Version 1.00 | 2025/06/18

Web UI Manual

Metro Ethernet Switch Series

DGS-1210/ME

Table of Contents

About This Guide

This guide provides step-by-step instructions on how install the D-Link DGS-1210/ME Cx Metro Management Ethernet Switches, how to use the Web Utility, and how to perform web-based management functions.

Note: The actual device purchased may appear slightly different from the illustrations shown in the document. Refer to the Product Instruction and Technical Specification sections for detailed information about the switch, its components, network connections, and technical specifications.

This guide is mainly divided into three parts:

1. Hardware Installation: Step-by-step hardware installation procedures.
2. Getting Started: A startup guide for basic switch installation and settings.
3. Configuration: Information about the function descriptions and configuration settings.

Terms/Usage

In this guide, the term “Switch” (first letter capitalized) refers to DGS-1210/ME Cx Metro Management Ethernet Switch, and “switch” (first letter lower case) refers to other Ethernet switches. Some technologies refer to terms “switch”, “bridge” and “switching hubs” interchangeably, and both are commonly accepted for Ethernet switches.

A **NOTE** indicates important information that helps a better use of the device.

A **CAUTION** indicates potential property damage or personal injury.

Copyright and Trademarks

Information in this document is subjected to change without notice.

© 2025 D-Link Corporation. All rights reserved.

Reproduction in any manner whatsoever without the written permission of D-Link Corporation is strictly forbidden.

Trademarks used in this text: D-Link and the D-LINK logo are trademarks of D-Link Corporation; Microsoft and Windows are registered trademarks of Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. D-Link Corporation disclaims any proprietary interest in trademarks and trade names other than its own.

1 Product Introduction

- *Switch Description*
- *Front Panel Description*
- *LED Indicators*
- *Rear Panel Description*
- *Side Panel Description*
- *Connecting the DPS-200A/500A/500DC to the RPS Port (for DGS-1210-10X/10XS/28X/28XS/52X/ME only)*
- *Installing the RPS into the Rack-mount Chassis*

Switch Description

The DGS-1210/ME Cx Metro Management Ethernet Switch is equipped with **Copper ports** (10/100/1000Mbps), **SFP ports** (1000Mbps), **SFP+ ports** (10Gbps) and **10G combo ports** that can be used to attach various networking devices to the network like Computers, Notebooks, Print Servers, Network Attached Storage devices, IP Cameras, VoIP PBX devices, and other Switches. The Small Form Factor Portable (SFP) ports can be used together with fiber-optical transceivers in order to connect various other networking devices, using a fiber-optic connection, to the network at Gigabit Ethernet speeds over great distances.

This DGS-1210/ME Cx Metro Management Ethernet Switch provides unsurpassed performance, fault tolerance, scalability, robust security, standard-based interoperability and impressive technology to future-proof departmental and enterprise network deployments.

It allows IGMP Snooping and Authentication, QoS, Bandwidth Control, ACL and many security functions. It can be managed by Web UI, or commands via Telnet.

The DGS-1210/ME Cx Metro Management Ethernet Switches have different port configuration (10/100/1000Base-T or SFP ports) that may be used in to uplink various network devices to the Switch, including PCs, hubs and other switches to provide a gigabit Ethernet uplink in full-duplex mode. The SFP (Small Form Factor Portable) ports are used with fiber-optical transceiver cabling in order to uplink various other networking devices for a gigabit link that may span great distances.

Front Panel Description

The front panel of the **DGS-1210-10X/ME** switch consists out of the following:

- 8 10/100/1000Mbps Copper Ports
- 2 1000Mbps/10Gbps SFP ports
- One RJ-45 Console Port
- LEDs for Power, Console, RPS, Link/Act for port 1 ~ 10

Figure 1.1 – DGS-1210-10X/ME Front Panel

CAUTION: The MiniGBIC ports should use UL listed Optical Transceiver product, Rated Laser Class I. 3.3Vdc.

The front panel of the **DGS-1210-10XP/ME** switch consists out of the following:

- 8 10/100/1000Mbps Copper Ports
- 2 1000Mbps/10Gbps SFP+ ports
- One RJ-45 Console Port
- LEDs for Power, PoE Max, Console, Link/Act for port 1 ~ 10

- Mode: By pressing the Mode button, the Port LED will switch between Link/Act and PoE modes.

Figure 1.2 – DGS-1210-10XP/ME Front Panel

CAUTION: The MiniGBIC ports should use UL listed Optical Transceiver product, Rated Laser Class I. 3.3Vdc.

The front panel of the **DGS-1210-10XS/ME** switch consists out of the following:

- 8 10/100/1000Mbps Copper Ports
- 2 100/1000/2.5G/5G/10G Copper ports (port 9 and port 10)
- 2 1000Mbps/10Gbps SFP+ ports
- One RJ-45 Console Port
- LEDs for Power, Console, RPS, Link/Act for port 1 ~ 10

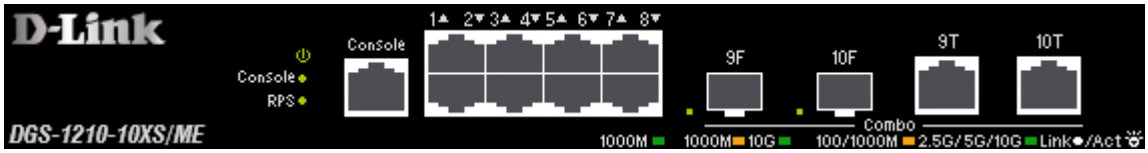


Figure 1.3 – DGS-1210-10XS/ME Front Panel

CAUTION: The MiniGBIC ports should use UL listed Optical Transceiver product, Rated Laser Class I. 3.3Vdc.

The front panel of the **DGS-1210-28X/ME** switch consists out of the following:

- 24 10/100/1000Mbps Copper Ports
- 4 1000Mbps/10Gbps SFP+ ports
- One RJ-45 Console Port
- LEDs for Power, Console, RPS, Link/Act for port 1 ~ 28

Figure 1.3 – DGS-1210-28X/ME Front Panel

CAUTION: The MiniGBIC ports should use UL listed Optical Transceiver product, Rated Laser Class I. 3.3Vdc.

The front panel of the **DGS-1210-28XS/ME** switch consists out of the following:

- 24 1000Mbps SFP ports
- 4 1000Mbps/10Gbps SFP+ ports
- One RJ-45 Console Port
- LEDs for Power, Console, RPS, Link/Act for port 1 ~ 20

Figure 1.4 – DGS-1210-28XS/ME Front Panel

CAUTION: The MiniGBIC ports should use UL listed Optical Transceiver product, Rated Laser Class I. 3.3Vdc.

The front panel of the **DGS-1210-52X/ME** switch consists out of the following:

- 48 10/100/1000Mbps Copper Ports
- 4 1000Mbps/10Gbps SFP+ ports
- One RJ-45 Console Port
- LEDs for Power, RPS, Console, Link/Act for port 1 ~ 52

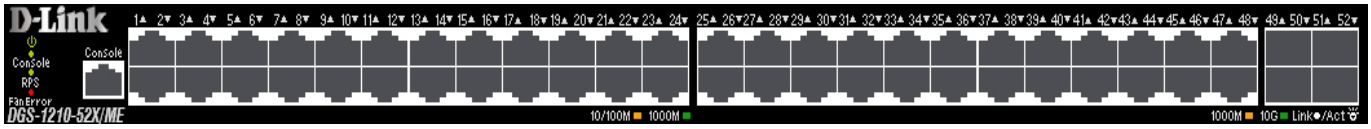


Figure 1.5 – DGS-1210-52X/ME Front Panel

CAUTION: The MiniGBIC ports should use UL listed Optical Transceiver product, Rated Laser Class I. 3.3Vdc.

T

LED Indicators

The Switch supports LED indicators for Power, Console, Fan, and Link/Act for each port. The following shows the LED indicators for the DGS-1210/ME CX Metro Management Ethernet Switch along with an explanation of each indicator.

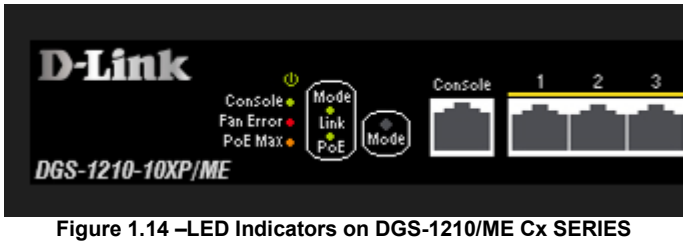


Figure 1.14 –LED Indicators on DGS-1210/ME Cx SERIES

Location	LED Indicative	Status	Description
Per Device	Power	Solid Green	Device Power On
		Light off	Device Power Off
	Console	Solid Green	RJ-45 Console on
		Light off	Console off
	RPS	Solid Green	RPS in use
		Light off	RPS off
	Fan Error	Solid Red	The fan has run time failure and is brought offline
		Light Off	All fan work normally
	PoE Max (DGS-1210-10XP/ME,	Solid Amber	Total power output exceeds Guard Band threshold. The PD will be denied based on port priority or other PoE rules

		Blinking Amber	When the available PoE power is more than the guard band power, the Max LED will blink for 5 seconds
		Light off	The PoE power is sufficient and below the guard band threshold
LED Mode = “Link/Act” LED Per 10/100/1000 Mbps copper Port (Dual LED with single color)	Link/ Act / Speed Status	Left	Solid Green: When there is a secure 1000 Mbps connection running at the port. Blinking Green: When there is reception or transmission running at 1000 Mbps at the port.
		Right	Solid Amber: When there is a secure 10/100 Mbps connection running at the port. Blinking Amber: When there is reception or transmission running at 10/100 Mbps at the port.
		Light Off	No link
LED Mode = “Link/Act” LED or “PoE “	Link/Act Mode	Light	Solid Green: When LED Mode button is Up
	PoE Mode	Light	Solid Green: When LED mode button Push to down
LED Mode = “PoE” LED Per PoE Port	PoE Status	Left	Solid Green: Power devices insert, and the PSE supplies the port power successfully.
LED Mode = “PoE” LED Per PoE Port LED Per 10GBASE-T Port	PoE Status Link/ Act / Speed Status	Right	Solid Amber: Power devices insert but failure occurs.
		Light Off	PoE Port is not activated, or no PD connected.
		Left	Solid Green: When there is a secure 2.5Gbps/ 5Gbps/ 10Gbps connection at the port. Blinking Green: When there is reception or transmission running at 2.5Gbps/ 5Gbps/ 10Gbps Mbps at the port.
LED Per 10GBASE-T Port	Link/ Act / Speed Status	Right	Solid Amber: When there is a secure 100/1000 Mbps connection running at the port. Blinking Amber: When there is reception or transmission running at 100/1000Mbps at the port.
		Light Off	No link

LED Per SFP Port (Single LED with dual colors)	Link/ Act/ Speed	Solid Green	When there is a secure 1000Mbps connection at the port
		Blinking Green	When there is reception or transmission occurring at the port
		Solid Amber	When there is a secure 100Mbps connection at the port
		Blinking Amber	When there is reception or transmission occurring at the port
		Light off	No link
LED Per 10G SFP+ Port (Single LED with dual colors)	Link/ Act/ Speed	Solid Green	When there is a secure 10Gbps connection at the port
		Blinking Green	When there is reception or transmission occurring at the port
		Solid Amber	When there is a secure 1000Mbps connection at the port
		Blinking Amber	When there is reception or transmission occurring at the port
		Light off	No link

Rear Panel Description

The rear panel of the Switch contains an AC power connector. The AC power connector is a standard three-pronged connector that supports the power cord. Plug-in the female connector of the provided power cord into this socket, and the male side of the cord into a power outlet. The Switch automatically adjusts its power setting to any supply voltage in the range from 100 to 240 VAC at 50 to 60 Hz. Connect the Kensington-compatible security lock, at the rear of the switch, to a secure immovable device. Insert the lock into the notch and turn the key to secure the lock.

The rear panel also includes an outlet for an optional external power supply and one RJ-45 console port. When a power failure occurs, the optional external RPS will immediately and automatically assume the power supply for the Switch.

DGS-1210-10X/ME

Figure 1.15— DGS-1210-10X/ME Rear Panel

DGS-1210-10XP/ME

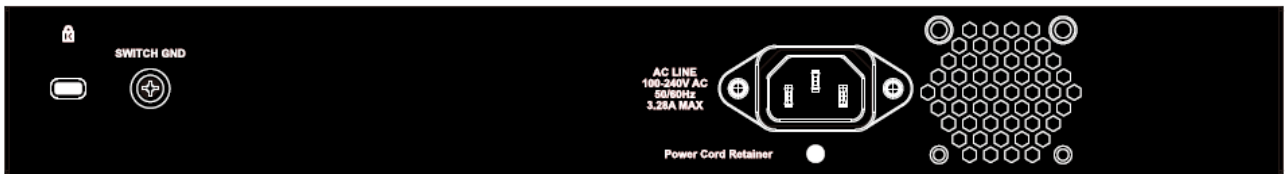


Figure 1.16— DGS-1210-10XP/ME Rear Panel

DGS-1210-10XS/ME

Figure 1.17— DGS-1210-10XS/ME Rear Panel

DGS-1210-28X/ME

Figure 1.18— DGS-1210-28X/ME Rear Panel

DGS-1210-28XS/ME

Figure 1.19—DGS-1210-28XS/ME Rear Panel

DGS-1210-52X/ME

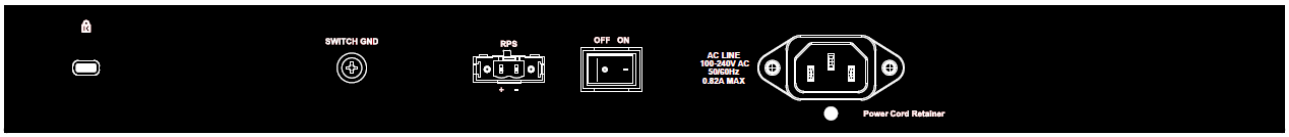


Figure 1.20 — DGS-1210-52X/ME Rear Panel

Side Panel Description

The left- and right-hand panels of the Switch have heat vents to dissipate heat. Do not block these openings, and leave at least 6 inches of space at the rear and sides of the Switch for proper ventilation. Be reminded that without proper heat dissipation and air circulation, system components might overheat, which could lead to system failure.

Figure 1.28 - Side panels of the DGS-1210/ME Cx SERIES

Gigabit Fiber Ports

The DGS-1210/ME CX Series features support four Small Form Factor Portable (SFP) ports (optional). See the diagram below to view the four SFP port modules being plugged into the Switch.

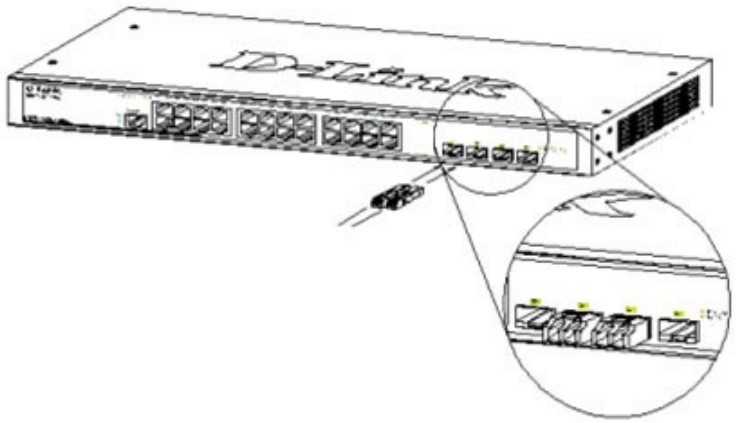


Figure 1.29 - Inserting the SFP modules into the Switch

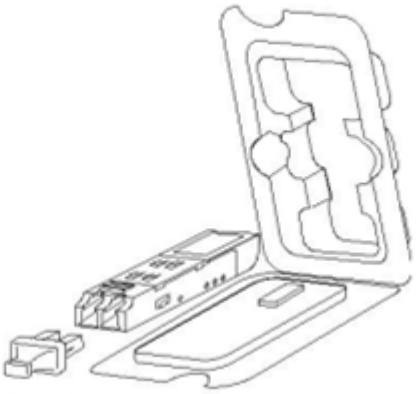


Figure 1.30 - Installing the SFP Module

The Switch is equipped with SFP ports, which are to be used with fiber-optical transceiver cabling in order to uplink various other networking devices for a gigabit link that may span great distances.

Connecting the DPS-200A/500A/500DC to the RPS Port (for DGS-1210-10X/10XS/28X/28XS/52X/ME only)

The DPS-200A/500A/500DC redundant power supply can be connected to the RPS port of the Switch using the DC power supply cord, called the DPS-CB150-2PS. It is important to notice that the DPS-200A/500A/500DC can supply power to one or two DGS-1210-10X/ME at the same time.

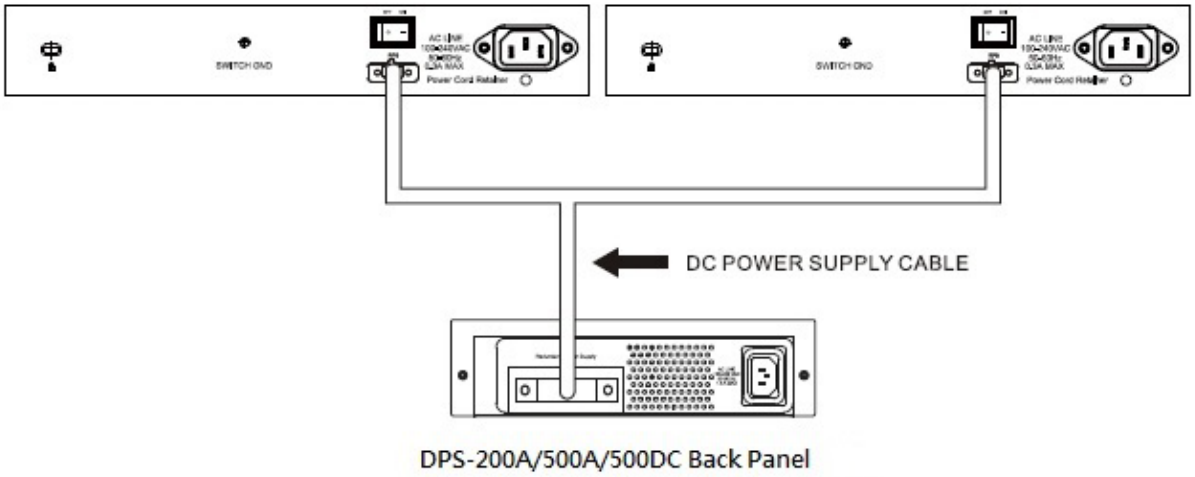


Figure 1.31 – Connecting two Switches to the DPS-200A/500A/500DC

The following section explains how to connect the DPS-200A/500A/500DC to the Switch.

- Disconnect the Switch from the main AC power source.
- Insert the 14-pin end of the DPS-CB150-2PS into the DPS-200A/500A/500DC and the 2-pin end into the receptacle of the RPS port on the Switch.
- Using a standard AC power cord, connect the DPS-200A/500A/500DC to the main AC power source. A green LED on the front panel of the DPS-200A/500A/500DC will illuminate to indicate a successful connection.
- Make sure that the ON/OFF toggle switch on the rear panel of the Switch is turned on.
- Re-connect the Switch to the AC power source and power on the DPS-200A/500A/500DC.

No configuration is needed in the Switch software for this installation.

NOTE: See the DPS-200A/500A/500DC Quick Installation Guide for more information.

Installing the RPS into a Rack-mount Chassis (for DGS-1210-10X/10XS/28X/28XS/52X/ME only)

The DPS-200A/500A/500DC are the redundant power supply unit designed to conform to the voltage requirements of the RPS port of the Switch being supported. The DPS-200A/500A/500DC can be installed into a DPS-800 rack-mount chassis unit.

CAUTION: DO NOT connect the RPS to the AC power before the DC power cable is connected. Connecting the AC power before the DC power is connected might damage the internal power supply.

DPS-800 Rack-mount Chassis

The DPS-800 is a standard-size rack-mount (1 standard unit in height) designed to hold up to three DPS-200A/500A/500DC redundant power supplies.

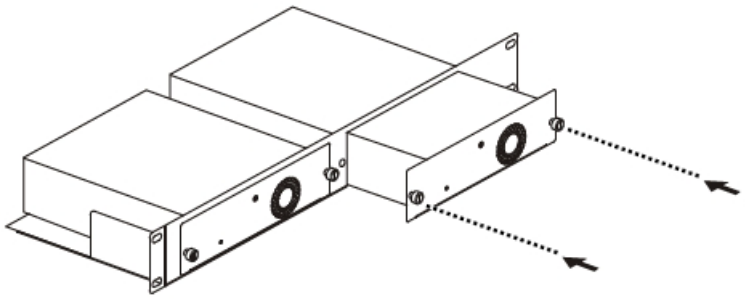


Figure 1.32 –Installing the DPS-200A/500A/500DC in the DPS-800

The DPS-800 rack-mount chassis can be mounted into a standard 19" rack. Use the following diagram for guidance.

2 Hardware Installation

This chapter provides unpacking and installation information for the D-Link DGS-1210/ME CX Metro Management Ethernet Switch.

Step 1: Unpacking

Open the shipping carton and carefully unpack its contents. Please consult the packing list located in the User Manual to make sure all items are present and undamaged. If any item is missing or damaged, please contact your local D-Link reseller for replacement.

One D-Link Metro Management Ethernet Switch
One multi-language Getting Started Guide
One CD
One RJ-45 console cable
Power cord clip
Power cord
Rack mount kit
Rubber feet

If any item is found missing or damaged, please contact the local reseller for replacement.

Step 2: Switch Installation

For safe switch installation and operation, it is recommended that:

Visually inspect the power cord to see that it is secured fully to the AC power connector.
Make sure that there is proper heat dissipation and adequate ventilation around the switch.
Do not place heavy objects on the switch.

Desktop or Shelf Installation

The DGS-1210/ME CX series switches come with a strip of four adhesive rubber pads that can be placed on the bottom of the device to prevent the device from damaging the desktop or shelf it is places on. To attach the rubber pads, simply remove them from the adhesive strip and stick one pad on each corner on the bottom panel of the Switch.

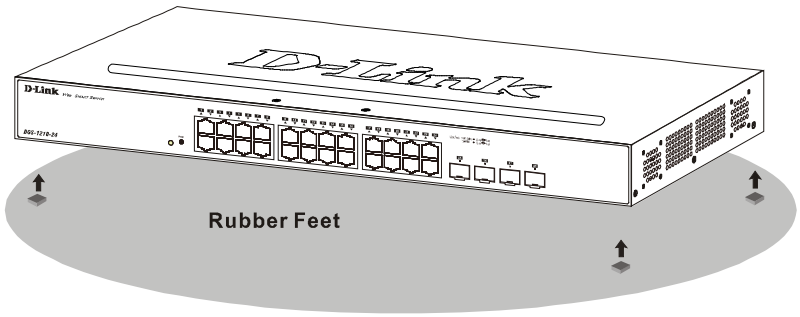


Figure 2.1 – Attach the adhesive rubber pads to the bottom

Rack Installation

The switch can be mounted in an EIA standard size 19-inch rack, which can be placed in a wiring closet with other equipment. To install, attach the mounting brackets to the switch's side panels (one on each side) and secure them with the screws provided (please note that these brackets are not designed for palm size switches).

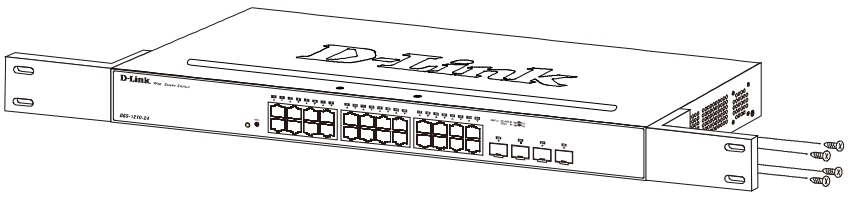


Figure 2.2 – Attach the mounting brackets to the Switch

Then, use the screws provided with the equipment rack to mount the switch in the rack.

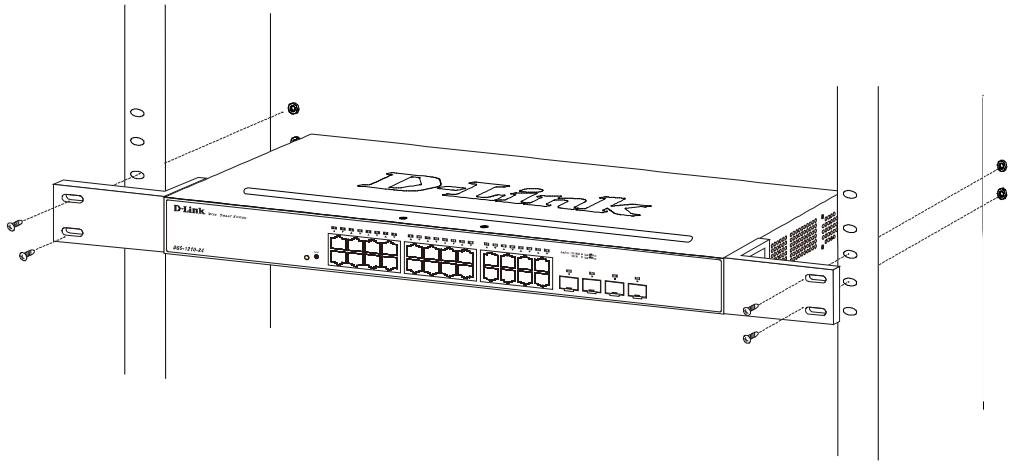


Figure 2.3 – Mount the Switch in the rack or chassis

Please be aware of following safety Instructions when installing:

A) Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.

B) Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

C) Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

D) Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit, and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

E) Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips)."

Step 3 – Plugging in the AC Power Cord

Users may now connect the AC power cord into the rear of the switch and to an electrical outlet (preferably one that is grounded and surge protected).

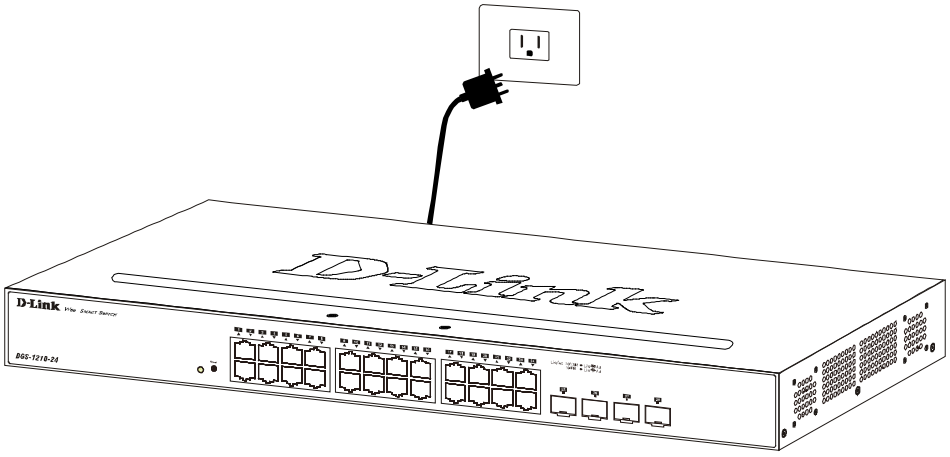


Figure 2.4 – Plugging the switch into an outlet

Power Failure

As a precaution, the switch should be unplugged in case of power failure. When power is resumed, plug the switch back in.

3 Getting Started

This chapter introduces the management interface of D-Link DGS-1210/ME Cx Metro Management Ethernet Switch.

- ***Management Options***
- ***Using Web-based Management***
- ***Connecting to the Console Port***

Management Options

The D-Link DGS-1210/ME Cx Metro Management Ethernet Switch can be managed through any port on the device by using the web-based management interface, or Console Interface (RJ45), or SNMP (Private MIB), or Telnet..

Each switch must be assigned its own IP address, which is used for communication with the web-based management interface or a SNMP network manager. The PC should have an IP address in the same range as the Switch. Each Switch allows up to four users to access the web-based management interface concurrently.

Using Web-based Management Interface

After successfully installing the Switch, user can configure the Switch, monitor the network status, and display statistics using a web browser.

Supported Web Browsers

The embedded Web-based Management currently supports the following web browsers:

Opera 112.0.5197.53
Microsoft Edge 25.0.2535.67
Chrome 125.0.6422.77
FireFox 126.0.1

Connecting to the Switch

The access the web interface user will need the following equipment:

1. A PC with a RJ45 Ethernet port.
2. A standard Ethernet cable

Connect on end of the Ethernet cable to any of the ports on the front panel of the Switch and connect the other end of Ethernet cable to the Ethernet port on the PC.

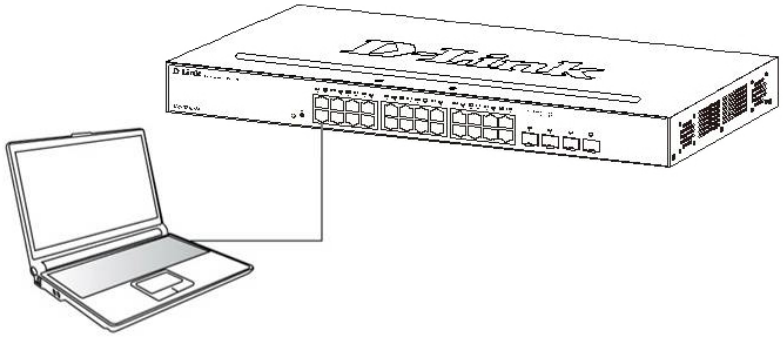


Figure 3.1 – Connected Ethernet cable

Accessing the Web-based Management Interface

In order to access the management interface, the PC must have an IP address in the same subnet as the switch. For example, if the switch has an IP address of **10.90.90.90**, the PC should have an IP address of

10.x.y.z (where x/y is a number between 0 ~ 254 and z is a number between 1 ~ 254), and a subnet mask of **255.0.0.0**. To launch the web interface, simply open any compatible web browser and enter **10.90.90.90** (the factory-default IP address) in the address bar. Then press <Enter>.

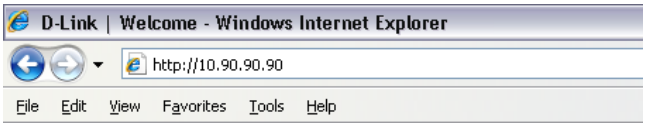


Figure 3.2 –Enter the IP address 10.90.90.90 in the web browser

NOTE: The switch's factory default IP address is 10.90.90.90 with a subnet mask of 255.0.0.0 and a default gateway of 0.0.0.0.

When the following logon dialog box appears, enter the password and choose the language of the Web-based Management interface then click **Login**.

By default, the Username and Password are empty.

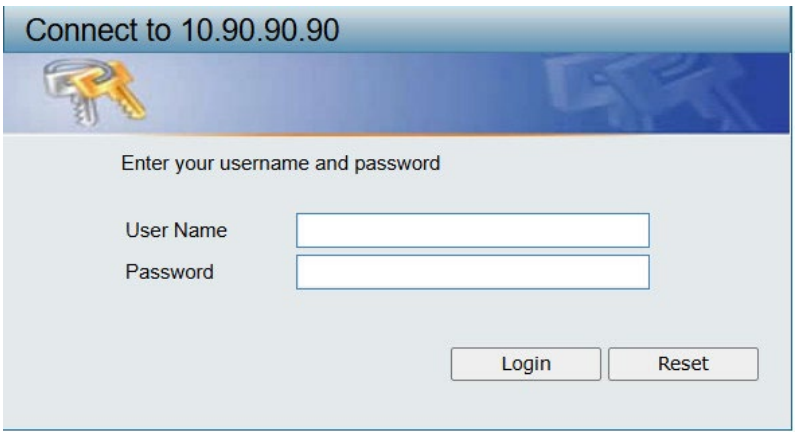


Figure 3.3 – Logon Dialog Box

Web-based Management

Please refer to Chapter 4 Configuration for detailed instructions.

4 Configuration

The features and functions of the D-Link DGS-1210/ME CX Metro Management Ethernet Switch can be configured through the web-based management interface.

Web-based Management

After press the **OK** button in Logon Dialog Box, directed to the page as shown:

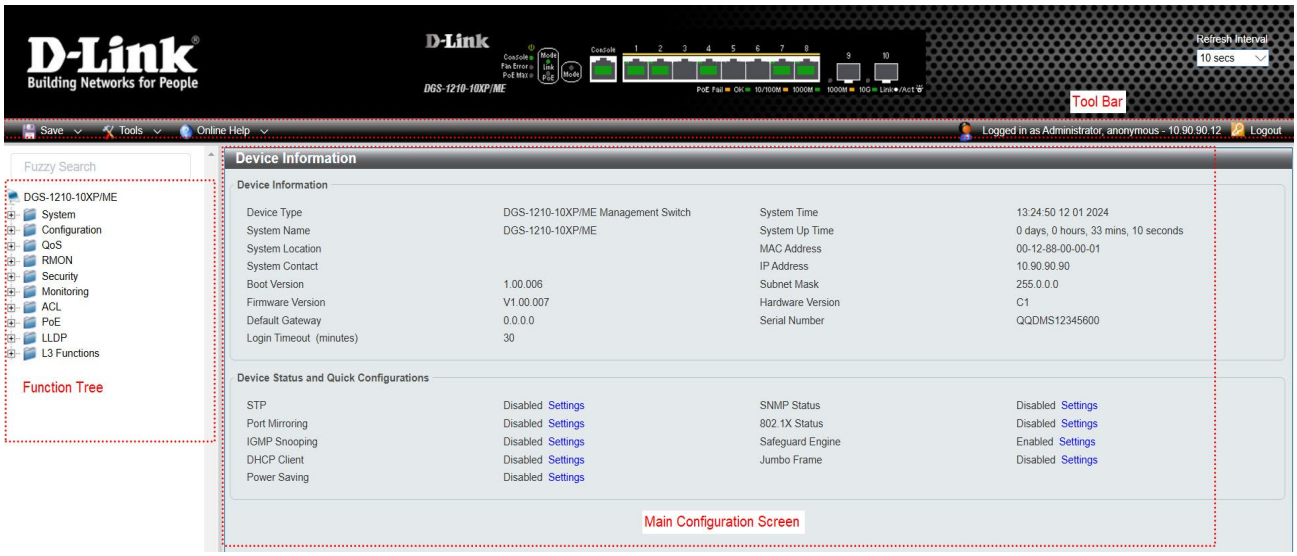


Figure 4.1 – Web-based Management

The three main areas are the **Tool Bar** on top, the **Function Tree** on the left, and the **Main Configuration Screen**.

The **Tool Bar** provides a quick and convenient way for accessing essential functions such as firmware upgrades and basic settings.

Clicking on a section or subsection in the function tree will display all the settings of that section in the main configuration screen. The main configuration screen will show the current status of the Switch by clicking the model name on top of the function tree.

In the upper-right corner of the screen the username and current IP address will be displayed.

Under the username is the **Logout** button. Click this to end this session.

NOTE: If user close the web browser without clicking the **Logout** button first, then it will be seen as an abnormal exit and the login session will still be occupied.

Finally, by clicking on the D-Link logo at the upper-left corner of the screen it will redirected to the local D-Link website.

Tool Bar > Save Menu

The Save Menu provides Save Configuration and Save Log functions.

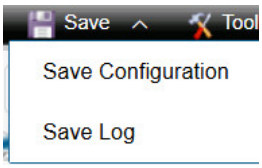


Figure 4.2 – Save Menu

Save Configuration

Select config ID in dropdown list and click **Save Config** to save running configurations into specified ID setion. Or select to boot up the device from which configuration of the device then click the **Apply** button to take effect.

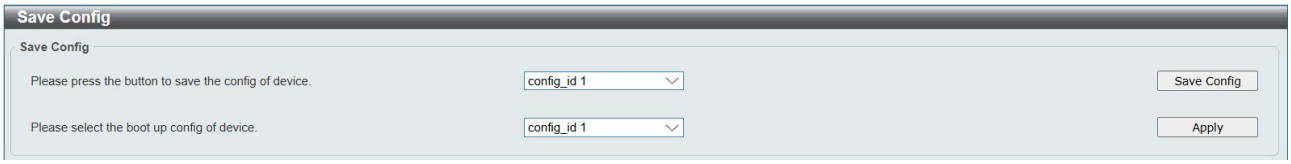


Figure 4.3 – Save Configuration

Save Log

Save the log entries to local drive and a pop-up message will prompt user for the file path. User can view or edit the log file by using text editor (e.g. Notepad).

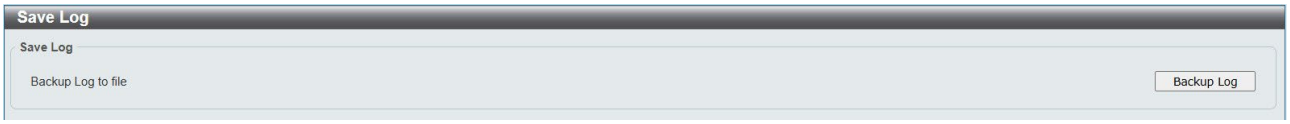


Figure 4.4 – Save Log

Tool Bar > Tool Menu

The Tool Menu offers global function controls such as Reset System, Reboot Device, Configuration Backup and Restore, Firmware Backup and Upgrade and Flash Information.

Figure 4.5 – Tool Menu

Reset System

Provide another safe reset option for the Switch. All configuration settings in non-volatile RAM will reset to factory default and the Switch will reboot.

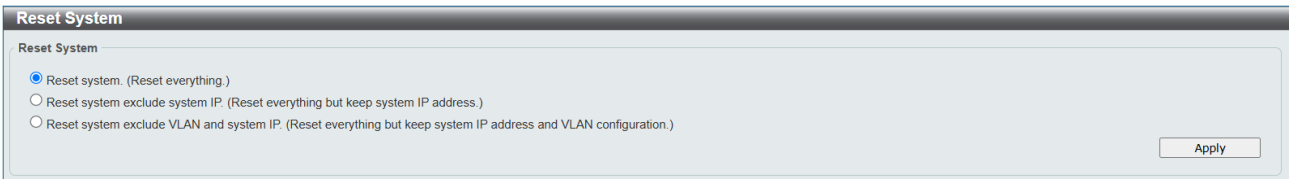


Figure 4.6 – Tool Menu > Reset System

Select the different reset method then click **Apply** to reset the system.

Reboot Device

Provide a safe way to reboot the system. Click **Reboot** to restart the switch.

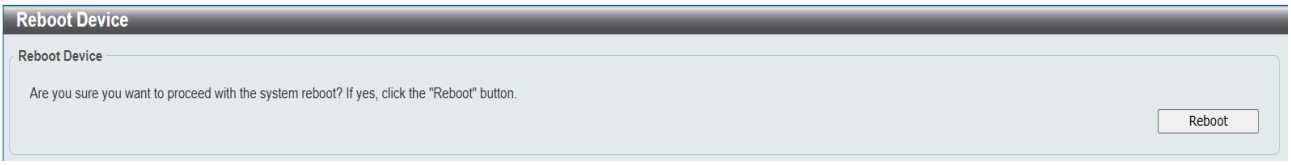


Figure 4.7 – Tool Menu > Reboot Device

Reboot Schedule

Provide configurable mechanism for scheduling device reboot. Countdown mode and Time mode are both available. Also, user is able save the current configuration before scheduled reboot. Reboot schedule configurations only valid for 1 time. When scheduled reboot executed, the schedule parameters returned to default.

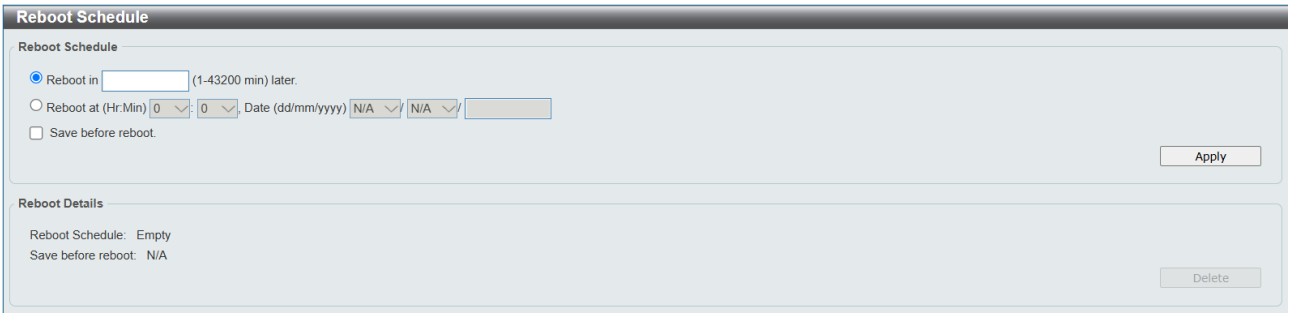


Figure 4.8 – Tool Menu > Reboot Schedule

Configuration Backup & Restore

Allow the current configuration settings to be saved to a file; and if necessary, the existed config file can be restored back to switch. Three methods can be selected: **HTTP, TFTP, SFTP or FTP**.

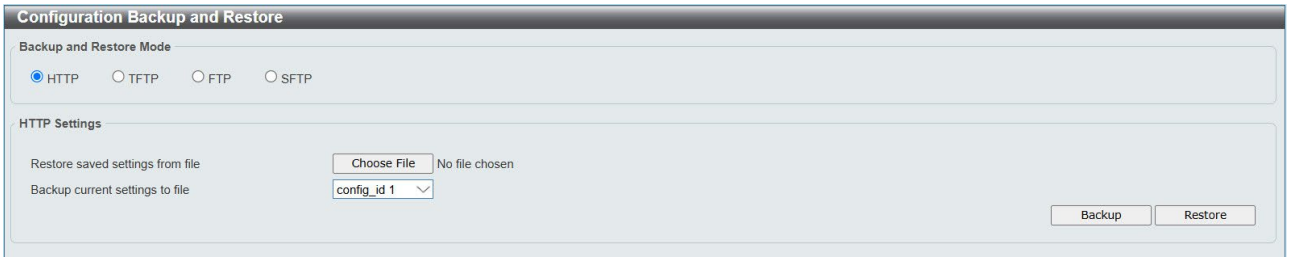


Figure 4.9 – Tool Menu > Configuration Backup and Restore

HTTP: Backup or restore the configuration file to or from the local drive via http.

Backup/Restore Config ID number: Specify the configuration ID number to be backup or restored.

Click **Backup** to save the current settings to local hard drive.

Click **Choose File** to specify the path location of the config file intend to use.

Click **Restore** after selecting the backup settings file want to restore.

TFTP: TFTP (Trivial File Transfer Protocol) is a file transfer protocol that allows user to transfer files to a remote TFTP server.

Backup/Restore Config ID number: Specify the configuration ID number to be backup or restored.

TFTP Server IP Address: Specify the IPv4 or IPv6 address.

TFTP File Name: Enter the file name which user wants to save/restore from for the configuration.

Click **Backup** to save the current settings to the TFTP server.

Click **Restore** after selecting the backup settings file user wants to restore.

SFTP: SFTP (Secret File Transfer Protocol) is a secret file transfer protocol that allows user to transfer files to a remote SFTP server.

Backup/Restore Config ID number: Specify the configuration ID number to be backup or restored.

SFTP Server IP Address: Specify the IPv4 or IPv6 address.

SFTP File Name: Enter the file name which user wants to save/restore from for the configuration.

Click **Backup** to save the current settings to the SFTP server.

Click **Restore** after selecting the backup settings file user wants to restore.

FTP: FTP (File Transfer Protocol) is a file transfer protocol that allows user to transfer file to a remote FTP server.

Backup/Restore Image ID number: Specify to image ID number to be updated on the Switch.

FTP Server IP Address: Specify the IPv4 or IPv6 address.

FTP username: Enter the user name for the FTP server.

FTP password: Enter the user password for the FTP server.

FTP port: Enter the FTP port number. The default is 21.

FTP path: Specify the FTP path where the configuration file located.

FTP File Name: Enter the file name which to be updated on the FTP server.

Click **Backup** to save the current settings to the FTP server.

Click **Restore** after selecting the backup settings file user wants to restore.

Note: Switch will reboot after restore, and all current configurations will be lost.

Firmware Backup & Upgrade

Allow for the firmware to be saved, or for an existing firmware file to be uploaded to the Switch. Protocols that available to selected: **HTTP**, **TFTP, SFTP and FTP**.

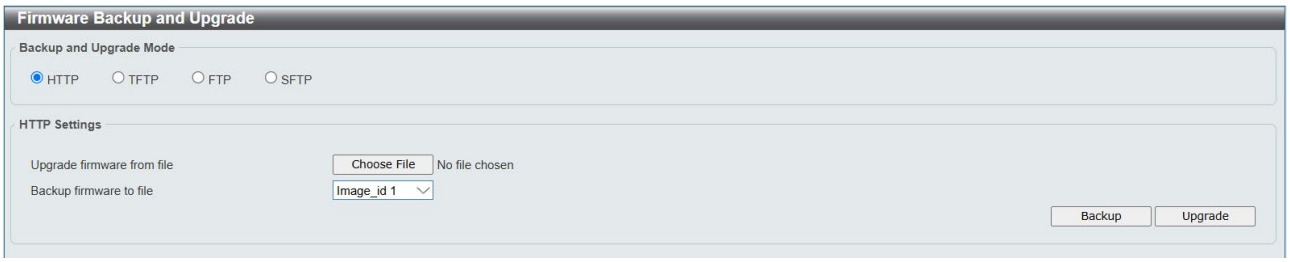


Figure 4.10 – Tool Menu > Firmware Backup and Upgrade

HTTP: Backup or upgrade the firmware to or from local hard drive via http.

Backup/Restore Image ID number: Specify the firmware image ID number to be backup or restored.

Click **Backup** to save the firmware to local hard drive.

Click **Choose File** to specify the path location of the firmware file intend to use.

Click **Upgrade** after selecting the firmware file user wants to restore. The image will be stored in non-running section automatically.

TFTP: Backup or upgrade the firmware to or from a remote TFTP server. The maximum Telnet Server connection is 4.

Backup/Restore Image ID number: Specify the firmware image ID number to be backup or restored.

TFTP Server IP Address: Specify the IPv4 or IPv6 address.

TFTP File Name: Enter the file name which user wants to save/restore from for the firmware.

Click **Backup** to save the firmware to the TFTP server.

Click **Upgrade** after selecting the firmware file user wants to restore.

SFTP: Backup or upgrade the firmware to or from a remote SFTP server.
Backup/Restore Image ID number: Specify the firmware image ID number to be backup or restored.
SFTP Server IP Address: Specify the IPv4 or IPv6 address.
SFTP File Name: Enter the file name which user wants to save/restore from for the firmware.
Click **Backup** to save the firmware to the SFTP server.
Click **Upgrade** after selecting the firmware file user wants to restore.

FTP: Backup or restore the firmware to or from a FTP server.
Backup/Restore Image ID number: Specify to image ID number to be updated on the Switch.
FTP Server IP Address: Specify the IPv4 or IPv6 address.
FTP username: Enter the user name for the FTP server.
FTP password: Enter the user password for the FTP server.
FTP port: Enter the FTP port number. The default is 21.
FTP path: Specify the FTP path where the firmware file located.
FTP File Name: Enter the file name which to be updated on the FTP server.
Click **Backup** to save the current firmware to the FTP server.
Click **Restore** after selecting the backup firmware file user wants to restore.

CAUTION: Do not disconnect the PC or remove the power cord from device until the upgrade completes. The Switch may crash if the Firmware upgrade is incomplete.

Flash Information

The Flash Information page displays the detail information of flash on the Switch.

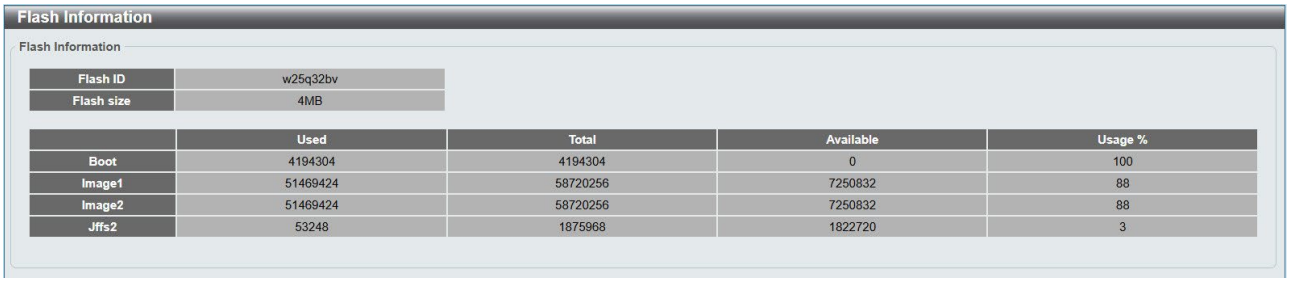


Figure 4.11 – Tool Menu > Flash Information

Tool Bar > Online Help

The Online Help provides two ways of online support:

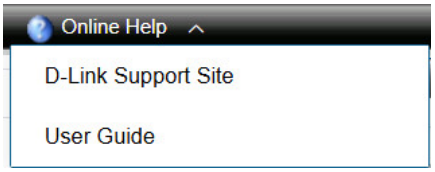


Figure 4.12 – Online Help

D-Link Support Site: This will lead to the D-Link website where user can find online resources such as updated firmware images.
User Guide: This can offer an immediate reference for the feature definition or configuration guide.

Select “D-Link Support Site or User Guide” to make configuration take effect.

Function Tree

All configuration options on the switch are accessed through the function menu on the left side of the screen. Click on the setup item that user wants to configure. The following sections provide more detailed description of each feature and function.

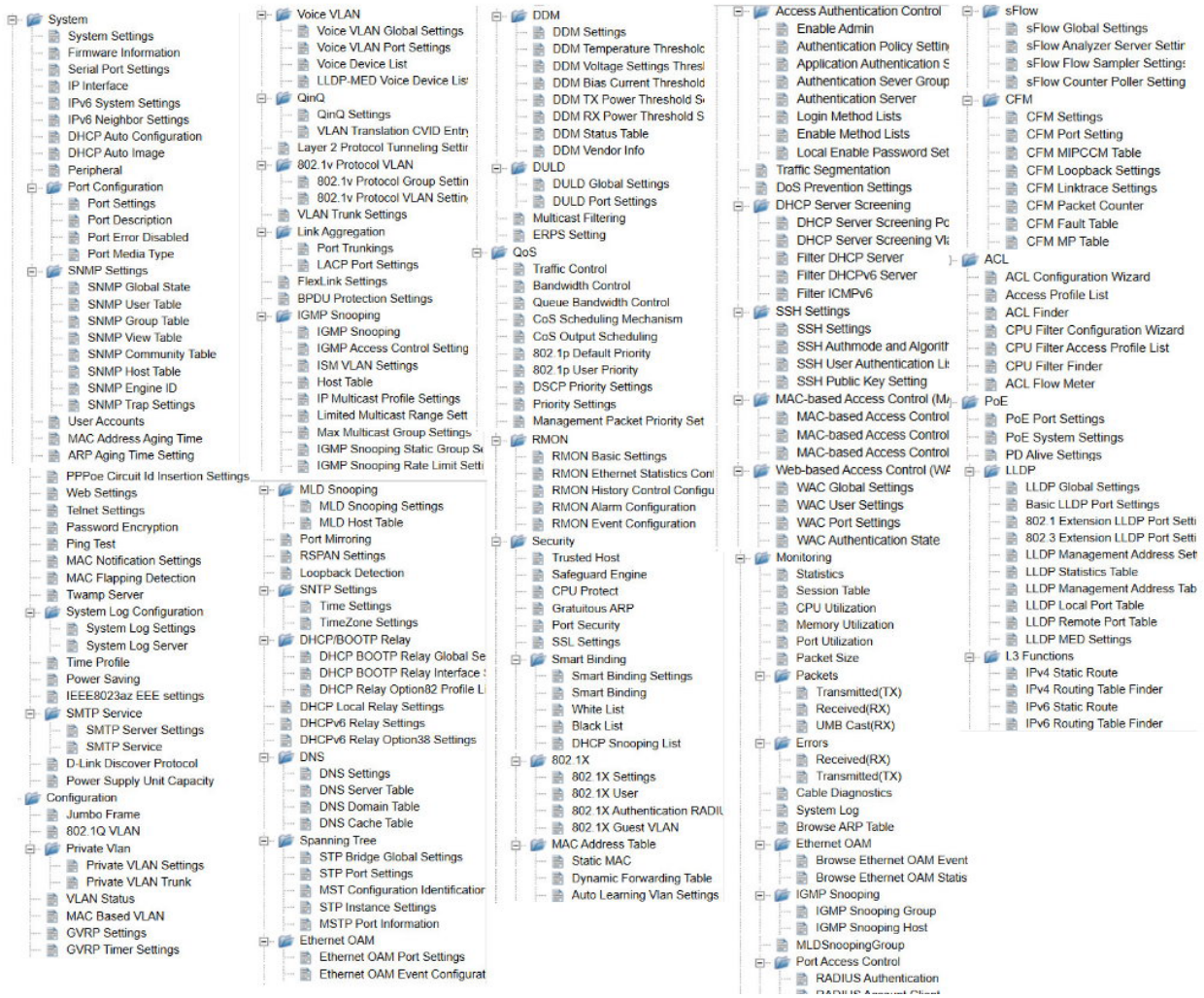


Figure 4.13 –Function Tree

Device Information

The Device Information provides an overview of the switch, including essential information such as firmware & hardware information, and IP address.

It also offers an overall status of common software features:

STP: Click **Settings** to link to Configuration > Spanning Tree > STP Bridge Global Settings. Default is disabled.

Port Mirroring: Click **Settings** to link to Configuration > Port Mirroring. Default is disabled.

IGMP Snooping: Click **Settings** to link to Configuration > IGMP Snooping > IGMP Snooping. Default is disabled.

DHCP Client: Click **Settings** to link to System > System Settings. Default is disabled.

Power Saving: Click **Settings** to link to System > Power Saving. Default is disabled.

SNMP Status: Click **Settings** to link to System > SNMP Settings > SNMP Global State. Default is enabled.

802.1X Status: Click **Settings** to link to Security > 802.1X > 802.1X Settings. Default is disabled.

Safeguard Engine: Click **Settings** to link to Security > Safeguard Engine. Default is enabled.

Jumbo Frame: Click **Settings** to link to Configuration > Jumbo Frame. Default is disabled.

Figure 4.14 – Device Information

System > System Settings

The System Setting allows the user to configure the IP address and the basic system information of the Switch.

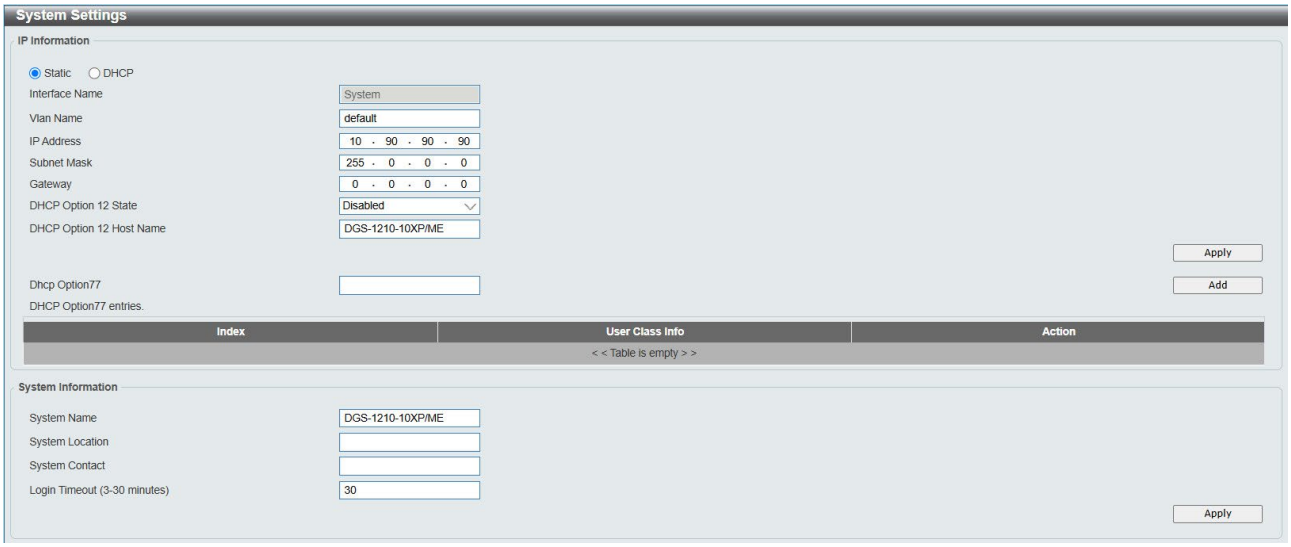


Figure 4.15 – System > System Settings

IP Information: There are two ways for the switch to obtain an IP address: Static and DHCP (Dynamic Host Configuration Protocol).

When using static mode, the **IP Address**, **Subnet Mask, Gateway**, **DHCP Option 12 State** and **DHCP Option 12 Host Name** can be manually configured. When using DHCP mode, the Switch will first look for a DHCP server to provide it with an IP address (including network mask and default gateway) before using the default or previously entered settings. By default the IP setting is static mode with IP address is **10.90.90.90** and subnet mask is **255.0.0.0**.

System Information: By entering a **System Name** and **System Location**, the device can more easily be recognized.

Login Timeout: The Login Timeout controls the idle time-out period for security purposes, and when there is no action for a specific time span in the Web-based Management. If the current session times out (expires), the user is required a re-login before using the Web-based Management again. Selective range is from 3 to 30 minutes, and the default setting is 5 minutes.

System > Firmware Information

The Firmware Information page displays the information of firmware. The user can specify configuration and image file to boot up when power on the Switch next time.

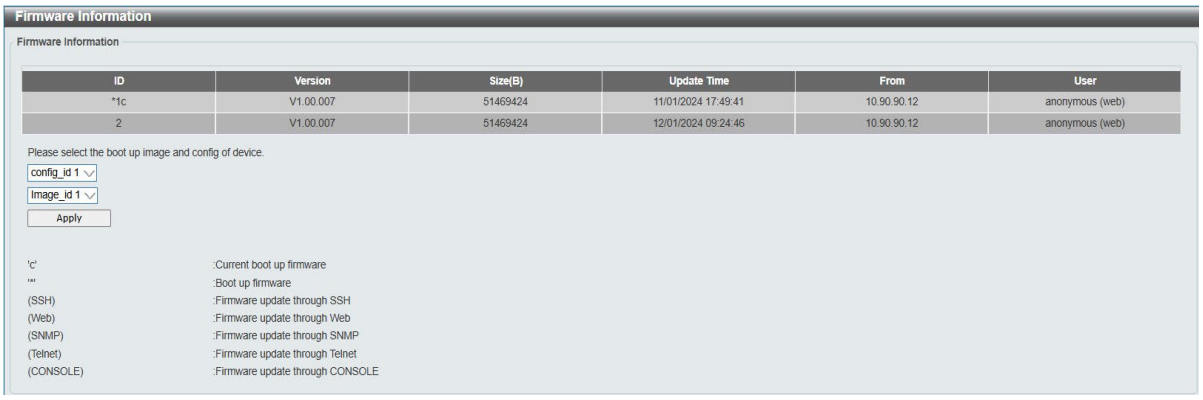


Figure 4.16 – System > Firmware Information

System > Serial Port Settings

The Serial Port Settings allows the user to adjust the Baud Rate and the Auto Logout values.

Figure 4.17 – System > Serial Port Settings

Baud Rate: Specify the baud rate for the serial port on the Switch. There are four possible baud rates to choose from, 9600, 19200, 38400 and 115200. For a connection to the Switch using the console port, the baud rate must be set to 9600, which is the default setting.

Auto Logout: Select the logout time used for the console interface. This automatically logs the user out after an idle period of time, as defined. Choose from the following options: 2, 5, 10, 15 minutes or Never. The default setting is 10 minutes.

Date Bits: Display the date bits used for the serial port connection.

Parity Bits: Display the parity bits used for the serial port connection.

Stop Bits: Display the stop bits used for the serial port connection.

Click Apply to make the configurations take effect.

System > IP Interface

The IP Interface page allow user to configure the IPv6 system settings.

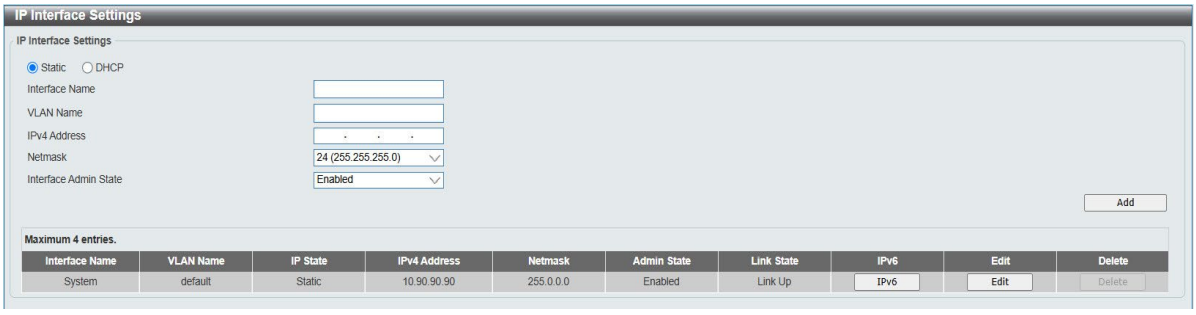


Figure 4.18 – System > IP Interface Settings

Interface Name: Specifies the name of IP interface.

VLAN Name: Specifies the VLAN name of IP interface.

IPv4 Address: Specifies the IPv4 address for the interface.
Netmask: Select the netmask of IP address.
Interface Admin State: Enables or disables the interface administration state.

Click **Add** for the settings to take effect.

System > IP Interface > IPv6 Interface Settings

The IPv6 Settings page allow user to configure the IPv6 system information

Figure 4.19 – System > IP Interface Settings -> IPv6 Settings

IPv6 Interface Settings:
Interface Name: Displays the interface name of IPv6.
IPv6 State: Specifies the IPv6 to be enabled or disabled.
DHCPv6 Client: Specifies the DHCPv6 client to be enabled or disabled.
IPv6 Network Address: Specifies the IPv6 Network Address.
NS Retransmit Time Settings:
NS Retransmit Time (1-3600): Enter the Neighbor solicitation's retransmit timer in second here. Specifies the NS retransmit time for IPv6. The field range is 1-3600, and default is 1 second.
Automatic Link Local State Settings: Specifies the automatic link is enabled or disabled
Automatic Link Local Address: Display link local address from automatic or manually.

System > IPv6 Neighbor Settings

The user can configure the Switch's IPv6 neighbor settings. The Switch's current IPv6 neighbor settings will be displayed in the table at the bottom of this window.

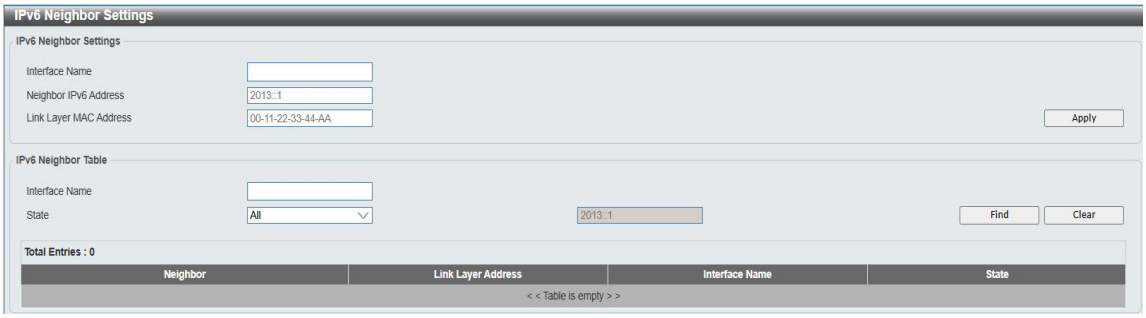


Figure 4.20 – System > IPv6 Neighbor Settings

Interface Name: Enter the interface name of the IPv6 neighbor.
Neighbor IPv6 Address: Specifies the neighbor IPv6 address.
Link Layer MAC Address: Specifies the link layer MAC address.
Click **Apply** to make the configurations take effect.

Interface Name: Specifies the interface name of the IPv6 neighbor. To search for all the current interfaces on the Switch, go to the second Interface Name field in the middle part of the window, tick the **All** check box. Tick the Hardware option to display all the neighbor cache entries which were written into the hardware table.

State: Use the drop-down menu to select All, Address, Static or Dynamic. When the user selects address from the drop-down menu, the user will be able to enter an IP address in the space provided next to the state option.

Click **Find** to locate a specific entry based on the information entered.

Click **Clear** to clear all the information entered in the fields.

System > DHCP Auto Configuration

The DHCP Auto Configuration page allows user to enable the DHCP Auto Configuration feature on the Switch. When enabled, the Switch becomes a DHCP client and gets the configuration file from a TFTP server automatically on next boot up. To accomplish this, the DHCP server must deliver the TFTP server IP address and configuration file name information in the DHCP reply packet. The TFTP server must be up and running and store the necessary configuration file in its base directory when the request is received from the Switch.

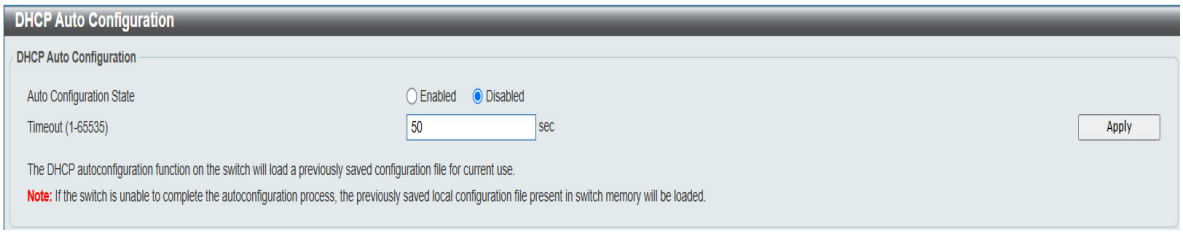


Figure 4.21 – System > DHCP Auto Configuration

System > DHCP Auto Image

The DHCP Auto Image page allows user to automatically download firmware image and upgrade the different firmware version image into the Switch.

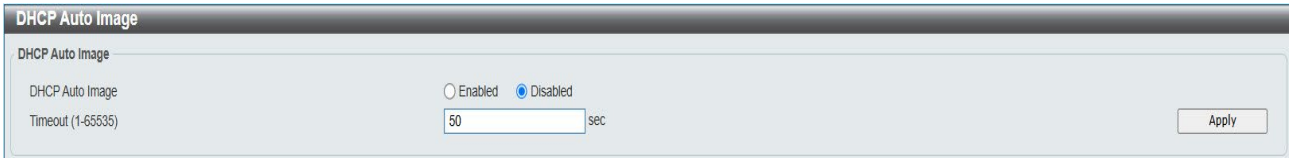


Figure 4.22 – System > DHCP Auto Image

System > Peripheral Settings

This window is used to display and configure the environment trap settings and environment temperature threshold settings.

To view the following window, click System > Peripheral Settings, as shown below:

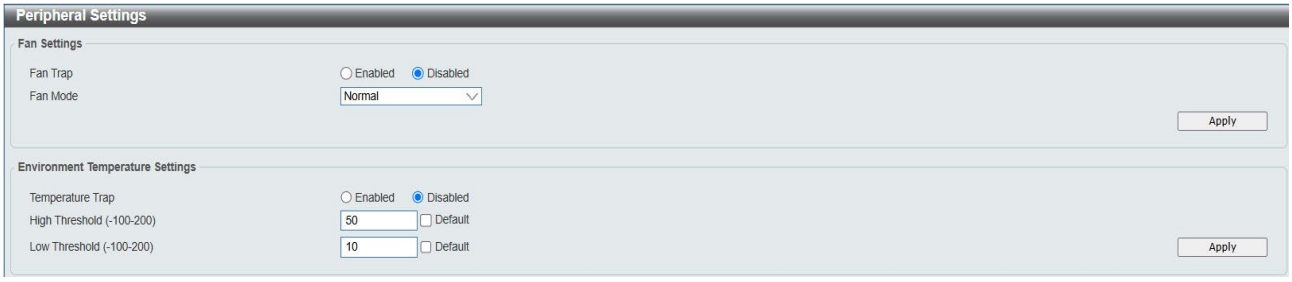


Figure 4.23 – System > Peripheral Settings

The fields that can be configured in **Environment Trap Settings** are described below:

Parameter	Description
Fan Trap	Select to enable or disable the fan trap state for waning fan event (fan failed or fan recover).
Fan Mode	Select to change Fan normal, quite and off mode.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Environment Temperature Threshold Settings** are described below:

Parameter	Description
Temperature Trap	Select to enable or disable the Temperature trap state.
High Threshold	Enter the high threshold value of the warning temperature setting. The range is from -100 to 200 degrees Celsius. Tick the **Default** check box to return to the default value.
Low Threshold	Enter the low threshold value of the warning temperature setting. The range is from -100 to 200 degrees Celsius. Tick the **Default** check box to return to the default value.

Click the **Apply** button to accept the changes made.

System > Port Configuration > Port Settings

In the Port Setting page, the status of all ports can be monitored and adjusted for optimum configuration. By selecting a range of ports (**From Port** and **To Port**), the **Speed** can be set for all selected ports by clicking **Apply**. Press the **Refresh** button to view the latest information.

