COMTREND

USER MANUAL

GS-7424, GS-7620, & GS-7624

Smart Lite Gigabit (PoE)

August 2018, v1.0

Copyright ©2018 Comtrend Corporation. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means without the prior written permission of Comtrend Corporation.

Technical Support

Thank you for choosing Comtrend. If you find the product to be inoperable or malfunctioning, please contact technical support by email (INT-support@comtrend.com) for immediate service.

For product updates, new product releases, manual revisions, or software upgrades, please visit our website at http://www.comtrend.com

Trademarks

Comtrend Corporation makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not Comtrend Corporation, its distributors, or its dealers) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, Comtrend Corporation reserves the right to revise this publication and to make changes from time to time in the contents thereof without obligation to notify any person of such revision or changes.

See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see http://www.gnu.org/licenses/.

This document is subject to change without notice.

Table of Contents

Safety and Regulatory

Audience

This guide is for the networking professional managing the standalone GS-7000 switch series. It is recommended that only professionals with experience working with Comtrend networking devices who are familiar with the Ethernet and local area networking terminology, should service the equipment.

Conventions

The following conventions are used in this manual to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in **boldface** text.
- Arguments for which you supply values are in *italic*.
- Square brackets ([ ]) mean optional elements.
- Braces ({ }) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

Interactive examples use these conventions:

- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >).

Notes and cautions use the following conventions and symbols:

Note

Means additional information. Notes contain additional useful information or references to material available outside of this document.

Caution

Indicates that the reader must be careful. In a situation where a Caution is listed, a user may cause equipment damage or loss of data.

1. Introduction

Thank you for choosing Comtrend GS-7424, GS-7620, or GS-7624 Smart Lite Gigabit (PoE) switch. This device is designed to be operational right out-of-the-box as a standard bridge. In the default configuration, it will forward packets between connecting devices after powered up.

Before you begin installing the switch, make sure you have all of the package contents available, and a PC with a web browser for using web-based system management tools.

1.1. Overview

The Comtrend GS-7620 and GS-7624 Smart Lite Gigabit PoE switches provide 20 and 24 Gigabit PoE+ ports, respectively.

While the GS-7620 provides four mini-GBIC/SFP slots for combo ports, the GS-7624 has four Gigabit SFP slots. In comparison the GS-7424 provides 24 Gigabit ports and four Gigabit SFP slots.

Designed for medium to large network environments, the Smart Lite Gigabit PoE Switch series include a standard 19-inch rack-mount design for greater installation options.

1.2. Package contents

Before using the product, verify that the following items are included in the packing contents. If any item is damaged, please contact your dealer immediately.

- GS-7620 Smart Lite Gigabit PoE Switch, GS-7624 Smart Lite Gigabit PoE Switch, or GS-7424 Smart Lite Gigabit Switch
- Quick Installation Guide
- Power Cord
- Rack Mount Kit
- Foot pads

1.3. Features

The following information displays the key features for the before mentioned models:

QoS

The switch offers a powerful QoS function. This function supports 802.1p VLAN tag priority and DSCP on Layer 3 of network framework.

VLAN

Supports Port-based VLAN and IEEE802.1Q Tag VLAN. Supports 24 active VLANs and VLAN ID 1~4094.

Port Trunking

Allows one or more links to be aggregated to form a Link Aggregation Group through the static setting.

Power Saving (PoE models)

The Power saving using the IEEE 802.3az, Energy-Efficient Ethernet to detect the client idle and cable length automatically and provide the different power. It can reduce the power consumption.

1.4. Specifications

- Supports up to 24 10/100/1000 Mbps Gigabit Ethernet ports and 4 SFP slots or 4 mini-GBIC/SFP slots
- IEEE 802.3af/at PoE compliant to simplify deployment and installation
- Supports PoE (GS-7620 and GS-7624) up to 30W per port with 330W total power budget
- Automatically detects powered devices (PD) and power consumption levels
- IEEE 802.1Q VLAN allows network segmentation to enhance performance and security
- Supports Access Control List (ACL)
- Switch capacity: GS-7624 & GS-7424: 56 Gbps; GS-7620: 40 Gbps, Forwarding rate: 35.7 Mbps
- Supports IGMP Snooping V1 / V2 / partial V3
- 8K MAC address table and 9K jumbo frames
- 19-inch rack-mountable metal case

1.5. Front and Back Panel Configuration

The following figures illustrate the front and back panels of the Smart Lite Gigabit switch series.

1.5.1. Ports

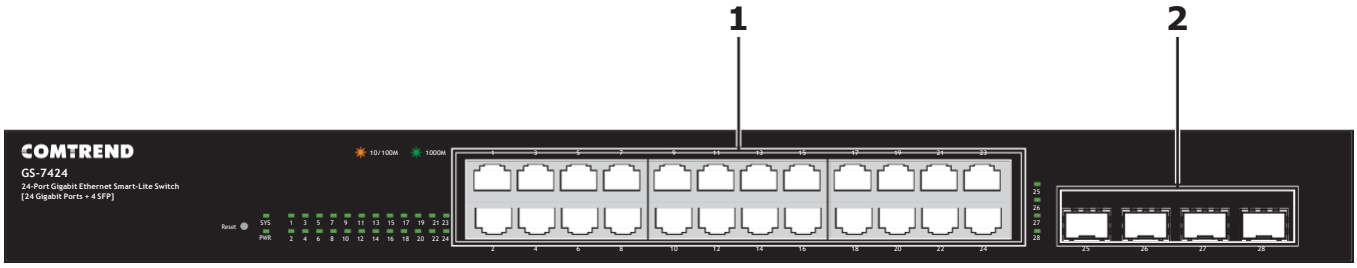


Figure 1 - GS-7424 Front Panel View

No.	Name	Description
1	RJ-45 LNK/ACT Port 1~24	Port 1 to Port 24 function as an Ethernet connection (10/100/1000 Mbps). Each has a corresponding 10/100/1000 Mbps LED.
2	SFP LNK/ACT Port 25~28	Ports 25 to 28 function as fiber connections. Each has a corresponding 1000Mbps LED.

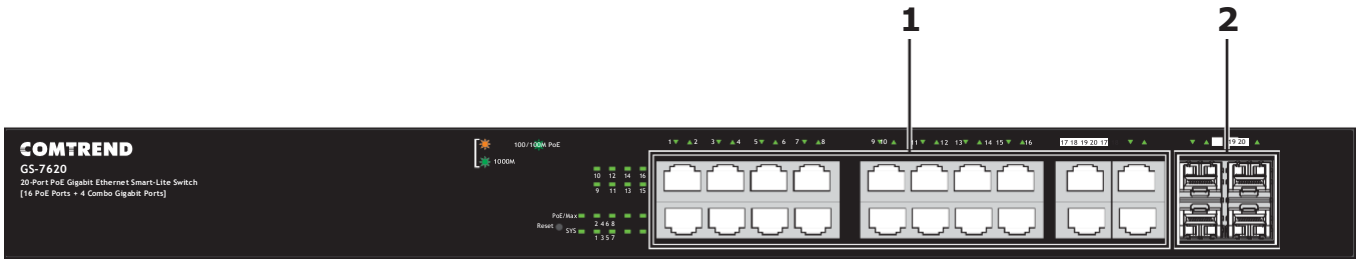


Figure 2 - GS-7620 Front Panel View

No.	Name	Description
1	RJ-45 LNK/ACT Port 1~20	Port 1 to Port 24 function as an Ethernet connection (10/100/1000 Mbps) and PoE connection. Each has a corresponding 10/100/1000 Mbps LED.
2	SFP LNK/ACT Port 21~24	Designed to install SFP modules and connect to network devices with a bandwidth of 1000Mbps. Each has a corresponding 1000Mbps LED.

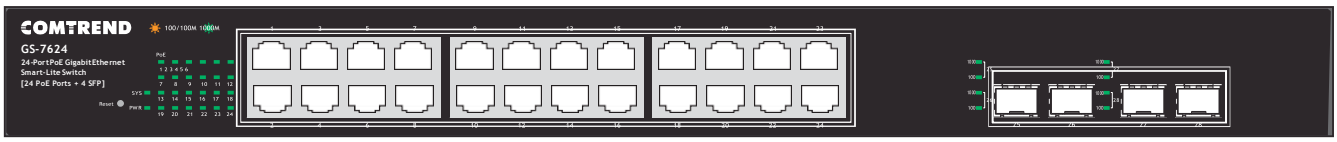


Figure 3 - GS-7624 Front Panel View

No.	Name	Description
1	RJ-45 LNK/ACT Port 1~24	Port 1 to Port 24 function as an Ethernet connection (10/100/1000 Mbps) and PoE connection. Each has a corresponding 10/100/1000 Mbps LED.
2	SFP LNK/ACT Port 25~28	Ports 25 to 28 function as fiber connections. Each has a corresponding 1000Mbps LED.

Figure 4 - GS-7424, GS-7620, and GS-7624 Back Panel View

No.	Name	Description
1	AC power inlet	100~240V/AC, 50/60Hz

1.5.2. LED Indicators

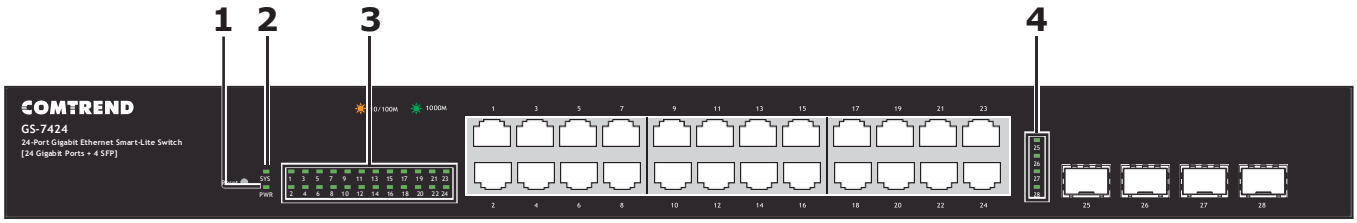


Figure 5 - GS-7424 Front Panel LED Indicators

No.	LED	Description
1	PWR	• Off: power off • On: power on
2	SYS	• Off: system not ready • On: system ready • Blinking: system boot-up
3	RJ-45 LNK/ACT Port 1~24	Bi-color LED: • Off: port disconnected or link fail • Green On/Blinking: 1000 Mbs connected/data transmitting • Amber On/Blinking: 10/100 Mbs connected/data transmitting
4	SFP LNK/ACT Port 25~28	• Off: port disconnected or link fail • Green On/Blinking: 1000 Mbs connected/data transmitting

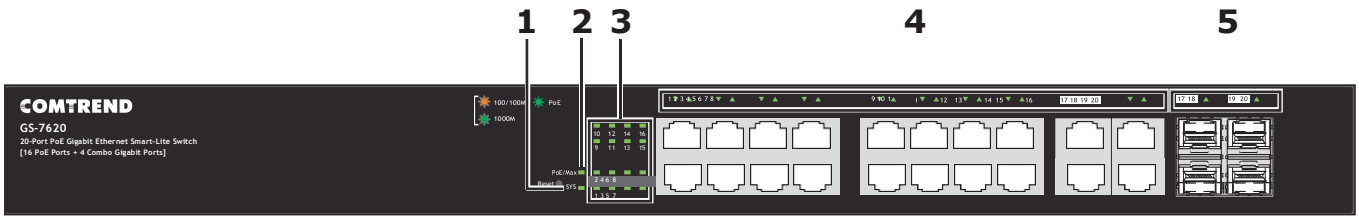


Figure 6 - GS-7620 Front Panel LED Indicators

No.	Name	Description
1	SYS	• Off: power off or fail • Green On: power on • Green Blinking: system boot-up
2	PoE/Max	• Off: PoE power output under 320W PoE power budget • Green On: PoE power output over 320W PoE power budget
3	Port LED (PoE)	• Off: PoE power output off • Green On: PoE power output on
4	Port LED (LINK/ACT)	Bi-color LED: • Off: port disconnected or link fail • Green On/Blinking: 1000 Mbs connected/data transmitting • Amber On/Blinking: 10/100 Mbs connected/data transmitting
5	SFP	• Off: port disconnected or link fail • Green On/Blinking: 1000 Mbs connected/data transmitting

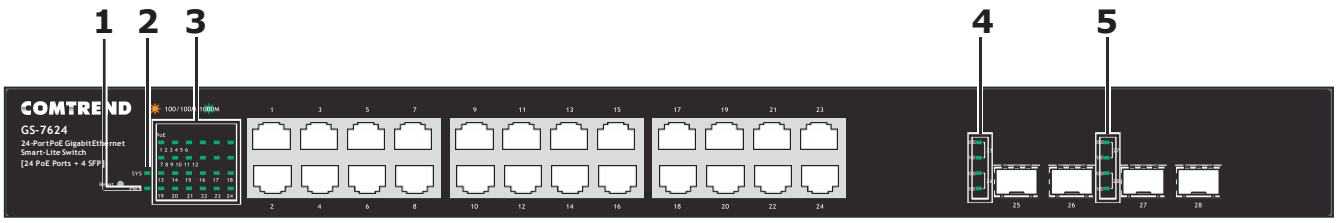


Figure 7 - GS-7624 Front Panel LED Indicators

No.	Name	Description
1	PWR	• Off: power off • On: power on
2	SYS	• Off: system not ready • On: system ready • Blinking: system boot-up
3	Port LED (PoE)	• Off: PoE power output off • Green On: PoE power output on
4	Copper port LED: per port 2 LEDs, on RJ45 phone jack	• Off: port disconnected or link fail • Green On (right side): 1000 Mbs connected • Yellow On (left side): 10/100 Mbs connected • Blinking: sending or receiving data
5	SFP	• Off: port disconnected or link fail • Green On/Blinking: 1000 Mbs connected/data transmitting

2. Installation

This chapter describes how to install and connect your Comtrend Switch. Read the following topics and perform the procedures in the correct order. Incorrect installation may cause damage to the product.

2.1. Mounting the Switch

There are two ways to physically set up the switch.

- Place the switch on a flat surface. To place the switch on a desktop, install the four rubber feet (included) on the bottom of the switch.
- Mount the switch in a standard rack (1 rack unit high).

2.1.1. Placement Tips

- Ambient Temperature—To prevent the switch from overheating, do not operate it in an area that exceeds an ambient temperature of 122°F (50°C).
- Air Flow—Be sure that there is adequate air flow around the switch.
- Mechanical Loading—Be sure that the switch is level and stable to avoid any hazardous conditions.
- Circuit Overloading—Adding the switch to the power outlet must not overload that circuit.

Follow these guidelines to install the switch securely.

- Put the switch in a stable place such as a desktop to prevent it from falling.
- Ensure the switch works in the proper AC input range and matches the voltage labeled.
- Ensure there is proper heat dissipation from and adequate ventilation around the switch.
- Ensure the switch’s location can support the weight of the switch and its accessories.

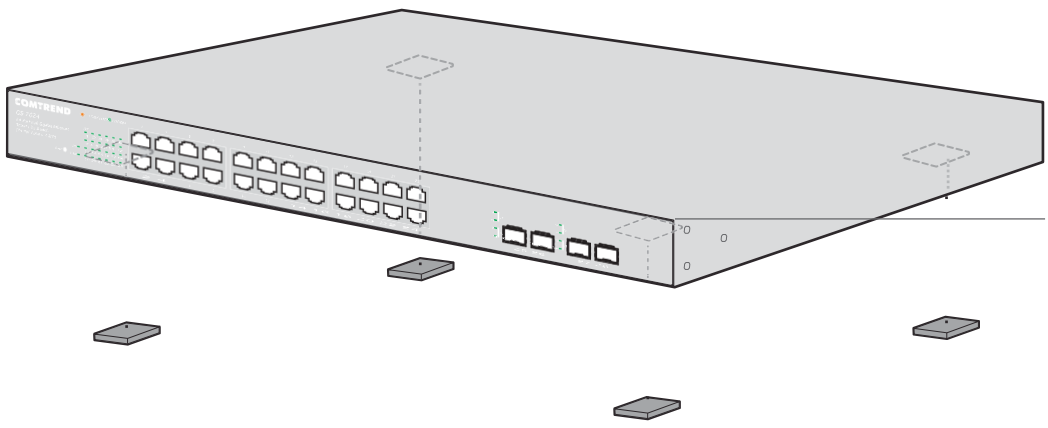


Figure 8 - Installing Rubber Feet

2.1.2. Rack Mounting

You can mount the switch in any standard sized 19-inch (482.6 mm) wide rack. The switch requires 1 rack unit (RU) of space, which is 1.75 inches (44.45 mm) high.

For stability, load the rack from the bottom to the top, with the heaviest devices on the bottom. A top-heavy rack is likely to be unstable and may tip over.

When mounting smaller switch products into a standard 19-inch rack, a pair of extension brackets, sometimes referred to as ears, are needed to adapt the switch to the rack size.

These extension brackets are mounted on the switch using the screws provided in the kit, and have two holes that are used to then screw the switch into the rack.

An example of one type of these extension brackets is shown in the following figure.

A common problem that occurs during rack mounting is the distance between the screw holes on the rack. Some racks are made with a uniform distance between all of the holes, and others have the holes organized into groups, see Figure 10 for further information.

When organized into groups, the switch must be placed in the rack so that the holes in the extension brackets line up correctly.

1. Align the mounting brackets with the mounting holes on the switch's side panels and secure the brackets with the screws provided.

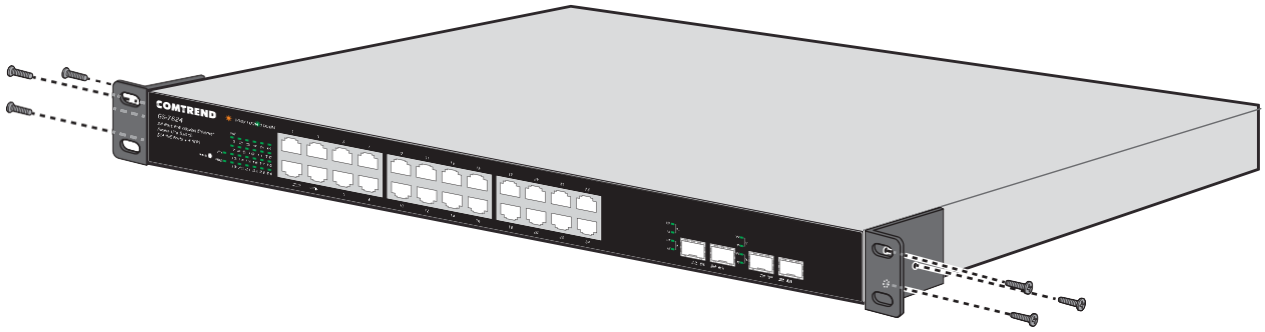


Figure 9 - Bracket Installation

2. Secure the switch on the equipment rack with the screws provided.

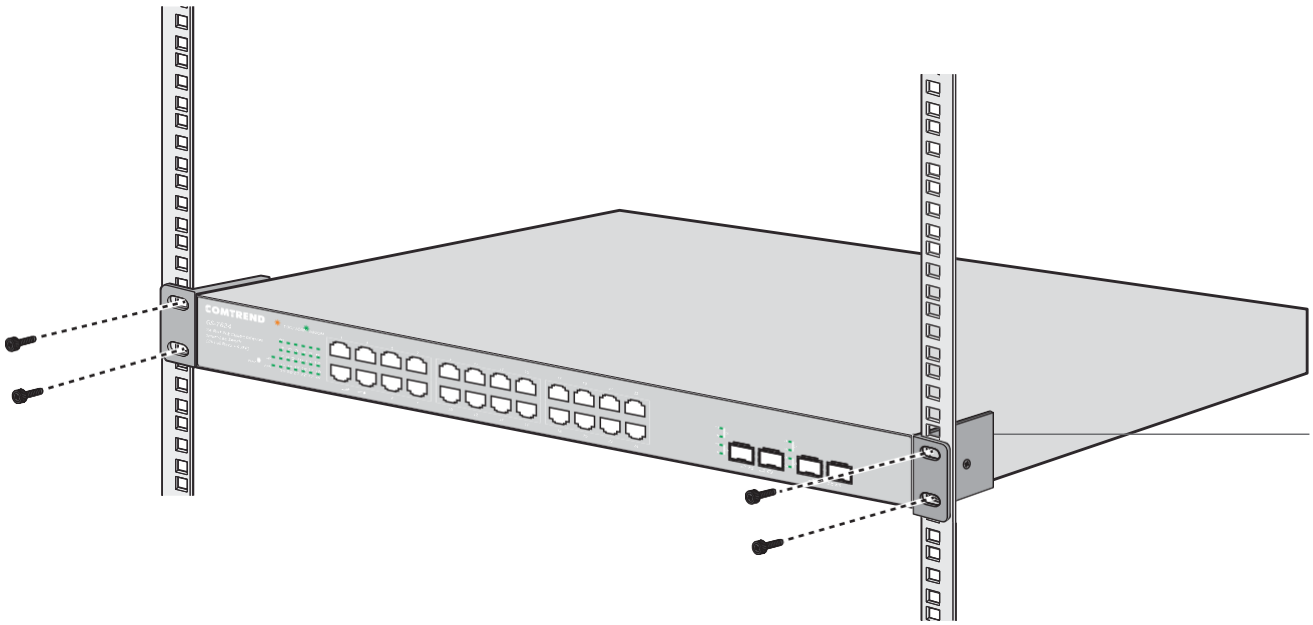


Figure 10 - Rack Installation

3. Getting Started

This section provides an introduction to the web-based configuration utility, and covers the following topics:

- Powering on the device
- Connecting to the network
- Power over Ethernet (PoE) considerations
- Starting the web-based configuration utility

3.1. Power

3.1.1. Connecting to Power

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

Disconnect the power cord before installation or cable wiring.

The switch is powered by an AC 100-240 V 50/60Hz internal high-performance power supply. It is recommended to connect the switch with a single-phase three-wire power source with a neutral outlet, or a multifunctional computer professional source.

Connect the AC power connector on the back panel of the switch to the external power source with the included power cord. The switch boots up and the power LED lights indicating that the switch is powered on.

Figure 11 - Power Socket Location, Rear View

3.1.2. Connecting to the Network

To connect the switch to the network:

1. Connect an Ethernet cable to the Ethernet port of a computer.
2. Connect the other end of the Ethernet cable to one of the numbered Ethernet ports of the switch. If activity is present on the port, the LED lights up.
3. Repeat for any remaining cable connections.

We strongly recommend using a CAT-5E or better cable to connect network devices. When connecting network devices, do not exceed the maximum cabling distance of 100 meters (328 feet). It can take up to one minute for attached devices or the LAN to be operational after it is connected. This is normal behavior.

4. Connect the switch to end nodes using a standard Cat 5/5e Ethernet cable (UTP/STP), see the following figure.

   Switch ports automatically adjust to the connected device's characteristics (MDI/MDI-X, speed, duplex).

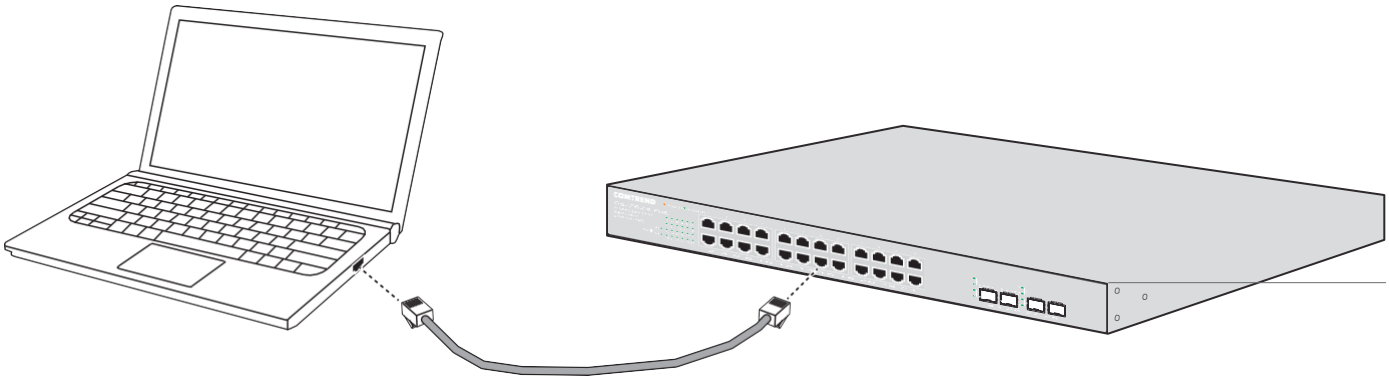


Figure 12 - Connecting to an End Node

3.1.3. Power over Ethernet (PoE) Considerations

For PoE switch models, consider the following information:

Devices considered a Power Sourcing Equipment (PSE), can support up to 30 Watts per PoE port.

Model	Power Dedicated to PoE	PoE Ports	PoE Standard Supported
GS-7620	330W	1 to 16	IEEE802.3at/af
GS-7624	330W	1 to 24	IEEE802.3at/af

Ports 1-24 provide PoE power supply functionality with a maximum output power up to 30W each port. This can supply power to PDs such as Internet phones, network cameras, wireless access points. Connect the switch PoE port directly to the PD port using a network cable.

When connecting switches capable of supplying PoE, consider the following information:

- Switch models with PoE function are PSEs. These models are capable of supplying DC power to attached PDs, such as VoIP phones, IP cameras, and wireless access points (APs). Additionally, PoE switches are capable of detecting and supplying power to pre-standard legacy PoE Power Devices. Due to the support for legacy PoE, there is a possibility that PoE switches acting as a PSE may inadvertently detect and supply power an attached PSE, including other PoE switches. This false detection may result in a PoE switch operating improperly and unable to supply power to attached PDs.
- The prevention of a false detection can be easily remedied by disabling PoE on the ports that are used to connect PSEs. Another simple practice to prevent a false detection is to first power up a PSE device before connecting it to a PoE switch.
- When a device is falsely detected as a PD, disconnect the device from the PoE port and power recycle the device with AC power before reconnecting it to the PoE port.

3.1.4. Starting the Web-based Configuration Utility

This section describes how to navigate the web-based switch configuration utility.

It is recommended to disable the pop-up blocker.

Browser Restrictions

- If you are using older versions of the Microsoft® Internet Explorer (IE), you cannot directly use an IPv6 address to access the device. You can, however, use the DNS (Domain Name System) server to create a domain name that contains the IPv6 address, and then use that domain name in the address bar in place of the IPv6 address.
- If you have multiple IPv6 interfaces on your management station, use the IPv6 global address instead of the IPv6 link local address to access the device from your browser.

Launching the Configuration Utility

To open the web-based configuration utility:

1. Open a Web browser.
2. Enter the IP address of the device you are configuring in the address bar on the browser (factory default IP address is 192.168.169.1) and then press Enter.

Your computer's IP address must be in the same subnet as the switch. For example, if the switch is using the factory default IP address (192.168.169.1.), your computer's IP address can be in the following range: 192.168.169.x (whereas x is a number from 2 to 254).

Switch settings (default): 192.168.169.1.

Connected device: 192.168.1.169.x (whereas x is a number from 2 to 254)

After a successful connection, the login window displays.

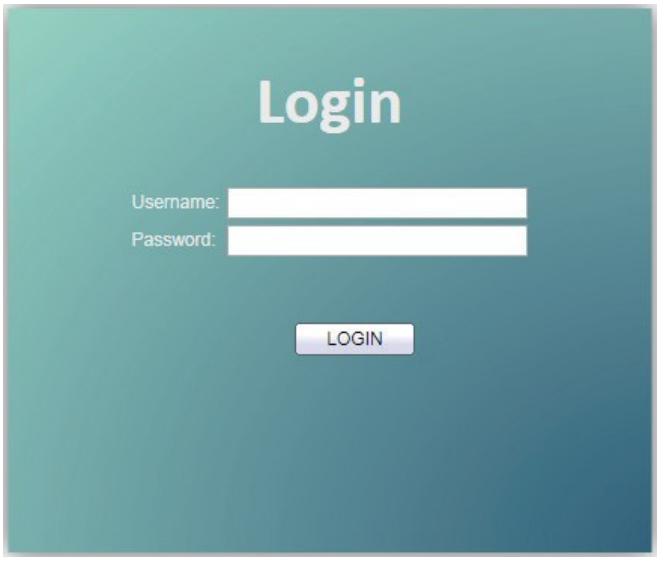


Figure 13 - Login Window

3.1.5. Logging In

To log in to the device configuration utility:

1. Open a browser window and enter the IP address in the browser's address bar.
2. In the Login Window, enter the default user ID (admin) and the default password (admin).

   If this is the first time that you logged on with the default user ID (admin) and the default password (admin). It is recommended that you change your password immediately. See "User Account" on page 113 for additional information.

   When the login attempt is successful, the **System Information** window displays.

