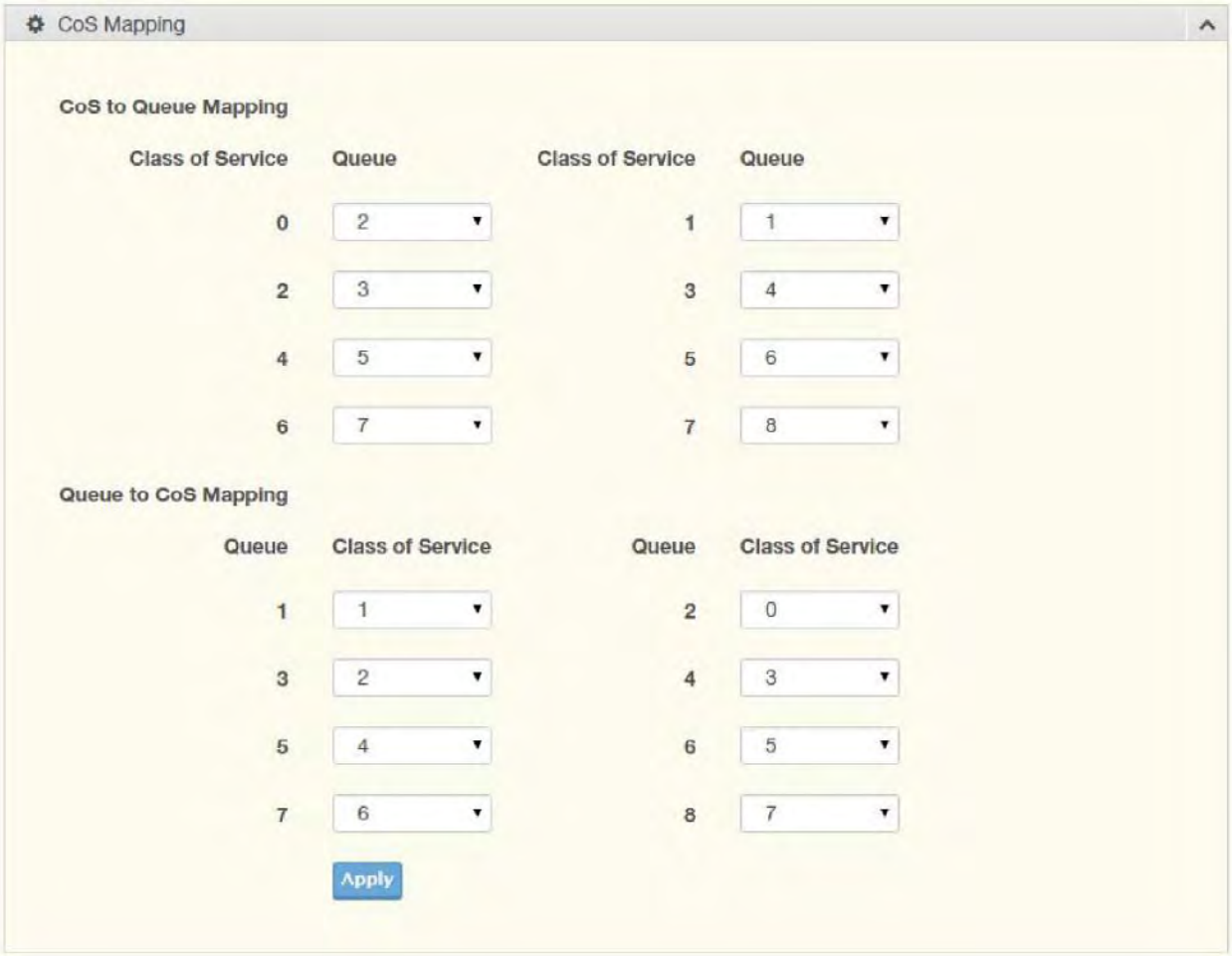


Figure 4-72. QoS > General > CoS Mapping

Table 4-70. QoS > General > 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 ensuing table for CoS Mapping Information settings are informational only: CoS and Mapping to Queue.

The ensuing table for Queue Mapping Information settings 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.

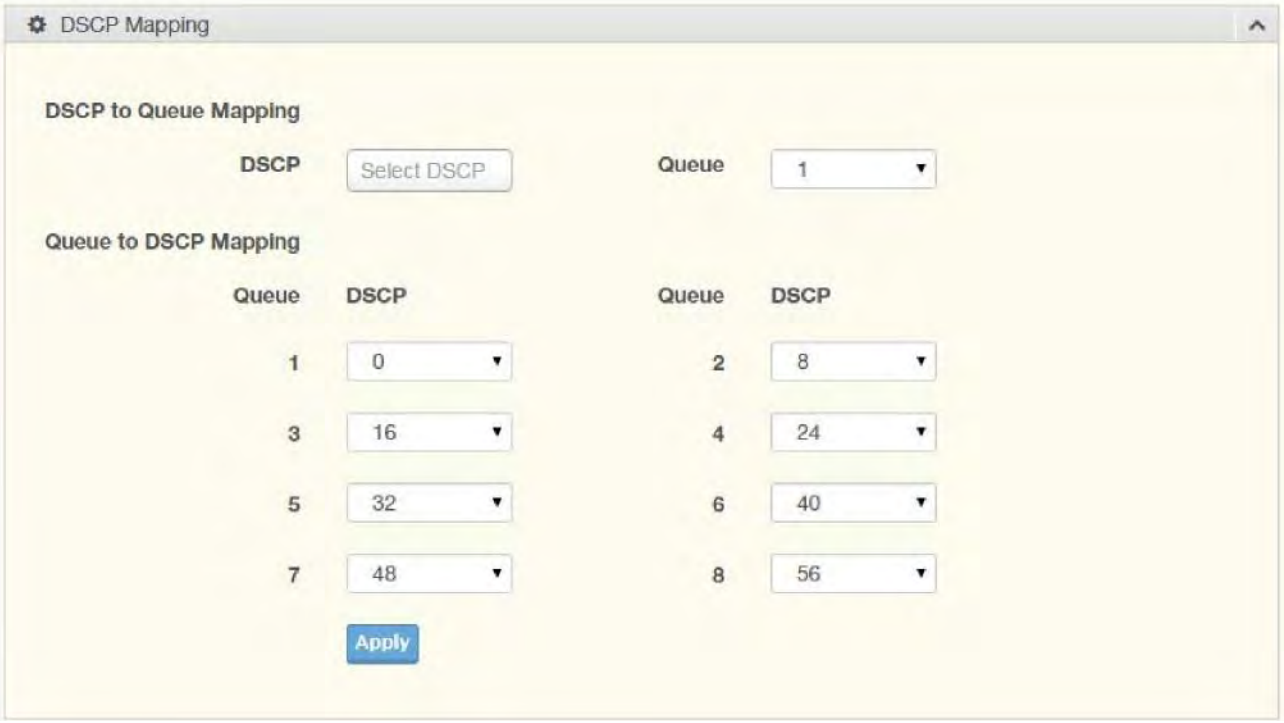


Figure 4-73. QoS > General > DSCP Mapping.

Table 4-71. QoS > General > 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 ensuing table for DSCP Mapping Information settings are informational only: DSCP and Mapping to Queue.

The ensuing table for Queue Mapping Information settings 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.

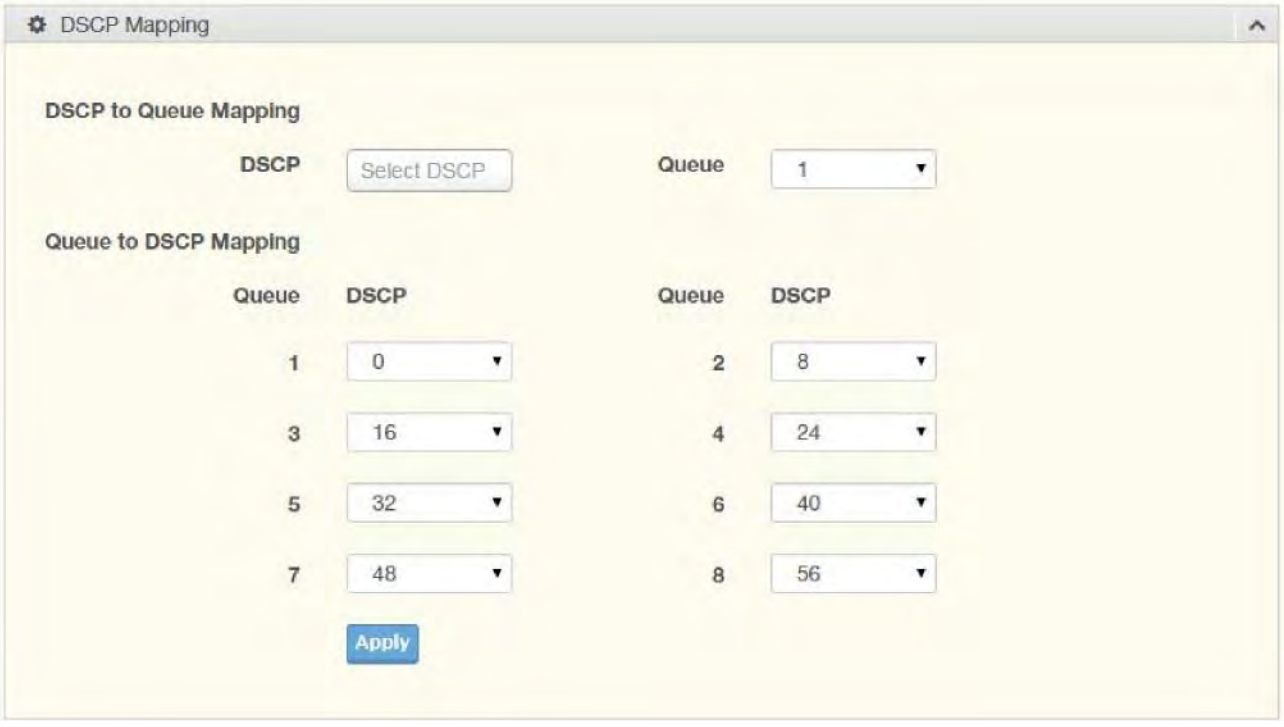


Figure 4-74. QoS > General > IP Precedence Mapping

Table 4-72. QoS > General > 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 ensuing table for IP Precedence Mapping Information settings are informational only: IP Precedence and Mapping to Queue.

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

4.8.2 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.

Figure 4-75. QoS > QoS Basic Mode > Global Settings

Table 4-73. QoS > 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 ensuing table for QoS Information settings 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.