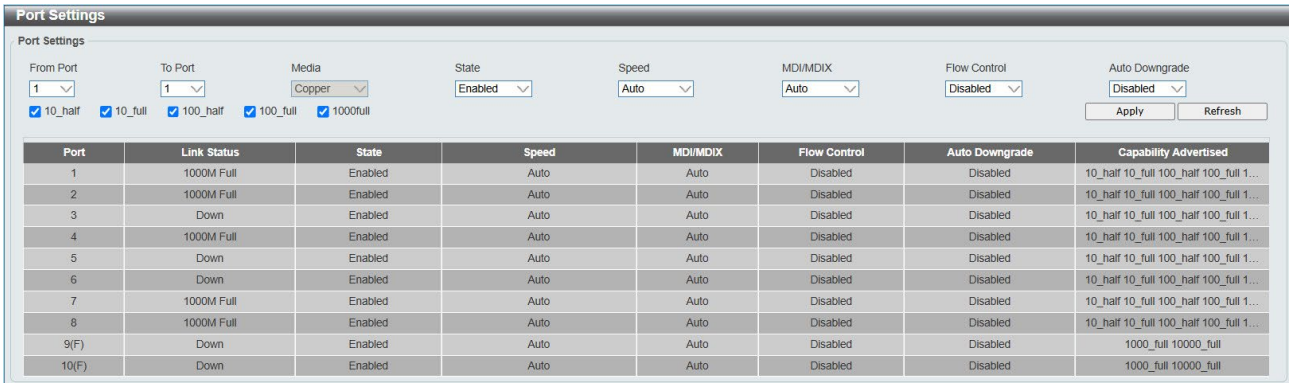


Figure 4.24 – System > Port Configuration > Port Settings

Media: Depending on the selected port type, two options for user. *Copper and Fiber_1G*.

State: Enable or disable the state of specified ports.

Speed: Gigabit Fiber connections can operate in 1000M Full Force Mode, Auto Mode or Disabled. Copper connections can operate in Forced Mode settings (1000M Full, 100M Full, 100M Half, 10M Full, 10M Half), Auto, or Disabled. The default setting for all ports is **Auto**.

NOTE: Be sure to adjust port speed settings appropriately after changing the connected cable media types.

MDI/MDIX:

A **medium dependent interface** (**MDI**) port is an Ethernet port connection typically used on the Network Interface Card (NIC) or Integrated NIC port on a PC. Switches and hubs usually use **Medium dependent interface crossover (MDIX)** interface. When connecting the Switch to end stations, user have to use straight through Ethernet cables to make sure the Tx/Rx pairs match up properly. When connecting the Switch to other networking devices, a crossover cable must be used.

This switch provides a configurable **MDI/MDIX** function for users. The switches can be set as an MDI port in order to connect to other hubs or switches without an Ethernet crossover cable.

Auto is designed on the switch to detect if the connection is backwards, and automatically chooses MDI or MDIX to properly match the connection. The default setting is "**Auto" MDI/MDIX**.

Flow Control: User can enable this function to mitigate the traffic congestion. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use backpressure flow control. The default setting is Disabled.

Auto Downgrade is the option to automatically downgrade the advertised speed. The default value is Disabled.

System > Port Configuration > Port Description

In the Port Description page, the user may name various ports on the Switch.

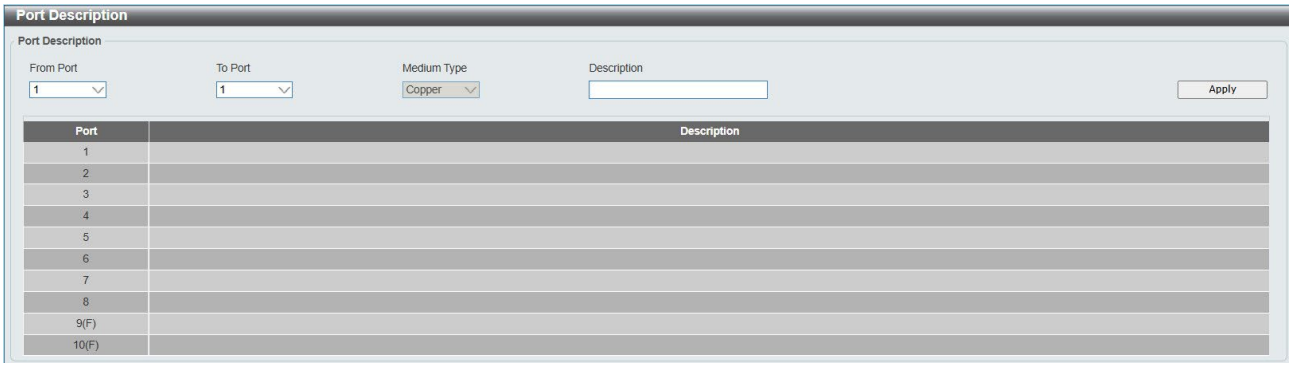


Figure 4.25 – System > Port Configuration > Port Description

From Port / To Port: Specify the range of ports to describe.

Medium Type: Depending on the selected port type, two options for user. *Copper and Fiber*.

Description: Specify the description of ports.

Click **Apply** to make the configurations take effect.

System > Port Configuration > Port Error Disabled

The Port Error Disabled page displays the information about ports that have had their connection status disabled, for reasons such as STP loopback detection or link down status.

Figure 4.26 – System > Port Configuration > Port Error Disabled

Port: Displays the port that has been error disabled.

Port State: Describes the current running state of the port, whether Enabled or Disabled.

Connection Status: This field will read the uplink status of the individual ports, whether Enabled or Disabled.

Reason: Describes the reason why the port has been error-disabled, such as a STP loopback occurrence.

System > Port Configuration > Port Media Type

The Port Media Type page displays the information about the port media type.

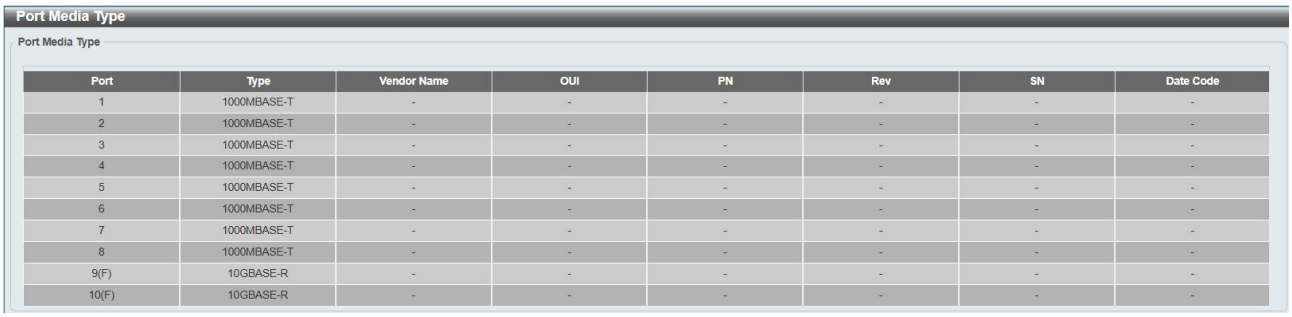


Figure 4.27 – System > Port Configuration > Port Media Type

Port: Displays the port number.

Type: Displays the port media type. The media types are 1000MBASE-T, 1000MBASE-X, 100MBASE-T, 100MBASE-X, 10MBASE-T and 10MBASE-X.

System > SNMP Settings > SNMP Global State

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) protocol designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems in the Switch or LAN.

Managed devices that support SNMP include software (referred to as an agent), which runs locally on the device. A defined set of variables (managed objects) is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The default SNMP global state is disabled. Select Enable and click **Apply** to enable the SNMP function.

Figure 4.28 – System > SNMP Settings > SNMP Global State

System > SNMP Settings > SNMP User Table

This page is used to maintain the SNMP user table for the use of SNMPv3. SNMPv3 allows or restricts users using the MIB OID, and also encrypts the SNMP messages sent out between users and Switch.

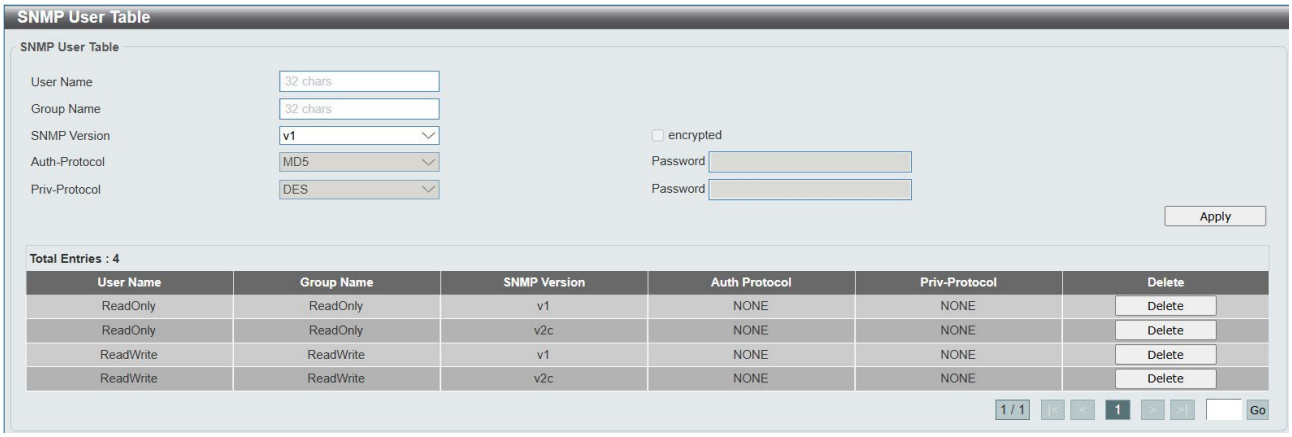


Figure 4.29 – System > SNMP Settings > SNMP User Table

User Name: Enter a SNMP user name of up to 32 characters.

Group Name: Specify the SNMP group of the SNMP user.

SNMP Version: Specify the SNMP version of the user. Only SNMPv3 encrypts the messages.

Encrypt: Specifies the Encrypt is enabled or disabled when the SNMP Version is V3.

Auth-Protocol/Password: Specify either HMAC-MD5-96 or HMAC-SHA to be the authentication protocol. Enter a password for SNMPv3 encryption in the right column.

Priv-Protocol/Password: Specify either **no authorization** or **DES 56-bit encryption** and then enter a password for SNMPv3 encryption in the right column.

Click **Apply** to create a new SNMP user account, and click **Delete** to remove any existing data.

System > SNMP Settings > SNMP Group Table

This page is used to maintain the SNMP Group Table associating to the users in SNMP User Table. SNMPv3 can control MIB access policy, security policy for a user group directly.

Group Name: Specify the SNMP user group of up to 32 characters.

Read View Name: Specify a SNMP group name for users that are allowed SNMP read privileges to the Switch's SNMP agent.

Write View Name: Specify a SNMP group name for users that are allowed SNMP write privileges to the Switch's SNMP agent.

Security Model: Select the SNMP security model.

SNMPv1 - SNMPv1 does not support the security features.

SNMPv2 - SNMPv2 supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.

SNMPv3 - SNMPv3 provides secure access to devices through a combination of authentication and encrypting packets over the network.

Security Level: This function is only available when user select SNMPv3 security level.

NoAuthNoPriv - No authorization and no encryption for packets sent between the Switch and SNMP manager.

AuthNoPriv - Authorization is required, but no encryption for packets sent between the Switch and SNMP manager.

AuthPriv – Both authorization and encryption are required for packets sent between the Switch and SNMP manger.

Notify View Name: Specify a SNMP group name for users that can receive SNMP trap messages generated by the Switch's SNMP agent.

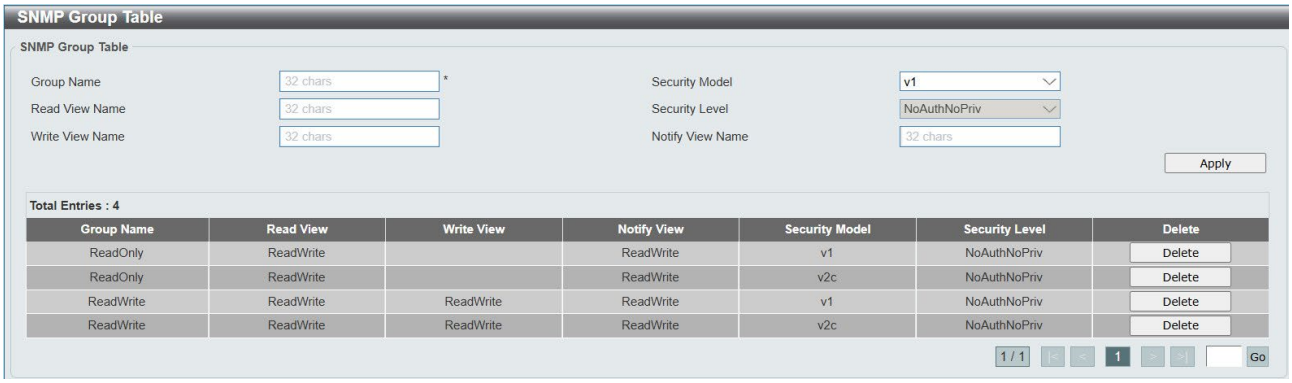


Figure 4.30– System > SNMP Settings > SNMP Group Table

System > SNMP Settings > SNMP View Table

This page allows user to maintain SNMP views to community strings that define the MIB objects which can be accessed by a remote SNMP manager.

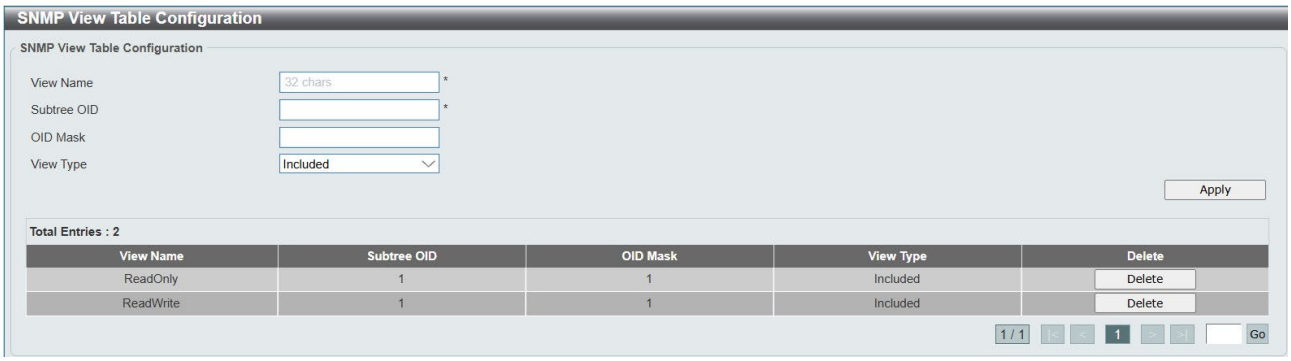


Figure 4.31 – System > SNMP Settings > SNMP View Table

View Name: Name of the view, up to 32 characters.

Subtree OID: The Object Identifier (OID) Subtree for the view. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.

OID Mask: The mask of the Subtree OID. 1 means this object number is concerned, 0 means do not concerned. For example 1.3.6.1.2.1.1 with mask 1.1.1.1.1.1.0 means 1.3.6.1.2.1.X.

View Type: Specify the configured OID is Included or Excluded that a SNMP manager can access.

Click **Apply** to create a new view, **Delete** to remove an existing view.

System > SNMP Settings > SNMP Community Table

This page is used to maintain the SNMP community string of the SNMP managers using the same community string are permitted to gain access to the Switch's SNMP agent.

Community Name: Name of the community string

User Name (View Policy): Specify the read/write or read-only level permission for the MIB objects accessible to the SNMP community.

Figure 4.32 – System > SNMP Settings > SNMP Community Table

Click **Apply** to create a new SNMP community, **Delete** to remove an existing community.

System > SNMP Settings > SNMP Host Table

This page is to configure the SNMP trap recipients.

Host IP Address: Select IPv4 or IPv6 and specify the IP address of SNMP management host.

SNMP Version: Specify the SNMP version to be used to the management host.

Community String/SNMPv3 User Name: Specify the community string or SNMPv3 user name for the management host.

Figure 4.33– System > SNMP Settings > SNMP Host Table

Click **Apply** to create a new SNMP host, **Delete** to remove an existing host.

System > SNMP Settings > SNMP Engine ID

The Engine ID is a unique identifier used to identify the SNMPv3 engine on the Switch.

Input the Engine ID then click **Apply** to apply the changes and click **Default** resets to default value.

Figure 4.34 – System > SNMP Settings > SNMP Engine ID

System > SNMP Settings > SNMP Trap Settings

The SNMP Trap Settings page provide user to Specify whether the device can send SNMP notifications.

Figure 4.35 – System > SNMP Settings > SNMP Trap Settings

Type	Description
SNMP Authentication Traps	Trap event of authentication failure.
System Coldstart Traps	Trap event of device cold boot up.
System Warmstart Traps	Trap event of device warn boot up.
Port Link Up / Link Down	Trap event of link state changes (link down/link up).
RSTP Port State Change	Trap event of Spanning Tree port state change.
Firmware Upgrade State	Trap event of firmware upgrade status (success/failure).
Trap notification if PoE Power	Trap event of PoE powering state in port basis.

On / Off	
Trap notification if PoE Power Error	Trap event of PoE error.
Trap notification if over max power budget	Trap event when device supplies power over the max power budget.
Port Security Violation	Trap event of violations for port security.
IMPB Violation	Trap event of violations of IP-MAC-Port binding feature.
Loopback Detection occuring / recovery	Trap events of state changes (detected/recovery) for loopback detection.
DHCP Server Screening	Trap events of DHCP sever screening.
Duplicate IP Detected	Trap event when duplicate IP address detected.
DHCPv6 Server Screening	Trap events of DHCPv6 sever screening.
ICMPv6 RA All Node Filter	Trap events of ICMPv6 RA filter feature.
Login / Logout	Trap events for account login/logout.
DULD Traps	Trap events of DULD feature.
DyingGasp Traps	Trap events of DyingGasp feature.
802.1x Traps	Trap events of 802.1x feature.
LinkChange Trap	Trap events of STP LinkChange feature by port settings.
Sending Trap Port Settings	This settings to enable/disable SNMP trap forward by interface.[Default all ports state enable]

Click **Apply** to make the configurations take effect.

System > User Accounts

The **User Accounts** page provides user to control user privileges. To add a new user by typing in a **User Name**, **Password** and retype the same password in the **Confirm Password** and choose the level of privilege(*Admin*, *Operator, PowerUser* or *User*) from the **Access Right** drop-down menu, then click the **Apply** button.

User can modify existing user account in the User Account Table. To change the password, type in the **Old Password**, **New Password** and retype it in the Confirm New Password entry field and select the Encrypt, then click the **Edit** button. To delete the user account, click on the **Delete** button.

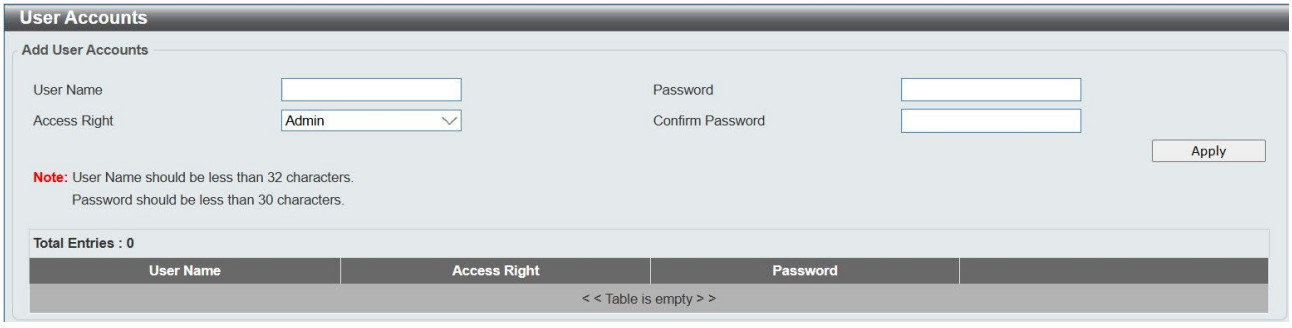


Figure 4.36– System > User Accounts

System > MAC Address Aging Time

The MAC Address Aging Time page specifies the length of time a learned MAC Address will remain in the forwarding table without being accessed (that is, how long a learned MAC address is allowed to remain idle). To change this, type in a different value representing the MAC address age-out time in seconds.

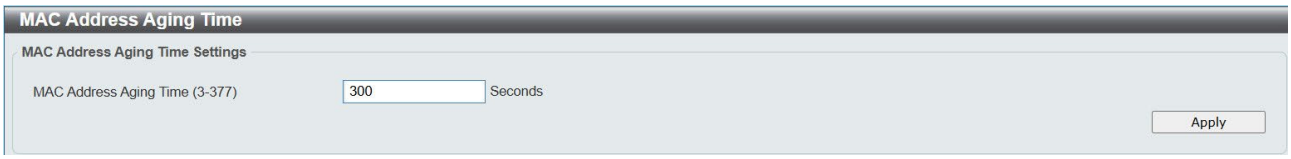


Figure 4.37 – System > MAC Address Aging Time

MAC Address Aging Time (3-377): Specifies the aging time of MAC address on the Switch. The range is from 3 to 377, and the default is 300 seconds.

System > ARP Aging Time Settings

The ARP Aging Time Settings page provides user to globally set the maximum amount of time, in minutes, and Address Resolution Protocol (ARP) entry can remain in the Switch's ARP table, without being accessed, before it is dropped from the table.

Figure 4.38 – System > ARP Aging Time Settings

ARP Aging Time (0-65535): Specifies the ARP aging time on the Switch. The range is from 0 to 65535 with a default setting of 5 minutes.

System > PPPoE Circuit ID Insertion Settings

The PPPoE Circuit ID Insertion Settings page specifies the configuration of settings. When enabled, the system will insert the circuit tag to the received PPPoE discover request and the request packet if the tag is absent. It will remove the circuit ID tag from the received PPPoE offer and session confirmation packet.

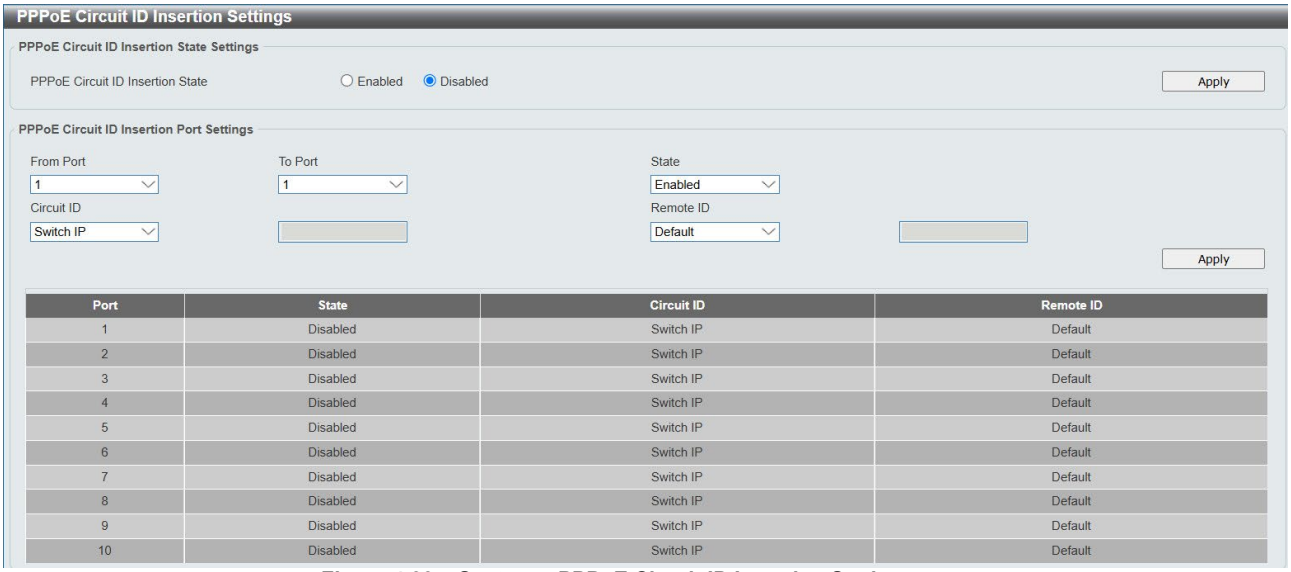


Figure 4.39 – System > PPPoE Circuit ID Insertion Settings

PPPoE Circuit ID Insertion State: Enable or disable the PPPoE circuit insertion state, and Click Apply to make the configurations take effect.

From Port/ To Port: Specifies the ports to be configured.

State: Enable or disable the state of specified ports.

Circuit ID: Specifies the Circuit ID is **Switch IP**, **Switch MAC, UDF String, Vendor2** and **Vendor3.**

Switch IP – The Switch's IP address will be used to encode the circuit ID option. This is the default.

Switch MAC – The MAC address of the Switch will be used to encode the circuit ID option.

UDF String – A user specified string to be used to encode the circuit ID option. Enter a string with the maximum length of 32.

Remote ID: Specifies the Remote ID is **Default**, **Vendor2** or **Vendor3**.

Click **Apply** to make the configurations take effect.

System > Web Settings

The WEB State is **Enabled** by default. If user chooses to disable this by selecting Disabled, user will lose the ability to configure the system through the web interface as soon as these settings are applied.

Figure 4.40– System > Web Settings

Port (1-65535): Specifies the Port number. The range is between 1 and 65535 with the well-known default is 80.

Click **Apply** to make the configurations take effect.

System > Telnet Settings

Telnet configuration is **Enabled** by default. If user does not want to allow the Telnet configuration, they only need to disable the Telnet State.

Figure 4.41 – System > Telnet Settings

Port (1-65535): The TCP port number. TCP ports are numbered between 1 and 65535. The well-known TCP port for the Telnet protocol is 23.

Click **Apply** to make the configurations take effect.

System > Password Encryption

The Password Encryption page is used to enable or disable the password encryption state. Select **Enabled** and click **Apply** to make the configurations take effect.

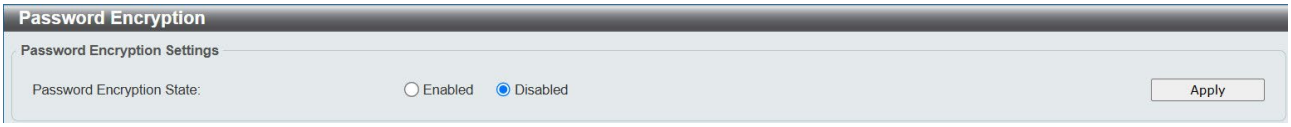


Figure 4.42 – System > Password Encryption

System > Ping Test

The Ping Test is a small program that sends ICMP Echo packets to the IP address user specified. The destination node then responds to or “echoes” the packets sent the Switch. This is very useful to verify connectivity between the Switch and other nodes on the network.

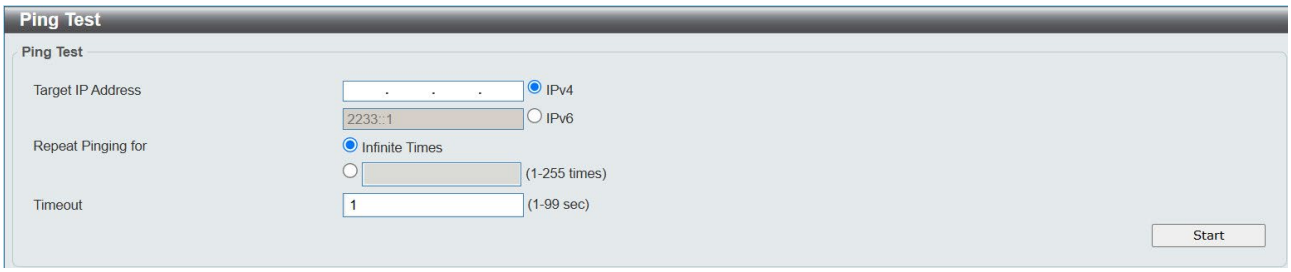


Figure 4.43 – System > Ping Test

Target IP address allows both **IPv4** and **IPv6** addresses format.

The time of ping can be configured in **Repeat Pinging** filed; **Infinite** and range of **1-255** are available options to use.

Timeout filed specifies the timeout value of every single ping packet. The timeout range from **1- 99** seconds.

Click **Start** to initiate the Ping Program

System > MAC Notification Settings

MAC Notification page is used to monitor MAC addresses learned and entered into the forwarding database. To globally set MAC notification on the Switch, user should enabled or disabled state, input the Time **Interval** between notification and **History Size** then click the **Apply** button.

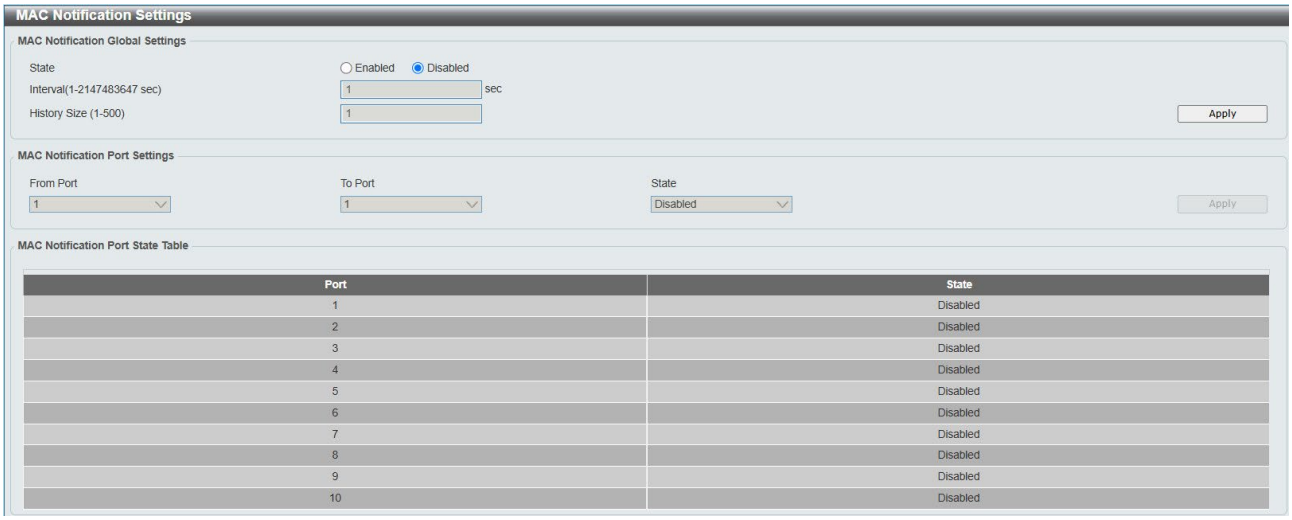


Figure 4.44 – System > MAC Notification Settings

State: Enabled or Disabled MAC notification globally on the Switch.

Interval (1-2147483647 sec): The time in seconds between notifications.

History Size (1-500): The maximum number of entries listed in the history log used for notification. Up to *500* entries can be specified.

Click **Apply** to make the configurations take effect.

To change MAC notification settings for a port or group of ports on the Switch, configure the following parameters. , then click the **Apply** button.

From Port / To Port: Select a port or group of ports to enable for MAC notification using the pull-down menus.

State: Enable MAC Notification for the ports selected using the pull-down menu.

System > MAC Flapping Settings

MAC Flapping page is used to detect interface flapping MAC address by flapping check interval.

Figure 4.45 – System > MAC Flapping Settings

State: Enabled or Disabled MAC flapping globally on the Switch.

Interval (1-3600 sec): The time in seconds between MAC flapping detect.

Click **Apply** to make the configurations take effect.

Total Entries: The maximum number of entries listed for MAC flapping detected. Up to *500* entries can be specified.

System > Twamp (Two-Way Active Measurement Protocol) Server Settings

Twamp Sever settings page is used to enable/disable Twamp Sever function.

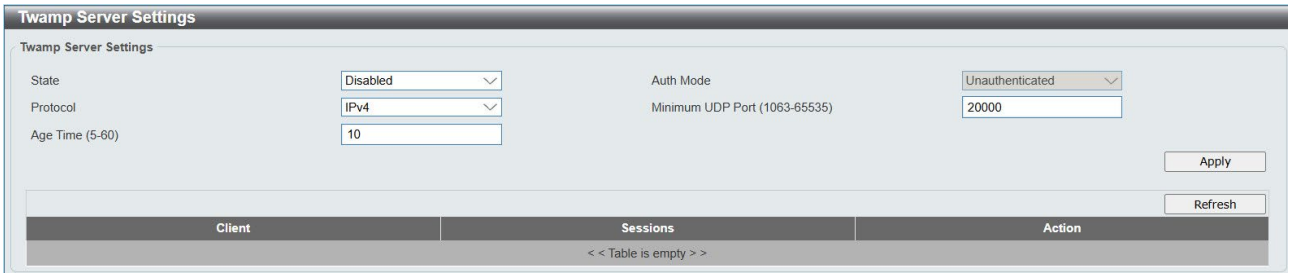


Figure 4.46 – System > Twamp Settings

State: Enabled or Disabled Twamp globally on the Switch.

Auto Mode: keep in Un-Authenticated. [No support Settings]

Protocol: Select IPv4 or IPv6.

Minimum UDP Port: Allow settings range (1063-65535), default 20000.

Age Time: Allow settings range (5-60), default 10.

Click **Apply** to make the configurations take effect.

System > System Log Configuration > System Log Settings

System Logs record and manage events, as well as report errors and informational messages. Message severity determines a set of event message will be sent. Click **Enable** so user can start to configure the related settings of remote system log server, then press **Apply** for the changes to take effect.

Figure 4.47 – System > System Log Configuration > System Log Settings

Save Mode: Use this drop-down menu to choose the method that will trigger a log entry. User can choose between **On Demand**, **Time Interaval** and **Log Trigger.**

Minutes: Enter a time intervel, in minutes, for which user would like a log entry to be made.

System > System Log Configuration > System Log Server

The user can send Syslog messages to up to four designated servers using the **System Log Server**. It supports maximum 500 system log entries. To set the System Log Server configuration, click **Apply**.

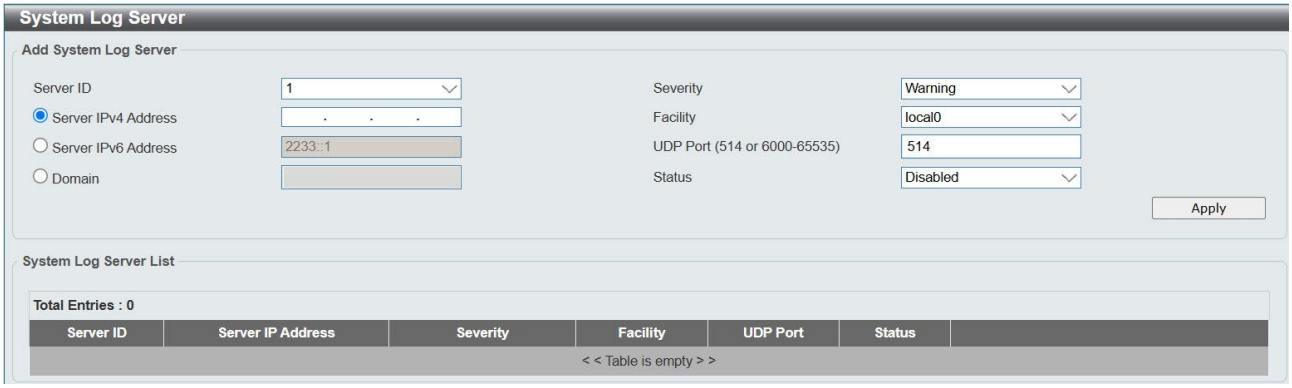


Figure 4.48 - System > System Log Configuration > System Log Server

Server ID: Specifies the Server ID. The field range is 1-4.

Severity: Specifies the minimum severity from which warning messages are sent to the server. There are three levels. When a severity level is selected, all severity level choices above the selection are selected automatically. The possible levels are:

Warning - The lowest level of a device warning. The device is functioning, but an operational problem has occurred.

Informational - Provides device information.

All - Displays all levels of system logs.

Server IPv4 Address: Specifies the IPv4 address of the system log server.

Server IPv6 Address: Specifies the IPv6 address of the system log server.

Facility: Specifies an application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility is overwritten. There are up to eight facilities can be assigned (Local 0 ~ Local 7).

UDP Port: Specifies the UDP port to which the server logs are sent. The possible range is *6000* – *65535*, and the default value is *514*.

Status: Specifies the status is enable or disable.

Note: Dying GASP log transmitted automatically when system log feature enabled.

System > Time Profile

The Time Profile page allows users to configure the time profile settings of the device.

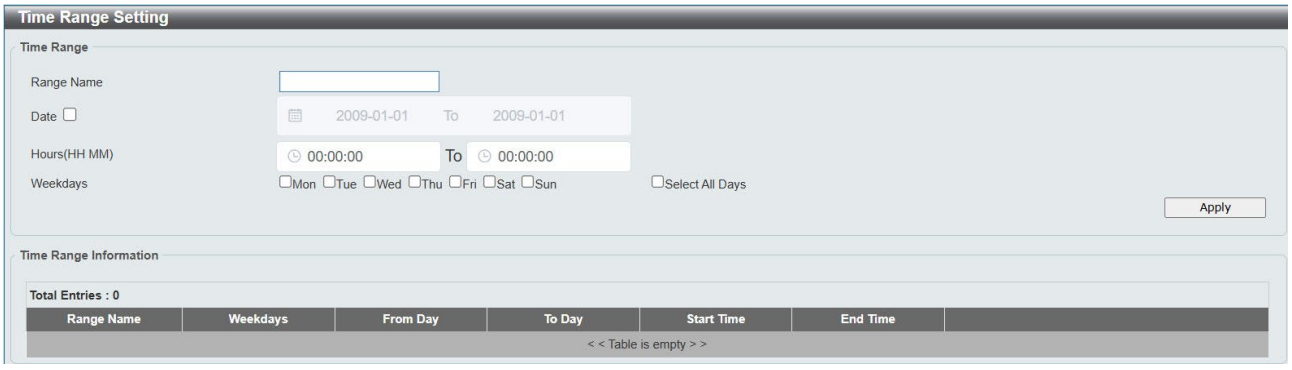


Figure 4.49 – System > Time Profile Settings

Range Name: Specifies the profile name for the time profile to be configured.

Date: Select Date and specifies the **From Day** and **To Day** of the time profile.

Hours (HH MM): Specifies the **Start Time** and **End Time.**

Weekdays: Specifies the work day for the time profile. Or tick **Select All Days** to select all days for the time profile.

Click **Apply** to create a new time profile or click **Delete** to delete a time profile from the table.

NOTE: The time must be set after current time, otherwise it will take effect on the next cycle time.

System > Power Saving

The Power Saving mode feature reduces power consumption automatically when the RJ-45 port is link down or the connected devices are turned off. Less power will be consumed also when the short cable is used (less than 20 meters).

By reducing power consumption, less heat is produced, resulting in extended product life and lower operating costs. By default, the Cable Length Detection and Link Status Detection are enabled. Click **Apply** to make the change effective.

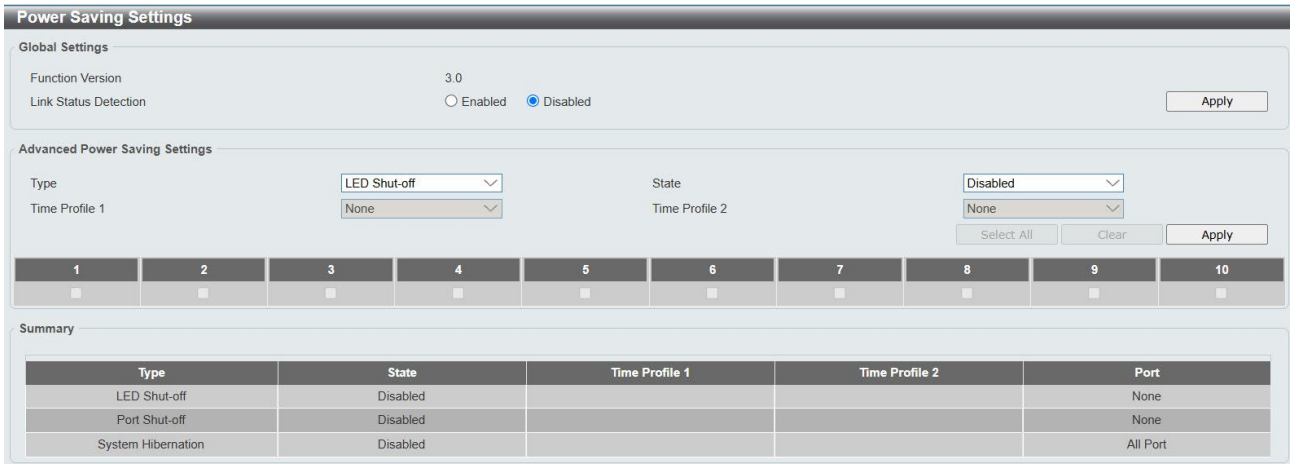


Figure 4.50 – System > Power Saving

Advanced Power Saving Settings:

Type: Specifies the Power Saving type to be LED Shut-off, Port Shut-off, Port Standby or System Hibernation.

LED Shut-off - The LED Shut-off gets high priority. If the user select LED Shut-off, the profile function will not take effect. It means the LED cannot be turned on after Time Profile time's up when the state is disabled. On the contrary, if the LED is enabled, the Time Profile function will work.

Port Shut-off - The Port Shut-off state has high priority (the priority rule is the same as LED.) Therefore, if the Port Shut-off sate is already disabled the Time Profile function will not take effect.

System Hibernation - In this mode, switches get most power-saving figures since main chipsets (both MAC and PHY) are disabled for all ports, and energy required to power the CPU is minimal.

State: Specifies the power saving state to be Enabled or Disabled.

Time Profile 1: Specifies the time profile or None.

Time Profile 2: Specifies the time profile or None.

Port: Specifies the ports to be configure of the Power Saving.

Click **Select All** configure all ports, or click **Clear** to uncheck all port. Then Click Apply to make the configurations take effect.

System > IEEE802.3az EEE Settings

The IEEE 802.3 EEE standard defines mechanisms and protocols intended to reduce the energy consumption of network links during periods of low utilization, by transitioning interfaces into a low-power state without interrupting the network connection. The transmitted and received sides should be IEEE802.3az EEE compliance. By default, the switch enabled the 802.3az EEE function. Users can disable this feature by individual port via the IEEE802.3az EEE setting page.

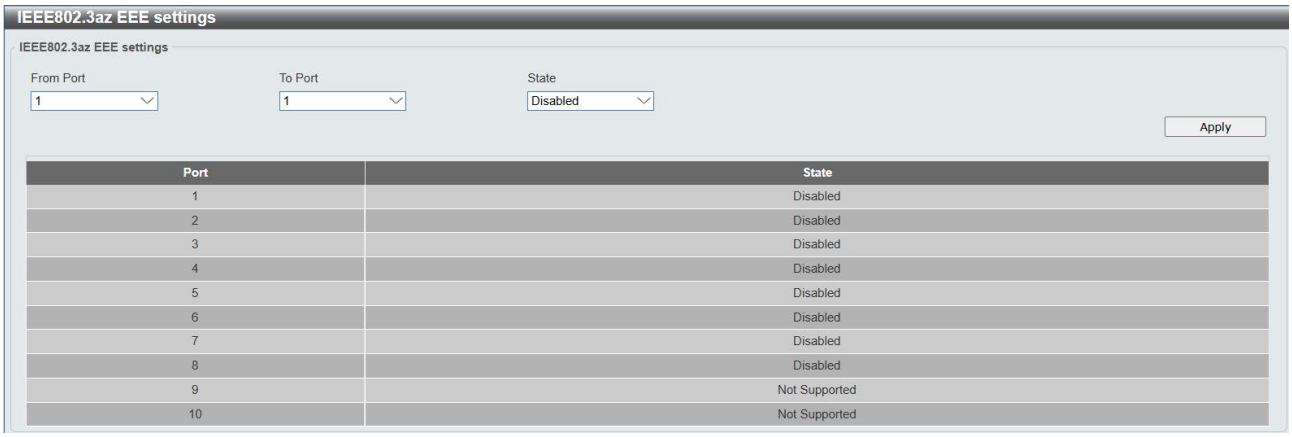


Figure 4.51 – System > IEEE802.3az EEE Settings

From Port / To Port: A consecutive group of ports may be configured starting with the selected port.

State: Enabled or Disabled the IEEE802.3az EEE for the specified ports. By default, all ports are disabled.

Click Apply to make the configurations take effect.

If the connection speed drops down from 1000M to 100M, or the first link up takes longer time, please follow below steps and check again:

1. Upgrade driver of Ethernet adapter or LAN controller for the host PC.
2. Disable EEE function on the switch port

System > SMTP Service > SMTP Server Settings

The SMTP Service Settings page is used to configure the fields to set up the SMTP server for the switch, along with setting e-mail addresses to which switch log file can be sent when a problem arises on the Switch.

User can **Enabled** or **Disabled** the SMTP State, then input the **SMTP Server Address**, **SMTP Server Port**, **Self Mail Address** and **Mail Receiver Address** then click **Apply** button to configure.

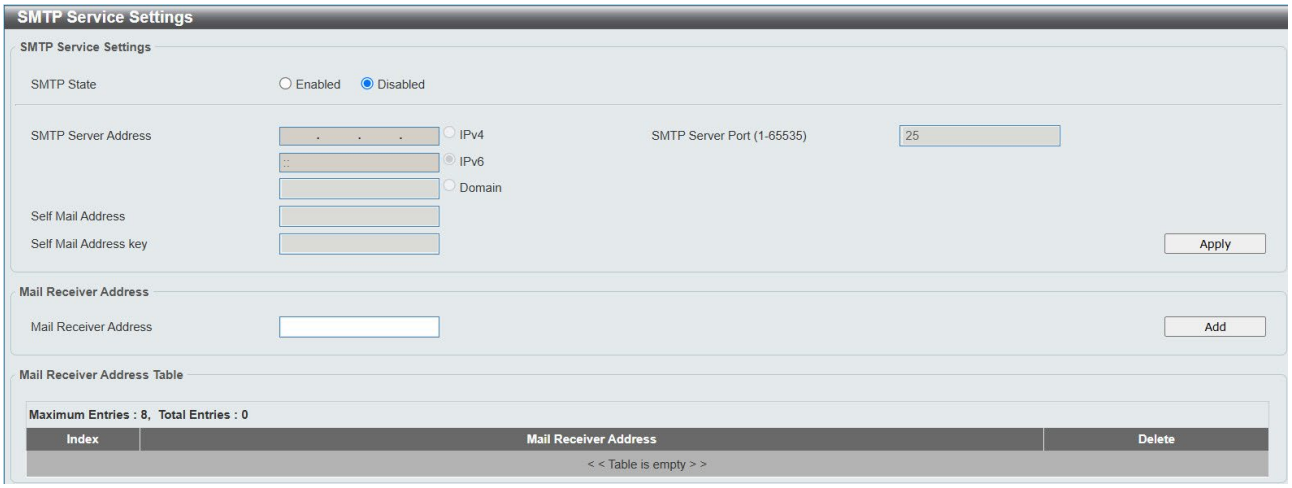


Figure 4.52 - System > SMTP Service > SMTP Server Settings

SMTP State: Enabled or Disabled the SMTP service on this device.

SMTP Server Address: Select IPv4 or IPv6 and enter the IP address of the SMTP server on a remote device. This will be the device that sends out the mail for user.

SMTP Server Port: Enter the virtual port number that the Switch will connect with on the SMTP server. The common port number for SMTP is *25*, yet a value between *1* and *65535* can be chosen.

Self Mail Address: Enter the e-mail address from which mail messages will be sent. This address will be the "from" address on the e-mail message sent to a recipient. Only one self mail address can be configured for this Switch. This string can be no more that *64* alphanumeric characters.

Mail Receiver Address: Enter a list of e-mail addresses so recipients can receive e-mail messages regarding Switch functions. Up to 8 e-mail addresses can be added per Switch. Do delete these addresses from the Switch, click **Delete** button from the Mail Receiver Address Table.

System > SMTP Service > SMTP Service

The SMTP Service is used to send test messages to all mail recipients configured on the Switch, thus testing the configurations set and the reliability of the SMTP server.

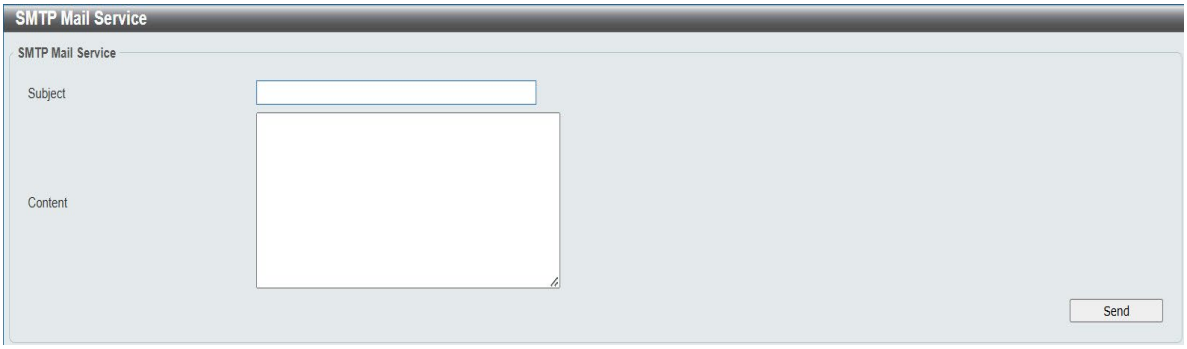


Figure 4.53 - System > SMTP Service > SMTP Service

Subject: Enter the subject of the test e-mail.

Content: Enter the content of the test e-mail.

Once the message is ready, click **Send** to send this mail to all recipients configured on the Switch for SMTP.

System > D-Link Discover Protocol Settings

For the D-Link Discovery Protocol (DDP) supported device, this page is an option for user to disable DDP or configure the DDP packet report timer.

D-Link Discover Protocol State: The default setting is **Disabled**.

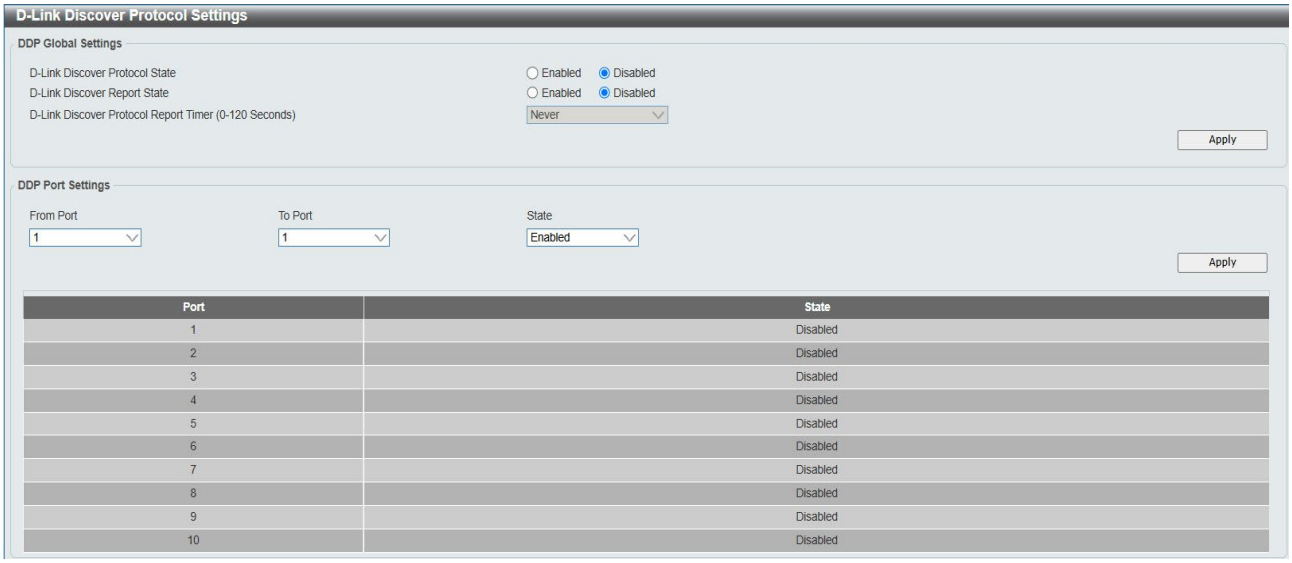


Figure 4.54 – System > D-Link Discover Protocol Settings

D-Link Discover Protocol Report Timer (Seconds): Configure the report timer of D-Link Discover Protocol in seconds. The values are 30, 60, 90, 120 or Never. The default is 30 seconds.

Click Apply to make the configurations take effect.

System > Power Supply Unit Capacity

Only DGS-1210-28X/ME support this power supply unit capacity settings, for DGS-1210-28X/ME maximum power battery Capacity settings.

Figure 4.55 – System > Power Supply Unit Capacity

PSU Max Battery Capacity: Allow settings range (0~65535), unit (mA).

Click Apply to make the configurations take effect.

Configuration > Jumbo Frame

Jumbo Frame support is designed to enhance Ethernet networking throughput and significantly reduce the CPU utilization of large file transfers like large multimedia files or large data files by enabling more efficient larger payloads per packet. The Jumbo Frame page allows network managers to enable Jumbo Frames on the device.

The Jumbo Frame default is disabled, Select Enabled then click **Apply** to turn on the jumbo frame support.

Figure 4.56 – Configuration > Jumbo Frame Settings

Configuration > 802.1Q VLAN

A VLAN is a group of ports that can be anywhere in the network, but communicate as though they were in the same area.

VLANs can be easily organized to reflect department groups (such as R&D, Marketing), usage groups (such as e-mail), or multicast groups (multimedia applications such as video conferencing), and therefore help to simplify network management by allowing users to move devices to a new VLAN without having to change any physical connections.

The IEEE 802.1Q VLAN Configuration page provides powerful VID management functions. The original settings have the VID as 1, no default name, and all ports as “Untagged”

Rename: Click to rename the VLAN group.

Delete VID: Click to delete the VLAN group.

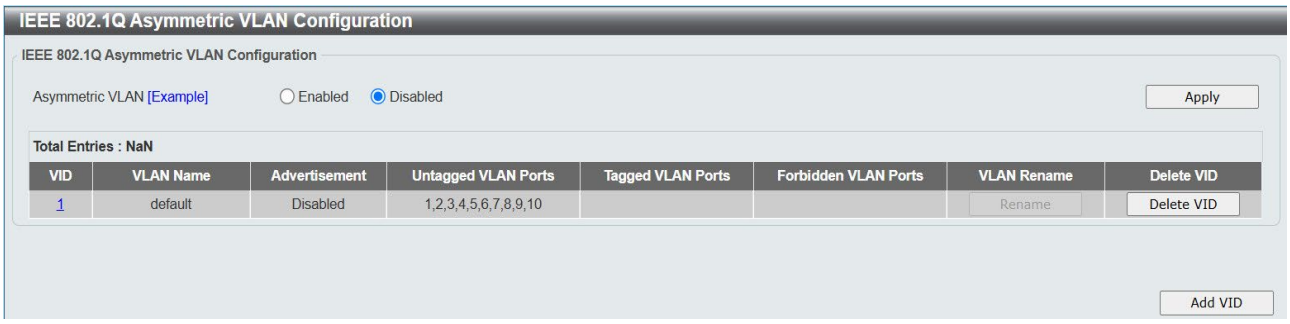


Figure 4.57 – Configuration > 802.1Q VLAN

Click **Add VID** to create a new VID group, assigning ports from 01 to 10 as **Untag**, **Tag**, **Forbidden** or **Not Member**. Enable or disable the **VLAN Advertisement**. A port can be untagged in only one VID. To save the VID group, click **Apply.**

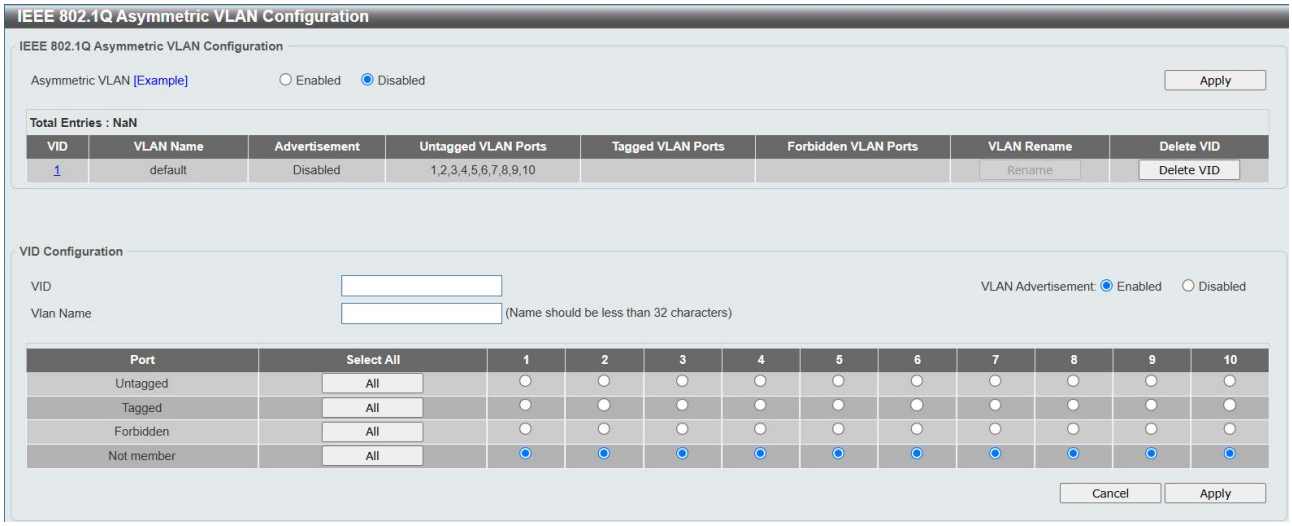


Figure 4.58 – Configuration > 802.1Q VLAN > Add VLAN

After click **Apply**, the 802.1Q VLAN Configuration Table will displayed with updates.

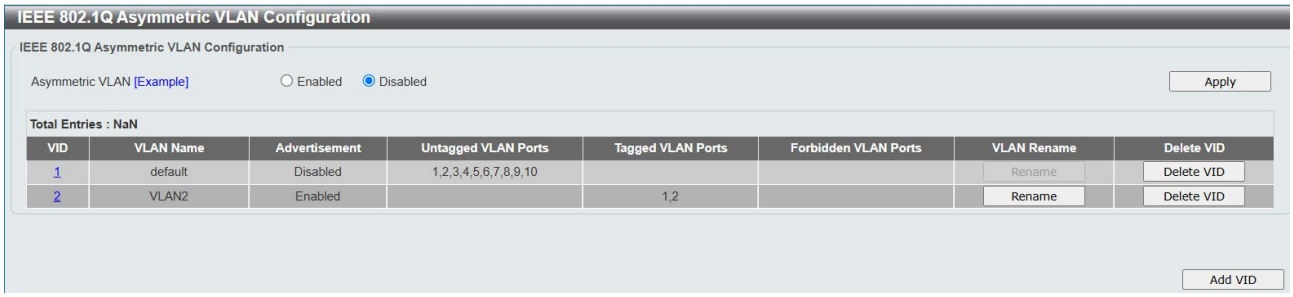


Figure 4.59 - Configuration > 802.1Q VLAN > Example VIDs

Click the VID number, the configuration of VLAN group which selected by user will displayed.

Change the port assignment then Click Apply to make the configurations take effect. User can also click the **Previous Page** to the go back to the previous page.

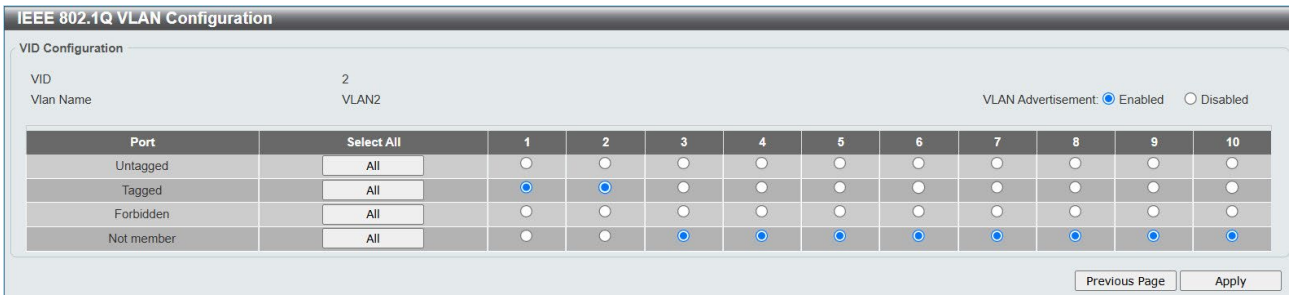


Figure 4.60 - Configuration > 802.1Q VLAN > VID Assignments

Select **Enabled** of Asymmetric VLAN and click **Apply** to change to Asymmetric VLAN mode:

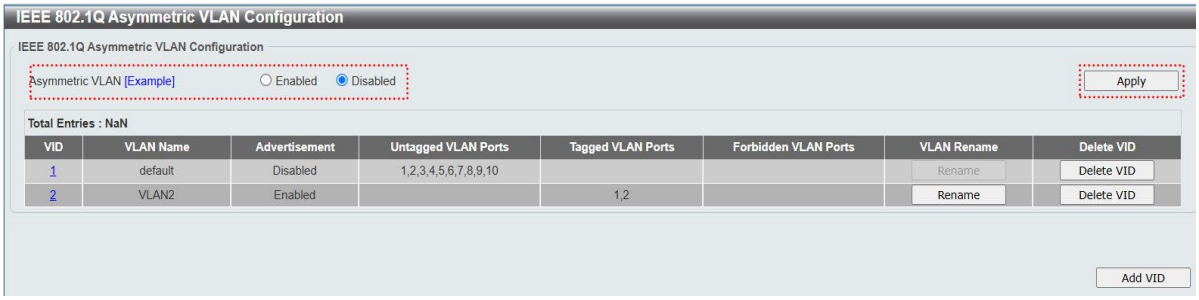


Figure 4.61 - Configuration > 802.1Q VLAN > VID Assignments

Configuration > Private VLAN > Private VLAN Settings

A private VLAN is comprised of a primary VLAN, up to one isolated VLAN, and a number of community VLANs. A private VLAN ID is presented by the VLAN ID of the primary VLAN. The command used to associate or disassociate a secondary VLAN with a primary VLAN.

A secondary VLAN cannot be associated with multiple primary VLANs. The untagged member port of the primary VLAN is named as the promiscuous port. The tagged member port of the primary VLAN is named as the trunk port. A promiscuous port of a private VLAN cannot be promiscuous port of other private VLANs. The primary VLAN member port cannot be a secondary VLAN member at the same time, or vice versa. A secondary VLAN can only have the untagged member port. The member port of a secondary VLAN cannot be member port of other secondary VLAN at the same time. When a VLAN is associated with a primary VLAN as the secondary VLAN, the promiscuous port of the primary VLAN will behave as the untagged member of the secondary VLAN, and the trunk port of the primary VLAN will behave as the tagged member of the secondary VLAN. A secondary VLAN cannot be specified with advertisement. Only the primary VLAN can be configured as a layer 3 interface. The private VLAN member port cannot be configured with the traffic segmentation function.

The Private VLAN Settings page allows the user to configure the Private VLAN settings.

Figure 4.62 - Configuration > Private VLAN > Private VLAN Settings

Add Private VLAN: Specify to add a private VLAN of the Switch.

VLAN Name: Enter a VLAN name for the private VLAN to be created. This name can be up to *32* characters in length.

VID (2-4094): Enter a VLAN ID for the private VLAN to be created. The value ranges between 2 and 4094.

VLAN List: Enter a list of VLAN ID for the private VLAN to be created.

Click **Add** to add a new entry based on the information entered.

Find Private VLAN: Specify to display a private VLAN information.

VLAN Name: Enter a VLAN name for the private VLAN to be displayed. This name can be up to *32* characters in length.

VID (2-4094): Enter a VLAN ID for the private VLAN to be displayed. The value ranges between 2 and 4094.

Click **Find** to locate a specific entry absed on the information entered.

Click **View All** to display all the existing entries.

Click **Edit** to configure the secondary VLAN as below:

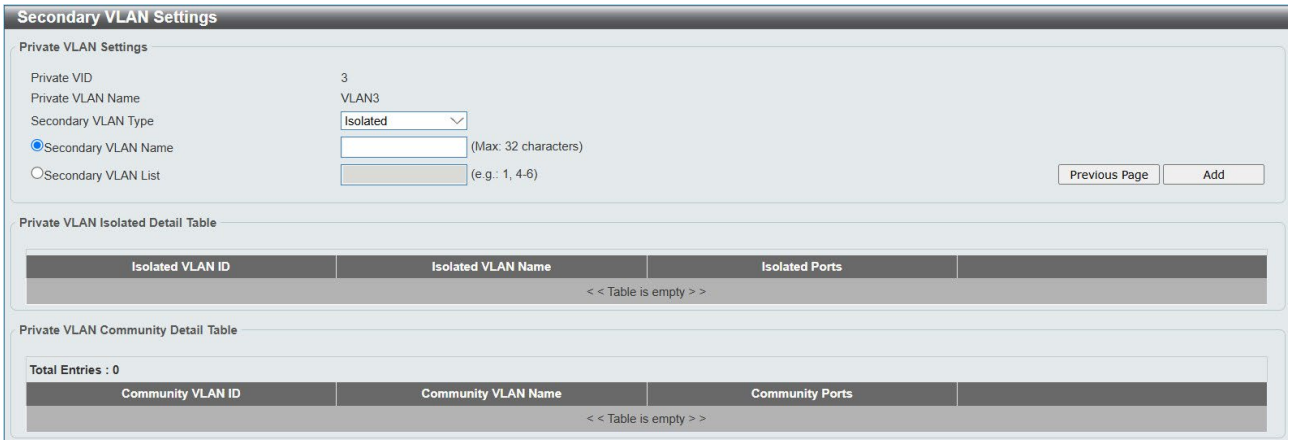


Figure 4.63 - Configuration > Private VLAN > Private VLAN Settings – Secondary VLAN Settings

Secondary VLAN Type: To specify the secondary VLAN type to be *Isolated* or *Community*.

Isolated – The ports within an isolated VLAN cannot communicate with each other at the Layer 2 level. Isolated ports are typically used for those endpoints that only require access to a limited number of outgoing interfaces on a Private VLAN enabled device. An endpoint connected to an isolated port will only possess the ability to communicate with those endpoints connected to promiscuous ports. Endpoints connected to isolated ports cannot communicate with one another.

Community – The ports within a community VLAN can communicate with each other but cannot communicate with ports in other communities at the Layer 2 level. Within a community, endpoints can communicate with one another and can also communicate with any configured promiscuous port. Endpoints belonging to one community cannot communicate with endpoints belonging to a different community or with endpoints connected to isolated ports.

Secondary VLAN Name: Enter a VLAN name for the secondary VLAN. This name can be up to *32* characters in length.

Secondary VLAN List: Enter a list of secondary VLAN ID. The value ranges between 2 and 4094.

Click **Add** to add a new entry based on the information entered.

Click **Previous Page** to the go back to the previous page.

Configuration > Private VLAN > Private VLAN Trunk

The Private VLAN Trunk setting page allows user to configure the trunk ports settings.

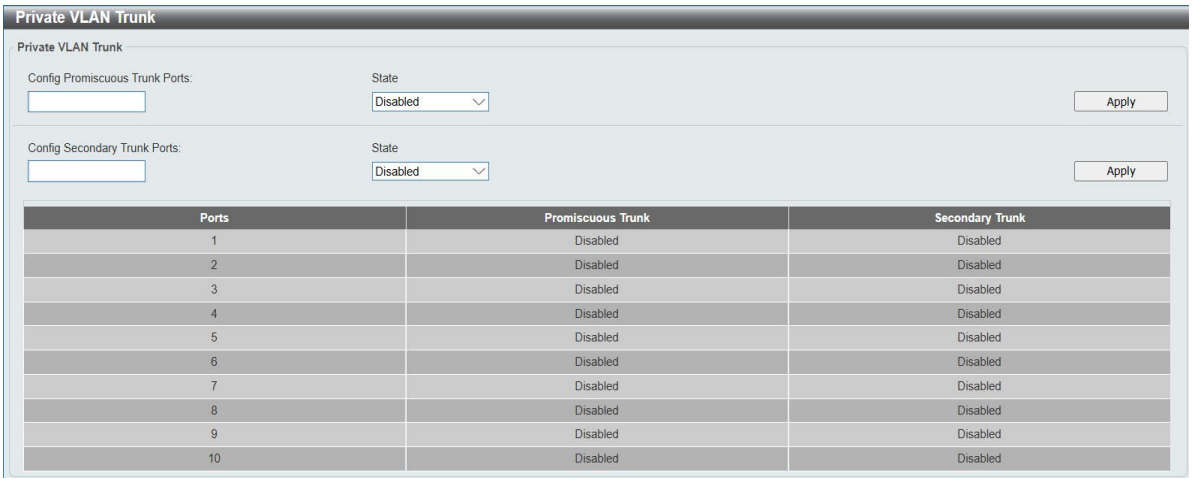


Figure 4.64 - Configuration > Private VLAN > Private VLAN Trunk

Config Promiscuous Trunk Ports: To specify the promiscuous trunk ports to the specified private VLAN to be enabled or disabled. A promiscuous port belongs to the primary VLAN and can communicate with all interfaces, including the community and isolated host ports and private VLAN trunk ports that belong to the secondary VLANs associated with the primary VLAN.

Config Secondary Trunk Ports: To specify the secondary trunk ports to the specified private VLAN to be enabled or disabled.

Click **Apply** to make the configurations take effect.

Configuration > VLAN Status

The VLAN Status page is for user to search the VLAN which has already existed on the Switch.