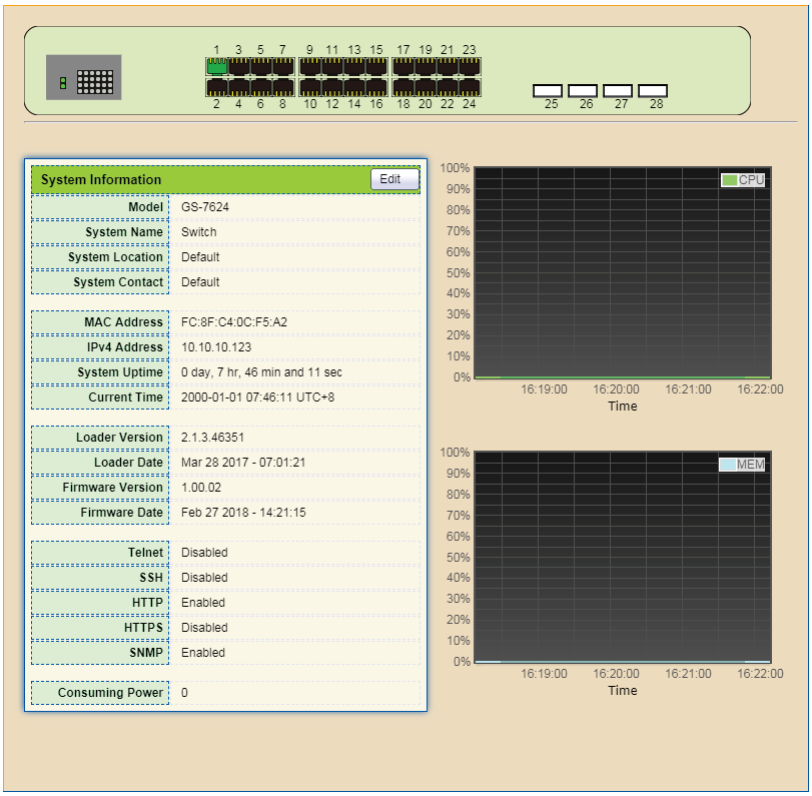


Figure 14 - Port Configuration

If you entered an incorrect username or password, an error message appears and the Login page remains displayed on the window. For further information about logging issues, please see the Launching the Configuration Utility section in the User Manual.

Logging Out

To logout, click Logout in the top right corner of any page. The system logs out of the device.

When a timeout occurs or you intentionally log out of the system, a message appears and the Login page appears. After you log in, the application returns to the initial page.

By default, the application logs out after ten minutes of inactivity.

4. Web-based Switch Configuration

The PoE smart switch software provides rich Layer 2 functionality for switches in your networks. This chapter describes how to use the web-based management interface (Web UI) to configure the switch's features.

For the purposes of this manual, the user interface is separated into four sections, as shown in the following figure:

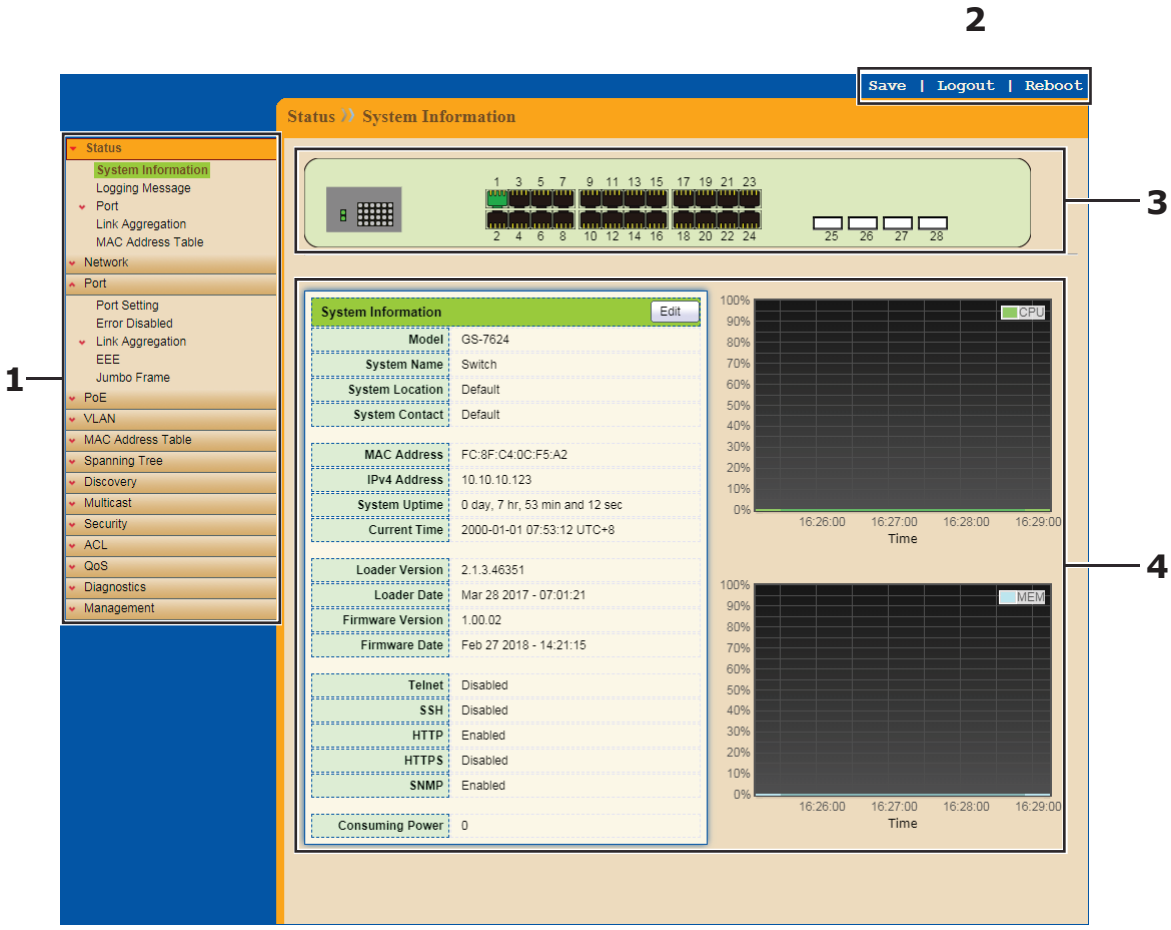


Figure 15 - User Interface

No.	Name	Description
1	Configuration menu	Navigation menu to locate specific switch functions.
2	Toolbar	Provides access to frequently used settings.
3	Current status	Ports highlighted in green represent an active port. Unlit ports indicate the port is inactive.
4	Configuration information	Edit specific function settings.

4.1. Status

4.1.1. System Information

The System Information menu provides status information such as Device ID, MAC address, IP Address and System Time.

To view the menu, navigate to Status > System Information.

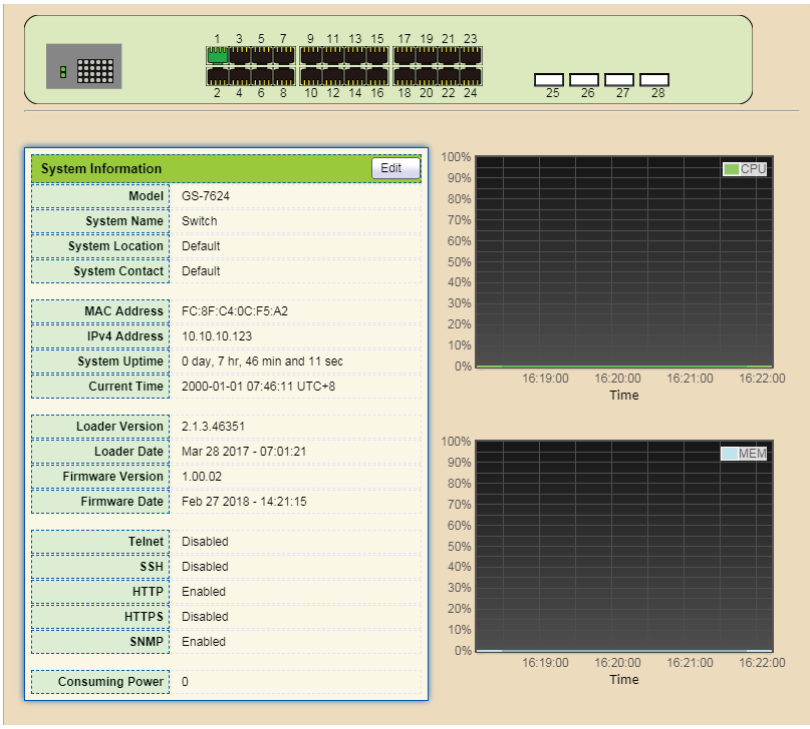


Figure 16 - Status > System Information

Item	Description
Model	Switch model name.
System Name	System name of the switch.
System Location	System location of the switch.
System Contact	System contact of the switch.
MAC Address	A unicast MAC address for which the switch has forwarding and/or filtering information. The format is a six-byte MAC address, with each byte separated by colons.
IPv4 Address	Switch IP address on the network.
System Uptime	Duration switch has been running since last reset or power off.
Current Time	Current date and time as reported by the system.
Loader Version	Current loader version of the switch.
Loader Date	Current loader build date of the switch.

Item	Description
Firmware Version	Current firmware version of the switch.
Firmware Date	Current firmware build date of the switch.
Telnet	Display the telnet function status.
SSH	Display the SSH function status.
HTTP	Display the HTTP function status.
HTTPS	Display the HTTPS function status.
SNMP	Display the SNMP function status.
Consuming Power	Display remaining power available or additional devices over PoE.
Edit	Click to edit the system information by entering the following data: • System Name • System Location • System Contact Apply: Click to save the information changes. Close: Click to return to the previous menu without saving any changes.

4.1.2. Logging Message

The page provides access to listed log notification and descriptions.

To view the menu, navigate to Status > Logging Message.

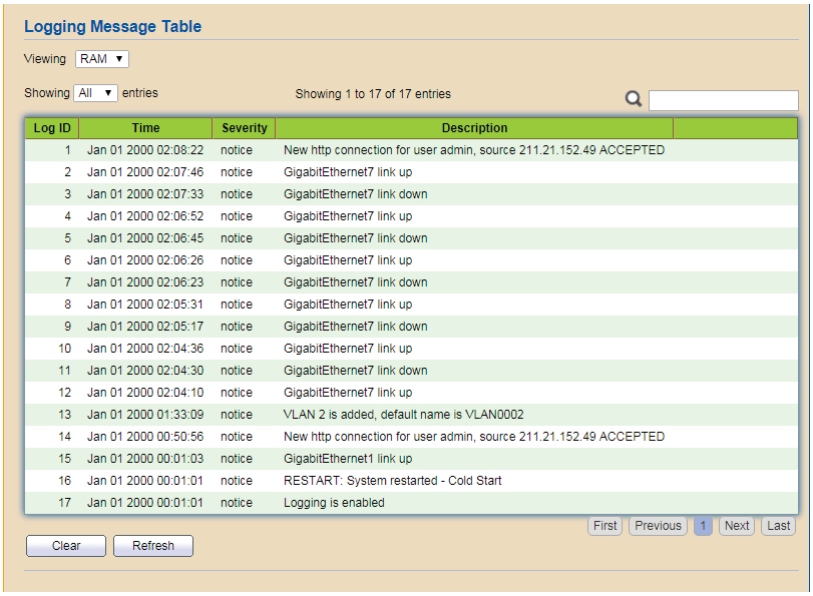


Figure 17 - Status > Logging Message

Item	Description
Viewing	Click the drop-down menu to select the type of log information to view. View RAM or Flash log entries saved as local log.
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.
Clear	Click to clear the logging message.
Refresh	Click to refresh the display.

4.1.3. Port

The Port menu provides access to port Statics, Error Disabled, and Bandwidth Utilization to monitor port function.

Statistics

To view the menu, navigate to Status > Port > Statistics.

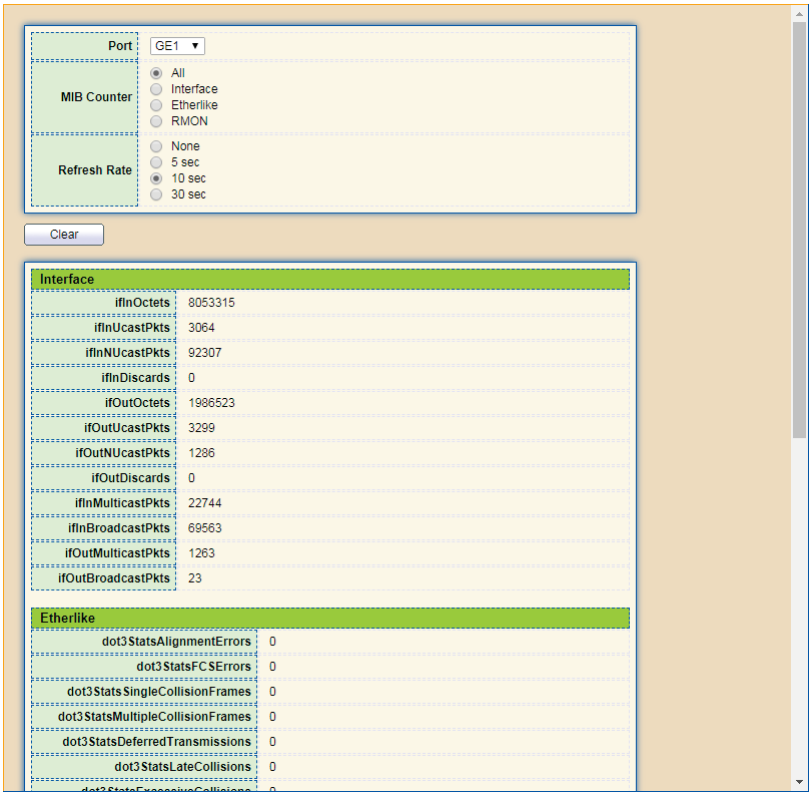


Figure 18 - Status > Port > Statistics

Item	Description
Port	Click the drop-down menu to select the port.
MIB Counter	Click the radio buttons to select MIB counter type for the selected port.
Refresh Rate	Click a radio button (None, 5, 10, 30 sec) to select refresh rate for the selected port.
Clear	Click to clear the MIB counters.

Error Disabled

The Error Disabled menu provides the function necessary to place a port in an error state – errors that may jeopardize stability to the switch or network.

Once a port is placed in an error state, an administrator must manually re-enable the port.

To view the menu, navigate to Status > Port > Error Disabled.

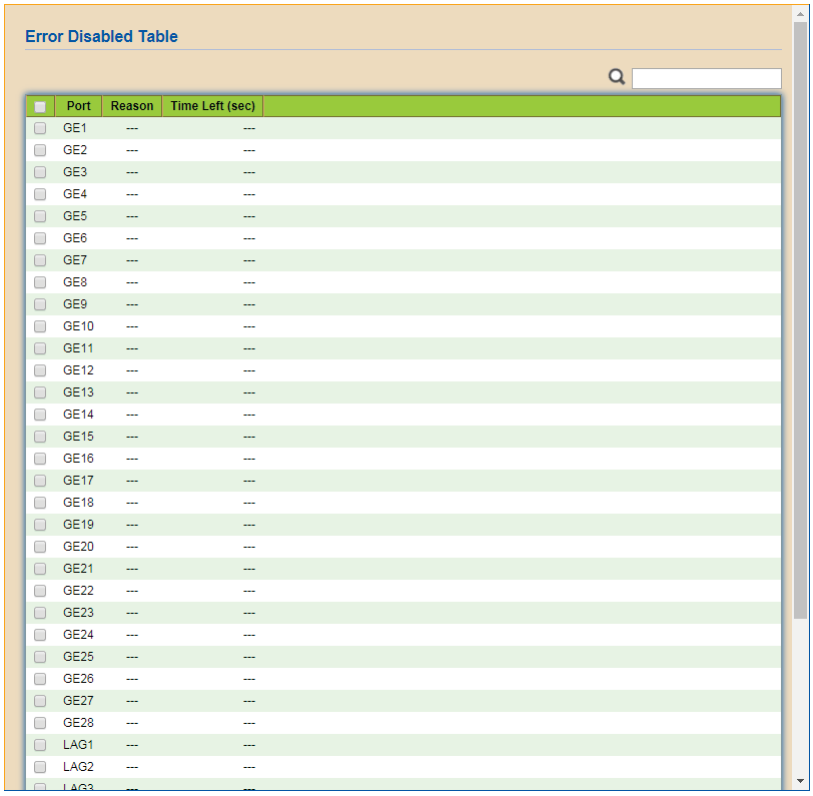


Figure 19 - Status > Port > Error Disabled

Item	Description
	Enter the keywords to use in the search function.
Refresh	Click to refresh the display.
Recover	Select the port and click Recover to recover the link from the error disabled status.

Bandwidth Utilization

The Bandwidth Utilization menu displays the network monitoring status performance of the switch.

To view the menu, navigate to Status > Port > Bandwidth Utilization.

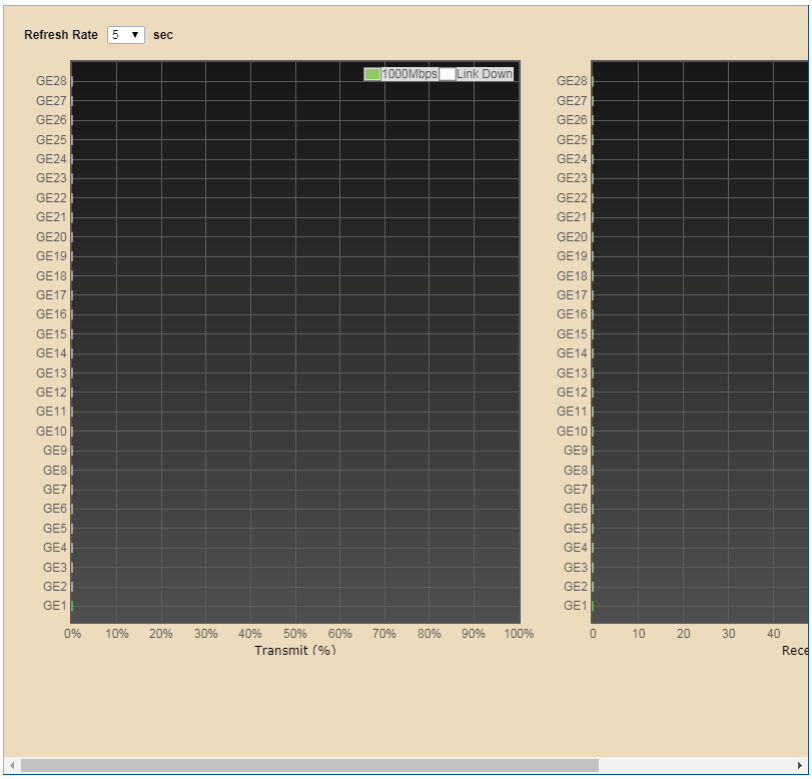


Figure 20 - Status > Port > Bandwidth Utilization

Item	Description
Refresh Rate	Click the drop-down menu to select the refresh rate time (2, 5, 10) in seconds.

4.1.4. Link Aggregation

The Link Aggregation menu displays the traffic loading usage among the specified ports.

To view the menu, navigate to Status > Link Aggregation.

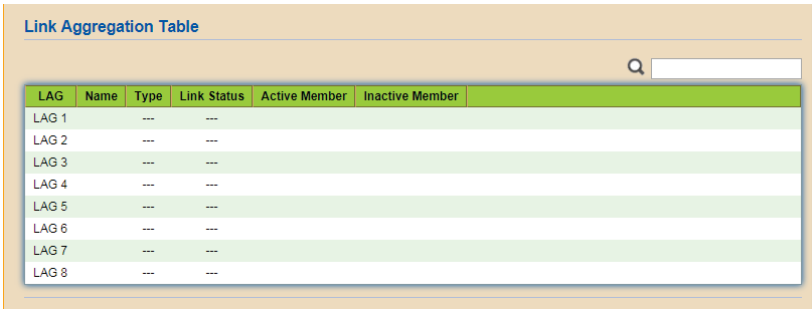


Figure 21 - Status > Link Aggregation

Item	Description
	Enter the keywords to use in the search function.

4.1.5. MAC Address Table

The MAC Address Table displays the listing of MAC addresses as they refer to a specific port.

To view the menu, navigate to Status > MAC Address Table.

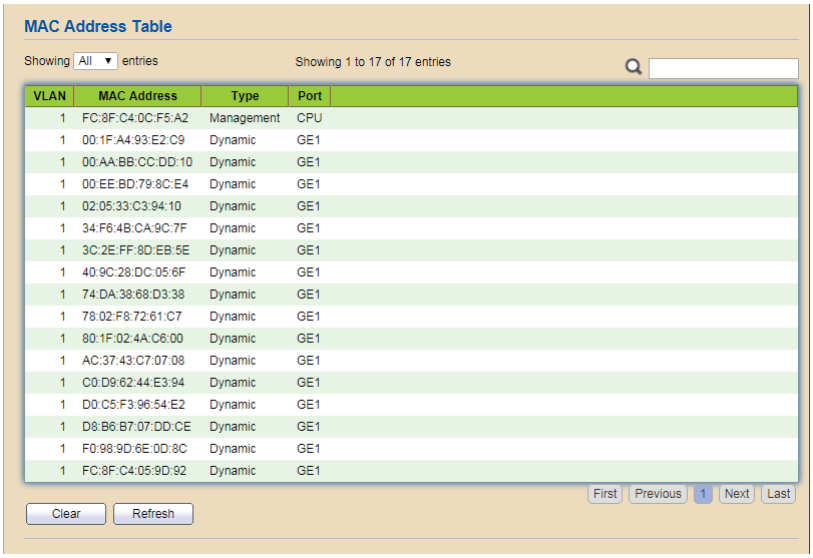


Figure 22 - Status > MAC Address Table

Item	Description
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.

Item	Description
Clear	Click to clear the current listed entries.
Refresh	Click to refresh the display.

4.2. Network

The Network menu provides access to the following functions for configuration: IPv4 Address, IPv6 Address, and Operational Status.

4.2.1. IP Address

The IP Address function enables the management of the device's IP and gateway (next hop) addresses for outgoing traffic.

To view the menu, navigate to Network > IP Address.

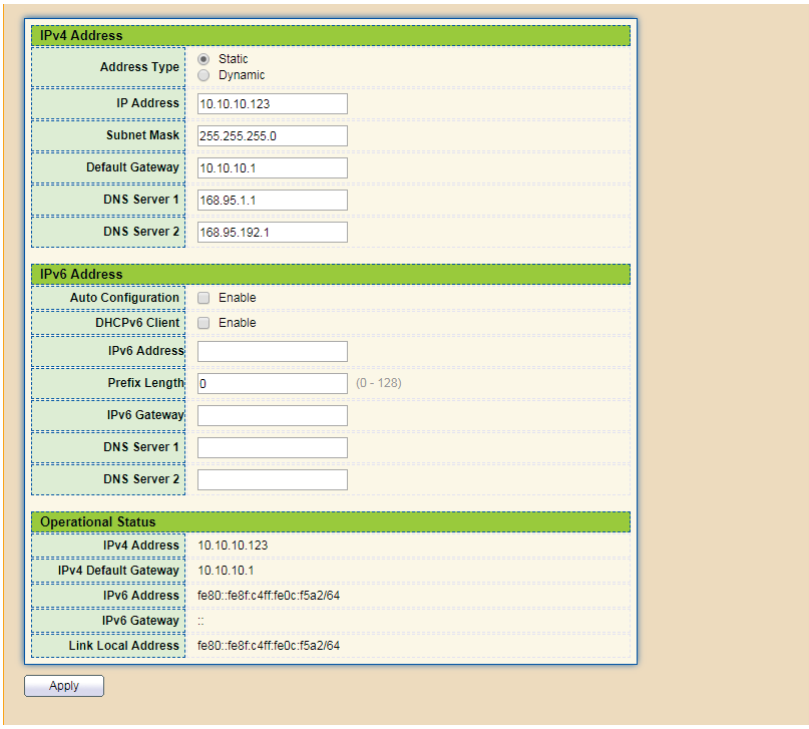


Figure 23 - Network > IP Address

Item	Description
IPv4 Address	
Address Type	Click the radio buttons to select the IP Address Setting mode: Static or Dynamic.
IP Address	Enter the variable to specify the IP address of the interface.
Subnet Mask	Enter the variable to specify the IP subnet mask for the interface.
Default Gateway	Enter the variable to specify the default gateway for the interface.

Item	Description
DNS Server 1	Enter the variable to specify the DNS server 1 for the interface.
DNS Server 2	Enter the variable to specify the DNS server 2 for the interface.
IPv6 Address	
Auto Configuration	Click the radio button to enable the IPv6.
DHCPv6 Client	Click the radio button to enable the DHCPv6 client function.
IPv6 Address	Enter the variable to specify the IPv6 address of the interface.
Prefix Length	Enter the variable to specify the IPv6 prefix Length.
IPv6 Gateway	Enter the variable to specify the default gateway for the interface.
DNS Server 1	Enter the variable to specify the DNS server 1 for the interface.
DNS Server 2	Enter the variable to specify the DNS server 2 for the interface.
Operational Status	
IPv4 Address	Display the assigned IPv4 address of the switch.
IPv4 Default Gateway	Display the assigned IPv4 gateway of the switch.
IPv6 Address	Display the assigned IPv6 address of the switch.
IPv6 Gateway	Display the assigned IPv6 gateway of the switch.
Link Local Address	Display the link local address valid only within the network segment (link).
Apply	Click to save the values and update the screen.

4.2.2. System Time

The System Time function enables the management of the system time and date on the device using automatic configuration, such as SNTP or a localhost (computer), or manual configuration settings.

To view the menu, navigate to Network > System Time.

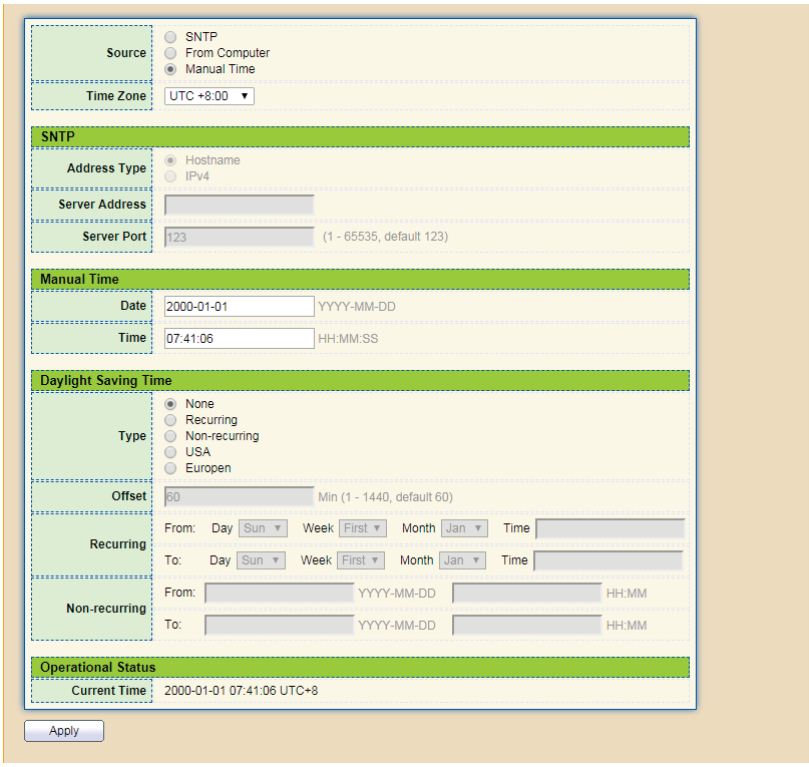


Figure 24 - Network > System Time

Item	Description
Source	Click the radio buttons to select the system time source.
Time Zone	Click the drop-down menu to select a system time zone.
SNTP	
Address Type	Click the radio buttons to select the SNTP address type.
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.
Server Port	Enter the port on the server to which SNTP requests are to be sent. Allowed range is 1 - 65535 (default: 123).
Manual Time	
Date	Enter to set the local date of the system.
Time	Enter to set the local time of the system.

Item	Description
Daylight Saving Time	
Type	Click the radio buttons to select the daylight saving time type.
Offset	Enter the offsetting variable in seconds to adjust for daylight saving time.
Recurring	Click the drop-down menu to designate the start date and time/end date and time for daylight saving time.
Non-recurring	Click the drop-down menu to designate the start date and time/end date and time for a non-recurring daylight saving time event.
Operational Status	
Current Time	Current date and time as reported by the system.
Apply	Click to save the values and update the screen.

4.3. Port

The Port menu provides access to port configuration settings such as: Port Setting, Error Disabled, Link Aggregation, EEE, and Jumbo Frame.

4.3.1. Port Setting

Use the page to configure settings for the switch ports, trunk, Layer 2 protocols and other switch features.

To view the menu, navigate to Port > Port Setting.

Figure 25 - Port > Port Setting

Item	Description
	Enter the keywords to use in the search function.