Figure 4-76. QoS > QoS Basic Mode > Port Settings

Table 4-74. QoS > 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 ensuing table for QoS Port Status settings are informational only: Port and Trust State.

4.8.3 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.

Figure 4-77. QoS > Rate Limit > Ingress Bandwidth Control

Table 4-75. QoS > Rate Limit > 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 ensuing table for Ingress Bandwidth Control Status settings 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.

Figure 4-78. QoS > Rate Limit > Egress Bandwidth Control

Table 4-76. QoS > Rate Limit > 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 ensuing table for Egress Bandwidth Control Status settings 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.

Figure 4-79. QoS > Rate Limit > Egress Queue

Table 4-77. QoS > Rate Limit > 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 ensuing table for FE1 Egress Per Queue Status settings are informational only: Queue Id and Egress Rate Limit (Kbps).

4.9. Management

4.9.1 LLDP

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

LLDP System Settings

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

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

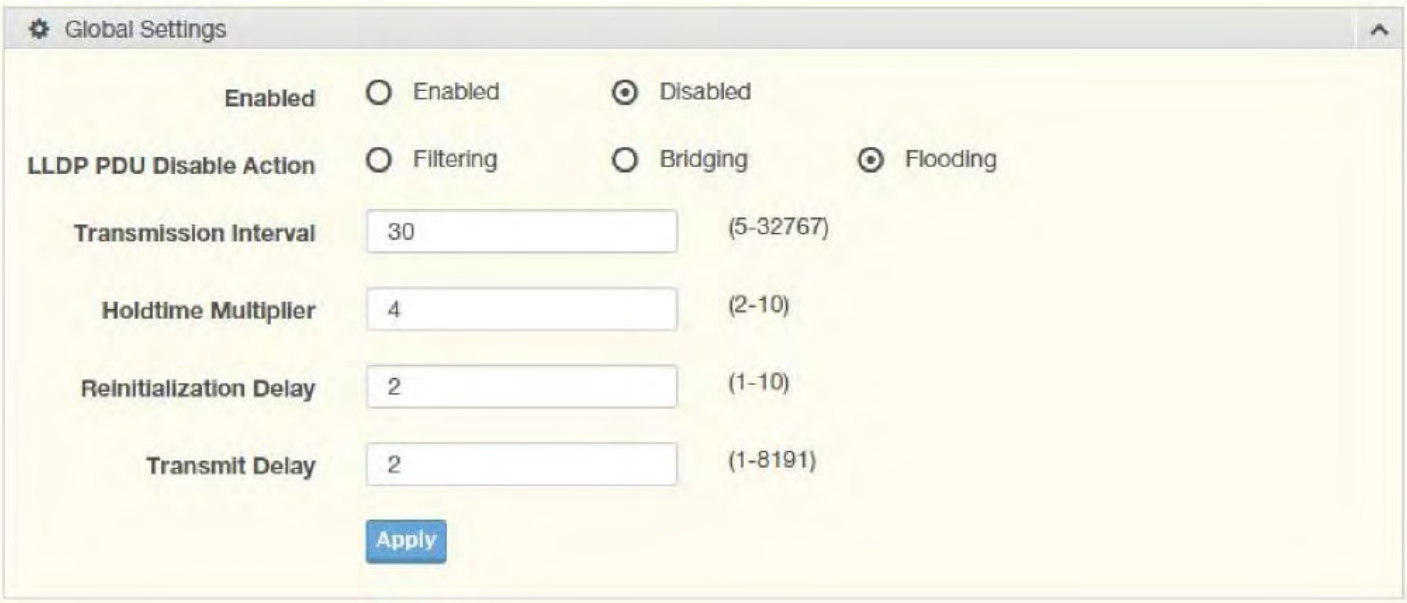


Figure 4-80. Management > LLDP > LLDP System Settings

Table 4-78. Management > LLDP > 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 ensuing table for LLDP Global Config settings are informational only: LLDP Enabled, LLDP PDU Disable Action, Transmission Interval, Holdtime Multiplier, Reinitialization Delay and Transmit Delay.

LLDP Port Settings

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

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

Figure 4-81. Management > LLDP > LLDP Port Settings > LLDP Port Configuration

Table 4-79. Management > LLDP > LLDP Port Settings > 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.

Figure 4-82. Management > LLDP > LLDP Port Settings > Optional TLVs Selection

Table 4-80. Management > LLDP > LLDP Port Settings > 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 ensuing table for LLDP Port Status settings are informational only: Port, State and Selected Optional TLVs.

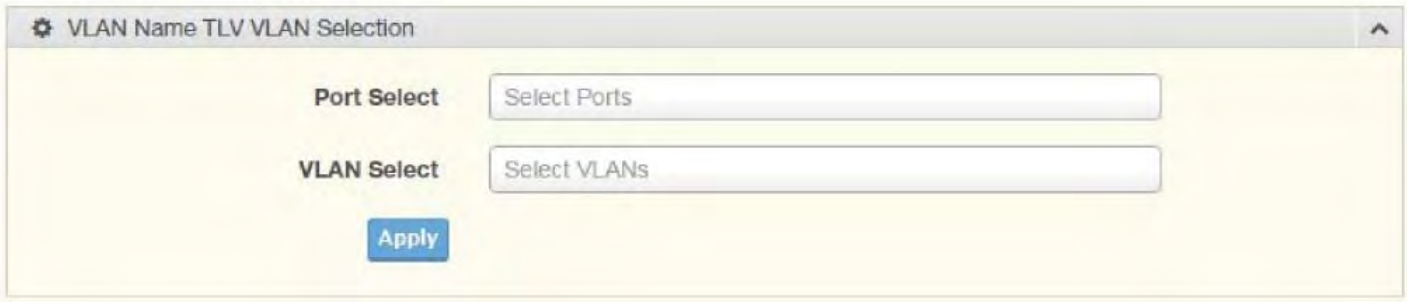


Figure 4-83. Management > LLDP > LLDP Port Settings > VLAN Name TLV VLAN Selection

Table 4-81. Management > LLDP > LLDP Port Settings > 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 ensuing table for LLDP Port VLAN TLV Status settings 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.

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

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

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

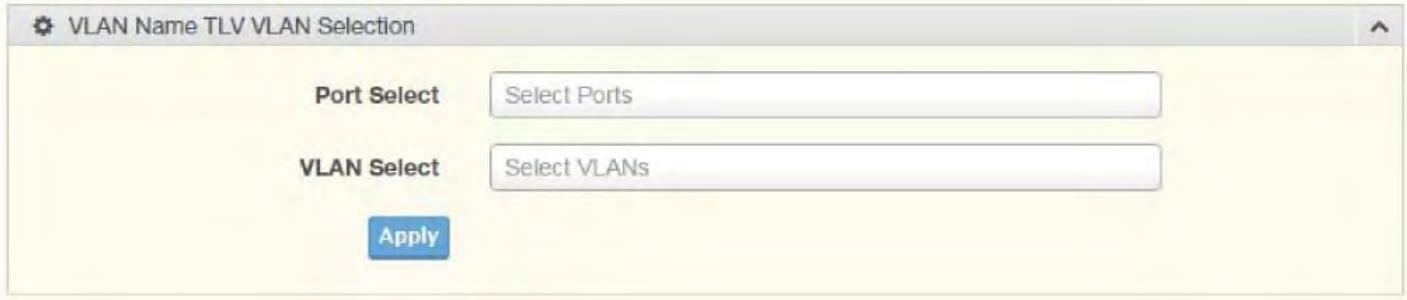


Figure 4-84. Management > LLDP > LLDP Remote Device Info

Table 4-82. Management > LLDP > 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.

LLDP Overloading

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

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

4.9.2 SNMP

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

SNMP Settings

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

Figure 4-85. Management > SNMP > SNMP Settings

Table 4-83. Management > SNMP > 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 ensuing table for SNMP Information settings 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.

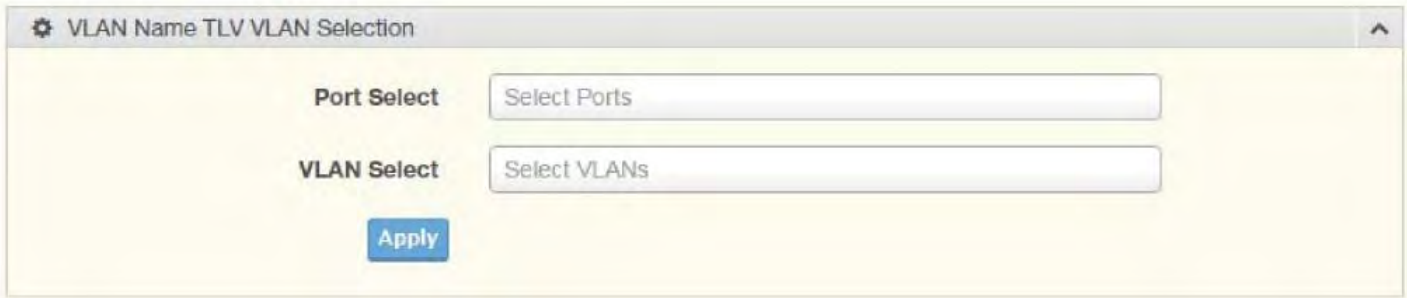


Figure 4-86. Management > SNMP > SNMP Community

Table 4-84. Management > SNMP > 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 ensuing table for Community Status settings are informational only: No., Community Name, Access Right and Delete (click to delete the desired community name).