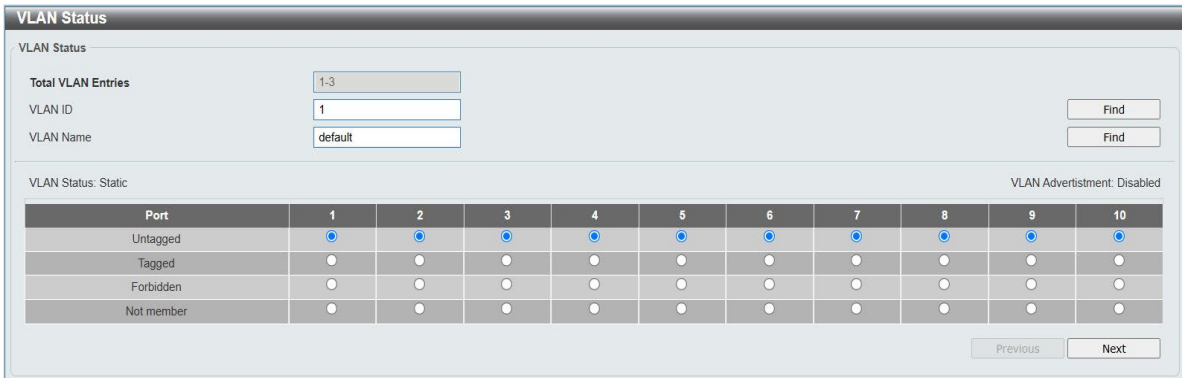


Figure 4.65 - Configuration > VLAN Status

Enter the **VLAN ID** or **VLAN Name** then click **Find** to show the existed VLAN.

Configuration > MAC-Based VLAN Settings

The table is used to create MAC-based VLAN entries on the switch. A MAC address can be mapped to any existing static VLAN and multiple MAC addresses can be mapped to the same VLAN. When a static MAC-based VLAN entry is created for a user, the traffic from this user is able to be serviced under the specified VLAN regardless of the authentication function operated on the port. Therefore each entry specifies a relationship of a source MAC address with a VLAN.

Figure 4.67 - Configuration > MAC-based VLAN

MAC Address: Specify the MAC address to be re-authenticated by entering it into the MAC Address field.

VID (1-4094) / VLAN Name: Enter the VID or VLAN name of a previously configured VLAN.

Configuration > GVRP Settings

The GVRP Settings page allows user to determine whether the Switch will share its VLAN configuration information with other **GARP VLAN Registration Protocol (GVRP)** enabled switches. In addition, Ingress Checking can be used to limit traffic by filtering incoming packets whose PVID does not match the PVID of the port. Results can be seen in the table under the configuration settings, as seen below.

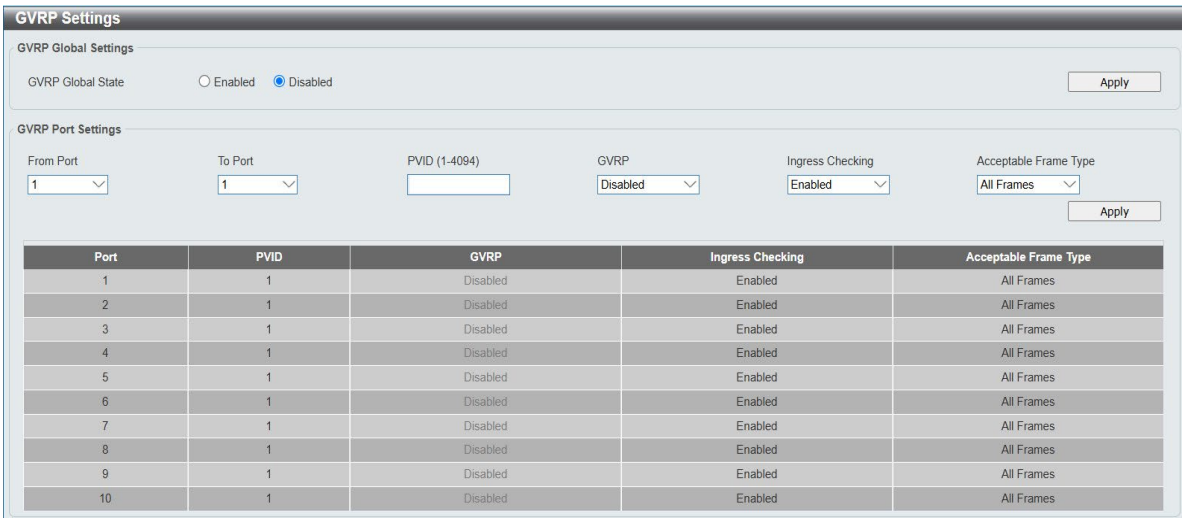


Figure 4.68 - Configuration > GVRP Settings

From Port/To Port: These two fields allow user to specify the range of ports that will be included in the Port-based VLAN that user is creating using the 802.1Q Port Settings page.

PVID (1-4094): The read-only field in the 802.1Q Port Table shows the current PVID assignment for each port, which may be manually assigned to a VLAN when created in the Settings table. The Switch's default is to assign all ports to the default VLAN with a VID of 1. The PVID is used by the port to tag outgoing, untagged packets, and to make filtering decisions about incoming packets. If the port is specified to accept only tagged frames - as tagging, and an untagged packet is forwarded to the port for transmission, the port will add an 802.1Q tag using the PVID to write the VID in the tag. When the packet arrives at its destination, the receiving device will use the PVID to make VLAN forwarding decisions. If the port receives a packet, and Ingress filtering is enabled, the port will compare the VID of the incoming packet to its PVID. If the two are unequal, the port will drop the packet. If the two are equal, the port will receive the packet.

GVRP: The Group VLAN Registration Protocol (GVRP) enables the port to dynamically become a member of a VLAN. GVRP is *Disabled* by default.

Ingress Checking: This field can be toggled using the space bar between Enabled and Disabled. Enabled enables the port to compare the VID tag of an incoming packet with the PVID number assigned to the port. If the two are different, the port filters (drops) the packet. Disabled disables ingress filtering. Ingress Checking is *Disabled* by default.

Acceptable Frame Type: This field denotes the type of frame that will be accepted by the port. The user may choose between **Tagged Only**, which means only VLAN tagged frames will be accepted, and Admit_All, which mean both tagged and untagged frames will be accepted. **Admit_All** is enabled by default.

Click Apply to make the configurations take effect.

Configuration > GVRP Timer Settings

The GVRP Timer Settings page allows user to configure the GARP timer values for application join, leave, and leave_all GARP timer values.

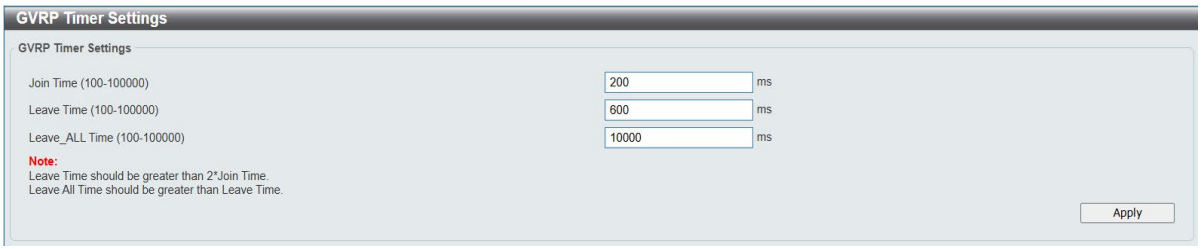


Figure 4.69 - Configuration > GVRP Timer Settings

Join Time (100-100000): Indicates the time in milliseconds that PDUs are transmitted. The default value is *200ms*.

Leave Time (100-100000): Indicates the amount of time in milliseconds that the device waits before leaving its GARP state. The leave time is activated by a leave all time message sent/received, and cancelled by the Join message. The default value is *600ms*.

Leave_All Time (100-100000): Used to confirm the port within the VLAN. The time in milliseconds between messages sent. The default value is *10000ms*.

Click Apply to make the configurations take effect.

Configuration > Voice VLAN > Voice VLAN Global Setting

Voice VLAN is a feature that allows user to automatically place the voice traffic from IP phone to an assigned VLAN to enhance the VoIP service. With a higher priority and individual VLAN, the quality and the security of VoIP traffic are guaranteed. If a VoIP packet comes with a VLAN tag, the Voice VLAN function won't replace the original VLAN tag.

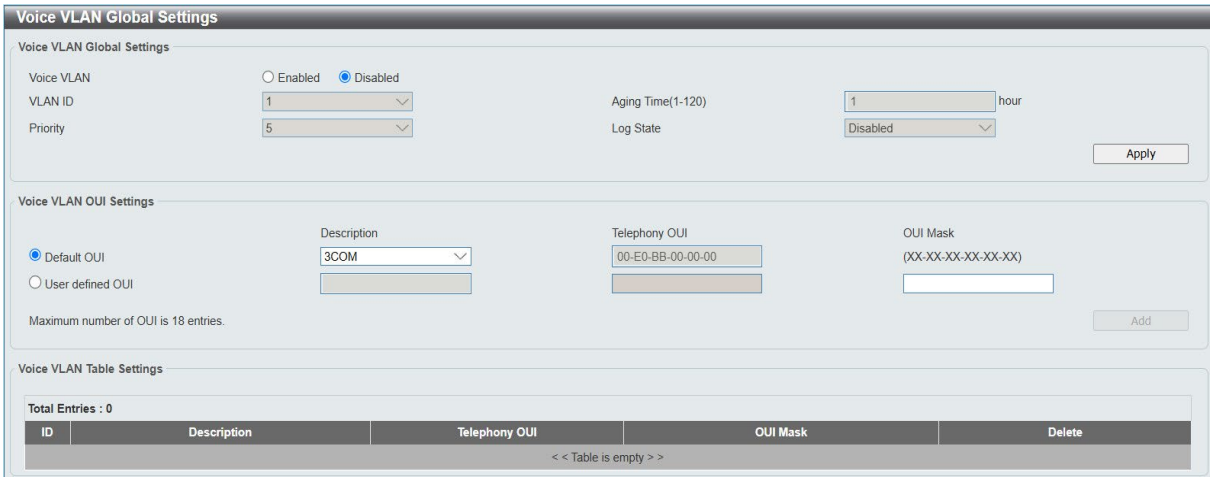


Figure 4.70 - Configuration > Voice VLAN > Voice VLAN Setting

Voice VLAN: Select to enable or disable Voice VLAN. The default is **Disabled**.

VLAN ID: The ID of VLAN that user wants to assign voice traffic to. User must assign the existed VLAN group as Voice VLAN. The member port configured in 802.1Q VLAN setting page will be the static member port of voice VLAN. To dynamically add ports into the voice VLAN, please enable the Auto Detection function

Priority: The 802.1p priority levels of the traffic in the Voice VLAN.

Aging Time (1-120): Enter a period of time (in hours) to remove a port from the voice VLAN if the port is an automatic VLAN member. When the last voice device stops sending traffic and the MAC address of this voice device is aged out, the voice VLAN aging timer will start. The port will be removed from the voice VLAN

after the expiration of the voice VLAN aging timer. Selectable range is from 1 to 120 hours, and default is 1. Click Apply to implement changes made.

Voice VLAN OUI Settings: This allows the user to configure the user-defined voice traffic's OUI. An Organizationally Unique Identifier (OUI) is the first three bytes of the MAC address. This identifier uniquely identifies a vendor, manufacturer, or other organization.

There are some pre-defined OUIs and when the user configures personal OUI, these pre-defined OUIs must be avoided. Below are the pre-defined voice traffic's OUI:

OUI	Vendor	Mnemonic Name
00:E0:BB	3Com	3com
00:03:6B	Cisco	cisco
00:E0:75	Veritel	veritel
00:D0:1E	Pingtel	pingtel
00:01:E3	Siemens	siemens
00:60:B9	NEC/ Philips	nec&philips
00:0F:E2	Huawei-3COM	huawei&3com
00:09:6E	Avaya	avaya

Default OUI: Pre-defined OUI values, including brand names of 3COM, Cisco, Veritel, Pingtel, Siemens, NEC/Philips, Huawei3COM, and Avaya.

User defined OUI: User can manually create a Telephony OUI with a description. The maximum number of user defined OUIs is 10. Select the OUI and press Add to the lower table to complete the Auto Voice VLAN setting. The OUI mask filed accepts empty value and default value FF-FF-FF-00-00-00 applied automatically.

Configuration > Voice VLAN > Voice VLAN Port Settings

The Voice VLAN Port Settings page allows users to automatically place the voice traffic from IP phone to an assigned VLAN to enhance the VoIP service. With a higher priority and individual VLAN, the quality and the security of VoIP traffic are guaranteed.

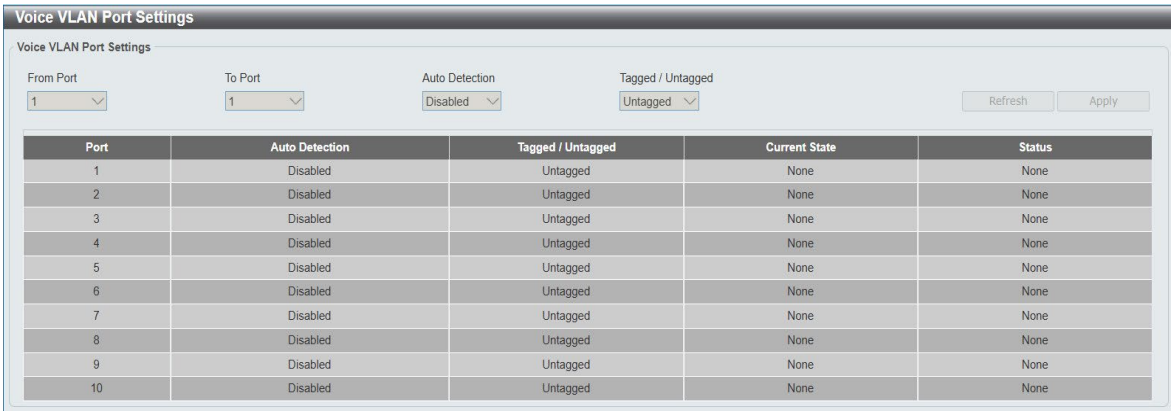


Figure 4.71 - Configuration > Voice VLAN > Voice VLAN Port Settings

From Port / To Port: A consecutive group of ports may be configured starting with the selected port.

Auto Detection: Switch will add ports to the voice VLAN automatically if it detects the device OUI matches the Telephony OUI configured in Voice VLAN OUI Setting page. Use the drop-down menu to enable or disable the OUI auto detection function. The default is Disabled

Tagged / Untagged: The role of specified port for auto detection of Voice VLAN member.

Click **Apply** to implement changes made and **Refresh** to refresh the Voice VLAN table.

Configuration > Voice VLAN > Voice Device List

The Voice Device List page displays the information of voice device learned from OUI.

Figure 4.72 - Configuration > Voice VLAN > Voice Device List

Configuration > Voice VLAN > LLDE-MED Voice Device List

The Voice Device List page displays the information of voice device learned from LLDP-MED protocol. The device information is retrieved from Network Policy contained in LLDP-MED packets.

Figure 4.73 - Configuration > Voice VLAN > LLDP-MED Voice Device List

Configuration > QinQ > QinQ Settings

The QinQ Settings page allows user to enable or disable the Q-in-Q function. Q-in-Q is designed for service providers to carry traffic from multiple users across a network.

Q-in-Q is used to maintain customer specific VLAN and Layer 2 protocol configurations even when the same VLAN ID is being used by different customers. This is achieved by inserting SPVLAN tags into the customer's frames when they enter the service provider's network, and then removing the tags when the frames leave the network.

Customers of a service provider may have different or specific requirements regarding their internal VLAN IDs and the number of VLANs that can be supported. Therefore customers in the same service provider network may have VLAN ranges that overlap, which might cause traffic to become mixed up. So assigning a unique range of VLAN IDs to each customer might cause restrictions on some of their configurations requiring intense processing of VLAN mapping tables which may exceed the VLAN mapping limit. Q-in-Q uses a single service provider VLAN (SPVLAN) for customers who have multiple VLANs. Customer's VLAN IDs are segregated within the service provider's network even when they use the same customer specific VLAN ID. Q-in-Q expands the VLAN space available while preserving the customer's original tagged packets and adding SPVLAN tags to each new frame. Select *Enabled* or *Disabled* then click **Apply** to enable or disable the Q-in-Q Global Settings.

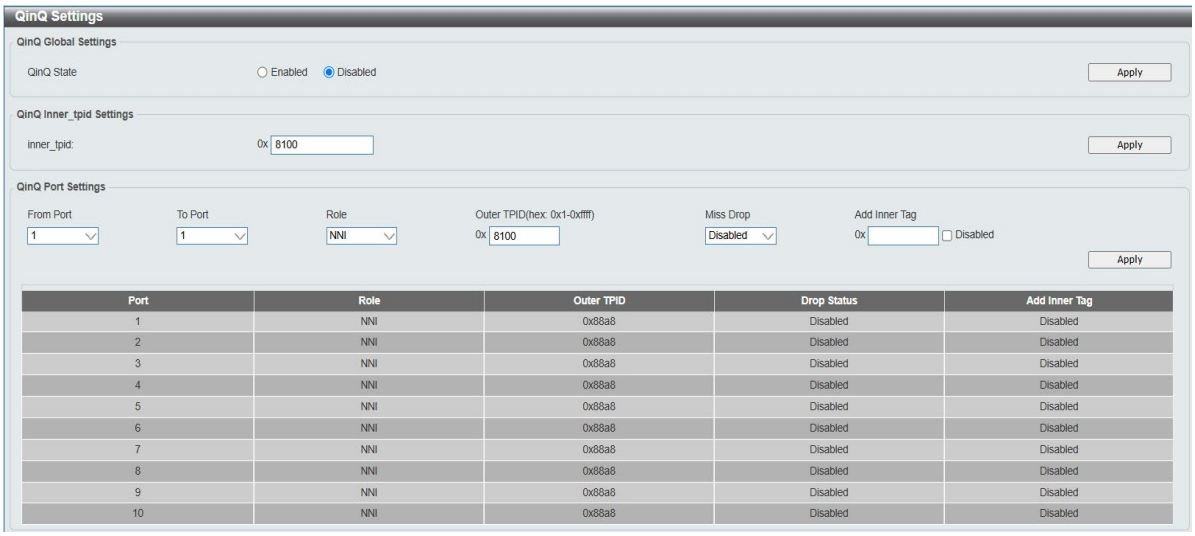


Figure 4.74 - Configuration > QinQ > QinQ Settings

From Port / To Port: A consecutive group of ports that are part of the VLAN configuration starting with the selected port.

Role: The user can choose between *UNI* or *NNI* role.

UNI – To select a user-network interface which specifies that communication between the specified user and a specified network will occur.

NNI – To select a network-to-network interface specifies that communication between two specified networks will occur.

Outer TPID (hex: 0x1-0xffff): The Outer TPID is used for learning and switching packets. The Outer TPID constructs and inserts the outer tag into the packet based on the VLAN ID and Inner Priority.

Miss Drop: Specifies to enable or disable the Miss Drop. If Miss Drop is enabled, the packet does not match any assignment rule in the VLAN translation and Q-in-Q profile will be dropped. If disabled, the packet will be forwarded and will be assigned to the PVID of the received port.

Add Inner Tag: Unselect the **Disable** check box and enter an entry that an Inner Tag will be added to the entry.

Click **Apply** to make the configurations take effect.

Configuration > QinQ > VLAN Translation CVID Entry Settings

The VLAN Translation translates the VLAN ID carried in the data packets it receives from private networks into those used in the Service Providers network.

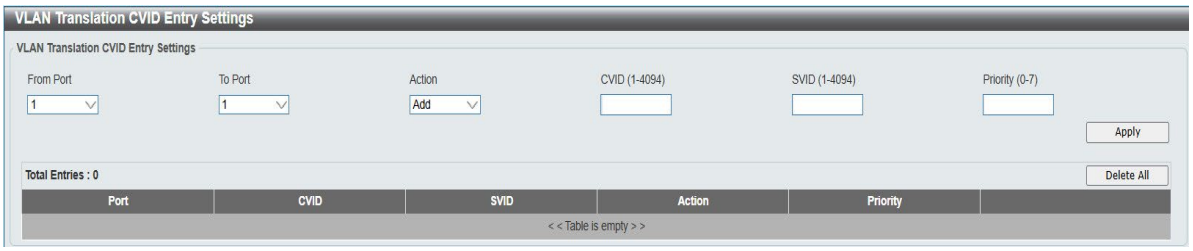


Figure 4.75 - Configuration > QinQ > VLAN Translation CVID Entry Settings

From Port / To Port: A consecutive group of ports that are part of the VLAN configuration starting with the selected port.

Action: Specify for SPVID packets to be added or replaced.

CVID List (1-4094): The customer VLAN ID List to which the tagged packets will be added.

SVID (1-4094): This configures the VLAN to join the Service Providers VLAN as a tagged member.

Priority: Specifies the CVID entry priority.

Click Apply to make the configurations take effect. Click **Delete All** to remove all the CVID entries.

Q-in-Q and VLAN Translation Rules:

For Ingress untagged packets at UNI ports:

1. The Switch does not reference the VLAN translation table.
2. Check the Switch VLAN tables. The Sequence is MAC-based VLAN -> subnet-based VLAN -> protocol-based VLAN -> port-based VLAN. If matched, the matched VLAN will become this packet's SPVLAN.

For Ingress tagged packets at UNI ports:

1. The Switch looks up the VLAN translation table. If matched, the VLAN tag will be translated (replace CEVLAN with SPVLAN, or add SPVLAN).
2. Or, check the Switch VLAN tables. The sequence is the same as above. The matched VLAN becomes this packet's SPVLAN.

Configuration > Layer 2 Protocol Tunneling Settings

The layer 2 protocol tunneling is used to tunnel the layer 2 protocol packets. When the device is operating with the Q-in-Q enabled, DA will be replaced by the tunnel multicast address, and the BPDU will be tagged with the tunnel VLAN based on the QinQ VLAN configuration and the tunnel/uplink setting. When the device is operating with the Q-in-Q disabled, the BPDU will have its DA replaced by the tunnel multicast address and is transmitted out based on the VLAN configuration and the tunnel/uplink setting.

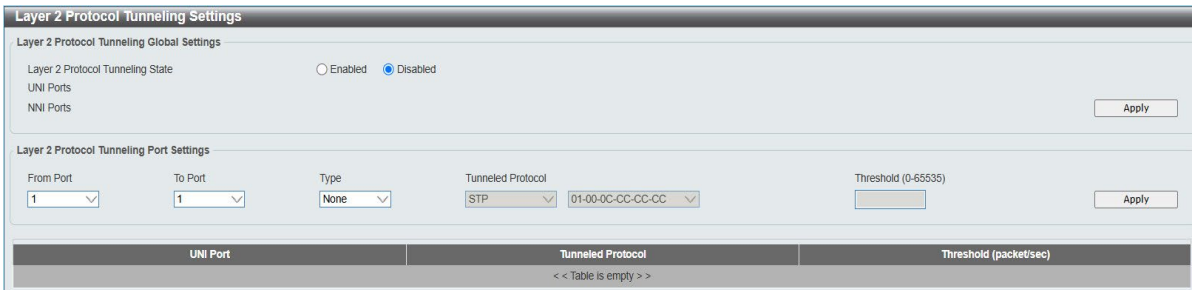


Figure 4.76 - Configuration > Layer2 Protocol Tunneling Settings

Layer 2 Protocol Tunneling State: Specify to enable or disable the layer 2 Protocol Tunneling of ports.

From Port / To Port: A consecutive group of ports that are part of the configuration starting with the selected port.

Type: Specify the layer 2 protocol tunnel type which will apply on the specified ports.

UNI – Specify the port is UNI port.

NNI – Specify the port is NNI port.

None – Disable the tunneling function.

Tunneled Protocol: Specify tunneled protocols on this UNI port.

STP – Specify the BPDU received on these UNI will be tunneled.

GVRP – Specify the GVRP PDU received on these UNI will be tunneled.

Protocol MAC – Specify the destination MAC address of the L2 protocol packets that will tunneled on these UNI ports. The MAC address can be 01-00-0C-CC-CC-CC or 01-00-0C-CC-CC-CD.

All – Specify all supported.

Threshold (0-65535): Specify the drop threshold for packets-per-second accepted on this UNI port. The port drops the PDU if the protocol's threshold is exceeded. The range of the threshold value is 0 to 65535 (packet/second). The value 0 means unlimited. By default, the value is 0.

Click Apply to make the configurations take effect.

Configuration > 802.1v Protocol VLAN > 802.1v Protocol Group Settings

The 802.1v Protocol Group Settings page allows user to configure the untagged ports of different protocols on the same physical port.

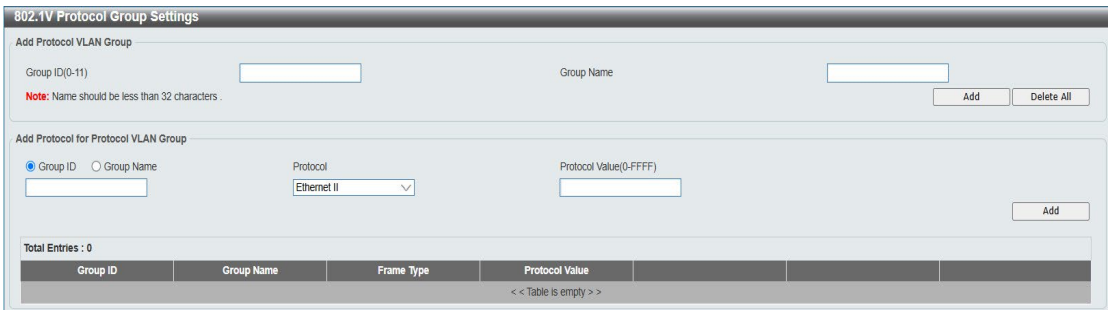


Figure 4.77 - Configuration > 802.1v Protocol VLAN > 802.1v Protocol Group Settings

Group ID (1-16): Select an ID number for the group. The value is between 1 and 16.

Group Name: Specifies the group name for the 802.1v protocol group.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete All** button to remove all the entries based on the information entered.

Protocol: Specifies the packets to protocol-defined VLANs by examining the type octet within the packet header to discover the type of protocol associated with it. The types are Ethernet II, IEEE802.3 SNAP, and IEEE802.3 LLC.

Protocol Value: Enter a value for the group. The protocol value is used to identify a protocol of the frame type specified. The form of the input is 0x0 to 0xffff.

Configuration > 802.1v Protocol VLAN > 802.1v Protocol VLAN Settings

The 802.1v Protocol VLAN Settings page allows user to configure the Protocol VLAN settings.

Figure 4.78 - Configuration > 802.1v Protocol VLAN > 802.1v Protocol VLAN Settings

Group ID: Select a previously configured Group ID from the drop-down menu.

VID (1-4094): Specifies the VID to be created.

Group Name: Select a previously configured Group Name from the drop-down menu.

VLAN Name: Specifies the VLAN name to be created.

Port List: Enter the specified ports to be configured or tick the **All Ports** check box.

Click the **Add** button to add a new entry based on the information entered.

Search Port List: Specifies the port to be searched.

Click the **Find** button to view the information with specified ports.

To display all previously configured port lists on the button half of the screen click the **Show All** button.

To clear all previously configured lists click the **Delete All** button.

Configuration > VLAN Trunk Settings

The VLAN Trunk Settings is used to combine a number of VLAN ports together to create VLAN trunks. To create VLAN Trunk Port settings on the Switch, enter the ports to be configured, change the state to *Enabled* and click **Apply**, the new settings will appear in the **VLAN Trunk Port Settings Table** below.

Figure 4.79 - Configuration > VLAN Trunk Settings

Click **Select All** to check all ports or click **Clear** to remove ports then click **Apply**.

Click Apply to make the configurations take effect.

Configuration > Link Aggregation > Port Trunkings

The Port Trunkings function enables the combining of two or more ports together to increase bandwidth. Up to eight Trunk groups may be created, and each group consists up to eight ports. Select **Enabled** and click **Apply** to active the Link Aggregation State.

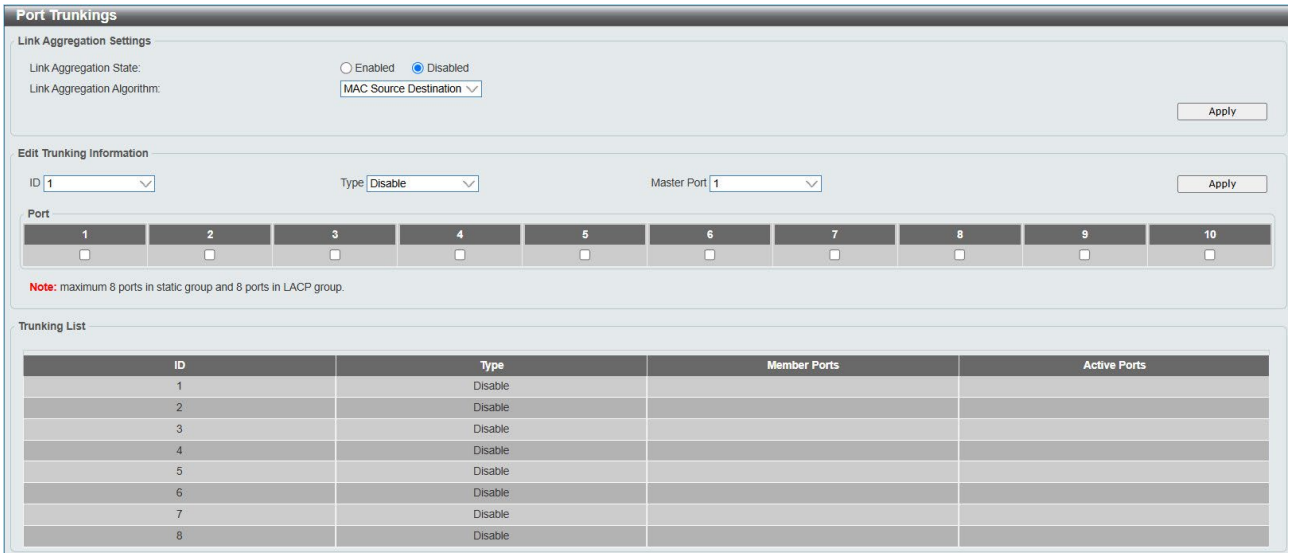


Figure 4.80 – Configuration > Link Aggregation > Port Trunkings

Link Aggregation Algorithm: Specify the algorithm to be *MAC Source, MAC Destination, MAC Source Destination, IP Source, IP Destination or IP Source Destination*, and then Click Apply to make the configurations take effect.

Edit Trunking Information:

Specify the **ID**, **Type** and **Master Port** then select the ports to be grouped together, and then click **Apply** to activate the selected Trunking groups. Two types of link aggregation can be selected:

Static - Static link aggregation.

LACP - LACP (Link Aggregation Control Protocol) is enabled on the device. LACP allows for the automatic detection of links in a Port Trunking Group.

Disable - Remove all members in this trunk group.

NOTE: Each combined trunk port must be connected to devices within the same VLAN group.

Configuration > Link Aggregation > LACP Port Settings

The LACP Port Settings is used to create port trunking groups on the Switch. The user may set which ports will be active and passive in processing and sending LACP control frames.

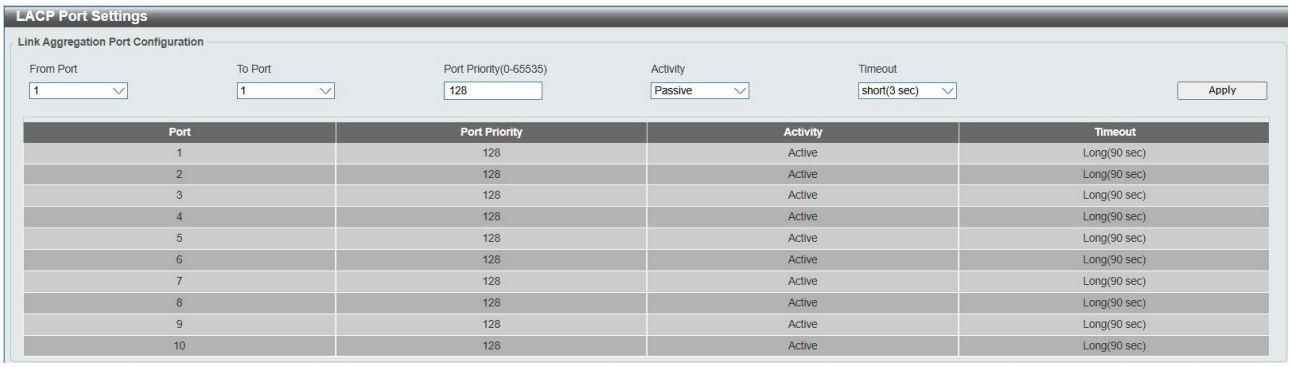


Figure 4.81 – Configuration > Link Aggregation > LACP Port Settings

From Port: The beginning of a consecutive group of ports may be configured starting with the selected port.

To Port: The ending of a consecutive group of ports may be configured starting with the selected port.

Port Priority (0-65535): Displays the LACP priority value for the port. Default is *128*.

Activity: There are two different roles of LACP ports:

Active - Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP.

Passive - LACP ports that are designated as passive cannot initially send LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, one end of the connection must have "active" LACP ports.

Timeout: Specify the administrative LACP timeout. The possible field values are:

Short (3 Sec) - Defines the LACP timeout as 3 seconds.

Long (90 Sec) - Defines the LACP timeout as 90 seconds. This is the default value.

Click **Apply** to implement the changes made.

Configuration > FlexLink Settings

The Flex Links are a pair of a Layer 2 interfaces (ports or port channels), where one interface is configured to act as a backup to the other.

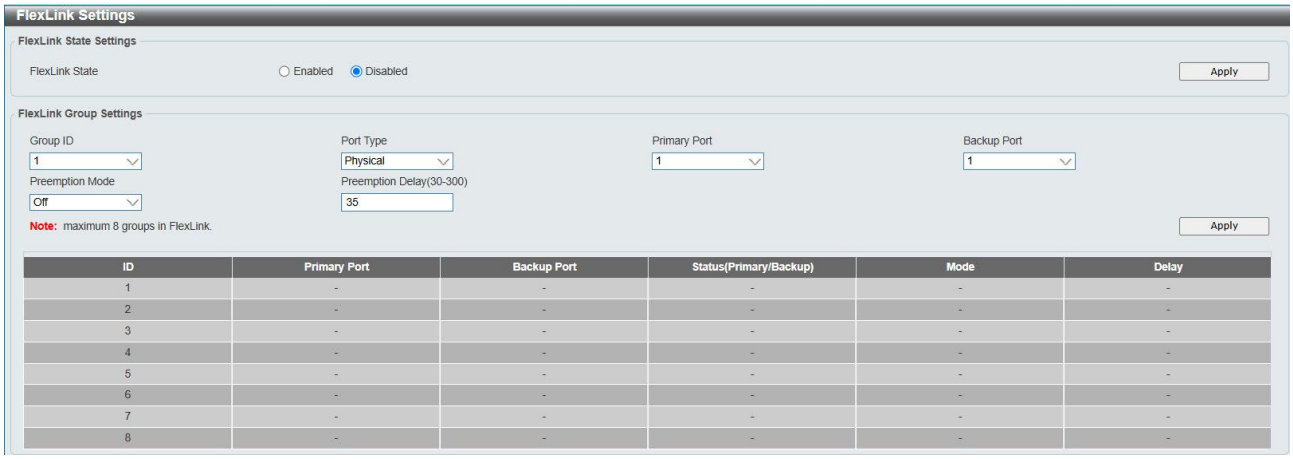


Figure 4.82 – Configuration > FlexLink Settings

Group ID: Select the group ID from 1~8.

Port Type: Select the type “Physical”, “Link Aggregation” or “Disable” for Flex link group.

Physical: Physical port interface

Link Aggregation: Link aggregation group (from channel group 1 to 8)

Disable: Used to remove the exist flex link group.

Primary Port: Select the port (or channel group) as primary port of flex link.

Backup Port: Select the port (or channel group) as backup port of flex link.

Preemption Mode: Select the preemption mode:

Force: The active interface always preempts the backup

Bandwidth: The interface with the higher bandwidth always acts as the active interface

Off: There is no preemption; the first interface that is up is put in forwarding mode.

Preemption Delay: Used to specify amount of time (in seconds) before preempting a working interface for another

Click **Apply** to implement the changes made.

Configuration > BPDU Protection Settings

The BPDU Protection Settings page allows user to configure the BPDU protection function for the ports on the Switch. In generally, there are two states in BPDU protection function. One is normal state, and another is under attack state. The under attack state have three modes: drop, block, and shutdown. A BPDU protection enabled port will enter and under attack state when it receives one STP BPDU packet. And it will take action based on the configuration. Thus, BPDU protection can only be enabled on the STP-disabled port. Select *Enabled* or *Disabled* and click **Apply** to enabled or disable the BPDU attack protection state.

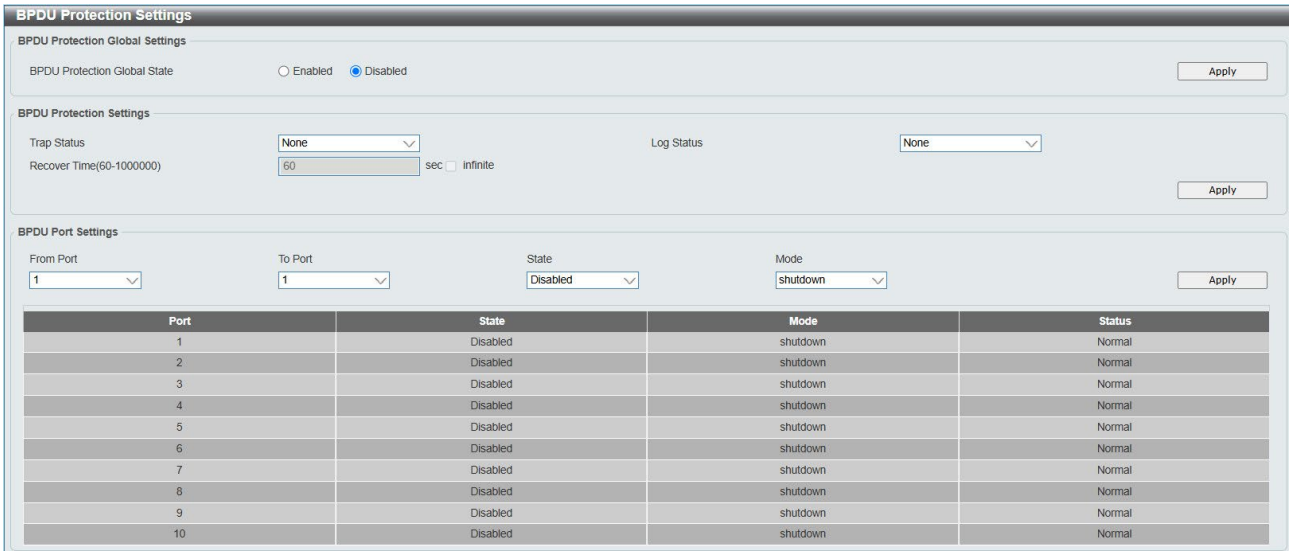


Figure 4.83 – Configuration > BPDU Protection Settings

Trap Status: Specify to send trap packet when *Attack Detected, Attack Cleared, None* or *Both.*

Log Status: Specify the Log Status when *Attack Detected, Attack Cleared, None* or *Both.*

Recover Time (60-1000000): Specify the BPDU protection Auto-Recovery timer, the range is from *60* to *1000000* and default is *60* seconds. Or select *infinite*.

Click **Apply** for changes to take effect.

From Port / To Port: Specify the port ranges to be configured.

State: To enabled or disable the protection mode for a specific port.

Mode: Specify the BPDU protection mode. The default mode is shutdown.

Drop – Drop all received BPDU packets when the port enters under attack stats.

Block – Drop all packets (includes BPDU and normal packets) when the port enters under attack state.

Shutdown – Shut down the port when the port enters under attack state.

Click **Apply** for changes to take effect.

Configuration > IGMP Snooping > IGMP Snooping

With Internet Group Management Protocol (IGMP) snooping, the DGS-1210/ME CX Metro Management Ethernet Switch can make intelligent multicast forwarding decisions by examining the contents of each frame's Layer 2 MAC header.

IGMP snooping can help reduce cluttered traffic on the LAN. With IGMP snooping enabled globally, the DGS-1210/ME CX Metro Management Ethernet Switch will forward multicast traffic only to connections that have group members attached.

The settings of IGMP snooping is set by each VLAN individually.

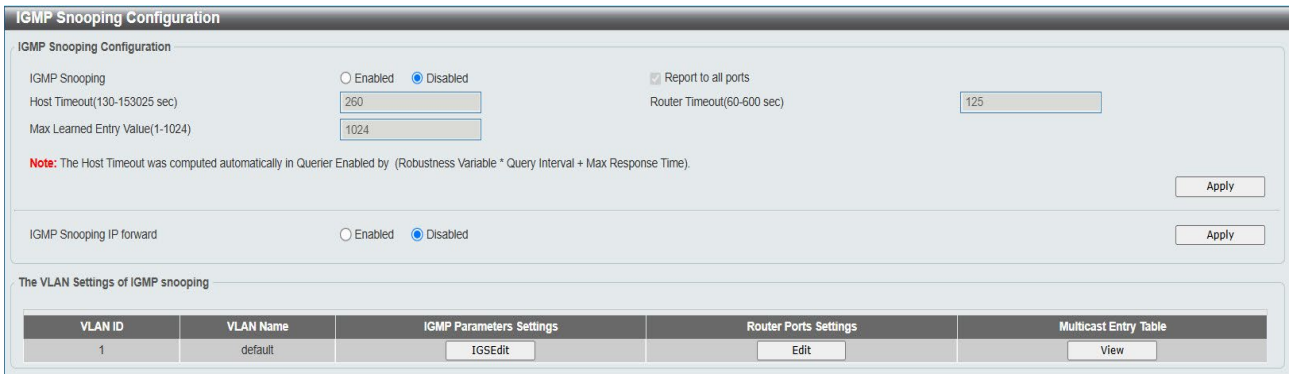


Figure 4.84 – Configuration > IGMP Snooping > IGMP Snooping

By default, IGMP is disabled. If enabled, the IGMP Global Settings will need to be entered:

Parameters	Description
IGMP Snooping	Used to control IGMP snooping global state; the radios buttons **enable**/**disable** to change the state.
Host Timeout (130-153025 sec)	This is the interval after which a learned host port entry will be purged. For each host port learned, a 'Port Purge Timer' runs for 'Host Port Purge Interval'. This timer will be restarted whenever a report message from host is received over that port. If no report messages are received for 'Host Port Purge Interval' time, the learned host entry will be purged from the multicast group. The default value is 260 seconds.
Router Timeout (60-600 sec)	This is the interval after which a learned router port entry will be purged. For each router port learned, a 'Router Port Purge Timer' runs for 'Router Port Purge Interval'. This timer will be restarted whenever a Query control message is received over that port. If there were no Query control messages received for 'Router Port Purge Interval' time, the learned router port entry will be purged. Default is 260 seconds.
Max Learned Entry Value (1-1024)	The maximum IGMP group(s) allowed to be learned for entire system. The range from 1 to 1024 groups. The default value is 1024 groups.
IGMP Snooping Rate Limit	Used to control if system has the maximum process limit especially for IGMP packet (IGMP report, IGMP leave and IGMP query). Lower rate helps to lower the CPU loading. **Rate Limit Value** is a range from 1-200 in PPS.

Clicking **Apply** button for apply the changes.

Click **IGSEdit** button to enter the IGMP Parameters Settings page.

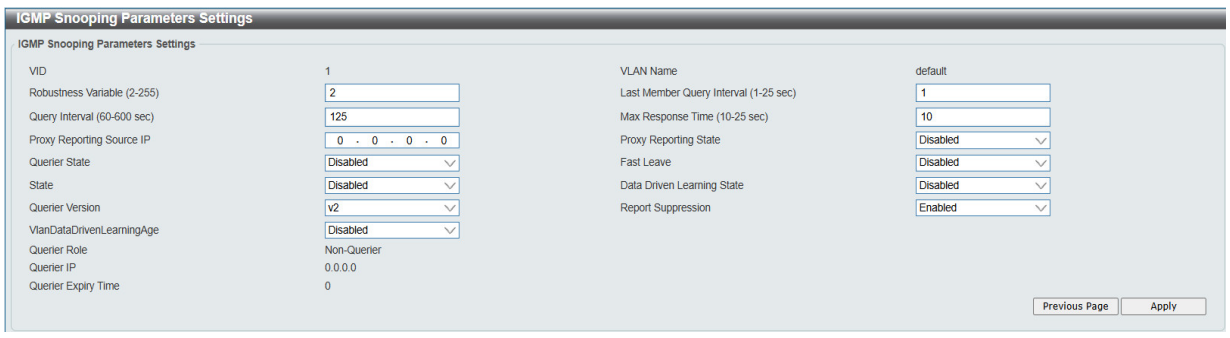


Figure 4.85 – Configuration > IGMP Snooping > IGMP Snooping Parameters Settings

Parameters	Description
State	Used to control IGMP snooping state for this particular VLAN group. The state **Enabled**/**Disabled** can be selected in drop-down list.
Robustness Variable (2-255 sec)	The Robustness Variable allows adjustment for the expected packet loss on network. The larger robustness variable help to prevent packet lost occurred in network; the key types of packet for IGMP: report, leave and query. The Robustness Variable cannot be set to zero, and it SHOULD NOT be. Default is 2 seconds
Query Interval (60-600 sec)	The Query Interval is the interval between General Queries sent. By adjusting the Query Interval, the number of IGMP messages can be increased or decreased; larger values will cause IGMP Queries to be sent less often. Default value is 125 seconds.
Last Member Query Interval (1-25 sec)	The Last Member Query Interval is the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query messages. This value may be adjusted to modify the "leave latency" of the network. A reduced value results in reduced time to detect the loss of the last member of a group. Default is 1 second.
Max Response Time (10-25 sec)	The Max Response Time specifies the maximum allowed time before sending a responding report message. Adjusting this setting effects the "leave latency", or the time between the moment the last host leaves a group and when the multicast server is notified that there are no more members. It also allows adjustments for controlling the frequency of IGMP traffic on a subnet. Default is 10 seconds.
Proxy Reporting Source IP	Enter the proxy reporting source IP address.
Proxy Reporting	Use the drop-down menu to enable and disable the proxy report state.
Querier State	Device starts sending general query packets by Query Interval when state configured to **Enabled**. Device stop sending general query packet when state configured to **Disabled**.
Querier Version	Specify the general query packet version; **v1**, **v2** and **v3** are available to use.
Fast Leave	If enabled, the membership is immediately removed when the system receive the IGMP leave message.
Data Driven Learning State	Data Driven learning is a mechanism that helps to register the IGMP group via multicast traffic packet. The feature helps to solve some special network application that end host does not support IGMP function but only sending multicast traffic; for example, IP camera.
VLANDateDrivenLearningAge	Specifies that the aging out of the entry will be enabled or disabled.
Report Suppression	By **Enabled Report Suppression**, the device forward 1 IGMP report that registered the same IGMP group in 10 seconds period.
Querier Role	Display the current information for **Querier Role**.
Querier IP	Display the current information of **Querier IP address**.
Querier Expiry Time	Display the current information for **Querier Expiry Time**.

Clicking **Apply** button for apply the changes.

Clicking **Previous Page** returned to IGMP Snooping Configuration page.

Click **Edit** button to enter the Router Port Settings page, and the ports to be assigned as router ports for IGMP snooping for the VLAN.

A router port configured manually is a **Static Router Port**, a **Forbidden Router Port** and a **Dynamic Router Port** is dynamically configured by the Switch when a query control message is received. Press **Apply** for changes to take effect.

Figure 4.86 – Configuration > IGMP Snooping > IGMP Snooping-Router Port Settings

To view the Multicast Entry Table for a given VLAN, press the **View** button.

Figure 4.87– Configuration > IGMP Snooping > IGMP Snooping-Multicast Entry Table

Configuration > IGMP Snooping > IGMP Access Control Settings

The IGMP Access Control Settings page is used to enable or disable the IGMP access control of selected ports.

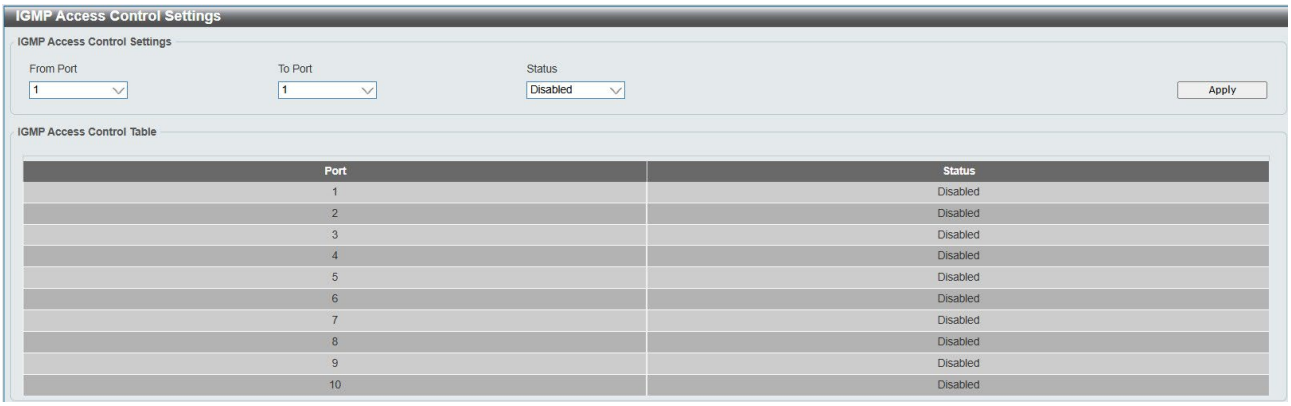


Figure 4.88 – Configuration > IGMP Snooping > IGMP Access Control Settings

From Port/To Port: Select the port ranges to be configured.

Status: Enable or disable the IGMP Access Control of specified ports.

Click **Apply** to make the configurations take effect.

Configuration > IGMP Snooping > ISM VLAN Settings

In a switching environment, multiple VLANs may exist. Every time a multicast query passes through the Switch, the switch must forward separate different copies of the data to each VLAN on the system, which, in turn, increases data traffic and may clog up the traffic path. To lighten the traffic load, multicast VLANs may

be incorporated. These multicast VLANs will allow the Switch to forward this multicast traffic as one copy to recipients of the multicast VLAN, instead of multiple copies.

Regardless of other normal VLANs that are incorporated on the Switch, users may add any ports to the multicast VLAN where they wish multicast traffic to be sent. Users are to set up a source port, where the multicast traffic is entering the switch, and then set the ports where the incoming multicast traffic is to be sent. The source port cannot be a recipient port and if configured to do so, will cause error messages to be produced by the switch. Once properly configured, the stream of multicast data will be relayed to the receiver ports in a much more timely and reliable fashion.

The ISM VLAN Settings page allows the user to configure the ISM VLAN.

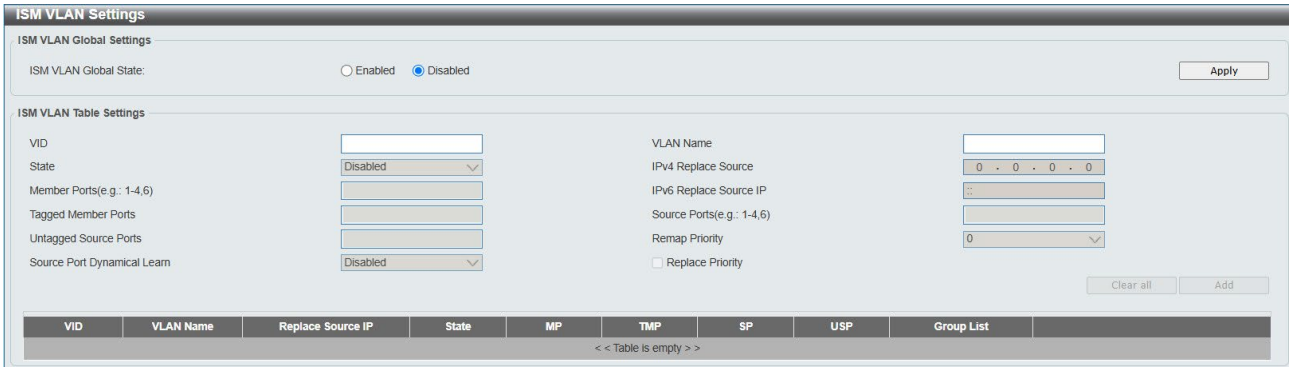


Figure 4.89 - Configuration > IGMP Snooping > ISM VLAN Settings

ISM VLAN Global State: Enable or disable the IGMP Snooping Multicast (ISM) VLAN Global State.

Click **Apply** button to confirm the ISM VLAN Global State.

VID: Add the corresponding VLAN ID of the Multicast VLAN. Users may enter a value between *2* and *4094.*

State: Use the drop-down menu to enable or disable the selected Multicast VLAN.

Member Ports: Enter a port or list of ports to be added to the Multicast VLAN. Member ports shall be the untagged members of the multicast VLAN.

Tagged Member Ports: Enter a port or list of ports that will become tagged members of the Multicast VLAN.

UnTagged Source Ports: Enter a port or list of ports that will become untagged members of the Multicast VLAN.

Source Port Dynamical Learn: Specify the source port dynamical learning to be enabled or disabled.

VLAN Name: Enter the name of the new Multicast VLAN to be created. This name can be up to *32* characters in length.

IPv4 Replace Source: This field is used to replace the source IPv4 address of incoming packets sent by the host before being forwarded to the source port.

IPv6 Replace Source IP: This field is used to replace the source IPv6 address of incoming packets sent by the host before being forwarded to the source port.

Source Ports: Enter a port or list of ports to be added to the Multicast VLAN. Source ports shall be the tagged members of the multicast VLAN.

Replace CVID: Specify the VID to be replaced in CVID. The range is from 1-4094.

Remap Priority: Specify the remap priority (0 to 7) to be associated with the data traffic to be forwarded on the multicast VLAN. Specify **None**, the packet's original priority is used. The default setting is None.

Click **Add** to add the ISM VLAN which will appear in the table, or click **Clear All** to clear all fields.

Click **Edit** button to modify the parameters and update the ISM VLAN Setting or click **Delete** to delete the ISM VLAN.

Click **View** to display the detail information of ISM VLAN.

Configuration > IGMP Snooping > Host Table

The Host Table page displays the information of Host Table. Including VLAN ID, Group, Port Number and Host IP.

Figure 4.90 - Configuration > IGMP Snooping > Host Table

Configuration > IGMP Snooping > IP Multicast Profile Settings

The IP Multicast Profile Settings page allows user to configure the IP Multicast Profile.

Figure 4.91 - Configuration > IGMP Snooping > IP Multicast Profile Settings

Profile ID: Specify the Profile ID.

Profile Name: Specify the Profile Name.

Click **Add** to create a new IP Multicast Profile or click **Delete All** to clear all the entries.

Configuration > IGMP Snooping > Limited Multicast Range Settings

The Limited Multicast Range Settings page allows user to configure the Limited Multicast. Specify the port range, select Access IP Type is *IPv4* or *IPv6* and select the Access is *Deny* or *Permit* then Click Apply to make the configurations take effect.

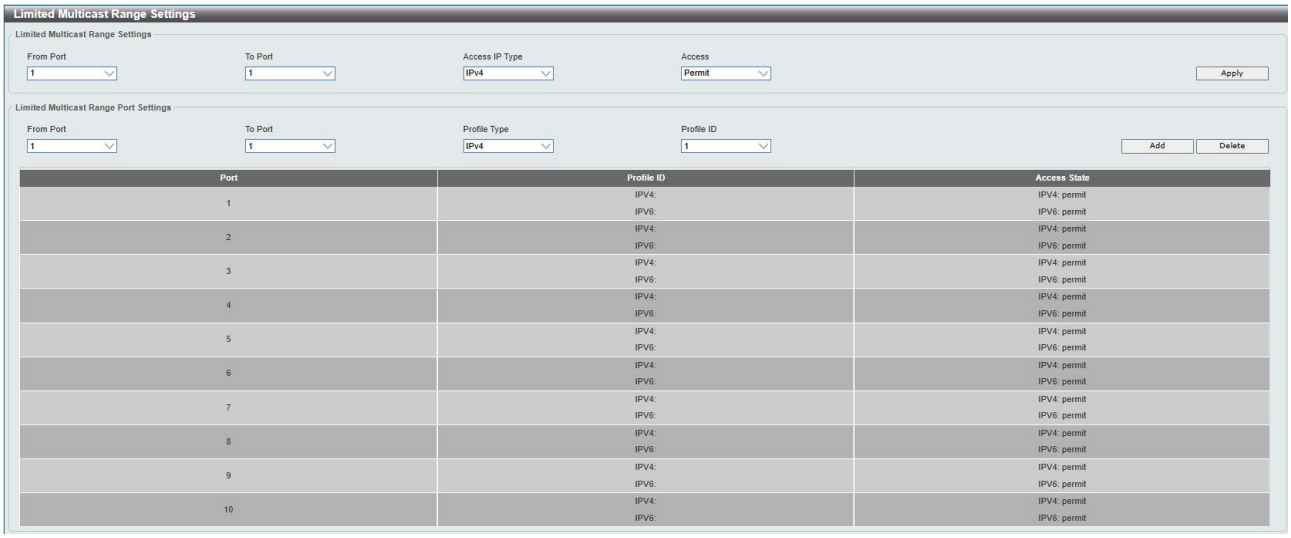


Figure 4.92- Configuration > IGMP Snooping > Limited Multicast Range Settings

From Port / To Port: Specify the port ranges to be configured.

Profile Type: Specify the profile type is IPv4 or IPv6.

Profile ID: Specify the Profile ID.

Click **Add** to create the Profile ID with specified ports or click **Delete** to remove the ports.

Configuration > IGMP Snooping > Max Multicast Group Settings

The Max Multicast Group Settings page allows user to configure the max multicast group for IGMP Snooping.

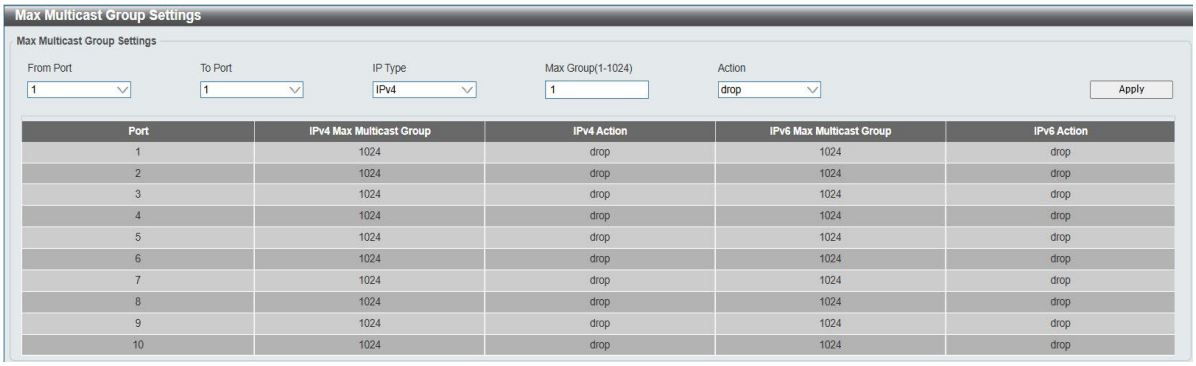


Figure 4.93- Configuration > IGMP Snooping > Max Multicast Group Settings

From Port / To Port: Specify the port ranges to be configured.

IP Type: Specify the IP type is IPv4 or IPv6.

Max Group (1-512): Specify the Max Group to be configured.

Action: Use the drop-down menu to select the appropriate action for this rule. The user can select **Drop** to initiate the drop action or the user can select **Replace** to initiate the replace action.

Click Apply to make the configurations take effect.

Configuration > IGMP Snooping > IGMP Snooping Static Group Settings

The IGMP Snooping Static Group Settings page allows the Switch to read the Multicast Group IP address and the corresponding MAC address from IGMP packets that pass through the Switch.

Figure 4.94- Configuration > IGMP Snooping > IGMP Snooping Static Group Settings

VLAN Name: Specifies the VLAN name of the multicast group.

VID List: Specifies the VID list or of the multicast group.

IPv4 Address: Specifies the IPv4 address.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Create** button to add a new entry based on the information entered.

Click the **Delete** button to remove the specific entry based on the information entered.

Click the **View All** button to display all the existing entries.

Click the **Edit** button to re-configure the specific entry.

After clicking the Edit button, the following page will appear:

Figure 4.95- Configuration > IGMP Snooping > IGMP Snooping Static Group Settings - Edit

Click the **Select All** button to select all the ports for configuration.

Click the **Clear All** button to unselect all the ports for configuration.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

Configuration > MLD Snooping > MLD Snooping Settings

The MLD Snooping Settings page allows user to configure the max multicast group for IGMP Snooping.

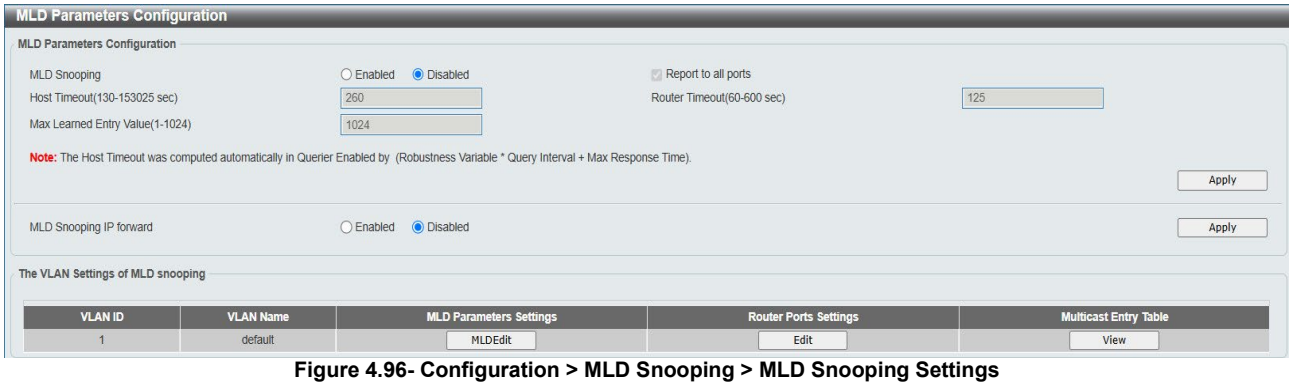


Figure 4.96- Configuration > MLD Snooping > MLD Snooping Settings

MLD Snooping: Enable or disable the MLD Snooping.

MLD Global Settings:

Host Timeout (130-153025 sec): Specifies the time interval in seconds after which a port is removed from a Multicast Group. Ports are removed if a Multicast group MLD report was not received from a Multicast port within the defined *Host Timeout* period. The possible field range is 130 - 153025 seconds. The default timeout is 260 seconds.

Router Timeout (60-600): Specifies the time interval in seconds the Multicast router waits to receive a message before it times out. The possible field range is 60 - 600 seconds. The default timeout is 125 seconds.

Max Learned Entry Value (1-1024): Specifies the max learned entry value for MLD Snooping. The field range is 1-1024. The default is 256.

Click **Apply** to make the configurations take effect. Press the **Edit** button under **Router Port Setting**, and select the ports to be assigned for MLD snooping for the VLAN, and press **Apply** for changes to take effect.

Configuration > MLD Snooping > MLD Host Table

The MLD Host Table page displays the MLD Snooping information.

Figure 4.97- Configuration > MLD Snooping > MLD Host Table

Configuration > Port Mirroring

Port Mirroring is a method of monitoring network traffic that forwards a copy of each incoming and/or outgoing packet from one port of the Switch to another port, where the packet can be studied. This enables network managers to better monitor network performances.

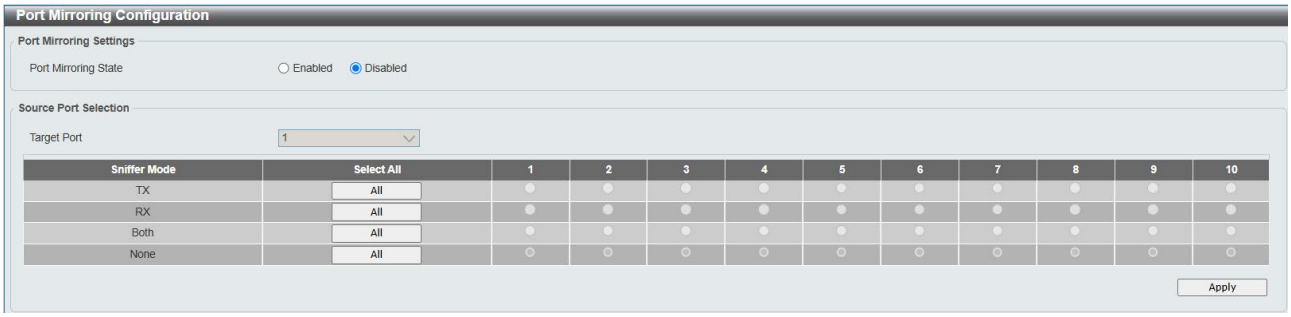


Figure 4.98 – Configuration > Port Mirroring

Port Mirroring: Enables or Disables the port mirroring feature.

Target Port: Specifies the target port.

Selection options for the Source Ports are as follows:

TX (transmit) mode: Duplicates the data transmitted from the source port and forwards it to the Target Port. Click “all” to include all ports into port mirroring.

RX (receive) mode: Duplicates the data that is received from the source port and forwards it to the Target Port. Click “all” to include all ports into port mirroring.

Both (TX and RX) mode: Duplicate both the data transmitted from and data sent to the source port, and forwards all the data to the assigned Target Port. Click “all” to include all ports into port mirroring.

None: Turns off the mirroring of the port. Click “all” to remove all ports from mirroring.

Click **Apply** to make the configurations take effect.

Configuration > RSPAN

The purpose of the RSPAN function is to mirror packets to a remote switch. A packet travels from the switch where the monitored packet is received, passing through the intermediate switch, and then to the switch where the sniffer is attached. The first switch is also named the source switch.

To make the RSPAN function work, the RSPAN VLAN source setting must be configured on the source switch. For the intermediate and the last switch, the RSPAN VLAN redirect setting must be configured.

Figure 4.99 – Configuration > RPSAN

The fields can be configured as described:

Parameter	Description
RSPAN State	Click the radio buttons to enable or disable the RSPAN feature.
VLAN Name	Create the RSPAN VLAN by VLAN name.

VID (1-4094)	Create the RSPAN VLAN by VLAN ID.

Click the **Apply** button to accept the changes made.
Click the **Add** button to add a new entry based on the information entered.
Click the **Modify** button to re-configure the specific entry.
Click the **Delete** button to remove the specific entry.

After clicking the **Modify** button, the following page will appear:

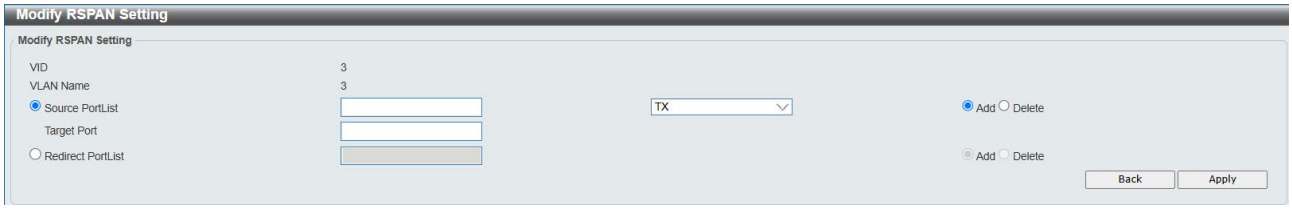


Figure 4.100 – Configuration > RPSAN > Modify RSPAN Setting

The fields can be configured as described

Parameter	Description
Source Ports	Select **RX, TX** or **Both** to specify in which direction the packets will be monitored. Click **Add** or **Delete** to add or delete source ports.
Target Ports	Specify the output port for the RSPAN VLAN packets. This configuration would also applied to “Port Mirroring” setting.
Redirect Port List	Specify the output port list for the RSPAN VLAN packets. If the redirect port is a Link Aggregation port, the Link Aggregation behavior will apply to the RSPAN packets. Click **Add** or **Delete** to add or delete redirect ports.

Click the **Apply** button to accept the changes made.
Click the **<<Back** button to discard the changes made and return to the previous page.

Configuration > Loopback Detection

The Loopback Detection function is used to detect the loop created by a specific port while Spanning Tree Protocol (STP) is not enabled in the network, especially when the down links are hubs or unmanaged switches. The Switch will automatically shut down the port and sends a log to the administrator. The Loopback Detection port will be unlocked when the Loopback Detection **Recover Time** times out. The Loopback Detection function can be implemented on a range of ports at the same time. User may enable or disable this function using the pull-down menu.