Item	Description
Edit	Select a port entry and click the Edit button to configure the following settings: • Description: Enter a string text to describe the device. • State: Tick the radio button to enable/disable the device state setting. • Speed: Click a radio button to select the device speed (Auto, Auto-10M, Auto-100M, Auto-1000M, Auto-10/100M, 10M, 100M, 1000M) • Duplex: Tick a radio button to select the communication signal type (Auto, Full, Half). • Flow control: Tick a radio button to select the data transmission type (Auto, Enable, Disable). Apply: Click to save the configuration settings. Close: Click to return to the previous menu without saving the configuration settings.

4.3.2. Error Disabled

The Error Disabled menu allows for the configuration of the Error Disable function.

To view the menu, navigate to Port > Error Disabled.

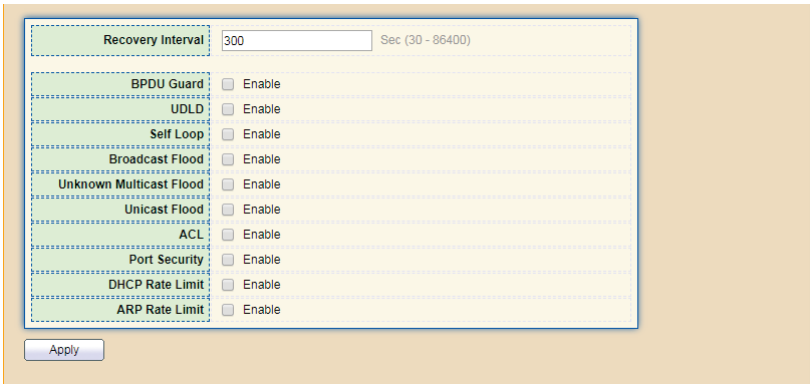


Figure 26 - Port > Error Disabled

Item	Description
Recovery Interval	Enter the variable to set the recovery interval time.
BPDU Guard	Click the radio button to recover the port being blocked by BPDU Guard after the time set in Recovery Interval.
UDLD	Click the radio button to recover the port being blocked by UDLD after the time set in Recovery Interval.
Self Loop	Click the radio button to recover the port being blocked by self loop after the time set in Recovery Interval.
Broadcast Flood	Click the radio button to recover the port being blocked by broadcast flood after the time set in Recovery Interval.

Item	Description
Unknown Multicast Flood	Click the radio button to recover the port being blocked by unknown multicast flood after the time set in Recovery Interval.
Unicast Flood	Click the radio button to recover the port being blocked by unicast flood after the time set in Recovery Interval.
ACL	Click the radio button to recover the port being blocked by ACL after the time set in Recovery Interval.
Port Security	Click the radio button to recover the port being blocked by port security after the time set in Recovery Interval.
DHCP Rate Limit	Click the radio button to recover the port being blocked by DHCP rate limit after the time set in Recovery Interval.
ARP Rate Limit	Click the radio button to recover the port being blocked by ARP rate limit after the time set in Recovery Interval.
Apply	Click to save the values and update the screen.

4.3.3. Link Aggregation

The Link Aggregation menu provides configuration for link aggregation settings: group, port settings, LACP.

Group

To view the menu, navigate to Port > Link Aggregation > Group.

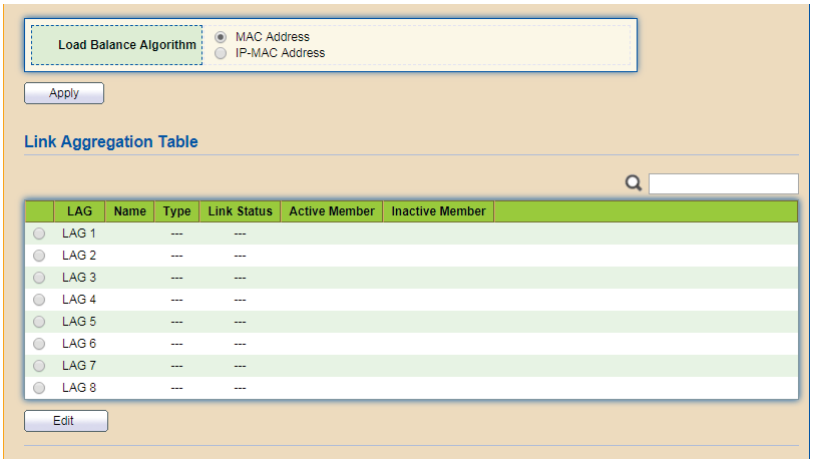


Figure 27 - Port > Link Aggregation > Group

Item	Description
Load Balance Algorithm	Click the radio buttons to select the Load balance algorithm. • MAC Address: Aggregated group will balance the traffic based on different MAC addresses. Therefore, the packets from different MAC addresses will be sent to different links. • IP-MAC Address: Aggregated group will balance the traffic based on MAC addresses and IP addresses. Therefore, the packets from same MAC addresses but different IP addresses will be sent to different links.
Apply	Click to save the values and update the screen.
	Enter the keywords to use in the search function.
Edit	Click to edit the link aggregation settings by entering the following data: • Name • Type • Member

Port Setting

To view the menu, navigate to Port > Link Aggregation > Port Setting.

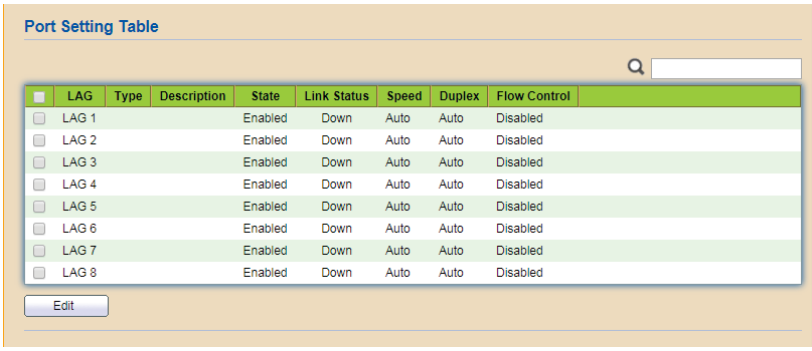


Figure 28 - Port > Link Aggregation > Port Setting

Item	Description
	Enter the keywords to use in the search function.
Edit	Click to edit the port settings by entering the following data: • Description • State • Speed • Flow Control

LACP

To view the menu, navigate to Port > Link Aggregation > LACP.

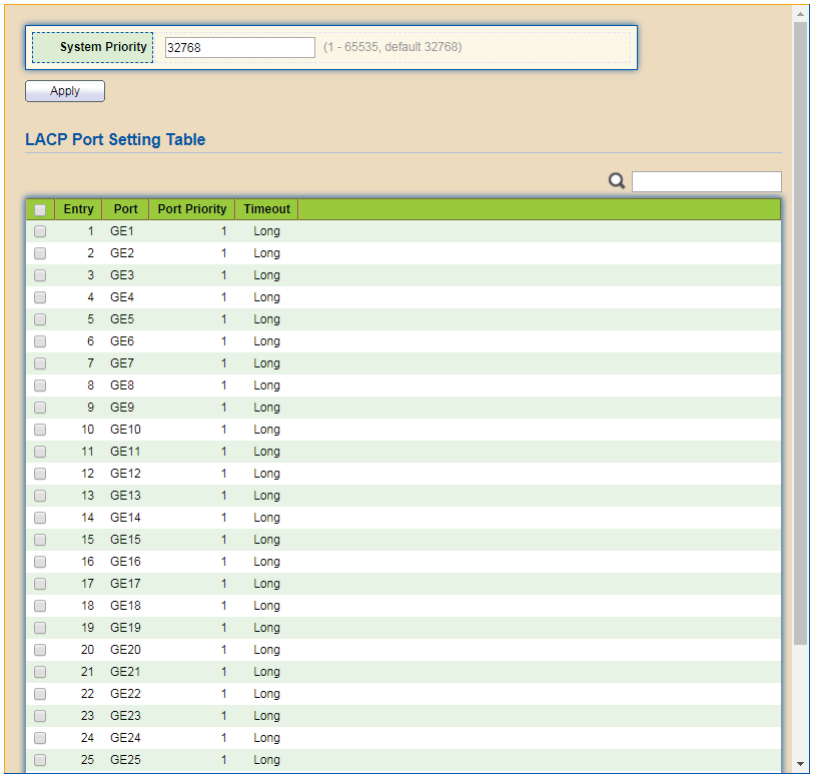


Figure 29 - Port > Link Aggregation > LACP

Item	Description
System Priority	Enter the variable to determine which switch (local or remote) on the LAG connection is able to decide LACP activities. The priority is defined by the number variable. A low number indicates a higher priority. A switch defined to have the highest priority gains the authority to define port participation in LAG at a given time.
Apply	Click to save the values and update the screen.
	Enter the keywords to use in the search function.
Edit	Click to edit the LACP port settings by entering the following data: • Port Priority • Timeout

4.3.4. EEE

The Energy Efficient Ethernet (EEE) menu reduces the power consumption during periods of low link utilization. The functions saves energy by putting part of the transmission circuit into low power mode when the link is idle.

To view the menu, navigate to Port > EEE.

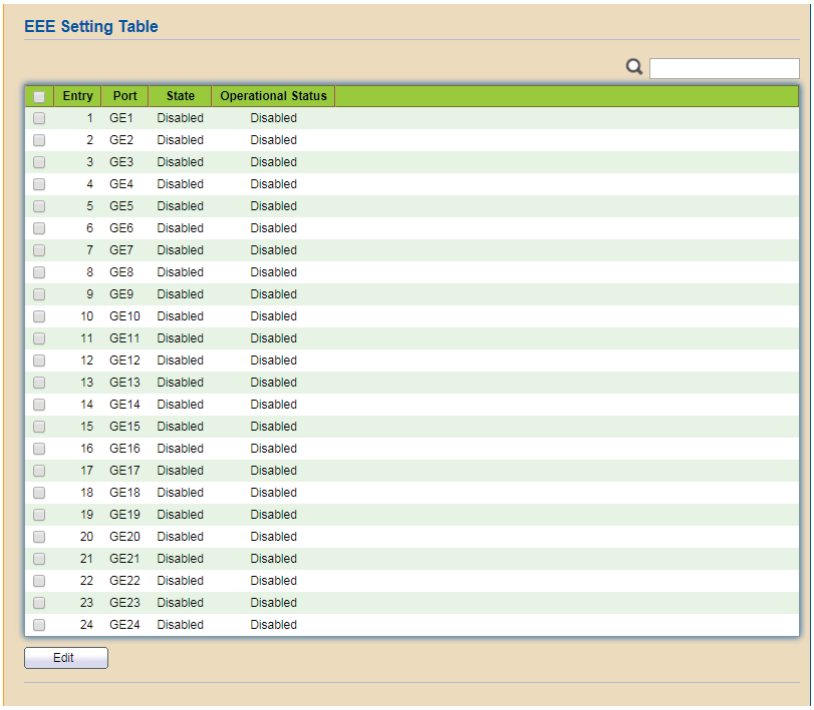


Figure 30 - Port > EEE

Item	Description
	Enter the keywords to use in the search function.
Edit	Click to enable or disable the EEE setting on the selected port. • Select a port and click Edit to enter the Setting menu. • Tick Enable in the State menu and click Apply to enable EEE on the port and save the settings. • Alternatively, click close to return to the previous menu without saving.

4.3.5. Jumbo Frame

Jumbo Frame is an Ethernet frame with a payload greater than the maximum transmission unit (MTU) of 1,500 bytes (standard). The Jumbo Frame menu provides configuration access to allow for local area networks that support at least 1 Gbps and as large as 9,000 bytes.

To view the menu, navigate to Port > Jumbo Frame.

Figure 31 - Port > Jumbo Frame

Item	Description
Jumbo Frame	Tick Enable to enable Jumbo Frame. Enter an MTU value between 1518 - 10000 (default: 1522).
Apply	Click to save the configuration.

4.4. PoE

Devices with PoE support are designed with PoE-capable ports capable of automatically supplying power to connected devices when the switch detects an absence of power on the circuit.

Supported device:

- an IEEE 802.3af-compliant powered device

Powered devices can receive redundant power when connected to a PoE-enabled port and to an AC power source. The devices do not receive redundant power when they are only connected to the PoE port.

4.4.1. Global Setting

To view the menu, navigate to PoE > Global Setting.

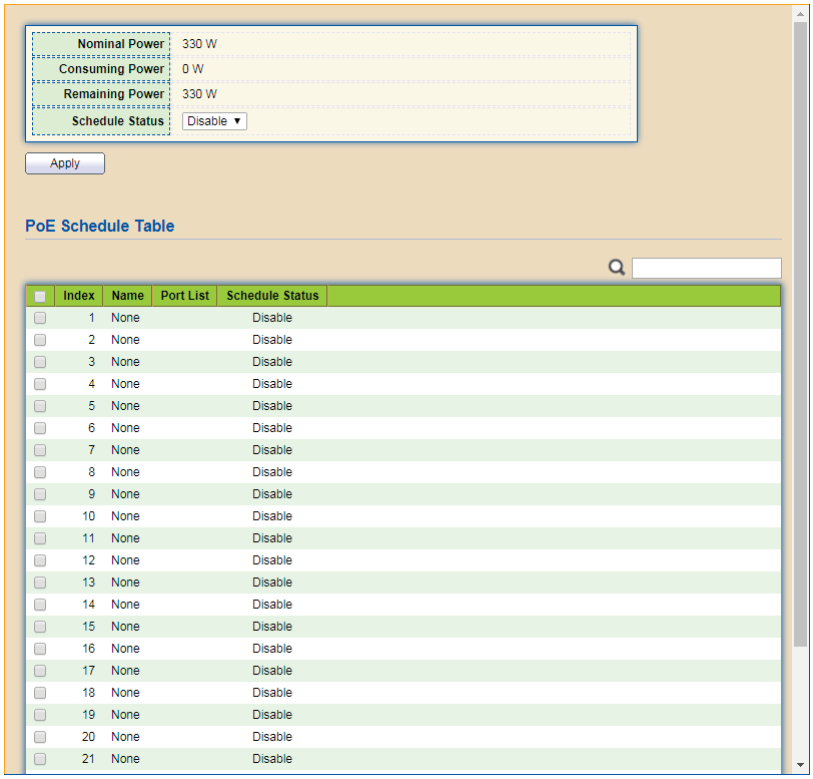


Figure 32 - PoE > Global Setting

Item	Description
Nominal Power	Specifies the design voltage and power values for the device.
Consuming Power	Display current power being consumed by all devices over PoE.
Remaining Power	Display remaining power that can be supplied to additional devices over PoE.

Item	Description
Schedule Status	Click the drop-down menu to enable or disable the Schedule Status. If enabled, a defined Time Range setting can be selected and applied to the port, see Edit in the following.
Apply	Click to save the values and update the screen.
	Enter the keywords to use in the search function.
Edit	Click to apply a Time Range setting: • Select a port and click Edit. • In the PoE Schedule Edit menu, tick Enable in Schedule Status. • In the Name drop-down menu, select a pre-defined Time Range setting. • In the Port List pane, select a specific port or click Enable to select all ports to apply the setting. Click Disable to unselect all ports. • Click Apply to save the new settings. • Alternatively, click Close to return to the previous menu without saving.

4.4.2. Priority Setting

The Priority Setting menu provides configuration for a PoE port to have a high power priority setting. In the event where there isn't sufficient power for all the PoE ports, available power is directed to the higher priority ports, while lower priority ports are shut down as needed.

To view the menu, navigate to PoE > Priority Setting.

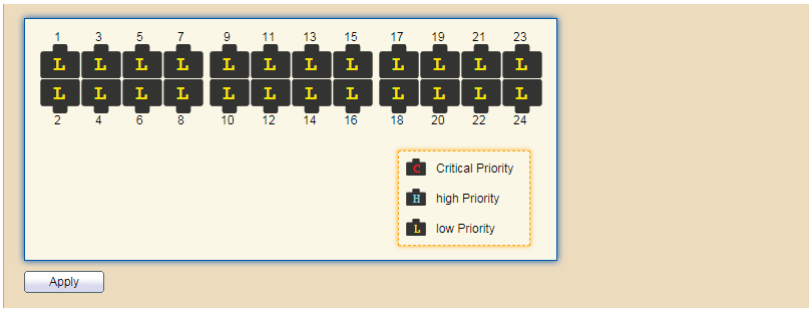


Figure 33 - PoE > Priority Setting

Item	Description
Ports	Click the ports to select priority for the PoE device. • L (Low): Set PoE device to low priority connection. • H (High): Set PoE device to high priority connection. • C (Critical): Set PoE device to highest priority connection.
Apply	Click to save the values and update the screen.

4.4.3. Power Limit

The Power Limit menu provides configuration to set the amount of power in milliwatts to the powered device connected to the selected port.

To view the menu, navigate to PoE > Power Limit.

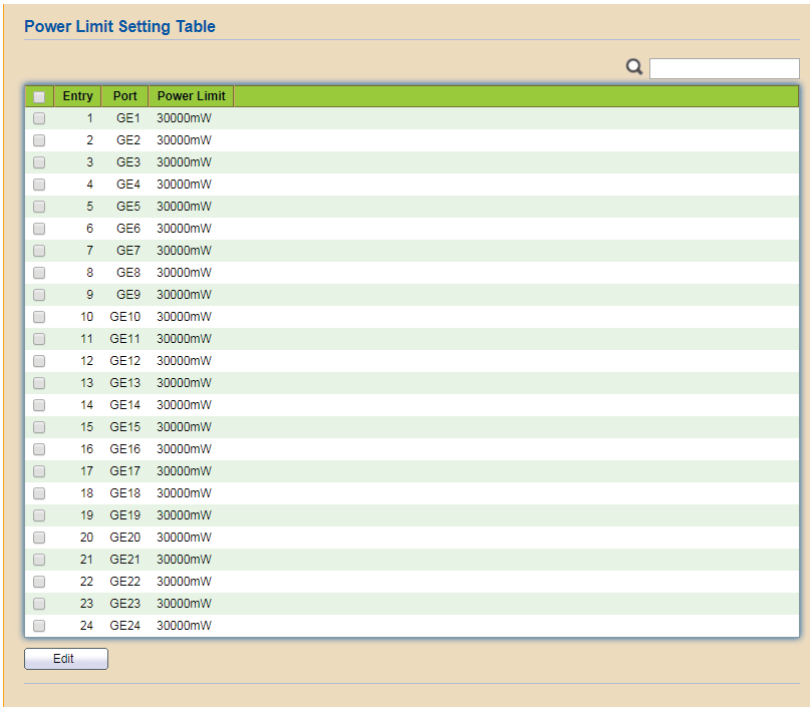


Figure 34 - PoE > Power Limit

Item	Description
	Enter the keywords to use in the search function.
Edit	Click to set a power limit setting: • Select a port and click Edit. • In the Power Limit Setting menu, enter a Power Limit variable: 0 - 30000 (default: 30000) in mW. • Click Apply to save the new settings. • Alternatively, click Close to return to the previous menu without saving.

4.4.4. Power Show

The Power Show menu provides the setting to enable or disable the viewing of the power function for each port.

To view the menu, navigate to PoE > Power Show.

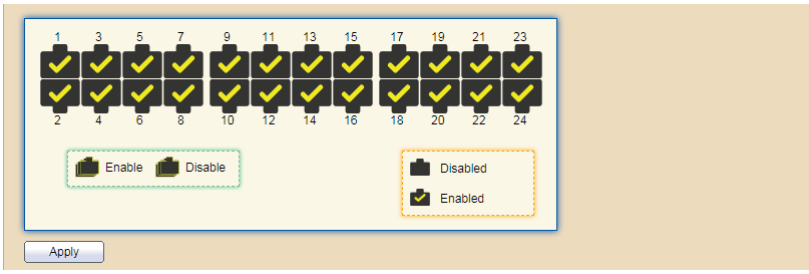


Figure 35 - PoE > Power Show

Item	Description
Ports	Click the ports to enable or disable power show for the PoE device. • Unselected: Disable power show. • Selected: Enable power show.
Apply	Click to save the values and update the screen.

4.5. VLAN

The virtual LAN (VLAN) menu provides functionality to divide the network into separate logical areas. A switch port belonging to a VLAN can receive unicast, broadcast, and multicast packets. Each VLAN is considered a logical network.

4.5.1. VLAN

In a switched network, a VLAN is a group of end stations that is logically segmented by either function, definition, or application, without regard to a user's physical location.

The VLAN menu provides the functionality to create, configure, set membership, and configure VLAN port settings.

Create VLAN

To view the menu, navigate to VLAN > VLAN > Create VLAN.

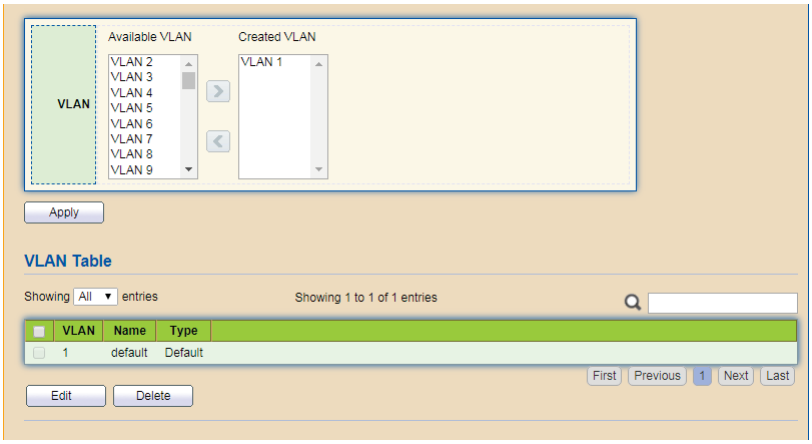


Figure 36 - VLAN > VLAN > Create VLAN

Item	Description
	Click to add a selected VLAN into a group.
	Click to remove an entry from the VLAN group. The default VLAN entry is included in the group by default. It cannot be deleted from the group.
Apply	Click to save the values and update the screen.
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.

Item	Description
Edit	An existing VLAN entry must be available before the Edit function can be selected. To modify a VLAN entry: • Select a VLAN entry and click Edit. • In the Edit VLAN Name menu, enter a text string to define the VLAN entry. • Click Apply to save the new settings. • Alternatively, click Close to return to the previous menu without saving.
Delete	To delete a VLAN entry: • Select a VLAN entry and click Delete. The entry is deleted and the VLAN Table refreshes to update the available entries.  When a VLAN is deleted, ports associated to that VLAN shut down, stopping traffic and dropping packets flowing to it.

VLAN Configuration

The VLAN Configuration menu provides the functionality to select and configure available ports to a defined VLAN group.

To view the menu, navigate to VLAN > VLAN > VLAN Configuration.

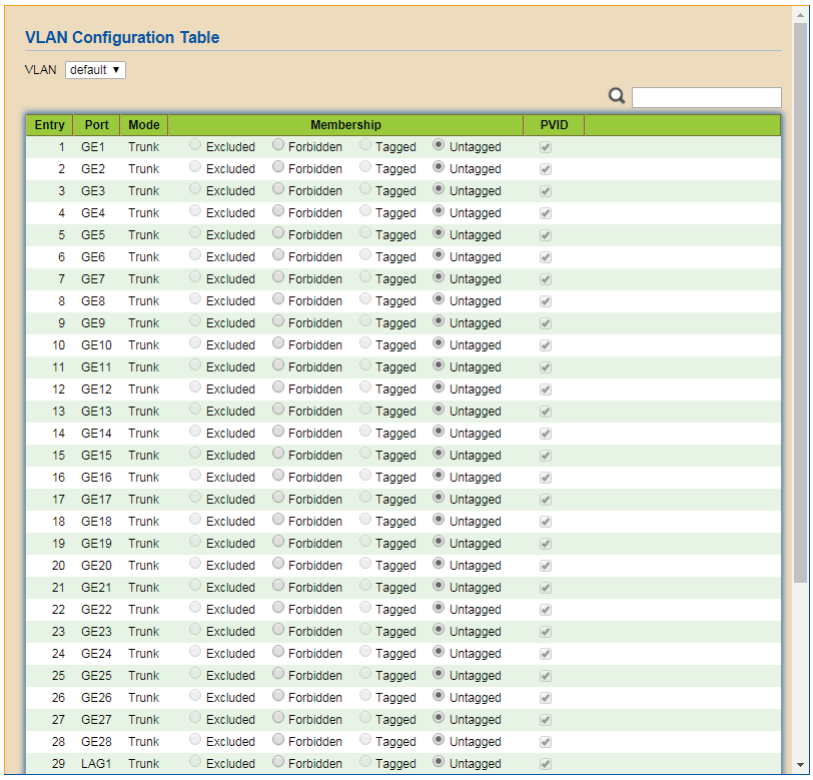


Figure 37 - VLAN > VLAN > VLAN Configuration

Item	Description
VLAN	Click the drop-down menu to select a defined VLAN, see “Create VLAN” on page 43. • Once selected, set the membership settings to associate to the port under the VLAN. • Click Apply to save the settings changes.
	Enter the keywords to use in the search function.
Membership	For each port, select the membership type to apply, see the following: • Excluded: Designate port as not a member of the VLAN. • Forbidden: Port is not able to join the VLAN group. • Tagged: The interface is a tagged member of the VLAN group. All packets are tagged containing the VLAN information and then forwarded. • Untagged: The interface is an untagged member of the VLAN group. Packets forwarded by the interface do not acquire a tag.
Apply	Click to save the values and update the VLAN definition.

Membership

To view the menu, navigate to VLAN > VLAN > Membership.

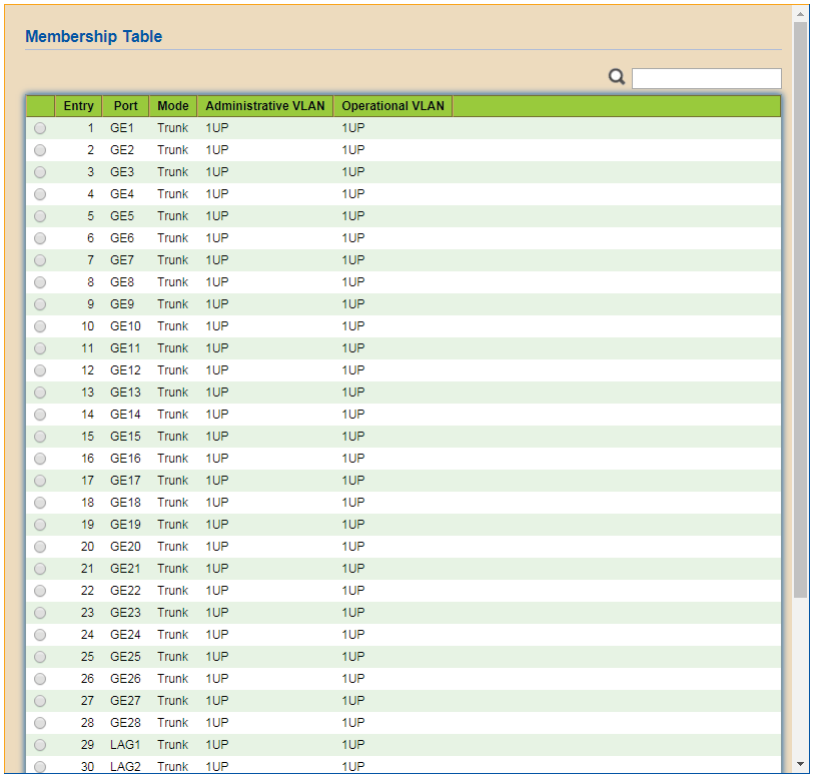


Figure 38 - VLAN > VLAN > Membership

Item	Description
	Enter the keywords to use in the search function.
Edit	Select an entry and click Edit the membership settings. In the Edit Port Setting menu, select a membership entry and click Select  to add the entry to the group. • Select a membership type (Forbidden, Tagged, Untagged). • Click Apply to save the configuration changes. • Alternatively, click Close to return to the previous menu without saving the changes.

Port Setting

The Port Setting menu provides configuration function for each selected port allowing setting changes to mode, PVID, frame type, and ingress filtering.

To view the menu, navigate to VLAN > VLAN > Port Setting.

Figure 39 - VLAN > VLAN > Port Setting

Item	Description
	Enter the keywords to use in the search function.
Edit	Select an entry and click Edit to modify the membership settings. In the Edit Port Setting menu, configure the following: • Mode: Hybrid, Access, Trunk. • PVID: Enter a value (1 - 4094) to define the virtual LAN segment for the port. • Accept Frame Type: All, Tag Only, Untag Only • Ingress Filtering: Tick to enable or disable the filtering function. • Click Apply to save the configuration changes. • Alternatively, click Close to return to the previous menu without saving the changes.

4.5.2. Voice VLAN

The Voice VLAN function enables the IP voice traffic access from an IP phone. When connected to an Internet phone, the device can receive voice traffic with Layer 3 IP precedence and Layer 2 class of service (CoS) values.

Property

To view the menu, navigate to VLAN > Voice VLAN > Property.