SNMP User Settings

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

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

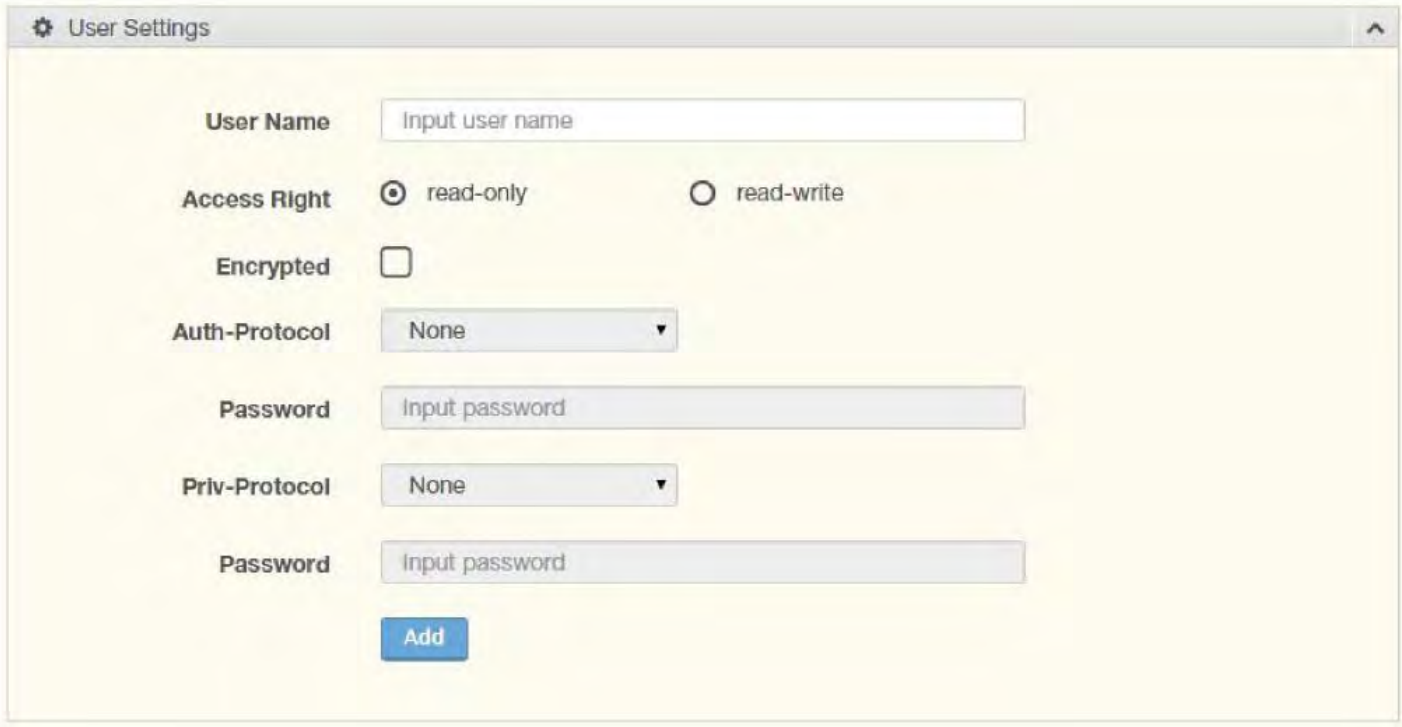


Figure 4-87. Management > SNMP > SNMP User Settings

Table 4-85. Management > SNMP > 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
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 ensuing table for User Status settings are informational only: User Name, Access Right, Auth-Protocol, Priv-Protocol and Delete (click to delete the desired user name).

SNMP Trap

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

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

Figure 4-88. Management > SNMP > SNMP Trap

Table 4-86. Management > SNMP > 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 or v2c).
Add	Click Add to save the values and update the screen.

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

4.9.3 Power Over Ethernet

Power Over Ethernet is the function supplying power to Powered Devices (PD) through the switch in the event that AC power is not readily available.

Power over Ethernet can be used for the following areas:

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

PoE System Settings

The PoE System Settings page allows you to configure the overload disconnect and the maximum available wattage.

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

Figure 4-89. Management > Power Over Ethernet > PoE System Settings

Table 4-87. Management > Power Over Ethernet > 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 ensuing table for PoE System Information settings 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.

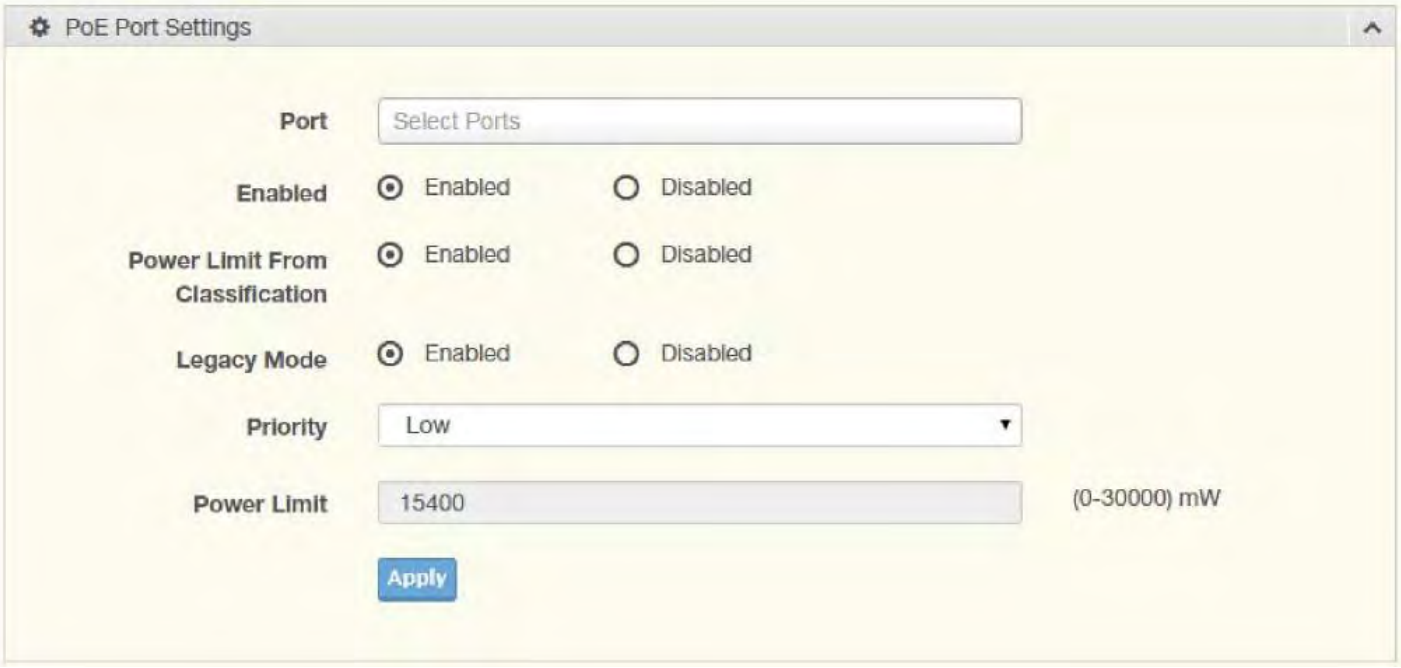


Figure 4-90. Management > Power Over Ethernet > PoE Port Settings

Table 4-88. Management > Power Over Ethernet > 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 Disabled 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 ensuing table for PoE Information settings 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.

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

4.9.4 TCP Modbus

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 > TCP Modbus Settings.

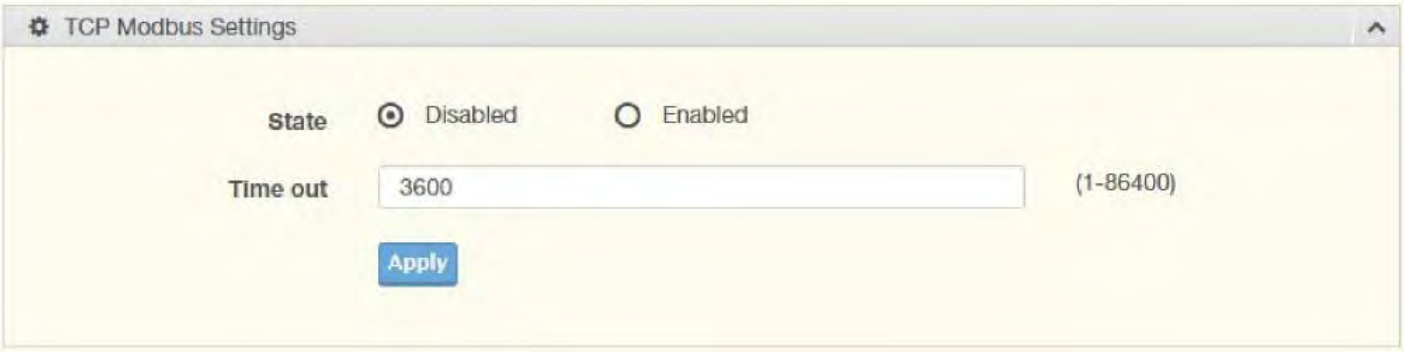


Figure 4-91. Management > TCP Modbus > TCP Modbus Settings

Table 4-89. Management > TCP Modbus > 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.

4.9.5 DHCP Server

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

Status Settings

The Status Settings page allows you to configure the DHCP server mode (enabled or disabled).

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

Figure 4-92. Management > DHCP Server > Status Settings

Table 4-90. Management > DHCP Server > 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 ensuing table for Status Information settings 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.

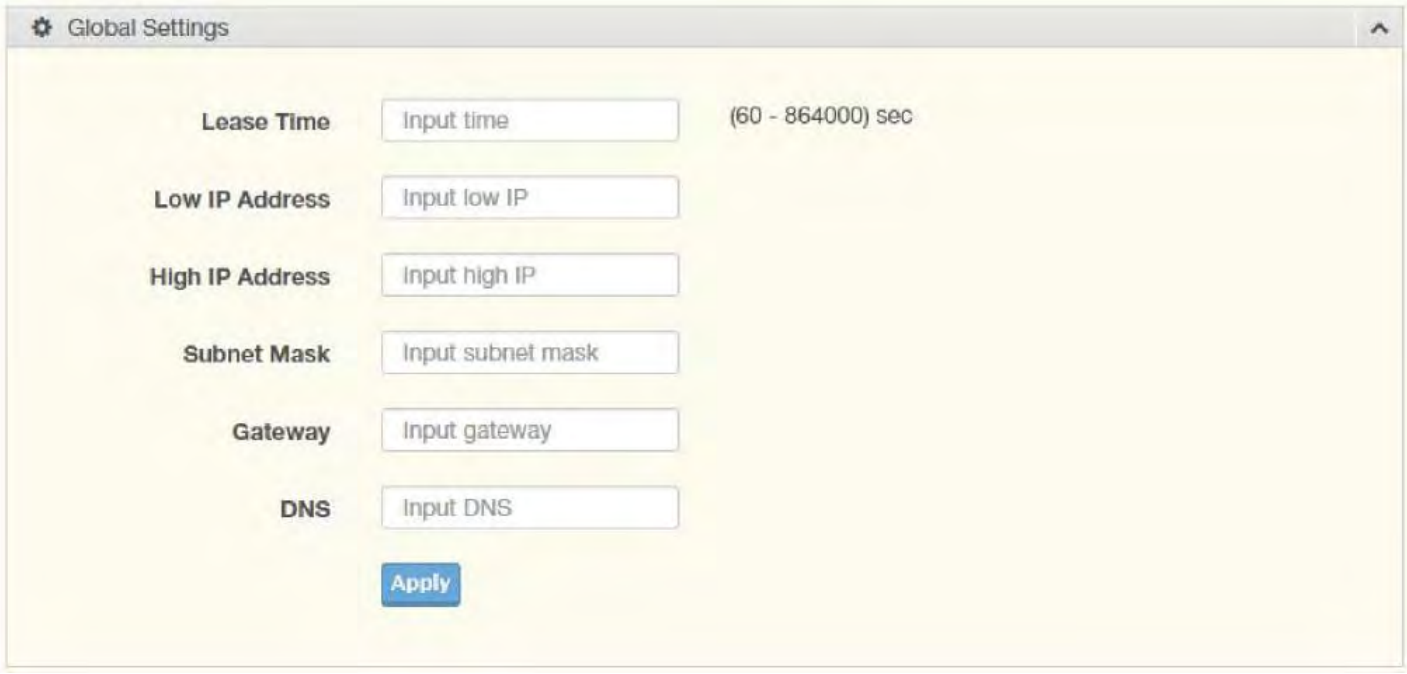


Figure 4-93. Management > DHCP Server > Global Settings

Table 4-91. Management > 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 ensuing table for Global Information settings are informational only: Lease Time, Low IP Address, High IP Address, Subnet Mask, Gateway, DNS and Clear (click to clear IP pool).