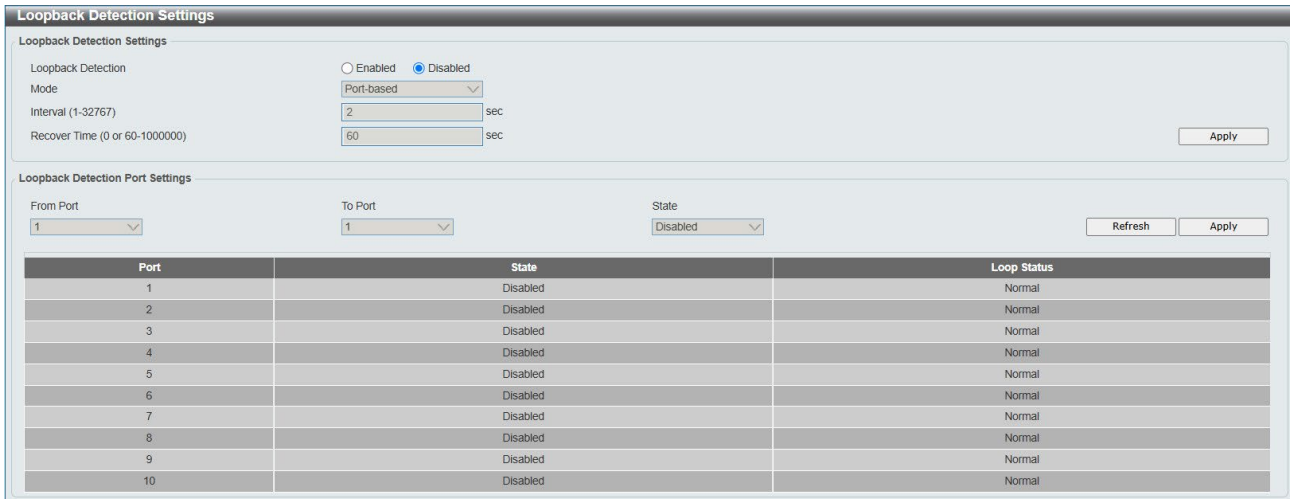


Figure 4.101 – Configuration > Loopback Detection

Loopback Detection State: Use the drop-down menu to enable or disable loopback detection. The default is *Disabled.*

Mode: Specify the Loopback Detection to be Port-based or VLAN-based.

Interval (1-32767): Set a Loop detection Interval between *1* and *32767* seconds. The default is 2 seconds.

Recover Time (0 or 60-1000000): Time allowed (in seconds) for recovery when a Loopback is detected. The Loop Detection Recover Time can be set at *0* seconds, or *60* to *1000000* seconds. Entering *0* will disable the Loop Detection Recover Time. The default is *60* seconds.

From Port: The beginning of a consecutive group of ports may be configured starting with the selected port.

To Port: The ending of a consecutive group of ports may be configured starting with the selected port.

State: Use the drop-down menu to toggle between *Enabled* and *Disabled.* Default is *Disabled*.

Click **Apply** to make the configurations take effect.

Configuration > SNTP Settings > Time Settings

SNTP or Simple Network Time Protocol is used by the Switch to synchronize the clock of the computer. The SNTP settings folders contain two windows: Time Settings and TimeZone Settings. Users can configure the time settings for the switch, and the following parameters can be set or are displayed in the Time Settings page.

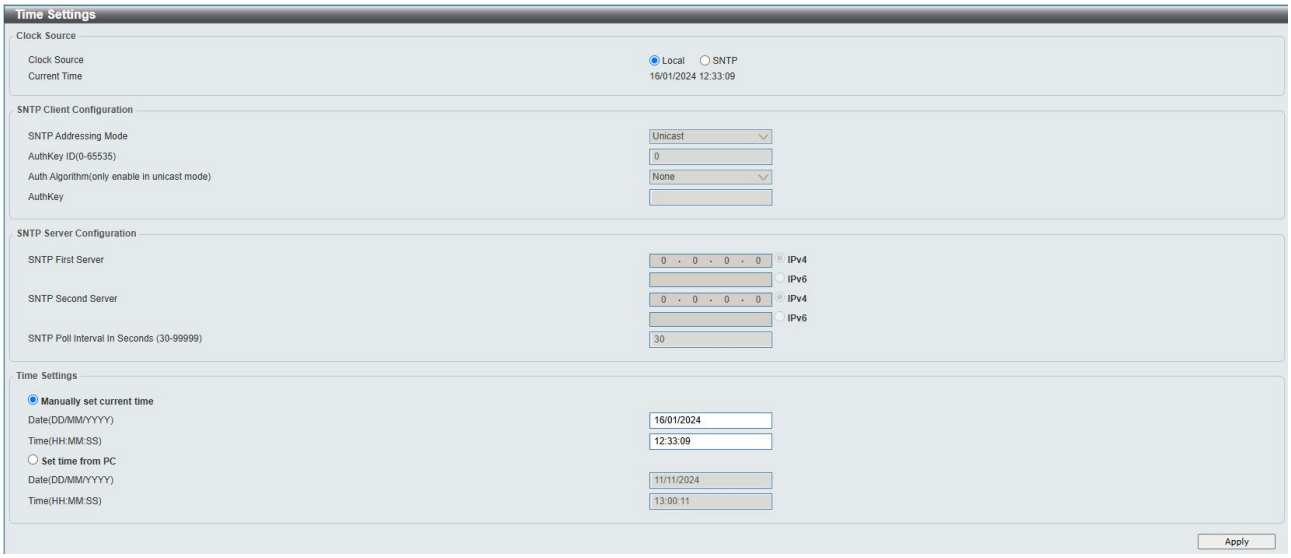


Figure 4.102 – Configuration > SNTP Settings > Time Settings

Clock Source: Specify the clock source by which the system time is set. The possible options are:

Local - Indicates that the system time is set locally by the device.

SNTP - Indicates that the system time is retrieved from a SNTP server.

SNTP Client Configuration:

SNTP Addressing Mode: Select the mode for transmitting SNTP packet. Selectable **Broadcast** and **Unicast**.

AuthKey Id (0-65535): Specify the ID used for authentication with SNTP server.

Auth Algorithm: Selectable option for **"MD5"** and **"None".**

AuthKey: Specified the key that used for authentication.

Current Time: Displays the current date and time for the switch.

If choosing **SNTP** for the clock source, then the following parameters will be available:

SNTP First Server: Select IPv4 or IPv6 and specify the IP address of the primary SNTP server from which the system time is retrieved.

SNTP Second Server: Select IPv4 or IPv6 and specify the IP address of the secondary SNTP server from which the system time is retrieved.

SNTP Poll Interval in Seconds (30-99999): Defines the interval (in seconds) at which the SNTP server is polled for Unicast information. The Poll Interval default is 30 seconds.

Click Apply to make the configurations take effect.

When selecting **Local** for the clock source, users can select from one of two options:

Manually set current time: Users input the system time manually.

Set time from PC: The system time will be synchronized from the local computer.

Configuration > SNTP Settings > TimeZone Settings

The TimeZone Setting Page is used to configure time zones and Daylight Savings time settings for SNTP.

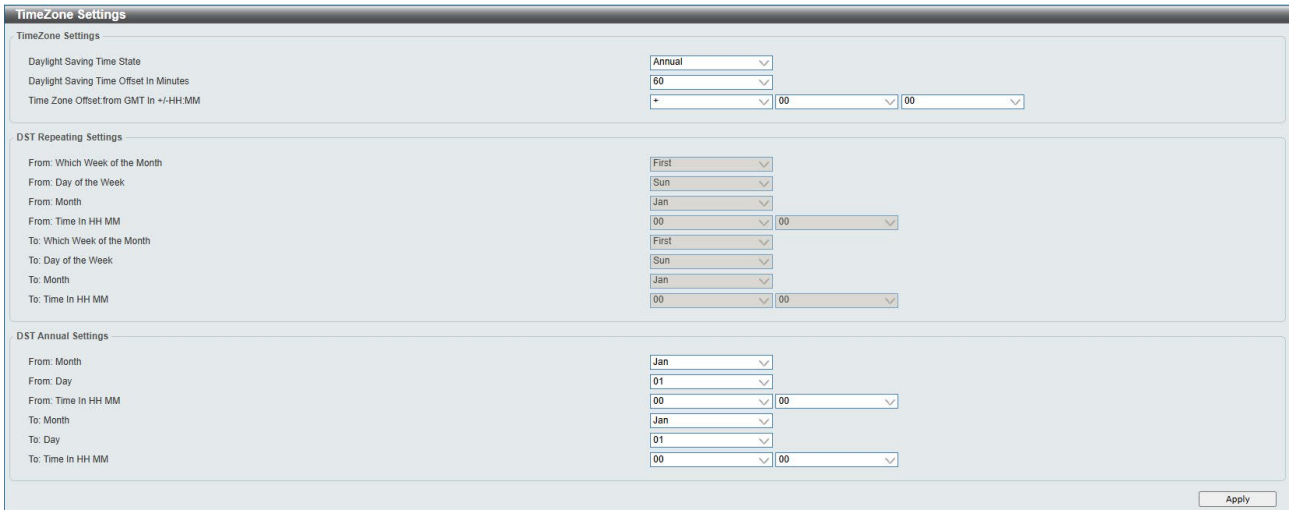


Figure 4.103 – Configuration > SNTP > TimeZone Settings

Daylight Saving Time State: Enable or disable the DST Settings.

Daylight Saving Time Offset: Use this drop-down menu to specify the amount of time that will constitute the local DST offset - *30*, *60*, *90*, or *120* minutes.

Time Zone Offset GMT +/- HH:MM: Use these drop-down menus to specify the local time zone's offset from Greenwich Mean Time (GMT.)

DST Repeating Settings:

From: Which Week of the Month: Enter the Week of Month will start on, each year.

From: Day of the Week: Enter the Day DST will start on, each year.

From: Month: Enter the month DST will start on, each year.

From: Time In HH:MM: Enter the time of day that DST will start on, each year.

To: Which Week of the Month: Enter the Week of Month will end on, each year.

To: Day of the Week: Enter the day of week that DST will end on, each year.

To: Month: Enter the month DST and date DST will end on, each year.

To: Time In HH:MM: Enter the time of day that DST will end on, each year.

DST Annual Settings:

From: Month / Day: Enter the month DST and date DST will start on, each year.

From: Time In HH:MM: Enter the time of day that DST will start on, each year.

To: Month / Day: Enter the month DST and date DST will end on, each year.

To: Time HH:MM: Enter the time of day that DST will end on, each year.

Click **Apply** to make the configurations take effect.

Configuration > DHCP/BOOTP Relay > DHCP/BOOTP Relay Global Settings

User can enable and configure DHCP/BOOTP Relay Global Settings on the Switch.

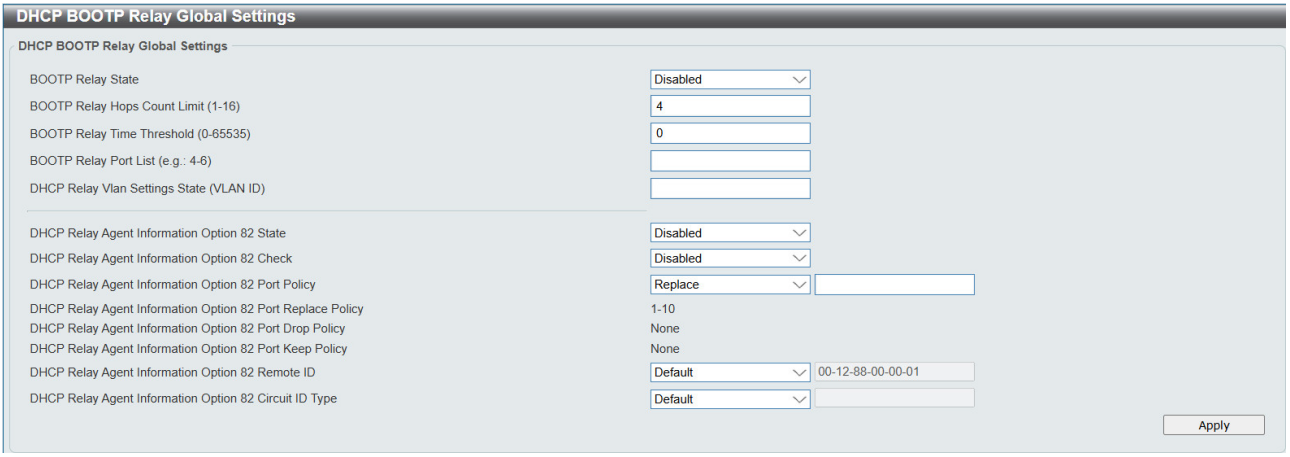


Figure 4.104 - Configuration > DHCP/BOOTP Relay > DHCP/BOOTP Relay Global Settings

Parameters	Descriptions
BOOTP Relay State	This field can be toggled between Enabled and Disabled using the pull-down menu. It is used to enable or disable the DHCP/BOOTP Relay service on the Switch. The default is *Disabled*.
BOOTP Relay Hops Count Limit (1-16)	This field allows an entry between *1* and *16* to define the maximum number of router hops DHCP/BOOTP messages can be forwarded across. The default hop count is 4.
BOOTP Relay Time Threshold (0-65535)	Allows an entry between *0* and *65535* seconds, and defines the maximum time limit for routing a DHCP/BOOTP packet. If a value of 0 is entered, the Switch will not process the value in the **seconds** field of the BOOTP or DHCP packet. If a non-zero value is entered, the Switch will use that value, along with the hop count to determine whether to forward a given BOOTP or DHCP packet.
BOOTP Relay Port List	Specify the ports for BOOTP relay.
DHCP Relay VLAN Setting State	Specify the VLAN ID to monitor DHCP client activity. The range is from 1 – 4094.
DHCP Relay Agent Information Option 82 State	It is used to enable or disable the DHCP Agent Information Option 82 on the Switch. The default is Disabled. **Enabled –** When this field is toggled to Enabled the relay agent will insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients. When the relay agent receives the DHCP request, it adds the option 82 information, and the IP address of the relay agent (if the relay agent is configured), to the packet. Once the option 82 information has been added to the packet it is sent on to the DHCP server. When the DHCP server receives the packet, if the server is capable of option 82, it can implement policies like restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option 82 field in the DHCP reply. The DHCP server unicasts reply to the back to the relay agent if the request was relayed to the server by the relay agent. The switch verifies that it originally inserted the option 82 data. Finally, the relay agent removes the option 82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request. **Disabled -** If the field is toggled to Disabled the relay agent will not

	insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients, and the check and policy settings will have no effect.
DHCP Relay Agent Information Option 82 Check	It filed is used to enable or disable the ability to check DHCP option 82 information in DHCP packets: Enabled – When the field is configured to Enabled, the relay agent checks if DHCP packets carries option 82 information. If option 82 does not carried, the DHCP packet would be dropped. Disabled – No check would be executed when check state configured to Disabled.
DHCP Relay Agent Information Option 82 Port Policy	This filed is used to configure the policy for each port. It is used to set the Switches policy for handling packets when the **DHCP Agent Information Option 82 Check** is set to Disabled. There are 3 policies available to use: **Replace** - The option 82 field will be replaced if the option 82 field already exists in the packet received from the DHCP client. **Drop** - The packet will be dropped if the option 82 field already exists in the packet received from the DHCP client. **Keep** -The option 82 field will be retained if the option 82 field already exists in the packet received from the DHCP client.
DHCP Relay Agent Information Option 82 Remote ID	This filed is used to configure the contents of Remote ID used in option 82. Options: **Default**, **User Define**, **vendor3**, **vendor7** and **vendor8** are available to use.
DHCP Relay Agent Information Option 82 Circuit ID Type	This field is used to configure the contents of Circuit ID used in option 82. Option: **Default**, **User Defined**, **User Defined Hex**, **vendor1**, **vendor2**, **vendor3**, **vendor4**, **vendor5**, **vendor6**, **vendor7** and **vendor8** are available to use.

Click **Apply** to apply the configurations.

NOTE: If the Switch receives a packet that contains the option-82 field from a DHCP client and the information-checking feature is enabled, the switch drops the packet because it is invalid. However, in some instances, user might configure a client with the option-82 field. In this situation, user should disable the information-check feature so that the switch does not remove the option-82 field from the packet. User can configure the action that the switch takes when it receives a packet with existing option-82 information by configuring the **DHCP Agent Information Option 82 Policy**.

Configuration > DHCP/BOOTP Relay > DHCP/BOOTP Relay Interface Settings

This page allows the user to set up a server, by IP address, for relaying DHCP/BOOTP information the switch. The user may enter a previously configured IP interface on the Switch that will be connected directly to the DHCP/BOOTP server using the following window. Properly configured settings will be displayed in the **BOOTP Relay Table** at the bottom of the following window, once the user clicks the **Add** button under the **Apply** heading. The user may add up to four server IPs per IP interface on the Switch. Entries may be deleted by clicking Delete button.

Figure 4.105 - Configuration > DHCP/BOOTP Relay > DHCP/BOOTP Relay Interface Settings

Interface: The IP interface on the Switch that will be connected directly to the Server.

Server IP: Enter the IP address of the DHCP/BOOTP server. Up to four server IPs can be configured per IP Interface.

Click **Apply** to make the configurations take effect.

Configuration > DHCP/BOOTP Relay > DHCP Relay Option82 Profile Setting

This window is used to display and configure the DHCP relay remote ID profile settings. This is used to create a new profile for DHCP relay Option 82.

Figure 4.106 - Configuration > DHCP/BOOTP Relay > DHCP Relay Option82 Profile Setting

Profile Name: Enter the profile name here. This string can be up to 32 characters long.

Profile: Enter the profile here. This string can be up to 64 characters long.

Click **Add** to make the configurations take effect.

Configuration > DHCP Local Relay Settings

The DHCP Local Relay Settings page allows the user to configure DHCP Local Relay. DHCP broadcasts are trapped by the switch CPU, and replacement broadcasts are forwarded with Option 82. Replies from the DHCP servers are trapped by the switch CPU, the Option 82 is removed and the reply is sent to the DHCP Client.

Figure 4.107 - Configuration > DHCP Local Relay Settings

DHCP/BOOTP Local Relay Status: Specifies whether DHCP Local Relay is enabled on the device.

Enabled – Enables DHCP Local Relay on the device.

Disabled – Disables DHCP Local Relay on the device. This is the default value.

DHCP/BOOTP Local Relay Port List: Specifies the port or ports for DHCP/BOOTP local relay port.

Config VLAN by: Configure the VLAN by VID or VLAN Name of drop-down menu.

State: Specifies whether DHCP Local Relay is enabled on the VLAN.

Enabled – Enables DHCP Local Relay on the VLAN.

Disabled – Disables DHCP Local Relay on the VLAN.

DHCP Local Relay VID List: Displays the list of VLANs on which DHCP Local Relay has been defined.

Click **Apply** to make the configurations take effect.

Configuration > DHCPv6 Relay Settings

The DHCPv6 Relay Settings page allows user to configure the DHCPv6 settings.

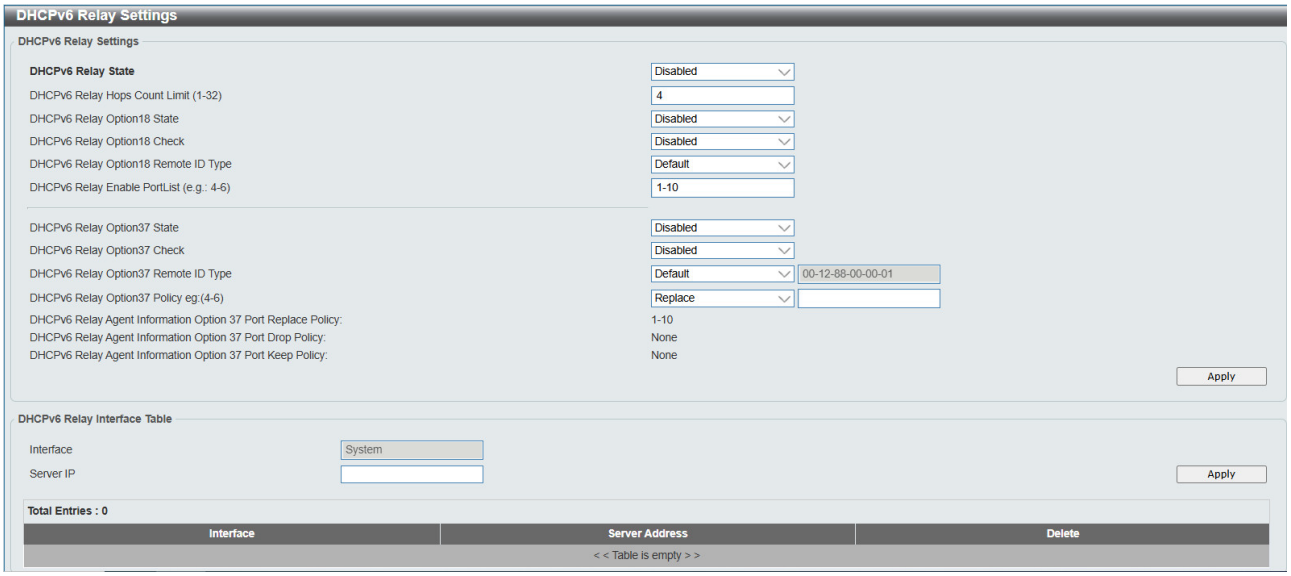


Figure 4.108 - Configuration > DHCPv6 Relay Settings

DHCPv6 Relay Status: Specifies whether DHCPv6 Relay is enabled on the device.

Enabled – Enables DHCPv6 Relay on the device.

Disabled – Disables DHCPv6 Relay on the device. This is the default value.

DHCPv6 Relay Hops Count Limit (1-32): The field allows and entry between 1 and 32 to define the maximum number of router hops DHCPv6 messages can be forwarded. The default hop count is 4.

DHCPv6 Relay Option18 State: Specifies the DHCPv6 Relay Option18 State to be enabled or disabled.

DHCPv6 Relay Option18 Check: Specifies the DHCPv6 Relay Option18 Check to be enabled or disabled.

DHCPv6 Relay Option18 Remote ID Type: Specifies the DHCPv6 Relay Option18 Remote ID type is **CID with User Defined**, **User Defined** or **VENDOR1**.

DHCPv6 Relay Option37 State: Specifies the DHCPv6 Relay Option37 State to be enabled or disabled.

DHCPv6 Relay Option37 Check: Specifies the DHCPv6 Relay Option37 Check to be enabled or disabled.

DHCPv6 Relay Option37 Remote ID Type: Specifies the DHCPv6 Relay Option37 Remote ID type is **CID with User Defined**, **User Defined** or **Default**.

Interface: Enter a name of the interface.

Server IP: Enter the server IP address.

Click **Apply** to make the configurations take effect.

Configuration > DHCPv6 Relay Option38 Settings

The DHCPv6 Relay Option38 Settings page allows user to configure the DHCPv6 relay option38 settings.

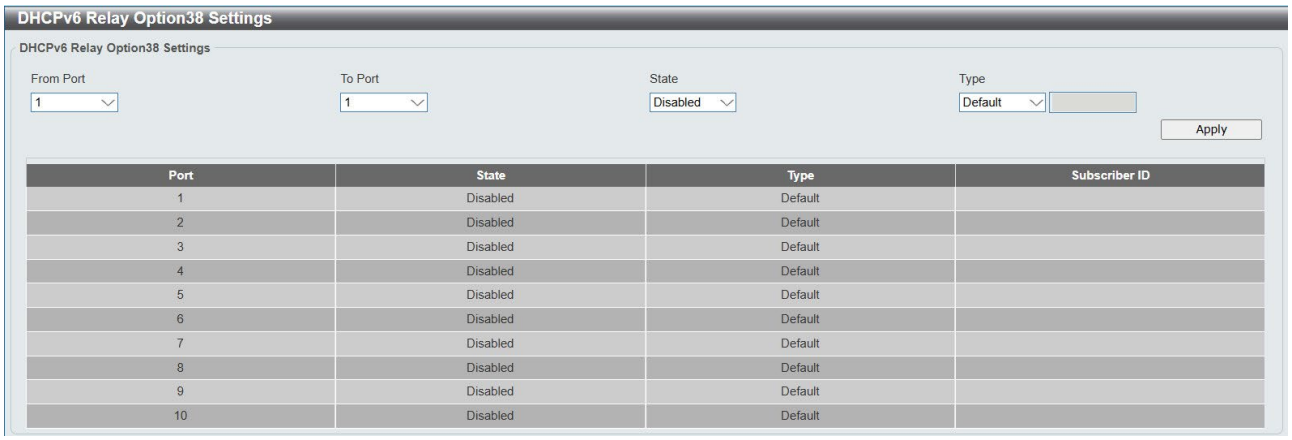


Figure 4.109 - Configuration > DHCPv6 Relay Option38 Settings

DHCPv6 Relay Option38 Port Index: Specify the port range to be configured.

DHCPv6 Relay Option38 Port State: Specify the port state of DHCPv6 relay option38 to be enabled or disabled.

DHCPv6 Relay Option38 Port Type: Specify the port type of DHCPv6 relay option38 to be enabled or disabled.

Click **Apply** to make the configurations take effect.

Configuration > DNS > DNS Settings

The Domain Name System (DNS) is used to map names to IP addresses throughout the Internet and has been adapted for use within intranets. For two DNS servers to communicate across different subnets, the DNS Relay of the Switch must be used. The DNS servers are identified by IP addresses.

Figure 4.110 - Configuration > DNS > DNS Settings

DnsQueryRetryCount (1-10): Specify the retry times to query DNS server.

DnsQueryTimeOut (1-100): Specify the timeout range for DNS query. Range from 1 second to 100 seconds.

DnsResolverMode: Specify the DNS resolver (switch) mode:

simultaneously: DNS query transmitting in simultaneously.

sequential: DNS query transmitting in sequence.

DnsPreferentialType: Select IPv4 or IPv6 mode.

DnsCacheTTL (60-3600): The time DNS entry cached in switch. Range from 60 seconds to 3600 seconds.

Click **Apply** to make the configurations take effect.

Configuration > DNS > DNS Server Table

The DNS Server Table is used to configure DNS server on switch.

Figure 4.111 - Configuration > DNS > DNS Server Table

Enter **IPv4** or **IPv6** address for DNS server.

Click **Apply** to make the configurations take effect.

Configuration > DNS > DNS Doman Table

The DNS Server Table is used to configure DNS domain name on switch.

Figure 4.112 - Configuration > DNS > DNS Domain Table

Enter **the Domain Name** for DNS resolver.

Click **Add** to add the entry.

Configuration > DNS > DNS Cache Table

The DNS Server Table is user to display current DNS cache on switch.

Figure 4.113 - Configuration > DNS > DNS Cache Table

Display current DNS query result.

Includes **DomaninName**, **NameServer**, **TTL** and **AnswerIP**.

Configuration > Spanning Tree > STP Bridge Global Settings

The Switch implements three versions of the Spanning Tree Protocol, the Rapid Spanning Tree Protocol (RSTP) as defined by the IEEE 802.1w specification and a version compatible with the IEEE 802.1D STP and Multiple Spanning Tree Protocol (MSTP) as defined by the IEEE802.1 specification. RSTP can operate with legacy equipment implementing IEEE 802.1D, however the advantages of using RSTP will be lost.

The IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1D STP standard. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent switching innovations. The basic function and much of the terminology is the same as STP. Most of the settings configured for STP are also used for RSTP. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

The IEEE 802.1 Multiple Spanning Tree (MSTP) provides various load balancing scenarios by allowing multiple VLANs to be mapped to a single spanning tree instance, providing multiple pathways across the network. For example, while port A is blocked in one STP instance, the same port can be placed in the Forwarding state in another STP instance.

By default, Rapid Spanning Tree is disabled. If enabled, the Switch will listen for BPDU packets and its accompanying Hello packet. BPDU packets are sent even if a BPDU packet was not received. Therefore, each link between bridges is sensitive to the status of the link. Ultimately this difference results in faster detection of failed links, and thus faster topology adjustment.

By default Multiple Spanning Tree is enabled. It will tag BPDU packets to receiving devices and distinguish spanning tree instances, spanning tree regions and the VLANs associated with them.

After enabling STP, setting the STP Global Setting includes the following options:

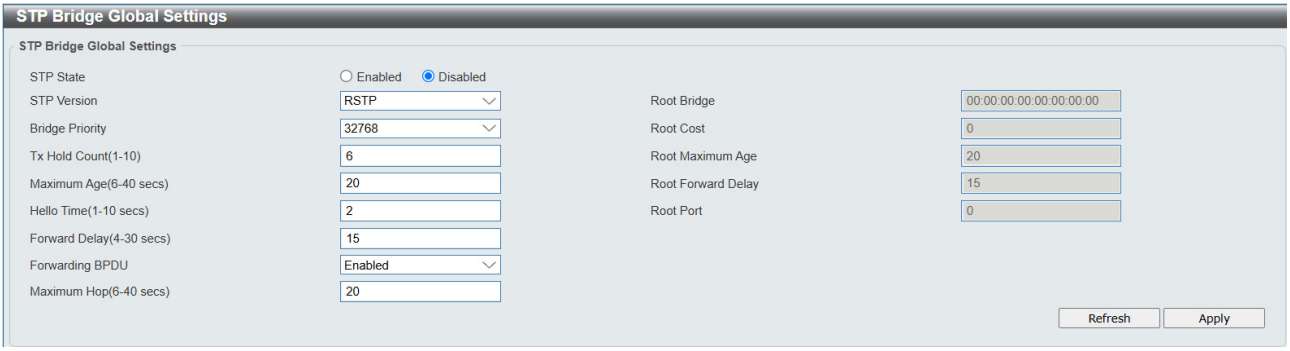


Figure 4.114 - Configuration > Spanning Tree > STP Bridge Global Settings

STP State: Specify the Spanning Tree Protocol to be Enabled or Disabled.

STP Version: Choose MSTP, RSTP or STP Compatible. The default setting is MSTP.

Bridge Priority: This value between 0 and 61410 specifies the priority for forwarding packets: the lower the value, the higher the priority. The default is *32768*.

TX Hold Count (1-10): Used to set the maximum number of Hello packets transmitted per interval. The count can be specified from *1* to *10*. The default is *6.*

Maximum Age (6-40 sec): This value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. If the value ages out and a BPDU has still not been received from the Root Bridge, the Switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that the Switch has the lowest Bridge Identifier, it will become the Root Bridge. A time interval may be chosen between *6* and *40* seconds. The default value is *20*. (Max Age has to have a value bigger than Hello Time)

Hello Time (1-10 sec): The user may set the time interval between transmissions of configuration messages by the root device, thus stating that the Switch is still functioning. The default is *2* seconds.

Forward Delay (4-30 sec): This sets the maximum amount of time that the root device will wait before changing states. The default is *15* seconds.

Forwarding BPDU: Bridges use Bridge Protocol Data Units (BPDU) to provide spanning tree information. STP BPDUs filtering is useful when a bridge interconnects two regions; each region needing a separate spanning tree. BPDU filtering functions only when STP is disabled either globally or on a single interface.

Enabled - BPDU filtering is enabled on the port.

Disabled - BPDU forwarding is enabled on the port (if STP is disabled).

Maximum Hop (6-40 secs): Specifies the number of hops between devices in a spanning tree region before the BPDU (bridge protocol data unit) packet sent by the Switch will be discarded. Each switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BPDU packet and the information held for the port will age out. The user may set a hop count from 6 to 40. The default is 20.

Root Bridge: Displays the MAC address of the Root Bridge.

Root Cost: Defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is *0* (auto).

Root Maximum Age: Displays the Maximum Age of the Root Bridge. The default is 20.

Root Forward Delay: Displays the Forward Delay of the Root Bridge. The default is 15.

Root port: Displays the root port.

Click **Apply** for the settings to take effect. Click **Refresh** to renew the page.

Configuration > Spanning Tree > STP Port Settings

STP can be set up on a port per port basis. In addition to setting Spanning Tree parameters for use on the switch level, the Switch allows for the configuration of the groups of ports, each port-group of which will have its own spanning tree, and will require some of its own configuration settings.

An STP Group spanning tree works in the same way as the switch-level spanning tree, but the root bridge concept is replaced with a root port concept. A root port is a port of the group that is elected based on port priority and port cost, to be the connection to the network for the group. Redundant links will be blocked, just as redundant links are blocked on the switch level.

The STP on the switch level blocks redundant links between switches (and similar network devices). The port level STP will block redundant links within an STP Group.

It is advisable to define an STP Group to correspond to a VLAN group of ports.

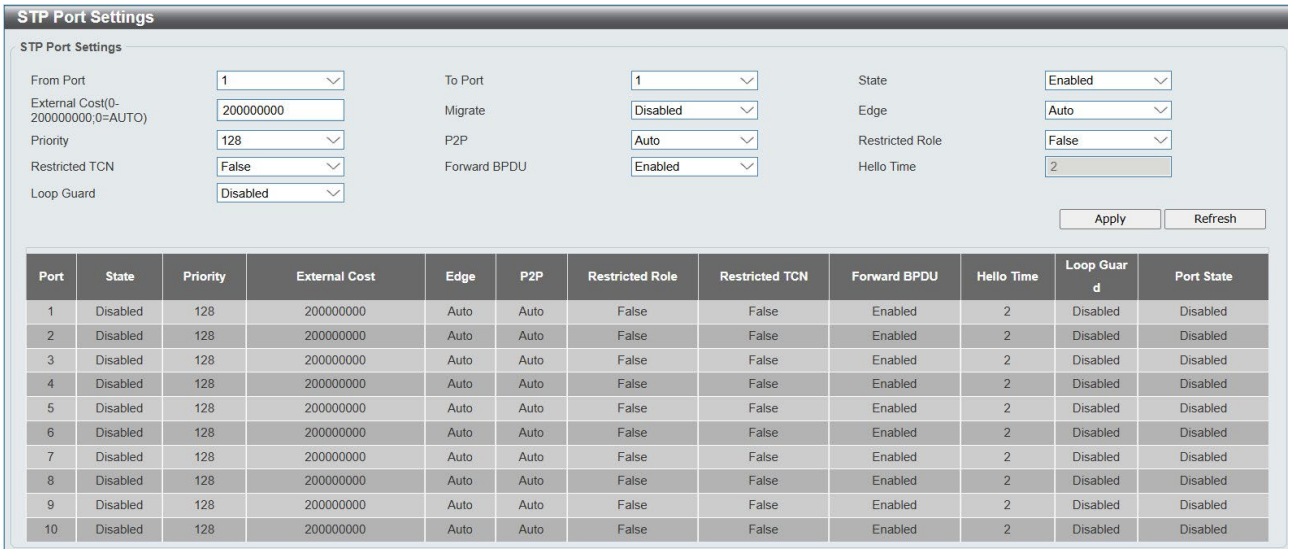


Figure 4.115 – Configuration > Spanning Tree > STP Port Settings

From Port/To Port: A consecutive group of ports may be configured starting with the selected port.

State: Use the drop-down menu to enable or disable STP by per-port based. It will be selectable after the global STP is enabled.

External Cost: This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. Thedefault value is *0* (auto).

0 (auto) - Setting 0 for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = 200000. Gigabit port = 20000.

Value 1-200000000 - Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets.

Migrate: Setting this parameter as *Yes* will set the ports to send out BPDU packets to other bridges, requesting information on their STP setting. If the Switch is configured for RSTP, the port will be capable to migrate from 802.1d STP to 802.1w RSTP. Migration should be set as yes on ports connected to network stations or segments that are capable of being upgraded to 802.1w RSTP on all or some portion of the segment.

Edge: Selecting the *True* parameter designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received, it automatically loses edge port status. Selecting the *False* parameter indicates that the port does not have edge port status. Selecting the *Auto* parameter indicates that the port have edge port status or not have edge port status automatically.

Priority: Specify the priority of each port. Selectable range is from 0 to 240, and the default setting is 128. The lower the number, the greater the probability the port will be chosen as a root port.

P2P: Choosing the *True* parameter indicates a point-to-point (P2P) shared link. P2P ports are similar to edge ports, however they are restricted in that a P2P port must operate in full-duplex.

Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A p2p value of *false* indicates that the port cannot have p2p status. *Auto* allows the port to have p2p status whenever possible and operate as if the p2p status were true. If the port cannot maintain this status, (for example if the port is forced to half-duplex operation) the p2p status changes to operate as if the p2p value were *False*. The default setting for this parameter is *Auto*.

Restricted Role: Toggle between *True* and *False* to set the restricted role state of the packet. If set to *True*, the port will never be selected to be the Root port. The default value is *False*.

Restricted TCN: Toggle between *True* and *False* to set the restricted TCN of the packet. Topology Change Notification (TCN) is a BPDU that a bridge sends out to its root port to signal a topology change. If set to *True*, it stops the port from propagating received TCN and to other ports. The default value is *False*.

Forwarding BPDU: Bridges use Bridge Protocol Data Units (BPDU) to provide spanning tree information. STP BPDUs filtering is useful when a bridge interconnects two regions; each region needing a separate spanning tree. BPDU filtering functions only when STP is disabled either globally or on a single interface. The possible field values are:

Disabled – BPDU filtering is enabled on the port.

Enabled – BPDU forwarding is enabled on the port (if STP is disabled).

Hello Time: The interval between two transmissions of BPDU packets sent by the Root Bridge to indicate to all other switches that it is indeed the Root Bridge. The default value is 2.

Click **Apply** to make the configurations take effect.

Click **Refresh** to renew the page.

Configuration > Spanning Tree > MST Configuration Identification

The MST Configuration Identification page allows user to configure a MSTI instance on the switch. These settings will uniquely identify a multiple spanning tree instance set on the switch. The Switch initially possesses one CIST or Common Internal Spanning Tree of which the user may modify the parameters for but cannot change the MSTI ID for, and cannot be deleted.

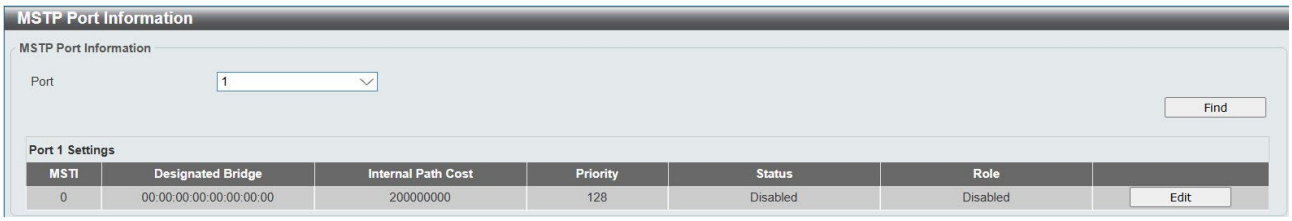


Figure 4.116 - Configuration > Spanning Tree > MST Configuration Identification

MST Configuration Identification Settings:

Configuration Name: A previously configured name set on the Switch to uniquely identify the MSTI (Multiple Spanning Tree Instance). If a configuration name is not set, this field will show the MAC address to the device running MSTP. This field can be set in the **STP Bridge Global Set-tings** window.

Revision Level: This value, along with the Configuration Name will identify the MSTP region configured on the Switch. The user may choose a value between *0* and *65535* with a default setting of *0*.

MSTI ID (1-15): Enter a number between *1* and *15* to set a new MSTI on the Switch.

Type: This field allows the user to choose a desired method for altering the MSTI settings.

Add VID - Select this parameter to add VIDs to the MSTI ID, in conjunction with the VID List parameter.

Remote VID – Select this parameter to remove VIDs from the MSTI ID, in con-junction with the VID List parameter.

VID List (1-4094): This field displays the VLAN IDs associated with the specific MSTI.

Click **Apply** to make the configurations take effect.

Configuration > Spanning Tree > STP Instance Settings

The STP Instance Settings page display MSTIs currently set on the Switch and allows users to change the Priority of the MSTPs.

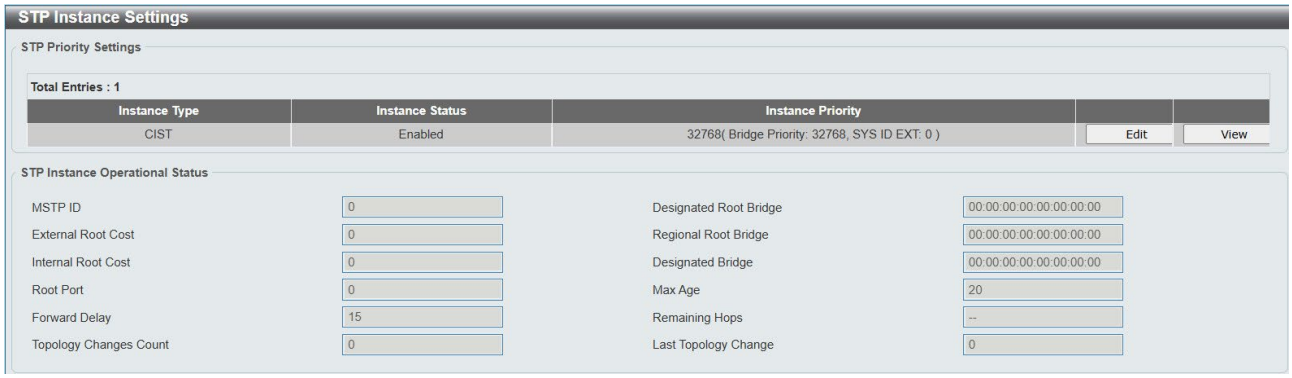


Figure 4.117 - Configuration > Spanning Tree > STP Instance Settings

To modify an entry on the table, click the **Edit** button. To view more information about and entry on the table at the top of the window, click the **view** button.

The window above contains the following information:

MSTI ID: Enter the MSTI ID in this field. An entry of *0* denotes the CIST (default MSTI).

Priority: Enter the new priority in the Priority field. The user may set a priority value between *0-61440*.

Click **Apply** to implement the new priority setting.

Configuration > Spanning Tree > MSTP Port Information

The MSTP Port Information page can be used to update the port configuration for an MSTI ID. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for interfaces to be selected for forwarding first. In instances where the priority value is identical, the MSTP function will implement the lowest MAC address into the forwarding state and other interfaces will be blocked.

To View the MSTI settings for a particular port, select the Port number and click **Find** button. To modify the settings for a particular MSTI Instance, click **Edit** button, then modify the MSTP Port Setting and click **Apply**.

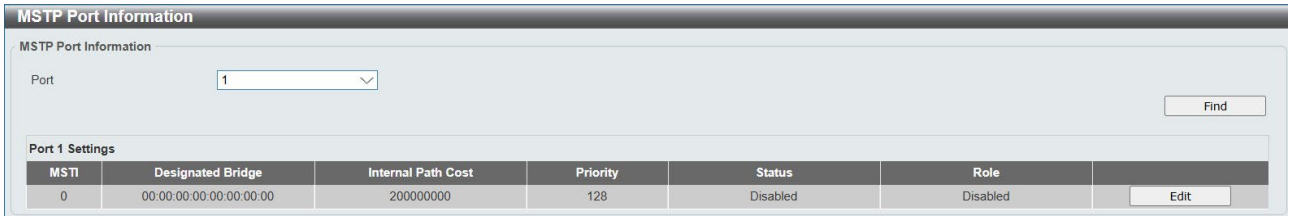


Figure 4.118 - Configuration > Spanning Tree > MST Port Information

MSTI: Displays the MSTI ID of the instance being configured. An entry of *0* in this field denotes the CIST (default MSTI).

Internal Path Cost (0=Auto): This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within a STP instance. The default setting is *0* (auto).

0 (Auto) - Selecting this parameter for the internal Cost will set quickest route automatically and optimally for an interface. The default value is derived from the media speed of the interface.

Value 0-2000000 - Selecting this parameter with a value in the range of *0* to *2000000* will set the quickest route then a loop occurs. A lower internal cost represents a quicker transmission.

Priority: Enter a value between *0* and *240* to set the priority for the port interface. A higher priority will designate the interface to forward packets first. A lower number denotes a higher priority.

Configuration > Ethernet OAM > Ethernet OAM Port Settings

The Ethernet OAM Port Settings page allows user to configure the Ethernet OAM settings.

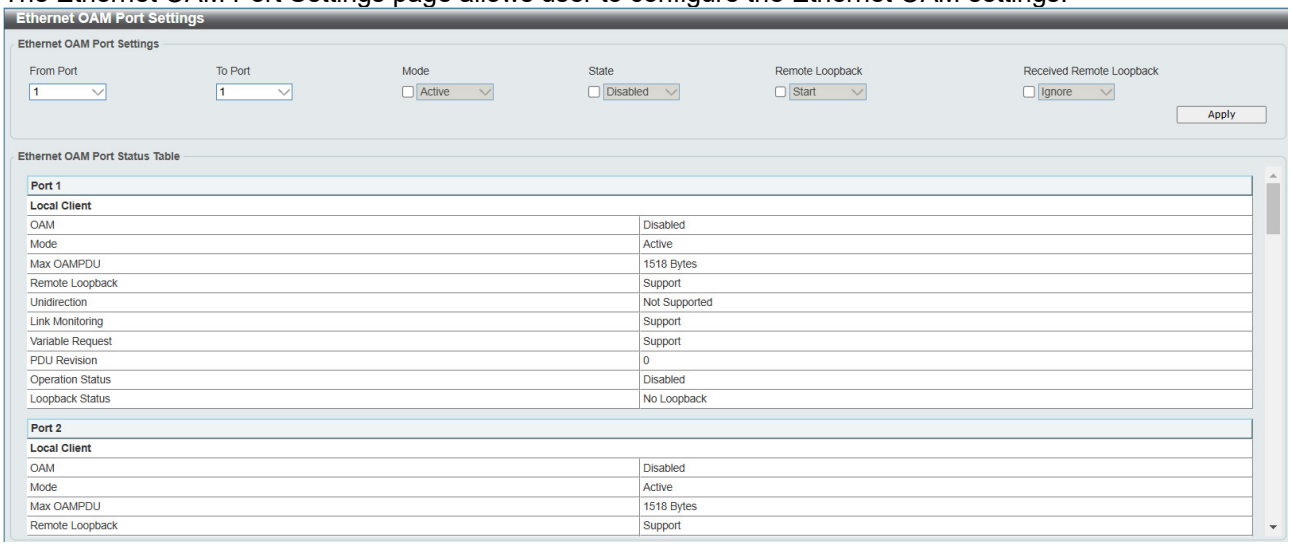


Figure 4.119 - Configuration > Ethernet OAM > Ethernet OAM Port Settings

From Port/To Port: Select a range of ports to be configured.

Mode: Use the drop-down menu to select to operate in either **Active** or **Passive**. The default mode is **Active**.

State: Use the drop-down menu to enable or disable the OAM function.

Remote Loopback: Specifies the Ethernet OAM remote loopback is None or Start.

None – Select to disable the remote loopback.

Start – Select to request the peer to change to the remote loopback mode.

Received Remote Loopback: To configure the client to process or to ignore the received Ethernet OAM remote loopback command.

Process – Select to process the received Ethernet OAM remote loopback command.

Ignore – Select to ignore the received Ethernet OAM remote loopback command.

Click **Apply** to make the configurations take effect.

Configuration > Ethernet OAM > Ethernet OAM Event Configuration

The Ethernet OAM Event Configuration page allows user to configure the Ethernet OAM configuration settings.

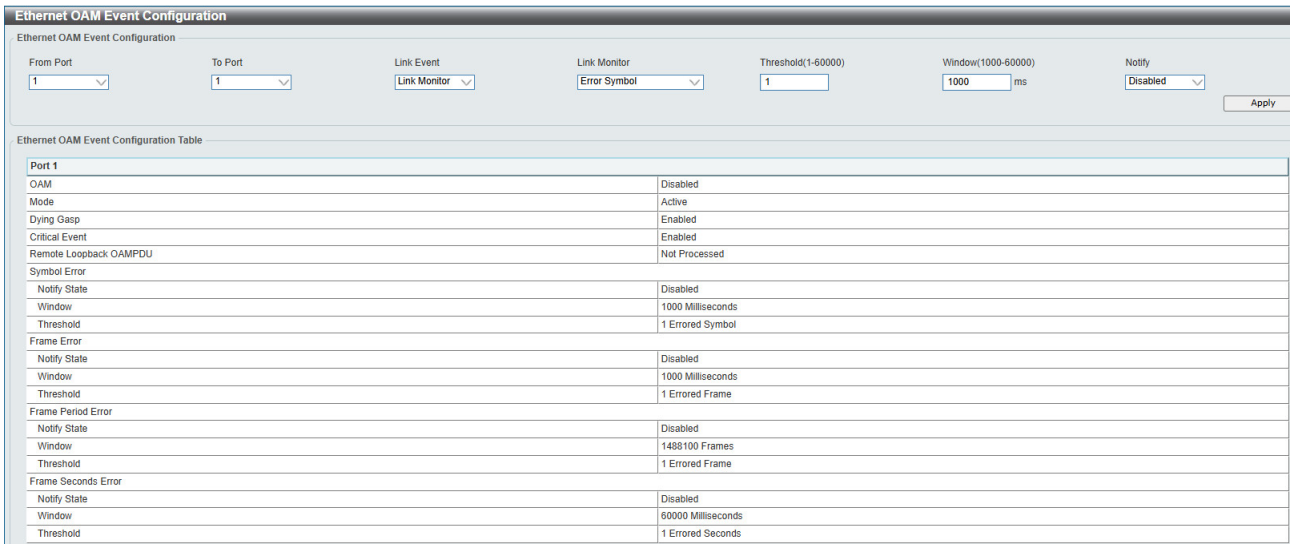


Figure 4.120 - Configuration > Ethernet OAM > Ethernet OAM Event Configuration

From Port / To Port: Select a range of ports to be configured.

Link Event: Select the link event, **Link Monitor** or **Critical Link Event.**

Link Monitor: Select the link monitor. Available options are **Error Symbol, Error Frame, Error Frame Period,** and **Error Frame Seconds.**

Threshold (0-4294967295): Enter the number of error frame or symbol in the period is required to be equal to or greater than in order for the event to be generated.

Window (1000-60000): Enter the period of error frame or symbol in milliseconds summary event.

Notify: Select the notification to be enabled or disabled.

Click the **Apply** button to accept the changes made.

Configuration > DDM > DDM Settings

The Digital Diagnostic Monitoring (DDM) functions allow the user to view the digital diagnostic monitoring status of SFP modules inserting to the Switch and to configure related settings.

The DDM Settings page allows user to configure the action that will occur for specific ports when an exceeding alarm threshold or warning threshold event is encountered.

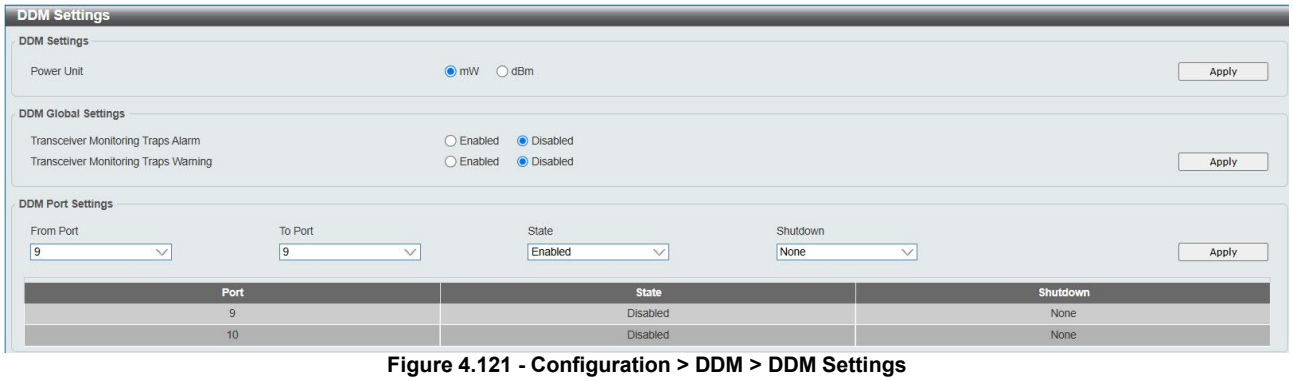


Figure 4.121 - Configuration > DDM > DDM Settings

Power Unit: Specifies the power unit for DDM. The options are mW (milliwatts) and dBm (decibel-milliwatts).

From Port / To Port: Specifies a port or range of ports to be configured.

State: Specifies to enable or disable the DDM settings state.

Shutdown: Specifies whether or not to shutdown the port, when the operating parameter exceeds the Alarm or Warning threshold.

Click the **Apply** button to accept the changes made.

Configuration > DDM > DDM Temperature Settings

The DDM Temperature Threshold Settings page allows user to configure the DDM temperature threshold for specific ports on the Switch.

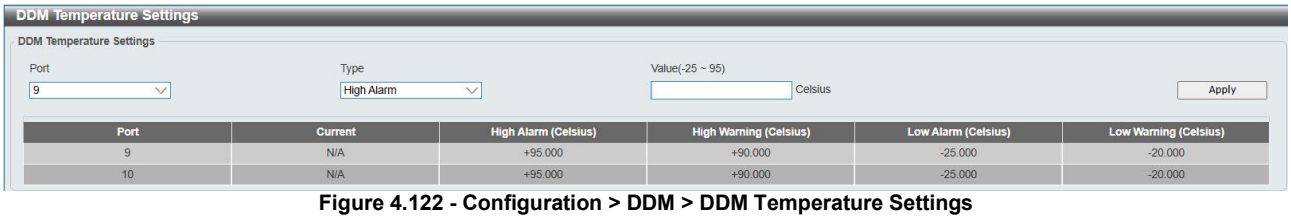


Figure 4.122 - Configuration > DDM > DDM Temperature Settings

Port: Specifies the port to be configured.

Type: Specifies the type for the operating parameter, the options are High Alarm, Low Alarm, High Warning and Low Warning.

High Alarm: Specifies the high threshold for the alarm. When the operating temperature rises above the configured value, the action associated with the alarm is taken.

Low Alarm: Specifies the low threshold for the alarm. When the operating temperature falls below the configured value, the action associated with the alarm is taken.

High Warning: Specifies the high threshold for the warning. When the operating temperature rises above the configured value, the action associated with the warning is taken.

Low Warning: Specifies the low threshold for the warning. When the operating temperature falls below the configured value, the action associated with the warning is taken.

Vaule (-128 – 127.996): Specifies the value for the specified type of port.

Click **Apply** to make the configurations take effect.

Configuration > DDM > DDM Voltage Settings

The DDM Voltage Settings Threshold Settings page is used to configure the DDM voltage threshold for specific ports on the Switch.

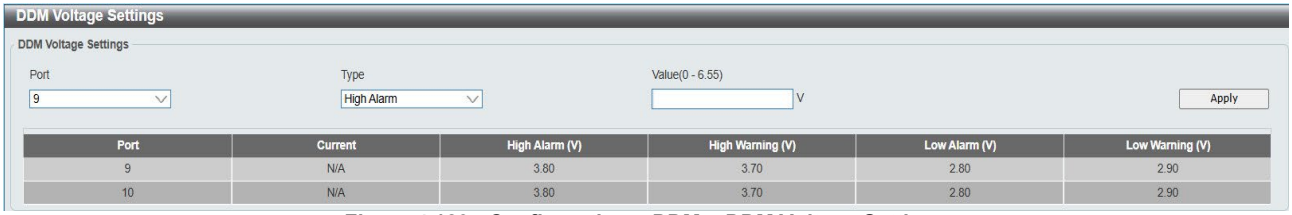


Figure 4.123 - Configuration > DDM > DDM Voltage Settings

Port: Specifies the port to be configured.

Type: Specifies the type for the operating parameter, the options are High Alarm, Low Alarm, High Warning and Low Warning.

High Alarm: Specifies the high threshold for the alarm. When the operating Voltage rises above the configured value, the action associated with the alarm is taken.

Low Alarm: Specifies the low threshold for the alarm. When the operating Voltage falls below the configured value, the action associated with the alarm is taken.

High Warning: Specifies the high threshold for the warning. When the operating Voltage rises above the configured value, the action associated with the warning is taken.

Low Warning: Specifies the low threshold for the warning. When the operating Voltage falls below the configured value, the action associated with the warning is taken.

Vaule (0 – 6.55): Specifies the value for the specified type of port.

Click the **Apply** button to accept the changes made.

Configuration > DDM > DDM Bias Current Settings

The DDM Bias Current Threshold Settings page is used to configure the DDM Bias current threshold for specific ports on the Switch.

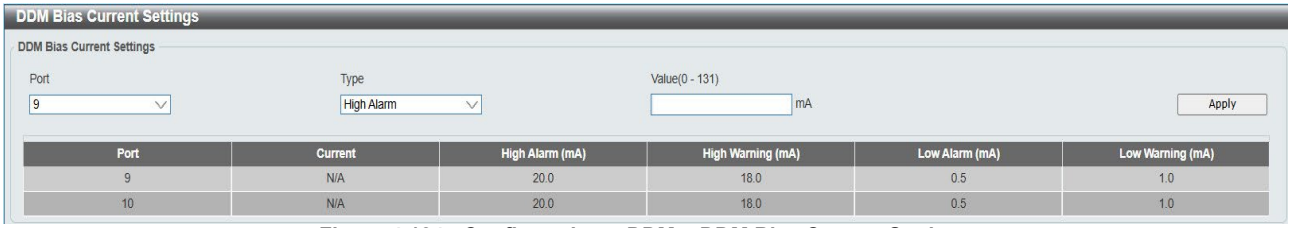


Figure 4.124 - Configuration > DDM > DDM Bias Current Settings

Port: Specifies the port to be configured.

Type: Specifies the type for the operating parameter, the options are High Alarm, Low Alarm, High Warning and Low Warning.

High Alarm: Specifies the high threshold for the alarm. When the Bias current threshold rises above the configured value, the action associated with the alarm is taken.

Low Alarm: Specifies the low threshold for the alarm. When the Bias current threshold falls below the configured value, the action associated with the alarm is taken.

High Warning: Specifies the high threshold for the warning. When the Bias current threshold rises above the configured value, the action associated with the warning is taken.

Low Warning: Specifies the low threshold for the warning. When the Bias current threshold falls below the configured value, the action associated with the warning is taken.

Vaule (0 – 131): Specifies the value for the specified type of port.

Click **Apply** to make the configurations take effect.

Configuration > DDM > DDM TX Power Settings

The DDM TX Power Threshold Settings page is used to configure the threshold of TX power for specific ports on the Switch.

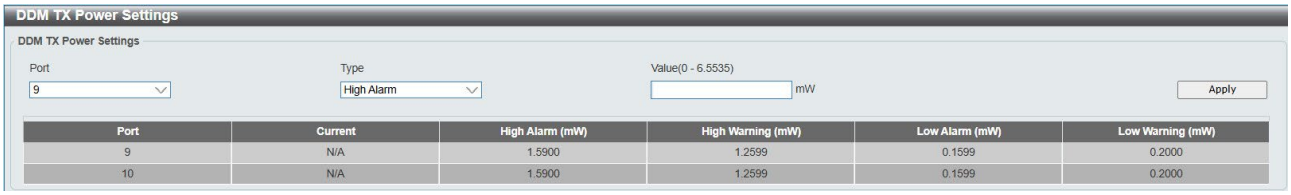


Figure 4.125 - Configuration > DDM > DDM TX Power Settings

Port: Specifies the port to be configured.

Type: Specifies the type for the operating parameter, the options are High Alarm, Low Alarm, High Warning and Low Warning.

High Alarm: Specifies the high threshold for the alarm. When the TX power threshold rises above the configured value, the action associated with the alarm is taken.

Low Alarm: Specifies the low threshold for the alarm. When the TX power threshold falls below the configured value, the action associated with the alarm is taken.

High Warning: Specifies the high threshold for the warning. When the TX power threshold rises above the configured value, the action associated with the warning is taken.

Low Warning: Specifies the low threshold for the warning. When the TX power threshold falls below the configured value, the action associated with the warning is taken.

Vaule (0 – 6.5535): Specifies the value for the specified type of port.

Click **Apply** to make the configurations take effect.

Configuration > DDM > DDM RX Power Threshold Settings

The DDM RX Power Threshold Settings page is used to configure the threshold of RX power for specific ports on the Switch.

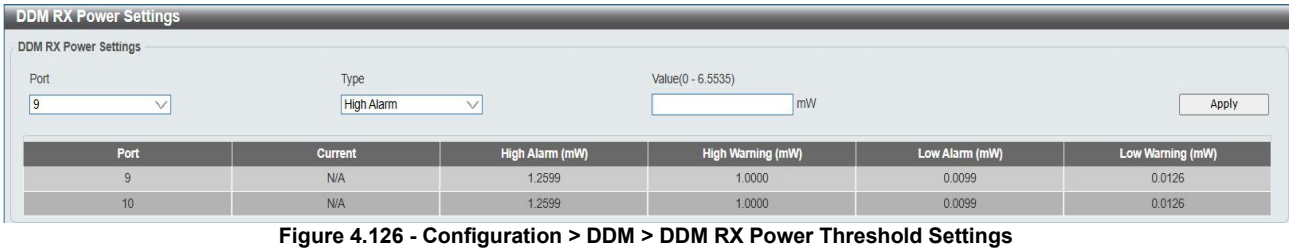


Figure 4.126 - Configuration > DDM > DDM RX Power Threshold Settings

Port: Specifies the port to be configured.

Type: Specifies the type for the operating parameter, the options are High Alarm, Low Alarm, High Warning and Low Warning.

High Alarm: Specifies the high threshold for the alarm. When the RX power threshold rises above the configured value, the action associated with the alarm is taken.

Low Alarm: Specifies the low threshold for the alarm. When the RX power threshold falls below the configured value, the action associated with the alarm is taken.

High Warning: Specifies the high threshold for the warning. When the RX power threshold rises above the configured value, the action associated with the warning is taken.

Low Warning: Specifies the low threshold for the warning. When the RX power threshold falls below the configured value, the action associated with the warning is taken.

Vaule (0 – 6.5535): Specifies the value for the specified type of port.

Click **Apply** to make the configurations take effect.

Configuration > DDM > DDM Status Table

The DDM Status Table page displays the current operating digital diagnostic monitoring parameters and their values on the SFP module for specified ports.

Figure 4.127 - Configuration > DDM > DDM Status Table

Configuration > DDM > DDM Vendor Info

The DDM Vendor Info Table page displays the vendor information obtained from DDM.

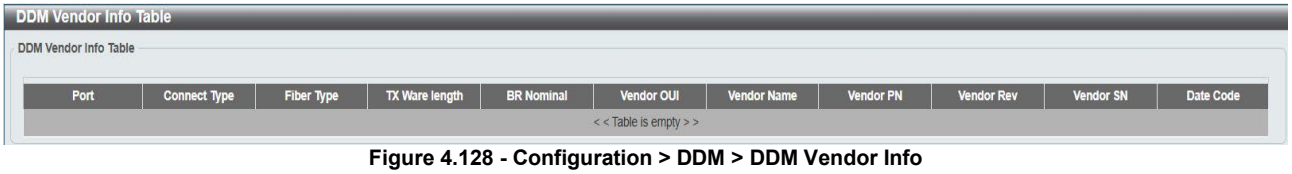


Figure 4.128 - Configuration > DDM > DDM Vendor Info

Configuration > DULD > DULD Global Settings

The DULD Global Settings page allows user to configure the DULD recover time.

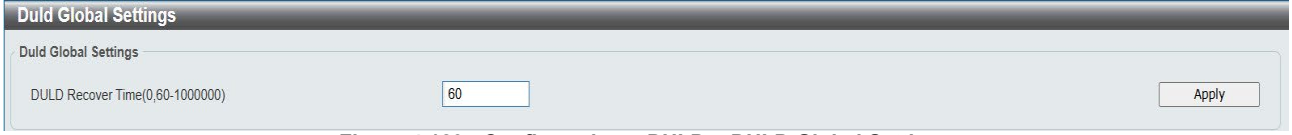


Figure 4.129 - Configuration > DULD > DULD Global Settings

DULD Recover Time (60-1000000): Specifies the DULD recover time.

Click the **Apply** button to accept the changes made.

Configuration > DULD > DULD Port Settings

The DULD Port Settings page allows user to configure the unidirectional link detection on ports. Unidirectional link detection provides discovery mechanism based on 802.3ah to discovery its neighbor. If the OAM discovery can complete in configured discovery time, it concludes the link is bidirectional. Otherwise, it starts detecting task to detect the link status.

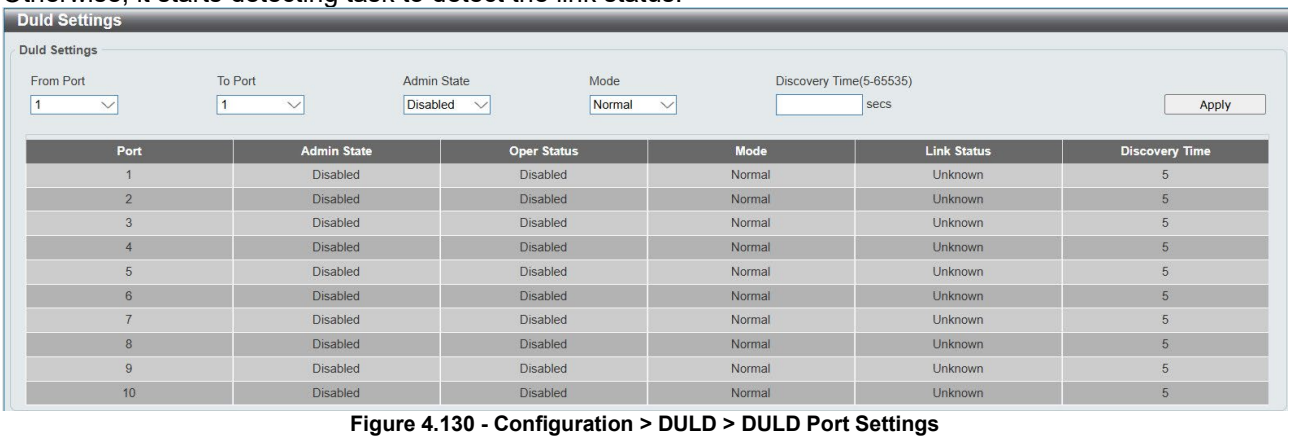


Figure 4.130 - Configuration > DULD > DULD Port Settings

From Port / To Port: Specifies a range of ports to be configured.

Admin State: Enable or disable the port unidirectional link detection status. The default is disabled.

Mode: Specifies the mode of DULD.

Normal – Only log and event when a unidirectional link is detected.

Shutdown – If any unidirectional link is detected, disable the port and log an event.

Discovery Time (5-65535): Specifies these ports neighbor discovery time. If the discovery is timeout, the unidirectional link detection will start. The default discovery time is **5** seconds.

Click **Apply** to make the configurations take effect.

Configuration > Multicast Forwarding & Filtering > Multicast Filtering

The Multicast Filtering Mode page allows user to set up the filtering mode.

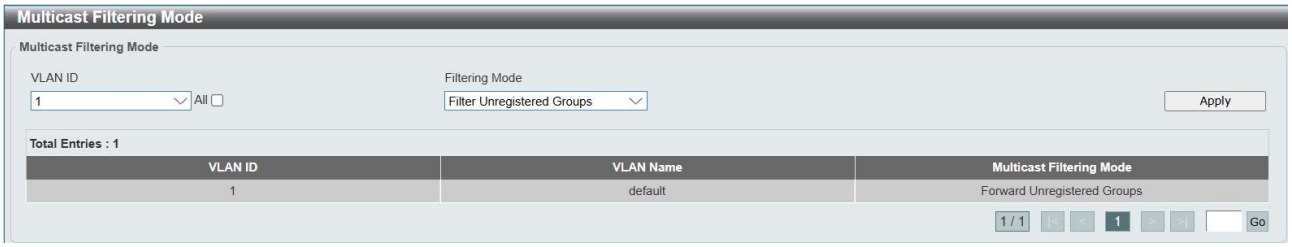


Figure 4.131 - Configuration > Multicast Forwarding & Filtering > Multicast Filtering

From Port / To Port: Specify the ports of the VLAN on which the corresponding MAC address belongs to.

Multicast Filtering Mode: This drop-down menu allows user to select the action the Switch will take when it receives a multicast packet that is to be forwarded to one of the ports in the range specified above.

Forward Unregistered Groups - This will instruct the Switch to forward a multicast packet whose destination is an unregistered multicast group residing within the range of ports specified above.

Filter Unregistered Groups - This will instruct the Switch to filter any multicast packets whose destination is an unregistered multicast group residing within the range of ports specified above.

Configuration > ERPS Setting

ERPS (Ethernet Ring Protection Switching) is the first industry standard (ITU-T G.8032) for Ethernet ring protection switching. It is achieved by integrating mature Ethernet operations, administration, and maintenance (OAM) functions and a simple automatic protection switching (APS) protocol for Ethernet ring

networks. ERPS provides sub-50ms protection for Ethernet traffic in a ring topology. It ensures that there are no loops formed at the Ethernet layer. One link within a ring will be blocked to avoid Loop (RPL, Ring Protection Link). When the failure happens, protection switching blocks the failed link and unblocks the RPL. When the failure clears, protection switching blocks the RPL again and unblocks the link on which the failure is cleared.

RPL (Ring Protection Link) – Link designated by mechanism that is blocked during Idle state to prevent loop on Bridged ring RPL Owner – Node connected to RPL that blocks traffic on RPL during Idle state and unblocks during Protected state R-APS (Ring – Automatic Protection Switching) - Protocol messages defined in Y.1731 and G.8032 used to coordinate the protection actions over the ring through RAPS VLAN (R-APS Channel). RAPS VLAN (R-APS Channel) – A separate ring-wide VLAN for transmission of R-APS messages Protected VLAN – The service traffic VLANs for transmission of normal network traffic.

The ERPS Setting page allows user to configure the settings of ERPS.

Figure 4.132 - Configuration > ERPS Setting

ERPS Global Settings:

ERPS State: To enable or disable the ERPS state.

ERPS Log: To enable or disable the ERPS log.

ERPS Trap: To enable or disable the ERPS trap.

R-APS VLAN Settings:

R-APS VLAN (1-4094): To configure the R-APS VLAN ID.

Click **Apply** or **Clear All** to implement changes made.

Click the **Delete** button to remove the specific entry.

Click the **Detail Information** link to view detailed information of the R-APS entry.
Click the **Sub-Ring Information** link to view the Sub-Ring information of the R-APS entry.