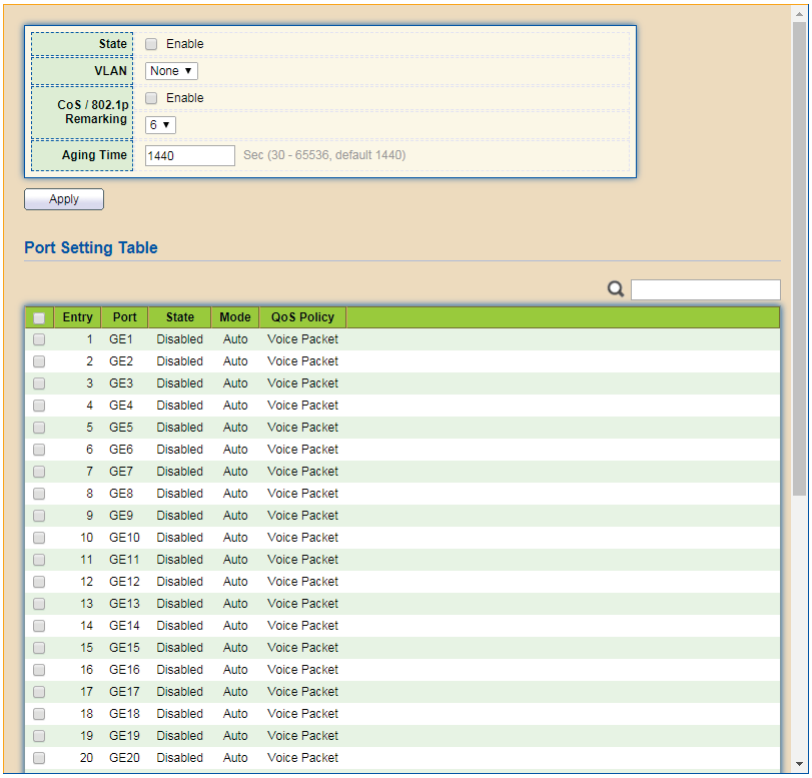


Figure 40 - VLAN > Voice VLAN > Property

Item	Description
State	Click the radio button to enable voice VLAN.
VLAN	Click the drop-down menu to select a defined VLAN or None.
CoS / 802.1p Remarking	Click the radio button to enable 802.1p remarking. If enabled, click the drop-down menu to specify the CoS/802.1p to use to identify ingress VoIP packet tagging.
Aging Time	Enter a value in seconds (30 - 65536, default: 1440) to define the VLAN aging time. If the time value since the last telephony MAC address was aged out exceeds the define aging time, the port is removed from the voice VLAN.
Apply	Click to save the values and update the screen.
	Enter the keywords to use in the search function.

Item	Description
Edit	Select an entry and click Edit the Property Port settings. In the Edit Port Setting menu, configure the following: • State: Tick to enable or disable the state mode. • Mode: Select either Auto or Manual. • QoS Policy: Select Voice Packet or All to set the QoS attributes. Voice packet attributes are applied only from voice packets. The All policy applies QoS attributes on to all packets classified to the voice VLAN.

Voice OUI

To view the menu, navigate to VLAN > Voice VLAN > Voice OUI.

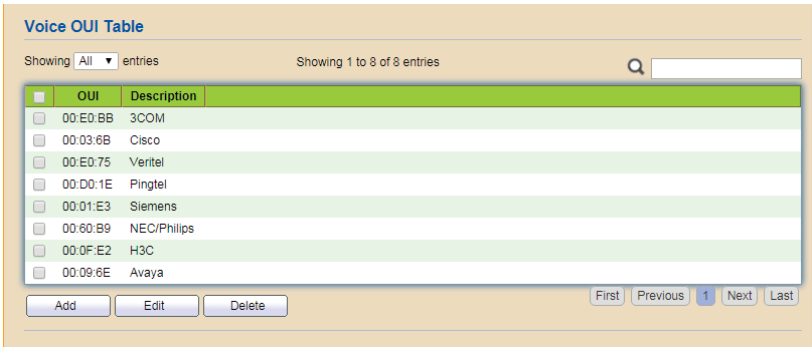


Figure 41 - VLAN > Voice VLAN > Voice OUI

Item	Description
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.
Add	Click to add a new voice OUI by entering the following data: • OUI • Description
Edit	Click to edit the voice OUI settings by entering the following data: • Description
Delete	Click to delete the desired entries.

4.5.3. MAC VLAN

MAC Group

To view the menu, navigate to VLAN > MAC VLAN > MAC Group.

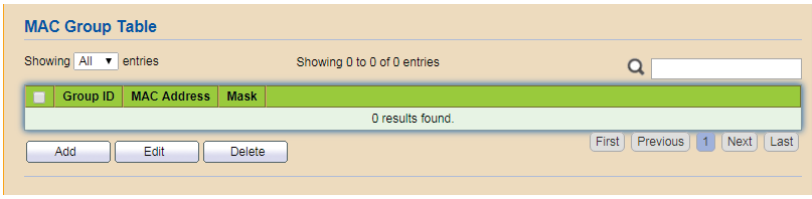


Figure 42 - VLAN > MAC VLAN > MAC Group

Item	Description
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.
Add	Click to add a new MAC group by entering the following data: • Group ID • MAC Address • Mask
Edit	Click to edit the MAC group settings by entering the following data: • MAC Address • Mask
Delete	Click to delete the desired entries.

Group Binding

To view the menu, navigate to VLAN > MAC VLAN > Group Binding.

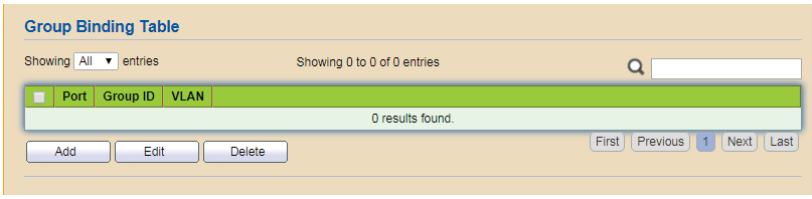


Figure 43 - VLAN > MAC VLAN > Group Binding

Item	Description
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.
Add	Click to add a new group binding by entering the following data: • Port • Group ID • VLAN
Edit	Click to edit the group binding settings by entering the following data: • Group ID • VLAN
Delete	Click to delete the desired entries.

4.6. MAC Address Table

4.6.1. Dynamic Address

To view the menu, navigate to MAC Address Table > Dynamic Address.

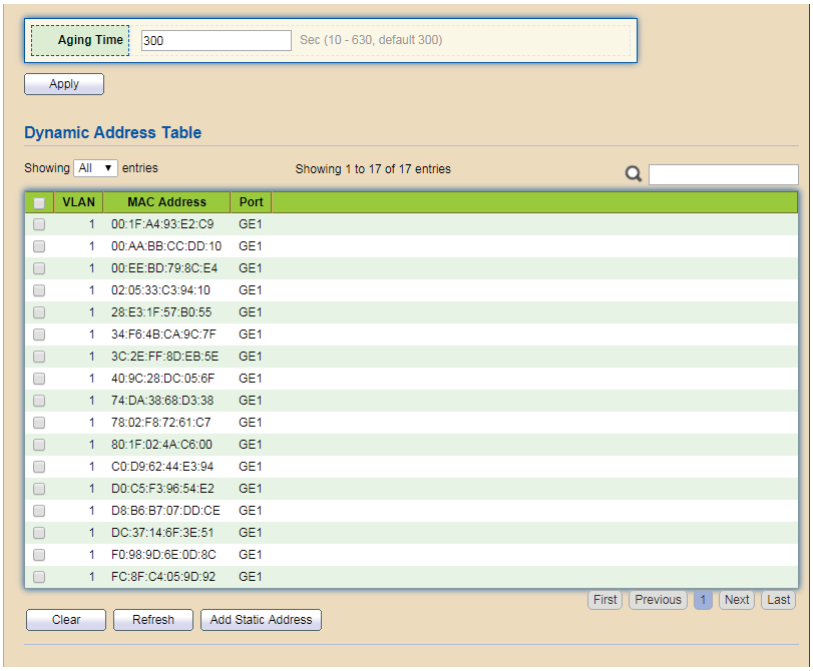


Figure 44 - MAC Address Table > Dynamic Address

Item	Description
Aging Time	Enter the variable to set the dynamic MAC address aging out value.
Apply	Click to save the values and update the screen.
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.
Clear	Click to clear the MAC address table.
Refresh	Click to refresh the display.
Add Static Address	Click to add the desired ports into the static MAC table.

4.6.2. Static Address

To view the menu, navigate to MAC Address Table > Static Address.

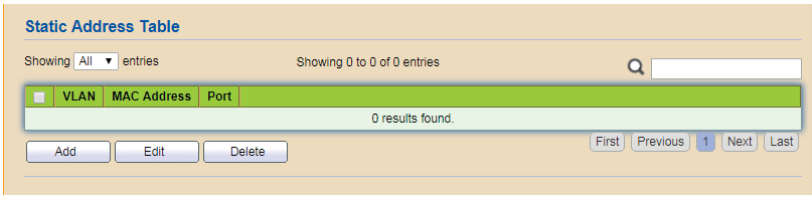


Figure 45 - MAC Address Table > Static Address

Item	Description
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.
Add	Click to add a new static address by entering the following data: • MAC Address • VLAN • Port
Edit	Click to edit the static address settings by entering the following data: • VLAN • Port
Delete	Click to delete the desired entries.

4.6.3. Filtering Address

To view the menu, navigate to MAC Address Table > Filtering Address.

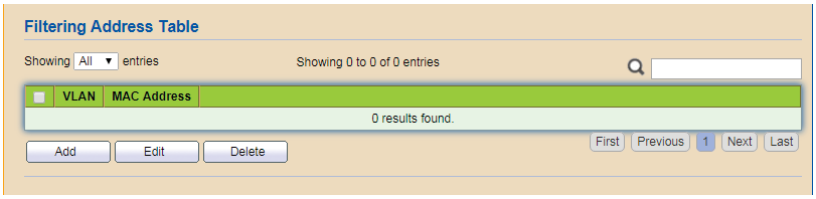


Figure 46 - MAC Address Table > Filtering Address

Item	Description
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.
Add	Click to add a new filtering address by entering the following data: • MAC Address • VLAN
Edit	Click to edit the filtering address settings by entering the following data: • VLAN
Delete	Click to delete the desired entries.

4.7. Spanning Tree

4.7.1. Property

To view the menu, navigate to Spanning Tree > Property.

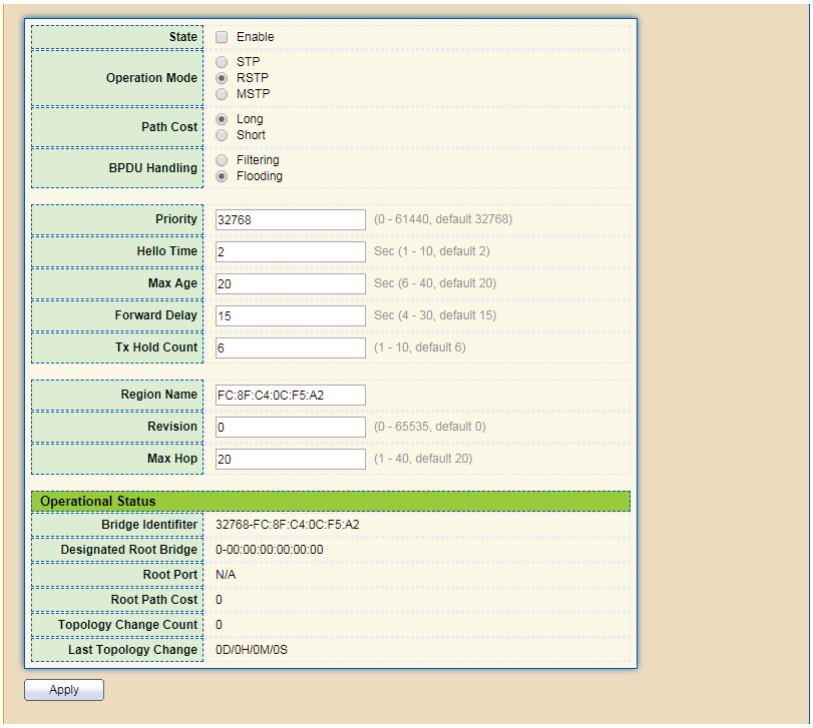


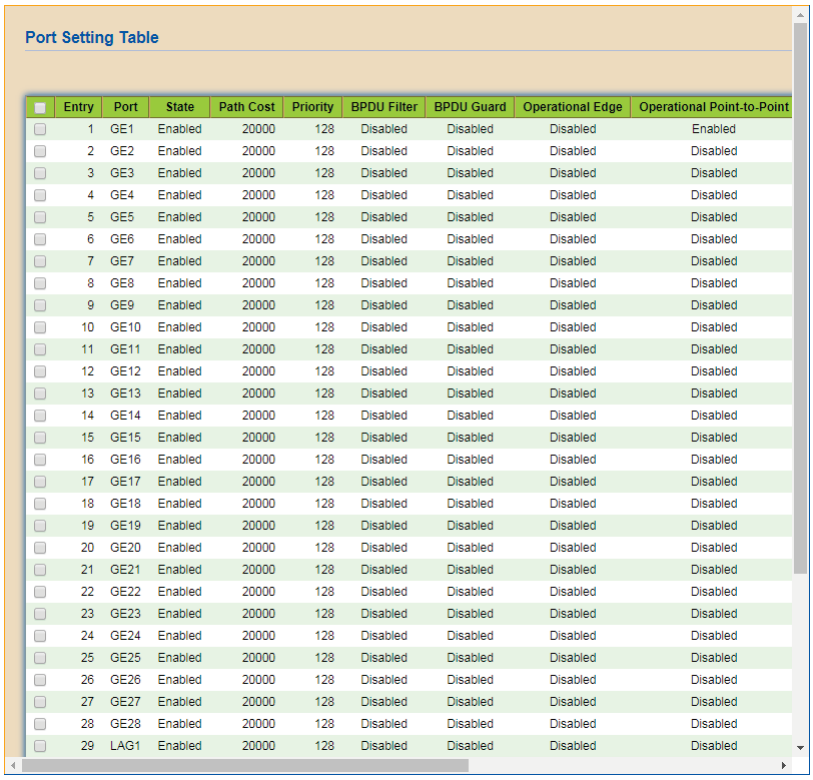
Figure 47 - Spanning Tree > Property

Item	Description
State	Click the radio button to enable the spanning tree protocol function.
Operation Mode	Click the radio buttons to set the operating mode of spanning tree (STP). • STP: Enable the Spanning Tree (STP) operation. • RSTP: Enable the Rapid Spanning Tree (RSTP) operation. • MSTP: Enable the Multiple Spanning Tree Protocol (MSTP) operation.
Path Cost	Click the radio buttons to specify the path cost method. • Long: Specifies that the default port path costs are within the range: 1 - 200000000. • Short: Specifies that the default port path costs are within the range: 1 - 65535.
BPDU Handling	Click the radio buttons to specify the BPDU forward method when the STP is disabled. • Filtering: Filter the BPDU when STP is disabled. • Flooding: Flood the BPDU when STP is disabled.

Item	Description
Priority	Enter the variable to specify the bridge priority. It ensures the probability that the switch is selected as the root bridge, and the lower value has the higher priority for the switch to be selected as the root bridge of the topology.
Hello Time	Enter the variable to specify the STP hello time in seconds to broadcast its hello message to other bridge by Designated Ports.
Max Age	Enter the variable to specify the time interval in seconds for a switch to wait for the configuration messages, without attempting to redefine its own configuration.
Forward Delay	Enter the variable to specify the STP forward delay time, which is the amount of time that a port remains in the Listening and Learning states before it enters the Forwarding state.
Tx Hold Count	Enter the variable to specify the tx-hold-count used to limit the maximum numbers of packets transmission per second.
Region Name	A spanning tree protocol allows for the interconnection of same configured regions. Enter the defined name spanning-tree configuration name.
Revision	Enter the value designating the spanning tree configuration revision (0 - 65535, default: 0).
Max Hop	Enter a value to define the maximum number of hops before the setting (0 - 40, default: 20).
Operational Status	
Bridge Identifier	Display the unique identifier to distinguish this device.
Designated Root Bridge	Display the root switch for the traffic in the assigned VLAN region.
Root Port	Display the root port identifier for the region.
Root Path Cost	Display the path cost through the defined region.
Topology Change Count	Display the counter identifying the number of topology changes.
Last Topology Change	Display the last identifying topology change counter.
Apply	Click to save the values and update the screen.

4.7.2. Port Setting

To view the menu, navigate to Spanning Tree > Port Setting.



Port Setting Table

Entry	Port	State	Path Cost	Priority	BPDU Filter	BPDU Guard	Operational Edge	Operational Point-to-Point
1	GE1	Enabled	20000	128	Disabled	Disabled	Disabled	Enabled
2	GE2	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
3	GE3	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
4	GE4	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
5	GE5	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
6	GE6	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
7	GE7	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
8	GE8	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
9	GE9	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
10	GE10	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
11	GE11	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
12	GE12	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
13	GE13	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
14	GE14	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
15	GE15	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
16	GE16	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
17	GE17	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
18	GE18	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
19	GE19	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
20	GE20	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
21	GE21	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
22	GE22	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
23	GE23	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
24	GE24	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
25	GE25	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
26	GE26	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
27	GE27	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
28	GE28	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled
29	LAG1	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled

Figure 48 - Spanning Tree > Port Setting

Item	Description
Edit	Click to edit the spanning tree port settings by entering the following data: • State • Path Cost • Priority • BPDU Filter • BPDU Guard • Edge Port • Point-to-Point
Protocol Migration Check	Click to force the port(s) specified above to send one RSTP BPDU (Rapid Spanning Tree Protocol Bridge Protocol Data Unit).

4.7.3. MST Instance

To view the menu, navigate to Spanning Tree > MST Instance.

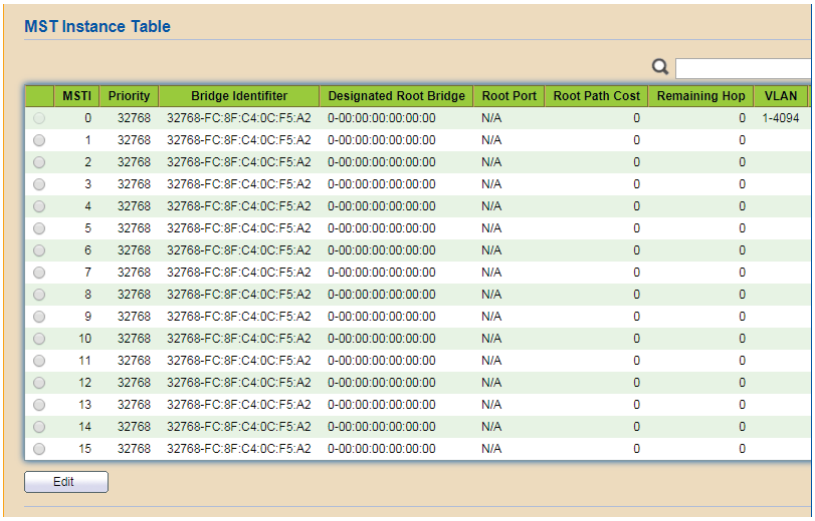
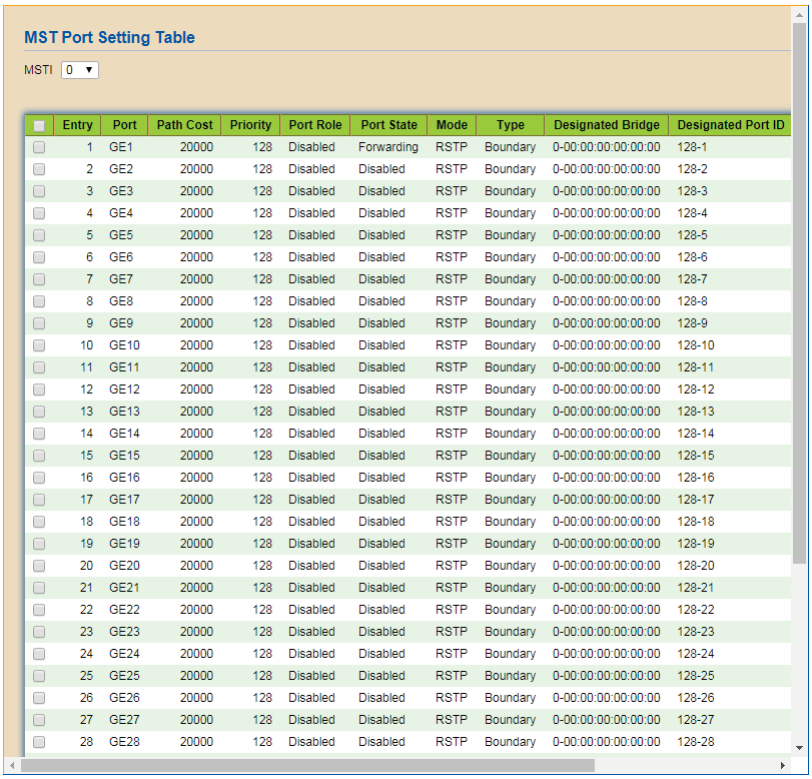


Figure 49 - Spanning Tree > MST Instance

Item	Description
	Enter the keywords to use in the search function.
Edit	Click to edit the MST instance settings by entering the following data: • VLAN • Priority

4.7.4. MST Port Setting

To view the menu, navigate to Spanning Tree > MST Port Setting.



Entry	Port	Path Cost	Priority	Port Role	Port State	Mode	Type	Designated Bridge	Designated Port ID
1	GE1	20000	128	Disabled	Forwarding	RSTP	Boundary	0-00:00:00:00:00:00	128-1
2	GE2	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-2
3	GE3	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-3
4	GE4	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-4
5	GE5	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-5
6	GE6	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-6
7	GE7	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-7
8	GE8	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-8
9	GE9	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-9
10	GE10	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-10
11	GE11	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-11
12	GE12	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-12
13	GE13	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-13
14	GE14	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-14
15	GE15	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-15
16	GE16	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-16
17	GE17	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-17
18	GE18	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-18
19	GE19	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-19
20	GE20	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-20
21	GE21	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-21
22	GE22	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-22
23	GE23	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-23
24	GE24	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-24
25	GE25	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-25
26	GE26	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-26
27	GE27	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-27
28	GE28	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-28

Figure 50 - Spanning Tree > MST Port Setting

Item	Description
MSTI	Click the drop-down menu to select the MST instance.
Edit	Click to edit the MST port settings by entering the following data: • Path Cost • Priority

4.7.5. Statistics

To view the menu, navigate to Spanning Tree > Statistics.

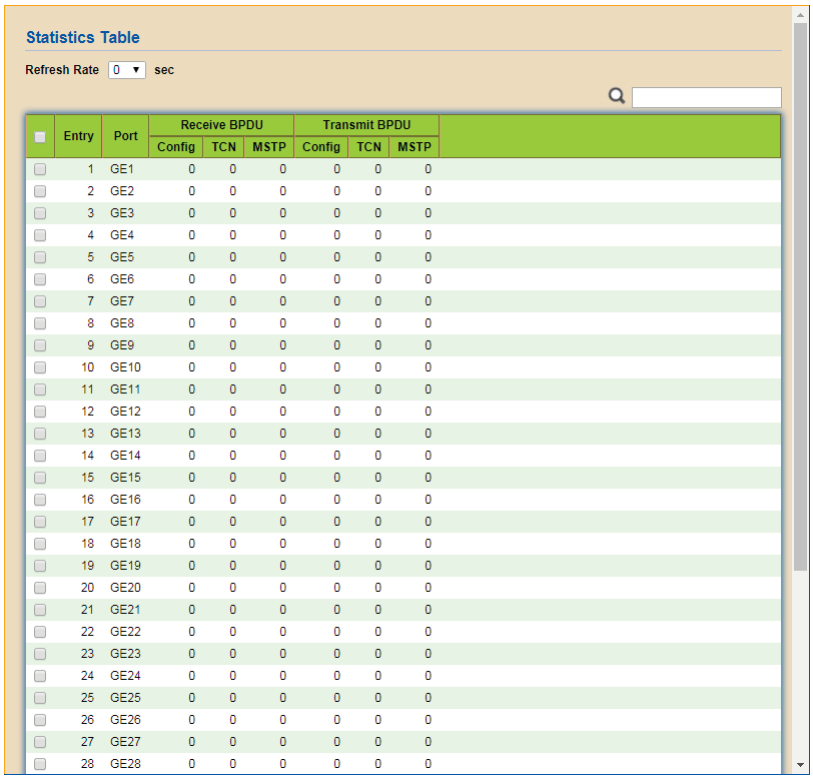


Figure 51 - Spanning Tree > Statistics

Item	Description
Refresh Rate	Click the drop-down menu to select refresh rate.
	Enter the keywords to use in the search function.
Clear	Click to clear the statistics table.
Refresh	Click to refresh the display.
View	Click to display the details for the desired port.

4.8. Discovery

4.8.1. LLDP

LLDP is a one-way protocol; there are no request/response sequences. Information is advertised by stations implementing the transmit function, and is received and processed by stations implementing the receive function.

Property

The page allows a user to set general settings for LLDP.

To view the menu, navigate to Discovery > LLDP > Property.

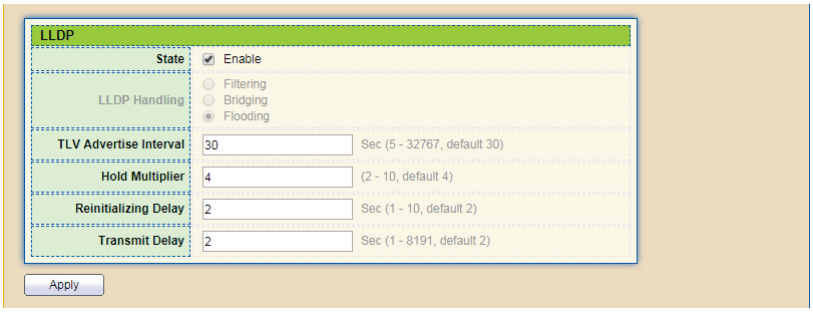


Figure 52 - Discovery > LLDP > Property

Item	Description
LLDP	
State	Click the radio button to enable LLDP protocol on this switch.
LLDP Handling	When LLDP State is disabled, click the radio button in the LLDP Handling field to specify the action to take if a packet matches the selected criteria: • Filtering: Deletes the matching packet. • Bridging: Forwards the matching packet to all configured Virtual Local Area Network (VLAN) members. • Flooding: Forwards the packet to all ports.
TLV Advertise Interval	Enter the variable to set the interval at which frames are transmitted.
Hold Multiplier	Enter the variable to set the multiplier on the transmit interval to assign to TTL.
Reinitializing Delay	Enter the variable to set the delay before a re-initialization.
Transmit Delay	Enter the variable to set the delay after an LLDP frame is sent.
Apply	Click to save the values and update the screen.

Port Setting

The page allows a user to select a specified port or all ports and specify its port setting(s).

To view the menu, navigate to Discovery > LLDP > Port Setting.

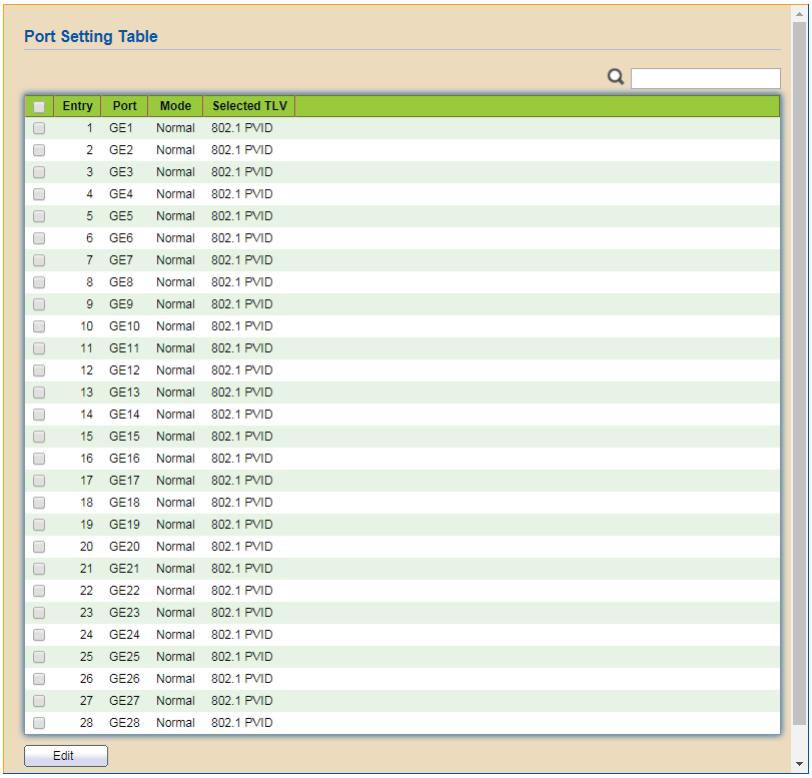


Figure 53 - Discovery > LLDP > Port Setting

Item	Description
	Enter the keywords to use in the search function.
Edit	Select an entry and clik to edit the LLDP port settings by entering the following data.