Port Settings

The Port Settings page allows you to configure selected ports for the DHCP function. To access this page, click Management > DHCP Server > Port Settings.

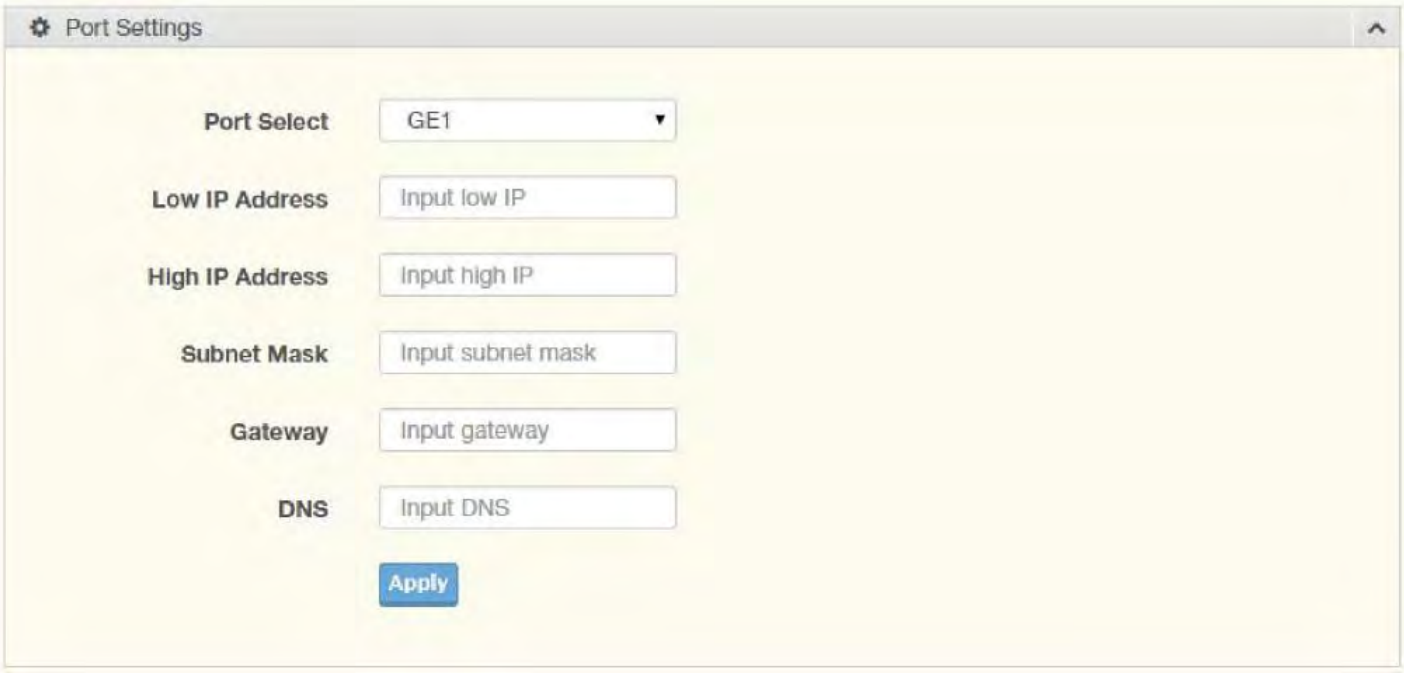


Figure 4-94. Management > DHCP Server > Port Settings

Table 4-92. Management > 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 ensuing table for Port Information settings are informational only: Port, Low IP Address, High IP Address, Subnet Mask, Gateway, DNS, Edit (click to modify the settings) and Clear (click to clear the settings).

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.

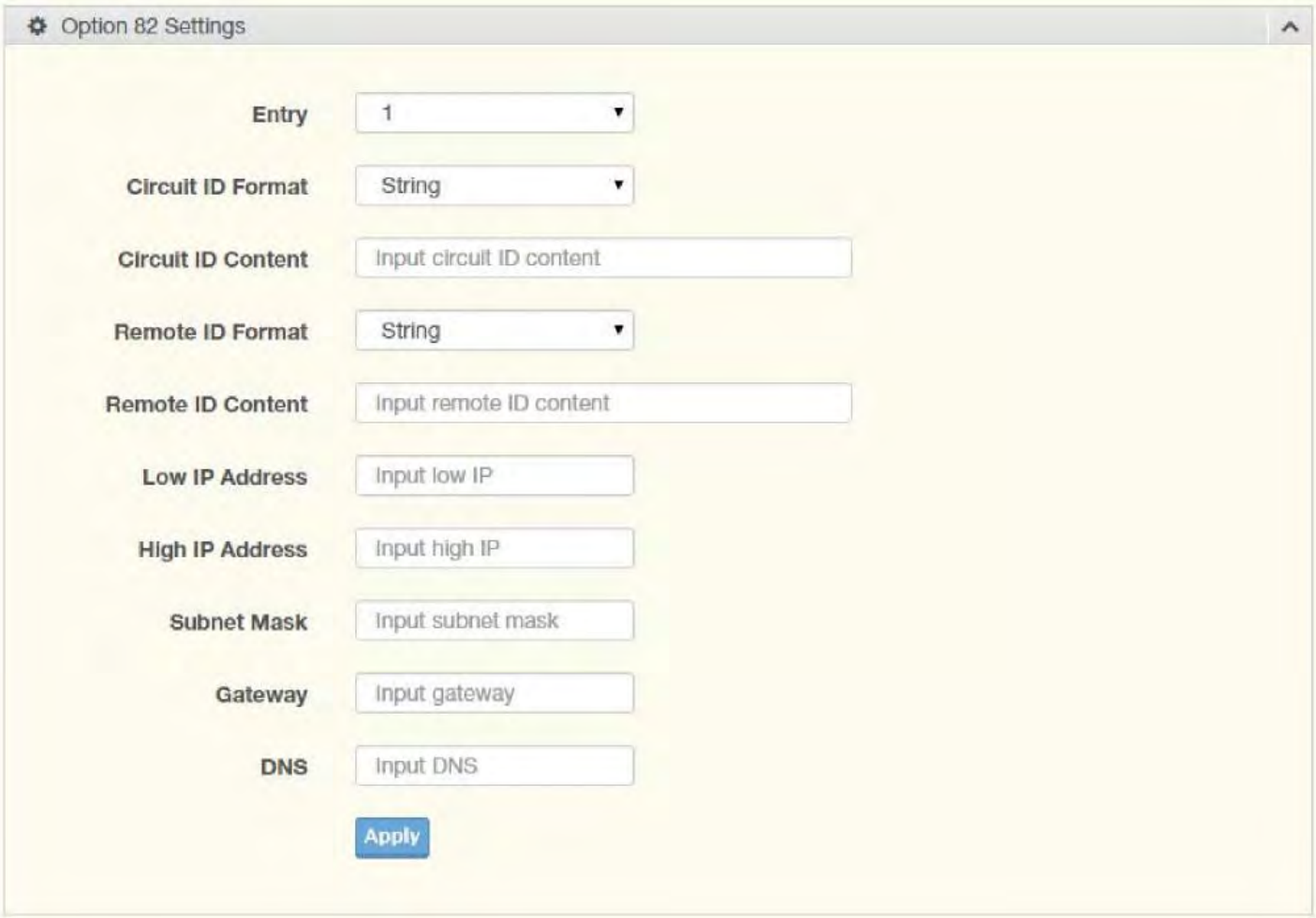


Figure 4-95. Management > DHCP Server > Option 82 Settings

Table 4-93. Management > DHCP Server > 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.
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 ensuing table for Entry Information settings 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).

Lease Entry

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

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

4.9.6 SMTP Client

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

Global Settings

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

Figure 4-96. Management > SMTP Client > Global Settings

Table 4-94. Management > 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 ensuing table for SMTP Information settings 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 for the listed profile.

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

Figure 4-97. Management > SMTP Client > Profile Settings > Profile Settings

Table 4-95. Management > SMTP Client > Profile Settings > 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.

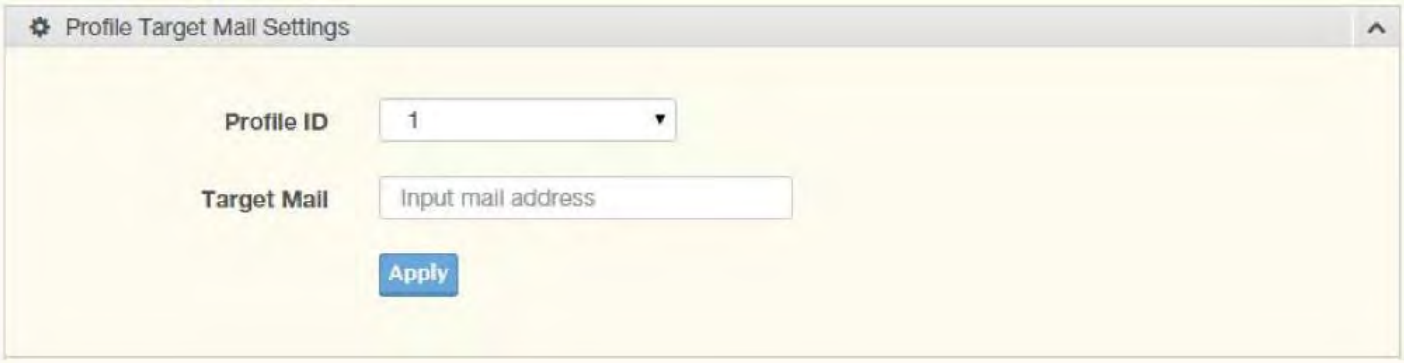


Figure 4-98. Management > SMTP Client > Profile Settings > Profile Target Mail Settings

Table 4-96. Management > SMTP Client > Profile Settings > 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 ensuing table for Profile Information settings are informational only: Profile ID (click the drop-down menu to select a profile ID), Server IP, Server Port and Sender Mail Address.

