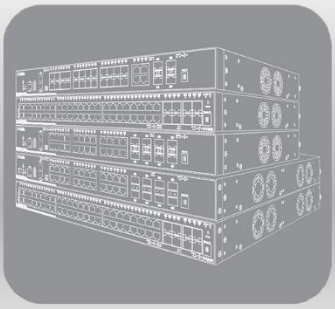


Web UI Reference Guide

Product Model: DGS-1250 Series

Gigabit Ethernet Smart Managed Switch

Release 2.03

November, 2021

Table of Contents

1. Introduction

This manual's software descriptions are based on the software release **2.03**. The features listed here are the subset of features that are supported by the DGS-1250 Series Switch.

Audience

This reference manual is intended for network administrators and other IT networking professionals responsible for managing the Switch by using the Web User Interface (Web UI). The Web UI is the secondary management interface to the DGS-1250 Series Switch, which will be generally be referred to simply as the "Switch" within this manual. This manual is written in a way that assumes that you already have the experience and knowledge of Ethernet and modern networking principles for Local Area Networks.

Other Documentation

The documents below are a further source of information in regards to configuring and troubleshooting the Switch. All the documents are available either from the CD, bundled with this Switch, or from the D-Link website. Other documents related to this Switch are:

- *DGS-1250 Series Hardware Installation Guide*
- *DGS-1250 Series CLI Reference Guide*

Conventions

Convention	Description
Boldface Font	Indicates a button, a toolbar icon, menu, or menu item. For example, open the **File** menu and choose **Cancel**. Used for emphasis. May also indicate system messages or prompts appearing on screen. For example, **You have mail**. Bold font is also used to represent filenames, program names, and commands. For example, use the **copy** command.
Initial capital letter	Indicates a window name. Names of keys on the keyboard have initial capitals. For example, Click Enter.
Menu Name > Menu Option	Indicates the menu structure. **Device > Port > Port Properties** means the **Port Properties** menu option under the **Port** menu option that is located under the **Device** menu.
`Blue Courier Font`	This convention is used to represent an example of a screen console display including example entries of CLI command input with the corresponding output.

Notes, Notices, and Cautions

Below are examples of the three types of indicators used in this manual. When administering your Switch using the information in this document, you should pay special attention to these indicators. Each example below provides an explanatory remark regarding each type of indicator.

NOTE: A note indicates important information that helps you make better use of your device.

NOTICE: A notice indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

CAUTION: A caution indicates a potential for property damage, personal injury, or death.

2. Web-based Switch Configuration

Management Options

The Switch provides multiple access platforms that can be used to configure, manage, and monitor networking features available on this Switch. Currently there are three management platforms available, which are described below.

Command Line Interface (CLI)

The Switch can be managed, out-of-band, by using the console port on the front panel of the Switch. Alternatively, the Switch can also be managed, in-band, by using a Telnet connection to any of the LAN ports on the Switch.

For more information about the CLI, refer to the *DGS-1250 Series CLI Reference Guide*.

SNMP-based Management

The Switch can be managed with an SNMP-compatible Network Management System (NMS). The Switch supports SNMP v1/v2c/v3. The SNMP agent on the Switch decodes the incoming SNMP messages and responds to requests with MIB objects stored in the database. The SNMP agent on the Switch updates the MIB objects to generate statistics and counters.

Web User Interface (Web UI)

The Web UI can be accessed from any computer running web browsing software connected to any of the RJ45 or SFP/SFP+ ports. The Web UI on the Switch can also be accessed using an HTTPS (SSL) connection.

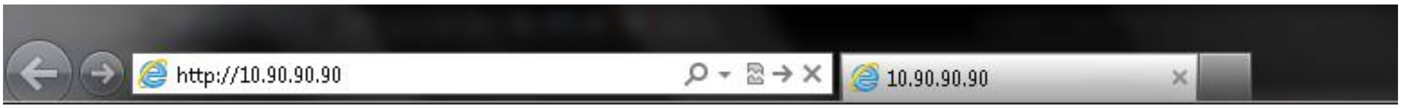
The Web UI is a graphical representation of the features that can be viewed and configured on the Switch. Most of the features available through the CLI can be accessed through the Web UI. Web browsers like Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, or Safari can be used.

Logging into the Web UI

To access the Web UI open a standard web browser and enter the IP address of the Switch into the address bar of the browser and press the ENTER key.

NOTE: The factory default IP address of the Switch is **10.90.90.90** with a subnet mask of **255.0.0.0**.

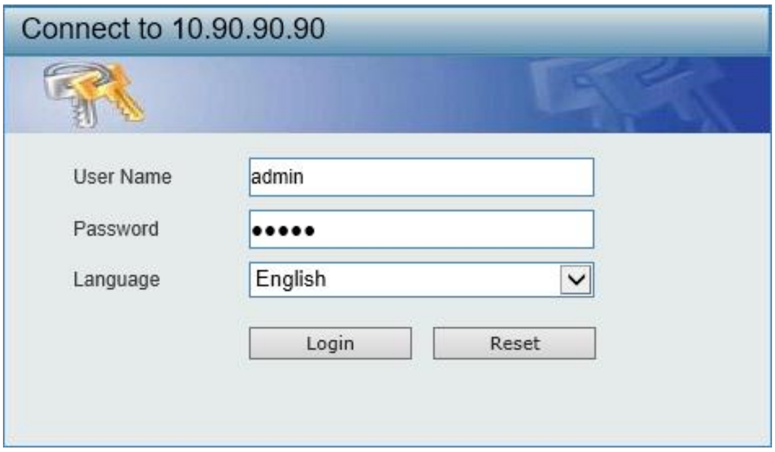
NOTE: The factory default username is *admin* and password is *admin*.



http://10.90.90.90

Figure 2-1 Displays entering the IP address in Internet Explorer

After pressing the **Enter** key, the following authentication window should appear, as shown below.



Connect to 10.90.90.90

User Name: admin

Password: •••••

Language: English

Figure 2-2 Web UI Login Window

Enter the **User Name** and **Password** in the corresponding fields and click the **Login** button.

After clicking the **Login** button, the Web UI opens.

The management features available in the Web UI of the Switch are explained in the chapters below.

NOTE: The Switch only supports ASCII characters for input values.

Smart Wizard

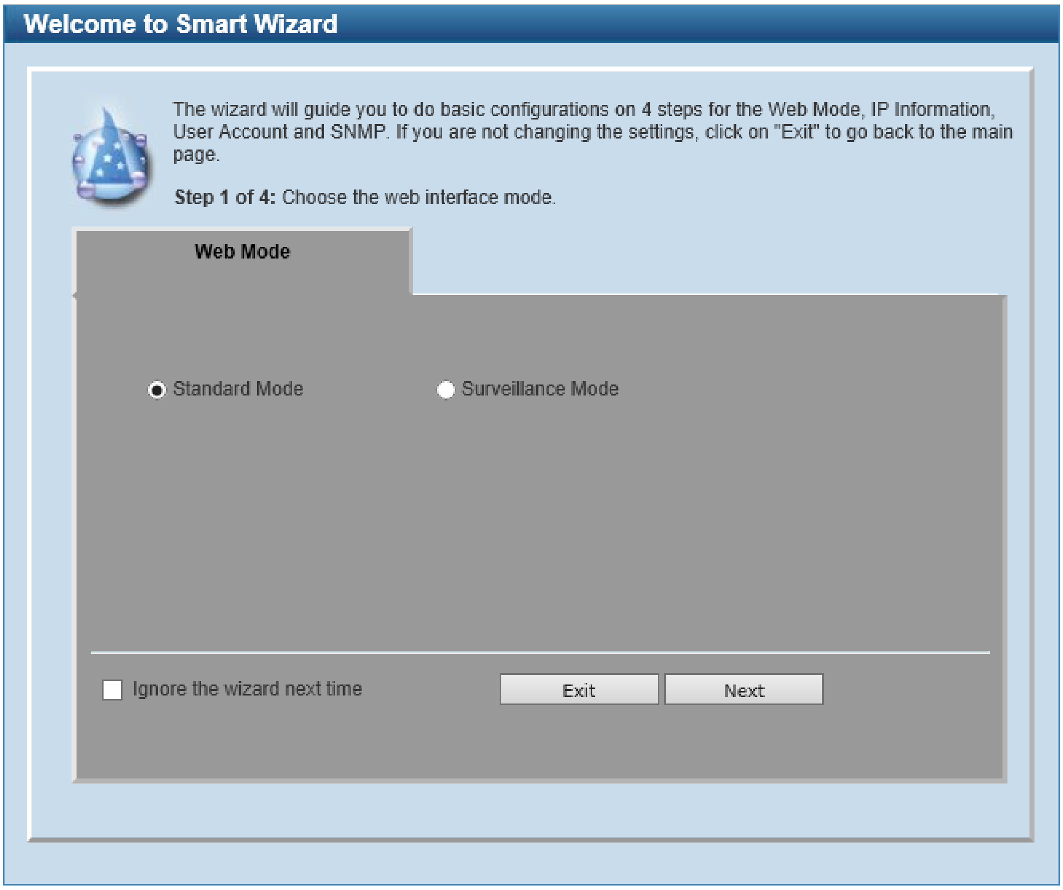
After successfully connecting to the Web UI for the first time, the **Smart Wizard** embedded Web utility will be launched. This wizard will guide the user through basic configuration steps that is essential for first time connection to the Switch.

Step 1 - Web Mode

The Switch supports two Web Modes: **Standard Mode** and **Surveillance Mode**.

- The **Standard Mode** is used to configure, manage, and monitor most of the software features on the Switch.
- The **Surveillance Mode** is an additional web mode specifically designed to assist the user with surveillance features supported by the Switch.

NOTE: The **Web Mode** can only be changed when one user session is connected to the Web UI of the Switch.



Welcome to Smart Wizard

The wizard will guide you to do basic configurations on 4 steps for the Web Mode, IP Information, User Account and SNMP. If you are not changing the settings, click on "Exit" to go back to the main page.

Step 1 of 4: Choose the web interface mode.

Web Mode

● Standard Mode ○ Surveillance Mode

□ Ignore the wizard next time

Figure 2-3 Web Mode

The fields that can be configured are described below:

Parameter	Description
Standard Mode	Select this option to access the Standard Mode after the Smart Wizard was completed.
Surveillance Mode	Select this option to access the Surveillance Mode after the Smart Wizard was completed.

Tick the **Ignore the wizard next time** option to skip the Smart Wizard on the next login.

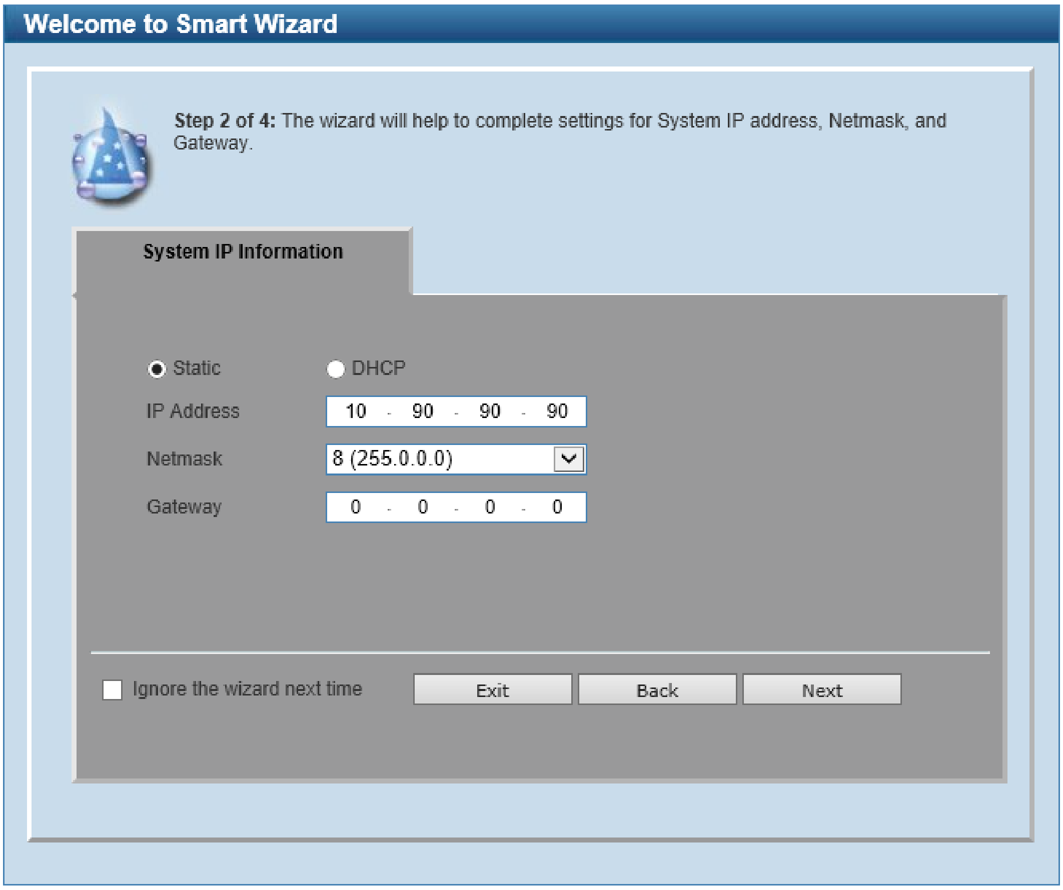
Click the **Exit** button to discard the changes made, exit the Smart Wizard, and continue to the Web UI.

Click the **Next** button to accept the changes made and continue to the next step.

Step 2 - System IP Information

In this step, we can configure System IP Information.

NOTE: The Switch will probe for surveillance devices every 30 seconds. If a surveillance device is not in the same subnet as the switch, it will not be discovered automatically. Place the Switch management IP in the same subnet as the surveillance devices for ONVIF cameras to be added to the Surveillance Mode Web UI automatically.



Welcome to Smart Wizard

Step 2 of 4: The wizard will help to complete settings for System IP address, Netmask, and Gateway.

System IP Information

● Static ○ DHCP

IP Address: 10 . 90 . 90 . 90

Netmask: 8 (255.0.0.0)

Gateway: 0 . 0 . 0 . 0

□ Ignore the wizard next time

Figure 2-4 System IP Information

The fields that can be configured are described below:

Parameter	Description
Static	Select this option to manually assign and configure the IP address settings for the Switch.
DHCP	Select this option to obtain IP address settings automatically from a DHCP server for the Switch.
IP Address	After selecting the **Static** option, manually enter the IP address of the Switch here.
Netmask	After selecting the **Static** option, manually select the Netmask option here.
Gateway	After selecting the **Static** option, manually enter the IP address of the default gateway here.

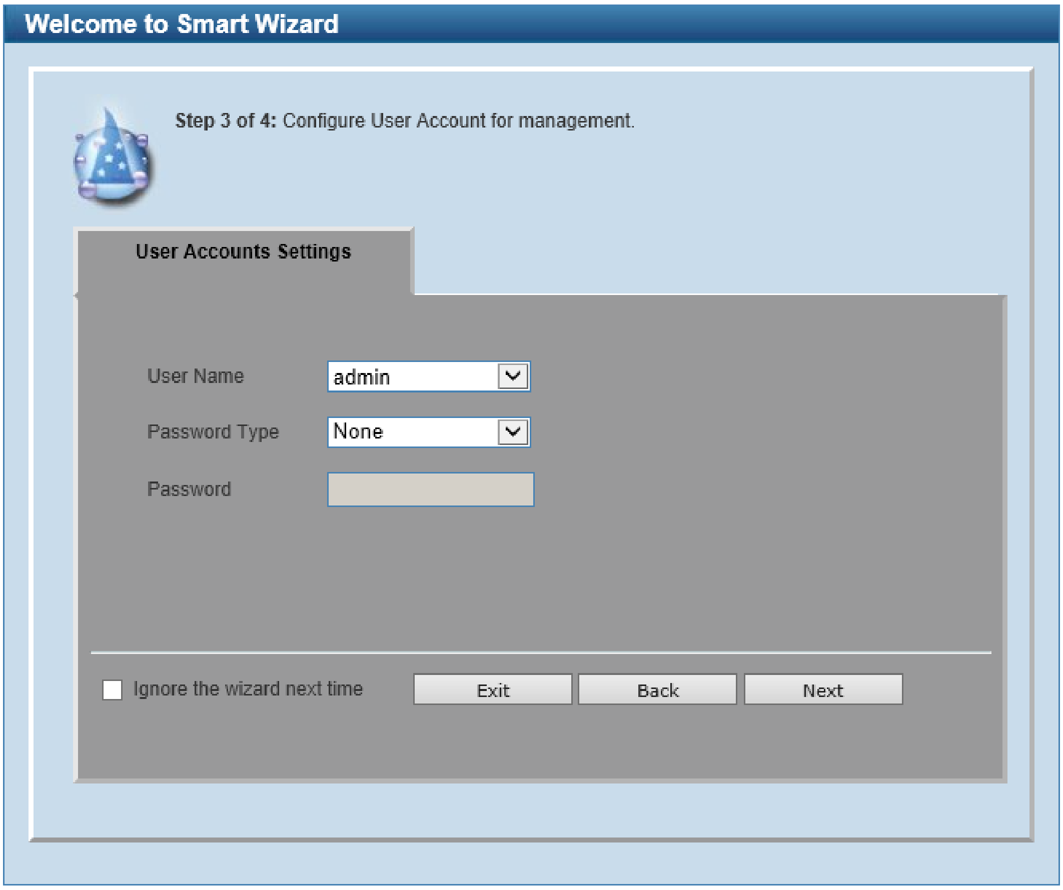
Tick the **Ignore the wizard next time** option to skip the Smart Wizard on the next login.

Click the **Exit** button to discard the changes made, exit the Smart Wizard, and continue to the Web UI.

Click the **Next** button to accept the changes made and continue to the next step.

Step 3 - User Accounts Settings

In this step, we can configure the user account settings.



Welcome to Smart Wizard

Step 3 of 4: Configure User Account for management.

User Accounts Settings

User Name: admin

Password Type: None

Password:

□ Ignore the wizard next time

Figure 2-5 User Account Settings

The fields that can be configured are described below:

Parameter	Description
User Name	Select the user name here.
Password Type	Select the password type here. Options to choose from are: • **None** - Specifies that no password will be configured for this user account. • **Plain Text** - Specifies that the password for this user account will be in the plain text form.
Password	After selecting **Plain Text** as the **Password Type**, enter the password for the user account here.

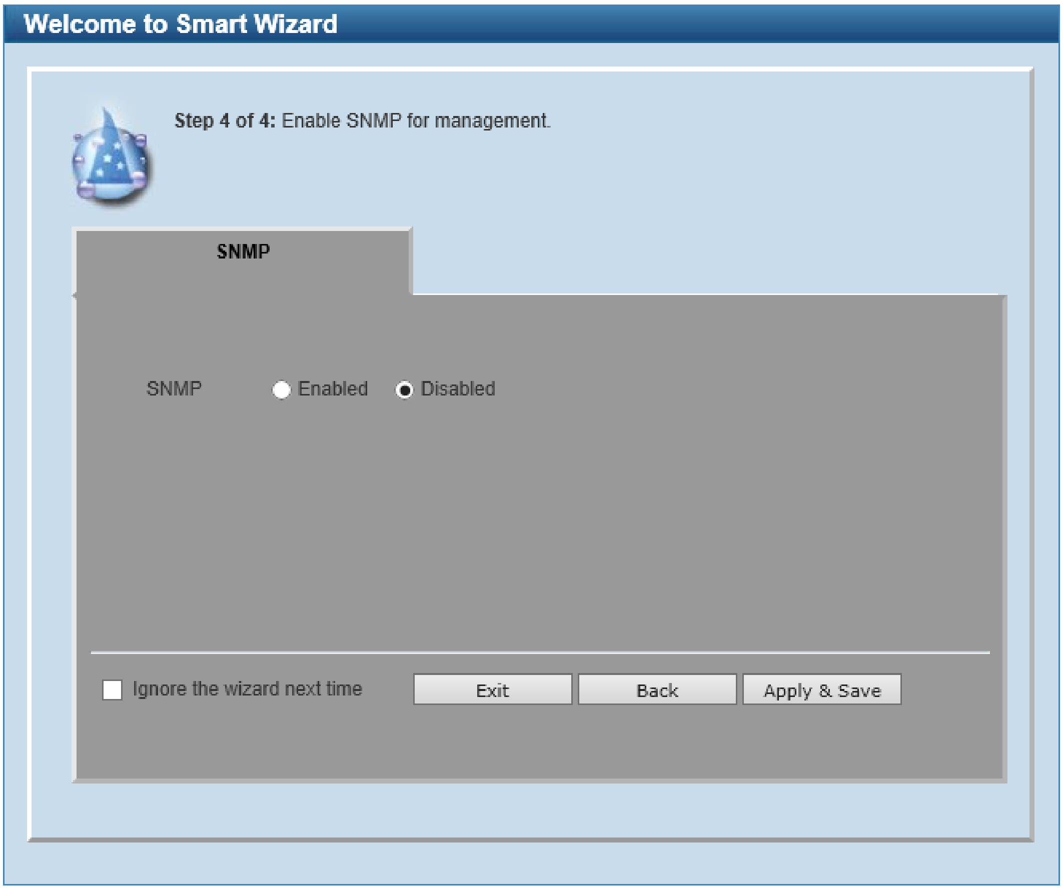
Tick the **Ignore the wizard next time** option to skip the Smart Wizard on the next login.

Click the **Exit** button to discard the changes made, exit the Smart Wizard, and continue to the Web UI.

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

Step 4 - SNMP Settings

In this step, we can enable or disable the SNMP feature.



Step 4 of 4: Enable SNMP for management.

SNMP ○ Enabled ● Disabled

□ Ignore the wizard next time

Figure 2-6 SNMP Window

The fields that can be configured are described below:

Parameter	Description
SNMP	Select to enable or disable the SNMP function here.

Tick the **Ignore the wizard next time** option to skip the Smart Wizard on the next login.

Click the **Exit** button to discard the changes made, exit the Smart Wizard, and continue to the Web UI.

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

Click the **Apply & Save** button to accept the changes made and continue to the Web UI.

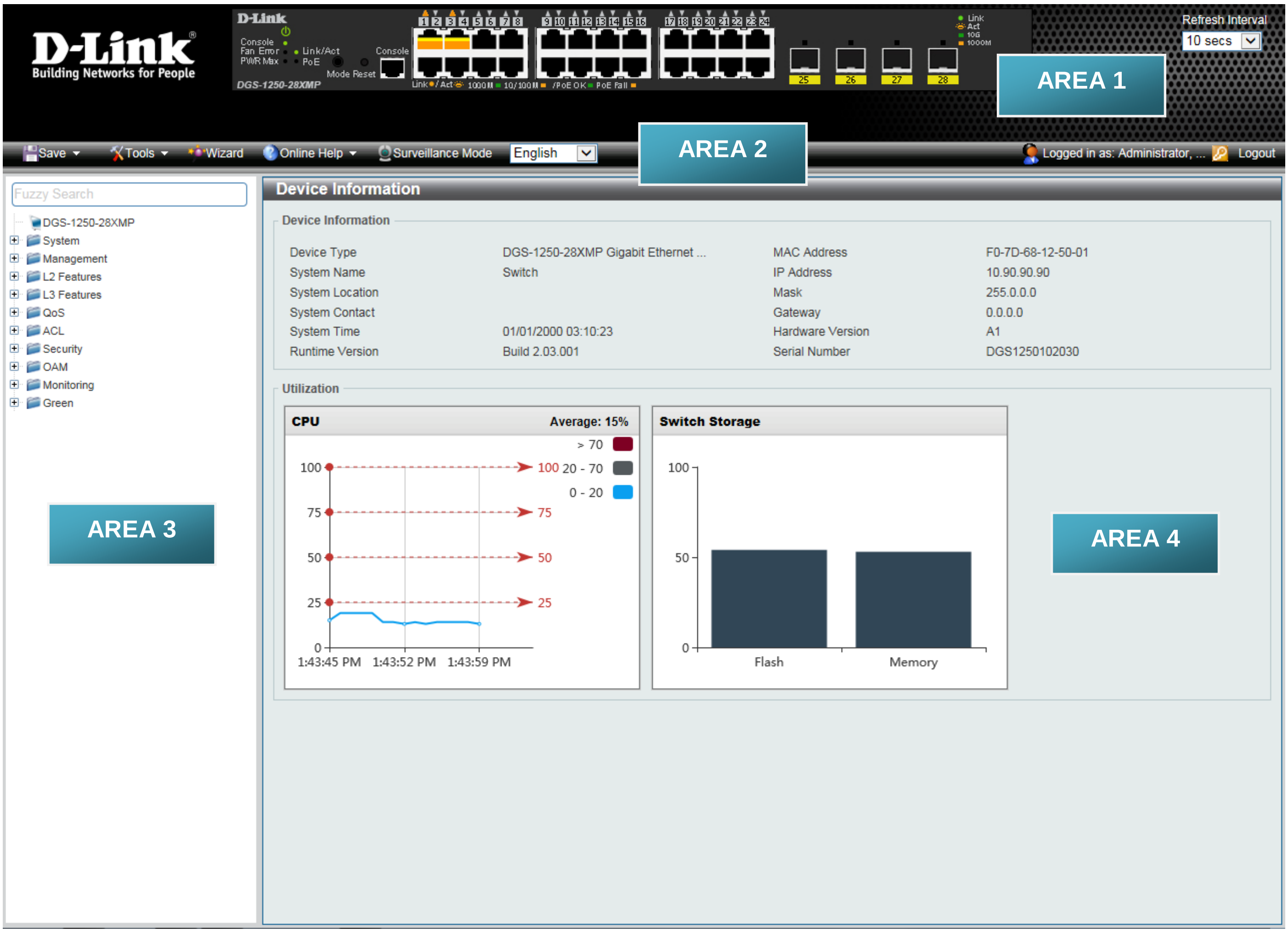
Web User Interface (Web UI)

Areas of the User Interface

The Web UI on the Switch can be divided into distinct Areas. Different areas in the Web UI provide different manageability options to simplify configuration and feature monitoring.

Standard Mode

After accessing the Web UI in the **Standard Mode**, the following will be displayed:



Device Information

Device Type	DGS-1250-28XMP Gigabit Ethernet ...	MAC Address	F0-7D-68-12-50-01
System Name	Switch	IP Address	10.90.90.90
System Location		Mask	255.0.0.0
System Contact		Gateway	0.0.0.0
System Time	01/01/2000 03:10:23	Hardware Version	A1
Runtime Version	Build 2.03.001	Serial Number	DGS1250102030

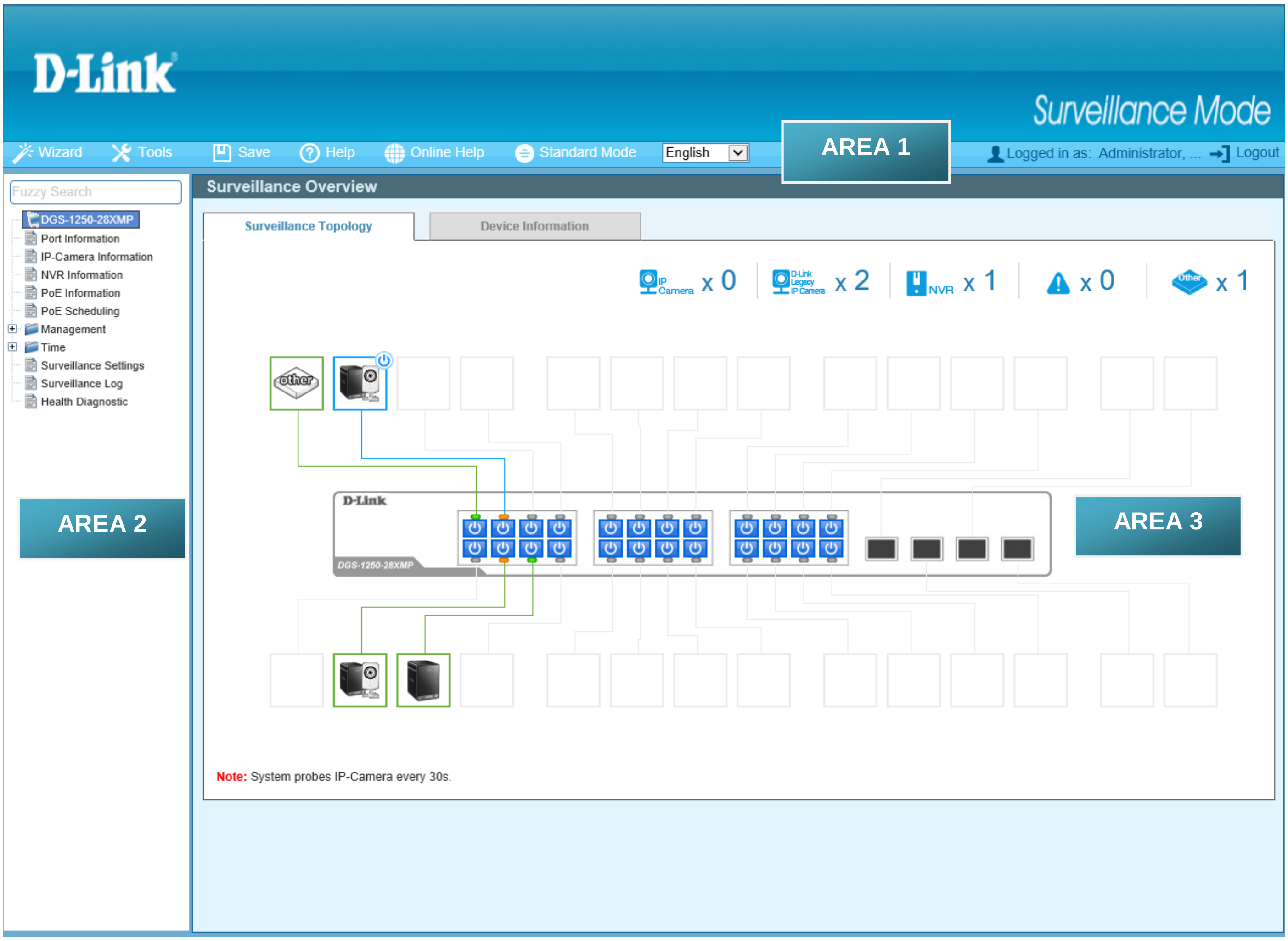
Figure 2-7 Web UI (Standard Mode)

Area Number	Description
AREA 1	In this area, a graphical near real-time image of the front panel of the Switch is displayed with ports and expansion modules. Port activity is displayed, depending on the specified mode. Some management functions like port monitoring are also accessible here. Click the D-Link logo to go to the D-Link website.
AREA 2	In this area is a toolbar used to access functions like **Save**, **Tools**, the **Wizard**, **Online Help**, accessing the Web UI in the **Surveillance Mode**, customized **Language** preference, and a **Logout** option. Click the **Surveillance Mode** option to change the switch mode from Standard Mode to Surveillance Mode. The user account and IP address currently logged into the Web UI will also be displayed in this toolbar.

Area Number	Description
AREA 3	In this area, the software features available in the Web UI of the Switch are grouped into folders containing hyperlinks that will open window frames in Area 4. There is also a search option in this area that can be used to search for specific feature keywords in the Web UI to easily find the link to the set of features.
AREA 4	In this area, configuration and monitoring window frames are available based on the selections made in Area 3.

Surveillance Mode

After accessing the Web UI in the **Surveillance Mode**, the following will be displayed:



Note: System probes IP-Camera every 30s.

Figure 2-8 Web UI (Surveillance Mode)

Area Number	Description
AREA 1	In this area is a toolbar used to access functions like the **Wizard**, **Tools**, **Save**, **Help**, **Online Help**, accessing the Web UI in the **Standard Mode**, customized **Language** preference, and a **Logout** option. Click the **Standard Mode** option to change the switch mode from Surveillance Mode to Standard Mode. The user account and IP address currently logged into the Web UI will also be displayed in this toolbar.
AREA 2	In this area, the software features available in the Web UI of the Switch are grouped into folders containing hyperlinks that will open window frames in Area 3.

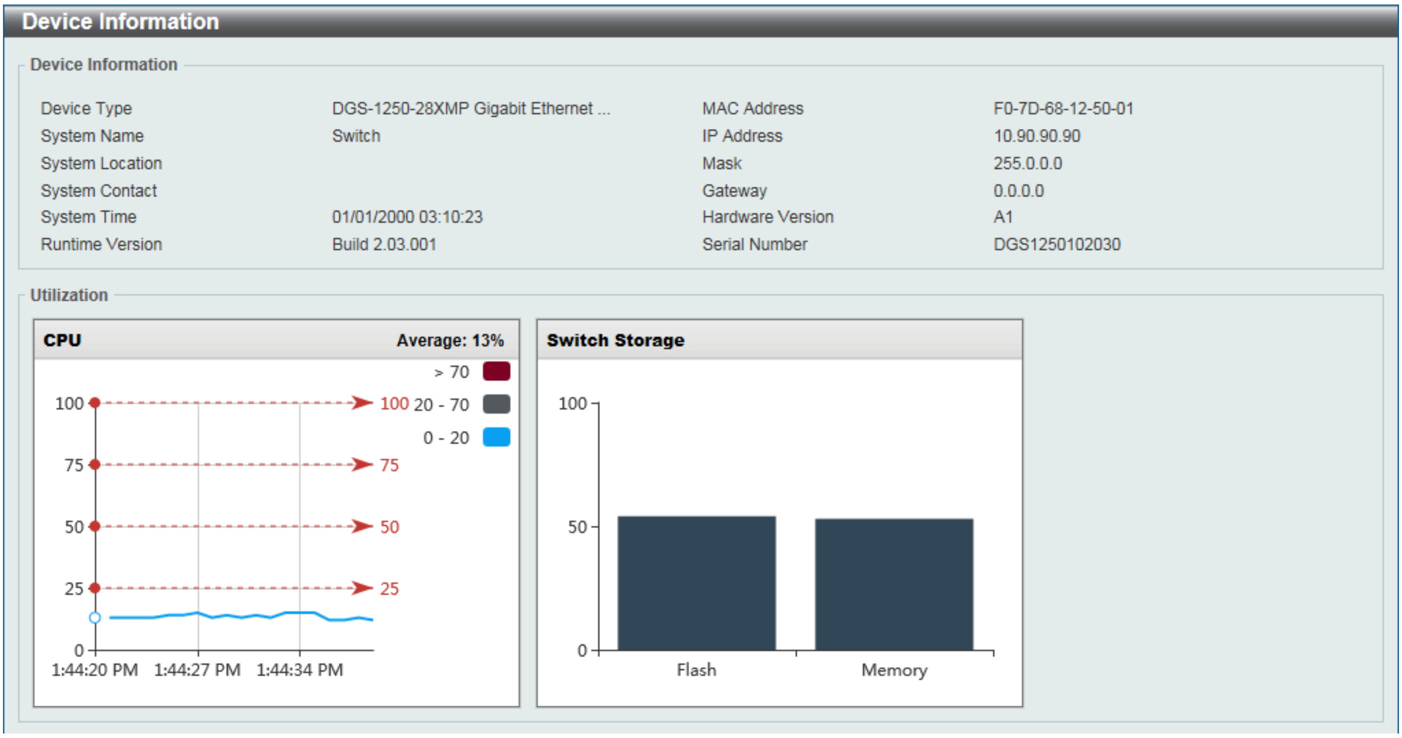
Area Number	Description
	There is also a search option in this area that can be used to search for specific feature keywords in the Web UI to find the link to the set of features.
AREA 3	In this area, configuration and monitoring window frames are available based on the selections made in Area 2. The status of devices, IP cameras, and NVRs discovered on the switch will also be displayed in this area.

NOTE: For more information about the Surveillance Mode, refer to **Surveillance Mode** on page 271.

3. System

Device Information

In the Device Information section, the user can view a list of basic information regarding the Switch. It appears automatically when you log on to the Switch. To return to the Device Information window after viewing other windows, click the **DGS-1250-28XMP** link.



Device Information

Device Information

Device Type	DGS-1250-28XMP Gigabit Ethernet ...	MAC Address	F0-7D-68-12-50-01
System Name	Switch	IP Address	10.90.90.90
System Location		Mask	255.0.0.0
System Contact		Gateway	0.0.0.0
System Time	01/01/2000 03:10:23	Hardware Version	A1
Runtime Version	Build 2.03.001	Serial Number	DGS1250102030

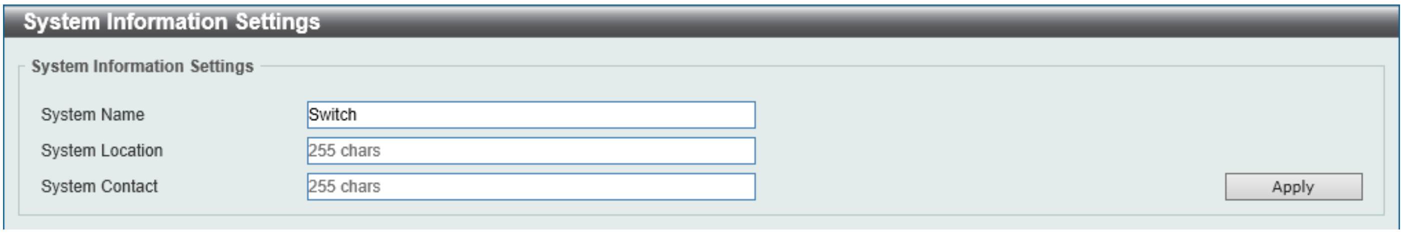
Utilization

Figure 3-1 Device Information Window

System Information Settings

This window is used to display and configure the system information settings and management interface configuration settings.

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



System Information Settings

System Information Settings

System Name: Switch

System Location: 255 chars

System Contact: 255 chars

Figure 3-2 System Information Settings Window

The fields that can be configured in **System Information Settings** are described below:

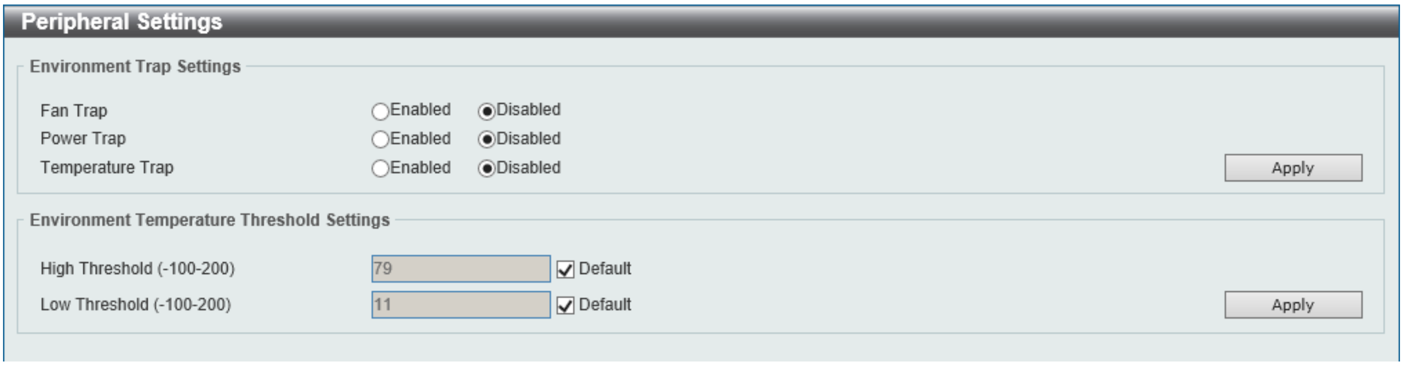
Parameter	Description
System Name	Enter the system name for the Switch here. This name will identify it in the Switch network.
System Location	Enter the location description of the Switch here.
System Contact	Enter the contact information for the Switch here.

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

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:



Peripheral Settings

Environment Trap Settings

Fan Trap ○Enabled ●Disabled

Power Trap ○Enabled ●Disabled

Temperature Trap ○Enabled ●Disabled

Environment Temperature Threshold Settings

High Threshold (-100-200): 79 ☑ Default

Low Threshold (-100-200): 11 ☑ Default

Figure 3-3 Peripheral Settings Window

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 warning fan event (fan failed or fan recover).
Power Trap	Select to enable or disable the power trap state for warning power event (power failed or power recover).
Temperature Trap	Select to enable or disable the temperature trap state for warning temperature event (temperature thresholds exceeded or temperature recover).

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
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.

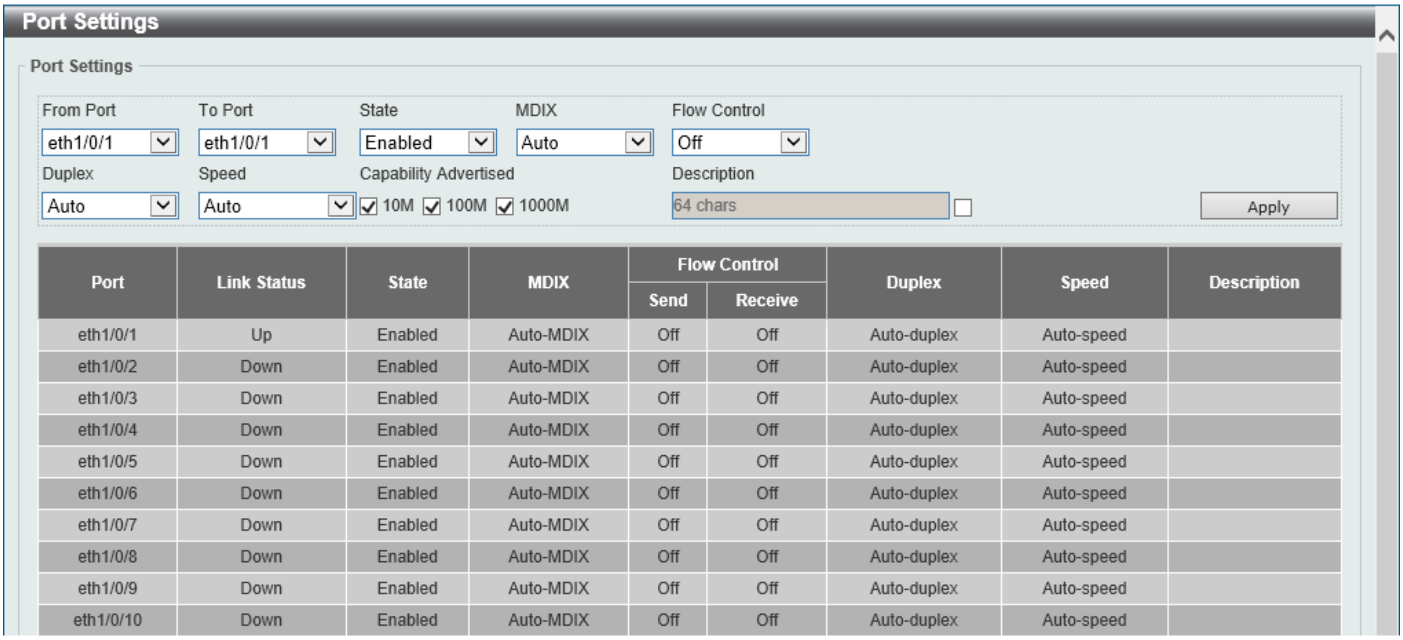
Click the **Apply** button to accept the changes made.

Port Configuration

Port Settings

This window is used to display and configure the Switch’s port settings.

To view the following window, click **System > Port Configuration > Port Settings**, as shown below:



Port Settings

Port Settings

From Port: eth1/0/1
To Port: eth1/0/1
State: Enabled
MDIX: Auto
Flow Control: Off
Duplex: Auto
Speed: Auto
Capability Advertised: ☑ 10M ☑ 100M ☑ 1000M
Description: 64 chars □

Port	Link Status	State	MDIX	Flow Control		Duplex	Speed	Description
				Send	Receive			
eth1/0/1	Up	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	
eth1/0/2	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	
eth1/0/3	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	
eth1/0/4	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	
eth1/0/5	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	
eth1/0/6	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	
eth1/0/7	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	
eth1/0/8	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	
eth1/0/9	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	
eth1/0/10	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	

Figure 3-4 Port Settings Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the physical port state here.
MDIX	Select the Medium Dependent Interface Crossover (MDIX) option here. Options to choose from are: • **Auto** - Select this option for auto-sensing of the optimal type of cabling. • **Normal** - Select this option for normal cabling. If this option is selected, the port is in the MDIX mode and can be connected to a PC NIC using a straight-through cable or a port (in the MDI mode) on another Switch through a crossover cable.

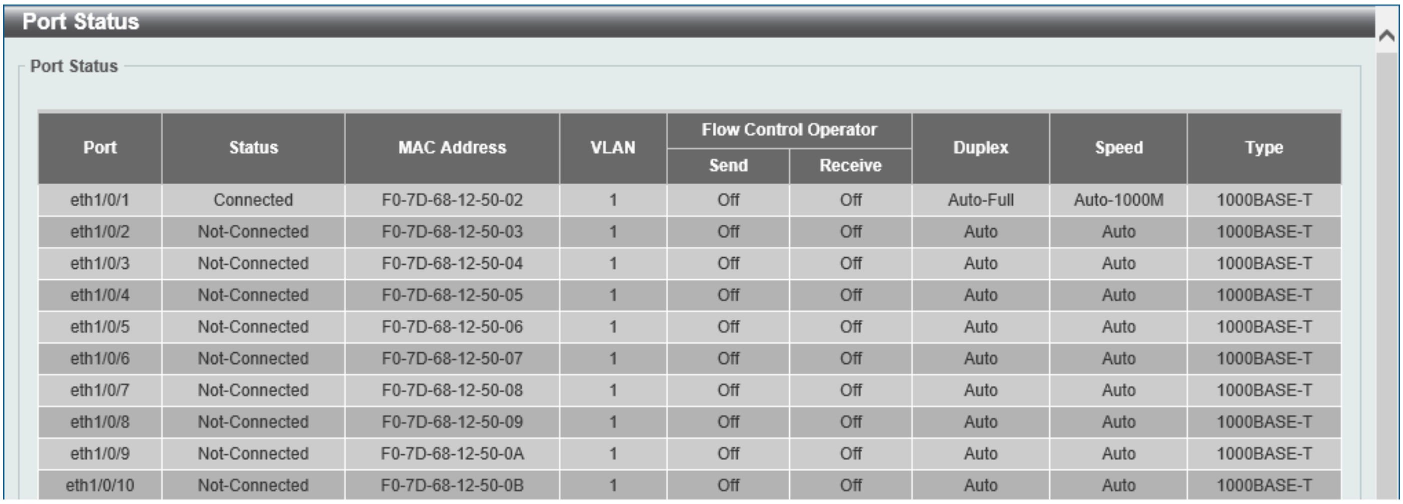
Parameter	Description
	• **Cross** - Select this option for crossover cabling. If this option is selected, the port is in the MDI mode and can be connected to a port (in the MDIX mode) on another Switch through a straight cable. **Note:** This option is only available on the 10/100/1000 Mbps RJ45 ports.
Flow Control	Select to turn flow control **On** or **Off** here.
Duplex	Select the duplex mode used here. Options to choose from are **Auto**, **Half**, and **Full**.
Speed	Select the port speed option here. This option will manually force the connection speed on the selected port to connect at the specified speed only. The **Master** setting will allow the port to advertise capabilities related to duplex, speed, and physical layer type. The master setting will also determine the master and slave relationship between the two connected physical layers. This relationship is necessary for establishing the timing control between the two physical layers. The timing control is set on a master physical layer by a local source. The **Slave** setting uses loop timing, where the timing comes from a data stream received from the master. If one connection is set for master, the other side of the connection must be set for slave. Any other configuration will result in a 'link down' status for both ports. Options to choose from are: • **Auto** - Specifies that for copper ports, auto-negotiation will start to negotiate the speed and flow control with its link partner. For fiber ports, auto-negotiation will start to negotiate the clock and flow control with its link partner. • **10M** - Specifies to force the port speed to 10 Mbps. • **100M** - Specifies to force the port speed to 100 Mbps. • **1000M** - Specifies to force the port speed to 1 Gbps. • **1000M Master** - Specifies to force the port speed to 1 Gbps and operates as the master, to facilitate the timing of transmit and receive operations. • **1000M Slave** - Specifies to force the port speed to 1 Gbps and operates as the slave, to facilitate the timing of transmit and receive operations. • **10G** - Specifies to force the port speed to 10 Gbps.
Capability Advertised	When the **Speed** is set to **Auto**, these capabilities are advertised during auto-negotiation.
Description	Select the checkbox and enter the description for the corresponding port here. This can be up to 64 characters long.

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

Port Status

This window is used to view the Switch's physical port status and settings.

To view the following window, click **System > Port Configuration > Port Status**, as shown below:



Port Status

Port Status

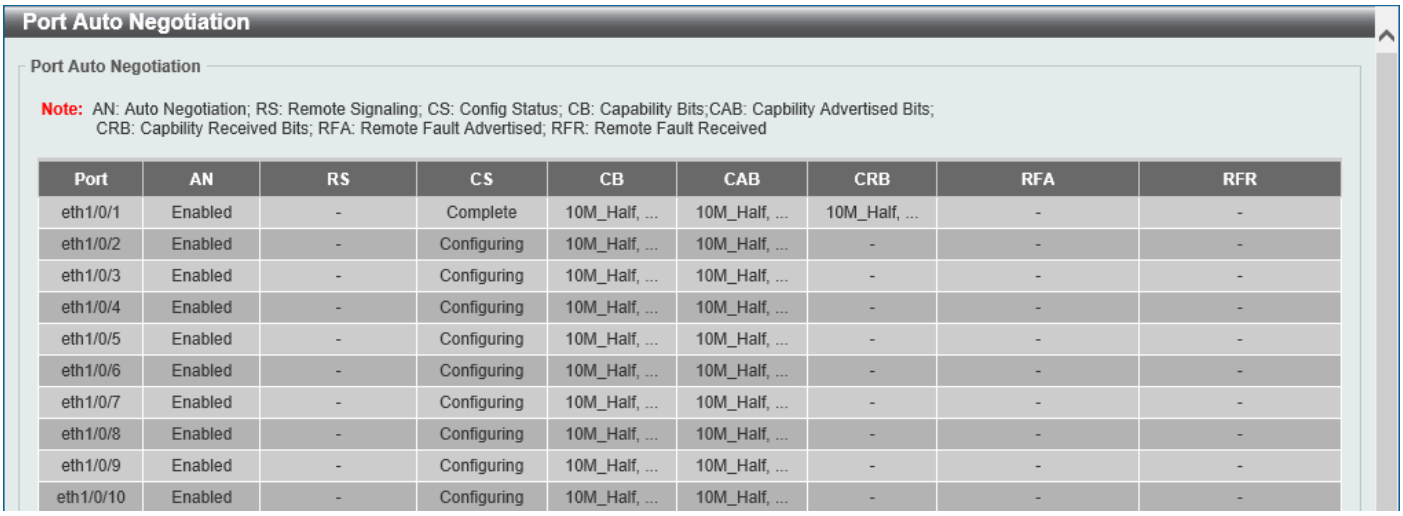
Port	Status	MAC Address	VLAN	Flow Control Operator		Duplex	Speed	Type
				Send	Receive			
eth1/0/1	Connected	F0-7D-68-12-50-02	1	Off	Off	Auto-Full	Auto-1000M	1000BASE-T
eth1/0/2	Not-Connected	F0-7D-68-12-50-03	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/3	Not-Connected	F0-7D-68-12-50-04	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/4	Not-Connected	F0-7D-68-12-50-05	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/5	Not-Connected	F0-7D-68-12-50-06	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/6	Not-Connected	F0-7D-68-12-50-07	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/7	Not-Connected	F0-7D-68-12-50-08	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/8	Not-Connected	F0-7D-68-12-50-09	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/9	Not-Connected	F0-7D-68-12-50-0A	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/10	Not-Connected	F0-7D-68-12-50-0B	1	Off	Off	Auto	Auto	1000BASE-T

Figure 3-5 Port Status Window

Port Auto Negotiation

This window is used to view detailed port auto-negotiation information.

To view the following window, click **System > Port Configuration > Port Auto Negotiation**, as shown below:



Port Auto Negotiation

Port Auto Negotiation

Note: AN: Auto Negotiation; RS: Remote Signaling; CS: Config Status; CB: Capability Bits;CAB: Capbility Advertised Bits; CRB: Capbility Received Bits; RFA: Remote Fault Advertised; RFR: Remote Fault Received

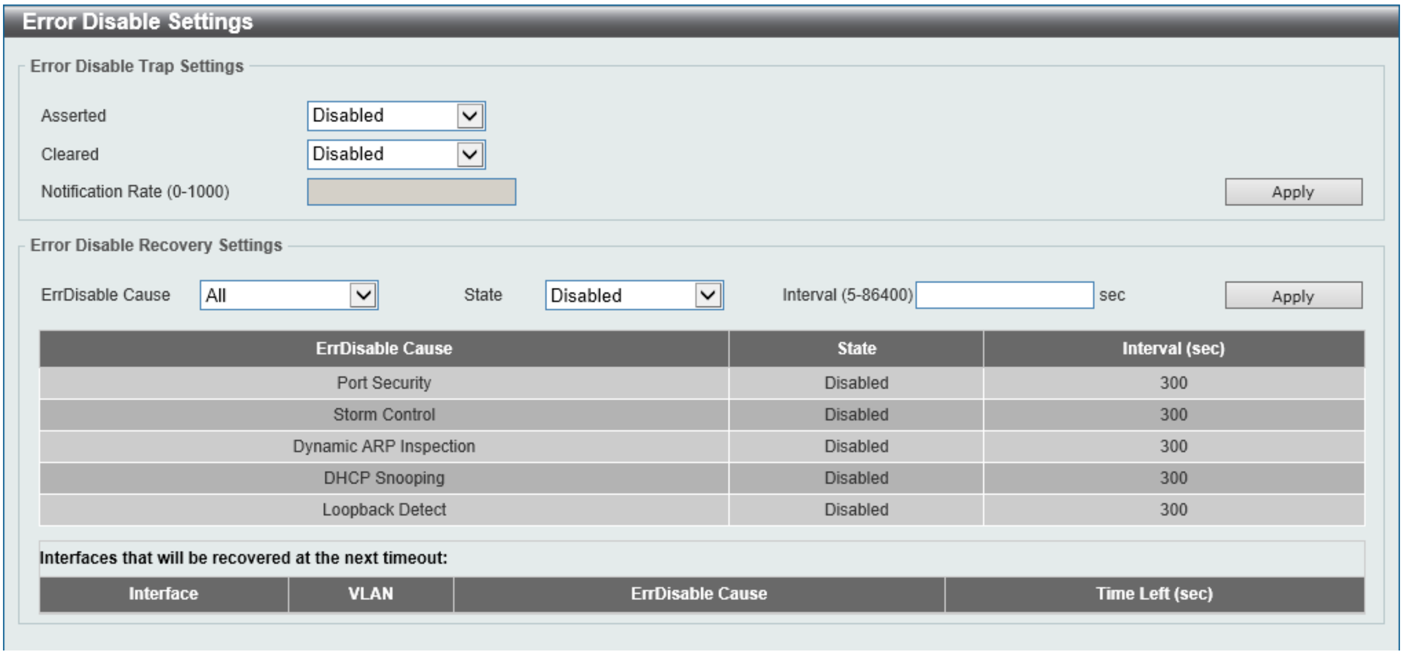
Port	AN	RS	CS	CB	CAB	CRB	RFA	RFR
eth1/0/1	Enabled	-	Complete	10M_Half, ...	10M_Half, ...	10M_Half, ...	-	-
eth1/0/2	Enabled	-	Configuring	10M_Half, ...	10M_Half, ...	-	-	-
eth1/0/3	Enabled	-	Configuring	10M_Half, ...	10M_Half, ...	-	-	-
eth1/0/4	Enabled	-	Configuring	10M_Half, ...	10M_Half, ...	-	-	-
eth1/0/5	Enabled	-	Configuring	10M_Half, ...	10M_Half, ...	-	-	-
eth1/0/6	Enabled	-	Configuring	10M_Half, ...	10M_Half, ...	-	-	-
eth1/0/7	Enabled	-	Configuring	10M_Half, ...	10M_Half, ...	-	-	-
eth1/0/8	Enabled	-	Configuring	10M_Half, ...	10M_Half, ...	-	-	-
eth1/0/9	Enabled	-	Configuring	10M_Half, ...	10M_Half, ...	-	-	-
eth1/0/10	Enabled	-	Configuring	10M_Half, ...	10M_Half, ...	-	-	-

Figure 3-6 Port Auto Negotiation Window

Error Disable Settings

This window is used to display and configure the recovery from the Error Disable causes and to configure the recovery interval.

To view the following window, click **System > Port Configuration > Error Disable Settings**, as shown below:



Error Disable Settings

Error Disable Trap Settings

Asserted: Disabled

Cleared: Disabled

Notification Rate (0-1000):

Error Disable Recovery Settings

ErrDisable Cause: All   State: Disabled   Interval (5-86400): sec

ErrDisable Cause	State	Interval (sec)
Port Security	Disabled	300
Storm Control	Disabled	300
Dynamic ARP Inspection	Disabled	300
DHCP Snooping	Disabled	300
Loopback Detect	Disabled	300

Interfaces that will be recovered at the next timeout:

Interface	VLAN	ErrDisable Cause	Time Left (sec)

Figure 3-7 Error Disable Settings Window

The fields that can be configured for **Error Disable Trap Settings** are described below:

Parameter	Description
Asserted	Specifies to enable or disable notifications for entering into the error-disabled state.
Cleared	Specifies to enable or disable notifications for exiting from the error-disabled state.
Notification Rate	Enter the notification rate value here. This sets the number of traps per minute. The packets that exceed the rate will be dropped. The range is from 0 to 1000. The default value (0) indicates that an SNMP trap will be generated for every change of the error disabled state.

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

The fields that can be configured for **Error Disable Recovery Settings** are described below:

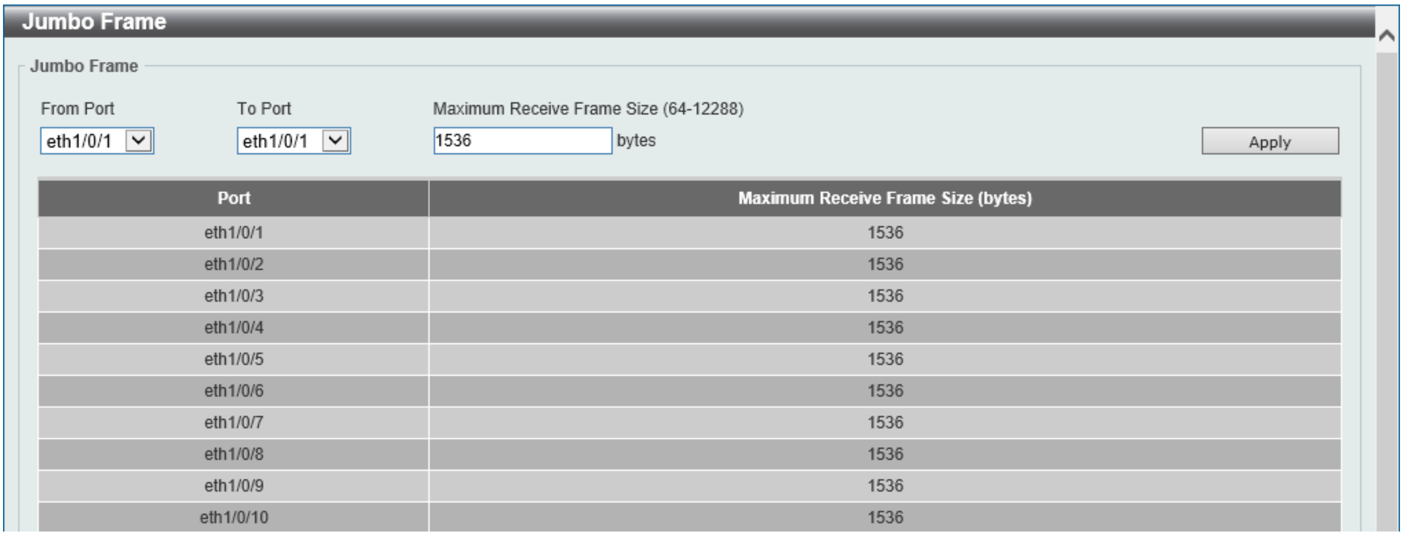
Parameter	Description
ErrDisable Cause	Select the error disabled cause here. Options to choose from are **Port Security**, **Storm Control**, **Dynamic ARP Inspection**, **DHCP Snooping**, and **Loopback Detect**.
State	Select to enable or disable the error disabled recovery feature here.
Interval	Enter the time, in seconds, to recover the port from the error state caused by the specified module. The range is from 5 to 86400.

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

Jumbo Frame

This window is used to display and configure the jumbo frame size and settings. The Switch supports jumbo frames. Jumbo frames are Ethernet frames with more than 1,518 bytes of payload. The Switch supports jumbo frames with a maximum frame size of up to 12,288 bytes.

To view the following window, click **System > Port Configuration > Jumbo Frame**, as shown below:



Jumbo Frame

Jumbo Frame

From Port: eth1/0/1

To Port: eth1/0/1

Maximum Receive Frame Size (64-12288): 1536 bytes

Port	Maximum Receive Frame Size (bytes)
eth1/0/1	1536
eth1/0/2	1536
eth1/0/3	1536
eth1/0/4	1536
eth1/0/5	1536
eth1/0/6	1536
eth1/0/7	1536
eth1/0/8	1536
eth1/0/9	1536
eth1/0/10	1536

Figure 3-8 Jumbo Frame Window

The fields that can be configured are described below:

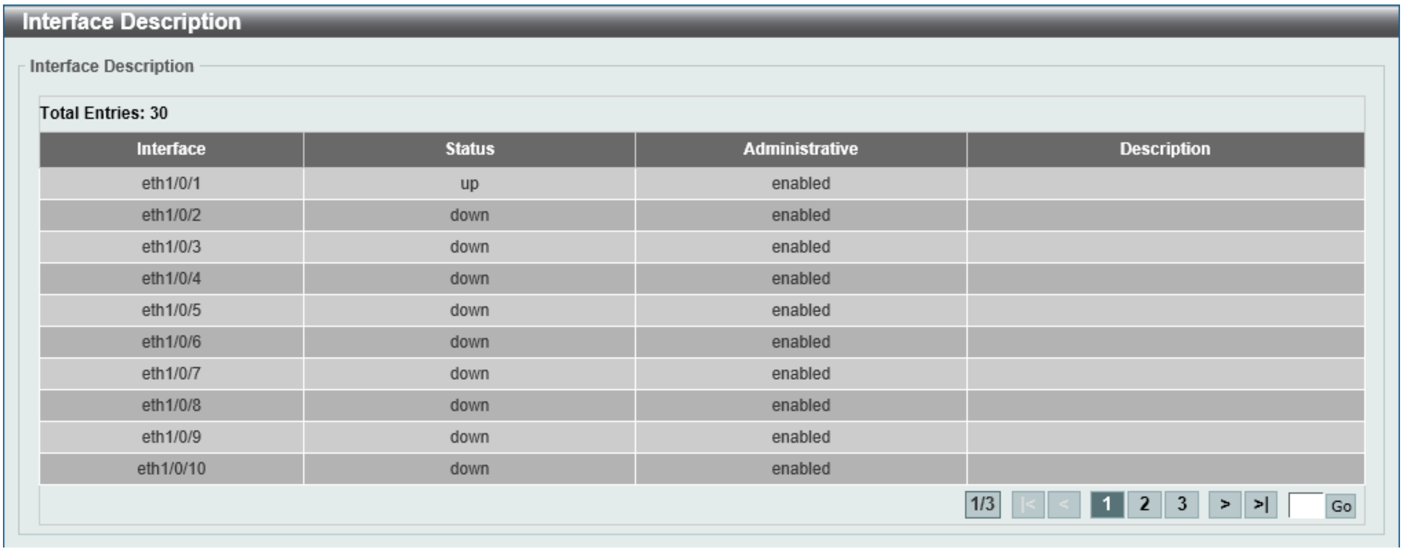
Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Maximum Receive Frame Size	Enter the maximum receive frame size value here. This value must be between 64 and 12288 bytes. By default, this value is 1536 bytes.

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

Interface Description

This window is used to display the status, administrative status, and description of each port on the Switch.

To view the following window, click **System > Interface Description**, as shown below:


Interface Description

Interface Description

Total Entries: 30

Interface	Status	Administrative	Description
eth1/0/1	up	enabled	
eth1/0/2	down	enabled	
eth1/0/3	down	enabled	
eth1/0/4	down	enabled	
eth1/0/5	down	enabled	
eth1/0/6	down	enabled	
eth1/0/7	down	enabled	
eth1/0/8	down	enabled	
eth1/0/9	down	enabled	
eth1/0/10	down	enabled	

Figure 3-9 Interface Description Window

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

PoE

The **DGS-1250-28XMP** and **DGS-1250-52XMP** switches support Power over Ethernet (PoE) as defined by the IEEE 802.3af and 802.3at. All PoE-supported ports can supply up to 30 Watts of power. The Switch ports can supply about 48 VDC power to Powered Devices (PDs) over Category 5 or Category 3 UTP Ethernet cables. The Switch follows the standard Power Sourcing Equipment (PSE) pin-out Alternative A, whereby power is sent out over pins 1, 2, 3, and 6. The Switches work with all D-Link 802.3af capable devices.

The Switch includes the following PoE features:

- Auto-discovery recognizes the connection of a PD and automatically sends power to it.
- The auto-disable feature occurs under two conditions:
    - If the total power consumption exceeds the system power limit
    - If the per-port power consumption exceeds the per port power limit
- Active circuit protection automatically disables the port if there is a short. Other ports will remain active.

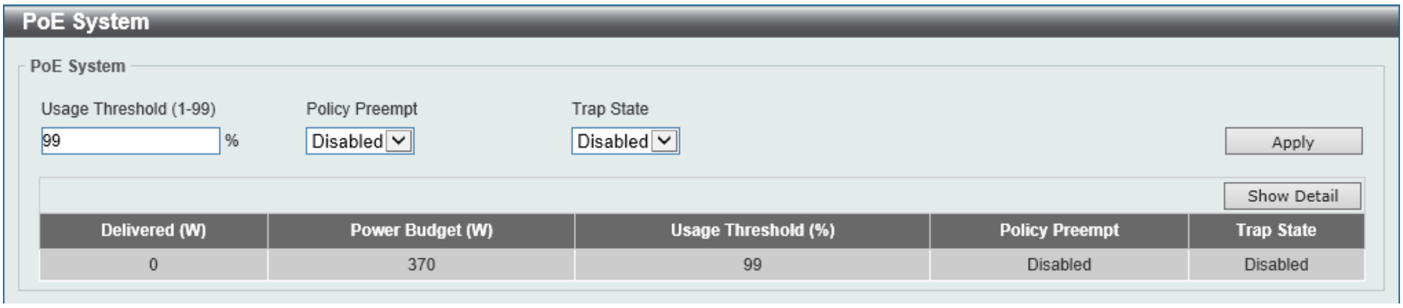
Based on IEEE 802.3af/at, power is received and supplied according to the following classifications:

Class	Maximum power used by the PD	Maximum power supplied by the Switch
0	12.95 Watts	15.4 Watts
1	3.84 Watts	4 Watts
2	6.49 Watts	7 Watts
3	12.95 Watts	15.4 Watts
4	25.5 Watts	30 Watts

PoE System

This window is used to configure the PoE system and display the detailed power information and PoE chip parameters for PoE modules.

To view the following window, click **System > PoE > PoE System**, as shown below:



PoE System

PoE System

Usage Threshold (1-99): 99 %

Policy Preempt: Disabled

Trap State: Disabled

Delivered (W)	Power Budget (W)	Usage Threshold (%)	Policy Preempt	Trap State
0	370	99	Disabled	Disabled

Figure 3-10 PoE System Window

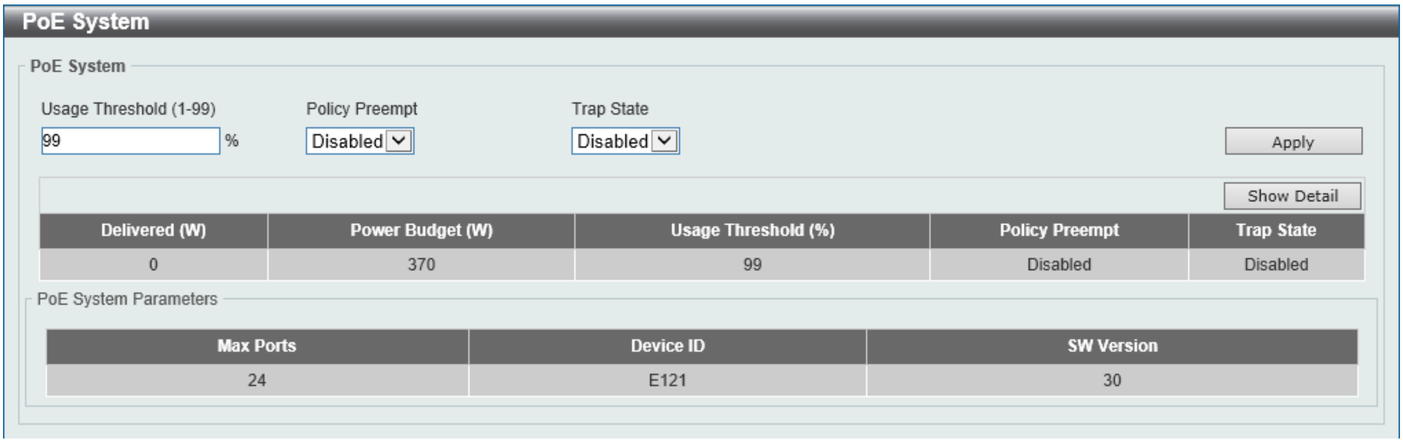
The fields that can be configured for **PoE System** are described below:

Parameter	Description
Usage Threshold	Enter the usage threshold to generate a log and send the corresponding standard notification. The range is from 1 to 99 percent.
Policy Preempt	Select this option to enable or disable the disconnection of the Powered Device (PD) that is power-provisioned with a lower priority in order to release the power to the new connected PD with higher priority under power shortage conditions.
Trap State	Select this option to enable or disable the sending of PoE trap notifications.

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

Click the **Show Detail** button to see the PoE system Parameters table at the bottom of the window.

After clicking the **Show Detail** button, the following window will appear.



PoE System

PoE System

Usage Threshold (1-99): 99 %

Policy Preempt: Disabled

Trap State: Disabled

Delivered (W)	Power Budget (W)	Usage Threshold (%)	Policy Preempt	Trap State
0	370	99	Disabled	Disabled

PoE System Parameters

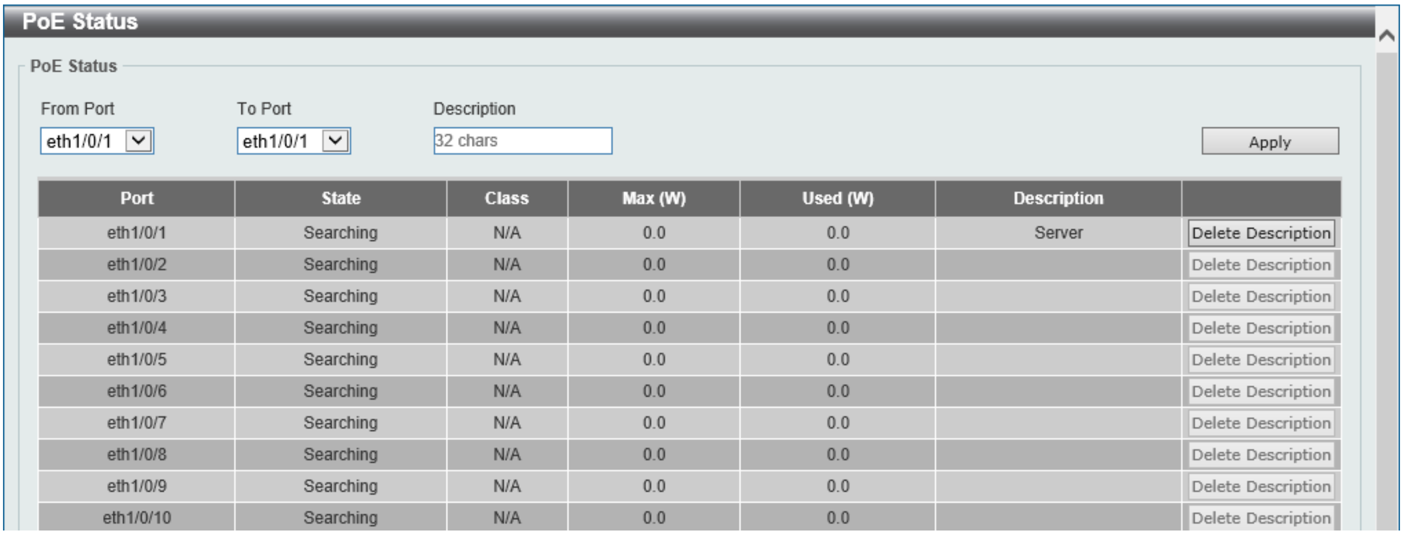
Max Ports	Device ID	SW Version
24	E121	30

Figure 3-11 PoE System (Show Detail) Window

PoE Status

This window is used to configure the description and display the PoE status of each port.

To view the following window, click **System > PoE > PoE Status**, as shown below:



From Port: eth1/0/1
To Port: eth1/0/1
Description: 32 chars

Port	State	Class	Max (W)	Used (W)	Description	
eth1/0/1	Searching	N/A	0.0	0.0	Server	Delete Description
eth1/0/2	Searching	N/A	0.0	0.0		Delete Description
eth1/0/3	Searching	N/A	0.0	0.0		Delete Description
eth1/0/4	Searching	N/A	0.0	0.0		Delete Description
eth1/0/5	Searching	N/A	0.0	0.0		Delete Description
eth1/0/6	Searching	N/A	0.0	0.0		Delete Description
eth1/0/7	Searching	N/A	0.0	0.0		Delete Description
eth1/0/8	Searching	N/A	0.0	0.0		Delete Description
eth1/0/9	Searching	N/A	0.0	0.0		Delete Description
eth1/0/10	Searching	N/A	0.0	0.0		Delete Description

Figure 3-12 PoE Status Window

The fields that can be configured for **PoE Status** are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Description	Enter the text that describes the PD connected to a PoE interface. The maximum length is 32 characters.

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

Click the **Delete Description** button to remove the description from the entry.

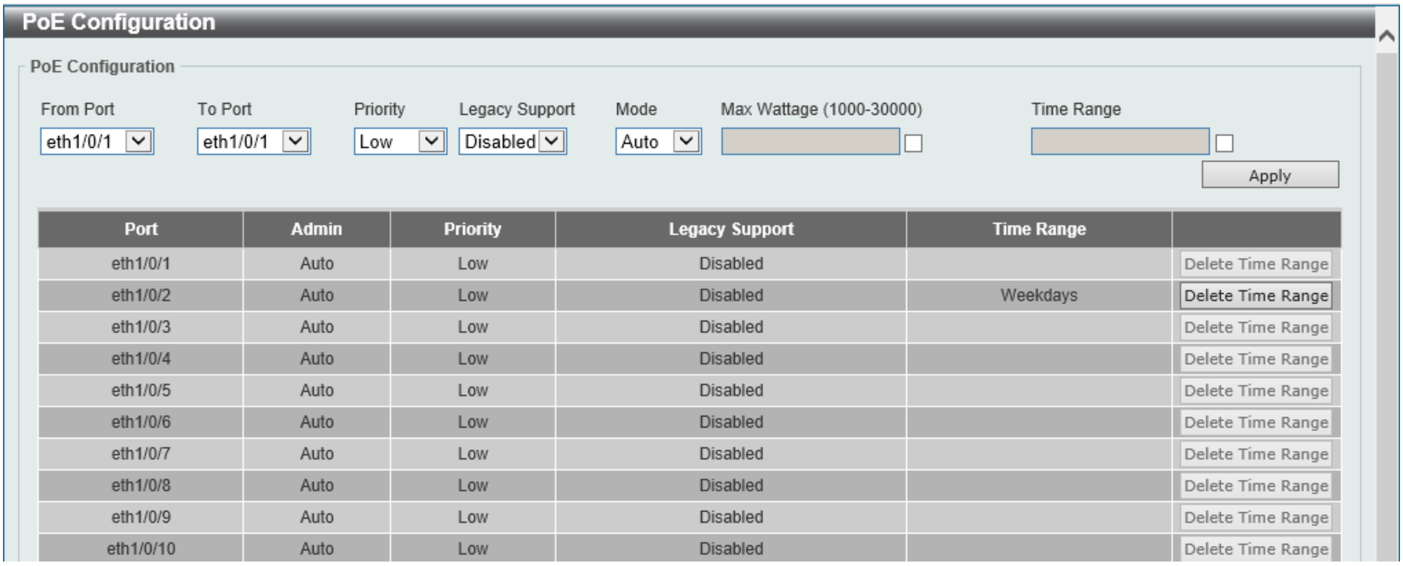
PoE Configuration

This window is used to display and configure the PoE configuration settings.

NOTE: If the Switch failed to supply power to the IEEE 802.3at PD,

- Check if the PD connected to the port supports the IEEE 802.3at standard
- Manually configure the PoE power limit value to 30 Watts for the corresponding port

To view the following window, click **System > PoE > PoE Configuration**, as shown below:



PoE Configuration

PoE Configuration

From Port: eth1/0/1
To Port: eth1/0/1
Priority: Low
Legacy Support: Disabled
Mode: Auto
Max Wattage (1000-30000): □
Time Range: □

Port	Admin	Priority	Legacy Support	Time Range	
eth1/0/1	Auto	Low	Disabled		Delete Time Range
eth1/0/2	Auto	Low	Disabled	Weekdays	Delete Time Range
eth1/0/3	Auto	Low	Disabled		Delete Time Range
eth1/0/4	Auto	Low	Disabled		Delete Time Range
eth1/0/5	Auto	Low	Disabled		Delete Time Range
eth1/0/6	Auto	Low	Disabled		Delete Time Range
eth1/0/7	Auto	Low	Disabled		Delete Time Range
eth1/0/8	Auto	Low	Disabled		Delete Time Range
eth1/0/9	Auto	Low	Disabled		Delete Time Range
eth1/0/10	Auto	Low	Disabled		Delete Time Range

Figure 3-13 PoE Configuration Window

The fields that can be configured for **PoE Configuration** are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Priority	Select the priority for provisioning power to the port. Options to choose from are **Critical**, **High** and **Low**.
Legacy Support	Select this option to enable or disable the support of legacy PD.
Mode	Select the power management mode for the PoE ports. Options to choose from are **Auto** and **Never**.
Max Wattage	When selecting **Auto** in the **Mode** drop-down list, this option appears. Tick the check box and enter the maximum wattage of power that can be provisioned to the auto-detected PD. If the value is not entered, the class of the PD automatically determines the maximum wattage that can be provisioned. The valid range for maximum wattage is between 1000 mW and 30000 mW.
Time Range	When selecting **Auto** in the **Mode** drop-down list, this option appears. Tick the check box and enter the name of the time range to determine the activation period.

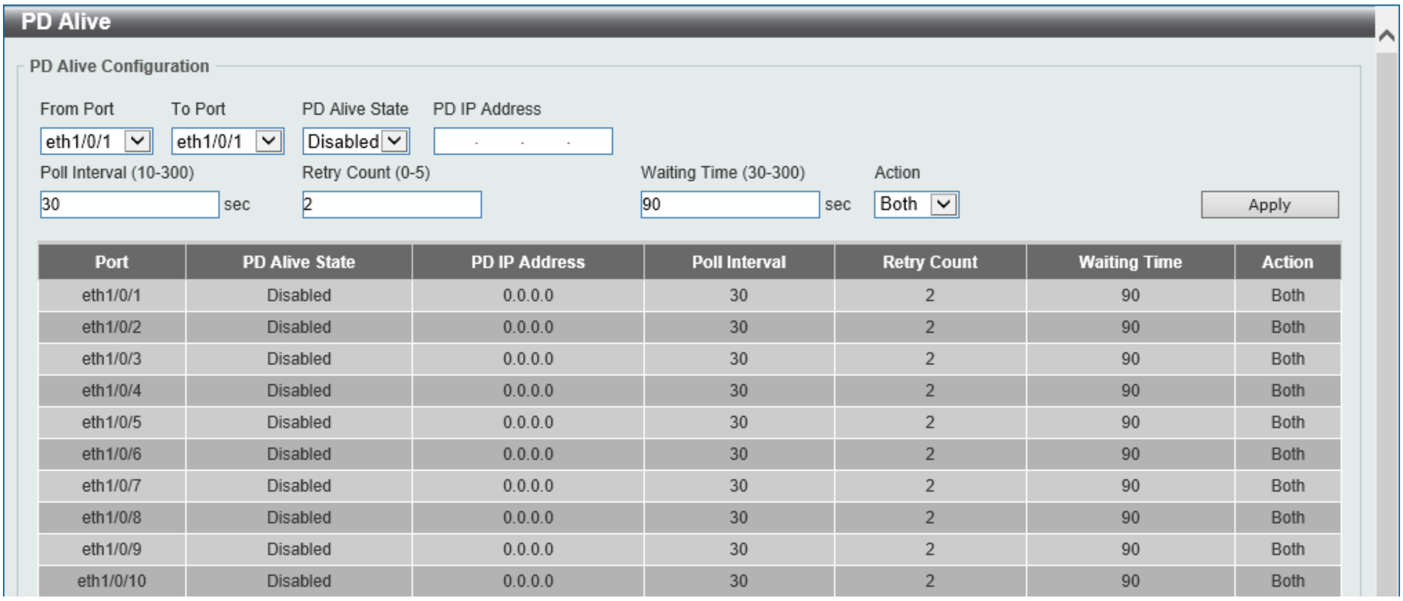
Click the **Apply** button to accept the changes made.

Click the **Delete Time Range** button remove the time range association for the entry.

PD Alive

This window is used to configure the PD Alive function for PDs connected to the PoE ports. The ping function is used to check if PDs, connected to the PoE ports, are active or not. When PDs appear to be inactive, the specified action (Reset, Notify, or Both) will be taken.

To view the following window, click **System > PoE > PD Alive**, as shown below:



From Port: eth1/0/1
To Port: eth1/0/1
PD Alive State: Disabled
PD IP Address: . . .
Poll Interval (10-300): 30 sec
Retry Count (0-5): 2
Waiting Time (30-300): 90 sec
Action: Both

Port	PD Alive State	PD IP Address	Poll Interval	Retry Count	Waiting Time	Action
eth1/0/1	Disabled	0.0.0.0	30	2	90	Both
eth1/0/2	Disabled	0.0.0.0	30	2	90	Both
eth1/0/3	Disabled	0.0.0.0	30	2	90	Both
eth1/0/4	Disabled	0.0.0.0	30	2	90	Both
eth1/0/5	Disabled	0.0.0.0	30	2	90	Both
eth1/0/6	Disabled	0.0.0.0	30	2	90	Both
eth1/0/7	Disabled	0.0.0.0	30	2	90	Both
eth1/0/8	Disabled	0.0.0.0	30	2	90	Both
eth1/0/9	Disabled	0.0.0.0	30	2	90	Both
eth1/0/10	Disabled	0.0.0.0	30	2	90	Both

Figure 3-14 PD Alive Window

The fields that can be configured are described below:

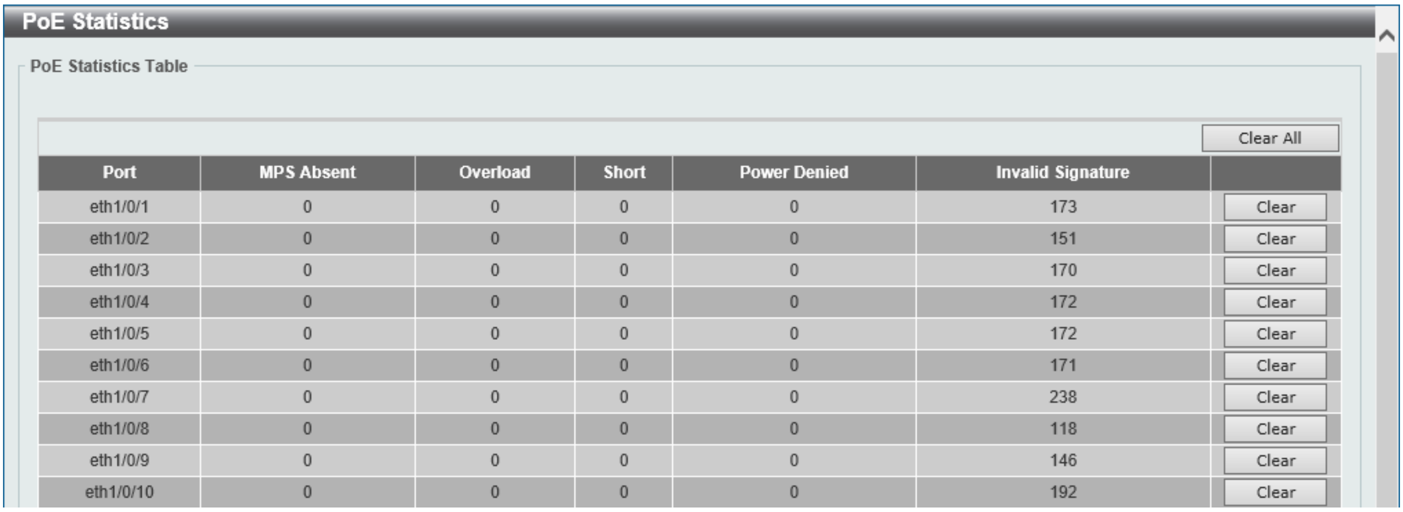
Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
PD Alive State	Select to enable or disable the PD Alive function on the specified port(s).
PD IP Address	Enter the IP address of the PD here.
Poll Interval	Enter the poll interval here. This is the interval between ping messages from the system to PDs connected to the PoE port(s). By default, this value is 30 seconds. The range is from 10 to 300 seconds.
Retry Count	Enter the retry count here. This is the amount of ping messages that will be sent (at each interval) when PDs are not responding. By default, this value is 2. The range is from 0 to 5.
Waiting Time	Enter the waiting time here. This is how long the system will wait before sending ping messages to the PD connected to the PoE port after the **Reset** action was taken. By default, this value is 90 seconds. The range is from 30 to 300 seconds.
Action	Select the action that will be taken here. Options to choose from are: • **Reset** - Specifies to reset the PoE port state (turn PoE off and on). • **Notify** - Specifies to send logs and traps to notify the administrator. • **Both** - Specifies to send logs and traps to notify the administrator and to reset the PoE port state (turn PoE off and on).

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

PoE Statistics

This window is used to display and clear the PoE statistics on the Switch ports.

To view the following window, click **System > PoE > PoE Statistics**, as shown below:



PoE Statistics

PoE Statistics Table

Port	MPS Absent	Overload	Short	Power Denied	Invalid Signature	
eth1/0/1	0	0	0	0	173	Clear
eth1/0/2	0	0	0	0	151	Clear
eth1/0/3	0	0	0	0	170	Clear
eth1/0/4	0	0	0	0	172	Clear
eth1/0/5	0	0	0	0	172	Clear
eth1/0/6	0	0	0	0	171	Clear
eth1/0/7	0	0	0	0	238	Clear
eth1/0/8	0	0	0	0	118	Clear
eth1/0/9	0	0	0	0	146	Clear
eth1/0/10	0	0	0	0	192	Clear

Figure 3-15 PoE Statistics Window

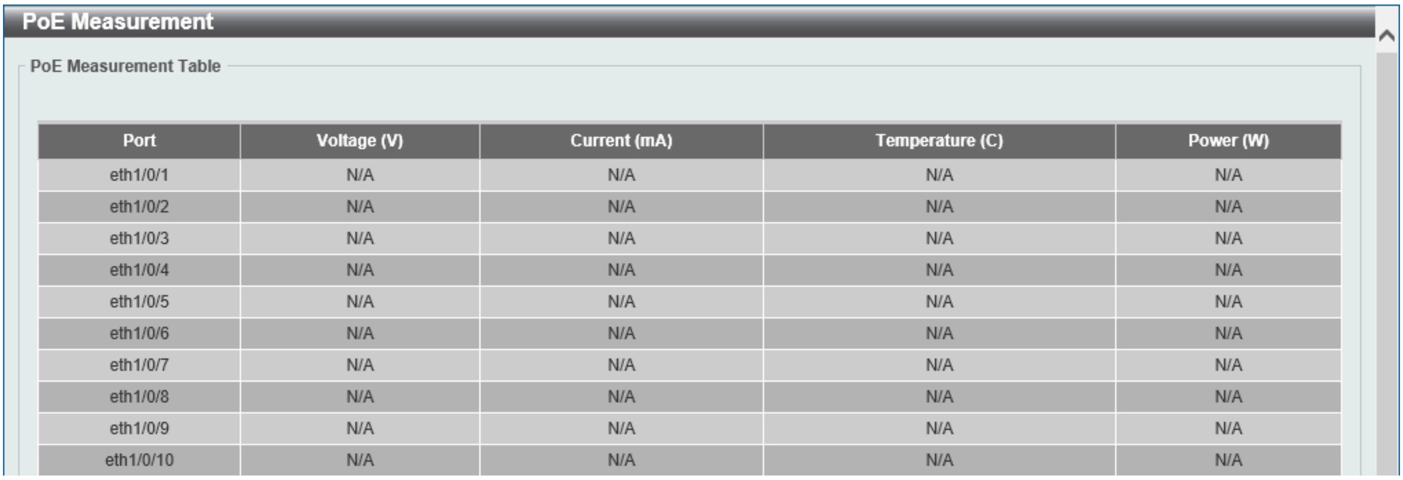
Click the **Clear All** button to clear PoE statistics for all ports.

Click the **Clear** button to clear the PoE statistics for the corresponding port.

PoE Measurement

This window is used to display the PoE measurement information on the Switch ports.

To view the following window, click **System > PoE > PoE Measurement**, as shown below:



PoE Measurement

PoE Measurement Table

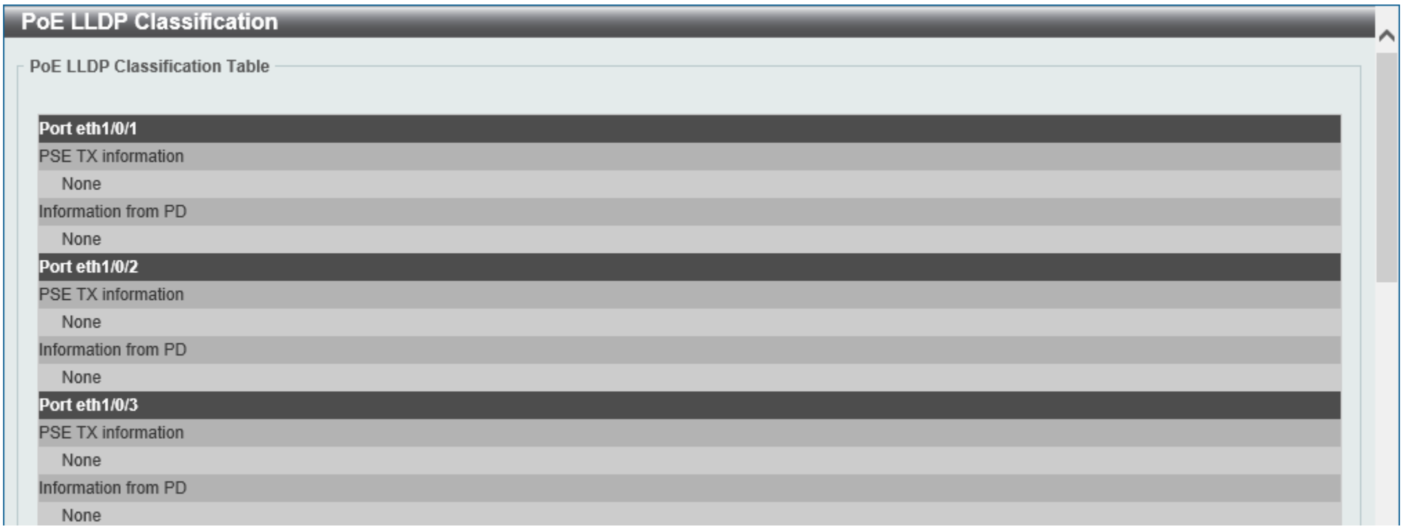
Port	Voltage (V)	Current (mA)	Temperature (C)	Power (W)
eth1/0/1	N/A	N/A	N/A	N/A
eth1/0/2	N/A	N/A	N/A	N/A
eth1/0/3	N/A	N/A	N/A	N/A
eth1/0/4	N/A	N/A	N/A	N/A
eth1/0/5	N/A	N/A	N/A	N/A
eth1/0/6	N/A	N/A	N/A	N/A
eth1/0/7	N/A	N/A	N/A	N/A
eth1/0/8	N/A	N/A	N/A	N/A
eth1/0/9	N/A	N/A	N/A	N/A
eth1/0/10	N/A	N/A	N/A	N/A

Figure 3-16 PoE Measurement Window

PoE LLDP Classification

This window is used to display the PoE Link Layer Discovery Protocol (LLDP) classification.

To view the following window, click **System > PoE > PoE LLDP Classification**, as shown below:



PoE LLDP Classification

PoE LLDP Classification Table

Port eth1/0/1	
PSE TX information	
	None
Information from PD	
	None
Port eth1/0/2	
PSE TX information	
	None
Information from PD	
	None
Port eth1/0/3	
PSE TX information	
	None
Information from PD	
	None

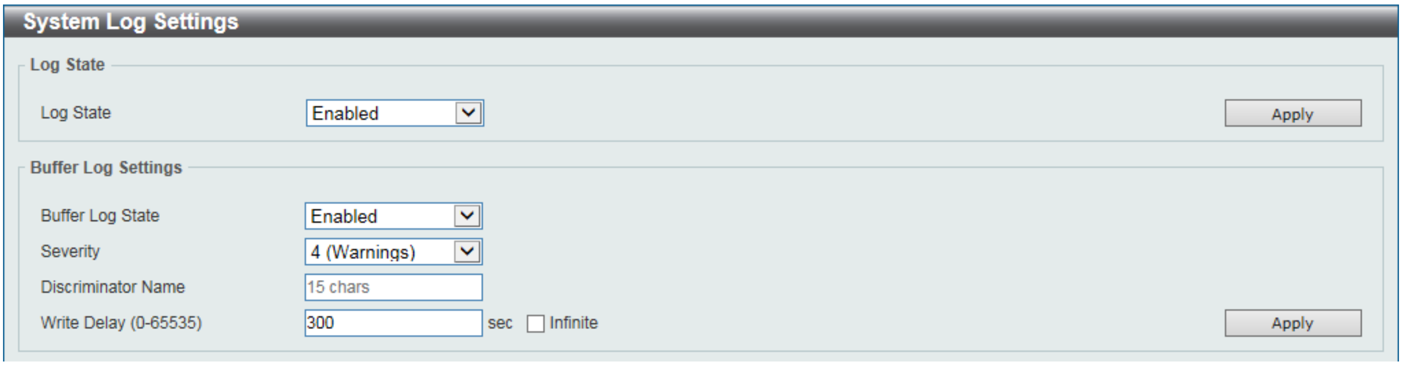
Figure 3-17 PoE LLDP Classification Window

System Log

System Log Settings

This window is used to display and configure the system log settings.

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



System Log Settings

Log State

Log State: Enabled

Buffer Log Settings

Buffer Log State: Enabled

Severity: 4 (Warnings)

Discriminator Name: 15 chars

Write Delay (0-65535): 300 sec □ Infinite

Figure 3-18 System Log Settings Window

The fields that can be configured for **Log State** are described below:

Parameter	Description
Log State	Select the enable or disable the global system log state here.

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

The fields that can be configured for **Buffer Log Settings** are described below:

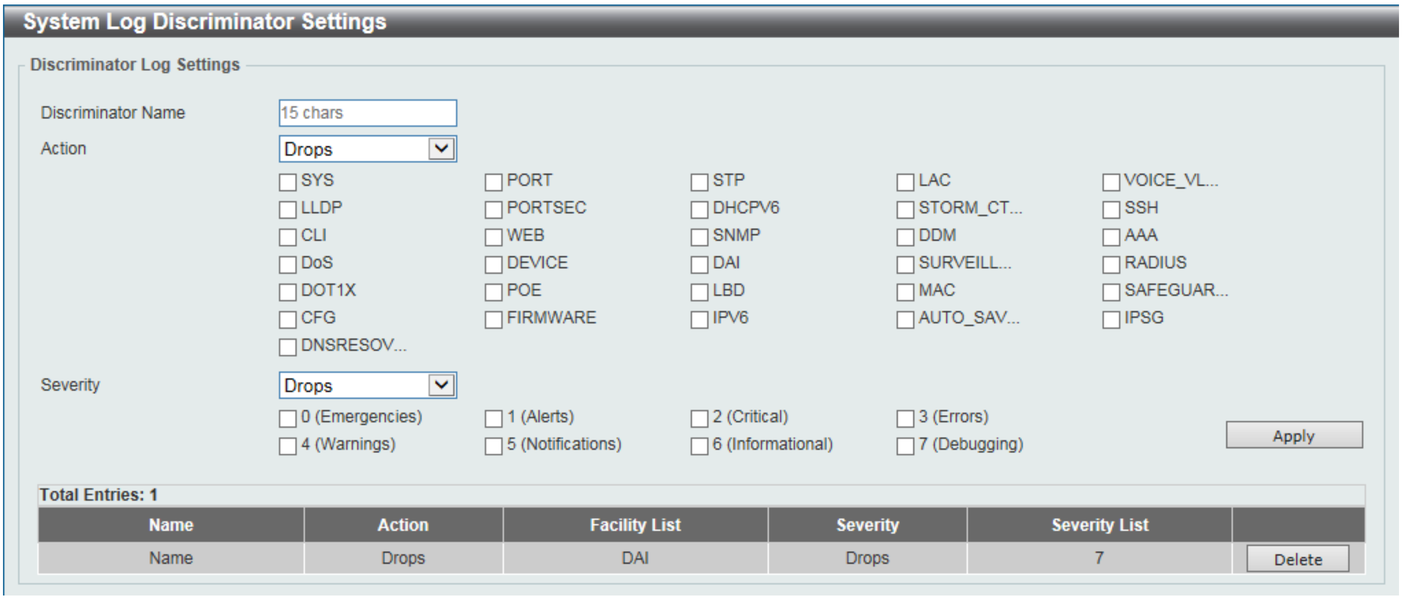
Parameter	Description
Buffer Log State	Select to globally enable or disable the buffer log state here. Options to choose from are **Enable**, **Disabled**, and **Default**. When selecting the **Default** option, the global buffer log state will follow the default behavior.
Severity	Select the severity value of the type of information that will be logged. Options to choose from are **0 (Emergencies)**, **1 (Alerts)**, **2 (Critical)**, **3 (Errors)**, **4 (Warnings)**, **5 (Notifications)**, **6 (Informational)**, and **7 (Debugging)**.
Discriminator Name	Enter the discriminator name used here. This name can be up to 15 characters long. This specifies the name of the discriminator profile that will be used to filter buffer log messages based on the filtering criteria specified within that profile.
Write Delay	Enter the log write delay value here. This value must be between 0 and 65535 seconds. By default, this value is 300 seconds. Tick the **Infinite** option, to disable the write delay feature.

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

System Log Discriminator Settings

This window is used to display and configure the system log discriminator settings.

To view the following window, click **System > System Log > System Log Discriminator Settings**, as shown below:



System Log Discriminator Settings

Discriminator Log Settings

Discriminator Name: 15 chars

Action: Drops

□ SYS □ PORT □ STP □ LAC □ VOICE_VL...
□ LLDP □ PORTSEC □ DHCPV6 □ STORM_CT... □ SSH
□ CLI □ WEB □ SNMP □ DDM □ AAA
□ DoS □ DEVICE □ DAI □ SURVEILL... □ RADIUS
□ DOT1X □ POE □ LBD □ MAC □ SAFEGUAR...
□ CFG □ FIRMWARE □ IPV6 □ AUTO_SAV... □ IPSG
□ DNSRESOV...

Severity: Drops

□ 0 (Emergencies) □ 1 (Alerts) □ 2 (Critical) □ 3 (Errors)
□ 4 (Warnings) □ 5 (Notifications) □ 6 (Informational) □ 7 (Debugging)

Apply

Total Entries: 1

Name	Action	Facility List	Severity	Severity List	
Name	Drops	DAI	Drops	7	Delete

Figure 3-19 System Log Discriminator Settings Window

The fields that can be configured are described below:

Parameter	Description
Discriminator Name	Enter the name of the discriminator profile here. This name can be up to 15 characters long.
Action	Select the facility behavior option and the type of facility that will be associated with the selected behavior here. Behavior options to choose from are **Drops** and **Includes**.
Severity	Select the severity behavior option and the value of the type of information that will be logged. Behavior options to choose from are **Drops** and **Includes**. Severity value options to choose from are **0 (Emergencies)**, **1 (Alerts)**, **2 (Critical)**, **3 (Errors)**, **4 (Warnings)**, **5 (Notifications)**, **6 (Informational)**, and **7 (Debugging)**.