After clicking the Detail Information link, the following window will appear:

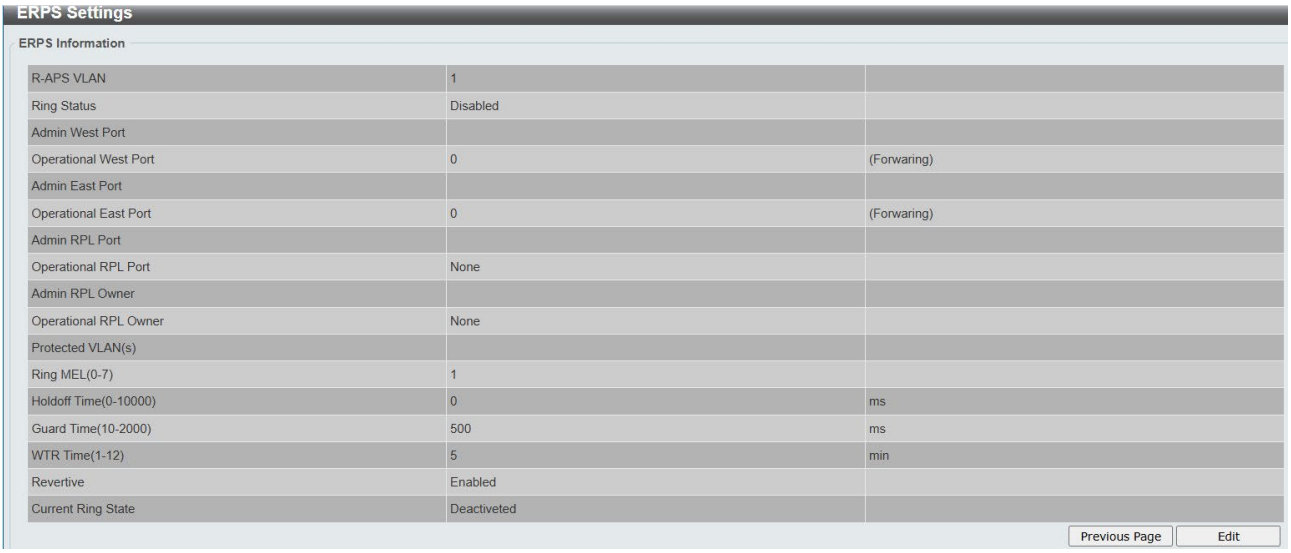


Figure 4.133 - Configuration > ERPS Setting - Detail

QoS > Traffic Control

The Traffic Control feature provides the ability to control the receive rate of broadcast, multicast, and unknown unicast packets. Once a packet storm has been detected, the Switch will drop packets coming into the Switch until the storm has subsided.

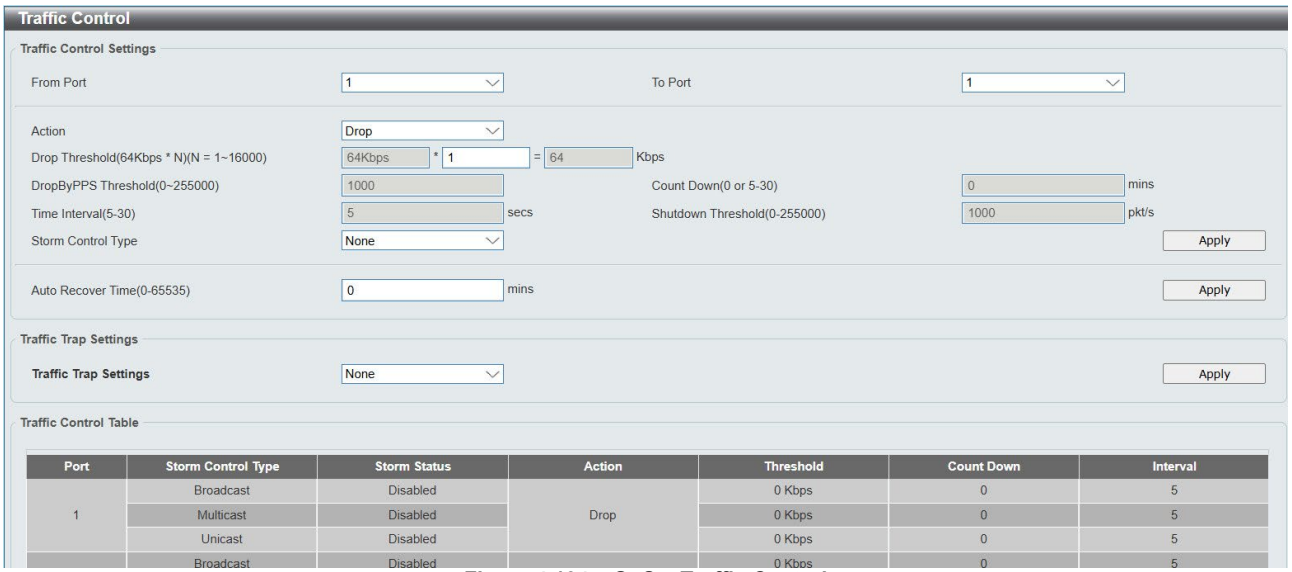


Figure 4.134 – QoS > Traffic Control

Parameter	Description
From Port / To Port	Specify the From and To port(s) to be configured.
Action	**Dropkbps**: Utilizes the hardware Traffic Control mechanism, which means the Switch's hardware will determine the Packet Storm based on the Threshold value stated and drop packets until the issue is resolved. **Shutdown**: Utilizes the Switch's software Traffic Control mechanism to determine the Packet Storm occurring. Once detected, the port will deny all incoming traffic to the port except STP BPDU packets, which are essential in keeping the Spanning Tree operational on the Switch. If the countdown timer has expired and yet the Packet Storm continues, the port will be placed in rest mode and if no action is taken will enter auto-recovery mode after a five minute period. Choosing this option obligates the user to

	configure the interval setting as well, which will provide packet count samplings from the Switch's chip to determine if a Packet Storm is occurring. **DropbyPPS**: Utilizes the hardware Traffic Control mechanism, which means the Switch's hardware will determine the Packet Storm based on the Threshold value stated and drop packets until the issue is resolved.
Drop Threshold (64Kbps * N)	Specify the threshold from 64 ~ 1,024,000 Kbit per second, with steps (N) of 64Kbps. N can be from 1 to 16000.
DropByPPS Threshold (0-255000)	Specify the threshold from 0-255000. The measurement unit is packet/second. This configure effected when Action configured to DropbyPPS.
Count Down (0 or 5-30)	The countdown timer is set to determine the amount of time, in minutes, that the Switch will wait before shutting down the port that is experiencing a traffic storm. This parameter is only useful for ports configured as Shutdown in their Action field and therefore will not operate for Hardware based Traffic Control implementations. The possible time settings for this field are 0, 5-30 minutes. 0 denotes that the port will never shutdown.
Time Interval (5-30)	The interval will set the time between Multicast and Broadcast packet counts sent from the Switch's chip to the Traffic Control function. These packet counts are the determining factor in deciding when incoming packets exceed the Threshold value. The interval may be set between 5 and 30 seconds with the default setting of 5 seconds.
Shutdown Threshold (0-255000)	Specify the shutdown threshold for traffic threshold.
Storm Control Type	User can select the different Storm type from Broadcast, Multicast, Broadcast + Multicast, Unknown Unicast, Broadcast + Unknown Unicast, Multicast + Unknown Unicast, and Broadcast + Multicast + Unknown Unicast.

Click **Apply** for the settings to take effect.

Auto Recover Time (0-65535): Specify the auto recover time. The value is from 0 to 65535.
Click **Apply** for the settings to take effect.

Traffic Trap Settings: Specify the traffic trap is **None**, **Storm Occurred**, **Storm Cleared** or **Both**.
Click **Apply** for the settings to take effect.

NOTE: Traffic Control cannot be implemented on ports that are set for Link Aggregation.

NOTE: Ports that are in the rest mode will be seen as Discarding in Spanning Tree windows and implementations though these ports will still be forwarding BPDUs to the Switch's CPU.

NOTE: Ports that are in rest mode will be seen as link down in all windows and screens until it enters the auto-recovery mode or the user recovers these ports by configuring the port state.

QoS > Bandwidth Control

The Bandwidth Control page allows network managers to define the bandwidth settings for a specified port's transmitting and receiving data rates.

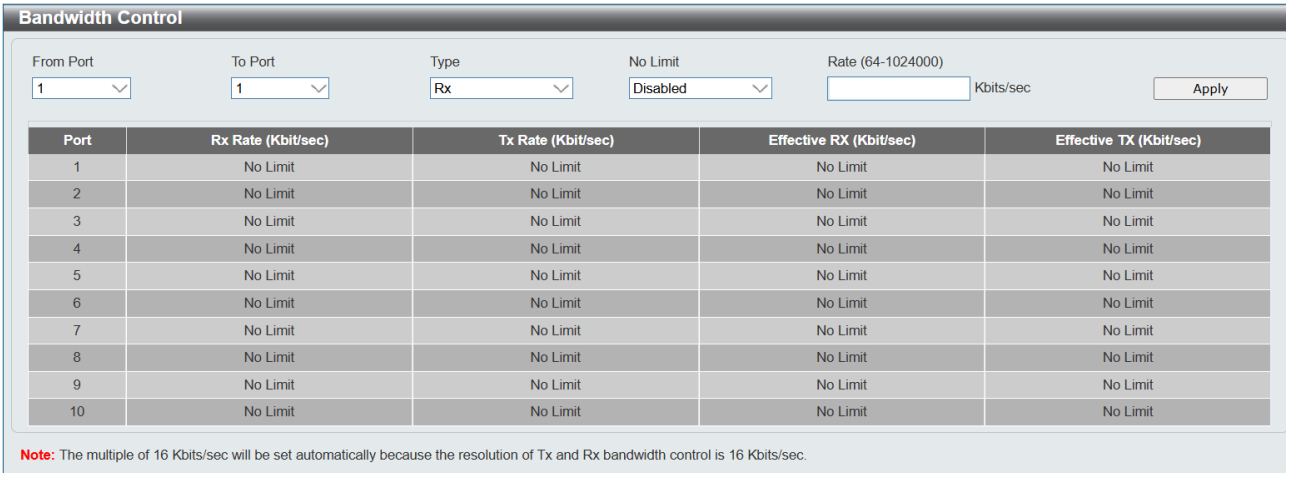


Figure 4.135 – QoS > Bandwidth Control

From Port / To Port: A consecutive group of ports may be configured starting with the selected port.

Type: This drop-down menu allows user to select between *RX* (receive), *TX* (transmit), and *Both*. This setting will determine whether the bandwidth ceiling is applied to receiving, transmitting, or both receiving and transmitting packets.

No Limit: This drop-down menu allows user to specify that the selected port will have no bandwidth limit.

Enabled disables the limit.

Rate (64-1024000): This field allows user to enter the data rate, in Kbits per second, will be the limit for the selected port. The value is between 64 and 1024000.

Click **Apply** to set the bandwidth control for the selected ports.

NOTE: The TX rate for Gigabit ports can only be configured in multiples of 16kbit. If any other value is used, the system automatically rounds it down to the lower multiple of 16Kbit.

QoS > Queue Bandwidth Control Settings

Queue Bandwidth Control feature allows user to configure a range (minimum rate/maximum rate) for each queue by port basis. This feature offers more flexibility and efficiency of use bandwidth in each queue.

Figure 4.136 – QoS > Queue Bandwidth Control Settings

The fields can be configured as described:

Parameter	Description
From Port / To Port	Use the drop-down menu to select the port range to use for this configuration.
From Queue / To Queue	Use the drop-down menu to select the queue range to use for this configuration.
Min Rate(64-1024000)	Specify the packet limit, in **Kbps** that the ports are allowed to receive. Tick the **No limit** check box to have unlimited rate of packets received by the specified queue.
Max Rate(64-1024000)	Specify the maximum rate for the queue. For no limit select the **No Limit** option.

Click the **Apply** button to apply the changes.

QoS > CoS Scheduling Mechanism

The CoS Scheduling Mechanism page allows user to select from **WRR and Strict** mechanism for emptying the priority classes.

Figure 4.137 - QoS > CoS Scheduling Mechanism

Parameter	Description
Strict Priority	The highest class of service is the first to process traffic. That is, the highest class of service will finish before other queues empty.
WRR:	Use the weighted round-robin (WRR) algorithm to handle packets in an even distribution in priority classes of service.
1st7wrr	Strict scheduling will set the highest queue while the other queues will follow the weighted round-robin scheduling scheme
2st6wrr	Strict scheduling will set the highest 2 queues while the other queues will follow the weighted round-robin scheduling scheme

Click **Apply** to make the configurations take effect.

QoS > CoS Output Scheduling

CoS can be customized by changing the output scheduling used for the hardware classes of service in the Switch. As with any changes to CoS implementation, careful consideration should be given to how network traffic in lower priority classes of service is affected. Changes in scheduling may result in unacceptable levels of packet loss or significant transmission delay. If user choose to customize this setting, it is important to monitor network performance, especially during peak demand, as bottlenecks can quickly develop if the CoS settings are not suitable.

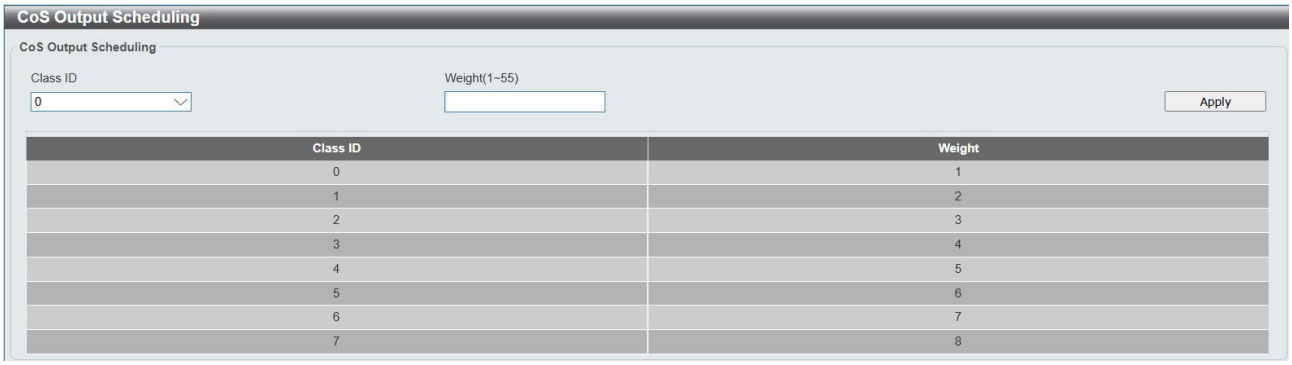


Figure 4.138 - QoS > CoS Output Scheduling

Class ID: Specify the priority queue for the switch. The value is from *0* to *7*.
Weight (1-55): Specify the weight for a CoS. The value is from *1* to *55*.

Click **Apply** to make the configurations take effect.

QoS > 802.1p Default Priority

QoS is an implementation of the IEEE 802.1p standard that allows network administrators to reserve bandwidth for important functions that require a larger bandwidth or that might have a higher priority, such as VoIP (voice-over Internet Protocol), web browsing applications, file server applications or video conferencing. Thus with larger bandwidth, less critical traffic is limited, and therefore excessive bandwidth can be saved.

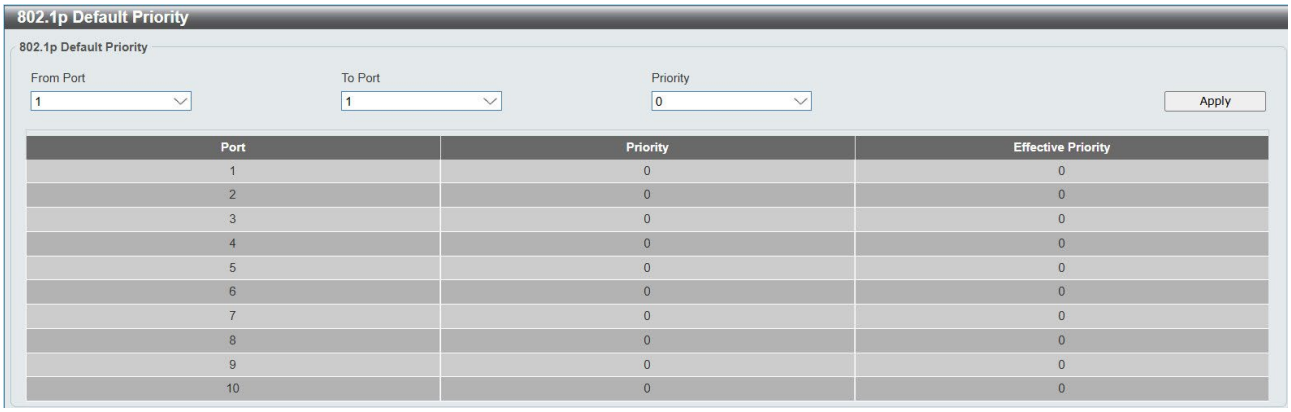


Figure 4.139 - QoS > 802.1p Default Priority

From Port / To Port: A consecutive group of ports may be configured starting with the selected port.

Priority: Defines the priority assigned to the port. The priority are 0~7.

Click **Apply** to make the configurations take effect.

QoS > 802.1p User Priority

When using 802.1p priority mechanism, the packet is examined for the presence of a valid 802.1p priority tag. If the tag is present, the packet is assigned to a programmable egress queue based on the value of the tagged priority. The tagged priority can be designated to any of the available queues.

The Switch allows the assignment of a class of service to each of the 802.1p priorities.

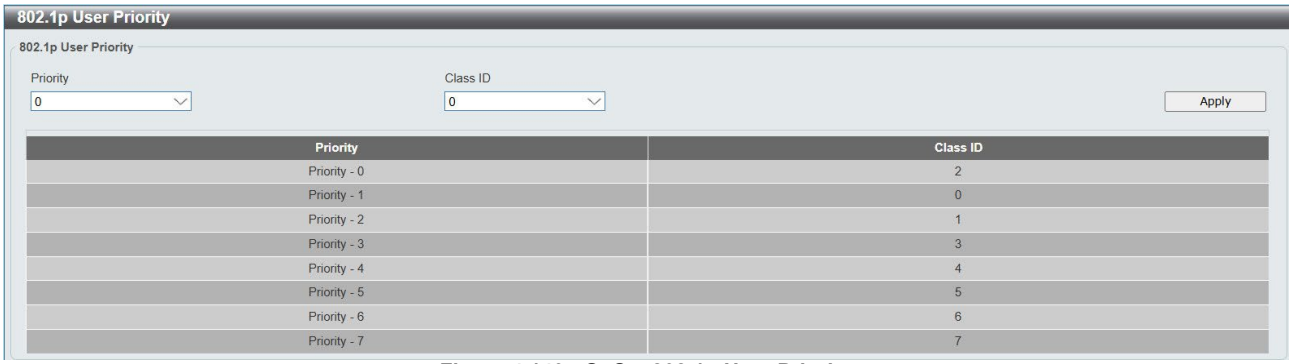


Figure 4.140 - QoS > 802.1p User Priority

Once the user had assigned a priority to the port groups on the Switch, user can then assign this Class to each of the four levels of 802.1p priorities. Click **Apply** to make the configurations take effect.

QoS > DSCP Priority Settings

When using the DSCP priority mechanism, the packet is classified based on the DSCP field in the IP header. If the tag is present, the packet is assigned to a programmable egress queue based on the value of the tagged priority. The tagged priority can be designated to any of the available queues. When a packet is received containing this DSCP tag, it will be mapped to the CoS queue configured here. These settings will only take effect if at least one of the priority settings per port is configured for DSCP. When DSCP is set to enable, TOS cannot be used, and when TOS is set to enable, DSCP cannot be used.

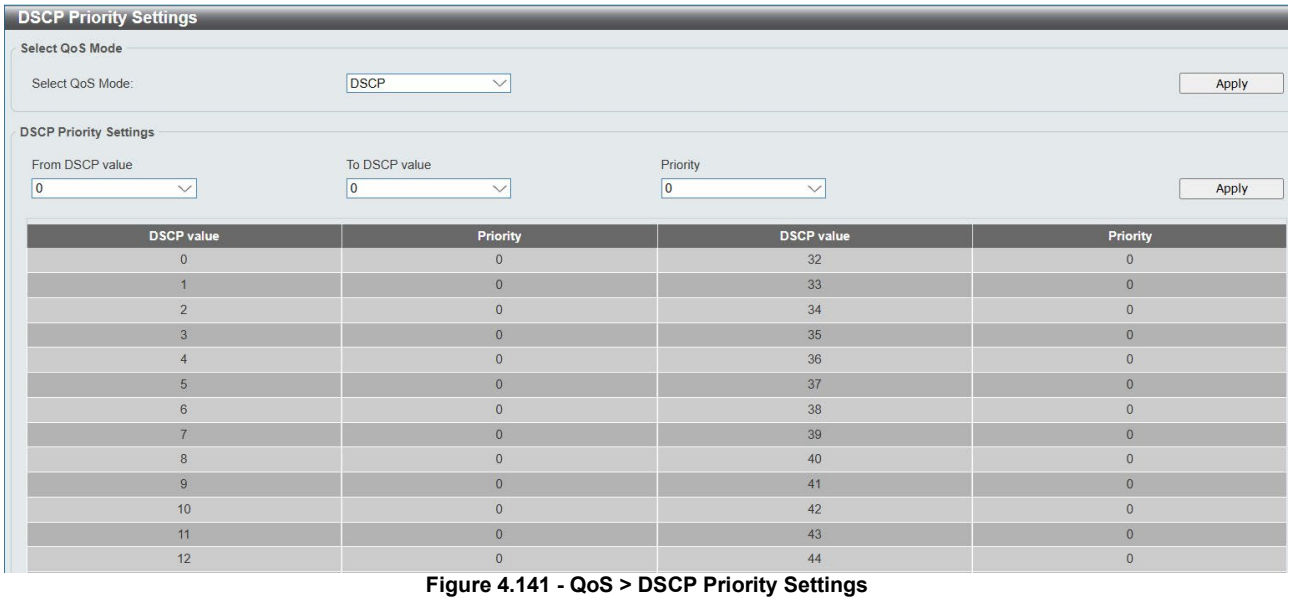


Figure 4.141 - QoS > DSCP Priority Settings

Select QoS Mode: Specify the mode to be DASP or TOS.

From DSCP value / To DSCP value: Specify the range of DSCP values.

Priority: Specify the priority queue for the switch. The value is from *0* to *7*.

Click **Apply** to make the configurations take effect.

QoS > Priority Settings

The Priority Setting page allow users to configure the CoS priority settings on a port or ports. When CoS tagged packets arrive on the switch, they are mapped to the settings configured here. For example, if a port has been assigned a MAC priority, the packet that has the CoS priority assigned to a MAC address will be sent to the CoS queue configured for that MAC address. Once the configuration has been completed, users may see the results in the Priority Settings Table seen here. After configuring the port priorities, users may adjust the individual CoS settings on the other windows located in the CoS folder of the Switch.

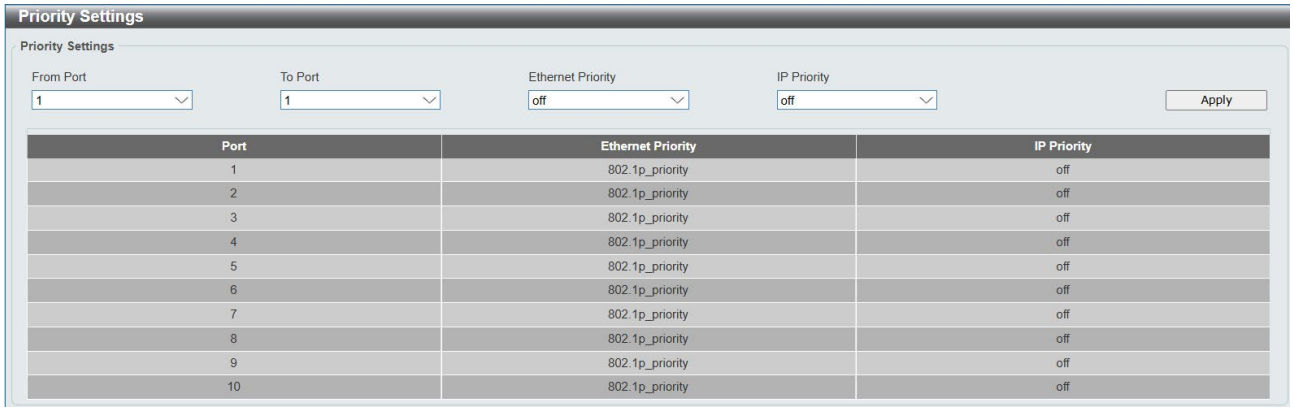


Figure 4.142 - QoS > Priority Settings

From Port/To Port: Users may select a port or group of ports to assign the priority settings.

Port Priority: Specify the Port Priority is *Off* or *On* on the port.
Ethernet Priority: Specify the Ethernet Priority is Off or 802.1p on the port.
IP Priority: Specify the IP Priority is Off or DSCP on the port.

Click **Apply** to make the configurations take effect.

QoS > Management Packet Priority Settings

This feature allow user to configure priority of management packets. For example, IGMP, BPDUPD, IGMP report, IGMP leave, IGMP query, etc.

Figure 4.143 – QoS > Management Packet Priority Settings

Management Packet Priority: User can specify the priority level from 0-7. Default value 7 represents the highest priority.

Click **Apply** to apply to configurations.

RMON > RMON Basic Settings

Users can enable and disable remote monitoring (RMON) status for the SNMP function on the Switch. In addition, RMON Rising and Falling Alarm Traps can be enabled and disabled. Click **Apply** to make effects.

Figure 4.144 - RMON > RMON Basic Settings

RMON > RMON Ethernet Statistics Configuration

The RMON Statistics Configuration page displays the information of RMON Ethernet Statistics and allows the user to configure the settings.

Figure 4.145 - RMON > RMON Ethernet Statistics Configuration

The RMON Ethernet Statistics Configuration contains the following fields:
Index (1 - 65535): Indicates the RMON Ethernet Statistics entry number.
Port: Specifies the port from which the RMON information was taken.
Owner: Displays the RMON station or user that requested the RMON information.

Click **Apply** to make the configurations take effect.

RMON > RMON History Control Configuration

The RMON History Control Configuration page contains information about samples of data taken from ports. For example, the samples may include interface definitions or polling periods.

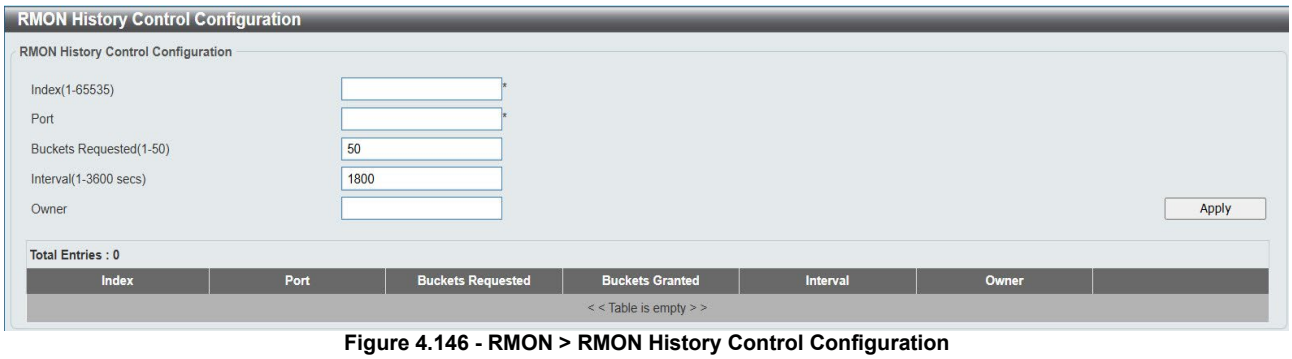


Figure 4.146 - RMON > RMON History Control Configuration

The History Control Configuration contains the following fields:

Index (1 - 65535): Indicates the history control entry number.

Port: Specifies the port from which the RMON information was taken.

Buckets Requested (1 ~ 50): Specifies the number of buckets that the device saves.

Interval (1 ~ 3600): Indicates in seconds the time period that samplings are taken from the ports. The field range is *1-3600*. The default is *1800* seconds (equal to 30 minutes).

Owner: Displays the RMON station or user that requested the RMON information.

Click **Apply** to make the configurations take effect.

RMON > RMON Alarm Configuration

The RMON Alarm Configuration page allows the user to configure the network alarms. Network alarms occur when a network problem, or event, is detected.

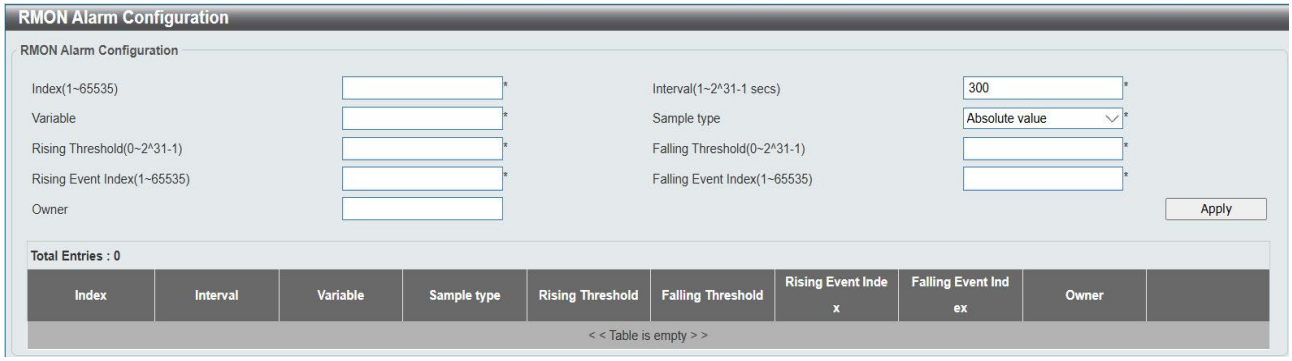


Figure 4.147 - RMON > RMON Alarm Settings

The configuration contains the following fields:

Index (1 - 65535): Indicates a specific alarm.

Variable: Specify the selected MIB variable value.

Rising Threshold (0 ~ 2^31-1): Displays the rising counter value that triggers the rising threshold alarm.

Rising Event Index (1 ~ 65535): Displays the event that triggers the specific alarm. The possible field values are user defined RMON events.

Owner: Displays the device or user that defined the alarm.

Interval (1 ~ 2^31-1): Defines the alarm interval time in seconds.

Sample type: Defines the sampling method for the selected variable and comparing the value against the thresholds. The possible field values are:

Delta value – Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.

Absolute value – Compares the values directly with the thresholds at the end of the sampling interval.

Falling Threshold (0 ~ 2^31-1): Displays the falling counter value that triggers the falling threshold alarm.

Falling Event Index (1 ~ 65535): Displays the event that triggers the specific alarm. The possible field values are user defined RMON events.

Click **Apply** to make the configurations take effect.

RMON > RMON Event Configuration

The RMON Event page contains fields for defining, modifying and viewing RMON events statistics.

Figure 4.148 - RMON > RMON Event Configuration

The RMON Events Page contains the following fields:

Index (1~ 65535): Displays the event.

Description: Specifies the user-defined event description.

Type: Specifies the event type. The possible values are:

None – Indicates that no event occurred.

Log – Indicates that the event is a log entry.

SNMP Trap – Indicates that the event is a trap.

Log and Trap – Indicates that the event is both a log entry and a trap.

Community: Specifies the community to which the event belongs.

Owner: Specifies the time that the event occurred.

Click **Apply** to add a new RMON event.

Security > Trusted Host

Use Trusted Host function to manage the switch from a remote station. User can specify up to ten designated management stations networks by defining the IP address/Subnet Mask as seen in the figure below.

Figure 4.149 - Security > Trusted Host

To define a management station IP setting, click the **Add Host** button and type in the IP address and Subnet mask. Click the **Apply** button to save the settings. User may permit only single or a range of IP addresses by different IP mask settings, the format can either be 192.168.1.1/255.255.255.0 or 192.168.0.1/24. Please see the example below for permitting the IP range

IP Address	Subnet Mask	Permitted IP
192.168.0.1	255.255.255.0	192.168.0.1~192.168.0.255
172.17.5.215	255.0.0.0	172.0.0.1~172.255.255.255

To delete the IP address, simply click the **Delete** button. Check the unwanted address, and then click **Apply**.

Security > Safeguard Engine

D-Link's **Safeguard Engine** is a robust and innovative technology that automatically throttles the impact of packet flooding into the switch's CPU. This function helps protect the Switch from being interrupted by malicious viruses or worm attacks. This option is enabled by default.

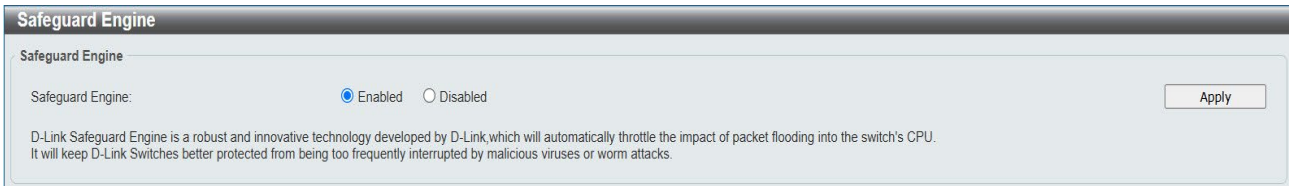


Figure 4.150 – Security > Safeguard Engine

Security > CPU Protect

The CPU Protect setting page allows user to view and configure the CPU protection type settings.

Figure 4.151 – Security > CPU Protect

CPU Protect State: Specifies the CPU protect state to be enabled or disabled.

Click the **Apply** button to accept the changes made.

The CPU Protect Types are **ARP**, **BPDU**, **ICMP**, **IGMP** and **SNMP**. Select the CPU Protect Type and enter the **Rate limit** which the value is between **0** and **65535** pps by ports. The default value is **no limit**.

Click the **Apply** button to apply settings.

Security > Gratuitous ARP

The Gratuitous ARP page shows the settings on the Switch. An ARP announcement (also known as Gratuitous ARP) is a packet (usually an ARP Request) containing a valid SHA (Sender Hardware Address) and SPA (Sender Protocol Address) for the host which sent it, with TPA (Target Protocol Address) equal to SPA. Such a request is not intended to solicit a reply, but merely update the ARP caches of other hosts which receive the packet and determine if there are any IP conflicts.

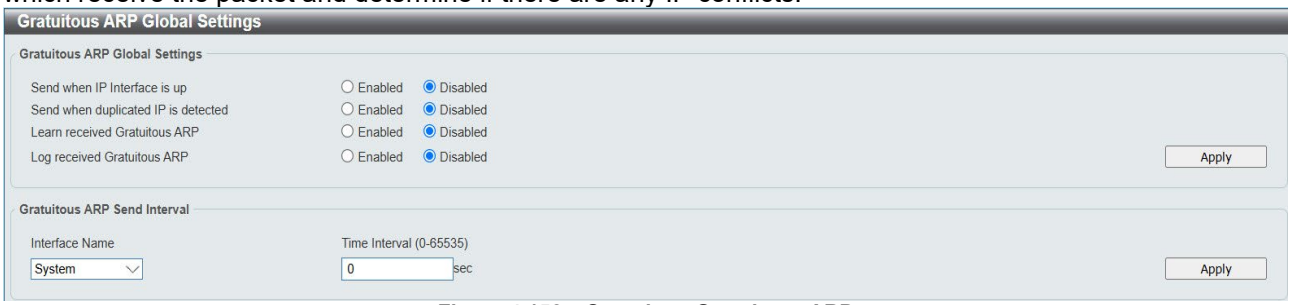


Figure 4.152 – Security > Gratuitous ARP

Send when IP Interface is up: This is used to enable/disable the sending of gratuitous ARP request packets while an IP interface comes up. This is used to automatically announce the interface's IP address to other nodes. By default, the state is *Disabled*, and only one ARP packet will be broadcast.
Send when duplicated IP is detected: This is used to enable/disable the sending of gratuitous ARP request packets while a duplicate IP is detected. By default, the state is *Disabled*. Duplicate IP detected means that the system received an ARP request packet that is sent by an IP address that matches the system's own IP address.
Learn received Gratuitous ARP: This is used to enable/disable updating ARP cache based on the received gratuitous ARP packet. If a switch receives a gratuitous ARP packet and the sender's IP address in its ARP table, it should update the ARP entry. This is D*isabled* by default.

Log received Gratuitous ARP: This is used to enable/disable send log feature when device received gratuitous ARP

Gratuitous ARP Send Interval: Specify the interval value.

Interface Name: Specify the Interface Name. The default is System.

Time Interval (0-65535): Specify the time interval, the range is from 0 to 65535, and the default is 0 seconds.

Click **Apply** to make configurations make effects.

Security > Port Security

Port Security is a security feature that prevents unauthorized computers (with source MAC addresses) unknown to the Switch prior to stopping auto-learning processing from gaining access to the network.

A given ports' (or a range of ports') dynamic MAC address learning can be stopped such that the current source MAC addresses entered into the MAC address forwarding table cannot be changed once the port is enabled.

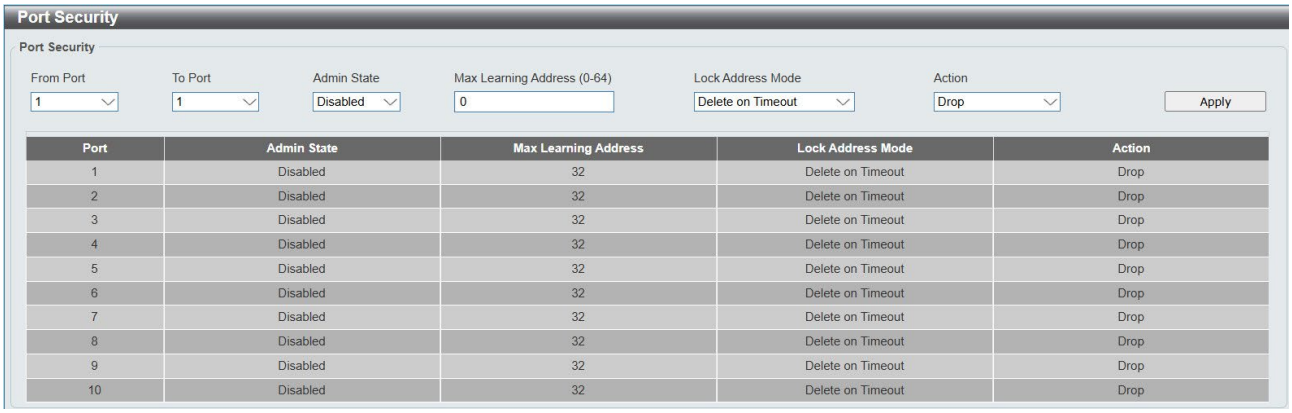


Figure 4.153 - Security > Port Security

The Port Security page contains the following fields:

From Port/To Port: A consecutive group of ports may be configured starting with the selected port.

Admin State: This pull-down menu allows users to enable or disable Port Security (locked MAC address table for the selected ports).

Max. Learning Address (0-64): The number of MAC addresses that will be in the MAC address-forwarding table for the selected switch and group of ports.

Lock Address Mode: This pull-down menu allows user to select how the MAC address table locking will be implemented on the Switch, for the selected group of ports. The options are:

Delete On Reset – The locked addresses will not age out until the Switch has been reset.

Delete On Timeout – The locked addresses will age out after the aging timer expires.

Permanent – The locked addresses will not age out after the aging timer expires.

Click **Apply** to make configurations make effects.

Security > SSL Settings

Secure Sockets Layer (SSL) is a security feature that provides a secure communication path between a Web Management host and the Switch Web UI by using authentication, digital signatures and encryption. These security functions are implemented by Ciphersuite, a security string that determines the cryptographic parameters, encryption algorithms and key sizes.

This page allows user to configure the SSL global state and the Ciphersuite settings. Select **Enable** or **Disable** and then click **Apply** to change the SSL state or the Ciphersuite settings of the Switch. By default, SSL is **Disabled** and all Ciphersuites are **Enabled**.

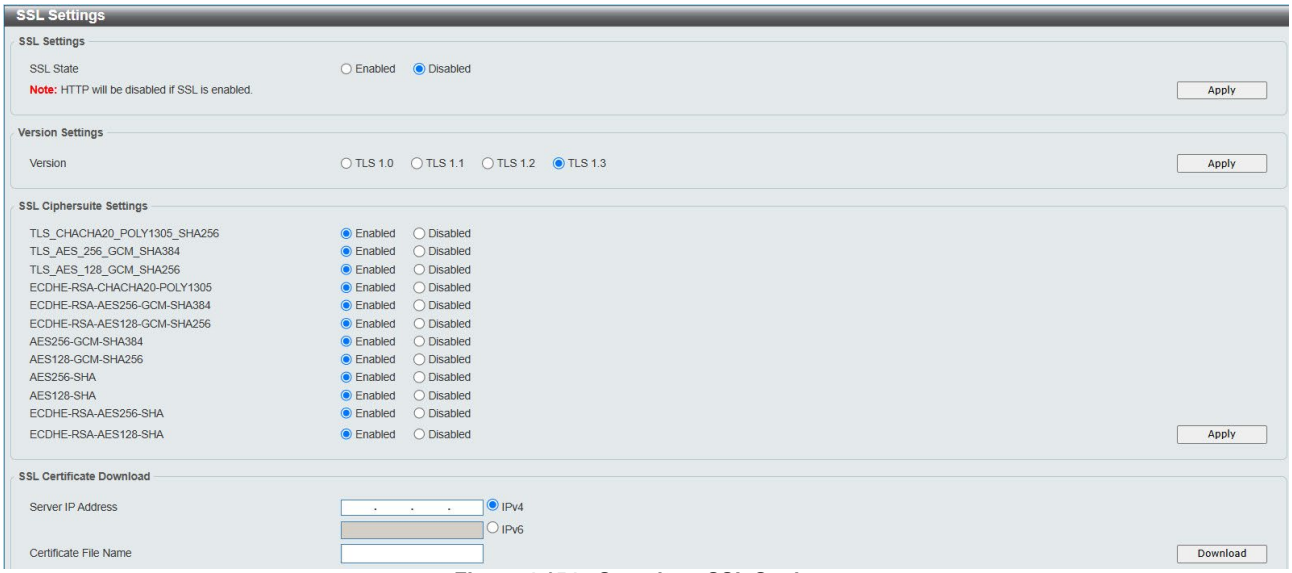


Figure 4.154 - Security > SSL Settings

The SSL Settings page allows users to download a certificate file for the SSL function on the Switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the client must have consistent certificate files for optimal use of the SSL function. The Switch only supports certificate files with .der file extensions. The Switch is shipped with a certificate pre-loaded though the user may need to download more, depending on user circumstances.

Server IP Address: Select IPv4 or IPv6 and enter the IP address of the TFTP server where the certificate files are located.

Certificate File Name: Enter the path and the filename of the certificate file to download. This file must have a .der extension. (Ex. c:/cert.der)

Click **Download** to download the certificate file.

NOTE: Enabling the SSL command will disable the web-based switch management. To log on to the Switch again, the header of the URL must begin with https://. Entering anything else into the address field of the web browser will result in an error and no authentication will be granted.

Security > Smart Binding > Smart Binding Settings

The primary purpose of Smart Binding is to restrict client access to a switch by enabling administrators to configure pairs of client MAC and IP addresses that are allowed to access networks through a switch.

The Smart Binding function is port-based, meaning that a user can enable or disable the function on any individual port. Once Smart Binding is enabled on a switch port, the switch will restrict or allow client access

by checking the pair of IP-MAC addresses with the pre-configured database, also known as the “IMPB white list”.

Users can enable or disable the **Packet Inspection** and **DHCP Snooping** on the Switch.

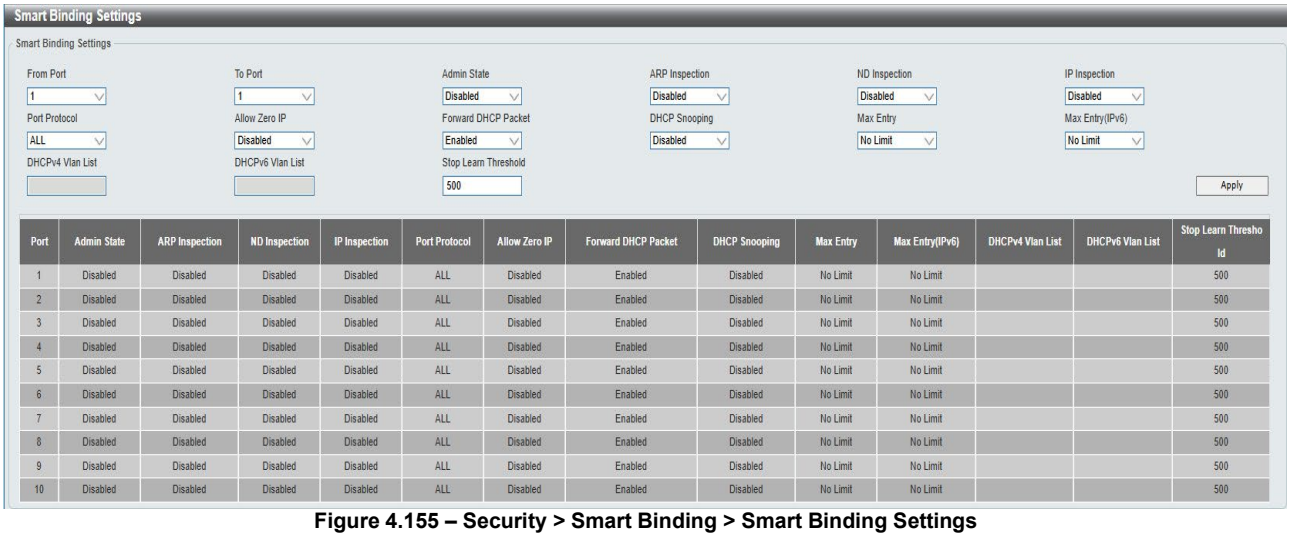


Figure 4.155 – Security > Smart Binding > Smart Binding Settings

The Smart Binding Settings page contains the following fields:

From Port/ To Port: Select a range of ports to set for IP-MAC-port binding.

Admin State: Use the drop-down menu to enable or disable these ports for Smart Binding.

Enabled –Enable Smart Binding with related configurations to the ports

Disabled –Disable Smart Binding.

ARP Inspection: If ARP inspection is enabled, the Switch will inspect incoming ARP packets and compare them with the Switch’s Smart Binding white list entries. If the IP-MAC pair of an ARP packet is not found in the white list, the Switch will block the MAC address. A major benefit of Loose state is that it uses less CPU resources. However, it cannot block malicious users who send only unicast IP packets. An example of this is that a malicious user can perform DoS attacks by statically configuring the ARP table on their PC. In this case, the Switch cannot block such attacks because the PC will not send out ARP packets.

IP Inspection: When IP Inspection is enabled, and ARP Inspection is disabled, all non-IP packets are forwarded by default. If **ARP Inspection** and **IP Inspection** mode are enabled, the Switch will inspect all incoming ARP and IP packets and compare them to the IMPB white list. If the IP-MAC pair find a match in the white list, the packets from that MAC address are unblocked. If not, the MAC address will stay blocked. While the mode examines every ingress ARP and IP packet, it enforces better security.

Allow Zero IP: Enable or disable to allow zero IP to configure the state which allows ARP packets with 0.0.0.0 source IP to bypass.

Forward DHCP Packet: Enable or disable to forward DHCP packet.

DHCP Snooping: By enable DHCP Snooping, the switch will snoop the packets sent from DHCP Server and clients, and update information to the White List.

Max Entry: Specifies the max entries of Smart Binding. The range is between 1 and 10, or No Limit.

Max Entry (IPv6): Specifies the IPv6 max entries of Smart Binding. The range is between 1 and 10, or No Limit.

Click **Apply** to make configurations make effects.

Security > Smart Binding > Smart Binding

The Smart Binding page allows the user to create Static IP-MAC-Port Binding entries on the Switch.

Figure 4.156 – Security > Smart Binding > Smart Binding

The Auto Scan Binding Settings contains the following fields:

Auto Scan: Specifies to scan connected devices in a range of IP address.

IP Address From/To: Specifies the range of IP Address to scan all devices in the network.

Click **Scan** and the search results will be listed in below table.

Binding: check the box to select desired binding devices.

Apply: click **Apply** to set IP-MAC-Port Binding entries."

Select All: to check the boxes of Binding for all found devices.

Clear All: to cancel the box of Binding.

Security > Smart Binding > White List

When IP+ARP Inspection Mode were selected, the White List page displays finished IP-MAC-Port Binding entries from page Smart Binding. Only IP packets or ARP packets carrying matched IP-MAC-Port information can access to the switch. User can cancel a device's authorization by deleting it from the table.

Figure 4.157 – Security > Smart Binding > White List

From Port / To Port: Specifies the port ranges for MAC address to bind to the IP address of Binding list.

IP Address: Specifies the IP address to bind to the MAC address set below.

MAC Address: Specifies the MAC address to bind to the IP address set above.

Click **Add** to add a new entry.

Delete: Select Manual white entries then push delete button that will deleted selected manual white entries.

Click **Select All** to select all entries of the table or click **Clear All** to select none entries. Please keep at least one management host in the White List.

Security > Smart Binding > Black List

The Black List page shows unauthorized accesses. When ARP Inspection is selected and a device sends out an ARP packet containing unmatched IP-MAC-Port information, the device will be forbidden and listed here.

Figure 4.158 – Security > Smart Binding > Black List

By giving conditions, desired devices information can be screened out below then click **Find** to search for a list of the entry:

VID: Enter the VLAN ID number of the device.

IP Address: Enter the IP Address of the device.

MAC Address: Enter the MAC Address of the device.

Port: Enter the port number which the device connects.

Check a box of **Delete** column to release an entry from the forbidden list then click **Apply** to delete an entry from the list.

Click **Select All** to select all entries, or click **Clear All** to select none of the entries.

Security > Smart Binding > DHCP Snooping List

The DHCP Snooping List page shows the DHCP Snooping list.

Figure 4.159 – Security > Smart Binding > DHCP Snooping List

Security > 802.1X > 802.1X Settings

Network switches provide easy and open access to resources by simply attaching a client PC. Unfortunately this automatic configuration also allows unauthorized personnel to easily intrude and possibly gain access to sensitive data.

IEEE-802.1X provides a security standard for network access control, especially in Wi-Fi wireless networks. 802.1X holds a network port disconnected until authentication is completed. The switch uses Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol client identity (such as a user name) with the client, and forward it to another remote RADIUS authentication server to verify access rights. The EAP packet from the RADIUS server also contains the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. Depending on the authenticated results, the port is either made available to the user, or the user is denied access to the network.

The RADIUS servers make the network a lot easier to manage for the administrator by gathering and storing the user lists.

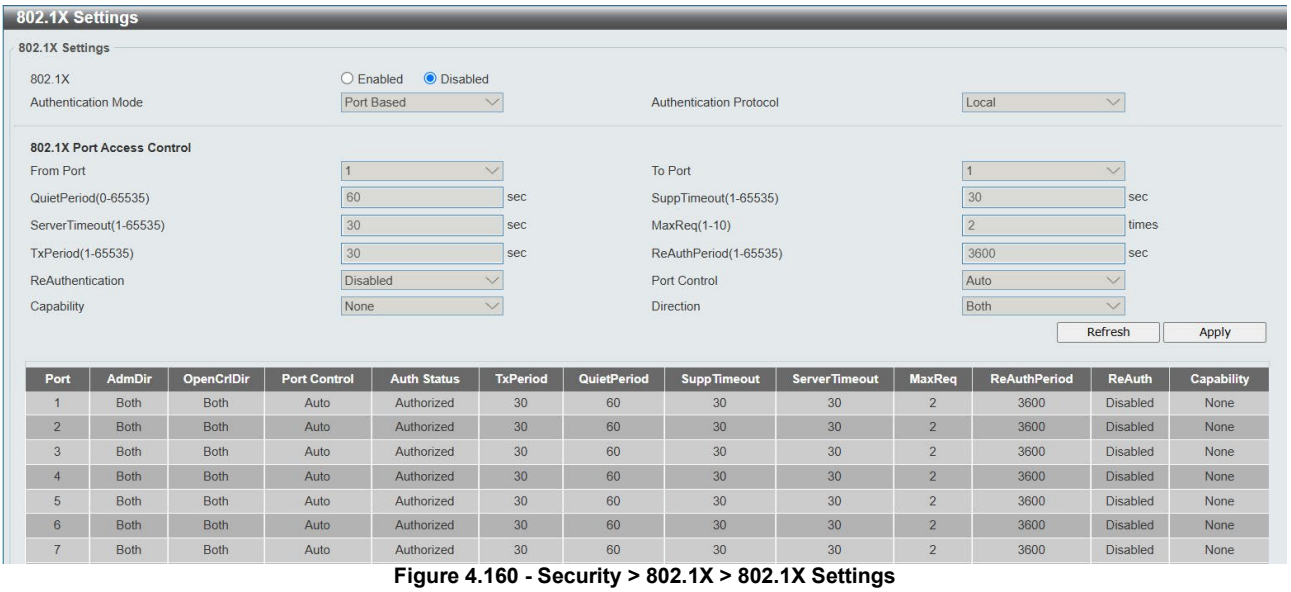


Figure 4.160 - Security > 802.1X > 802.1X Settings

By default, 802.1X is disabled. To use EAP for security, select enabled and set the **Authentication Mode** and **Authentication Protocol** then click **Apply**.

Authentication Mode: Indicates the 802.1X mode enabled on the device. The possible field values are:

Port Based – Enables 802.1X on ports. This is the default value.

MAC Based – Enables 802.1X on MAC addresses.

Authentication Protocol: Indicates the 802.1X Protocol on the device. The possible field values are *Local* and *RADIUS EAP*.

From Port/To Port: Enter the port or ports to be set.

QuietPeriod (0 – 65535 sec): Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. Default is *60* seconds.

ServerTimeout (1 – 65535 sec): Sets the amount of time the switch waits for a response from the client before resending the response to the authentication server. Default is *30* seconds.

TxPeriod (1 – 65535 sec): This sets the TxPeriod of time for the authenticator PAE state machine. This value determines the period of an EAP Request/Identity packet transmitted to the client. Default is *30* seconds.

ReAuthentication: Determines whether regular reauthentication will take place on this port. The default setting is *Disabled*.

Capability: Indicates the capability of the 802.1X. The possible field values are:

Authenticator – Specify the Authenticator settings to be applied on a per-port basis.

None – Disable 802.1X functions on the port.

SuppTimeout (1 – 65535 sec): This value determines timeout conditions in the exchanges between the Authenticator and the client. Default is *30* seconds.

MaxReq (1 – 10): This parameter specifies the maximum number of times that the switch retransmits an EAP request (md-5challnege) to the client before it times out the authentication session. Default is *2* times.

ReAuthPeriod (1 – 65535 sec): A constant that defines a nonzero number of seconds between periodic reauthentication of the client. The default setting is *3600* seconds.

Port Control: This allows user to control the port authorization state.

Select **ForceAuthorized** to disable 802.1X and cause the port to transition to the authorized state without any authentication exchange required. This means the port transmits and receives normal traffic without 802.1X-based authentication of the client.

If **ForceUnauthorized** is selected, the port will remain in the unauthorized state, ignoring all attempts by the client to authenticate. The Switch cannot provide authentication services to the client through the interface.

If **Auto** is selected, it will enable 802.1X and cause the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The Switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server.

The default setting is *Auto***.**

Direction: Sets the administrative-controlled direction on the port. The possible field values are:

Both – Specify the control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field.

In – Disables the support in the present firmware release.

Click **Apply** to make the configurations take effect.

Security > 802.1X > 802.1X User

The **802.1X User** page allows user to set different local users on the Switch. Enter a **802.1X User** name, **Password** and **Confirm Password**. Properly configured local users will be displayed in the table.

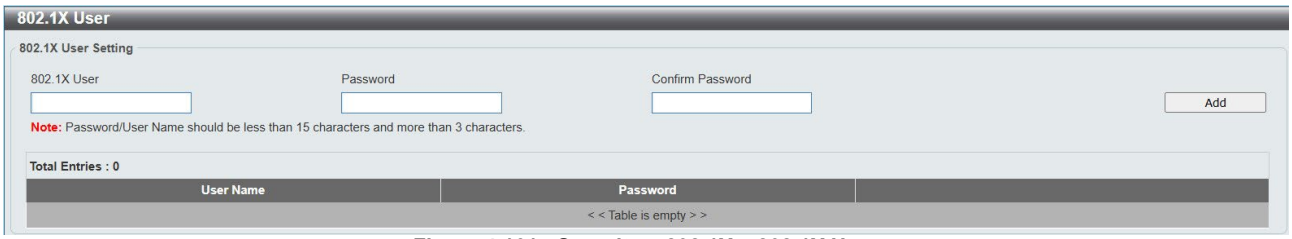


Figure 4.161 - Security > 802.1X > 802.1X User

Click **Add** to add a new 802.1X user.

Security > 802.1X > 802.1X Authentication RADIUS

The 802.1X Authentication RUAIUS of the Switch allows user to facilitate centralized user administration as well as providing protection against a sniffing, active hacker.

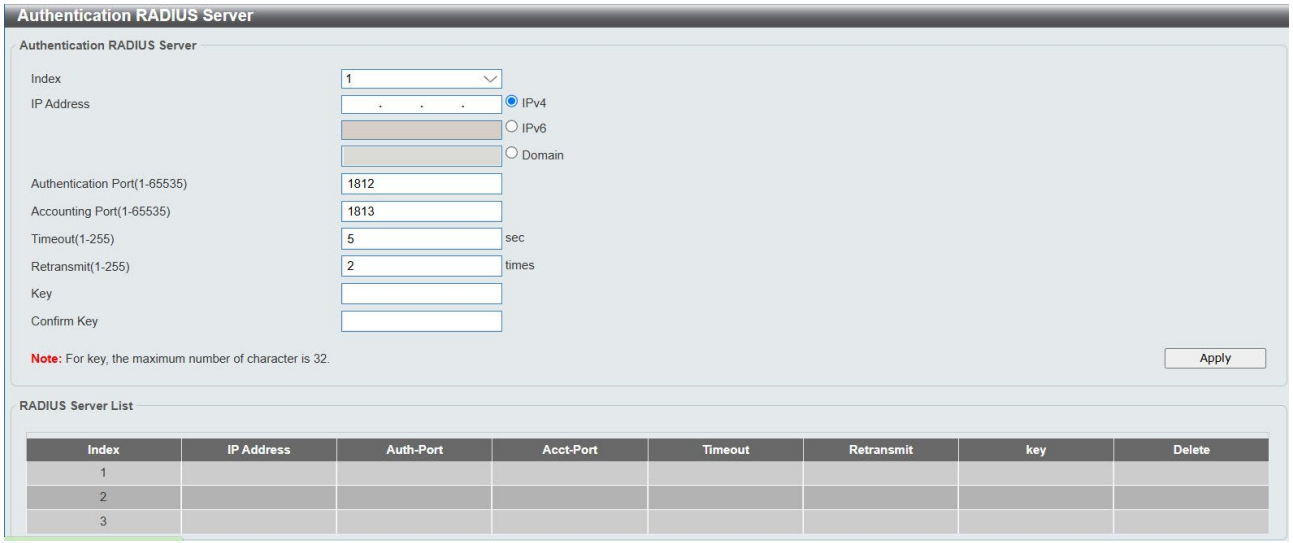


Figure 4.162 - Security > 802.1X > 802.1X Authentication RUDIUS

Index: Choose the desired RADIUS server to configure: 1, 2 or 3.

IP Address: Select IPv4 or IPv6 and enter the IP address.

Authentication Port (1 - 65535): Set the RADIUS authentic server(s) UDP port. The default port is 1812.

Accounting Port (1 - 65535): Set the RADIUS account server(s) UDP port. The default port is 1813.

Timeout (1 – 255 sec): This field will set the time the Switch will wait for a response of authentication from the user. The user may set a time between *1* and *255* seconds. The default setting is *5* seconds.

Retransmit (1 – 255 times): This command will configure the maximum number of times the Switch will accept authentication attempts. Users failing to be authenticated after the set amount of attempts will be denied access to the Switch and will be locked out of further authentication attempts. Command line interface users will have to wait 60 seconds before another authentication attempt. Telnet and web users will be disconnected from the Switch. The user may set the number of attempts from *1* to *255*. The default setting is *2*.

Key: Set the key the same as that of the RADIUS server.

Confirm Key: Confirm the shared key is the same as that of the RADIUS server.

Click **Apply** to make the configurations take effect.

Security > 802.1X > 802.1X Guest VLAN

The 802.1X Guest VLAN page allows user to set a Guest VLAN, and the user must first configure a normal VLAN which can be enabled here for Guest VLAN status.

Enter the pre-configured VLAN name to create as a Guest 802.1X VLAN and select the port or ports. Click **Apply** to implement the settings.

Figure 4.163 - Security > 802.1X > 802.1X Guest VLAN

Security > MAC Address Table > Static MAC

This feature provides two distinct functions. The **Disable Auto Learning** table allows turning off the function of learning MAC address automatically, if a port isn't specified as an uplink port (for example, connects to a DHCP Server or Gateway). By default, this feature is Off (disabled).

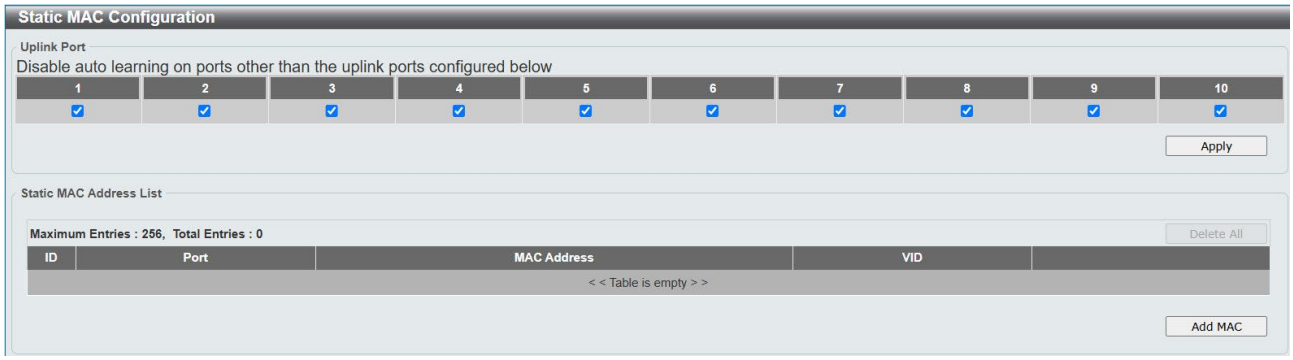


Figure 4.164 - Security > MAC Address Table > Static Mac Address

To initiate the removal of auto-learning for any of the uplink ports, click **On** to enable this feature, and then select the port(s) for auto learning to be disabled.

The **Static MAC Address List** table displays the static MAC addresses connected, as well as the VID. Click **Add Mac** to add a new MAC address, user also need to select the assigned Port number, enter both the Mac Address and VID and Click **Apply**. Click **Delete** to remove one entry or click **Delete all** to clear the list. User can also copy a learned MAC address from **Dynamic Forwarding Table** (please refer to **Security > MAC Address Table > Dynamic Forwarding Table** for details).

By disabling Auto Learning capability and specify the static MAC addresses, the network is protected from potential threats like hackers because traffic from illegal MAC addresses will not be forwarded by the Switch.

Click **Add MAC** button, select the **Port, VID** and enter the **MAC address** then click **Apply** to add a new MAC address.

Figure 4.165 - Security > MAC Address Table > Static Mac Address-add MAC

Security > MAC Address Table > Dynamic Forwarding Table

This allows the Switch's dynamic MAC address forwarding table to be viewed. When the Switch learns an association between a MAC address and a port number, it makes an entry into its forwarding table. These entries are then used to forward packets through the Switch.

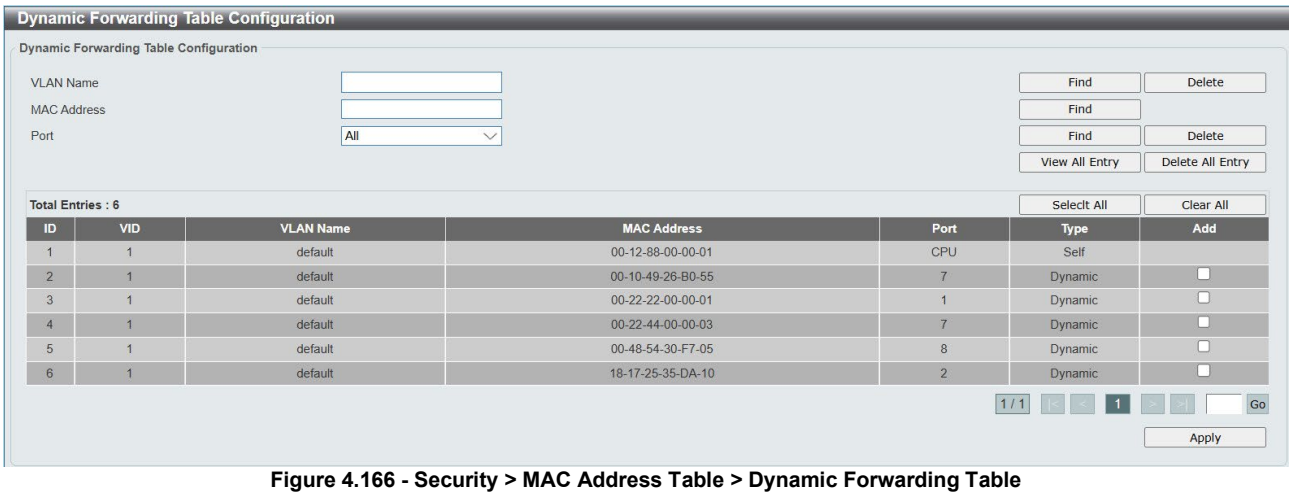


Figure 4.166 - Security > MAC Address Table > Dynamic Forwarding Table

VLAN Name: Enter a VLAN Name by which to browse the forwarding table.

MAC Address: Enter a MAC address by which to browse the forwarding table.

Port: Select the port or all ports by using the corresponding pull-down menu.

Find: Allows the user to move to a sector of the database corresponding to a user defined port, VLAN or MAC address.

VID: The VLAN ID of the VLAN of which the port is a member.

MAC Address: The MAC address entered into the address table.

Port: The port to which the MAC address above corresponds.

Type: Describes the method which the Switch discovered the MAC address. The possible entries are Dynamic, Self, and Static.

View All Entry: Clicking this button will allow the user to view all entries of the address table.

Security > MAC Address Table > Auto Learning Vlan Settings

The Auto Learning Vlan Settings page allows user to enable or disable the auto learning VLAN feature.

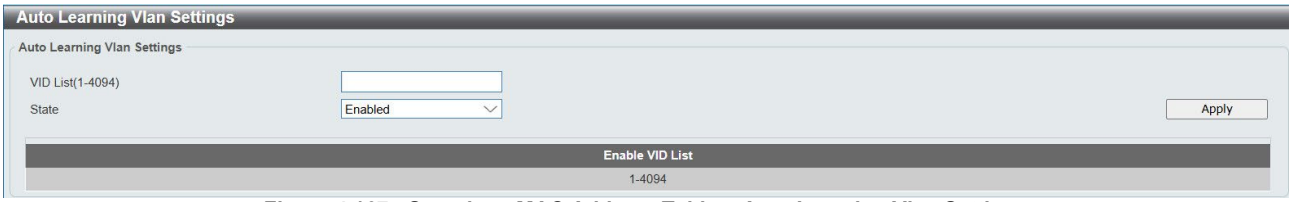


Figure 4.167 - Security > MAC Address Table > Auto Learning Vlan Settings

VLAN List (1-4094): Enter the VID.

State: Specifies to enable or disable the auto learning VLAN state.

Click **Apply** to make the configurations take effect.

Security > Access Authentication Control > Enable Admin

Users who have logged on to the Switch on user (or lower) privilege can be promoted to administrator privilege by “Enable Admin” feature. To gain the authentication, the particular protocols (local, TACACS+ or Radius) can be configured in “Enable Method Lists”

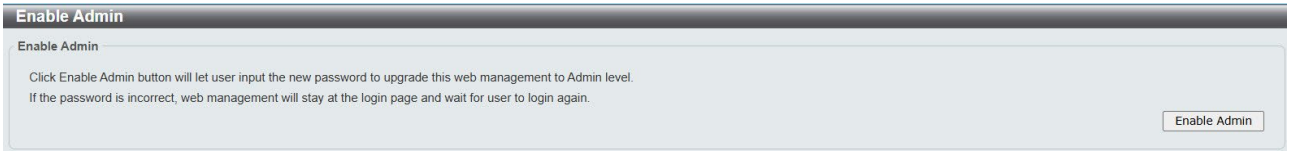


Figure 4.168 - Security > Access Authentication Control > Enable Admin

By clicking the **Enable Admin** button, the web page automatically redirected to Login page for password as shown:

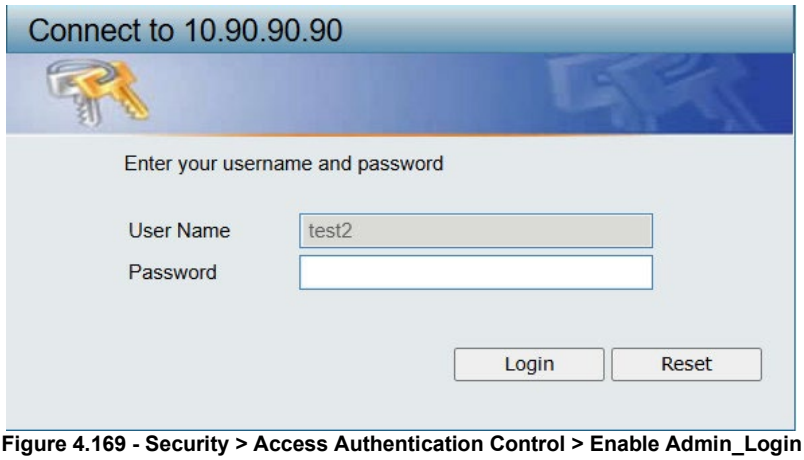


Figure 4.169 - Security > Access Authentication Control > Enable Admin_Login

Security > Access Authentication Control > Authentication Policy Settings

This feature will enable an administrator-defined authentication policy for users trying to access the Switch. When enabled, the device will check the Login Method List and choose a technique for user authentication upon login.