Sending Message

The Sending Message page allows you to setup the log message for use with the SMTP client.

To access this page, click Management > SMTP Client > Sending Message.

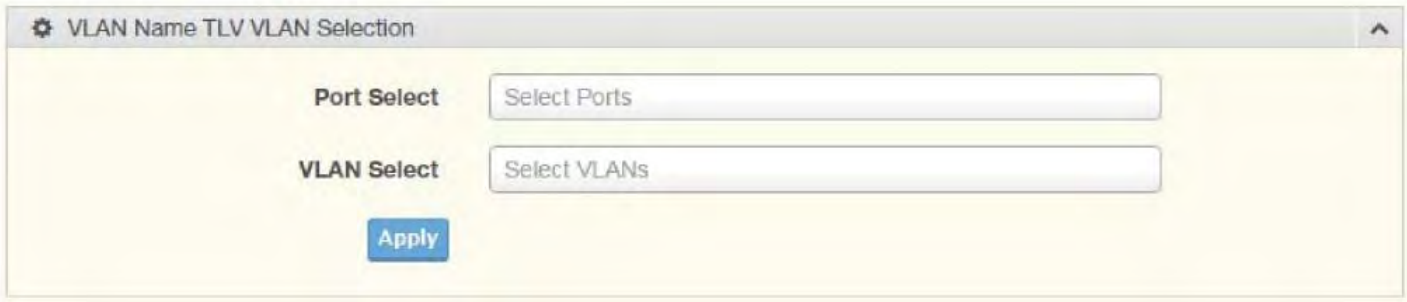


Figure 4-99. Management > SMTP Client > Sending Message

Table 4-97. Management > SMTP Client > 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.

4.9.7 RMON

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

RMON Statistics

The RMON Statistics page allows you to view information regarding packet sizes and information for physical layer errors. The information displayed is according to the RMON standard.

To access this page, click Management > RMON > RMON Statistics.

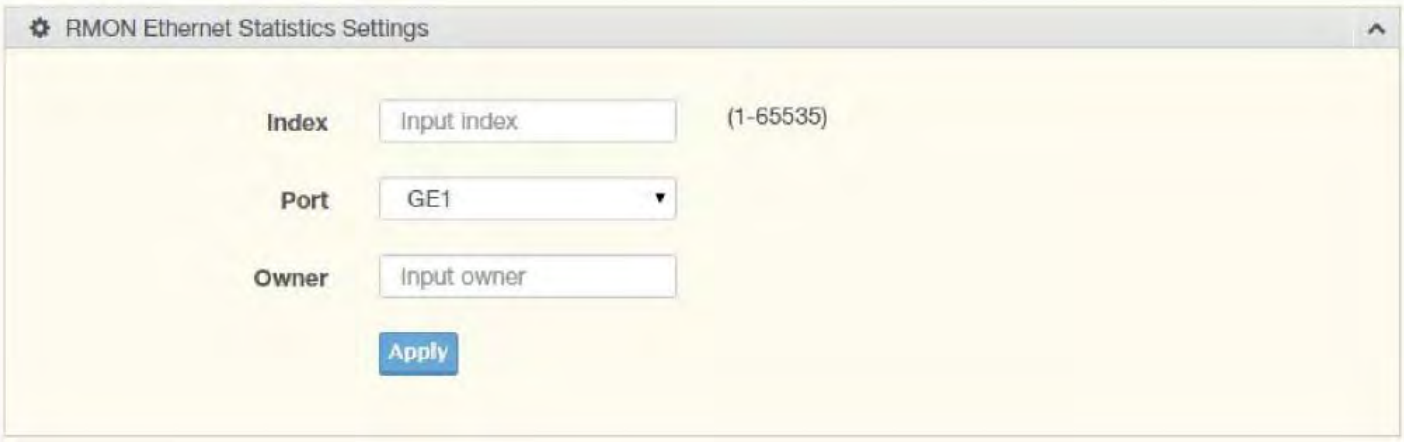


Figure 4-100. Management > RMON > Rmon Statistics

Table 4-98. Management > RMON > 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 ensuing table for Statistics Information settings are informational only: Index, Port, Drop Events, Octets, Packets, Broadcast, Multicast, Owner and Delete (click to delete the desired index).

RMON History

The RMON History page allows you to configure the display of history entries. To access this page, click Management > RMON > RMON History.

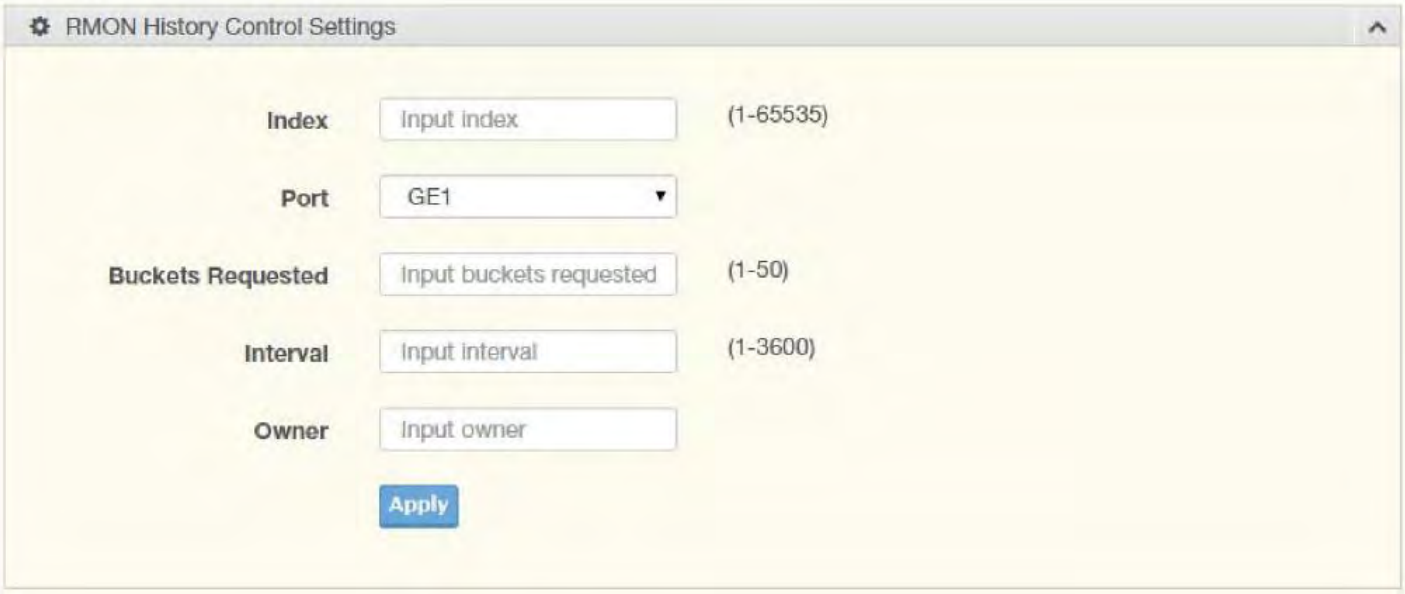


Figure 4-101. Management > RMON > RMON History

Table 4-99. Management > RMON > 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 ensuing table for History Information settings 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.

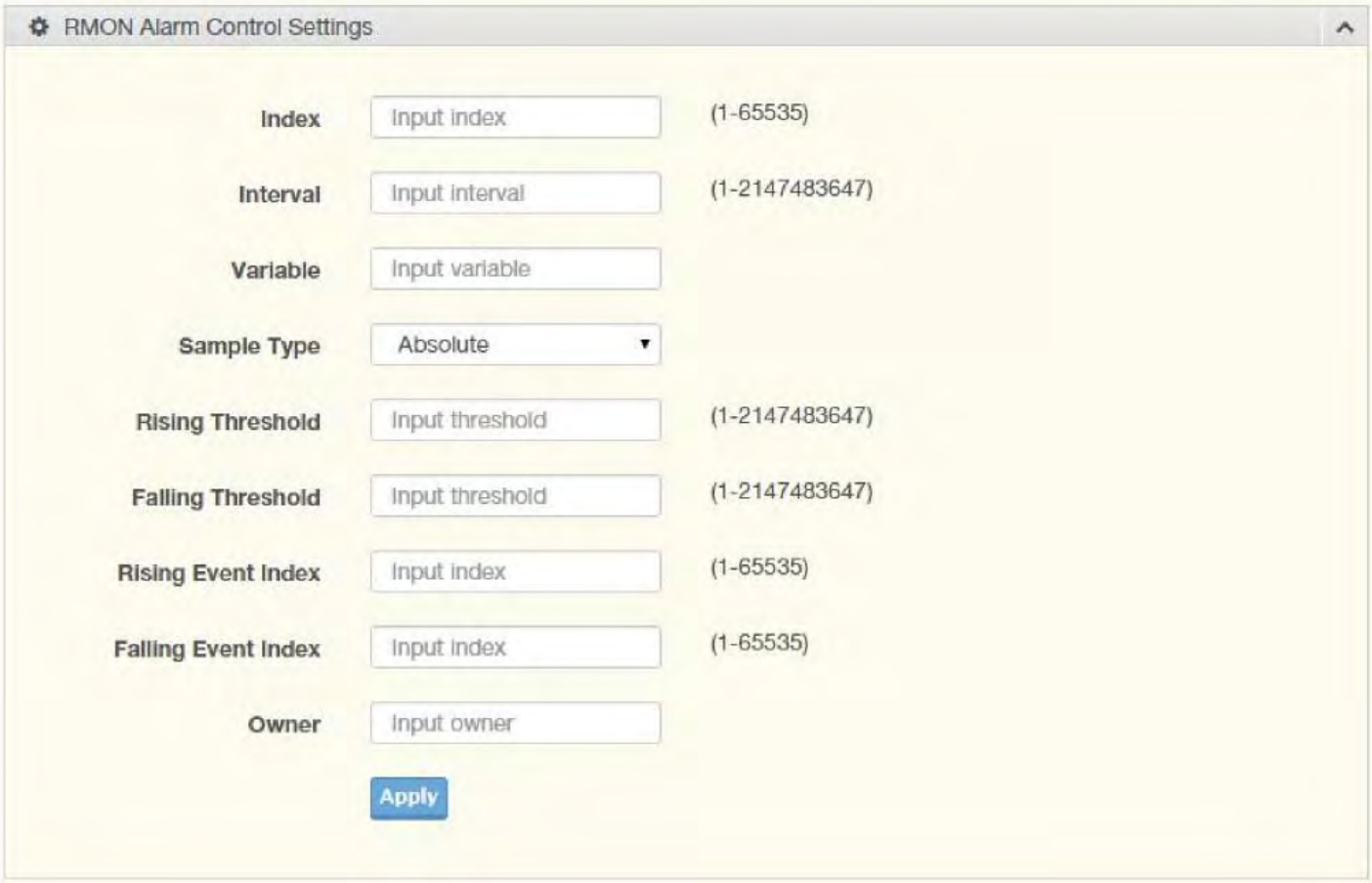


Figure 4-102. Management > RMON > Rmon Alarm

Table 4-100. Management > RMON > 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 ensuing table for Alarm Information settings are informational only: Index, Interval, Variable, Sample Type, Rising Threshold, Falling Threshold, Rising Event Index, Falling Event Index, Owner and Delete (click to delete the desired index).