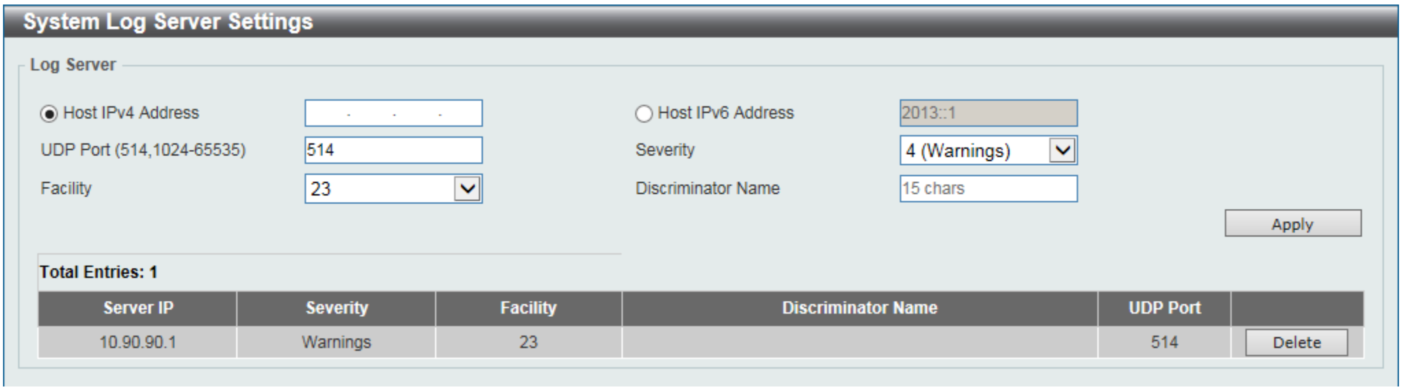
Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete the specified entry.

System Log Server Settings

This window is used to display and configure the system log server settings.

To view the following window, click **System > System Log > System Log Server Settings**, as shown below:



System Log Server Settings

Log Server

● Host IPv4 Address: . . .
○ Host IPv6 Address: 2013::1
UDP Port (514,1024-65535): 514
Severity: 4 (Warnings)
Facility: 23
Discriminator Name: 15 chars

Total Entries: 1

Server IP	Severity	Facility	Discriminator Name	UDP Port	
10.90.90.1	Warnings	23		514	Delete

Figure 3-20 System Log Server Settings Window

The fields that can be configured are described below:

Parameter	Description		
Host IPv4 Address	Enter the system log server IPv4 address here.		
Host IPv6 Address	Enter the system log server IPv6 address here.		
UDP Port	Enter the system log server UDP port number here. This value must be either 514 or between 1024 and 65535. By default, this value is 514.		
Severity	Select the severity value of the type of information that will be logged. Options to choose from are **0 (Emergencies)**, **1 (Alerts)**, **2 (Critical)**, **3 (Errors)**, **4 (Warnings)**, **5 (Notifications)**, **6 (Informational)**, and **7 (Debugging)**.		
Facility	Select the facility number that will be logged here. The range is from **0** to **23**. Each facility number is associated with a specific facility. See the table below:		
	Facility Number	**Facility Name**	**Facility Description**
	0	kern	Kernel messages
	1	user	User-level messages
	2	mail	Mail system
	3	daemon	System daemons
	4	auth1	Security/authorization messages
	5	syslog	Messages generated internally by the SYSLOG
	6	lpr	Line printer sub-system
	7	news	Network news sub-system
	8	uucp	UUCP sub-system
	9	clock1	Clock daemon
	10	auth2	Security/authorization messages
	11	ftp	FTP daemon
	12	ntp	NTP subsystem

Parameter	Description		
	13	logaudit	Log audit
	14	logalert	Log alert
	15	clock2	Clock daemon
	16	local0	Local use 0 (local0)
	17	local1	Local use 1 (local1)
	18	local2	Local use 2 (local2)
	19	local3	Local use 3 (local3)
	20	local4	Local use 4 (local4)
	21	local5	Local use 5 (local5)
	22	local6	Local use 6 (local6)
	23	local7	Local use 7 (local7)
Discriminator Name	Enter the name of the discriminator that will be used to filter messages sent to the log server here. This name can be up to 15 characters long.		

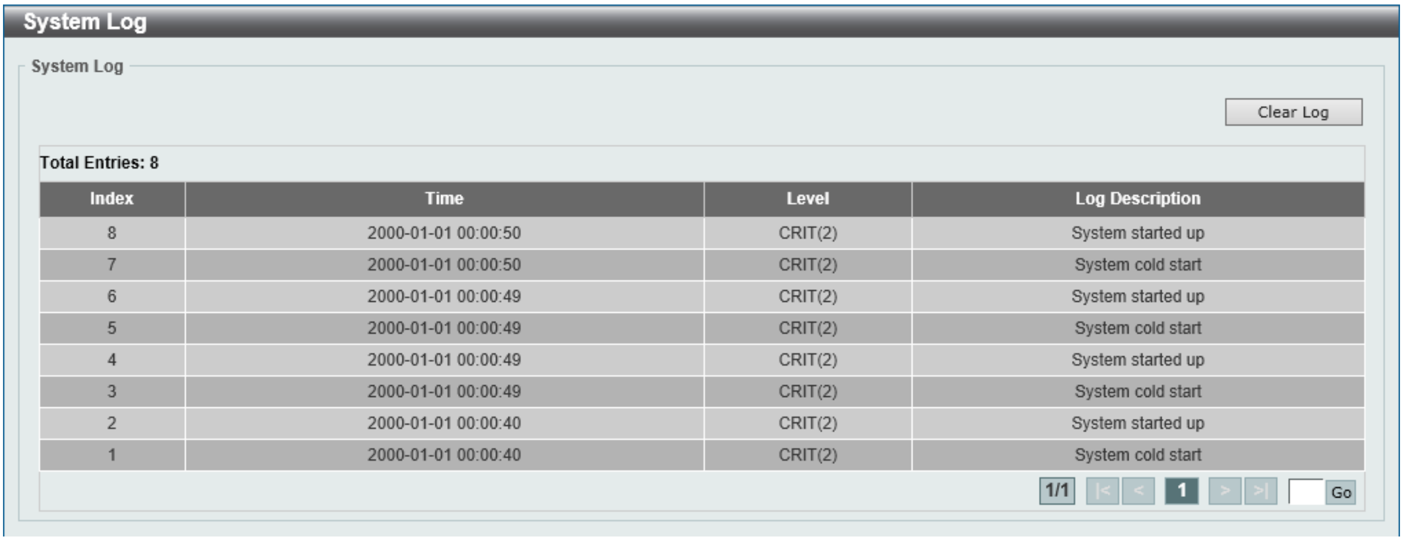
Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete the specified entry.

System Log

This window is used to view and clear the system log.

To view the following window, click **System > System Log > System Log**, as shown below:



Total Entries: 8

Index	Time	Level	Log Description
8	2000-01-01 00:00:50	CRIT(2)	System started up
7	2000-01-01 00:00:50	CRIT(2)	System cold start
6	2000-01-01 00:00:49	CRIT(2)	System started up
5	2000-01-01 00:00:49	CRIT(2)	System cold start
4	2000-01-01 00:00:49	CRIT(2)	System started up
3	2000-01-01 00:00:49	CRIT(2)	System cold start
2	2000-01-01 00:00:40	CRIT(2)	System started up
1	2000-01-01 00:00:40	CRIT(2)	System cold start

Figure 3-21 System Log Window

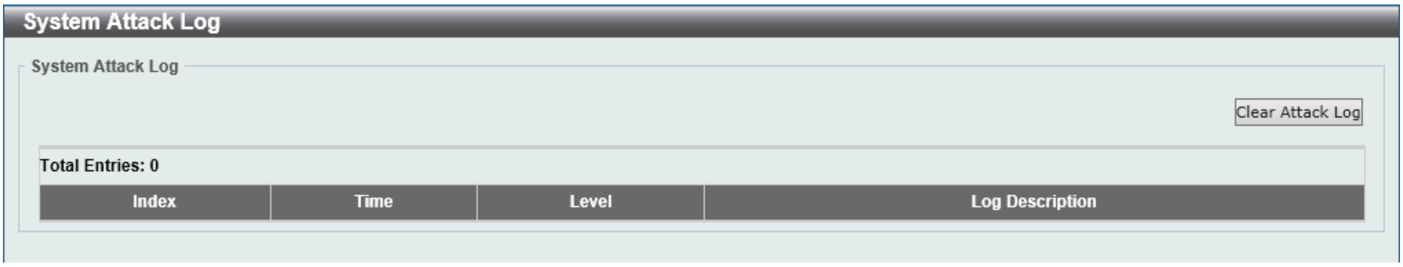
Click the **Clear Log** button to clear the system log entries displayed in the table.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

System Attack Log

This window is used to view and clear the system attack log.

To view the following window, click **System > System Log > System Attack Log**, as shown below:



Total Entries: 0

Index	Time	Level	Log Description

Figure 3-22 System Attack Log Window

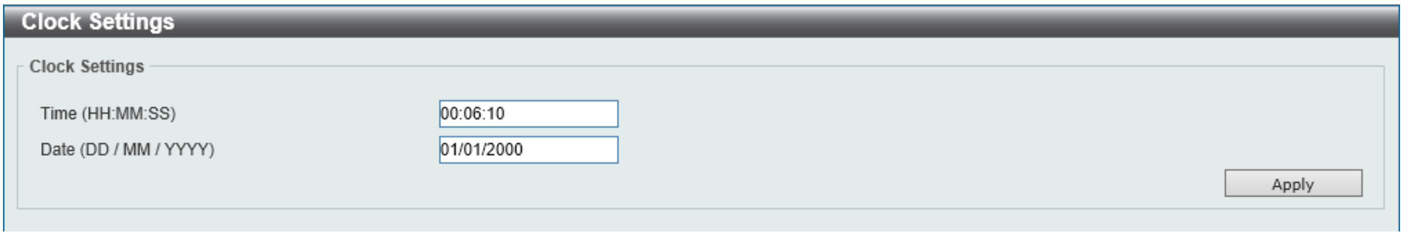
Click the **Clear Attack Log** button to clear the system attack log entries displayed in the table.

Time and SNTP

Clock Settings

This window is used to display and configure the time settings for the Switch.

To view the following window, click **System > Time and SNTP > Clock Settings**, as shown below:



Time (HH:MM:SS) 00:06:10
Date (DD / MM / YYYY) 01/01/2000

Figure 3-23 Clock Settings Window

The fields that can be configured are described below:

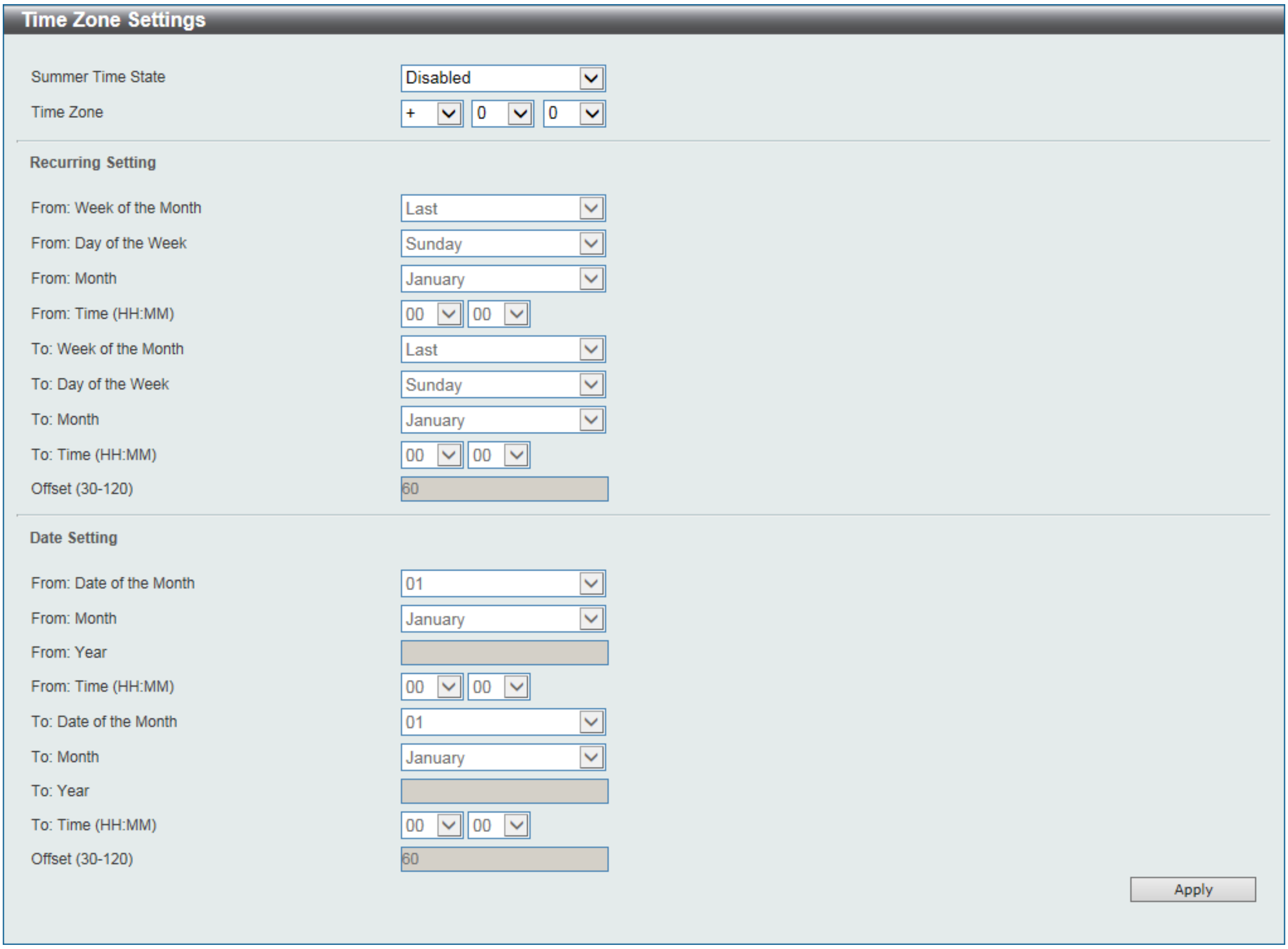
Parameter	Description
Time	Enter the current time in hours (HH), minutes (MM), and seconds (SS) here. For example, 18:30:30.
Date	Enter the current day (DD), month (MM), and year (YYYY) here. For example, 30/09/2019.

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

Time Zone Settings

This window is used to display and configure time zones and Daylight Savings Time settings for SNTP.

To view the following window, click **System > Time and SNTP > Time Zone Settings**, as shown below:



Summer Time State	Disabled
Time Zone	+ 0 0
Recurring Setting	
From: Week of the Month	Last
From: Day of the Week	Sunday
From: Month	January
From: Time (HH:MM)	00 00
To: Week of the Month	Last
To: Day of the Week	Sunday
To: Month	January
To: Time (HH:MM)	00 00
Offset (30-120)	60
Date Setting	
From: Date of the Month	01
From: Month	January
From: Year	
From: Time (HH:MM)	00 00
To: Date of the Month	01
To: Month	January
To: Year	
To: Time (HH:MM)	00 00
Offset (30-120)	60

Figure 3-24 Time Zone Settings Window

The fields that can be configured are described below:

Parameter	Description
Summer Time State	Select the summer time setting. Options to choose from are: • **Disabled** - Select to disable the summer time setting. • **Recurring Setting** - Select to configure the summer time that should start and end on the specified weekday of the specified month. • **Date Setting** - Select to configure the summer time that should start and end on the specified date of the specified month.
Time Zone	Select to specify your local time zone offset from Coordinated Universal Time (UTC).

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

Parameter	Description
From: Week of the Month	Select week of the month that summer time will start.
From: Day of the Week	Select the day of the week that summer time will start.

Parameter	Description
From: Month	Select the month that summer time will start.
From: Time	Select the time of the day that summer time will start.
To: Week of the Month	Select week of the month that summer time will end.
To: Day of the Week	Select the day of the week that summer time will end.
To: Month	Select the month that summer time will end.
To: Time	Select the time of the day that summer time will end.
Offset	Enter the number of minutes to add during summer time. The default value is 60. The range of this offset is between 30 and 120.

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

Parameter	Description
From: Date of the Month	Select date of the month that summer time will start.
From: Month	Select the month that summer time will start.
From: Year	Enter the year that the summer time will start.
From: Time	Select the time of the day that summer time will start.
To: Date of the Month	Select date of the month that summer time will end.
To: Month	Select the month that summer time will end.
To: Year	Enter the year that the summer time will end.
To: Time	Select the time of the day that summer time will end.
Offset	Enter the number of minutes to add during summer time. The default value is 60. The range of this offset is between 30 and 120.

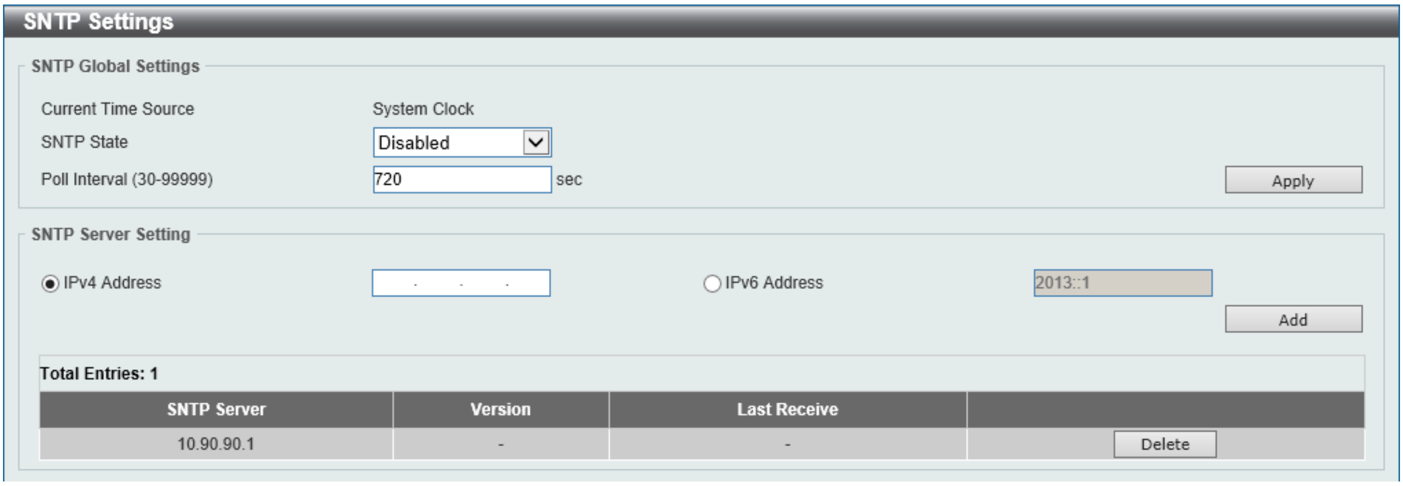
Click the **Apply** button to accept the changes made.

SNTP Settings

The Simple Network Time Protocol (SNTP) is a protocol for synchronizing computer clocks through the Internet. It provides comprehensive mechanisms to access national time and frequency dissemination services, coordinate the SNTP subnet of servers and clients, and adjust the system clock on each participant.

This window is used to display and configure the SNTP settings for the Switch.

To view the following window, click **System > Time and SNTP > SNTP Settings**, as shown below:



SNTP Settings

SNTP Global Settings

Current Time Source: System Clock

SNTP State: Disabled

Poll Interval (30-99999): 720 sec

SNTP Server Setting

● IPv4 Address: . . .

○ IPv6 Address: 2013::1

Total Entries: 1

SNTP Server	Version	Last Receive	
10.90.90.1	-	-	Delete

Figure 3-25 SNTP Settings Window

The fields that can be configured in **SNTP Global Settings** are described below:

Parameter	Description
SNTP State	Select this option to enable or disable SNTP.
Poll Interval	Enter the synchronizing interval in seconds. The value is from 30 to 99999 seconds. The default interval is 720 seconds.

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

The fields that can be configured in **SNTP Server Settings** are described below:

Parameter	Description
IPv4 Address	Enter the IPv4 address of the SNTP server that provides the SNTP reference.
IPv6 Address	Enter the IPv6 address of the SNTP server that provides the SNTP reference.

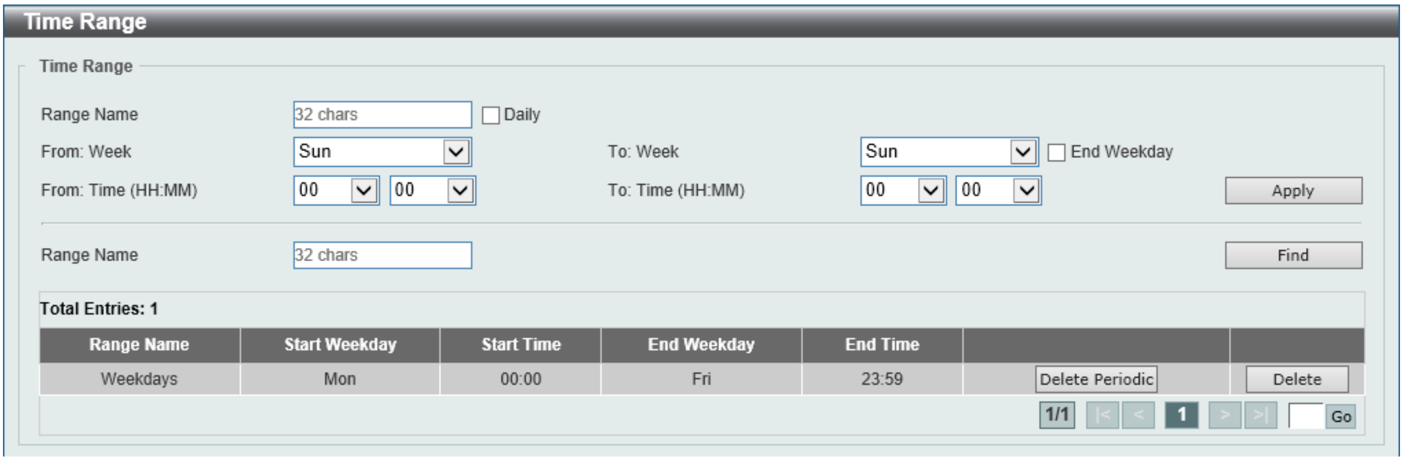
Click the **Add** button to add the SNTP server.

Click the **Delete** button to remove the specified entry.

Time Range

This window is used to display and configure the time profile settings.

To view the following window, click **System > Time Range**, as shown below:



Time Range

Time Range

Range Name: 32 chars □ Daily

From: Week: Sun — To: Week: Sun □ End Weekday

From: Time (HH:MM): 00 00 — To: Time (HH:MM): 00 00

Range Name: 32 chars

Total Entries: 1

Range Name	Start Weekday	Start Time	End Weekday	End Time		
Weekdays	Mon	00:00	Fri	23:59	Delete Periodic	Delete

Figure 3-26 Time Range Window

The fields that can be configured are described below:

Parameter	Description
Range Name	Enter the time profile range name here. This name can be up to 32 characters long.
From Week ~ To Week	Select the starting and ending days of the week that will be used for this time profile. Tick the **Daily** option to use this time profile for every day of the week. Tick the **End Week Day** option to use this time profile from the starting day of the week until the end of the week.
From Time ~ To Time	Select the starting and ending time of the day that will be used for this time profile. The first drop-down menu selects the hour and the second drop-down menu selects the minute.

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 Periodic** button to delete the periodic entry.

Click the **Delete** button to delete the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

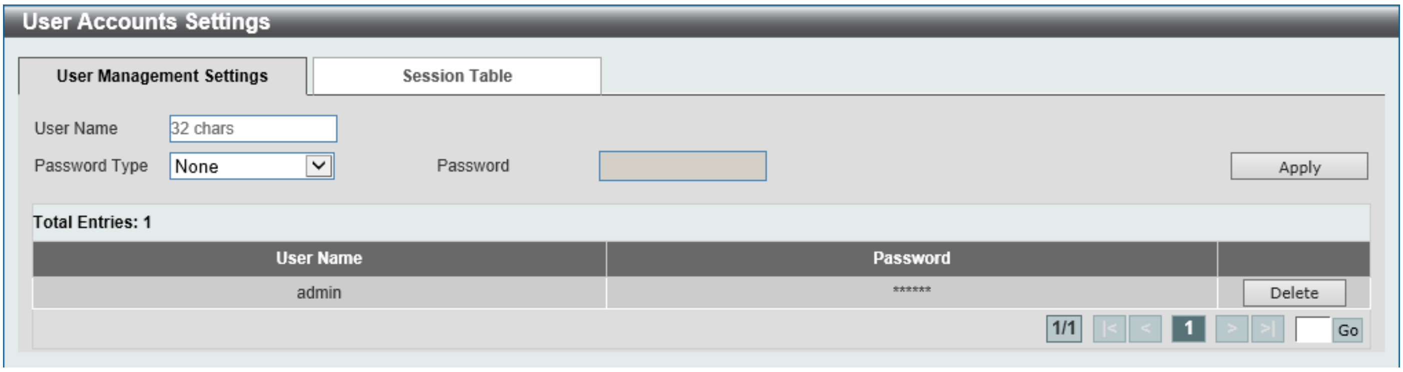
4. Management

User Accounts Settings

On this page, user accounts can be created and updated. Active user account sessions can also be viewed on this page.

To view the following window, click **Management > User Accounts Settings**, as shown below:

After selecting the **User Management Settings** tab, the following page will appear.



User Accounts Settings

User Name: 32 chars

Password Type: None

Password:

Total Entries: 1

User Name	Password	
admin	******	Delete

Figure 4-1 User Accounts Settings Window

The fields that can be configured are described below:

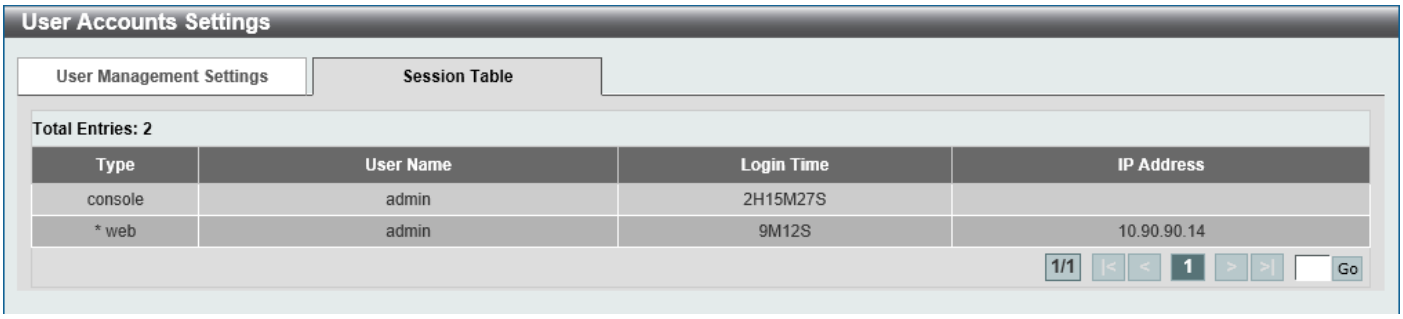
Parameter	Description
User Name	Enter the user account name here. This name can be up to 32 characters long.
Password Type	Select the password type for this user account here. Options to choose from are **None** and **Plain Text**.
Password	After selecting **Plain Text** as the password type, enter the password for this user account here.

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

Click the **Delete** button to delete the specified user account entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After selecting the **Session Table** tab, the following page will appear.



User Accounts Settings

Total Entries: 2

Type	User Name	Login Time	IP Address
console	admin	2H15M27S	
* web	admin	9M12S	10.90.90.14

Figure 4-2 Session Table Window

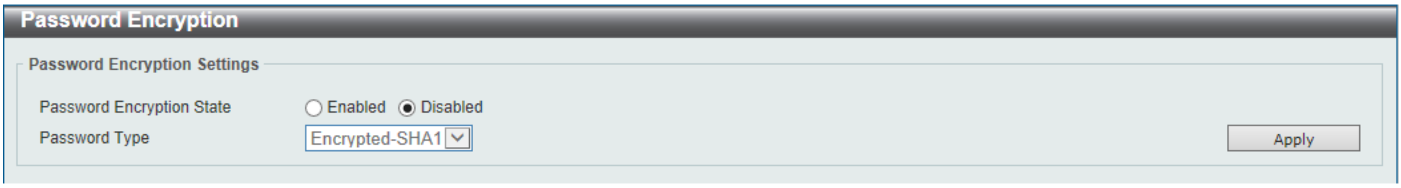
On this page, a list of active user account session will be displayed.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Password Encryption

This window is used to display and configure whether to save the encryption of the password in the configuration file.

To view the following window, click **Management > Password Encryption**, as shown below:



Password Encryption

Password Encryption Settings

Password Encryption State ○ Enabled ● Disabled

Password Type: Encrypted-SHA1

Figure 4-3 Password Encryption Window

The fields that can be configured are described below:

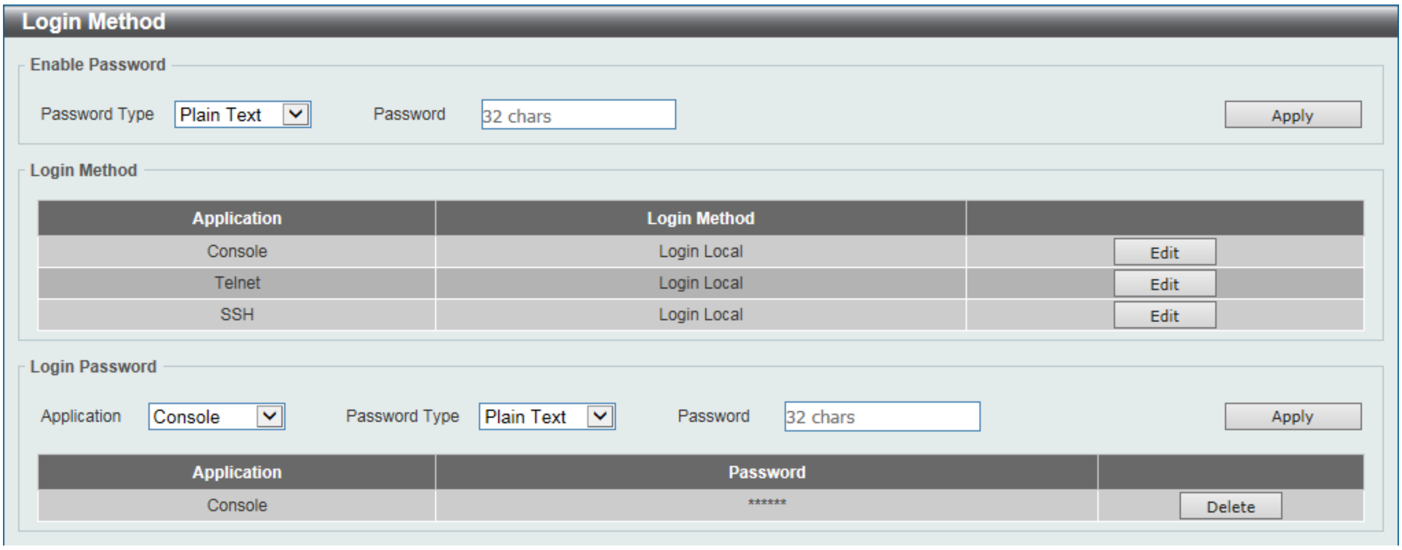
Parameter	Description
Password Encryption State	Select this option to enable or disable the encryption of the password before being stored in the configuration file.
Password Type	When the state is enabled, select the password encryption type here. Options to choose from are: • **Encrypted-SHA1** - Specifies that the password is encrypted using SHA-1. • **Encrypted-MD5** - Specifies that the password is encrypted using MD5.

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

Login Method

This window is used to display and configure the login method for each management interface that is supported by the Switch.

To view the following window, click **Management > Login Method**, as shown below:



Login Method

Enable Password

Password Type: Plain Text
Password: 32 chars
Apply

Login Method

Application	Login Method	
Console	Login Local	Edit
Telnet	Login Local	Edit
SSH	Login Local	Edit

Login Password

Application: Console
Password Type: Plain Text
Password: 32 chars
Apply

Application	Password	
Console	******	Delete

Figure 4-4 Login Method Window

The fields that can be configured in **Enable Password** are described below:

Parameter	Description
Password Type	Select the password type for the user here. Options to choose from are: • **Plain Text** - Specifies that the password will be in plain text. This is the default option. • **Encrypted** - Specifies that the password will be encrypted based on SHA-1. • **Encrypted-MD5** - Specifies that the password will be encrypted based on MD5.
Password	Enter the password for the user account here. In the plain-text form, the password can be up to 32 characters long, is case-sensitive, and can contain spaces. In the encrypted form, the password must be 35 bytes long and is case-sensitive. In the encrypted MD5 form, the password must be 31 bytes long and is case-sensitive.

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

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

The fields that can be configured in **Login Method** are described below:

Parameter	Description
Login Method	After clicking the **Edit** button, this parameter can be configured. Select the login method for the specified application here. Options to choose from are **No Login**, **Login** and **Login Local**. • **No Login** requires no login authentication to access the specified application. • **Login** will require the user to at least enter a password when trying to access the application specified. • **Login Local** requires the user to enter a username and a password to access the specified application.

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

The fields that can be configured in **Login Password** are described below:

Parameter	Description
Application	Select the application that will be configured here. Options to choose from are **Console**, **Telnet** and **SSH**.
Password Type	Select the password encryption type that will be used here. Options to choose from are **Plain Text**, **Encrypted**, and **Encrypted-MD5**.
Password	Enter the password for the selected application here. This password will be used when the **Login Method** for the specified application is set as **Login**. In the plain-text form, the password can be up to 32 characters long, is case-sensitive, and can contain spaces. In the encrypted form, the password must be 35 bytes long and is case-sensitive. In the encrypted MD5 form, the password must be 31 bytes long and is case-sensitive.

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

Click the **Delete** button to remove the password from the specified application.

SNMP

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) 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, monitor performance, and detect potential problems with the Switch, switch group, or network.

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 Switch supports the SNMP versions 1, 2c, and 3. The three versions of SNMP vary in the level of security provided between the management station and the network device.

In SNMPv1 and SNMPv2c, user authentication is accomplished using ‘community strings’, which function like passwords. The remote user SNMP application and the Switch SNMP must use the same community string. SNMP packets from any station that has not been authenticated are ignored (dropped). The default community strings for the Switch used for SNMPv1 and SNMPv2c management access are:

- **public** - Allows authorized management stations to retrieve MIB objects.
- **private** - Allows authorized management stations to retrieve and modify MIB objects.

The SNMPv3 protocol uses a more sophisticated authentication process that is separated into two parts. The first part maintains a list of users and their attributes that are allowed to act as SNMP managers. The second part describes what each user in that list can do as an SNMP manager. The SNMPv3 protocol also provides an additional layer of security that can be used to encrypt SNMP messages.

The Switch allows groups of users to be listed and configured with a shared set of privileges. The SNMP version may also be set for a listed group of SNMP managers. Thus, you may create a group of SNMP managers that are allowed to view read-only information or receive traps using SNMPv1 while assigning a higher level of security to another group, granting read/write privileges using SNMPv3.

Using SNMPv3, users or groups can be allowed or be prevented from performing specific SNMP management functions. These are defined using the Object Identifier (OID) associated with a specific MIB.

MIBs

A Management Information Base (MIB) stores management and counter information. The Switch uses the standard MIB-II Management Information Base module, and so values for MIB objects can be retrieved using any SNMP-based network management software. In addition to the standard MIB-II, the Switch also supports its own proprietary enterprise MIB as an extended Management Information Base. Specifying the MIB Object Identifier may also retrieve the proprietary MIB. MIB values can be either read-only or read-write.

The Switch incorporates a flexible SNMP management system that can be customized to suit the needs of the networks and the preferences of the network administrator. The three versions of SNMP vary in the level of security provided between the management station and the network device. SNMP settings are configured using the menus located in the **SNMP** folder of the Web UI.

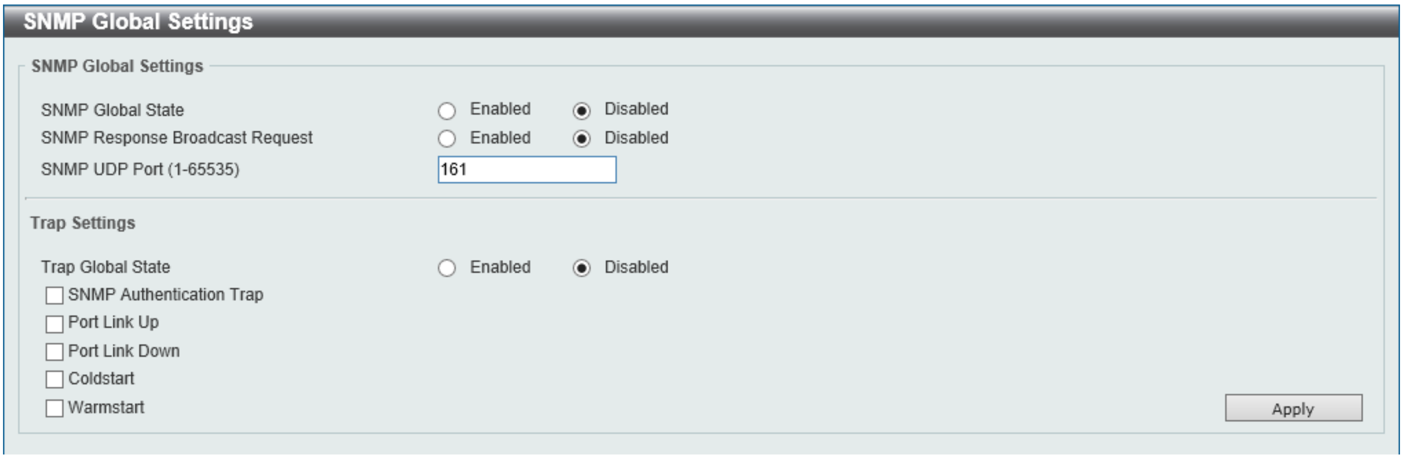
Traps

Traps are messages that alert network personnel of events that occur on the Switch. The events can be as serious as a reboot (someone accidentally turned the Switch off/unplugged the Switch), or less serious like a port status change. The Switch generates traps and sends them to the trap recipient (or network manager). Typical traps include trap messages for Authentication Failure, Topology Change, and Broadcast/Multicast Storm.

SNMP Global Settings

This window is used to display and configure the global SNMP and trap settings.

To view the following window, click **Management > SNMP > SNMP Global Settings**, as shown below:



SNMP Global Settings

SNMP Global Settings

SNMP Global State ○ Enabled ● Disabled

SNMP Response Broadcast Request ○ Enabled ● Disabled

SNMP UDP Port (1-65535) 161

Trap Settings

Trap Global State ○ Enabled ● Disabled

□ SNMP Authentication Trap

□ Port Link Up

□ Port Link Down

□ Coldstart

□ Warmstart

Figure 4-5 SNMP Global Settings Window

The fields that can be configured in **SNMP Global Settings** are described below:

Parameter	Description
SNMP Global State	Select this option to enable or disable the SNMP feature.
SNMP Response Broadcast Request	Select this option to enable or disable the server to response to broadcast SNMP GetRequest packets.
SNMP UDP Port	Enter the SNMP UDP port number.

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

Parameter	Description
Trap Global State	Select this option to enable or disable the sending of all or specific SNMP notifications.

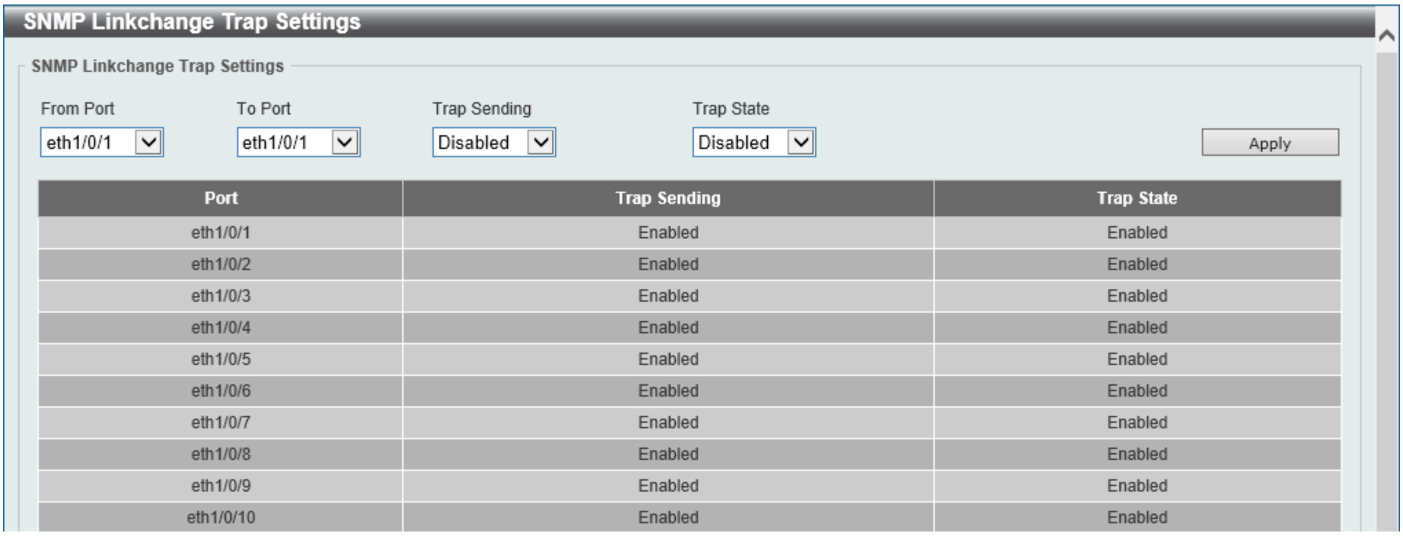
Parameter	Description
SNMP Authentication Trap	Tick this option to control the sending of SNMP authentication failure notifications. An *authenticationFailuretrap* trap is generated when the device receives an SNMP message that is not properly authenticated. The authentication method depends on the version of SNMP being used. For SNMPv1 or SNMPv2c, authentication failure occurs if packets are formed with an incorrect community string.
Port Link Up	Tick this option to control the sending of port link up notifications. A *linkUp* trap is generated when the device recognizes that one of the communication links has come up.
Port Link Down	Tick this option to control the sending of port link down notifications. A *linkDown* trap is generated when the device recognizes that a one of the communication links is down.
Coldstart	Tick this option to control the sending of SNMP *coldStart* notifications.
Warmstart	Tick this option to control the sending of SNMP *warmStart* notifications.

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

SNMP Linkchange Trap Settings

This window is used to display and configure the SNMP link change trap settings.

To view the following window, click **Management > SNMP > SNMP Linkchange Trap Settings**, as shown below:



SNMP Linkchange Trap Settings

SNMP Linkchange Trap Settings

From Port: eth1/0/1
To Port: eth1/0/1
Trap Sending: Disabled
Trap State: Disabled

Port	Trap Sending	Trap State
eth1/0/1	Enabled	Enabled
eth1/0/2	Enabled	Enabled
eth1/0/3	Enabled	Enabled
eth1/0/4	Enabled	Enabled
eth1/0/5	Enabled	Enabled
eth1/0/6	Enabled	Enabled
eth1/0/7	Enabled	Enabled
eth1/0/8	Enabled	Enabled
eth1/0/9	Enabled	Enabled
eth1/0/10	Enabled	Enabled

Figure 4-6 SNMP Linkchange Trap Settings Window

The fields that can be configured are described below:

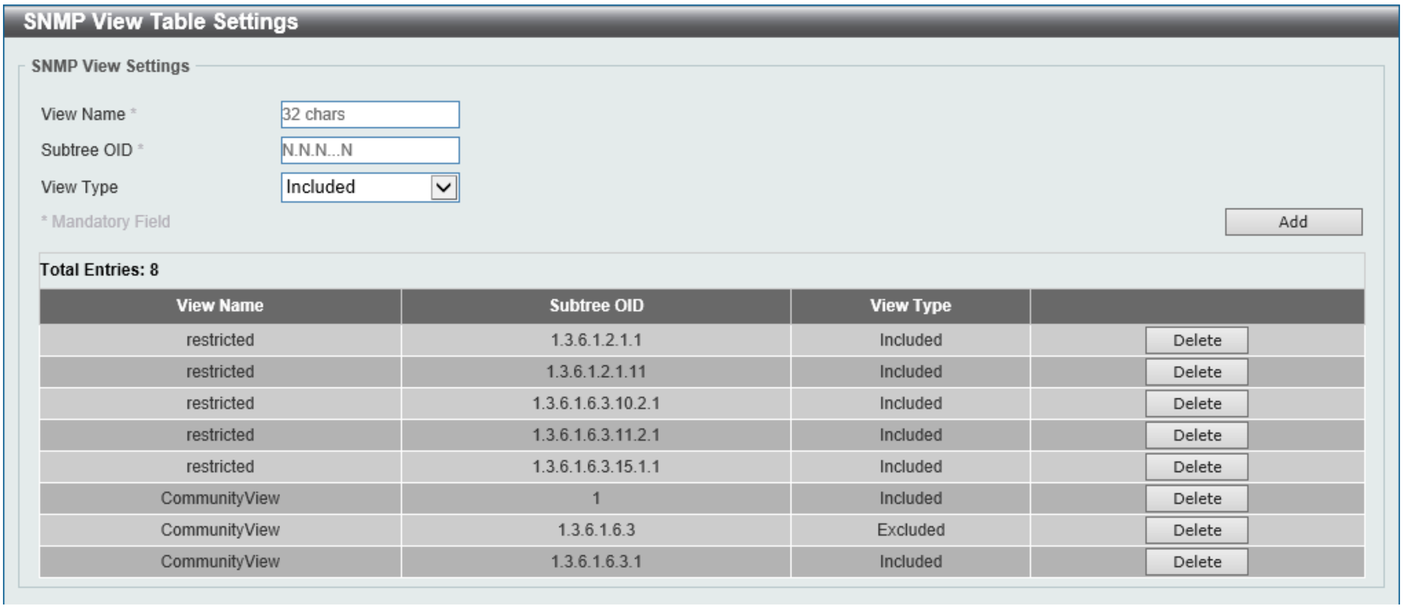
Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Trap Sending	Select this option to enable or disable the sending of the SNMP notification traps that are generated by the system.
Trap State	Select this option to enable or disable the SNMP *linkChange* trap.

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

SNMP View Table Settings

This window is used to assign views to community strings that define which MIB objects can be accessed by a remote SNMP manager. The SNMP sub-tree OID created with this table maps SNMP users to the views created in the **SNMP User Table Settings** window.

To view the following window, click **Management > SNMP > SNMP View Table Settings**, as shown below:



SNMP View Table Settings

SNMP View Settings

View Name *: 32 chars

Subtree OID *: N.N.N...N

View Type: Included

* Mandatory Field

Total Entries: 8

View Name	Subtree OID	View Type	
restricted	1.3.6.1.2.1.1	Included	Delete
restricted	1.3.6.1.2.1.11	Included	Delete
restricted	1.3.6.1.6.3.10.2.1	Included	Delete
restricted	1.3.6.1.6.3.11.2.1	Included	Delete
restricted	1.3.6.1.6.3.15.1.1	Included	Delete
CommunityView	1	Included	Delete
CommunityView	1.3.6.1.6.3	Excluded	Delete
CommunityView	1.3.6.1.6.3.1	Included	Delete

Figure 4-7 SNMP View Table Settings Window

The fields that can be configured are described below:

Parameter	Description
View Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP view being created.
Subtree OID	Type the Object Identifier (OID) sub-tree for the view. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.
View Type	Select the view type here. Options to choose from are: • **Included** - Select to include this object in the list of objects that an SNMP manager can access. • **Excluded** - Select to exclude this object from the list of objects that an SNMP manager can access.

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

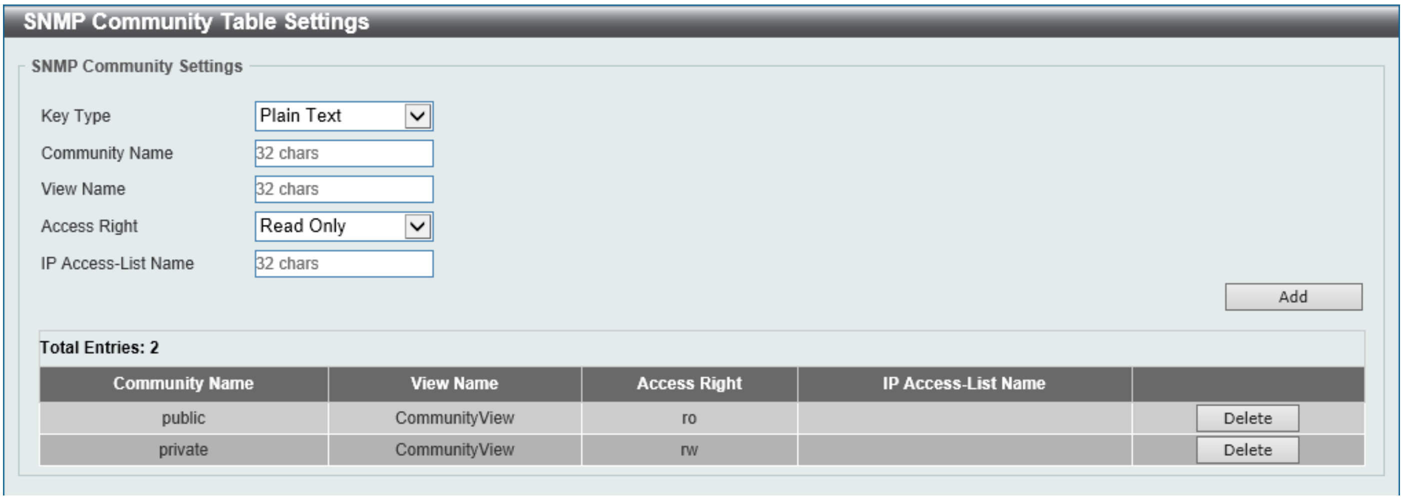
Click the **Delete** button to remove the specified entry.

SNMP Community Table Settings

This window is used to create an SNMP community string to define the relationship between the SNMP manager and an agent. The community string acts like a password to permit access to the agent on the Switch. One or more of the following characteristics can be associated with the community string:

- An access list containing IP addresses of SNMP managers that are permitted to use the community string to gain access to the Switch’s SNMP agent.
- Any MIB view that defines the subset of MIB objects that will be accessible to the SNMP community.
- Read-write or read-only level permissions for the MIB objects accessible to the SNMP community.

To view the following window, click **Management > SNMP > SNMP Community Table Settings**, as shown below:



SNMP Community Table Settings

SNMP Community Settings

Key Type	Plain Text
Community Name	32 chars
View Name	32 chars
Access Right	Read Only
IP Access-List Name	32 chars

Total Entries: 2

Community Name	View Name	Access Right	IP Access-List Name	
public	CommunityView	ro		Delete
private	CommunityView	rw		Delete

Figure 4-8 SNMP Community Table Settings Window

The fields that can be configured are described below:

Parameter	Description
Key Type	The only supported key type is **Plain Text**.
Community Name	Enter an alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.
View Name	Enter an alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. The view name must exist in the SNMP View Table.
Access Right	Select the access right here. Options to choose from are: • **Read Only** - SNMP community members using the community string created can only read the contents of the MIBs on the Switch. • **Read Write** - SNMP community members using the community string created can read from, and write to the contents of the MIBs on the Switch.
IP Access-List Name	Enter the name of the standard access list to restrict the users that can use this community string to access to the SNMP agent.

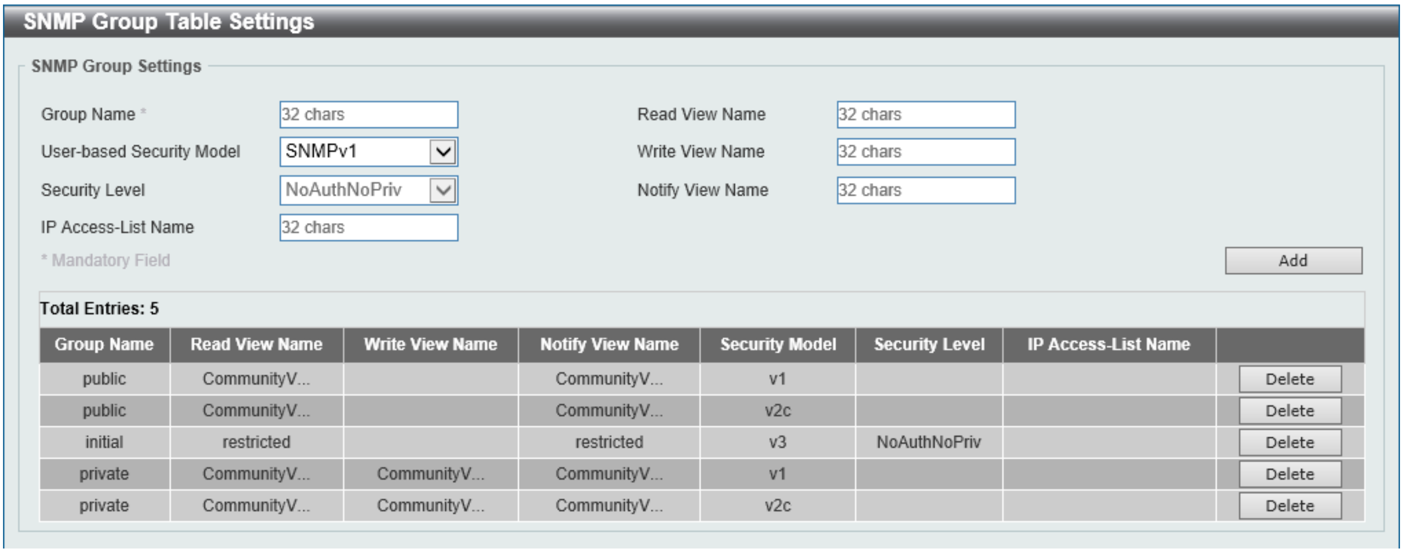
Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove the specified entry.

SNMP Group Table Settings

An SNMP group created with this table maps SNMP users to the views created in the **SNMP View Table Settings** window.

To view the following window, click **Management > SNMP > SNMP Group Table Settings**, as shown below:



SNMP Group Table Settings

SNMP Group Settings

Group Name * 32 chars
User-based Security Model SNMPv1
Security Level NoAuthNoPriv
IP Access-List Name 32 chars
Read View Name 32 chars
Write View Name 32 chars
Notify View Name 32 chars

* Mandatory Field

Total Entries: 5

Group Name	Read View Name	Write View Name	Notify View Name	Security Model	Security Level	IP Access-List Name	
public	CommunityV...		CommunityV...	v1			Delete
public	CommunityV...		CommunityV...	v2c			Delete
initial	restricted		restricted	v3	NoAuthNoPriv		Delete
private	CommunityV...	CommunityV...	CommunityV...	v1			Delete
private	CommunityV...	CommunityV...	CommunityV...	v2c			Delete

Figure 4-9 SNMP Group Table Settings Window

The fields that can be configured are described below:

Parameter	Description
Group Name	Enter the SNMP group name here. This name can be up to 32 characters long. Spaces are not allowed.
Read View Name	Enter the read view name that users of the group can access.
User-based Security Model	Select the security model here. Options to choose from are: • **SNMPv1** - Select to allow the group to use the SNMPv1 security model. • **SNMPv2c** - Select to allow the group to use the SNMPv2c security model. • **SNMPv3** - Select to allow the group to use the SNMPv3 security model.
Write View Name	Enter the write view name that the users of the group can access.
Security Level	When selecting **SNMPv3** in the **User-based Security Model** drop-down list, this option is available. • **NoAuthNoPriv** - Specify that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. • **AuthNoPriv** - Specify that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. • **AuthPriv** - Specify that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.
Notify View Name	Enter the notify view name that users of the group can access. The notify view describes the object that can be reported its status via trap packets to the group user.
IP Access-List Name	Enter the standard IP access control list (ACL) to associate with the group.

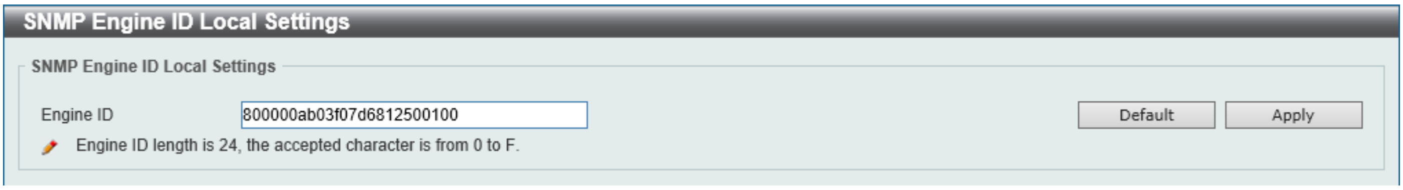
Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove the specified entry.

SNMP Engine ID Local Settings

The Engine ID is a unique identifier used for SNMPv3 implementations on the Switch.

To view the following window, click **Management > SNMP > SNMP Engine ID Local Settings**, as shown below:



SNMP Engine ID Local Settings

SNMP Engine ID Local Settings

Engine ID: 800000ab03f07d6812500100

Engine ID length is 24, the accepted character is from 0 to F.

Figure 4-10 SNMP Engine ID Local Settings Window

The fields that can be configured are described below:

Parameter	Description
Engine ID	Enter the SNMP engine ID string here. This string can be up to 24 characters long.

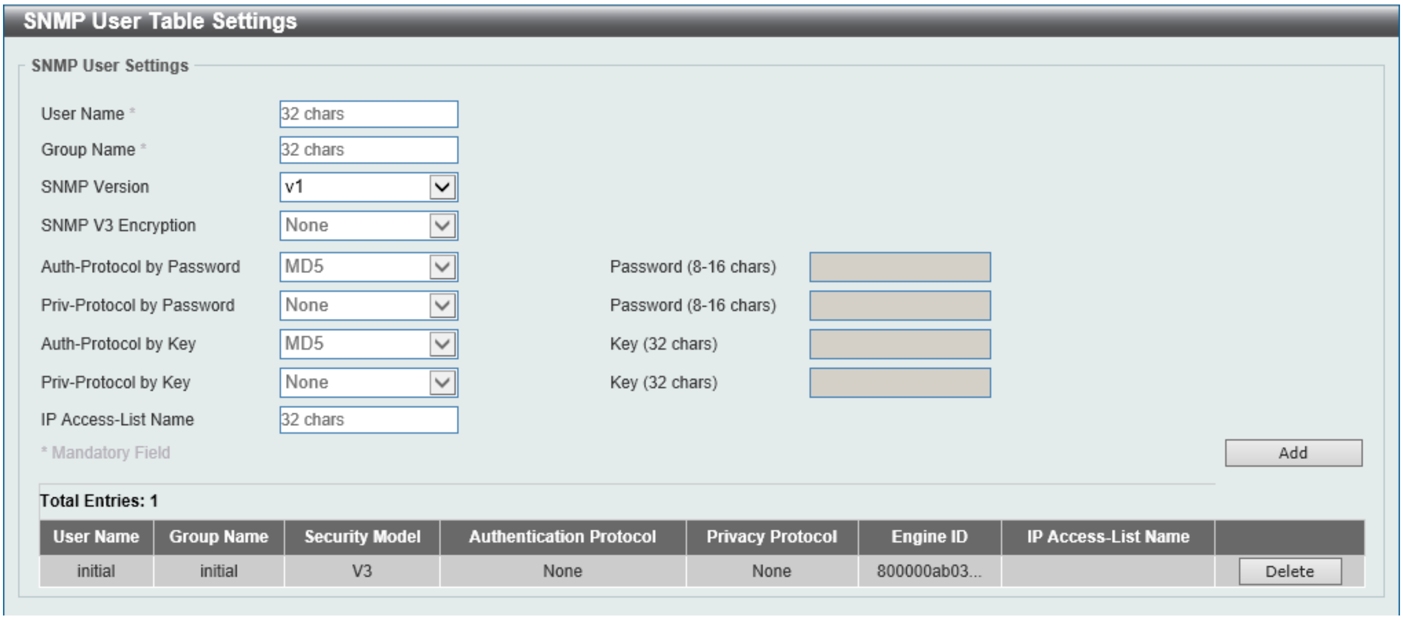
Click the **Default** button to revert the engine ID to the default.

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

SNMP User Table Settings

This window is used to display and configure the SNMP users that are currently configured on the Switch.

To view the following window, click **Management > SNMP > SNMP User Table Settings**, as shown below:



SNMP User Table Settings

SNMP User Settings

User Name *: 32 chars

Group Name *: 32 chars

SNMP Version: v1

SNMP V3 Encryption: None

Auth-Protocol by Password: MD5 — Password (8-16 chars)

Priv-Protocol by Password: None — Password (8-16 chars)

Auth-Protocol by Key: MD5 — Key (32 chars)

Priv-Protocol by Key: None — Key (32 chars)

IP Access-List Name: 32 chars

* Mandatory Field

Total Entries: 1

User Name	Group Name	Security Model	Authentication Protocol	Privacy Protocol	Engine ID	IP Access-List Name	
initial	initial	V3	None	None	800000ab03...		Delete

Figure 4-11 SNMP User Table Settings Window

The fields that can be configured are described below:

Parameter	Description
User Name	Enter SNMP user name here. This name can be up to 32 characters long. This is used to identify the SNMP user.
Group Name	Enter the SNMP group name to which the user belongs. This name can be up to 32 characters long. Spaces are not allowed.

Parameter	Description
SNMP Version	Select the SNMP version. Options to choose from are **v1**, **v2c**, and **v3**.
SNMP V3 Encryption	When selecting **v3** in the **SNMP Version** drop-down list, this option is available. Options to choose from are **None**, **Password**, and **Key**.
Auth-Protocol by Password	When selecting **v3** in the **SNMP Version** drop-down list, and selecting **Password** in the SNMP V3 Encryption drop-down list, this option is available. Select the authentication level. Options to choose from are: • **MD5** - Select to use the HMAC-MD5-96 authentication level. This field will require the user to enter a password or key. • **SHA** - Specify that the HMAC-SHA authentication protocol will be used. This field will require the user to enter a password or key.
Password	Enter the **Auth-Protocol** password here. For **MD5** this password must be between 8 and 16 characters long. For **SHA** this password must be between 8 and 20 characters long.
Priv-Protocol by Password	When selecting **v3** in the **SNMP Version** drop-down list, and selecting **Password** in the SNMP V3 Encryption drop-down list, this option is available. Select the private protocol. Options to choose from are: • **None** - Specify that no authorization protocol is in use. • **DES56** - Specify that DES 56-bit encryption is in use, based on the CBC-DES (DES-56) standard. This field will require the user to enter a password or a key.
Password	Enter the **Priv-Protocol** password here. For **none**, this field will be disabled. For **DES56** the password must be between 8 and 16 characters long.
Auth-Protocol by Key	When selecting **v3** in the **SNMP Version** drop-down list, and selecting **Key** in the SNMP V3 Encryption drop-down list, this option is available. Select the authentication level. Options to choose from are: • **MD5** - Select to use the HMAC-MD5-96 authentication level. This field will require the user to enter a password or a key. • **SHA** - Specify that the HMAC-SHA authentication protocol will be used. This field will require the user to enter a password or a key.
Key	Enter the **Auth-Protocol** key here. For **MD5** this key must be 32 characters long. For **SHA** this key must be 40 characters long.
Priv-Protocol by Key	When selecting **v3** in the **SNMP Version** drop-down list, and selecting **Key** in the SNMP V3 Encryption drop-down list, this option is available. Select the private protocol. Options to choose from are: • **None** - Specify that no authorization protocol is in use. • **DES56** - Specify that DES 56-bit encryption is in use, based on the CBC-DES (DES-56) standard. This field will require the user to enter a password or a key.
Key	Enter the **Priv-Protocol** key here. For **none**, this field will be disabled. For **DES56** the key must be 32 characters long.
IP Access-List Name	Enter the standard IP access control list (ACL) to associate with the user.

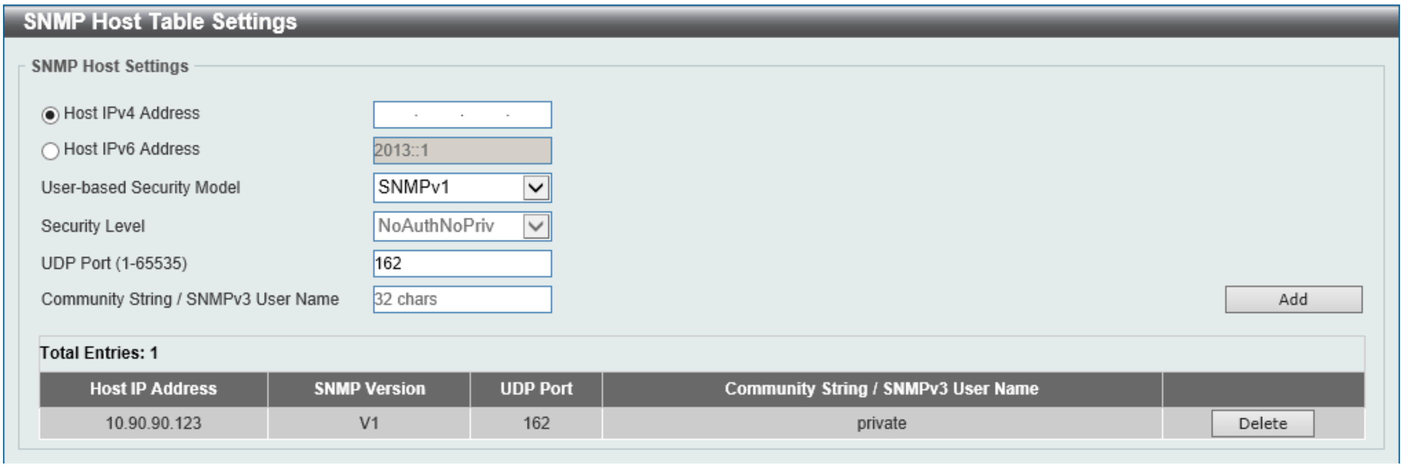
Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove the specified entry.

SNMP Host Table Settings

This window is used to display and configure the recipient of the SNMP notification.

To view the following window, click **Management > SNMP > SNMP Host Table Settings**, as shown below:



SNMP Host Table Settings

SNMP Host Settings

● Host IPv4 Address	. . .
○ Host IPv6 Address	2013::1
User-based Security Model	SNMPv1
Security Level	NoAuthNoPriv
UDP Port (1-65535)	162
Community String / SNMPv3 User Name	32 chars

Total Entries: 1

Host IP Address	SNMP Version	UDP Port	Community String / SNMPv3 User Name	
10.90.90.123	V1	162	private	Delete

Figure 4-12 SNMP Host Table Settings Window

The fields that can be configured are described below:

Parameter	Description
Host IPv4 Address	Enter the IPv4 address of the SNMP notification host.
Host IPv6 Address	Enter the IPv6 address of the SNMP notification host.
User-based Security Model	Select the security model here. Options to choose from are: • **SNMPv1** - Select to allow the group user to use the SNMPv1 security model. • **SNMPv2c** - Select to allow the group user to use the SNMPv2c security model. • **SNMPv3** - Select to allow the group user to use the SNMPv3 security model.
Security Level	When selecting **SNMPv3** in the **User-based Security Model** drop-down list, this option is available. • **NoAuthNoPriv** - Specify that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. • **AuthNoPriv** - Specify that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. • **AuthPriv** - Specify that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.
UDP Port	Enter the UDP port number. The default trap UDP port number is 162. The range of UDP port numbers is from 1 to 65535. Some port numbers may conflict with other protocols.
Community String / SNMPv3 User Name	Enter the community string or SNMPv3 user name to be sent with the notification packet.

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

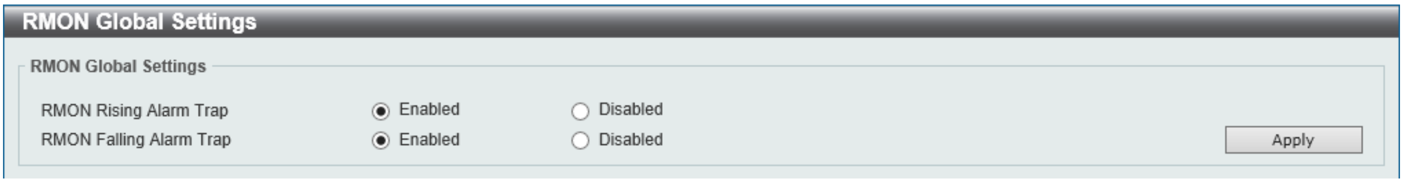
Click the **Delete** button to remove the specified entry.

RMON

RMON Global Settings

This window is used to enable or disable remote monitoring (RMON) for the rising and falling alarm trap feature for the SNMP function on the Switch.

To view the following window, click **Management > RMON > RMON Global Settings**, as shown below:



RMON Global Settings

RMON Global Settings

RMON Rising Alarm Trap	● Enabled	○ Disabled
RMON Falling Alarm Trap	● Enabled	○ Disabled

Figure 4-13 RMON Global Settings Window

The fields that can be configured are described below:

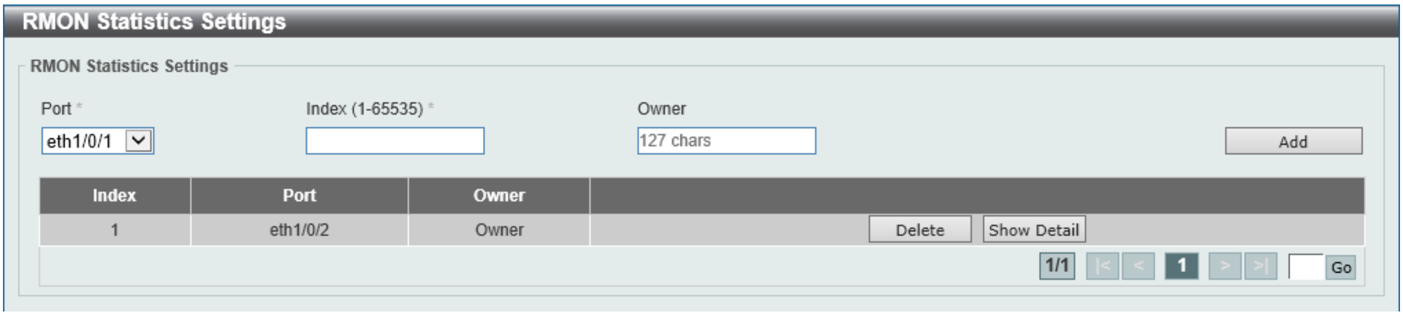
Parameter	Description
RMON Rising Alarm Trap	Select this option to enable or disable the RMON Rising Alarm Trap Feature.
RMON Falling Alarm Trap	Select this option to enable or disable the RMON Falling Alarm Trap Feature.

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

RMON Statistics Settings

This window is used to display and configure the RMON statistics on the specified port.

To view the following window, click **Management > RMON > RMON Statistics Settings**, as shown below:



RMON Statistics Settings

RMON Statistics Settings

Port * eth1/0/1

Index (1-65535) *

Owner 127 chars

Index	Port	Owner
1	eth1/0/2	Owner

Figure 4-14 RMON Statistics Settings Window

The fields that can be configured are described below:

Parameter	Description
Port	Select to choose the port.
Index	Enter the RMON table index. The value is from 1 to 65535.
Owner	Enter the owner string. The string can be up to 127 characters.

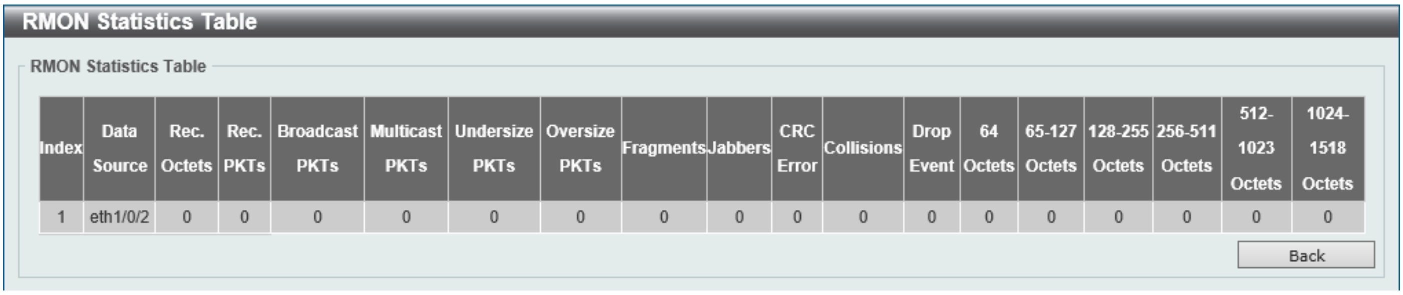
Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove the specified entry.

Click the **Show Detail** button to see the detail information of the specific port.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Show Detail** button, the following window will appear.



RMON Statistics Table

RMON Statistics Table

Index	Data Source	Rec. Octets	Rec. PKTs	Broadcast PKTs	Multicast PKTs	Undersize PKTs	Oversize PKTs	Fragments	Jabbers	CRC Error	Collisions	Drop Event	64 Octets	65-127 Octets	128-255 Octets	256-511 Octets	512-1023 Octets	1024-1518 Octets
1	eth1/0/2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

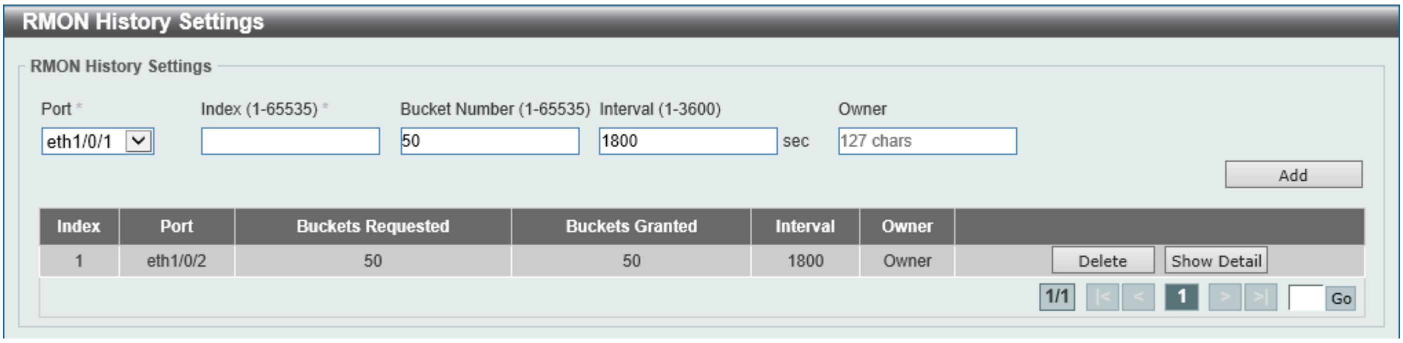
Figure 4-15 RMON Statistics Settings (Show Detail) Window

Click the **Back** button to return to the previous window.

RMON History Settings

This window is used to display and configure RMON MIB history statistics gathered on the specified port.

To view the following window, click **Management > RMON > RMON History Settings**, as shown below:



RMON History Settings

RMON History Settings

Port *: eth1/0/1

Index (1-65535) *:

Bucket Number (1-65535): 50

Interval (1-3600): 1800 sec

Owner: 127 chars

Index	Port	Buckets Requested	Buckets Granted	Interval	Owner	
1	eth1/0/2	50	50	1800	Owner	Delete Show Detail

Figure 4-16 RMON History Settings Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the port that will be used here.
Index	Enter the history group table index. The value is from 1 to 65535.
Bucket Number	Enter the number of buckets specified for the RMON collection history group of statistics. The range is from 1 to 65535. The default value is 50.
Interval	Enter the time in seconds in each polling cycle. The range is from 1 to 3600.
Owner	Enter the owner string. The string can be up to 127 characters.

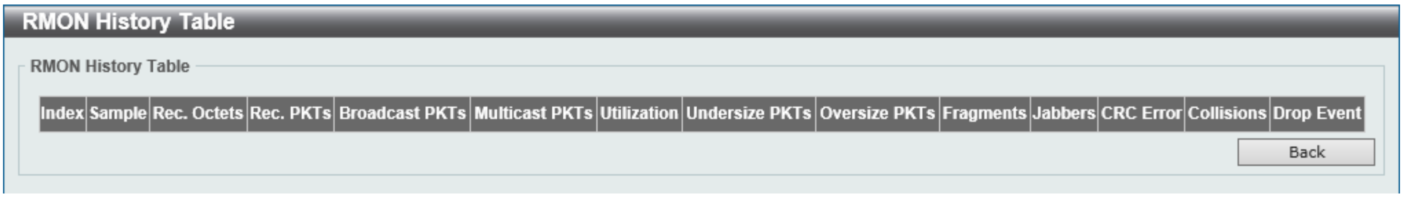
Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove the specified entry.

Click the **Show Detail** button to see the detail information of the specific port.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Show Detail** button, the following window will appear.



RMON History Table

RMON History Table

Index	Sample	Rec. Octets	Rec. PKTs	Broadcast PKTs	Multicast PKTs	Utilization	Undersize PKTs	Oversize PKTs	Fragments	Jabbers	CRC Error	Collisions	Drop Event

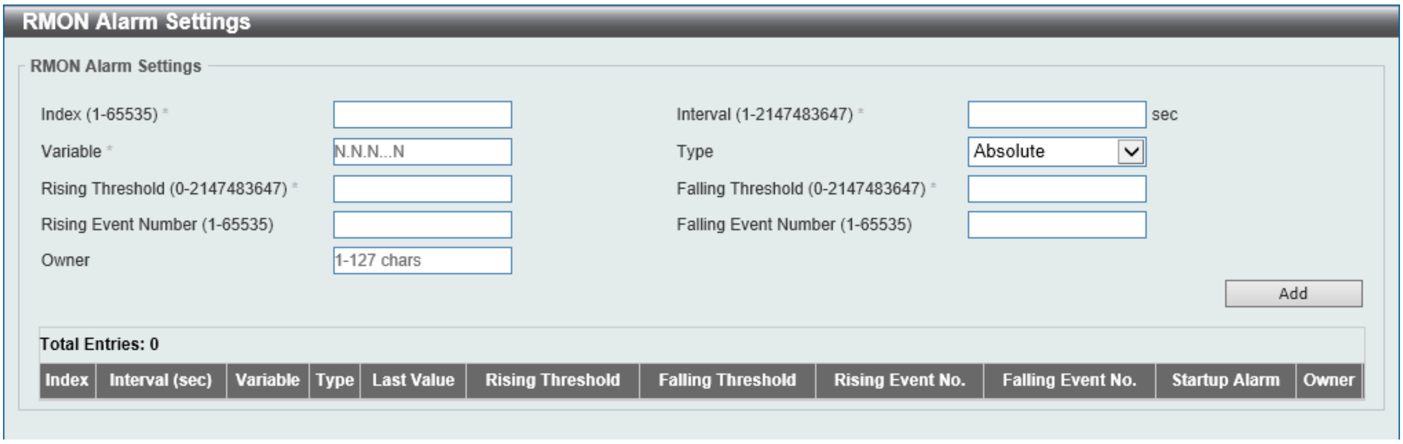
Figure 4-17 RMON History Settings (Show Detail) Window

Click the **Back** button to return to the previous window.

RMON Alarm Settings

This window is used to display and configure alarm entries to monitor an interface.

To view the following window, click **Management > RMON > RMON Alarm Settings**, as shown below:



RMON Alarm Settings

RMON Alarm Settings

Index (1-65535) *		Interval (1-2147483647) *	sec
Variable *	N.N.N...N	Type	Absolute
Rising Threshold (0-2147483647) *		Falling Threshold (0-2147483647) *	
Rising Event Number (1-65535)		Falling Event Number (1-65535)	
Owner	1-127 chars		

Total Entries: 0

Index	Interval (sec)	Variable	Type	Last Value	Rising Threshold	Falling Threshold	Rising Event No.	Falling Event No.	Startup Alarm	Owner

Figure 4-18 RMON Alarm Settings Window

The fields that can be configured are described below:

Parameter	Description
Index	Enter the alarm index. The range is from 1 to 65535.
Interval	Enter the interval in seconds for the sampling of the variable and checking against the threshold. The valid range is from 1 to 2147483648 seconds.
Variable	Enter the object identifier of the variable to be sampled.
Type	Select the monitoring type. Options to choose from are **Absolute** and **Delta**.
Rising Threshold	Enter the rising threshold value between 0 and 2147483647.
Falling Threshold	Enter the falling threshold value between 0 and 2147483647.
Rising Event Number	Enter the index of the event entry that is used to notify the rising threshold crossing event. The valid range is from 1 to 65535. If not specified, no action is taken while crossing the ringing threshold.
Falling Event Number	Enter the index of the event entry that is used to notify the falling threshold crossing event. The valid range is from 1 to 65535. If not specified, no action is taken while crossing the falling threshold.
Owner	Enter the owner string up to 127 characters.

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

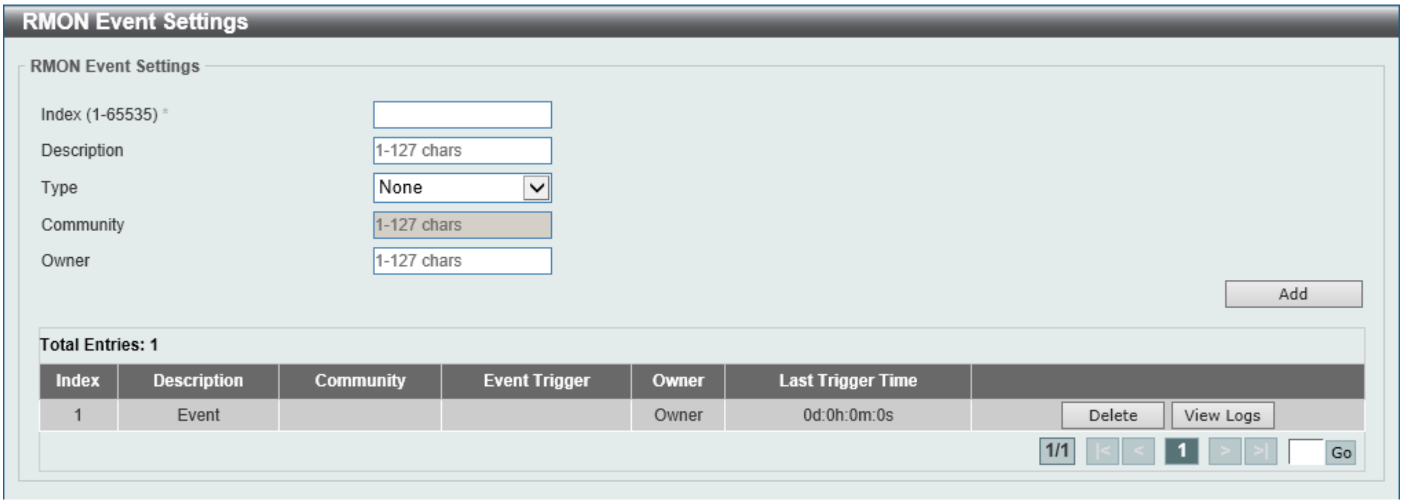
Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

RMON Event Settings

This window is used to display and configure event entries.

To view the following window, click **Management > RMON > RMON Event Settings**, as shown below:



RMON Event Settings

RMON Event Settings

Index (1-65535) *
Description: 1-127 chars
Type: None
Community: 1-127 chars
Owner: 1-127 chars

Total Entries: 1

Index	Description	Community	Event Trigger	Owner	Last Trigger Time	
1	Event			Owner	0d:0h:0m:0s	Delete View Logs

Figure 4-19 RMON Event Settings Window

The fields that can be configured are described below:

Parameter	Description
Index	Enter the index value of the alarm entry here. The range is from 1 to 65535.
Description	Enter a description for the RMON event entry. The string is up to 127 characters long.
Type	Select the RMON event entry type. Options to choose from are **None**, **Log**, **Trap**, and **Log and Trap**.
Community	Enter the community string. The string can be up to 127 characters.
Owner	Enter the owner string. The string can be up to 127 characters.

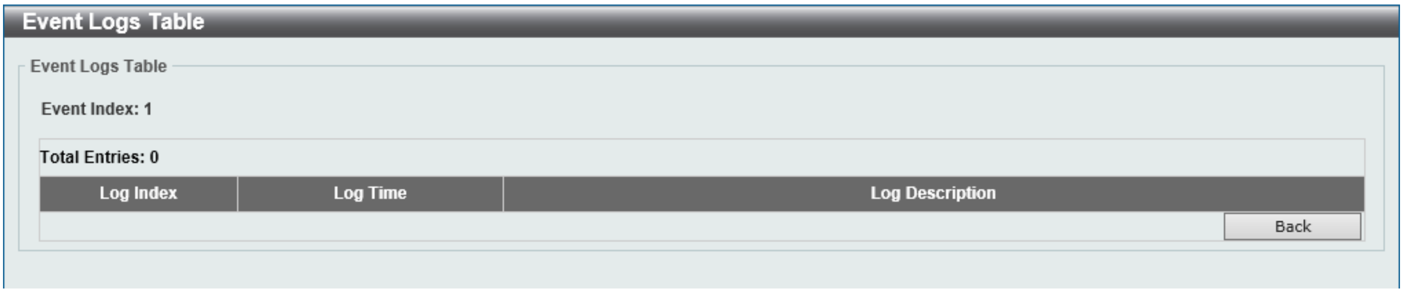
Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove the specified entry.

Click the **View Logs** button to see the detail information of the specific port.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **View Logs** button, the following window will appear.



Event Logs Table

Event Logs Table

Event Index: 1

Total Entries: 0

Log Index	Log Time	Log Description

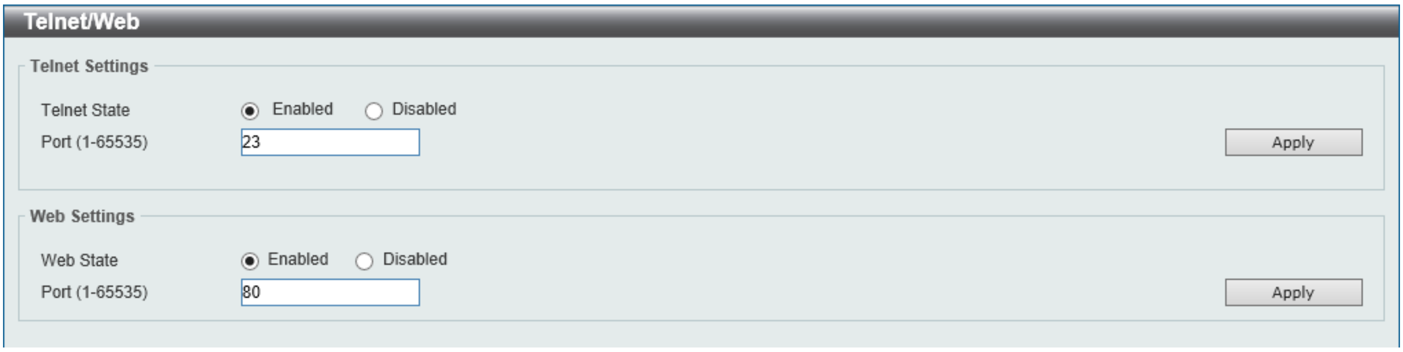
Figure 4-20 RMON Event Settings (View Logs) Window

Click the **Back** button to return to the previous window.

Telnet/Web

This window is used to display and configure Telnet and Web settings on the Switch.

To view the following window, click **Management > Telnet/Web**, as shown below:



Telnet/Web

Telnet Settings

Telnet State ● Enabled ○ Disabled

Port (1-65535) 23

Apply

Web Settings

Web State ● Enabled ○ Disabled

Port (1-65535) 80

Apply

Figure 4-21 Telnet/Web Window

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

Parameter	Description
Telnet State	Select to enable or disable the Telnet server feature here.
Port	Enter the TCP port number used for Telnet management of the Switch. The well-known TCP port for the Telnet protocol is 23. The range is from 1 to 65535.

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

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

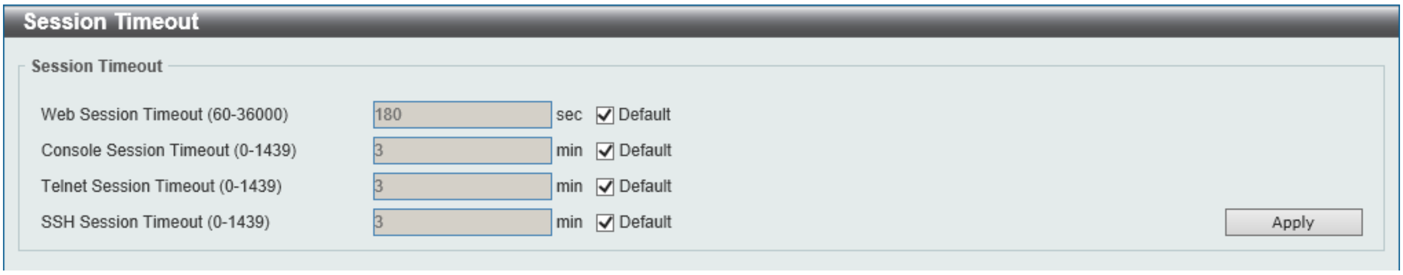
Parameter	Description
Web State	Select this option to enable or disable the configuration through the web.
Port	Enter the TCP port number used for Web management of the Switch. The well-known TCP port for the Web protocol is 80. The range is from 1 to 65535.

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

Session Timeout

This window is used to display and configure the session timeout settings. The outgoing session timeout values are used for Console/Telnet/SSH connections through the CLI of the Switch to the Telnet interface of another switch.

To view the following window, click **Management > Session Timeout**, as shown below:



Session Timeout

Session Timeout

Web Session Timeout (60-36000) 180 sec ☑ Default

Console Session Timeout (0-1439) 3 min ☑ Default

Telnet Session Timeout (0-1439) 3 min ☑ Default

SSH Session Timeout (0-1439) 3 min ☑ Default

Apply

Figure 4-22 Session Timeout Window

The fields that can be configured are described below:

Parameter	Description
Web Session Timeout	Enter the web session timeout value here. The range is from 60 to 36000 seconds. The default value is 180 seconds. Select the **Default** option to use the default value.
Console Session Timeout	Enter the console session timeout value here. The range is from 0 to 1439 minutes. Enter 0 to disable the timeout. The default value is 3 minutes. Select the **Default** option to use the default value.
Telnet Session Timeout	Enter the Telnet session timeout value here. The range is from 0 to 1439 minutes. Enter 0 to disable the timeout. The default value is 3 minutes. Select the **Default** option to use the default value.
SSH Session Timeout	Enter the SSH session timeout value here. The range is from 0 to 1439 minutes. Enter 0 to disable the timeout. The default value is 3 minutes. Select the **Default** option to use the default value.

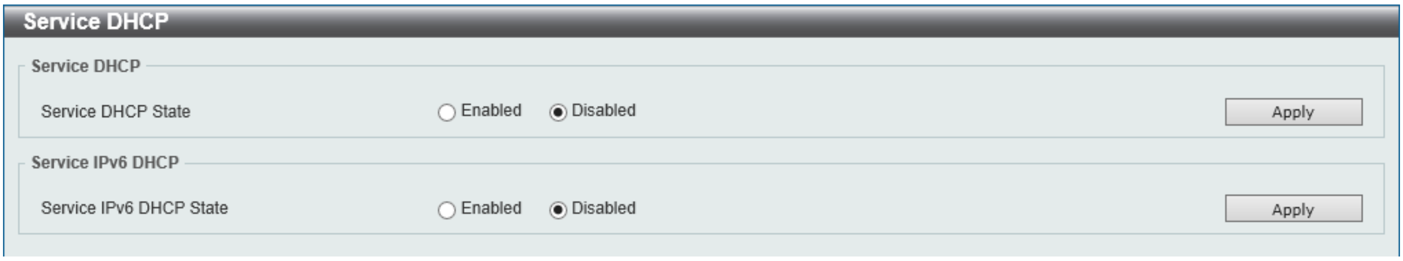
Click the **Apply** button to accept the changes made.

DHCP

Service DHCP

This window is used to display and configure the DHCP service on the Switch.

To view the following window, click **Management > DHCP > Service DHCP**, as shown below:



Service DHCP

Service DHCP

Service DHCP State ○ Enabled ● Disabled

Service IPv6 DHCP

Service IPv6 DHCP State ○ Enabled ● Disabled

Figure 4-23 Service DHCP Window

The fields that can be configured in **Service DHCP** are described below:

Parameter	Description
Service DHCP State	Select this option to enable or disable the DHCP service.

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

The fields that can be configured in **Service IPv6 DHCP** are described below:

Parameter	Description
Service IPv6 DHCP State	Select this option to enable or disable the IPv6 DHCP service.

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

DHCP Class Settings

This window is used to display and configure the DHCP class and the DHCP option matching pattern for the DHCP class.

To view the following window, click **Management > DHCP > DHCP Class Settings**, as shown below:

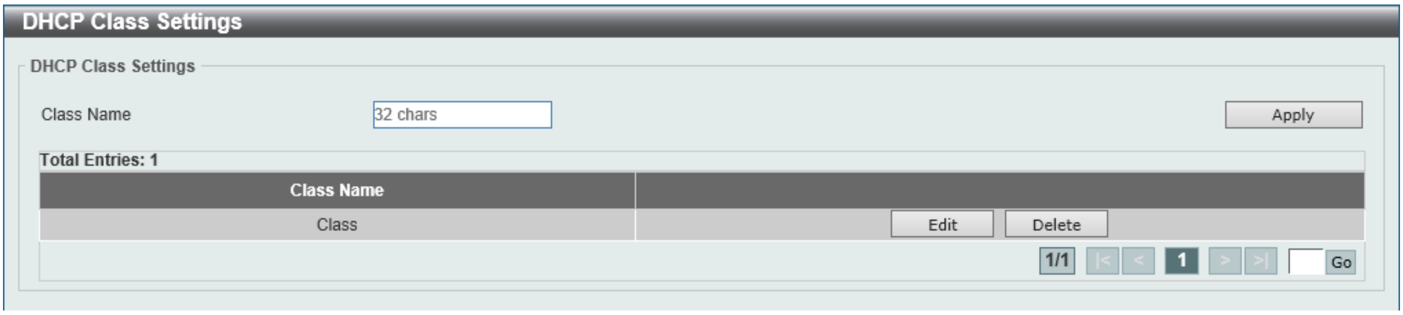


Figure 4-24 DHCP Class Settings Window

The fields that can be configured are described below:

Parameter	Description
Class Name	Enter the DHCP class name with a maximum of 32 characters.

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

Click the **Edit** button to modify the DHCP option matching pattern for the corresponding DCHP class.

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Edit** button, the following window will appear.

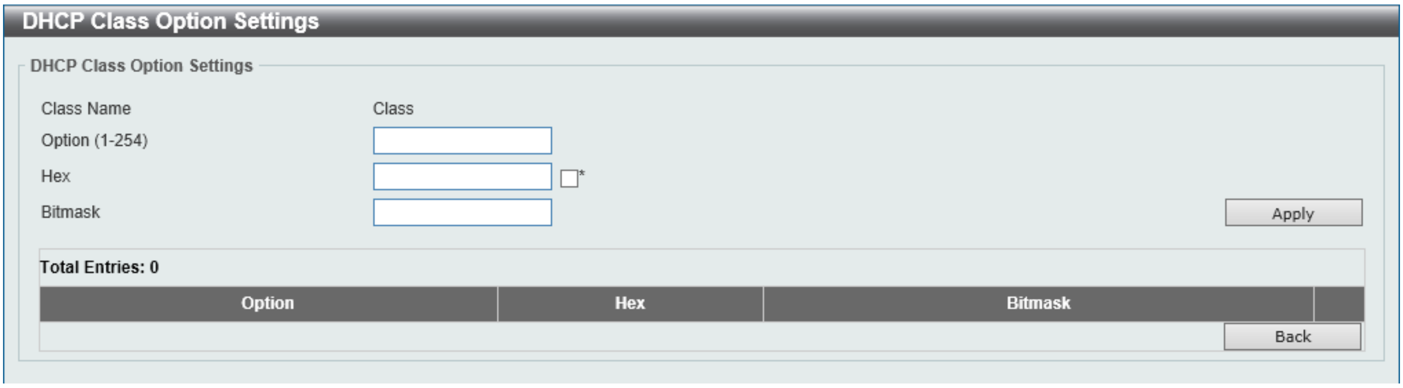


Figure 4-25 DHCP Class Settings (Edit) Window

The fields that can be configured are described below:

Parameter	Description
Option	Enter the DHCP option number. The range is from 1 to 254.
Hex	Enter the hex pattern of the specified DHCP option. Tick the ***** check box not to match the remaining bits of the option.
Bitmask	Enter the hex bit mask for masking of the pattern. The masked pattern bits will be matched. If not specified, all bits entered in the **Hex** field will be checked.

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

Click the **Delete** button to remove the specified entry.

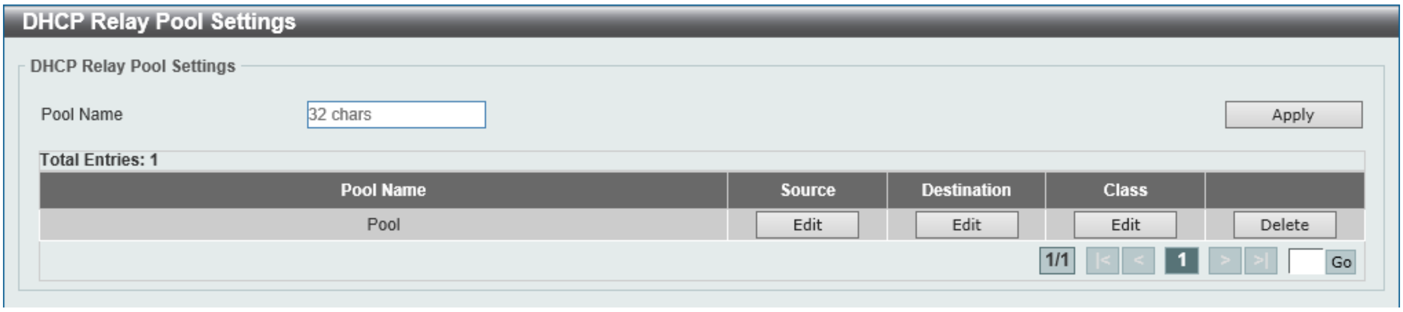
Click the **Back** button to return to the previous window.

DHCP Relay

DHCP Relay Pool Settings

This window is used to display and configure the DHCP relay pool on a DHCP relay agent.

To view the following window, click **Management > DHCP > DHCP Relay > DHCP Relay Pool Settings**, as shown below:



DHCP Relay Pool Settings

DHCP Relay Pool Settings

Pool Name: 32 chars

Total Entries: 1

Pool Name	Source	Destination	Class	
Pool	Edit	Edit	Edit	Delete

Figure 4-26 DHCP Relay Pool Settings Window

The fields that can be configured are described below:

Parameter	Description
Pool Name	Enter the address pool name with a maximum of 32 characters.

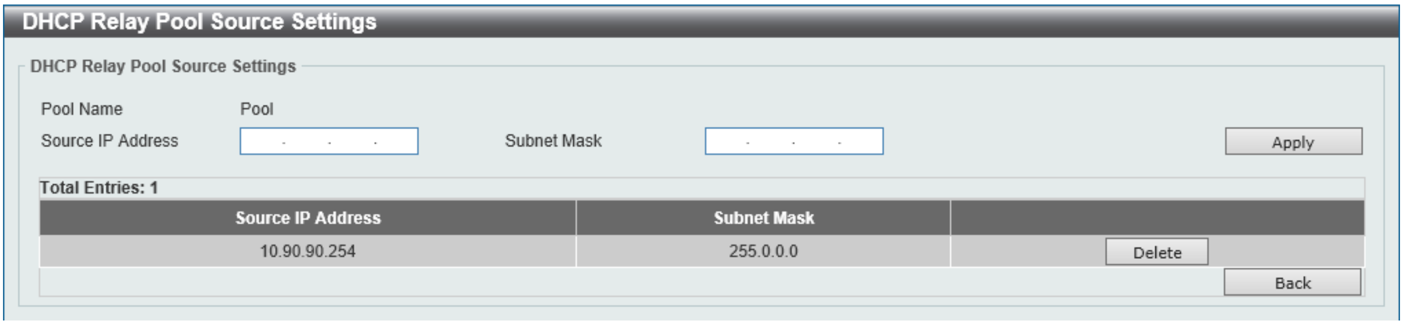
Click the **Apply** button to accept the changes made.

Click the **Edit** button to modify the corresponding information of the specific DHCP pool.

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Edit** button under **Source**, the following window will appear.



DHCP Relay Pool Source Settings

DHCP Relay Pool Source Settings

Pool Name: Pool

Source IP Address: . . .