Select an entry to edit. The following screen displays.

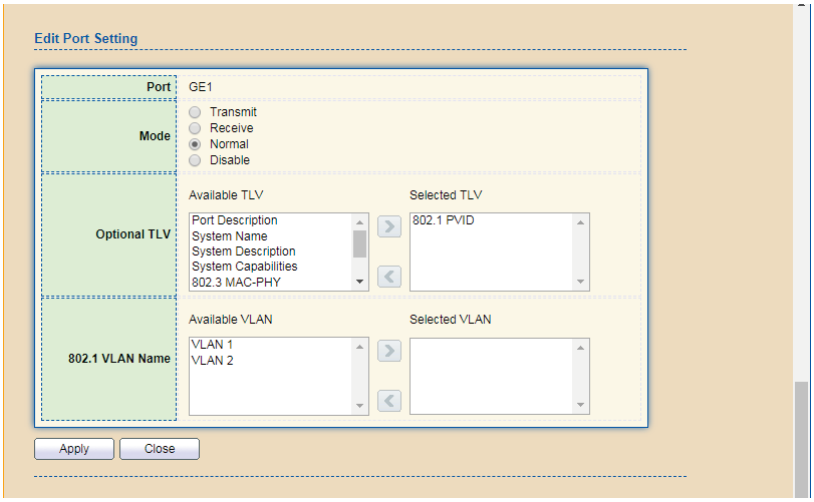


Figure 54 - Discovery > LLDP > Port Setting >Edit

Item	Description
Port	Selected port (s).
Mode	Select the transmission state of LLDP port interface. • Transmit: Transmit LLDP PDUs only. • Receive: Receive LLDP PDUs only. • Normal : Transmit and receive LLDP PDUs both. • Disable : Disable the transmission of LLDP PDUs.
Optional TLV	Select the LLDP optional TLVs to be carried (multiple selections are allowed). • Port Description • System Name • System Description • System Capabilities • 802.3 MAC-PHY • 802.3 Link Aggregation • 802.3 Maximum Frame Size • Management Address
802.1 VLAN Name	Select the VLAN name ID from the Available VLAN field to be carried.
Apply	Click to save the new settings.
Close	Click to return to the previous menu without saving.

Packet View

To view the menu, navigate to Discovery > LLDP > Packet View.

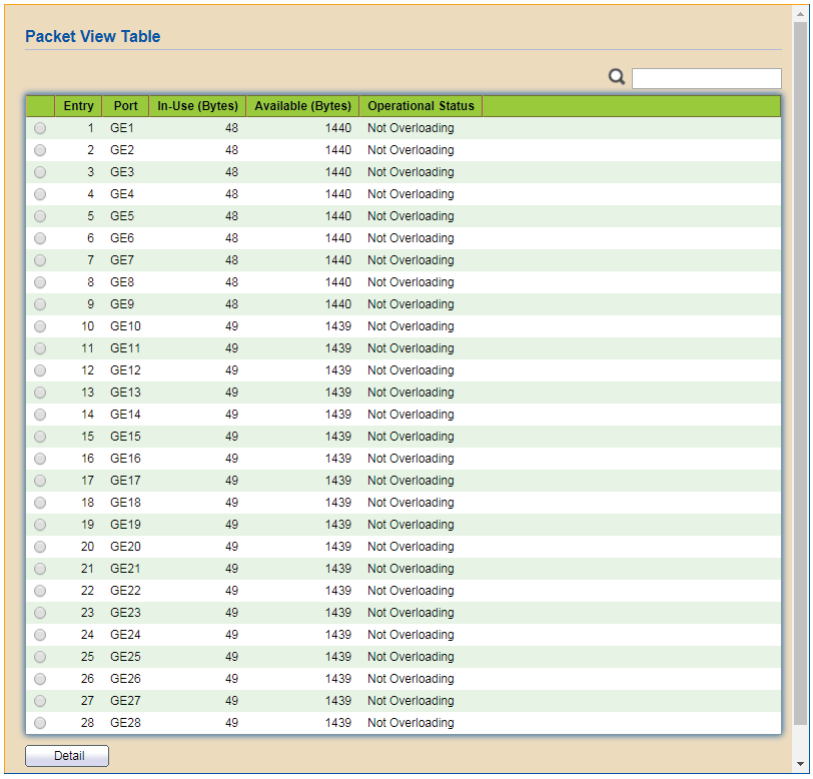


Figure 55 - Discovery > LLDP > Packet View

Item	Description
	Enter the keywords to use in the search function.
Detail	Click to display the packet transmission details in bytes (port, mandatory TLVs, 802.3 TLVs, Optional TLVs, 802.1 TLVs, and Total) for the selected port.

Local Information

To view the menu, navigate to Discovery > LLDP > Local Information.

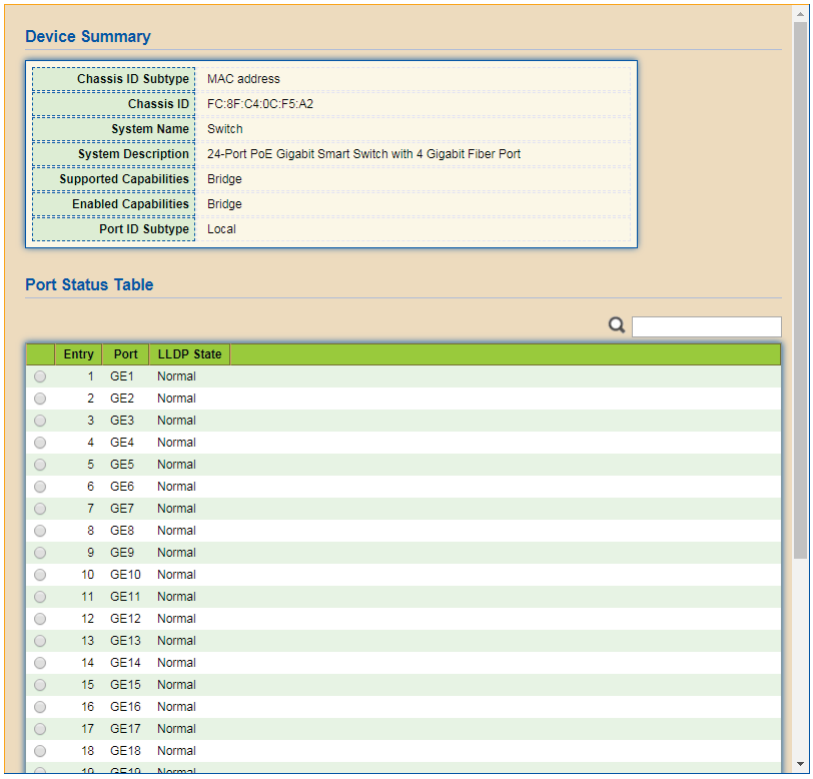


Figure 56 - Discovery > LLDP > Local Information

Item	Description
Chassis ID Subtype	Display the type of chassis ID, such as the MAC address.
Chassis ID	Display Identifier of chassis. Where the chassis ID subtype is a MAC address, the MAC address of the switch is displayed.
System Name	Display model name of switch.
System Description	Display description of switch.
Supported Capabilities	Display the primary functions of the device, such as Bridge, WLAN AP, or Router.
Enabled Capabilities	Primary enabled functions of the device.
Port ID Subtype	Display the type of the port identifier.
	Enter the keywords to use in the search function.
Detail	Click to display the details for the desired port.

Neighbor

To view the menu, navigate to Discovery > LLDP > Neighbor.

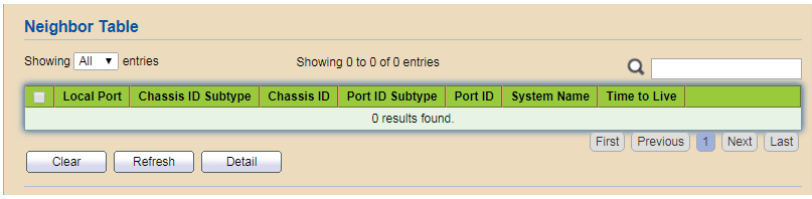


Figure 57 - Discovery > LLDP > Neighbor

Item	Description
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.
Clear	Click to clear the neighbor table.
Refresh	Click to refresh the display.
Detail	Click to display the details for the desired port.

Statistics

To view the menu, navigate to Discovery > LLDP > Statistics.

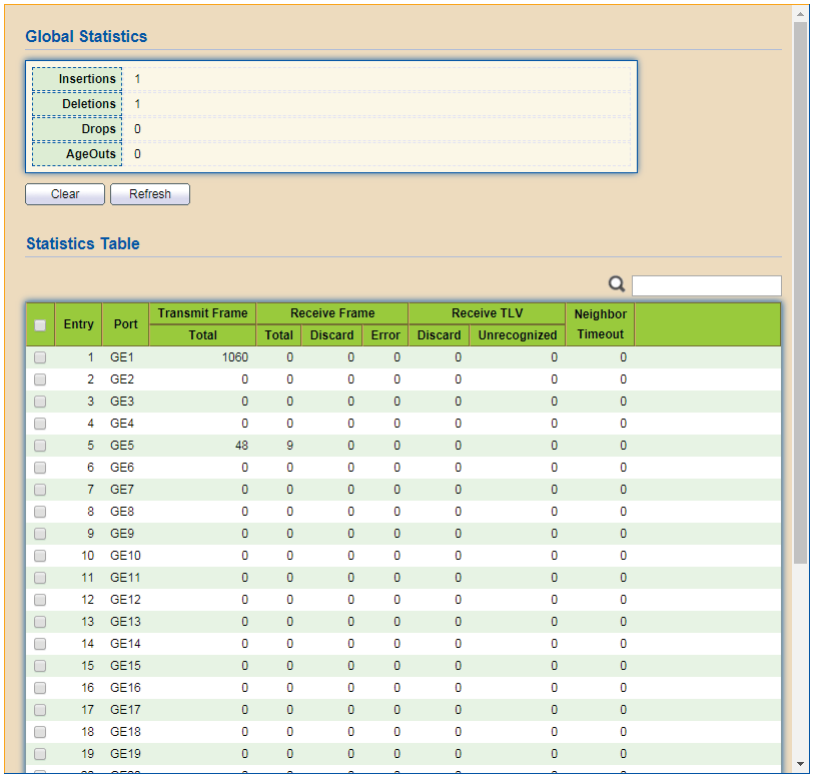


Figure 58 - Discovery > LLDP > Statistics

Item	Description
Insertions	Display the number of insertions made to the database table.
Deletions	Display the number of deletions made to the database table.
Drops	Display the number of LLDP frames dropped from the database table due to errors.
AgeOuts	Display the number of entries to the database table that have aged out of the table.
Clear	Click to clear the global statistics table.
Refresh	Click to refresh the display.
	Enter the keywords to use in the search function.
Clear	Click to clear the statistics table.
Refresh	Click to refresh the display.

4.9. Multicast

4.9.1. General

Property

To view the menu, navigate to Multicast > General > Property.

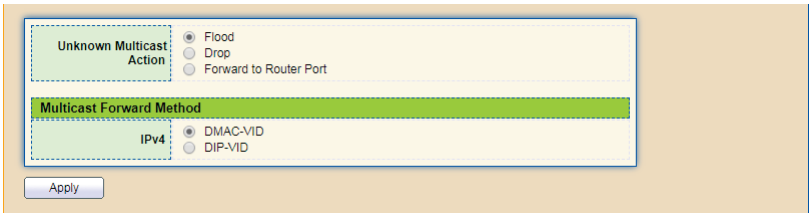


Figure 59 - Multicast > General > Property

Item	Description
Unknown Multicast Action	Click the radio buttons to select an action for the switch to handle with unknown multicast packet. • Flood: Flood the unknown multicast data. • Drop: Drop the unknown multicast data. • Forward to Router port: Forward the unknown multicast data to router port.
Multicast Forward Method	
IPv4	Click the radio buttons to select the IPv4 multicast forward method. • DMAC-VID: Forward using destination multicast MAC address and VLAN IDs. • DIP-VID: Forward using destination multicast IP address and VLAN ID.
Apply	Click to save the values and update the screen.

Group Address

To view the menu, navigate to Multicast > General > Group Address.

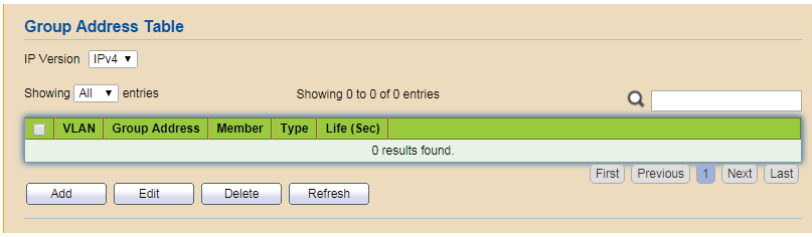


Figure 60 - Multicast > General > Group Address

Item	Description
IP Version	Click the drop-down menu to select the IP version for the multicast group.
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.
Add	Click to add a new group address by entering the following data: • VLAN • IP Version • Group Address • Member
Edit	Click to edit the group address settings by entering the following data: • IP Version • Group Address • Member
Delete	Click to delete the desired entries.
Refresh	Click to refresh the display.

Router Port

To view the menu, navigate to Multicast > General > Router Port.

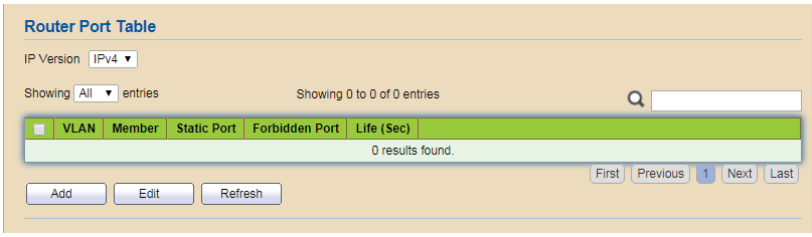


Figure 61 - Multicast > General > Router Port

Item	Description
IP Version	Click the drop-down menu to select the IP version for the multicast group.
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.
Add	Click to add a new router port by entering the following data: • VLAN • IP Version • Type • Port
Edit	Click to edit the router port settings by entering the following data: • IP Version • Type • Port
Refresh	Click to refresh the display.

4.9.2. IGMP Snooping

IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic.

Property

The page allows the network administrator to enable/disable IGMP function, select snooping version, and enable/disable snooping report suppression.

To view the menu, navigate to Multicast > IGMP Snooping > Property.

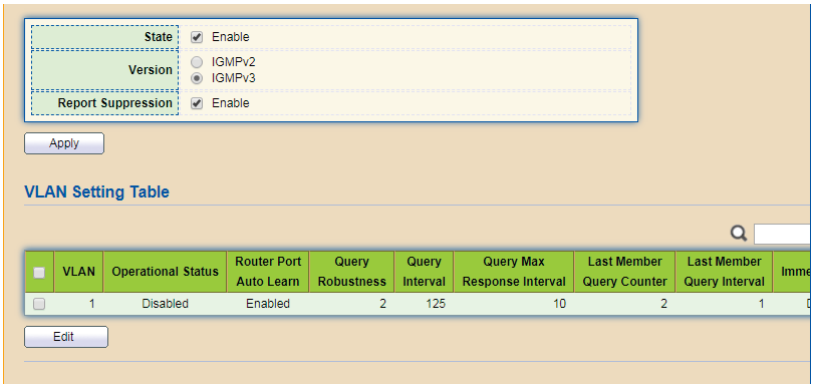


Figure 62 - Multicast > IGMP Snooping > Property

Item	Description
State	Click the radio button to enable the IGMP function.
Version	Click the radio buttons to set the IGMP snooping version. • IGMPv2: Only support process IGMP v2 packet. • IGMPv3: Support IGMP v3 basic and IGMP v2.
Report Suppression	Click the radio button to allow the switch to handle IGMP reports between router and host, suppressing bandwidth used by IGMP.
Apply	Click to save the values and update the screen.
	Enter the keywords to use in the search function.

Item	Description
Edit	Click to edit the IGMP settings by entering the following data: • State • Router Port Auto Learn • Query Robustness • Query Interval • Query Max Response Interval • Last Member Query Counter • Last Member Query Interval • Immediate leave

Querier

The page allows a user to configure Querier settings on specific VLAN of IGMP Snooping.

To view the menu, navigate to Multicast > IGMP Snooping > Querier.

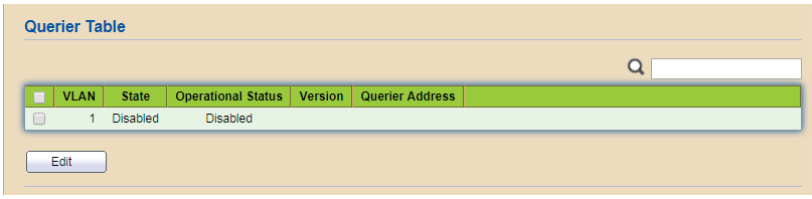


Figure 63 - Multicast > IGMP Snooping > Querier

Item	Description
	Enter the keywords to use in the search function.
Edit	Click to edit the IGMP Querier settings by entering the following data: • State • Version

Statistics

To view the menu, navigate to Multicast > IGMP Snooping > Statistics.

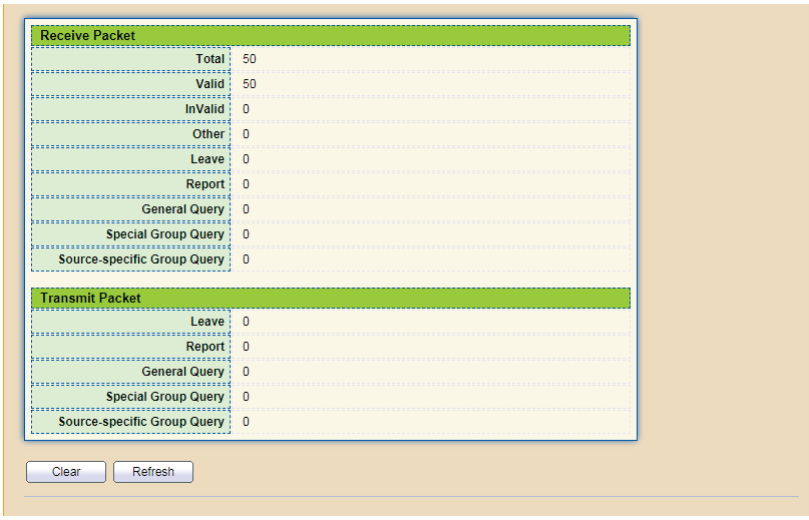


Figure 64 - Multicast > IGMP Snooping > Statistics

Item	Description
Receive Packet	
Total	Display the counter total of IGMP packets received.
Valid	Display the number of valid IGMP packets received.
InValid	Display the number of invalid IGMP packets received.
Other	Display the number of unspecified IGMP packets received.
Leave	Display the number of leave messages received at the interface.
Report	Display the total membership reports received at the interface.
General Query	Display the total number of general queries received at the interface.
Special Group Query	Display the total group queries received at the interface.
Source-specific Group Query	Display the total number of group queries received by a specific source at the interface.
Transmit Packet	
Leave	Display the number of leave messages transmitted at the interface.
Report	Display the total membership reports transmitted at the interface.
General Query	Display the total number of general queries transmitted at the interface.
Special Group Query	Display the total group queries transmitted at the interface.

Item	Description
Source-specific Group Query	Display the total number of group queries transmitted by a specific source at the interface.
Clear	Click to clear the IGMP snooping statistic tables.
Refresh	Click to refresh the display.

4.9.3. MVR

Multicast VLAN Registration (MVR) can route packets received in a multicast source VLAN to one or more destination VLANs. LAN users are in the destination VLANs and the multicast server is in the source VLAN.

MVR can continuously send multicast stream for traffic in the multicast VLAN, but isolate the streams from the source VLANs for bandwidth and security reasons.

In general, MVR is able to:

- Identify the MVR IP multicast streams and their associated IP multicast group
- Intercept the IGMP messages

Property

The page allows the network administrator to configure general settings for MVR, such as enabling function, selecting VLAN ID (as source VLAN) and specify IP address(es) for receiver/LAN users.

To view the menu, navigate to Multicast > MVR > Property.

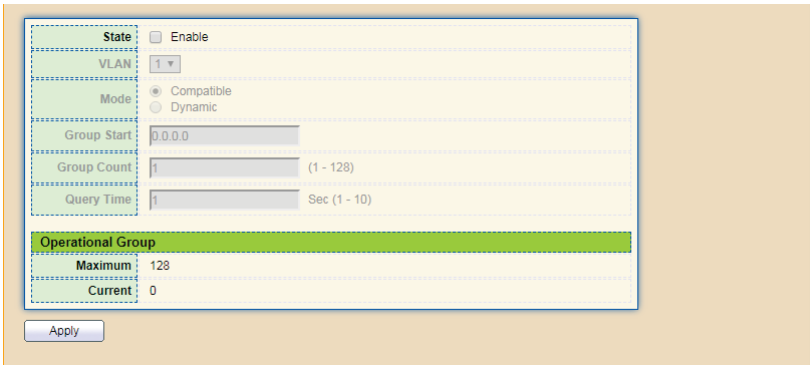


Figure 65 - Multicast > MVR > Property

Item	Description
State	Click the radio button to enable the MVR function.
VLAN	Click the drop-down menu to select the VLAN ID as multicast source VLAN which will receive multicast data. All source ports must belong to this VLAN. Each VLAN ID shall be configured with group address and member port (defined in Multicast > MVR > Group Address).

Item	Description
Mode	Click the radio buttons to select the mode for MVR operation. • Compatible: Multicast data received by MVR hosts (multicast server) will be forwarded to all MVR receiver ports. • Dynamic: Multicast data received by MVR hosts (multicast server) on Vigor switch will be forwarded from those MVR data and client ports grouped under MVR server.
Group Start	Enter an IP address. Any multicast data sent to this IP address will be sent to all source ports on Vigor switch; and all receiver ports will accept /receive data from that multicast address.
Group Count	Select a number to configure a contiguous series of MVR group addresses.
Query Time	Enter the variable to define the maximum time to wait for IGMP report members on a receiver port before the port is removed from multicast group.
Operational Group	
Maximum	Display the maximum group for MVR operation.
Current	Display the current group for MVR operation.
Apply	Click to save the values and update the screen.

Port Setting

Use the page to specify destination port and source port (GE/LAG) for Vigor system to perform MVR operation.

To view the menu, navigate to Multicast > MVR > Port Setting.

Figure 66 - Multicast > MVR > Port Setting

Item	Description
	Enter the keywords to use in the search function.
Edit	Click to edit the port settings by entering the following data: • Role • Immediate Leave

Group Address

The page allows the network administrator to configure the IP address and specify the port member for the selected VLAN.

To view the menu, navigate to Multicast > MVR > Group Address.

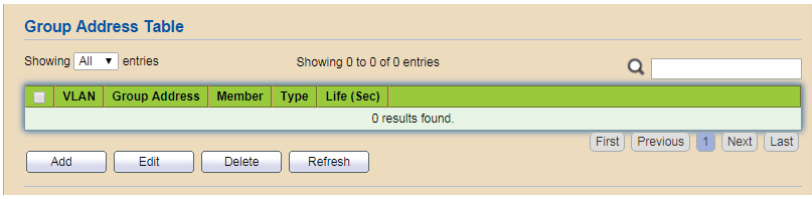


Figure 67 - Multicast > MVR > Group Address

Item	Description
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.
Add	Click to add a new MVR group by entering the following data: • Group Address • Member
Edit	Click to edit the MVR group settings by entering the following data: • VLAN
Delete	Click to delete the desired entries.
Refresh	Click to refresh the display.

4.10. Security

4.10.1. RADIUS

The page allows the network administrator to add and configure multiple RADIUS servers.

To view the menu, navigate to Security > RADIUS.

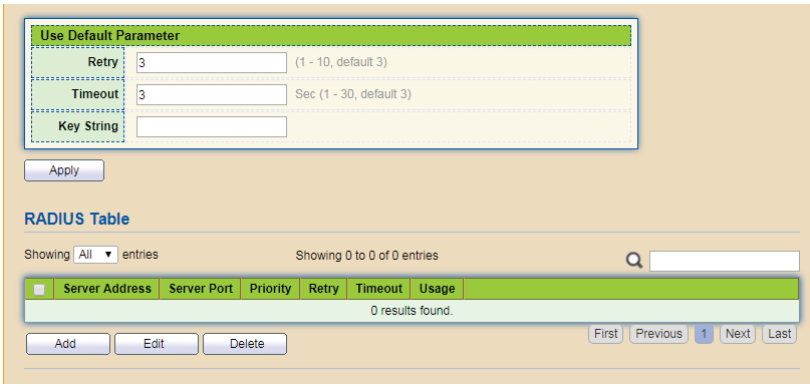


Figure 68 - Security > RADIUS

Item	Description
Use Default Parameter	
Retry	Enter the variable to set the retry time before the switch being considered not-reachable.
Timeout	Enter the variable to set the time before the switch being considered lost connection.
Key String	Enter the string used to encrypt and authenticate with RADIUS server.
Apply	Click to save the values and update the screen.
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.
Add	Click to add a new RADIUS server by entering the following data: • Address Type • Server Address • Server Port • Priority • Key String • Retry • Timeout • Usage

Item	Description
Edit	Click to edit the RADIUS server settings by entering the following data: • Server Address • Server Port • Priority • Key String • Retry • Timeout • Usage
Delete	Click to delete the desired entries.

4.10.2. Management Access

Management Service

To view the menu, navigate to Security > Management Access > Management Service.

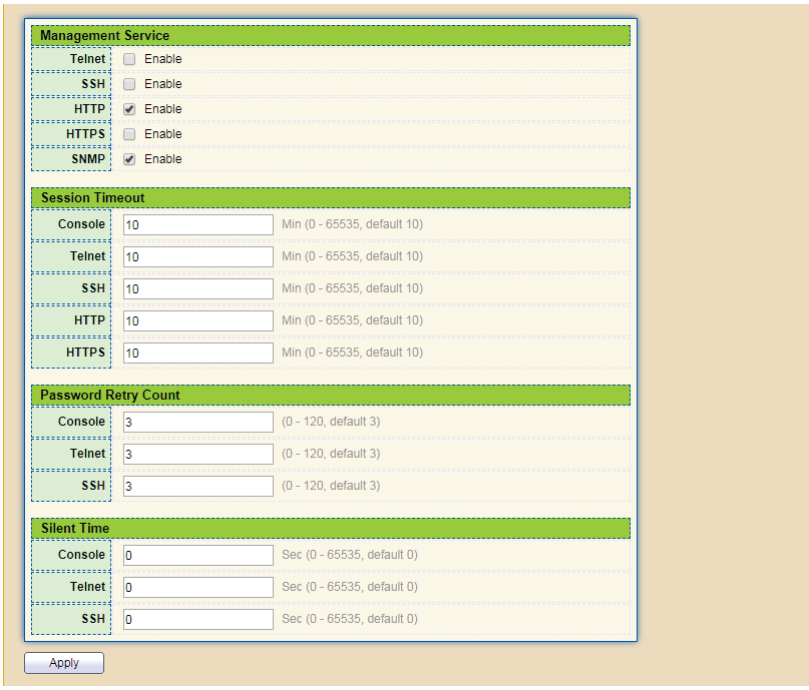


Figure 69 - Security > Management Access > Management Service

Item	Description
Management Service	
Telnet	Click the radio button to enable the telnet service.
SSH	Click the radio button to enable the SSH service.
HTTP	Click the radio button to enable the HTTP service.

Item	Description
HTTPS	Click the radio button to enable the HTTPS service.
SNMP	Click the radio button to enable the SNMP service.
Session Timeout	
Console	Enter the variable to define the timeout period for the console session.
Telnet	Enter the variable to define the timeout period for the telnet session.
SSH	Enter the variable to define the timeout period for the SSH session.
HTTP	Enter the variable to define the timeout period for the HTTP session.
HTTPS	Enter the variable to define the timeout period for the HTTPS session.
Password Retry Count	
Console	Enter a value (0 - 120, default:3) to designate the number of allowed attempts through a console interface.
Telnet	Enter a value (0 - 120, default:3) to designate the number of allowed attempts through a Telnet interface.
SSH	Enter a value (0 - 120, default:3) to designate the number of allowed attempts through a SSH interface.
Silent Time	
Console	Enter a value (0 - 65535, default:0) to designate the period of time the interface is inaccessible after a console session failed access event.
Telnet	Enter a value (0 - 65535, default:0) to designate the period of time the interface is inaccessible after a Telnet session failed access event.
SSH	Enter a value (0 - 65535, default:0) to designate the period of time the interface is inaccessible after a SSH session failed access event.
Apply	Click to save the values and update the screen.

Management ACL

The page allows a user to add, edit, and delete Management Access Control profiles.

To view the menu, navigate to Security > Management Access > Management ACL.