RMON Event

The RMON Event page is used to configure RMON event groups. To access this page, click Management > RMON > RMON Event.

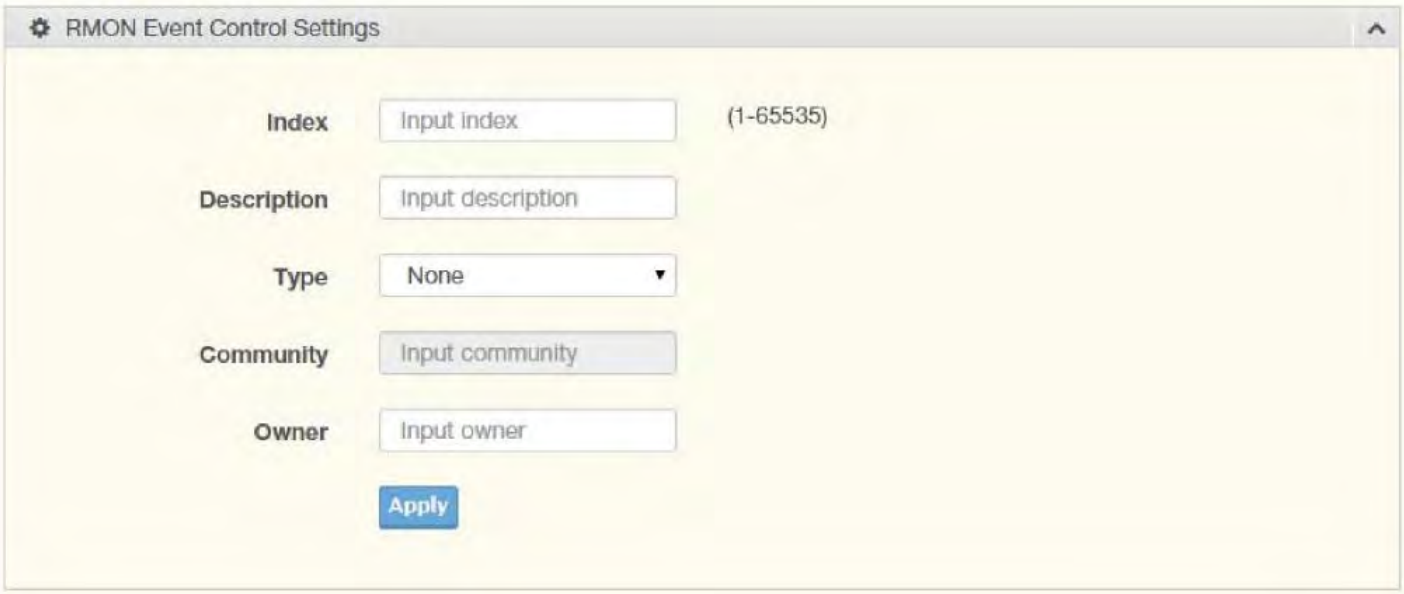


Figure 4-103. Management > RMON > RMON Event

Table 4-101. Management > RMON > 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 ensuing table for Event Information settings are informational only: Index, Description, Type, Community, Owner and Delete (click to delete the desired index).

4.10 Diagnostics

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

4.10.1 Cable Diagnostics

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

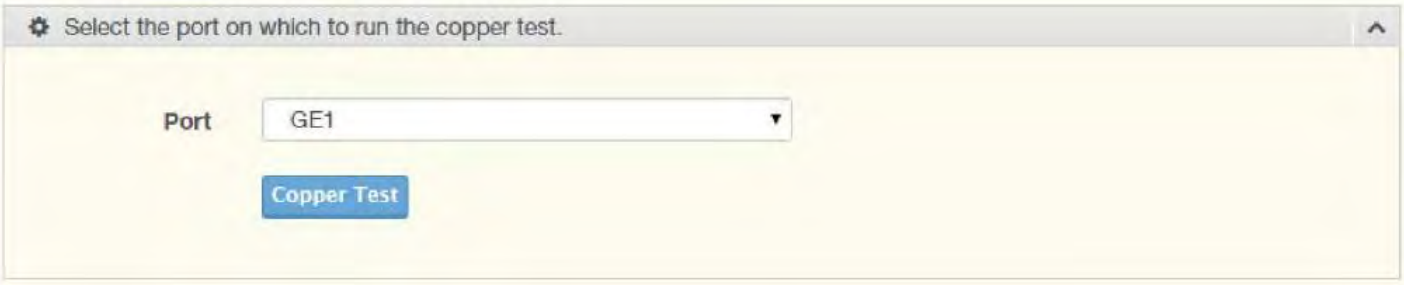


Figure 4-104. Diagnostics > Cable Diagnostics

Table 4-102. Diagnostics > 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 ensuing table for Test Result settings are informational only: Port, Channel A, Cable Length A, Channel B, Cable Length B, Channel C, Cable Length C, Channel D and Cable Length D.

4.10.2 Ping Test

The Ping Test page allows you to configure the test log page. To access this page, click Diagnostics > Ping Test.

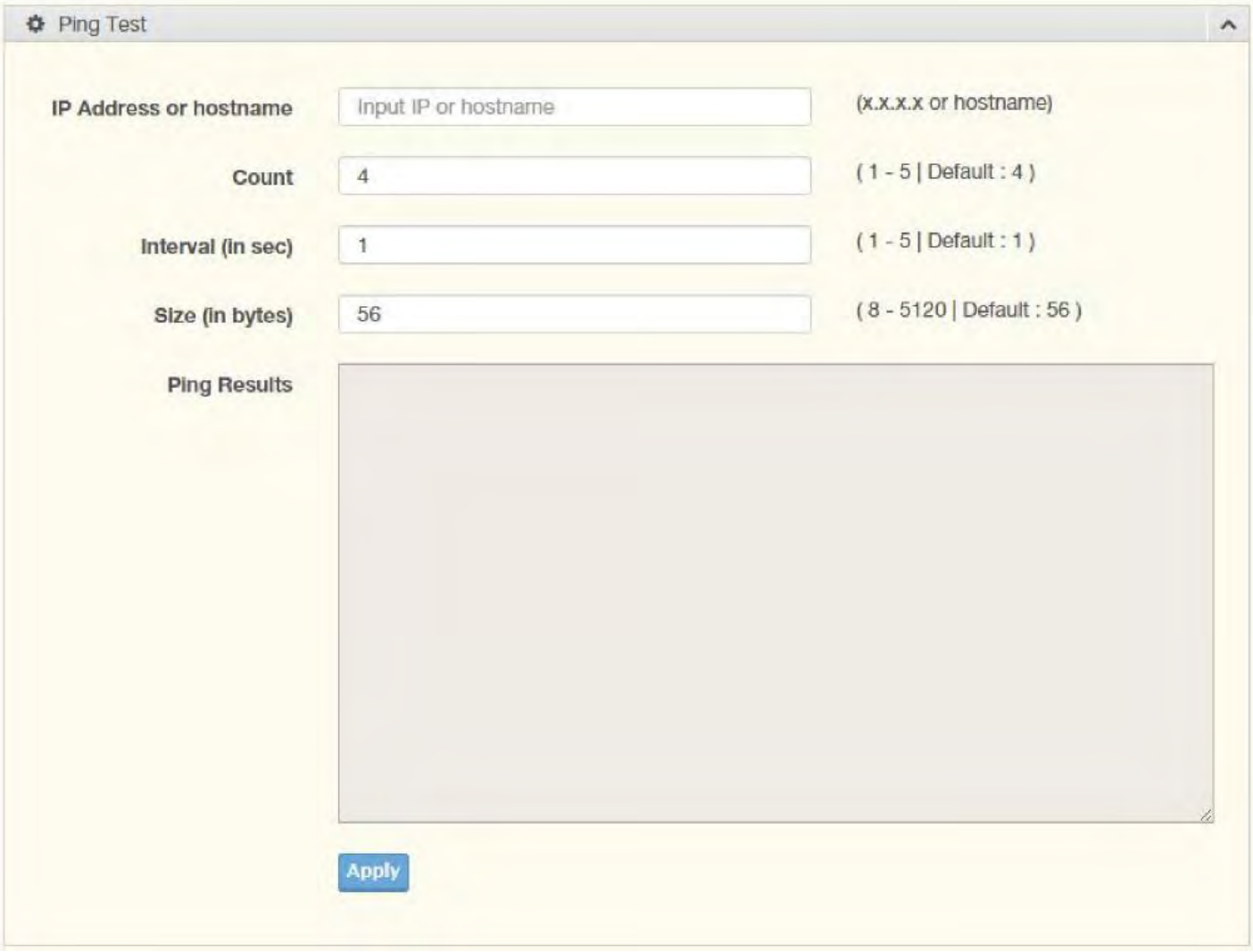


Figure 4-105. Diagnostics > Ping Test

Table 4-103. Diagnostics > 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.
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.

4.10.3 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.