Subnet Mask: . . .

Total Entries: 1

Source IP Address	Subnet Mask	
10.90.90.254	255.0.0.0	Delete

Figure 4-27 DHCP Relay Pool Source Settings Window

The fields that can be configured are described below:

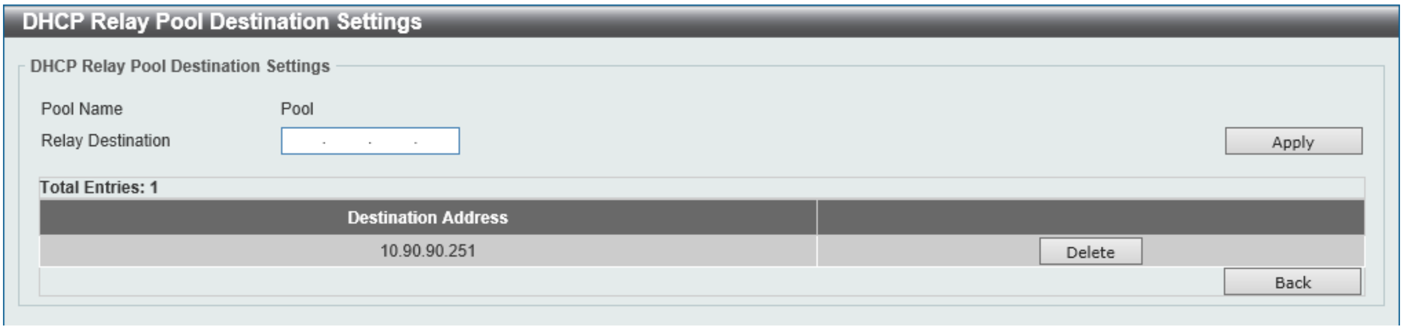
Parameter	Description
Source IP Address	Enter the source subnet of client packets.
Subnet Mask	Enter the network mask of the source subnet.

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

Click the **Delete** button to remove the specified entry.

Click the **Back** button to return to the previous window.

After clicking the **Edit** button under **Destination**, the following window will appear.



DHCP Relay Pool Destination Settings

DHCP Relay Pool Destination Settings

Pool Name: Pool

Relay Destination: . . .

Total Entries: 1

Destination Address	
10.90.90.251	Delete

Figure 4-28 DHCP Relay Pool Destination Settings Window

The fields that can be configured are described below:

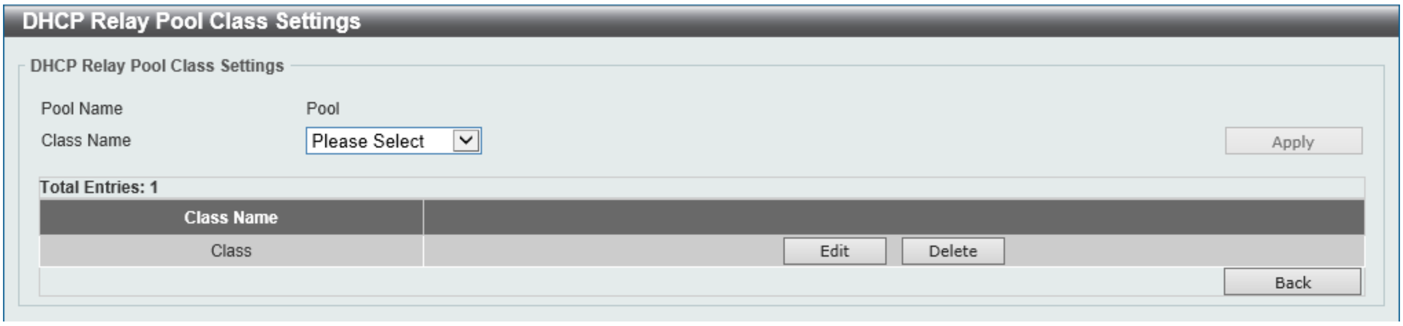
Parameter	Description
Relay Destination	Enter the relay destination DHCP server IP address.

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

Click the **Delete** button to remove the specified entry.

Click the **Back** button to return to the previous window.

After clicking the **Edit** button under **Class**, the following window will appear.



DHCP Relay Pool Class Settings

DHCP Relay Pool Class Settings

Pool Name: Pool

Class Name: Please Select

Total Entries: 1

Class Name	
Class	Edit Delete

Figure 4-29 DHCP Relay Pool Class Settings Window

The fields that can be configured are described below:

Parameter	Description
Class Name	Select the DHCP class name.

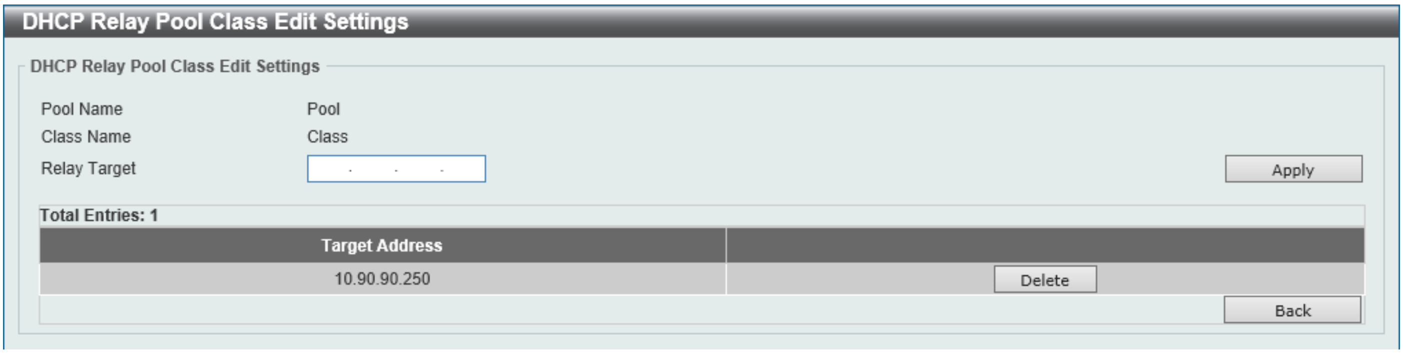
Click the **Apply** button to accept the changes made.

Click the **Edit** button to edit more information.

Click the **Delete** button to remove the specified entry.

Click the **Back** button to return to the previous window.

After clicking the **Edit** button, the following window will appear.



DHCP Relay Pool Class Edit Settings

DHCP Relay Pool Class Edit Settings

Pool Name: Pool
Class Name: Class
Relay Target: . . .

Total Entries: 1

Target Address	
10.90.90.250	Delete

Figure 4-30 DHCP Relay Pool Class Edit Settings Window

The fields that can be configured are described below:

Parameter	Description
Relay Target	Enter the DHCP relay target for relaying packets that matches the value pattern of the option defined in the DHCP class.

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

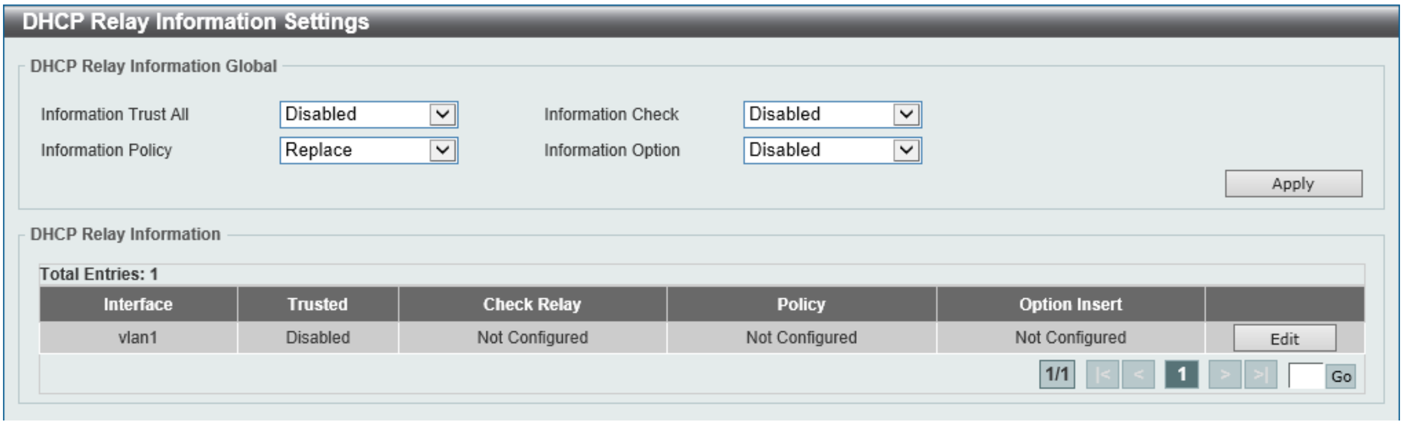
Click the **Delete** button to remove the specified entry.

Click the **Back** button to return to the previous window.

DHCP Relay Information Settings

This window is used to display and configure the DHCP relay information.

To view the following window, click **Management > DHCP > DHCP Relay > DHCP Relay Information Settings**, as shown below:



DHCP Relay Information Settings

DHCP Relay Information Global

Information Trust All: Disabled
Information Check: Disabled
Information Policy: Replace
Information Option: Disabled

DHCP Relay Information

Total Entries: 1

Interface	Trusted	Check Relay	Policy	Option Insert	
vlan1	Disabled	Not Configured	Not Configured	Not Configured	Edit

Figure 4-31 DHCP Relay Information Settings Window

The fields that can be configured are described below:

Parameter	Description
Information Trust All	Select this option to enable or disable the DHCP relay agent to trust the IP DHCP relay information for all interfaces.
Information Check	Select this option to enable or disable the DHCP relay agent to validate and remove the relay agent information option in the received DHCP reply packet.

Parameter	Description
Information Policy	Select the Option 82 re-forwarding policy for the DHCP relay agent. Options to choose from are: • **Keep** - Select to keep the packet that already has the relay option. The packet is left unchanged and directly relayed to the DHCP server. • **Drop** - Select to discard the packet that already has the relay option. • **Replace** - Select to replace the packet that already has the relay option. The packet will be replaced with a new option.
Information Option	Select this option to enable or disable the insertion of relay agent information (Option 82) during the relay of DHCP request packets.

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

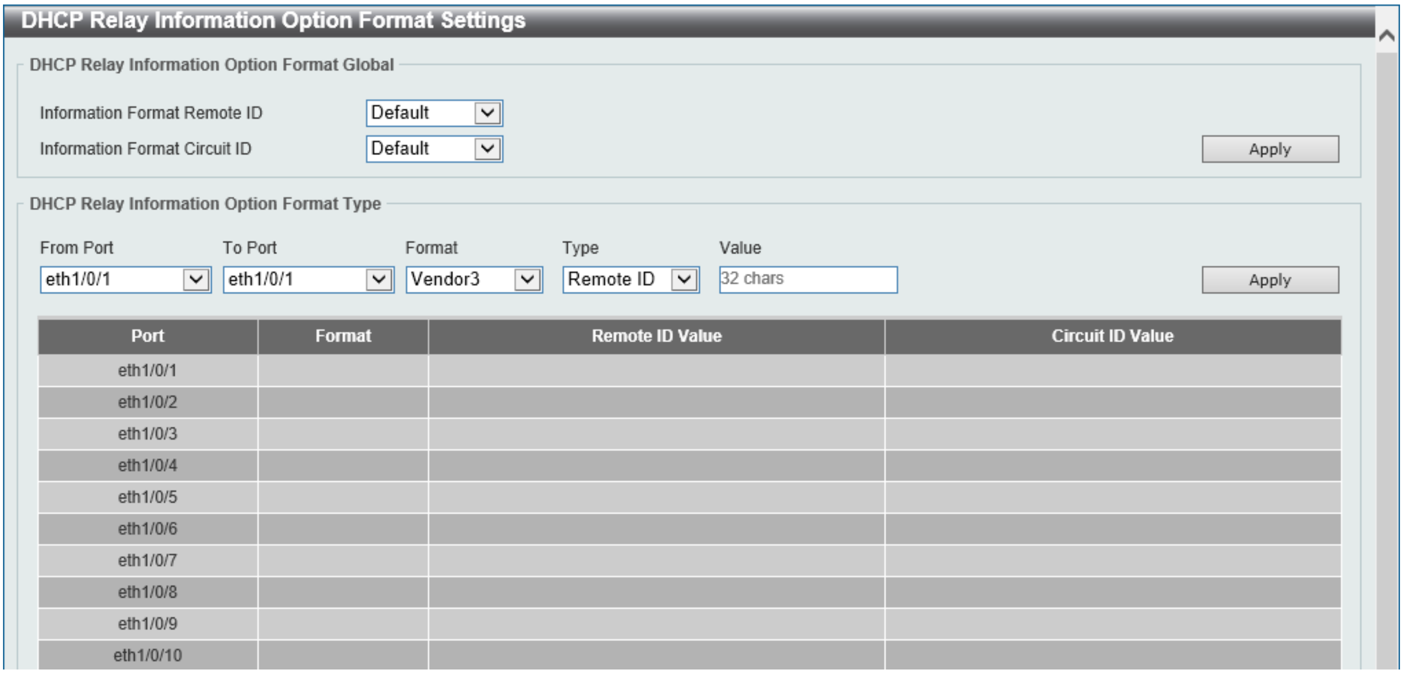
Click the **Edit** button to modify the corresponding interface.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

DHCP Relay Information Option Format Settings

This window is used to display and configure the DHCP information format.

To view the following window, click **Management > DHCP > DHCP Relay > DHCP Relay Information Option Format Settings**, as shown below:



DHCP Relay Information Option Format Settings

DHCP Relay Information Option Format Global

Information Format Remote ID: Default

Information Format Circuit ID: Default

DHCP Relay Information Option Format Type

From Port: eth1/0/1 | To Port: eth1/0/1 | Format: Vendor3 | Type: Remote ID | Value: 32 chars

Port	Format	Remote ID Value	Circuit ID Value
eth1/0/1			
eth1/0/2			
eth1/0/3			
eth1/0/4			
eth1/0/5			
eth1/0/6			
eth1/0/7			
eth1/0/8			
eth1/0/9			
eth1/0/10			

Figure 4-32 DHCP Relay Information Option Format Settings Window

The fields that can be configured in **DHCP Relay Information Option Format Global** are described below:

Parameter	Description
Information Format Remote ID	Select the DHCP information remote ID sub-option. Options to choose from are: • **Default** - Select to use the Switch's system MAC address as the remote ID. • **User Define** - Select to use a user-defined remote ID. Enter the user-defined string with the maximum of 32 characters in the text box. • **Vendor2** - Select to use vendor 2 as the remote ID. • **Vendor3** - Select to use vendor 3 as the remote ID.
Information Format Circuit ID	Select the DHCP information circuit ID sub-option. Options to choose from are: • **Default** - Select to use the default circuit ID sub-option.

Parameter	Description
	• **User Define** - Select to use a user-defined circuit ID. Enter the user-defined string with the maximum of 32 characters in the text box. • **Vendor1** - Select to use vendor 1 as the circuit ID. • **Vendor2** - Select to use vendor 2 as the circuit ID. • **Vendor3** - Select to use vendor 3 as the circuit ID. • **Vendor4** - Select to use vendor 4 as the circuit ID. • **Vendor5** - Select to use vendor 5 as the circuit ID. • **Vendor6** - Select to use vendor 6 as the circuit ID.

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

The fields that can be configured in **DHCP Relay Information Option Format Global** are described below:

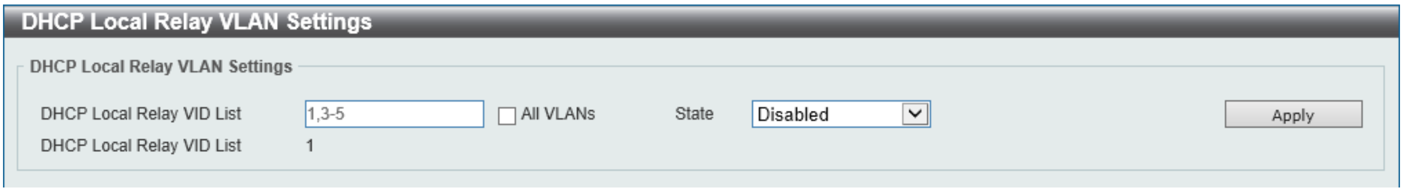
Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
Format	Specifies that the vendor 3 format will be used.
Type	Select to use the **Remote ID** type or **Circuit ID** type here.
Value	Enter the vendor-defined string for Option 82 information in the remote/circuit ID sub-option here. This string can be up to 32 characters long.

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

DHCP Local Relay VLAN Settings

This window is used to display and configure local relay on a VLAN or a group of VLANs.

To view the following window, click **Management > DHCP > DHCP Relay > DHCP Local Relay VLAN Settings**, as shown below:



DHCP Local Relay VLAN Settings

DHCP Local Relay VLAN Settings

DHCP Local Relay VID List: 1,3-5 □ All VLANs State: Disabled

DHCP Local Relay VID List 1

Figure 4-33 DHCP Local Relay VLAN Settings Window

The fields that can be configured are described below:

Parameter	Description
DHCP Local Relay VID List	Enter the VLAN ID for DHCP local relay. Tick the **All VLANs** check box to select all VLANs.
State	Select this option to enable or disable the DHCP local relay on the specific VLAN(s).

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

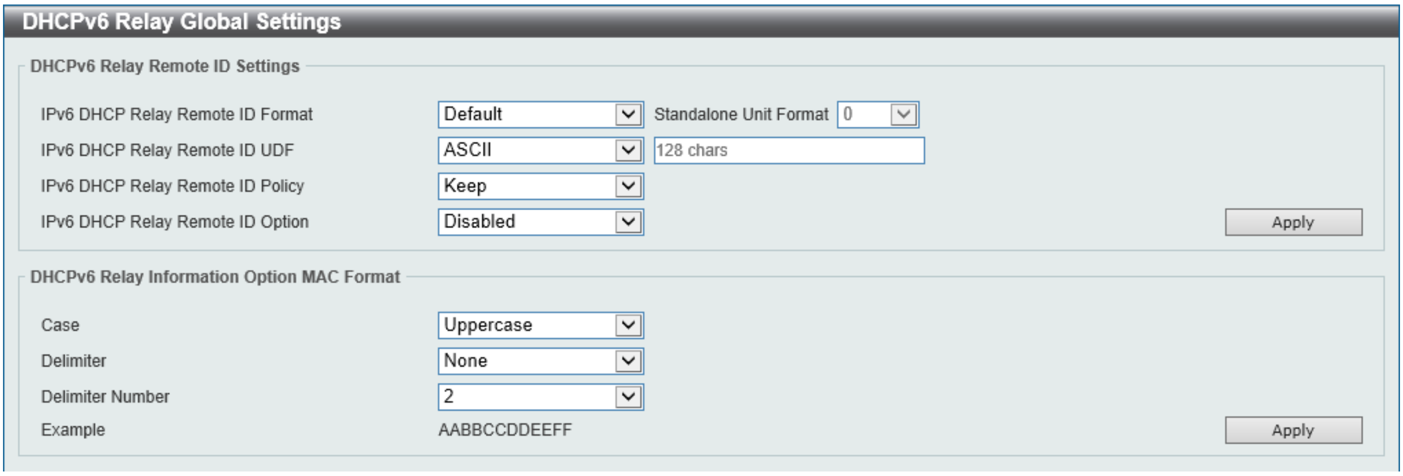
NOTE: When the state of the DHCP relay port is disabled, the port will not relay or locally relay received DHCP packets.

DHCPv6 Relay

DHCPv6 Relay Global Settings

This window is used to display and configure the DHCPv6 Relay remote ID settings.

To view the following window, click **Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Global Settings**, as shown below:



DHCPv6 Relay Global Settings

DHCPv6 Relay Remote ID Settings

IPv6 DHCP Relay Remote ID Format: Default — Standalone Unit Format: 0
IPv6 DHCP Relay Remote ID UDF: ASCII — 128 chars
IPv6 DHCP Relay Remote ID Policy: Keep
IPv6 DHCP Relay Remote ID Option: Disabled

DHCPv6 Relay Information Option MAC Format

Case: Uppercase
Delimiter: None
Delimiter Number: 2
Example: AABBCCDDEEFF

Figure 4-34 DHCPv6 Relay Global Settings Window

The fields that can be configured in **DHCPv6 Relay Remote ID Settings** are described below:

Parameter	Description
IPv6 DHCP Relay Remote ID Format	Select the IPv6 DHCP Relay remote ID format that will be used here. Options to choose from are **Default**, **CID with User Define**, **User Define**, and **Expert UDF**.
Standalone Unit Format	After selecting the **Expert UDF** option, select the standalone unit format here. Options to choose from are **0** and **1**.
IPv6 DHCP Relay Remote ID UDF	Select to choose the User Define Field (UDF) for remote ID. Options to choose from are: • **None** - Select to remove UDF for remote ID. • **ASCII** - Select to enter the ASCII string with a maximum of 128 characters in the text box. • **HEX** - Select to enter the hexadecimal string with a maximum of 256 characters in the text box.
IPv6 DHCP Relay Remote ID Policy	Select to choose Option 37 forwarding policy for the DHCPv6 relay agent. Options to choose from are: • **Keep** - Select that the DHCPv6 request packet that already has the relay agent Remote-ID option is left unchanged and directly relayed to the DHCPv6 server. • **Drop** - Select to discard the packet that already has the relay agent Remote-ID Option 37.
IPv6 DHCP Relay Remote ID Option	Select this option to enable or disable the insertion of the relay agent remote ID Option 37 during the relay of DHCP for IPv6 request packets.

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

The fields that can be configured in **DHCPv6 Relay Information Option MAC Format** are described below:

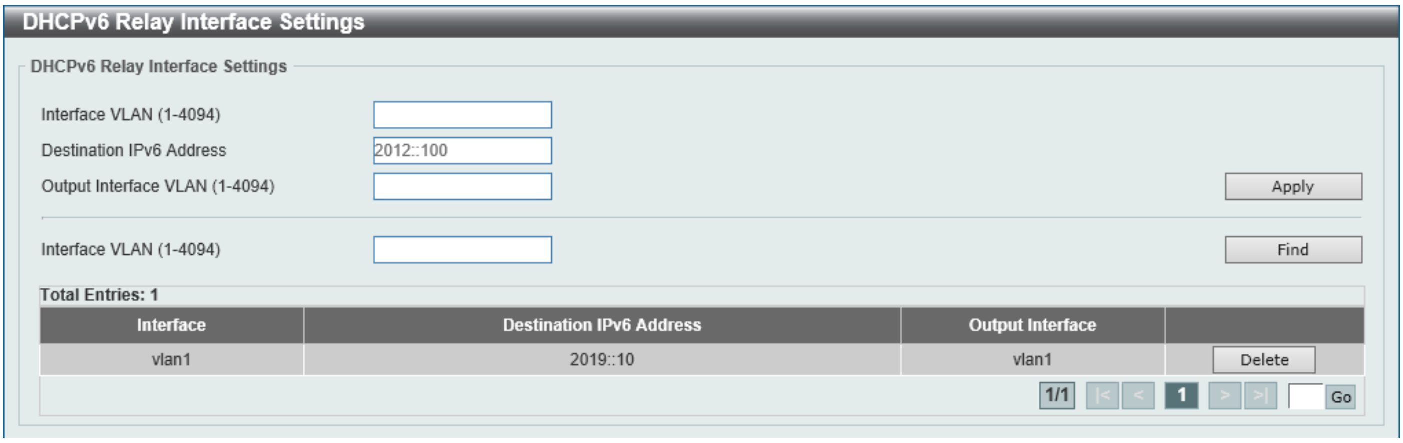
Parameter	Description
Case	Select the case that will be used here. Options to choose from are: • **Lowercase** - Specifies that the MAC format will be lowercase. ○ For example, aa-bb-cc-dd-ee-ff. • **Uppercase** - Specifies that the MAC format will be uppercase. ○ For example, AA-BB-CC-DD-EE-FF.
Delimiter	Select the delimiter that will be used here. Options to choose from are: • **Hyphen** - Specifies that the MAC address format will contain hyphens. For example, AA-BB-CC-DD-EE-FF. • **Colon** - Specifies that the MAC address format will contain colons. For example, AA:BB:CC:DD:EE:FF. • **Dot** - Specifies that the MAC address format will contain dots. For example, AA.BB.CC.DD.EE.FF. • **None** - Specifies that the MAC address format will contain no delimiters. For example, AABBCCDDEEFF.
Delimiter Number	Specifies the delimiter number that will be used in the MAC address format here. Options to choose from are: • **1 -** Specifies to use a single delimiter. For example, AABBCC.DDEEFF. • **2 -** Specifies to use two delimiters. For example, AABB.CCDD.EEFF • **5 -** Specifies to use multiple delimiters. For example, AA.BB.CC.DD.EE.FF

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

DHCPv6 Relay Interface Settings

This window is used to display and configure the DHCPv6 relay interface settings.

To view the following window, click **Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Interface Settings**, as shown below:



DHCPv6 Relay Interface Settings

DHCPv6 Relay Interface Settings

Interface VLAN (1-4094)

Destination IPv6 Address: 2012::100

Output Interface VLAN (1-4094)

Interface VLAN (1-4094)

Total Entries: 1

Interface	Destination IPv6 Address	Output Interface	
vlan1	2019::10	vlan1	Delete

Figure 4-35 DHCPv6 Relay Interface Settings Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the interface VLAN ID used in the DHCPv6 relay here. The range is from 1 to 4094.
Destination IPv6 Address	Enter the DHCPv6 relay destination address.
Output Interface VLAN	Enter the output interface VLAN ID for the relay destination here. The range is from 1 to 4094.

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

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

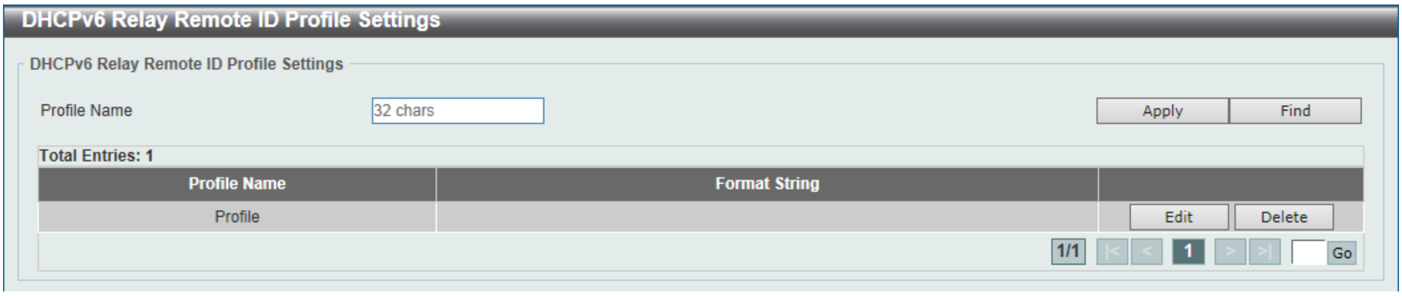
Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

DHCPv6 Relay Remote ID Profile Settings

This window is used to display and configure the DHCPv6 relay remote ID profile settings. This is used to create a new profile for DHCPv6 relay Option 82.

To view the following window, click **Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Remote ID Profile Settings**, as shown below:



DHCPv6 Relay Remote ID Profile Settings

DHCPv6 Relay Remote ID Profile Settings

Profile Name: 32 chars

Total Entries: 1

Profile Name	Format String	
Profile		Edit Delete

Figure 4-36 DHCPv6 Relay Remote ID Profile Settings Window

The fields that can be configured are described below:

Parameter	Description
Profile Name	Enter the profile name here. This string can be up to 32 characters long.
Format String	After clicking the **Edit** button, enter the Option 82 format string here. This string can be up to 251 characters long. The following rules need to be considered: • This string can be a hexadecimal value, an ASCII string, or any combination of hexadecimal values and ASCII characters. An ASCII string needs to be enclosed with quotation marks ("") like "Ethernet". Any ASCII characters outside of the quotation marks will be interpreted as hexadecimal values. • A formatted key string is a string that should be translated before being encapsulated in the packet. A formatted key string can be contained both ASCII strings and hexadecimal values. For example, **"%" +"$"+"1~32"+ "keyword"+":":** ○ **%** - Indicates that the string that follows this character is a formatted key string. ○ **"$"** or **"0"** - (Optional) Indicates a fill indicator. This option specifies how to fill the formatted key string to meet the length option. This option can be either "$" or "0", and cannot be specified as both at the same time. ▪ **"$"** - Indicates to fill the leading space (0x20).

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td></td><td>▪ <b>"0"</b> - Indicates to fill the leading 0. The fill the leading 0 (0) is the default setting.
○ <b>1~32</b> - (Optional) Indicates a length option. This specifies how many characters or bytes the translated key string should occupy. If the actual length of the translated key string is less than the length specified by this option, a fill indicator will be used to fill it. Otherwise, this length option and fill indicator will be ignored and the actual string will be used directly.
○ <b>keyword</b> - Indicates that the keyword will be translated based on the actual value of the system. The following keyword definitions specifies that a command will be refused if an unknown or unsupported keyword is detected:
▪ <b>devtype</b> - The model name of the device. Only an ASCII string is allowed.
▪ <b>sysname</b> - Indicates the System name of the Switch. Only an ASCII string is allowed.
▪ <b>ifdescr</b> - Derived from <i>ifDescr</i> (IF-MIB). Only an ASCII string is allowed.
▪ <b>portmac</b> - Indicates the MAC address of a port. This can be either an ASCII string or a hexadecimal value. When in the format of an ASCII string, the MAC address format can be customized using special CLI commands. When in the format of a hexadecimal value, the MAC address will be encapsulated in order in hexadecimal.
▪ <b>sysmac</b> - Indicates the system MAC address. This can be either an ASCII string or a hexadecimal value. In the ASCII string format, the MAC address format can be customized using special CLI commands. In the hexadecimal format, the MAC address will be encapsulated in order in hexadecimal.
▪ <b>module</b> - Indicates the module ID number. This can be either an ASCII string or a hexadecimal value.
▪ <b>port</b> - Indicates the local port number. This can be either an ASCII string or a hexadecimal value.
▪ <b>svlan</b> - Indicates the outer VLAN ID. This can be either an ASCII string or a hexadecimal value.
▪ <b>cvlan</b> - Indicates the inner VLAN ID. This can be either an ASCII string or a hexadecimal value.
○ <b>:</b> - Indicates the end of the formatted key sting. If a formatted key string is the last parameter of the command, its ending character (":") can be ignored. The space (0x20) between "%" and ":" will be ignored. Other spaces will be encapsulated.
• ASCII strings can be any combination of formatted key strings and 0~9, a~z, A~Z, !@#$%^&*()_+|-=\[]{};:'"/?.,<>`, and space characters. "\" is the escape character. The special character after "\" is the character itself, for example, "\%" is "%" itself, not the start indicator of a formatted key string. Spaces not in the formatted key string will also be encapsulated.
• Hexadecimal values can be any combination of formatted key strings and 0~9, A~F, a~f, and space characters. The formatted key strings only support keywords that support hexadecimal values. Spaces not in the formatted key string will be ignored.</td></tr>
</table>

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

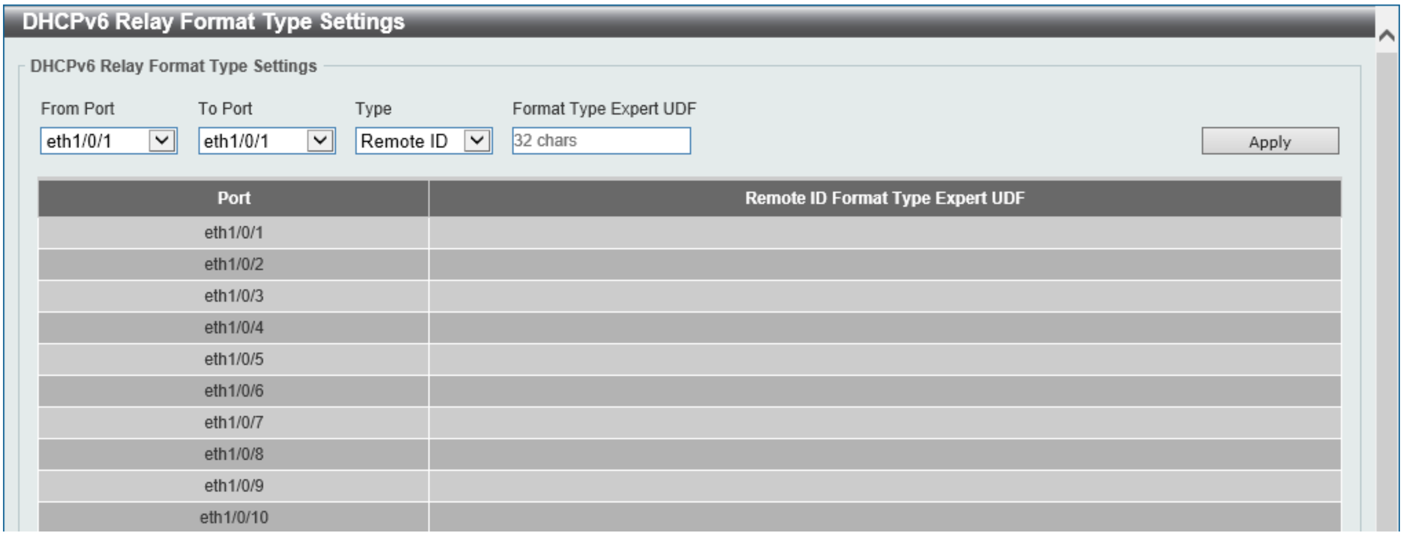
Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

DHCPv6 Relay Format Type Settings

This window is used to display and configure the DHCPv6 relay format type settings. This is used to configure DHCPv6 relay Option 37 and Option 18 of the expert UDF string of each port.

To view the following window, click **Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Format Type Settings**, as shown below:



DHCPv6 Relay Format Type Settings

DHCPv6 Relay Format Type Settings

From Port: eth1/0/1
To Port: eth1/0/1
Type: Remote ID
Format Type Expert UDF: 32 chars

Port	Remote ID Format Type Expert UDF
eth1/0/1	
eth1/0/2	
eth1/0/3	
eth1/0/4	
eth1/0/5	
eth1/0/6	
eth1/0/7	
eth1/0/8	
eth1/0/9	
eth1/0/10	

Figure 4-37 DHCPv6 Relay Format Type Settings Window

The fields that can be configured are described below:

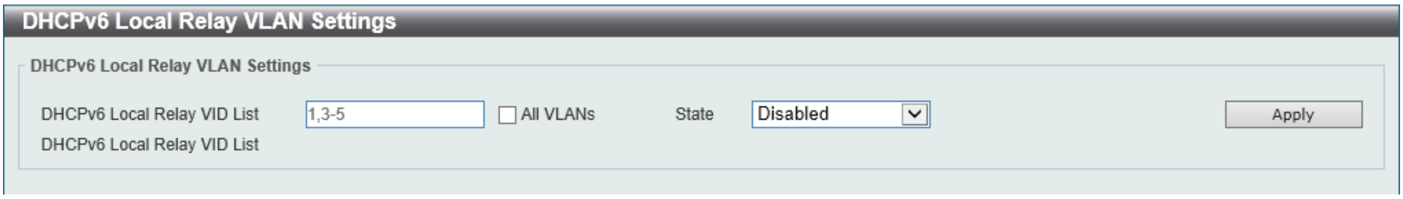
Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
Type	Specifies to configure the Expert UDF format type string for DHCPv6 Option 37.
Format Type Expert UDF	Enter the format type expert UDF string that will be used on the specified port(s) here.

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

DHCPv6 Local Relay VLAN Settings

This window is used to display and configure the DHCPv6 local relay VLAN settings. When DHCPv6 local relay is enabled, it will add Option 37 and Option 18 to the request packets from the client. If the check state of Option 37 is enabled, it will check the request packet from the client and drop the packet if it contains the Option 37 DHCPv6 relay function. If disabled, the local relay function will always add Option 37 to request packets, whether the state of Option 37 is enabled or disabled. The DHCPv6 local relay function will directly forward the packet from the server to the client.

To view the following window, click **Management > DHCP > DHCPv6 Relay > DHCPv6 Local Relay VLAN Settings**, as shown below:



DHCPv6 Local Relay VLAN Settings

DHCPv6 Local Relay VLAN Settings

DHCPv6 Local Relay VID List: 1,3-5 □ All VLANs State: Disabled

DHCPv6 Local Relay VID List

Figure 4-38 DHCPv6 Local Relay VLAN Settings Window

The fields that can be configured are described below:

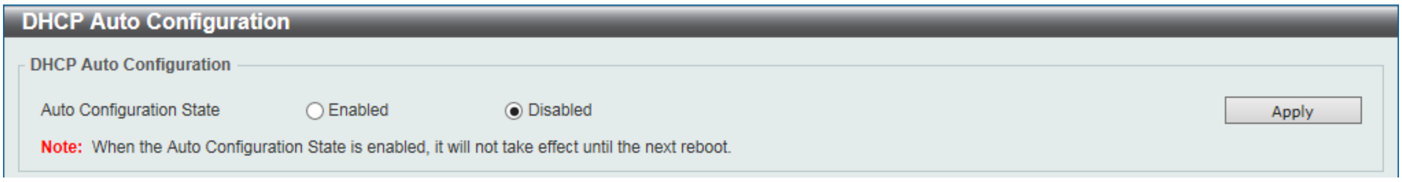
Parameter	Description
DHCPv6 Local Relay VID List	Enter the DHCPv6 local relay VLAN ID(s) here. More than one VLAN ID can be entered here. Select the **All VLANs** option to apply this setting on all configured VLANs on this Switch.
State	Select to enable or disable the DHCPv6 local relay feature on the specified VLAN(s) here.

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

DHCP Auto Configuration

This window is used to display and configure the DHCP auto-configuration function.

To view the following window, click **Management > DHCP Auto Configuration**, as shown below:



DHCP Auto Configuration

DHCP Auto Configuration

Auto Configuration State ○ Enabled ● Disabled

Note: When the Auto Configuration State is enabled, it will not take effect until the next reboot.

Figure 4-39 DHCP Auto Configuration Window

The fields that can be configured are described below:

Parameter	Description
Auto Configuration State	Select this option to enable or disable the auto-configuration function.

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

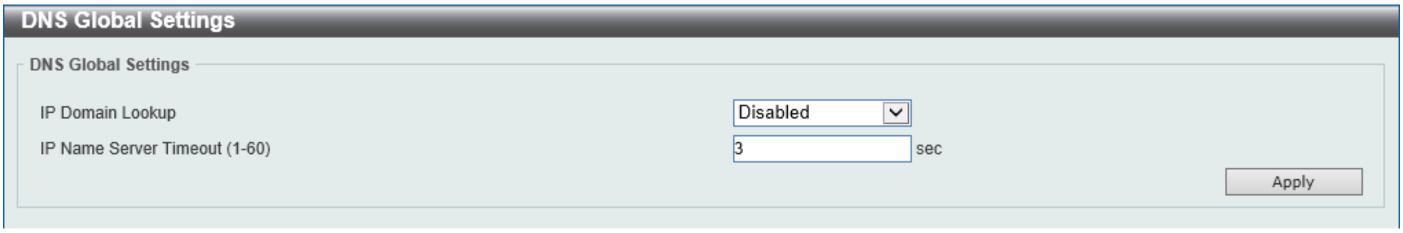
DNS

The Domain Name System (DNS) is used to map human-readable domain names to the IP addresses used by computers to communicate. A DNS server performs name-to-address translation, and may need to contact several name servers to translate a domain to an address. The address of the machine that supplies domain name service is often supplied by a DHCP or BOOTP server, or can be entered manually and configured into the operating system at startup.

DNS Global Settings

This window is used to display and configure the global DNS settings.

To view the following window, click **Management > DNS > DNS Global Settings**, as shown below:



DNS Global Settings

DNS Global Settings

IP Domain Lookup: Disabled

IP Name Server Timeout (1-60): 3 sec

Figure 4-40 DNS Global Settings Window

The fields that can be configured in **DNS Global Settings** are described below:

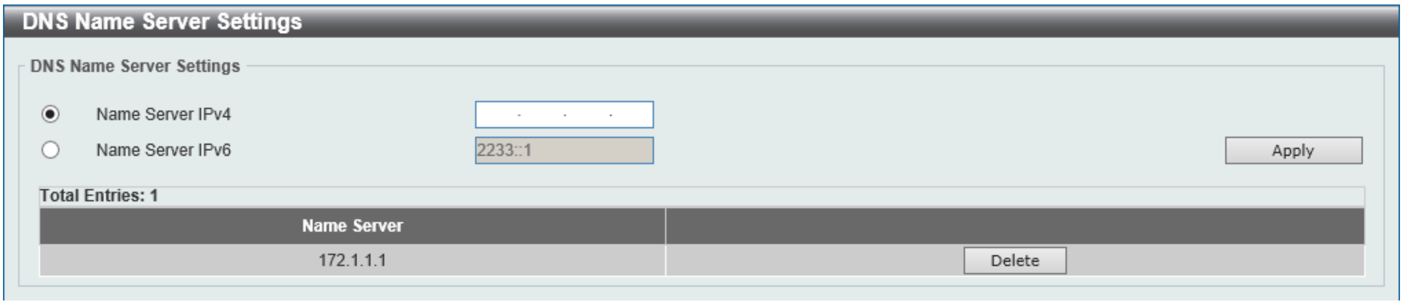
Parameter	Description
IP Domain Lookup	Select to enable or disable the IP domain lookup state here.
IP Name Server Timeout	Enter the maximum time to wait for a response from a specified name server. This value is between 1 and 60 seconds.

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

DNS Name Server Settings

This window is used to display and configure the IP address of a domain name server.

To view the following window, click **Management > DNS > DNS Name Server Settings**, as shown below:



DNS Name Server Settings

DNS Name Server Settings

● Name Server IPv4 . . .

○ Name Server IPv6 2233::1

Total Entries: 1

Name Server	
172.1.1.1	Delete

Figure 4-41 DNS Name Server Settings Window

The fields that can be configured are described below:

Parameter	Description
Name Server IPv4	Select and enter the IPv4 address of the DNS server.
Name Server IPv6	Select and enter the IPv6 address of the DNS server.

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

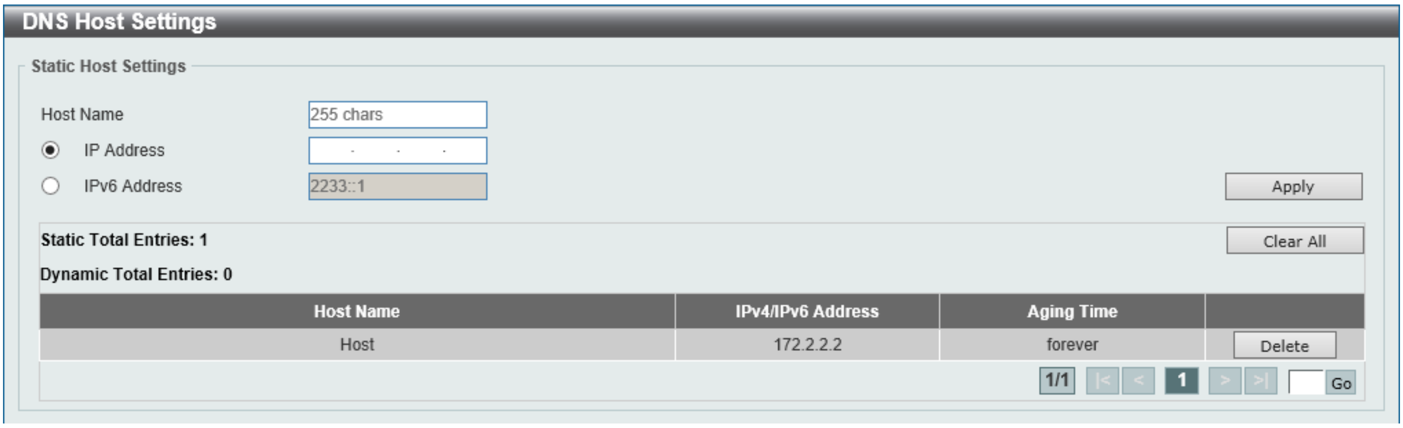
Click the **Find** button to locate a specific entry based on the information entered.

Click the **Delete** button to remove the specified entry.

DNS Host Settings

This window is used to display and configure the static mapping entry for the host name and the IP address in the host table.

To view the following window, click **Management > DNS > DNS Host Settings**, as shown below:



DNS Host Settings

Static Host Settings

Host Name: 255 chars

● IP Address: . . .

○ IPv6 Address: 2233::1

Static Total Entries: 1

Dynamic Total Entries: 0

Host Name	IPv4/IPv6 Address	Aging Time	
Host	172.2.2.2	forever	Delete

Figure 4-42 DNS Host Settings Window

The fields that can be configured are described below:

Parameter	Description
Host Name	Enter the host name of the equipment.
IP Address	Select and enter the IPv4 address of the equipment.
IPv6 Address	Select and enter the IPv6 address of the equipment.

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

Click the **Clear All** button to clear the information entered in all the fields on this page.

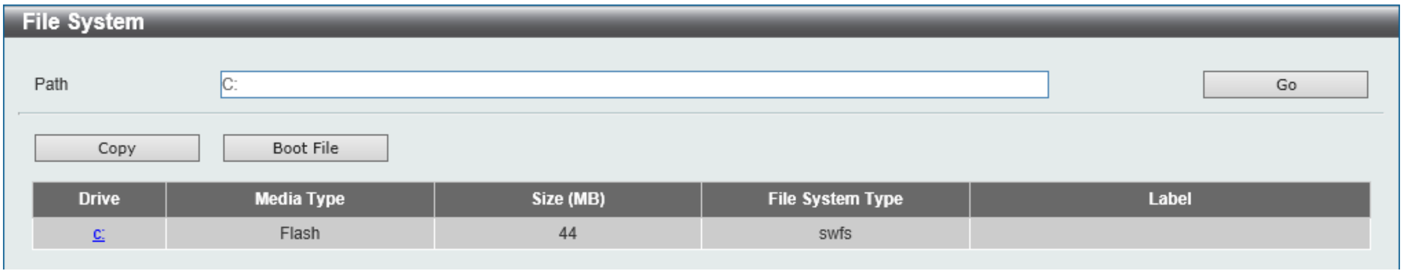
Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

File System

This window is used to view, manage, and configure the Switch file system.

To view the following window, click **Management > File System**, as shown below:



File System

Path: C:

Drive	Media Type	Size (MB)	File System Type	Label
c:	Flash	44	swfs	

Figure 4-43 File System Window

The fields that can be configured are described below:

Parameter	Description
Path	Enter the path string.

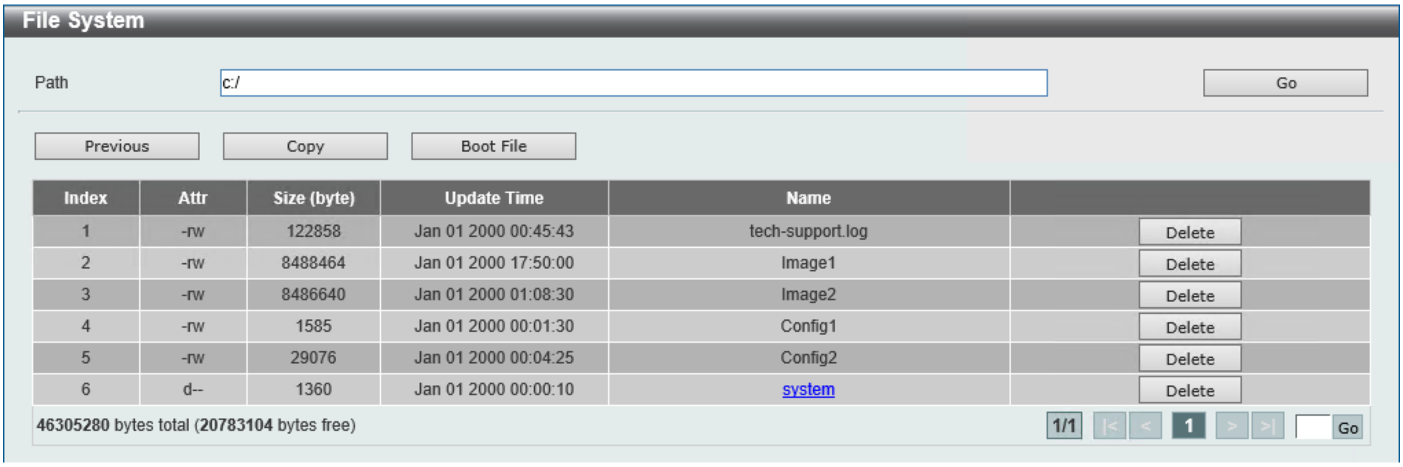
Click the **Go** button to navigate to the path entered.

Click the **Copy** button to copy a specific file to the Switch.

Click the **Boot File** button to configure the bootup image and configuration file settings.

Click the c: hyperlink to navigate the C: drive

After clicking the c: hyperlink, the following window will appear:



File System

Path: c:/

Index	Attr	Size (byte)	Update Time	Name	
1	-rw	122858	Jan 01 2000 00:45:43	tech-support.log	Delete
2	-rw	8488464	Jan 01 2000 17:50:00	Image1	Delete
3	-rw	8486640	Jan 01 2000 01:08:30	Image2	Delete
4	-rw	1585	Jan 01 2000 00:01:30	Config1	Delete
5	-rw	29076	Jan 01 2000 00:04:25	Config2	Delete
6	d--	1360	Jan 01 2000 00:00:10	system	Delete

46305280 bytes total (**20783104** bytes free)

Figure 4-44 File System (Drive) Window

Click the **Go** button to navigate to the path entered.

Click the **Previous** button to return to the previous window.

Click the **Copy** button to copy a specific file to the Switch.

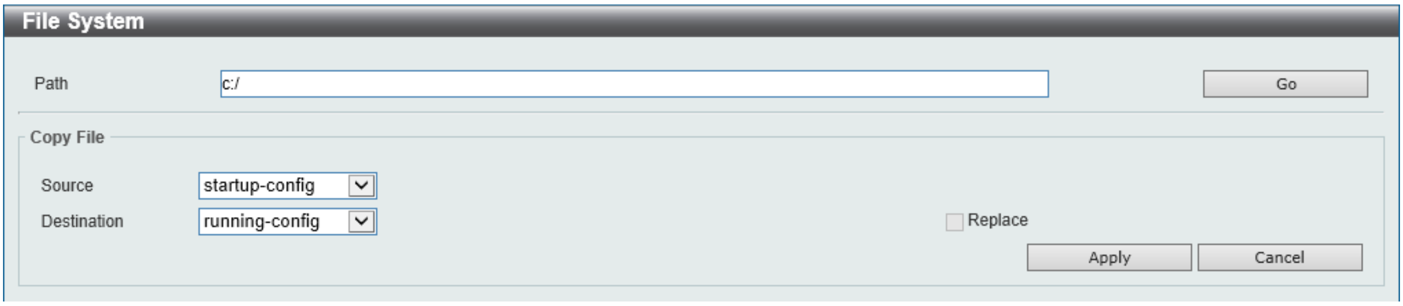
Click the **Boot File** button to configure the bootup image and configuration file settings.

Click the **Delete** button to remove a specific file from the file system.

NOTE: If the boot configuration file is damaged, the Switch will automatically revert back to the default configuration.

NOTE: If the boot image file is damaged, the Switch will automatically use the backup image file in the next boot up.

After clicking the **Copy** button, the following window will appear.



File System

Path: c:/

Copy File

Source: startup-config

Destination: running-config

□ Replace

Figure 4-45 File System (Copy) Window

The fields that can be configured in **Copy File** are described below:

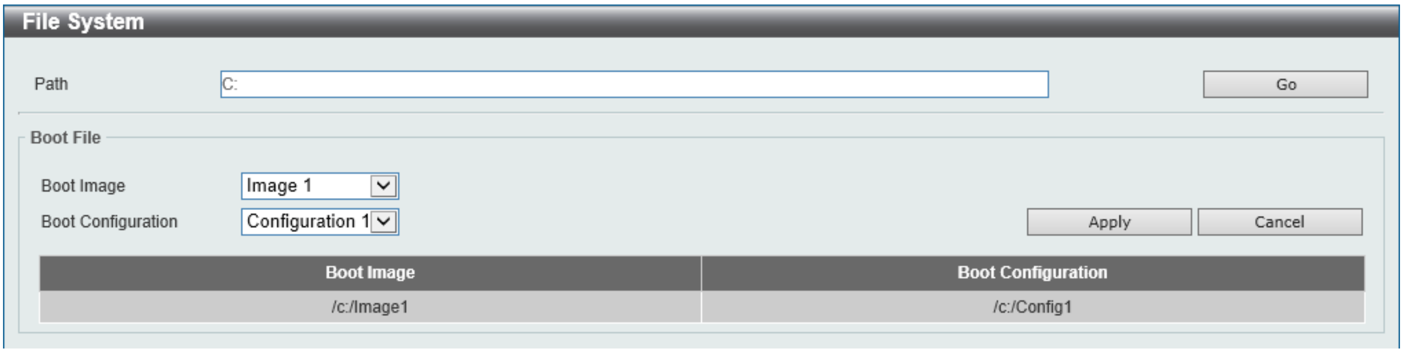
Parameter	Description
Source	Select the source for the copy here. Options to choose from are: • **startup-config** - Specifies to copy the startup configuration as the source. • **Image 1** - Specifies to copy firmware "**Image 1**" as the source.

Parameter	Description
	• **Image 2** - Specifies to copy firmware "**Image 2**" as the source. • **Configuration 1** - Specifies to copy "**Configuration 1**" as the source. • **Configuration 2** - Specifies to copy "**Configuration 2**" as the source.
Destination	Select the destination for the copy here. Options to choose from are: • **running-config** - Specifies to overwrite the running configuration with the source. • **startup-config** - Specifies to overwrite the start-up configuration with the source. • **Image 1** - Specifies to overwrite "**Image 1**" with the source. • **Image 2** - Specifies to overwrite "**Image 2**" with the source. • **Configuration 1** - Specifies to overwrite "**Configuration 1**" with the source. • **Configuration 2** - Specifies to overwrite "**Configuration 2**" with the source.
Replace	Specifies to replace the current running configuration with the indicated configuration file.

Click the **Apply** button to initiate the copy.

Click the **Cancel** button the discard the process.

After clicking the **Boot File** button, the following window will appear.



Path: C:

Boot Image: Image 1

Boot Configuration: Configuration 1

Boot Image	Boot Configuration
/c:/Image1	/c:/Config1

Figure 4-46 File System (Boot File) Window

The fields that can be configured in **Boot File** are described below:

Parameter	Description
Boot Image	Select the boot image here. Options to choose from are **Image 1** and **Image 2**.
Boot Configuration	Select the boot configuration here. Options to choose from are **Configuration 1** and **Configuration 2**.

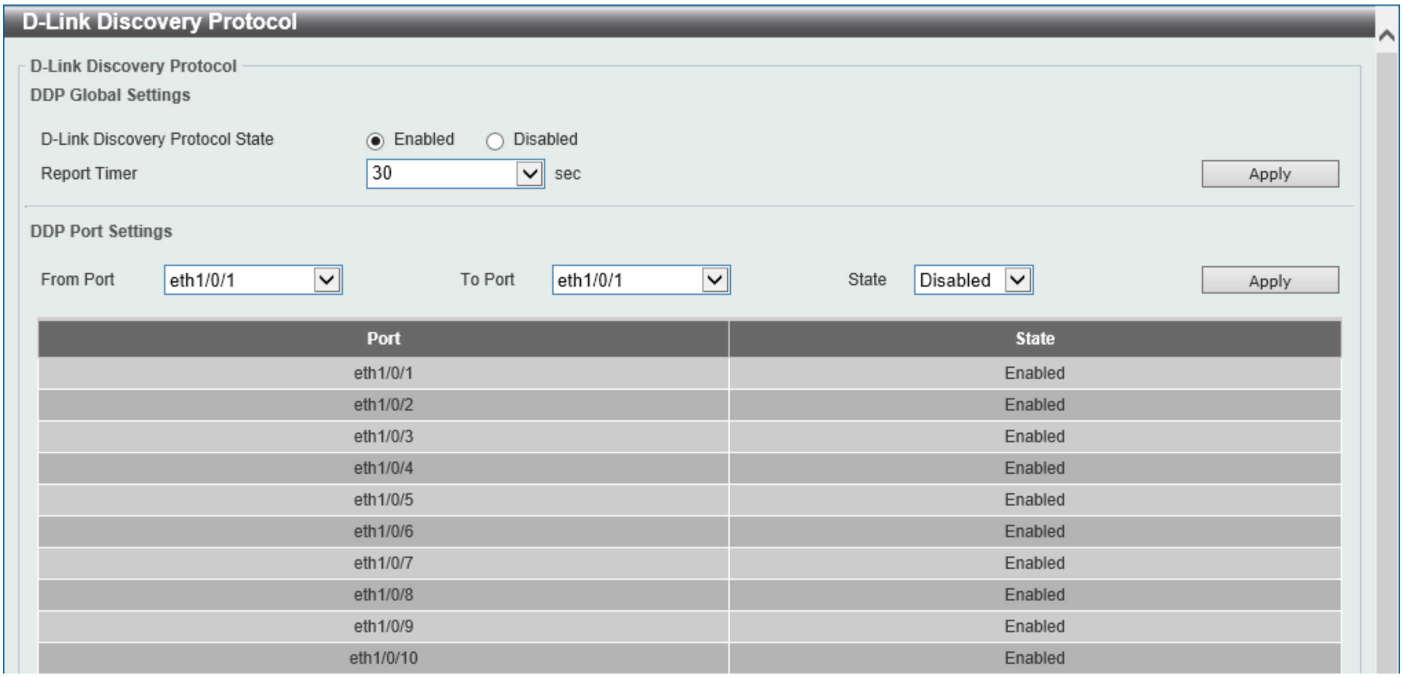
Click the **Apply** button to accept the changes made.

Click the **Cancel** button to discard the changes made.

D-Link Discovery Protocol

This window is used to display and configure the D-Link Discovery Protocol (DDP) settings.

To view the following window, click **Management > D-Link Discovery Protocol**, as shown below:



D-Link Discovery Protocol

D-Link Discovery Protocol

DDP Global Settings

D-Link Discovery Protocol State ● Enabled ○ Disabled

Report Timer 30 sec

DDP Port Settings

From Port eth1/0/1 To Port eth1/0/1 State Disabled

Port	State
eth1/0/1	Enabled
eth1/0/2	Enabled
eth1/0/3	Enabled
eth1/0/4	Enabled
eth1/0/5	Enabled
eth1/0/6	Enabled
eth1/0/7	Enabled
eth1/0/8	Enabled
eth1/0/9	Enabled
eth1/0/10	Enabled

Figure 4-47 D-Link Discovery Protocol Window

The fields that can be configured in **D-Link Discovery Protocol** are described below:

Parameter	Description
D-Link Discovery Protocol State	Select to globally enable or disable the DDP feature here.
Report Timer	Select the report timer value here. This is used to configure interval between two consecutive DDP report messages. Options to choose from are **30**, **60**, **90**, **120** seconds, or **Never**. Selecting **Never** instructs the Switch to stop sending report messages.

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

The fields that can be configured in **DDP Port Settings** are described below:

Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
State	Select to enable or disable the DDP feature on the specified port(s) here.

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

5. Layer 2 Features

FDB
VLAN
STP
Loopback Detection
Link Aggregation
L2 Multicast Control
LLDP

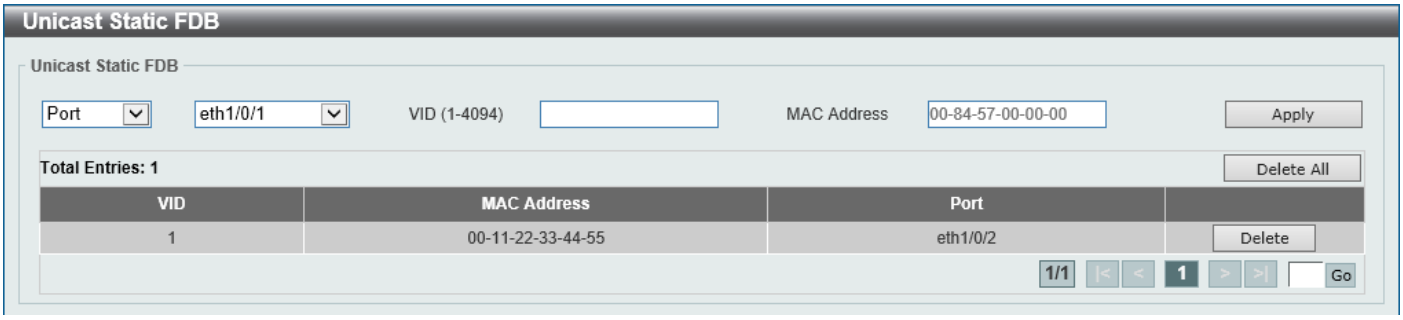
FDB

Static FDB

Unicast Static FDB

This window is used to display and configure the static unicast forwarding settings on the Switch.

To view the following window, click **L2 Features > FDB > Static FDB > Unicast Static FDB**, as shown below:



Unicast Static FDB

Unicast Static FDB

Port | eth1/0/1 | VID (1-4094): | MAC Address: 00-84-57-00-00-00

Total Entries: 1

VID	MAC Address	Port	
1	00-11-22-33-44-55	eth1/0/2	Delete

Figure 5-1 Unicast Static FDB Window

The fields that can be configured are described below:

Parameter	Description
Port/Drop	Allows the selection of the port number on which the MAC address entered resides. This option could also drop the MAC address from the unicast static FDB. Select the port number when selecting the **Port**.
Port Number	After selecting the **Port** option, select the port number used here.
VID	Enter the VLAN ID on which the associated unicast MAC address resides.
MAC Address	Enter the MAC address to which packets will be statically forwarded. This must be a unicast MAC address.

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

Click the **Delete All** button to delete all the entries found in the display table.

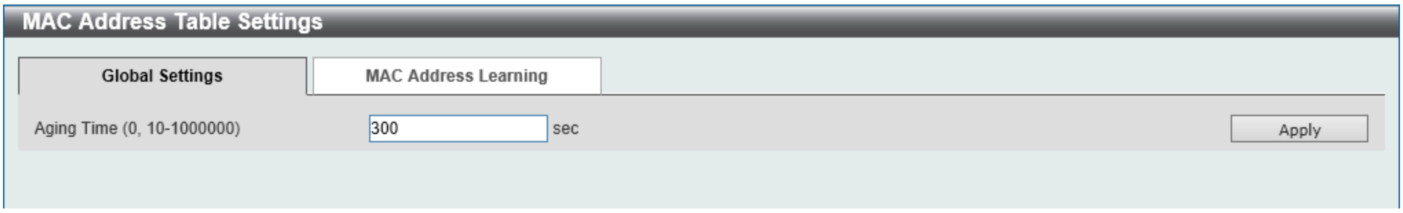
Click the **Delete** button to delete the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

MAC Address Table Settings

This window is used to display and configure the global MAC address table settings.

To view the following window, click **L2 Features > FDB > MAC Address Table Settings**, as shown below:



MAC Address Table Settings

Global Settings | MAC Address Learning

Aging Time (0, 10-1000000) 300 sec

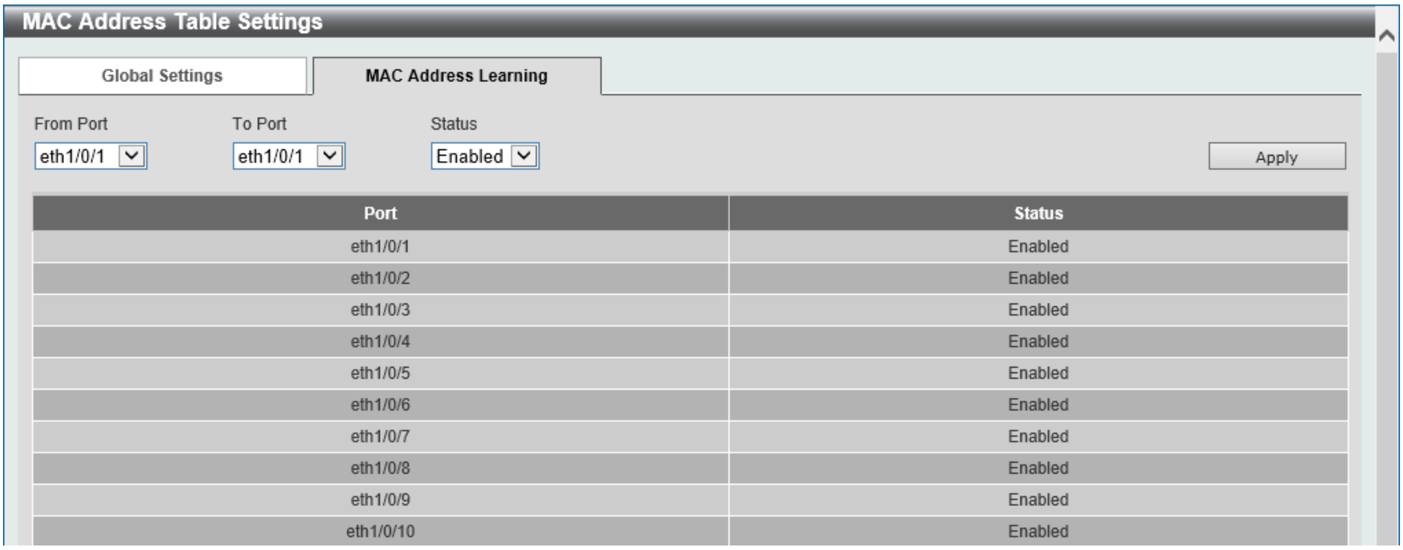
Figure 5-2 MAC Address Table Settings (Global Settings) Window

The fields that can be configured are described below:

Parameter	Description
Aging Time	Enter the MAC address table aging time here. This value must be between 10 and 1000000 seconds. Entering 0 will disable MAC address aging. By default, this value is 300 seconds.

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

After clicking the **MAC Address Learning** tab, at the top of the page, the following page will be available.



MAC Address Table Settings

Global Settings | MAC Address Learning

From Port: eth1/0/1 To Port: eth1/0/1 Status: Enabled

Port	Status
eth1/0/1	Enabled
eth1/0/2	Enabled
eth1/0/3	Enabled
eth1/0/4	Enabled
eth1/0/5	Enabled
eth1/0/6	Enabled
eth1/0/7	Enabled
eth1/0/8	Enabled
eth1/0/9	Enabled
eth1/0/10	Enabled

Figure 5-3 MAC Address Table Settings (MAC Address Port Learning Settings) Window

The fields that can be configured are described below:

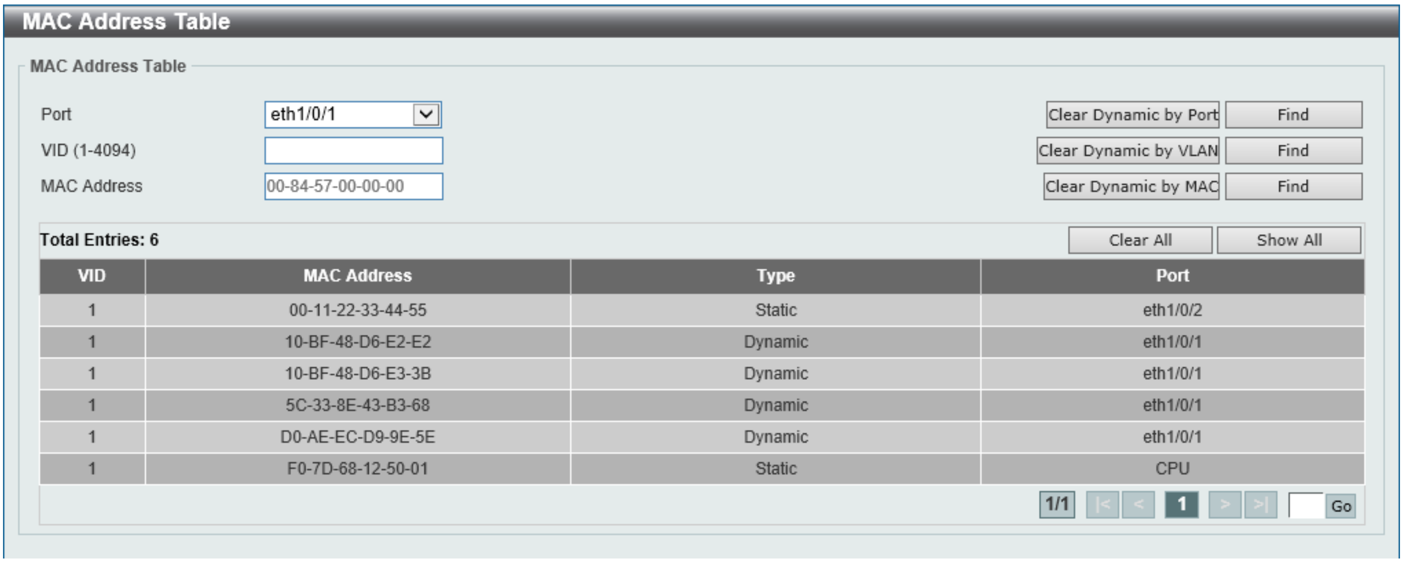
Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
Status	Select to enable or disable the MAC address learning function on the ports specified here.

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

MAC Address Table

This window is used to view the entries listed in the MAC address table.

To view the following window, click **L2 Features > FDB > MAC Address Table**, as shown below:



MAC Address Table

MAC Address Table

Port: eth1/0/1

VID (1-4094):

MAC Address: 00-84-57-00-00-00

Total Entries: 6

VID	MAC Address	Type	Port
1	00-11-22-33-44-55	Static	eth1/0/2
1	10-BF-48-D6-E2-E2	Dynamic	eth1/0/1
1	10-BF-48-D6-E3-3B	Dynamic	eth1/0/1
1	5C-33-8E-43-B3-68	Dynamic	eth1/0/1
1	D0-AE-EC-D9-9E-5E	Dynamic	eth1/0/1
1	F0-7D-68-12-50-01	Static	CPU

Figure 5-4 MAC Address Table Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the port that will be used here.
VID	Enter the VLAN ID that will be used for this configuration here.
MAC Address	Enter the MAC address that will be used for this configuration here.

Click the **Clear Dynamic by Port** button to clear the dynamic MAC address listed on the corresponding port.

Click the **Clear Dynamic by VLAN** button to clear the dynamic MAC address listed on the corresponding VLAN.

Click the **Clear Dynamic by MAC** button to clear the dynamic MAC address entered.

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

Click the **Clear All** button to clear all dynamic MAC addresses.

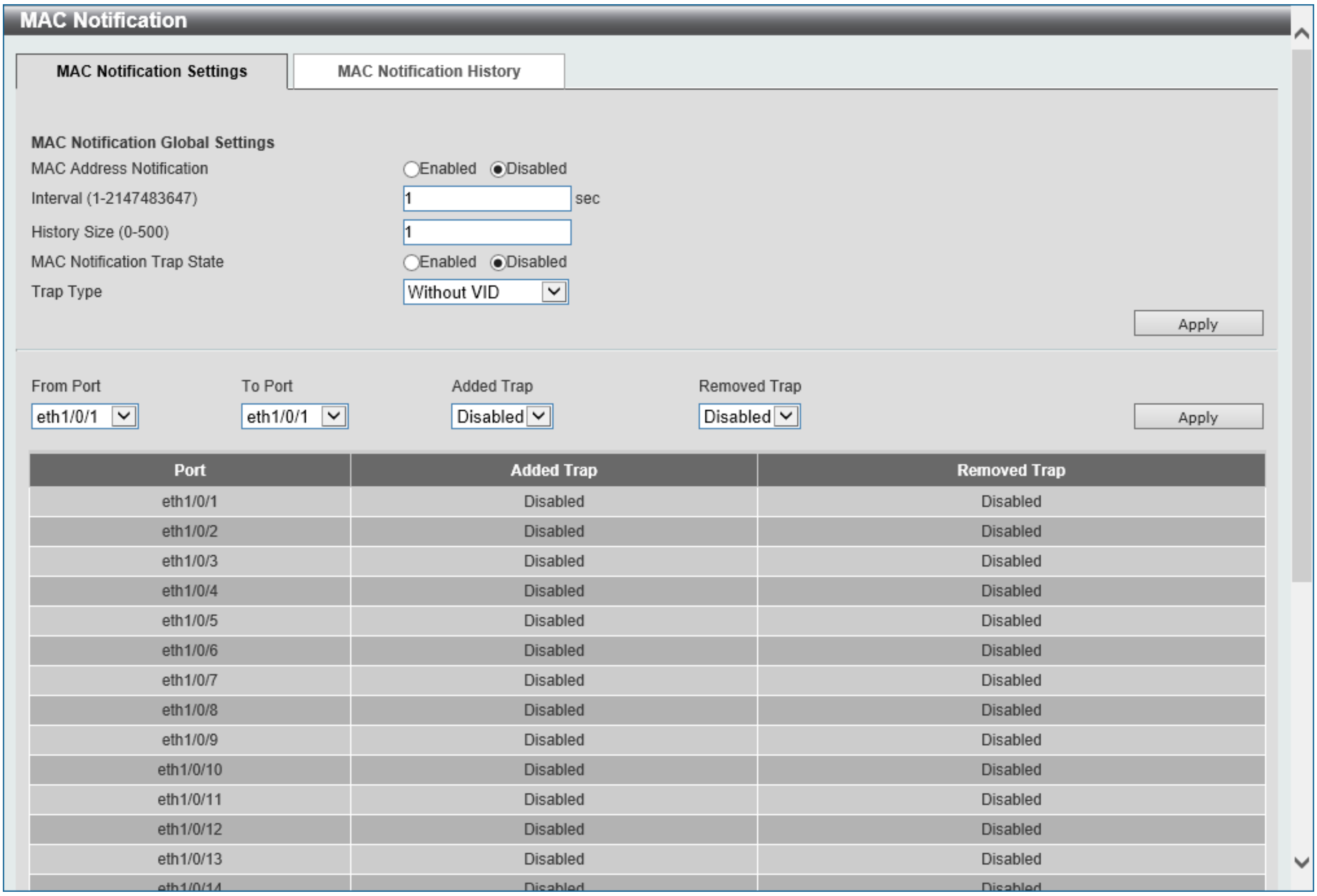
Click the **Show All** button to display all the MAC addresses recorded in the MAC address table.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

MAC Notification

This window is used to display and configure MAC notification.

To view the following window, click **L2 Features > FDB > MAC Notification**, as shown below:



MAC Notification Global Settings

MAC Address Notification ○Enabled ●Disabled

Interval (1-2147483647) 1 sec

History Size (0-500) 1

MAC Notification Trap State ○Enabled ●Disabled

Trap Type Without VID

From Port	To Port	Added Trap	Removed Trap
eth1/0/1	eth1/0/1	Disabled	Disabled

Port	Added Trap	Removed Trap
eth1/0/1	Disabled	Disabled
eth1/0/2	Disabled	Disabled
eth1/0/3	Disabled	Disabled
eth1/0/4	Disabled	Disabled
eth1/0/5	Disabled	Disabled
eth1/0/6	Disabled	Disabled
eth1/0/7	Disabled	Disabled
eth1/0/8	Disabled	Disabled
eth1/0/9	Disabled	Disabled
eth1/0/10	Disabled	Disabled
eth1/0/11	Disabled	Disabled
eth1/0/12	Disabled	Disabled
eth1/0/13	Disabled	Disabled
eth1/0/14	Disabled	Disabled

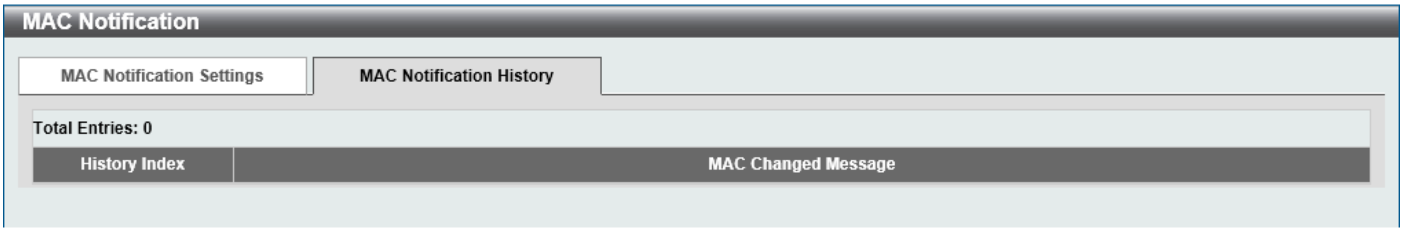
Figure 5-5 MAC Notification (MAC Notification Settings) Window

The fields that can be configured are described below:

Parameter	Description
MAC Address Notification	Select to globally enable or disable the MAC notification function.
Interval	Enter the time value between notifications. This value must be between 1 and 2147483647 seconds. By default, this value is 1 second.
History Size	Enter the maximum number of entries listed in the history log used for notification. This value must be between 0 and 500. By default, this value is 1.
MAC Notification Trap State	Select to enable or disable the MAC notification trap state.
Trap Type	Specifies the trap type. Options to choose from are **Without VID** and **With VID**.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Added Trap	Select to enable or disable the added trap for the port(s) selected.
Removed Trap	Select to enable or disable the removed trap for the port(s) selected.

Click the **Apply** button to accept the changes made for each individual section.

After selecting the **MAC Notification History** tab, at the top of the page, the following page will be available.



MAC Notification

Total Entries: 0

History Index	MAC Changed Message

Figure 5-6 MAC Notification (MAC Notification History) Window

On this page, a list of MAC notification messages will be displayed.

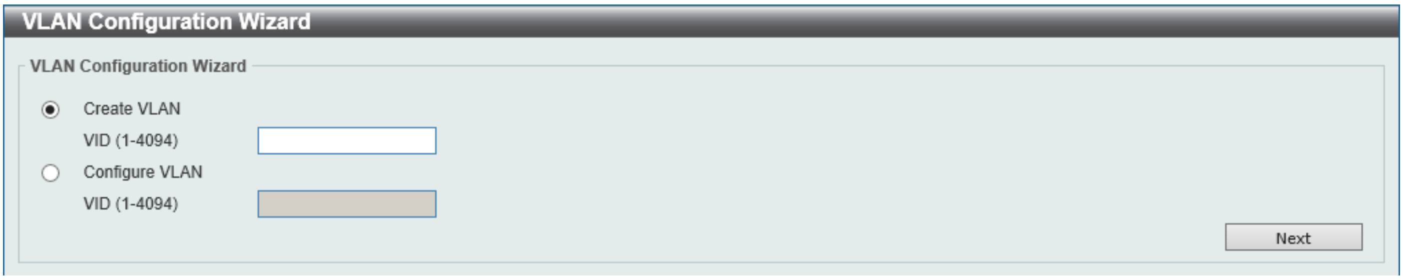
VLAN

VLAN Configuration Wizard

This window is used to start the VLAN configuration wizard.

Create/Configure VLAN

To view the following window, click **L2 Features > VLAN > VLAN Configuration Wizard**, as shown below:



VLAN Configuration Wizard

VLAN Configuration Wizard

● Create VLAN

VID (1-4094)

○ Configure VLAN

VID (1-4094)

Figure 5-7 VLAN Configuration Wizard (Step 1) Window

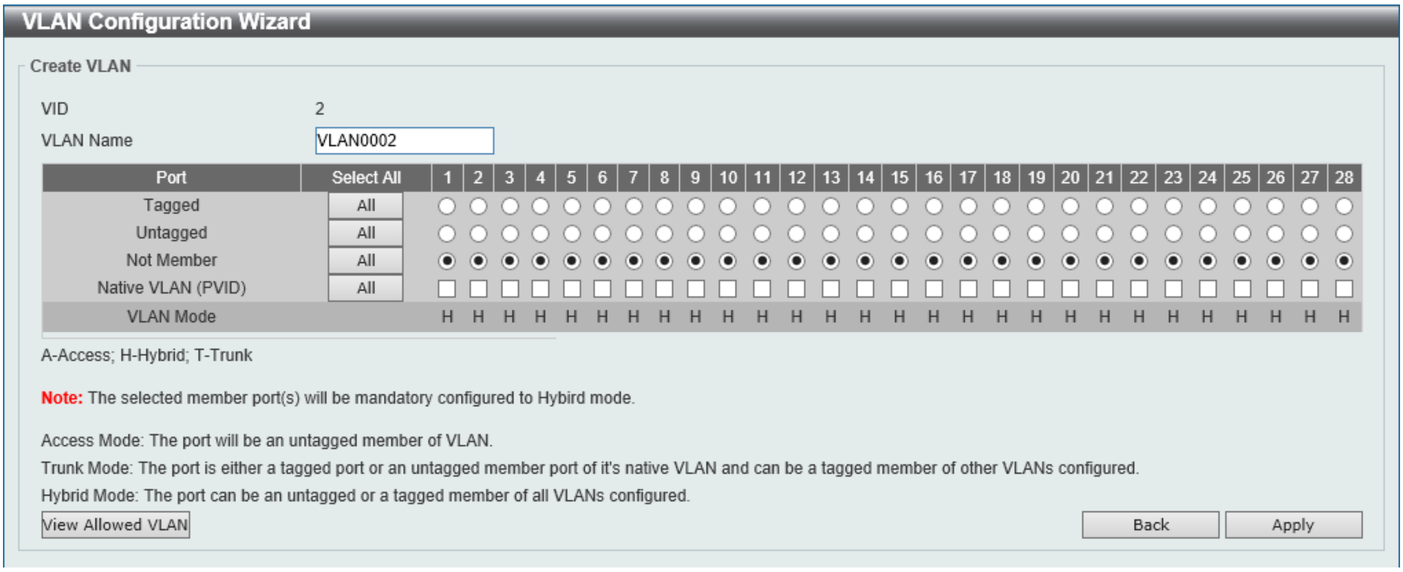
The fields that can be configured are described below:

Parameter	Description
Create VLAN	Select this option to create a new VLAN. • **VID** - Enter the VLAN ID here. The range is from 1 to 4094.
Configure VLAN	Select this option to configure an existing VLAN. • **VID** - Enter the VLAN ID here. The range is from 1 to 4094.

Click the **Next** button to continue to the next step.

Create VLAN

After selecting the **Create VLAN** option and clicking the **Next** button, the following window will appear.



VID 2

VLAN Name VLAN0002

Port	Select All	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Tagged	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Untagged	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Not Member	All	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Native VLAN (PVID)	All	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
VLAN Mode		H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H

A-Access; H-Hybrid; T-Trunk

Note: The selected member port(s) will be mandatory configured to Hybird mode.

Access Mode: The port will be an untagged member of VLAN.
Trunk Mode: The port is either a tagged port or an untagged member port of it's native VLAN and can be a tagged member of other VLANs configured.
Hybrid Mode: The port can be an untagged or a tagged member of all VLANs configured.

Figure 5-8 VLAN Configuration Wizard (Create VLAN) Window

The fields that can be configured are described below:

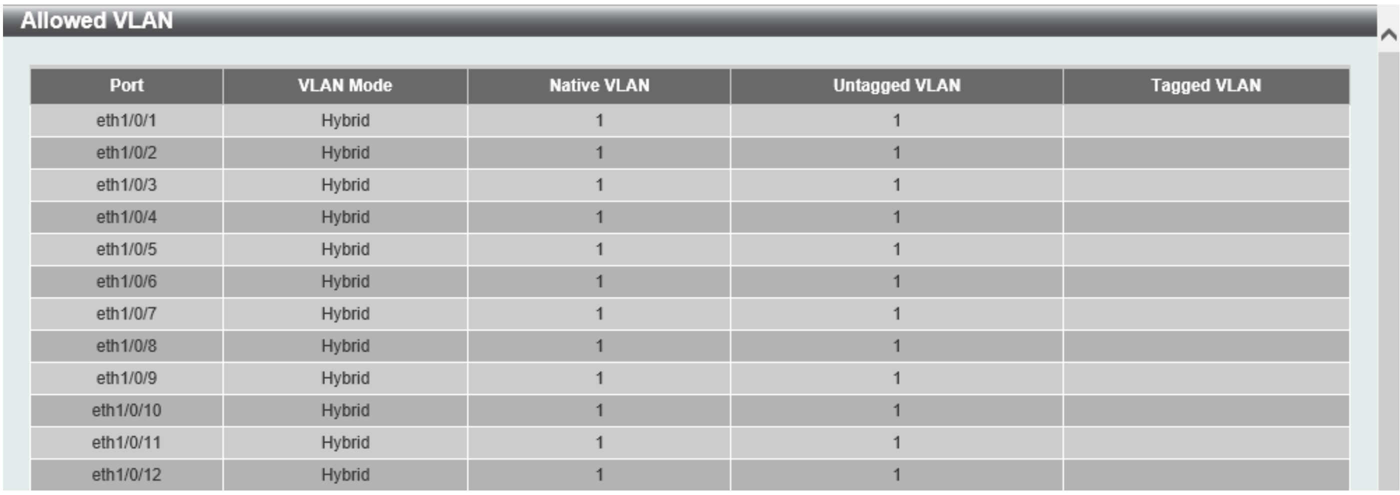
Parameter	Description
VLAN Name	Enter the name for the VLAN here.
Tagged	Select the switch ports that are tagged members of this VLAN here.
Untagged	Select the switch ports that are untagged members of this VLAN here.
Not Member	Select the switch ports that are not members of this VLAN here.
Native VLAN (PVID)	Select the switch ports that support the native VLAN here.

Click the **View Allowed VLAN** button view the allowed VLAN settings.

Click the **Back** button to return to the previous step.

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

After clicking the **View Allowed VLAN** button, the following window will appear.

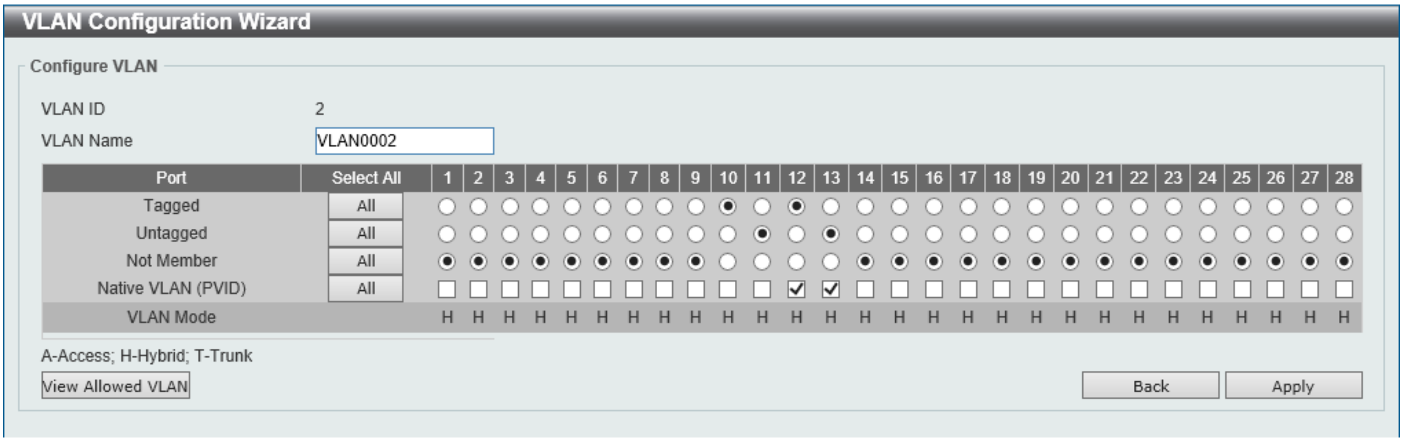


Port	VLAN Mode	Native VLAN	Untagged VLAN	Tagged VLAN
eth1/0/1	Hybrid	1	1	
eth1/0/2	Hybrid	1	1	
eth1/0/3	Hybrid	1	1	
eth1/0/4	Hybrid	1	1	
eth1/0/5	Hybrid	1	1	
eth1/0/6	Hybrid	1	1	
eth1/0/7	Hybrid	1	1	
eth1/0/8	Hybrid	1	1	
eth1/0/9	Hybrid	1	1	
eth1/0/10	Hybrid	1	1	
eth1/0/11	Hybrid	1	1	
eth1/0/12	Hybrid	1	1	

Figure 5-9 Allowed VLAN Window

Configure VLAN

After selecting the **Configure VLAN** option and clicking the **Next** button, the following window will appear.



VLAN Configuration Wizard

Configure VLAN

VLAN ID 2

VLAN Name VLAN0002

Port	Select All	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Tagged	All	○	○	○	○	○	○	○	○	○	●	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Untagged	All	○	○	○	○	○	○	○	○	○	○	●	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Not Member	All	●	●	●	●	●	●	●	●	●	○	○	○	○	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Native VLAN (PVID)	All	□	□	□	□	□	□	□	□	□	□	□	☑	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
VLAN Mode		H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H

A-Access; H-Hybrid; T-Trunk

Figure 5-10 VLAN Configuration Wizard (Configure VLAN) Window

The fields that can be configured are described below:

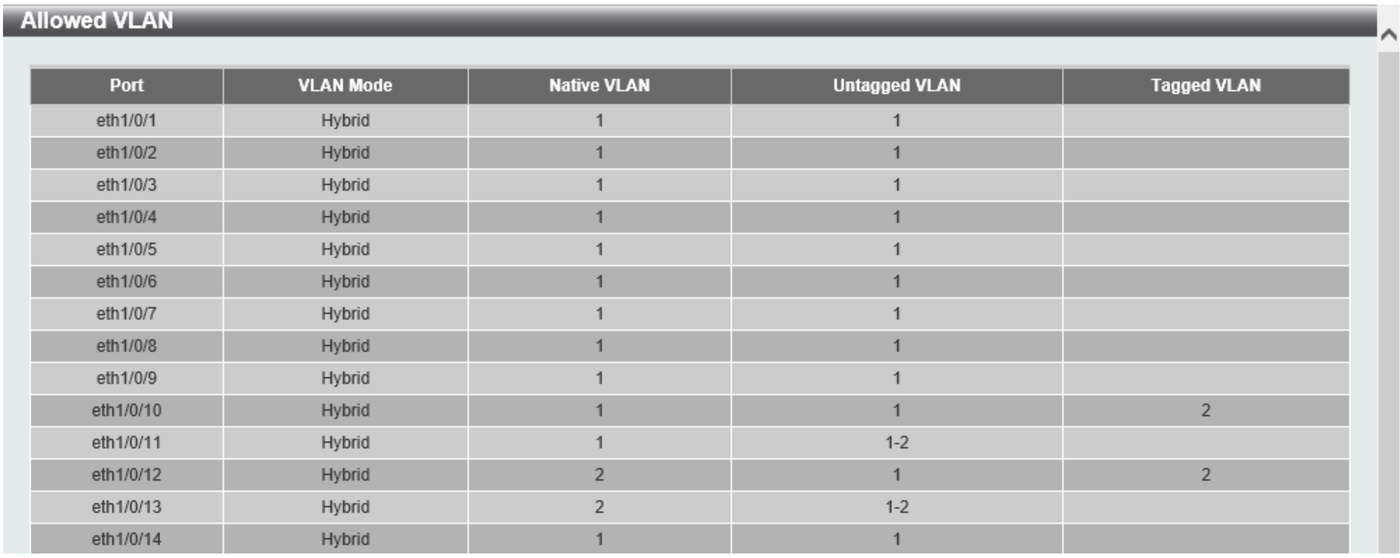
Parameter	Description
VLAN Name	Enter the name for the VLAN here.
Tagged	Select the switch ports that are tagged members of this VLAN here.
Untagged	Select the switch ports that are untagged members of this VLAN here.
Not Member	Select the switch ports that are not members of this VLAN here.
Native VLAN (PVID)	Select the switch ports that support the native VLAN here.

Click the **View Allowed VLAN** button view the allowed VLAN settings.

Click the **Back** button to return to the previous step.

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

After clicking the **View Allowed VLAN** button, the following window will appear.



Allowed VLAN

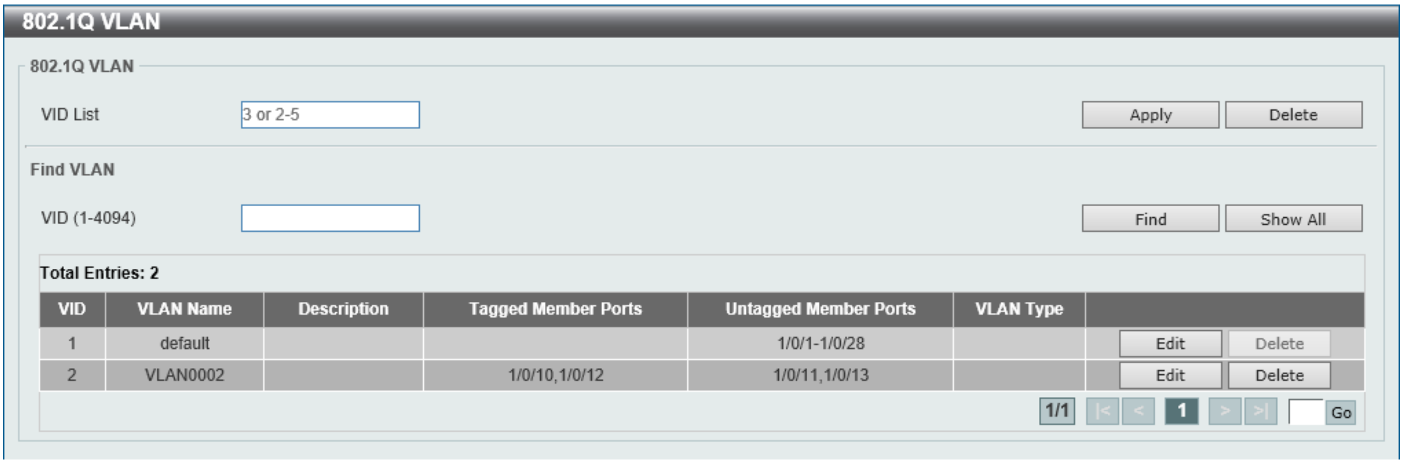
Port	VLAN Mode	Native VLAN	Untagged VLAN	Tagged VLAN
eth1/0/1	Hybrid	1	1	
eth1/0/2	Hybrid	1	1	
eth1/0/3	Hybrid	1	1	
eth1/0/4	Hybrid	1	1	
eth1/0/5	Hybrid	1	1	
eth1/0/6	Hybrid	1	1	
eth1/0/7	Hybrid	1	1	
eth1/0/8	Hybrid	1	1	
eth1/0/9	Hybrid	1	1	
eth1/0/10	Hybrid	1	1	2
eth1/0/11	Hybrid	1	1-2	
eth1/0/12	Hybrid	2	1	2
eth1/0/13	Hybrid	2	1-2	
eth1/0/14	Hybrid	1	1	

Figure 5-11 Allowed VLAN Window

802.1Q VLAN

This window is used to display and configure the VLAN settings on this Switch.

To view the following window, click **L2 Features > VLAN > 802.1Q VLAN**, as shown below:



802.1Q VLAN

802.1Q VLAN

VID List: 3 or 2-5

Find VLAN

VID (1-4094):

Total Entries: 2

VID	VLAN Name	Description	Tagged Member Ports	Untagged Member Ports	VLAN Type	
1	default			1/0/1-1/0/28		Edit Delete
2	VLAN0002		1/0/10,1/0/12	1/0/11,1/0/13		Edit Delete

Figure 5-12 802.1Q VLAN Window

The fields that can be configured in **802.1Q VLAN** are described below:

Parameter	Description
VID List	Enter the VLAN ID list that will be created here.

Click the **Apply** button to create a new 802.1Q VLAN.

Click the **Delete** button to remove the 802.1Q VLAN specified.

The fields that can be configured in **Find VLAN** are described below:

Parameter	Description
VID	Enter the VLAN ID that will be displayed here.

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

Click the **Show All** button to locate all the entries.

Click the **Edit** button to modify the VLAN name.

Click the **Delete** button to remove the specific entry.

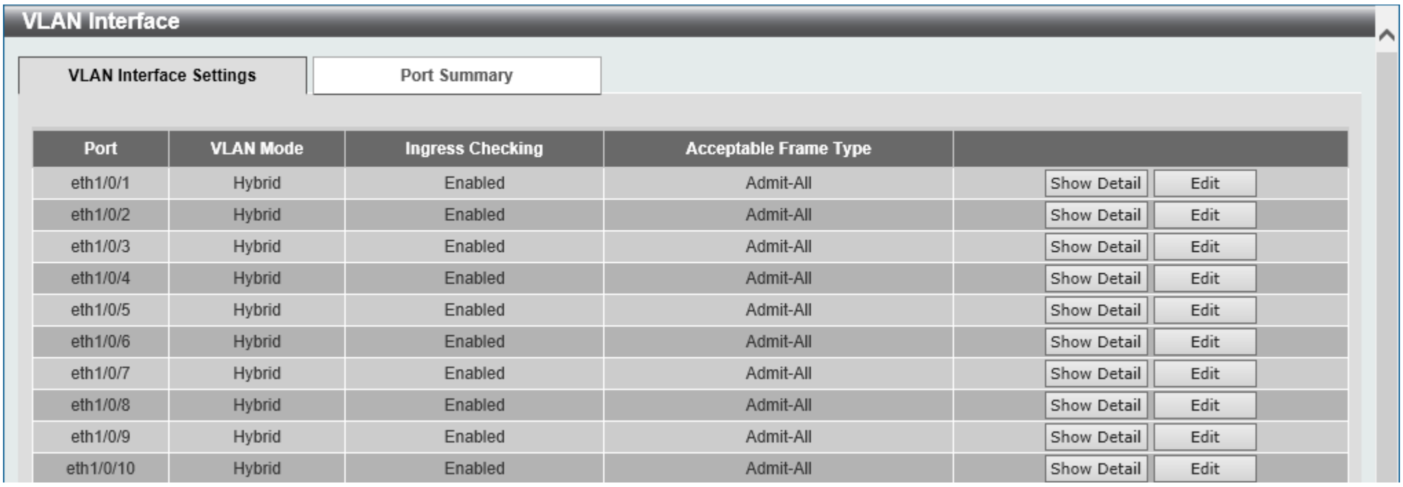
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

VLAN Interface

VLAN Interface Settings

This window is used to display and configure the VLAN interface settings.

To view the following window, click **L2 Features > VLAN > VLAN Interface**, as shown below:



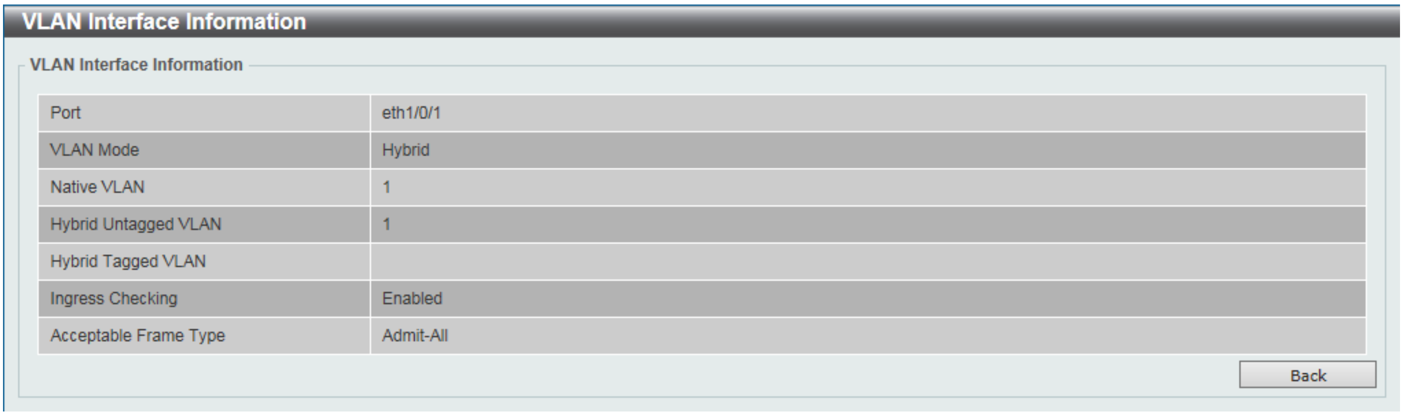
Port	VLAN Mode	Ingress Checking	Acceptable Frame Type	
eth1/0/1	Hybrid	Enabled	Admit-All	Show Detail Edit
eth1/0/2	Hybrid	Enabled	Admit-All	Show Detail Edit
eth1/0/3	Hybrid	Enabled	Admit-All	Show Detail Edit
eth1/0/4	Hybrid	Enabled	Admit-All	Show Detail Edit
eth1/0/5	Hybrid	Enabled	Admit-All	Show Detail Edit
eth1/0/6	Hybrid	Enabled	Admit-All	Show Detail Edit
eth1/0/7	Hybrid	Enabled	Admit-All	Show Detail Edit
eth1/0/8	Hybrid	Enabled	Admit-All	Show Detail Edit
eth1/0/9	Hybrid	Enabled	Admit-All	Show Detail Edit
eth1/0/10	Hybrid	Enabled	Admit-All	Show Detail Edit

Figure 5-13 VLAN Interface Window

Click the **Show Detail** button to view detailed information about the VLAN on the specific interface.