Figure 4.170 – Security > Access Authentication control > Authentication Policy Settings

Authentication Policy: Use the pull-down menu to enable or disable the Authentication Policy on the Switch.

Response Timeout (0 - 255): This field will set the time the Switch will wait for a response of authentication from the user. The user may set a time between *0* and *255* seconds. The default setting is *30* seconds.

User attempts (1 - 255): This command will configure the maximum number of times the Switch will accept authentication attempts. Users failing to be authenticated after the set amount of attempts will be denied access to the Switch and will be locked out of further authentication attempts. Command line interface users will have to wait 60 seconds before another authentication attempt. Telnet and web users will be disconnected from the Switch. The user may set the number of attempts from *1* to *255*. The default setting is *3*.

Click **Apply** to make the configurations take effect.

Security > Access Authentication Control > Application Authentication Settings

The Application Authentication Settings page allows user to configure switch configuration applications (Console, Telnet, SSH, HTTP) for login at the user level and at the administration level (Enable Admin) utilizing a previously configured method list.

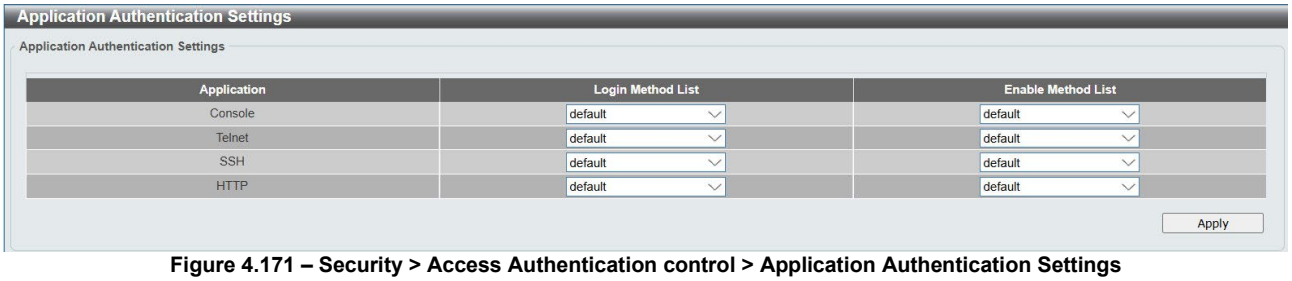


Figure 4.171 – Security > Access Authentication control > Application Authentication Settings

Application: Lists the configuration applications on the Switch. The user may configure the Login Method List and Enable Method List for authentication for Console, Telnet application, SSH and the WEB (HTTP) application.

Login Method List: Using the pull-down menu, configure an application for normal login on the user level, utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user.

Enable Method List: Using the pull-down menu, configure an application for normal login on the user level, utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user.

Click **Apply** to implement configuration changes.

Security > Access Authentication Control > Authentication Server Group

A server group is a technique used to group TACACS+ and RADIUS server hosts into user-defined categories for authentication using method lists. The user may define the type of server group by protocol or by previously defined server group. The Switch has three built-in Authentication Server Groups that cannot be removed but can be modified.

To add a user-defined group to the list, click the **Add** button in the **Authentication Server Group** page.

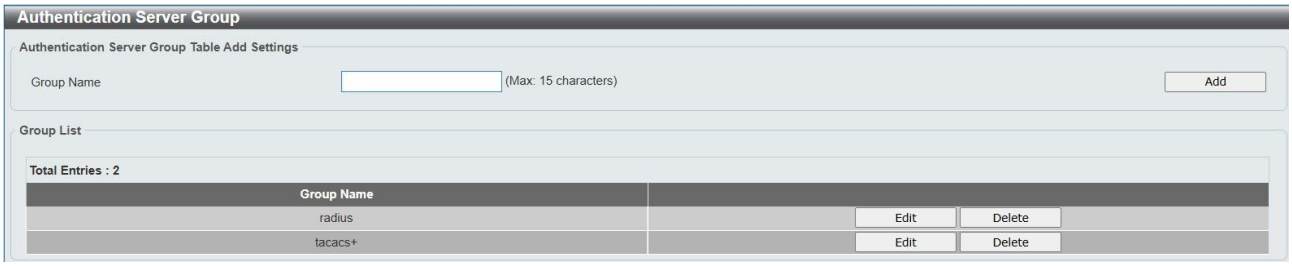


Figure 4.172 – Security > Access Authentication control > Authentication Server Group

Simply enter a group name of no more than 15 alphanumeric characters to define the user group to add. After clicking **Apply**, the new user-defined group will be displayed in the **Server Group** table. Here, it can be configured as the user desires.

F

The Switch has two built-in Authentication Server Groups that cannot be removed but can be modified. To modify a particular group, click **Edit** button, which will then display the following window.

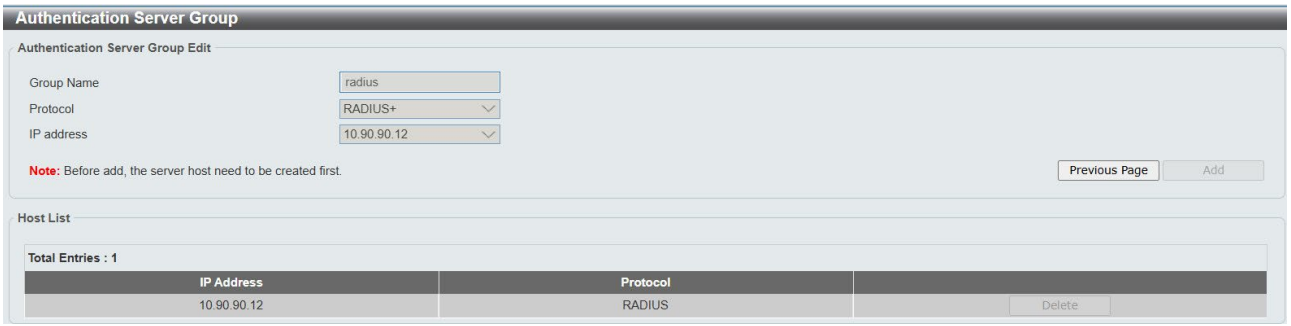


Figure 4.173 – Security > Access Authentication control > Authentication Server Group-Edit

Select **Group Name**, **Protocol** and **IP address** then click **Add** to implement the changes.

NOTE: The user must configure Authentication Server Hosts using the Authentication Server Hosts page before adding hosts to the list. Authentication Server Hosts must be configured for their specific protocol on a remote centralized server before this function can work properly.

NOTE: The two built in server groups can only have server hosts running the same TACACS

daemon. The TACACS+ and RADIUS protocols are separate entities and are not compatible with each other.

Security > Access Authentication Control > Authentication Server

This Authentication Server page will set user-defined **Authentication Server Hosts** for the TACACS+ and RADIUS security protocols on the Switch. When a user attempts to access the Switch with Authentication Policy enabled, the Switch will send authentication packets to a remote TACACS+ or RADIUS server host on a remote host. The TACACS+ or RADIUS server host will then verify or deny the request and return the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS+ and RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is *16*.

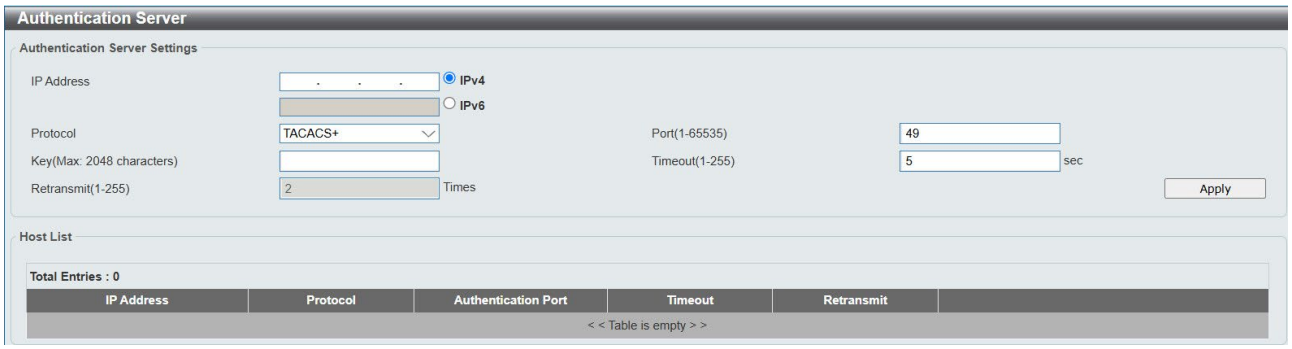


Figure 4.174 – Security > Access Authentication control > Authentication Server

To add an Authentication Server Host:

IP Address: Select IPv4 or IPv6 and enter the IP address.

Protocol: The protocol used by the server host. The user may choose one of the following:

TACACS+ – Enter this parameter if the server host utilizes the TACACS+ protocol.

RADIUS – Enter this parameter if the server host utilizes the RADIUS protocol.

Key: Authentication key to be shared with a configured TACACS+ or RADIUS servers only. Specify an alphanumeric string up to *254* characters.

Port (1 - 65535): Enter a number between *1* and *65535* to define the virtual port number of the authentication protocol on a server host. The default port number is *49* for TACACS+ server and *1813* for RADIUS servers but the user may set a unique port number for higher security.

Timeout (1 - 255): Enter the time in seconds the Switch will wait for the server host to reply to an authentication request. The default value is *5* seconds.

Retransmit (1 - 255): Enter the value in the retransmit field to change how many times the device will resend an authentication request when the TACACS server does not respond.

Click **Apply** to add a new Authentication Server Host.

NOTE: More than one authentication protocol can be run on the same physical server host.

Security > Access Authentication Control > Login Method Lists

This feature will configure a user-defined or default Login Method List of authentication techniques for users logging on to the Switch. Successful login using any of these techniques will give the user a "**User**" privilege only. To upgrade his or her status to the administrator level, the user must use the **Enable Admin** window, in which the user must enter a previously configured password, set by the administrator.

The Switch contains one Method List that is set and cannot be removed, yet can be modified. To delete a Login Method List defined by the user, click **Delete** button. To modify the Login Method List, click **Edit** button.

Figure 4.175 – Security > Access Authentication control > Login Method Lists

To define a Login Method List, set the following parameters and click **Apply**:

Method List Name: Enter a method list name defined by the user of up to *15* characters.

Priority 1, 2, 3, 4: The user may add one, or a combination of up to four of the following authentication methods to this method list:

none – Adding this parameter will require an authentication to access the Switch.

local – Adding this parameter will require the user to be authenticated using the local user account database on the Switch.

tacacs+ – Adding this parameter will require the user to be authenticated using the TACACS+ protocol from a remote TACACS+ server.

radius – Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server.

Security > Access Authentication Control > Enable Method Lists

The Enable Method Lists page is used to set up Method Lists to promote users with user level privileges to Administrator (Admin) level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight Enable Method Lists can be implemented on the Switch, one of which is a default Enable Method List. This default Enable Method List cannot be deleted but can be configured.

To delete an Enable Method List defined by the use, click Delete button to the entry desired to be deleted. To modify and Enable Method List, click **Edit** button to make the changes and click **Apply**.

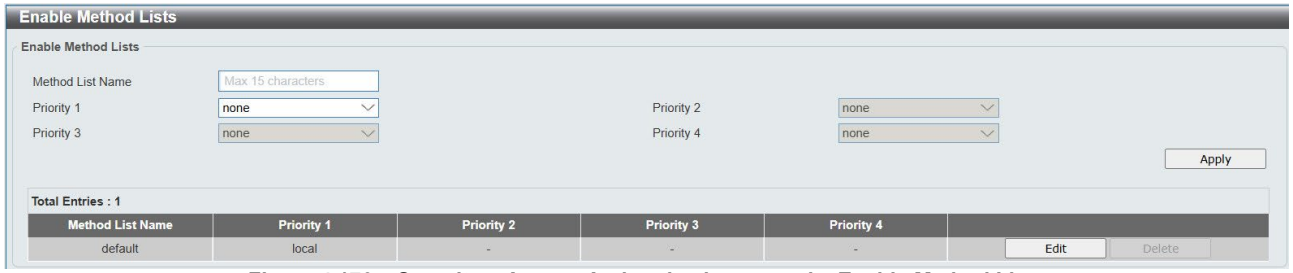


Figure 4.176 – Security > Access Authentication control > Enable Method Lists

To define an Enable Login Method List, set the following parameter and click **Apply**:

Method List Name: Enter a method list name defined by the user of up to *15* characters.

Priority 1, 2, 3, 4: The user may add one, or a combination of up to four of the following authentication methods to this method list:

none – Adding this parameter will require an authentication to access the Switch.

local – Adding this parameter will require the user to be authenticated using the local user account database on the Switch.

tacacs+ – Adding this parameter will require the user to be authenticated using the TACACS+ protocol from a remote TACACS+ server.

radius – Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server.

Security > Access Authentication Control > Local Enable Password Settings

The Local Enable Password Settings page allows user to configure the locally enabled password. When a user chooses the "local_enable" method to promote user level privileges to administrator privileges, he or she will be prompted to enter the password configured here that is locally set on the Switch.

Figure 4.177 – Security > Access Authentication control > Local Enable Password Settings

To set the Local Enable Password, set the following parameters and click **Apply**:

Old Local Enable Password: If a password was previously configured for this entry, enter it here in order to change it to a new password.

New Local Enable Password: Enter the new password that user specified for the Switch to authenticate users attempting to access Administrator Level privileges on the Switch. The user may set a password of up to 15 characters.

Confirm Local Enable Password: Confirm the new password entered above. Entering a different password here from the one set in the New Local Enabled field will result in a fail message.

Security > Traffic Segmentation

This feature provides administrators to limit traffic flow from a single port to a group of ports on a single Switch. This method of segmenting the flow of traffic is similar to using VLANs to limit traffic, but is more restrictive.

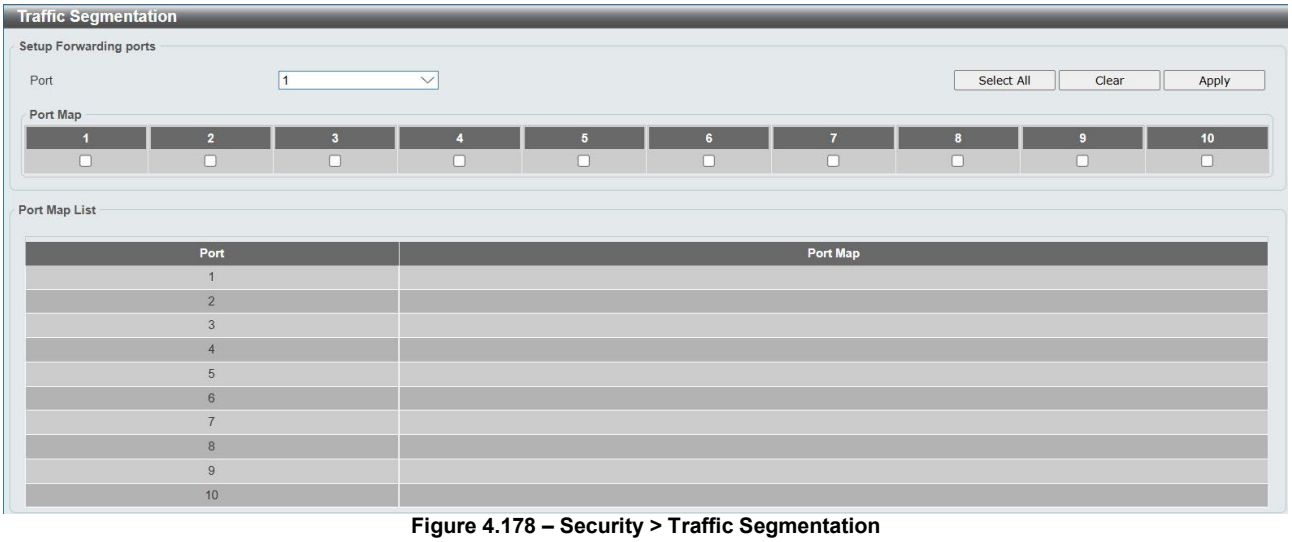


Figure 4.178 – Security > Traffic Segmentation

To configure traffic segmentation specify a port or All ports from the switch, using the **Port** pull-down menu and select **Port Map** then click **Apply** to enter the settings into the Switch's **Traffic Segmentation** table.

Click **Select All** to select all port maps or click **Clear** button to uncheck port maps.

Security > DoS Prevention Settings

The DoS is a malicious attack against a network. This attack is designed to stop a network from functioning by flooding it with useless traffic. Symptoms of a malicious attack include the inability to access any web site or a particular web site being unavailable and network performance slowing down.

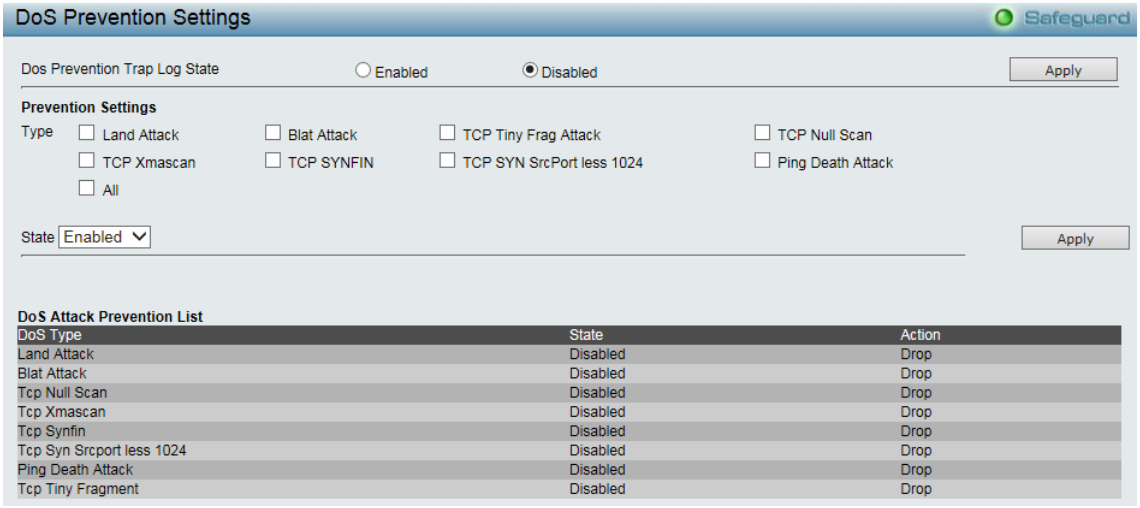


Figure 4.179 – Security > DoS Prevention Settings

Prevention Settings:

Type: Select the attack types to be prevented. The types are *Land Attack, TCP Tine Frag Attack, TCP Null Scan, TCP Xmascan, TCP SYNFIN, TCP SYN SrcPortless 1024, Ping Death Attack* or *All*.

State: Specify the state to be enabled or disabled.

Click **Apply** to make the configurations take effect.

Security > DHCP Server Screening > DHCP Server Screening Port Settings

DHCP Server Screening function allows user to restrict the illegal DHCP server by discarding the DHCP service from distrusted ports. This page allows user to configure the DHCP Server Screening state for each port and designed trusted DHCP server IP address.

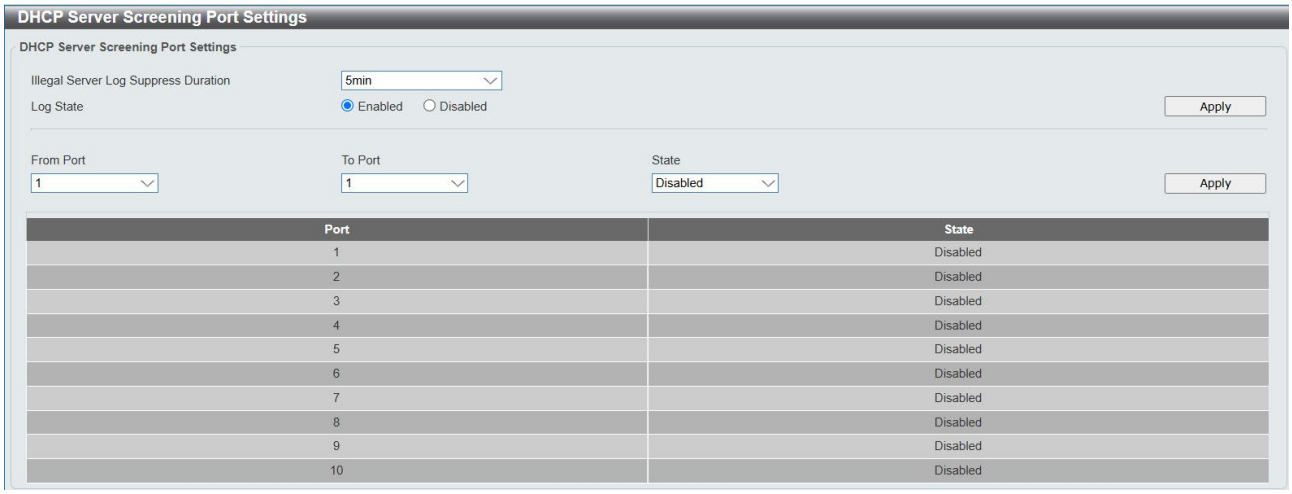


Figure 4.180– Security > DHCP Server Screening > DHCP Server Screening Port Settings

Illegal Server Log Suppress Duration: Specifies the illegal server log suppress duration for DHCP server screening port.

From Port/ To Port: Specifies a range of ports to be DHCP server screening port.

Log State: Specifies the logging mechanism to be enabled or disable for DHCP server screening events.

State: Specifies the DHCP server screening port to be enabled or disabled.

Click **Apply** to make the configurations take effect.

Security > DHCP Server Screening > DHCP Server Screening VLAN Settings

The DHCP Server Screening VLAN Settings page allows the user to view and configure the VLAN state for the DHCP Server Screening.

Figure 4.181– Security > DHCP Server Screening > DHCP Server Screening VLAN Settings

VID List (1-4094): Specifies the VLAN ID to be configured.

State: Specifies to enable or disable the DHCP Server Screening for the specified VLAN.

Click **Apply** to make the configurations take effect.

Security > DHCP Server Screening > Filter DHCP Server

This Filter DHCP Server page allows user to designed trusted DHCP Server IP address and Client MAC Address.

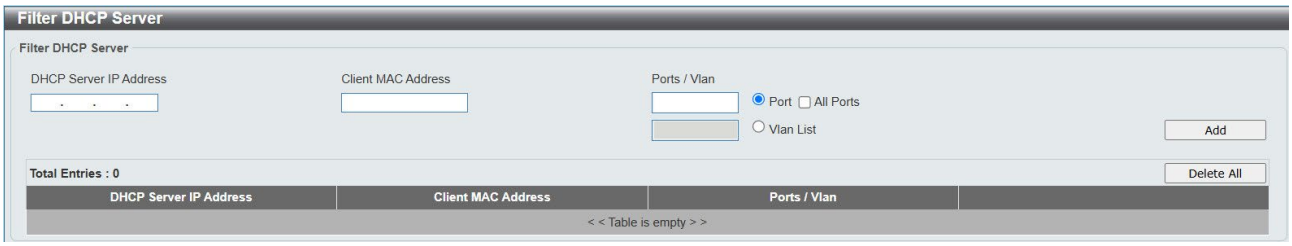


Figure 4.182 – Security > DHCP Server Screening > Filter DHCP Server

To add the DHCP Trusted DHCP Server, set the following fields and click **Add**. Or click **Delete All** to remove all DHCP Server IP Address.

DHCP Server IP Address: Specifies the IP address of the DHCP server to be trusted.

Client MAC Address: Specify the MAC address of the client which allowed the requested IP address from the DHCP Address server.

Ports/VLAN: Enter the list of ports to use the given filter DHCP server entry. Tick the **All Ports** check box to select all ports. Or click the **VLAN List** and enter the VLAN.

Security > DHCP Server Screening > Filter DHCPv6 Server

This Filter DHCPv6 Server page allows user to designed trusted DHCPv6 Server IP address.

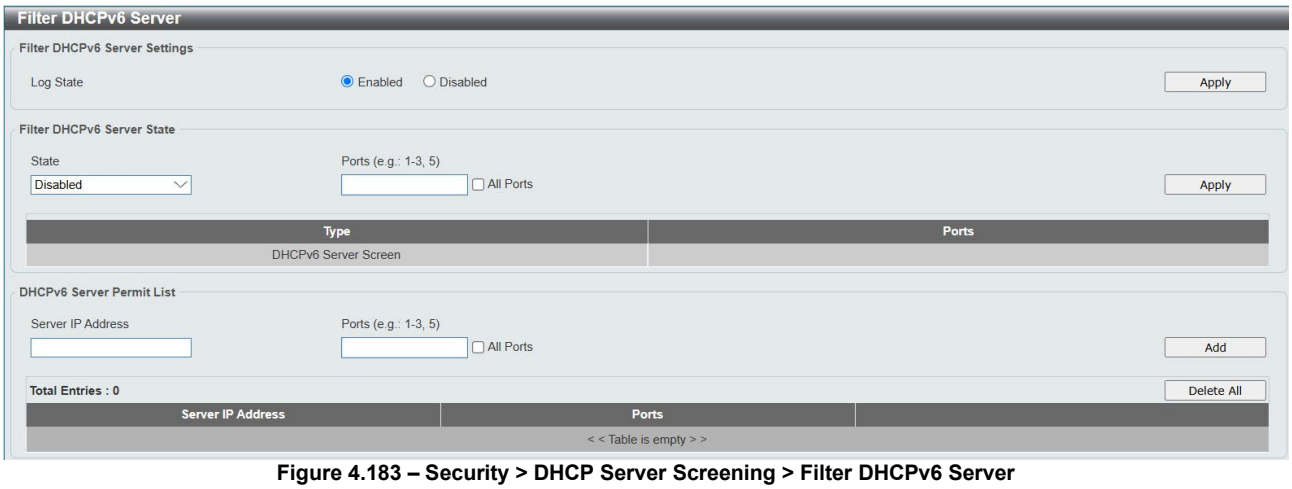


Figure 4.183 – Security > DHCP Server Screening > Filter DHCPv6 Server

Log State: Specify to enable or disable the log state for filter DHCPv6 server.
Click **Apply** to makes effects.

Filter DHCPv6 Server State:
Ports: Specify the ports, or select **All Ports**.
State: Specify to enable or disable the filter DHCPv6 server state for the specified ports.
Click **Apply** to makes effects.

DHCPv6 Server Permit List:
Server IP Address: Specify the IP address for the DHCPv6 server.
Ports: Specify the ports, or select **All Ports**.

Click the **Add** button to add a DHCPv6 server permit list or click the **Delete** button to remove a DHCPv6 server permit list.
Click the **Delete All** button to remove all DHCPv6 server permit list.

Security > DHCP Server Screening > Filter ICMPv6
This **Filter ICMPv6** page allows user to designed trusted ICMPv6 Server IP address.

Figure 4.184 – Security > DHCP Server Screening > Filter ICMPv6

Log State: Specify to enable or disable the log state for filter ICMPv6 server.
Click **Apply** to makes effects.

Filter ICMPv6 RA_All_Node State:
Ports: Specify the ports, or select **All Ports**.
State: Specify to enable or disable the filter ICMPv6 RA_All_Node state for the specified ports.
Click **Apply** to makes effects.

ICMPv6 RA_All_Node Permit:
Server IP Address: Specify the IP address for the ICMPv6 RA_All_Node Permit.
Ports: Specify the ports, or select **All Ports**.

Click the **Add** button to add an ICMPv6 RA_All_Node permit list or click the **Delete** button to remove a ICMPv6 RA_All_Node permit list.
Click the **Delete All** button to remove all ICMPv6 RA_All_Node permit list.

Security > SSH Settings > SSH Settings

SSH is an abbreviation of Secure Shell, which is a program allowing secure remote login and secure network services over an insecure network. It allows a secure login to remote host computers, a safe method of executing commands on a remote end node, and will provide secure encrypted and authenticated communication between two non-trusted hosts. SSH, with its array of unmatched security features is an essential tool in today's networking environment. It is a powerful guardian against numerous existing security hazards that now threaten network communications.

Figure 4.185 – Security > SSH Settings > SSH Settings

To configure the SSH server on the Switch, modify the following parameters and click **Apply**:

SSH State: Enabled or Disabled SSH on the Switch. The default is *Disabled*.

Max Session (1 - 4): Enter a value between *1* and 4 to set the number of users that may simultaneously access the Switch. The default setting is *1*.

Connection Timeout (120 - 600): Allows the user to set the connection timeout. The use may set a time between *120* and *600* seconds. The default setting is *120* seconds.

Authfail Attempts (2 - 20): Allows the Administrator to set the maximum number of attempts that a user may try to log on to the SSH Server utilizing the SSH authentication. After the maximum number of attempts has been exceeded, the Switch will be disconnected and the user must reconnect to the Switch to attempt another login. The number of maximum attempts may be set between *2* and *20*. The default setting is *2*.

Rekey Timeout: Using the pull-down menu uses this field to set the time period that the Switch will change the security shell encryptions. The available options are *Never*, *10 min*, *30 min*, and *60 min.* The default setting is *60 min.*

Security > SSH Settings > SSH Authmode and Algorithm Settings

The SSH Authentication and Algorithm Settings page allows user to configure the desired types of SSH algorithms used for authentication encryption.

Figure 4.186 – Security > SSH Settings > SSH Authmode and Algorithm Settings

SSH Authentication Mode Settings:

Password: Allows user to use a locally configured password for authentication on the Switch.

Public Key: This parameter may be enabled if the administrator wishes to use a public key configuration set on a SSH server, for authentication on the Switch.

Host Based: This parameter may be enabled if the administrator wishes to use a host computer for authentication. This parameter is intended for Linux users requiring SSH authentication techniques and the host computer is running the Linux operating system with a SSH program previously installed.

Encryption Algorithm:

3DES-CBC: Use the check box to enable or disable the Triple Data Encryption Standard encryption algorithm with Cipher Block Chaining. The default is enabled.

Data Integrity Algorithm:

HMAC-MD5: Use the check box to enable the supports of hash for message Authentication Code (HMAC) MD5 Message Digest (MD5) mechanism.

HMAC-SHA1: Use the check box to enable the supports of hash for message Authentication Code (HMAC) Secure Hash Algorithm (SHA) mechanism.

Public Key Algorithm:

HMAC-RSA: Use the check box to enable the supports of Hash for Message Authentication Code (HMAC) mechanism utilizing the RSA encryption algorithm.

Click **Apply** to make the configurations take effect.

Security > SSH Settings > SSH User Authentication Lists

The SSH User Authentication Lists page is used to configure parameters for users attempting to access the Switch through SSH.

Figure 4.187 – Security > SSH Settings > SSH User Authentication Lists

The user may view the following parameters:

User Name: A name of no more than *15* characters to identify the SSH user. This User Name must be a previously configured user account on the Switch.

Auth. Mode: The administrator may choose one of the following to set the authorization for users attempting to access the Switch.

Host Based – This parameter should be chosen if the administrator wishes to use a remote SSH server for authentication purposes.

Password – This parameter should be chosen if the administrator wishes to use an administrator-defined password for authentication. Upon entry of this parameter, the Switch will prompt the administrator for a password, and then to re-type the password for confirmation.

Public Key – This parameter should be chosen if the administrator wishes to use the public key on an SSH server for authentication.

Host Name: Enter an alphanumeric string of no more than *32* characters to identify the remote SSH user. This parameter is only used in conjunction with the *Host Based* choice in the Auth. Mode field.

Host IP: Enter the corresponding IP address of the SSH user. This parameter is only used in conjunction with the *Host Based* choice in the Auth. Mode field.

MAC-based Access Control (MAC)

MAC-based Access Control is a method to authenticate and authorize access using either a port or host. For port-based MAC, the method decides port access rights, while for host-based MAC, the method determines the MAC access rights.

A MAC user must be authenticated before being granted access to a network. Both local authentication and remote RADIUS server authentication methods are supported. In M AC-based Access Control, M AC user information in a local database or a RADIUS server data base is searched for authentication. Following the authentication result, users achieve different levels of Authorization.

Notes about MAC-based Access Control

There are certain limitations and regulations regarding MAC-based Access Control:

1. Once this feature is enabled for a port, the Switch will clear the FDB of that port.

2. If a port is granted clearance for a MAC address in a VLAN that is not a Guest VLAN, other MAC addresses on that port must be authenticated for access and otherwise will be blocked by the Switch.

3. A port accepts a maximum of two hundred authenticated MAC addresses per physical port of a VLAN that is not a Guest VLAN. Other MAC addresses attempting authentication on a port with the maximum number of authenticated MAC addresses will be blocked.

4. Ports that have been enabled for Link Aggregation, Port Security, or GVRP authentication cannot be enabled for MAC-based Authentication.

Security > MAC-based Access Control (MAC) > MAC-based Access Control Settings

The MAC-based Access Control Settings page is used to configure the MAC Settings for the MA C-based Access Control function on the Switch. The user can set the running state, method of authentication, RA DIUS password, view the Guest VLAN configuration to be associated with the MAC-based Access Control function of the Switch, and configure ports to be enabled or disabled for the MAC-based Access Control feature of the Switch. Please rem ember, ports enabled for certain other features, listed previously, cannot be enabled for MAC-based Access Control.

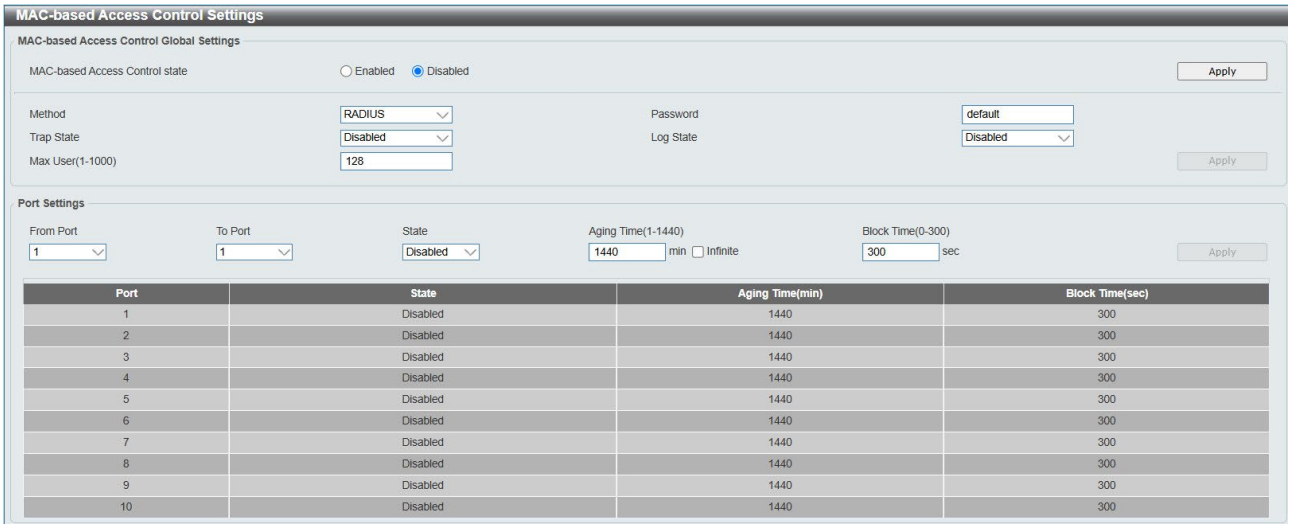


Figure 4.188 – Security > MAC-based Access Control (MAC) > MAC-based Access Control Settings

MAC-based Access Control Global Settings:

MAC-based Access Control State: Enable or disable the MAC-based Access Control function on the Switch. Click **Apply** button to take effect.

Configuring the MAC Authentication Method:

Method: Specify the type of authentication to be used.

> ***Local* –** Use this method to utilize the locally set MAC address database as the authenticator for MAC-based Access Control.
>
> ***RADIUS* –** Use this method to utilize a remote RADIUS server as the authenticator for MAC-based Access Control.

Password: Enter the password for the RADIUS server, which is to be used for packets being sent requesting authentication. The default password is "default".

Trap State: Enable or disable the MAC-based Access Control trap state. The default is disabled.

Log State: Enable or disable the MAC-based Access Control log state. The default is disabled.

Max User (1-1000): Specify the max users. The value is between 1~1000, and the default is 128.

Click the **Apply** button to implement the configuration changes.

Port Settings:

From Port / To Port: The ports of range to be configured for MAC-based Access Control.

State: Enable or disable MAC-based Access Control on the port or range of ports.

Aging Time (1-1440): Specify the aging time. The default is 1440.

Block Time (0-300): Specify the block time. The default is 300 and the value is between 1 to 300 seconds.

Click the **Apply** button to implement the configuration changes.

Security > MAC-based Access Control (MAC) > MAC-based Access Control Local Settings

Users can set a list of M AC addresses, along with their corresponding target VLAN, which will be authenticated for the Switch. Once a queried MAC address is matched in this window, it will be placed in the VLAN associated with it he re. The Switch administrator may enter up to 128 MAC addresses to be authenticated using the local method configured here.

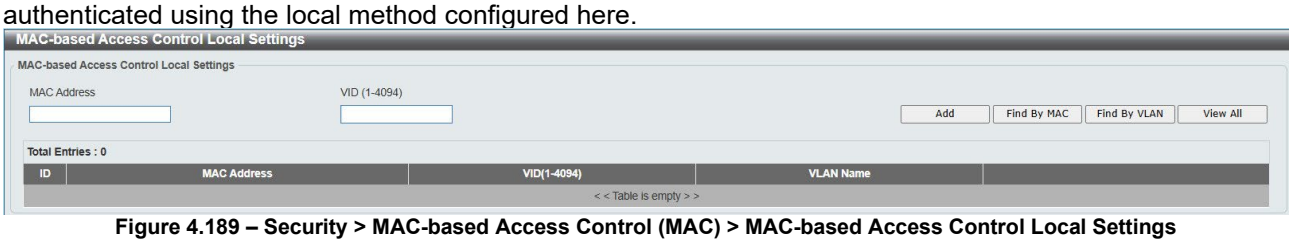


Figure 4.189 – Security > MAC-based Access Control (MAC) > MAC-based Access Control Local Settings

To add a MAC address to the local authentication list, enter the MAC address and the target VLAN ID into their appropriate fields and click **Add**. To search for a specific MAC Address, enter the MAC address in the first field and then click the **Find By MAC** button. To search for a specific VLAN Name, enter the VID in the second field and then click the **Find By VLAN** button.

Security > MAC-based Access Control (MAC) > MAC-based Access Control Authentication State

The MAC-based Access Control Authentication State page allows user to configure the authentication state of ports.

Figure 4.190 – Security > MAC-based Access Control (MAC) > MAC-based Access Control Authentication State

Security > Web Based Access Control > WAC Global Settings

The WAC (Web-Based Access Control) Global settings page allows user to configure WAC Global settings.

Figure 4.191 – Security > Web Access Control > WAC Global Settings

Web-based Access Control (WAC) is a feature designed to authenticate a user when the user is trying to access the Internet via the Switch. The authentication process uses the HTTP or HTTPS protocol.

WAC Global State: Select to enable or disable the Web authentication feature's global state.

Virtual IP: Select the switch IP interface. All Web authentication processes communicate with this IP address,

Virtual IPv6: Enter the virtual IPv6 address used here. If the IPv6 virtual IP is not configured, the IPv6 access cannot start a Web authentication.

Redirection Path: Enter the redirection path here. This path can be up to 128 characters long. Please enter IP format address, NOT support domain name recently.

Method: Select “Local” or “Radius” as authentication method.

HTTP(s) Port (1-65535): Enter the specific port switch would listen to authentication. Protocol available for HTTP and HTTPS.

Security > Web Access Control > WAC User Settings

The WAC (Web-Based Access Control) User settings page allows user to configure WAC user settings.

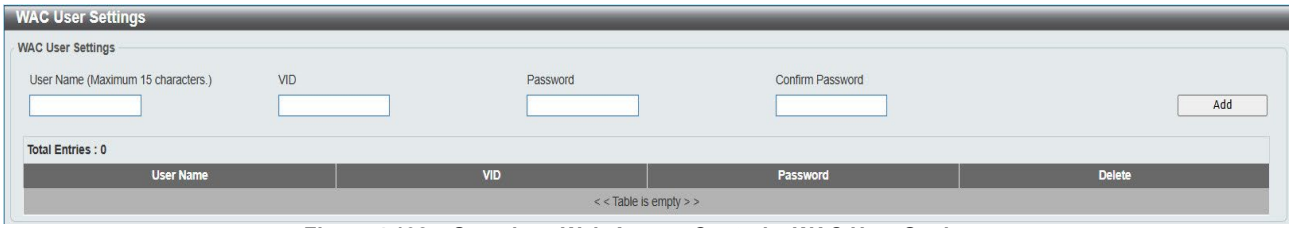


Figure 4.192 – Security > Web Access Control > WAC User Settings

User Name: Enter the username string. Supports up to 15 characters.

VID: Enter the VLAN this specific user.

Password: Enter the password string.

Confirm Password: Re-enter the password for confirmation.

Security > Web Access Control > WAC Port Settings

The WAC (Web-Based Access Control) Port settings page allows user to configure WAC port settings.

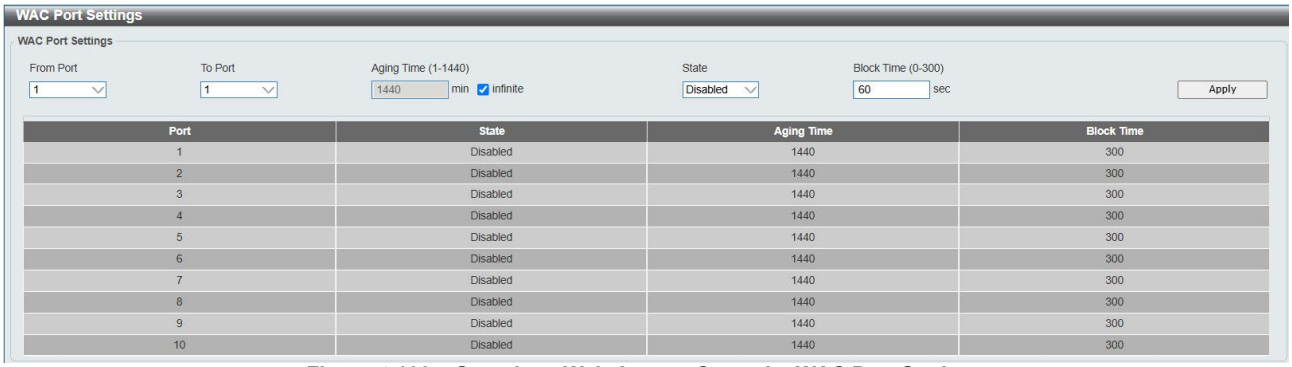


Figure 4.193 – Security > Web Access Control > WAC Port Settings

From Port / To Port: User the drop-down to specify the list of ports to be configured.

Aging Time: The specific time to remove the authenticated entry. **Infinite** is available by checked the box.

State: Select the state for **Enable** or **Disable**.

Block Time: Specify the time (in seconds) for blocking authentication failed clients.

Security > Web Access Control > WAC Authentication State

The WAC (Web-Based Access Control) Authentication State page allows user to check current authentication state.

Figure 4.194 – Security > Web Access Control > WAC Authentication State

Port List: Enter the port number and click **Find** to find the information. Click the button **Clear by Port** would remove the authentication entries in port basis and re-start the authentication process.

Click the button **Clear all host** would remove all the authentication entries and re-start the authentication process.

Monitoring > Statistics

The Statistics screen displays the status of each port packet count.

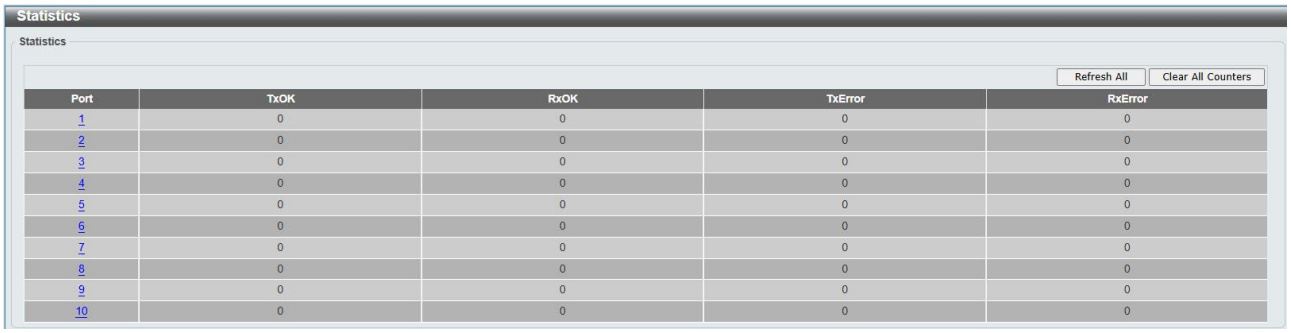


Figure 4.195 – Monitoring > Statistics

Refresh All: Renews the details collected and displayed.
Clear All: To reset the details displayed.
TxOK: Number of packets transmitted successfully.
RxOK: Number of packets received successfully.
TxError: Number of transmitted packets resulting in error.
RxError: Number of received packets resulting in error.

To view the statistics of individual ports, click one of the linked port numbers for details.

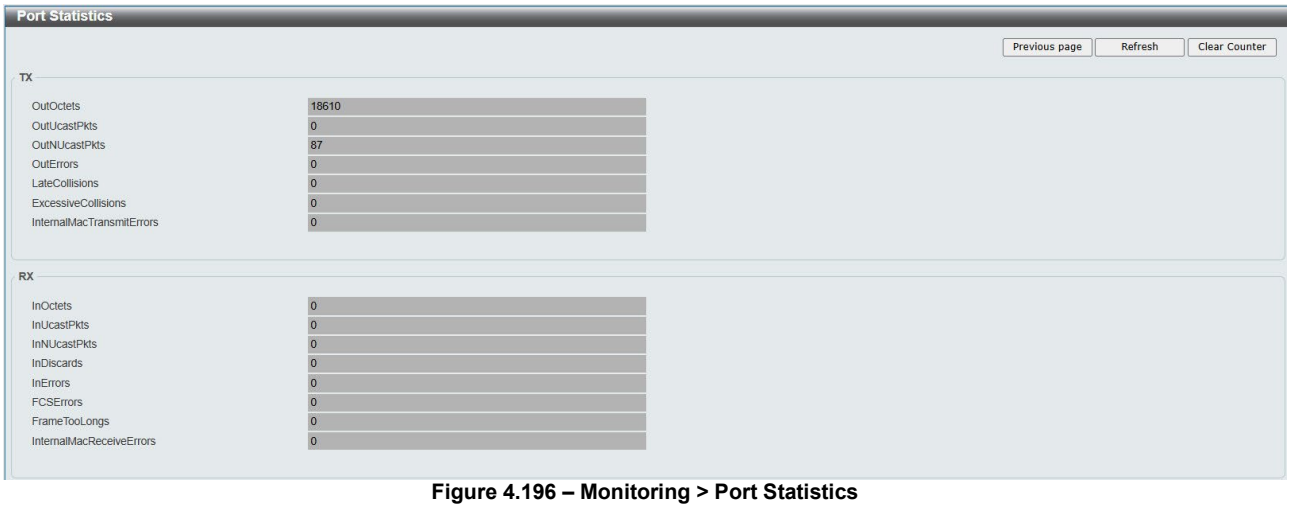


Figure 4.196 – Monitoring > Port Statistics

Previous Page: Go back to the Statistics main page.
Refresh: To renew the details collected and displayed.
Clear Counter: To reset the details displayed.

Monitoring > Session Table

The Session Table allows the user to view detailed information on the current configuration session of the Switch. Information such as the Session **ID** of the user, initial **Login Time**, **Live Time**, configuration connection **From** the Switch, **Level** and **Name** of the user are displayed. Click **Reload** to refresh this window.

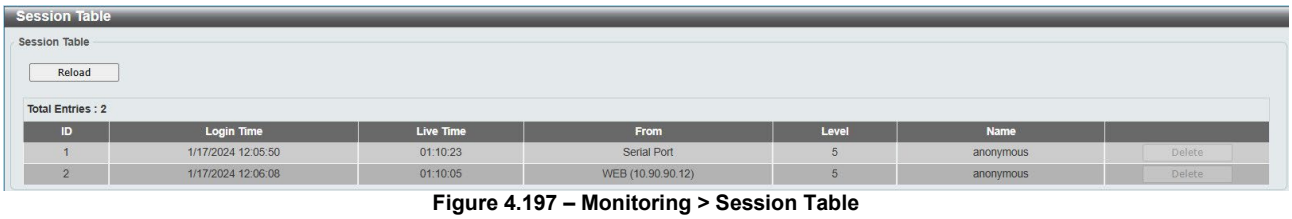


Figure 4.197 – Monitoring > Session Table

Monitoring > CPU Utilization

The **CPU Utilization** displays the percentage of the CPU being used, expressed as an integer percentage and calculated as a simple average by time interval. The window will automatically refresh with new updated statistics.

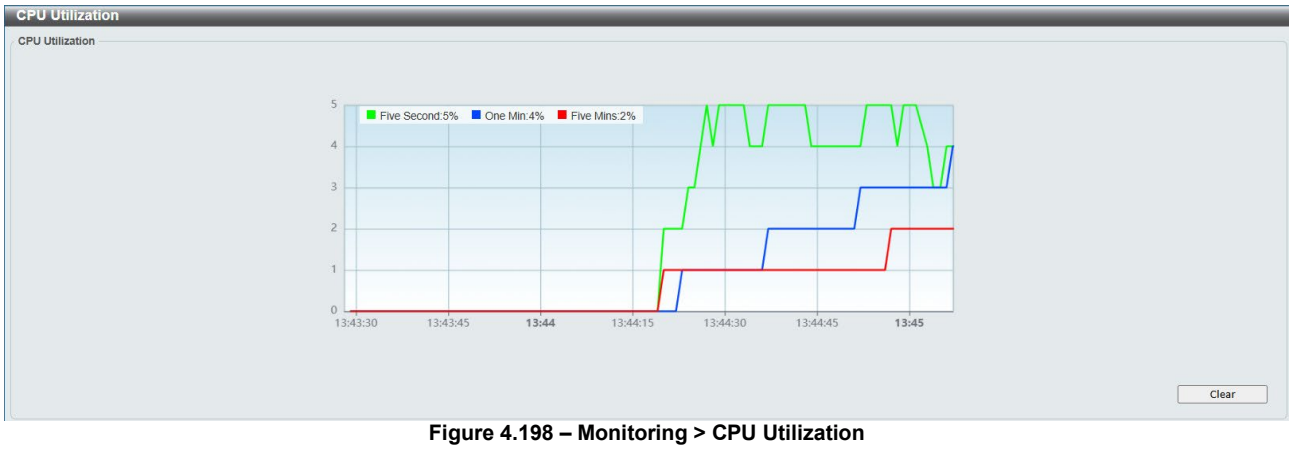


Figure 4.198 – Monitoring > CPU Utilization

Clear: Clicking this button clears all statistics counters on this window.

Monitoring > Memory Utilization

The Memory Utilization displays the percentage of the memory being used, expressed as an integer percentage and calculated as a simple average by time interval. Click **Apply** to implement the configured settings. The window will automatically refresh with new updated statistics.

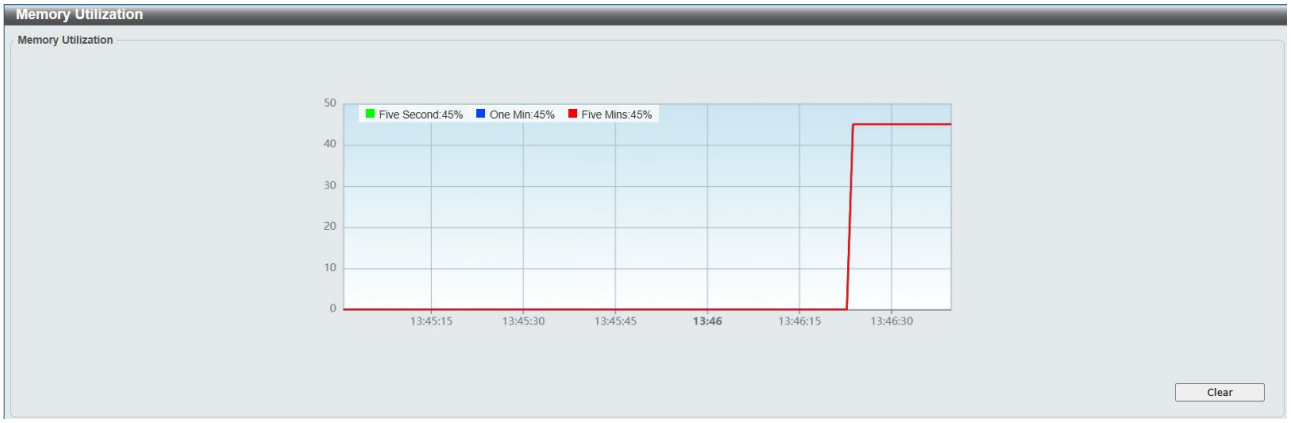


Figure 4.199 – Monitoring > Memory Utilization

The information is described as follows:

Time Interval: Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is *one* second.

Record Number: Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.

Show/Hide: Check whether to display *Five Secs*, *One Min*, and/or *Five Mins*.

Clear: Clicking this button clears all statistics counters on this window.

Monitoring > Port Utilization

The Port Utilization page displays the percentage of the total available bandwidth being used on the port.

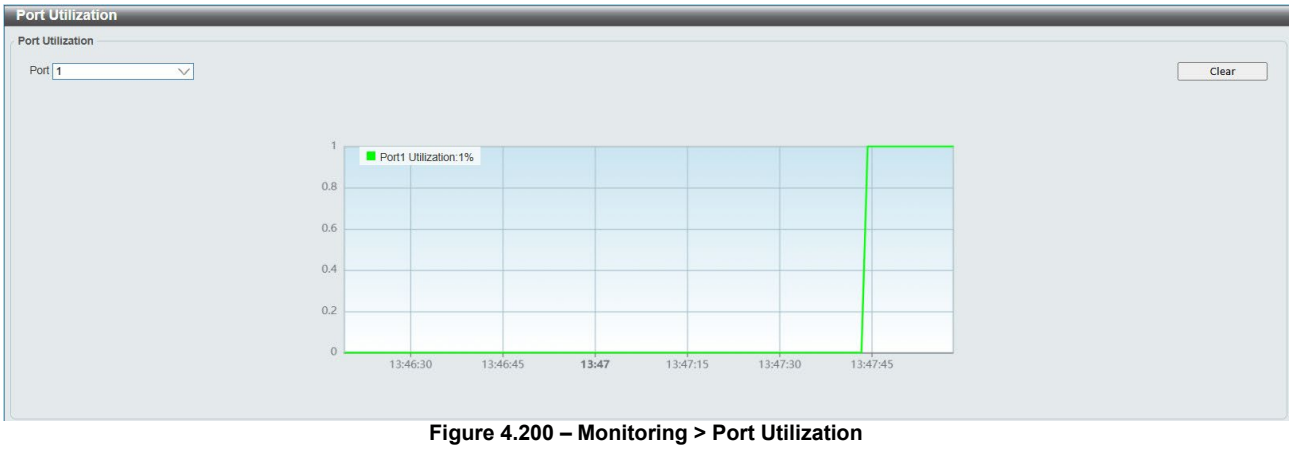


Figure 4.200 – Monitoring > Port Utilization

The user may use the real-time graphic of the Switch at the top of the web page to view utilization statistics per port by clicking on a port. Click Apply to make the configurations take effect. The following field can be set:

Time Interval: Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is *one* second.

Record Number: Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.

Show/Hide: Check whether to display Utilization.

Clear: Clicking this button clears all statistics counters on this window.

Monitoring > Packet Size

The Web Manager allows packets received by the Switch, arranged in six groups and classed by size, to be viewed as either a line graph or a table. Two windows are offered. To select a port to view these statistics for, select the port by using the **Port** pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

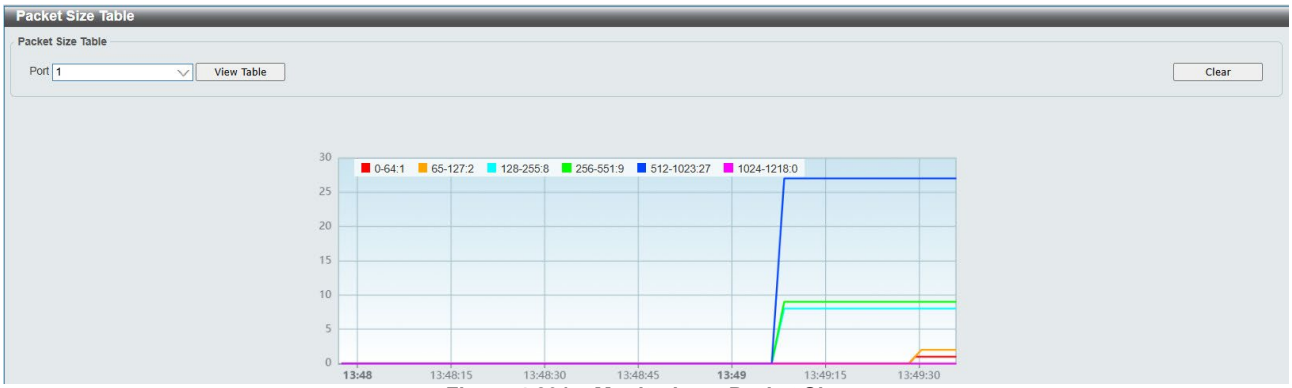


Figure 4.201 – Monitoring > Packet Size

To view the **Packet Size Analysis Table**, click the link View Table, which will show the following table:

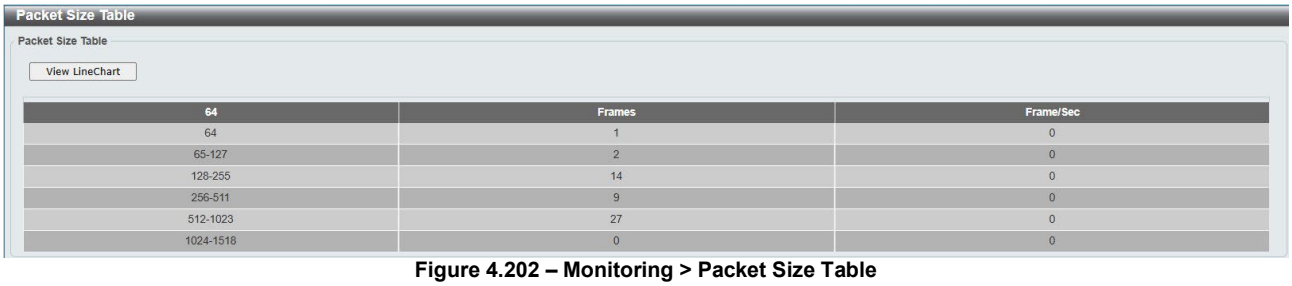


Figure 4.202 – Monitoring > Packet Size Table

The following fields can be set or viewed:

Time Interval: Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is *one* second.

Record Number: Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.

64: The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).

65-127: The total number of packets (including bad packets) received that were between *65* and *127* octets in length inclusive (excluding framing bits but including FCS octets).

128-255: The total number of packets (including bad packets) received that were between *128* and *255* octets in length inclusive (excluding framing bits but including FCS octets).

256-511: The total number of packets (including bad packets) received that were between *256* and *511* octets in length inclusive (excluding framing bits but including FCS octets).

512-1023: The total number of packets (including bad packets) received that were between *512* and *1023* octets in length inclusive (excluding framing bits but including FCS octets).

1024-1518: The total number of packets (including bad packets) received that were between *1024* and *1518* octets in length inclusive (excluding framing bits but including FCS octets).

Show/Hide: Check whether or not to display *64*, *65-127*, *128-255*, *256-511*, *512-1023*, and *1024-1518* packets received.

Clear: Clicking this button clears all statistics counters on this window.

View Table: Clicking this button instructs the Switch to display a table rather than a line graph.

View Line Chart: Clicking this button instructs the Switch to display a line graph rather than a table.

Monitoring > Packets > Transmitted (TX)

The Transmitted (TX) page displays the following graph of packets transmitted from the Switch. To select a port to view these statistics for, use the **Port** pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

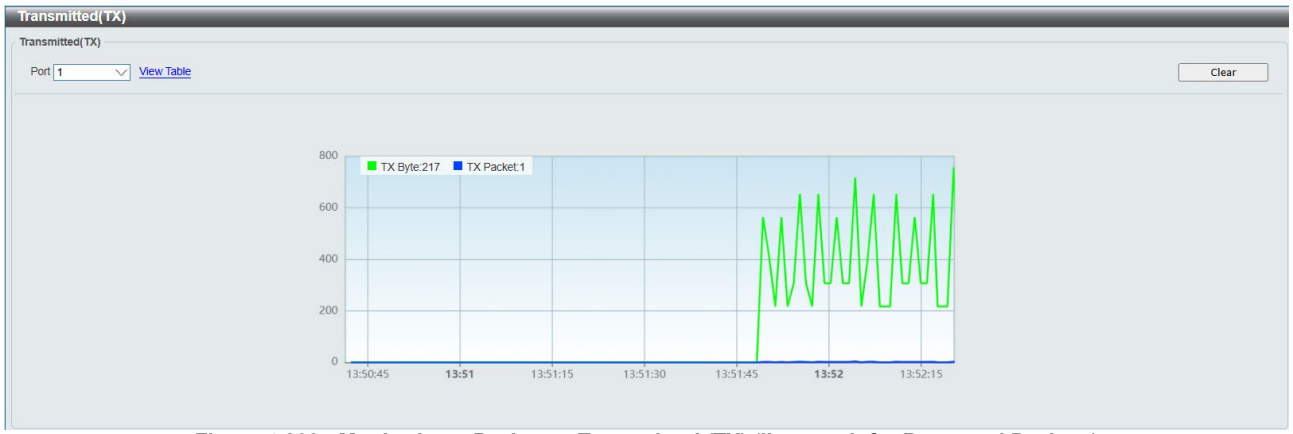


Figure 4.203 - Monitoring > Packets > Transmitted (TX) (line graph for Bytes and Packets)

To view the **Transmitted (TX) Table**, click the link View Table, which will show the following table:

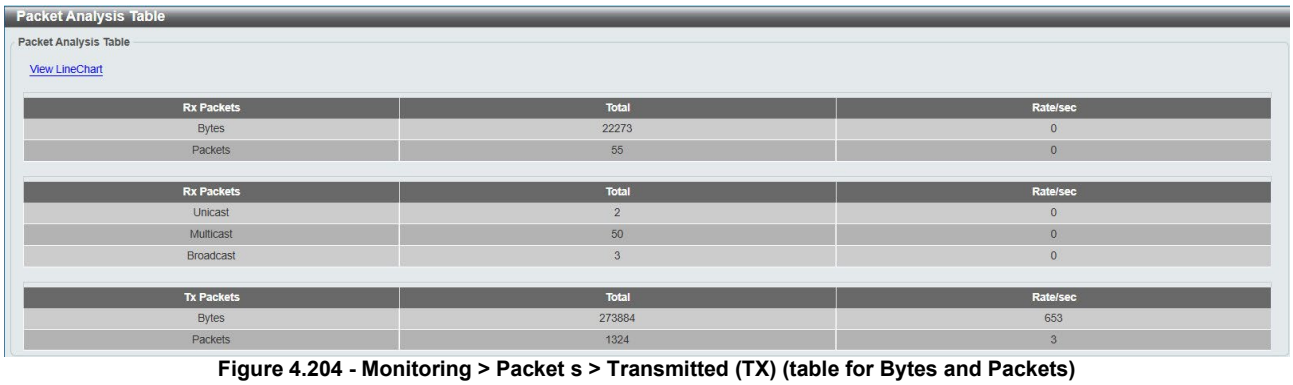


Figure 4.204 - Monitoring > Packet s > Transmitted (TX) (table for Bytes and Packets)

The following fields can be set or viewed:

Time Interval: Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is *one* second.

Record Number: Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.

Bytes: Counts the number of bytes successfully sent from the port.

Packets: Counts the number of packets successfully sent on the port.

Unicast: Counts the total number of good packets that were transmitted by a unicast address.

Multicast: Counts the total number of good packets that were transmitted by a multicast address.

Broadcast: Counts the total number of good packets that were transmitted by a broadcast address.

Show/Hide: Check whether or not to display Bytes and Packets.

Clear: Clicking this button clears all statistics counters on this window.

View Table: Clicking this button instructs the Switch to display a table rather than a line graph.

View Line Chart: Clicking this button instructs the Switch to display a line graph rather than a table.

Monitoring > Packets > Received (RX)

The Received (RX) page displays the following graph of packets received on the Switch. To select a port to view these statistics for, use the **Port** pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

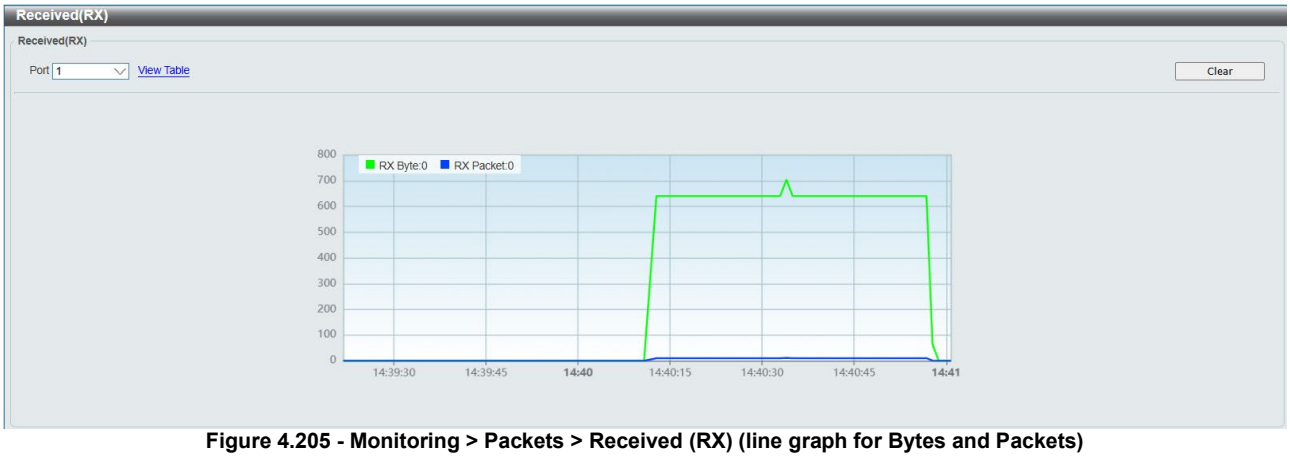


Figure 4.205 - Monitoring > Packets > Received (RX) (line graph for Bytes and Packets)

To view the **Received Packets Table**, click the link View Table, which will show the following table:

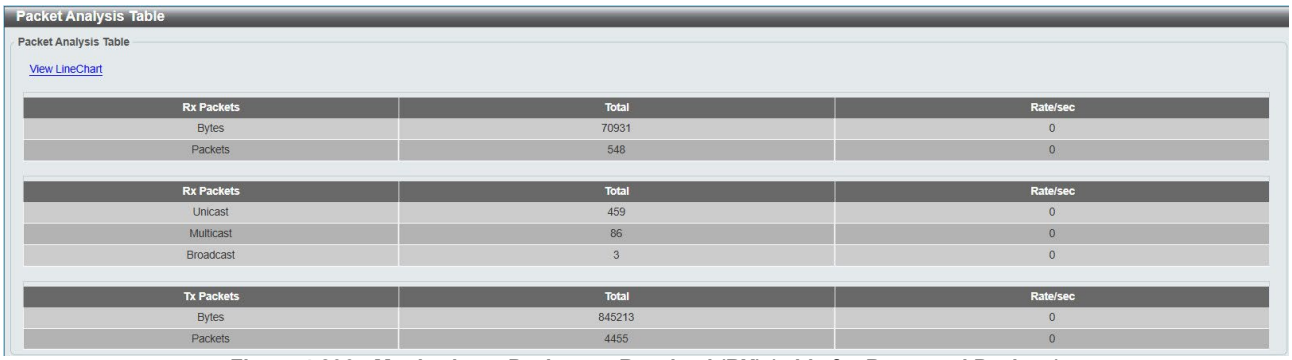


Figure 4.206 - Monitoring > Packet s > Received (RX) (table for Bytes and Packets)

The following fields can be set or viewed:

Time Interval: Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is *one* second.

Record Number: Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.

Bytes: Counts the number of bytes received on the port.

Packets: Counts the number of packets received on the port.

Unicast: Counts the total number of good packets that were received by a unicast address.

Multicast: Counts the total number of good packets that were received by a multicast address.

Broadcast: Counts the total number of good packets that were received by a broadcast address.

Show/Hide: Check whether or not to display Bytes and Packets.

Clear: Clicking this button clears all statistics counters on this window.

View Table: Clicking this button instructs the Switch to display a table rather than a line graph.

View Line Chart: Clicking this button instructs the Switch to display a line graph rather than a table.