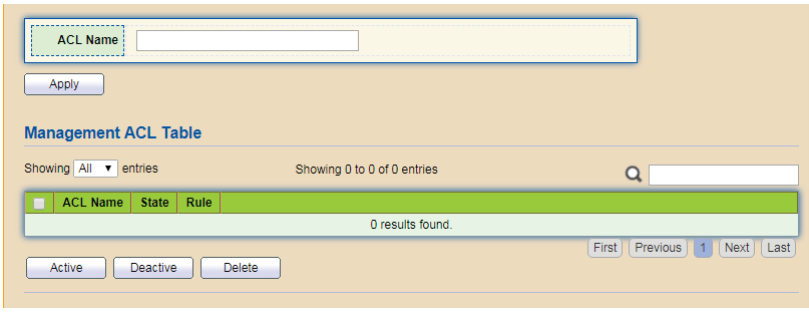


Figure 70 - Security > Management Access > Management ACL

Item	Description
ACL Name	Enter the string to create a profile for ACL.
Apply	Click to save the values and update the screen.
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.
Active	Click to active the desired entry.
Deactive	Click to deactive the desired entry.
Delete	Click to delete the desired entries.

Management ACE

This page allows a user to add, edit, or remove Access Control Entries (ACE) of the Management Access Control profiles. However, only the ACE of inactive profiles can be modified, and before configuring ACE, at least one ACL profile should be created.

To view the menu, navigate to Security > Management Access > Management ACE.

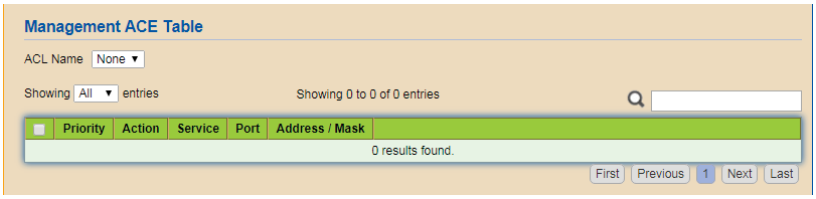


Figure 71 - Security > Management Access > Management ACE

Item	Description
ACL Name	Click the drop-down menu to select the inactive ACL to modify.
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).

Item	Description
	Enter the keywords to use in the search function.
Add	Click to add a new management ACE by entering the following data: • Priority • Action • Service • Port • IP Version • IPv4 • IPv6
Edit	Click to edit the management ACE settings by entering the following data: • Service • Action • Port • IP Version • IPv4 • IPv6
Delete	Click to delete the desired entries.

4.10.3. Authentication Manager

The authentication manager allows you to configure secure access for any host connected to a physical port. Multiple authentication is available for each port.

Property

The device supports 802.1x and MAC-based authentication methods. In the Property page, you can specify authentication type, enable Guest VLAN function, specify a VID and select the format for MAC address entry.

To view the menu, navigate to Security > Authentication Manager > Property.

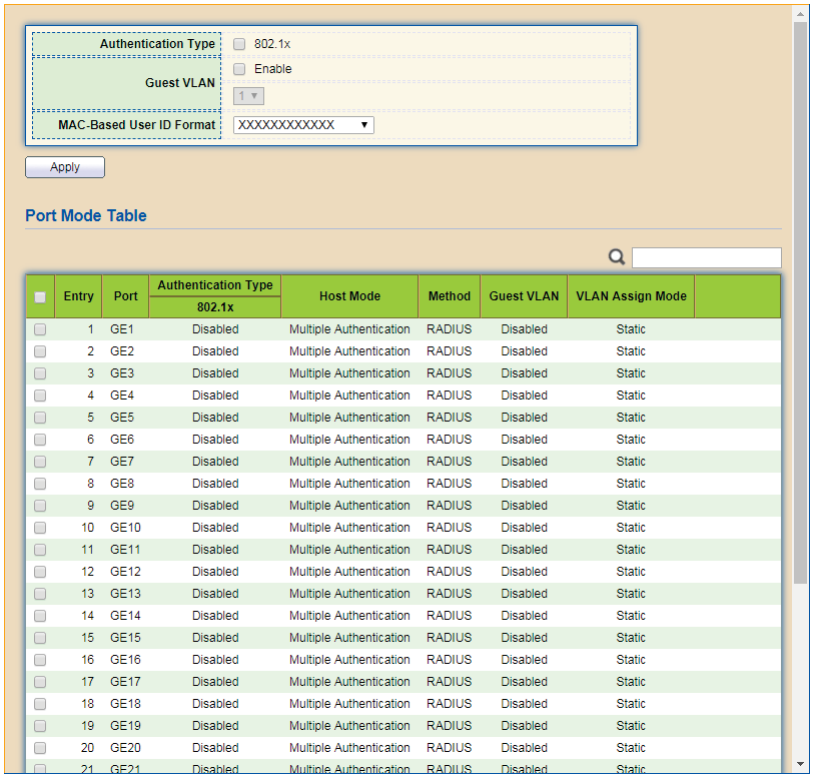


Figure 72 - Security > Authentication Manager > Property

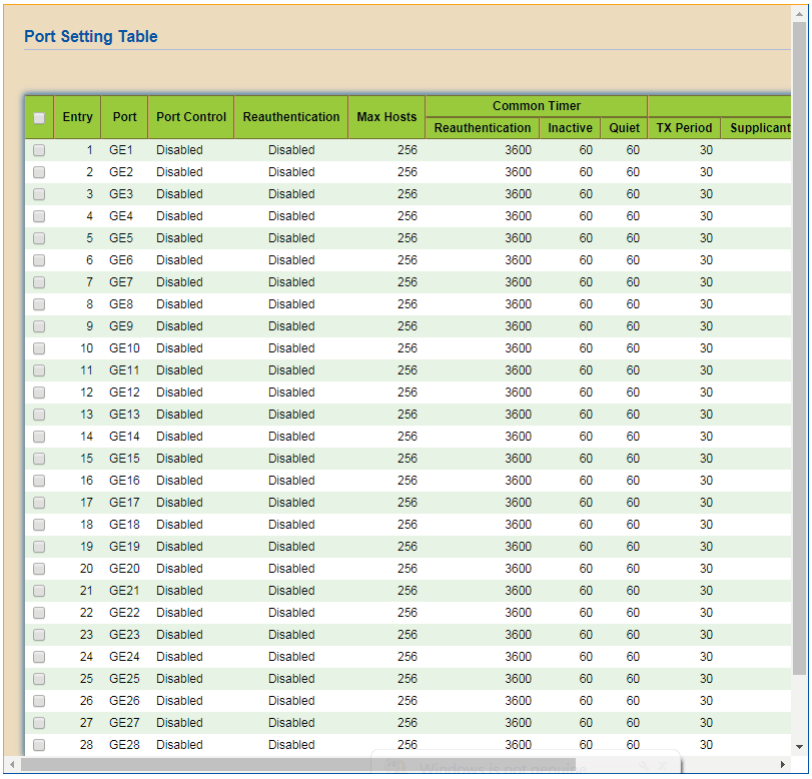
Item	Description
Authentication Type	Click the radio button to specify which type (802.1x, MAC-based) will be used for authentication. Choose to enable 802.1x or MAC-based authentication method for host connecting to Ethernet port. You may configure which type to be used per port, but enabling any per port without enabling here will not be effective.
Guest VLAN	Click the radio button to enable a Guest VLAN for those that have not successfully authenticated with any given methods. Click the drop-down menu to select a VLAN ID as a Guest VLAN.

Item	Description
MAC-Based User ID Format	Click the drop-down menu to specify how the MAC-based user ID should be expressed in EAP message between AAA server and switch.
Apply	Click to save the values and update the screen.
	Enter the keywords to use in the search function.
Edit	Click to edit the authentication port mode settings by entering the following data: • Authentication Type • Host Mode • Method • Guest VLAN • VLAN Assign Mode

Port Setting

The page allows the network administrator to controls port setting, based on 802.1X, for Ethernet port authentication.

To view the menu, navigate to Security > Authentication Manager > Port Setting.



Port Setting Table

Entry	Port	Port Control	Reauthentication	Max Hosts	Common Timer				
					Reauthentication	Inactive	Quiet	TX Period	Supplicant
1	GE1	Disabled	Disabled	256	3600	60	60	30	
2	GE2	Disabled	Disabled	256	3600	60	60	30	
3	GE3	Disabled	Disabled	256	3600	60	60	30	
4	GE4	Disabled	Disabled	256	3600	60	60	30	
5	GE5	Disabled	Disabled	256	3600	60	60	30	
6	GE6	Disabled	Disabled	256	3600	60	60	30	
7	GE7	Disabled	Disabled	256	3600	60	60	30	
8	GE8	Disabled	Disabled	256	3600	60	60	30	
9	GE9	Disabled	Disabled	256	3600	60	60	30	
10	GE10	Disabled	Disabled	256	3600	60	60	30	
11	GE11	Disabled	Disabled	256	3600	60	60	30	
12	GE12	Disabled	Disabled	256	3600	60	60	30	
13	GE13	Disabled	Disabled	256	3600	60	60	30	
14	GE14	Disabled	Disabled	256	3600	60	60	30	
15	GE15	Disabled	Disabled	256	3600	60	60	30	
16	GE16	Disabled	Disabled	256	3600	60	60	30	
17	GE17	Disabled	Disabled	256	3600	60	60	30	
18	GE18	Disabled	Disabled	256	3600	60	60	30	
19	GE19	Disabled	Disabled	256	3600	60	60	30	
20	GE20	Disabled	Disabled	256	3600	60	60	30	
21	GE21	Disabled	Disabled	256	3600	60	60	30	
22	GE22	Disabled	Disabled	256	3600	60	60	30	
23	GE23	Disabled	Disabled	256	3600	60	60	30	
24	GE24	Disabled	Disabled	256	3600	60	60	30	
25	GE25	Disabled	Disabled	256	3600	60	60	30	
26	GE26	Disabled	Disabled	256	3600	60	60	30	
27	GE27	Disabled	Disabled	256	3600	60	60	30	
28	GE28	Disabled	Disabled	256	3600	60	60	30	

Figure 73 - Security > Authentication Manager > Port Setting

Item	Description
Edit	Click to edit the authentication port settings by entering the following data: • Port Control • Reauthentication • Max Hosts • Reauthentication • Quiet • TX Period • Supplicant Timeout • Server Timeout • Max Request

Sessions

To view the menu, navigate to Security > Authentication Manager > Sessions.

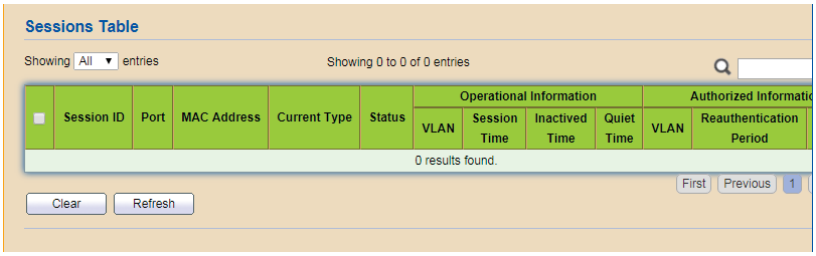


Figure 74 - Security > Authentication Manager > Sessions

Item	Description
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.
Clear	Click to clear the session table.
Refresh	Click to refresh the display.

4.10.4. Port Security

The Port Security setting allows you to enable the function and set a limit on the number of MAC addresses a port can learn. The range is 0 to 256. The default is 0, which indicates that only static addresses are supported on the interface.

When a port exceed the defined number of learned address, an action on that violation can also be defined (discard packets, forward packets, or shutdown port).

To view the menu, navigate to Security > Port Security.

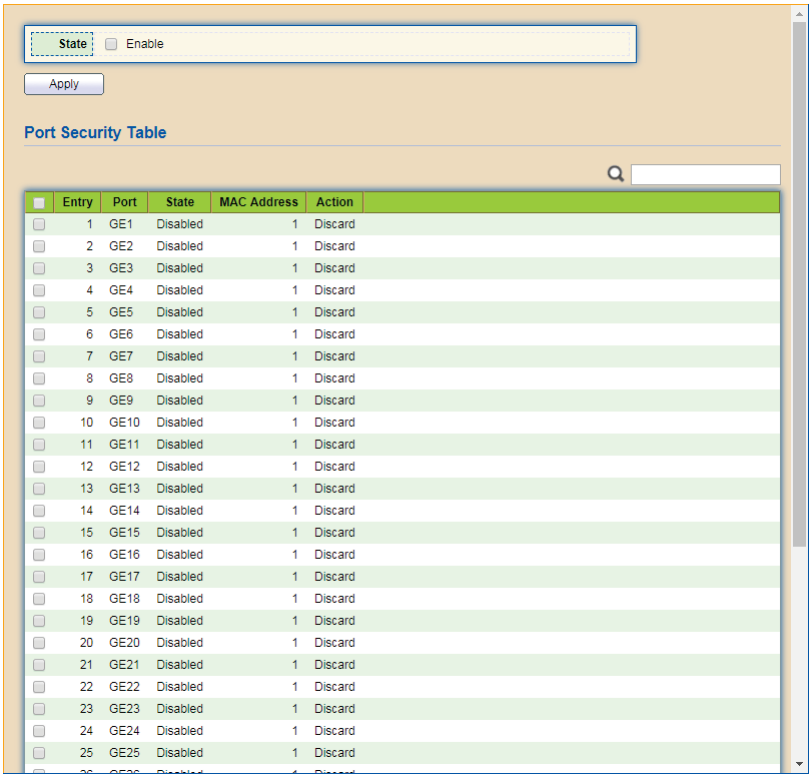


Figure 75 - Security > Port Security

Item	Description
State	Click the radio button to enable the port security function.
Apply	Click to save the values and update the screen.
	Enter the keywords to use in the search function.
Edit	Click to edit the port security settings.

Select an entry to edit. The following screen displays.

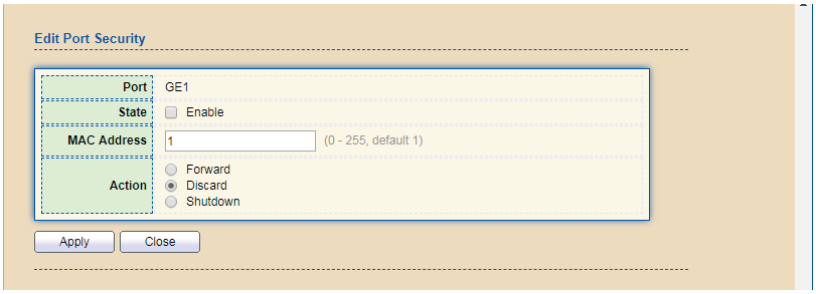


Figure 76 - Security > Port Security > Edit

Item	Description
Port	Displays the selected port.
State	Displays if the setting is enabled (must be selected) or disabled.
MAC Address	Enter the maximum number of MAC Addresses the port is allowed to store.
Action	• Discard: Discards packets from any unlearned source. • Forward: Forwards packets from an unknown source without learning the MAC address. • Shutdown: Discards the packet (s) from any unleared source, and shuts down the port. The port remains in the shut down mode until it is reactivated, or until the device is rebooted.
Apply	Click to save the new settings.
Close	Click to return to the previous menu without saving.

4.10.5. Protected Port

The page allows the network administrator to configure protected port setting to prevent the selected ports from communication with each other. Protected port is only allowed to communicate with unprotected port.

To view the menu, navigate to Security > Protected Port.

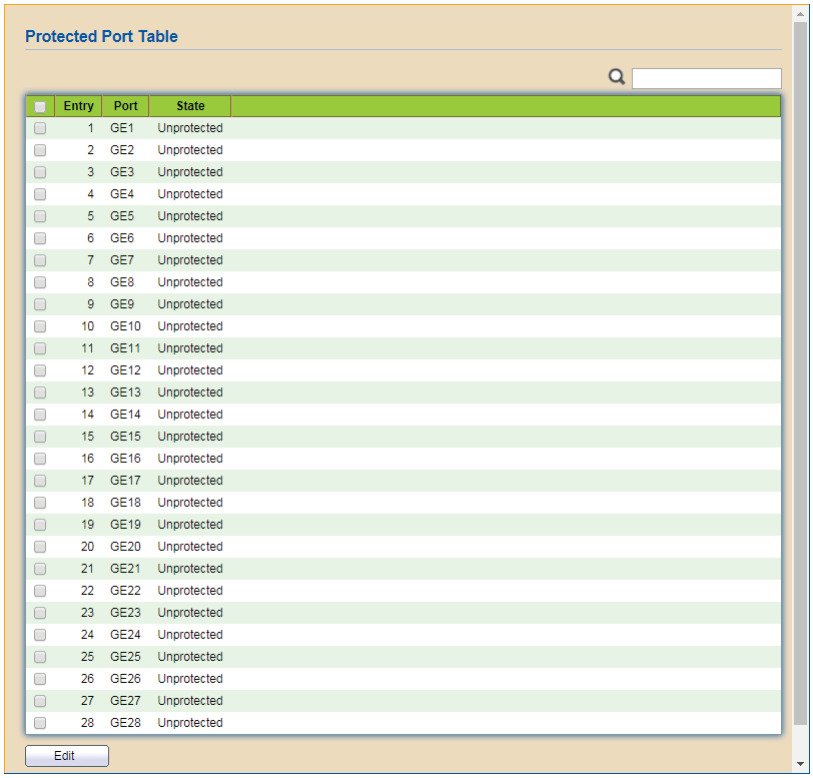


Figure 77 - Security > Protected Port

Item	Description
	Enter the keywords to use in the search function.
Edit	Click to edit the protected port settings by entering the following data: • State

4.10.6. Storm Control

Storm Control helps to suppress possible broadcast, unknown multicast or unknown unicast storm by applying a rate limit on those packets.

To view the menu, navigate to Security > Storm Control.

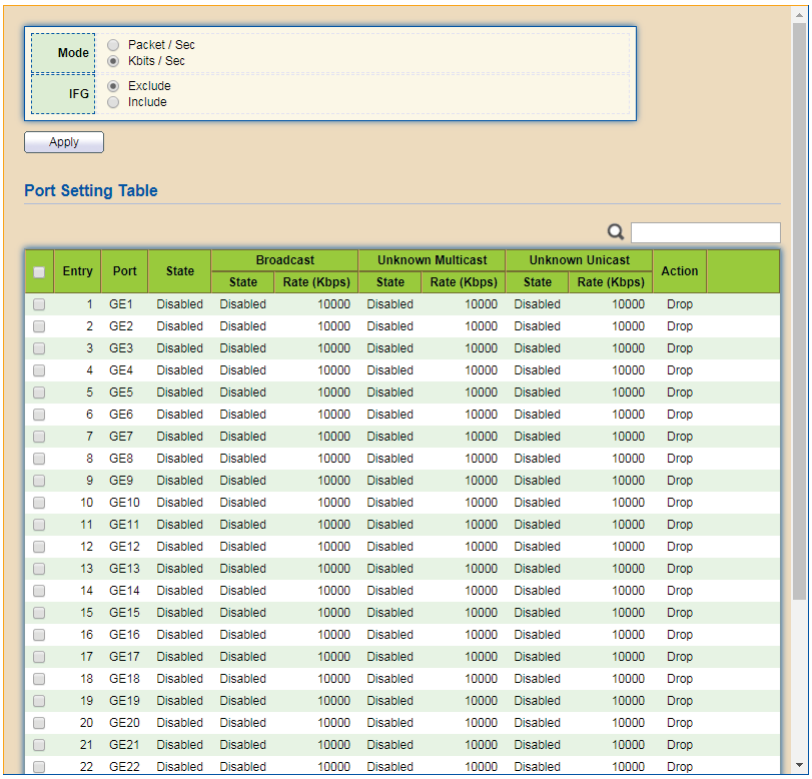


Figure 78 - Security > Storm Control

Item	Description
Mode	Click the radio buttons to select the mode of the storm control. • Packet / Sec: Storm control rate will be calculated by packet-based. • Kbits / Sec: Storm control rate will be calculated by octet-based.
IFG	Click the radio buttons to select the rate calculation with/ without Inter Frame Gap (IFG). • Excluded: Exclude preamble & IFG (20 bytes) when count ingress storm controls rate. • Included: Include preamble & IFG (20 bytes) when count ingress storm controls rate.
Apply	Click to save the values and update the screen.
	Enter the keywords to use in the search function.

Item	Description
Edit	Click to edit the storm control port settings by entering the following data: • State • Broadcast • Unknown Multicast • Unknown Unicast • Action

4.10.7. DoS

A Denial of Service (DoS) attack is a hacker attempt to make a device unavailable to its users. DoS attacks saturate the device with external communication requests, so that it cannot respond to legitimate traffic. These attacks usually lead to a device CPU overload.

The DoS protection feature is a set of predefined rules that protect the network from malicious attacks. The DoS Security Suite Setting enables activating the security suite.

Property

To view the menu, navigate to Security > DoS > Property.

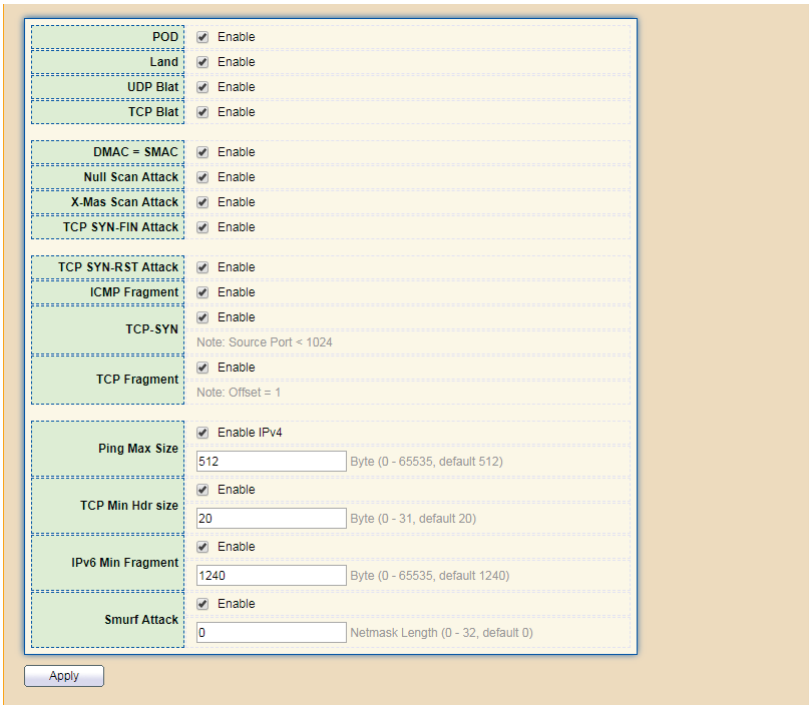


Figure 79 - Security > DoS > Property

Item	Description
POD	Avoid ping of death attack. Ping packets that length are larger than 65535 bytes. Click the radio button to enable the function.
Land	Drop the packets if the source IP address is equal to the destination IP address. Click the radio button to enable the function.
UDP Blat	Drop the packets if the UDP source port equals to the UDP destination port. Click the radio button to enable the function.

Item	Description
TCP Blat	Drop the packages if the TCP source port is equal to the TCP destination port. Click the radio button to enable the function.
DMAC = SMAC	Drop the packets if the destination MAC address is equal to the source MAC address. Click the radio button to enable the function.
Null Scan Attack	Drop the packets with NULL scan. Click the radio button to enable the function.
X-Mas Scan Attack	Drop the packets if the sequence number is zero, and the FIN, URG and PSH bits are set. Click the radio button to enable the function.
TCP SYN-FIN Attack	Drop the packets with SYN and FIN bits set. Click the radio button to enable the function.
TCP SYN-RST Attack	Drop the packets with SYN and RST bits set. Click the radio button to enable the function.
ICMP Fragment	Drop the fragmented ICMP packets. Click the radio button to enable the function.
TCP-SYN	Drop SYN packets with sport less than 1024. Click the radio button to enable the function.
TCP Fragment	Drop the fragmented ICMP packets. Click the radio button to enable the function.
Ping Max Size	Determine the IPv4/IPv6 PING packet with the length. Specify the maximum size of the ICMPv4/ICMPv6 ping packets. Click the radio button to enable the function. Enter the variable to specify the setting.
TCP Min Hdr size	Check the minimum TCP header and drops the TCP packets with the header smaller than the minimum size. Click the radio button to enable the function. Enter the variable to specify the setting.
IPv6 Min Fragment	Check the minimum size of IPv6 fragments, and drop the packets smaller than the minimum size. Click the radio button to enable the function. Enter the variable to specify the setting.
Smurf Attack	Avoid smurf attack. Click the radio button to enable the function. Enter the variable to specify the setting.
Apply	Click to save the values and update the screen.

Port Setting

The page allows a user to configure and display the state of DoS protection for interfaces. The configuration result for each port will be displayed on the table listed on this web page.

To view the menu, navigate to Security > DoS > Port Setting.

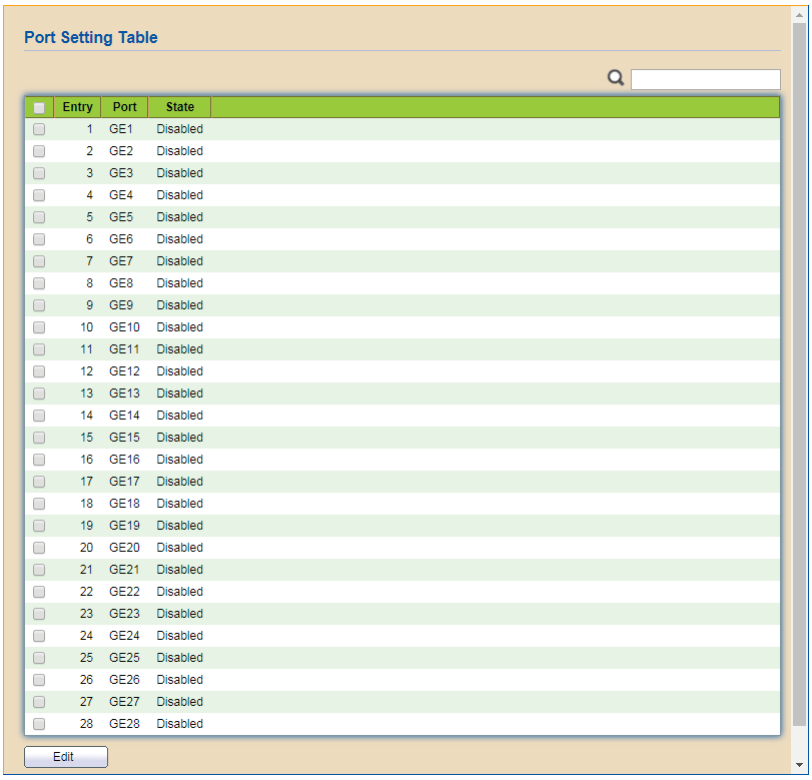


Figure 80 - Security > DoS > Port Setting

Item	Description
	Enter the keywords to use in the search function.
Edit	Click to edit the DoS port settings by entering the following data: • State

4.10.8. DHCP Snooping

DHCP snooping is able to validate DHCP messages obtained from untrusted sources and filter out invalid messages.

For DHCP snooping to function properly, it is suggested to connect DHCP servers to the device through trusted interfaces; because untrusted DHCP messages will be forwarded to trusted interfaces only.

Property

The page allows a user to configure global property settings for the function of DHCP snooping Inspection.

To view the menu, navigate to Security > DHCP Snooping > Property.

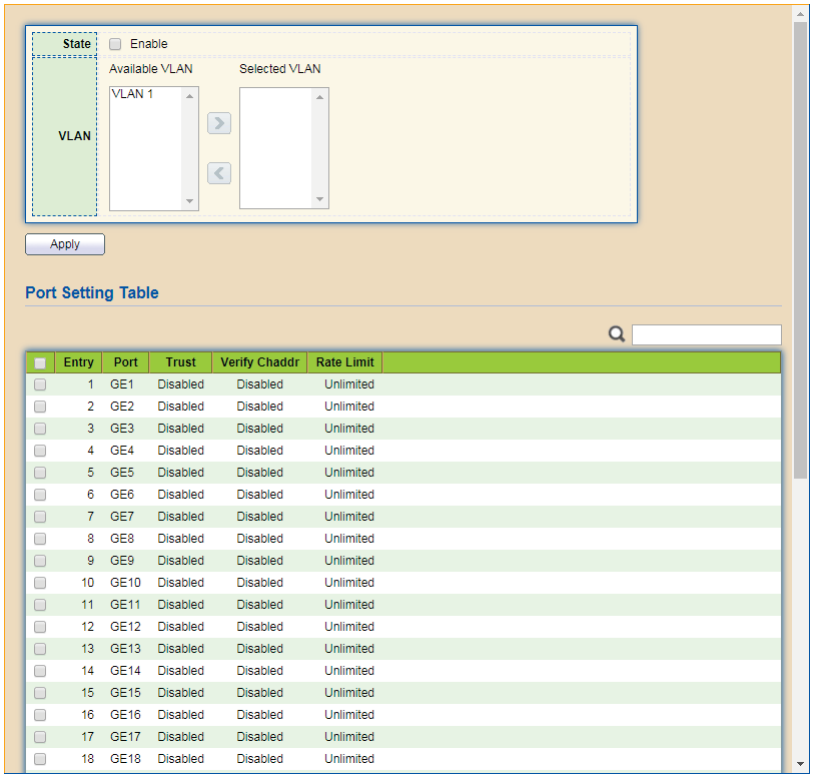


Figure 81 - Security > DHCP Snooping > Property

Item	Description
State	Click the radio button to enable global property settings.
	Click to add the desired VLANs.
	Click to delete the desired VLANs.
Apply	Click to save the values and update the screen.
	Enter the keywords to use in the search function.