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

After clicking the **Show Detail** button, the following page will appear.



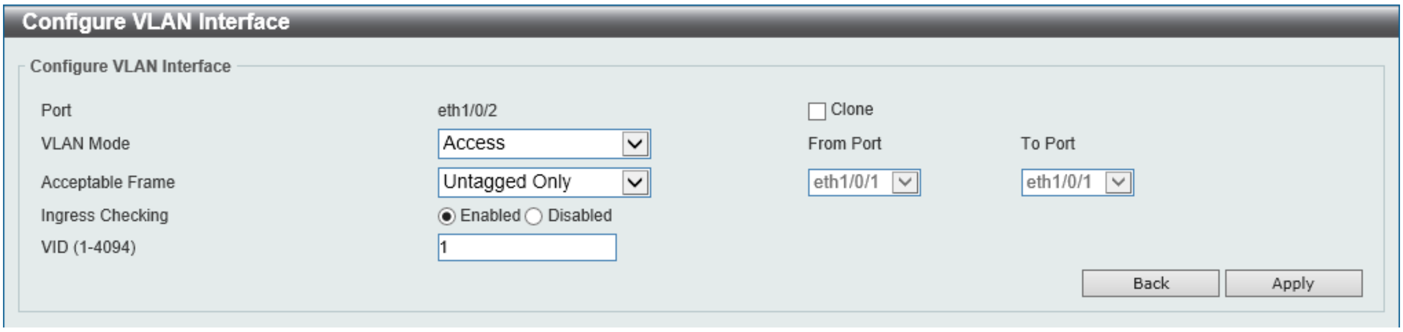
Port	eth1/0/1
VLAN Mode	Hybrid
Native VLAN	1
Hybrid Untagged VLAN	1
Hybrid Tagged VLAN	
Ingress Checking	Enabled
Acceptable Frame Type	Admit-All

Figure 5-14 VLAN Interface (VLAN Detail) Window

On this page, detailed information about the VLAN of the specific interface is displayed.

Click the **Back** button to return to the previous page.

After click the **Edit** button, the following page will appear. This is a dynamic page that will change when a different **VLAN Mode** is selected. When **Access** was selected as the **VLAN Mode**, the following page will appear.



Configure VLAN Interface

Configure VLAN Interface

Port: eth1/0/2
□ Clone
VLAN Mode: Access
From Port: eth1/0/1
To Port: eth1/0/1
Acceptable Frame: Untagged Only
Ingress Checking: ● Enabled ○ Disabled
VID (1-4094): 1

Figure 5-15 VLAN Interface (Access) Window

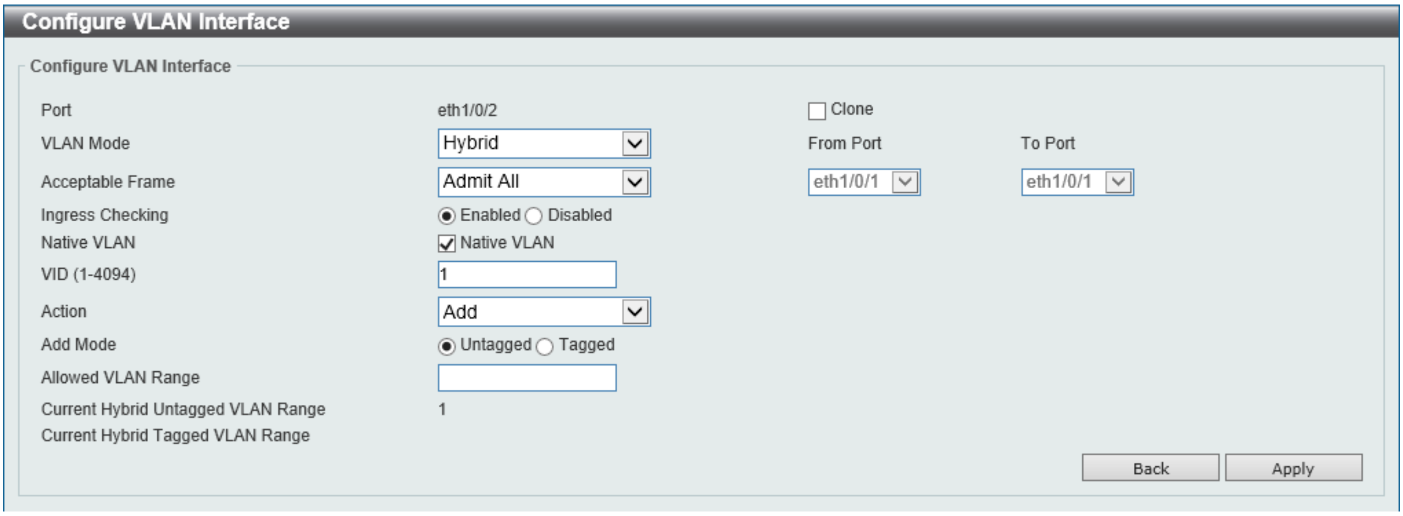
The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are **Access**, **Hybrid**, and **Trunk**.
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are **Tagged Only**, **Untagged Only**, and **Admit All**.
Ingress Checking	Select to enable or disable the ingress checking function.
VID	Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.
Clone	Select this option to enable the clone feature.
From Port - To Port	Select the range of ports that will be used in the clone feature here.

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

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

When **Hybrid** was selected as the **VLAN Mode**, the following page will appear.



Configure VLAN Interface

Configure VLAN Interface

Port: eth1/0/2
□ Clone
VLAN Mode: Hybrid
From Port: eth1/0/1
To Port: eth1/0/1
Acceptable Frame: Admit All
Ingress Checking: ● Enabled ○ Disabled
Native VLAN: ☑ Native VLAN
VID (1-4094): 1
Action: Add
Add Mode: ● Untagged ○ Tagged
Allowed VLAN Range:
Current Hybrid Untagged VLAN Range: 1
Current Hybrid Tagged VLAN Range:

Figure 5-16 VLAN Interface (Hybrid) Window

The fields that can be configured are described below:

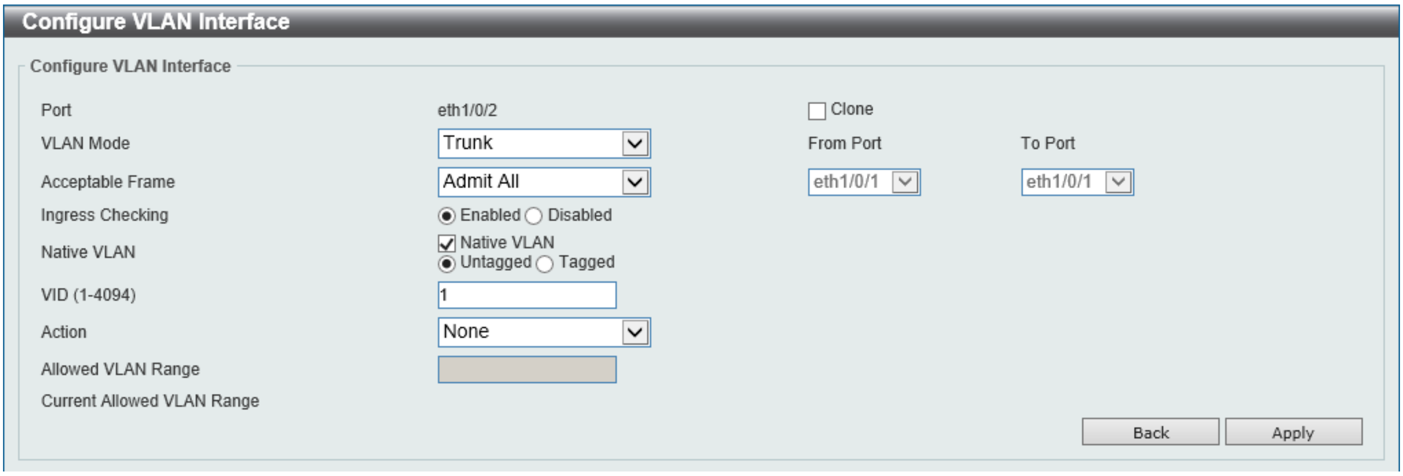
Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are **Access**, **Hybrid**, and **Trunk**.

Parameter	Description
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are **Tagged Only**, **Untagged Only**, and **Admit All**.
Ingress Checking	Select to enable or disable the ingress checking function.
Native VLAN	Tick this option to enable the native VLAN function.
VID	After ticking the **Native VLAN** option, the following parameter will be available. Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.
Action	Select the action that will be taken here. Options to choose from are **Add**, **Remove**, **Tagged**, and **Untagged**.
Add Mode	Select whether to add an **Untagged** or **Tagged** parameters.
Allowed VLAN Range	Enter the allowed VLAN range here.
Clone	Select this option to enable the clone feature.
From Port - To Port	Select the range of ports that will be used in the clone feature here.

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

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

When **Trunk** was selected as the **VLAN Mode**, the following page will appear.



Configure VLAN Interface

Configure VLAN Interface

Port: eth1/0/2

VLAN Mode: Trunk

Acceptable Frame: Admit All

Ingress Checking: ● Enabled ○ Disabled

Native VLAN: ☑ Native VLAN ● Untagged ○ Tagged

VID (1-4094): 1

Action: None

Allowed VLAN Range:

Current Allowed VLAN Range

□ Clone

From Port: eth1/0/1

To Port: eth1/0/1

Figure 5-17 VLAN Interface (Trunk) Window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are **Access**, **Hybrid**, and **Trunk**.
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are **Tagged Only**, **Untagged Only**, and **Admit All**.
Ingress Checking	After selecting **Trunk** as the **VLAN Mode**, the following parameter will be available. Select to enable or disable the ingress checking function.
Native VLAN	Tick this option to enable the native VLAN function. Also, select if this VLAN supports **Untagged** or **Tagged** frames.
VID	After ticking the **Native VLAN** option, the following parameter will be available. Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.
Action	Select the action that will be taken here. Options to choose from are **All**, **Add**, **Remove**, **Except**, and **Replace**.
Allowed VLAN Range	Enter the allowed VLAN range here.

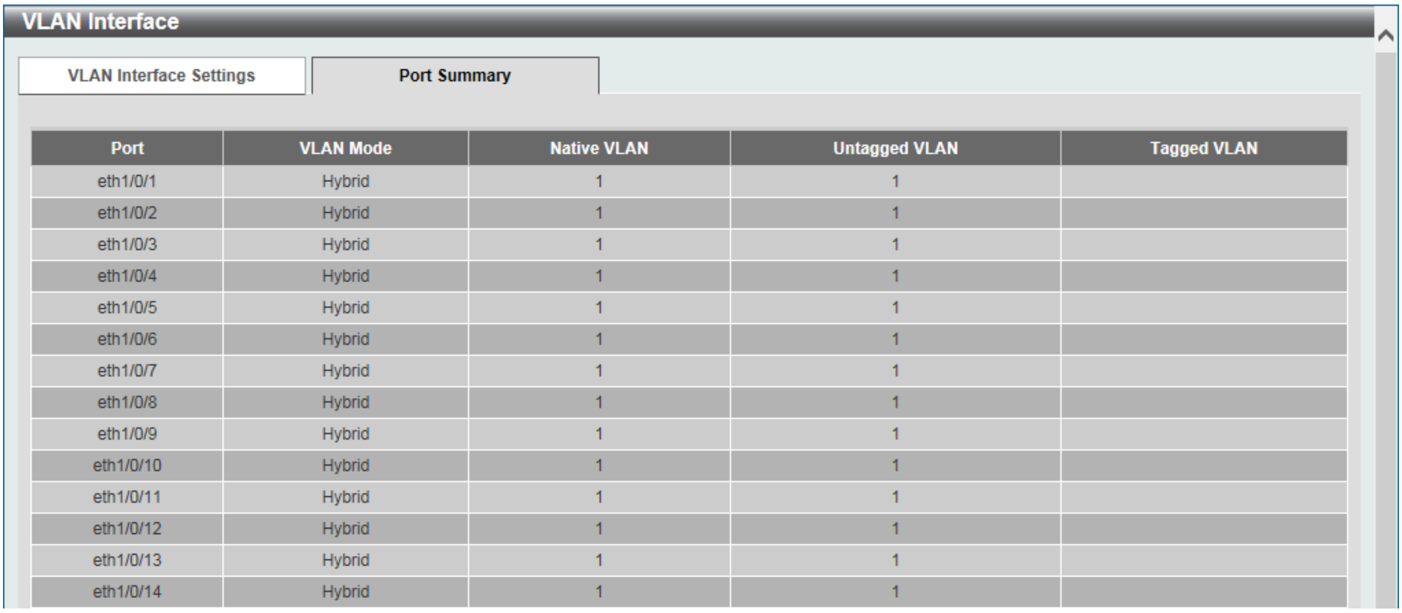
Parameter	Description
Clone	Select this option to enable the clone feature.
From Port - To Port	Select the range of ports that will be used in the clone feature here.

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

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

Port Summary

After selecting the **Port Summary** tab, the following page will be available.



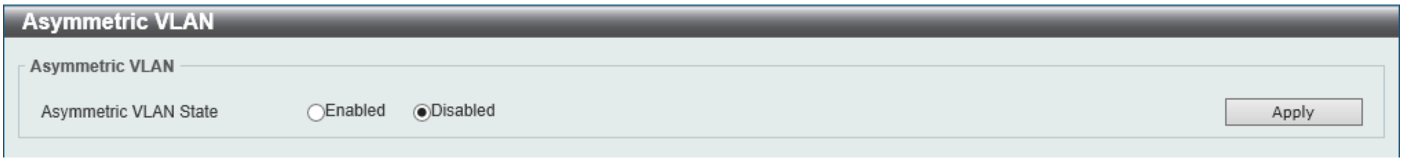
Port	VLAN Mode	Native VLAN	Untagged VLAN	Tagged VLAN
eth1/0/1	Hybrid	1	1	
eth1/0/2	Hybrid	1	1	
eth1/0/3	Hybrid	1	1	
eth1/0/4	Hybrid	1	1	
eth1/0/5	Hybrid	1	1	
eth1/0/6	Hybrid	1	1	
eth1/0/7	Hybrid	1	1	
eth1/0/8	Hybrid	1	1	
eth1/0/9	Hybrid	1	1	
eth1/0/10	Hybrid	1	1	
eth1/0/11	Hybrid	1	1	
eth1/0/12	Hybrid	1	1	
eth1/0/13	Hybrid	1	1	
eth1/0/14	Hybrid	1	1	

Figure 5-18 VLAN Interface Port Summary Window

Asymmetric VLAN

This window is used to display and configure the asymmetric VLAN settings.

To view the following window, click **L2 Features > VLAN > Asymmetric VLAN**, as shown below:



Asymmetric VLAN State ○Enabled ●Disabled

Figure 5-19 Asymmetric VLAN Window

The fields that can be configured are described below:

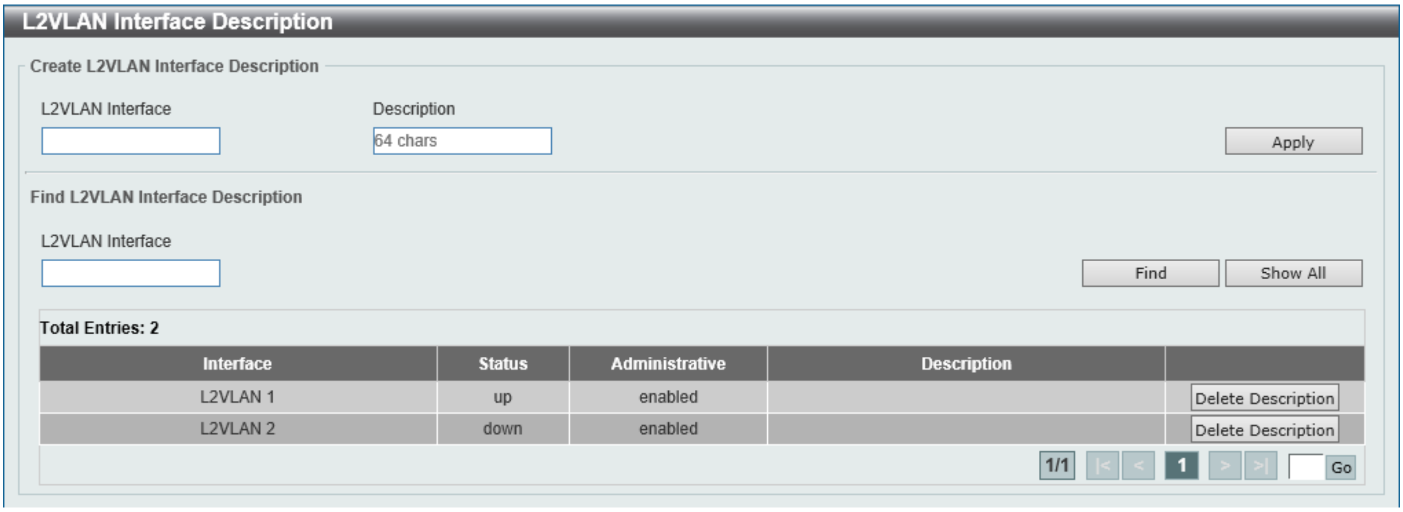
Parameter	Description
Asymmetric VLAN State	Select to enable or disable the asymmetric VLAN feature here.

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

L2VLAN Interface Description

This window is used to display and configure the Layer 2 VLAN interface description.

To view the following window, click **L2 Features > VLAN > L2VLAN Interface Description**, as shown below:



L2VLAN Interface Description

Create L2VLAN Interface Description

L2VLAN Interface

Description: 64 chars

Find L2VLAN Interface Description

L2VLAN Interface

Total Entries: 2

Interface	Status	Administrative	Description	
L2VLAN 1	up	enabled		Delete Description
L2VLAN 2	down	enabled		Delete Description

Figure 5-20 L2VLAN Interface Description Window

The fields that can be configured are described below:

Parameter	Description
L2VLAN Interface	Enter the ID of the Layer 2 VLAN interface here.
Description	Enter the description for the Layer 2 VLAN interface here.

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

Click the **Find** button to generate the display based on the information entered.

Click the **Show All** button to display all the available entries.

Click the **Delete Description** button to remove the description from the specified Layer 2 VLAN.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Auto Surveillance VLAN

Auto Surveillance Properties

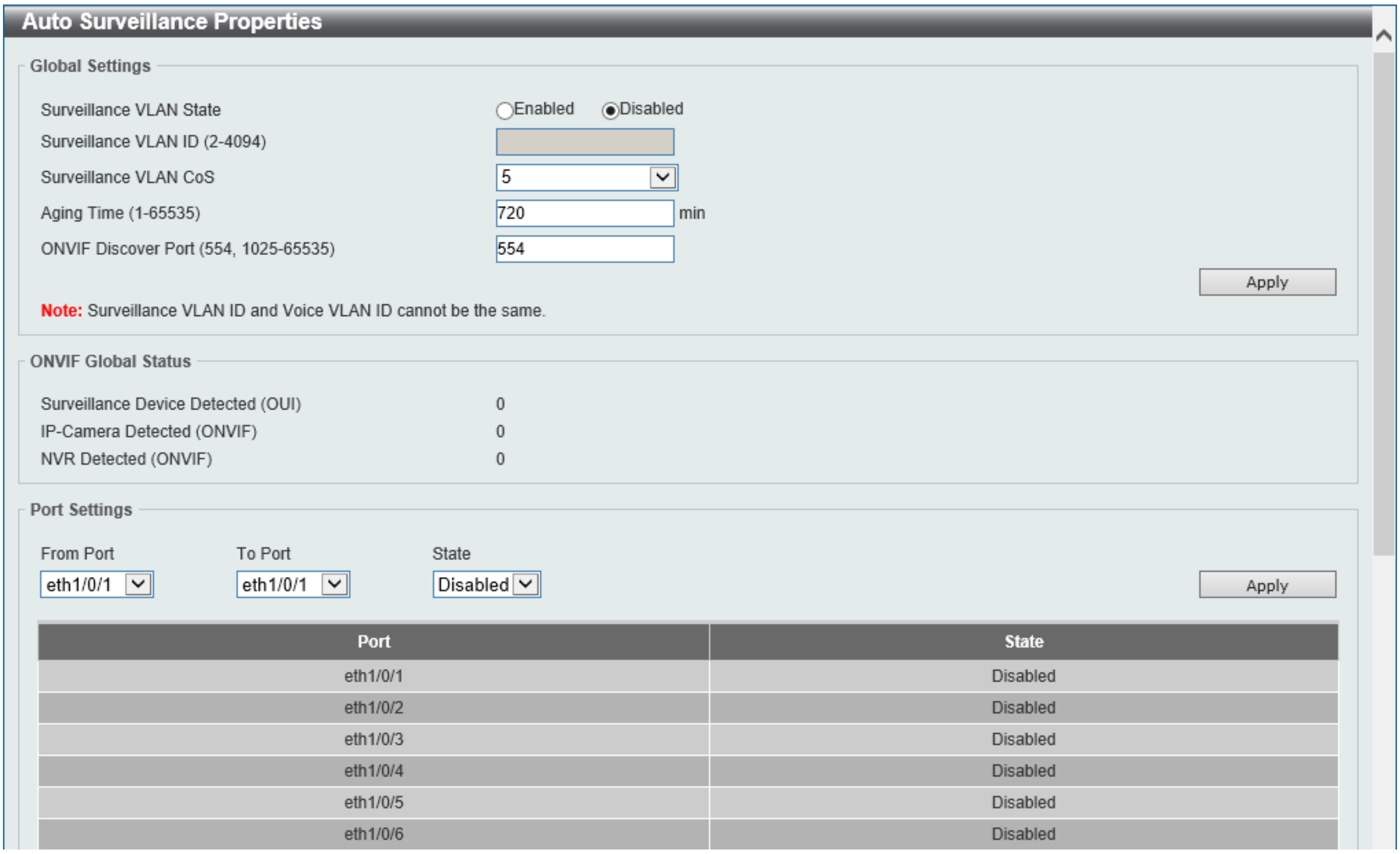
This window is used to configure the auto-surveillance VLAN global settings and display the ports surveillance VLAN information.

The Switch regards a host as an NVR once it connects to the IPC via HTTP, HTTPS, or RTSP. The Switch will learn the NVR on this port and move it into the surveillance VLAN until the triggered aging mechanism age-out or the LAN cable is removed.

When the host sends an ARP request to an IPC, the Switch still regards the host as an NVR but only temporarily move it into the surveillance VLAN. The host will automatically be moved out of the surveillance VLAN after about 30 seconds if it is not recognized as an NVR anymore.

NOTE: The same PC, or PCs connected to the same LAN port on the Switch, cannot simultaneously manage the Switch and the IP cameras connected to the Switch.

To view the following window, click **L2 Features > VLAN > Auto Surveillance VLAN > Auto Surveillance Properties**, as shown below:



Auto Surveillance Properties

Global Settings

Surveillance VLAN State ○Enabled ●Disabled

Surveillance VLAN ID (2-4094)

Surveillance VLAN CoS 5

Aging Time (1-65535) 720 min

ONVIF Discover Port (554, 1025-65535) 554

Note: Surveillance VLAN ID and Voice VLAN ID cannot be the same.

ONVIF Global Status

Surveillance Device Detected (OUI) 0

IP-Camera Detected (ONVIF) 0

NVR Detected (ONVIF) 0

Port Settings

From Port eth1/0/1 To Port eth1/0/1 State Disabled

Port	State
eth1/0/1	Disabled
eth1/0/2	Disabled
eth1/0/3	Disabled
eth1/0/4	Disabled
eth1/0/5	Disabled
eth1/0/6	Disabled

Figure 5-21 Auto Surveillance Properties Window

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

Parameter	Description
Surveillance VLAN State	Select to enable or disable the surveillance VLAN feature here.
Surveillance VLAN ID	Enter the VLAN ID of the surveillance VLAN here. The range is from 2 to 4094. A normal VLAN needs to be created before assigning the VLAN as a surveillance VLAN.
Surveillance VLAN CoS	Enter the Class of Service (CoS) value for the surveillance VLAN here. The surveillance packets arriving at the surveillance VLAN enabled port are marked with the CoS specified here. The remarking of CoS allows the surveillance VLAN traffic to be distinguished from data traffic in quality of service. The range is from 0 to 7.
Aging Time	Enter the aging time value here. This is used to configure the aging time for aging out the surveillance VLAN dynamic member ports. The range is from 1 to 65535 minutes. When the last surveillance device connected to the port stops sending traffic and the MAC address of this surveillance device is aged out, the surveillance VLAN aging timer will be started. The port will be removed from the surveillance VLAN after expiration of surveillance VLAN aging timer. If the surveillance traffic resumes during the aging time, the aging timer will be cancelled.
ONVIF Discover Port	Enter the TCP/UDP port number here. The range is either 554, or from 1025 to 65535. This is used to configure the TCP/UDP port number for RTSP stream snooping. ONVIF-capable IPC and ONVIF-capable NVR utilize WS-Discovery to find other devices. Once IPCs are discovered, the Switch can further discover NVRs by snooping RTSP, HTTP, and HTTPS packets between NVRs and IPCs. These packets cannot be snooped if the TCP/UDP port is not equal to the RTSP port number.

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

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

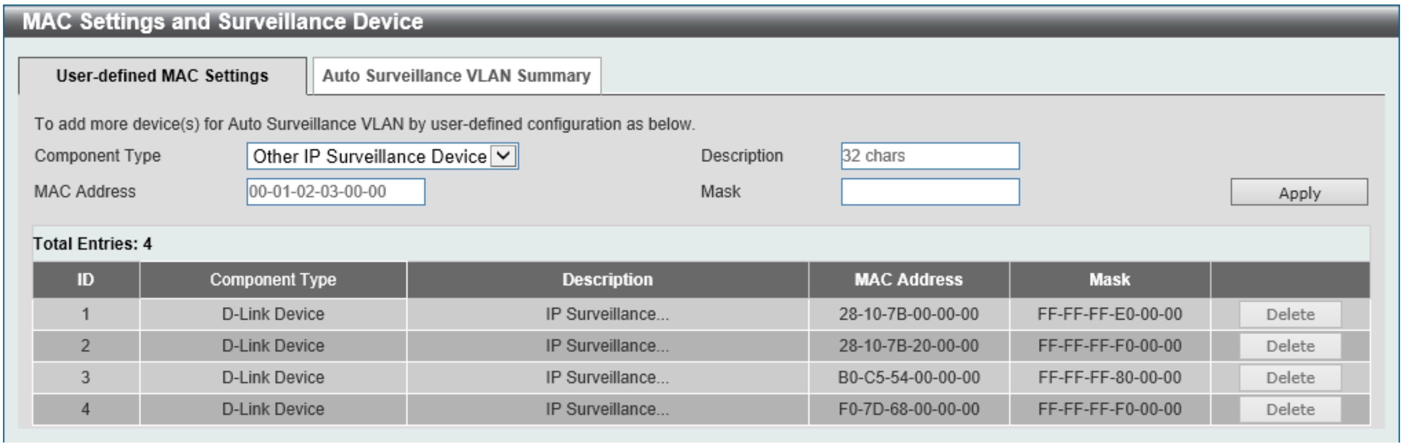
Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
State	Select to enable or disable the surveillance VLAN feature on the specified port(s) here. When surveillance VLAN is enabled for a port, the port will automatically be learned as an untagged surveillance VLAN member and the received untagged surveillance packets will be forwarded to the surveillance VLAN. The received packets are determined as surveillance packets if the source MAC addresses of the packets comply with the Organizationally Unique Identifier (OUI) addresses.

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

MAC Settings and Surveillance Device

This window is used to display and configure surveillance devices and their MAC settings.

To view the following window, click **L2 Features > VLAN > Auto Surveillance VLAN > MAC Settings and Surveillance Device**, as shown below:


MAC Settings and Surveillance Device
User-defined MAC Settings
Auto Surveillance VLAN Summary
Apply

To add more device(s) for Auto Surveillance VLAN by user-defined configuration as below.

Component Type: Other IP Surveillance Device
Description: 32 chars
MAC Address: 00-01-02-03-00-00
Mask:

Total Entries: 4

ID	Component Type	Description	MAC Address	Mask	
1	D-Link Device	IP Surveillance...	28-10-7B-00-00-00	FF-FF-FF-E0-00-00	Delete
2	D-Link Device	IP Surveillance...	28-10-7B-20-00-00	FF-FF-FF-F0-00-00	Delete
3	D-Link Device	IP Surveillance...	B0-C5-54-00-00-00	FF-FF-FF-80-00-00	Delete
4	D-Link Device	IP Surveillance...	F0-7D-68-00-00-00	FF-FF-FF-F0-00-00	Delete

Figure 5-22 MAC Settings and Surveillance Device Window

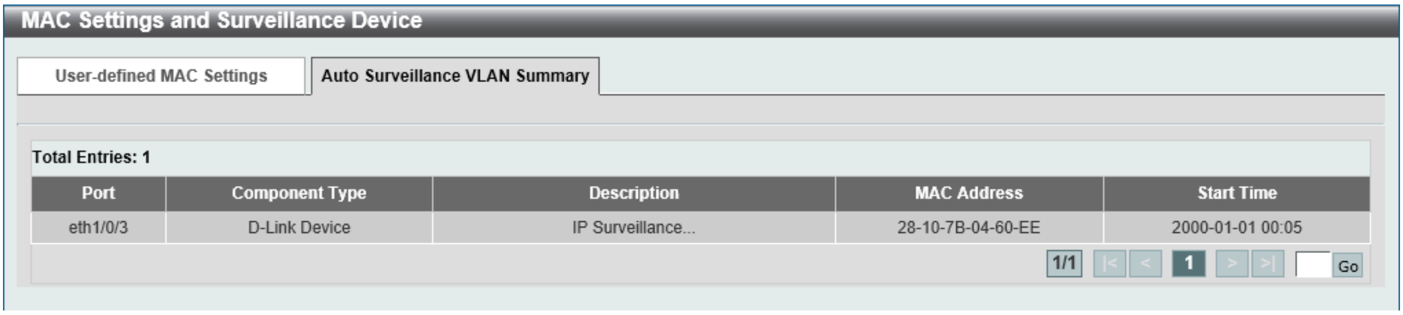
The fields that can be configured are described below:

Parameter	Description
Component Type	Select the component type here. Option to choose from are: • **Video Management server** - Specifies the surveillance device type as Video Management Server (VMS). • **VMS Client/Remote Viewer** - Specifies the surveillance device type as VMS client. • **Video Encoder** - Specifies the surveillance device type as Video Encoder. • **Network Storage** - Specifies the surveillance device type as Network Storage. • **Other IP Surveillance Device** - Specifies the surveillance device type as other IP Surveillance Devices.
Description	Enter the description for the user-defined OUI here. This string can be up to 32 characters long.
MAC Address	Enter the OUI MAC address here. If the source MAC addresses of the received packet matches any of the OUI pattern, the received packet is determined as a surveillance packet.
Mask	Enter the matching bitmask for the OUI MAC address here.

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

Click the **Delete** button to delete the specified entry.

After clicking the **Auto Surveillance VLAN Summary** tab, at the top of the page, the following page will be available.


MAC Settings and Surveillance Device
User-defined MAC Settings
Auto Surveillance VLAN Summary
1/1
1
Go

Total Entries: 1

Port	Component Type	Description	MAC Address	Start Time
eth1/0/3	D-Link Device	IP Surveillance...	28-10-7B-04-60-EE	2000-01-01 00:05

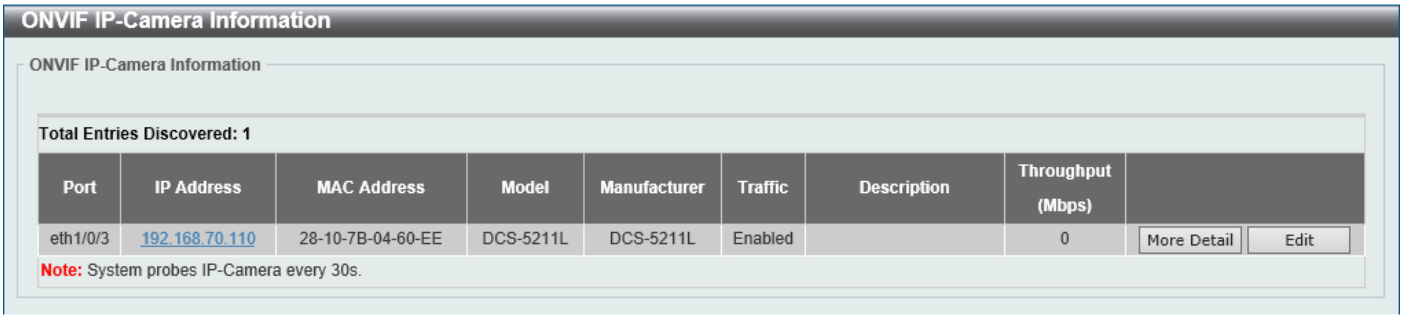
Figure 5-23 MAC Settings and Surveillance Device (Auto Surveillance VLAN Summary) Window

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

ONVIF IP-Camera Information

This window is used to display ONVIF IP camera information.

To view the following window, click **L2 Features > VLAN > Auto Surveillance VLAN > ONVIF IP-Camera Information**, as shown below:



Total Entries Discovered: 1

Port	IP Address	MAC Address	Model	Manufacturer	Traffic	Description	Throughput (Mbps)	
eth1/0/3	192.168.70.110	28-10-7B-04-60-EE	DCS-5211L	DCS-5211L	Enabled		0	More Detail Edit

Note: System probes IP-Camera every 30s.

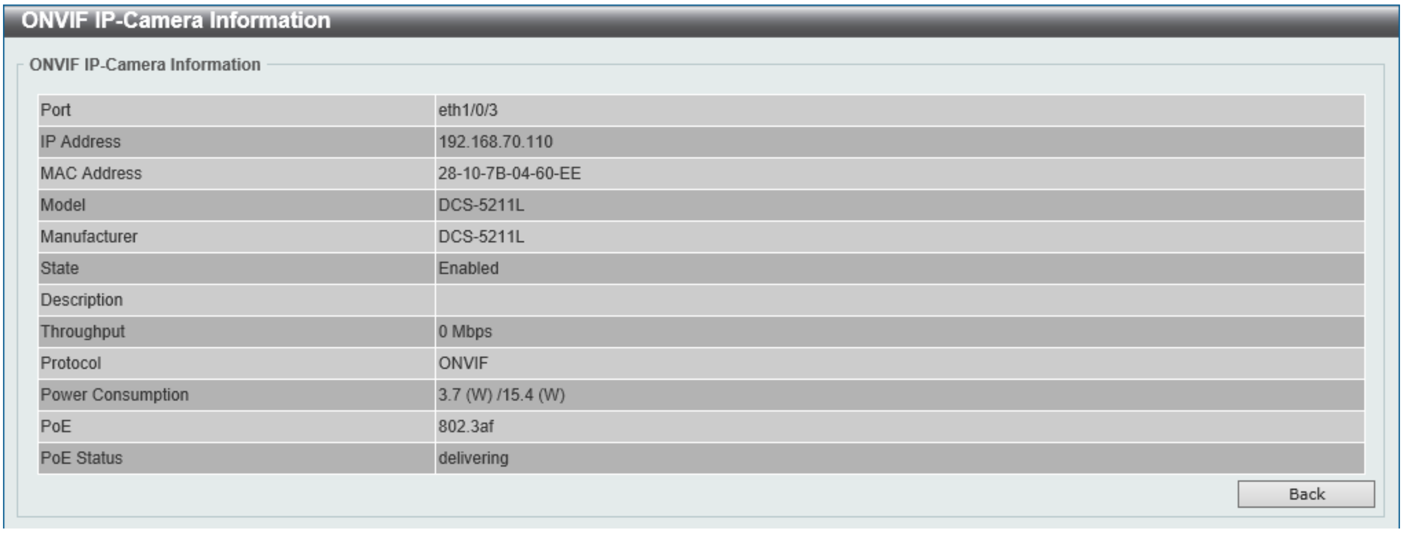
Figure 5-24 ONVIF IP-Camera Information Window

Click the IP address hyperlink to connect to the Web Interface of the IP camera.

Click the **More Detail** button to view detailed ONVIF IP camera information.

Click the **Edit** button to configure the state and description of the IP camera.

After click the **More Detail** button, the following window will appear.



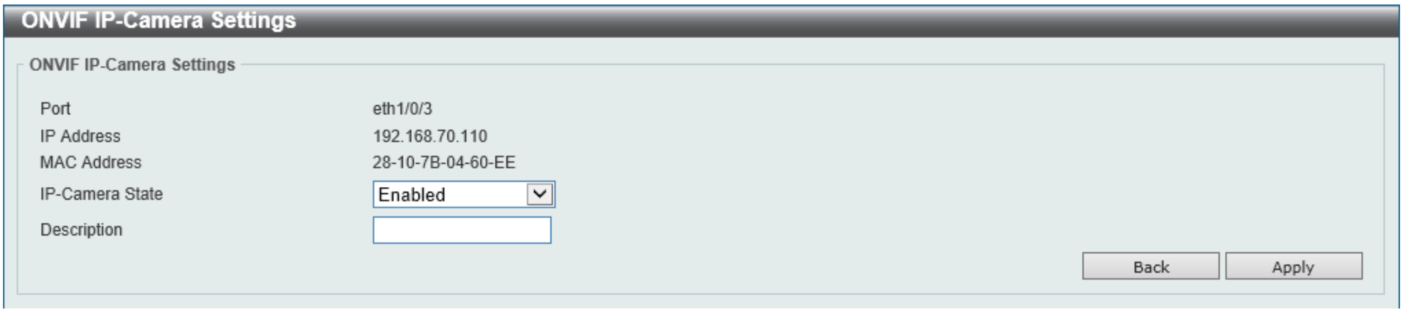
ONVIF IP-Camera Information

ONVIF IP-Camera Information

Port	eth1/0/3
IP Address	192.168.70.110
MAC Address	28-10-7B-04-60-EE
Model	DCS-5211L
Manufacturer	DCS-5211L
State	Enabled
Description	
Throughput	0 Mbps
Protocol	ONVIF
Power Consumption	3.7 (W) /15.4 (W)
PoE	802.3af
PoE Status	delivering

Figure 5-25 ONVIF IP-Camera Information (More Detail) Window

After click the **Edit** button, the following window will appear.



ONVIF IP-Camera Settings

ONVIF IP-Camera Settings

Port eth1/0/3

IP Address 192.168.70.110

MAC Address 28-10-7B-04-60-EE

IP-Camera State Enabled

Description

Figure 5-26 ONVIF IP-Camera Information (Edit) Window

The fields that can be configured are described below:

Parameter	Description
IP-Camera State	Select to enable or disable the IP camera state here.
Description	Enter the description for this IP camera here.

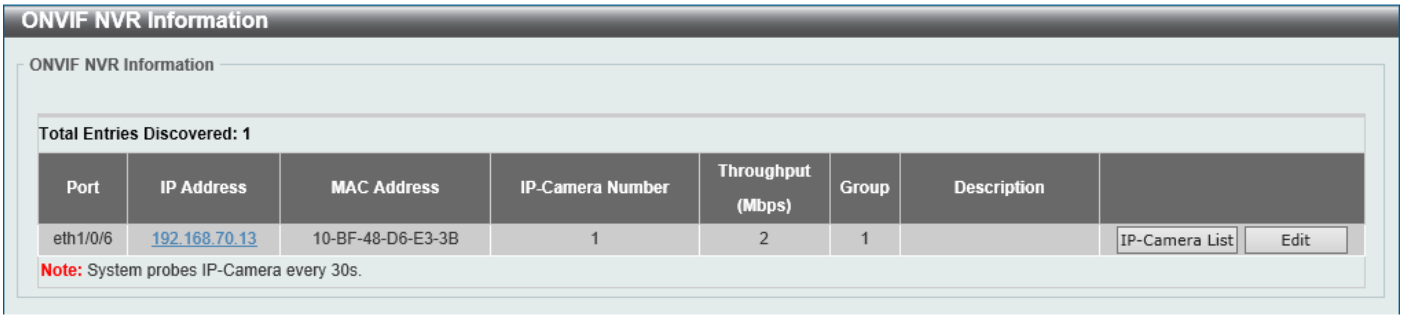
Click the **Back** button to discard the changes made and return to the previous window.

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

ONVIF NVR Information

This window is used to display ONVIF Network Video Recorder (NVR) information.

To view the following window, click **L2 Features > VLAN > Auto Surveillance VLAN > ONVIF NVR Information**, as shown below:



ONVIF NVR Information

ONVIF NVR Information

Total Entries Discovered: 1

Port	IP Address	MAC Address	IP-Camera Number	Throughput (Mbps)	Group	Description	
eth1/0/6	192.168.70.13	10-BF-48-D6-E3-3B	1	2	1		IP-Camera List Edit

Note: System probes IP-Camera every 30s.

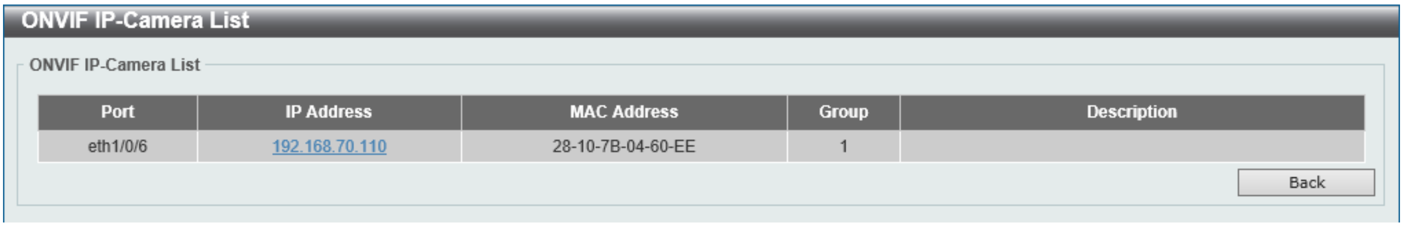
Figure 5-27 ONVIF NVR Information Window

Click the IP address hyperlink to connect to the Web Interface of the NVR.

Click the **IP-Camera List** button to view the list of IP cameras that are connected to the NVR.

Click the **Edit** button to configure the description of the NVR.

After click the **IP-Camera List** button, the following window will appear.



ONVIF IP-Camera List

ONVIF IP-Camera List

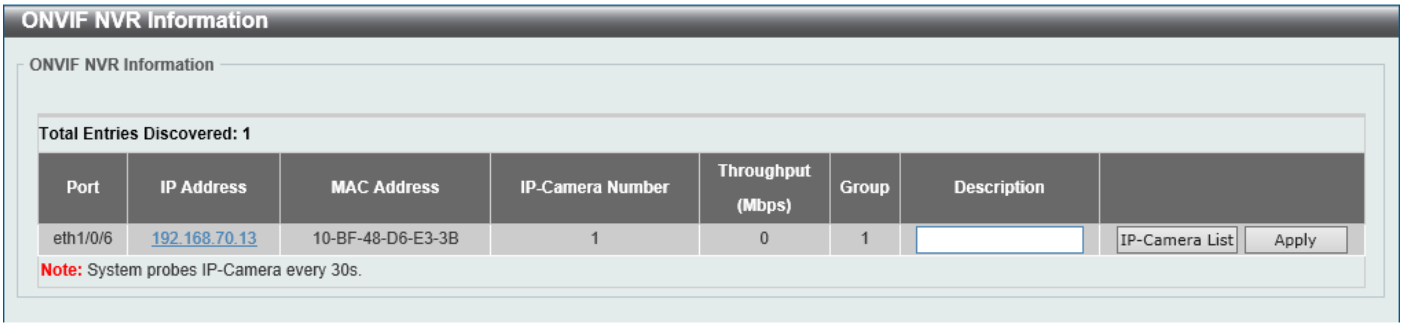
Port	IP Address	MAC Address	Group	Description
eth1/0/6	192.168.70.110	28-10-7B-04-60-EE	1	

Figure 5-28 ONVIF NVR Information (IP-Camera List) Window

Click the IP address hyperlink to connect to the Web Interface of the IP camera.

Click the **Back** button to return to the previous window.

After click the **Edit** button, the following window will appear.



ONVIF NVR Information

ONVIF NVR Information

Total Entries Discovered: 1

Port	IP Address	MAC Address	IP-Camera Number	Throughput (Mbps)	Group	Description	
eth1/0/6	192.168.70.13	10-BF-48-D6-E3-3B	1	0	1		IP-Camera List Apply

Note: System probes IP-Camera every 30s.

Figure 5-29 ONVIF NVR Information (Edit) Window

The additional fields that can be configured are described below:

Parameter	Description
Description	Enter the description for this NVR here.

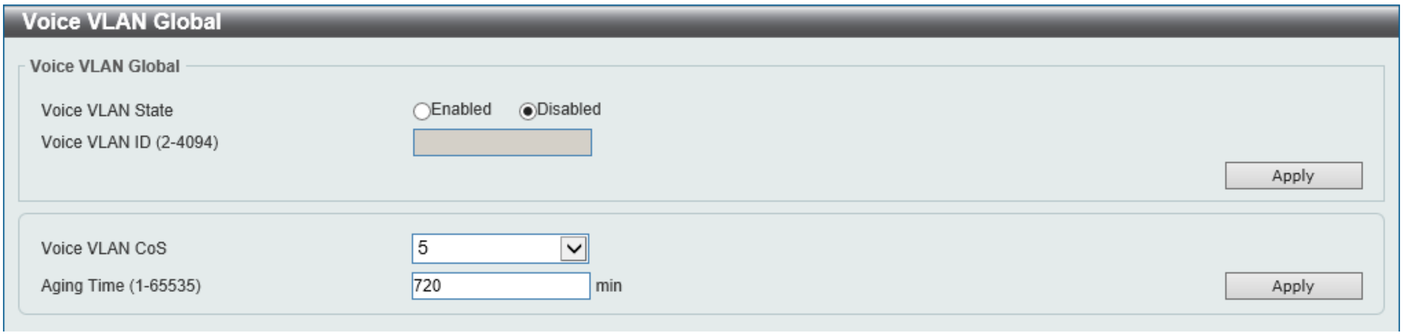
Click the **Apply** button to accept the changes made.

Voice VLAN

Voice VLAN Global

This window is used to display and configure the global voice VLAN settings. This is used to enable the global voice VLAN function and to specify the voice VLAN on the Switch. The Switch has only one voice VLAN.

To view the following window, click **L2 Features > VLAN > Voice VLAN > Voice VLAN Global**, as shown below:



Voice VLAN Global

Voice VLAN Global

Voice VLAN State ○Enabled ●Disabled

Voice VLAN ID (2-4094)

Voice VLAN CoS 5

Aging Time (1-65535) 720 min

Figure 5-30 Voice VLAN Global Window

The fields that can be configured are described below:

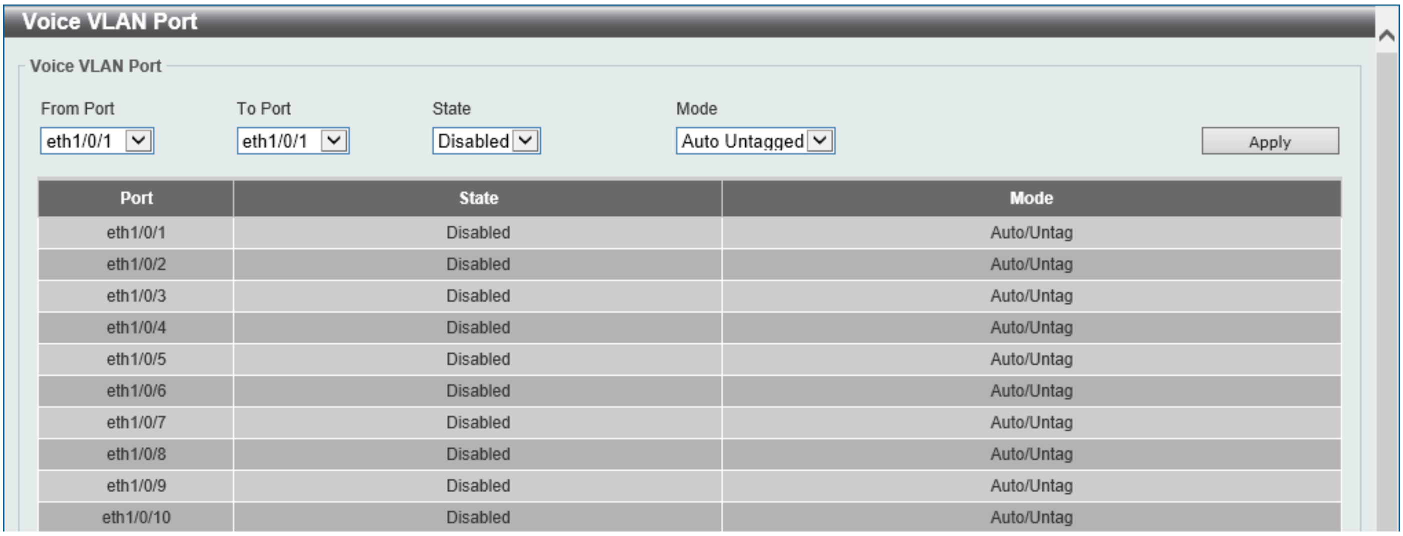
Parameter	Description
Voice VLAN State	Select to globally enable or disable the voice VLAN feature here.
Voice VLAN ID	Enter the VLAN ID of the voice VLAN here. The VLAN to be specified as the voice VLAN needs to pre-exist before configuration. The range is from 2 to 4094.
Voice VLAN CoS	Select the CoS of the voice VLAN here. The range is from 0 to 7. The voice packets arriving at the voice VLAN enabled port are marked as the CoS specified here. The remarking of CoS packets allow the voice VLAN traffic to be distinguished from data traffic in Quality of Service.
Aging Time	Enter the aging time value here. This is used to configure the aging time for aging out the automatically learned voice device and voice VLAN information. When the last voice device connected to the port stops sending traffic and the MAC address of this voice device is aged out from FDB, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after the expiration of the voice VLAN aging timer. If voice traffic resumes during the aging time, the aging timer will be cancelled. The range is from 1 to 65535 minutes.

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

Voice VLAN Port

This window is used to display and configure the voice VLAN interface settings.

To view the following window, click **L2 Features > VLAN > Voice VLAN > Voice VLAN Port**, as shown below:



From Port: eth1/0/1
To Port: eth1/0/1
State: Disabled
Mode: Auto Untagged

Port	State	Mode
eth1/0/1	Disabled	Auto/Untag
eth1/0/2	Disabled	Auto/Untag
eth1/0/3	Disabled	Auto/Untag
eth1/0/4	Disabled	Auto/Untag
eth1/0/5	Disabled	Auto/Untag
eth1/0/6	Disabled	Auto/Untag
eth1/0/7	Disabled	Auto/Untag
eth1/0/8	Disabled	Auto/Untag
eth1/0/9	Disabled	Auto/Untag
eth1/0/10	Disabled	Auto/Untag

Figure 5-31 Voice VLAN Port Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
State	Select to enable or disable the voice VLAN feature on the specified port(s) here. When the voice VLAN is enabled for a port, the received voice packets will be forwarded in the voice VLAN. The received packets are determined as voice packets if the source MAC addresses of packets complies with the OUI addresses.
Mode	Select the mode here. Options to choose from are: • **Auto Untagged** - Specifies that voice VLAN untagged membership will be automatically learned. • **Auto Tagged** - Specifies that voice VLAN tagged membership will be automatically learned. • **Manual** - Specifies that voice VLAN membership will be manually configured. If auto-learning is enabled, the port will automatically be learned as a voice VLAN member. This membership will automatically be aged out. When the port is working in the auto-tagged mode and the port captures a voice device through the device's OUI, it will join the voice VLAN as a tagged member automatically. When the voice device sends tagged packets, the Switch will change its priority. When the voice device sends untagged packets, it will forward them in the Port VLAN ID (PVID). When the port is working in auto-untagged mode, and the port captures a voice device through the device's OUI, it will join the voice VLAN as an untagged member automatically. When the voice device sends tagged packets, the Switch will change its priority. When the voice device sends untagged packets, it will forward them in the voice VLAN. When the Switch receives LLDP-MED packets, it checks the VLAN ID, tagged flag, and priority flag. The Switch should follow the tagged flag and priority setting.

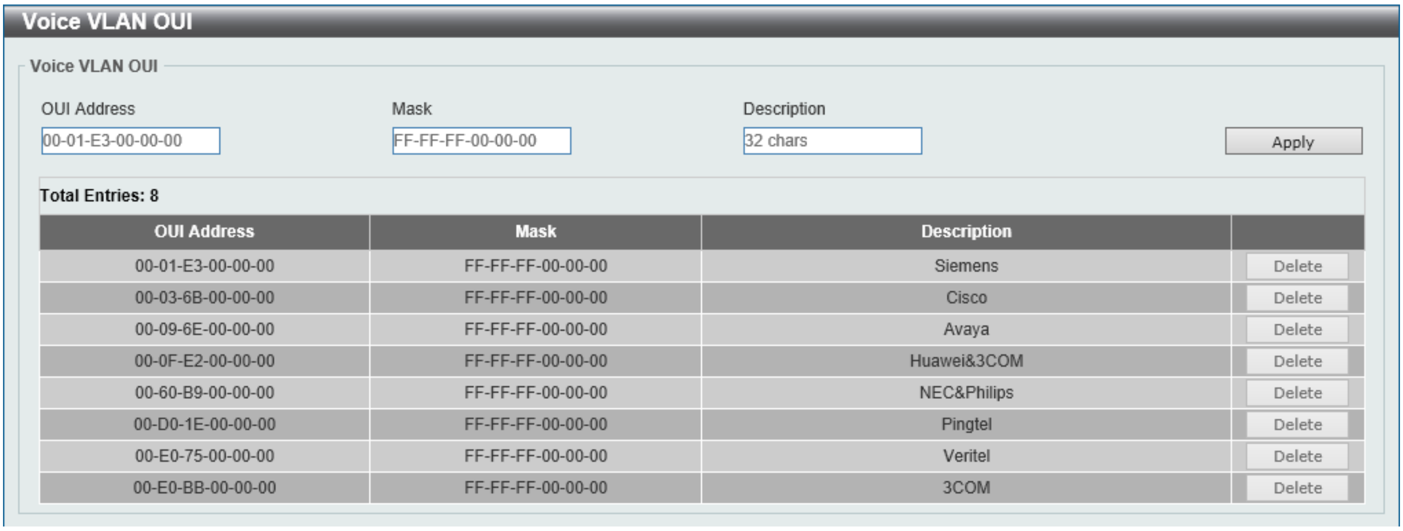
Click the **Apply** button to accept the changes made.

Voice VLAN OUI

This window is used to display and configure the voice VLAN OUI settings. Use this window to add a user-defined OUI for the voice VLAN. The OUI for the voice VLAN is used to identify the voice traffic by using the voice VLAN function. If the source MAC address of the received packet matches any of the OUI patterns, the received packet is determined as a voice packet.

The user-defined OUI cannot be the same as the default OUI. The default OUI cannot be deleted.

To view the following window, click **L2 Features > VLAN > Voice VLAN > Voice VLAN OUI**, as shown below:



Voice VLAN OUI

Voice VLAN OUI

OUI Address: 00-01-E3-00-00-00

Mask: FF-FF-FF-00-00-00

Description: 32 chars

Apply

Total Entries: 8

OUI Address	Mask	Description	
00-01-E3-00-00-00	FF-FF-FF-00-00-00	Siemens	Delete
00-03-6B-00-00-00	FF-FF-FF-00-00-00	Cisco	Delete
00-09-6E-00-00-00	FF-FF-FF-00-00-00	Avaya	Delete
00-0F-E2-00-00-00	FF-FF-FF-00-00-00	Huawei&3COM	Delete
00-60-B9-00-00-00	FF-FF-FF-00-00-00	NEC&Philips	Delete
00-D0-1E-00-00-00	FF-FF-FF-00-00-00	Pingtel	Delete
00-E0-75-00-00-00	FF-FF-FF-00-00-00	Veritel	Delete
00-E0-BB-00-00-00	FF-FF-FF-00-00-00	3COM	Delete

Figure 5-32 Voice VLAN OUI Window

The fields that can be configured are described below:

Parameter	Description
OUI Address	Enter the voice VLAN OUI MAC address here.
Mask	Enter the matching bitmask for the voice VLAN OUI MAC address here.
Description	Enter the description for the user-defined OUI MAC address here. This string can be up to 32 characters long.

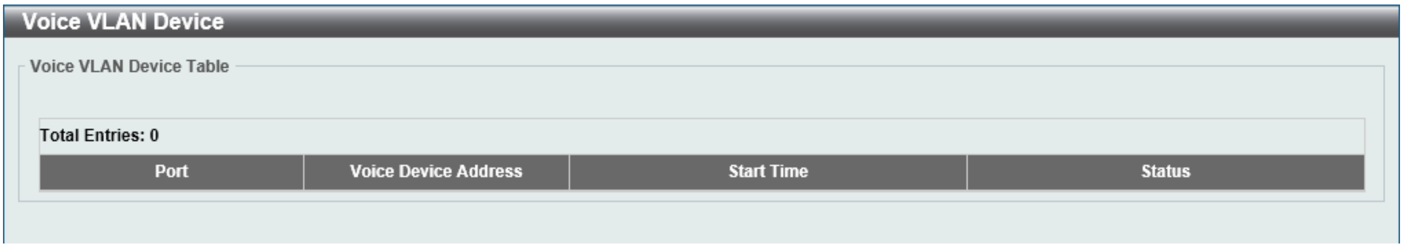
Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete the specified entry.

Voice VLAN Device

This window is used to view the voice VLAN device table.

To view the following window, click **L2 Features > VLAN > Voice VLAN > Voice VLAN Device**, as shown below:



Voice VLAN Device

Voice VLAN Device Table

Total Entries: 0

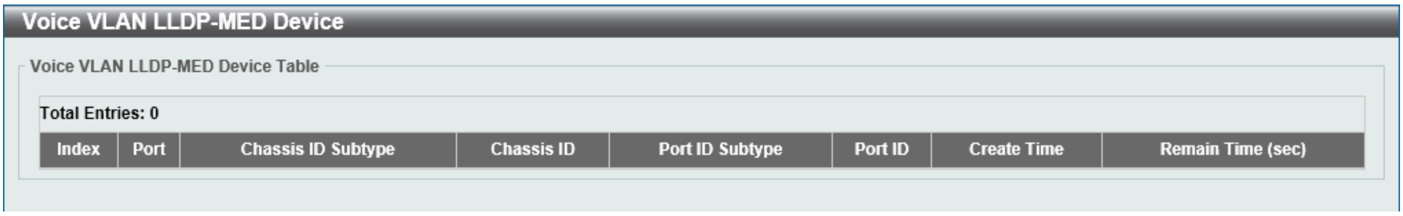
Port	Voice Device Address	Start Time	Status

Figure 5-33 Voice VLAN Device Window

Voice VLAN LLDP-MED Device

This window is used to view the voice VLAN LLDP-MED device table.

To view the following window, click **L2 Features > VLAN > Voice VLAN > Voice VLAN LLDP-MED Device**, as shown below:



Voice VLAN LLDP-MED Device

Voice VLAN LLDP-MED Device Table

Total Entries: 0

Index	Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	Create Time	Remain Time (sec)

Figure 5-34 Voice VLAN LLDP-MED Device Window

STP

This Switch supports three versions of the Spanning Tree Protocol (STP): IEEE 802.1D-1998 STP, IEEE 802.1D-2004 Rapid STP, and IEEE 802.1Q-2005 MSTP. The IEEE 802.1D-1998 STP standard will be familiar to most networking professionals. However, as IEEE 802.1D-2004 RSTP and IEEE 802.1Q-2005 MSTP have been recently introduced to D-Link managed Ethernet Switches, a brief introduction to the technology is provided below followed by a description of how to set up IEEE 802.1D-1998 STP, IEEE 802.1D-2004 RSTP, and IEEE 802.1Q-2005 MSTP.

802.1Q-2005 MSTP

The Multiple Spanning Tree Protocol (MSTP) is a standard defined by the IEEE community that allows multiple VLANs to be mapped to a single spanning tree instance, which will provide multiple pathways across the network. Therefore, these MSTP configurations will balance the traffic load, preventing wide scale disruptions when a single spanning tree instance fails. This will allow for faster convergences of new topologies for the failed instance.

Frames designated for these VLANs will be processed quickly and completely throughout interconnected bridges utilizing any of the three spanning tree protocols (STP, RSTP, or MSTP).

A Multiple Spanning Tree Instance (MSTI) ID will classify these instances. MSTP will connect multiple spanning trees with a Common and Internal Spanning Tree (CIST). The CIST will automatically determine each MSTP region, its maximum possible extent and will appear as one virtual bridge that runs a single spanning tree instance. Frames assigned to different VLANs will follow different data routes within administratively established regions on the network, continuing to allow simple and full processing of frames, regardless of administrative errors in defining VLANs and their respective spanning trees.

Each Switch utilizing the MSTP on a network will share a single MSTP configuration that will have the following three attributes:

- A configuration name defined by an alphanumeric string of up to 32 characters (defined in the **MST Configuration Identification** window in the **Configuration Name** field).
- A configuration revision number (named here as a **Revision Level** and found in the **MST Configuration Identification** window)
- A 4094-element table (defined here as a VID List in the **MST Configuration Identification** window), which will associate each of the possible 4094 VLANs supported by the Switch for a given instance.

To utilize the MSTP function on the Switch, three steps need to be taken:

- The Switch must be set to the MSTP setting (found in the **STP Global Settings** window in the **STP Mode** field).
- The correct spanning tree priority for the MSTP instance must be entered (defined here as a **Priority** in the **MSTP Port Information** window when configuring MSTI ID settings).
- VLANs that will be shared must be added to the MSTP Instance ID (defined here as a **VID List** in the **MST Configuration Identification** window when configuring an MSTI ID settings).

802.1D-2004 Rapid Spanning Tree

The Switch implements three versions of the Spanning Tree Protocol, the Multiple Spanning Tree Protocol (MSTP) as defined by IEEE 802.1Q-2005, the Rapid Spanning Tree Protocol (RSTP) as defined by IEEE 802.1D-2004 and a version compatible with IEEE 802.1D-1998. RSTP can operate with legacy equipment implementing IEEE 802.1D-1998; however, the advantages of using RSTP will be lost. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

Port Transition States

An essential difference between the three protocols is in the way ports transition to a forwarding state and in the way, this transition relates to the role of the port (forwarding or not forwarding) in the topology. MSTP and RSTP combine the transition states Disabled, Blocking, and Listening used in 802.1D-1998 and creates a single state called Discarding. In either case, ports do not forward packets. In the STP port, transition states Disabled, Blocking or Listening or in the RSTP/MSTP port state Discarding, there is no functional difference, the port is not active in the network topology. Table 7-3 below compares how the three protocols differ regarding the port state transition.

All three protocols calculate a stable topology in the same way. Every segment will have a single path to the root bridge. All bridges listen for BPDU packets. However, BPDU packets are sent more frequently, with every 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 therefore faster topology adjustment. A drawback of IEEE 802.1D-1998 is this absence of immediate feedback from adjacent bridges.

802.1Q-2005 MSTP	802.1D-2004 RSTP	802.1D-1998 STP	Forwarding	Learning
Disabled	Disabled	Disabled	No	No
Discarding	*Discarding*	*Blocking*	No	No
Discarding	*Discarding*	*Listening*	No	No
Learning	*Learning*	*Learning*	No	**Yes**
Forwarding	**Forwarding**	**Forwarding**	**Yes**	**Yes**

RSTP is capable of a more rapid transition to the Forwarding state. RSTP no longer relies on timer configurations and RSTP-compliant bridges are sensitive to feedback from other RSTP-compliant bridge links. Ports do not need to wait for the topology to stabilize before transitioning to a Forwarding state. In order to allow this rapid transition, the protocol introduces two new variables: the Edge Port and the Point-to-Point (P2P) port.

Edge Port

A port can be configured as an Edge Port if it is directly connected to a segment where a loop cannot be created. An example would be a port connected directly to a single workstation. Ports that are designated as edge ports transition to a forwarding state immediately without going through the Listening and Learning states. An Edge Port loses its status if it receives a BPDU packet, after which it immediately becomes a normal spanning tree port.

P2P Port

A P2P port is also capable of rapid transition. P2P ports may be used to connect to other bridges. Under RSTP/MSTP, all ports operating in full-duplex mode are considered to be P2P ports unless manually overridden through configuration.

802.1D-1998/802.1D-2004/802.1Q-2005 Compatibility

MSTP or RSTP can interoperate with legacy equipment and are capable of automatically adjusting BPDU packets to 802.1D-1998 format when necessary. However, any segment using 802.1D-1998 STP will not benefit from the rapid transition and rapid topology change detection of MSTP or RSTP. The protocol also includes a variable used for migration in the event that legacy equipment on a segment is updated to use RSTP or MSTP.

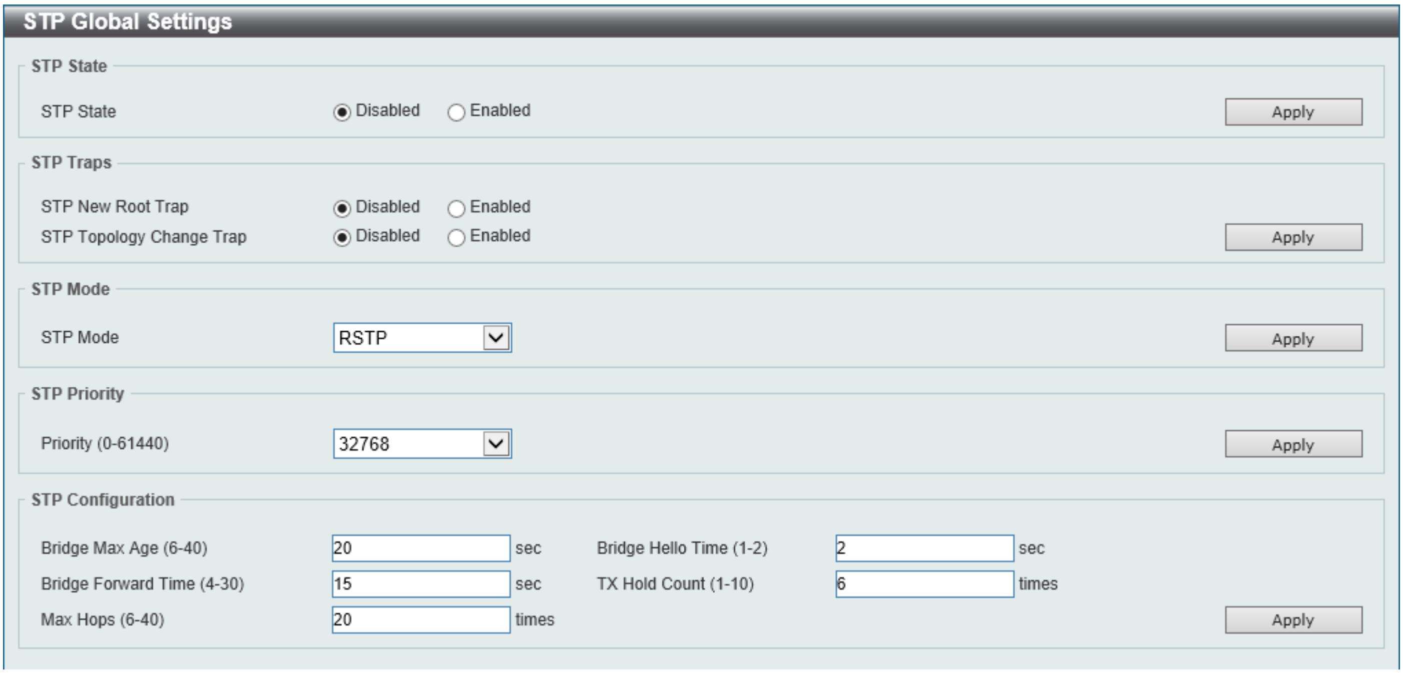
The Spanning Tree Protocol (STP) operates on two levels:

- On the Switch level, the settings are globally implemented.
- On the port level, the settings are implemented on a user-defined group of ports.

STP Global Settings

This window is used to display and configure the global STP settings.

To view the following window, click **L2 Features > STP > STP Global Settings**, as shown below:



STP Global Settings

STP State

STP State: ● Disabled ○ Enabled

STP Traps

STP New Root Trap: ● Disabled ○ Enabled

STP Topology Change Trap: ● Disabled ○ Enabled

STP Mode

STP Mode: RSTP

STP Priority

Priority (0-61440): 32768

STP Configuration

Bridge Max Age (6-40): 20 sec

Bridge Hello Time (1-2): 2 sec

Bridge Forward Time (4-30): 15 sec

TX Hold Count (1-10): 6 times

Max Hops (6-40): 20 times

Figure 5-35 STP Global Settings Window

The field that can be configured for **STP State** is described below:

Parameter	Description
STP State	Select to enable or disable the global STP state here.

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

The fields that can be configured for **STP Traps** are described below:

Parameter	Description
STP New Root Trap	Select to enable or disable the STP New Root Trap option here.
STP Topology Change Trap	Select to enable or disable the STP Topology Change Trap option here.

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

The fields that can be configured for **STP Mode** are described below:

Parameter	Description
STP Mode	Select the STP mode used here. Options to choose from are **MSTP**, **RSTP**, and **STP**.

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

The fields that can be configured for **STP Priority** are described below:

Parameter	Description
Priority	Select the STP priority value here. This value is between 0 and 61440. By default, this value is 32768. The lower the value, the higher the priority.

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

The fields that can be configured for **STP Configuration** are described below:

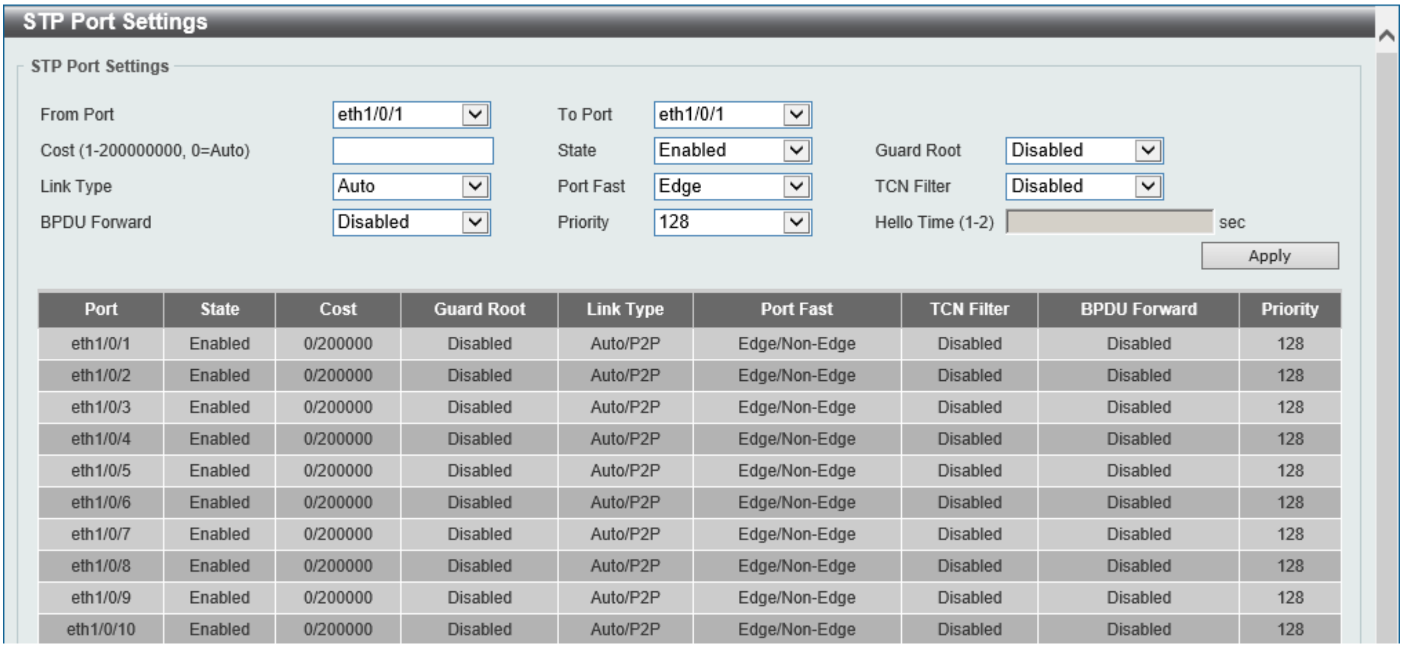
Parameter	Description
Bridge Max Age	Enter the bridge Maximum Age value here. This value must be between 6 and 40 seconds. By default, this value is 20 seconds. The Maximum Age value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing 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.
Bridge Hello Time	After selecting **RSTP/STP** as the **Spanning Tree Mode**, this parameter will be available. Enter the bridge Hello Time value here. This value must be between 1 and 2 seconds. By default, this value is 2 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge. This field will only appear here when STP or RSTP is selected for the STP version. For MSTP, the Hello Time must be set on a port per-port basis.
Bridge Forward Time	Enter the bridge Forwarding Time value here. This value must be between 4 and 30 seconds. By default, this value is 15 seconds. Every port on the Switch spends this time in the Listening state while moving from the Blocking state to the Forwarding state.
TX Hold Count	Enter the Transmit Hold Count value here. This value must be between 1 and 10 times. By default, this value is 6 times. This value is used to set the maximum number of Hello packets transmitted per interval.
Max Hops	Enter the maximum number of hops that are allowed. This value must be between 6 and 40 hops. By default, this value is 20 hops. This value is used to set the number of hops between devices in a spanning tree region before the Bridge Protocol Data Unit (BPDU) 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 BDPU packet and the information held for the port will age out.

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

STP Port Settings

This window is used to display and configure the STP port settings.

To view the following window, click **L2 Features > STP > STP Port Settings**, as shown below:



STP Port Settings

STP Port Settings

From Port	eth1/0/1	To Port	eth1/0/1		
Cost (1-200000000, 0=Auto)		State	Enabled	Guard Root	Disabled
Link Type	Auto	Port Fast	Edge	TCN Filter	Disabled
BPDU Forward	Disabled	Priority	128	Hello Time (1-2)	sec

Port	State	Cost	Guard Root	Link Type	Port Fast	TCN Filter	BPDU Forward	Priority
eth1/0/1	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
eth1/0/2	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
eth1/0/3	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
eth1/0/4	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
eth1/0/5	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
eth1/0/6	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
eth1/0/7	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
eth1/0/8	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
eth1/0/9	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128
eth1/0/10	Enabled	0/200000	Disabled	Auto/P2P	Edge/Non-Edge	Disabled	Disabled	128

Figure 5-36 STP Port Settings Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
Cost	Enter the cost value here. This value must be between 1 and 200000000. This value 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). 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. The default port cost for a 100Mbps port is 200000, a Gigabit port is 20000, and a 10 Gigabit port is 2000. The lower the number, the greater the probability the port will be chosen to forward packets.
State	Select to enable or disable the STP port state.
Guard Root	Select to enable or disable the Guard Root function.
Link Type	Select the link type here. Options to choose from are **Auto**, **P2P**, and **Shared**. A full-duplex port is considered to have a Point-to-Point (**P2P**) connection. The port cannot transit into the forwarding state rapidly by setting the link type to **Shared**. By default, this option is **Auto**.
Port Fast	Select the Port Fast option here. Options to choose from are: • In the **Network** mode, the port will remain in the non-port-fast state for three seconds. The port will change to the port-fast state if no BPDU is received and changes to the forwarding state. If the port received the BPDU later, it will change to the non-port-fast state. • In the **Disable** mode, the port will always be in the non-port-fast state. It will always wait for the forward-time delay to change to the forwarding state. • In the **Edge** mode, the port will directly change to the spanning-tree forwarding state when a link-up occurs without waiting for the forward-time delay. If the interface receives a BPDU later, its operation state changes to the non-port-fast state. This is the default option.

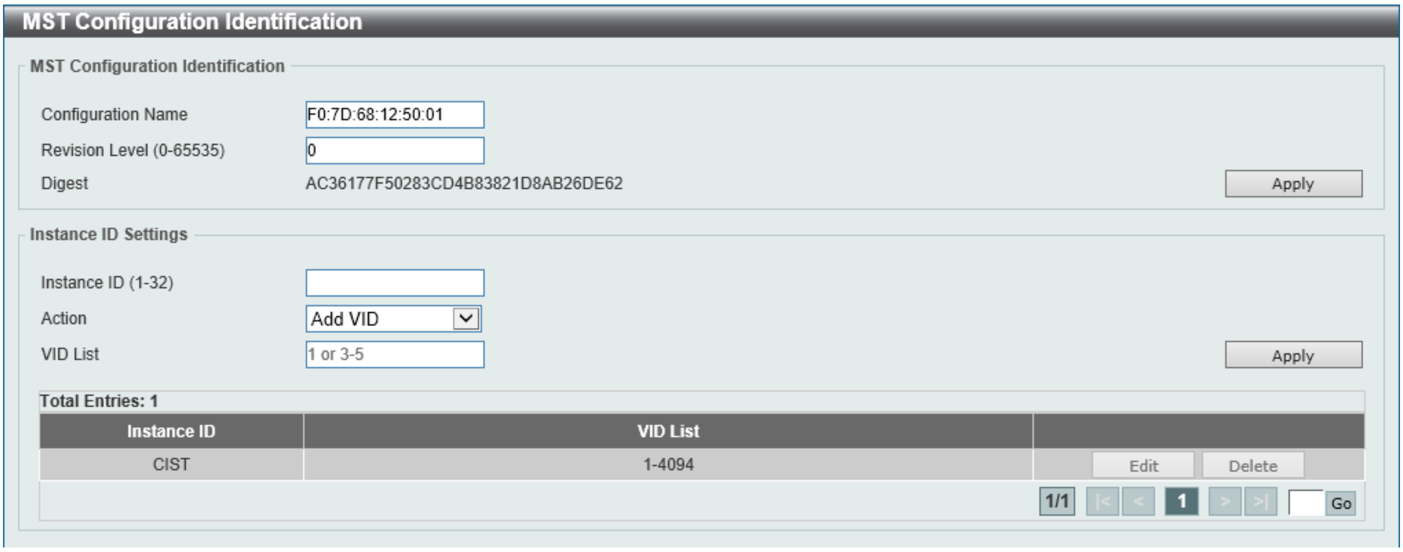
Parameter	Description
TCN Filter	Select to enable or disable the TCN Filter option. When a port is set to the TCN filter mode, the TC event received by the port will be ignored. By default, this option is **Disabled**.
BPDU Forward	Select to enable or disable BPDU forwarding. If enabled, the received STP BPDU will be forwarded to all VLAN member ports in the untagged form. By default, this option is **Disabled**.
Priority	Select the priority value here. Options to choose from are **0** to **240**. By default, this option is **128**. A lower value has higher priority.
Hello Time	Enter the hello time value here. This value must be between **1** and **2** seconds. This value specifies the interval that a designated port will wait between the periodic transmissions of each configuration message.

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

MST Configuration Identification

This window is used to display and configure the MST configuration identification settings. These settings will uniquely identify an MSTI configured on the Switch. The Switch initially possesses one Common Internal Spanning Tree (CIST) of which the user may modify the parameters for but cannot change or delete the MSTI ID.

To view the following window, click **L2 Features > STP > MST Configuration Identification**, as shown below:



MST Configuration Identification

MST Configuration Identification

Configuration Name: F0:7D:68:12:50:01

Revision Level (0-65535): 0

Digest: AC36177F50283CD4B83821D8AB26DE62

Instance ID Settings

Instance ID (1-32):

Action: Add VID

VID List: 1 or 3-5

Total Entries: 1

Instance ID	VID List	
CIST	1-4094	Edit Delete

Figure 5-37 MST Configuration Identification Window

The fields that can be configured for **MST Configuration Identification** are described below:

Parameter	Description
Configuration Name	Enter the MST. This name uniquely identifies 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.
Revision Level	Enter the revision level value here. This value must be between 0 and 65535. By default, this value is 0. This value, along with the Configuration Name, identifies the MSTP region configured on the Switch.

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

The fields that can be configured for **Instance ID Settings** are described below:

Parameter	Description
Instance ID	Enter the instance ID here. This value must be between 1 and 32.
Action	Select the action that will be taken here. Options to choose from are **Add VID** and **Remove VID**.
VID List	Enter the VID list value here. This field is used to specify the VID range from configured VLANs set on the Switch.

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

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

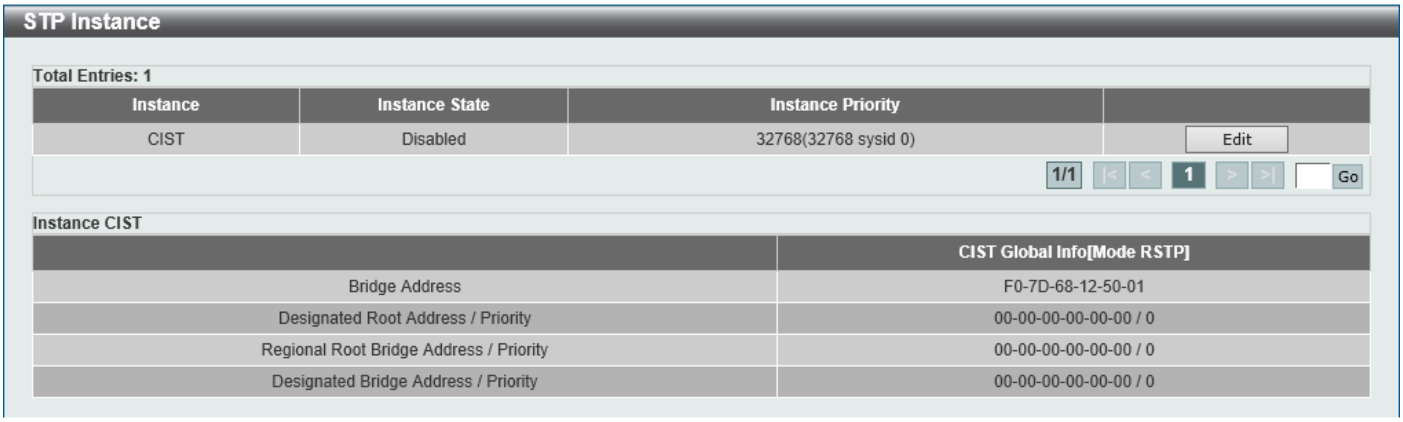
Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

STP Instance

This window is used to display and configure the STP instance settings.

To view the following window, click **L2 Features > STP > STP Instance**, as shown below:



STP Instance

Total Entries: 1

Instance	Instance State	Instance Priority	
CIST	Disabled	32768(32768 sysid 0)	Edit

Instance CIST

	CIST Global Info[Mode RSTP]
Bridge Address	F0-7D-68-12-50-01
Designated Root Address / Priority	00-00-00-00-00-00 / 0
Regional Root Bridge Address / Priority	00-00-00-00-00-00 / 0
Designated Bridge Address / Priority	00-00-00-00-00-00 / 0

Figure 5-38 STP Instance Window

The fields that can be configured are described below:

Parameter	Description
Instance Priority	After clicking the **Edit** button, enter the Instance Priority value here. The range is from 0 to 61440.

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

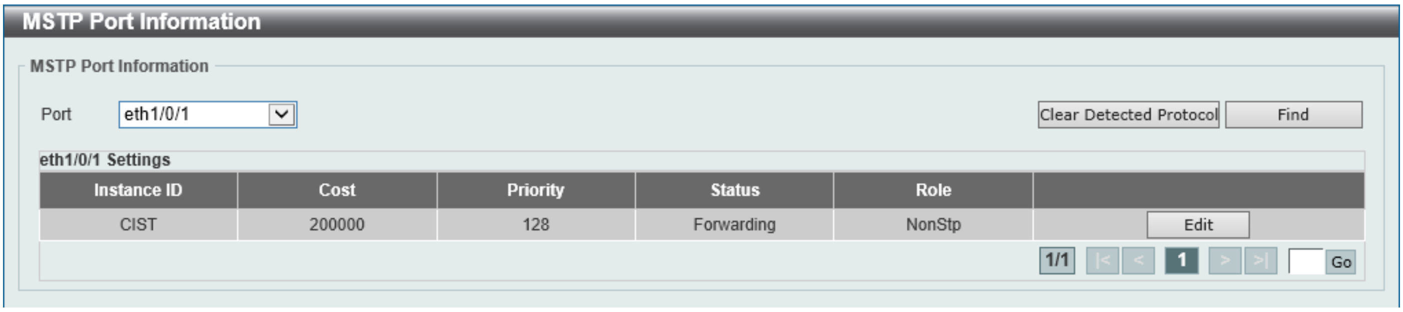
Click the **Apply** button to accept the changes made.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

MSTP Port Information

This window is used to display and configure the MSTP port information settings.

To view the following window, click **L2 Features > STP > MSTP Port Information**, as shown below:



Instance ID	Cost	Priority	Status	Role	
CIST	200000	128	Forwarding	NonStp	Edit

Figure 5-39 MSTP Port Information Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the port number that will be cleared here.
Cost	After clicking the **Edit** button, enter the cost value here. This value must be between 1 and 200000000.
Priority	After clicking the **Edit** button, select the priority value here. Options to choose from are **0** to **240**. By default, this option is **0**. A lower value has higher priority.

Click the **Clear Detected Protocol** button to clear the detected protocol settings for the port selected.

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

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

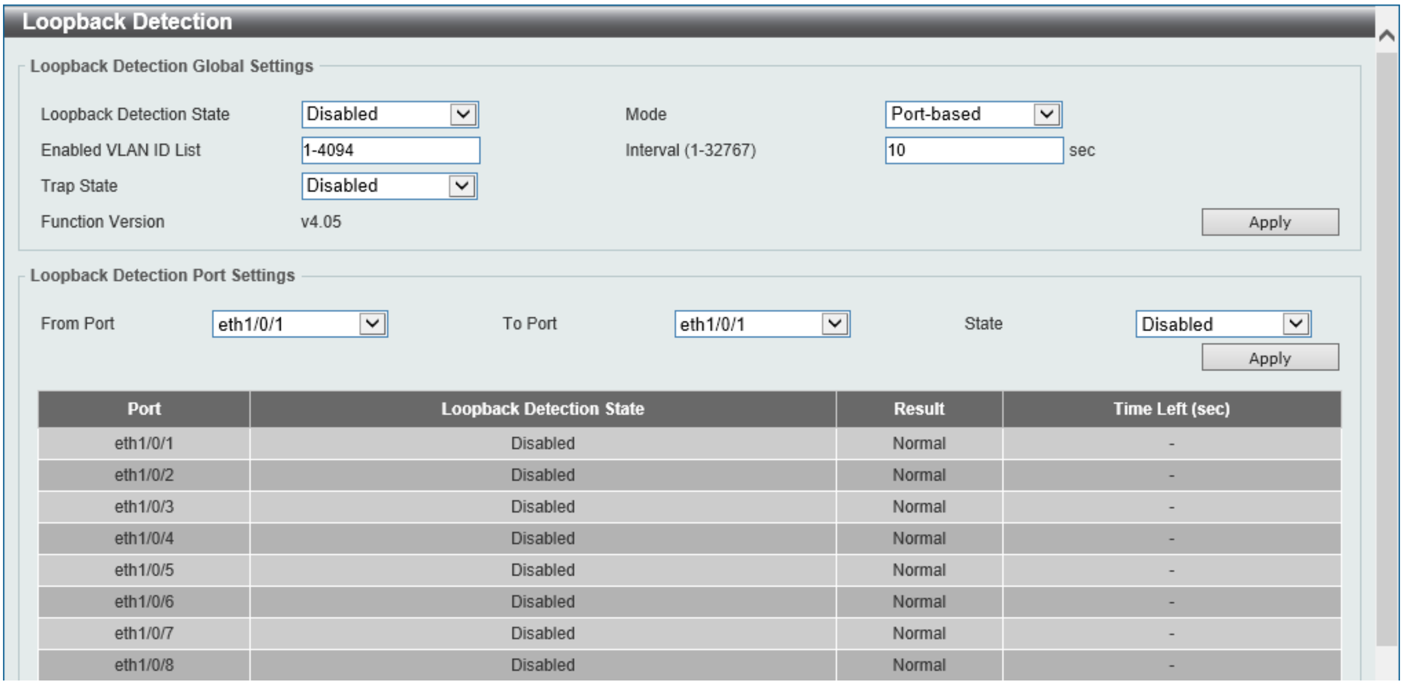
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Loopback Detection

The Loopback Detection (LBD) function is used to detect the loop created by a specific port. This feature is used to temporarily shut down a port on the Switch when a CTP (Configuration Testing Protocol) packet has been looped back to the Switch. When the Switch detects CTP packets received from a port or a VLAN, this signifies a loop on the network. The Switch will automatically block the port or the VLAN and send an alert to the administrator. The Loopback Detection port will restart (change to normal state) when the Loopback Detection Recover Time times out.

The Loopback Detection function can be implemented on a range of ports at a time. The user may enable or disable this function using the drop-down menu.

To view the following window, click **L2 Features > Loopback Detection**, as shown below:



Loopback Detection

Loopback Detection Global Settings

Loopback Detection State: Disabled
Mode: Port-based
Enabled VLAN ID List: 1-4094
Interval (1-32767): 10 sec
Trap State: Disabled
Function Version: v4.05

Loopback Detection Port Settings

From Port: eth1/0/1
To Port: eth1/0/1
State: Disabled

Port	Loopback Detection State	Result	Time Left (sec)
eth1/0/1	Disabled	Normal	-
eth1/0/2	Disabled	Normal	-
eth1/0/3	Disabled	Normal	-
eth1/0/4	Disabled	Normal	-
eth1/0/5	Disabled	Normal	-
eth1/0/6	Disabled	Normal	-
eth1/0/7	Disabled	Normal	-
eth1/0/8	Disabled	Normal	-

Figure 5-40 Loopback Detection Window

The fields that can be configured in **Loopback Detection Global Settings** are described below:

Parameter	Description
Loopback Detection State	Select to enable or disable loopback detection. The default is **Disabled**.
Mode	Select the loopback detection mode. Options to choose from are **Port-based** and **VLAN-based**.
Enabled VLAN ID List	Enter the VLAN ID for loop detection. This only takes effect when **VLAN-based** is selected in the **Mode** drop-down list.
Interval	Enter the interval in seconds that the device will use to transmit Configuration Test Protocol (CTP) packets to detect a loopback event. The valid range is from 1 to 32767 seconds. The default setting is 10 seconds.
Trap State	Select to enable or disable the loopback detection trap state.

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

The fields that can be configured in **Loopback Detection Port Settings** are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select this option to enable or disable the state of the port.

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

Link Aggregation

Understanding Port Trunk Groups

Port trunk groups are used to combine a number of ports together to make a single high-bandwidth data pipeline. The Switch supports up to 8 port trunk groups with up to 8 ports in each group.

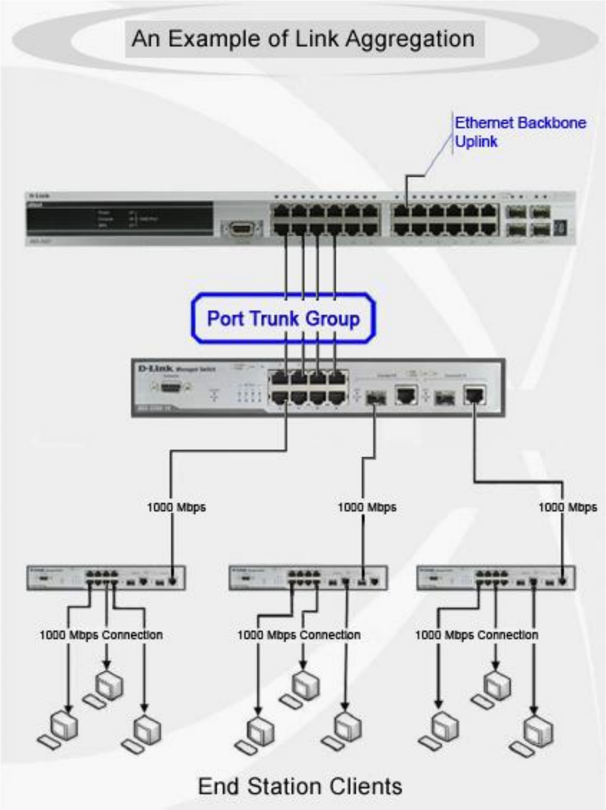


Figure 5-41 Example of Port Trunk Group

The Switch treats all ports in a trunk group as a single port. Data transmitted to a specific host (destination address) will always be transmitted over the same port in a trunk group. This allows packets in a data stream to arrive in the same order they were sent.

Link aggregation allows several ports to be grouped together and to act as a single link. This results in a bandwidth that is a multiple of a single link's bandwidth.

Link aggregation is most commonly used to link bandwidth intensive network devices, such as servers, to the backbone of a network.

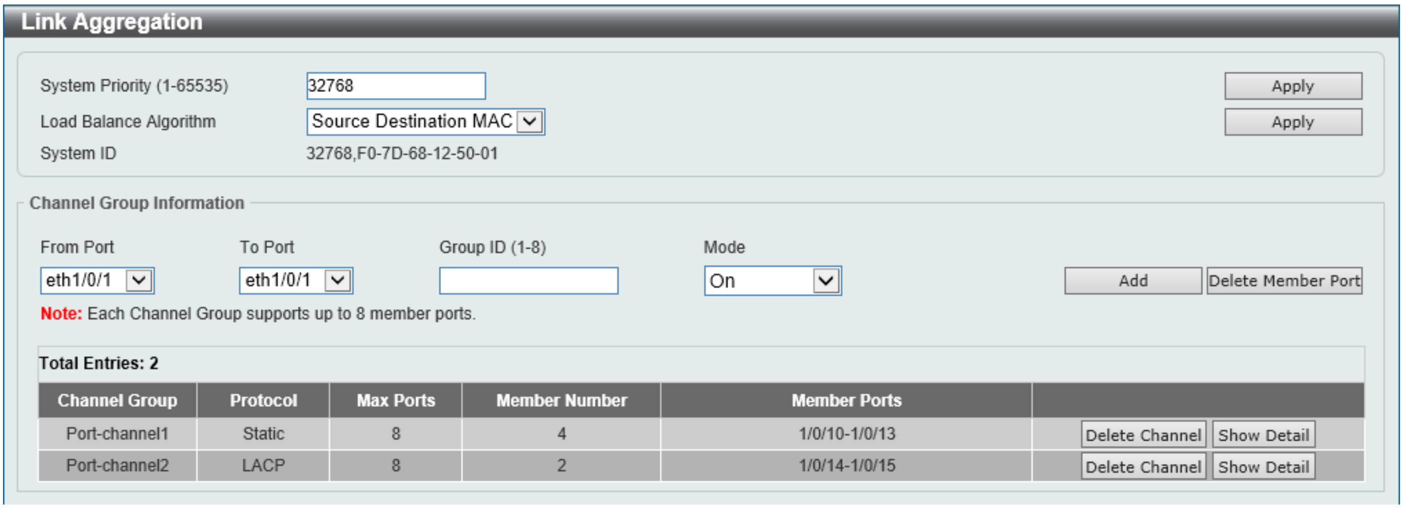
The Switch allows the creation of up to 8 link aggregation groups, each group consisting of up to 8 links (ports). Each port can only belong to a single link aggregation group.

Load balancing is automatically applied to the ports in the aggregated group, and a link failure within the group causes the network traffic to be directed to the remaining links in the group.

The Spanning Tree Protocol will treat a link aggregation group as a single link. If two redundant link aggregation groups are configured on the Switch, STP will block one entire group; in the same way, STP will block a single port that has a redundant link.

NOTE: If any ports within the trunk group become disconnected, packets intended for the disconnected port will be load shared among the other linked ports of the link aggregation group.

This window is used to display and configure the link aggregation settings. To view the following window, click **L2 Features > Link Aggregation**, as shown below:



System Priority (1-65535): 32768

Load Balance Algorithm: Source Destination MAC

System ID: 32768,F0-7D-68-12-50-01

Channel Group Information

From Port: eth1/0/1

To Port: eth1/0/1

Group ID (1-8):

Mode: On

Note: Each Channel Group supports up to 8 member ports.

Total Entries: 2

Channel Group	Protocol	Max Ports	Member Number	Member Ports	
Port-channel1	Static	8	4	1/0/10-1/0/13	Delete Channel Show Detail
Port-channel2	LACP	8	2	1/0/14-1/0/15	Delete Channel Show Detail

Figure 5-42 Link Aggregation Window

The fields that can be configured for **Link Aggregation** are described below:

Parameter	Description
System Priority	Enter the system priority value used here. This value must be between 1 and 65535. By default, this value is 32768. The system priority determines which ports can join a port-channel and which ports are put in the stand-alone mode. The lower value has a higher priority. If two or more ports have the same priority, the port number determines the priority.
Load Balance Algorithm	Select the load-balancing algorithm that will be used here. Options to choose from are **Source MAC**, **Destination MAC**, **Source Destination MAC**, **Source IP**, **Destination IP**, and **Source Destination IP**. By default, this option is **Source Destination MAC**.

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

The fields that can be configured for **Channel Group Information** are described below:

Parameter	Description
From Port - To Port	Select the list of ports that will be associated with this configuration here.
Group ID	Enter the channel group number here. This value must be between 1 and 8. The system will automatically create the port-channel when a physical port first joins a channel group. An interface can only join one channel-group.
Mode	Select the mode option here. Options to choose from are **On**, **Active**, and **Passive**. If the mode **On** is specified, the channel group type is static. If the mode **Active** or **Passive** is specified, the channel group type is LACP. A channel group can only consist of either static members or LACP members. Once the type of channel group has been determined, other types of interfaces cannot join the channel group.

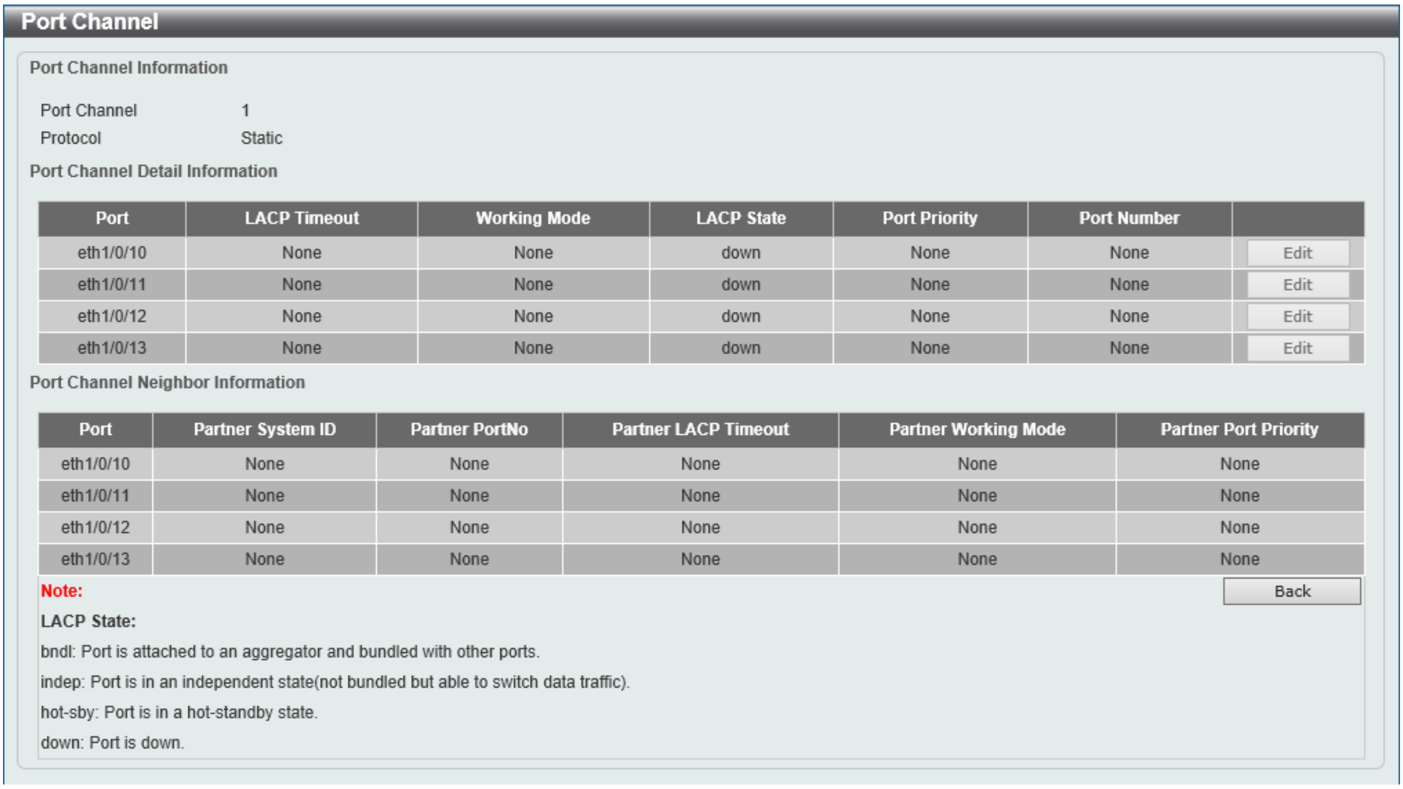
Click the **Add** button to add a new channel group.