Monitoring > Packets > UMB Cast (RX)

The **UMB Cast (RX)** page displays the following graph of UMB cast packets received on the Switch. To select a port to view these statistics for, use the **Port** pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

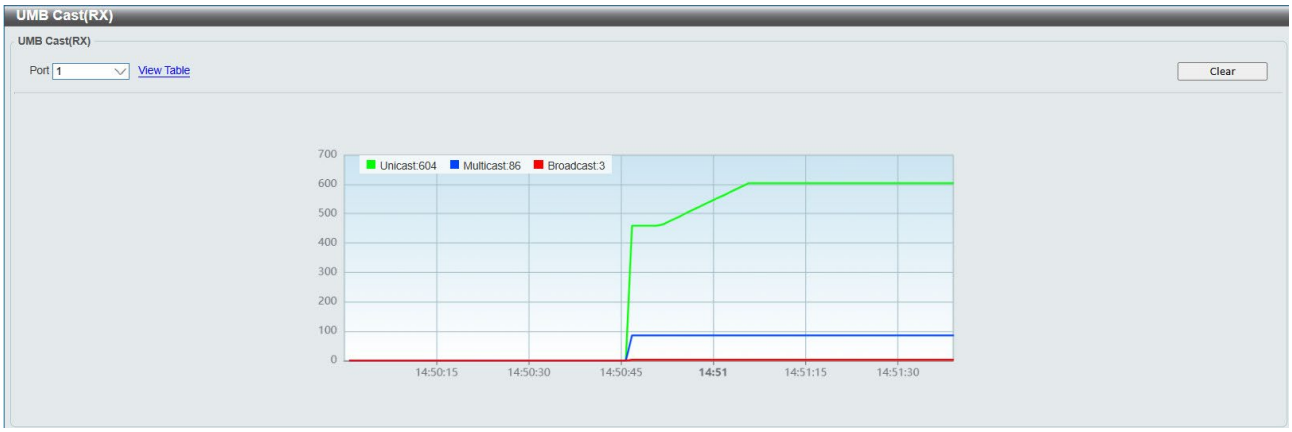
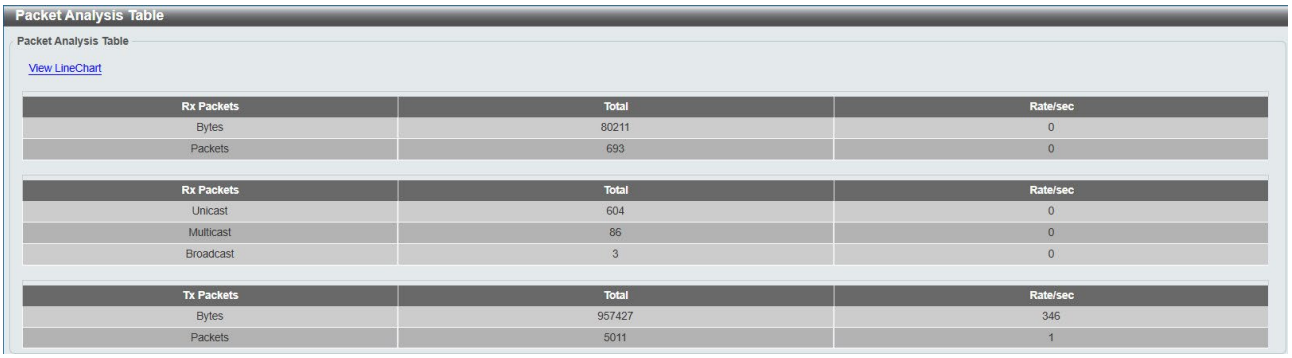


Figure 4.207 - Monitoring > Packets > UMB Cast (RX) (line graph for Unicast, Multicast and Broadcast Packets)

To view the **UMB Cast Table**, click the View Table link, which will show the following table:



Rx Packets	Total	Rate/sec
Bytes	80211	0
Packets	693	0

Rx Packets	Total	Rate/sec
Unicast	604	0
Multicast	86	0
Broadcast	3	0

Tx Packets	Total	Rate/sec
Bytes	957427	346
Packets	5011	1

Figure 4.208 - Monitoring > Packets > UMB Cast (RX) (table for Unicast, Multicast and Broadcast Packets)

The following fields can be set or viewed:

Time Interval: Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is *one* second.

Record Number: Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.

Unicast: Counts the total number of good packets that were received by a unicast address.

Multicast: Counts the total number of good packets that were received by a multicast address.

Broadcast: Counts the total number of good packets that were received by a broadcast address.

Show/Hide: Check whether or not to display Multicast, Broadcast and Unicast packets.

Clear: Clicking this button clears all statistics counters on this window.

View Table: Clicking this button instructs the Switch to display a table rather than a line graph.

View Line Chart: Clicking this button instructs the Switch to display a line graph rather than a table.

Monitoring > Errors > Received (RX)

This page displays the following graph of error packets received on the Switch. To select a port to view these statistics for, select the port by using the **Port** pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

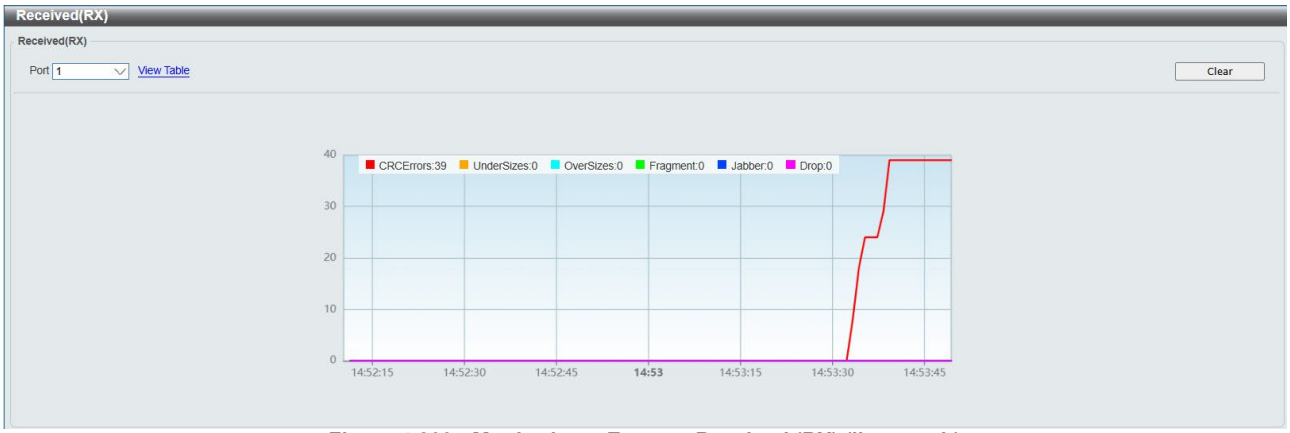
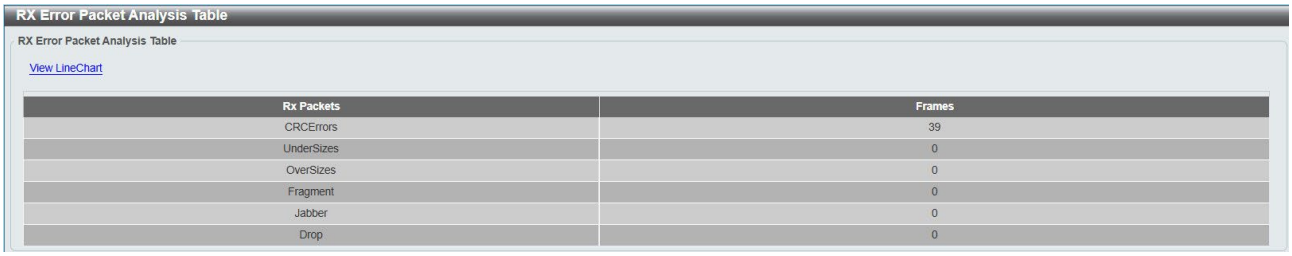


Figure 4.209 - Monitoring > Errors > Received (RX) (line graph)

To view the **Received Error Packets Table**, click the link **View Table**, which will show the following table:



Rx Packets	Frames
CRCErrors	39
UnderSizes	0
OverSizes	0
Fragment	0
Jabber	0
Drop	0

Figure 4.210 - Monitoring > Errors > Received (RX) (table)

The following fields can be set or viewed:

Time Interval: Select the desired setting between *1s* and *60s*, where “s” stands for seconds. The default value is *one* second.

Record Number: Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.

CRC Error: Counts otherwise valid packets that did not end on a byte (octet) boundary.

UnderSize: The number of packets detected that are less that the minimum permitted packets size of *64* bytes and have a good CRC. Undersize packets usually indicate collision fragments, a normal network occurrence.

OverSize: Counts packets received that were longer that *1518* octets, or if a VLAN frame is *1522* octets, and less that the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to *1522*.

Fragment: The number of packets less than *64* bytes with either bad framing or an invalid CRC. These are normally the result of collisions.

Jabber: The number of packets with lengths more than the MAX_PKT_LEN bytes. Internally, MAX_PKT_LEN is equal to *1522*.

Drop: The number of packets that are dropped by this port since the last Switch reboot.

Show/Hide: Check whether or not to display CRC Error, Under Size, Over Size, Fragment, Jabber, and Drop errors.

Clear: Clicking this button clears all statistics counters on this window.

View Table: Clicking this button instructs the Switch to display a table rather than a line graph.

View Line Chart: Clicking this button instructs the Switch to display a line graph rather than a table.

Monitoring > Errors > Transmitted (TX)

This page displays the following graph of error packets transmitted on the Switch. To select a port to view these statistics for, select the port by using the **Port** pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

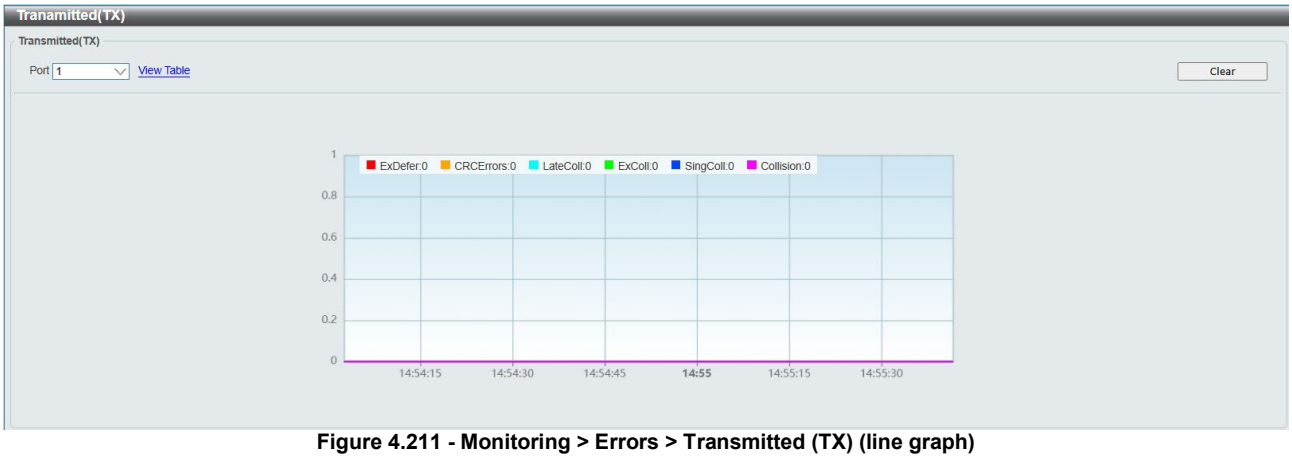
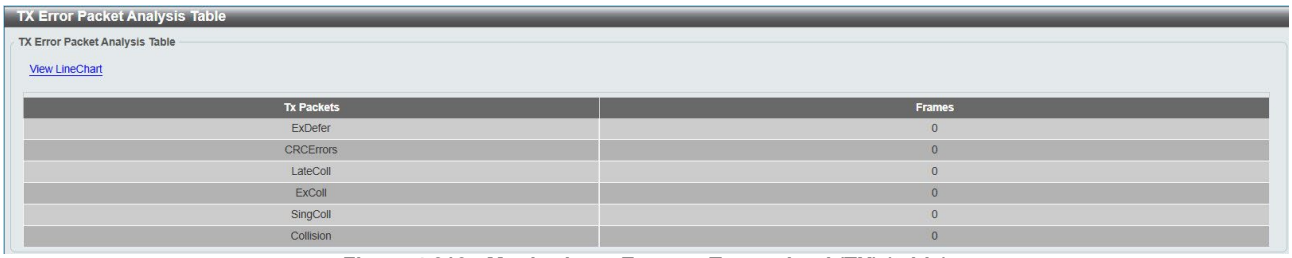


Figure 4.211 - Monitoring > Errors > Transmitted (TX) (line graph)

To view the **Transmitted Error Packets Table**, click the link View Table, which will show the following table:



Tx Packets	Frames
ExDefer	0
CRCErrors	0
LateColl	0
ExColl	0
SingColl	0
Collision	0

Figure 4.212 - Monitoring > Errors > Transmitted (TX) (table)

The following fields can be set or viewed:

Time Interval: Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is *one* second.

Record Number: Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.

ExDefet: Counts the number of packets for which the first transmission attempt on a particular interface was delayed because the medium was busy.

CRC Error: Counts otherwise valid packets that did not end on a byte (octet) boundary.

LateColl: Counts the number of times that a collision is detected later than *512* bit-times into the transmission of a packet.

ExColl: Excessive Collisions. The number of packets for which transmission failed due to excessive collisions.

SingColl: Single Collision Frames. The number of successfully transmitted packets for which transmission is inhibited by more than one collision.

Coll: An estimate of the total number of collisions on this network segment.

Show/Hide: Check whether or not to display ExDefer, LateColl, ExColl, SingColl, and Coll errors.

Clear: Clicking this button clears all statistics counters on this window.

View Table: Clicking this button instructs the Switch to display a table rather than a line graph.

View Line Chart: Clicking this button instructs the Switch to display a line graph rather than a table.

Monitoring > Cable Diagnostics

The Cable Diagnostics is designed primarily for administrators and customer service representatives to examine of the copper cable quality. It rapidly determines the type of cable errors occurred in the cable.

Select a port and then click the **Test Now** button to start the diagnosis.

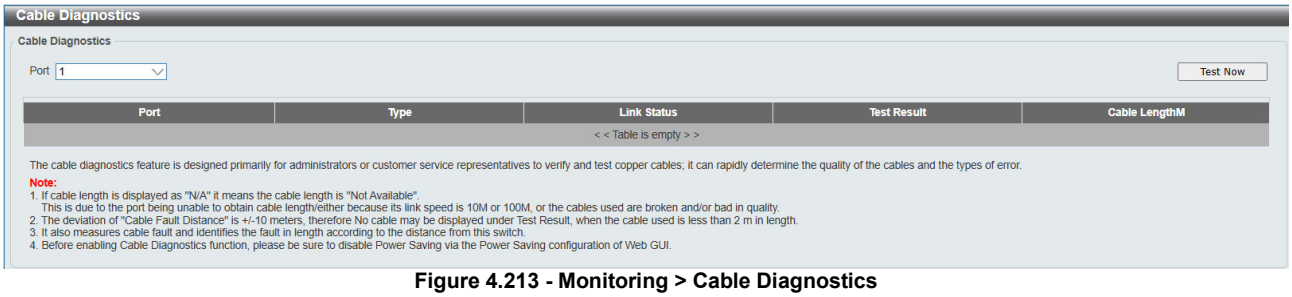


Figure 4.213 - Monitoring > Cable Diagnostics

Test Result: The description of the cable diagnostic results.

- **OK** means the cable is good for the connection.
- **Short in Cable** means the wires of the RJ45 cable may be in contact somewhere.
- **Open in Cable** means the wires of RJ45 cable may be broken or the other end of the cable is simply disconnected.
- **Test Failed** means some other errors occurred during cable diagnostics. Please select the same port and test again.

Cable Fault Distance (meters): Indicates the distance of the cable fault from the Switch port, if the cable is less than 2 meters, it will show “No Cable”, whether the fiber is connected to the port or not.

Cable Length (meter): If the test result shows OK, then cable length will be indicated for the total length of the cable. The cable lengths are categorized into four types: <50 meters, 50~80 meters, 80~100 meters and >100 meters. Deviation is +/-2 meters, therefore "No Cable" may be displayed under "Test Result," when the cable used is less than 2 m in length. This test can only be performed when the port is up and operating at 1 Gbps.

NOTE: Cable length detection is effective on Gigabit ports only.

The definition of cable pair is listed below:

Pair1: PIN4, PIN5
Pair2: PIN1, PIN2
Pair3: PIN3, PIN6
Pair4: PIN7, PIN8

Monitoring > System Log

The System Log page provides information about system logs, including information when the device was booted, how the ports are operating, when users logged in, when sessions timed out, as well as other system information.

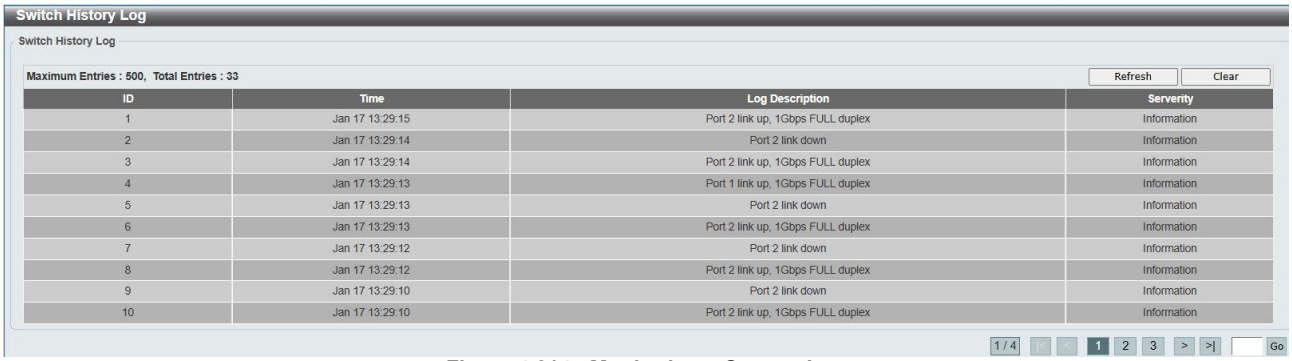


Figure 4.214 - Monitoring > System Log

ID: Displays an incremented counter of the System Log entry. The Maximum entries are 500.

Time: Displays the time in days, hours, and minutes the log was entered.

Log Description: Displays the description of event recorded.

Severity: Displays a severity level of the event recorded.

Click **Refresh** to renew the page, and click **Clear** to clean out all log entries.

Monitoring > Browse ARP Table

The Browse ARP Table page provides information regarding ARP VLANs, including which IP address was mapped to what MAC address. To clear the ARP Table, click **Clear All.**

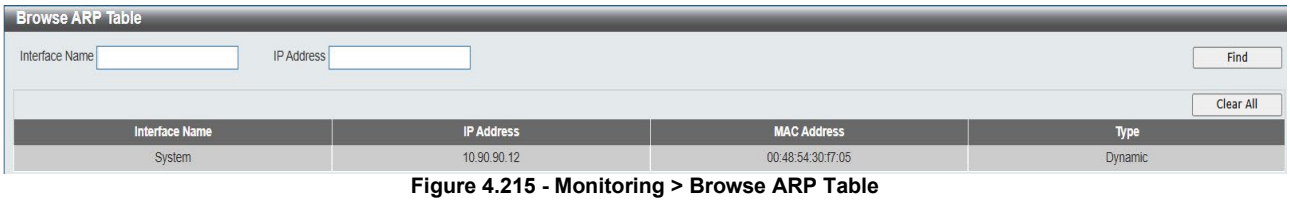


Figure 4.215 - Monitoring > Browse ARP Table

Click **Find**, The table updates and displays the values required.

Interface Name: Defines the name of ARP mappings.

IP Address: Defines the station IP address, which is associated with the MAC address.

MAC Address: Displays the MAC address associated with the IP address.

Type: Indicates how the MAC was assigned. The possible values are:

Dynamic – Indicates that the MAC address is dynamically created.

Static – Indicates the MAC address is a static IP address.

Port: Defines the ARP mapping ports.

Monitoring > Ethernet OAM > Browse Ethernet OAM Event Log

The Browse Ethernet OAM Event Log page displays the ports Ethernet OAM event log information.

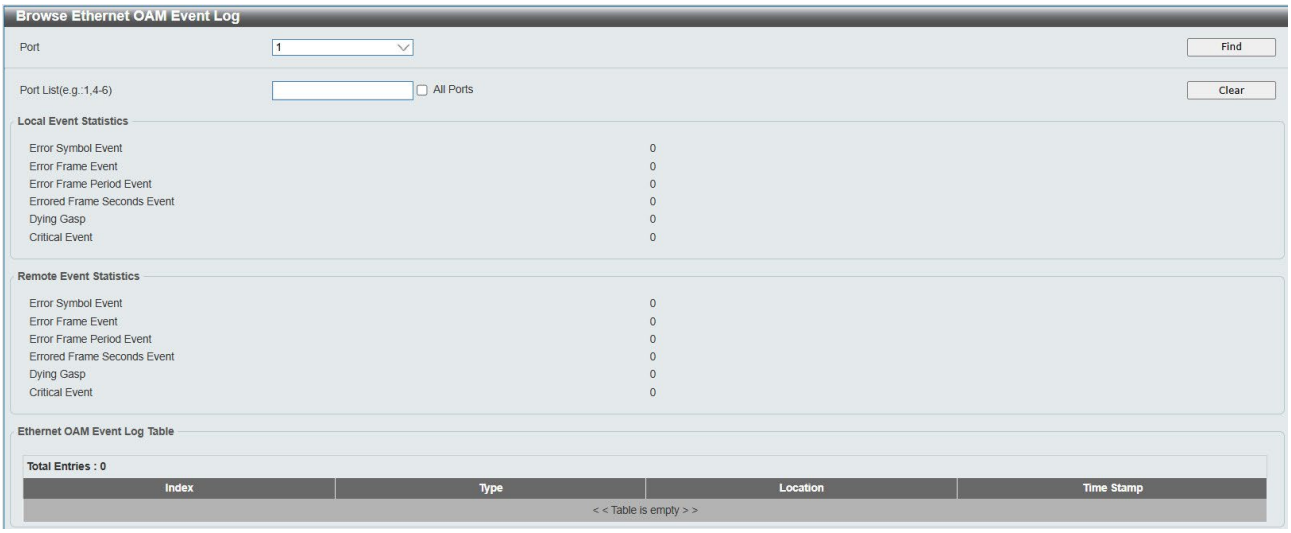


Figure 4.216 - Monitoring > Ethernet OAM > Browse Ethernet OAM Event Log

Port: Select the port to be viewed.

Port List: Enter a list of ports. Tick the **All Ports** check box to select all ports.

Click **Find** to locate a specific entry based on the information entered.

Click **Clear** to clear all the information entered in the fields.

Monitoring > Ethernet OAM > Browse Ethernet OAM Statistics

The Browse Ethernet OAM Statistics page displays the ports Ethernet OAM statistics information.

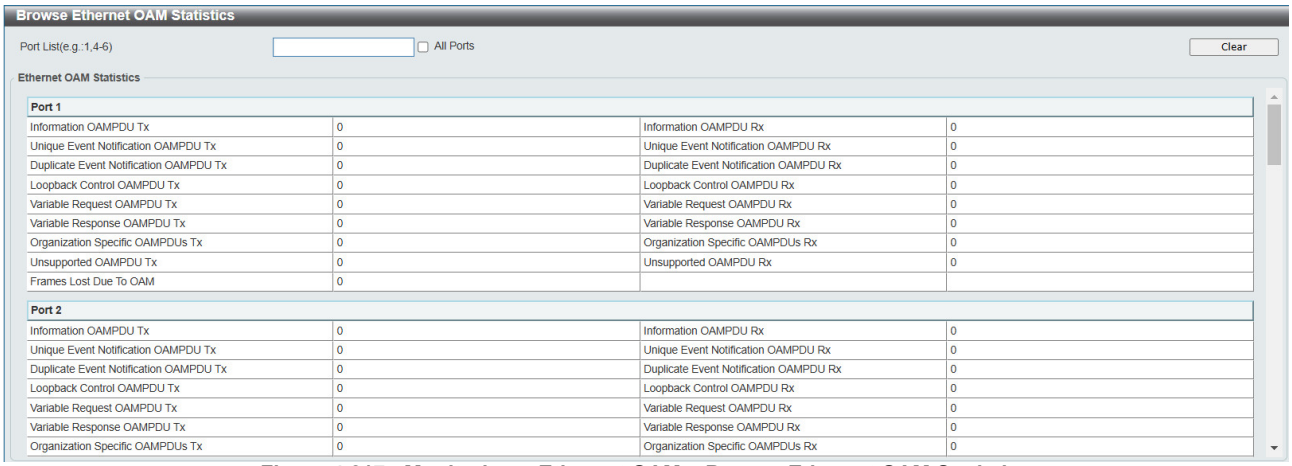


Figure 4.217 - Monitoring > Ethernet OAM > Browse Ethernet OAM Statistics

Port List: Enter a list of ports. Tick the **All Ports** check box to select all ports.

Click **Clear** to clear all the information entered in the fields.

Monitoring > IGMP Snooping > IGMP Snooping Group

The IGMP Snooping Group page is used to display the current IGMP snooping static group information on the Switch.

Figure 4.218 - Monitoring > IGMP Snooping > IGMP Snooping Group

VLAN Name: Specify the name of the VLAN for which to be displayed the IGMP Snooping Group information.

VID: Specify the list of the VLAN IDs for which to be displayed the IGMP Snooping Group information.

Group IP Address: Specify the static group address for which to be displayed the IGMP Snooping static group information.

Click **Find VLAN** to display the IGMP group information or click **Clear Data Driven** to clear the IGMP group information.

Monitoring > IGMP Snooping > IGMP Snooping Host

The IGMP Snooping Host page allows user to display the information of IGMP Snooping Host.

Figure 4.219 - Monitoring > IGMP Snooping > IGMP Snooping Host

VLAN Name: Specify the name of the VLAN for which to be displayed the IGMP Snooping Host information.

VID (1-4094): Specify the list of the VLAN IDs for which to be displayed the IGMP Snooping Host information.

Port: Specify the ports of IGMP Snooping Host information to be displayed.
Group: Specify the group of IGMP Snooping Host information to be displayed.

Click **Find** to display the information.

Monitoring > MLD Snooping > MLD Snooping Group

The MLD Snooping Group page allows user to configure the MLD Snooping group settings.

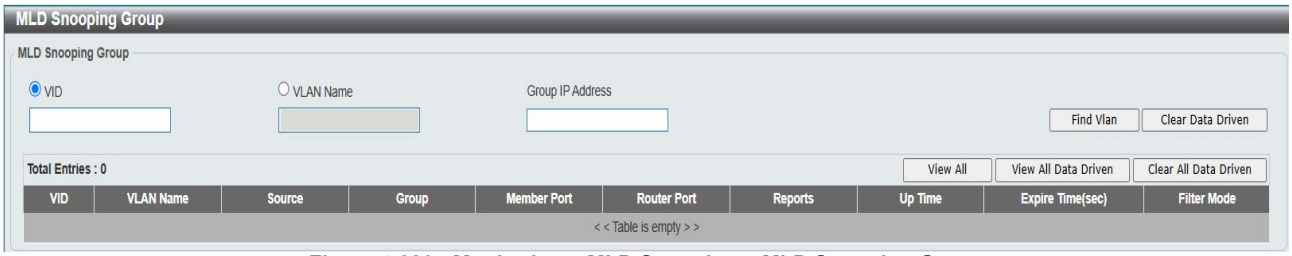


Figure 4.220 - Monitoring > MLD Snooping > MLD Snooping Group

VLAN Name: Specify the VLAN name for MLD Snooping group.
VID: Specify the VID for MLD Snooping group.
Group IP Address: Specify the IP address for the specified VLAN.

Click **Find Vlan** to locate a specific entry based on the information entered.
Click **View All** to display all the existing entries.
Click **View All Data Driven** to display all existing entire entries.
Click **Clear All Data Driven** to clear data driven information for all entries.

Monitoring > Port Access Control > RADIUS Authentication

This table contains information concerning the activity of the RADIUS authentication client on the client side of the RADIUS authentication protocol. It has one row for each RADIUS authentication server that the client shares a secret with.

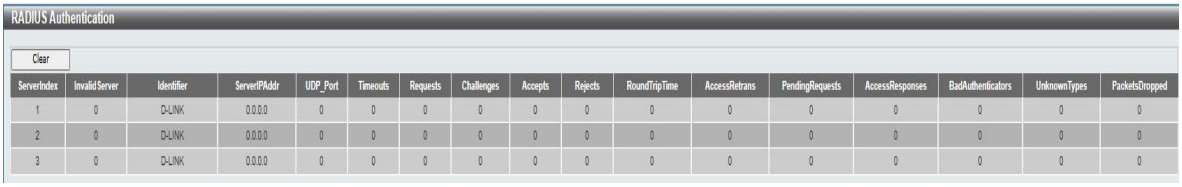


Figure 4.221 - Monitoring > Port Access Control > RADIUS Authentication

The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where “s” stands for seconds. The default value is one second. To clear the current statistics shown, click the **Clear** button in the top left hand corner.

The following fields can be viewed:

Server Index: The identification number assigned to each RADIUS Authentication server that the client shares a secret with.

UDP Port: The UDP port the client is using to send requests to this server.

Timeouts: The number of authentication timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

Requests: The number of RADIUS Access-Request packets sent to this server. This does not include retransmissions.

Challenges: The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.

Accepts: The number of RADIUS Access-Accept packets (valid or invalid) received from this server.

Rejects: The number of RADIUS Access-Reject packets (valid or invalid) received from this server.

RoundTripTime: The time interval (in hundredths of a second) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.

AccessRetrans: The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.

PendingRequests: The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject or Access-Challenge, a timeout or retransmission.

AccessResponses: The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or Signature attributes or known types are not included as malformed access responses.

BadAuthenticators: The number of RADIUS Access-Response packets containing invalid authenticators or Signature attributes received from this server.

UnknownTypes: The number of RADIUS packets of unknown type which were received from this server on the authentication port.

PacketsDropped: The number of RADIUS packets of which were received from this server on the authentication port and dropped for some other reason.

Monitoring > Port Access Control > RADIUS Account Client

This RADIUS Account Client page shows managed objects used for managing RADIUS accounting clients, and the current statistics associated with them. It has one row for each RADIUS authentication server that the client shares a secret with.

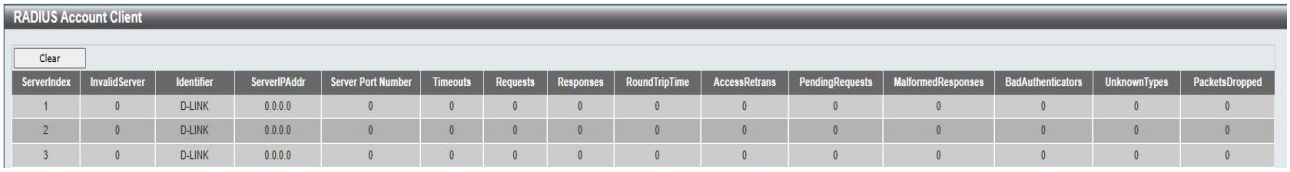


Figure 4.222 - Monitoring > Port Access Control > RADIUS Account Client

The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where “s” stands for seconds. The default value is *one* second. To clear the current statistics shown, click the Clear button in the top left hand corner.

The following fields can be viewed:

Server IP Addr: The IP address assigned to each RADIUS Accounting server that the client shares a secret with.

Server Port Number: The UDP port the client is using to send requests to this server.

Timeouts: The number of accounting timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.

Requests: The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.

Responses: The number of RADIUS packets received on the accounting port from this server.

RoundTripTime: The time interval between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.

AccessRetrans: The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.

PendindRequests: The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response. This variable is incremented when an Accounting-Request is sent and decremented due to receipt of an Accounting-Response, a timeout or a retransmission.

MalformedResponses: The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.

BadAuthenticators: The number of RADIUS Accounting-Response packets, which contained invalid authenticators, received from this server.

UnknownTypes: The number of RADIUS packets of unknown type which were received from this server on the accounting port.

PacketsDropped: The number of RADIUS packets, which were received from this server on the accounting port and dropped for some other reason.

Monitoring > sFlow > sFlow Global Settings

sFlow (RFC3176) is a technology for monitoring traffic in data networks containing switches and routers. The sFlow monitoring system consists of an sFlow Agent (embedded in a switch or router or in a standalone probe) and a central sFlow Collector. The architecture and sampling techniques used in the sFlow monitoring system were designed for providing continuous site-wide (and enterprise-wide) traffic monitoring of high speed switched and routed networks.

This sFlow Global Settings page allows user to configure the sFlow Global configuration.

Figure 4.223 - Monitoring > sFlow > sFlow Global Settings

sFlow State: Specify to enable or disable the sFlow feature.

Click **Apply** to make the configurations take effect.

Monitoring > sFlow > sFlow Analyzer Server Settings

The Switch can support 4 different Analyzer Servers at the same time and each sampler or poller can select a collector to send the samples. We can send different samples from different samplers or pollers to different collectors.

This sFlow Analyzer Server Settings page allows user to configure the sFlow analyzer server configuration.

Figure 4.224 - Monitoring > sFlow > sFlow Analyzer Server Settings

Analyzer Server ID (1-4): The analyzer server ID specifies the ID of a server analyzer where the packet will be forwarded.

Owner Name: The entity making use of this sFlow analyzer server. When owner is set or modified, the timeout value will become 400 automatically.

Timeout (1-2000000): The length of time before the server times out. When the analyzer server times out, all of the flow samplers and counter pollers associated with this analyzer server will be deleted. If not specified, its default value is 400. Tick the Infinite check box to have unlimited time.

Collector (IPv6) Address: The IP address of the analyzer server. If not specified or set a 0 address, the entry will be inactive.

Collector Port (1-65535): The destination UDP port for sending the sFlow datagrams. If not specified, the default value is 6343.

Max Datagram Size (300-1400): The maximum number of data bytes that can be packed in a single sample datagram. If not specified, the default value is 1400.

Click **Apply** to make the configurations take effect.

Monitoring > sFlow > sFlow Flow Sampler Settings

This sFlow Flow Sampler Settings page allows user to configure the sFlow flow sampler parameters. By configuring the sampling function for a port, a sample packet received by this port will be encapsulated and forwarded to the analyzer server at the specified interval.

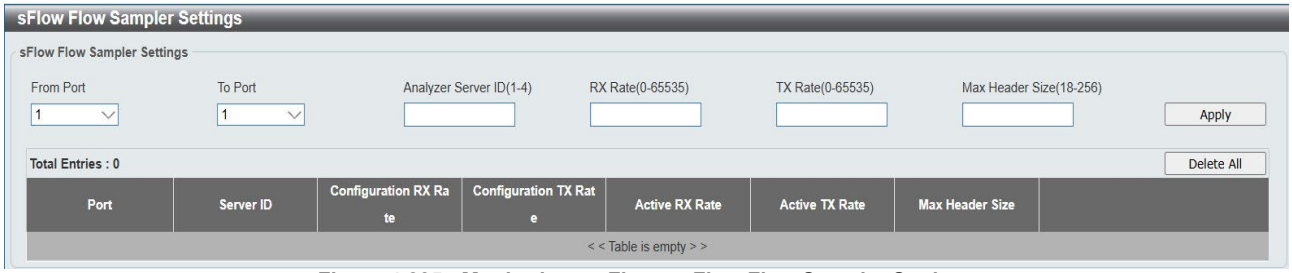


Figure 4.225 - Monitoring > sFlow > sFlow Flow Sampler Settings

From Port / To Port: User the drop-down to specify the list of ports to be configured.

Analyzer Server ID (1-4): The analyzer server ID specifies the ID of a server analyzer where the packet will be forwarded.

RX Rate (0-65535): The sampling rate for packet Rx sampling. The configured rate value multiplied by 256 is the actual rate. For example, if the rate is 20, the actual rate 5120. One packet will be sampled from every 5120 packets. If set to 0, the sampler is disabled. If the rate is not specified, its default value is 0.

TX Rate (0-65535): The sampling rate for packet Tx sampling. The configured rate value multiplied by 256 is the actual rate. For example, if the rate is 20, the actual rate 5120. One packet will be sampled from every 5120 packets. If set to 0, the sampler is disabled. If the rate is not specified, its default value is 0.

Max Header Size (18-256): The maximum number of leading bytes in the packet which has been sampled that will be encapsulated and forwarded to the server. If not specified, the default value is 128.

Click **Apply** to make the configurations take effect.

Click **Delete All** to remove all entries.

Monitoring > sFlow > sFlow Counter Poller Settings

This sFlow Counter Poller Settings page allows user to configure the sFlow counter poller settings. If the user wants to change the analyzer server ID, he needs to delete the counter poller and create a new one.

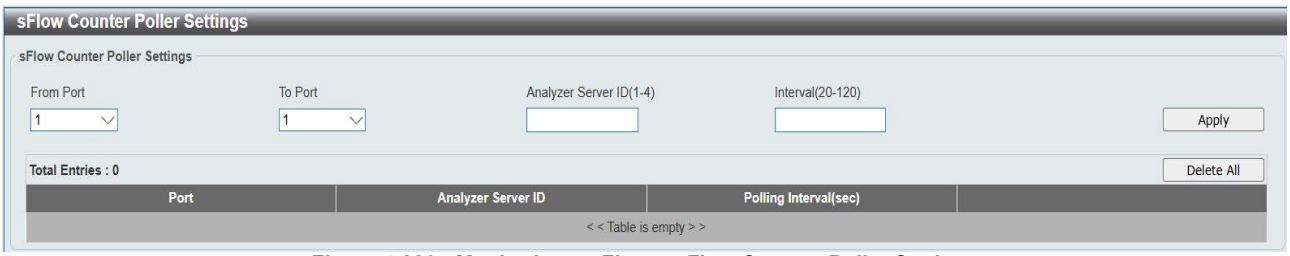


Figure 4.226 - Monitoring > sFlow > sFlow Counter Poller Settings

From Port / To Port: Use the drop-down menus to specify the list of ports to be configured.

Analyzer Server ID (1-4): The analyzer server ID specifies the ID of a server analyzer where the packet will be forwarded.

Interval (20-120): The maximum number of seconds between successive samples of the counters.

Click **Apply** to make the configurations take effect.

Click **Delete All** to remove all entries.

Monitoring > CFM > CFM Settings

On this page the user can configure the CFM (Connectivity Fault Management) parameters.

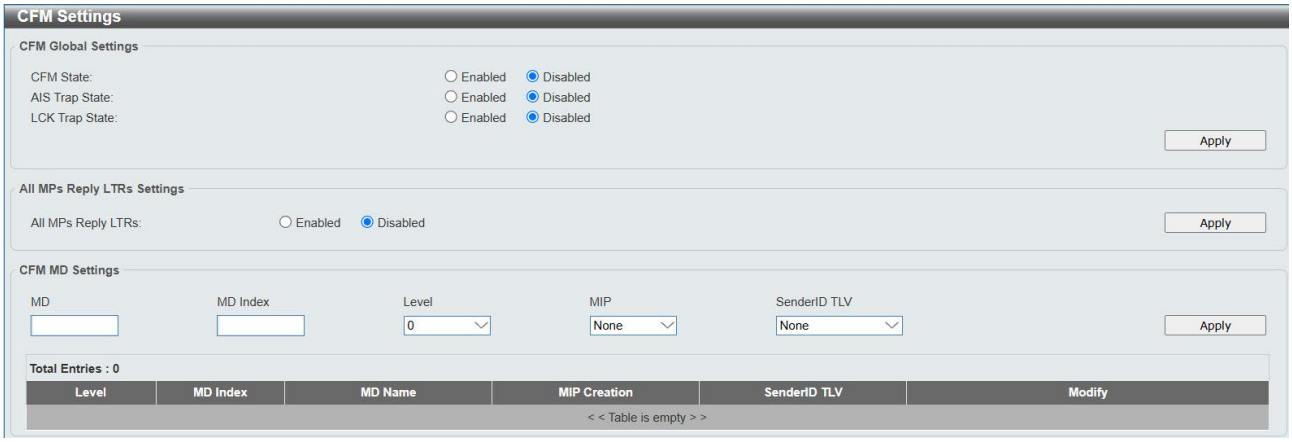


Figure 4.227 - Monitoring > CFM > CFM Settings

The fields can be configured as described:

Parameter	Description
CFM State	Click the radio buttons to enable or disable the CFM function.
AIS Trap State	Click the radio buttons to enable or disable the AIS trap state.
LCK Trap State	Click the radio buttons to enable or disable the LCK trap state.
All MPs Reply LTRs	Click the radio buttons to enable or disable all MPs to reply LTRs.
MD	Enter the string for maintenance domain name.
MD Index	Enter the integer maintenance domain index used.
Level	Use the drop-down menu to select the maintenance domain level.
MIP	This is the control creations of MIPs. *None* – Don't create MIPs. This is the default value. *Auto* – MIPs can always be created on any ports in this MD, if that port is not configured with an MEP of this MD. For the intermediate switch in an MA, the setting must be auto in order for the MIPs to be created on this device. *Explicit* – MIPs can be created on any ports in this MD, only if the next existent lower level has an MEP configured on that port, and that port is not configured with an MEP of this MD.
SenderID TLV	This is the control transmission of the SenderID TLV. *None* – Don't transmit sender ID TLV. This is the default value. *Chassis* – Transmit sender ID TLV with chassis ID information. *Manage* – Transmit sender ID TLV with managed address information. *Chassis Manage* – Transmit sender ID TLV with chassis ID information and manage address information.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Edit** button to re-configure the specific entry.
Click the **Delete** button to remove the specific entry.

By clicking “Add MA” button leads to CFM MA Settings page as shown:

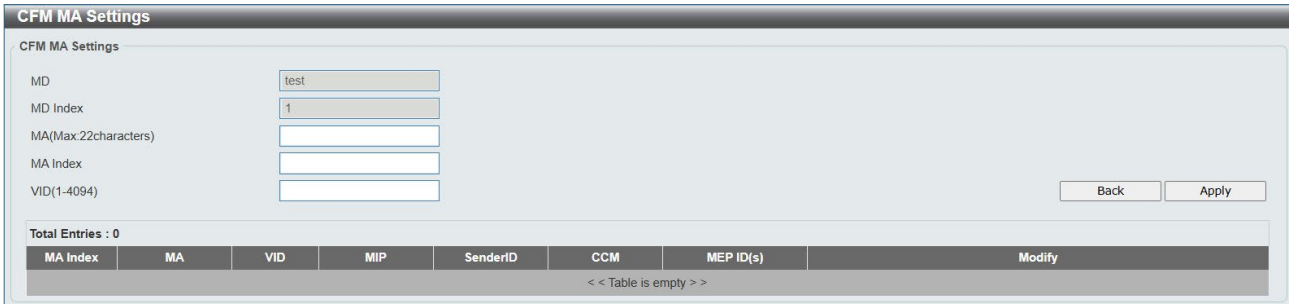


Figure 4.228 - Monitoring > CFM > CFM MA Settings

Parameter	Description
MA	Enter the maintenance association name.
MA Index	Enter the maintenance association index.
VID (1-4094)	VLAN Identifier. Different MA must be associated with different VLANs.

Click the **Add** button to add a new entry based on the information entered.
Click the **<<Back** button to discard the changes made and return to the previous page.
Click the **Edit** button to re-configure the specific entry.
Click the **Delete** button to remove the specific entry.
Click the **MIP Port Table** button to view the CFM MIP Table.
Click the **Add MEP** button to add a Maintenance End Point entry.

By clicking Edit button, the following parameters can be configured:

Figure 4.229 - Monitoring > CFM > CFM MA Edit

Parameter	Description
MIP	This is the control creation of MIPs. *None* - Don’t create MIPs. *Auto* - MIPs can always be created on any ports in this MA, if that port is not configured with an MEP of that MA. *Explicit* - MIP can be created on any ports in this MA, only if the next existent lower level has an MEP configured on that port, and that port is not configured with an MEP of this MA. *Defer* - Inherit the setting configured for the maintenance domain that this MA is associated with. This is the default value.
SenderID	This is the control transmission of the sender ID TLV. *None* - Don’t transmit sender ID TLV. This is the default

	value. *Chassis* - Transmit sender ID TLV with chassis ID information. *Manage* - Transmit sender ID TLV with manage address information. *Chassis Manage* - Transmit sender ID TLV with chassis ID information and manage address information. *Defer* - Inherit the setting configured for the maintenance domain that this MA is associated with. This is the default value.
CCM	This is the CCM interval. 100ms - 100 milliseconds. Not recommended. For test purpose. 1sec - One second. 10sec - Ten seconds. This is the default value. 1min - One minute. 10min - Ten minutes.
MEPID(s)	This is to specify the MEP IDs contained in the maintenance association. The range of the MEP ID is 1-8191.

Click the **Apply** button to accept the changes made.

By clicking **MIP Port Table** button, it leads to the following page:

Figure 4.230 - Monitoring > CFM > CFM MIP Port Table

Click the **<<Back** button to return to the previous page.

By clicking the **Add MEP** button, it leads to the following page as shown:

Figure 4.231 - Monitoring > CFM > CFM MEP Settings

Parameter	Description
MEP Name	Enter an MEP name. It is unique among all MEPs configured on the device.
MEP ID (1-8191)	Enter an MEP ID configured in the MA's MEP ID list.
Port	Use the drop-down menu to select port number. This port should be a member of the MA's associated VLAN.
MEP Direction	This is the MEP direction.

	Inward - Inward facing (up) MEP. *Outward* - Outward facing (down) MEP.

Click the **Add** button to add a new entry based on the information entered.
Click the **<<Back** button to discard the changes made and return to the previous page.
Click the **View Detail** hyperlink for more information of specified MEP.
Click the **Delete** button to remove the specific entry.

By clicking **View Detail** hyperlink, it leads to the following page as shown:

Figure 4.232 - Monitoring > CFM > CFM MEP Information

Click the **Edit** button to re-configure the specific entry.
Click the **<<Back** button to discard the changes made and return to the previous page.

By clicking Edit button, it leads to the following page as shown:

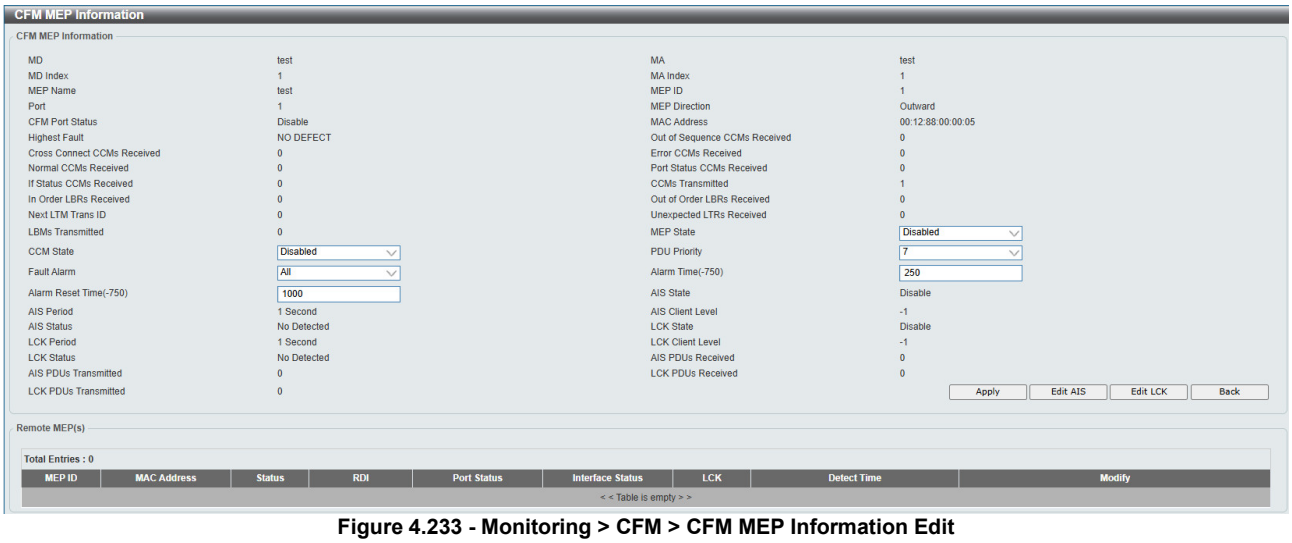


Figure 4.233 - Monitoring > CFM > CFM MEP Information Edit

Parameter	Description
MEP State	This is the MEP administrative state. *Enable* - MEP is enabled. *Disable* - MEP is disabled. This is the default value.
CCM State	This is the CCM transmission state. *Enable* - CCM transmission enabled. *Disable* - CCM transmission disabled. This is the default

	value.
PDU Priority	The 802.1p priority is set in the CCMs and the LTMs messages transmitted by the MEP. The default value is 7.
Fault Alarm	This is the control types of the fault alarms sent by the MEP. *All* - All types of fault alarms will be sent. *MAC Status* - Only the fault alarms whose priority is equal to or higher than “Some Remote MEP MAC Status Error” are sent. *Remote CCM* - Only the fault alarms whose priority is equal to or higher than “Some Remote MEP Down” are sent. *Errors CCM* - Only the fault alarms whose priority is equal to or higher than “Error CCM Received” are sent. *Xcon CCM* - Only the fault alarms whose priority is equal to or higher than “Cross-connect CCM Received” are sent. *None* - No fault alarm is sent. This is the default value.
Alarm Time (250-1000)	This is the time that a defect must exceed before the fault alarm can be sent. The unit is in centiseconds, the range is 250-1000. The default value is 250.
Alarm Reset Time (250-1000)	This is the dormant duration time before a defect is triggered before the fault can be re-alarmed. The unit is in centiseconds, the range is 250-1000. The default value is 1000.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

Click the **Edit AIS** button to configure the AIS settings.

Click the **Edit LCK** button to configure the LCK settings.

By clicking **Edit AIS** button, it leads to the follow page as shown:

Figure 4.234 - Monitoring > CFM > CFM Extension AIS Settings

Parameter	Description
State	Check the check box and use the drop-down menu to enable or disable the AIS function.
Period	Check the check box and use the drop-down menu to select the transmitting interval of AIS PDU.
Level	Tick the check box and use the drop-down menu to select the client level ID to which the MEP sends AIS PDU. The default client MD level is MD level at which the most immediate client layer MIPs and MEPs exist. Options to choose from are values between 0 and 7.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

By clicking **Edit LCK** button, it leads to the follow page as shown:

Figure 4.235 - Monitoring > CFM > CFM Extension LCK Settings

Parameter	Description
State	Check the check box and use the drop-down menu to enable or disable the LCK function.
Period	Check the check box and use the drop-down menu to select the transmitting interval of LCK PDU.
Level	Tick the check box and use the drop-down menu to select the client level ID to which the MEP sends LCK PDU. The default client MD level is MD level at which the most immediate client layer MIPs and MEPs exist. Options to choose from are values between 0 and 7.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

Monitoring > CFM > CFM Port Settings

On this page the user can configure the CFM port state.

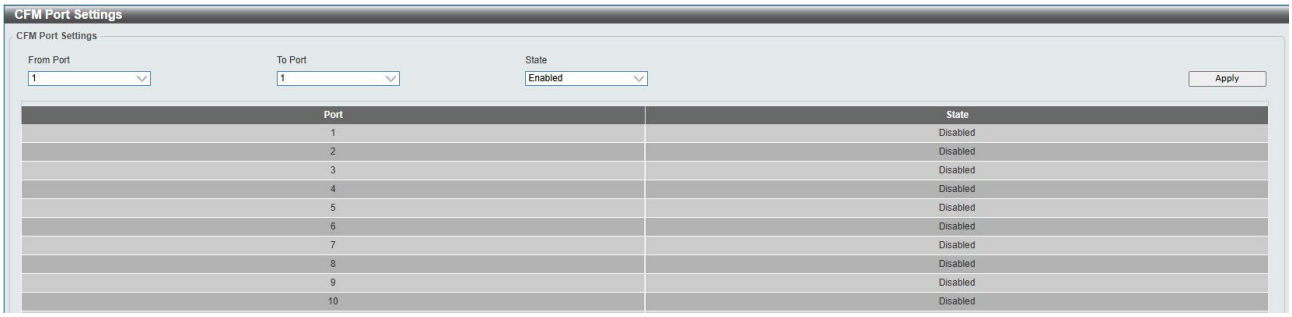


Figure 4.236 - Monitoring > CFM > CFM Port Settings

From Port / To Port: Use the drop-down menu to select a range of ports used for this configuration.
State: Use the drop-down menu to enable or disable the state of specific port regarding the CFM configuration.

Monitoring > CFM > CFM MIPCCM Table

This page is used to display CFM MIPCCM information.

Figure 4.237 - Monitoring > CFM > CFM MIPCCM Table

Monitoring > CFM > CFM Loopback Settings

This page is used to CFM loopback settings.

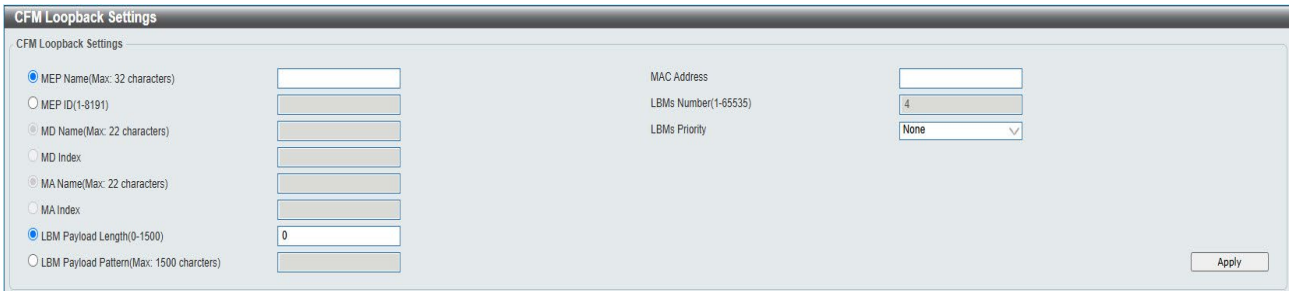


Figure 4.238 - Monitoring > CFM > CFM Loopback Settings

Parameter	Description
MEP Name	Select and enter the Maintenance End Point name used.
MEP ID	Select and enter the Maintenance End Point ID used.
MD Name	Select and enter the Maintenance Domain name used.
MD Index	Select and enter the Maintenance Domain index used.
MA Name	Select and enter the Maintenance Association name used.
MA Index	Select and enter the Maintenance Association index used.
MAC Address	Enter the destination MAC address used here.
LBMs Number (1-65535)	Number of LBMs to be sent. The default value is 4.
LBM Payload Length	The payload length of LBM to be sent. The default is 0.
LBM Payload Pattern	User-defined payload pattern. Maximum supports up to 1500 characters.
LBMs Priority	The 802.1p priority to be set in the transmitted LBMs.

Click the **Apply** button to execute the Loopback test.

Monitoring > CFM > CFM Linktrace Settings

This page is used to CFM Linktrace settings

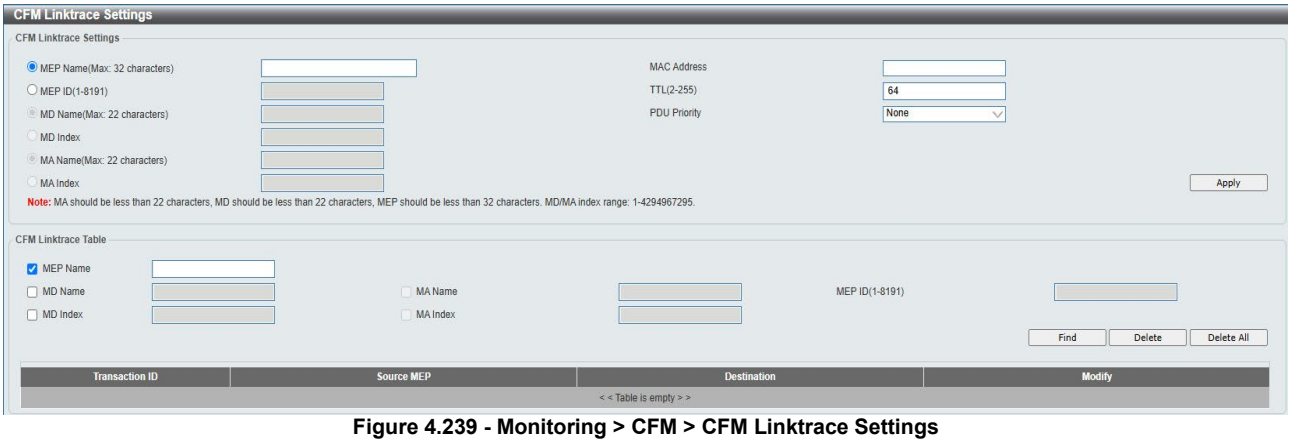


Figure 4.239 - Monitoring > CFM > CFM Linktrace Settings

Parameter	Description
MEP Name	Select and enter the Maintenance End Point name used.
MEP ID	Select and enter the Maintenance End Point ID used.
MD Name	Select and enter the Maintenance Domain name used.
MD Index	Select and enter the Maintenance Domain index used.

MA Name	Select and enter the Maintenance Association name used.
MA Index	Select and enter the Maintenance Association index used.
MAC Address	Enter the destination MAC address used here.
TTL	Link-trace message TTL value. The default value is 64.
PDU Priority	The payload length of LBM to be sent. The default is 0.

Click the **Apply** button to accept the changes made.
Click the **Find** button to locate a specific entry based on the information entered.
Click the **Delete** button to remove the specific entry based on the information entered.
Click the **Delete All** button to remove all the entries listed.

Monitoring > CFM > CFM Packet Counter

This page is used to display the counter for CFM packets.

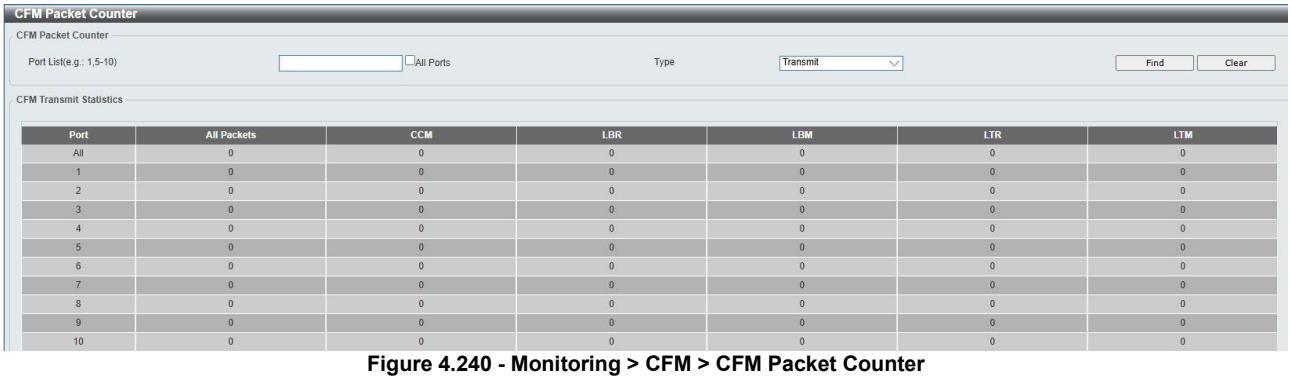


Figure 4.240 - Monitoring > CFM > CFM Packet Counter

Port List: Enter a port or range of ports to display. Check the **All Ports** check box to display all ports.
Type*:* Specify the type of packet to display
Transmit – Selecting this option will display all the CFM packets transmitted.
Receive – Selecting this option will display all the CFM packets received.
CCM – Selecting this option will display all the CFM packets transmitted and received.

Monitoring > CFM > CFM Fault Table

This page is used to display the CFM fault information.

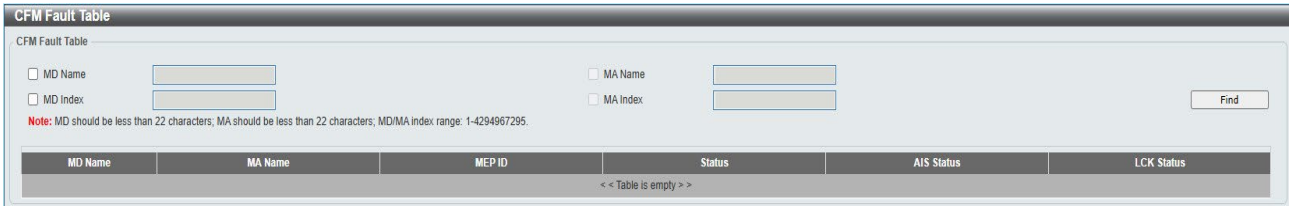


Figure 4.241 - Monitoring > CFM > CFM Fault Table

Parameter	Description
MD Name	Select and enter the Maintenance Domain name used.
MD Index	Select and enter the Maintenance Domain index used.
MA Name	Select and enter the Maintenance Association name used.
MA Index	Select and enter the Maintenance Association index used.

Click the **Find** button to locate a specific entry based on the information entered.

Monitoring > CFM > CFM MP Table

This page is used to display the CFM MP information.

Figure 4.242 - Monitoring > CFM > CFM MP Table

Parameter	Description
Port	Use the drop-down menu to select the unit the port number to view.
Level	Enter the level to view.
Direction	Use the drop-down menu to select the direction to view. *Inward* - Inward facing (up) MP. *Outward* - Outward facing (down) MP.
VID	Enter the VLAN ID to view.

Click the **Find** button to locate a specific entry based on the information entered.

ACL > ACL Configuration Wizard

Access Control List (ACL) allows user to establish criteria to determine whether or not the Switch will forward packets based on the information contained in each packet's header. These criteria can be specified on a basis of MAC address, or IP address.

The **ACL Configuration Wizard** will aid with the creation of access profiles and ACL Rules. The ACL Wizard will create the access rule and profile automatically. The maximum usable profiles are 50 and with 240 Rules in total for the switch.

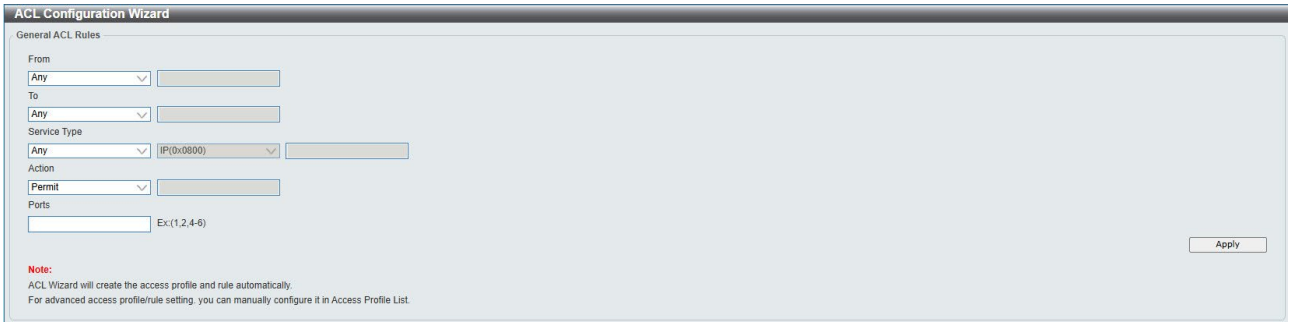


Figure 4.243 - ACL > ACL Configuration Wizard

From: Specify the origin of accessible packets. The possible values are:

Any - Indicates ACL action will be on packets from any source.

MAC Address - Indicates ACL action will be on packets from this MAC address.

IPv4 Addresses - Indicates ACL action will be on packets from this IPv4 source address.

IPv6 Addresses - Indicates ACL action will be on packets from this IPv6 source address

To: Specify the destination of accessible packets. The possible values are:

Any - Indicates ACL action will be on packets from any source.

MAC Address - Indicates ACL action will be on packets from this MAC address. The field of format is xx-xx-xx-xx-xx-xx.

IPv4 Addresses - Indicates ACL action will be on packets from this IPv4 source address.

IPv6 Addresses - Indicates ACL action will be on packets from this IPv6 source address.

Service Type: Specify the type of service. The possible values are:

Any - Indicates ACL action will be on packets from any service type.

Ether type - Specifies an Ethernet type for filtering packets.

ICMP All - Indicates ACL action will be on packets from ICMP packets.
IGMP - IGMP packets can be filtered by IGMP message type.
TCP All - Indicates ACL action will be on packets from TCP Packets.
TCP Source Port - Matches the packet to the TCP Source Port.
TCP Destination Port - Matches the packet to the TCP Destination Port.
UDP All - Indicates ACL action will be on packets from UDP Packets.
UDP Source Port - Matches the packet to the UDP Source Port.
UDP Destination Port - Matches the packet to the UDP Destination Port.

Action: Specify the ACL forwarding action matching the rule criteria.
Permit - Forwards packets if all other ACL criteria are met.
Deny - Drops packets if all other ACL criteria is met.
Mirror - Mirrors packets if all other ACL criteria is met.
Rate Limit - Rate limiting is activated if all other ACL criteria is met.
Replace DSCP - Reassigns a new DSCP value to the packet if all other ACL criteria are met.

Ports: Enter a range of ports to be configured.

Press **Apply** for the settings to take effect.

NOTE: Once the ACL rules conflict, rules with smaller rule ID will take higher priority.

NOTE: Be careful when configuring ACL rules, an inappropriate may cause management access failed.

ACL > Access Profile List

The Access Profile List provides information for configuring ACL Profiles manually. ACL profiles are attached to interfaces, and define how packets are forwarded if they match the ACL criteria.

Figure 4.244 - ACL > Access Profile List

The contents of Access Profile List table include:

Profile ID: Indicates the profile Identification number. The possible configured profile IDs are 1~50, and profile ID 51~55 are reserved for the pre-defined features.

Owner Type: The owner type of ACL profile; it can be normal ACL, Voice VLAN or Surveillance VLAN.

Profile Summary: Displays the profile summary.

Show Details: To display an ACL's profile details. The ACL profile details are displayed below the ACL table.

Show Rules: To show the access rule in this profile.

To add a new rule, please see **Access Rule List** in the next section.

Delete: To delete an access profile.

To manually add a profile, click **Add ACL Profile**:

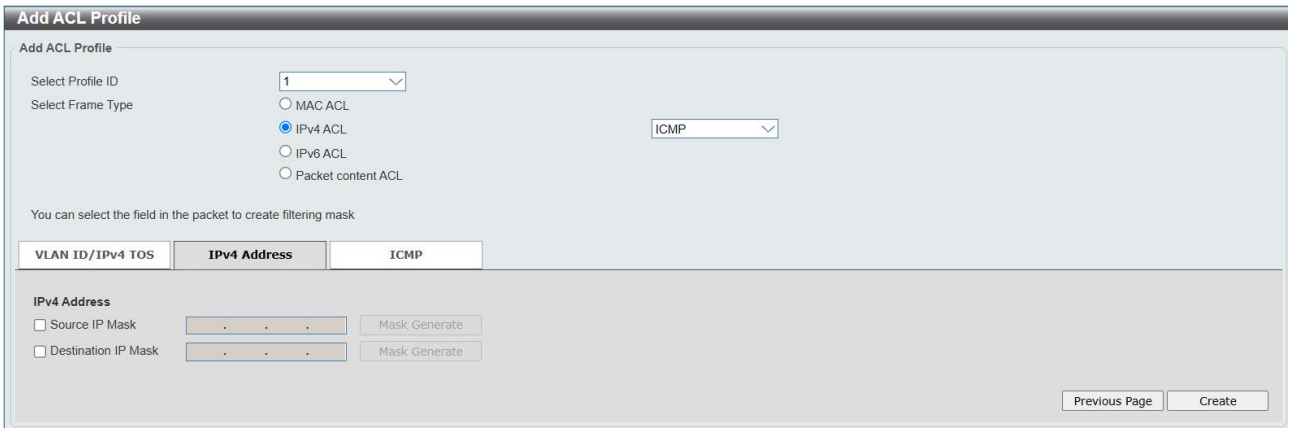


Figure 4.245 - Add ACL Profile

The steps of adding an access profile is like below:

1) After selecting the **Profile ID** and **Frame Type** (MAC, IPv4, IPv6 or Packet content ACL), specify attributes like Untagged/Tagged (for MAC), ICMP/IGMP/TCP/UDP/Protocol ID (for IPv4), or ICMPv6/TCP/UDP (for IPv6), then click **Select** and a simplified frame diagram will be displayed.

2) Select the field of interest and related columns will be displayed in lower part of the page. Enter the filtering mask and click **Create** when done. A filtering mask is to specify the digit that user wants to check. For example, if user wants to check a network of 192.168.1.0/24, then it should enter the IP mask as 255.255.255.0.

NOTE: Unable to select Payload in a MAC ACL, or L2 Header in IP ACL.

3) After the **Profile ID** has been created, it will go back to the main Access Profile List page.

ACL > ACL Finder

The ACL Finder page is used to help user to find a previously configured ACL entry. To search for an entry, enter the Profile ID from the drop-down menu, select a port that user would like to view and click **Find.** The table on the lower half of the screen will display the entries. To delete an entry click the corresponding **Delete** button.

Figure 4.246 - ACL > ACL Finder

ACL > CPU Filter Configuration Wizard

The CPU Filter Configuration Wizard will aid with the creation of CPU Filter Rules.