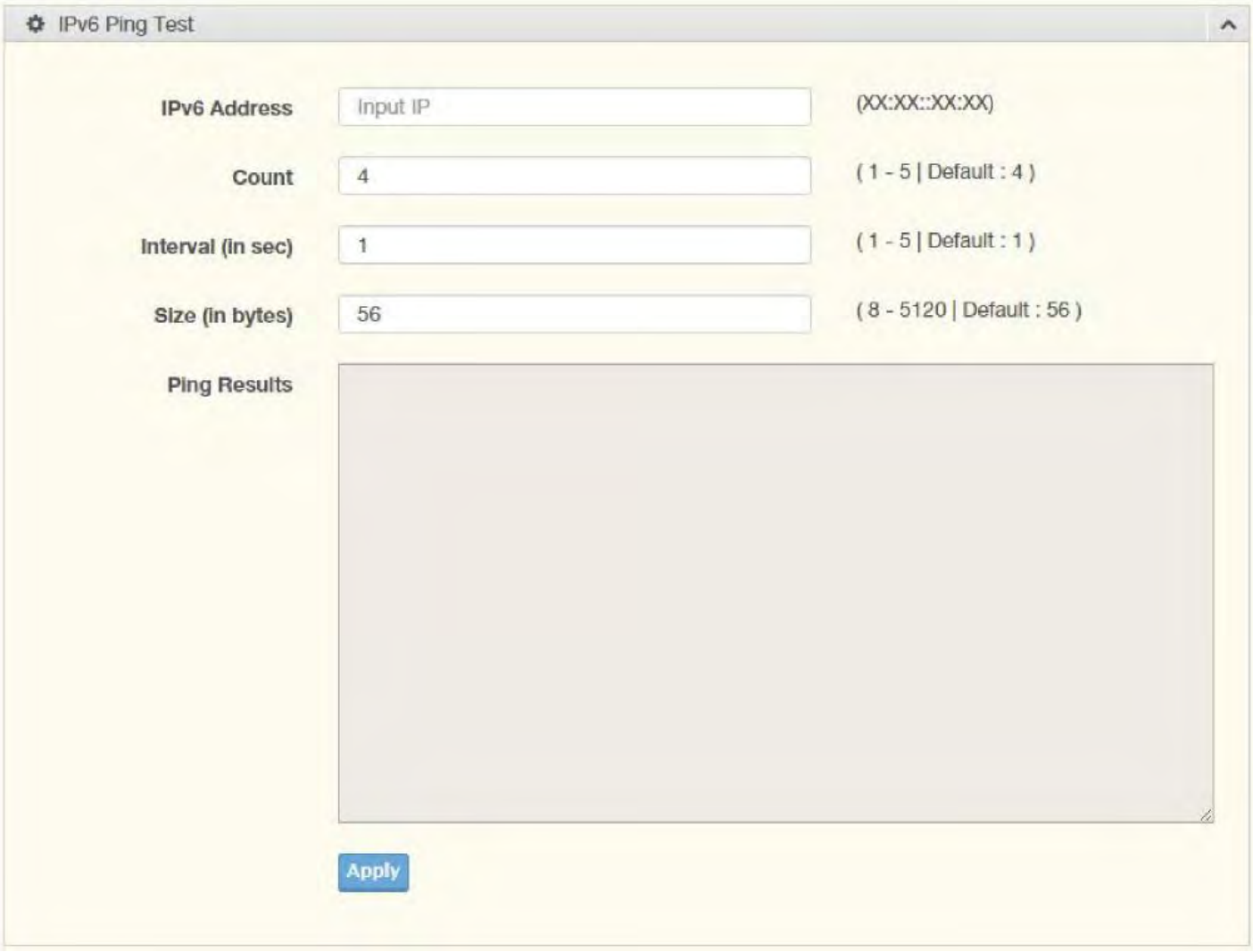


Figure 4-106. Diagnostics > IPv6 Ping Test

Table 4-104. Diagnostics > IPv6 Ping Test

Item	Description
IPv6 Address	Enter the IP address or host name of the station you want the switch to ping. The initial value is blank. The IP Address or host name you enter is not retained across a power cycle. Host names are composed of series of labels concatenated with dots. Each label must be between 1 and 63 characters long, and the entire hostname has a maximum of 64 characters.
Count	Enter the number of echo requests you want to send. The default value is 4. The value ranges from 1 to 5. The count you enter is not retained across a power cycle.
Interval (in sec)	Enter the interval between ping packets in seconds. The default value is 1. The value ranges from 1 to 5. The interval you enter is not retained across a power cycle.
Size (in bytes)	Enter the size of ping packet. The default value is 56. The value ranges from 8 to 5120. The size you enter is not retained across a power cycle.
Ping Results	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.

4.10.4 System Log

Logging Service

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

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

Figure 4-107. Diagnostics > System Log > Logging Services

Table 4-105. Diagnostics > System Log > 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 ensuing table for Logging Information settings 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.

Figure 4-108. Diagnostics > System Log > Local Logging

Table 4-106. Diagnostics > System Log > 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 ensuing table for Local Logging Settings Status settings 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.

Figure 4-109. Diagnostics > System Log > System Log Server

Table 4-107. Diagnostics > System Log > System Log Server

Item	Description
Server Address	Enter the IP address of the log server.
Server Port	Enter the Udp port number of the log server.
Severity	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 ensuing table for Remote Logging Setting Status settings are informational only: Status, Server Info, Severity, Facility and Delete (click to delete the desired server address).

4.10.5 DDM

The DDM page allows you to setup the diagnostic alarm status. To access this page, click Diagnostics > DDM.

Figure 4-110. Diagnostics > DDM

Table 4-108. Diagnostics > DDM

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

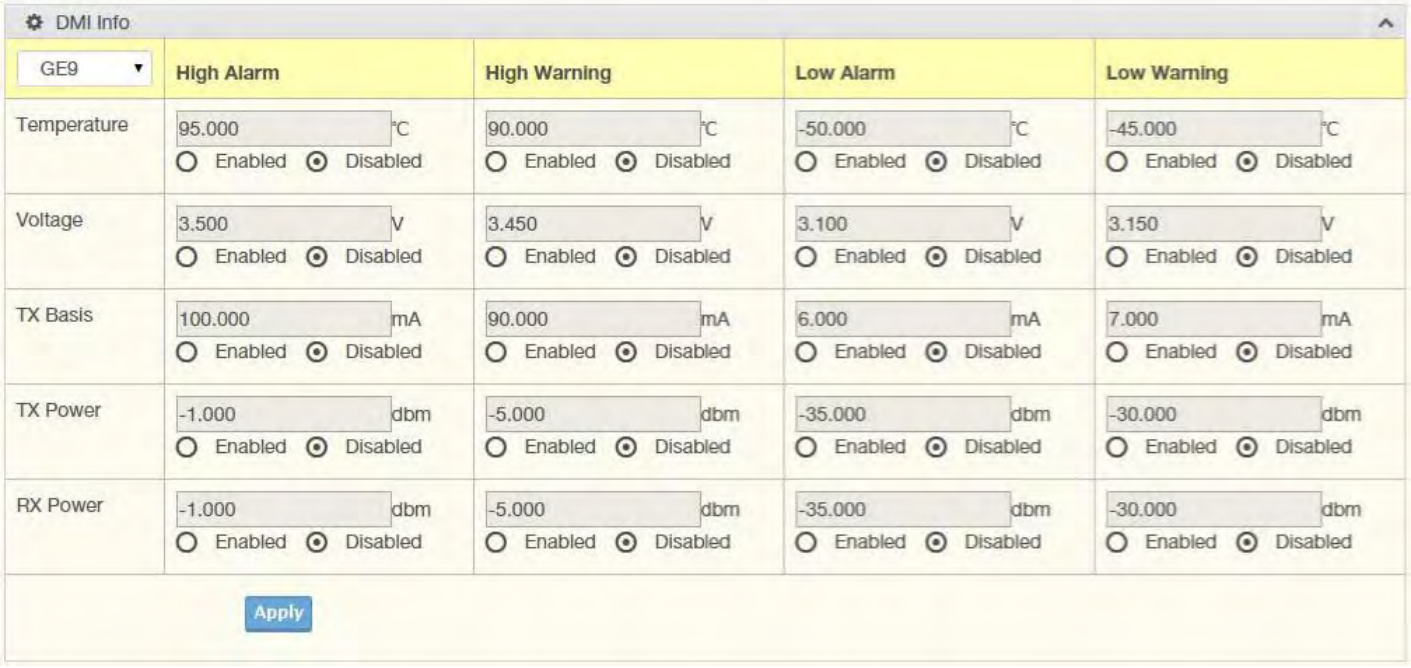


Figure 4-111. Diagnostics > DDM

Table 4-109. Diagnostics > DDM

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

4.11. Tools

4.11.1 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.

Figure 4-112. Tools > IXM

Table 4-110. Tools > 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.
Previous	Click Previous to back to previous page.
Next	Click Next to go to next page.

4.11.2 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.

To access this page, click Tools > Backup Manager.