Click the **Delete Member Port** button, to delete the member port(s) specified from the group.

Click the **Delete Channel** button to delete the specified channel group.

Click the **Show Detail** button to view detailed information about the channel.

After clicking the **Show Detail** button at an entry that uses the ***Static* Protocol**, the following page will be available.



Port Channel

Port Channel Information

Port Channel 1
Protocol Static

Port Channel Detail Information

Port	LACP Timeout	Working Mode	LACP State	Port Priority	Port Number	
eth1/0/10	None	None	down	None	None	Edit
eth1/0/11	None	None	down	None	None	Edit
eth1/0/12	None	None	down	None	None	Edit
eth1/0/13	None	None	down	None	None	Edit

Port Channel Neighbor Information

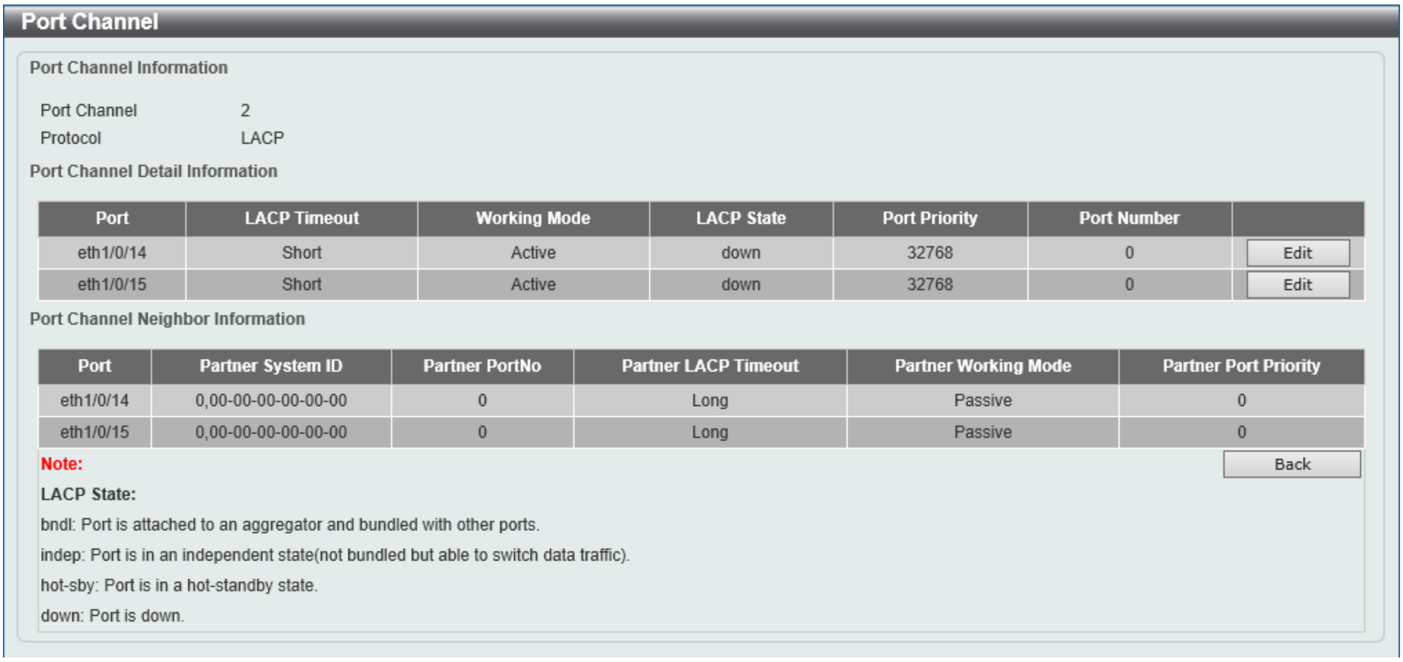
Port	Partner System ID	Partner PortNo	Partner LACP Timeout	Partner Working Mode	Partner Port Priority
eth1/0/10	None	None	None	None	None
eth1/0/11	None	None	None	None	None
eth1/0/12	None	None	None	None	None
eth1/0/13	None	None	None	None	None

Note:
LACP State:
bndl: Port is attached to an aggregator and bundled with other ports.
indep: Port is in an independent state(not bundled but able to switch data traffic).
hot-sby: Port is in a hot-standby state.
down: Port is down.

Figure 5-43 Link Aggregation (Channel 1 Detail) Window

Click the **Back** button to return to the previous page.

After clicking the **Show Detail** button at an entry that uses the ***LACP* Protocol**, the following page will be available.



Port Channel

Port Channel Information

Port Channel 2
Protocol LACP

Port Channel Detail Information

Port	LACP Timeout	Working Mode	LACP State	Port Priority	Port Number	
eth1/0/14	Short	Active	down	32768	0	Edit
eth1/0/15	Short	Active	down	32768	0	Edit

Port Channel Neighbor Information

Port	Partner System ID	Partner PortNo	Partner LACP Timeout	Partner Working Mode	Partner Port Priority
eth1/0/14	0,00-00-00-00-00-00	0	Long	Passive	0
eth1/0/15	0,00-00-00-00-00-00	0	Long	Passive	0

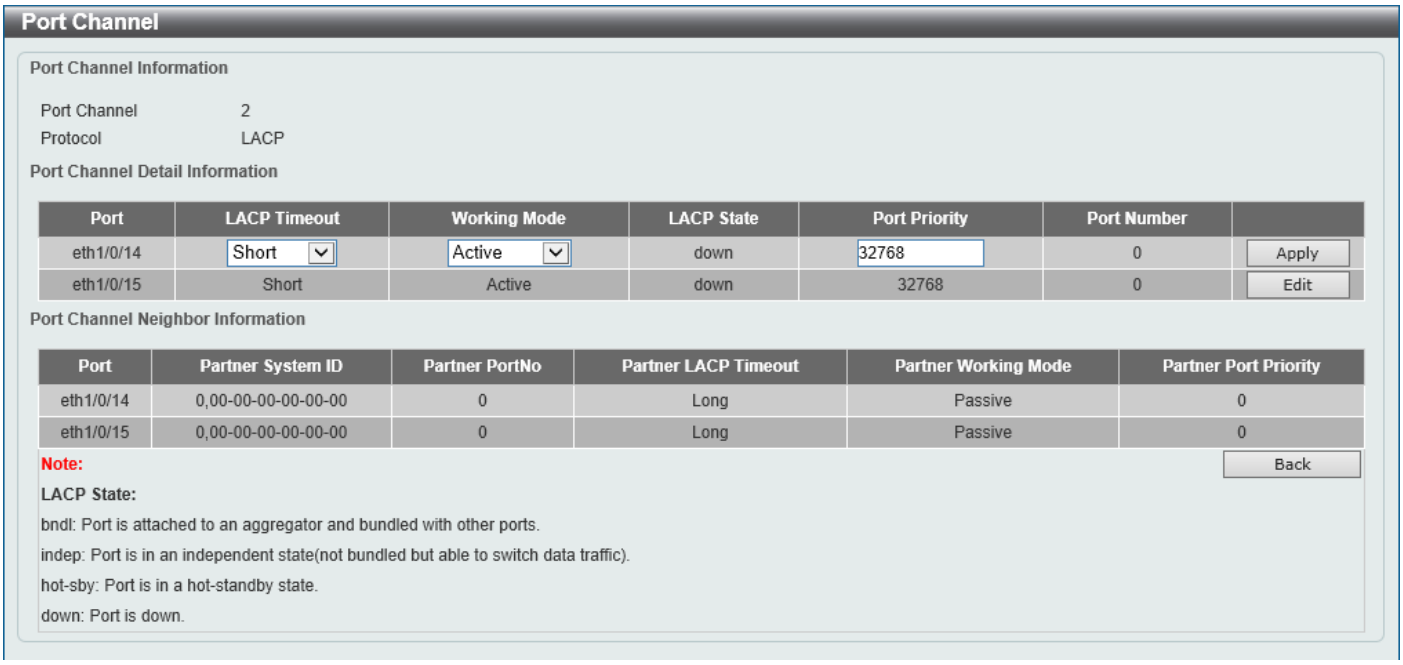
Note:
LACP State:
bndl: Port is attached to an aggregator and bundled with other ports.
indep: Port is in an independent state(not bundled but able to switch data traffic).
hot-sby: Port is in a hot-standby state.
down: Port is down.

Figure 5-44 Link Aggregation (Channel 2 Detail) Window

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

Click the **Back** button to return to the previous page.

After clicking the **Edit** button, the following page will be available.



Port Channel

Port Channel Information

Port Channel	2
Protocol	LACP

Port Channel Detail Information

Port	LACP Timeout	Working Mode	LACP State	Port Priority	Port Number	
eth1/0/14	Short	Active	down	32768	0	Apply
eth1/0/15	Short	Active	down	32768	0	Edit

Port Channel Neighbor Information

Port	Partner System ID	Partner PortNo	Partner LACP Timeout	Partner Working Mode	Partner Port Priority
eth1/0/14	0,00-00-00-00-00-00	0	Long	Passive	0
eth1/0/15	0,00-00-00-00-00-00	0	Long	Passive	0

Note:

LACP State:

bndl: Port is attached to an aggregator and bundled with other ports.

indep: Port is in an independent state(not bundled but able to switch data traffic).

hot-sby: Port is in a hot-standby state.

down: Port is down.

Figure 5-45 Link Aggregation (Channel 2 Detail, Edit) Window

The fields that can be configured are described below:

Parameter	Description
LACP Timeout	Select the LACP timeout option here. Options to choose from are: • **Short** - Specifies that there is 3 seconds before received LACPDU information is declared as invalid. Once the partner recognizes the information in the received PDU, periodic transmissions of LACP PDUs are sent at 1-second intervals on the interface. This is the default option. • **Long** - Specifies that there is 90 seconds before received LACPDU information is declared as invalid. Once the partner recognizes the information in the received PDU, periodic transmissions of LACP PDUs are sent at 30-second intervals on the interface.
Working Mode	Select the working mode here. Options to choose from are: • **Passive** - Specifies to operate in the LACP passive mode. • **Active** - Specifies to operate in the LACP active mode.
Port Priority	Enter the port priority value here. This determines which port can join the port-channel and which port operates in the stand-alone mode. A lower value carries a higher priority. The range is from 1 to 65535. By default, this value is 32768.

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

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

Click the **Back** button to return to the previous page.

L2 Multicast Control

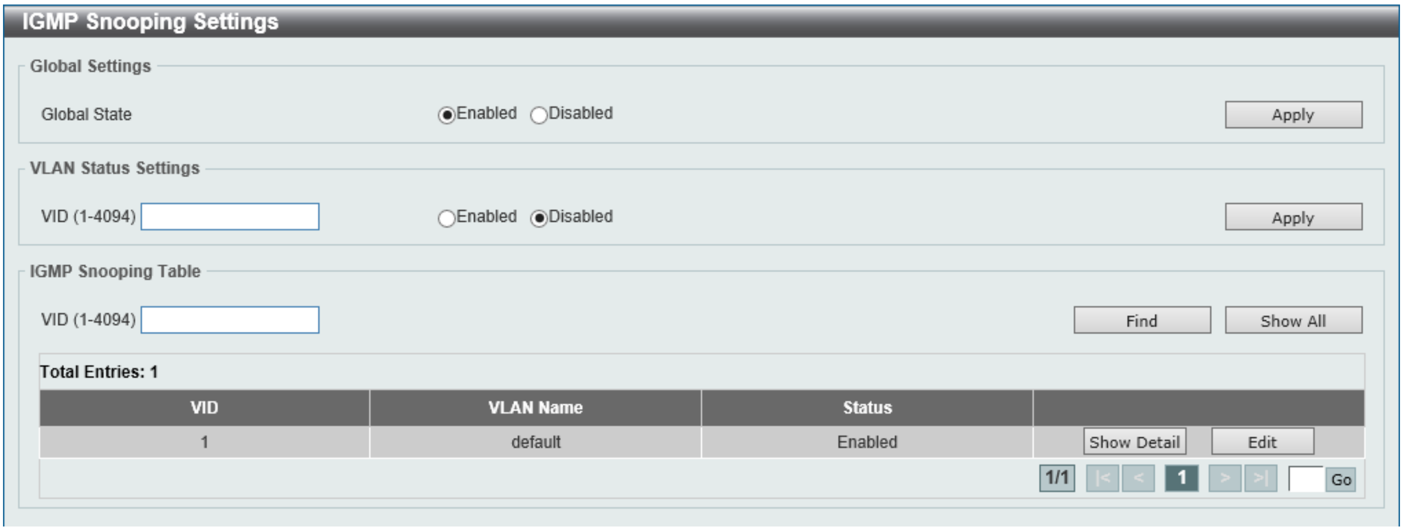
IGMP Snooping

Internet Group Management Protocol (IGMP) snooping allows the Switch to recognize IGMP queries and reports sent between network stations or devices and an IGMP host.

IGMP Snooping Settings

In order to use IGMP Snooping it must first be enabled for the entire Switch under IGMP **Global Settings** at the top of the window. You may then fine-tune the settings for each VLAN by clicking the corresponding **Edit** button. When enabled for IGMP snooping, the Switch can open or close a port to a specific multicast group member based on IGMP messages sent from the device to the IGMP host or vice versa. The Switch monitors IGMP messages and discontinues forwarding multicast packets when there are no longer hosts requesting that they continue.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Settings**, as shown below:



IGMP Snooping Settings

Global Settings

Global State ● Enabled ○ Disabled

VLAN Status Settings

VID (1-4094) ○ Enabled ● Disabled

IGMP Snooping Table

VID (1-4094)

Total Entries: 1

VID	VLAN Name	Status	
1	default	Enabled	Show Detail Edit

Figure 5-46 IGMP Snooping Settings Window

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

Parameter	Description
Global State	Select to globally enable or disable IGMP snooping here. By default, this is disabled.

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

The fields that can be configured in **VLAN Status Settings** are described below:

Parameter	Description
VID	Enter the VLAN ID here. The range is from 1 to 4094. Select to enable or disable IGMP snooping on the VLAN.

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

The fields that can be configured in **IGMP Snooping Table** are described below:

Parameter	Description
VID	Enter the VLAN ID from 1 to 4094.

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

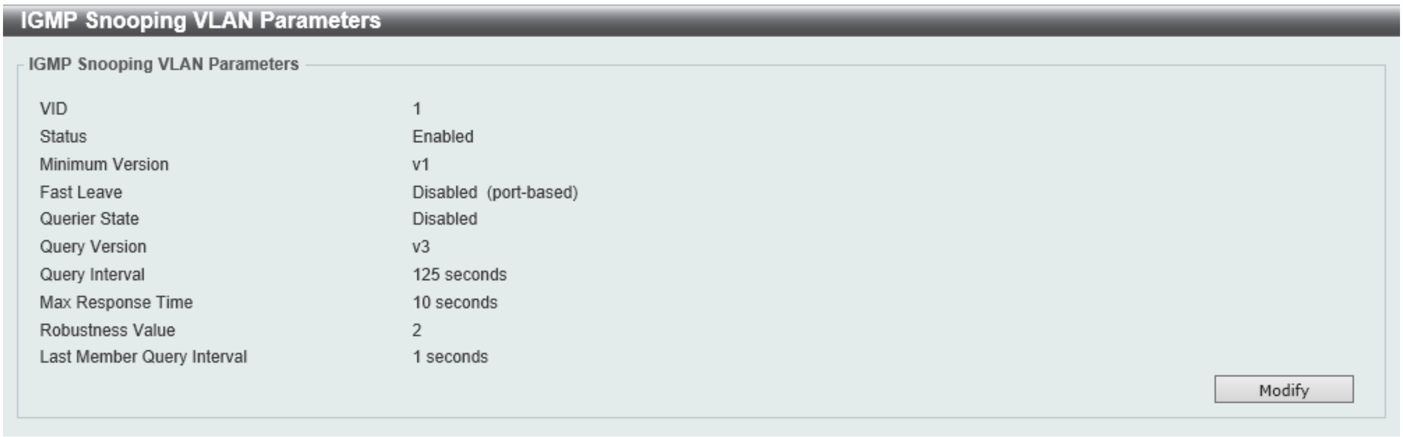
Click the **Show All** button to view all the entries.

Click the **Show Detail** button to see the detail information of the specific VLAN.

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

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Show Detail** button, the following window will appear.



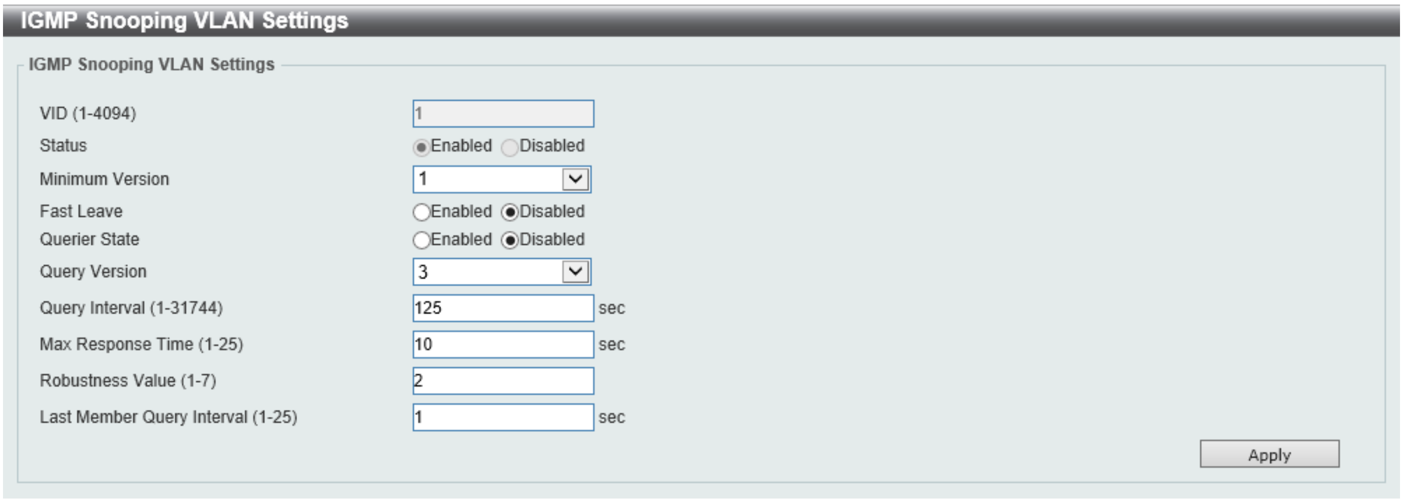
VID	1
Status	Enabled
Minimum Version	v1
Fast Leave	Disabled (port-based)
Querier State	Disabled
Query Version	v3
Query Interval	125 seconds
Max Response Time	10 seconds
Robustness Value	2
Last Member Query Interval	1 seconds

Figure 5-47 IGMP Snooping Settings (Show Detail) Window

The window displays the detail information about IGMP snooping VLAN.

Click the **Modify** button to edit the information in the following window.

After clicking the **Modify** or **Edit** button in IGMP Snooping Settings window, the following window will appear.



VID (1-4094)	1
Status	● Enabled ○ Disabled
Minimum Version	1
Fast Leave	○ Enabled ● Disabled
Querier State	○ Enabled ● Disabled
Query Version	3
Query Interval (1-31744)	125 sec
Max Response Time (1-25)	10 sec
Robustness Value (1-7)	2
Last Member Query Interval (1-25)	1 sec

Figure 5-48 IGMP Snooping Settings (Modify, Edit) Window

The fields that can be configured are described below:

Parameter	Description
Minimum Version	Select the minimum IGMP host version that is allowed on the VLAN. Options to choose from are **1**, **2**, and **3**.
Fast Leave	Select this option to enable or disable the IGMP snooping Fast Leave function. If enabled, the membership is immediately removed when the system receives the IGMP done message from the last member. When fast leave is enabled, the Switch will not generate specific queries. When fast leave is disabled, the Switch will generate specific queries.
Querier State	Select this option to enable or disable the querier state.

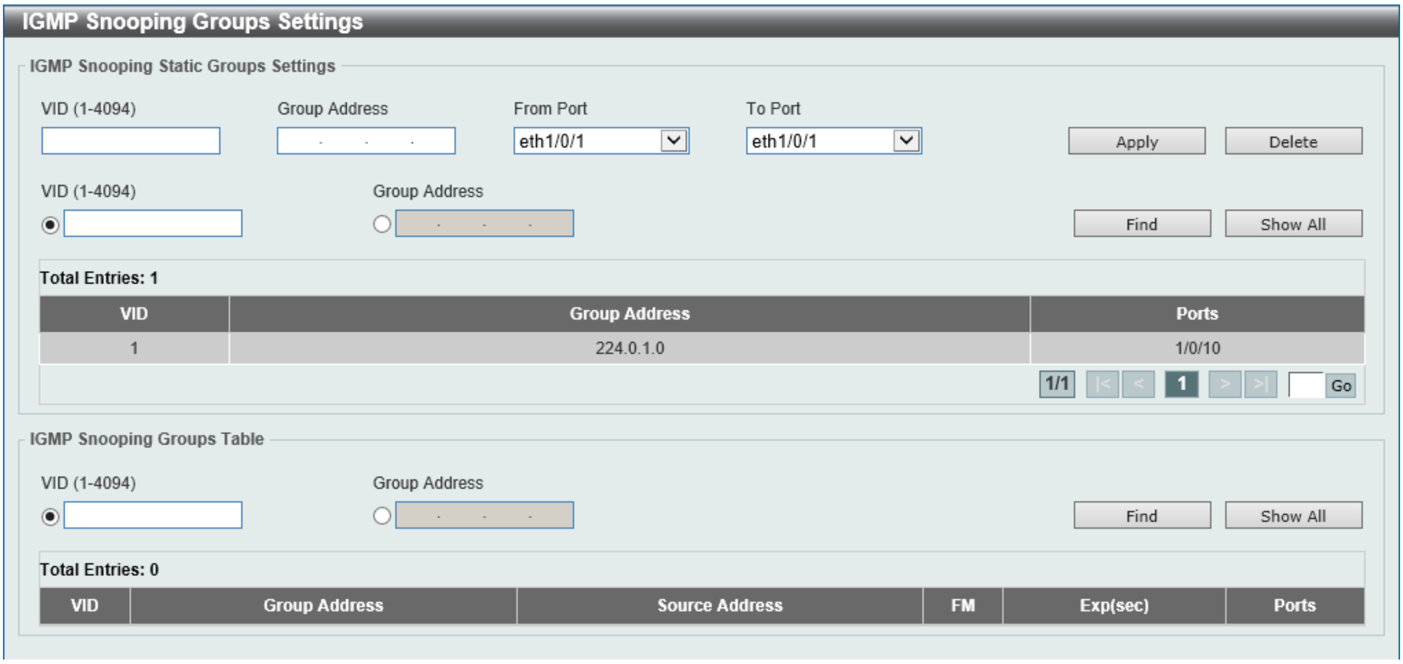
Parameter	Description
Query Version	Select the general query packet version sent by the IGMP snooping querier. Options to choose from are **1**, **2**, and **3**.
Query Interval	Enter the interval at which the IGMP snooping querier sends IGMP general query messages periodically. The range is from 1 to 31744.
Max Response Time	Enter the maximum response time, in seconds, advertised in IGMP snooping queries. The range is from 1 to 25.
Robustness Value	Enter the robustness variable used in IGMP snooping. The range is from 1 to 7.
Last Member Query Interval	Enter the interval at which the IGMP snooping querier sends IGMP group-specific or group-source-specific (channel) query messages. The range is from 1 to 25.

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

IGMP Snooping Groups Settings

This window is used to display and configure the IGMP snooping static group, and view IGMP snooping group.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Groups Settings**, as shown below:



Total Entries: 1

VID	Group Address	Ports
1	224.0.1.0	1/0/10

Total Entries: 0

VID	Group Address	Source Address	FM	Exp(sec)	Ports

Figure 5-49 IGMP Snooping Groups Settings Window

The fields that can be configured in **IGMP Snooping Static Groups Settings** are described below:

Parameter	Description
VID	Enter a VLAN ID of the multicast group. The range is from 1 to 4094.
Group Address	Enter an IP multicast group address.
From Port - To Port	Select the appropriate port range used for the configuration here.
VID	Click the radio button and enter a VLAN ID of the multicast group. The range is from 1 to 4094.
Group Address	Click the radio button and enter an IP multicast group address.

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

Click the **Delete** button to remove the specified entry.

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

Click the **Show All** button to view all the entries.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

The fields that can be configured or displayed for **IGMP Snooping Groups Table** are described below:

Parameter	Description
VID	Click the radio button and enter a VLAN ID of the multicast group. The range is from 1 to 4094.
Group Address	Click the radio button and enter an IP multicast group address.
FM	Displays the filter mode. The following can be displayed: • **EX** (Exclude) - The filter mode is Exclude. • **IN** (Include) - The filter mode is Include.
Exp (sec)	Displays the time left in seconds before the entry expires.

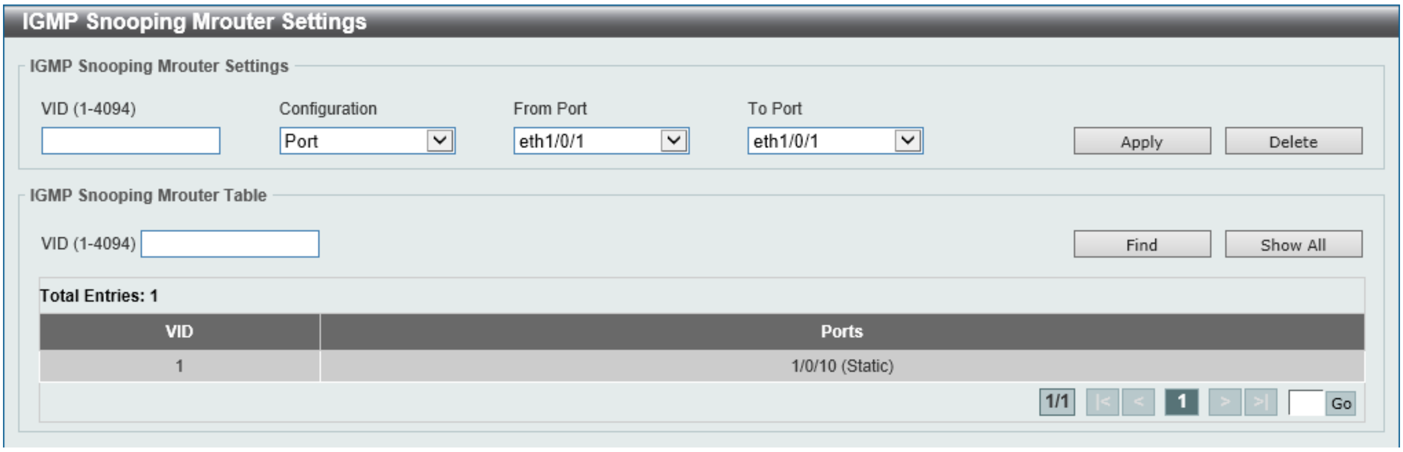
Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to view all the entries.

IGMP Snooping Mrouter Settings

This window is used to display and configure the IGMP Snooping Mrouter settings.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Mrouter Settings**, as shown below:



IGMP Snooping Mrouter Settings

IGMP Snooping Mrouter Settings

VID (1-4094):
Configuration: Port
From Port: eth1/0/1
To Port: eth1/0/1

IGMP Snooping Mrouter Table

VID (1-4094):

Total Entries: 1

VID	Ports
1	1/0/10 (Static)

Figure 5-50 IGMP Snooping Mrouter Settings Window

The fields that can be configured in **IGMP Snooping Mrouter Settings** are described below:

Parameter	Description
VID	Enter the VLAN ID used here. The range is from 1 to 4094.
Configuration	Select the port configuration. Options to choose from are: • **Port** - Select to have the configured ports to be static multicast router ports. • **Forbidden Port** - Select to have the configured ports not to be multicast router ports.
From Port - To Port	Select the appropriate port range used for the configuration here.

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

Click the **Delete** button to remove the specified entry.

The fields that can be configured in **IGMP Snooping Mrouter Table** are described below:

Parameter	Description
VID	Enter the VLAN ID used here. The range is from 1 to 4094.

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

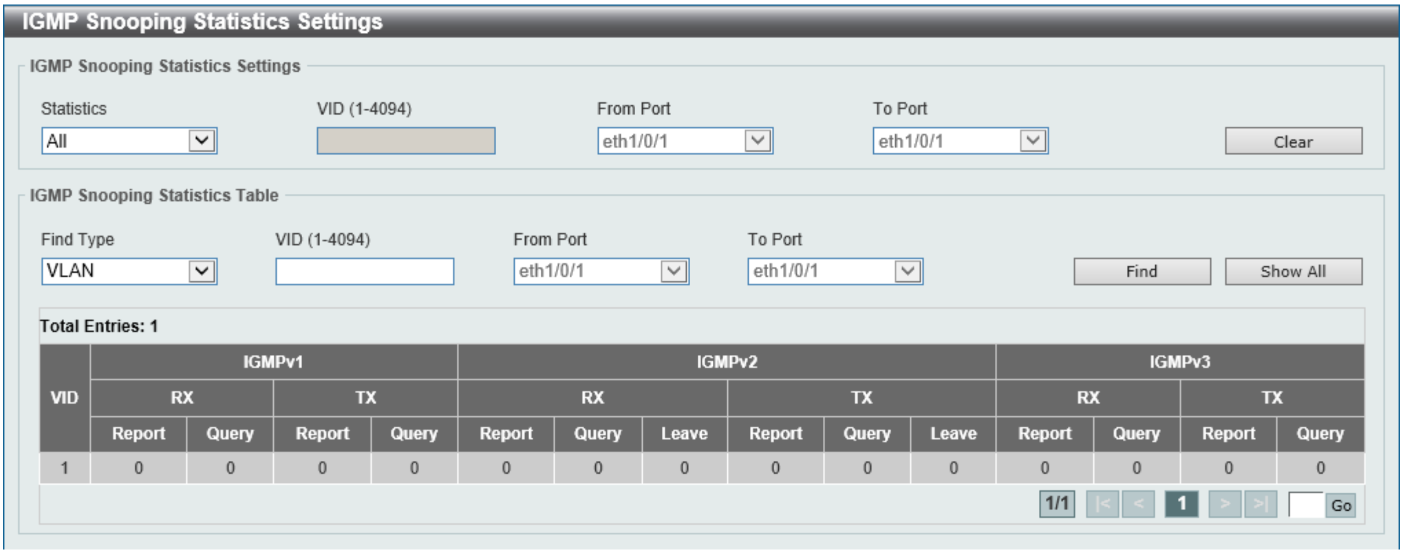
Click the **Show All** button to view all the entries.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IGMP Snooping Statistics Settings

This window is used to view and clear the IGMP snooping related statistics.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Statistics Settings**, as shown below:



IGMP Snooping Statistics Settings

IGMP Snooping Statistics Settings

Statistics: All

VID (1-4094):

From Port: eth1/0/1

To Port: eth1/0/1

IGMP Snooping Statistics Table

Find Type: VLAN

VID (1-4094):

From Port: eth1/0/1

To Port: eth1/0/1

Total Entries: 1

VID	IGMPv1				IGMPv2						IGMPv3			
	RX		TX		RX			TX			RX		TX	
	Report	Query	Report	Query	Report	Query	Leave	Report	Query	Leave	Report	Query	Report	Query
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 5-51 IGMP Snooping Statistics Settings Window

The fields that can be configured in **IGMP Snooping Statistics Settings** are described below:

Parameter	Description
Statistics	Select the interface here. Options to choose from are **All**, **VLAN**, and **Port**.
VID	Enter a VLAN ID between 1 and 4094. This is available when **VLAN** is selected in the **Statistics** drop-down list.
From Port - To Port	Select the appropriate port range used for the configuration here. This is available when **Port** is selected in the **Statistics** drop-down list.

Click the **Clear** button to clear the IGMP snooping related statistics.

The fields that can be configured in **IGMP Snooping Statistics Table** are described below:

Parameter	Description
Find Type	Select the interface type. Options to choose from are **VLAN**, and **Port**.
VID	Enter a VLAN ID between 1 and 4094. This is available when **VLAN** is selected in the **Find Type** drop-down list.
From Port - To Port	Select the appropriate port range used for the configuration here. This is available when **Port** is selected in the **Find Type** drop-down list.

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

Click the **Show All** button to view all the entries.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

MLD Snooping

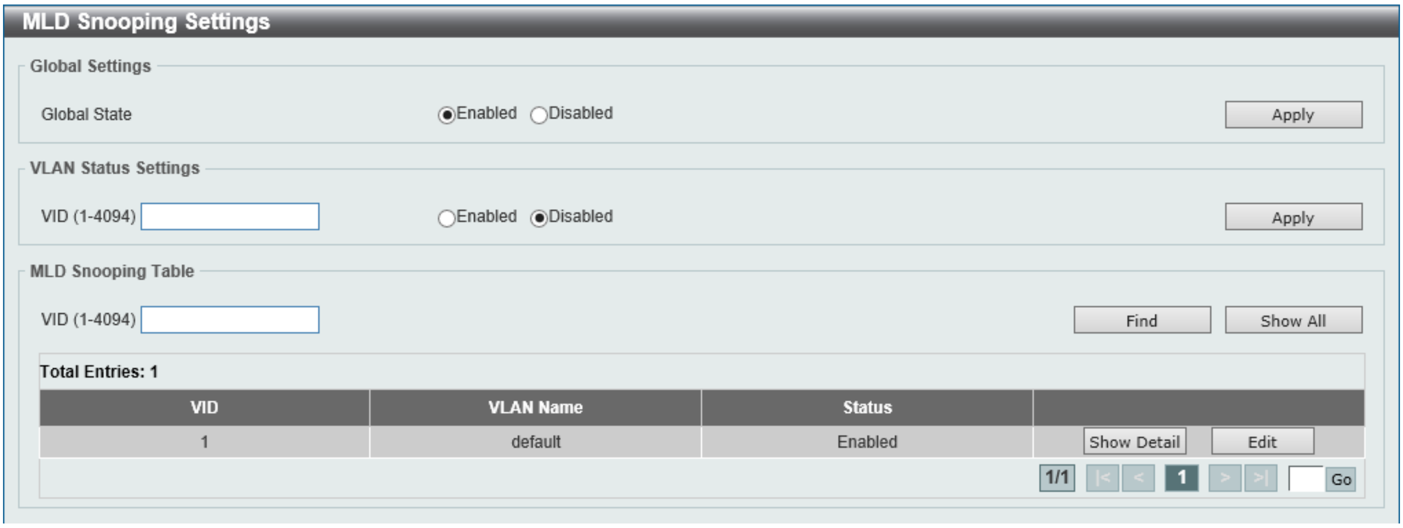
Multicast Listener Discovery (MLD) Snooping is an IPv6 function used similarly to IGMP snooping in IPv4. It is used to discover ports on a VLAN that are requesting multicast data. Instead of flooding all ports on a selected VLAN with multicast traffic, MLD snooping will only forward multicast data to ports that wish to receive this data through the use of queries and reports produced by the requesting ports and the source of the multicast traffic.

MLD snooping is accomplished through the examination of the layer 3 part of an MLD control packet transferred between end nodes and a MLD router. When the Switch discovers that this route is requesting multicast traffic, it adds the port directly attached to it into the correct IPv6 multicast table, and begins the process of forwarding multicast traffic to that port. This entry in the multicast routing table records the port, the VLAN ID, and the associated multicast IPv6 multicast group address, and then considers this port to be an active listening port. The active listening ports are the only ones to receive multicast group data.

MLD Snooping Settings

This window is used to display and configure the MLD snooping settings.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Settings**, as shown below:



MLD Snooping Settings

Global Settings

Global State ● Enabled ○ Disabled

VLAN Status Settings

VID (1-4094) ○ Enabled ● Disabled

MLD Snooping Table

VID (1-4094)

Total Entries: 1

VID	VLAN Name	Status	
1	default	Enabled	Show Detail Edit

Figure 5-52 MLD Snooping Settings Window

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

Parameter	Description
Global State	Select this option to enable or disable the global MLD snooping state.

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

The fields that can be configured in **VLAN Status Settings** are described below:

Parameter	Description
VID	Enter a VLAN ID from 1 to 4094, and select to enable or disable MLD snooping on the VLAN.

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

The fields that can be configured in **MLD Snooping Table** are described below:

Parameter	Description
VID	Enter a VLAN ID from 1 to 4094.

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

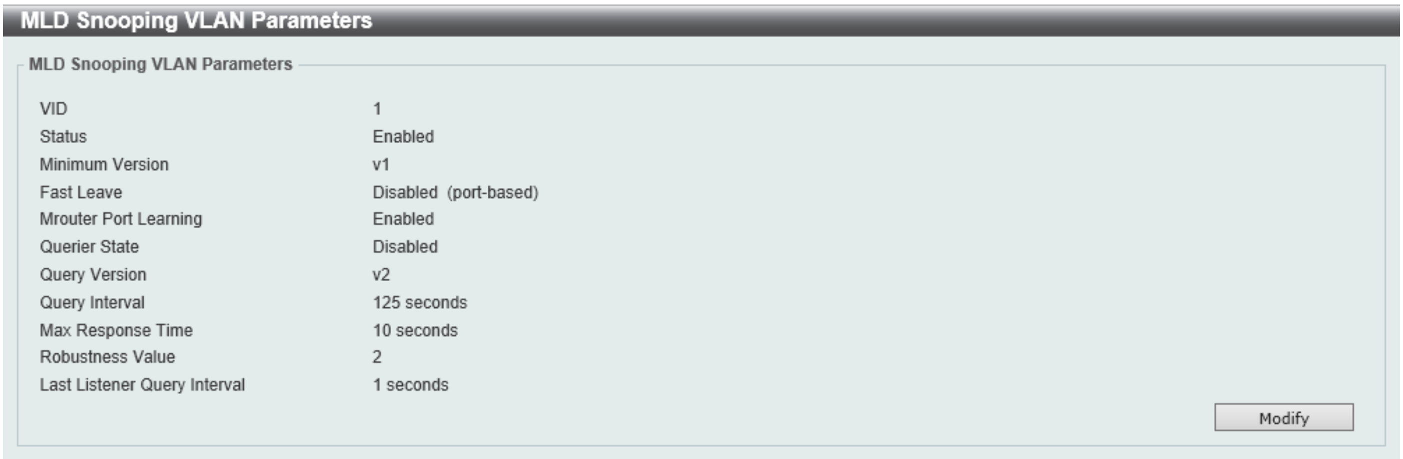
Click the **Show All** button to view all the entries.

Click the **Show Detail** button to see the detail information of the specific VLAN.

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

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Show Detail** button, the following window will appear.



MLD Snooping VLAN Parameters

MLD Snooping VLAN Parameters

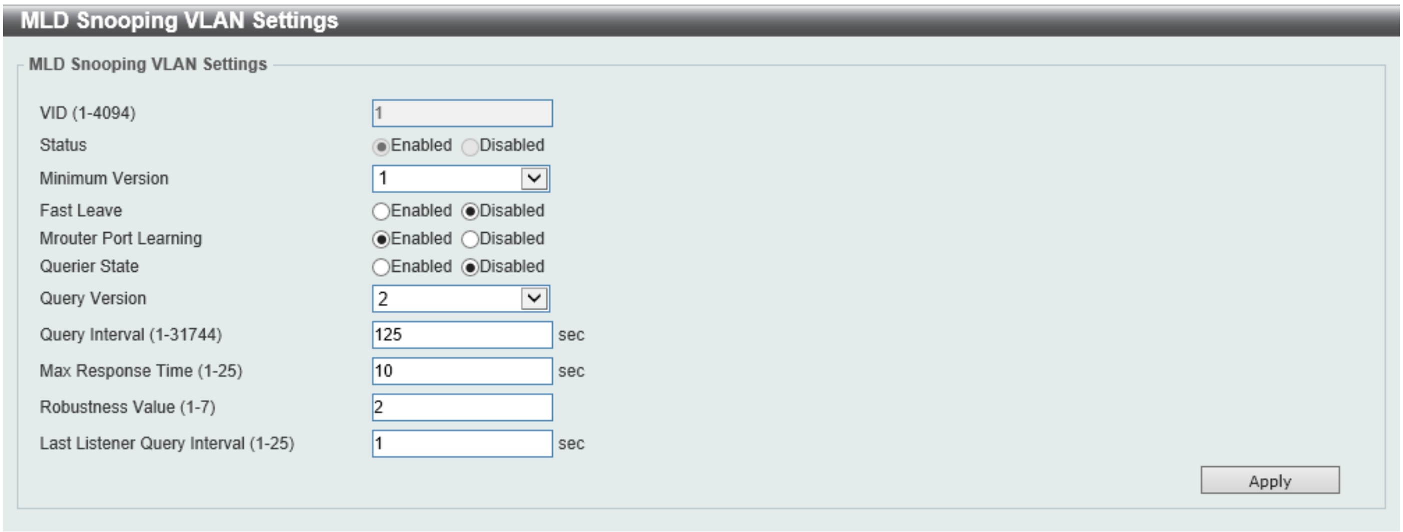
VID	1
Status	Enabled
Minimum Version	v1
Fast Leave	Disabled (port-based)
Mrouter Port Learning	Enabled
Querier State	Disabled
Query Version	v2
Query Interval	125 seconds
Max Response Time	10 seconds
Robustness Value	2
Last Listener Query Interval	1 seconds

Figure 5-53 MLD Snooping Settings (Show Detail) Window

The window displays the detail information about MLD snooping VLAN.

Click the **Modify** button to edit the information in the following window.

After clicking the **Modify** or **Edit** button in MLD Snooping Settings window, the following window will appear.



MLD Snooping VLAN Settings

MLD Snooping VLAN Settings

VID (1-4094)	1	
Status	● Enabled ○ Disabled	
Minimum Version	1	
Fast Leave	○ Enabled ● Disabled	
Mrouter Port Learning	● Enabled ○ Disabled	
Querier State	○ Enabled ● Disabled	
Query Version	2	
Query Interval (1-31744)	125	sec
Max Response Time (1-25)	10	sec
Robustness Value (1-7)	2	
Last Listener Query Interval (1-25)	1	sec

Figure 5-54 MLD Snooping Settings (Modify, Edit) Window

The fields that can be configured are described below:

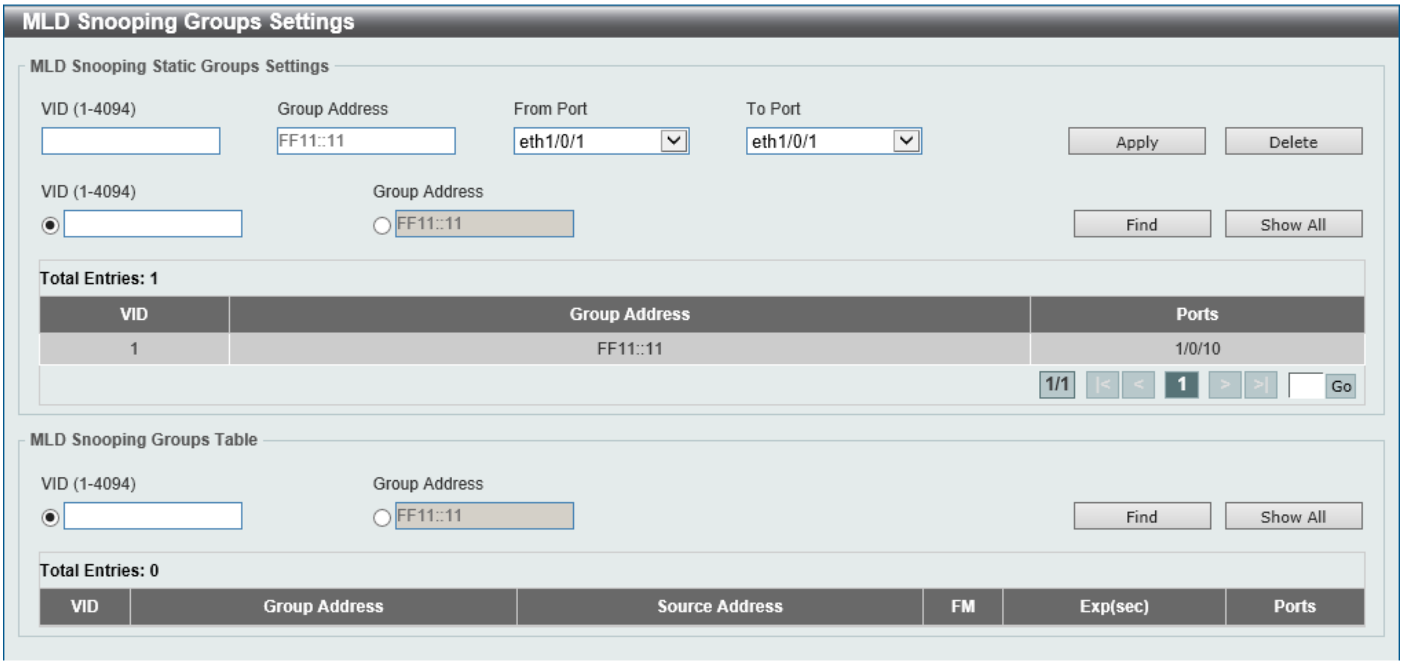
Parameter	Description
Minimum Version	Select the minimum version of MLD hosts that is allowed on the VLAN. Options to choose from are **1** and **2**.
Fast Leave	Select this option to enable or disable the MLD snooping Fast Leave function. If enabled, the membership is immediately removed when the system receives the MLD done message from the last member.
Mrouter Port Learning	Select this option to enable or disable Mrouter port learning.
Querier State	Select this option to enable or disable the querier state.
Query Version	Select the general query packet version sent by the MLD snooping querier. Options to choose from are **1**, and **2**.
Query Interval	Enter the interval at which the MLD snooping querier sends MLD general query messages periodically. The range is from 1 to 31744.
Max Response Time	Enter the maximum response time, in seconds, advertised in MLD snooping queries. The range is from 1 to 25.
Robustness Value	Enter the robustness variable used in MLD snooping. The range is from 1 to 7.
Last Listener Query Interval	Enter the interval at which the MLD snooping querier sends MLD group-specific or group-source-specific (channel) query messages. The range is from 1 to 25.

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

MLD Snooping Groups Settings

This window is used to display and configure the MLD snooping static group, and view MLD snooping group.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Groups Settings**, as shown below:



MLD Snooping Groups Settings

MLD Snooping Static Groups Settings

VID (1-4094):
Group Address: FF11::11
From Port: eth1/0/1
To Port: eth1/0/1

VID (1-4094) ●
Group Address ○ FF11::11

Total Entries: 1

VID	Group Address	Ports
1	FF11::11	1/0/10

MLD Snooping Groups Table

VID (1-4094) ●
Group Address ○ FF11::11

Total Entries: 0

VID	Group Address	Source Address	FM	Exp(sec)	Ports

Figure 5-55 MLD Snooping Groups Settings Window

The fields that can be configured in **MLD Snooping Static Groups Settings** are described below:

Parameter	Description
VID	Enter the VLAN ID of the multicast group here. The range is from 1 to 4094.

Parameter	Description
Group Address	Enter the IPv6 multicast group address here.
From Port - To Port	Select the appropriate port range used for the configuration here.
VID	Click the radio button and enter a VLAN ID of the multicast group. The range is from 1 to 4094.
Group Address	Click the radio button and enter an IPv6 multicast group address.

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

Click the **Delete** button to remove the specified entry.

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

Click the **Show All** button to view all the entries.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

The fields that can be configured or displayed for **MLD Snooping Groups Table** are described below:

Parameter	Description
VID	Click the radio button and enter a VLAN ID of the multicast group. The range is from 1 to 4094.
Group Address	Click the radio button and enter an IPv6 multicast group address.
FM	Displays the filter mode. The following can be displayed: • **EX** (Exclude) - The filter mode is Exclude. • **IN** (Include) - The filter mode is Include.
Exp (sec)	Displays the time left in seconds before the entry expires.

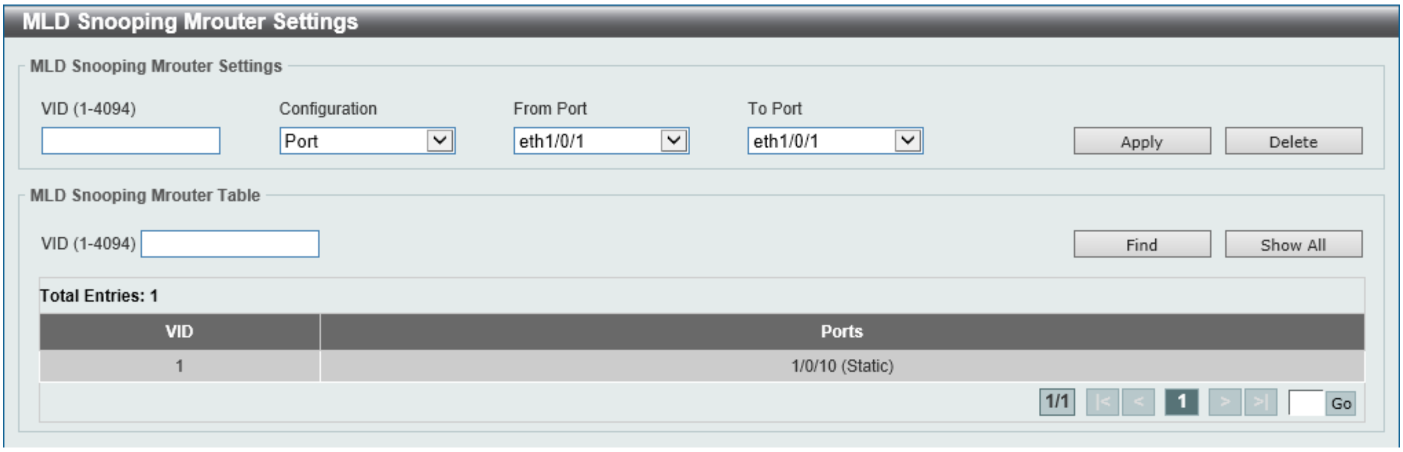
Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to view all the entries.

MLD Snooping Mrouter Settings

This window is used to display and configure the specified interface(s) as the router ports or forbidden to be IPv6 multicast router ports on the VLAN on the Switch.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Mrouter Settings**, as shown below:



MLD Snooping Mrouter Settings

MLD Snooping Mrouter Settings

VID (1-4094):

Configuration: Port

From Port: eth1/0/1

To Port: eth1/0/1

MLD Snooping Mrouter Table

VID (1-4094):

Total Entries: 1

VID	Ports
1	1/0/10 (Static)

Figure 5-56 MLD Snooping Mrouter Settings Window

The fields that can be configured in **MLD Snooping Mrouter Settings** are described below:

Parameter	Description
VID	Enter a VLAN ID between 1 and 4094.
Configuration	Select the port configuration. Options to choose from are: • **Port** - Select to have the configured ports as being connected to multicast-enabled routers. • **Forbidden Port** - Select to have the configured ports as being not connected to multicast-enabled routers. • **Learn pimv6** - Select to enable dynamic learning of multicast router port.
From Port - To Port	Select the appropriate port range used for the configuration here.

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

Click the **Delete** button to remove the specified entry.

The fields that can be configured in **MLD Snooping Mrouter Table** are described below:

Parameter	Description
VID	Enter a VLAN ID between 1 and 4094.

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

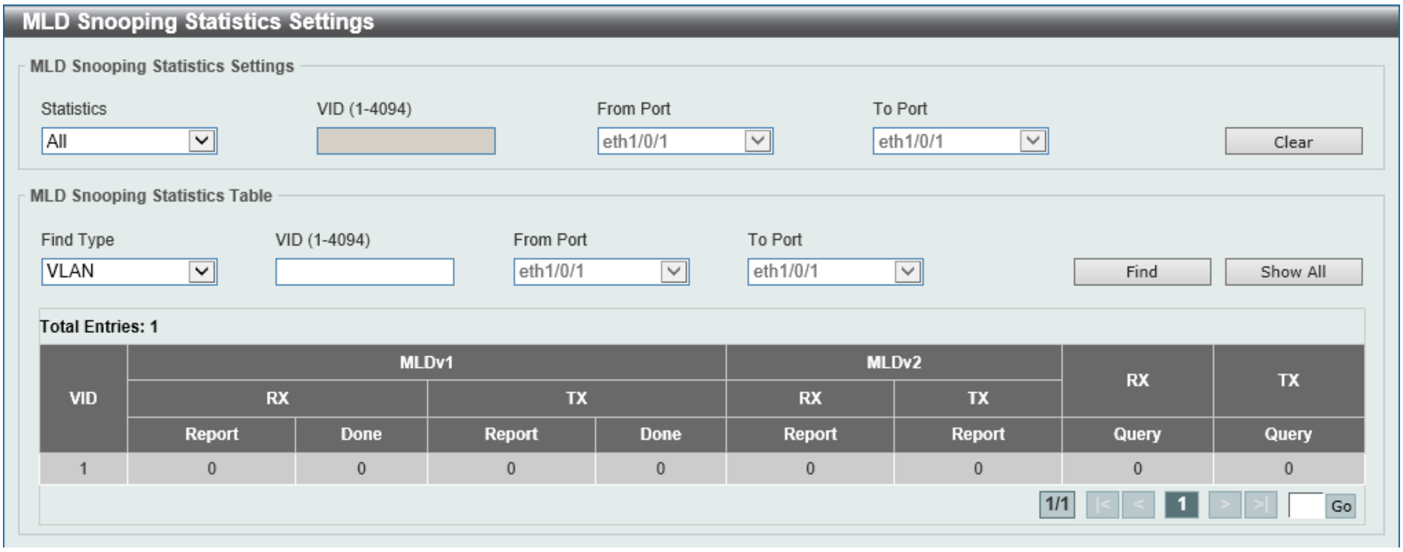
Click the **Show All** button to view all the entries.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

MLD Snooping Statistics Settings

This window is used to view and clear the MLD snooping related statistics.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Statistics Settings**, as shown below:



MLD Snooping Statistics Settings

MLD Snooping Statistics Settings

Statistics: All
VID (1-4094):
From Port: eth1/0/1
To Port: eth1/0/1

MLD Snooping Statistics Table

Find Type: VLAN
VID (1-4094):
From Port: eth1/0/1
To Port: eth1/0/1

Total Entries: 1

VID	MLDv1				MLDv2		RX	TX
	RX		TX		RX	TX		
	Report	Done	Report	Done	Report	Report	Query	Query
1	0	0	0	0	0	0	0	0

Figure 5-57 MLD Snooping Statistics Settings Window

The fields that can be configured in **MLD Snooping Statistics Settings** are described below:

Parameter	Description
Statistics	Select the interface here. Options to choose from are **All**, **VLAN**, and **Port**.

Parameter	Description
VID	Enter a VLAN ID between 1 and 4094. This is available when **VLAN** is selected in the **Statistics** drop-down list.
From Port - To Port	Select the appropriate port range used for the configuration here. This is available when **Port** is selected in the **Statistics** drop-down list.

Click the **Clear** button to clear the MLD snooping related statistics.

The fields that can be configured in **MLD Snooping Statistics Table** are described below:

Parameter	Description
Find Type	Select the interface type. Options to choose from are **VLAN**, and **Port**.
VID	Enter a VLAN ID between 1 and 4094. This is available when **VLAN** is selected in the **Find Type** drop-down list.
From Port - To Port	Select the appropriate port range used for the configuration here. This is available when **Port** is selected in the **Find Type** drop-down list.

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

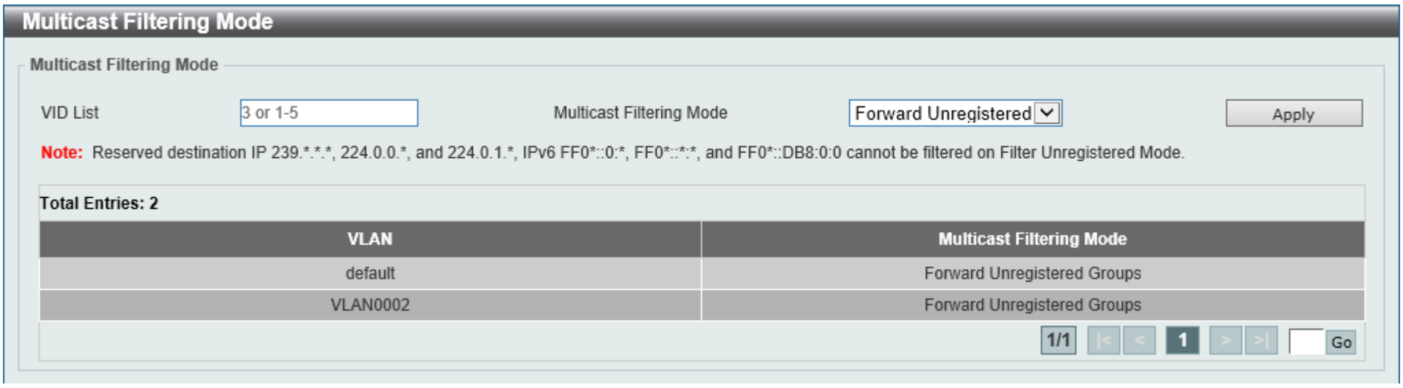
Click the **Show All** button to view all the entries.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Multicast Filtering Mode

This window is used to display and configure the Layer 2 multicast filtering settings.

To view the following window, click **L2 Features > L2 Multicast Control > Multicast Filtering Mode**, as shown below:



Multicast Filtering Mode

Multicast Filtering Mode

VID List: 3 or 1-5

Multicast Filtering Mode: Forward Unregistered

Note: Reserved destination IP 239.*.*.*, 224.0.0.*, and 224.0.1.*, IPv6 FF0*::0:*, FF0*::*:*, and FF0*::DB8:0:0 cannot be filtered on Filter Unregistered Mode.

Total Entries: 2

VLAN	Multicast Filtering Mode
default	Forward Unregistered Groups
VLAN0002	Forward Unregistered Groups

Figure 5-58 Multicast Filtering Mode Window

The fields that can be configured are described below:

Parameter	Description
VID List	Enter the VLAN ID list that will be used for this configuration here.
Multicast Filter Mode	Select the multicast filter mode here. Options to choose from are: • **Forward Unregistered** - Specifies that registered multicast packets will be forwarded based on the forwarding table and all unregistered multicast packets will be flooded based on the VLAN domain. • **Forward All** - Specifies that all multicast packets will be flooded based on the VLAN domain. • **Filter Unregistered** - Specifies that registered packets will be forwarded based on the forwarding table and all unregistered multicast packets will be filtered.

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

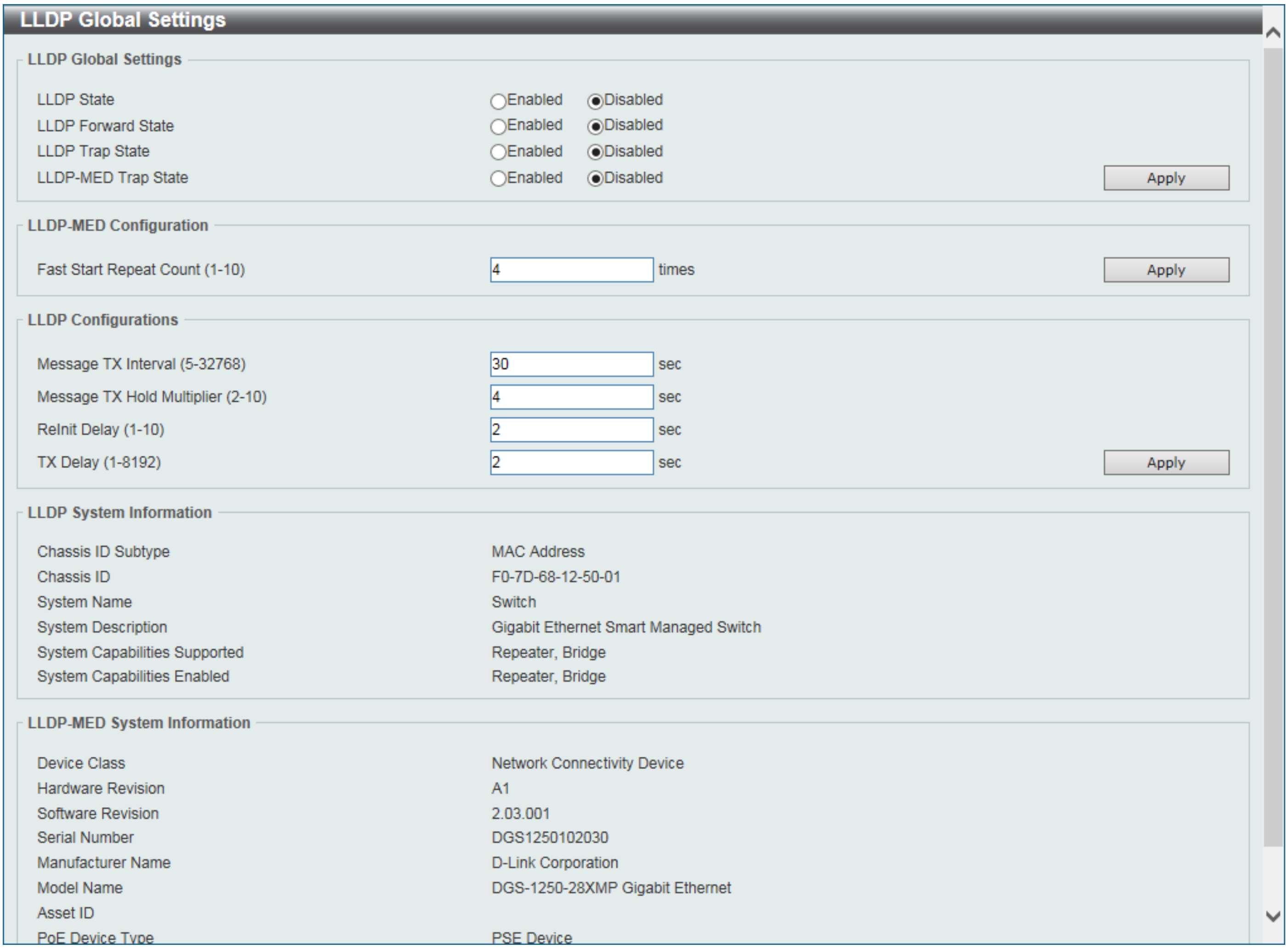
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

LLDP

LLDP Global Settings

This window is used to display and configure the global LLDP settings.

To view the following window, click **L2 Features > LLDP > LLDP Global Settings**, as shown below:



LLDP Global Settings

LLDP Global Settings

LLDP State ○Enabled ●Disabled

LLDP Forward State ○Enabled ●Disabled

LLDP Trap State ○Enabled ●Disabled

LLDP-MED Trap State ○Enabled ●Disabled

Apply

LLDP-MED Configuration

Fast Start Repeat Count (1-10): 4 times

Apply

LLDP Configurations

Message TX Interval (5-32768): 30 sec

Message TX Hold Multiplier (2-10): 4 sec

ReInit Delay (1-10): 2 sec

TX Delay (1-8192): 2 sec

Apply

LLDP System Information

Chassis ID Subtype	MAC Address
Chassis ID	F0-7D-68-12-50-01
System Name	Switch
System Description	Gigabit Ethernet Smart Managed Switch
System Capabilities Supported	Repeater, Bridge
System Capabilities Enabled	Repeater, Bridge

LLDP-MED System Information

Device Class	Network Connectivity Device
Hardware Revision	A1
Software Revision	2.03.001
Serial Number	DGS1250102030
Manufacturer Name	D-Link Corporation
Model Name	DGS-1250-28XMP Gigabit Ethernet
Asset ID	
PoE Device Type	PSE Device

Figure 5-59 LLDP Global Settings Window

The fields that can be configured in **LLDP Global Settings** are described below:

Parameter	Description
LLDP State	Select this option to enable or disable the LLDP feature. By default, this is disabled.
LLDP Forward State	Select this option to enable or disable LLDP forward state. When the **LLDP State** is disabled and **LLDP Forward Sate** is enabled, the received LLDPDU packet will be forwarded.
LLDP Trap State	Select this option to enable or disable the LLDP trap state.
LLDP-MED Trap State	Select this option to enable or disable the LLDP-MED trap state.

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

The fields that can be configured in **LLDP-MED Settings** are described below:

Parameter	Description
Fast Start Repeat Count	Enter the LLDP-MED fast start repeat count value. This value must be between 1 and 10.

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

The fields that can be configured in **LLDP Configurations** are described below:

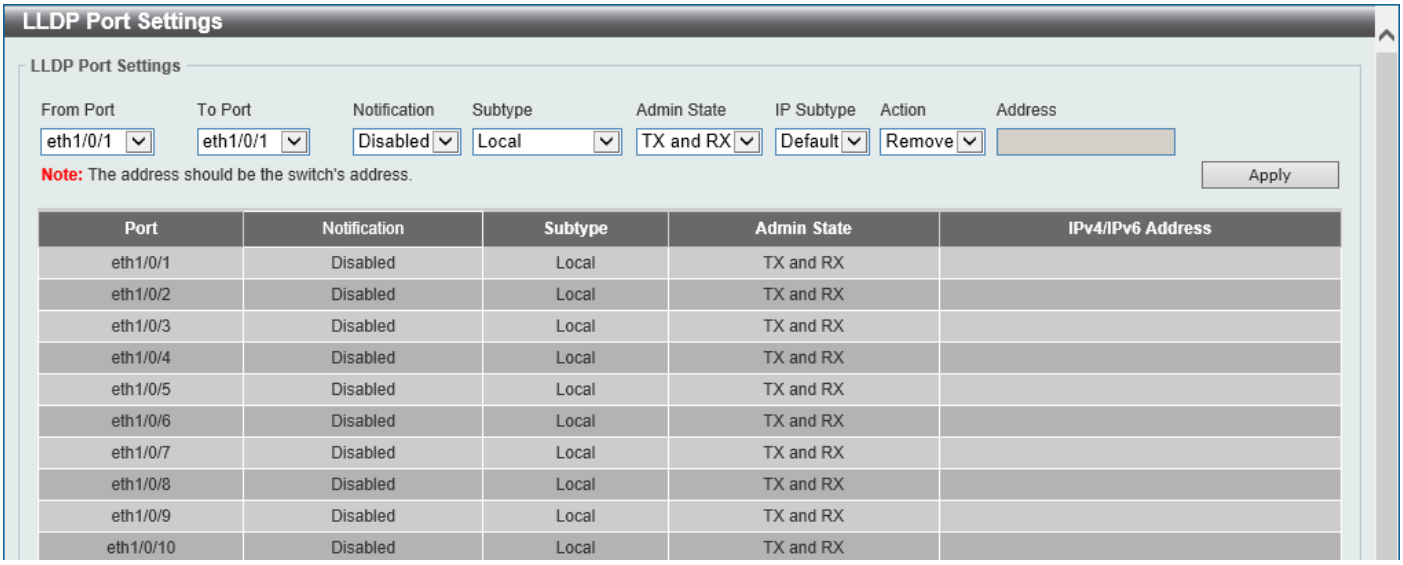
Parameter	Description
Message TX Interval	Enter the interval between consecutive transmissions of LLDP advertisements on each physical interface. The range is from 5 to 32768 seconds.
Message TX Hold Multiplier	Enter the multiplier on the LLDPDUs transmission interval that used to calculate the TTL value of an LLDPDU. This value must be between 2 and 10.
ReInit Delay	Enter the delay value for LLDP initialization on an interface. This value must be between 1 and 10 seconds.
TX Delay	Enter the delay value for sending successive LLDPDUs on an interface. The valid values are from 1 to 8192 seconds and should not be greater than one-fourth of the transmission interval timer.

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

LLDP Port Settings

This window is used to display and configure the LLDP port settings.

To view the following window, click **L2 Features > LLDP > LLDP Port Settings**, as shown below:



LLDP Port Settings

LLDP Port Settings

From Port: eth1/0/1
To Port: eth1/0/1
Notification: Disabled
Subtype: Local
Admin State: TX and RX
IP Subtype: Default
Action: Remove
Address:

Note: The address should be the switch's address.

Port	Notification	Subtype	Admin State	IPv4/IPv6 Address
eth1/0/1	Disabled	Local	TX and RX	
eth1/0/2	Disabled	Local	TX and RX	
eth1/0/3	Disabled	Local	TX and RX	
eth1/0/4	Disabled	Local	TX and RX	
eth1/0/5	Disabled	Local	TX and RX	
eth1/0/6	Disabled	Local	TX and RX	
eth1/0/7	Disabled	Local	TX and RX	
eth1/0/8	Disabled	Local	TX and RX	
eth1/0/9	Disabled	Local	TX and RX	
eth1/0/10	Disabled	Local	TX and RX	

Figure 5-60 LLDP Port Settings Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Notification	Select to enable or disable the notification feature here.

Parameter	Description
Subtype	Select the subtype of LLDP TLV(s). Options to choose from are **MAC Address**, and **Local**.
Admin State	Select the local LLDP agent and allow it to send and receive LLDP frames on the port. Options to choose from are: • **TX** - The local LLDP agent can only transmit LLDP frames. • **RX** - The local LLDP agent can only receive LLDP frames. • **TX and RX** - The local LLDP agent can both transmit and receive LLDP frames. This is the default option. • **Disabled** - The local LLDP agent can neither transmit nor receive LLDP frames.
IP Subtype	Select the type of the IP address information to be sent. Options to choose from are **Default**, **IPv4**, and **IPv6**.
Action	Select the action that will be taken here. Options to choose from are **Remove** and **Add**.
Address	Enter the IP address that will be sent.

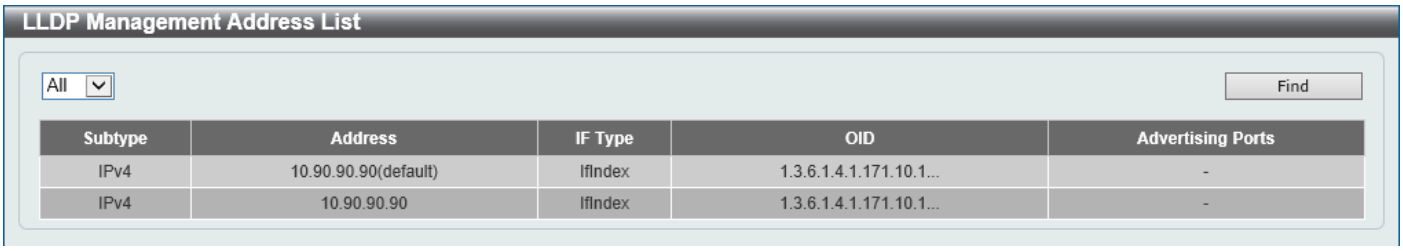
Click the **Apply** button to accept the changes made.

NOTE: The IPv4 or IPv6 address entered here should be an existing LLDP management IP address.

LLDP Management Address List

This window is used to view the LLDP management address list.

To view the following window, click **L2 Features > LLDP > LLDP Management Address List**, as shown below:



LLDP Management Address List

All ▾

Subtype	Address	IF Type	OID	Advertising Ports
IPv4	10.90.90.90(default)	IfIndex	1.3.6.1.4.1.171.10.1...	-
IPv4	10.90.90.90	IfIndex	1.3.6.1.4.1.171.10.1...	-

Figure 5-61 LLDP Management Address List Window

The fields that can be configured are described below:

Parameter	Description
Subtype	Select the subtype. Options to choose from are **All**, **IPv4** and **IPv6**. After selecting the **IPv4** option, enter the IPv4 address in the space provided. After selecting the **IPv6** option, enter the IPv6 address in the space provided.

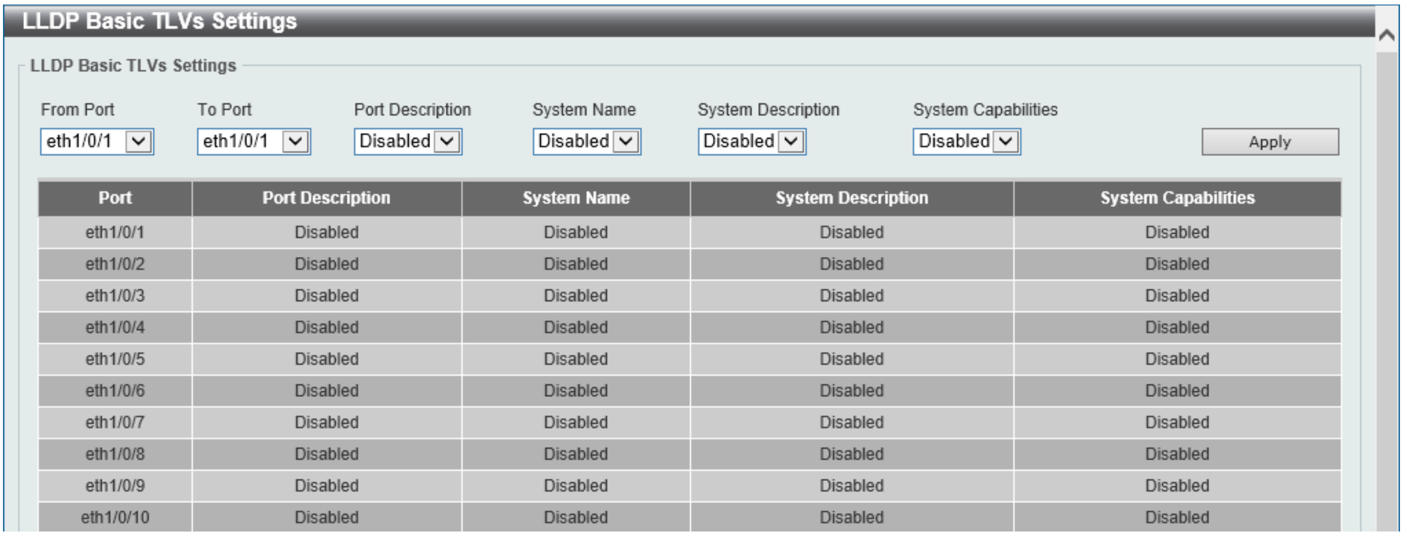
Click the **Find** button to locate a specific entry based on the selection made.

LLDP Basic TLVs Settings

The Type-Length-Value (TLV) field allows specific information to be sent within LLDP packets. This window is used to configure basic TLV settings. An active LLDP port on the Switch always includes mandatory data in its outbound advertisements. There are four optional data types that can be configured to exclude one or more of these data types from outbound LLDP advertisements. The mandatory data type includes four basic types of TLVs: end of LLDPDU

TLV, chassis ID TLV, port ID TLV, and TTL TLV. The mandatory data types cannot be disabled. There are also four data types that can be optionally selected. These include Port Description, System Name, System Description, and System Capability.

To view the following window, click **L2 Features > LLDP > LLDP Basic TLVs Settings**, as shown below:



LLDP Basic TLVs Settings

LLDP Basic TLVs Settings

From Port: eth1/0/1
To Port: eth1/0/1
Port Description: Disabled
System Name: Disabled
System Description: Disabled
System Capabilities: Disabled

Port	Port Description	System Name	System Description	System Capabilities
eth1/0/1	Disabled	Disabled	Disabled	Disabled
eth1/0/2	Disabled	Disabled	Disabled	Disabled
eth1/0/3	Disabled	Disabled	Disabled	Disabled
eth1/0/4	Disabled	Disabled	Disabled	Disabled
eth1/0/5	Disabled	Disabled	Disabled	Disabled
eth1/0/6	Disabled	Disabled	Disabled	Disabled
eth1/0/7	Disabled	Disabled	Disabled	Disabled
eth1/0/8	Disabled	Disabled	Disabled	Disabled
eth1/0/9	Disabled	Disabled	Disabled	Disabled
eth1/0/10	Disabled	Disabled	Disabled	Disabled

Figure 5-62 LLDP Basic TLVs Settings Window

The fields that can be configured are described below:

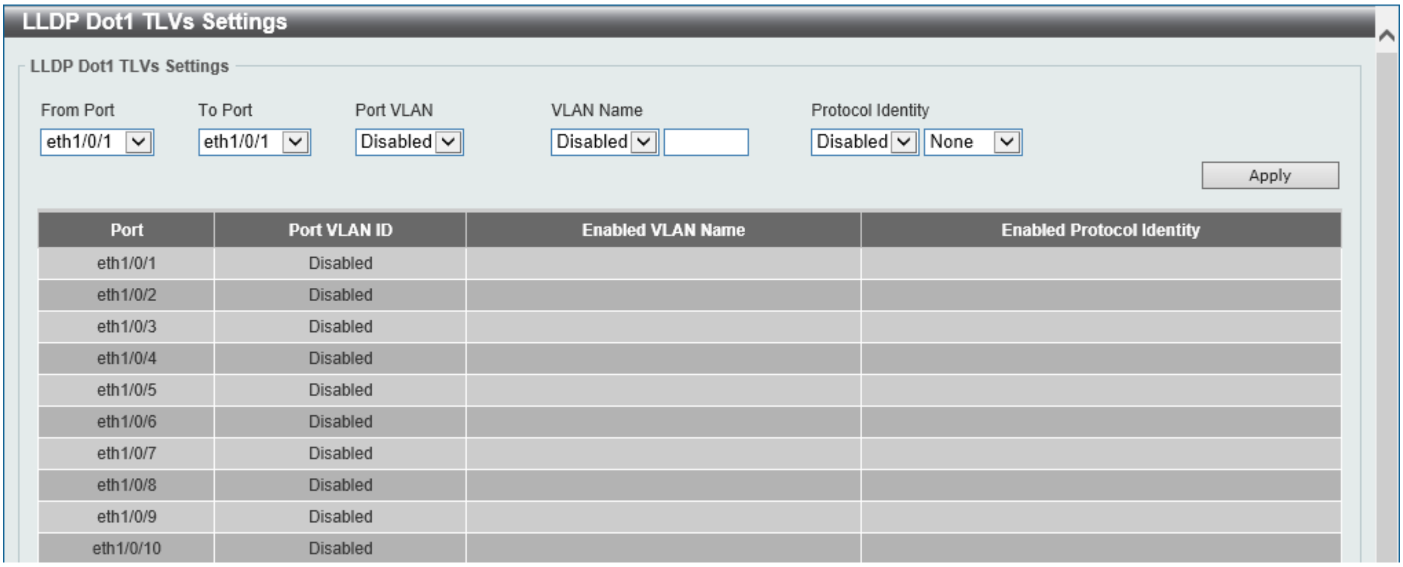
Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Port Description	Select this option to enable or disable the Port Description option.
System Name	Select this option to enable or disable the System Name option.
System Description	Select this option to enable or disable the System Description option.
System Capabilities	Select this option to enable or disable the System Capabilities option.

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

LLDP Dot1 TLVs Settings

The LLDP Dot1 TLVs Settings page is used to enable or disable outbound LLDP advertisements for IEEE 802.1 organizationally unique port VLAN ID TLVs.

To view the following window, click **L2 Features > LLDP > LLDP Dot1 TLVs Settings**, as shown below:



LLDP Dot1 TLVs Settings

LLDP Dot1 TLVs Settings

From Port: eth1/0/1
To Port: eth1/0/1
Port VLAN: Disabled
VLAN Name: Disabled
Protocol Identity: Disabled None

Port	Port VLAN ID	Enabled VLAN Name	Enabled Protocol Identity
eth1/0/1	Disabled		
eth1/0/2	Disabled		
eth1/0/3	Disabled		
eth1/0/4	Disabled		
eth1/0/5	Disabled		
eth1/0/6	Disabled		
eth1/0/7	Disabled		
eth1/0/8	Disabled		
eth1/0/9	Disabled		
eth1/0/10	Disabled		

Figure 5-63 LLDP Dot1 TLVs Settings Window

The fields that can be configured are described below:

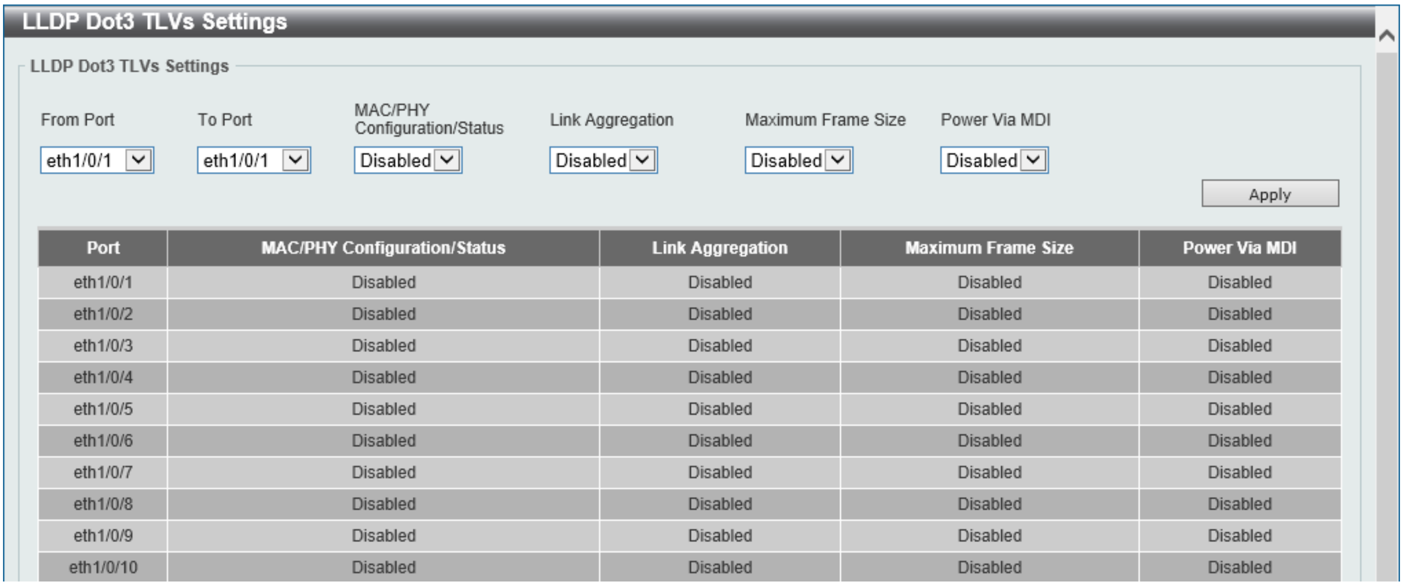
Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Port VLAN	Select this option to enable or disable sending the port VLAN ID TLV. The Port VLAN ID TLV is an optional fixed length TLV that allows a VLAN bridge port to advertise the port VLAN ID (PVID) that will be associated with untagged or priority tagged frames.
VLAN Name	Select this option to enable or disable sending the VLAN name TLV. Enter the ID of the VLAN in the VLAN name TLV.
Protocol Identity	Select this option to enable or disable sending the Protocol Identity TLV and the protocol name. Options for protocol name to choose from are **None**, **EAPOL**, **LACP**, **STP**, and **All**.

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

LLDP Dot3 TLVs Settings

The LLDP Dot3 TLVs Settings page is used to enable or disable outbound LLDP advertisements for IEEE 802.3 organizationally unique TLVs.

To view the following window, click **L2 Features > LLDP > LLDP Dot3 TLVs Settings**, as shown below:



LLDP Dot3 TLVs Settings

LLDP Dot3 TLVs Settings

From Port	To Port	MAC/PHY Configuration/Status	Link Aggregation	Maximum Frame Size	Power Via MDI
eth1/0/1	eth1/0/1	Disabled	Disabled	Disabled	Disabled

Port	MAC/PHY Configuration/Status	Link Aggregation	Maximum Frame Size	Power Via MDI
eth1/0/1	Disabled	Disabled	Disabled	Disabled
eth1/0/2	Disabled	Disabled	Disabled	Disabled
eth1/0/3	Disabled	Disabled	Disabled	Disabled
eth1/0/4	Disabled	Disabled	Disabled	Disabled
eth1/0/5	Disabled	Disabled	Disabled	Disabled
eth1/0/6	Disabled	Disabled	Disabled	Disabled
eth1/0/7	Disabled	Disabled	Disabled	Disabled
eth1/0/8	Disabled	Disabled	Disabled	Disabled
eth1/0/9	Disabled	Disabled	Disabled	Disabled
eth1/0/10	Disabled	Disabled	Disabled	Disabled

Figure 5-64 LLDP Dot3 TLVs Settings Window

The fields that can be configured are described below:

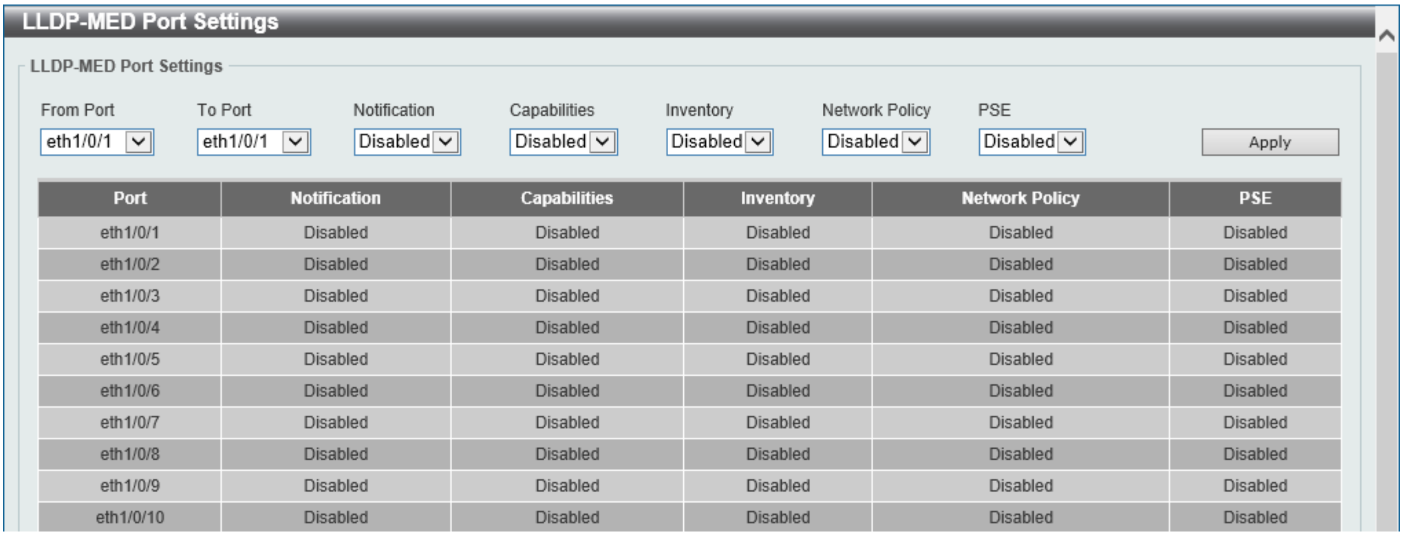
Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
MAC/PHY Configuration/Status	Select this option to enable or disable the MAC/PHY Configuration/Status TLV to send. The MAC/PHY Configuration/Status TLV is an optional TLV that identifies (1) the duplex and bit-rate capability of the sending IEEE 802.3 LAN node, and (2) the current duplex and bit-rate settings of the sending IEEE 802.3 LAN node.
Link Aggregation	Select this option to enable or disable the Link Aggregation TLV to send. The Link Aggregation TLV indicates contains the following information. Whether the link is capable of being aggregated, whether the link is currently in an aggregation, and the aggregated port channel ID of the port. If the port is not aggregated, then the ID is 0.
Maximum Frame Size	Select this option to enable or disable the Maximum Frame Size TLV to send. The Maximum Frame Size TLV indicates the maximum frame size capability of the implemented MAC and PHY.
Power Via MDI	Select this option to enable or disable the power via MDI TLV to send. IEEE 802.3 PMD implementations allow power to be supplied over the link for connected non-powered systems. The Power Via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending IEEE 802.3 LAN station.

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

LLDP-MED Port Settings

The LLDP-MED Port Settings page is used to enable or disable outbound LLDP advertisements for LLDP-MED TLVs.

To view the following window, click **L2 Features > LLDP > LLDP-MED Port Settings**, as shown below:



From Port: eth1/0/1, To Port: eth1/0/1, Notification: Disabled, Capabilities: Disabled, Inventory: Disabled, Network Policy: Disabled, PSE: Disabled

Port	Notification	Capabilities	Inventory	Network Policy	PSE
eth1/0/1	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/2	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/3	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/4	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/5	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/6	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/7	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/8	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/9	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/10	Disabled	Disabled	Disabled	Disabled	Disabled

Figure 5-65 LLDP-MED Port Settings Window

The fields that can be configured are described below:

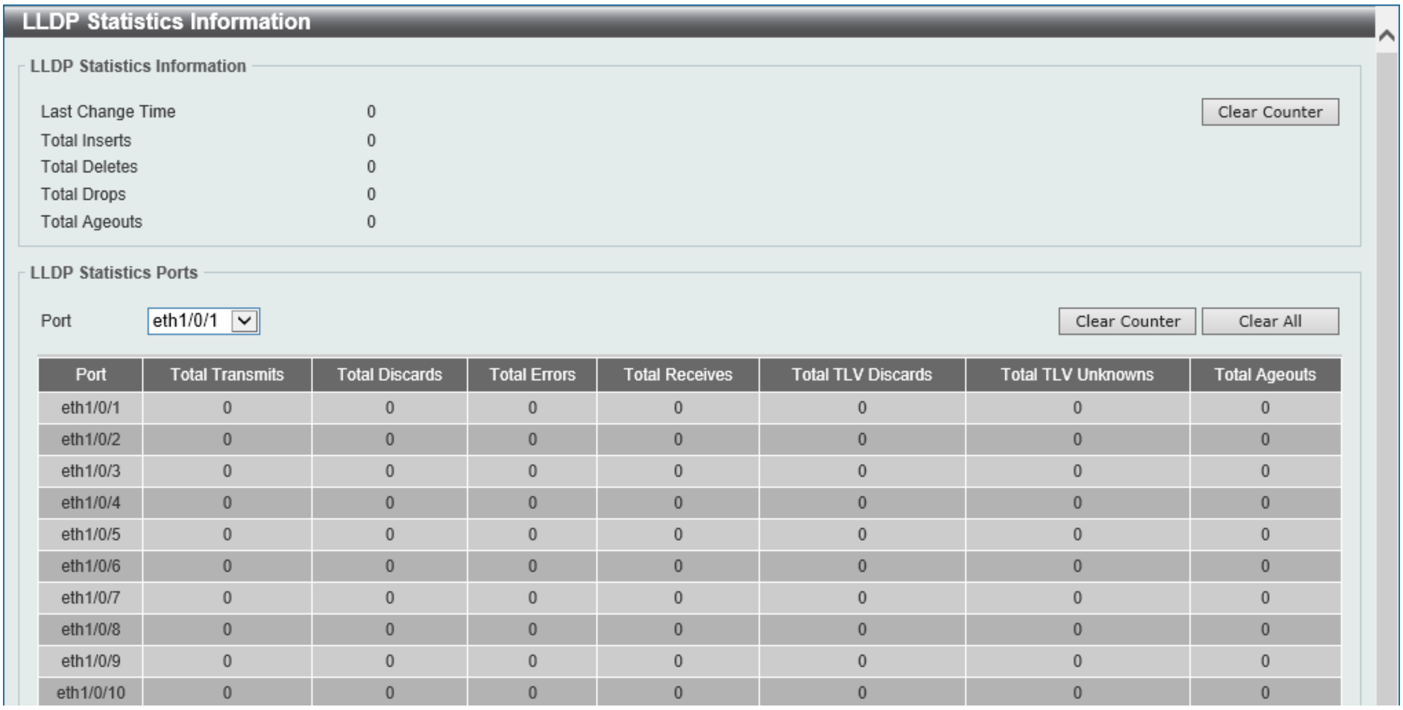
Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Notification	Select this option to enable or disable transmitting the LLDP-MED notification TLV.
Capabilities	Select this option to enable or disable transmitting the LLDP-MED capabilities TLV.
Inventory	Select this option to enable or disable transmitting the LLDP-MED inventory management TLV.
Network Policy	Select this option to enable or disable transmitting the LLDP-MED network policy TLV.
PSE	Select this option to enable or disable transmitting the LLDP-MED extended power via MDI TLV, if the local device is PSE device or PD device.

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

LLDP Statistics Information

This window is used to view the neighbor detection activity, LLDP Statistics, and the settings for individual ports on the Switch.

To view the following window, click **L2 Features > LLDP > LLDP Statistics Information**, as shown below:



LLDP Statistics Information

Last Change Time	0
Total Inserts	0
Total Deletes	0
Total Drops	0
Total Ageouts	0

LLDP Statistics Ports

Port: eth1/0/1

Port	Total Transmits	Total Discards	Total Errors	Total Receives	Total TLV Discards	Total TLV Unknowns	Total Ageouts
eth1/0/1	0	0	0	0	0	0	0
eth1/0/2	0	0	0	0	0	0	0
eth1/0/3	0	0	0	0	0	0	0
eth1/0/4	0	0	0	0	0	0	0
eth1/0/5	0	0	0	0	0	0	0
eth1/0/6	0	0	0	0	0	0	0
eth1/0/7	0	0	0	0	0	0	0
eth1/0/8	0	0	0	0	0	0	0
eth1/0/9	0	0	0	0	0	0	0
eth1/0/10	0	0	0	0	0	0	0

Figure 5-66 LLDP Statistics Information Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the port number that will be used here.

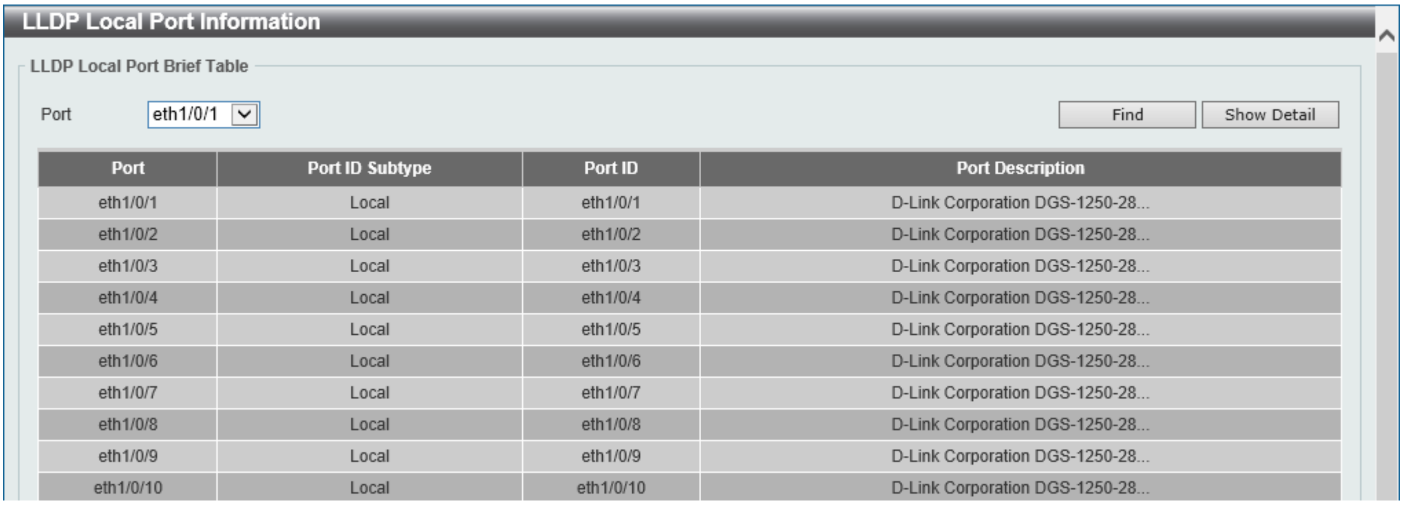
Click the **Clear Counter** button to clear the counter information for the statistics displayed.

Click the **Clear All** button to clear all the counter information displayed.

LLDP Local Port Information

This window is used to display the information currently available for populating outbound LLDP advertisements.

To view the following window, click **L2 Features > LLDP > LLDP Local Port Information**, as shown below:



LLDP Local Port Information

LLDP Local Port Brief Table

Port: eth1/0/1

Port	Port ID Subtype	Port ID	Port Description
eth1/0/1	Local	eth1/0/1	D-Link Corporation DGS-1250-28...
eth1/0/2	Local	eth1/0/2	D-Link Corporation DGS-1250-28...
eth1/0/3	Local	eth1/0/3	D-Link Corporation DGS-1250-28...
eth1/0/4	Local	eth1/0/4	D-Link Corporation DGS-1250-28...
eth1/0/5	Local	eth1/0/5	D-Link Corporation DGS-1250-28...
eth1/0/6	Local	eth1/0/6	D-Link Corporation DGS-1250-28...
eth1/0/7	Local	eth1/0/7	D-Link Corporation DGS-1250-28...
eth1/0/8	Local	eth1/0/8	D-Link Corporation DGS-1250-28...
eth1/0/9	Local	eth1/0/9	D-Link Corporation DGS-1250-28...
eth1/0/10	Local	eth1/0/10	D-Link Corporation DGS-1250-28...

Figure 5-67 LLDP Local Port Information Window

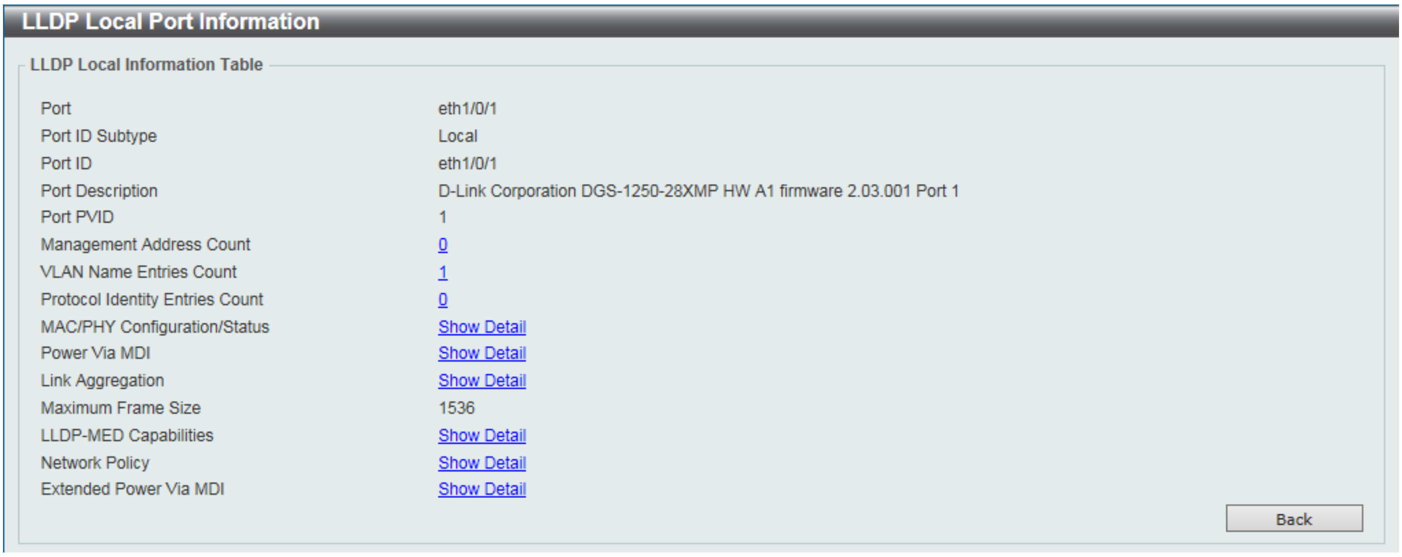
The fields that can be configured are described below:

Parameter	Description
Port	Select the port number that will be displayed.

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

Click the **Show Detail** button to view detailed information of the specific port.

After clicking the **Show Detail** button, the following window will appear.