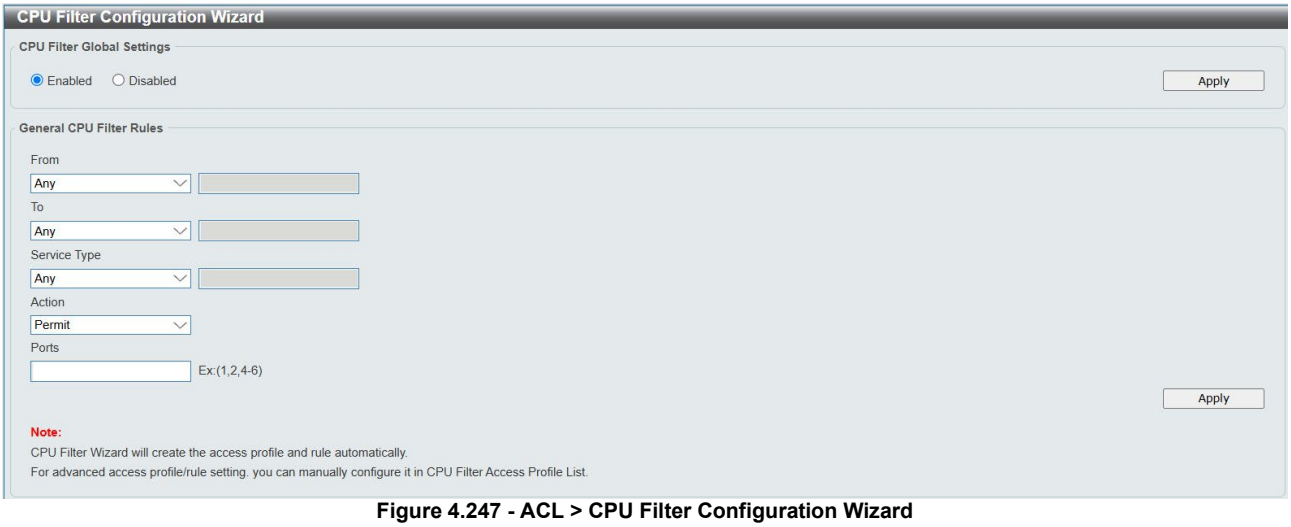


Figure 4.247 - ACL > CPU Filter Configuration Wizard

CPU Filter Global Settings: To enable or disable the CPU filter feature.
Press **Apply** for the settings to take effect.

From: Specify the origin of accessible packets. The possible values are:

Any - Indicates CPU Filter action will be on packets from any source.

MAC Address - Indicates CPU Filter action will be on packets from this MAC address.

IPv4 Addresses - Indicates CPU Filter action will be on packets from this IPv4 source address.

IPv6 - Indicates CPU Filter action will be on packets from this IPv6 source address.

To: Specify the destination of accessible packets. The possible values are:

Any - Indicates CPU Filter action will be on packets to any source.

MAC Address - Indicates CPU Filter action will be on packets to this MAC address. The field of format is xx-xx-xx-xx-xx-xx.

IPv4 Addresses - Indicates CPU Filter action will be on packets to this IPv4 source address.

IPv6 - Indicates CPU Filter action will be on packets to this IPv6 source address.

Service Type: Specify the type of service. The possible values are:

Any - Indicates CPU Filter action will be on packets of any service type.

Ether type - Specifies an Ethernet type for filtering packets.

ICMP All - Indicates CPU Filter action will be on all ICMP packets.

IGMP - IGMP packets can be filtered by IGMP message type.

TCP All - Indicates CPU Filter action will be on all TCP Packets.

TCP Source Port - Take effect if TCP Source Port matches.

TCP Destination Port - Take effect if TCP Destination Port matches.

UDP All - Indicates CPU Filter action will be on all UDP Packets.

UDP Source Port - Take effect if UDP Source Port matches.

UDP Destination Port - Take effect if UDP Destination Port matches.

Action: Specify the CPU Filter forwarding action matching the rule criteria.

Permit - Forwards packets if all other CPU Filter criteria are met.

Deny - Drops packets if all other CPU Filter criteria is met.

Press **Apply** for the settings to take effect.

ACL > CPU Filter Access Profile List

The CPU Filter Access Profile List provides information for configuring CPU Profiles manually. CPU Filter Access profiles are attached to interfaces, and define how packets are forwarded if they match the CPU Filter criteria.

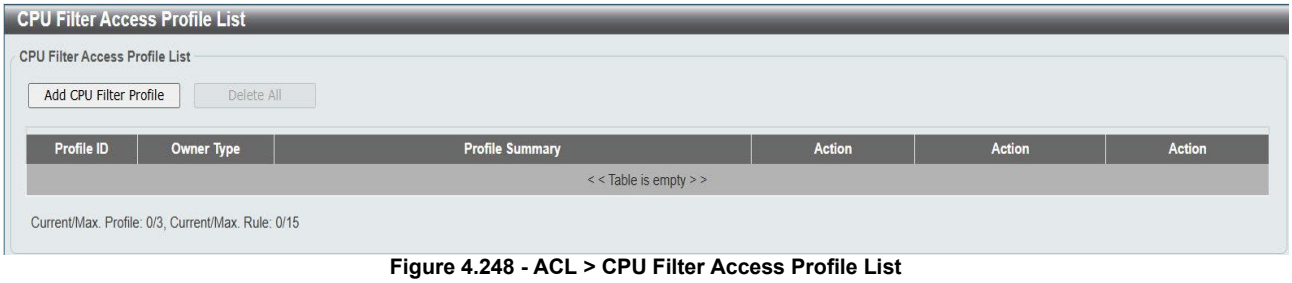


Figure 4.248 - ACL > CPU Filter Access Profile List

The contents of CPU Filter Access Profile List table include:

Profile ID: Indicates the profile Identification number. The possible configured profile IDs are *1~50*, and profile ID *51* is reserved for Voice VLAN.

Owner Type: The owner type of CPU Filter profile, it can be normal CPU Filter, Voice VLAN or Surveillance VLAN.

Profile Summary: Displays the profile summary.

Show Details: To display a CPU Filter's profile details. The CPU Filter profile details are displayed below the CPU Filter table.

Edit/New Rules: To configure or add the CPU access rule in this profile.

To add a new rule, please see **Add CPU Filter Profile** in the next section.

Delete All: To delete all access profile.

To manually add a profile, click **Add CPU Filter Profile**.

Figure 4.249 - ACL > CPU Filter Access Profile List -Add CPU Filter Profile

The steps of adding a CPU Filter profile is like below:

1) After selecting the **Profile ID** and **Frame Type** (MAC, IPv4 or IPv6), specify attributes like Untagged/Tagged (for MAC), or ICMP/IGMP/TCP/UDP/Protocol ID (for IPv4), or Traffic Class (for IPv6), then click **Select** and a simplified frame diagram will be displayed.

2) Select the field of interest and related columns will be displayed in lower part of the page. Enter the filtering mask and click **Create** when done. A filtering mask is to specify the digit that user wants to check. For example, if user wants to check a network of 192.168.1.0/24, then it should enter the IP mask as 255.255.255.0.

3) After the **Profile ID** has been created, it will go back to the main **CPU Filter Access Profile** List page.

ACL > CPU Filter Finder

The CPU Filter Finder page is used to help user to find a previously configured CPU entry. To search for an entry, enter the Profile ID from the drop-down menu, select a port that user would like to view and click **Find.** The table on the lower half of the screen will display the entries. To delete an entry click the corresponding **Delete** button.

Figure 4.250 - ACL > CPU Filter Finder

ACL > ACL Flow Meter

ACL Flow Metering table is a per flow bandwidth control used to limit the bandwidth of the ingress traffic. When the users create an ACL rule to filter packets, a metering rule can be created to associate with this ACL rule to limit traffic. The step of bandwidth is 64kbps. Due to limited metering rules, not all ACL rules can associate with a metering rule.

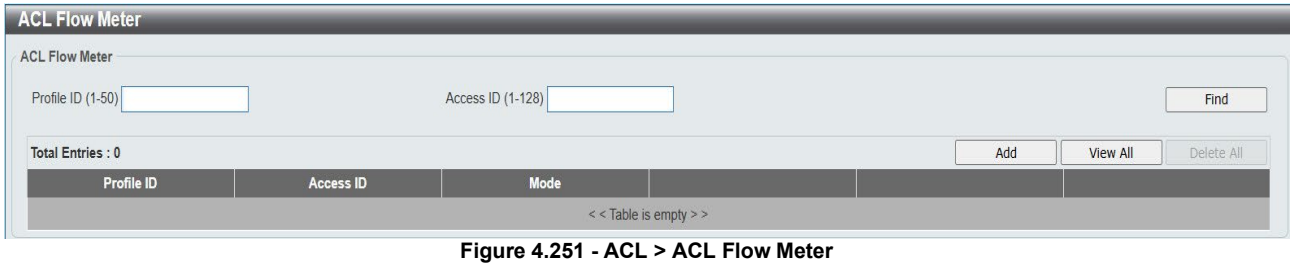


Figure 4.251 - ACL > ACL Flow Meter

Profile ID: The pre-configured Profile ID for which to configure the Flow Metering parameter.

Access ID (1-128): The pre-configured Access ID for which to configure the Flow Metering parameters.

Enter the appropriate information and click **Find** the entries will be displayed on the lower half of the table. To edit and entry click the corresponding **Modify** button, to delete an entry click the corresponding **Delete** button, to add a new entry click the **Add** button which will display the following window for the user to configure.

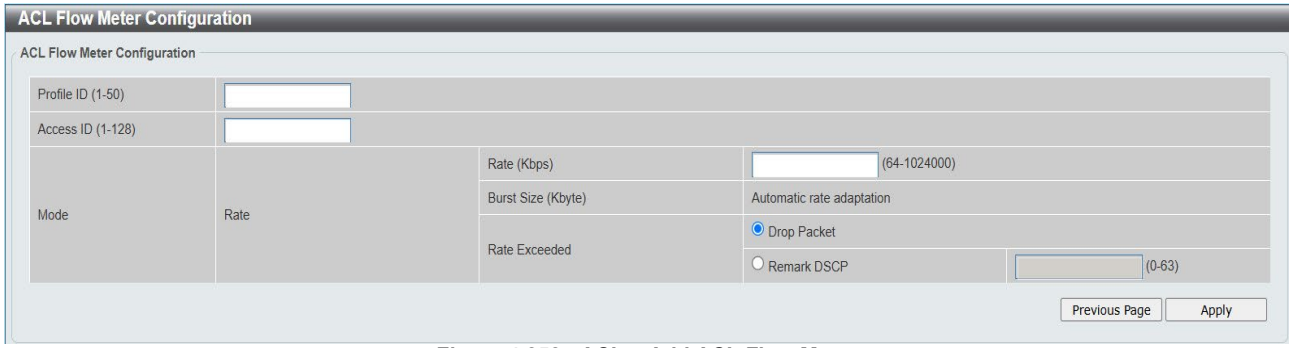


Figure 4.252 - ACL > Add ACL Flow Meter

Profile ID (1-50): Specify the profile ID.

Access ID (1-128): Specify the Access ID that will be used to configure the Flow Metering parameters, enter a value between 1 and 128.

Mode: To be used the corresponding information.

- Rate: Specify the committed information Rate of the packet. The range is from 64 to 1024000 kbyte.

Rate Exceed: Specifies the action when the packet is in yellow color mode.

- Drop Packet: Drops the packet.
- Replace DSCP: Allow user to change the DSCP of the packet.

Click **Apply** to make the configurations take effect.

PoE > PoE Port Settings (DGS-1210-10XP/ME only)

DGS-1210-10XP/ME supports Power over Ethernet (PoE) as defined by the IEEE specification.DGS-1210-10XP/ME supplies power to PD device up to 30W, meeting IEEE802.3af standards and pre-802.3at standards.

DGS-1210-10XP/ME works with all D-Link 802.3af or 802.3at capable devices. The Switch also works in PoE mode with all non-802.3af capable D-Link AP, IP Cam and IP phone equipment via the PoE splitter DWL-P50.

IEEE 802.3at defined that the PSE provides power according to the following classification:

Class	Usage	Output power limit by PSE
0	Default	15.4W
1	Optional	4.0W
2	Optional	7.0W
3	Optional	15.4W
4	Reserved	30W

The PoE port table will display the PoE status including, Port Enable, Power Limit, Power (W), Voltage (V), Current (mA), Classification, Port Status. User can select **From Port** / **To Port** to control the PoE functions of a port. DGS-1210-10XP/ME will auto disable the ports if port current is over 375mA in 802.3af mode or 625mA in pre-802.3at mode.

Note: The PoE Status information of Power current, Power Voltage, and Current is the power usage information of the connected PD; please "Refresh" to renew the information.

Note: The following table listed PoE hardware specifications for each model of DGS-1210/ME CX series:

Model	802.3at compliance port	System Budget
DGS-1210-10XP/ME	1-8	240 Watts

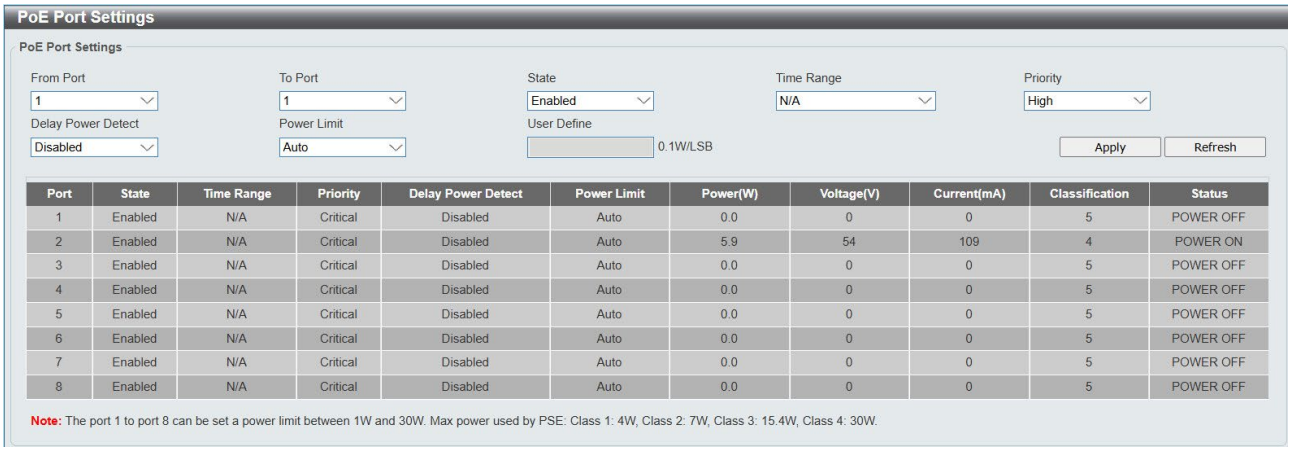


Figure 4.253 – PoE > PoE Port Settings

Parameter	Description
From Port/To Port	Specifies the PoE function of a port or ports

State	Select “Enabled” or “Disabled” to configure PoE function for designated port(s). Default is **Enabled**
Time Range	Select the PoE time profile configured from Time-Based PoE > Time Range Settings to enable the time-based PoE function on designated port(s). Default setting is **N/A**
Priority	Configure the power supply priority as “**Low**”, “**Normal**”, or “**Critical**” on designated port(s). Default is **Normal**.
Delay Power Detect	Configure the delay power detection. Default is Disabled. This switch conforms to IEEE 802.3af and 802.3at standards. The IEEE PoE standard requires a switch to shut off power to a port if the power draw is less than 10mA within a 400ms time interval. To support some non-standard devices that may take longer, user may enable this feature to extend the time interval to 500ms. If the PD is still not powering on, please contact the vendor of the device for support.
Power Limit	This feature allows user to specify the power limit for each ports. If a port requested the power exceeds its power limit, it will shut down. There are options as the following list: **Auto:** Automatic classification the PD’s power consumption. **Class 1:** Specifies that the power limit will be set to 4W **Class 2:** Specifies that the power limit will be set to 7W **Class 3:** Specifies that the power limit will be set to 15.4W **Class 4:** For 802.3at compliance PD devices. Supports up to 30W in this class. **User Define:** Maximum supports to 30W

Click **Apply** to make the configurations take effect or click **Refresh** to redisplay the table.

PoE > PoE System Settings (DGS-1210-10XP/ME only)

This PoE System Settings page will display the PoE status including **System Budget Power**, **Support Total Power**, **Remainder Power**, and **The ratio of system power supply**.

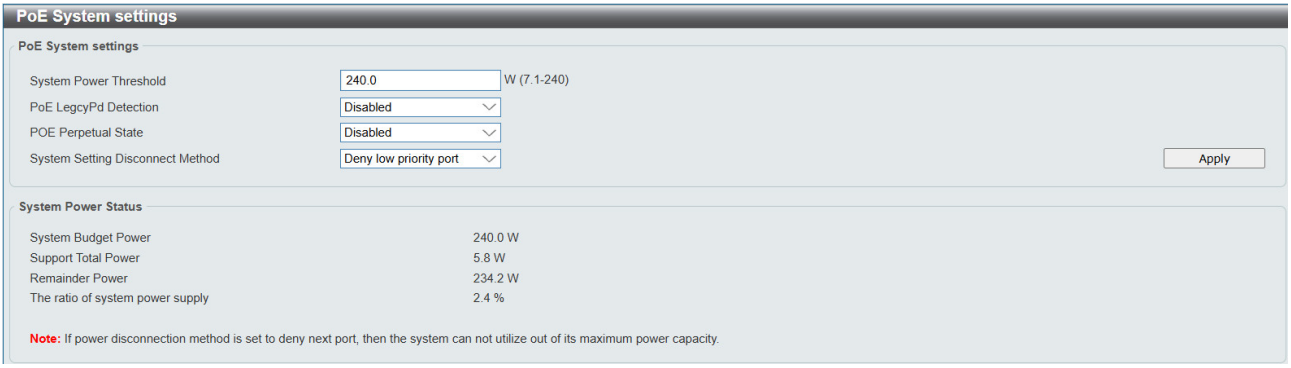


Figure 4.254 – PoE > PoE System Settings

System Power Threshold: Manually configure the system power budget 7 ~ 240 watts for DGS-1210-10XP/ME.

PoE LeacyPD Detection: Specifies the legacy PDs detection status.

System Setting Disconnect Method: Defines the method used to deny power to a port once the threshold is reached. The possible fields are:

Deny next port: When the power budget is exceeded, the next port attempting to power up is denied, regardless of the port priority.

Deny low priority port: The port with the lower priority will be shut down to allow the higher priority port to power up.

Click **Apply** to make the configurations take effect.

System Power Status: Displays the system power status of device.

System Budget Power: Displays the total PoE power budget of this switch.

Support Total Power: Displays the current used power of the switch.

Remainder Power: Displays the spare power of the switch.

The ratio of system power supplied: Displays the percentage of system power supplied of the switch.

PoE > PoE Port Settings > Time Range Settings

The Time Profile page allows users to configure the time profile settings of the device, and PoE Port Settings can select time range via created time profile.

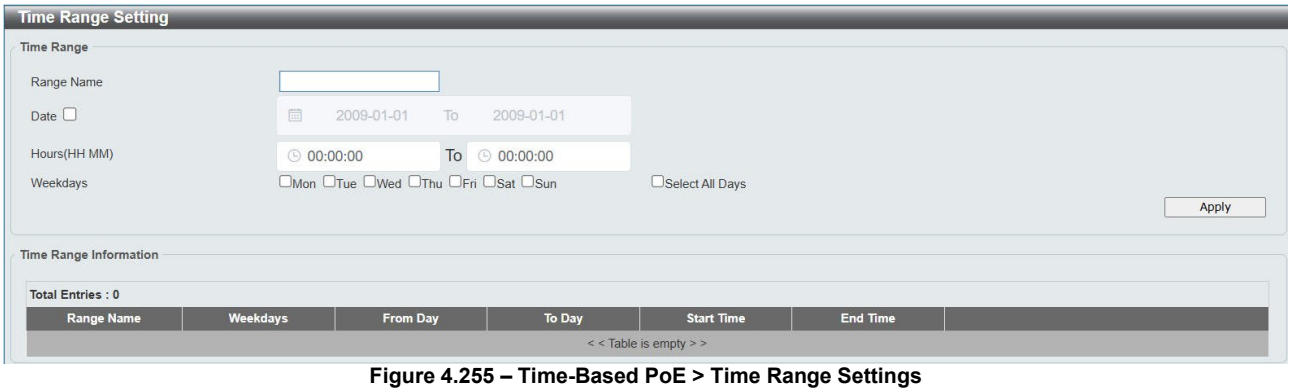


Figure 4.255 – Time-Based PoE > Time Range Settings

Range Name: Specifies the range name.

Date: Specifies the From Day and To Day.

Hours(HH MM): Specifies the Start Time and End Time.

Weekdays: Specifies the work day.

Click **Apply** to create a new time range or click **Delete** to delete a time profile from the table.

PoE > PD Alive Settings(Only for DGS-1210-10XP/ME)

The PD Alive function checks the PoE PD device all the time via ping action. Once the PD device stop responding, DGS-1210/ME Cx series will recycle the PoE port power or notify the network administrator.

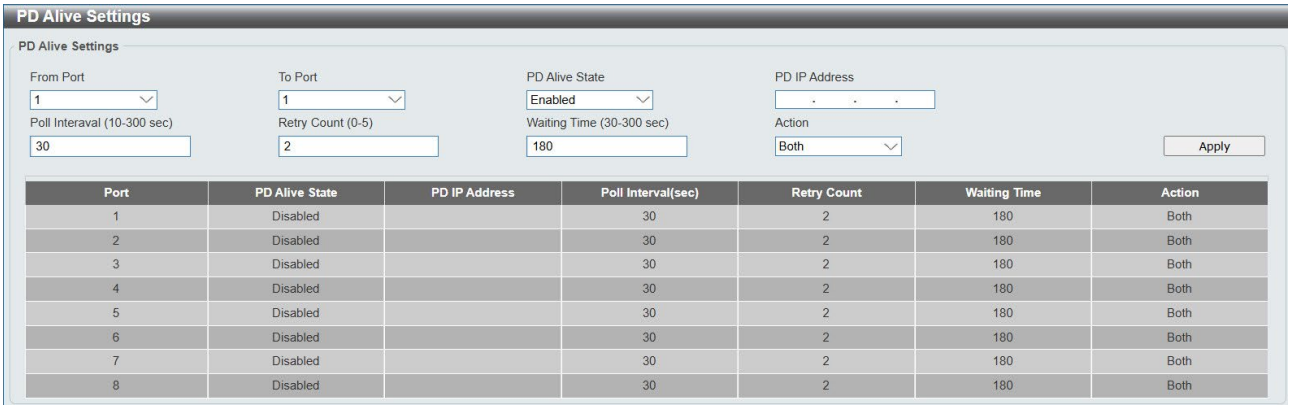


Figure 4.256 –PoE > PD Alive Settings

PD Alive State: To Enable/Disable PD Alive feature.

PD IP Address: Specify the IP address of PD.

Poll Interval: Specify the time interval to check the PD IP address via ping packet. (10~300 Sec, default 30 Sec).

Retry Count: Specify the retry time when PD not responding to ping. (Default: 2 times)

Waiting Time: Specify the time waiting time between each retry. (10~300 Sec, default 180 Sec).

Action: Select the action when PD not responding: Reset, Notify (syslog) or Both. (Default Both).

LLDP > LLDP Global Settings

LLDP (Link Layer Discovery Protocol) provides IEEE 802.1AB standards-based method for switches to advertise themselves to neighbor devices, as well as to learn about neighbor LLDP devices. The switch will keep the information in the Management Information Base (MIB). SNMP utilities can learn the network topology by obtaining the MIB information in each LLDP device. The LLDP function is enabled by default.

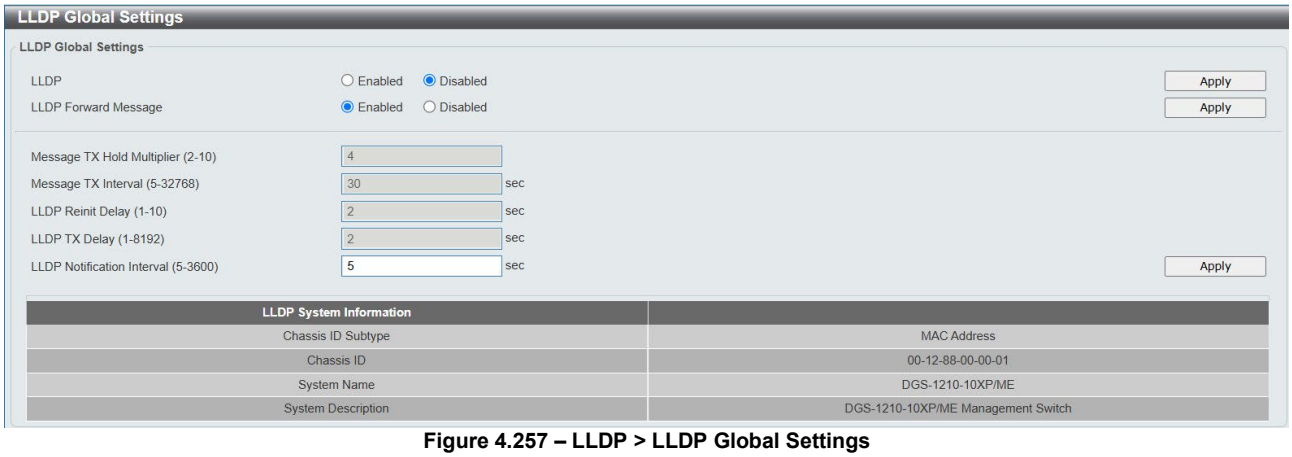


Figure 4.257 – LLDP > LLDP Global Settings

LLDP: When this function is *Enabled*, the switch can start to transmit, receive and process the LLDP packets. For the advertisement of LLDP packets, the switch announces the information to its neighbor through ports. For the receiving of LLDP packets, the switch will learn the information from the LLDP packets advertised from the neighbor in the neighbor table. Click **Apply** to make the change effective.

Message TX Hold Multiplier (2-10): This parameter is a multiplier that determines the actual TTL value used in an LLDPDU. The default value is **4**.

Message TX Interval (5-32768): This parameter indicates the interval at which LLDP frames are transmitted on behalf of this LLDP agent. The default value is **30** seconds.

LLDP Reinit Delay (1-10): This parameter indicates the amount of delay from the time adminStatus becomes "disabled" until re-initialization is attempted. The default value is **2** seconds.

LLDP TX Delay (1-8192): This parameter indicates the delay between successive LLDP frame transmissions initiated by value or status changes in the LLDP local systems MIB. The value for txDelay is set by the following range formula: 1 < txDelay < (0.25 °— msgTxInterval). The default value is **2** seconds.

LLDP > Basic LLDP Port Settings

The Basic LLDP Port Settings page displays LLDP port information and contains parameters for configuring LLDP port settings.

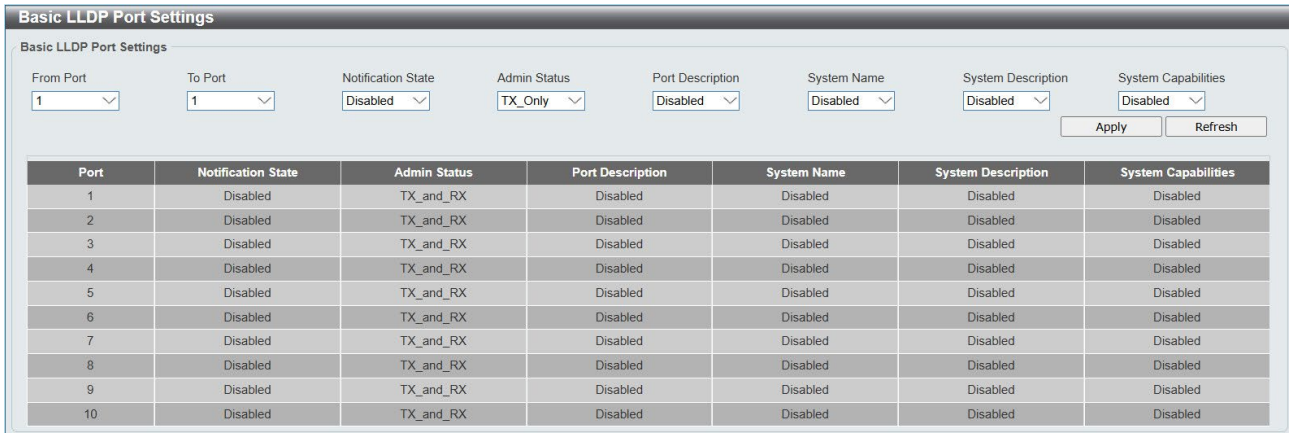


Figure 4.258– LLDP > Basic LLDP Port Settings

From Port/ To Port: A consecutive group of ports may be configured starting with the selected port.

Notification State: Specifies whether notification is sent when an LLDP topology change occurs on the port. The possible field values are:

Enabled – Enables LLDP notification on the port.

Disabled – Disables LLDP notification on the port. This is the default value.

Admin Status: Specifies the LLDP transmission mode on the port. The possible field values are:

TX_Only – Enables transmitting LLDP packets only.

RX_Only – Enables receiving LLDP packets only.

TX_and_RX – Enables transmitting and receiving LLDP packets. This is the default.

Disabled – Disables LLDP on the port.

Port Description: Specifies whether the Port Description TLV is enabled on the port. The possible field values are:

Enabled – Enables the Port Description TLV on the port.

Disabled – Disables the Port Description TLV on the port.

System Name: Specifies whether the System Name TLV is enabled on the port. The possible field values are:

Enabled – Enables the System Name TLV on the port.

Disabled – Disables the System Name TLV on the port.

System Description: Specifies whether the System Description TLV is enabled on the port. The possible field values are:

Enabled – Enables the System Description TLV on the port.

Disabled – Disables the System Description TLV on the port.

System Capabilities: Specifies whether the System Capabilities TLV is enabled on the port. The possible field values are:

Enabled – Enables the System Capabilities TLV on the port.

Disabled – Disables the System Capabilities TLV on the port.

Define these parameter fields. Click **Apply** to implement changes made and click **Refresh** to refresh the table information.

LLDP > 802.1 Extension LLDP Port Settings

This 802.1 Extension LLDP Port Settings page is used to configure the LLDP Port settings.

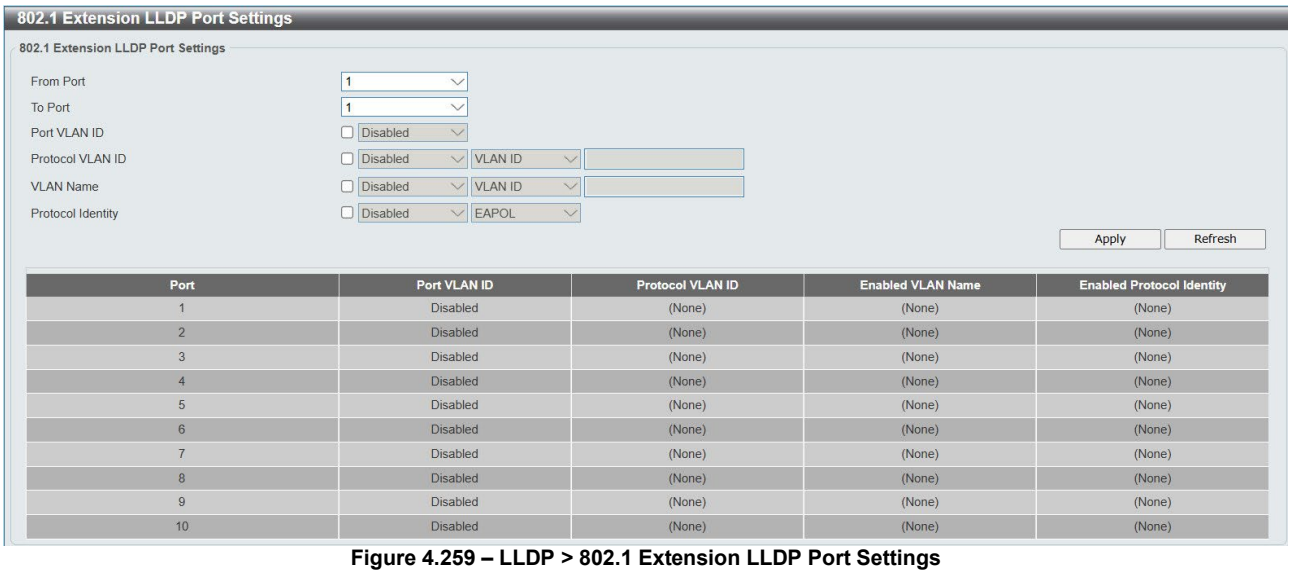


Figure 4.259 – LLDP > 802.1 Extension LLDP Port Settings

From Port / To Port : A consecutive group of ports may be configured starting with the selected port.

Port VLAN ID : Specifies the Port VLAN ID to be enabled or disabled.

Protocol VLAN ID : Specifies the VLAN ID to be enabled or disabled in the LLDP port. If select Enabled, users can specifies the content of VLAN ID.

VLAN Name : Specifies the VLAN name to be enabled or disabled in the LLDP port. If select Enabled, users can specifies the content of VLAN Name.

Protocol Identity : Specifies the Protocol Identity to be enabled or disabled in the LLDP port. If select Enabled, users can specifies the EAPOL, LACP, GVRP, STP or ALL.

Click **Apply** to implement changes made and click **Refresh** to refresh the table information.

LLDP > 802.3 Extension LLDP Port Settings

The 802.3 Extension LLDP Port Settings page displays 802.3 Extension LLDP port information and contains parameters for configuring 802.3 Extension LLDP port settings.

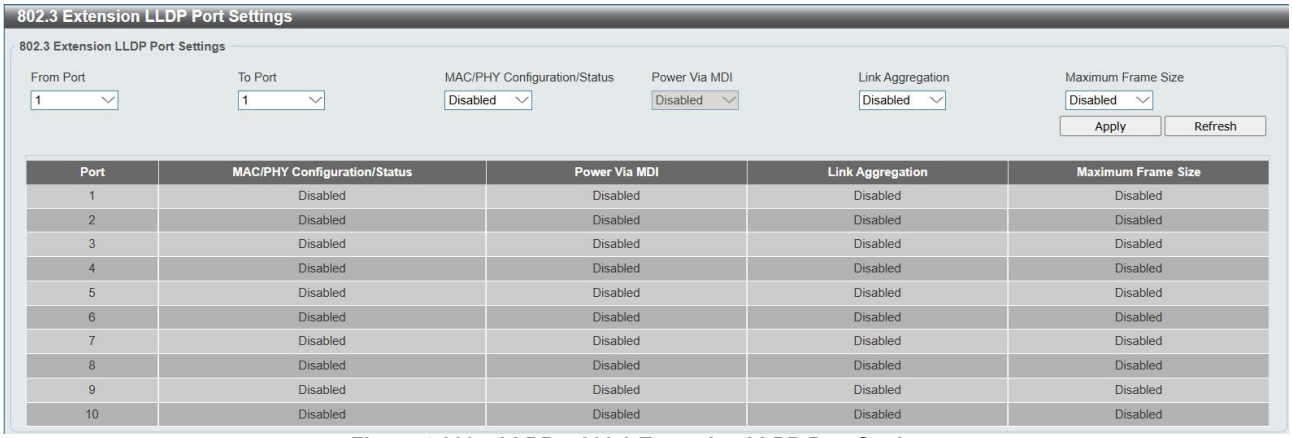


Figure 4.260 – LLDP > 802.3 Extension LLDP Port Settings

From Port/To Port: A consecutive group of ports may be configured starting with the selected port.

MAC/PHY Configuration/Status: Specifies whether the MAC/PHY Configuration Status is enabled on the port. The possible field values are:

Enabled – Enables the MAC/PHY Configuration Status on the port.

Disabled – Disables the MAC/PHY Configuration Status on the port.

Power Via MDI: Advertises the Power via MDI implementations supported by the port. The possible field values are:

Enabled – Enables the Power via MDI configured on the port.

Disabled – Disables the Power via MDI configured on the port.

Link Aggregation: Specifies whether the link aggregation is enabled on the port. The possible field values are:

Enabled – Enables the link aggregation configured on the port.

Disabled – Disables the link aggregation configured on the port.

Maximum Frame Size: Specifies whether the Maximum Frame Size is enabled on the port. The possible field values are:

Enabled – Enables the Maximum Frame Size configured on the port.

Disabled – Disables the Maximum Frame Size configured on the port.

Define these parameter fields. Click **Apply** to implement changes made and click **Refresh** to refresh the table information.

LLDP > LLDP Management Address Settings

The LLDP Management Address Settings allows the user to set management address which is included in LLDP information transmitted.

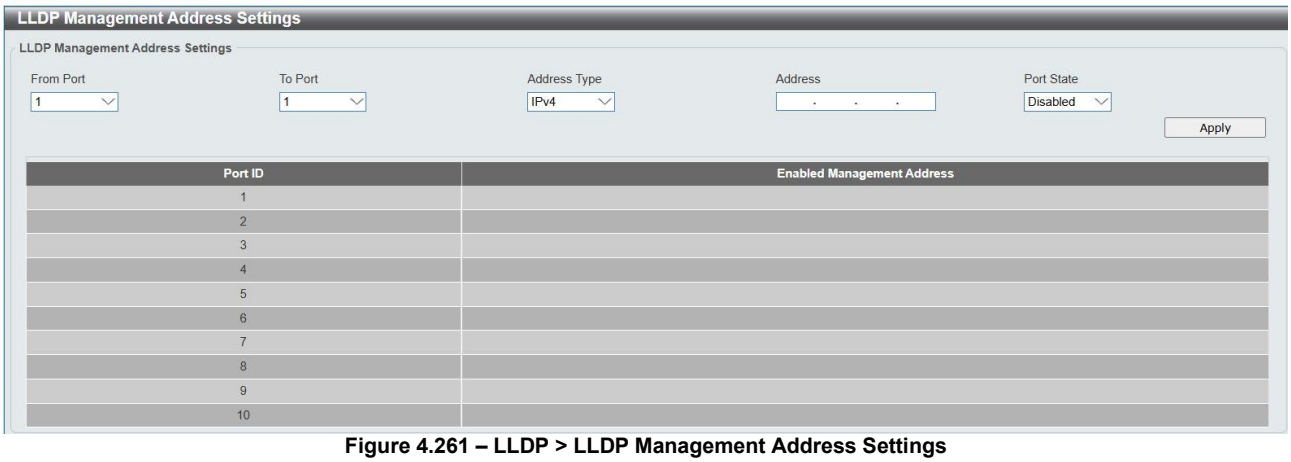


Figure 4.261 – LLDP > LLDP Management Address Settings

From Port/To Port: A consecutive group of ports may be configured starting with the selected port.

Address Type: Specify the LLDP address type on the port. The value is IPv4/IPv6.

Address: Specify the address.

Port State: Specify whether the Port State is enabled n the port. The possible field values are:

Enabled – Enables the port state configured on the port.

Disabled – Disables the port state configured on the port.

Click Apply to make the configurations take effect.

LLDP > LLDP Statistics Table

The LLDP Statistics page displays an overview of all LLDP traffic.

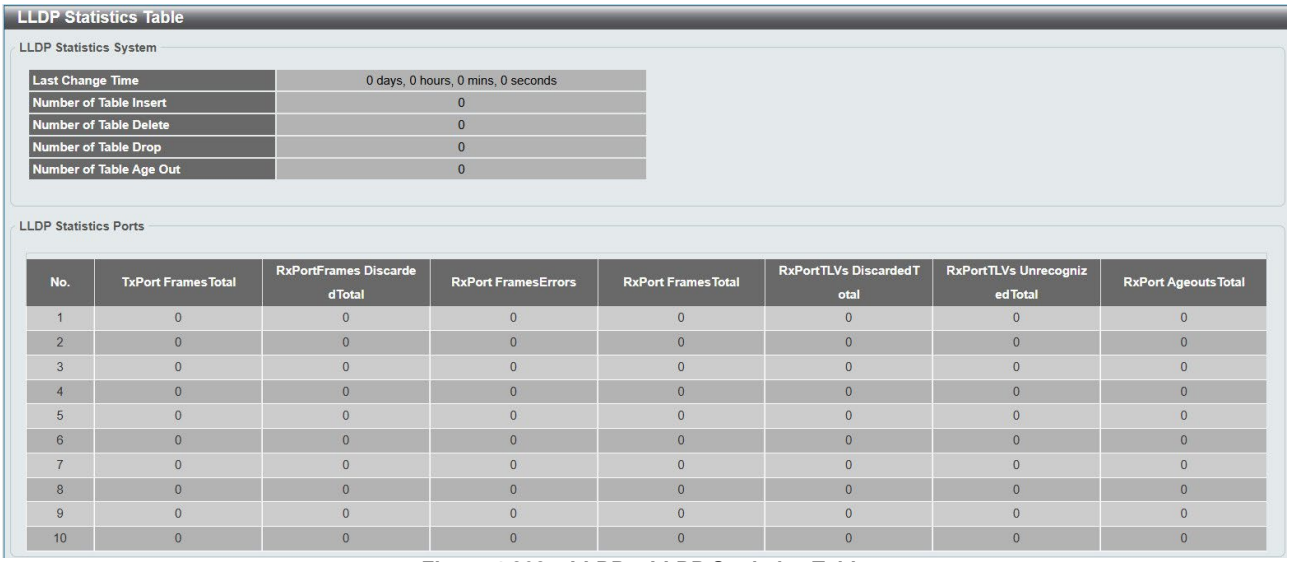


Figure 4.262 – LLDP > LLDP Statistics Table

The following information can be viewed:

LLDP Statistics System: Displays the counters that refer to the whole switch.

Last Change Time – Displays the time for when the last change entry was last deleted or added. It is also displays the time elapsed since last change was detected.

Number of Table Insert – Displays the number of new entries inserted since switch reboot.

Number of Table Delete – Displays the number of new entries deleted since switch reboot.

Number of Table Drop – Displays the number of LLDP frames dropped due to that the table was full.

Number of Table Age Out – Displays the number of entries deleted due to Time-To-Live expiring.

LLDP Port Statistics: Displays the counters that refer to the ports.

TxPort FramesTotal – Displays the total number of LLDP frames transmitted on the port.

RxPort FramesDiscarded – Displays the total discarded frame number of LLDP frames received on the port.

RxPort FramesErrors – Displays the Error frame number of LLDP frames received on the port.

RxPort Frames – Displays the total number of LLDP frames received on the port.

RxPortTLVsDiscarded – Each LLDP frame can contain multiple pieces of information, known as TLVs. If a TLV is malformed, it is counted and discarded.

RxPortTLVsUnrecognized – Displays the number of well-formed TLVs, but with a known type value.

RxPort Ageouts – Each LLDP frame contains information about how long time the LLDP information is valid. If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.

LLDP > LLDP Management Address Table

The LLDP Management Address Table page displays the detailed management address information for the entry.

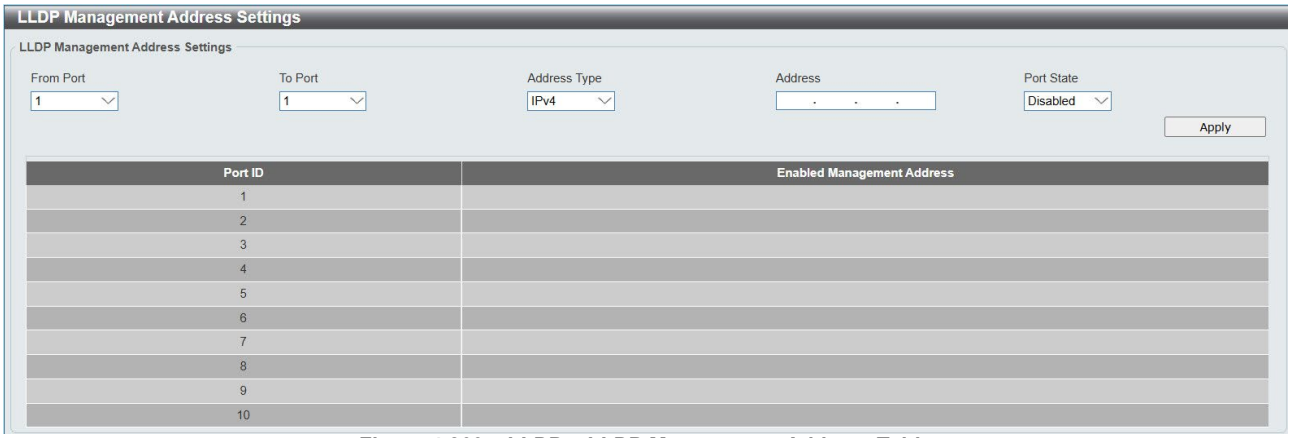


Figure 4.263 – LLDP > LLDP Management Address Table

From Port/To Port: A consecutive group of ports may be configured starting with the selected port.

Subtype: Displays the managed address subtype. For example, IPv4 or IPv6.

Address: Set Management IP address.

Port State: Enable/Disable LLDP Management Address Settings..

LLDP > LLDP Local Port Table

The LLDP Local Port Table page displays LLDP local port information.

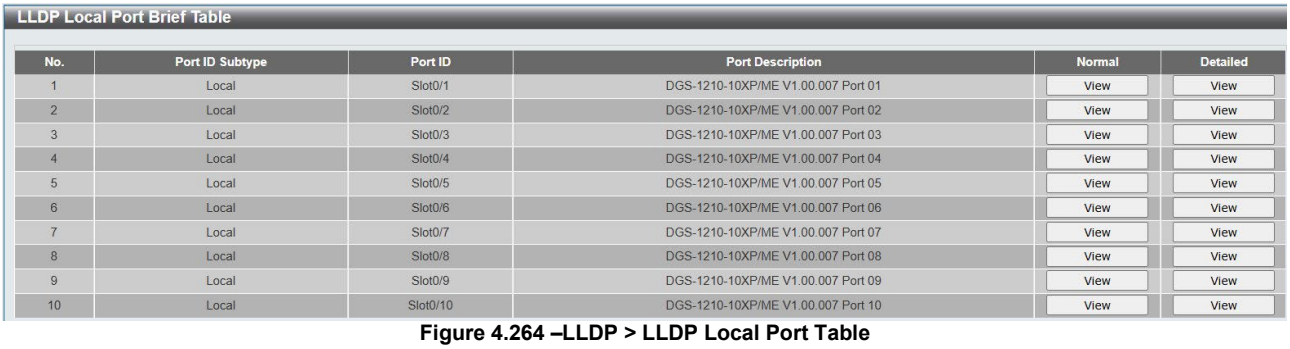


Figure 4.264 –LLDP > LLDP Local Port Table

No: Displays the port number.

Port ID Subtype: Displays the port ID subtype.

Port ID: Displays the port ID (Unit number/Port number).

Port Description: Displays the port description.

Click **View** of Normal column to display more information.

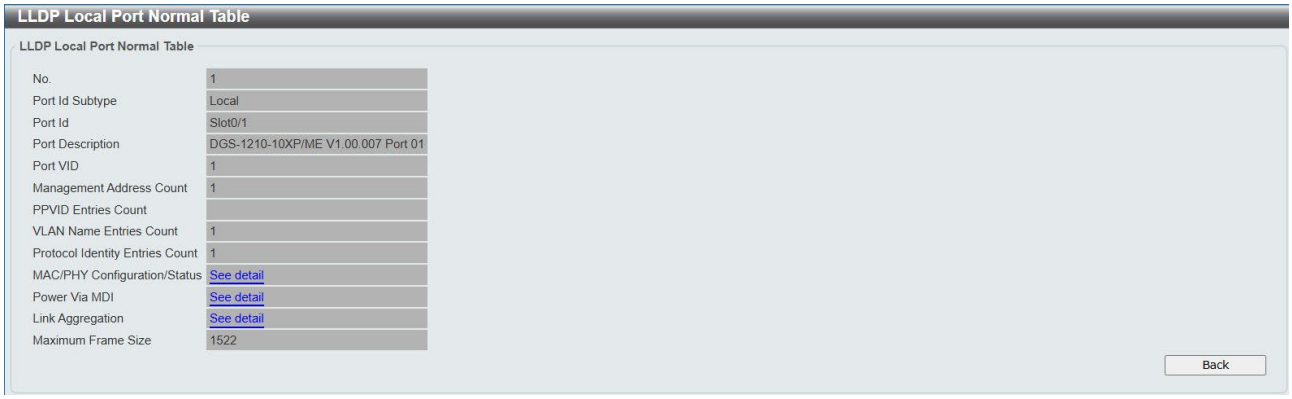


Figure 4.265 – LLDP > LLDP Local Port Normal Table

Click **View** of Detailed column to display detail information.

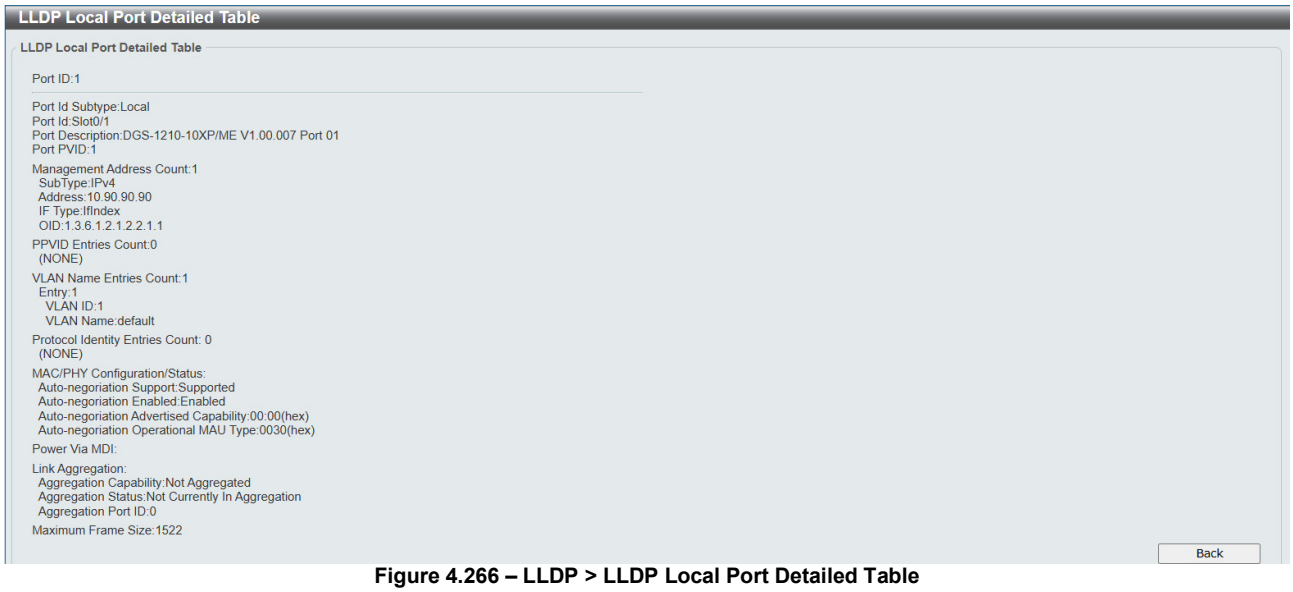


Figure 4.266 – LLDP > LLDP Local Port Detailed Table

LLDP > LLDP Remote Port Table

This LLDP Remote Port Table page is used to display the LLDP Remote Port Brief Table. Select port number and click **Search** to display additional information.

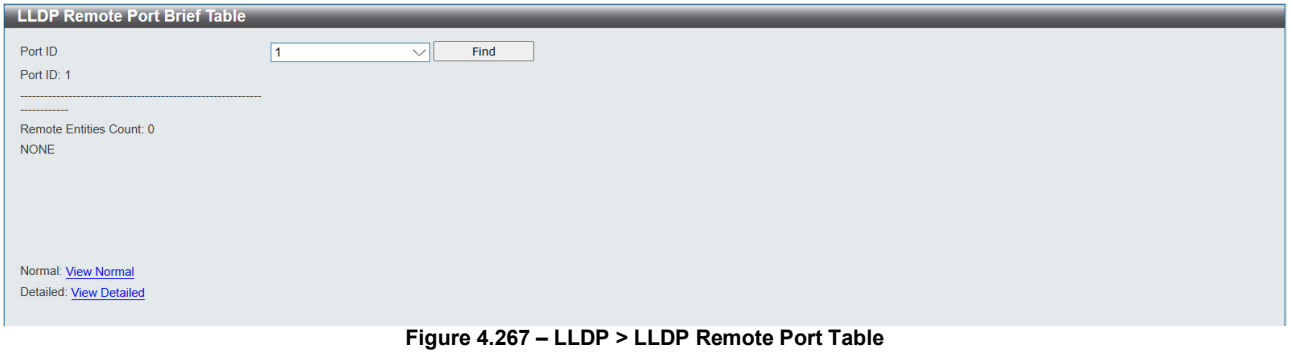


Figure 4.267 – LLDP > LLDP Remote Port Table

To view the settings for a remote port, click **View Normal** and the following page displays.

Figure 4.268– LLDP > LLDP Remote Port Normal Table

To view the detail settings for a remote port, click **View Detailed** and the following page displays.

Figure 4.269 – LLDP > LLDP Remote Port Detailed Table

LLDP > LLDP-MED Settings (Only DGS-1210-10XP/ME support settings)

By selecting a range of ports (**From Port** and **To Port**), the power PSE TLV type can be enabled for all selected ports to indicate the power source equipment (PSE) switch to transmit high power (15.4 to 30 Watts) to the pre-standard of 802.3at power devices via LLDP MDI TLV. Through this feature, the PSE can provide precise output power to the pre-standard of 802.3at power devices and achieve optimal power management.

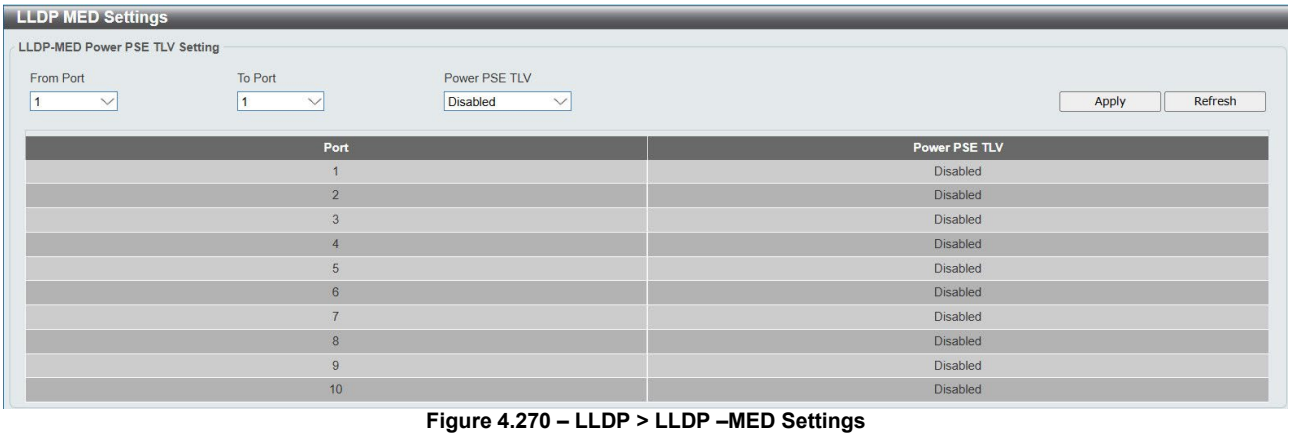


Figure 4.270 – LLDP > LLDP –MED Settings

L3 Functions > IPv4 Static Route

The Switch supports static routing for IPv4 formatted addressing. User can create up to 256 static route entries for IPv4. For IPv4 static routes, once a static route has been set, the Switch will send an ARP request packet to the next hop router that has been set by the user. Once an ARP response has been retrieved by the Switch from that next hop, the route becomes enabled. However, if the ARP entry already exists, an ARP request will not be sent.

The Switch also supports a floating static route, which means that the user may create an alternative static route to a different next hop. This secondary next hop device route is considered as a backup static route for

when the primary static route is down. If the primary route is lost, the backup route will uplink and its status will become active. Entries into the Switch's forwarding table can be made using both an IP address subnet mask and a gateway.

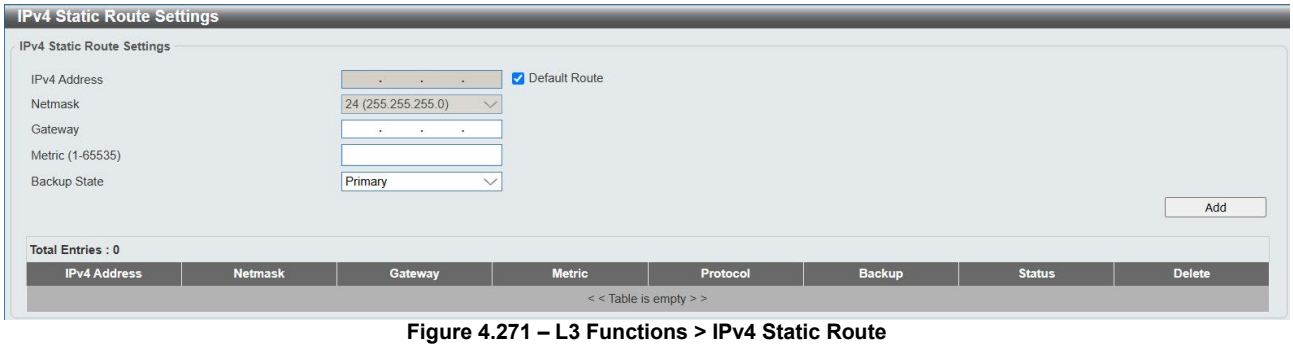


Figure 4.271 – L3 Functions > IPv4 Static Route

IPv4 Address: Specifies an IPv4 address to be assigned to the static route.

Netmask: Specifies a subnet mask to be applied to the corresponding subnet mask of the IPv4 address.

Gateway: Specifies the entry of a Gateway IP address to be applied to the corresponding gateway of the IPv4 address.

Metric (1-65535): Represents the metric value of the IP interface entered into the table. The value ranges between 1 and 65535.

Backup State: Each IP address can only have one primary route, while other routes should be assigned to the backup state. When the primary route failed, Switch will try the backup routes according to the order learnt by the routing table until route success. The field represents the Backup state that the Static and Default Route is configured for.

Click **Add** to create a new IPv4 static route entry.

L3 Functions > IPv4 Routing Table Finder

The IPv4 routing table stores all the external routes information of the Switch. The **IPv4 Routing Table Finder** page displays all the routing information on the Switch.

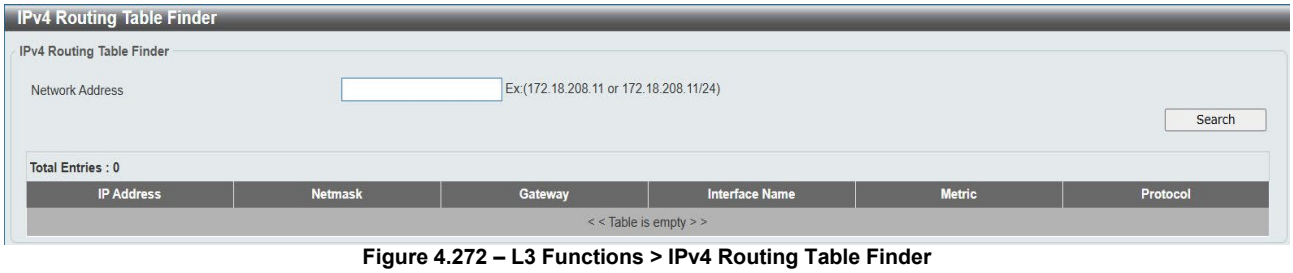


Figure 4.272 – L3 Functions > IPv4 Routing Table Finder

Network Address; Specifies the destination network address of the route to be displayed.

Click **Search** to display the information of specified route entry.

L3 Functions > IPv6 Static Route

A static entry of an IPv6 address can be entered into the Switch's routing table for IPv6 formatted addresses.

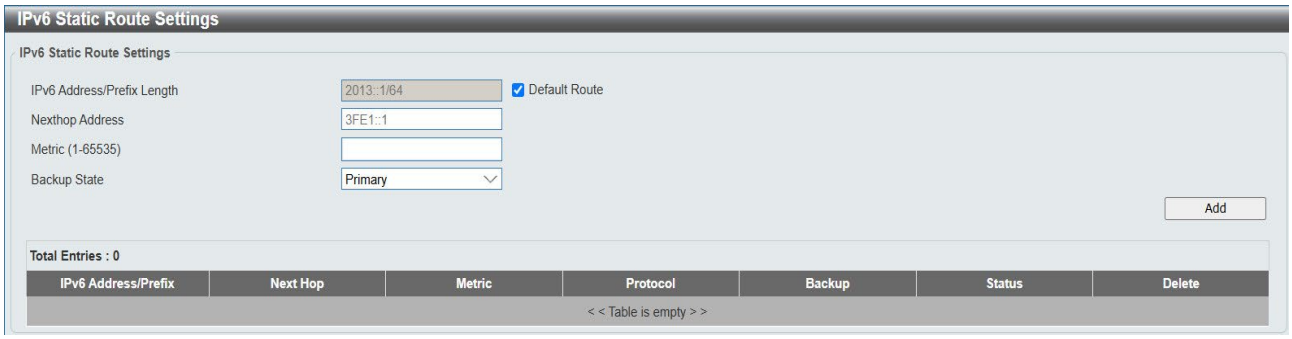


Figure 4.273 – L3 Functions > IPv6 Static Route

IPv6 Address / Prefix Length: Specifies an IPv6 address to be assigned to the static route.

Nexthop Address: Specifies the corresponding IPv6 address for the next hop gateway address in IPv6 format.

Metric (1-65535): Specifies a metric of the IPv6 interface into the table representing the number of routers between the Switch and the IPv6 address above. The value ranges between 1 and 65535.

Backup State: Each IPv6 address can only have one primary route, while other routes should be assigned to the backup state. When the primary route failed, the Switch will try the backup routes according to the order learnt by the routing table until route success. This field represents the backup state for the IPv6 configured. This field may be **Primary** or **Backup**.

Click **Add** to create a new IPv6 static route entry.

L3 Functions > IPv6 Routing Table Finder

The IPv6 routing table stores all the external routes information of the Switch. The **IPv6 Routing Table Finder** page displays all the routing information on the Switch.

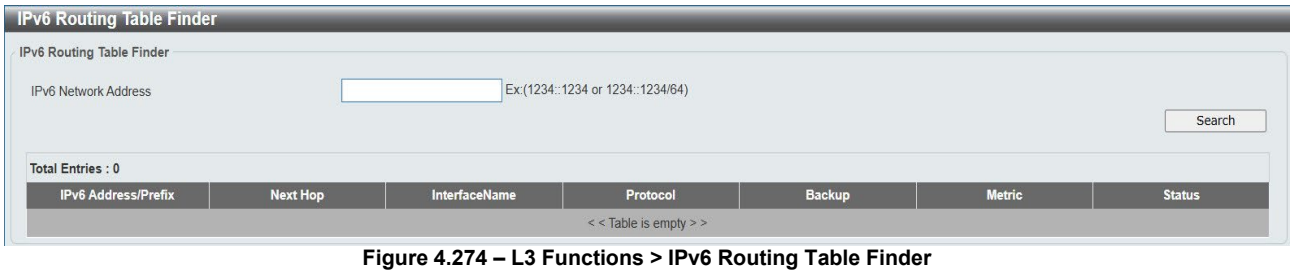


Figure 4.274 – L3 Functions > IPv6 Routing Table Finder

Network Address; Specifies the destination network address of the route to be displayed.

Click **Search** to display the information of specified route entry.

Appendix A - Ethernet Technology

This chapter will describe the features of the D-Link and provide some background information about Ethernet/Fast Ethernet/Gigabit Ethernet switching technology.

Gigabit Ethernet Technology

Gigabit Ethernet is an extension of IEEE 802.3 Ethernet utilizing the same packet structure, format, and support for CSMA/CD protocol, full duplex, and management objects, but with a tenfold increase in theoretical throughput of over 100-Mbps Fast Ethernet and a hundredfold increase over 10-Mbps Ethernet. Since it is compatible with all 10-Mbps and 100-Mbps Ethernet environments, Gigabit Ethernet provides a straightforward upgrade without wasting existing investments in hardware, software, or trained personnel.

The increased speed and extra bandwidth offered by Gigabit Ethernet is essential in solving network bottlenecks, which frequently develops as more advanced computer users and newer applications continue to demand greater network resources. Upgrading key components, such as backbone connections and servers to Gigabit Ethernet technology, can greatly improve network response times as well as significantly speed up the traffic between subnets.

Gigabit Ethernet enables fast optical fiber connections to support video conferencing, complex imaging, and similar data-intensive applications. Likewise, since data transfers occur 10 times faster than Fast Ethernet, servers outfitted with Gigabit Ethernet NIC's are able to perform 10 times the number of operations in the same amount of time.

In addition, the phenomenal bandwidth delivered by Gigabit Ethernet is the most cost-effective method to take advantage of today and tomorrow's rapidly improving switching and routing internetworking technologies. With expected advances in the coming years in silicon technology and digital signal processing, which will enable Gigabit Ethernet to eventually operate over unshielded twisted-pair (UTP) cabling, a flexible foundation for the next generation of network technology products will be created. This will outfit your network with a powerful 1000-Mbps-capable backbone/server connection.

Fast Ethernet Technology

The growing importance of LANs, and the increasing complexity of desktop computing applications are fueling the need for high performance networks. A number of high-speed LAN technologies have been proposed to provide greater bandwidth and improve client/server response times. Among them, 100BASE-T (Fast Ethernet) provides a non-disruptive, smooth evolution from the current 10BASE-T technology. The non-disruptive and smooth evolution nature, and the dominating potential market base, virtually guarantees cost-effective and high performance Fast Ethernet solutions.

100Mbps Fast Ethernet is a standard specified by the IEEE 802.3 LAN committee. It is an extension of the 10Mbps Ethernet standard with the ability to transmit and receive data at 100Mbps, while maintaining the CSMA/CD Ethernet protocol. Since the 100Mbps Fast Ethernet is compatible with all other 10Mbps Ethernet environments, it provides a straightforward upgrade and utilizes existing investments in hardware, software, and personnel training.

Switching Technology

Another approach to push beyond the limits of Ethernet technology is the development of switching technology. A switch bridges Ethernet packets at the MAC address level of the Ethernet protocol transmitting among connected Ethernet or Fast Ethernet LAN segments.

Switching is a cost-effective way of increasing the total network capacity available to users on a local area network. A switch increases capacity and decreases network loading by dividing a local area network into different segments, which won't compete with each other for network transmission capacity.

The switch acts as a high-speed selective bridge between the individual segments. The switch, without interfering with any other segments, automatically forwards traffic that needs to go from one segment to another. By doing this the total network capacity is multiplied, while still maintaining the same network cabling and adapter cards.

Appendix B - Features

L2 Features

Supports up to 16K MAC address
Supports 256 static MAC
IGMP snooping:

- Supports 1024 multicast groups shared with MLD

- Supports at least 256 static multicast groups

Limited IP Multicast:
- Support up to 24 profiles and each profile can add up to 1024 multicast groups
- Able to configure the maximum multicast group number for a port, ranging from 1-256

MLD Snooping:
- Supports 1024 MLD snooping groups shared with IGMP
- Supports 256 static multicast addresses

802.1D Spanning Tree
802.1w RSTP
802.1s MSTP: up to 64 instances
Loopback Detection
802.3ad Link Aggregation: Support max 8 groups per device, 8 ports per group
Port mirroring
IPv6 Neighbor Discovery:
- Supports Max 512 ND entries
- Support up to 64 static ND entries

SNTP
LLDP
L2 Multicast Filtering

VLAN

802.1Q VLAN standard (VLAN Tagging)
Total 4094 VLAN groups
Asymmetric VLAN
Management VLAN
ISM VLAN
Private VLAN
GVRP: Support 256 dynamic VLANs
VLAN Trunking
Supports Port-based Q-in-Q

L3 Features

ARP:
- Max 256 ARP entries
- Support 256 static ARP

IPv4 / IPv6 Static Route

QoS (Quality of Service)

Be able to classify packets according to follow contents:

- Switch port
- 802.1p priority
- VID
- MAC address
- IP address
- IPv6 Traffic Class
- TCP/UDP Port
- DSCP
- TOS
- Protocol type
- TCP/UDP port number Up to 8 queues per port

Supports Strict / WRR mode in queue handling
Support Port and Flow based bandwidth control

AAA

802.1X Local/RADIUS/TACACS+ server
802.1X port-based/MAC-based access control
RADIUS Accounting: Support Network accounting (for 802.1x user)
User Account Privilege for Management Access:
- Support 4 level user accounts
  - Operator (Read/Write)
  - Administrator (Read/Write)
  - Power user (for account management and service)
  - User (read only)

ACL

Max 6 ingress ACL profile, 128 ingress ACL rules per AC: profile, total 768 ingress ACL rules
Each rule can be associated to a single port, multiple ports
Support different ACL policy packet contents:

- Switch port
- MAC address
- Ether type
- IPv4 address
- IPv6 address
- TOS
- 802.1p
- DSCP
- Protocol type
- TCP/UDP port number
- IPv6 traffic class

Security

Trusted Host
Safeguard Engine
CPU Protect
Gratuitous ARP
Port Security: Support 64 MACs per port
Traffic Segmentation
D-Link Safeguard Engine
802.1x
DHCP Server Screening: Able to configure IPv4 and IPv6 addresses for DHCP server.
SSH: Support v2 and IPv6
SSL: Support TLS 1.0/1.1/1.2/1.3, IPv4 and IPv6
Smart Binding

- Supports D-Link IMPB

- Supports ARP packet Inspection as default, ARP and IP packet Inspection as option.

- Supports DHCP Snooping

Dos Attack Prevention
MAC-based Access Control
WAC

OAM

Cable Diagnostics: Detect and show cable length and status
802.3ah
- Support 802.3ah link layer remote loopback and discovery
- 802.3ah D-Link extension: D-link Undirectional Link Detection (DULD)

Management

Web-based GUI
D-Link proprietary CLI
Telnet Server
SNMP support
DHCP client
DHCP Relay: Support DHCP local relay, option 82 and 12.
DHCPv6 Relay: Support DHCP local relay and option 37
SNMP Trap
System Log: Support log server with IPv4 or IPv6 address
RMON v1/v2
Password access control
Password Encryption
Web-based configuration backup / restoration
Reset, Reboot


D-Link
Building Networks for People