Item	Description
Edit	Click to edit the DHCP port settings by entering the following data: • Trust • Verify Chaddr • Rate Limit

Statistics

The page displays all statistics recorded by DHCP snooping function.

To view the menu, navigate to Security > DHCP Snooping > Statistics.

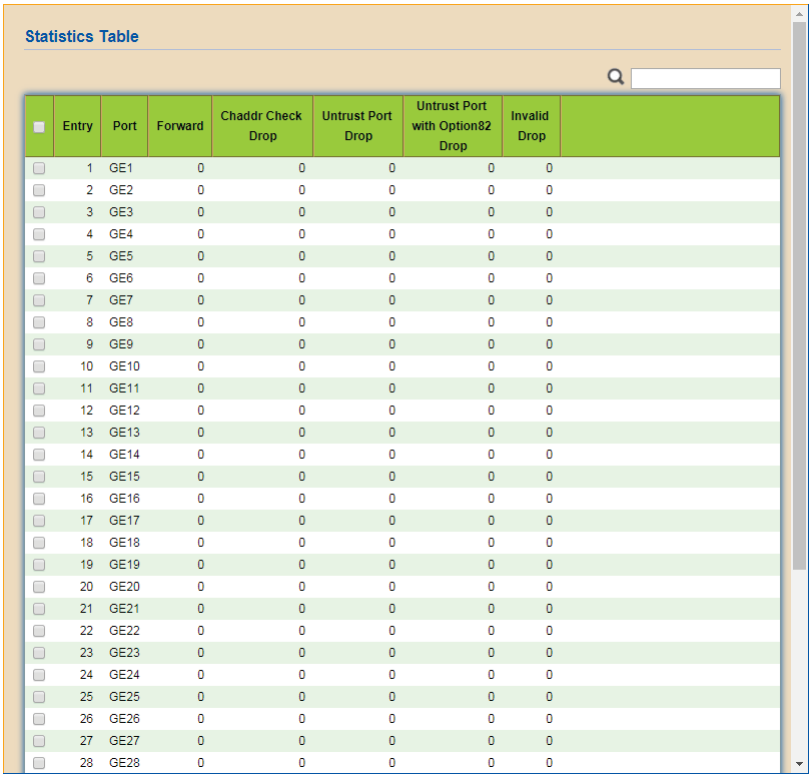


Figure 82 - Security > DHCP Snooping > Statistics

Item	Description
	Enter the keywords to use in the search function.
Clear	Click to clear the statistics table.
Refresh	Click to refresh the display.

Option82 Property

The page allows a user to set string as remote ID for DHCP option82. For example, use a switch-configured hostname or specify an ASCII text string as remote ID.

To view the menu, navigate to Security > DHCP Snooping > Option82 Property.

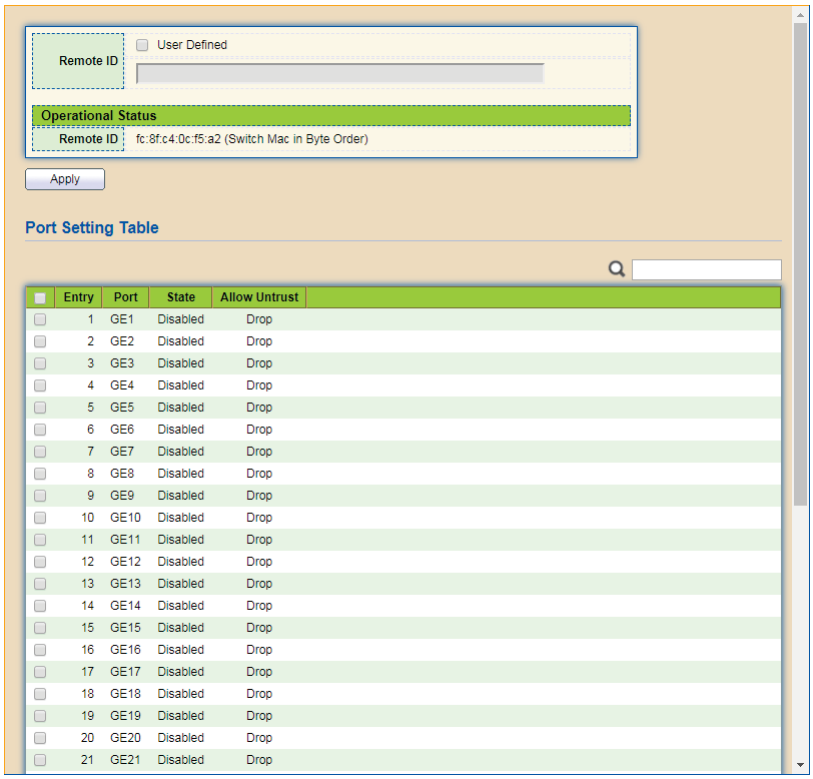


Figure 83 - Security > DHCP Snooping > Option82 Property

Item	Description
Remote ID	Check the radio button to manually set the remote ID. Enter the string to specify the remote ID.
Operational Status	
Remote ID	Display the remote ID.
Apply	Click to save the values and update the screen.
	Enter the keywords to use in the search function.
Edit	Click to edit the Option82 port settings by entering the following data: • State • Allow Untrust

Option82 Circuit ID

To view the menu, navigate to Security > DHCP Snooping > Option82 Circuit ID.

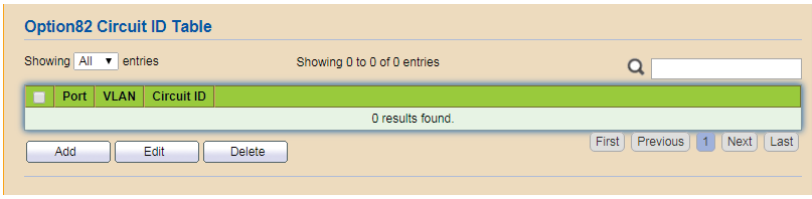


Figure 84 - Security > DHCP Snooping > Option82 Circuit ID

Item	Description
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.
Add	Click to add a new Option82 circuit ID by entering the following data: • Port • VLAN • Circuit ID
Edit	Click to edit the Option82 circuit ID settings by entering the following data: • Circuit ID
Delete	Click to delete the desired entries.

4.10.9. IP Source Guard

By using the source IP address filtering function, IP source guard can prevent a malicious host from feigning a legal host with its IP address and performing malicious attack.

Port Setting

To view the menu, navigate to Security > IP Source Guard > Port Setting.

Figure 85 - Security > IP Source Guard > Port Setting

Item	Description
	Enter the keywords to use in the search function.
Edit	Click to edit the port settings by entering the following data: • State • Verify Source • Max Entry

IMPV Binding

The page allows the network administrator to set the filtering conditions (binding type, MAC address, IPv4 address) for packets through the specified LAN port.

To view the menu, navigate to Security > IP Source Guard > IMPV Binding.

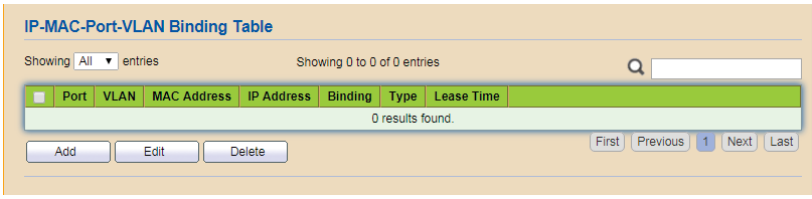


Figure 86 - Security > IP Source Guard > IMPV Binding

Item	Description
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.
Add	Click to add a new Option82 circuit ID by entering the following data: • Port • VLAN • Binding • MAC Address • IP Address
Edit	Click to edit the Option82 circuit ID settings by entering the following data: • Port • VLAN (optional) • IP Address
Delete	Click to delete the desired entries.

Save Database

The page allows the network administrator to configure the DHCP Snooping database.

To view the menu, navigate to Security > IP Source Guard > Save Database.

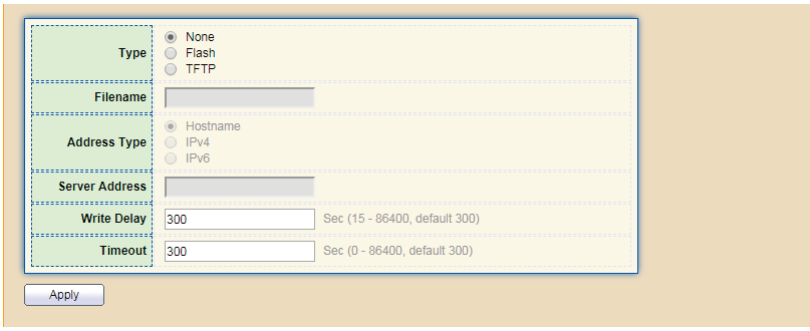


Figure 87 - Security > IP Source Guard > Save Database

Item	Description
Type	Click the radio buttons to select the database type. • None: Do not save the database. • Flash: Save the database to flash memory. • TFTP: Save the database to a TFTP server.
Filename	Enter the string to specify the file name if TFTP is used.
Address Type	Click the radio buttons to select the address type if TFTP is used. • Hostname: Use hostname as server address. • IPv4: Use IPv4 address.
Server Address	Enter an IP address or hostname of the TFTP server if TFTP is used.
Write Delay	Enter the variable to set the transfer work will be delayed, after the database is changed.
Timeout	Enter the variable to set the waiting time if it is not finished then stop the transfer process.
Apply	Click to save the values and update the screen.

4.11. ACL

An Access Control List (ACL) is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the frame is accepted.

4.11.1. MAC ACL

The page shows the Access Control List (ACL) based on Layer 2 filtering, the MAC layer. The ACL is composed by many Access Control Element (ACE) rules. You can create a new ACL here; then add multiple ACEs.

To view the menu, navigate to ACL > MAC ACL.

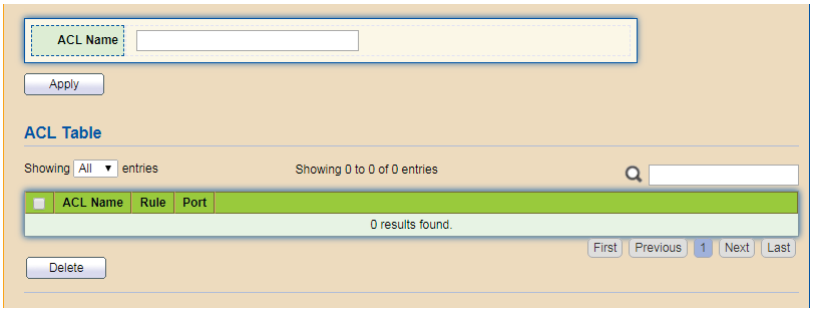


Figure 88 - ACL > MAC ACL

Item	Description
ACL Name	Enter the string to create a new MAC ACL.
Apply	Click to save the values and update the screen.
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.
Delete	Click to delete the desired entries.

4.11.2. MAC ACE

The page shows ACE based on MAC address. You may choose ACL, permit, and deny particular packet or frame, even shutdown the port.

To view the menu, navigate to ACL > MAC ACE.

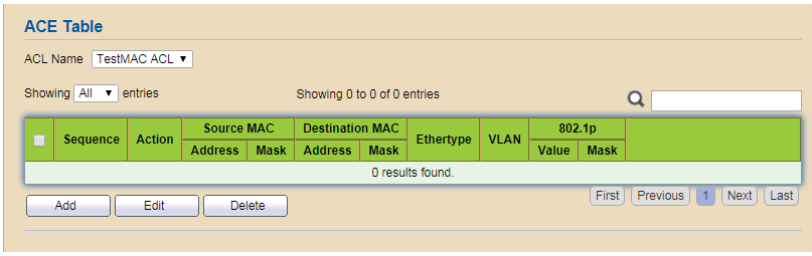


Figure 89 - ACL > MAC ACE

Item	Description
ACL Name	Click the drop-down menu to select the defined MAC ACL.
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.
Add	Click to add a new MAC ACE by entering the following data: • Sequence • Action • Source MAC • Destination MAC • Ethertype • VLAN • 802.1p
Edit	Click to edit the MAC ACE settings by entering the following data: • Action • Source MAC • Destination MAC • Ethertype • VLAN • 802.1p
Delete	Click to delete the desired entries.

4.11.3. IPv4 ACL

The page shows the Access Control List (ACL) based on Layer 2 to Layer 4 filtering, the IPv4. The ACL is composed by many Access Control Element (ACE) rules. You may create a new ACL here; then add multiple ACEs.

To view the menu, navigate to ACL > IPv4 ACL.

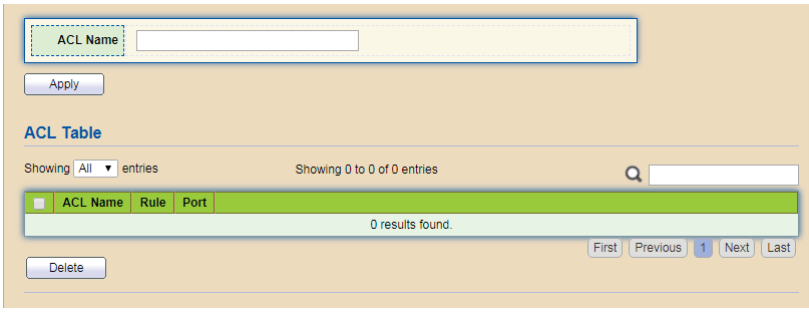


Figure 90 - ACL > IPv4 ACL

Item	Description
ACL Name	Enter the string to create a new IPv4 ACL.
Apply	Click to save the values and update the screen.
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.
Delete	Click to delete the desired entries.

4.11.4. IPv4 ACE

This page shows ACE based on IPv4 address. You may choose ACL, permit, and deny particular packet or frame, even shutdown the port.

To view the menu, navigate to ACL > IPv4 ACE.

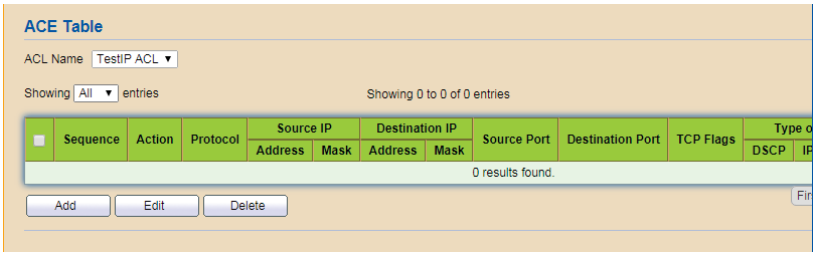


Figure 91 - ACL > IPv4 ACE

Item	Description
ACL Name	Click the drop-down menu to select the defined IPv4 ACL.
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).

Item	Description
Add	Click to add a new IPv4 ACE by entering the following data: • Sequence • Action • Source MAC • Protocol • Source IP • Destination IP • Type of Service • Source Port • Destination Port • TCP Flags • ICMP Type • ICMP Code
Edit	Click to edit the IPv4 ACE settings by entering the following data: • Action • Source MAC • Protocol • Source IP • Destination IP • Type of Service • Source Port • Destination Port • TCP Flags • ICMP Type • ICMP Code
Delete	Click to delete the desired entries.

4.11.5. ACL Binding

The page allows you to bind Access Control Lists created in previous section to an interface (physical port or aggregation).

To view the menu, navigate to ACL > ACL Binding.

Figure 92 - ACL > ACL Binding

Item	Description
	Enter the keywords to use in the search function.
Bind	Click to bind ACL for the desired entries.
Unbind	Click to unbind ACL for the desire entries.
Edit	Click to edit the ACL binding settings by entering the following data: • MAC ACL • IPv4 ACL

4.12. QoS

QoS (Quality of Service) functions to provide different quality of service for various network applications and requirements and optimize the bandwidth resource distribution so as to provide a network service experience of a better quality.

4.12.1. General

Property

To view the menu, navigate to QoS > General > Property.

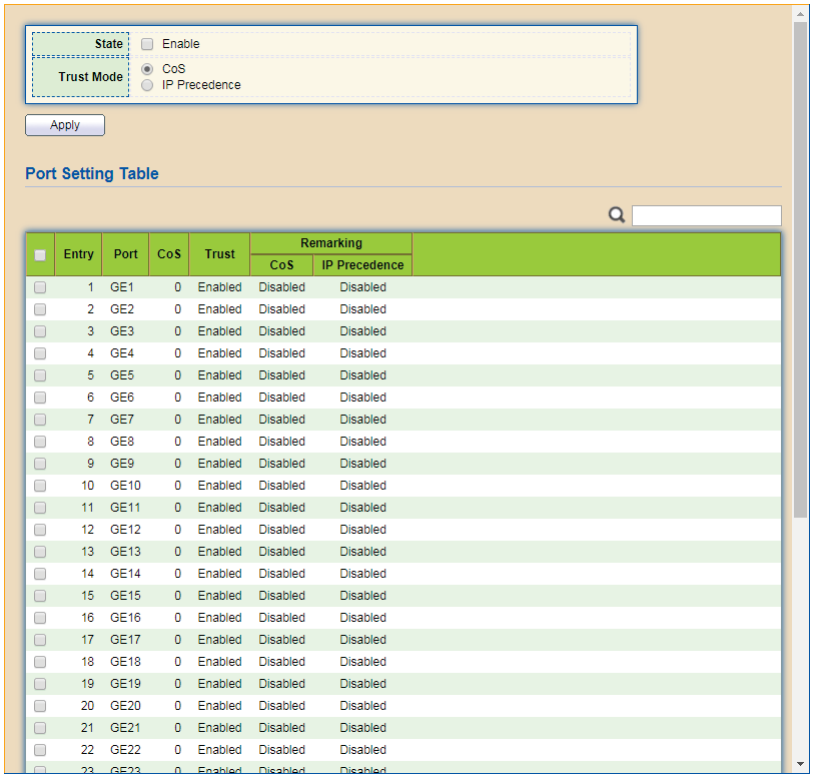


Figure 93 - QoS > General > Property

Item	Description
State	Click the radio button to enable the function.
Trust Mode	Click the radio buttons to select the QoS operation mode. • CoS: Traffic is mapped to queues based on the CoS field in the VLAN tag, or based on the per-port default CoS value if there is no VLAN tag on the incoming packet. • IP Precedence: All IP traffic is mapped to queues based on the DSCP field in the IP header. If traffic is not IP but has VLAN tag, mapped to queues based on the CoS value in the VLAN tag.
Apply	Click to save the values and update the screen.

Item	Description
	Enter the keywords to use in the search function.
Edit	Click to edit the QoS port settings by entering the following data: • CoS • Trust • CoS • IP Precedence

Queue Scheduling

The device supports multiple queues for each interface. The higher numbered queue represents the higher priority. The following lists the types of supported priority queue:

- Strict Priority (SP): Egress traffic from the higher priority queue will be transmitted first, lower priority queue shall wait until all traffic in SP queue is transmitted.
- Weighted Round Robin (WRR): The number of packets sent from the queue is proportional to the weight of the queue.

To view the menu, navigate to QoS > General > Queue Scheduling.

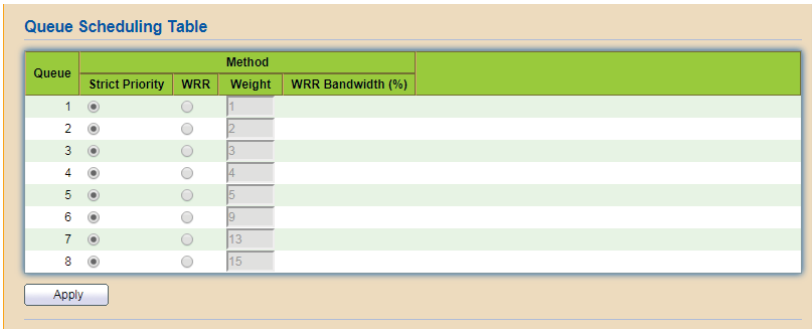


Figure 94 - QoS > General > Queue Scheduling

Item	Description
Strict Priority	Click the radio button to set queue to strict priority type.
WRR	Click the radio button to set queue to weight round robin (WRR) type.
Weight	Enter the variable to set the queue weight for the queue if the queue type is WRR.
WRR Bandwidth (%)	Display the percentage of traffic which can be sent by current queue compared to total WRR queues.
Apply	Click to save the values and update the screen.

CoS Mapping

The page allows user to configure how ingress frames with CoS/802.1p tag map to QoS queues, and QoS queues to CoS/802.1p on egress frames.

Actual effectiveness is based on how QoS is configured in previous QoS section. This page provides settings for the user to configure mapping only.

To view the menu, navigate to QoS > General > CoS Mapping.

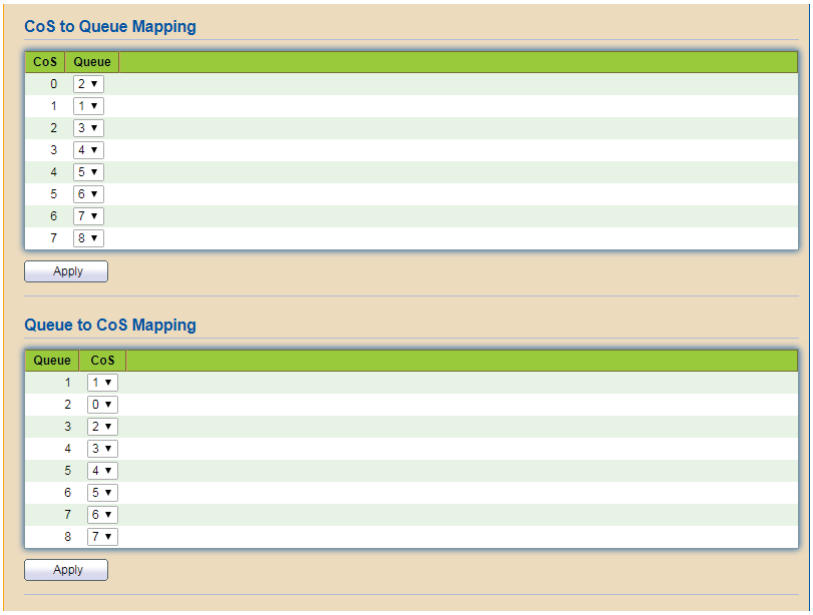


Figure 95 - QoS > General > CoS Mapping

Item	Description
CoS to Queue Mapping	
Queue	Click the drop-down menu to define the queue ID for the different class of service values.
Apply	Click to save the values and update the screen.
Queue to CoS Mapping	
CoS	Click the drop-down menu to define the class of service value.
Apply	Click to save the values and update the screen.

IP Precedence Mapping

The page allows user to configure how ingress packets with IP Precedence tag map to QoS queues, and QoS queues to IP Precedence on egress packets.

Actual effectiveness is based on how QoS is configured in previous QoS section. This page provides settings for user to configure mapping only.

To view the menu, navigate to QoS > General > IP Precedence Mapping.

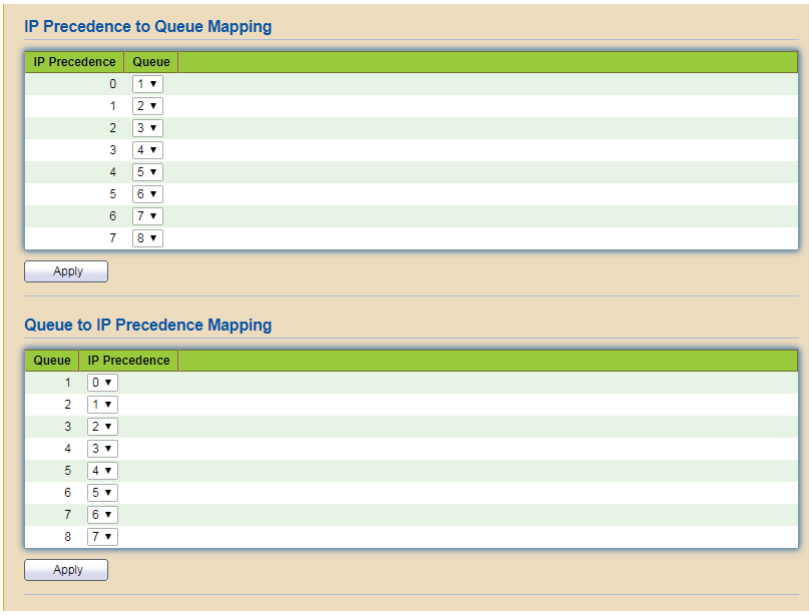


Figure 96 - QoS > General > IP Precedence Mapping

Item	Description
IP Precedence to Queue Mapping	
Queue	Click the drop-down menu to define the queue ID for the different IP Precedence values.
Apply	Click to save the values and update the screen.
Queue to IP Precedence Mapping	
IP Precedence	Click the drop-down menu to define the different IP Precedence values.
Apply	Click to save the values and update the screen.

4.12.2. Rate Limit

Ingress / Egress Port

The page allows a user to configure ingress/egress port rate limit.

The ingress rate limit is the number of bits per second that can be received from the ingress interface. Excess bandwidth above this limit is discarded. The configuration result for each port will be displayed on the table listed on the lower side of this web page.

The egress rate limit is the number of bits per second that can be received from the egress interface. Excess bandwidth above this limit is discarded.

To view the menu, navigate to QoS > Rate Limit > Ingress / Egress Port.

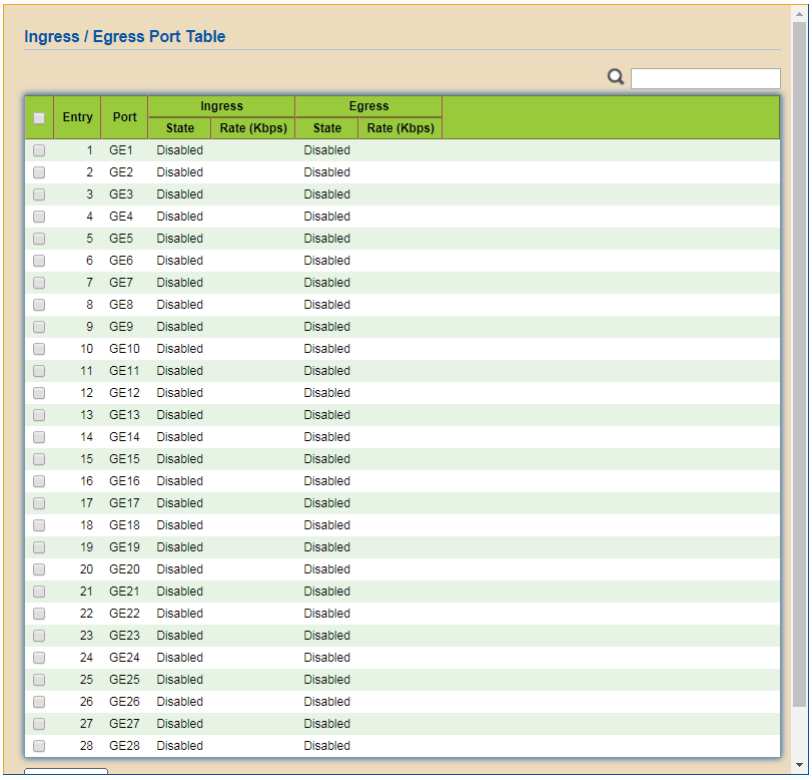


Figure 97 - QoS > Rate Limit > Ingress / Egress Port

Item	Description
	Enter the keywords to use in the search function.
Edit	Click to edit the Ingress / Egress port settings by entering the following data: • Ingress • Egress

4.13. Diagnostics

4.13.1. Logging

Property

To view the menu, navigate to Diagnostics > Logging > Property.

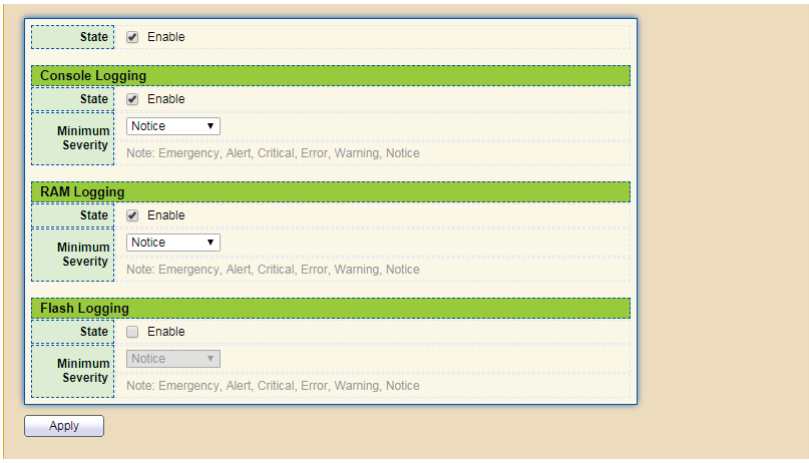


Figure 98 - Diagnostics > Logging > Property

Item	Description
State	Click the radio button to enable the logging function.
Console Logging	
State	Click the radio button to enable the logging function.
Minimum Severity	Click the drop-down menu to select the severity of message which you want to filter out for review.
RAM Logging	
State	Click the radio button to enable the logging function.
Minimum Severity	Click the drop-down menu to select the severity of message which you want to filter out for review.
Flash Logging	
State	Click the radio button to enable the logging function.
Minimum Severity	Click the drop-down menu to select the severity of message which you want to filter out for review.
Apply	Click to save the values and update the screen.