LLDP Local Port Information

LLDP Local Information Table

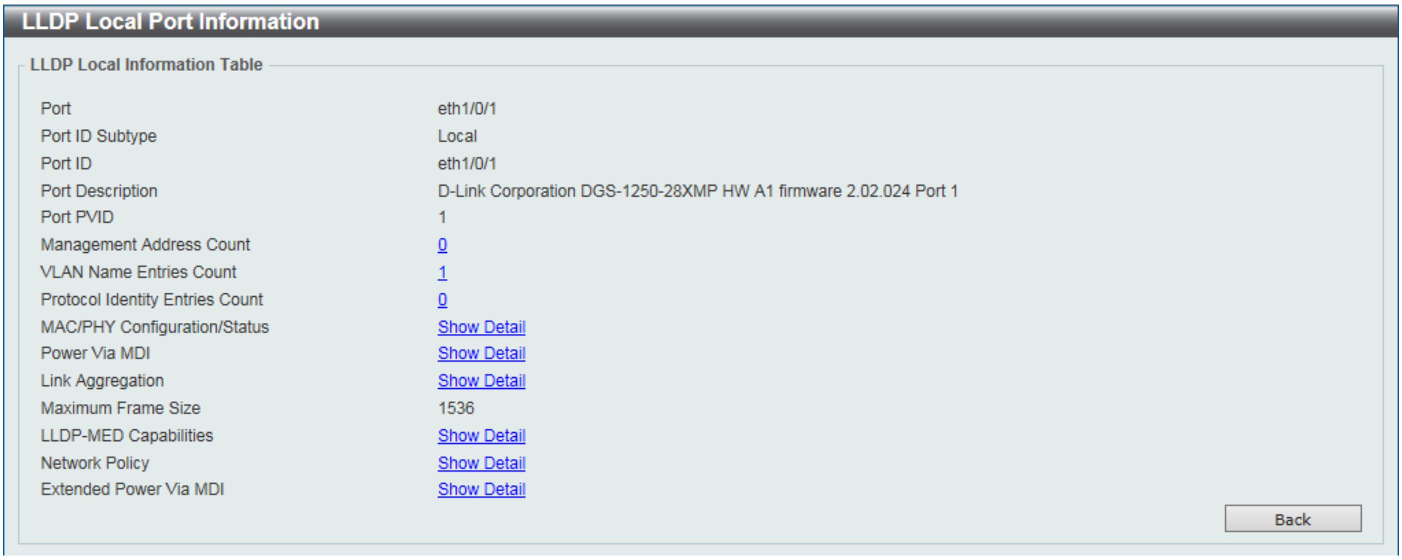
Port	eth1/0/1
Port ID Subtype	Local
Port ID	eth1/0/1
Port Description	D-Link Corporation DGS-1250-28XMP HW A1 firmware 2.03.001 Port 1
Port PVID	1
Management Address Count	0
VLAN Name Entries Count	1
Protocol Identity Entries Count	0
MAC/PHY Configuration/Status	Show Detail
Power Via MDI	Show Detail
Link Aggregation	Show Detail
Maximum Frame Size	1536
LLDP-MED Capabilities	Show Detail
Network Policy	Show Detail
Extended Power Via MDI	Show Detail

Figure 5-68 LLDP Local Port Information (Show Detail) Window

To view more details about, for example, the **MAC/PHY Configuration/Status**, click the Show Detail hyperlink.

Click the **Back** button to return to the previous window.

After clicking the Show Detail hyperlink, a new section will appear at the bottom of the window.



LLDP Local Port Information

LLDP Local Information Table

Port	eth1/0/1
Port ID Subtype	Local
Port ID	eth1/0/1
Port Description	D-Link Corporation DGS-1250-28XMP HW A1 firmware 2.02.024 Port 1
Port PVID	1
Management Address Count	0
VLAN Name Entries Count	1
Protocol Identity Entries Count	0
MAC/PHY Configuration/Status	Show Detail
Power Via MDI	Show Detail
Link Aggregation	Show Detail
Maximum Frame Size	1536
LLDP-MED Capabilities	Show Detail
Network Policy	Show Detail
Extended Power Via MDI	Show Detail

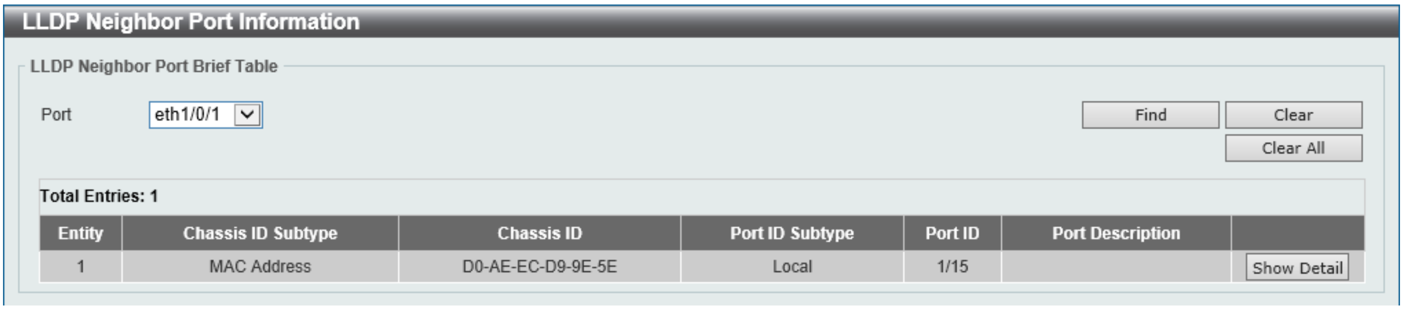
Figure 5-69 LLDP Local Port Information (Show Detail) Window

Click the **Back** button to return to the previous window.

LLDP Neighbor Port Information

This window is used to display the LLDP information learned from neighboring switches. The Switch receives packets from a remote station but is able to store the information locally.

To view the following window, click **L2 Features > LLDP > LLDP Neighbor Port Information**, as shown below:



LLDP Neighbor Port Information

LLDP Neighbor Port Brief Table

Port: eth1/0/1

Total Entries: 1

Entity	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	Port Description	
1	MAC Address	D0-AE-EC-D9-9E-5E	Local	1/15		Show Detail

Figure 5-70 LLDP Neighbor Port Information Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the port number that will be displayed.

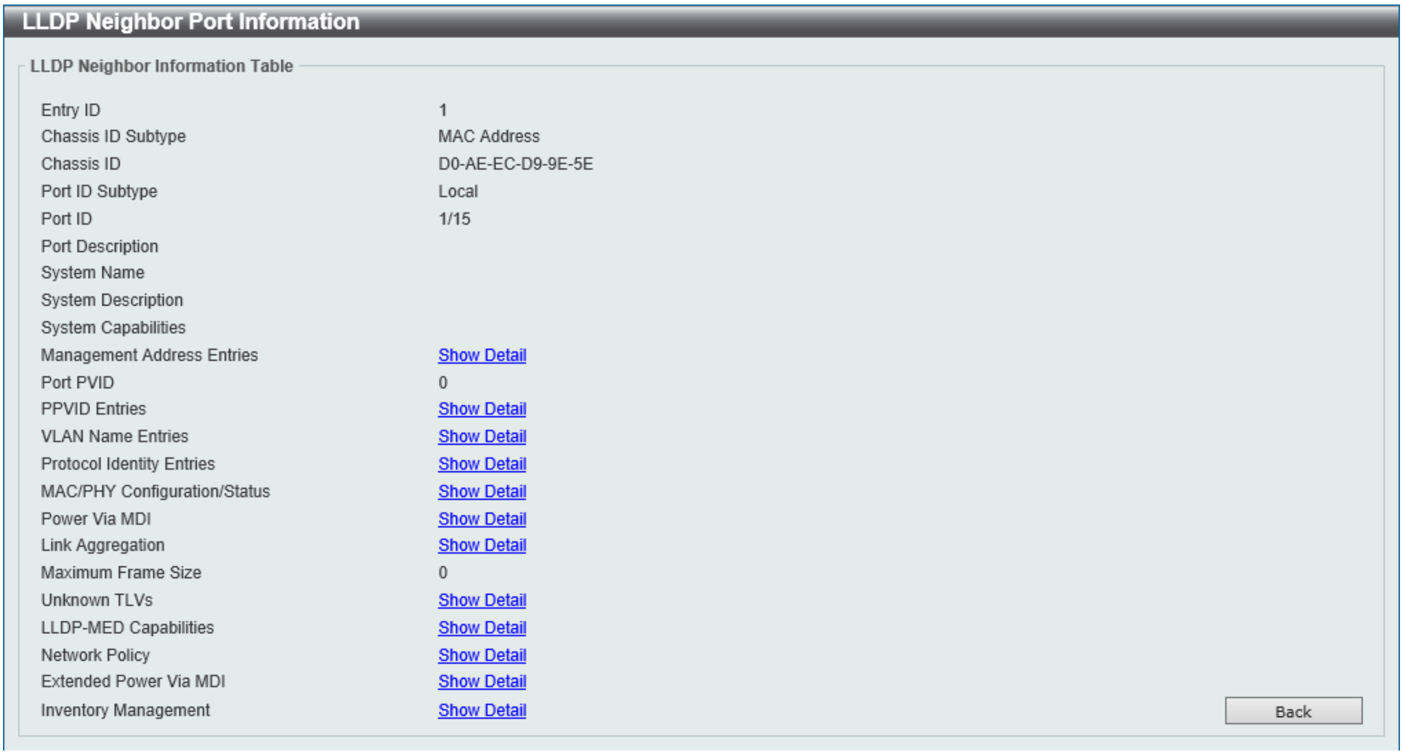
Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear** button to clear the specific port information.

Click the **Clear All** button to clear all the port information displayed.

Click the **Show Detail** button to view detailed information of the specific port.

After clicking the **Show Detail** button, the following window will appear.



LLDP Neighbor Port Information

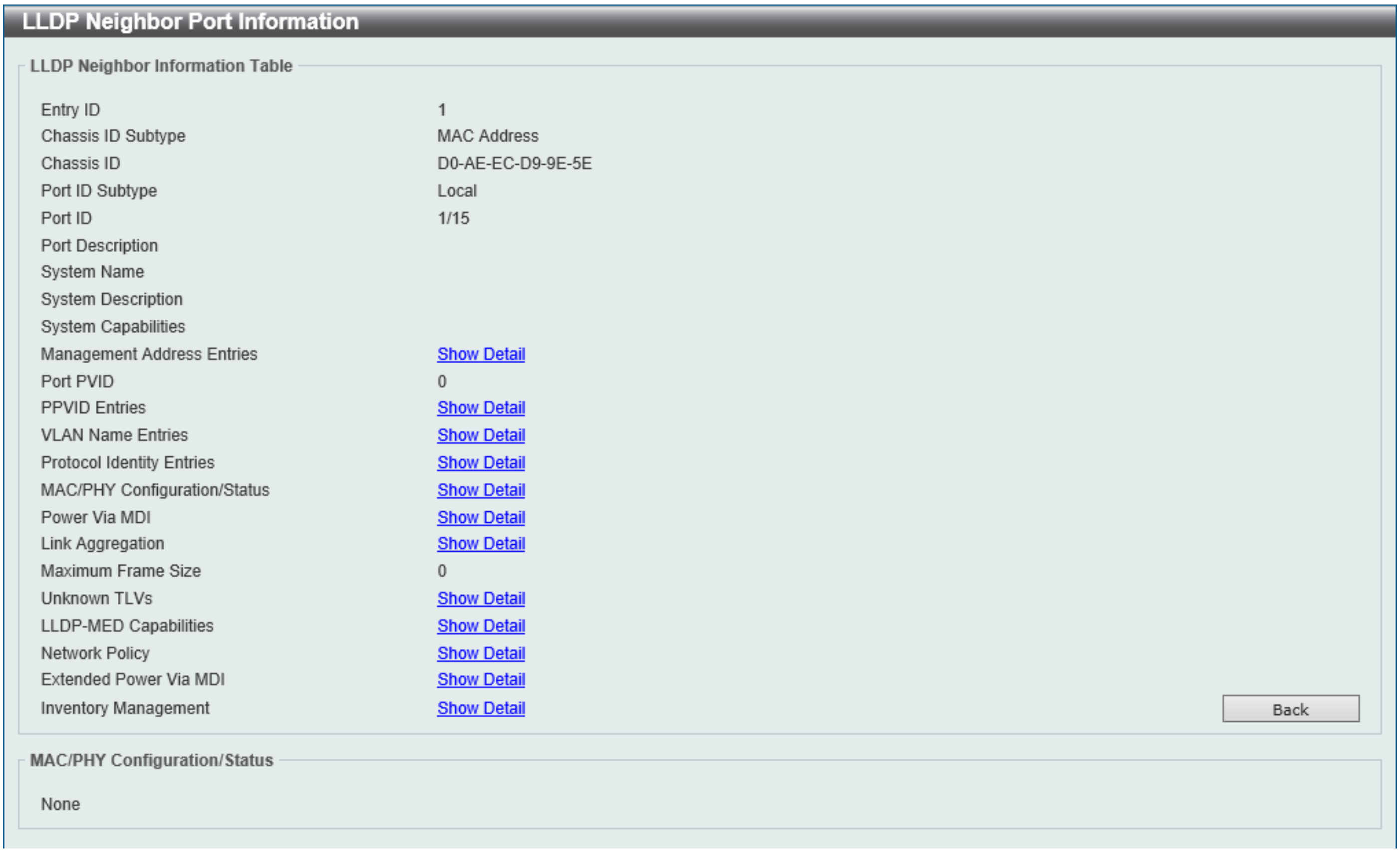
LLDP Neighbor Information Table

Entry ID	1
Chassis ID Subtype	MAC Address
Chassis ID	D0-AE-EC-D9-9E-5E
Port ID Subtype	Local
Port ID	1/15
Port Description	
System Name	
System Description	
System Capabilities	
Management Address Entries	Show Detail
Port PVID	0
PPVID Entries	Show Detail
VLAN Name Entries	Show Detail
Protocol Identity Entries	Show Detail
MAC/PHY Configuration/Status	Show Detail
Power Via MDI	Show Detail
Link Aggregation	Show Detail
Maximum Frame Size	0
Unknown TLVs	Show Detail
LLDP-MED Capabilities	Show Detail
Network Policy	Show Detail
Extended Power Via MDI	Show Detail
Inventory Management	Show Detail

Figure 5-71 LLDP Neighbor Port Information (Show Detail) Window

To view more details about, for example, the **MAC/PHY Configuration/Status**, click the Show Detail hyperlink. Click the **Back** button to return to the previous window.

After clicking the Show Detail hyperlink, a new section will appear at the bottom of the window.



LLDP Neighbor Port Information

LLDP Neighbor Information Table

Entry ID	1
Chassis ID Subtype	MAC Address
Chassis ID	D0-AE-EC-D9-9E-5E
Port ID Subtype	Local
Port ID	1/15
Port Description	
System Name	
System Description	
System Capabilities	
Management Address Entries	Show Detail
Port PVID	0
PPVID Entries	Show Detail
VLAN Name Entries	Show Detail
Protocol Identity Entries	Show Detail
MAC/PHY Configuration/Status	Show Detail
Power Via MDI	Show Detail
Link Aggregation	Show Detail
Maximum Frame Size	0
Unknown TLVs	Show Detail
LLDP-MED Capabilities	Show Detail
Network Policy	Show Detail
Extended Power Via MDI	Show Detail
Inventory Management	Show Detail

MAC/PHY Configuration/Status

None

Figure 5-72 LLDP Neighbor Port Information (Show Detail) Window

Click the **Back** button to return to the previous window.

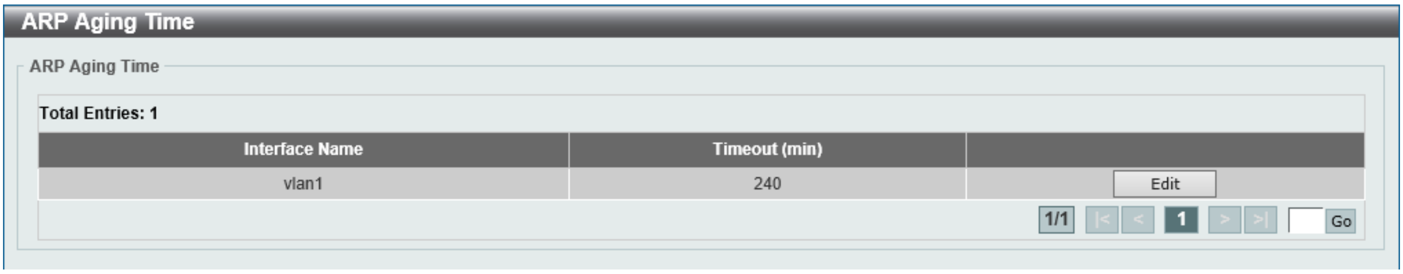
6. Layer 3 Features

ARP

ARP Aging Time

This window is used to display and configure the ARP aging time settings.

To view the following window, click **L3 Features > ARP > ARP Aging Time**, as shown below:



ARP Aging Time

ARP Aging Time

Total Entries: 1

Interface Name	Timeout (min)	
vlan1	240	Edit

Figure 6-1 ARP Aging Time Window

The fields that can be configured are described below:

Parameter	Description
Timeout	After click the **Edit** button, enter the ARP aging timeout value here. The range is from 0 to 65535. If this is 0, entries will never timeout.

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

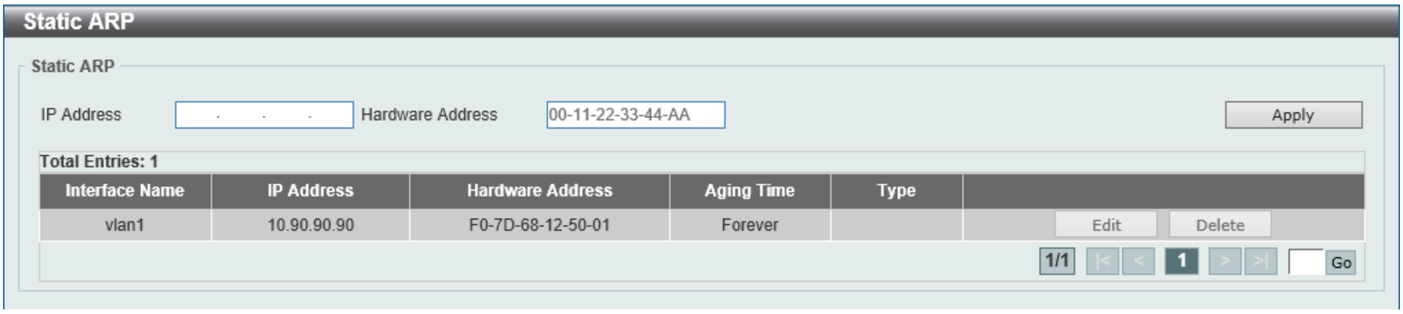
Click the **Apply** button to accept the changes made.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Static ARP

This window is used to display and configure the static ARP settings.

To view the following window, click **L3 Features > ARP > Static ARP**, as shown below:



IP Address: . . .
Hardware Address: 00-11-22-33-44-AA

Total Entries: 1

Interface Name	IP Address	Hardware Address	Aging Time	Type	
vlan1	10.90.90.90	F0-7D-68-12-50-01	Forever		Edit Delete

Figure 6-2 Static ARP Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the IP address that will be associated with the MAC address here.
Hardware Address	Enter the MAC address that will be associated with the IP address here.

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

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

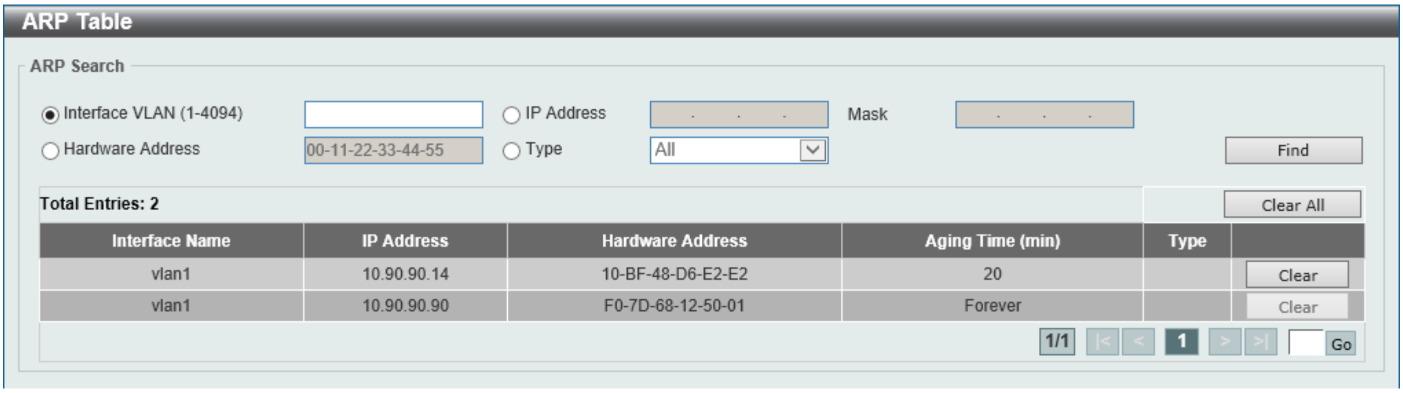
Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

ARP Table

This window is used to display and clear the dynamic ARP cache.

To view the following window, click **L3 Features > ARP > ARP Table**, as shown below:



● Interface VLAN (1-4094):
○ IP Address: . . .
Mask: . . .
○ Hardware Address: 00-11-22-33-44-55
○ Type: All

Total Entries: 2

Interface Name	IP Address	Hardware Address	Aging Time (min)	Type	
vlan1	10.90.90.14	10-BF-48-D6-E2-E2	20		Clear
vlan1	10.90.90.90	F0-7D-68-12-50-01	Forever		Clear

Figure 6-3 ARP Table Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the interface VLAN ID used here. This value must be between **1** and **4094**.
IP Address	Select and enter the IP address to display here.

Parameter	Description
Mask	After the **IP Address** option was selected, enter the mask address for the IP address here.
Hardware Address	Select and enter the MAC address to display here.
Type	Select the Type option here. Options to choose from are **All** and **Dynamic**.

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

Click the **Clear All** button to clear all dynamic ARP cache.

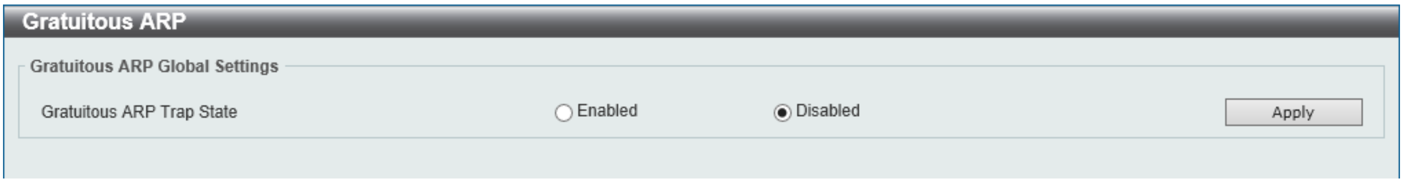
Click the **Clear** button to clear the dynamic ARP cache associated with the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Gratuitous ARP Trap

This window is used to configure the gratuitous ARP trap settings.

To view the following window, click **L3 Features > Gratuitous ARP**, as shown below:



Gratuitous ARP

Gratuitous ARP Global Settings

Gratuitous ARP Trap State ○ Enabled ● Disabled

Figure 6-4 Gratuitous ARP Trap Window

The fields that can be configured are described below:

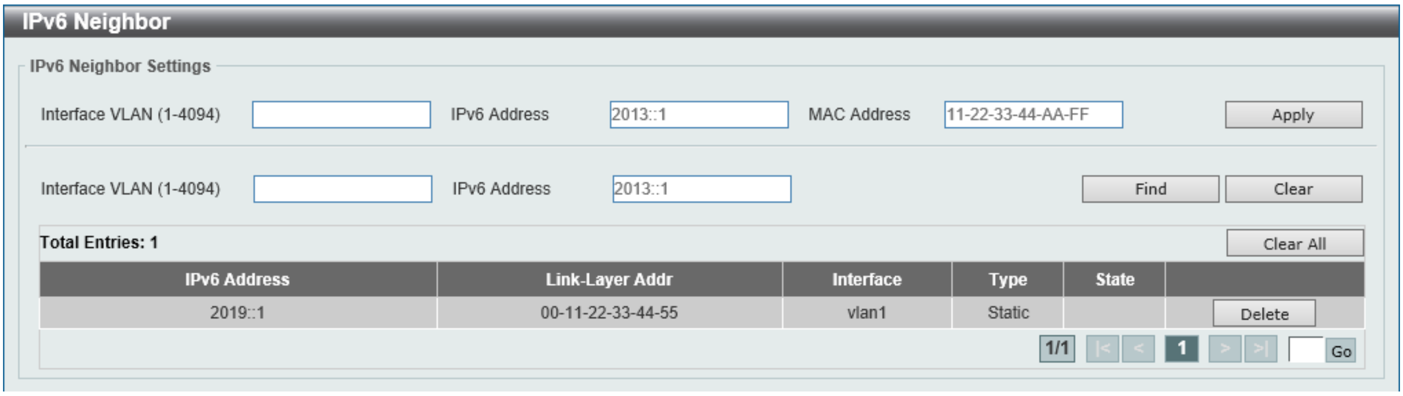
Parameter	Description
Gratuitous ARP Trap State	Select to enable or disable the gratuitous ARP trap state here. When the state is enabled and an IP address conflict occurs, this trap is sent.

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

IPv6 Neighbor

This window is used to display and configure the IPv6 neighbor settings.

To view the following window, click **L3 Features > IPv6 Neighbor**, as shown below:



IPv6 Neighbor

IPv6 Neighbor Settings

Interface VLAN (1-4094) IPv6 Address 2013::1 MAC Address 11-22-33-44-AA-FF

Interface VLAN (1-4094) IPv6 Address 2013::1

Total Entries: 1

IPv6 Address	Link-Layer Addr	Interface	Type	State	
2019::1	00-11-22-33-44-55	vlan1	Static		Delete

Figure 6-5 IPv6 Neighbor Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID here.
IPv6 Address	Enter the IPv6 address.
MAC Address	Enter the MAC address.

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 **Clear** button to clear all the dynamic information for the specific interface.

Click the **Clear All** button to clear all the dynamic IPv6 neighbor information in this table.

Click the **Delete** button to remove the specific entry.

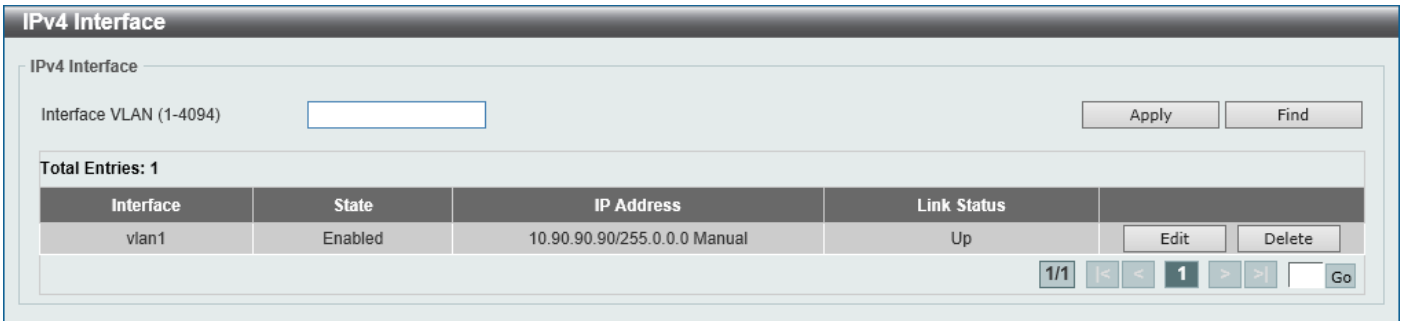
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Interface

IPv4 Interface

This window is used to display and configure the IPv4 interface settings.

To view the following window, click **L3 Features > Interface > IPv4 Interface**, as shown below:



IPv4 Interface

IPv4 Interface

Interface VLAN (1-4094)

Total Entries: 1

Interface	State	IP Address	Link Status	
vlan1	Enabled	10.90.90.90/255.0.0.0 Manual	Up	Edit Delete

Figure 6-6 IPv4 Interface Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the interface VLAN ID here. This value must be between 1 and 4094.

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

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Edit** button, the following page will be available.

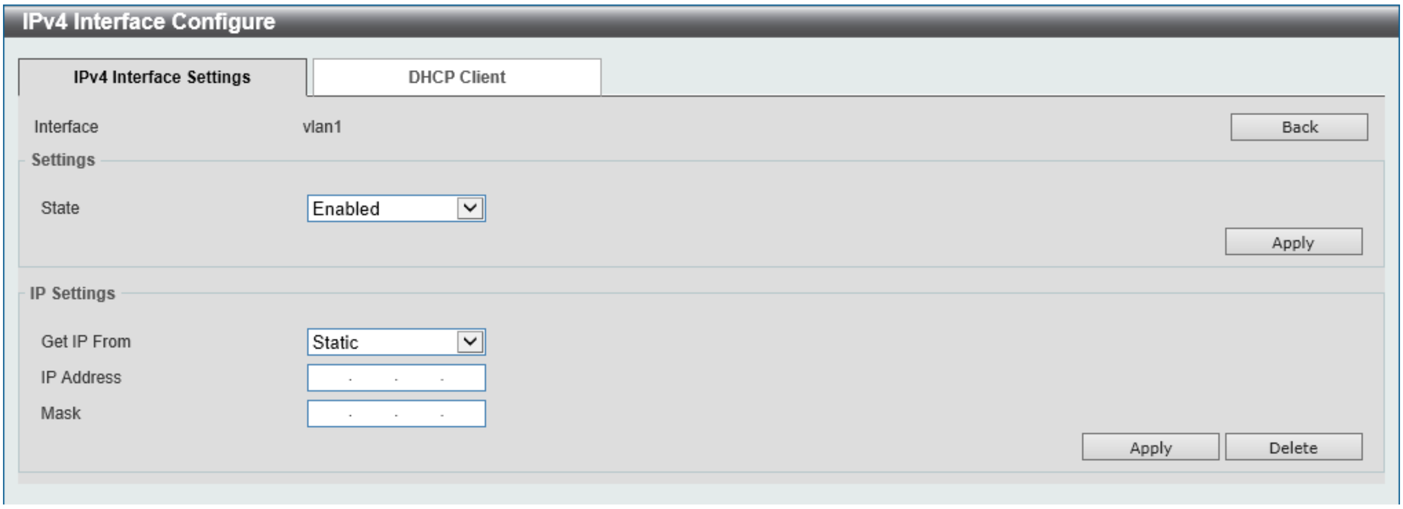


Figure 6-7 IPv4 Interface (Edit) Window

The fields that can be configured in the **Settings** section are described below:

Parameter	Description
State	Select to enable or disable the IPv4 interface global state.

Click the **Back** button to return to the previous window.

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

The fields that can be configured in the **Primary IP Settings** section are described below:

Parameter	Description
Get IP From	Select the get IP from option here. Options to choose from are: • When the **Static** option is selected, users can enter the IPv4 address of this interface manually in the fields provided. • When the **DHCP** option is selected, this interface will obtain IPv4 information automatically from the DHCP server located on the local network.
IP Address	Enter the primary IPv4 address for this interface here.
Mask	Enter the primary IPv4 subnet mask for this interface here.

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

Click the **Delete** button to remove the specific entry.

After selecting the **DHCP Client** tab, the following page will appear.

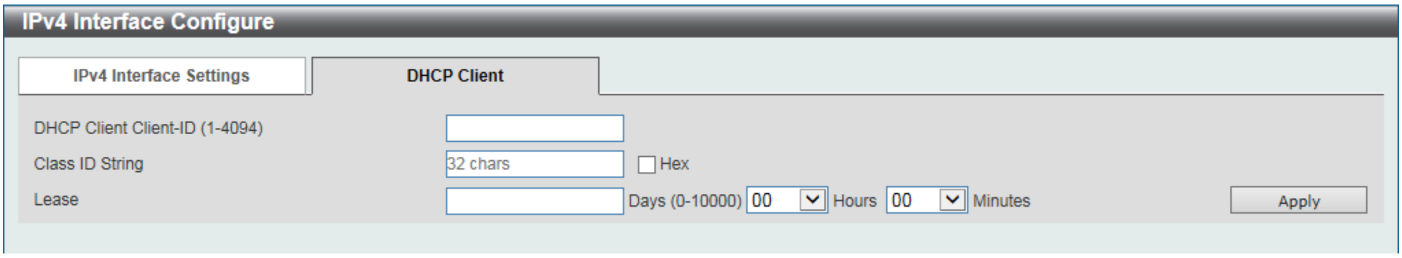


Figure 6-8 IPv4 Interface (Edit, DHCP Client) Window

The fields that can be configured are described below:

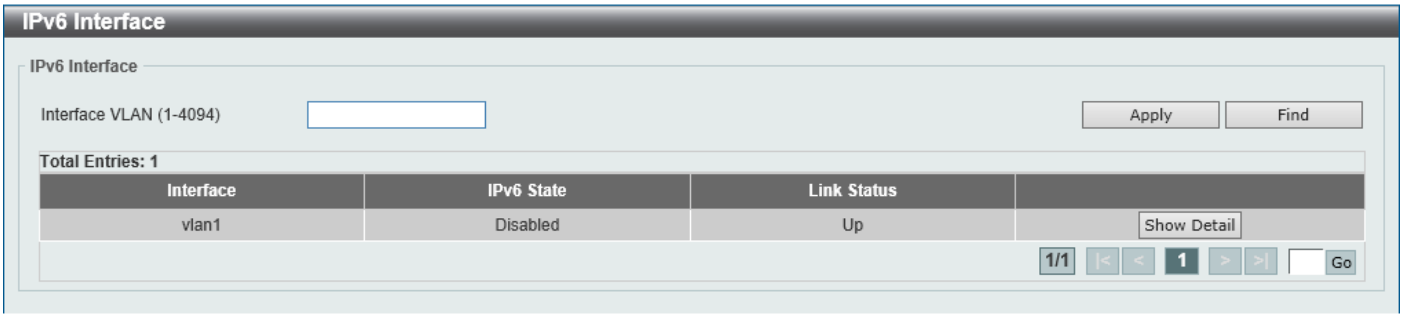
Parameter	Description
DHCP Client Client-ID	Enter the DHCP Client ID here. The range is from 1 to 4094. This parameter is used to specify the VLAN interface whose hexadecimal MAC address will be used as the client ID sent with the discover message.
Class ID String	Enter the class ID string here. This string can be up to 32 characters long. Select the **Hex** option to enter the Class ID string in the hexadecimal format. This string can be up to 64 characters long. This parameter is used to specify the vendor class identifier used as the value of Option 60 in the DHCP discover message.
Lease	Enter and optionally select the DHCP client lease time here. In the text box, the lease time, in days, can be entered. The range is from 0 to 10000 days. **Hours** and **Minutes** can also be selected optionally.

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

IPv6 Interface

This window is used to display and configure the IPv6 interface settings.

To view the following window, click **L3 Features > Interface > IPv6 Interface**, as shown below:



IPv6 Interface

IPv6 Interface

Interface VLAN (1-4094)

Total Entries: 1

Interface	IPv6 State	Link Status	
vlan1	Disabled	Up	Show Detail

Figure 6-9 IPv6 Interface Window

The fields that can be configured in **IPv6 Interface** are described below:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID that will be associated with the IPv6 entry.

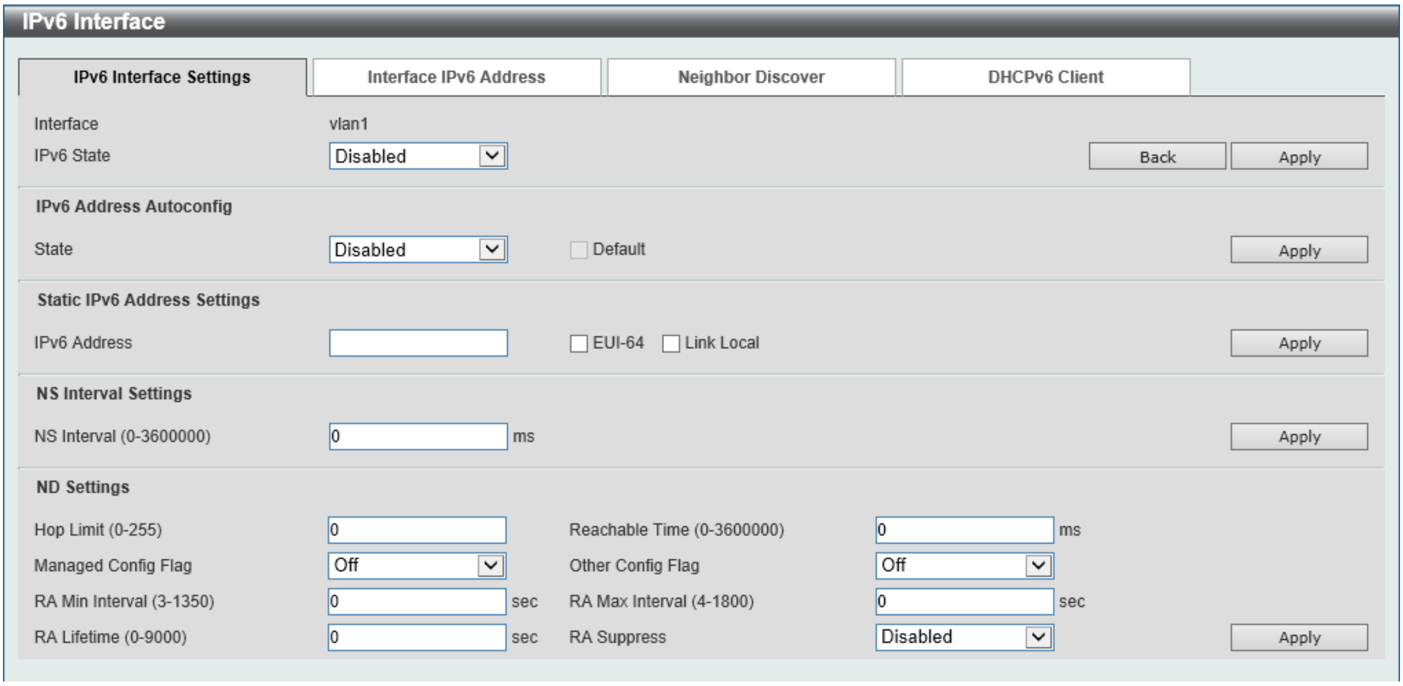
Click the **Apply** button to accept the changes made.

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

Click the **Show Detail** button to view and configure detailed settings for the IPv6 interface entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Show Detail** button, the following page will be available.



Interface: vlan1
IPv6 State: Disabled

IPv6 Address Autoconfig

State: Disabled □ Default

Static IPv6 Address Settings

IPv6 Address: □ EUI-64 □ Link Local

NS Interval Settings

NS Interval (0-3600000): 0 ms

ND Settings

Hop Limit (0-255): 0
Reachable Time (0-3600000): 0 ms
Managed Config Flag: Off
Other Config Flag: Off
RA Min Interval (3-1350): 0 sec
RA Max Interval (4-1800): 0 sec
RA Lifetime (0-9000): 0 sec
RA Suppress: Disabled

Figure 6-10 IPv6 Interface (Detail, IPv6 Interface Settings) Window

The fields that can be configured are described below:

Parameter	Description
IPv6 State	Select to enable or disable the IPv6 interface global state here.

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

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

The fields that can be configured for **IPv6 Address Autoconfig** are described below:

Parameter	Description
State	Select to enable or disable the automatic configuration of the IPv6 address using stateless auto-configuration here. Select the **Default** option to insert the default route to the IPv6 routing table based on the received router advertisement. The type of the default route is SLAAC.

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

The fields that can be configured for **Static IPv6 Address Settings** are described below:

Parameter	Description
IPv6 Address	Enter the IPv6 address for this IPv6 interface here. Select the **EUI-64** option to configure an IPv6 address on the interface using the EUI-64 interface ID. Select the **Link Local** option to configure a link-local address for the IPv6 interface.

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

The fields that can be configured for **NS Interval Settings** are described below:

Parameter	Description
NS Interval	Enter the Neighbor Solicitation (NS) interval value here. The range is from 0 to 3600000 milliseconds, in multiples of 1000. If the specified time is 0, the router will

Parameter	Description
	use 1 second on the interface and advertise 0 (unspecified) in the Router Advertisement (RA) message.

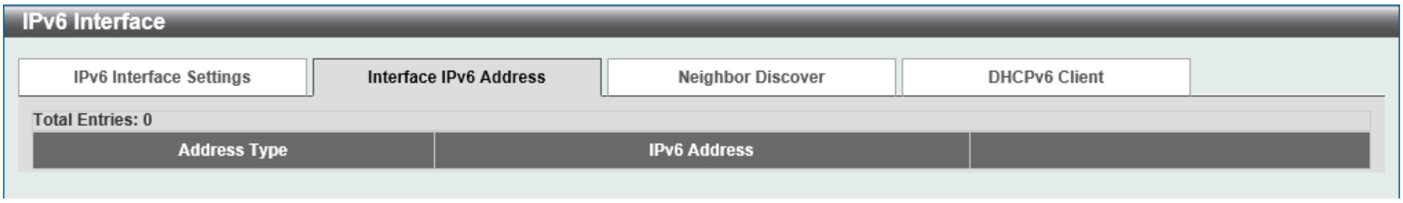
Click the **Apply** button to accept the changes made.

The fields that can be configured for **ND Settings** are described below:

Parameter	Description
Hop Limit	Enter the hop limit value here. The range is from 0 to 255. The IPv6 packet originated by the system will also use this value as the initial hop limit.
Reachable Time	Enter the Reachable Time here. The range is from 0 to 3600000 milliseconds. If the specified time is 0, the router will use 1200 seconds on the interface and advertise 0 (unspecified) in the RA message. The Reachable Time is used by the IPv6 node in determining the reachability of the neighbor nodes.
Managed Config Flag	Turn the Managed Config Flag option **On** or **Off** here. When the neighbor host receives the RA which has flag turned on, the host should use a stateful configuration protocol to obtain IPv6 addresses.
Other Config Flag	Turn the Other Config Flag option **On** or **Off** here. By setting the other configuration flag on, the router instructs the connected hosts to use a stateful configuration protocol to obtain auto-configuration information other than the IPv6 address.
RA Min Interval	Enter the minimum RA interval time value here. The range is from 3 to 1350 seconds. This value must be smaller than 0.75 times the maximum value.
RA Max Interval	Enter the maximum RA interval time value here. The range is from 4 to 1800 seconds.
RA Lifetime	Enter the RA lifetime value here. The range is from 0 to 9000 seconds. The lifetime value in RA instructs the received host the lifetime value for taking the router as the default router.
RA Suppress	Select to enable or disable the RA suppress feature here.

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

After clicking the **Interface IPv6 Address** tab, at the top of the page, the following page will be available.



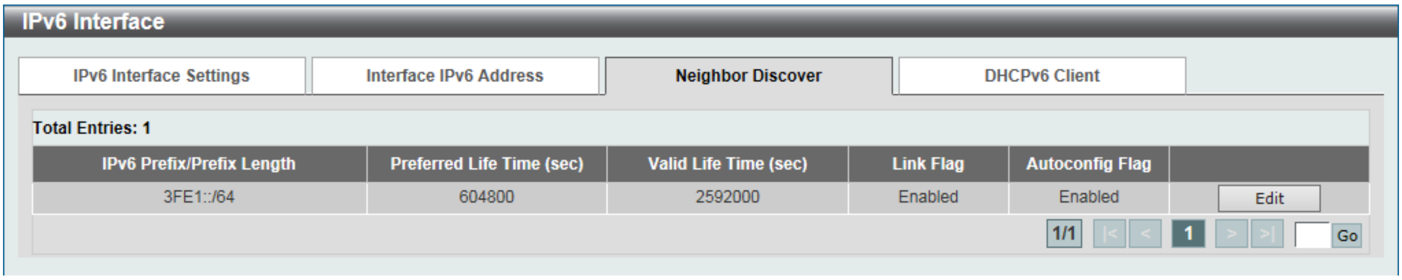
Total Entries: 0

Address Type	IPv6 Address	

Figure 6-11 IPv6 Interface (Detail, Interface IPv6 Address) Window

Click the **Delete** button to delete the specified entry.

After clicking the **Neighbor Discover** tab, at the top of the page, the following page will be available.

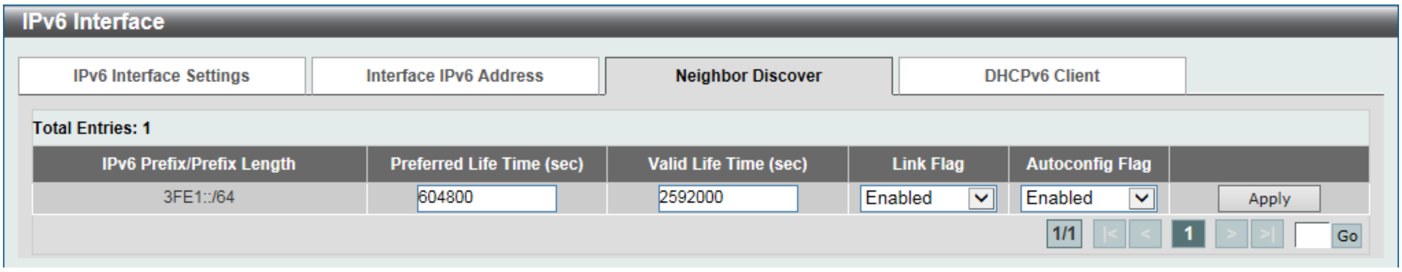


Total Entries: 1

IPv6 Prefix/Prefix Length	Preferred Life Time (sec)	Valid Life Time (sec)	Link Flag	Autoconfig Flag	
3FE1::/64	604800	2592000	Enabled	Enabled	Edit

Figure 6-12 IPv6 Interface (Detail, Neighbor Discover) Window

Click the **Edit** button to configure the following parameters:



Total Entries: 1

IPv6 Prefix/Prefix Length	Preferred Life Time (sec)	Valid Life Time (sec)	Link Flag	Autoconfig Flag	
3FE1::/64	604800	2592000	Enabled	Enabled	Apply

Figure 6-13 IPv6 Interface (Detail, Neighbor Discover, Edit) Window

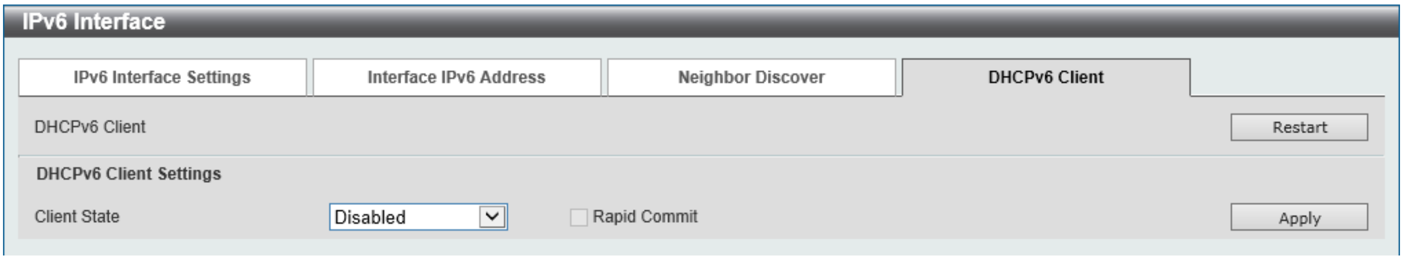
The fields that can be configured are described below:

Parameter	Description
Preferred Life Time	Enter the preferred lifetime value here. The range is from 0 to 4294967295 seconds. The default value is 604800 seconds (7 days).
Valid Life Time	Enter the valid lifetime value here. The range is from 0 to 4294967295 seconds. The default value is 2592000 seconds (30 days).
Link Flag	Select to enable or disable the on-link flag here. The default option is **Enabled**.
Autoconfig Flag	Select to enable or disable the auto-configure flag here. The default option is **Enabled**.

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

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **DHCPv6 Client** tab, at the top of the page, the following page will be available.



DHCPv6 Client

DHCPv6 Client Settings

Client State: Disabled
□ Rapid Commit

Figure 6-14 IPv6 Interface (Detail, DHCPv6 Client) Window

Click the **Restart** button to restart the DHCPv6 client service.

The fields that can be configured for **DHCPv6 Client Settings** are described below:

Parameter	Description
Client State	Select to enable or disable the DHCPv6 client service here. Select the **Rapid Commit** option to proceed with two-message exchange for address delegation. The rapid-commit option will be included in the Solicit message to request a two-message handshake.

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

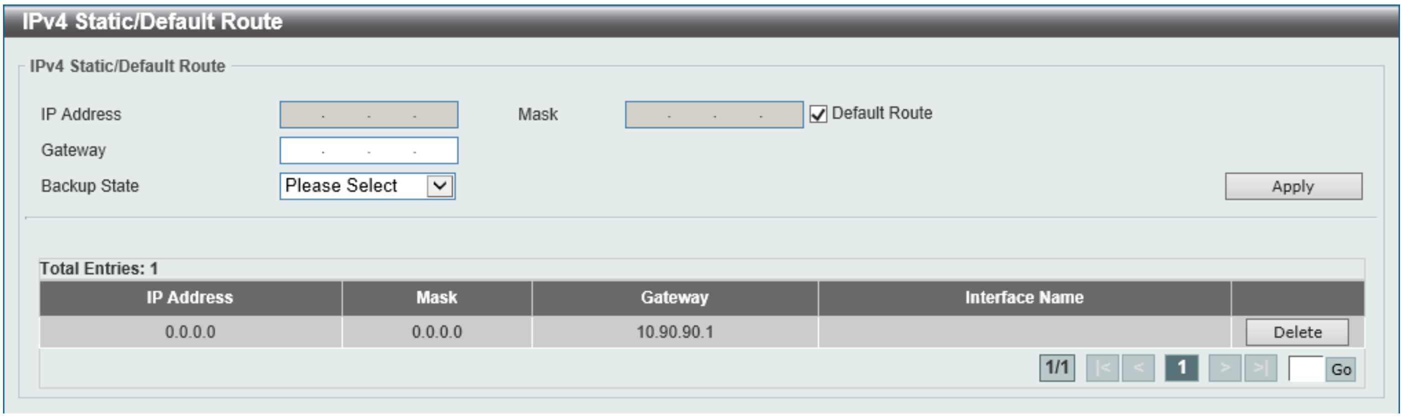
IPv4 Static/Default Route

This window is used to display and configure the IPv4 static and default route settings. The Switch supports static routing for IPv4 formatted addressing. Users can create up to 124 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 with a different next hop. This secondary next hop device route is considered as a backup static route when the primary static route is down. If the primary route is lost, the backup route will become active and begin forwarding traffic.

Entries into the Switch's forwarding table can be made using an IP address, subnet mask, and gateway.

To view the following window, click **L3 Features > IPv4 Static/Default Route**, as shown below:



IPv4 Static/Default Route

IPv4 Static/Default Route

IP Address: . . . Mask: . . . ☑ Default Route

Gateway: . . .

Backup State: Please Select

Total Entries: 1

IP Address	Mask	Gateway	Interface Name	
0.0.0.0	0.0.0.0	10.90.90.1		Delete

Figure 6-15 IPv4 Static/Default Route Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the IPv4 address for this route here. Tick the **Default Route** option to use the default route as the IPv4 address.
Mask	Enter the IPv4 network mask for this route here.
Gateway	Enter the gateway address for this route here.
Backup State	Select the backup state option here. Options to choose from are: • **Primary** - Specifies the route as the primary route to the destination. • **Backup** - Specifies the route as the backup route to the destination.

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

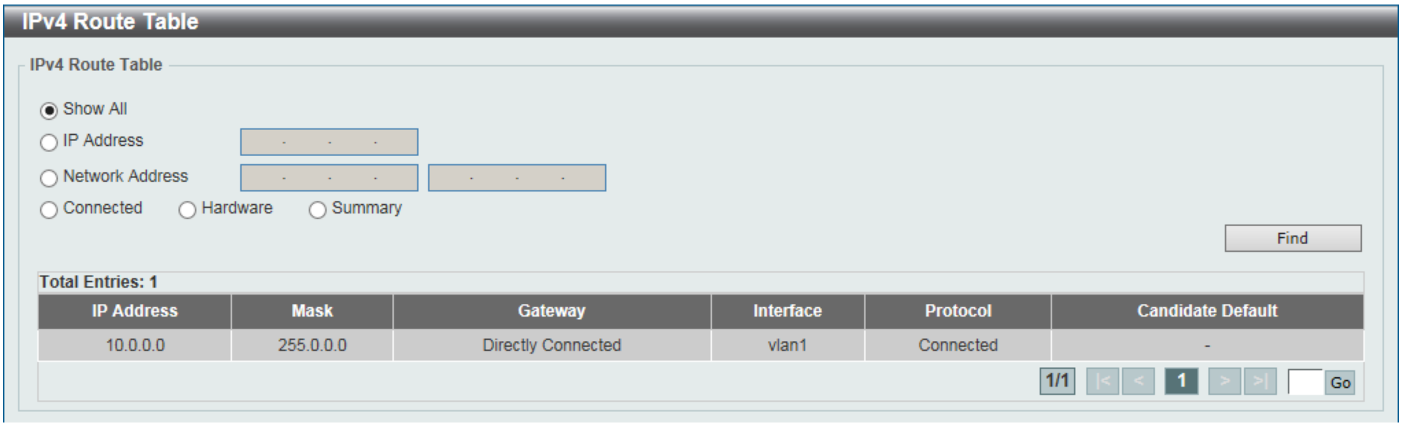
Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IPv4 Route Table

This window is used to display and configure the IPv4 route table settings.

To view the following window, click **L3 Features > IPv4 Route Table**, as shown below:



IPv4 Route Table

IPv4 Route Table

● Show All

○ IP Address

○ Network Address

○ Connected ○ Hardware ○ Summary

Total Entries: 1

IP Address	Mask	Gateway	Interface	Protocol	Candidate Default
10.0.0.0	255.0.0.0	Directly Connected	vlan1	Connected	-

Figure 6-16 IPv4 Route Table Window

The fields that can be configured are described below:

Parameter	Description
Show All	Select this option to display all IPv4 routes.
IP Address	Select and enter the single IPv4 address here.
Network Address	Select and enter the IPv4 network address here. In the first space enter the network prefix and in the second space enter the network mask.
Connected	Select this option to display only connected routes.
Hardware	Select this option to display only hardware routes. Hardware routes are routes that have been written into the hardware chip.
Summary	Select this option to display a summary and count of the route sources configured on this Switch.

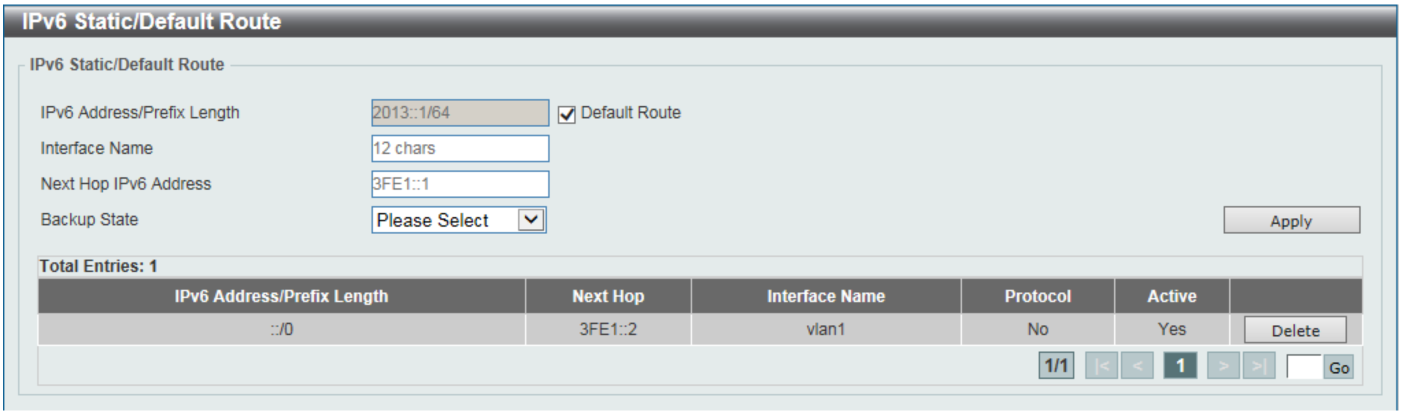
Click the **Find** button to locate a specific entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IPv6 Static/Default Route

This window is used to display and configure the IPv6 static or default routes.

To view the following window, click **L3 Features > IPv6 Static/Default Route**, as shown below:



IPv6 Static/Default Route

IPv6 Static/Default Route

IPv6 Address/Prefix Length: 2013::1/64 ☑ Default Route

Interface Name: 12 chars

Next Hop IPv6 Address: 3FE1::1

Backup State: Please Select

Total Entries: 1

IPv6 Address/Prefix Length	Next Hop	Interface Name	Protocol	Active	
::/0	3FE1::2	vlan1	No	Yes	Delete

Figure 6-17 IPv6 Static/Default Route Window

The fields that can be configured are described below:

Parameter	Description
IPv6 Address/Prefix Length	Enter the IPv6 address and prefix length for this route here. Tick the **Default Route** option to use this route as the default route.
Interface Name	Enter the name of the interface that will be associated with this route here.
Next Hop IPv6 Address	Enter the next hop IPv6 address here.
Backup State	Select the backup state option here. Options to choose from are **Primary**, and **Backup**. When the **Primary** option is selected, the route is specified as the primary route to the destination. When the **Backup** option is selected, the route is specified as the backup route to the destination.

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

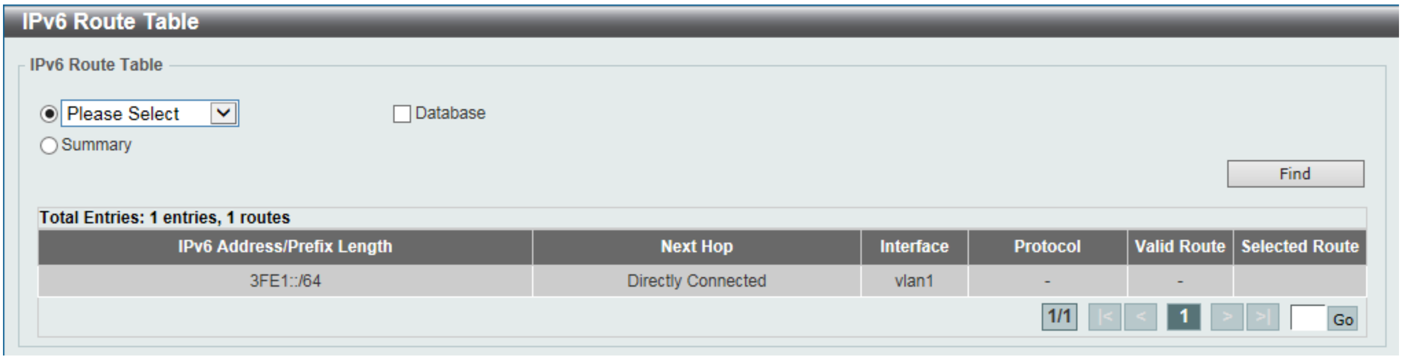
Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IPv6 Route Table

This window is used to display and configure the IPv6 route table.

To view the following window, click **L3 Features > IPv6 Route Table**, as shown below:



IPv6 Route Table

IPv6 Route Table

● Please Select ☐ Database

○ Summary

Total Entries: 1 entries, 1 routes

IPv6 Address/Prefix Length	Next Hop	Interface	Protocol	Valid Route	Selected Route
3FE1::/64	Directly Connected	vlan1	-	-	

Figure 6-18 IPv6 Route Table Window

The fields that can be configured are described below:

Parameter	Description
Connected	Select this option to display only connected routes.
Database	Select this option to display all the related entries in the routing database instead of just the best route.
Summary	Select this option to display a summary and count of the route sources configured on this Switch.

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

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

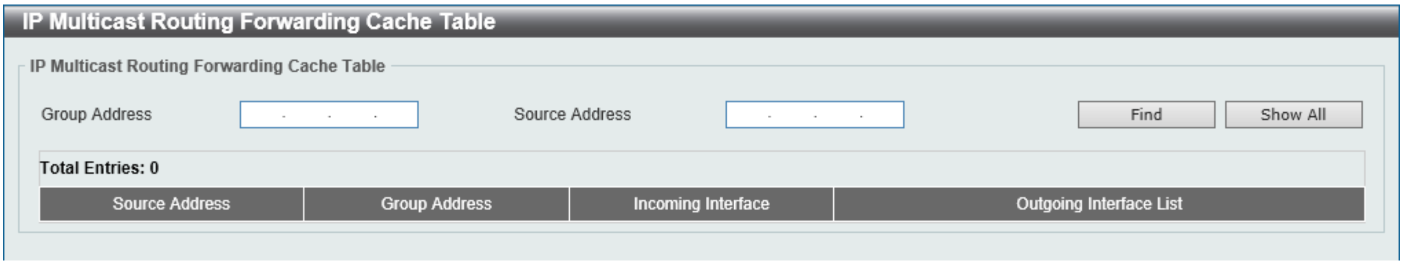
IP Multicast Routing Protocol

IPMC

IP Multicast Routing Forwarding Cache Table

This window is used to display the content of the IP multicast routing forwarding cache database.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > IPMC > IP Multicast Routing Forwarding Cache Table**, as shown below:



IP Multicast Routing Forwarding Cache Table

IP Multicast Routing Forwarding Cache Table

Group Address: . . .

Source Address: . . .

Total Entries: 0

Source Address	Group Address	Incoming Interface	Outgoing Interface List

Figure 6-19 IP Multicast Routing Forwarding Cache Table Window

The fields that can be configured are described below:

Parameter	Description
Group Address	Enter the multicast group IP address here.
Source Address	Enter the source IP address here.

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

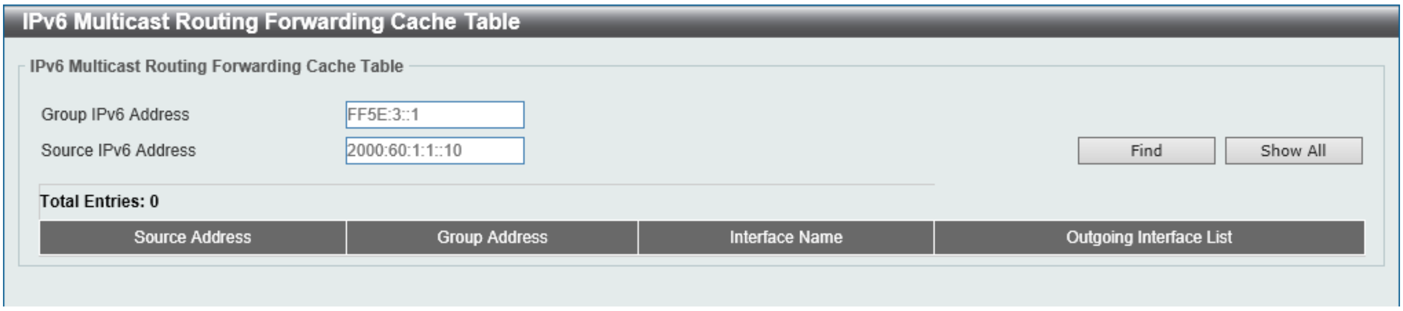
Click the **Show All** button to display all the entries.

IPv6MC

IPv6 Multicast Routing Forwarding Cache Table

This window is used to display the contents of the IPv6 multicast routing forwarding cache database.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > IPv6MC > IPv6 Multicast Routing Forwarding Cache Table**, as shown below:


IPv6 Multicast Routing Forwarding Cache Table
IPv6 Multicast Routing Forwarding Cache Table
Find
Show All

Group IPv6 Address: FF5E:3::1

Source IPv6 Address: 2000:60:1:1::10

Total Entries: 0

Source Address	Group Address	Interface Name	Outgoing Interface List

Figure 6-20 IPv6 Multicast Routing Forwarding Cache Table Window

The fields that can be configured are described below:

Parameter	Description
Group IPv6 Address	Enter the multicast group IPv6 address here.
Source IPv6 Address	Enter the source IPv6 address here.

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

Click the **Show All** button to display all the entries.

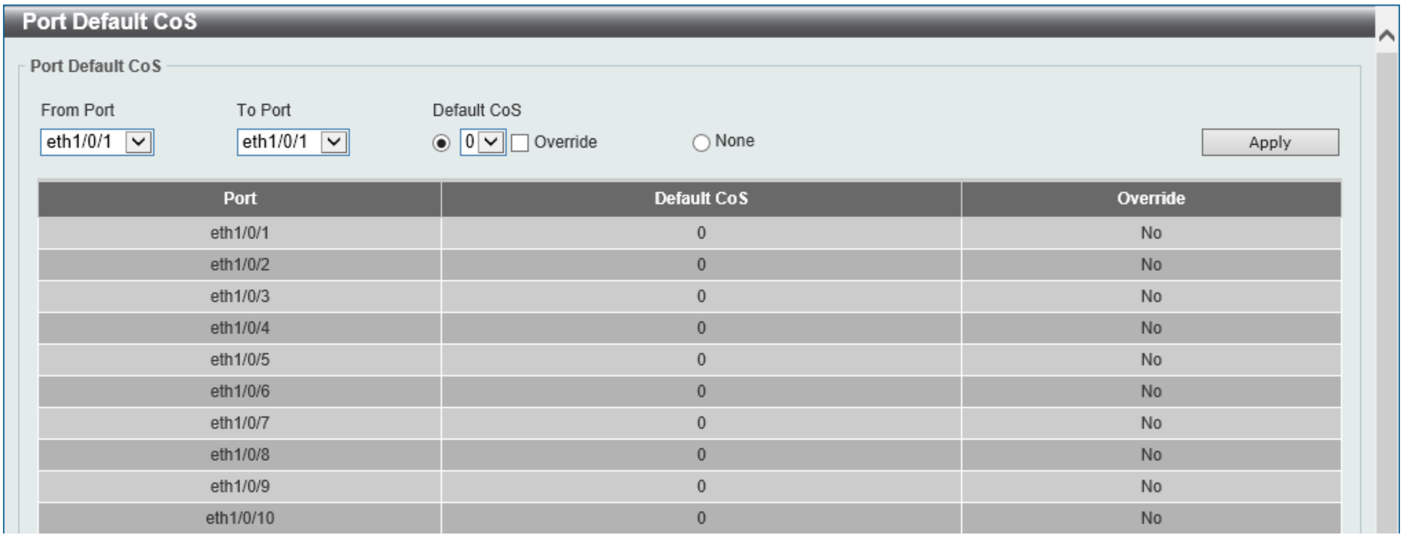
7. Quality of Service (QoS)

Basic Settings

Port Default CoS

This window is used to display and configure the port default CoS settings.

To view the following window, click **QoS > Basic Settings > Port Default CoS**, as shown below:



Port Default CoS

Port Default CoS

From Port: eth1/0/1
To Port: eth1/0/1
Default CoS: ● 0 □ Override ○ None

Port	Default CoS	Override
eth1/0/1	0	No
eth1/0/2	0	No
eth1/0/3	0	No
eth1/0/4	0	No
eth1/0/5	0	No
eth1/0/6	0	No
eth1/0/7	0	No
eth1/0/8	0	No
eth1/0/9	0	No
eth1/0/10	0	No

Figure 7-1 Port Default CoS Window

The fields that can be configured are described below:

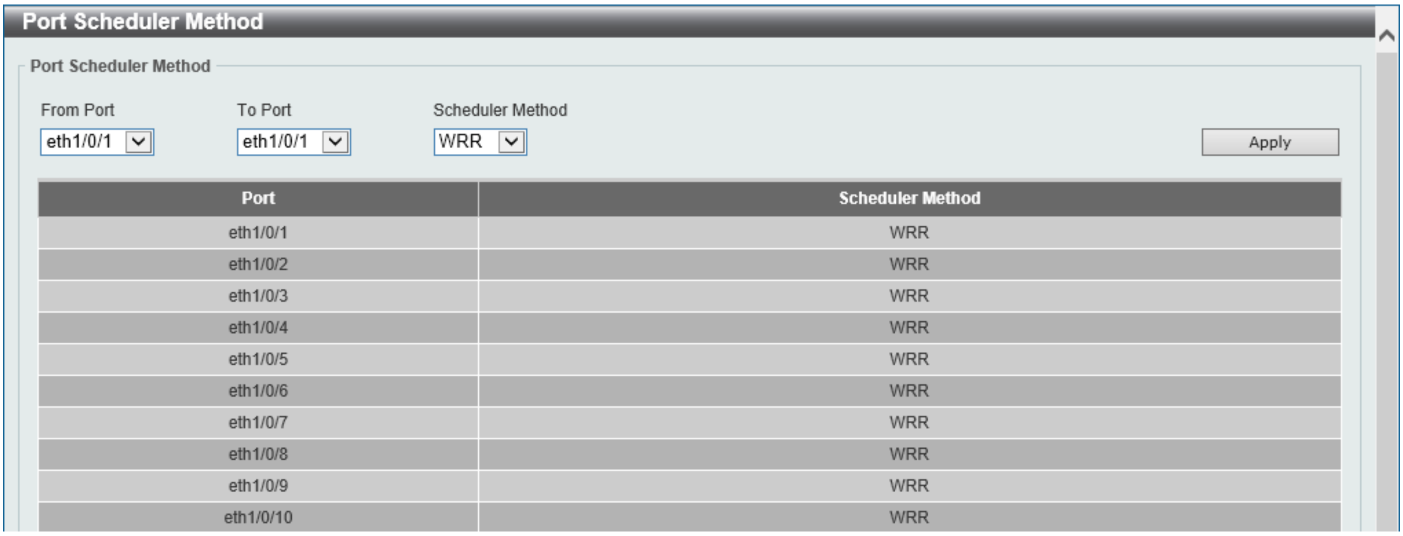
Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
Default CoS	Select the default CoS option for the port(s) specified here. Options to choose from are 0 to 7. Select the **Override** option to override the CoS of the packets. The default CoS will be applied to all incoming packets, tagged or untagged, received by the port. Select the **None** option to specify that the CoS of the packets will be the packet’s CoS if the packets are tagged, and will be the port default CoS if the packet is untagged.

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

Port Scheduler Method

This window is used to display and configure the port scheduler method settings.

To view the following window, click **QoS > Basic Settings > Port Scheduler Method**, as shown below:



Port Scheduler Method

Port Scheduler Method

From Port: eth1/0/1
To Port: eth1/0/1
Scheduler Method: WRR

Port	Scheduler Method
eth1/0/1	WRR
eth1/0/2	WRR
eth1/0/3	WRR
eth1/0/4	WRR
eth1/0/5	WRR
eth1/0/6	WRR
eth1/0/7	WRR
eth1/0/8	WRR
eth1/0/9	WRR
eth1/0/10	WRR

Figure 7-2 Port Scheduler Method Window

The fields that can be configured are described below:

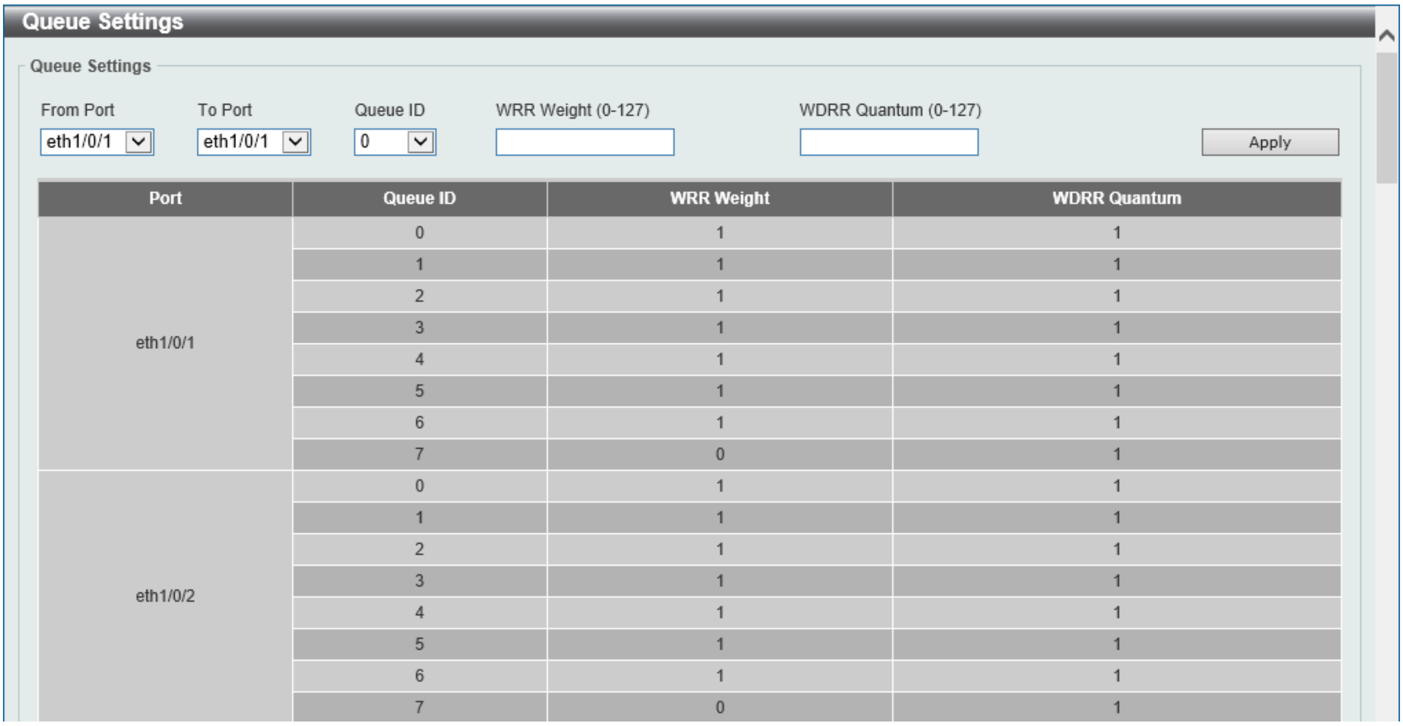
Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
Scheduler Method	Select the scheduler method that will be applied to the specified port(s). Options to choose from are: • **SP** (Strict Priority) - Specifies that all queues use strict priority scheduling. It provides strict priority access to the queues from the highest CoS queue to the lowest. • **RR** (Round-Robin) - Specifies that all queues use round-robin scheduling. It provides fair access to service a single packet at each queue before moving on to the next one. • **WRR** (Weighted Round-Robin) - Specifies to transmit permitted packets into the transmit queue in a round robin order. Initially, each queue sets its weight to a configurable weighting. Every time a packet from a higher priority CoS queue is sent, the corresponding weight is subtracted by 1 and the packet in the next lower CoS queue will be serviced. When the weight of a CoS queue reaches zero, the queue will not be serviced until its weight is replenished. When weights of all CoS queues reach 0, the weights get replenished at a time. This is the default option. • **WDRR** (Weighted Deficit Round-Robin) - Specifies to serve an accumulated set of backlogged credits in the transmit queue in a round robin order. Initially, each queue sets its credit counter to a configurable quantum value. Every time a packet from a CoS queue is sent, the size of the packet is subtracted from the corresponding credit counter and the service right is turned over to the next lower CoS queue. When the credit counter drops below 0, the queue is no longer serviced until its credits are replenished. When the credit counters of all CoS queues reaches 0, the credit counters will be replenished at that time. All packets are serviced until their credit counter is zero or negative and the last packet is transmitted completely. When this condition happens, the credits are replenished. When the credits are replenished, a quantum of credits are added to each CoS queue credit counter. The quantum for each CoS queue may be different based on the user configuration. To set a CoS queue in the **SP** mode, any higher priority CoS queue must also be in the strict priority mode.

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

Queue Settings

This window is used to display and configure the queue settings.

To view the following window, click **QoS > Basic Settings > Queue Settings**, as shown below:



Queue Settings

Queue Settings

From Port	To Port	Queue ID	WRR Weight (0-127)	WDRR Quantum (0-127)	
eth1/0/1	eth1/0/1	0			Apply

Port	Queue ID	WRR Weight	WDRR Quantum
eth1/0/1	0	1	1
	1	1	1
	2	1	1
	3	1	1
	4	1	1
	5	1	1
	6	1	1
	7	0	1
eth1/0/2	0	1	1
	1	1	1
	2	1	1
	3	1	1
	4	1	1
	5	1	1
	6	1	1
	7	0	1

Figure 7-3 Queue Settings Window

The fields that can be configured are described below:

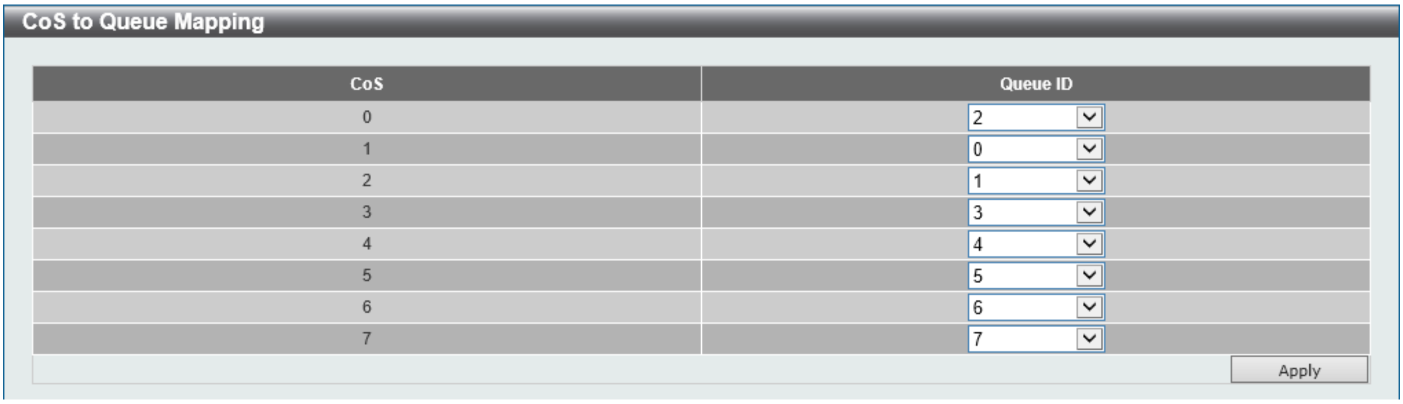
Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
Queue ID	Enter the queue ID value here. This value must be between 0 and 7.
WRR Weight	Enter the WRR weight value here. This value must be between 0 and 127. To satisfy the behavior requirements of Expedited Forwarding (EF), the highest queue is always selected by the Per-hop Behavior (PHB) EF and the schedule mode of this queue should be strict priority scheduling. Therefore, the weight of the last queue should be zero while the Differentiate Service is supported.
WDRR Quantum	Enter the WDRR quantum value here. This value must be between 0 and 127.

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

CoS to Queue Mapping

This window is used to display and configure the CoS-to-Queue mapping settings.

To view the following window, click **QoS > Basic Settings > CoS to Queue Mapping**, as shown below:



CoS to Queue Mapping

CoS	Queue ID
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

Figure 7-4 CoS to Queue Mapping Window

The fields that can be configured are described below:

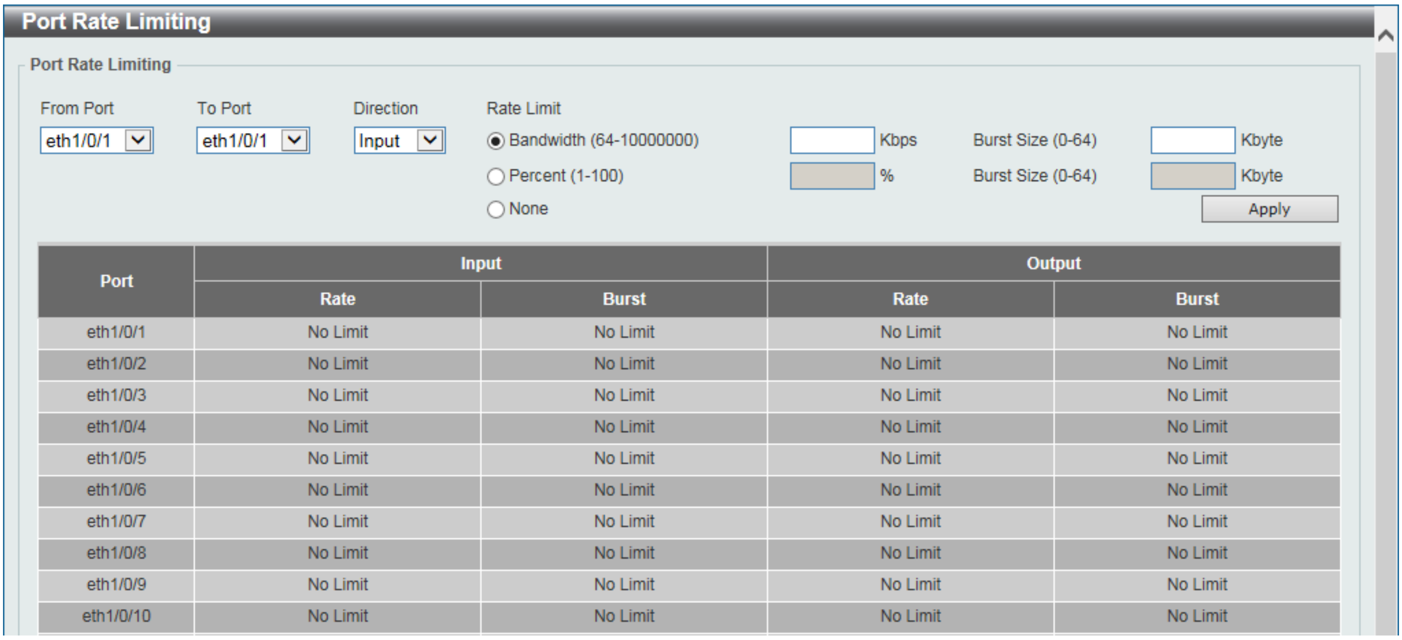
Parameter	Description
Queue ID	Select the queue ID that will be mapped to the corresponding CoS value. Options to choose from are 0 to 7.

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

Port Rate Limiting

This window is used to display and configure the port rate limiting settings.

To view the following window, click **QoS > Basic Settings > Port Rate Limiting**, as shown below:



Port Rate Limiting

Port Rate Limiting

From Port: eth1/0/1
To Port: eth1/0/1
Direction: Input
Rate Limit:
● Bandwidth (64-10000000) Kbps Burst Size (0-64) Kbyte
○ Percent (1-100) % Burst Size (0-64) Kbyte
○ None

Port	Input		Output	
	Rate	Burst	Rate	Burst
eth1/0/1	No Limit	No Limit	No Limit	No Limit
eth1/0/2	No Limit	No Limit	No Limit	No Limit
eth1/0/3	No Limit	No Limit	No Limit	No Limit
eth1/0/4	No Limit	No Limit	No Limit	No Limit
eth1/0/5	No Limit	No Limit	No Limit	No Limit
eth1/0/6	No Limit	No Limit	No Limit	No Limit
eth1/0/7	No Limit	No Limit	No Limit	No Limit
eth1/0/8	No Limit	No Limit	No Limit	No Limit
eth1/0/9	No Limit	No Limit	No Limit	No Limit
eth1/0/10	No Limit	No Limit	No Limit	No Limit

Figure 7-5 Port Rate Limiting Window

The fields that can be configured are described below:

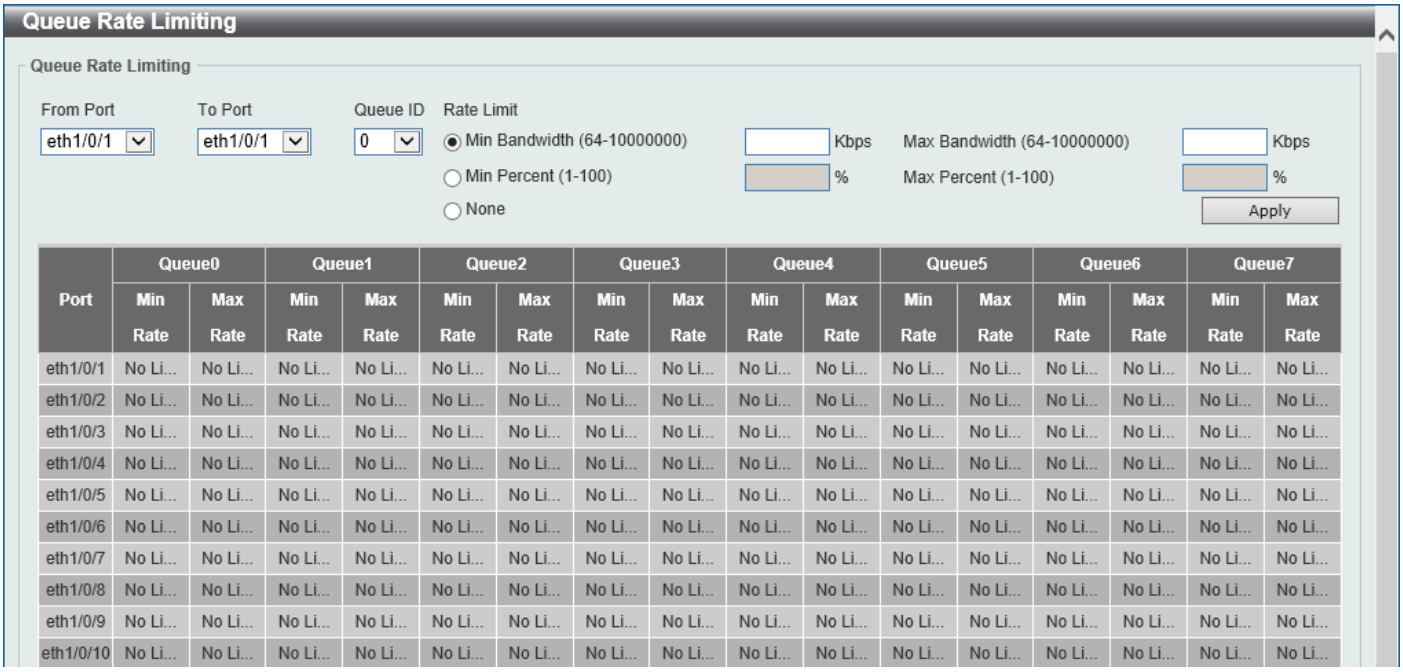
Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
Direction	Select the direction option here. Options to choose from are: • **Input** - The rate limit for ingress packets is configured. • **Output** - The rate limit for egress packets is configured.
Rate Limit	Select and enter the rate limit value here. • When **Bandwidth** is selected, enter the input/output bandwidth value used in the space provided. This value must be between 64 and 10000000 kbps. Also, enter the **Burst Size** value in the space provided. This value must be between 0 and 64 kilobytes. When the burst size is 0, the rate limit function is disabled. No rate limit is applied on the specified interface. • When **Percent** is selected, enter the input/output bandwidth percentage value used in the space provided. This value must be between 1 and 100 percent (%). Also, enter the **Burst Size** value in the space provided. This value must be between 0 and 64 kilobytes. • Select the **None** option to remove the rate limit on the specified port(s). The specified limitation cannot exceed the maximum speed of the specified interface. For the ingress bandwidth limitation, the ingress will send a pause frame or a flow control frame when the received traffic exceeds the limitation.

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

Queue Rate Limiting

This window is used to display and configure the queue rate limiting settings.

To view the following window, click **QoS > Basic Settings > Queue Rate Limiting**, as shown below:



Queue Rate Limiting

Queue Rate Limiting

From Port: eth1/0/1

To Port: eth1/0/1

Queue ID: 0

Rate Limit

● Min Bandwidth (64-10000000) Kbps — Max Bandwidth (64-10000000) Kbps

○ Min Percent (1-100) % — Max Percent (1-100) %

○ None

Port	Queue0		Queue1		Queue2		Queue3		Queue4		Queue5		Queue6		Queue7	
	Min Rate	Max Rate	Min Rate	Max Rate	Min Rate	Max Rate	Min Rate	Max Rate	Min Rate	Max Rate	Min Rate	Max Rate	Min Rate	Max Rate	Min Rate	Max Rate
eth1/0/1	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/2	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/3	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/4	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/5	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/6	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/7	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/8	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/9	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/10	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...

Figure 7-6 Queue Rate Limiting Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.

Parameter	Description
Queue ID	Select the queue ID that will be configured here. Options to choose from are 0 to 7.
Rate Limit	Select and enter the queue rate limit settings here. • When the **Min Bandwidth** option is selected, enter the minimum bandwidth rate limit value in the space provided. This value must be between 64 and 10000000 kbps. Also, enter the maximum bandwidth (**Max Bandwidth**) rate limit in the space provided. This value must be between 64 and 10000000 kbps. When the minimal bandwidth is configured, the packet transmitted from the queue can be guaranteed. When the maximum bandwidth is configured, packets transmitted from the queue cannot exceed the maximum bandwidth even if the bandwidth is available. When configuring the minimal bandwidth, the aggregate of the configured minimum bandwidth must be less than 75 percent of the interface bandwidth to make sure the configured minimal bandwidth can be guaranteed. It is not necessary to set the minimum guaranteed bandwidth for the highest strict priority queue. This is because the traffic in this queue will be serviced first if the minimal bandwidth of all queues is satisfied. The configuration of this command can only be attached to a physical port but not a port-channel. That is the minimum guaranteed bandwidth of one CoS cannot be used across physical ports. • When the **Min Percent** option is selected, enter the minimum bandwidth percentage value in the space provided. This value must be between 1 and 100 percent (%). Also, enter the maximum percentage value (**Max Percent**) in the space provided. This value must be between 1 and 100 percent (%). • Select the **None** option to remove the rate limit on the specified port(s).

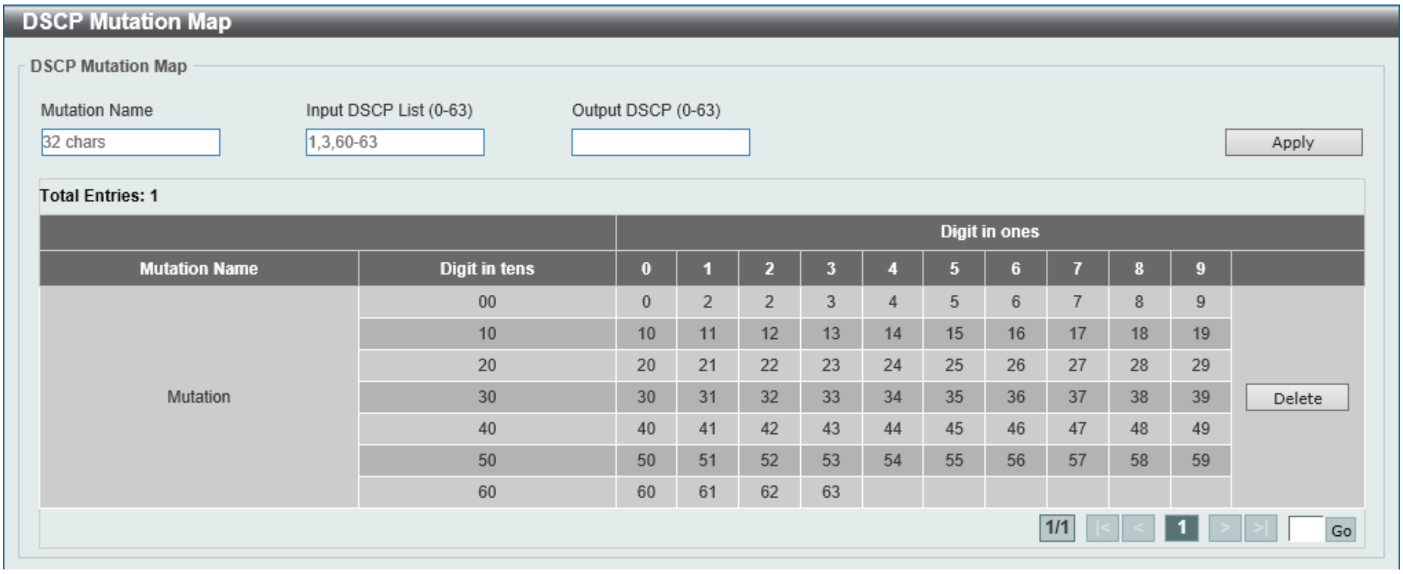
Click the **Apply** button to accept the changes made.

Advanced Settings

DSCP Mutation Map

This window is used to display and configure the Differentiated Services Code Point (DSCP) mutation map settings. When a packet is received by an interface, based on a DSCP mutation map, the incoming DSCP can be mutated to another DSCP immediately before any QoS operations. The DSCP mutation is helpful to integrate domains with different DSCP assignments. The DSCP-CoS map will still be based on the original DSCP of the packet. All the subsequent operations will base on the mutated DSCP.

To view the following window, click **QoS > Advanced Settings > DSCP Mutation Map**, as shown below:



DSCP Mutation Map

DSCP Mutation Map

Mutation Name: 32 chars

Input DSCP List (0-63): 1,3,60-63

Output DSCP (0-63):

Total Entries: 1

		Digit in ones										
Mutation Name	**Digit in tens**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	
Mutation	00	0	2	2	3	4	5	6	7	8	9	Delete
	10	10	11	12	13	14	15	16	17	18	19	
	20	20	21	22	23	24	25	26	27	28	29	
	30	30	31	32	33	34	35	36	37	38	39	
	40	40	41	42	43	44	45	46	47	48	49	
	50	50	51	52	53	54	55	56	57	58	59	
	60	60	61	62	63							

Figure 7-7 DSCP Mutation Map Window

The fields that can be configured are described below:

Parameter	Description
Mutation Name	Enter the DSCP mutation map name here. This name can be up to 32 characters long.
Input DSCP List	Enter the input DSCP list value here. This value must be between 0 and 63.
Output DSCP List	Enter the output DSCP list value here. This value must be between 0 and 63.

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

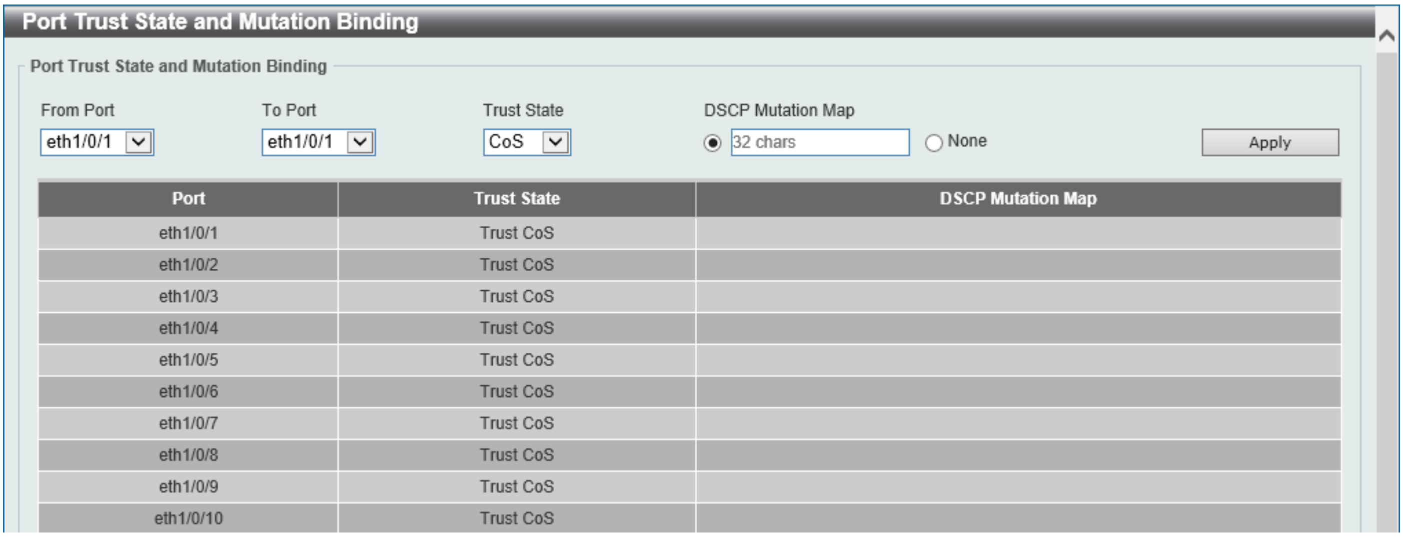
Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Port Trust State and Mutation Binding

This window is used to display and configure the port trust state and mutation binding settings.

To view the following window, click **QoS > Advanced Settings > Port Trust State and Mutation Binding**, as shown below:



Port Trust State and Mutation Binding

Port Trust State and Mutation Binding

From Port: eth1/0/1

To Port: eth1/0/1

Trust State: CoS

DSCP Mutation Map: ● 32 chars ○ None

Port	Trust State	DSCP Mutation Map
eth1/0/1	Trust CoS	
eth1/0/2	Trust CoS	
eth1/0/3	Trust CoS	
eth1/0/4	Trust CoS	
eth1/0/5	Trust CoS	
eth1/0/6	Trust CoS	
eth1/0/7	Trust CoS	
eth1/0/8	Trust CoS	
eth1/0/9	Trust CoS	
eth1/0/10	Trust CoS	

Figure 7-8 Port Trust State and Mutation Binding Window

The fields that can be configured are described below:

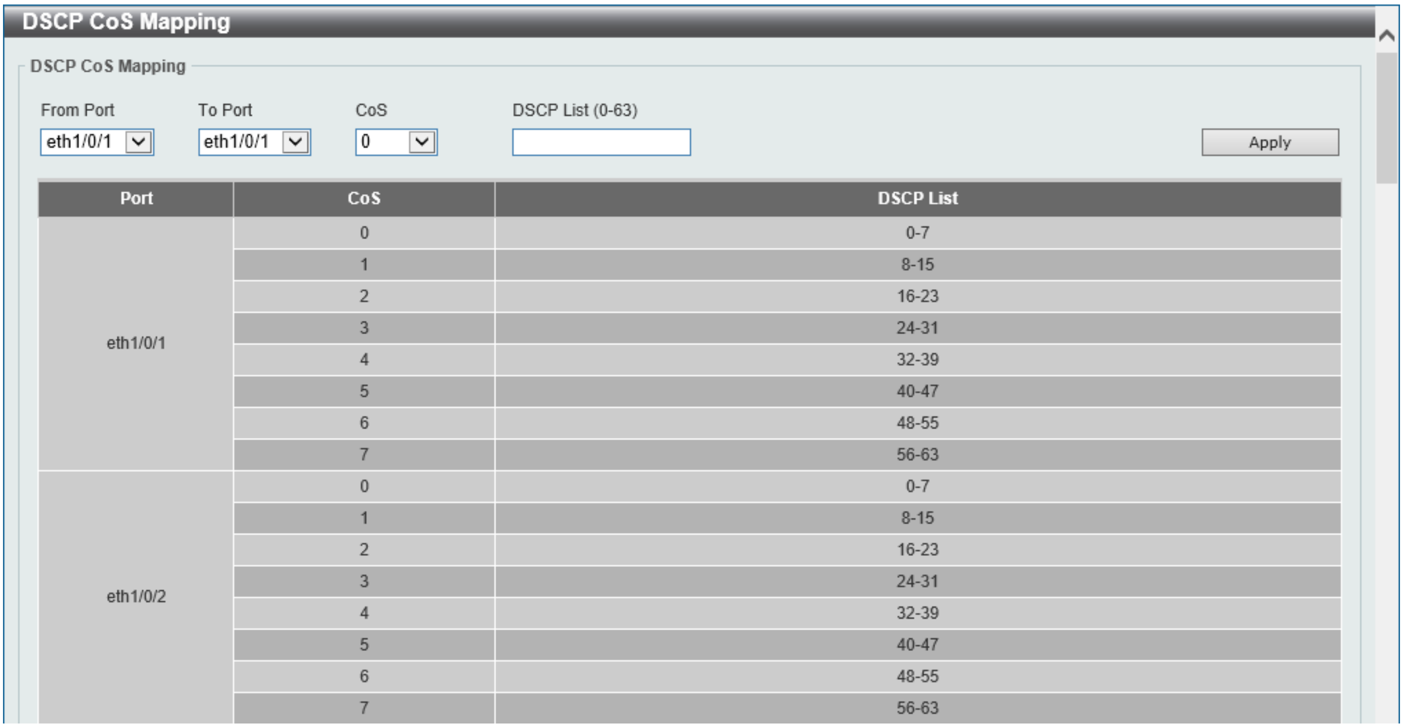
Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
Trust State	Select the port trust state option here. Options to choose from are **CoS** and **DSCP**.
DSCP Mutation Map	Select and enter the DSCP mutation map name used here. This name can be up to 32 characters long. Select the **None** option to not allocate a DSCP mutation map to the port(s).

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

DSCP CoS Mapping

This window is used to display and configure the DSCP CoS mapping settings.

To view the following window, click **QoS > Advanced Settings > DSCP CoS Mapping**, as shown below:



DSCP CoS Mapping

DSCP CoS Mapping

From Port: eth1/0/1
To Port: eth1/0/1
CoS: 0
DSCP List (0-63):

Port	CoS	DSCP List
eth1/0/1	0	0-7
	1	8-15
	2	16-23
	3	24-31
	4	32-39
	5	40-47
	6	48-55
	7	56-63
eth1/0/2	0	0-7
	1	8-15
	2	16-23
	3	24-31
	4	32-39
	5	40-47
	6	48-55
	7	56-63

Figure 7-9 DSCP CoS Mapping Window

The fields that can be configured are described below:

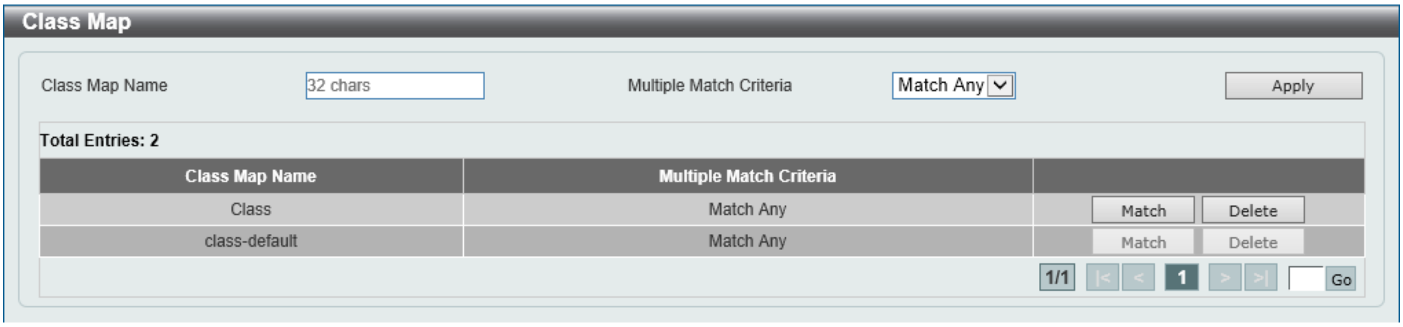
Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
CoS	Select the CoS value to map to the DSCP list. Options to choose from are 0 to 7.
DSCP List	Enter the DSCP list value to map to the CoS value here. This value must be between 0 and 63.