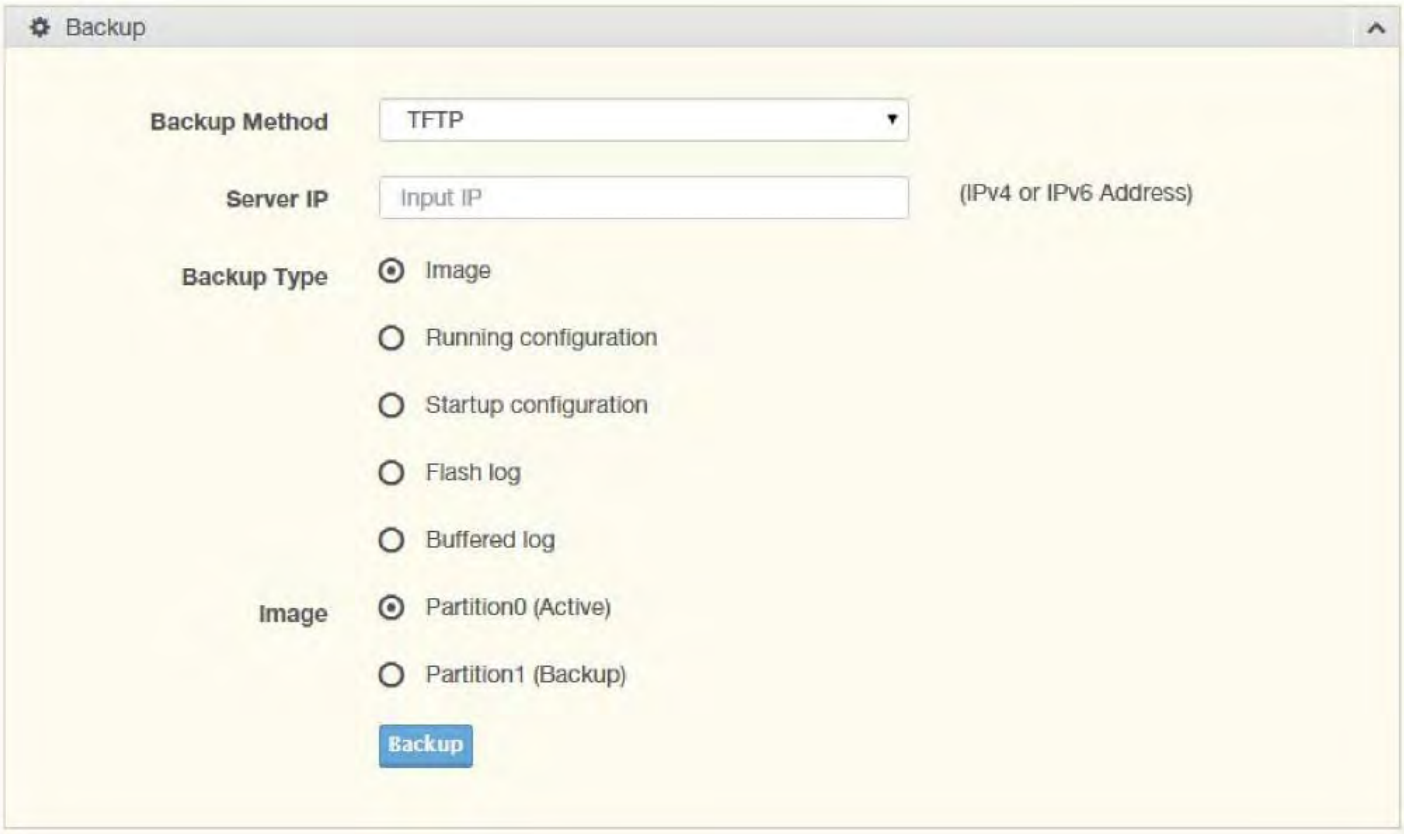


Figure 4-113. Tools > Backup Manager

Table 4-111. Tools > 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: 7428GE_2C_1_00_13.bix (Active) or vmlinux.bix (backup).
Backup	Click Backup to backup the settings.

4.11.3 Upgrade Manager

The Upgrade Manager page allows you to configure a remote TFTP sever or host file system in order to upload firmware upgrade images or configuration files.

To access this page, click Tools > Upgrade Manager.

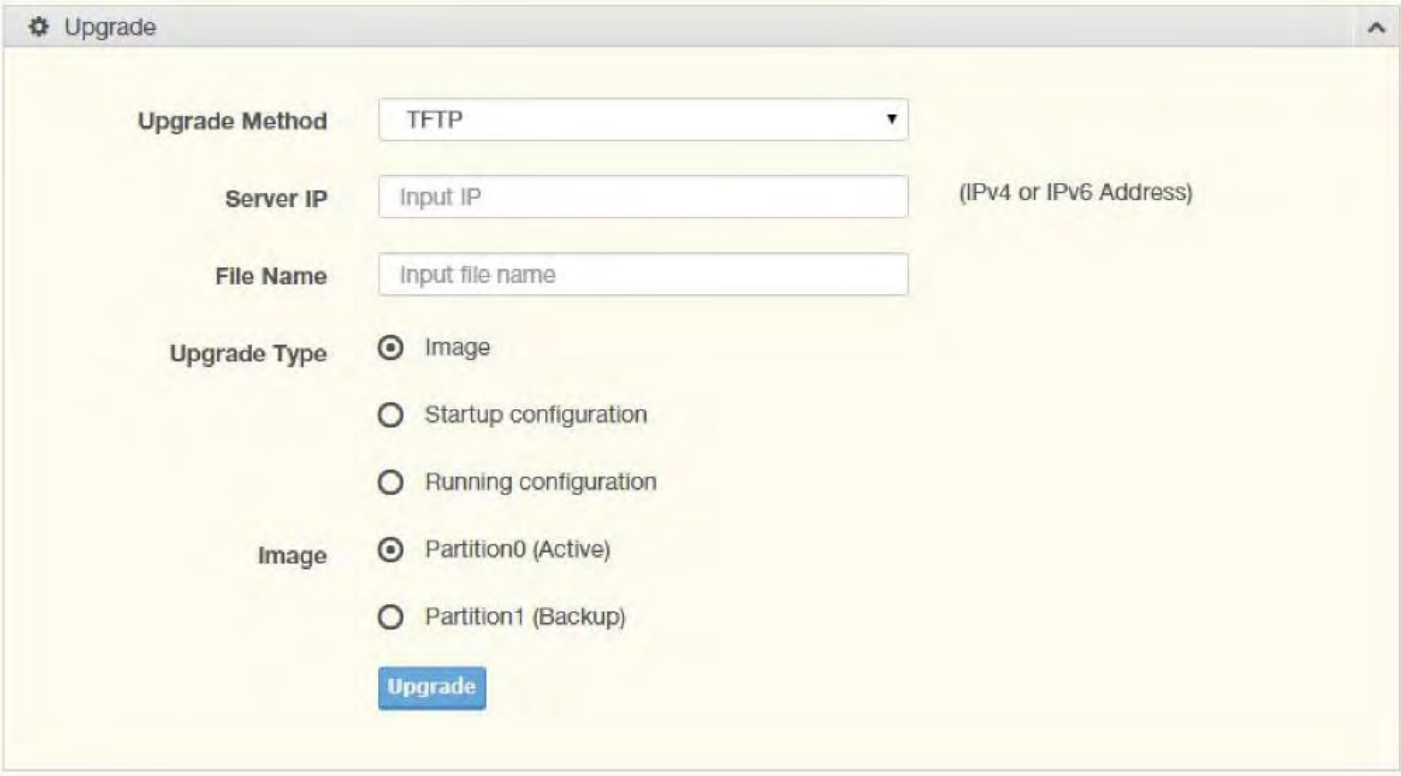


Figure 4-114. Tools > Upgrade Manager

Table 4-112. Tools > 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: 7428G_2C_1_00_13.bix (Active) or vmlinux.bix (backup).
Upgrade	Click Upgrade to upgrade to the current version.

4.11.4 Dual Image

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

To access this page, click Tools > Dual Image.

Figure 4-115. Tools > Dual Image

Table 4-113. Tools > 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 ensuing table for Image Information 0/1 settings are informational only: Flash Partition, Image Name, Image Size and Created Time.

4.11.5 Save Configuration

To access this page, click Tools > Save Configuration.

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

4.11.6 User Account

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

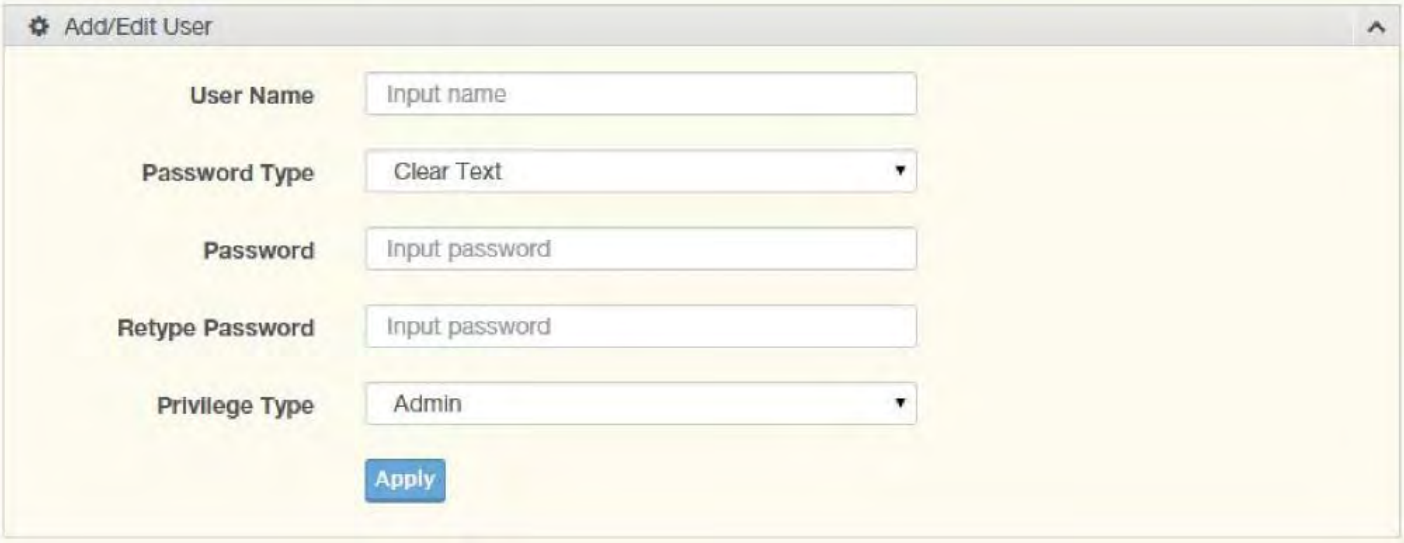


Figure 4-116. Tools > User Account

Table 4-114. Tools > 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 ensuing table for Local Users settings are informational only: User Name, Password Type, Privilege Type and Delete (click to delete the desired user account).

4.11.7 Reset System

To access this page, click Tools > Reset System.

Click Restore to have all configuration parameters reset to their factory default values. All changes that have been made will be lost, even if you have issued a save.

Reset settings take effect after a system reboot.

4.11.8 Reboot Device

To access this page, click Tools > Reboot Device.

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

APPENDIX

Troubleshooting

» Verify that is using the right power cord/adapter (DC 12-48V), please don't use the 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 switch 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 be sure 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 switch 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. Then check for loose power connections, power losses or surges at power outlet. If you still cannot resolve the problem, contact the 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.

ComNet Customer Service
Customer Care is ComNet Technology's global service center, where our professional staff is ready to answer your questions at any time.
Email ComNet Global Service Center: customercare@comnet.net

comnet
Communication Networks

3 CORPORATE DRIVE | DANBURY, CT 06810 | USA
T: 203.796.5300 | F: 203.796.5303 | TECH SUPPORT: 1.888.678.9427 | INFO@COMNET.NET
8 TURNBERRY PARK ROAD | GILDERSOME | MORLEY | LEEDS, UK LS27 7LE
T: +44 (0)113 307 6400 | F: +44 (0)113 253 7462 | INFO-EUROPE@COMNET.NET