Remote Server

To view the menu, navigate to Diagnostics > Logging > Remote Server.

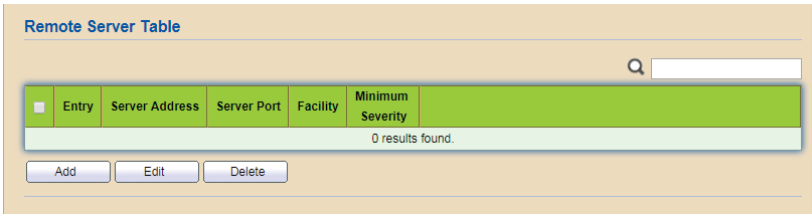


Figure 99 - Diagnostics > Logging > Remote Server

Item	Description
	Enter the keywords to use in the search function.
Add	Click to add a new remote server by entering the following data: • Address Type • Server Address • Server Port • Facility • Minimum Severity
Edit	Click to edit the remote server settings by entering the following data: • Server Port • Facility • Minimum Severity
Delete	Click to delete the desired entries.

4.13.2. Mirroring

To view the menu, navigate to Diagnostics > Mirroring.

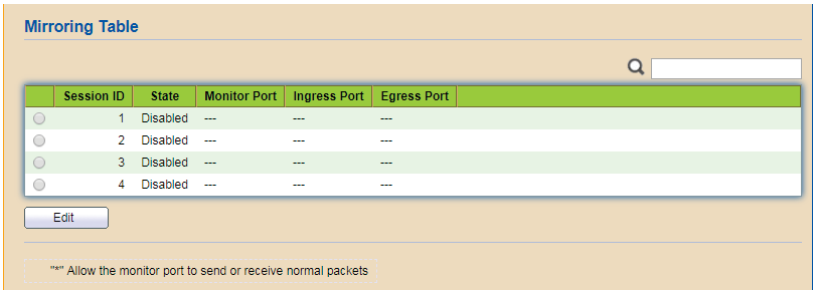


Figure 100 - Diagnostics > Mirroring

Item	Description
	Enter the keywords to use in the search function.
Edit	Click to edit the mirroring settings by entering the following data: • State • Monitor Port • Ingress Port • Egress Port

4.13.3. Ping

After the ping test is complete, the results from the test are displayed as seen in the following figure under Ping Results.

To view the menu, navigate to Diagnostics > Ping.

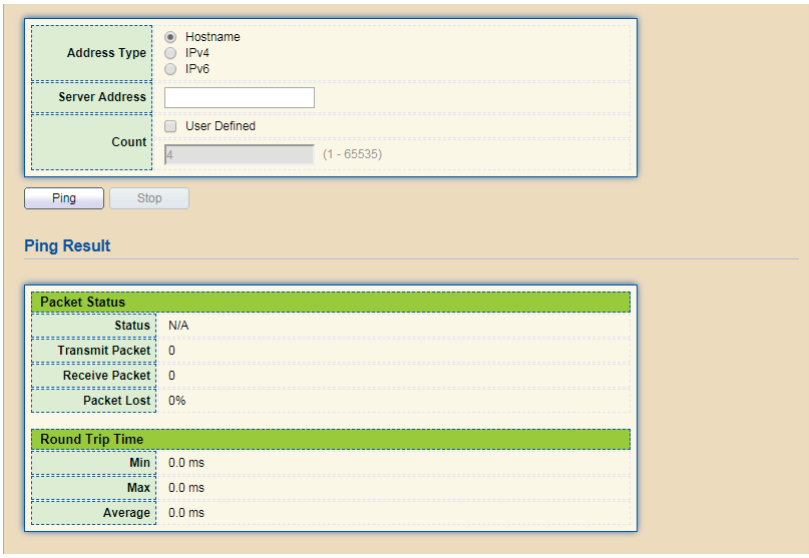


Figure 101 - Diagnostics > Ping

Item	Description
Address Type	Click the radio buttons to select the IP address type for sending ping to check if network path is ok.
Server Address	Enter the hostname or IP address of SNMP server based on the protocol selected above.
Count	Specify the total numbers of ICMP ping packets to be sent.
Ping	Click to perform ping action.
Stop	Click to terminate ping action.

4.13.4. Traceroute

To view the menu, navigate to Diagnostics > Traceroute.

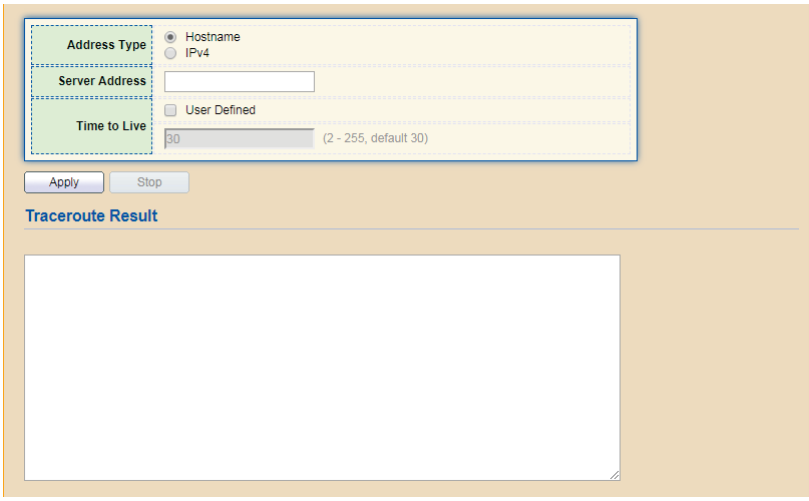


Figure 102 - Diagnostics > Traceroute

Item	Description
Address Type	Click the radio buttons to select the IP address type for sending ping to check if the network path is ok.
Server Address	Enter the hostname or IP address of the SNMP server based on the protocol selected above.
Time to Live	Click User Defined and enter the value in seconds (2 - 255, default: 30) to set Time to Live. The value, alternatively known as the hop limit, is used to determine the intermediate routers crossed towards the final destination.
Apply	Click to perform traceroute action.
Stop	Click to terminate traceroute action.

4.13.5. Copper Test

To view the menu, navigate to Diagnostics > Copper Test.

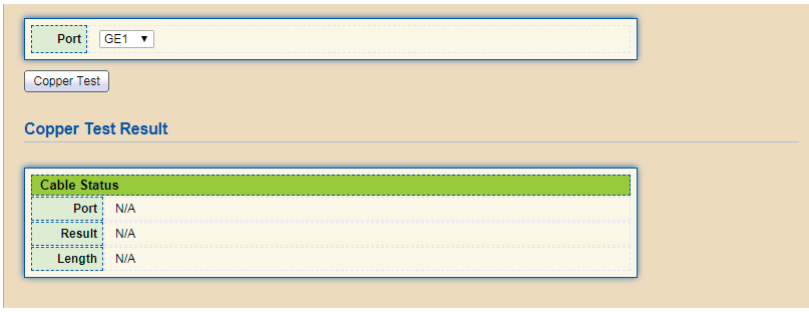


Figure 103 - Diagnostics > Copper Test

Item	Description
Port	Click the drop-down menu to select the port for copper test.
Copper Test	Click to perform the copper test action.

4.13.6. Fiber Module

To view the menu, navigate to Diagnostics > Fiber Module.

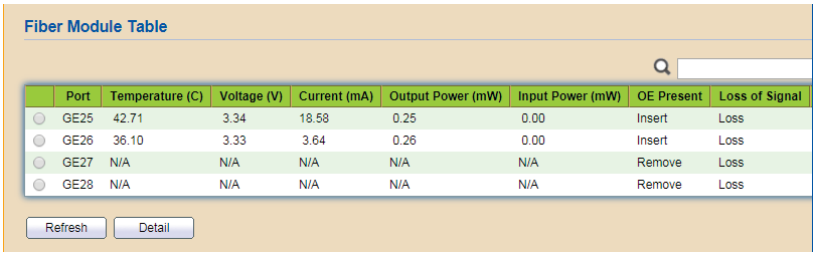


Figure 104 - Diagnostics > Fiber Module

Item	Description
	Enter the keywords to use in the search function.
Refresh	Click to refresh the display.
Detail	Click to display the details for the desired port.

4.13.7. UDLD

Property

To view the menu, navigate to Diagnostics > UDLD > Property.

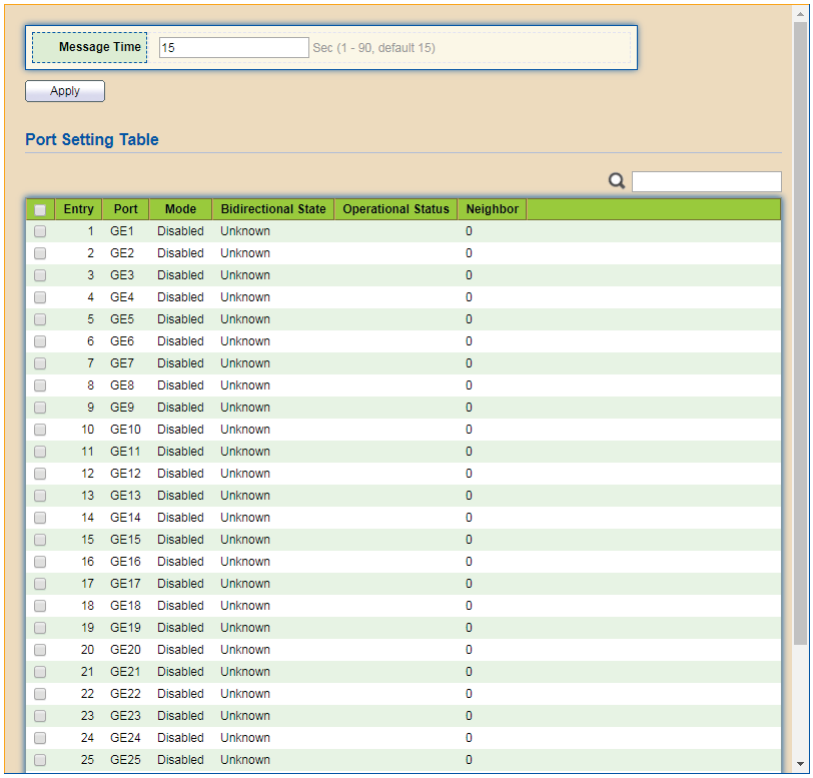


Figure 105 - Diagnostics > UDLD > Property

Item	Description
Message Time	Enter the variable to specify the message time.
Apply	Click to save the values and update the screen.
	Enter the keywords to use in the search function.
Edit	Click to edit the UDID port settings by entering the following data: • Mode

Neighbor

To view the menu, navigate to Diagnostics > UDLD > Neighbor.

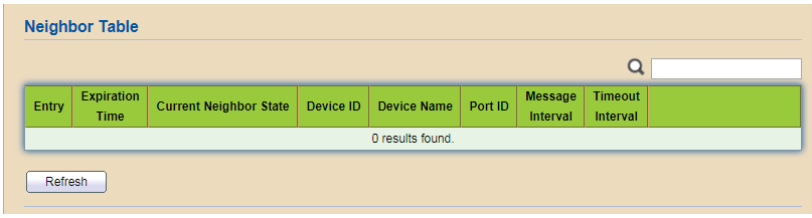


Figure 106 - Diagnostics > UDLD > Neighbor

Item	Description
	Enter the keywords to use in the search function.
Refresh	Click to refresh the display.

4.14. Management

4.14.1. User Account

To view the menu, navigate to Management > User Account.

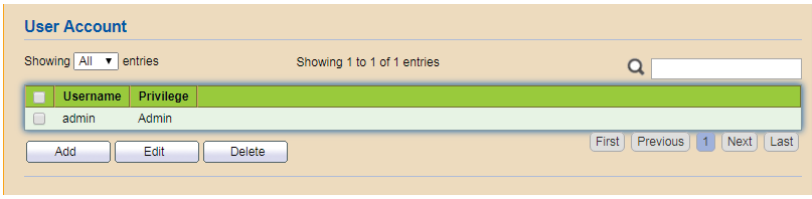


Figure 107 - Management > User Account

Item	Description
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.
Add	Click to add a new user account by entering the following data: • Username • Password • Confirm Password • Privilege

Item	Description
Edit	Click to edit the user account settings by entering the following data: • Password • Confirm Password • Privilege
Delete	Click to delete the desired entries.

4.14.2. Firmware

Upgrade / Backup

The page allows a user to upgrade or backup the firmware image on the device to remote TFTP server or host file stem through HTTP protocol.

To view the menu, navigate to Management > Firmware > Upgrade / Backup.

Figure 108 - Management > Firmware > Upgrade / Backup

Item	Description
Action	Click the radio buttons to select upgrade firmware or backup firmware.
Method	Click the radio buttons to select upgrade method. • TFTP: Using TFTP to upgrade firmware. • HTTP: Using WEB browser to upgrade firmware.
Address Type	It is available when TFTP is selected as Method. Click the radio buttons to select the IP address type for upgrading or backing up firmware.
Server Address	It is available when TFTP is selected as Method. Enter the hostname or IP address for the TFTP server.
Filename	It is available when TFTP is selected as Method. Enter the firmware image name on the TFTP server.
Filename	It is available when HTTP is selected as Method. Click Browse... to choose the firmware located in your computer.
Apply	Click to save the values and update the screen.

Active Image

To view the menu, navigate to Management > Firmware > Active Image.

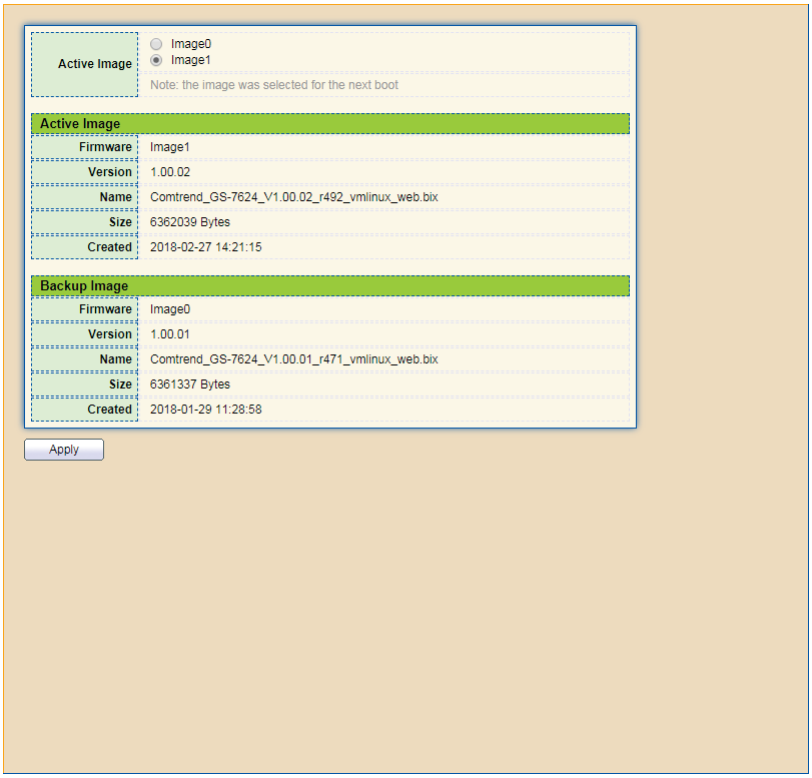


Figure 109 - Management > Firmware > Active Image

Item	Description
Active Image	Click the radio buttons to select as primary firmware.
Apply	Click to save the values and update the screen.

4.14.3. Configuration

Upgrade / Backup

To view the menu, navigate to Management > Configuration > Upgrade / Backup.

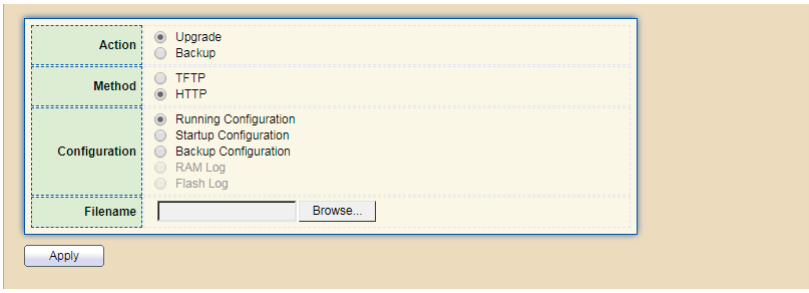


Figure 110 - Management > Configuration > Upgrade / Backup

Item	Description
Action	Click the radio buttons to select upgrade firmware or backup configuration.
Method	Click the radio buttons to select upgrade method. • TFTP: Using TFTP to upgrade configuration. • HTTP: Using WEB browser to upgrade configuration.
Configuration	Click the radio buttons to select the configuration type.
Address Type	It is available when TFTP is selected as the Method. Click the radio buttons to select the IP address type for upgrading or backing up the configuration.
Server Address	It is available when TFTP is selected as the Method. Enter the hostname or IP address for the TFTP server.
Filename	It is available when TFTP is selected as the Method. Enter the firmware image name on the TFTP server.
Filename	It is available when HTTP is selected as the Method. Click Browse... to choose the configuration file located in your computer.
Apply	Click to save the values and update the screen.

Save Configuration

Standard industrial switch devices save running configuration settings in RAM. The Save Configuration function provides setting option to save the running configuration from RAM to FLASH or even FLASH to RAM.

To view the menu, navigate to Management > Configuration > Save Configuration.

Figure 111 - Management > Configuration > Save Configuration

Item	Description
Source File	Select to define the Save Configuration function. First select a source file and then how it is to be specified. • Running Configuration: Refers to the configuration settings stored in RAM. • Startup Configuration: Refers to the configuration sequence in the defined startup file. The file is stored in nonvolatile storage, typically named with a suffix *.cfg. • Backup Configuration: Refers to the configuration sequence in the defined backup file. The file is stored in nonvolatile storage, typically named with a suffix *.cfg.
Destination File	Select to define the Destination File. The settings determine the use of the Source File sequence.
Apply	Click 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 device.
Restore Factory Default	Click to return factory default settings.

Unless the Running Configuration is copied to the Startup Configuration, rebooting the device removes all changes since last save. Save the Running Configuration to the Startup Configuration before logging off to preserve any changes made during the current session.

4.14.4. SNMP

Simple Network Management Protocol (SNMP) is an "Internet-standard protocol for managing devices on IP networks". Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks and more.

SNMP is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

An SNMP-managed network consists of three key components:

- Managed device
- Agent - software which runs on managed devices
- Network management station (NMS) - software which runs on the manager

A managed device is a network node that implements an SNMP interface that allows unidirectional (read-only) or bidirectional (read and write) access to node-specific information. Managed devices exchange node-specific information with the NMSs. Sometimes called network elements, the managed devices can be any type of device, including, but not limited to, routers, access servers, switches, bridges, hubs, IP telephones, IP video cameras, computer hosts, and printers.

An agent is a network-management software module that resides on a managed device. An agent has local knowledge of management information and translates that information to or from an SNMP-specific form.

A network management station (NMS) executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs may exist on any managed network.

View

This page allows the network administrator to create MIB views (Management information base) and then include or exclude OID (Object Identifier) in a view.

To view the menu, navigate to Management > SNMP > View.

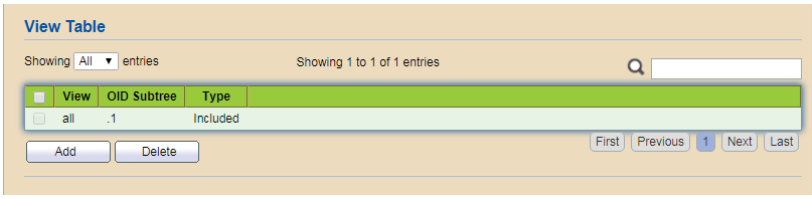


Figure 112 - Management > SNMP > View

Item	Description
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.
Add	Click to add a new MIB view by entering the following data: • View • OID Subtree • Type
Delete	Click to delete the desired entries.

Group

This page allows the network administrator to group SNMP users and assign different authorization and access privileges.

To view the menu, navigate to Management > SNMP > Group.

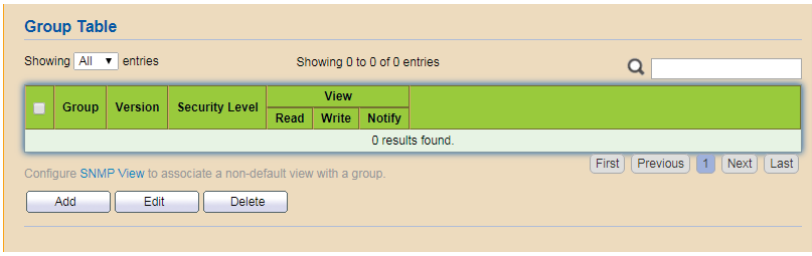


Figure 113 - Management > SNMP > Group

Item	Description
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.

Item	Description
Add	Click to add a new SNMP group by entering the following data: • Group • Version • Security Level • View
Edit	Click to edit the SNMP group settings by entering the following data: • Version • Security Level • View
Delete	Click to delete the desired entries.

Community

The page allows a user to add/remove multiple communities of SNMP.

To view the menu, navigate to Management > SNMP > Community.

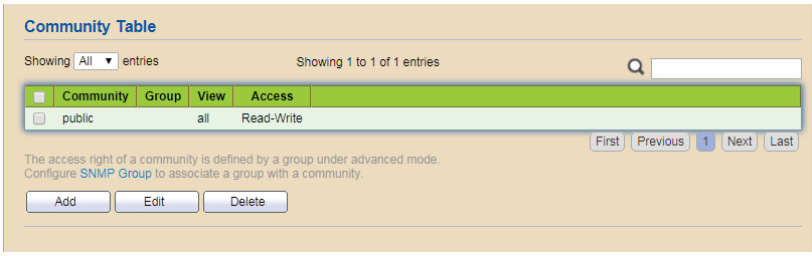


Figure 114 - Management > SNMP > Community

Item	Description
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.
Add	Click to add a new SNMP community by entering the following data: • Community • Type • View • Access • Group

Item	Description
Edit	Click to edit the SNMP community settings by entering the following data: • Type • View • Access • Group
Delete	Click to delete the desired entries.

User

The page allows a user to configure SNMP user profile.

To view the menu, navigate to Management > SNMP > User.

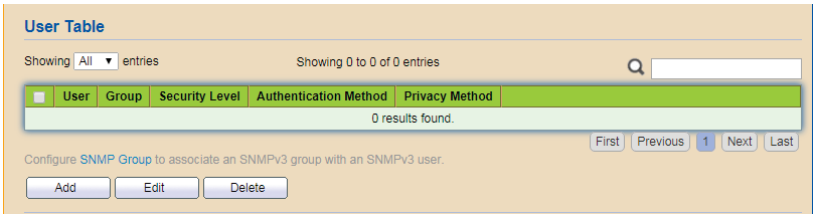


Figure 115 - Management > SNMP > User

Item	Description
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.
Add	Click to add a new SNMP user by entering the following data: • User • Group • Security Level • Method • Password
Edit	Click to edit the SNMP user settings by entering the following data: • Group • Security Level • Method • Password
Delete	Click to delete the desired entries.

Engine ID

The page allows a user to configure and display SNMP local engine ID.

To view the menu, navigate to Management > SNMP > Engine ID.

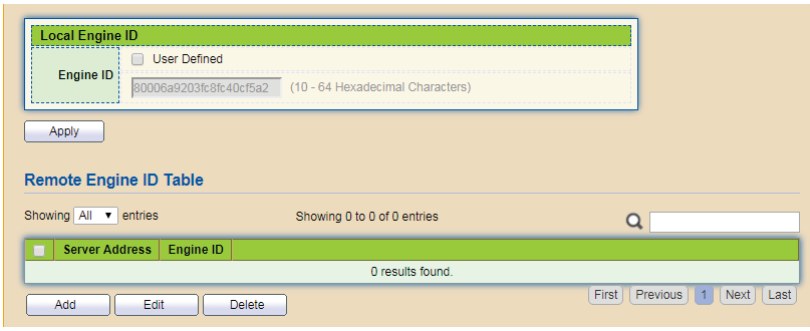


Figure 116 - Management > SNMP > Engine ID

Item	Description
Local Engine ID	
Engine ID	Click the radio button to enable manually specified local engine ID. Enter the string to defined the engine ID.
Apply	Click to save the values and update the screen.
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.
Add	Click to add a new remote engine ID by entering the following data: • Address Type • Server Address • Engine ID
Edit	Click to edit the remote engine ID settings by entering the following data: • Engine ID
Delete	Click to delete the desired entries.

Trap Event

The page allows a user to add or delete an SNMP trap receiver IP address and community name.

To view the menu, navigate to Management > SNMP > Trap Event.

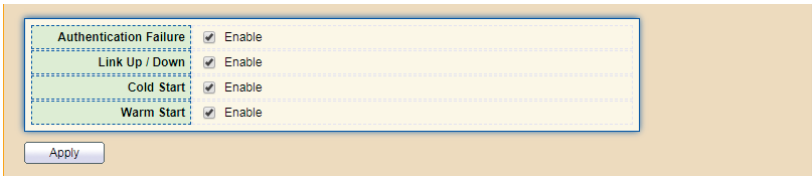


Figure 117 - Management > SNMP > Trap Event

Item	Description
Authentication Failure	Click the radio button to reboot the device when encountering authentication failure (including community not match or user password not match).
Link Up / Down	Click the radio button to reboot the device while encountering port link up or down trap.
Cold Start	Click the radio button to reboot the device while encountering user trap.
Warm Start	Click the radio button to reboot the device while encountering power down trap.
Apply	Click to save the values and update the screen.

Notification

The page allows a user to configure a host to receive SNMPv1/v2/v3 notification.

To view the menu, navigate to Management > SNMP > Notification.

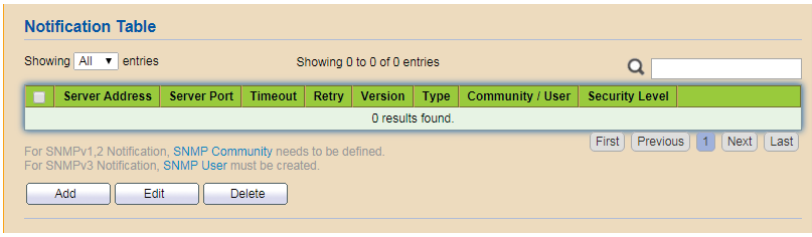


Figure 118 - Management > SNMP > Notification

Item	Description
Showing	Click the drop-down menu to select the number of entries to display (All, 10, 30, 50, 100).
	Enter the keywords to use in the search function.

Item	Description
Add	Click to add a new SNMP user by entering the following data: • Address Type • Server Address • Version • Type • Community / User • Security Level • Server Port • Timeout • Retry
Edit	Click to edit the SNMP user settings by entering the following data: • Version • Type • Community / User • Security Level • Server Port • Timeout • Retry
Delete	Click to delete the desired entries.

4.14.5. Time Range

To view the menu, navigate to Management > Time Range.

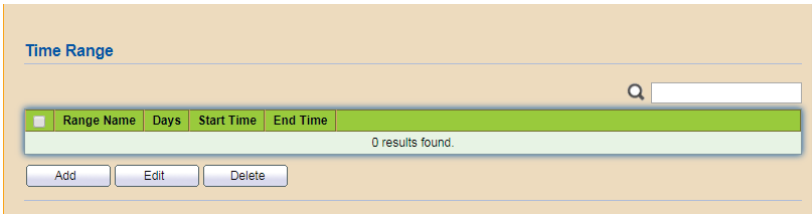


Figure 119 - Management > Time Range

Item	Description
	Enter the keywords to use in the search function.
Add	Click to add a new time range by entering the following data: • Range Name • Date
Edit	Click to edit the time range settings by entering the following data: • Date
Delete	Click to delete the desired entries.

5. Federal Communication Commission Interference Statement

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

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

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

FCC Caution

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE). The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Bulgaria, Cyprus, Czech, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Turkey, and United Kingdom. The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not Intended for Use

None

Protect Our Environment

When the equipment has reached the end of its useful life, it must be taken to a recycling center and processed separate from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this switch can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with your household waste; you may be subject to penalties or sanctions under the law.