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

Class Map

This window is used to display and configure the class map settings.

To view the following window, click **QoS > Advanced Settings > Class Map**, as shown below:



Class Map

Class Map Name: 32 chars
Multiple Match Criteria: Match Any

Total Entries: 2

Class Map Name	Multiple Match Criteria	
Class	Match Any	Match Delete
class-default	Match Any	Match Delete

Figure 7-10 Class Map Window

The fields that can be configured are described below:

Parameter	Description
Class Map Name	Enter the class map name here. This name can be up to 32 characters long.
Multiple Match Criteria	Select the multiple match criteria option here. Options to choose from are **Match All** and **Match Any**.

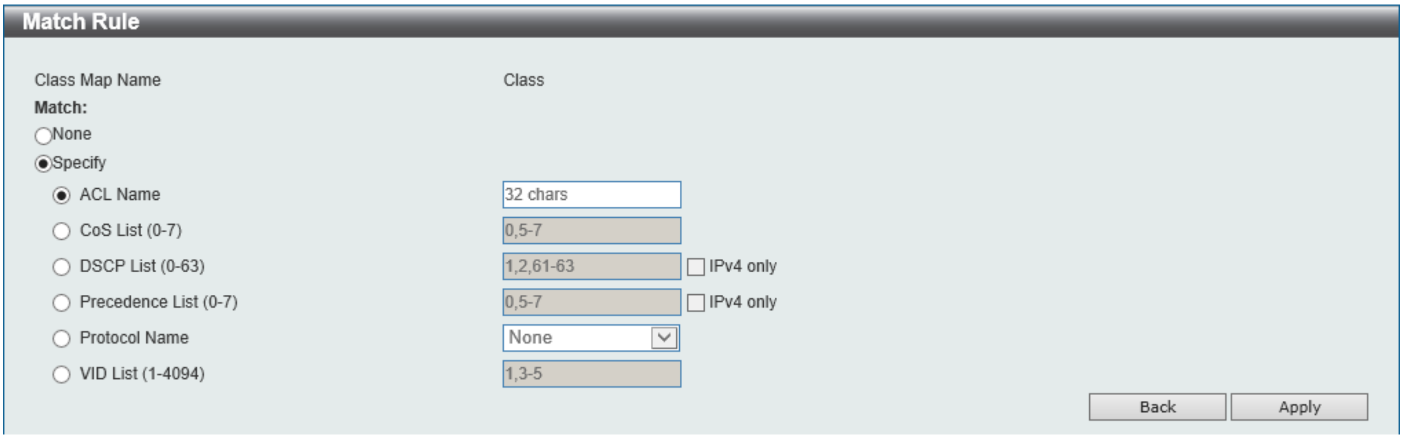
Click the **Apply** button to accept the changes made.

Click the **Match** button to configure the specific entry.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Match** button, the following page will be available.



Match Rule

Class Map Name Class

Match:

○None

●Specify

● ACL Name 32 chars

○ CoS List (0-7) 0,5-7

○ DSCP List (0-63) 1,2,61-63 □ IPv4 only

○ Precedence List (0-7) 0,5-7 □ IPv4 only

○ Protocol Name None

○ VID List (1-4094) 1,3-5

Figure 7-11 Class Map (Match) Window

The fields that can be configured are described below:

Parameter	Description
None	Select this option to match nothing to this class map.
Specify	Select the option to match something to this class map.
ACL Name	Select and enter the access list name that will be matched with this class map here. This name can be up to 32 characters long.
CoS List	Select and enter the CoS list value that will be matched with this class map here. This value must be between 0 and 7.
DSCP List	Select and enter the DSCP list value that will be matched with this class map here. This value must be between 0 and 63. Tick the **IPv4 only** option to match IPv4 packets only. If not specified, the match is for both IPv4 and IPv6 packets.
Precedence List	Select and enter the precedence list value that will be matched with this class map here. This value must be between 0 and 7. Tick the **IPv4 only** option to match IPv4 packets only. If not specified, the match is for both IPv4 and IPv6 packets. For IPv6 packets, the precedence is most three significant bits of traffic class of IPv6 header.
Protocol Name	Select the protocol name that will be matched with the class map here. Options to choose from are **ARP**, **BGP**, **DHCP**, **DNS**, **EGP**, **FTP**, **IPv4**, **IPv6**, **NetBIOS**, **NFS**, **NTP**, **OSPF**, **PPPOE**, **RIP**, **RTSP**, **SSH**, **Telnet**, and **TFTP**.
VLAN List	Select and enter the VLAN list value that will be matched with the class map here. This value must be between 1 and 4094.

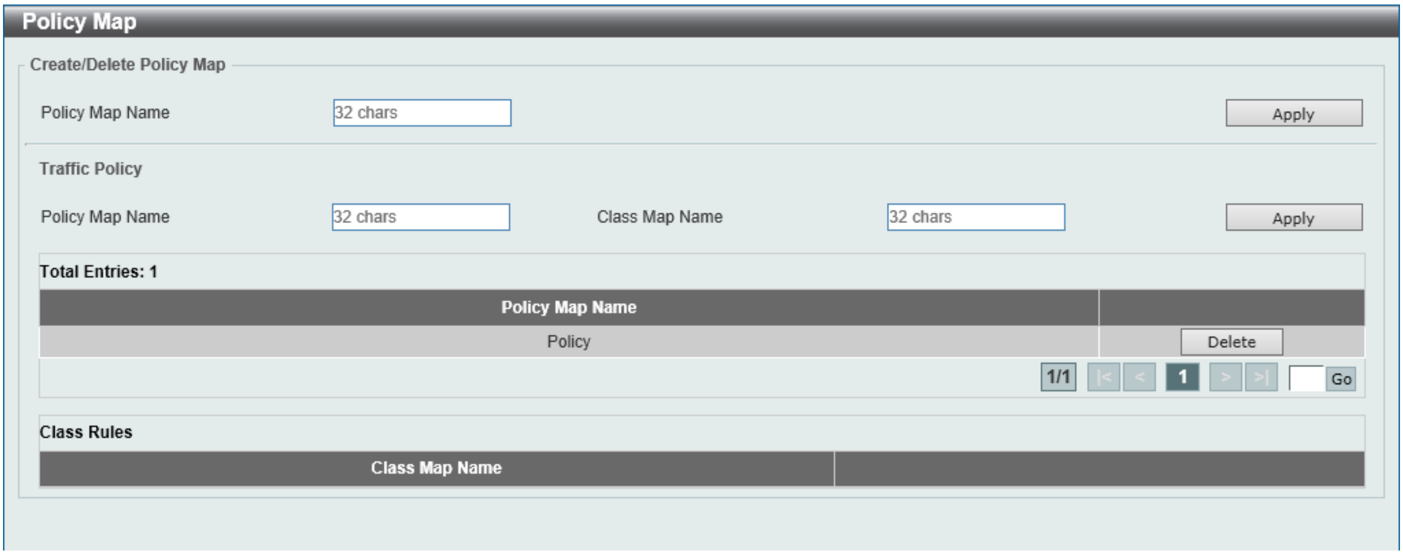
Click the **Apply** button to accept the changes made.

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

Policy Map

This window is used to display and configure the policy map settings.

To view the following window, click **QoS > Advanced Settings > Policy Map**, as shown below:



Total Entries: 1

Policy Map Name	
Policy	Delete

1/1 |< < 1 > >|

Class Map Name	

Figure 7-12 Policy Map Window

The fields that can be configured for **Create/Delete Policy Map** are described below:

Parameter	Description
Policy Map Name	Enter the name of the policy map that will be created here. This name can be up to 32 characters long.

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

The fields that can be configured for **Traffic Policy** are described below:

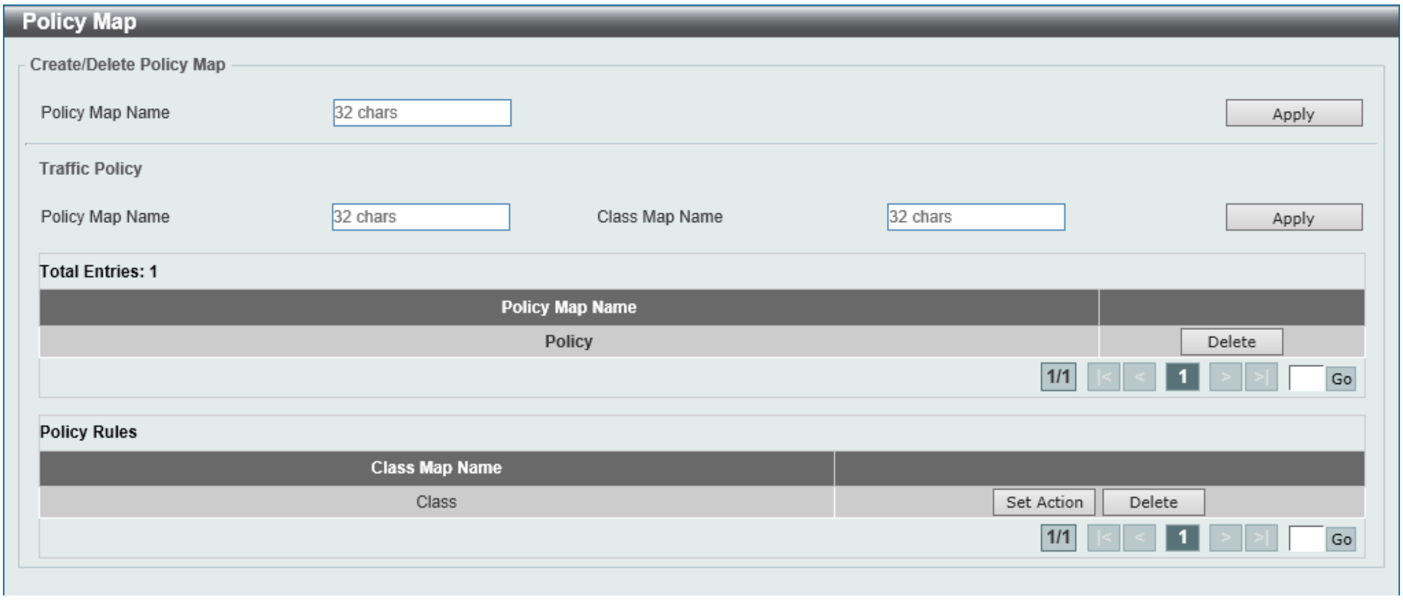
Parameter	Description
Policy Map Name	Enter the policy map name here. This name can be up to 32 characters long.
Class Map Name	Enter the class map name here. This name can be up to 32 characters long.

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

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

To view the **Class Rules** assigned to a Policy, select the **Policy Map** entry in the Policy Map table. The class rules assigned to the Policy will be displayed in the **Class Rules** table, as shown below:



Policy Map

Create/Delete Policy Map

Policy Map Name: 32 chars

Traffic Policy

Policy Map Name: 32 chars

Class Map Name: 32 chars

Total Entries: 1

Policy Map Name	
Policy	Delete

Policy Rules

Class Map Name	
Class	Set Action Delete

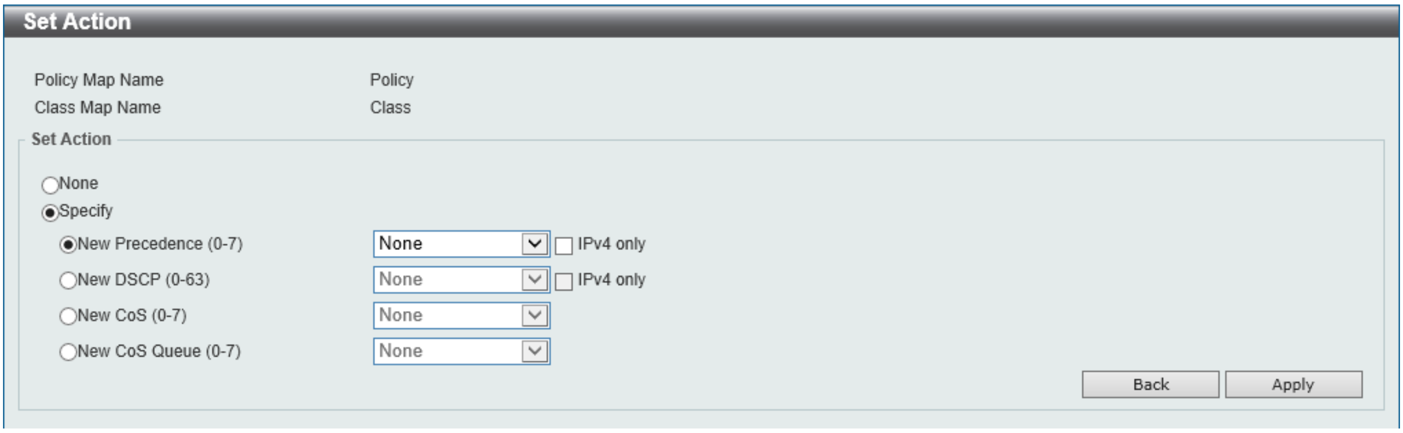
Figure 7-13 Policy Map (Class Rules) Window

Click the **Set Action** button to configure the set action settings for the specified entry.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Set Action** button, the following page will appear.



Set Action

Policy Map Name: Policy

Class Map Name: Class

Set Action

○ None

● Specify

● New Precedence (0-7): None □ IPv4 only

○ New DSCP (0-63): None □ IPv4 only

○ New CoS (0-7): None

○ New CoS Queue (0-7): None

Figure 7-14 Policy Map (Set Action) Window

The fields that can be configured are described below:

Parameter	Description
None	Select this option to specify that no action will be taken.
Specify	Select this option to specify that action will be taken based on the configurations made.
New Precedence	Select the new precedence value for the packet here. The range is from 0 to 7. Select the **IPv4 only** option to specify that IPv4 precedence will be marked only. If not selected, then both IPv4 and IPv6 precedence will be marked. For IPv6 packets, the precedence is the most three significant bits of the traffic class of the IPv6 header. Setting the precedence will not affect the CoS queue selection.
New DSCP	Select the new DSCP value for the packet here. The range is from 0 to 63. Select the **IPv4 only** option to specify that the IPv4 DSCP will be marked only. If not

Parameter	Description
	selected, then both the IPv4 and IPv6 DSCP will be marked. Setting the DSCP will not affect the CoS queue selection.
New CoS	Select the new CoS value to packets here. The range is from 0 to 7. Setting the CoS will not affect the CoS queue selection. The CoS will only be marked.
New Cos Queue	Select the new CoS queue value to packets here. This will overwrite the original CoS queue selection. Setting the CoS queue will take effect if the policy map is applied on the interface.

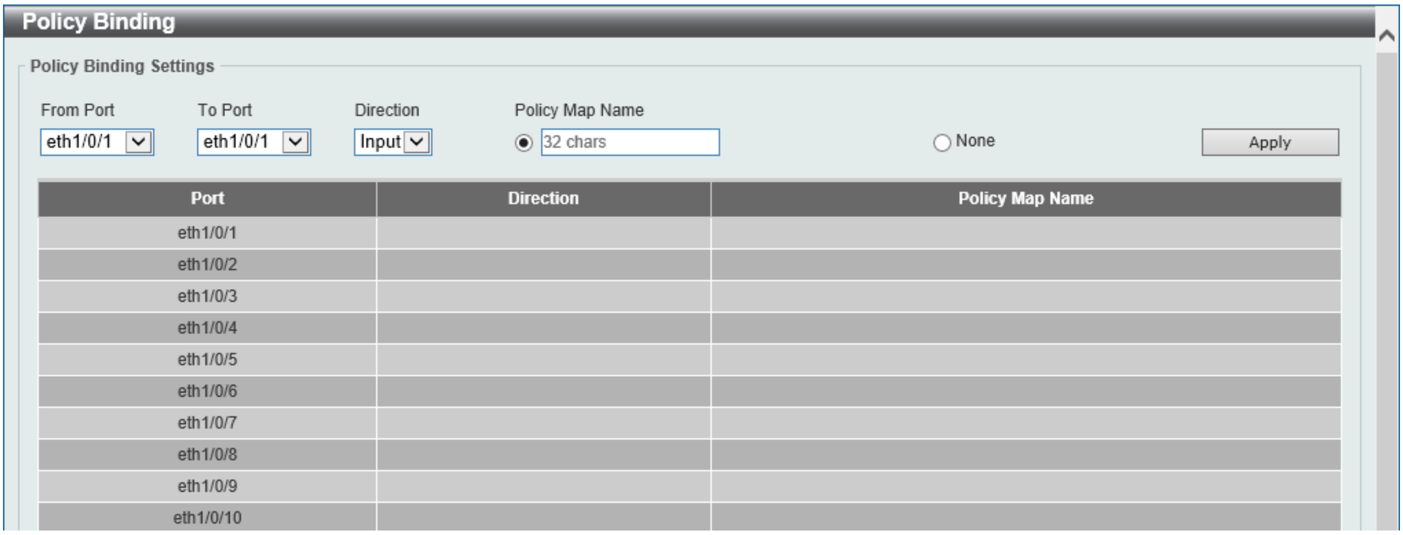
Click the **Back** button to return to the previous window.

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

Policy Binding

This window is used to display and configure the policy binding settings.

To view the following window, click **QoS > Advanced Settings > Policy Binding**, as shown below:



From Port: eth1/0/1 To Port: eth1/0/1 Direction: Input Policy Map Name: ● 32 chars ○ None

Port	Direction	Policy Map Name
eth1/0/1		
eth1/0/2		
eth1/0/3		
eth1/0/4		
eth1/0/5		
eth1/0/6		
eth1/0/7		
eth1/0/8		
eth1/0/9		
eth1/0/10		

Figure 7-15 Policy Binding Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
Direction	Select the direction option here. **Input** specifies ingress traffic.
Policy Map Name	Enter the policy map name here. This name can be up to 32 characters long. Select the **None** option to not tie a policy map to this entry.

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

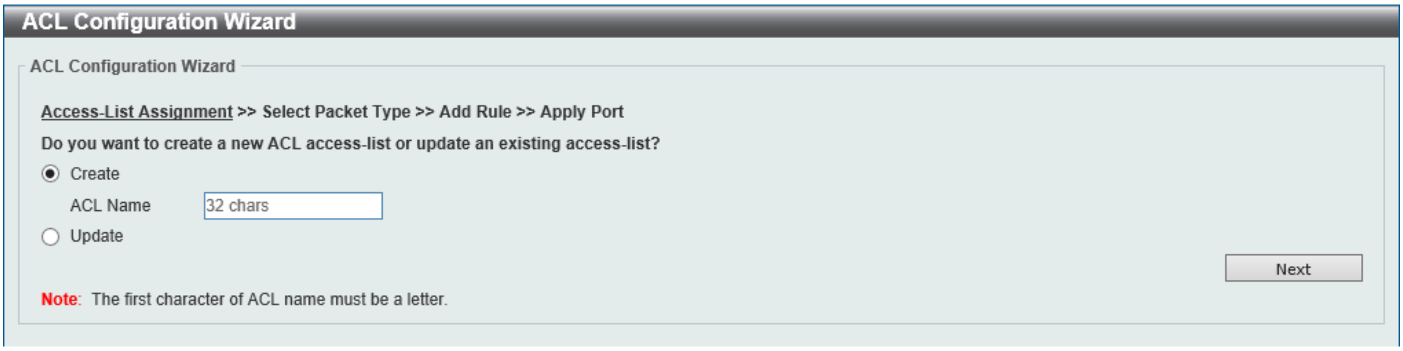
8. Access Control List (ACL)

ACL Configuration Wizard

This window is used to guide the user to create a new ACL access list or configure an existing ACL access list.

Step 1 - Create/Update

To view the following window, click **ACL > ACL Configuration Wizard**, as shown below:



ACL Configuration Wizard

ACL Configuration Wizard

Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port

Do you want to create a new ACL access-list or update an existing access-list?

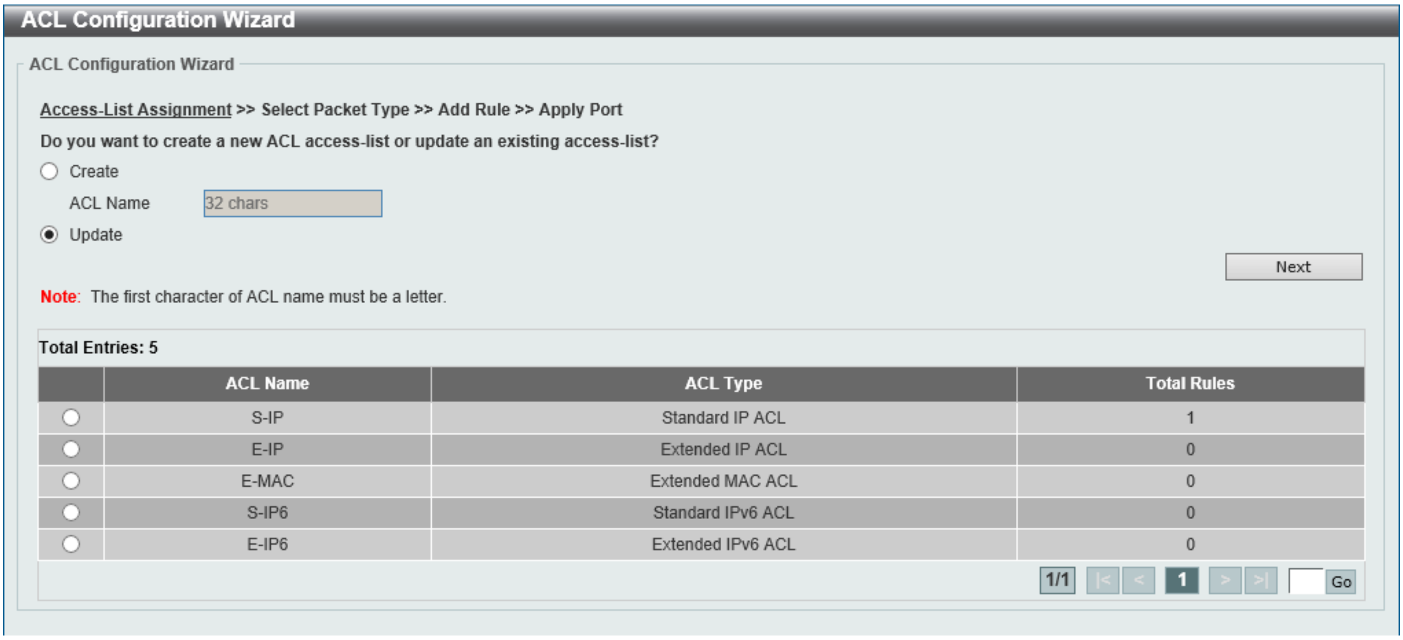
● Create

ACL Name: 32 chars

○ Update

Note: The first character of ACL name must be a letter.

Figure 8-1 ACL Configuration Wizard (Create) Window



ACL Configuration Wizard

ACL Configuration Wizard

Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port

Do you want to create a new ACL access-list or update an existing access-list?

○ Create

ACL Name: 32 chars

● Update

Note: The first character of ACL name must be a letter.

Total Entries: 5

	ACL Name	ACL Type	Total Rules
○	S-IP	Standard IP ACL	1
○	E-IP	Extended IP ACL	0
○	E-MAC	Extended MAC ACL	0
○	S-IP6	Standard IPv6 ACL	0
○	E-IP6	Extended IPv6 ACL	0

Figure 8-2 ACL Configuration Wizard (Update) Window

The fields that can be configured are described below:

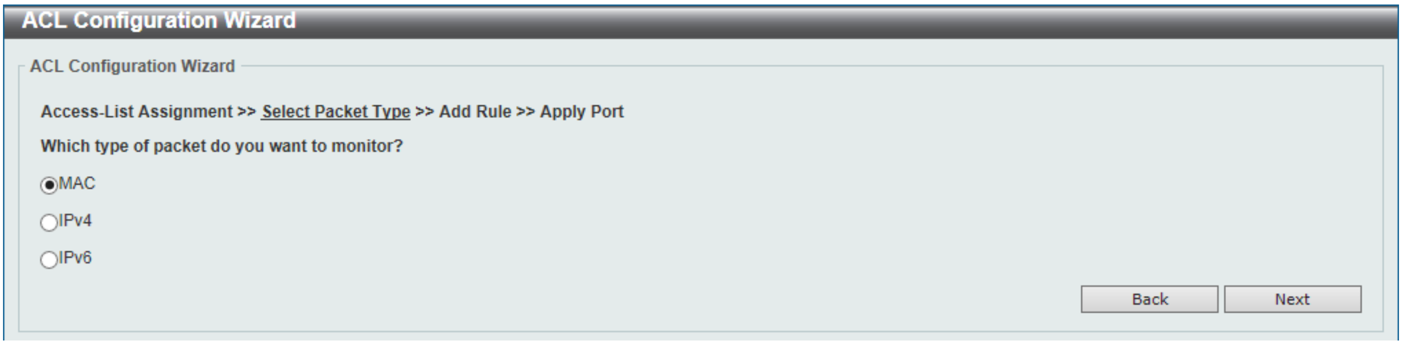
Parameter	Description
Create	Select this option to create a new ACL access list using the configuration wizard.
ACL Name	Enter the new ACL name here. This name can be up to 32 characters long.
Update	Select this option to update an existing ACL access list. Select the existing ACL in the table to process with the update.

Click the **Next** button to continue to the next step.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Step 2 - Select Packet Type

After clicking the **Next** button, the following window will appear.



ACL Configuration Wizard

ACL Configuration Wizard

Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port

Which type of packet do you want to monitor?

● MAC

○ IPv4

○ IPv6

Figure 8-3 ACL Configuration Wizard (Create, Packet Type) Window

The fields that can be configured are described below:

Parameter	Description
MAC	Select to create/update a MAC ACL.
IPv4	Select to create/update an IPv4 ACL.
IPv6	Select to create/update an IPv6 ACL.

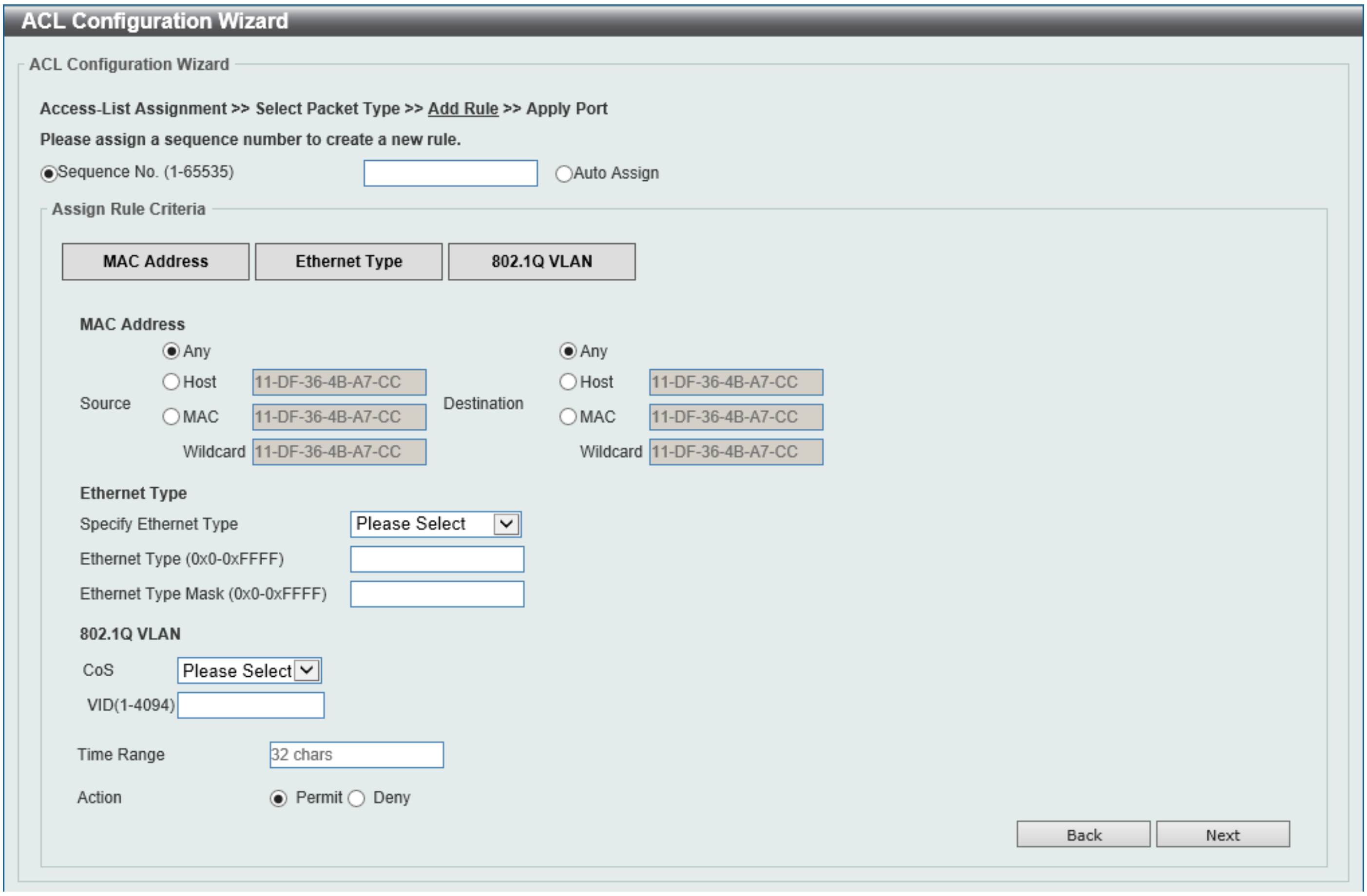
Click the **Back** button to return to the previous step.

Click the **Next** button to continue to the next step.

Step 3 - Add Rule

MAC

After clicking the **MAC** radio button and the **Next** button, the following window will appear.



ACL Configuration Wizard

ACL Configuration Wizard

Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port

Please assign a sequence number to create a new rule.

● Sequence No. (1-65535) ○ Auto Assign

Assign Rule Criteria

MAC Address | Ethernet Type | 802.1Q VLAN

MAC Address

Source: ● Any ○ Host 11-DF-36-4B-A7-CC ○ MAC 11-DF-36-4B-A7-CC Wildcard 11-DF-36-4B-A7-CC

Destination: ● Any ○ Host 11-DF-36-4B-A7-CC ○ MAC 11-DF-36-4B-A7-CC Wildcard 11-DF-36-4B-A7-CC

Ethernet Type

Specify Ethernet Type: Please Select

Ethernet Type (0x0-0xFFFF)

Ethernet Type Mask (0x0-0xFFFF)

802.1Q VLAN

CoS: Please Select

VID(1-4094)

Time Range: 32 chars

Action: ● Permit ○ Deny

Back | Next

Figure 8-4 ACL Configuration Wizard (Create, Packet Type, MAC) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. This value must be between 1 and 65535. Select **Auto Assign** to automatically generate an ACL rule number for this entry.
Source	Select and enter the source MAC address information here. Options to choose from are: • **Any** - When this option is selected, any source traffic will be evaluated according to the conditions of this rule. • **Host** - When this option is selected, enter the source host MAC address here. • **MAC** - When this option is selected, the **Wildcard** option will also be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination	Select and enter the destination MAC address information here. Options to choose from are: • **Any** - When this option is selected, any destination traffic will be evaluated according to the conditions of this rule. • **Host** - When this option is selected, enter the destination host MAC address here. • **MAC** - When this option is selected, the **Wildcard** option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.

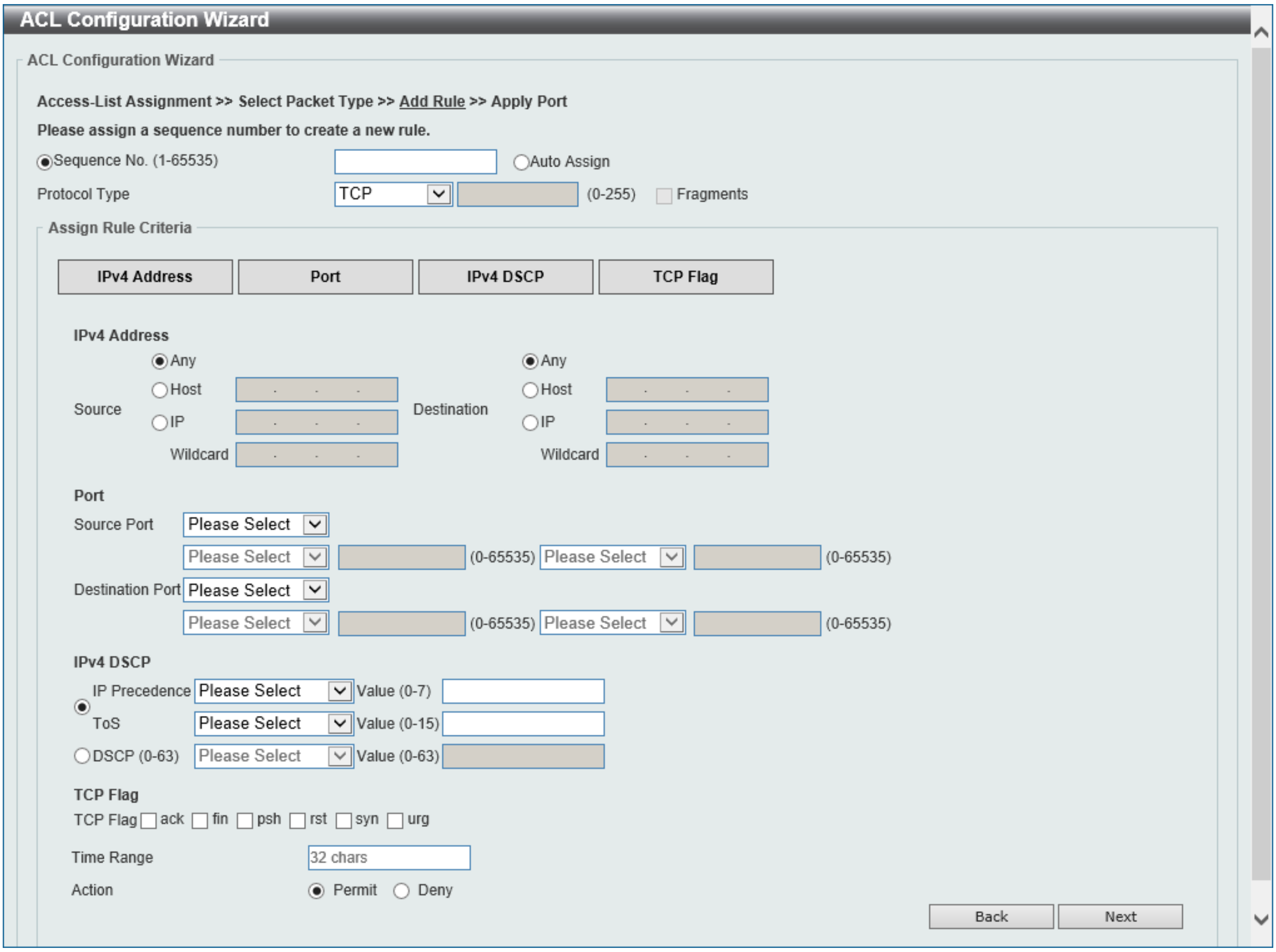
Parameter	Description
Specify Ethernet Type	Select the Ethernet type option here. Options to choose from are **aarp**, **appletalk**, **decent-iv**, **etype-6000**, **etype-8042**, **lat**, **lavc-sca**, **mop-console**, **mop-dump**, **vines-echo**, **vines-ip**, **xns-idp**, and **arp**.
Ethernet Type	Enter the Ethernet type hexadecimal value here. This value must be between 0x0 and 0xFFFF. When any Ethernet type profile is selected in the **Specify Ethernet Type** drop-down list, the appropriate hexadecimal value will automatically be entered.
Ethernet Type Mask	Enter the Ethernet type mask hexadecimal value here. This value must be between 0x0 and 0xFFFF. When any Ethernet type profile is selected in the **Specify Ethernet Type** drop-down list, the appropriate hexadecimal value will automatically be entered.
CoS	Select the CoS value that will be used here. The range is from **0** to **7**.
VID	Enter the VLAN ID that will be associated with this ACL rule here. The range is from 1 to 4094.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.

Click the **Back** button to return to the previous step.

Click the **Next** button to continue to the next step.

IPv4

After clicking the **IPv4** radio button and the **Next** button, the following window will appear.



ACL Configuration Wizard

ACL Configuration Wizard

Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port

Please assign a sequence number to create a new rule.

● Sequence No. (1-65535) ○ Auto Assign

Protocol Type: TCP (0-255) □ Fragments

Assign Rule Criteria

IPv4 Address | Port | IPv4 DSCP | TCP Flag

IPv4 Address

Source: ● Any ○ Host ○ IP Wildcard

Destination: ● Any ○ Host ○ IP Wildcard

Port

Source Port: Please Select; Please Select (0-65535) Please Select (0-65535)

Destination Port: Please Select; Please Select (0-65535) Please Select (0-65535)

IPv4 DSCP

● IP Precedence: Please Select Value (0-7)
ToS: Please Select Value (0-15)
○ DSCP (0-63): Please Select Value (0-63)

TCP Flag

TCP Flag □ ack □ fin □ psh □ rst □ syn □ urg

Time Range: 32 chars

Action: ● Permit ○ Deny

Back | Next

Figure 8-5 ACL Configuration Wizard (Create, Packet Type, IPv4) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. This value must be between 1 and 65535. Select **Auto Assign** to automatically generate an ACL rule number for this entry.
Protocol Type	Select the protocol type option here. Options to choose from are **TCP**, **UDP**, **ICMP**, **EIGRP** (88), **ESP** (50), **GRE** (47), **IGMP** (2), **OSPF** (89), **PIM** (103), **VRRP** (112), **IP-in-IP** (94), **PCP** (108), **Protocol ID**, and **None**. • **Value** - The protocol ID can also manually be entered here. The range is from 0 to 255. • **Fragments** - Select this option to include packet fragment filtering.

The fields that can be configured in **Assign rule criteria** are described below:

Parameter	Description
Source	Select and enter the source information here. Options to choose from are **Any**, **Host**, and **IP**. • When the **Any** option is selected, any source traffic will be evaluated according to the conditions of this rule. • When the **Host** option is selected, enter the source host IP address here.

Parameter	Description
	• When the **IP** option is selected, the **Wildcard** option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are **Any**, **Host**, and **IP**. • When the **Any** option is selected, any destination traffic will be evaluated according to the conditions of this rule. • When the **Host** option is selected, enter the destination host IP address here. • When the **IP** option is selected, the **Wildcard** option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source Port	Select and enter the source port value here. Options to choose from are **=**, **>**, **<**, **≠**, and **Range**. • When selecting the **=** option, the specific selected port number will be used. • When selecting the **>** option, all ports greater than the selected port, will be used. • When selecting the **<** option, all ports smaller than the selected port, will be used. • When selecting the **≠** option, all ports, excluding the selected port, will be used. • When selecting the **Range** option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. This parameter is only available in the protocol type **TCP** and **UDP**.
Destination Port	Select and enter the destination port value here. Options to choose from are **=**, **>**, **<**, **≠**, and **Range**. • When selecting the **=** option, the specific selected port number will be used. • When selecting the **>** option, all ports greater than the selected port, will be used. • When selecting the **<** option, all ports smaller than the selected port, will be used. • When selecting the **≠** option, all ports, excluding the selected port, will be used. • When selecting the **Range** option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. This parameter is only available in the protocol type **TCP** and **UDP**.
Specify ICMP Message Type	Select the ICMP message type used here. This parameter is only available in the protocol type **ICMP**.
ICMP Message Type	When the **ICMP Message Type** is not selected, enter the ICMP Message Type numerical value used here. The range is from 0 to 255. When the **ICMP Message Type** is selected, this numerical value will automatically be entered. This parameter is only available in the protocol type **ICMP**.
Message Code	When the **ICMP Message Type** is not selected, enter the Message Code numerical value used here. The range is from 0 to 255. When the **ICMP Message Type** is selected, this numerical value will automatically be entered. This parameter is only available in the protocol type **ICMP**.
IP Precedence	Select the IP precedence value used here. Options to choose from are **routine** (0), **priority** (1), **immediate** (2), **flash** (3), **flash-override** (4), **critical** (5), **internet** (6), and **network** (7).

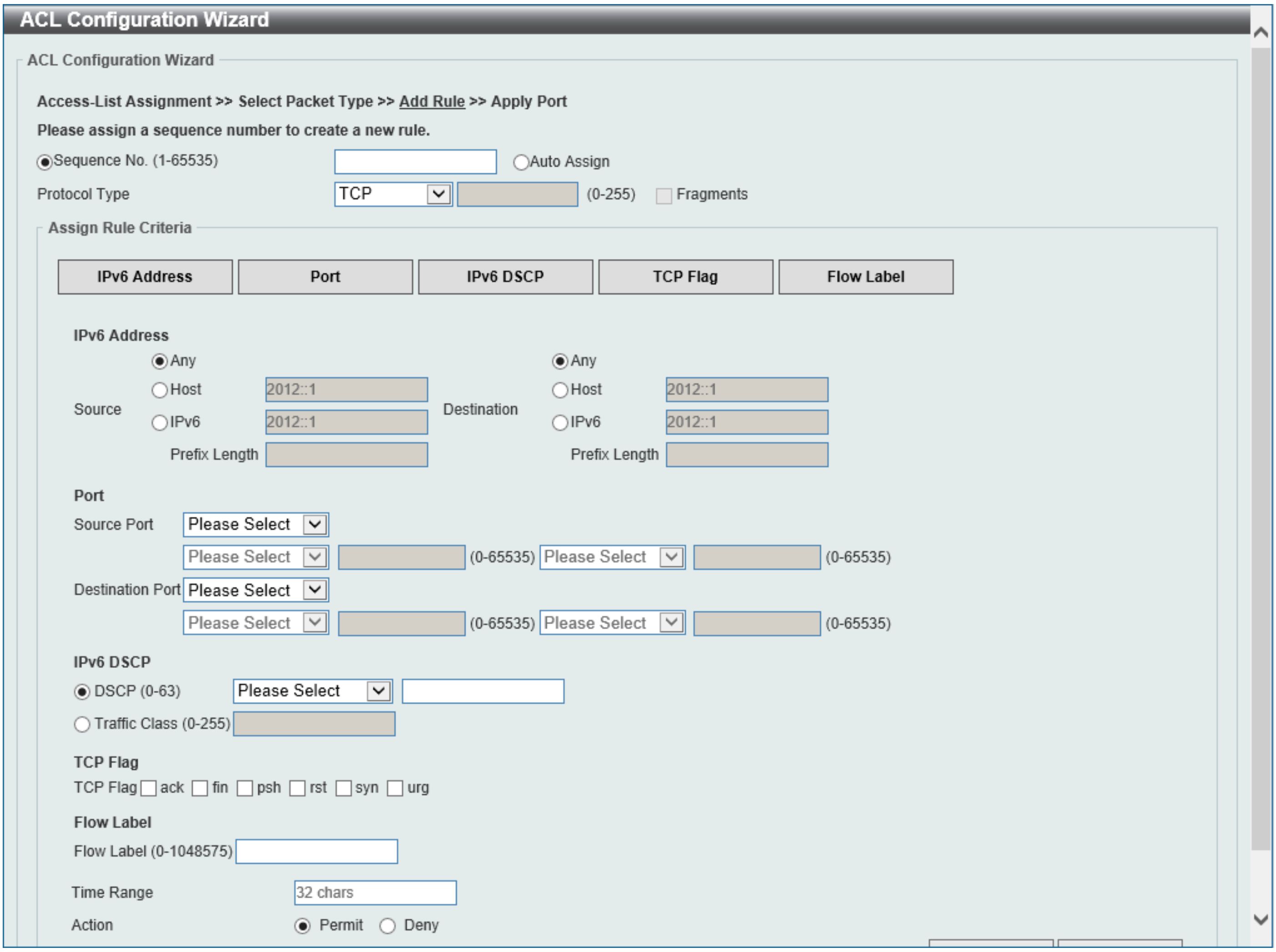
Parameter	Description
	• **Value -** The IP precedence value can also manually be entered here. The range is from 0 to 7.
ToS	Select the Type-of-Service (**ToS**) value that will be used here. Options to choose from are **normal** (0), **min-monetary-cost** (1), **max-reliability** (2), **max-throughput** (4), and **min-delay** (8). • **Value -** The ToS value can also manually be entered here. The range is from 0 to 15.
DSCP	Select the DSCP value that will be used here. Options to choose from are **default** (0), **af11** (10), **af12** (12), **af13** (14), **af21** (18), **af22** (20), **af23** (22), **af31** (26), **af32** (28), **af33** (30), **af41** (34), **af42** (36), **af43** (38), **cs1** (8), **cs2** (16), **cs3** (24), **cs4** (32), **cs5** (40), **cs6** (48), **cs7** (56), and **ef** (46). • **Value -** The DSCP value can also manually be entered here. The range is from 0 to 63.
TCP Flag	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are **ack**, **fin**, **psh**, **rst**, **syn**, and **urg**. This parameter is only available in the protocol type **TCP**.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.

Click the **Back** button to return to the previous step.

Click the **Next** button to continue to the next step.

IPv6

After clicking the **IPv6** radio button and the **Next** button, the following window will appear.



ACL Configuration Wizard

ACL Configuration Wizard

Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port

Please assign a sequence number to create a new rule.

● Sequence No. (1-65535) ○ Auto Assign

Protocol Type: TCP (0-255) □ Fragments

Assign Rule Criteria

IPv6 Address

Source: ● Any ○ Host 2012::1 ○ IPv6 2012::1 Prefix Length

Destination: ● Any ○ Host 2012::1 ○ IPv6 2012::1 Prefix Length

Port

Source Port: Please Select; Please Select (0-65535) Please Select (0-65535)

Destination Port: Please Select; Please Select (0-65535) Please Select (0-65535)

IPv6 DSCP

● DSCP (0-63) Please Select

○ Traffic Class (0-255)

TCP Flag

TCP Flag □ ack □ fin □ psh □ rst □ syn □ urg

Flow Label

Flow Label (0-1048575)

Time Range: 32 chars

Action: ● Permit ○ Deny

Figure 8-6 ACL Configuration Wizard (Create, Packet Type, IPv6) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. This value must be between 1 and 65535. Select **Auto Assign** to automatically generate an ACL rule number for this entry.
Protocol Type	Select the protocol type option here. Options to choose from are **TCP**, **UDP**, **ICMP**, **Protocol ID**, **ESP** (50), **PCP** (108), **SCTP** (132), and **None**. • **Value** - The protocol ID can also manually be entered here. The range is from 0 to 255. • **Fragments** - Select this option to include packet fragment filtering.

The fields that can be configured in **Assign rule criteria** are described below:

Parameter	Description
Source	Select and enter the source information here. Options to choose from are **Any**, **Host**, and **IPv6**. • When the **Any** option is selected, any source traffic will be evaluated according to the conditions of this rule. • When the **Host** option is selected, enter the source host IPv6 address here.

Parameter	Description
	• When the **IPv6** option is selected, the **Prefix Length** option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are **Any**, **Host**, and **IPv6**. • When the **Any** option is selected, any destination traffic will be evaluated according to the conditions of this rule. • When the **Host** option is selected, enter the destination host IPv6 address here. • When the **IPv6** option is selected, the **Prefix Length** option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Source Port	Select and enter the source port value here. Options to choose from are **=**, **>**, **<**, **≠**, and **Range**. • When selecting the **=** option, the specific selected port number will be used. • When selecting the **>** option, all ports greater than the selected port, will be used. • When selecting the **<** option, all ports smaller than the selected port, will be used. • When selecting the **≠** option, all ports, excluding the selected port, will be used. • When selecting the **Range** option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. This parameter is only available in the protocol type **TCP** and **UDP**.
Destination Port	Select and enter the destination port value here. Options to choose from are **=**, **>**, **<**, **≠**, and **Range**. • When selecting the **=** option, the specific selected port number will be used. • When selecting the **>** option, all ports greater than the selected port, will be used. • When selecting the **<** option, all ports smaller than the selected port, will be used. • When selecting the **≠** option, all ports, excluding the selected port, will be used. • When selecting the **Range** option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. This parameter is only available in the protocol type **TCP** and **UDP**.
Specify ICMP Message Type	Select the ICMP message type used here. This parameter is only available in the protocol type **ICMP**.
ICMP Message Type	When the **ICMP Message Type** is not selected, enter the ICMP Message Type numerical value used here. The range is from 0 to 255. When the **ICMP Message Type** is selected, this numerical value will automatically be entered. This parameter is only available in the protocol type **ICMP**.
Message Code	When the **ICMP Message Type** is not selected, enter the Message Code numerical value used here. The range is from 0 to 255. When the **ICMP Message Type** is selected, this numerical value will automatically be entered. This parameter is only available in the protocol type **ICMP**.
DSCP	Select the DSCP value that will be used here. Options to choose from are **default** (0), **af11** (10), **af12** (12), **af13** (14), **af21** (18), **af22** (20), **af23** (22), **af31** (26), **af32** (28), **af33** (30), **af41** (34), **af42** (36), **af43** (38), **cs1** (8), **cs2** (16), **cs3** (24), **cs4** (32), **cs5** (40), **cs6** (48), **cs7** (56), and **ef** (46). • **Value -** The DSCP value can also manually be entered here. The range is from 0 to 63.

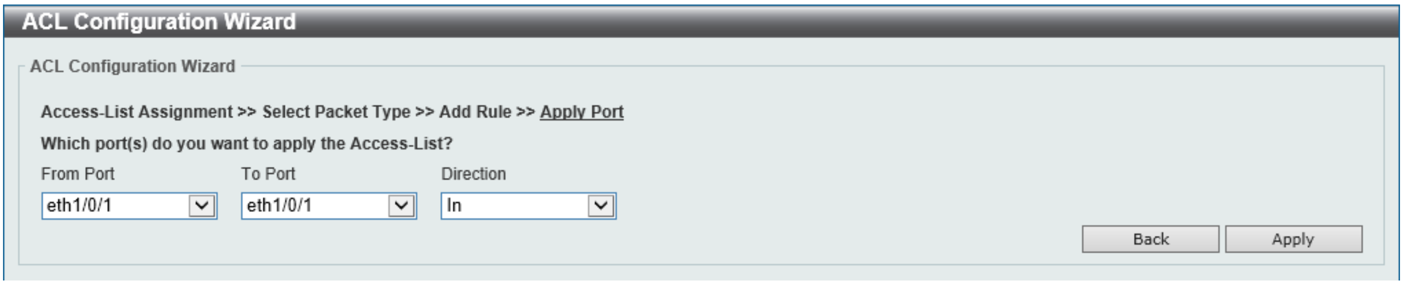
Parameter	Description
Traffic Class	Select and enter the traffic class value here. The range is from 0 to 255.
TCP Flag	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are **ack**, **fin**, **psh**, **rst**, **syn**, and **urg**. This parameter is only available in the protocol type **TCP**.
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.

Click the **Back** button to return to the previous step.

Click the **Next** button to continue to the next step.

Step 4 - Apply Port

After clicking the **Next** button, the following window will appear.


ACL Configuration Wizard

ACL Configuration Wizard

Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port

Which port(s) do you want to apply the Access-List?

From Port: eth1/0/1
To Port: eth1/0/1
Direction: In

Figure 8-7 ACL Configuration Wizard (Create, Port) Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Direction	Specifies that the **In** direction is used.

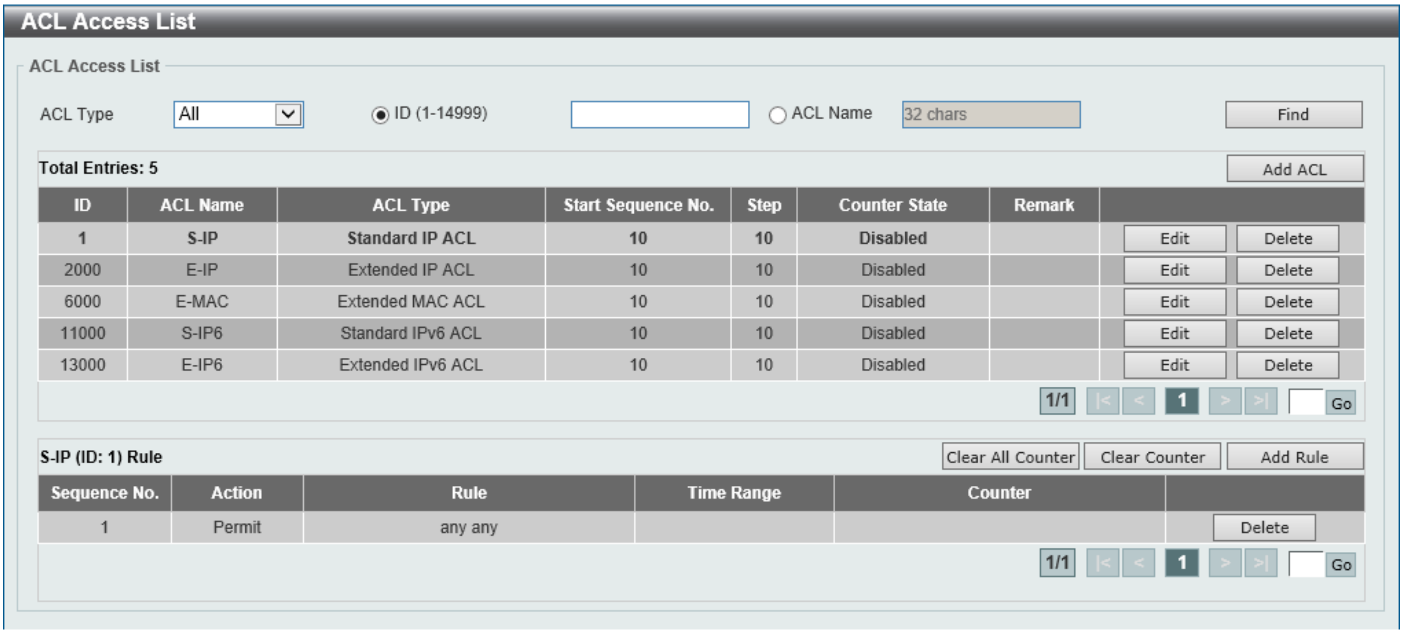
Click the **Back** button to return to the previous step.

Click the **Apply** button to accept the changes made and return to the main ACL Wizard window.

ACL Access List

This window is used to display and configure the ACLs, ACL rules, and settings.

To view the following window, click **ACL > ACL Access List**, as shown below:



ACL Access List

ACL Access List

ACL Type: All ● ID (1-14999) ○ ACL Name: 32 chars

Total Entries: 5

ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	
1	S-IP	Standard IP ACL	10	10	Disabled		Edit Delete
2000	E-IP	Extended IP ACL	10	10	Disabled		Edit Delete
6000	E-MAC	Extended MAC ACL	10	10	Disabled		Edit Delete
11000	S-IP6	Standard IPv6 ACL	10	10	Disabled		Edit Delete
13000	E-IP6	Extended IPv6 ACL	10	10	Disabled		Edit Delete

S-IP (ID: 1) Rule

Sequence No.	Action	Rule	Time Range	Counter	
1	Permit	any any			Delete

Figure 8-8 ACL Access List Window

The fields that can be configured are described below:

Parameter	Description
ACL Type	Select the ACL type to find here. Options to choose from are **All**, **IP ACL**, **IPv6 ACL**, and **MAC ACL**.
ID	Select and enter the access list ID here. The range is from 1 to 14999.
ACL Name	Select and enter the access list name here. This name can be up to 32 characters long.

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

Click the **Add ACL** button to create a new ACL.

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

Click the **Delete** button, next to the ACL, to remove the specific ACL.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **Clear All Counter** button to clear all the counter information displayed.

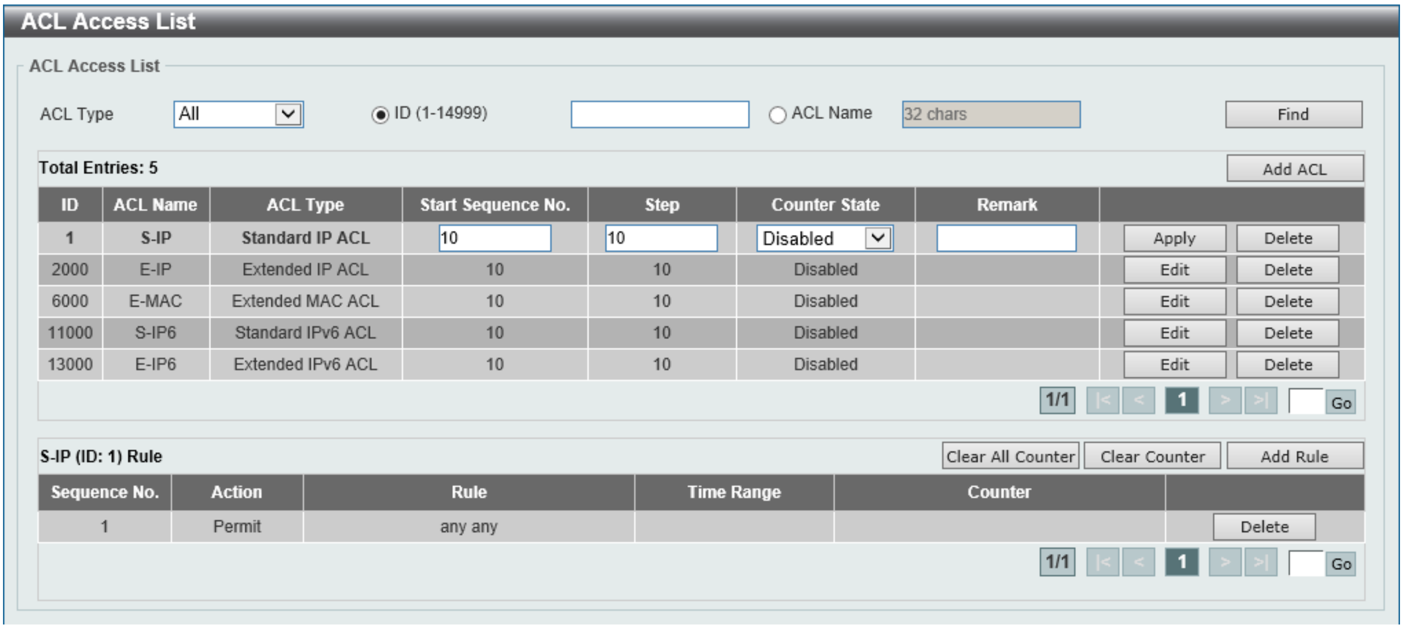
Click the **Clear Counter** button to clear the counter information for the rule displayed.

Click the **Add Rule** button to create an ACL rule for the ACL selected.

Click the **Delete** button, next to the ACL rule, to remove the specific ACL rule.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Edit** button, the following page will appear.



ACL Access List

ACL Access List

ACL Type: All ● ID (1-14999) ○ ACL Name: 32 chars

Total Entries: 5

ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	
1	S-IP	Standard IP ACL	10	10	Disabled		Apply Delete
2000	E-IP	Extended IP ACL	10	10	Disabled		Edit Delete
6000	E-MAC	Extended MAC ACL	10	10	Disabled		Edit Delete
11000	S-IP6	Standard IPv6 ACL	10	10	Disabled		Edit Delete
13000	E-IP6	Extended IPv6 ACL	10	10	Disabled		Edit Delete

S-IP (ID: 1) Rule

Sequence No.	Action	Rule	Time Range	Counter	
1	Permit	any any			Delete

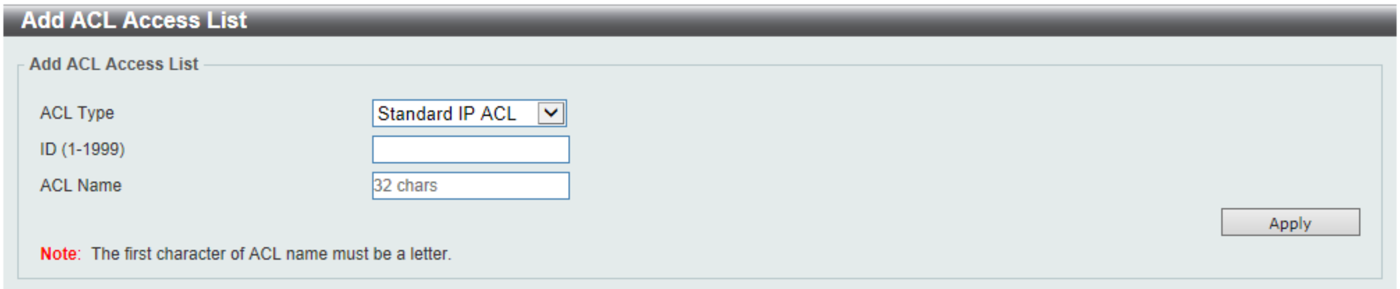
Figure 8-9 ACL Access List (Edit) Window

After clicking the **Edit** button, the fields that can be configured are described below:

Parameter	Description
Start Sequence No.	Enter the start sequence number here.
Step	Enter the sequence number step here. The step range is from 1 to 32. This specifies the number that the sequence numbers step. The default value is 10. For example, if the increment (step) value is 5 and the beginning sequence number is 20, the subsequent sequence numbers are 25, 30, 35, 40, and so on.
Counter State	Select to enable or disable the counter state option here.
Remark	Enter an optional remark that will be associated with this ACL here.

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

After clicking the **Add ACL** button, the following page will appear.



Add ACL Access List

Add ACL Access List

ACL Type: Standard IP ACL

ID (1-1999):

ACL Name: 32 chars

Note: The first character of ACL name must be a letter.

Figure 8-10 ACL Access List (Add ACL) Window

After clicking the **Add ACL** button, the fields that can be configured are described below:

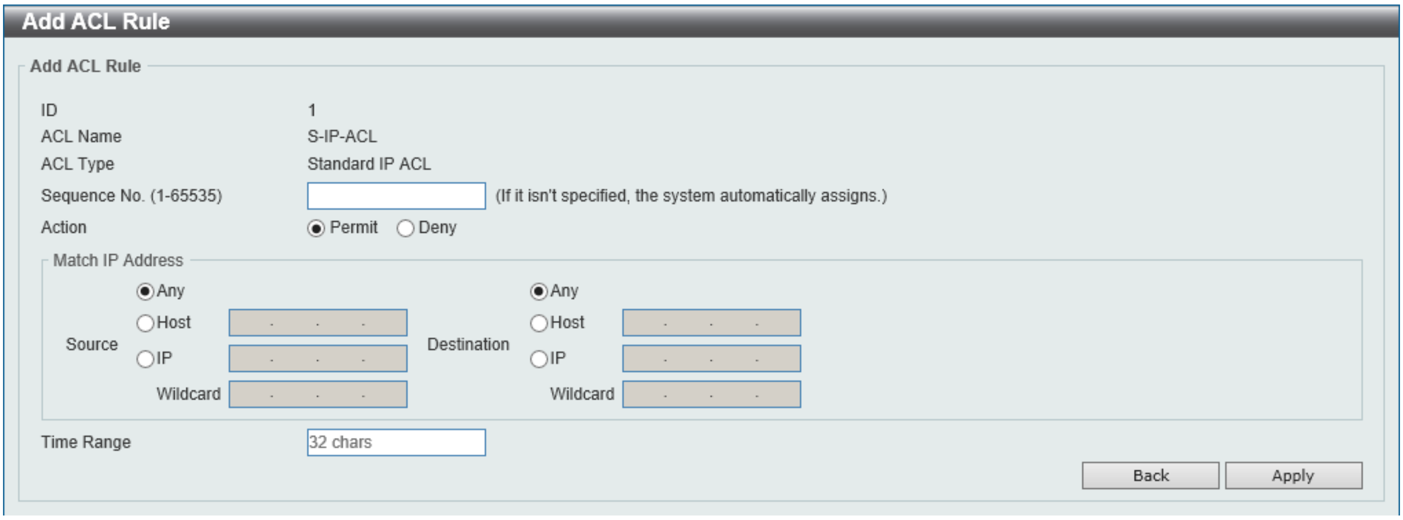
Parameter	Description
ACL Type	Select the ACL type that will be created here. Options to choose from are **Standard IP ACL**, **Extended IP ACL**, **Standard IPv6 ACL**, **Extended IPv6 ACL**, and **Extended MAC ACL**.
ID	Enter the ID for the ACL here. • For a **Standard IP ACL**, the range from 1 to 1999. • For an **Extended IP ACL**, the range from 2000 to 3999.

Parameter	Description
	• For a **Standard IPv6 ACL**, the range from 11000 to 12999. • For an **Extended IPv6 ACL**, the range from 13000 to 14999. • For an **Extended MAC ACL**, the range from 6000 to 7999.
ACL Name	Enter the name of the ACL here. This name can be up to 32 characters long.

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

Standard IP ACL

After selecting a Standard IP ACL and clicking the **Add Rule** button, the following page will appear.



Add ACL Rule

Add ACL Rule

ID 1

ACL Name S-IP-ACL

ACL Type Standard IP ACL

Sequence No. (1-65535) (If it isn't specified, the system automatically assigns.)

Action ● Permit ○ Deny

Match IP Address

Source ● Any ○ Host ○ IP Wildcard

Destination ● Any ○ Host ○ IP Wildcard

Time Range 32 chars

Back Apply

Figure 8-11 Standard IP ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the sequence number of this ACL rule here. The range is from 1 to 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.
Source	Select and enter the source information here. Options to choose from are **Any**, **Host**, **IP**, and **Wildcard**. • When the **Any** option is selected, any source traffic will be evaluated according to the conditions of this rule. • When the **Host** option is selected, enter the source host IP address here. • When the **IP** option is selected, the **Wildcard** option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are **Any**, **Host**, **IP**, and **Wildcard**. • When the **Any** option is selected, any destination traffic will be evaluated according to the conditions of this rule. • When the **Host** option is selected, enter the destination host IP address here. • When the **IP** option is selected, the **Wildcard** option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.

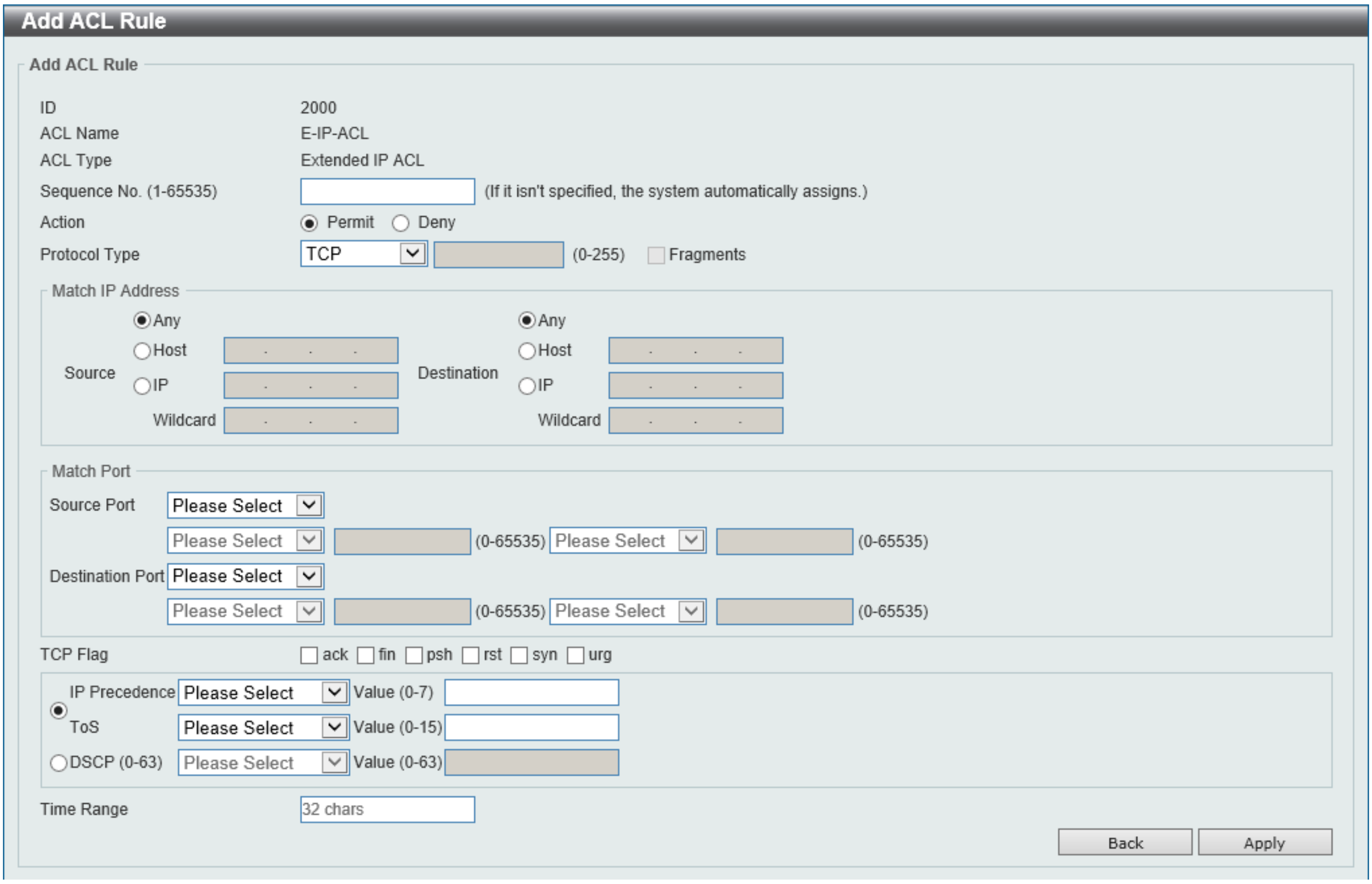
Parameter	Description
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.

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

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

Extended IP ACL

After selecting an Extended IP ACL and clicking the **Add Rule** button, the following page will appear.



Add ACL Rule

Add ACL Rule

ID 2000
ACL Name E-IP-ACL
ACL Type Extended IP ACL
Sequence No. (1-65535) (If it isn't specified, the system automatically assigns.)
Action ● Permit ○ Deny
Protocol Type TCP (0-255) □ Fragments

Match IP Address
Source ● Any ○ Host ○ IP Wildcard
Destination ● Any ○ Host ○ IP Wildcard

Match Port
Source Port Please Select
Please Select (0-65535) Please Select (0-65535)
Destination Port Please Select
Please Select (0-65535) Please Select (0-65535)

TCP Flag □ ack □ fin □ psh □ rst □ syn □ urg

● IP Precedence Please Select Value (0-7)
ToS Please Select Value (0-15)
○ DSCP (0-63) Please Select Value (0-63)

Time Range 32 chars

Figure 8-12 Extended IP ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the sequence number of this ACL rule here. The range is from 1 to 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.
Protocol Type	Select the protocol type option here. Options to choose from are **TCP**, **UDP**, **ICMP**, **EIGRP** (88), **ESP** (50), **GRE** (47), **IGMP** (2), **OSPF** (89), **PIM** (103), **VRRP** (112), **IP-in-IP** (94), **PCP** (108), **Protocol ID**, and **None**. • **Value** - The protocol ID can also manually be entered here. The range is from 0 to 255. • **Fragments** - Select this option to include packet fragment filtering.
Source	Select and enter the source IP information here. Options to choose from are **Any**, **Host**, and **IP**.

Parameter	Description
	• When the **Any** option is selected, any source traffic will be evaluated according to the conditions of this rule. • When the **Host** option is selected, enter the source host IP address here. • When the **IP** option is selected, the **Wildcard** option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination IP information here. Options to choose from are **Any**, **Host**, and **IP**. • When the **Any** option is selected, any destination traffic will be evaluated according to the conditions of this rule. • When the **Host** option is selected, enter the destination host IP address here. • When the **IP** option is selected, the **Wildcard** option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source Port	Select and enter the source port value here. Options to choose from are **=**, **>**, **<**, **≠**, and **Range**. • When selecting the **=** option, the specific selected port number will be used. • When selecting the **>** option, all ports greater than the selected port, will be used. • When selecting the **<** option, all ports smaller than the selected port, will be used. • When selecting the **≠** option, all ports, excluding the selected port, will be used. • When selecting the **Range** option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. This parameter is only available in the protocol type **TCP** and **UDP**.
Destination Port	Select and enter the destination port value here. Options to choose from are **=**, **>**, **<**, **≠**, and **Range**. • When selecting the **=** option, the specific selected port number will be used. • When selecting the **>** option, all ports greater than the selected port, will be used. • When selecting the **<** option, all ports smaller than the selected port, will be used. • When selecting the **≠** option, all ports, excluding the selected port, will be used. • When selecting the **Range** option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. This parameter is only available in the protocol type **TCP** and **UDP**.
Specify ICMP Message Type	Select the ICMP message type used here. This parameter is only available in the protocol type **ICMP**.
ICMP Message Type	When the **ICMP Message Type** is not selected, enter the ICMP Message Type numerical value used here. The range is from 0 to 255. When the **ICMP Message Type** is selected, this numerical value will automatically be entered. This parameter is only available in the protocol type **ICMP**.
Message Code	When the **ICMP Message Type** is not selected, enter the Message Code numerical value used here. The range is from 0 to 255. When the **ICMP Message Type** is selected, this numerical value will automatically be entered. This parameter is only available in the protocol type **ICMP**.
TCP Flag	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are **ack**, **fin**, **psh**, **rst**, **syn**, and **urg**.

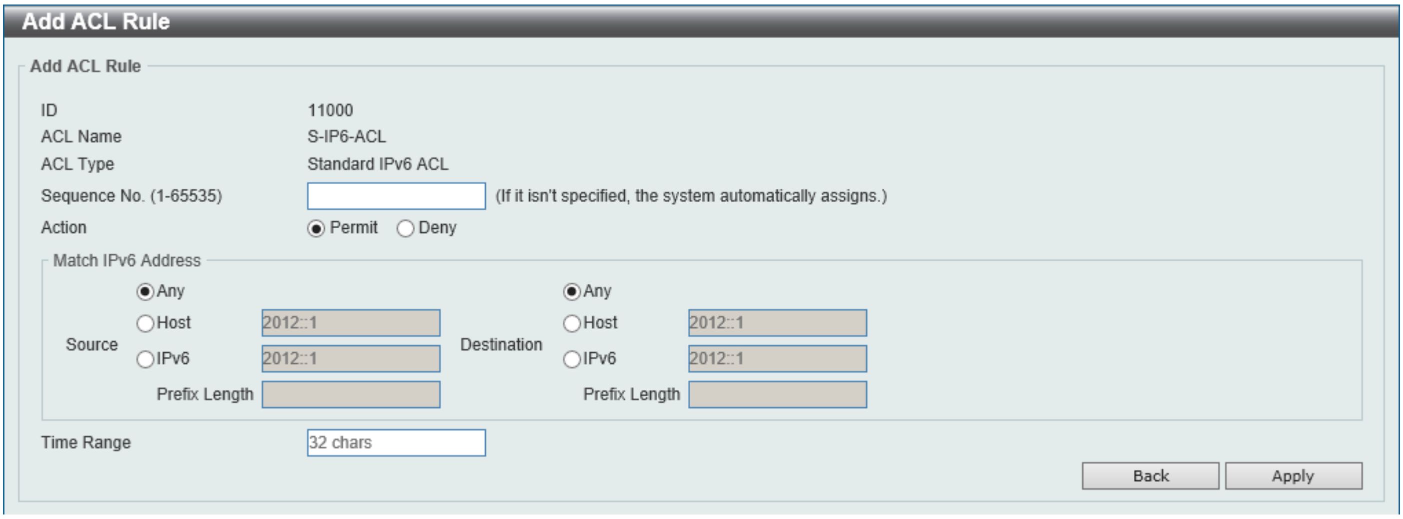
Parameter	Description
	This parameter is only available in the protocol type **TCP**.
IP Precedence	Select the IP precedence value used here. Options to choose from are **routine** (0), **priority** (1), **immediate** (2), **flash** (3), **flash-override** (4), **critical** (5), **internet** (6), and **network** (7). • **Value** - The IP precedence value can also manually be entered here. The range is from 0 to 7.
ToS	Select the Type-of-Service (**ToS**) value that will be used here. Options to choose from are **normal** (0), **min-monetary-cost** (1), **max-reliability** (2), **max-throughput** (4), and **min-delay** (8). • **Value** - The ToS value can also manually be entered here. The range is from 0 to 15.
DSCP	Select the DSCP value that will be used here. Options to choose from are **default** (0), **af11** (10), **af12** (12), **af13** (14), **af21** (18), **af22** (20), **af23** (22), **af31** (26), **af32** (28), **af33** (30), **af41** (34), **af42** (36), **af43** (38), **cs1** (8), **cs2** (16), **cs3** (24), **cs4** (32), **cs5** (40), **cs6** (48), **cs7** (56), and **ef** (46). • **Value** - The DSCP value can also manually be entered here. The range is from 0 to 63.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.

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

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

Standard IPv6 ACL

After selecting a Standard IPv6 ACL and clicking the **Add Rule** button, the following page will appear.



Add ACL Rule

Add ACL Rule

ID 11000
ACL Name S-IP6-ACL
ACL Type Standard IPv6 ACL
Sequence No. (1-65535) (If it isn't specified, the system automatically assigns.)
Action ● Permit ○ Deny

Match IPv6 Address

Source: ● Any ○ Host 2012::1 ○ IPv6 2012::1 Prefix Length
Destination: ● Any ○ Host 2012::1 ○ IPv6 2012::1 Prefix Length

Time Range 32 chars

Figure 8-13 Standard IPv6 ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the sequence number of this ACL rule here. The range is from 1 to 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.
Source	Select and enter the source IPv6 information here. Options to choose from are **Any**, **Host**, **IPv6**, and **Prefix Length**.

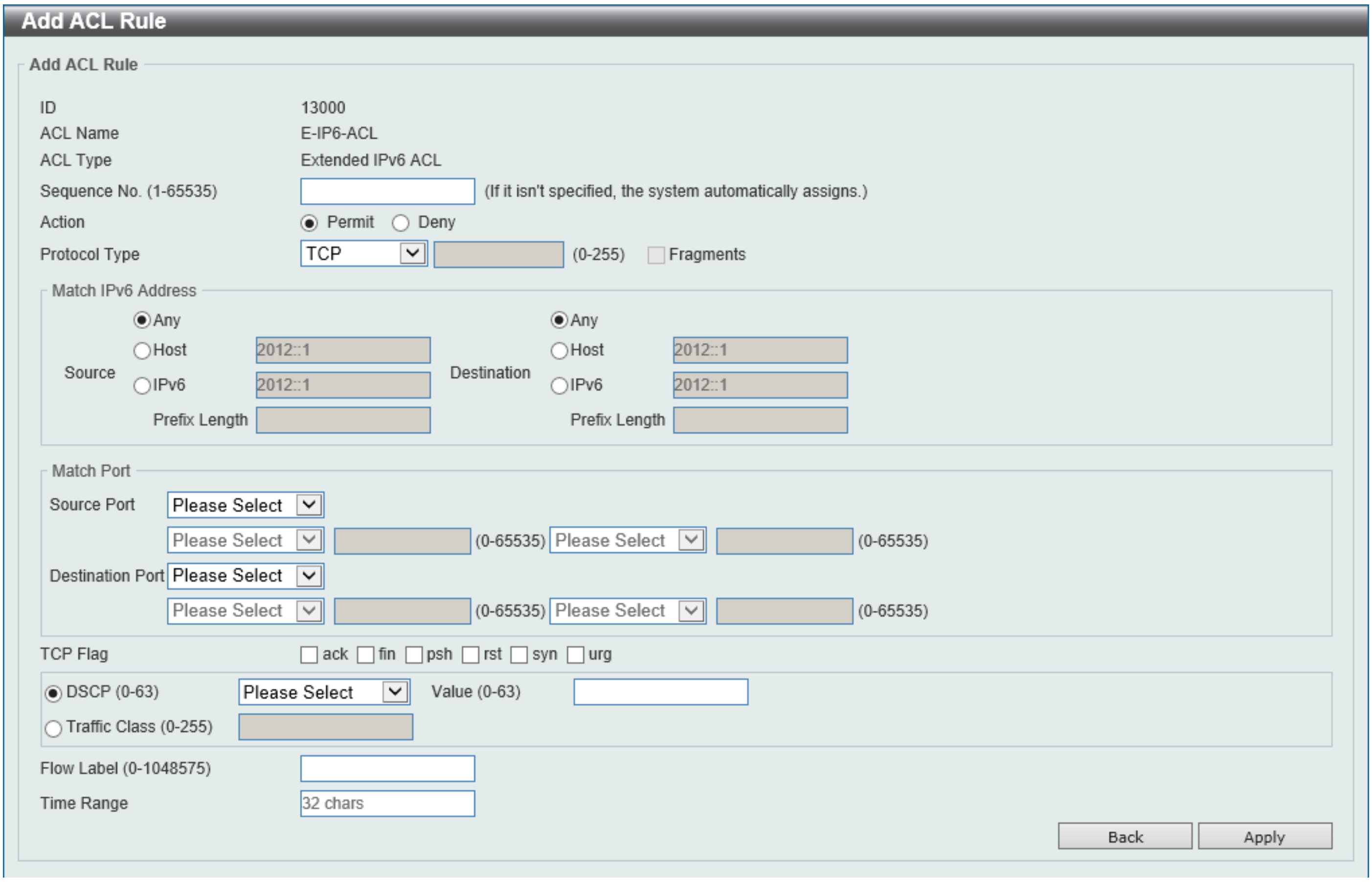
Parameter	Description
	• When the **Any** option is selected, any source traffic will be evaluated according to the conditions of this rule. • When the **Host** option is selected, enter the source host IPv6 address here. • When the **IPv6** option is selected, the **Prefix Length** option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination IPv6 information here. Options to choose from are **Any**, **Host**, **IPv6**, and **Prefix Length**. • When the **Any** option is selected, any destination traffic will be evaluated according to the conditions of this rule. • When the **Host** option is selected, enter the destination host IPv6 address here. • When the **IPv6** option is selected, the **Prefix Length** option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.

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

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

Extended IPv6 ACL

After selecting an Extended IPv6 ACL and clicking the **Add Rule** button, the following page will appear.



Add ACL Rule

Add ACL Rule

ID 13000

ACL Name E-IP6-ACL

ACL Type Extended IPv6 ACL

Sequence No. (1-65535) (If it isn't specified, the system automatically assigns.)

Action ● Permit ○ Deny

Protocol Type TCP (0-255) □ Fragments

Match IPv6 Address

Source ● Any ○ Host 2012::1 ○ IPv6 2012::1 Prefix Length

Destination ● Any ○ Host 2012::1 ○ IPv6 2012::1 Prefix Length

Match Port

Source Port Please Select

Please Select (0-65535) Please Select (0-65535)

Destination Port Please Select

Please Select (0-65535) Please Select (0-65535)

TCP Flag □ ack □ fin □ psh □ rst □ syn □ urg

● DSCP (0-63) Please Select Value (0-63)

○ Traffic Class (0-255)

Flow Label (0-1048575)

Time Range 32 chars

Figure 8-14 Extended IPv6 ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the sequence number of this ACL rule here. The range is from 1 to 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.
Protocol Type	Select the protocol type option here. Options to choose from are **TCP**, **UDP**, **ICMP**, **Protocol ID**, **ESP** (50), **PCP** (108), **SCTP** (132), and **None**. • **Value -** The protocol ID can also manually be entered here. The range is from 0 to 255. • **Fragments -** Select this option to include packet fragment filtering.
Source	Select and enter the source IPv6 information here. Options to choose from are **Any**, **Host**, and **IPv6**. • When the **Any** option is selected, any source traffic will be evaluated according to the conditions of this rule. • When the **Host** option is selected, enter the source host IPv6 address here. • When the **IPv6** option is selected, the **Prefix Length** option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination IPv6 information here. Options to choose from are **Any**, **Host**, and **IPv6**. • When the **Any** option is selected, any destination traffic will be evaluated according to the conditions of this rule. • When the **Host** option is selected, enter the destination host IPv6 address here. • When the **IPv6** option is selected, the **Prefix Length** option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Source Port	Select and enter the source port value here. Options to choose from are **=**, **>**, **<**, **≠**, and **Range**. • When selecting the **=** option, the specific selected port number will be used. • When selecting the **>** option, all ports greater than the selected port, will be used. • When selecting the **<** option, all ports smaller than the selected port, will be used. • When selecting the **≠** option, all ports, excluding the selected port, will be used. • When selecting the **Range** option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. This parameter is only available in the protocol type **TCP** and **UDP**.
Destination Port	Select and enter the destination port value here. Options to choose from are **=**, **>**, **<**, **≠**, and **Range**. • When selecting the **=** option, the specific selected port number will be used. • When selecting the **>** option, all ports greater than the selected port, will be used. • When selecting the **<** option, all ports smaller than the selected port, will be used. • When selecting the **≠** option, all ports, excluding the selected port, will be used. • When selecting the **Range** option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. This parameter is only available in the protocol type **TCP** and **UDP**.

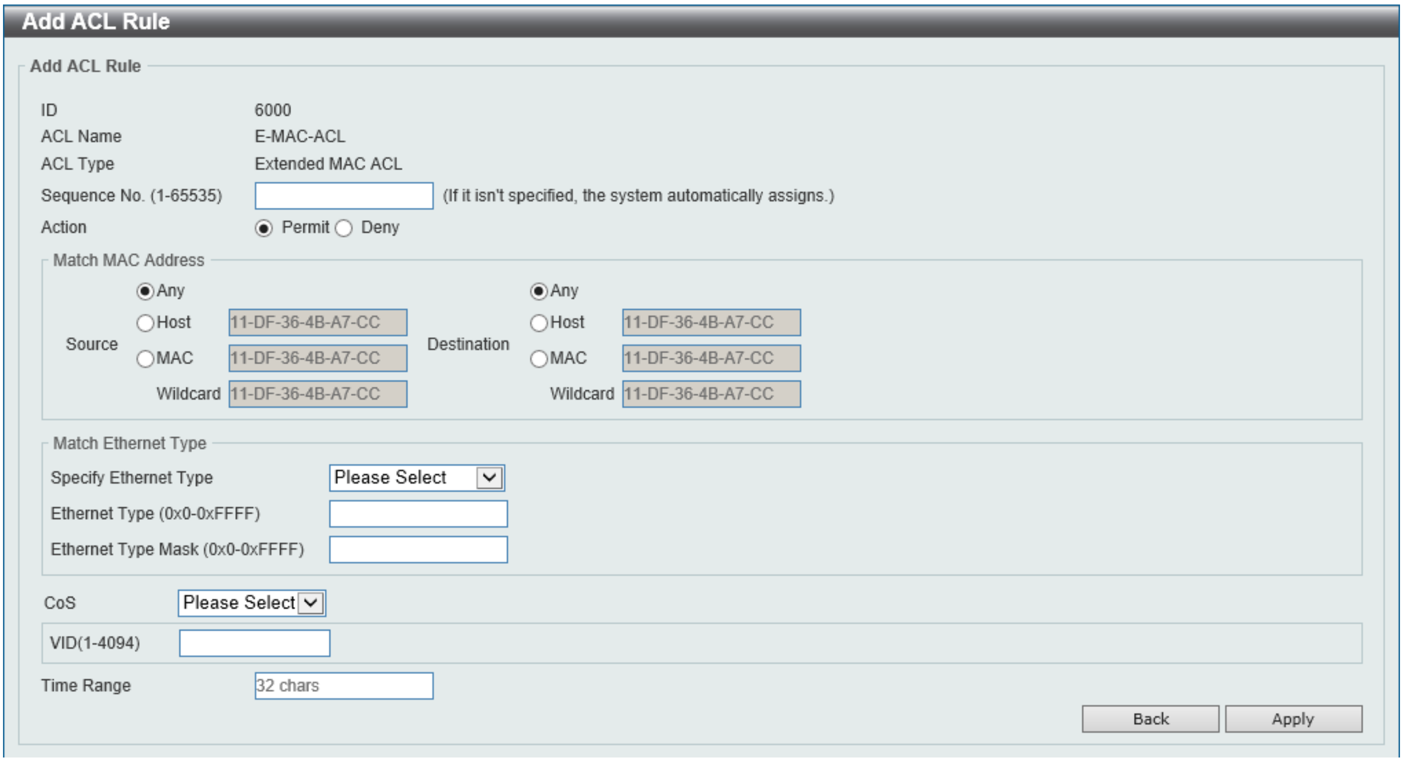
Parameter	Description
TCP Flag	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are **ack**, **fin**, **psh**, **rst**, **syn**, and **urg**. This parameter is only available in the protocol type **TCP**.
Specify ICMP Message Type	Select the ICMP message type used here. This parameter is only available in the protocol type **ICMP**.
ICMP Message Type	When the **ICMP Message Type** is not selected, enter the ICMP Message Type numerical value used here. The range is from 0 to 255. When the **ICMP Message Type** is selected, this numerical value will automatically be entered. This parameter is only available in the protocol type **ICMP**.
Message Code	When the **ICMP Message Type** is not selected, enter the Message Code numerical value used here. The range is from 0 to 255. When the **ICMP Message Type** is selected, this numerical value will automatically be entered. This parameter is only available in the protocol type **ICMP**.
DSCP	Select the DSCP value that will be used here. Options to choose from are **default** (0), **af11** (10), **af12** (12), **af13** (14), **af21** (18), **af22** (20), **af23** (22), **af31** (26), **af32** (28), **af33** (30), **af41** (34), **af42** (36), **af43** (38), **cs1** (8), **cs2** (16), **cs3** (24), **cs4** (32), **cs5** (40), **cs6** (48), **cs7** (56), and **ef** (46). • **Value** - The DSCP value can also manually be entered here. The range is from 0 to 63.
Traffic Class	Select and enter the traffic class value here. The range is from 0 to 255.
Flow Label	Enter the flow label value here. This value must be between 0 and 1048575.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.

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

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

Extended MAC ACL

After selecting an Extended MAC ACL and clicking the **Add Rule** button, the following page will appear.



Add ACL Rule

Add ACL Rule

ID 6000

ACL Name E-MAC-ACL

ACL Type Extended MAC ACL

Sequence No. (1-65535) (If it isn't specified, the system automatically assigns.)

Action ● Permit ○ Deny

Match MAC Address

Source: ● Any ○ Host 11-DF-36-4B-A7-CC ○ MAC 11-DF-36-4B-A7-CC Wildcard 11-DF-36-4B-A7-CC

Destination: ● Any ○ Host 11-DF-36-4B-A7-CC ○ MAC 11-DF-36-4B-A7-CC Wildcard 11-DF-36-4B-A7-CC

Match Ethernet Type

Specify Ethernet Type: Please Select

Ethernet Type (0x0-0xFFFF)

Ethernet Type Mask (0x0-0xFFFF)

CoS: Please Select

VID(1-4094)

Time Range: 32 chars

Figure 8-15 Extended MAC ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the sequence number of this ACL rule here. The range is from 1 to 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.
Source	Select and enter the source MAC address information here. Options to choose from are **Any**, **Host**, **MAC**, and **Wildcard**. • When the **Any** option is selected, any source traffic will be evaluated according to the conditions of this rule. • When the **Host** option is selected, enter the source host MAC address here. • When the **MAC** option is selected, the **Wildcard** option will also be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination	Select and enter the destination MAC address information here. Options to choose from are **Any**, **Host**, **MAC**, and **Wildcard**. • When the **Any** option is selected, any destination traffic will be evaluated according to the conditions of this rule. • When the **Host** option is selected, enter the destination host MAC address here. • When the **MAC** option is selected, the **Wildcard** option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
Specify Ethernet Type	Select the Ethernet type option here. Options to choose from are **aarp**, **appletalk**, **decent-iv**, **etype-6000**, **etype-8042**, **lat**, **lavc-sca**, **mop-console**, **mop-dump**, **vines-echo**, **vines-ip**, **xns-idp**, and **arp**.
Ethernet Type	Enter the Ethernet type hexadecimal value here. This value must be between 0x0 and 0xFFFF. When the Ethernet type profile is selected, above, the appropriate hexadecimal value will automatically be entered.
Ethernet Type Mask	Enter the Ethernet type mask hexadecimal value here. This value must be between 0x0 and 0xFFFF. When the Ethernet type profile is selected, above, the appropriate hexadecimal value will automatically be entered.
CoS	Select the CoS value that will be used here. The range is from **0** to **7**.
VID	Enter the VLAN ID that will be associated with this ACL rule here. The range is from 1 to 4094.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.

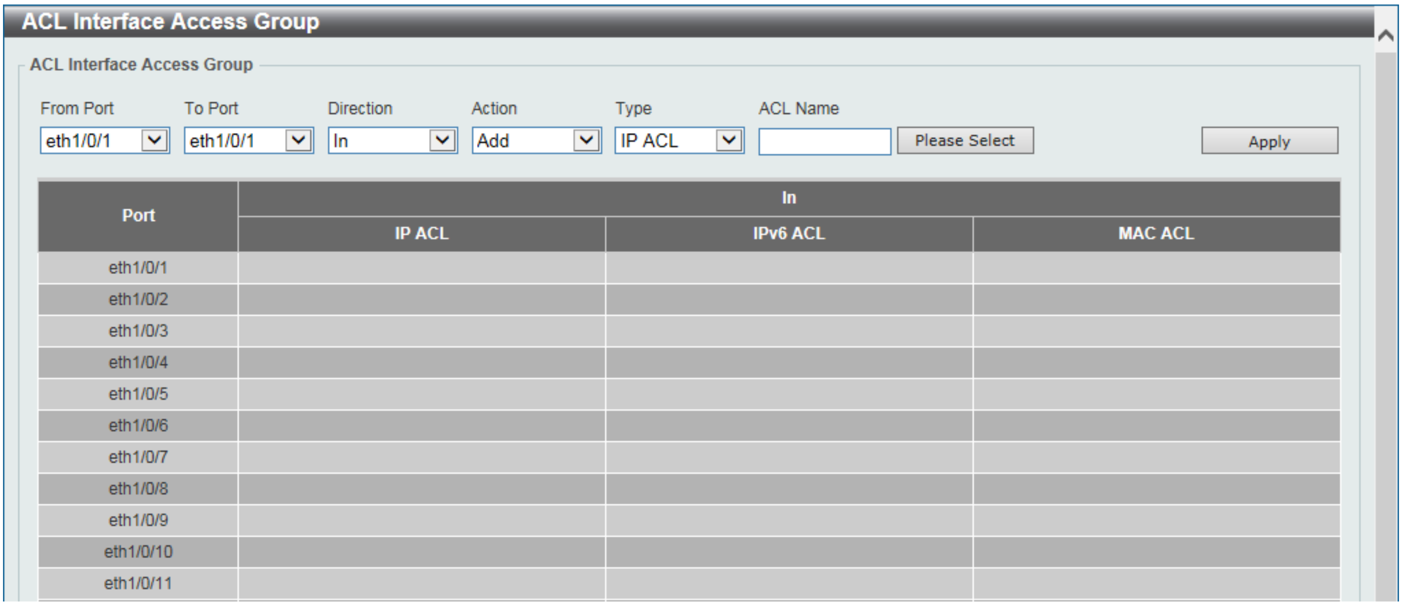
Click the **Apply** button to accept the changes made.

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

ACL Interface Access Group

This window is used to display and configure the ACL interface access group settings.

To view the following window, click **ACL > ACL Interface Access Group**, as shown below:



ACL Interface Access Group

ACL Interface Access Group

From Port: eth1/0/1
To Port: eth1/0/1
Direction: In
Action: Add
Type: IP ACL
ACL Name:

Port	In		
	IP ACL	IPv6 ACL	MAC ACL
eth1/0/1			
eth1/0/2			
eth1/0/3			
eth1/0/4			
eth1/0/5			
eth1/0/6			
eth1/0/7			
eth1/0/8			
eth1/0/9			
eth1/0/10			
eth1/0/11			

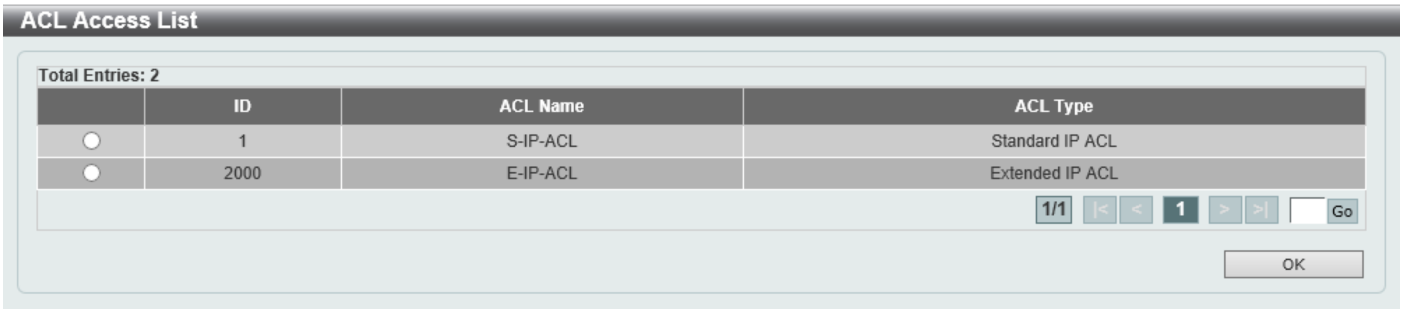
Figure 8-16 ACL Interface Access Group Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
Direction	Specifies that the **In** direction is used.
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**.
Type	Select the ACL type here. Options to choose from are **IP ACL**, **IPv6 ACL**, and **MAC ACL**.
ACL Name	Enter the ACL name here. This name can be up to 32 characters long. Click the **Please Select** button to select an existing ACL from the list.

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

After clicking the **Please Select** button, the following window will appear:



ACL Access List

Total Entries: 2

	ID	ACL Name	ACL Type
○	1	S-IP-ACL	Standard IP ACL
○	2000	E-IP-ACL	Extended IP ACL

Figure 8-17 ACL Interface Access Group (Please Select) Window

Select the radio button next to the entry to use that ACL in the configuration.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **OK** button to accept the selection made.

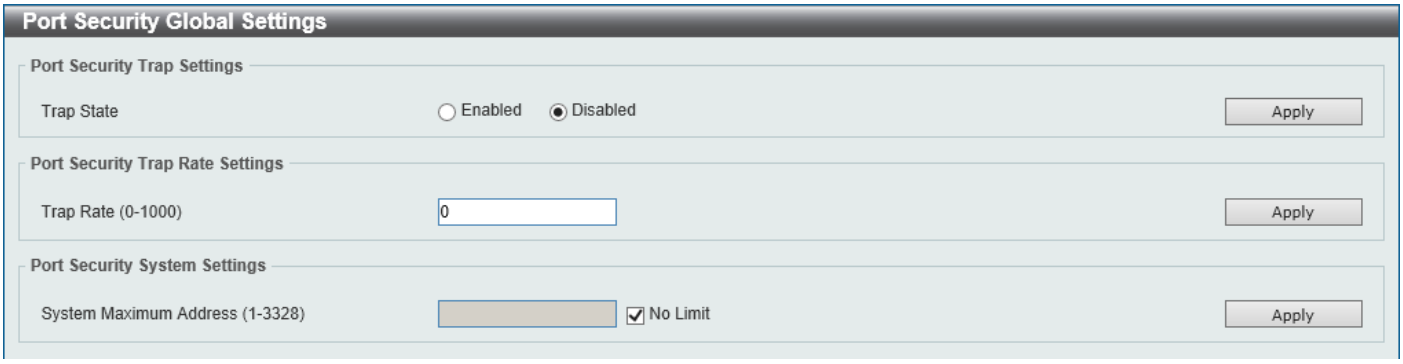
9. Security

Port Security

Port Security Global Settings

This window is used to display and configure the global port security settings. Port Security is a security feature that prevents unauthorized computers (with source MAC addresses) unknown to the Switch prior to locking the port (or ports) from connecting to the Switch's locked ports and gaining access to the network.

To view the following window, click **Security > Port Security > Port Security Global Settings**, as shown below:



Port Security Global Settings

Port Security Trap Settings

Trap State ○ Enabled ● Disabled

Port Security Trap Rate Settings

Trap Rate (0-1000): 0

Port Security System Settings

System Maximum Address (1-3328) ☑ No Limit

Figure 9-1 Port Security Global Settings Window

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

Parameter	Description
Trap State	Select to enable or disable port security traps on the Switch.

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

The fields that can be configured in **Port Security Trap Rate Settings** are described below:

Parameter	Description
Trap Rate	Enter the number of traps per second. The range is from 0 to 1000. The default value 0 indicates an SNMP trap to be generated for every security violation.

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

The fields that can be configured in **Port Security System Settings** are described below:

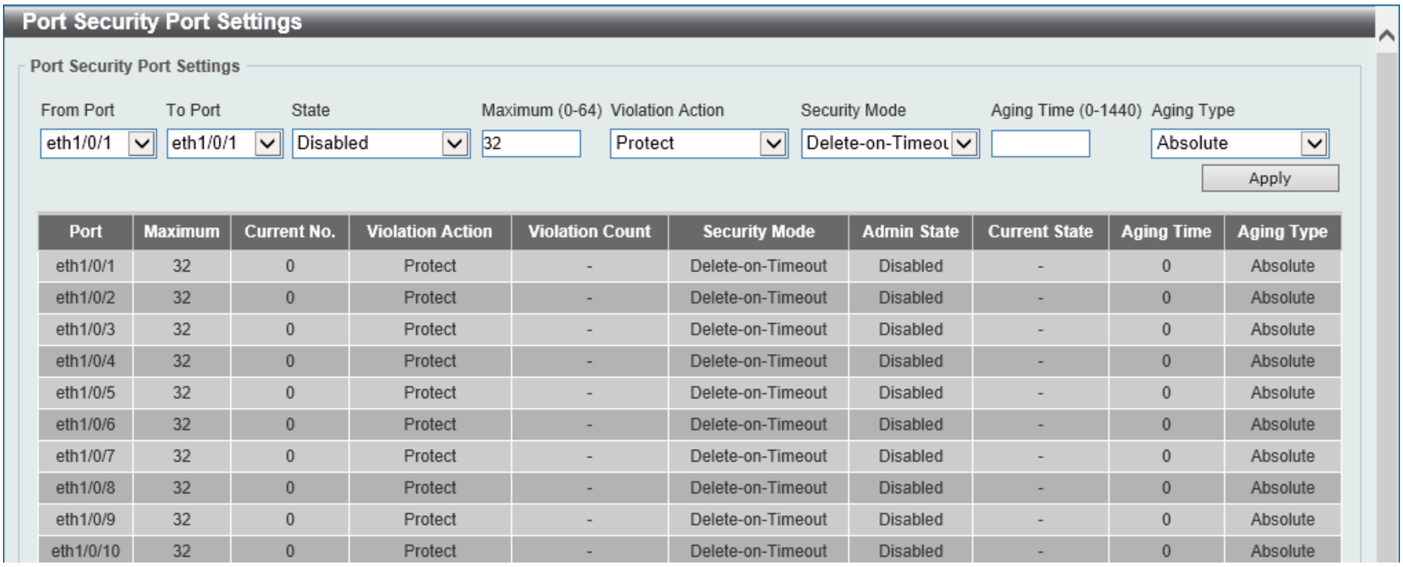
Parameter	Description
System Maximum Address	Enter the maximum number of secure MAC addresses allowed. If not specified, the default value is No Limit. The valid range is from 1 to 3328. Tick the **No Limit** checkbox to allow the maximum number of secure MAC address.

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

Port Security Port Settings

This window is used to display and configure the port security port settings.

To view the following window, click **Security > Port Security > Port Security Port Settings**, as shown below:



Port Security Port Settings

From Port: eth1/0/1
To Port: eth1/0/1
State: Disabled
Maximum (0-64): 32
Violation Action: Protect
Security Mode: Delete-on-Timeou
Aging Time (0-1440):
Aging Type: Absolute

Port	Maximum	Current No.	Violation Action	Violation Count	Security Mode	Admin State	Current State	Aging Time	Aging Type
eth1/0/1	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/2	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/3	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/4	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/5	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/6	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/7	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/8	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/9	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
eth1/0/10	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute

Figure 9-2 Port Security Port Settings Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the port security feature on the port(s) specified.
Maximum	Enter the maximum number of secure MAC addresses that will be allowed on the port(s) specified. This value must be between 0 and 64. By default, this value is 32.
Violation Action	Select the violation action that will be taken here. Options to choose from are: • **Protect** - Specifies to drop all packets from the insecure hosts at the port-security process level, but does not increment the security-violation count. • **Restrict** - Specifies to drop all packets from the insecure hosts at the port-security process level and increments the security-violation count and record the system log. • **Shutdown** - Specifies to shut down the port if there is a security violation and record the system log.
Security Mode	Select the security mode option here. Options to choose from are: • **Permanent** - Specifies that under this mode, all learned MAC addresses would not be purged out unless the user manually deletes those entries.

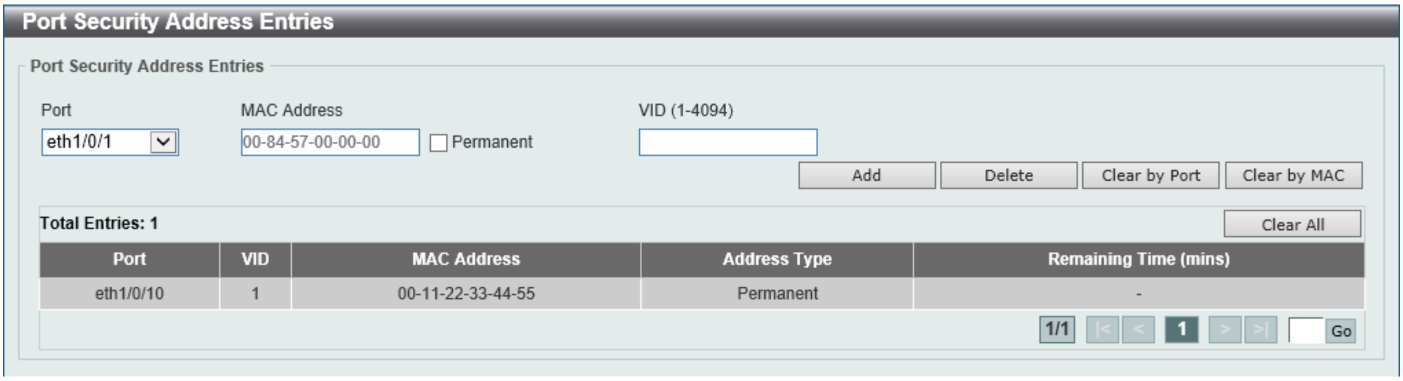
Parameter	Description
	• **Delete-on-Timeout** - Specifies that under this mode, all learned MAC addresses would be purged out when an entry is aged out or when the user manually deletes these entries.
Aging Time	Enter the aging time value used for auto-learned dynamic secured addresses on the specified port here. This value must be between 0 and 1440 minutes.
Aging Type	Specifies that **Absolute** is used. All the secure addresses on this port age out exactly after the time specified and is removed from the secure address list.

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

Port Security Address Entries

This window is used to view, clear, and configure the port security address entries.

To view the following window, click **Security > Port Security > Port Security Address Entries**, as shown below:



Port Security Address Entries

Port Security Address Entries

Port: eth1/0/1

MAC Address: 00-84-57-00-00-00 □ Permanent

VID (1-4094):

Total Entries: 1

Port	VID	MAC Address	Address Type	Remaining Time (mins)
eth1/0/10	1	00-11-22-33-44-55	Permanent	-

Figure 9-3 Port Security Address Entries Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the appropriate port range used for the configuration here.
MAC Address	Enter the MAC address here. Select the **Permanent** option to specify that all learned MAC addresses would not be purged out unless the user manually deletes those entries.
VID	Enter the VLAN ID here. This value must be between 1 and 4094.

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

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

Click the **Clear by Port** button to clear the information based on the port selected.

Click the **Clear by MAC** button to clear the information based on the MAC address entered.

Click the **Clear All** button to clear all the information in this table.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

802.1X

802.1X (Port-based and Host-based Access Control)

The IEEE 802.1X standard is a security measure for authorizing and authenticating users to gain access to various wired or wireless devices on a specified Local Area Network by using a Client and Server based access control model. This is accomplished by using a RADIUS server to authenticate users trying to access a network by relaying Extensible Authentication Protocol over LAN (EAPOL) packets between the Client and the Server.

The following figure represents a basic EAPOL packet:

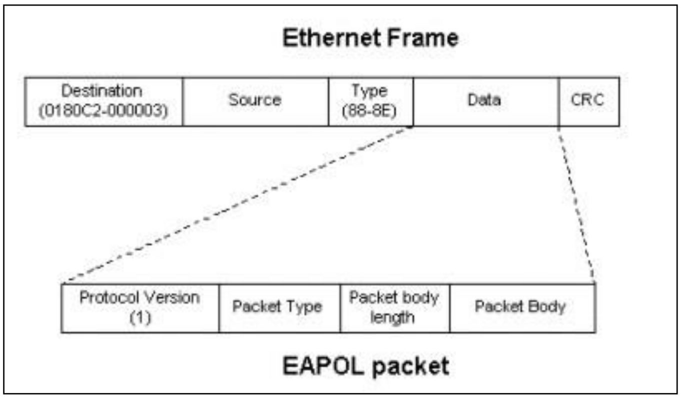


Figure 9-4 The EAPOL Packet

Utilizing this method, unauthorized devices are restricted from connecting to a LAN through a port to which the user is connected. EAPOL packets are the only traffic that can be transmitted through the specific port until authorization is granted. The 802.1X access control method has three roles, each of which are vital to creating and up keeping a stable and working Access Control security method.

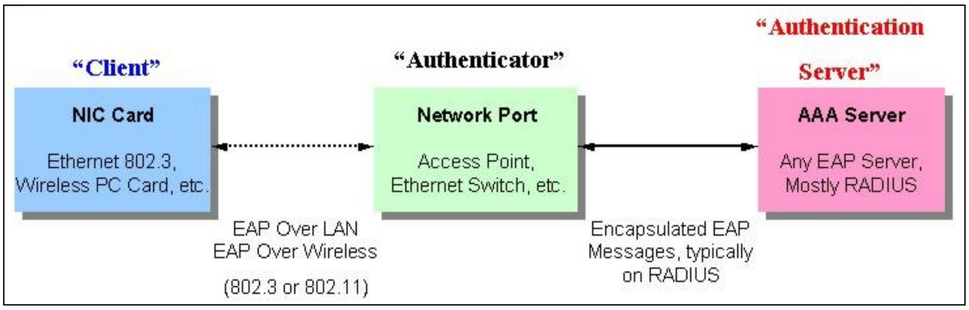

"Client"
NIC Card
Ethernet 802.3, Wireless PC Card, etc.
"Authenticator"
Network Port
Access Point, Ethernet Switch, etc.
"Authentication Server"
AAA Server
Any EAP Server, Mostly RADIUS
EAP Over LAN
EAP Over Wireless
(802.3 or 802.11)
Encapsulated EAP Messages, typically on RADIUS

Figure 9-5 The three roles of 802.1X

The following section will explain the three roles of Client, Authenticator, and Authentication Server in greater detail.

Authentication Server

The Authentication Server is a remote device that is connected to the same network as the Client and Authenticator, must be running a RADIUS Server program and must be configured properly on the Authenticator (Switch). Clients connected to a port on the Switch must be authenticated by the Authentication Server (RADIUS) before attaining any services offered by the Switch on the LAN. The role of the Authentication Server is to certify the identity of the Client attempting to access the network by exchanging secure information between the RADIUS server and the Client through EAPOL packets and, in turn, informs the Switch whether or not the Client is granted access to the LAN and/or switches services.

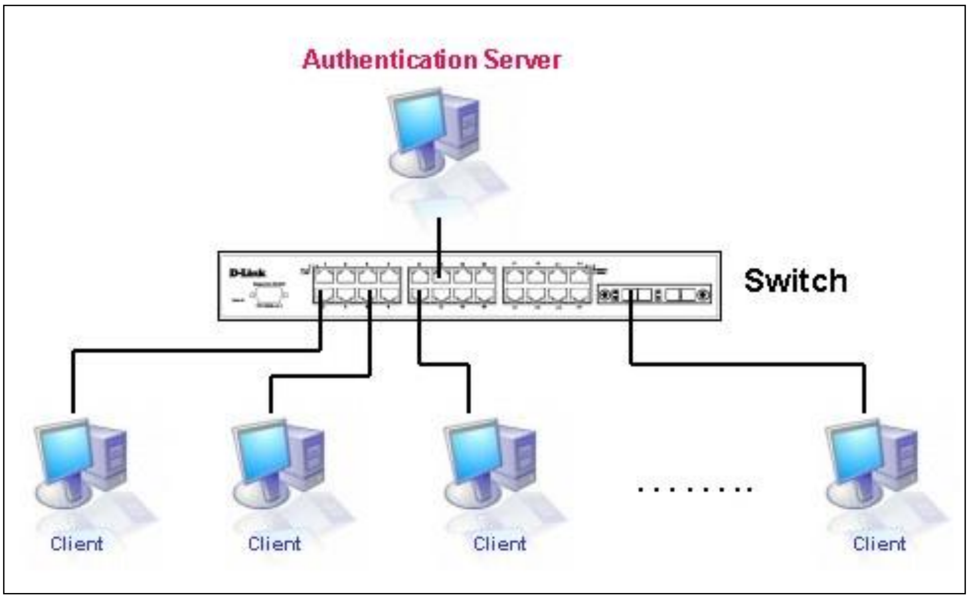


Figure 9-6 The Authentication Server

Authenticator

The Authenticator (the Switch) is an intermediary between the Authentication Server and the Client. The Authenticator serves two purposes when utilizing the 802.1X function. The first purpose is to request certification information from the Client through EAPOL packets, which is the only information allowed to pass through the Authenticator before access is granted to the Client. The second purpose of the Authenticator is to verify the information gathered from the Client with the Authentication Server, and to then relay that information back to the Client.

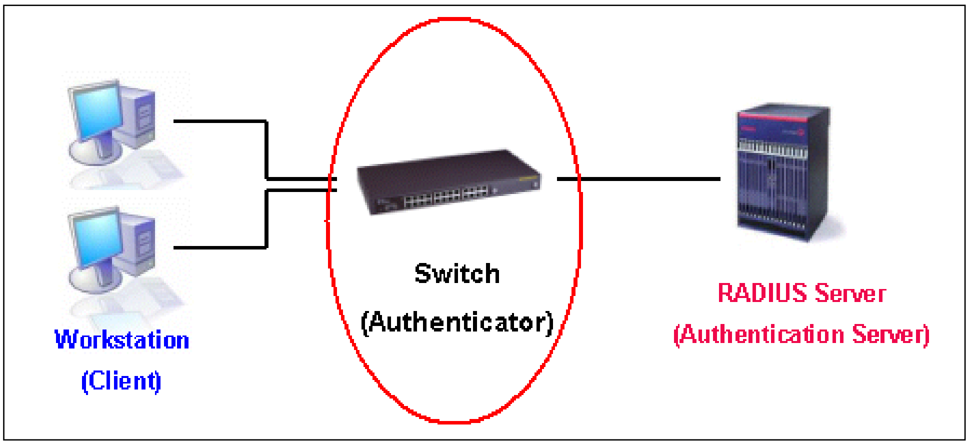


Figure 9-7 The Authenticator

Three steps must be implemented on the Switch to properly configure the Authenticator.

- The 802.1X State must be Enabled. (**Security > 802.1X > 802.1X Global Settings**)
- The 802.1X settings must be implemented by port (**Security > 802.1X > 802.1X Port Settings**)
- A RADIUS server must be configured on the Switch. (**Security > RADIUS > RADIUS Server Settings**)

Client

The Client is simply the end station that wishes to gain access to the LAN or switch services. All end stations must be running software that is compliant with the 802.1X protocol. For users running windows XP and windows Vista, that software is included within the operating system. All other users are required to attain 802.1X client software from an outside source. The Client will request access to the LAN and or Switch through EAPOL packets and, in turn will respond to requests from the Switch.

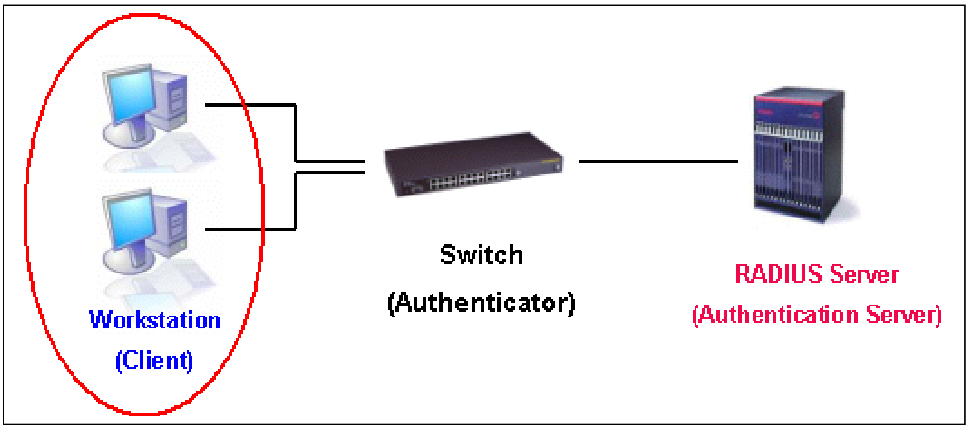


Figure 9-8 The Client

Authentication Process

Utilizing the three roles stated above, the 802.1X protocol provides a stable and secure way of authorizing and authenticating users attempting to access the network. Only EAPOL traffic is allowed to pass through the specified port before a successful authentication is made. This port is “locked” until the point when a Client with the correct username and password (and MAC address if 802.1X is enabled by MAC address) is granted access and therefore successfully “unlocks” the port. Once the port is unlocked, normal traffic is allowed to pass through the port. The following figure displays a more detailed explanation of how the authentication process is completed between the three roles stated above.

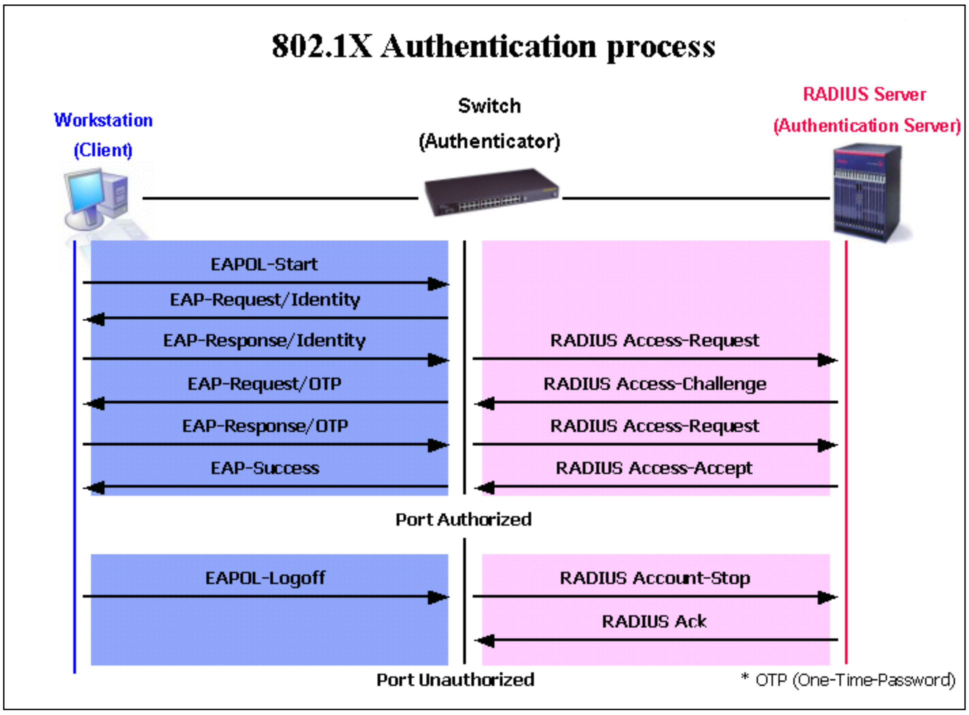


Figure 9-9 The 802.1X Authentication Process

The D-Link implementation of 802.1X allows network administrators to choose between two types of Access Control used on the Switch, which are:

- **Port-based Access Control** - This method requires only one user to be authenticated per port by a remote RADIUS server to allow the remaining users on the same port access to the network.
- **Host-based Access Control** - Using this method, the Switch will automatically learn up to a maximum of 1000 MAC addresses by port and set them in a list. Each MAC address must be authenticated by the Switch using a remote RADIUS server before being allowed access to the Network.

Understanding 802.1X Port-based and Host-based Network Access Control

The original intent behind the development of 802.1X was to leverage the characteristics of point-to-point in LANs. As any single LAN segment in such infrastructures has no more than two devices attached to it, one of which is a Bridge Port. The Bridge Port detects events that indicate the attachment of an active device at the remote end of the link, or an active device becoming inactive. These events can be used to control the authorization state of the Port and initiate the process of authenticating the attached device if the Port is unauthorized. This is the Port-based Network Access Control.

Port-based Network Access Control

Once the connected device has successfully been authenticated, the Port then becomes Authorized, and all subsequent traffic on the Port is not subject to access control restriction until an event occurs that causes the Port to become Unauthorized. Hence, if the Port is actually connected to a shared media LAN segment with more than one attached device, successfully authenticating one of the attached devices effectively provides access to the LAN for all devices on the shared segment. Clearly, the security offered in this situation is open to attack.

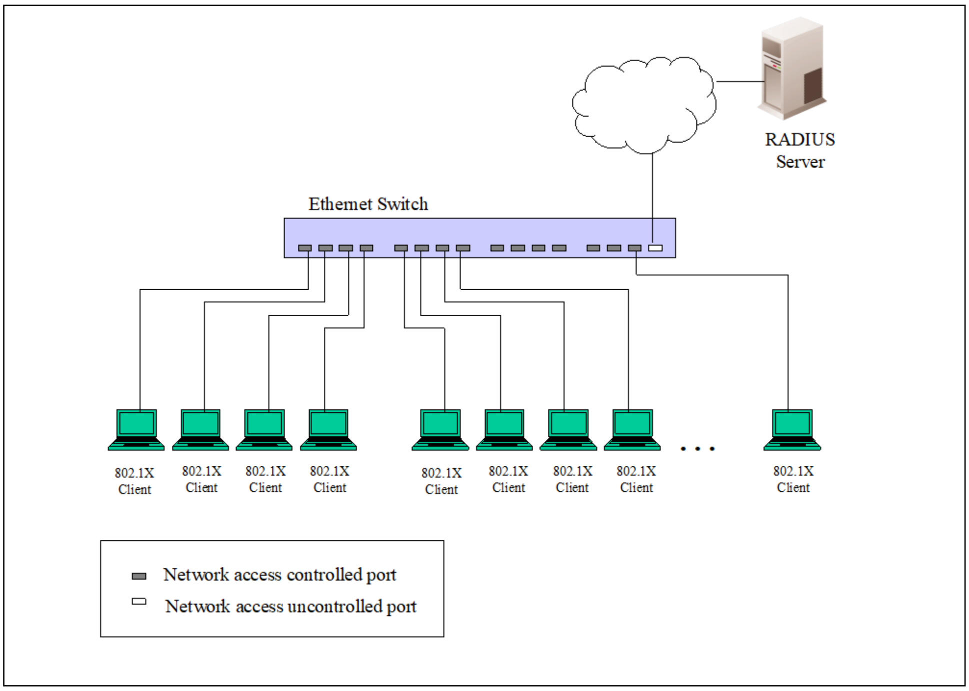


Figure 9-10 Example of Typical Port-based Configuration

Host-based Network Access Control

In order to successfully make use of 802.1X in a shared media LAN segment, it would be necessary to create “logical” Ports, one for each attached device that required access to the LAN. The Switch would regard the single physical Port connecting it to the shared media segment as consisting of a number of distinct logical Ports, each logical Port being independently controlled from the point of view of EAPOL exchanges and authorization state. The Switch learns each attached devices’ individual MAC addresses, and effectively creates a logical Port that the attached device can then use to communicate with the LAN via the Switch.

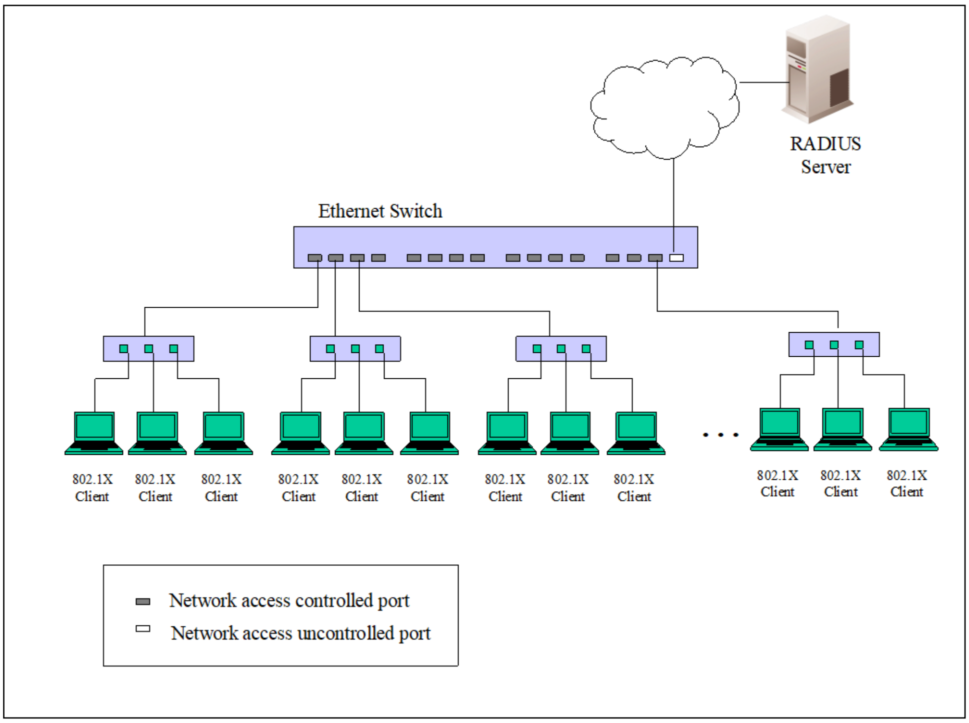
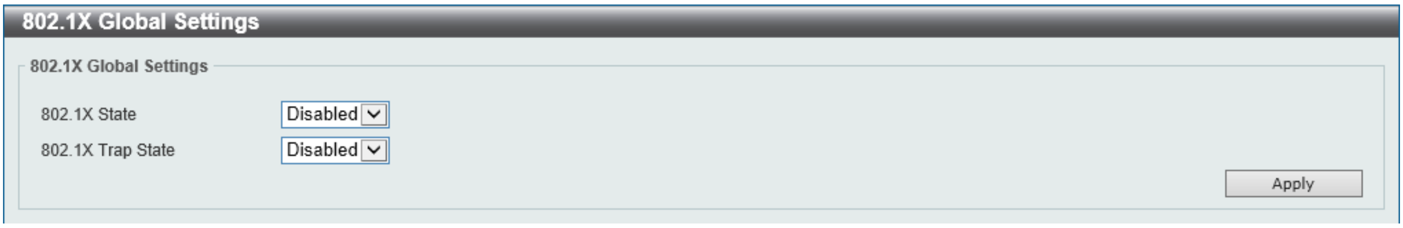

RADIUS Server
Ethernet Switch
802.1X Client
. . .
▬ Network access controlled port
▭ Network access uncontrolled port

Figure 9-11 Example of Typical Host-based Configuration

802.1X Global Settings

This window is used to display and configure the global 802.1X settings.

To view the following window, click **Security > 802.1X > 802.1X Global Settings**, as shown below:



802.1X State: Disabled

802.1X Trap State: Disabled

Figure 9-12 802.1X Global Settings Window

The fields that can be configured are described below:

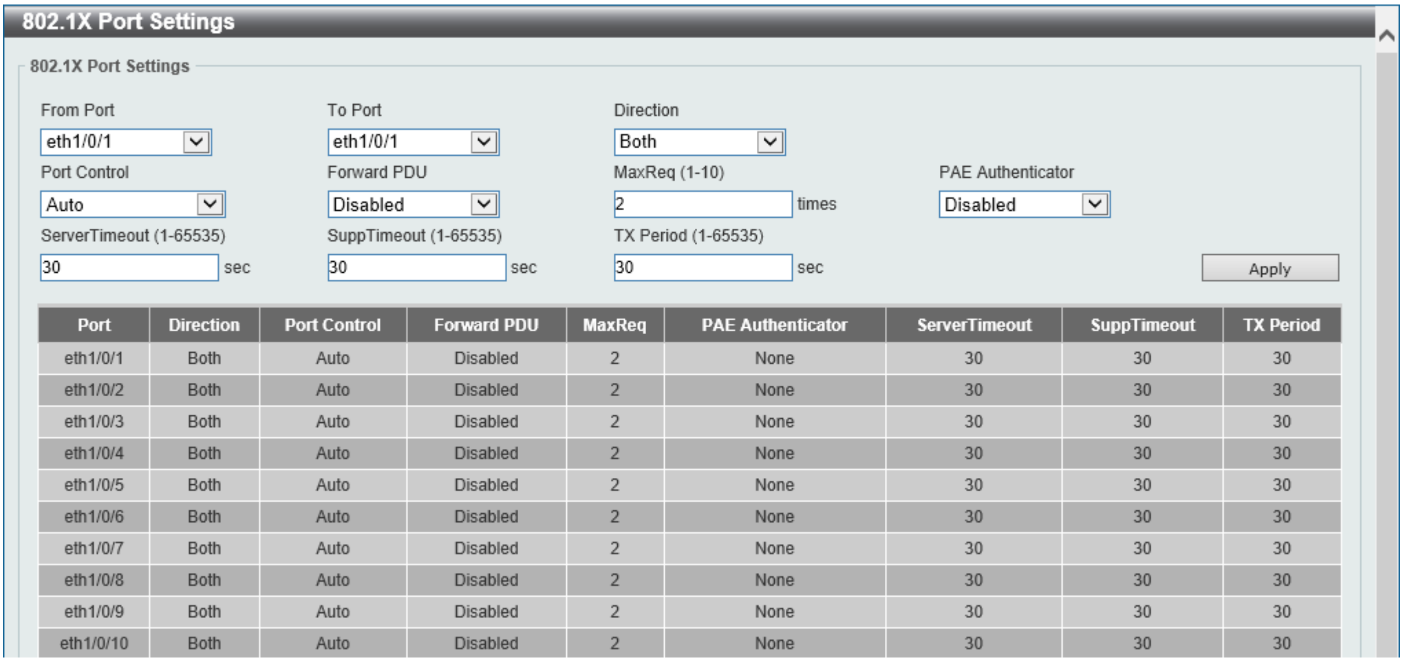
Parameter	Description
802.1X State	Select to enable or disable the global 802.1X state here.
802.1X Trap State	Select to enable or disable the 802.1X trap state here.

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

802.1X Port Settings

This window is used to display and configure the 802.1X port settings.

To view the following window, click **Security > 802.1X > 802.1X Port Settings**, as shown below:



802.1X Port Settings

802.1X Port Settings

From Port: eth1/0/1
To Port: eth1/0/1
Direction: Both
Port Control: Auto
Forward PDU: Disabled
MaxReq (1-10): 2 times
PAE Authenticator: Disabled
ServerTimeout (1-65535): 30 sec
SuppTimeout (1-65535): 30 sec
TX Period (1-65535): 30 sec

Port	Direction	Port Control	Forward PDU	MaxReq	PAE Authenticator	ServerTimeout	SuppTimeout	TX Period
eth1/0/1	Both	Auto	Disabled	2	None	30	30	30
eth1/0/2	Both	Auto	Disabled	2	None	30	30	30
eth1/0/3	Both	Auto	Disabled	2	None	30	30	30
eth1/0/4	Both	Auto	Disabled	2	None	30	30	30
eth1/0/5	Both	Auto	Disabled	2	None	30	30	30
eth1/0/6	Both	Auto	Disabled	2	None	30	30	30
eth1/0/7	Both	Auto	Disabled	2	None	30	30	30
eth1/0/8	Both	Auto	Disabled	2	None	30	30	30
eth1/0/9	Both	Auto	Disabled	2	None	30	30	30
eth1/0/10	Both	Auto	Disabled	2	None	30	30	30

Figure 9-13 802.1X Port Settings Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Direction	Select the direction here. Options to choose from are **Both** and **In**. This option configures the direction of the traffic on a controlled port as unidirectional (In) or bidirectional (Both). The In control direction is only valid when the **Host Mode** is configured as **Multi Host** in the ***Network Access Authentication Port Settings*** window.
Port Control	Select the port control option here. Options to choose from are **ForceAuthorized**, **Auto**, and **ForceUnauthorized**. If the port control is set to force-authorized, then the port is not controlled in both directions. If the port control is set to automatic, then the access to the port for the controlled direction needs to be authenticated. If the port control is set to force-unauthorized, then the access to the port for the controlled direction is blocked.
Forward PDU	Select to enable or disable the forward PDU option here.
MaxReq	Enter the maximum required times value here. This value must be between 1 and 10. By default, this value is 2. This option configures the maximum number of times that the backend authentication state machine will retransmit an Extensible Authentication Protocol (EAP) request frame to the supplicant before restarting the authentication process.
PAE Authenticator	Select to enable or disable the PAE authenticator option here. This option configures a specific port as an IEEE 802.1X port access entity (PAE) authenticator.
Server Timeout	Enter the server timeout value here. This value must be between 1 and 65535 seconds. By default, this value is 30 seconds.
SuppTimeout	Enter the supplicant timeout value here. This value must be between 1 and 65535 seconds. By default, this value is 30 seconds.

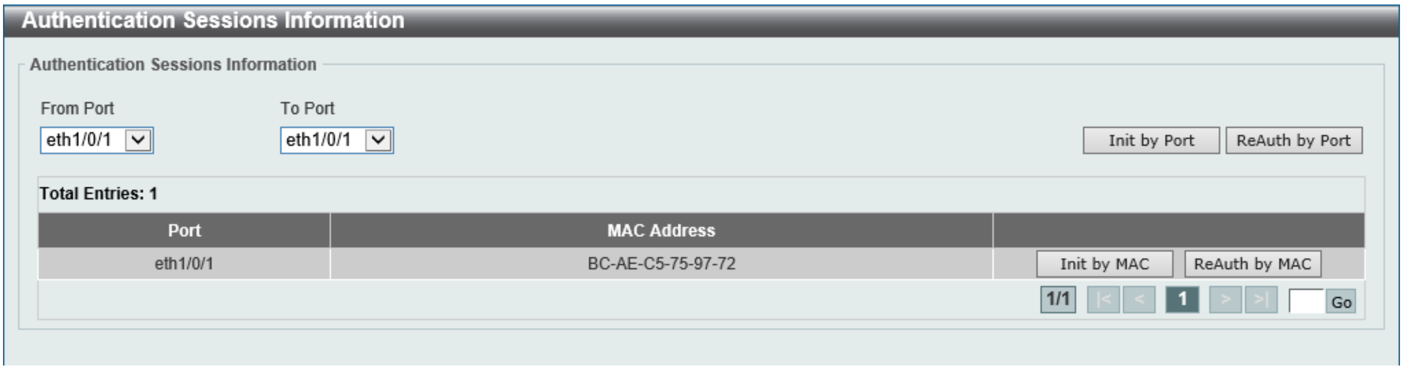
Parameter	Description
TX Period	Enter the transmission period value here. This value must be between 1 and 65535 seconds. By default, this value is 30 seconds.

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

Authentication Sessions Information

This window is used to display and configure the authentication session information.

To view the following window, click **Security > 802.1X > Authentication Sessions Information**, as shown below:



Authentication Sessions Information

Authentication Sessions Information

From Port: eth1/0/1

To Port: eth1/0/1

Total Entries: 1

Port	MAC Address	
eth1/0/1	BC-AE-C5-75-97-72	Init by MAC ReAuth by MAC

Figure 9-14 Authentication Sessions Information Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.

Click the **Init by Port** button to initiate the session information based on the port selections made.

Click the **ReAuth by Port** button to re-authenticate the session information based on the port selections made.

Click the **Init by MAC** button to initiate the session information based on MAC address.

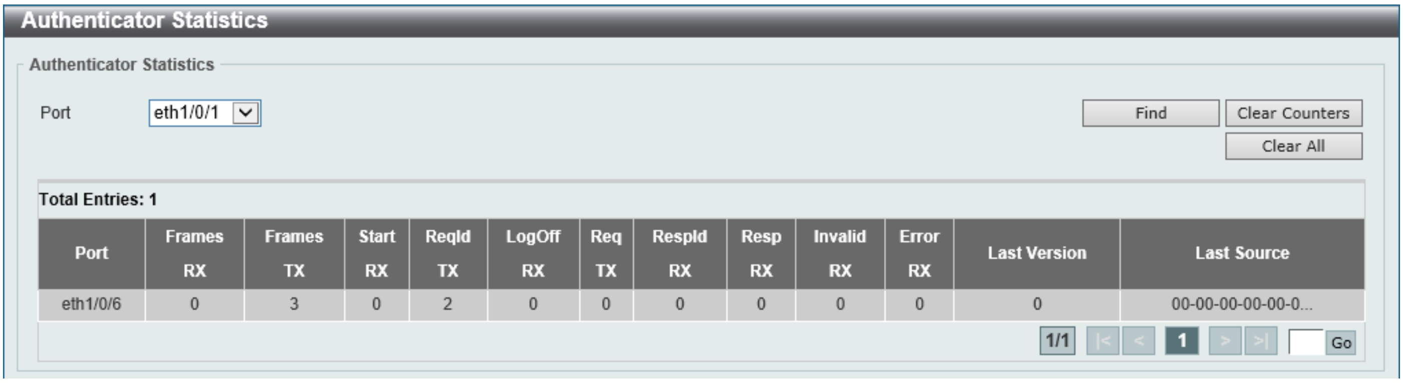
Click the **ReAuth by MAC** button to re-authenticate the session information based on MAC address.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Authenticator Statistics

This window is used to view and clear the authenticator statistics.

To view the following window, click **Security > 802.1X > Authenticator Statistics**, as shown below:



Authenticator Statistics

Authenticator Statistics

Port: eth1/0/1

Total Entries: 1

Port	Frames RX	Frames TX	Start RX	ReqId TX	LogOff RX	Req TX	RespId RX	Resp RX	Invalid RX	Error RX	Last Version	Last Source
eth1/0/6	0	3	0	2	0	0	0	0	0	0	0	00-00-00-00-00-0...

Figure 9-15 Authenticator Statistics Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the appropriate port used for the query here.

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

Click the **Clear Counters** button to clear the counter information based on the selections made.

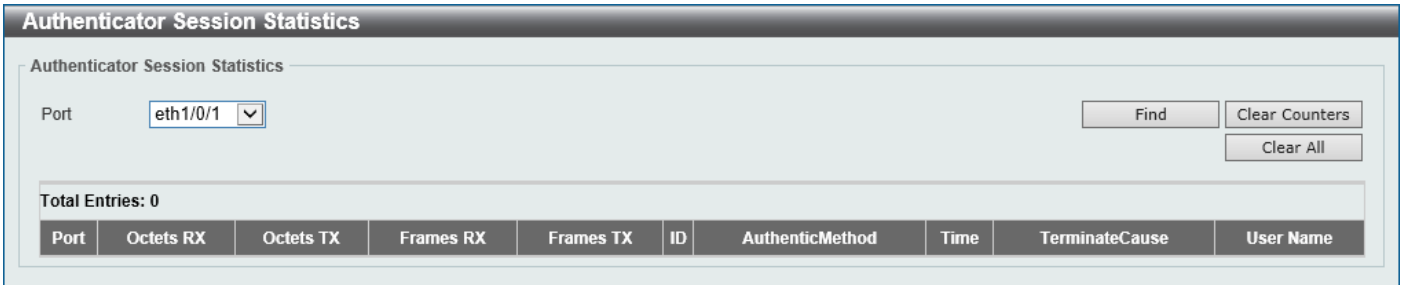
Click the **Clear All** button to clear all the information in this table.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Authenticator Session Statistics

This window is used to view and clear the authenticator session statistics.

To view the following window, click **Security > 802.1X > Authenticator Session Statistics**, as shown below:


Authenticator Session Statistics
Authenticator Session Statistics
Find
Clear Counters
Clear All

Port: eth1/0/1

Total Entries: 0

Port	Octets RX	Octets TX	Frames RX	Frames TX	ID	AuthenticMethod	Time	TerminateCause	User Name

Figure 9-16 Authenticator Session Statistics Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the appropriate port used for the query here.

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

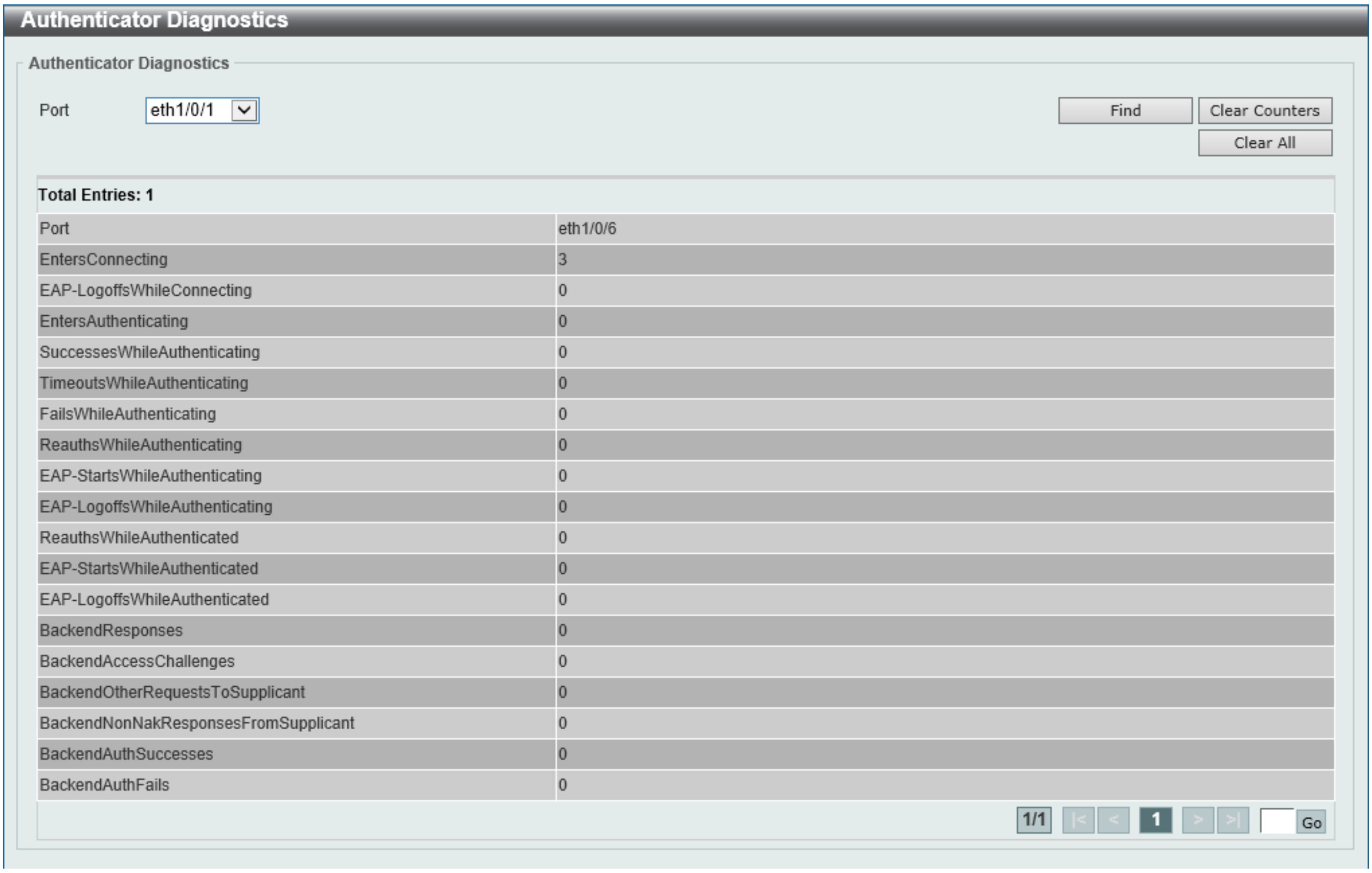
Click the **Clear Counters** button to clear the counter information based on the selections made.

Click the **Clear All** button to clear all the information in this table.

Authenticator Diagnostics

This window is used to view and clear the authenticator diagnostics information.

To view the following window, click **Security > 802.1X > Authenticator Diagnostics**, as shown below:



Port eth1/0/1

Total Entries: 1

Port	eth1/0/6
EntersConnecting	3
EAP-LogoffsWhileConnecting	0
EntersAuthenticating	0
SuccessesWhileAuthenticating	0
TimeoutsWhileAuthenticating	0
FailsWhileAuthenticating	0
ReauthsWhileAuthenticating	0
EAP-StartsWhileAuthenticating	0
EAP-LogoffsWhileAuthenticating	0
ReauthsWhileAuthenticated	0
EAP-StartsWhileAuthenticated	0
EAP-LogoffsWhileAuthenticated	0
BackendResponses	0
BackendAccessChallenges	0
BackendOtherRequestsToSupplicant	0
BackendNonNakResponsesFromSupplicant	0
BackendAuthSuccesses	0
BackendAuthFails	0

Figure 9-17 Authenticator Diagnostics Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the appropriate port used for the query here.

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

Click the **Clear Counters** button to clear the counter information based on the selections made.

Click the **Clear All** button to clear all the information in this table.

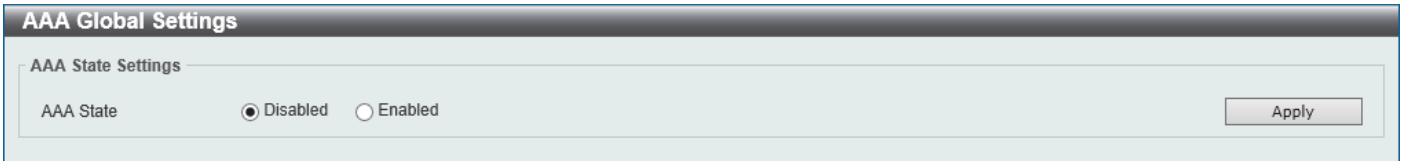
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

AAA

AAA Global Settings

This window is used to enable or disable the global Authentication, Authorization, and Accounting (AAA) state.

To view the following window, click **Security > AAA > AAA Global Settings**, as shown below:



AAA Global Settings

AAA State Settings

AAA State ● Disabled ○ Enabled

Figure 9-18 AAA Global Settings Window

The fields that can be configured are described below:

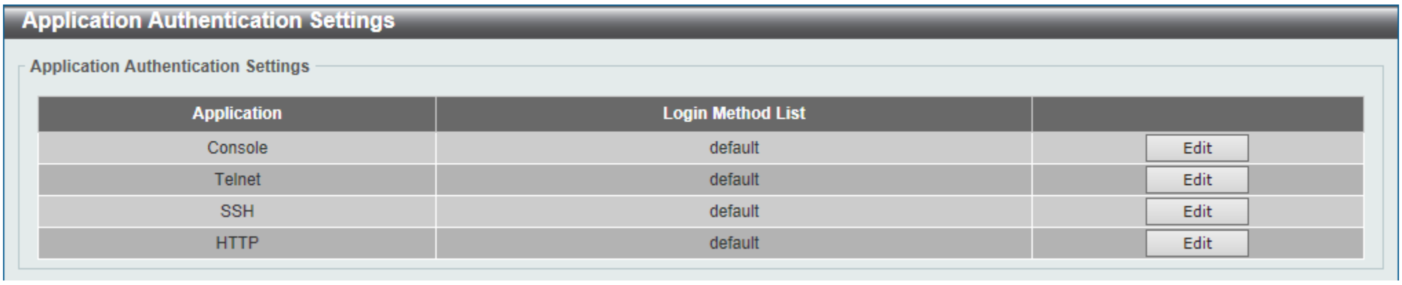
Parameter	Description
AAA State	Select to enable or disable the global Authentication, Authorization, and Accounting (AAA) state. By default, this is disabled.

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

Application Authentication Settings

This window is used to display and configure the application authentication settings.

To view the following window, click **Security > AAA > Application Authentication Settings**, as shown below:



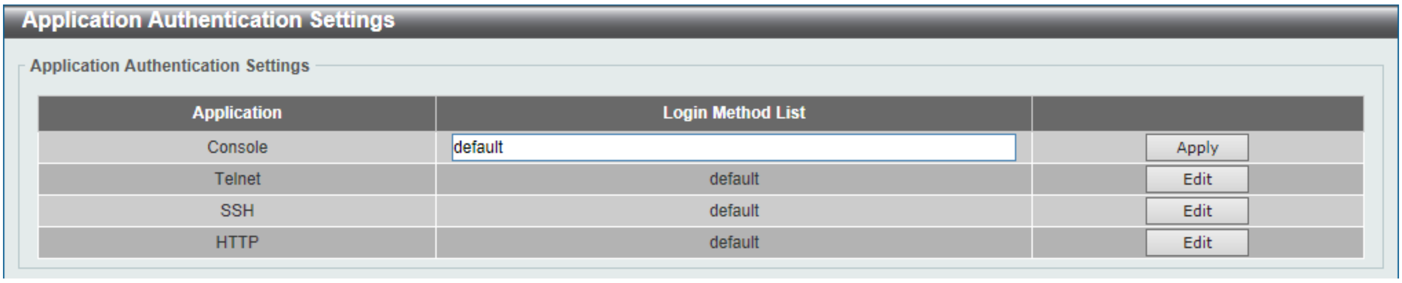
Application Authentication Settings

Application Authentication Settings

Application	Login Method List	
Console	default	Edit
Telnet	default	Edit
SSH	default	Edit
HTTP	default	Edit

Figure 9-19 Application Authentication Settings Window

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



Application Authentication Settings

Application Authentication Settings

Application	Login Method List	
Console	default	Apply
Telnet	default	Edit
SSH	default	Edit
HTTP	default	Edit

Figure 9-20 Application Authentication Settings (Edit) Window

The fields that can be configured are described below:

Parameter	Description
Login Method List	After clicking the **Edit** button for the specific entry, enter the login method list name used here.

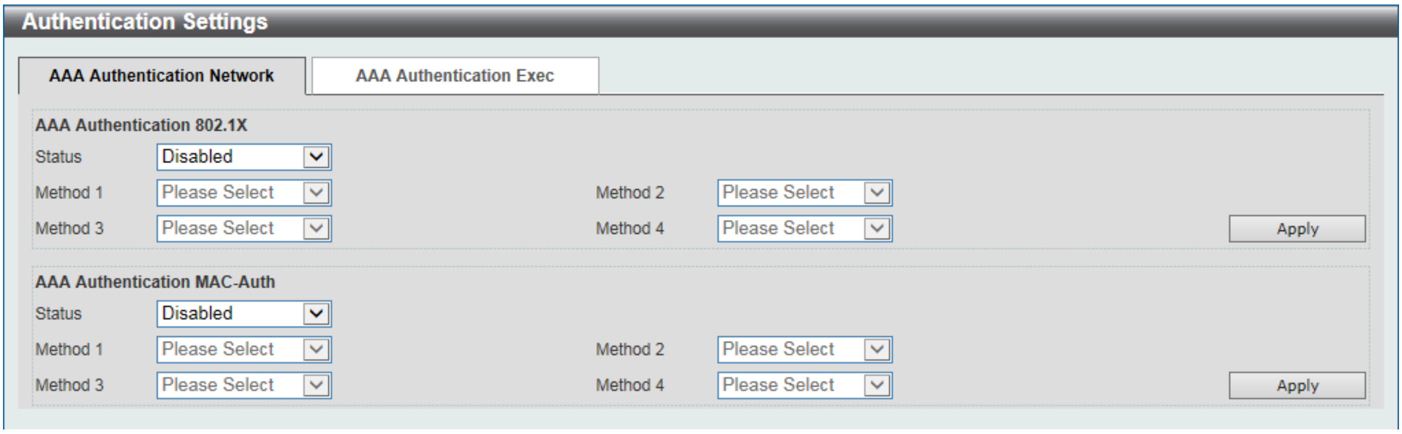
Click the **Edit** button to re-configure the specific entry.

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

Authentication Settings

This window is used to display and configure the AAA network and EXEC authentication settings.

To view the following window, click **Security > AAA > Authentication Settings**, as shown below:



Authentication Settings

AAA Authentication Network | AAA Authentication Exec

AAA Authentication 802.1X

Status: Disabled

Method 1: Please Select | Method 2: Please Select

Method 3: Please Select | Method 4: Please Select

Apply

AAA Authentication MAC-Auth

Status: Disabled

Method 1: Please Select | Method 2: Please Select

Method 3: Please Select | Method 4: Please Select

Apply

Figure 9-21 Authentication Settings Window

The fields that can be configured in **AAA Authentication 802.1X** are described below:

Parameter	Description
Status	Select to enable or disable the AAA 802.1X authentication state here.
Method 1 ~ Method 4	Select the method lists that will be used for this configuration here. Options to choose from are: • **none** - Normally, the method is listed as the last method. The user will pass authentication if it is not denied by previous method authentication. • **local** - Specifies to use the local database for authentication. • **group** - Specifies to use the server groups defined by the AAA group server. Enter the AAA group server name in the space provided. This string can be up to 32 characters long. • **radius** - Specifies to use the servers defined by the RADIUS server host command.

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

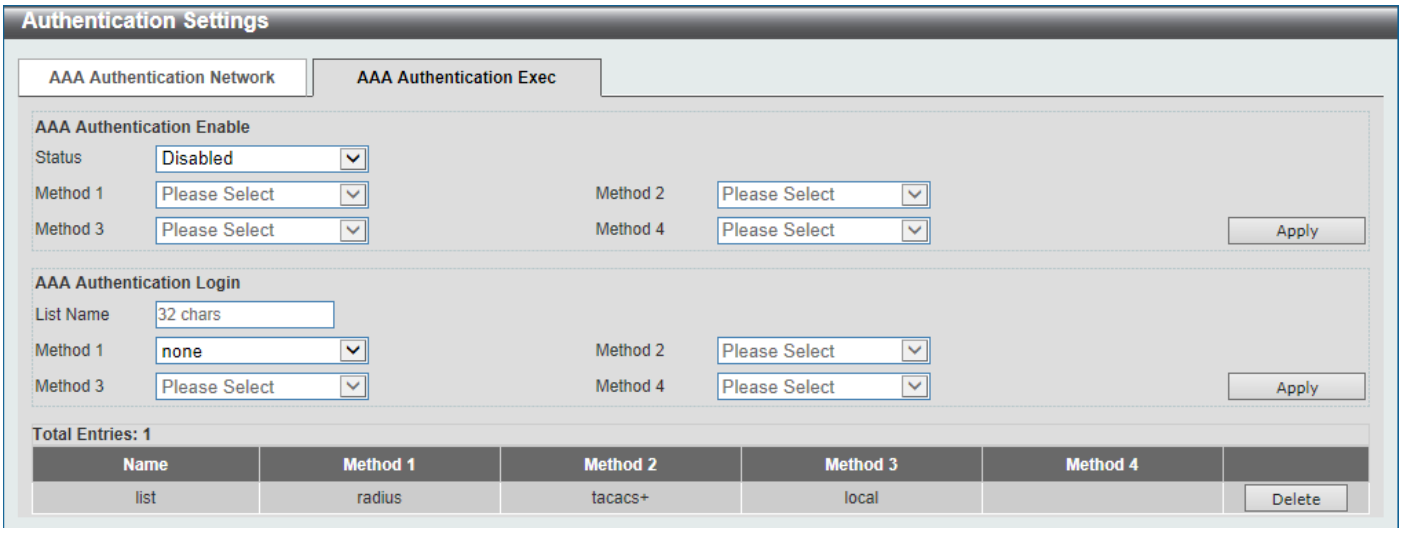
The fields that can be configured in **AAA Authentication MAC-Auth** are described below:

Parameter	Description
Status	Select to enable or disable the AAA MAC authentication state here.
Method 1 ~ Method 4	Select the method lists that will be used for this configuration here. Options to choose from are: • **none** - Normally, the method is listed as the last method. The user will pass authentication if it is not denied by previous method authentication.

Parameter	Description
	• **local** - Specifies to use the local database for authentication. • **group** - Specifies to use the server groups defined by the AAA group server. Enter the AAA group server name in the space provided. This string can be up to 32 characters long. • **radius** - Specifies to use the servers defined by the RADIUS server host command.

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

After clicking the **AAA Authentication Exec** tab, the following page will appear.



Status: Disabled
Method 1: Please Select
Method 2: Please Select
Method 3: Please Select
Method 4: Please Select

List Name: 32 chars
Method 1: none
Method 2: Please Select
Method 3: Please Select
Method 4: Please Select

Total Entries: 1

Name	Method 1	Method 2	Method 3	Method 4	
list	radius	tacacs+	local		Delete

Figure 9-22 Authentication Settings (AAA Authentication EXEC) Window

The fields that can be configured in **AAA Authentication Enable** are described below:

Parameter	Description
Status	Select to enable or disable the AAA authentication enable state here.
Method 1 ~ Method 4	Select the method lists that will be used for this configuration here. Options to choose from are: • **none** - Normally, the method is listed as the last method. The user will pass the authentication if it is not denied by previous method authentication. • **enable** - Specifies to use the local enable password for authentication. • **group** - Specifies to use the server groups defined by the AAA group server command. Enter the AAA group server name in the space provided. This string can be up to 32 characters long. • **radius** - Specifies to use the servers defined by the RADIUS server host command. • **tacacs+** - Specifies to use the servers defined by the TACACS+ server host command.

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

The fields that can be configured in **AAA Authentication Login** are described below:

Parameter	Description
List Name	Enter the method list name that will be used with the AAA authentication login option here.
Method 1 ~ Method 4	Select the method lists that will be used for this configuration here. Options to choose from are:

Parameter	Description
	• **none** - Normally, the method is listed as the last method. The user will pass authentication if it is not denied by previous method's authentication. • **local** - Specifies to use the local database for authentication. • **group** - Specifies to use the server groups defined by the AAA group server command. Enter the AAA group server name in the space provided. This string can be up to 32 characters long. • **radius** - Specifies to use the servers defined by the RADIUS server host command. • **tacacs+** - Specifies to use the servers defined by the TACACS+ server host command.

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

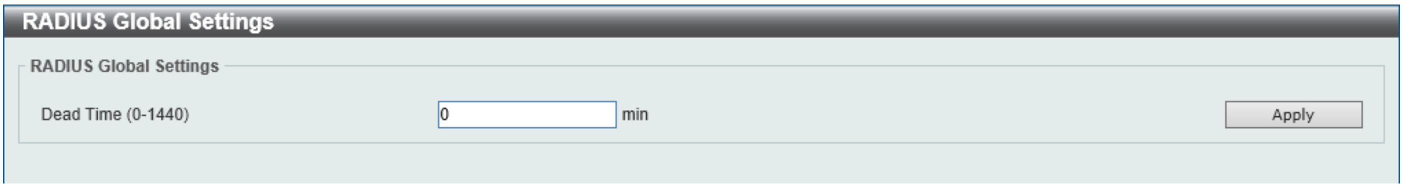
Click the **Delete** button to remove the specified entry.

RADIUS

RADIUS Global Settings

This window is used to display and configure the global RADIUS settings.

To view the following window, click **Security > RADIUS > RADIUS Global Settings**, as shown below:



RADIUS Global Settings

RADIUS Global Settings

Dead Time (0-1440): 0 min

Figure 9-23 RADIUS Global Settings Window

The fields that can be configured in **RADIUS Global Settings** are described below:

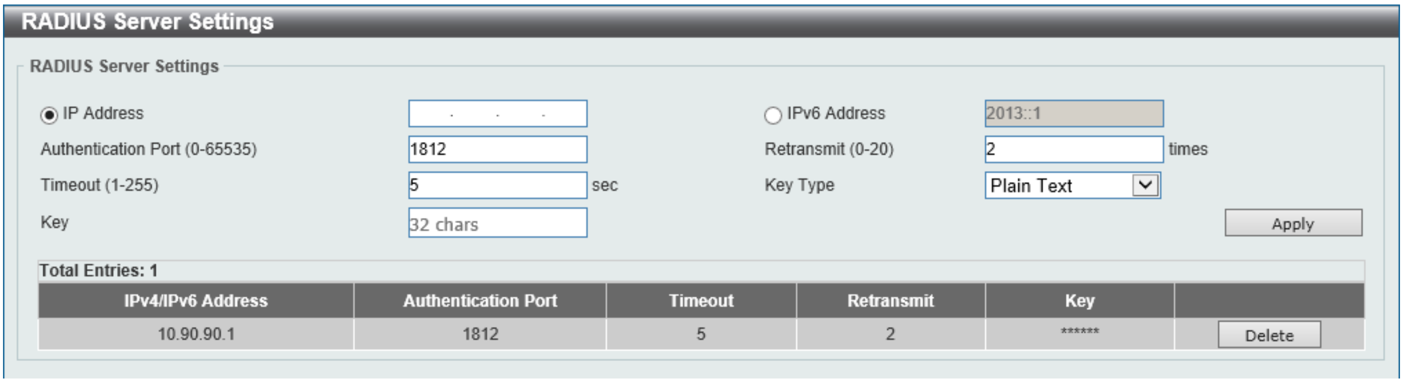
Parameter	Description
Dead Time	Enter the dead time value here. This value must be between 0 and 1440 minutes. By default, this value is 0 minutes. When this option is 0, the unresponsive server will not be marked as dead. This setting can be used to improve the authentication processing time by setting the dead time to skip the unresponsive server host entries. When the system performs authentication with the authentication server, it attempts one server at a time. If the attempted server does not respond, the system will attempt the next server. When the system finds a server does not respond, it will mark the server as down, start a dead time timer, and skip them in authentication of the following requests until expiration of the dead time.

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

RADIUS Server Settings

This window is used to display and configure the RADIUS server settings.

To view the following window, click **Security > RADIUS > RADIUS Server Settings**, as shown below:



RADIUS Server Settings

RADIUS Server Settings

● IP Address: . . .

○ IPv6 Address: 2013::1

Authentication Port (0-65535): 1812

Retransmit (0-20): 2 times

Timeout (1-255): 5 sec

Key Type: Plain Text

Key: 32 chars

Total Entries: 1

IPv4/IPv6 Address	Authentication Port	Timeout	Retransmit	Key	
10.90.90.1	1812	5	2	******	Delete

Figure 9-24 RADIUS Server Settings Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the RADIUS server IPv4 address here.
IPv6 Address	Enter the RADIUS server IPv6 address here.
Authentication Port	Enter the authentication port number used here. This value must be between 0 and 65535. By default, this value is 1812. If no authentication is used, use the value 0.
Retransmit	Enter the retransmit value used here. This value must be between 0 and 20. By default, this value is 2. To disable this option, enter the value 0.
Timeout	Enter the timeout value used here. This value must be between 1 and 255 seconds. By default, this value is 5 seconds.
Key Type	Select the key type that will be used here. Options to choose from are **Plain Text** and **Encrypted**.
Key	Enter the key, used to communicate with the RADIUS server, here. This key can be up to 32 characters long.

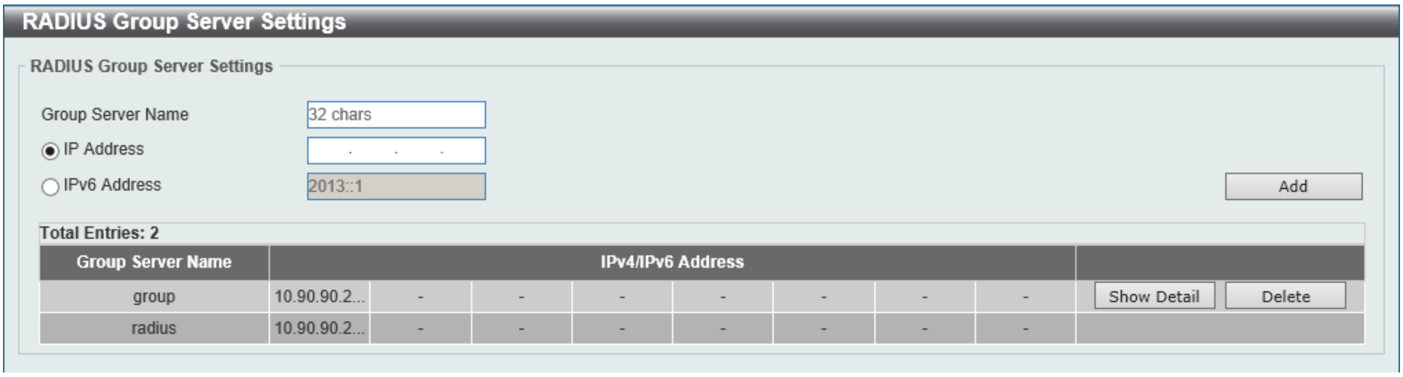
Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

RADIUS Group Server Settings

This window is used to display and configure the RADIUS group server settings.

To view the following window, click **Security > RADIUS > RADIUS Group Server Settings**, as shown below:



RADIUS Group Server Settings

RADIUS Group Server Settings

Group Server Name: 32 chars

● IP Address: . . .

○ IPv6 Address: 2013::1

Total Entries: 2

Group Server Name	IPv4/IPv6 Address								
group	10.90.90.2...	-	-	-	-	-	-	-	Show Detail Delete
radius	10.90.90.2...	-	-	-	-	-	-	-	

Figure 9-25 RADIUS Group Server Settings Window

The fields that can be configured are described below:

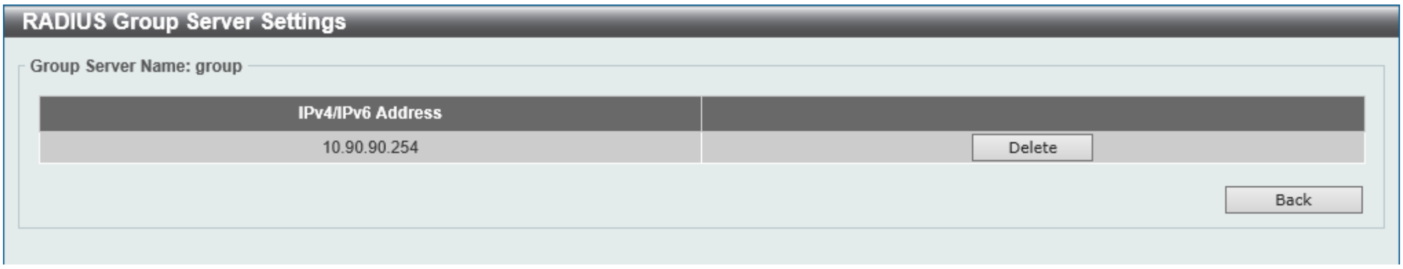
Parameter	Description
Group Server Name	Enter the RADIUS group server name here. This name can be up to 32 characters long.
IP Address	Enter the group server IPv4 address here.
IPv6 Address	Enter the group server IPv6 address here.

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

Click the **Show Detail** button to view and configure detailed settings for the RADIUS group server.

Click the **Delete** button to remove the specified entry.

After clicking the **Show Detail** button, the following page will be available.



RADIUS Group Server Settings

Group Server Name: group

IPv4/IPv6 Address	
10.90.90.254	Delete

Figure 9-26 RADIUS Group Server Settings (Detail) Window

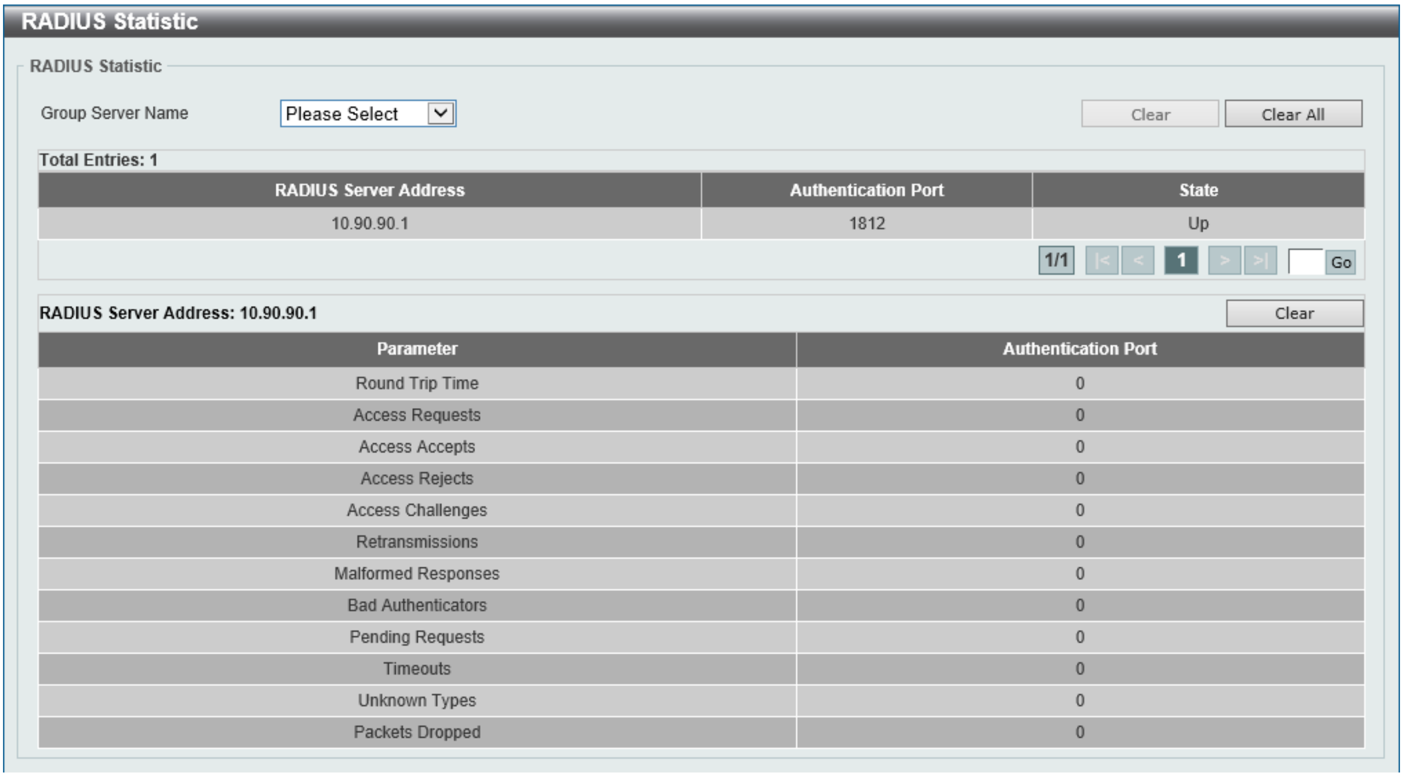
Click the **Delete** button to remove the specified entry.

Click the **Back** button to return to the previous window.

RADIUS Statistic

This window is used to view and clear the RADIUS statistics information.

To view the following window, click **Security > RADIUS > RADIUS Statistic**, as shown below:



Total Entries: 1

RADIUS Server Address	Authentication Port	State
10.90.90.1	1812	Up

RADIUS Server Address: 10.90.90.1

Parameter	Authentication Port
Round Trip Time	0
Access Requests	0
Access Accepts	0
Access Rejects	0
Access Challenges	0
Retransmissions	0
Malformed Responses	0
Bad Authenticators	0
Pending Requests	0
Timeouts	0
Unknown Types	0
Packets Dropped	0

Figure 9-27 RADIUS Statistic Window

The fields that can be configured are described below:

Parameter	Description
Group Server Name	Select the RADIUS group server name from this list here.

Click the **Clear** button to clear the information based on the selections made.

Click the **Clear All** button to clear all the information in this table.

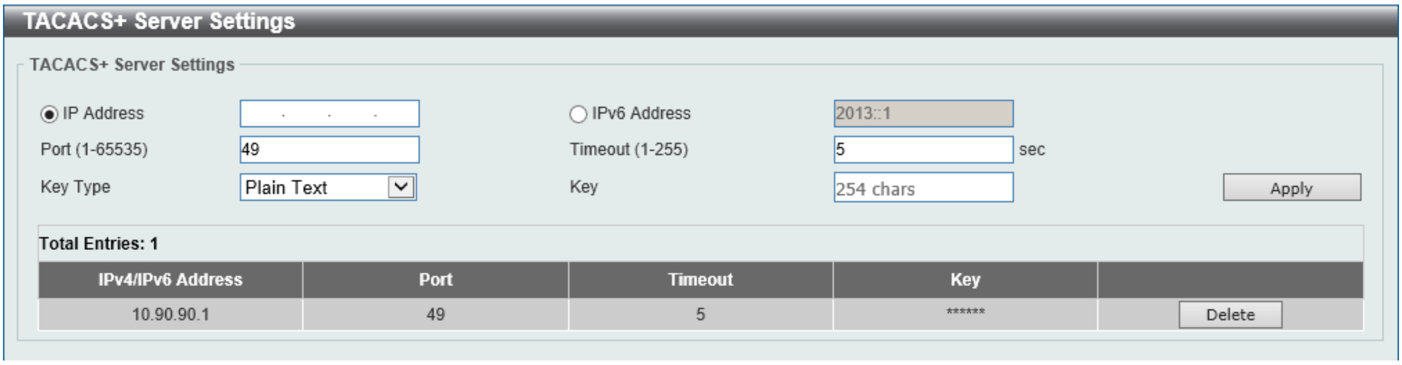
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

TACACS+

TACACS+ Server Settings

This window is used to display and configure the TACACS+ server settings.

To view the following window, click **Security > TACACS+ > TACACS+ Server Settings**, as shown below:



TACACS+ Server Settings

TACACS+ Server Settings

● IP Address . . .

○ IPv6 Address 2013::1

Port (1-65535) 49

Timeout (1-255) 5 sec

Key Type Plain Text

Key 254 chars

Total Entries: 1

IPv4/IPv6 Address	Port	Timeout	Key	
10.90.90.1	49	5	******	Delete

Figure 9-28 TACACS+ Server Settings Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the TACACS+ server IPv4 address here.
IPv6 Address	Enter the TACACS+ server IPv6 address here.
Port	Enter the port number used here. This value must be between 1 and 65535. By default, this value is 49.
Timeout	Enter the timeout value here. This value must be between 1 and 255 seconds. By default, this value is 5 seconds.
Key Type	Select the key type that will be used here. Options to choose from are **Plain Text** and **Encrypted**.
Key	Enter the key, used to communicate with the TACACS+ server, here. This key can be up to 254 characters long.

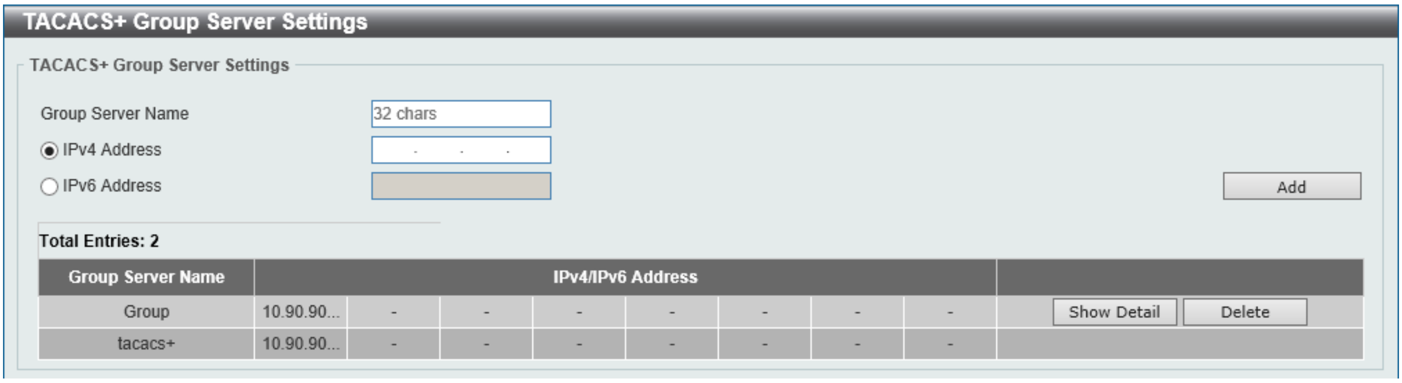
Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

TACACS+ Group Server Settings

This window is used to display and configure the TACACS+ group server settings.

To view the following window, click **Security > TACACS+ > TACACS+ Group Server Settings**, as shown below:



TACACS+ Group Server Settings

TACACS+ Group Server Settings

Group Server Name: 32 chars

● IPv4 Address: . . .

○ IPv6 Address

Total Entries: 2

Group Server Name	IPv4/IPv6 Address								
Group	10.90.90...	-	-	-	-	-	-	-	Show Detail Delete
tacacs+	10.90.90...	-	-	-	-	-	-	-	

Figure 9-29 TACACS+ Group Server Settings Window

The fields that can be configured are described below:

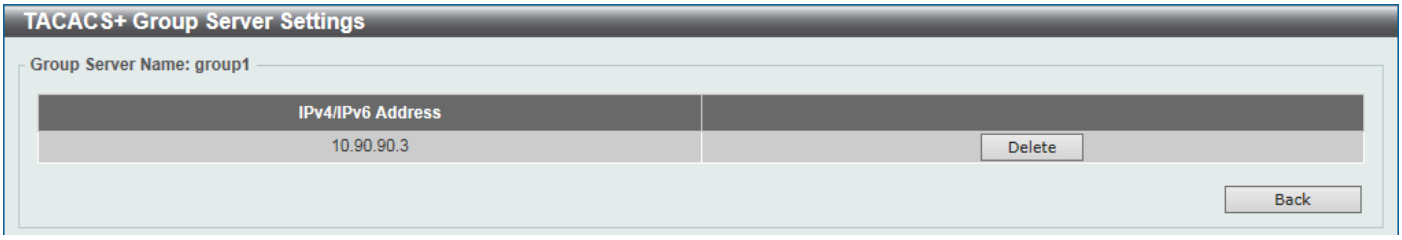
Parameter	Description
Group Server Name	Enter the TACACS+ group server name here. This name can be up to 32 characters long.
IPv4 Address	Enter the IPv4 address of the TACACS+ group server here.
IPv6 Address	Enter the IPv6 address of the TACACS+ group server here.

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

Click the **Show Detail** button to view and configure more detailed settings for the TACACS+ group server.

Click the **Delete** button to remove the specified entry.

After clicking the **Show Detail** button, the following page will be available.



TACACS+ Group Server Settings

Group Server Name: group1

IPv4/IPv6 Address	
10.90.90.3	Delete

Figure 9-30 TACACS+ Group Server Settings (Show Detail) Window

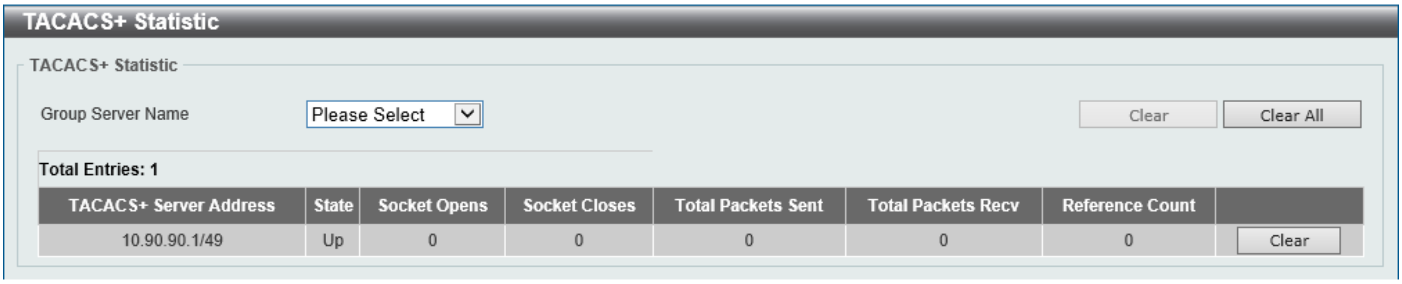
Click the **Delete** button to remove the specified entry.

Click the **Back** button to return to the previous window.

TACACS+ Statistic

This window is used to view and clear the TACACS+ statistic information.

To view the following window, click **Security > TACACS+ > TACACS+ Statistic**, as shown below:



TACACS+ Statistic

TACACS+ Statistic

Group Server Name: Please Select

Total Entries: 1

TACACS+ Server Address	State	Socket Opens	Socket Closes	Total Packets Sent	Total Packets Recv	Reference Count	
10.90.90.1/49	Up	0	0	0	0	0	Clear

Figure 9-31 TACACS+ Statistic Window

The fields that can be configured are described below:

Parameter	Description
Group Server Name	Select the TACACS+ group server name from this list here.

Click the first **Clear** button to clear the information based on the group selected.

Click the **Clear All** button to clear all the information in this table.

Click the second **Clear** button to clear all the information for the specific entry.

IMPB

The IP network layer uses a four-byte address. The Ethernet link-layer uses a six-byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP-MAC-Port Binding (IMPB) is to restrict the access to a Switch to a number of authorized users. Authorized clients can access a Switch’s port by either checking the pair of IP-MAC addresses with the pre-configured database or if DHCP snooping has been enabled in which case the Switch will automatically learn the IP/MAC pairs by snooping DHCP packets and saving them to the IMPB white list. If an unauthorized user tries to access an IP-MAC binding enabled port, the system will block the access by dropping its packet. Active and inactive entries use the same database. The function is port-based, meaning a user can enable or disable the function on the individual port.

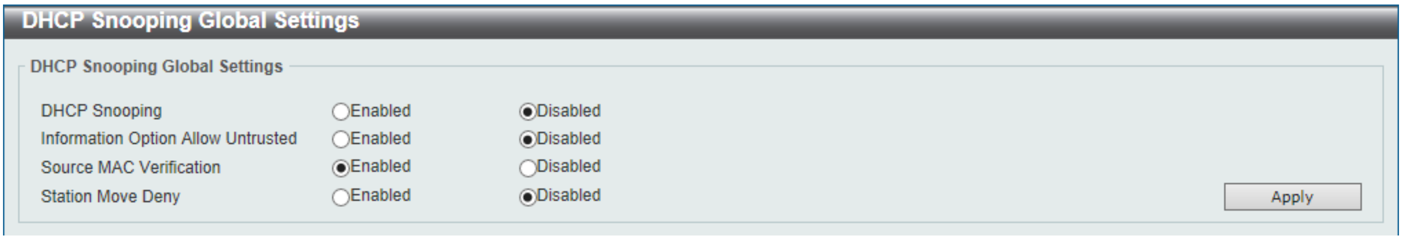
IPv4

DHCPv4 Snooping

DHCP Snooping Global Settings

This window is used to display and configure the global DHCP snooping settings.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Global Settings**, as shown below:



DHCP Snooping Global Settings

DHCP Snooping Global Settings

DHCP Snooping	○Enabled	●Disabled
Information Option Allow Untrusted	○Enabled	●Disabled
Source MAC Verification	●Enabled	○Disabled
Station Move Deny	○Enabled	●Disabled

Figure 9-32 DHCP Snooping Global Settings Window

The fields that can be configured are described below:

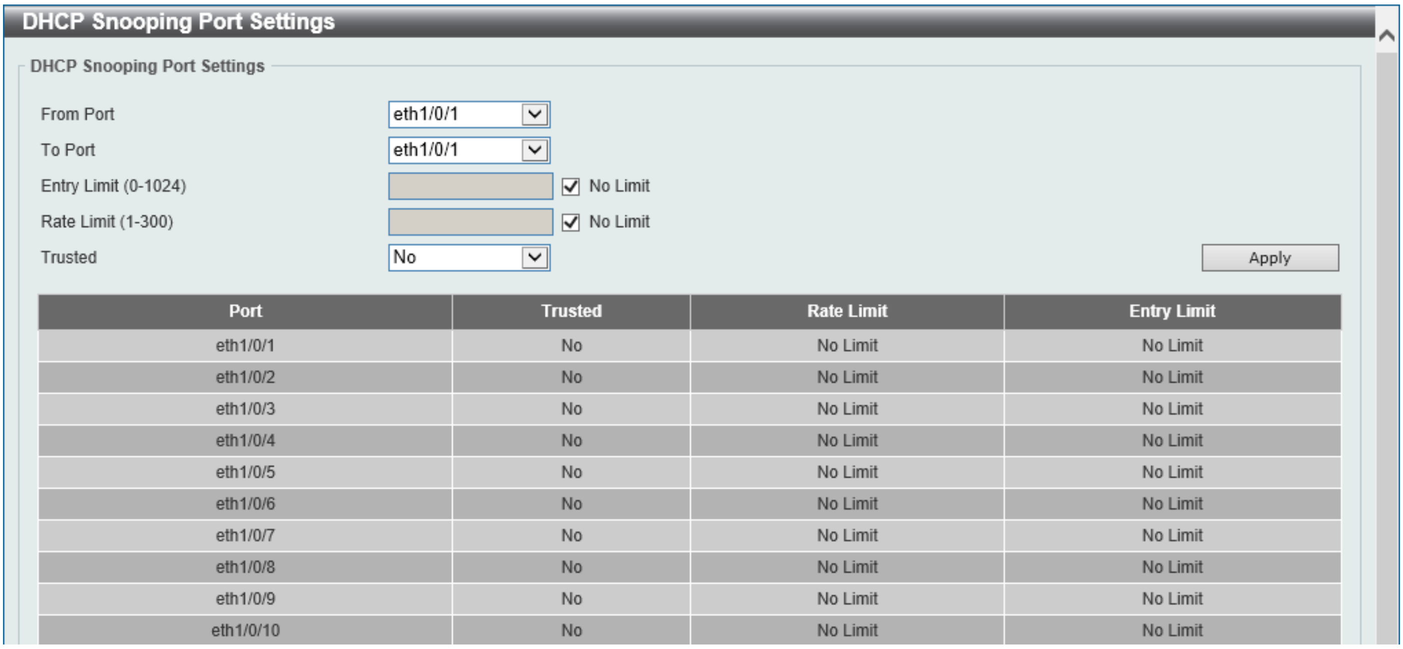
Parameter	Description
DHCP Snooping	Select to enable or disable the global DHCP snooping status.
Information Option Allow Untrusted	Select to enable or disable the option to globally allow DHCP packets with the relay Option 82 on the untrusted interface.
Source MAC Verification	Select to enable or disable the verification that the source MAC address in a DHCP packet matches the client hardware address.
Station Move Deny	Select to enable or disable the DHCP snooping station move state. When DHCP snooping station move is enabled, the dynamic DHCP snooping binding entry with the same VLAN ID and MAC address on the specific port can move to another port if it detects that a new DHCP process belong to the same VLAN ID and MAC address.

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

DHCP Snooping Port Settings

This window is used to display and configure the DHCP snooping port settings.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Port Settings**, as shown below:



DHCP Snooping Port Settings

DHCP Snooping Port Settings

From Port: eth1/0/1

To Port: eth1/0/1

Entry Limit (0-1024): ☑ No Limit

Rate Limit (1-300): ☑ No Limit

Trusted: No

Port	Trusted	Rate Limit	Entry Limit
eth1/0/1	No	No Limit	No Limit
eth1/0/2	No	No Limit	No Limit
eth1/0/3	No	No Limit	No Limit
eth1/0/4	No	No Limit	No Limit
eth1/0/5	No	No Limit	No Limit
eth1/0/6	No	No Limit	No Limit
eth1/0/7	No	No Limit	No Limit
eth1/0/8	No	No Limit	No Limit
eth1/0/9	No	No Limit	No Limit
eth1/0/10	No	No Limit	No Limit

Figure 9-33 DHCP Snooping Port Settings Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Entry Limit	Enter the entry limit value here. This value must be between 0 and 1024. Tick the **No Limit** option to disable the function.
Rate Limit	Enter the rate limit value here. This value must be between 1 and 300. Tick the **No Limit** option to disable the function.
Trusted	Select the trusted option here. Options to choose from are **No** and **Yes**. Ports connected to the DHCP server or to other Switches should be configured as

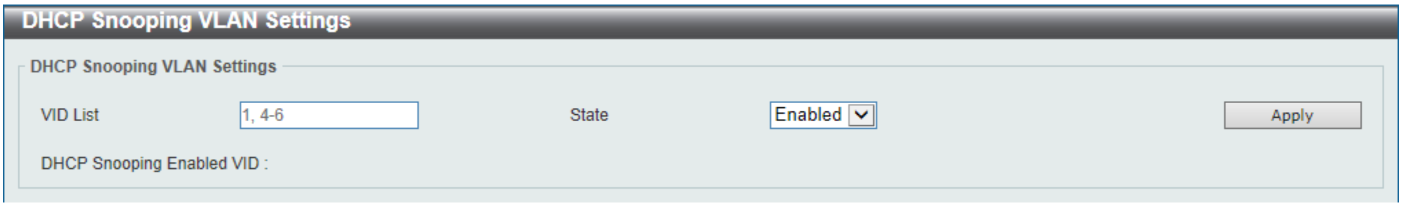
Parameter	Description
	trusted interfaces. The ports connected to DHCP clients should be configured as untrusted interfaces. DHCP snooping acts as a firewall between untrusted interfaces and DHCP servers.

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

DHCP Snooping VLAN Settings

This window is used to display and configure the DHCP snooping VLAN settings.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping VLAN Settings**, as shown below:


DHCP Snooping VLAN Settings

DHCP Snooping VLAN Settings

VID List: 1, 4-6

State: Enabled

DHCP Snooping Enabled VID :

Figure 9-34 DHCP Snooping VLAN Settings Window

The fields that can be configured are described below:

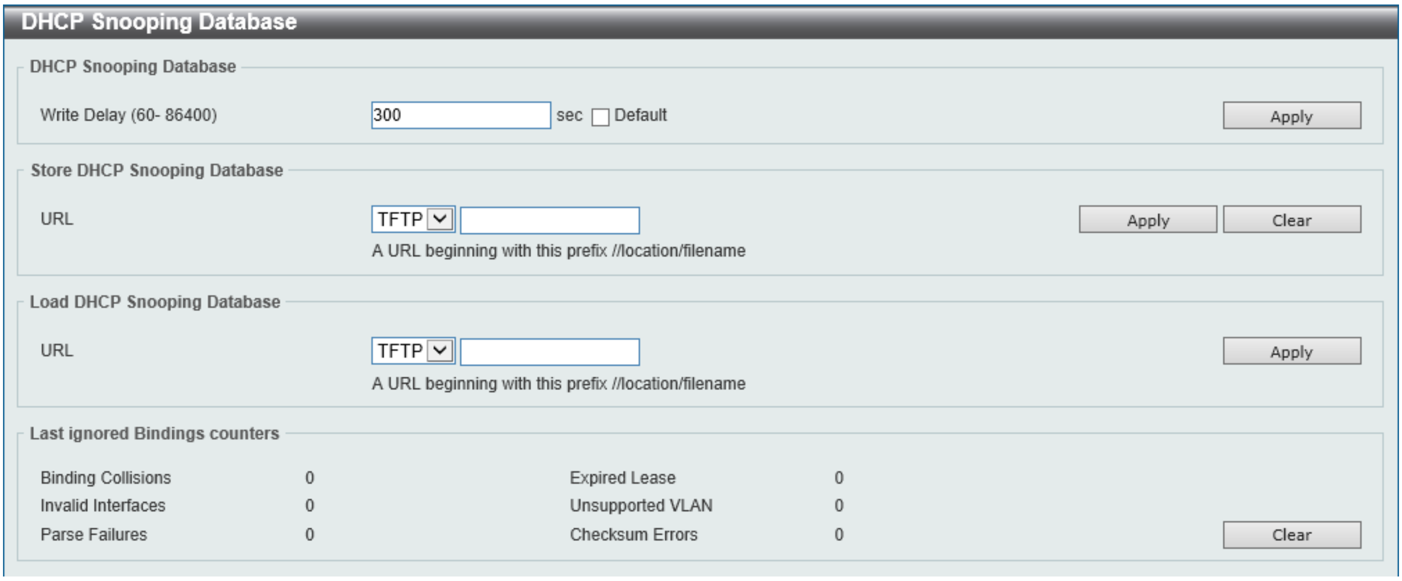
Parameter	Description
VID List	Enter the VLAN ID list used here.
State	Select to enable or disable the DHCP snooping VLAN setting here.

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

DHCP Snooping Database

This window is used to display and configure the DHCP snooping database settings.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Database**, as shown below:


DHCP Snooping Database

DHCP Snooping Database

Write Delay (60- 86400): 300 sec □ Default

Store DHCP Snooping Database

URL: TFTP

A URL beginning with this prefix //location/filename

Load DHCP Snooping Database

URL: TFTP

A URL beginning with this prefix //location/filename

Last ignored Bindings counters

Binding Collisions	0	Expired Lease	0
Invalid Interfaces	0	Unsupported VLAN	0
Parse Failures	0	Checksum Errors	0

Figure 9-35 DHCP Snooping Database Window

The fields that can be configured in **DHCP Snooping Database** are described below:

Parameter	Description
Write Delay	Enter the write delay time value here. This value must be between 60 and 86400 seconds. By default, this value is 300 seconds.

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

The fields that can be configured in **Store DHCP Snooping Database** are described below:

Parameter	Description
URL	Specifies to store the DHCP snooping database on a **TFTP** server. Enter the URL in the space provided.

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

The fields that can be configured in **Load DHCP Snooping Database** are described below:

Parameter	Description
URL	Specifies to load the DHCP snooping database from a **TFTP** server. Enter the URL in the space provided.

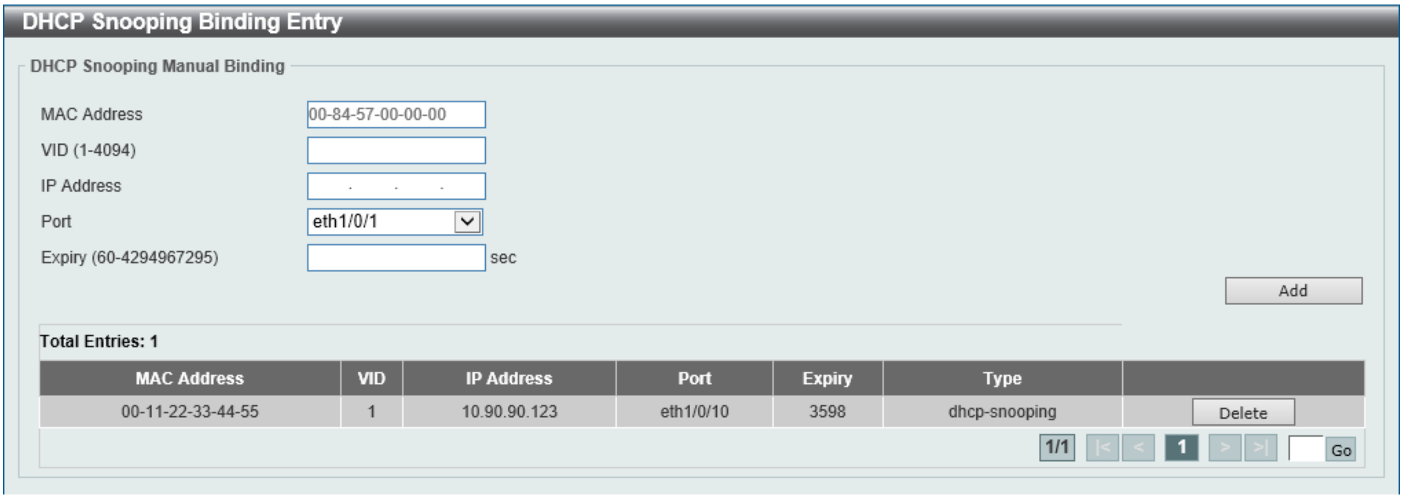
Click the **Apply** button to accept the changes made.

Click the **Clear** button to clear all the counter information.

DHCP Snooping Binding Entry

This window is used to display and configure the DHCP snooping binding entries.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Binding Entry**, as shown below:



DHCP Snooping Binding Entry

DHCP Snooping Manual Binding

MAC Address	00-84-57-00-00-00
VID (1-4094)	
IP Address	. . .
Port	eth1/0/1
Expiry (60-4294967295)	sec

Total Entries: 1

MAC Address	VID	IP Address	Port	Expiry	Type	
00-11-22-33-44-55	1	10.90.90.123	eth1/0/10	3598	dhcp-snooping	Delete

Figure 9-36 DHCP Snooping Binding Entry Window

The fields that can be configured are described below:

Parameter	Description
MAC Address	Enter the MAC address of the DHCP snooping binding entry here.
VID	Enter the VLAN ID of the DHCP snooping binding entry here. This value must be between 1 and 4094.

Parameter	Description
IP Address	Enter the IP address of the DHCP snooping binding entry here.
Port	Select the appropriate port used for the configuration here.
Expiry	Enter the expiry time value used here. This value must be between 60 and 4294967295 seconds.

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

Click the **Delete** button to remove the specified entry.

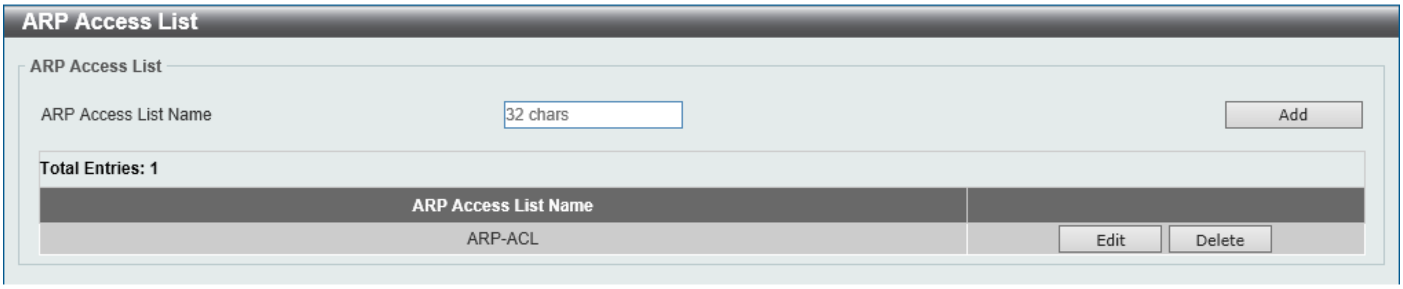
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Dynamic ARP Inspection

ARP Access List

This window is used to display and configure the dynamic ARP inspection settings.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Access List**, as shown below:



ARP Access List

ARP Access List

ARP Access List Name: 32 chars

Add

Total Entries: 1

ARP Access List Name	
ARP-ACL	Edit Delete

Figure 9-37 ARP Access List Window

The fields that can be configured are described below:

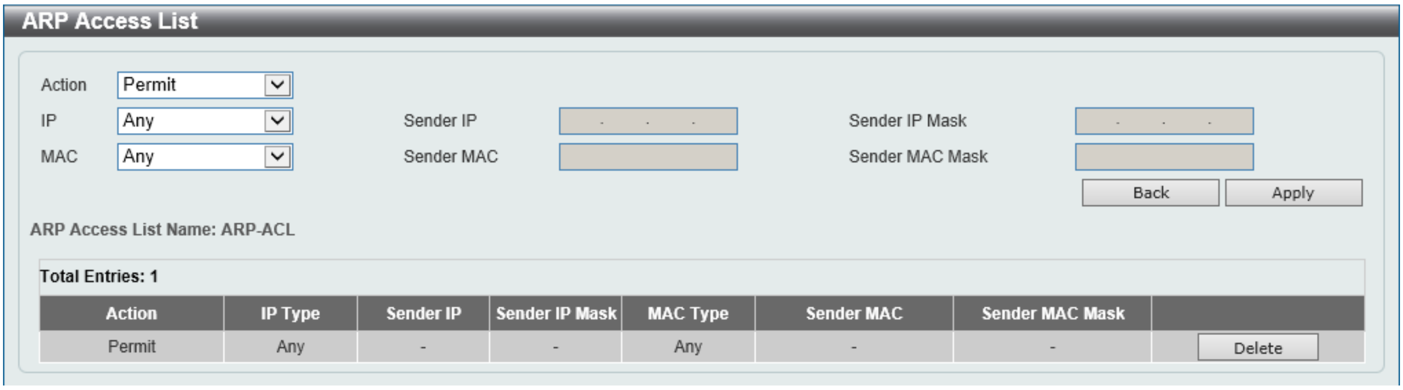
Parameter	Description
ARP Access List Name	Enter the ARP access list name used here. This name can be up to 32 characters long.

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

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

Click the **Delete** button to remove the specified entry.

After clicking the **Edit** button, the following window will appear.



ARP Access List

Action: Permit

IP: Any

Sender IP: . . .

Sender IP Mask: . . .

MAC: Any

Sender MAC:

Sender MAC Mask:

Back Apply

ARP Access List Name: ARP-ACL

Total Entries: 1

Action	IP Type	Sender IP	Sender IP Mask	MAC Type	Sender MAC	Sender MAC Mask	
Permit	Any	-	-	Any	-	-	Delete

Figure 9-38 ARP Access List (Edit) Window

The fields that can be configured are described below:

Parameter	Description
Action	Select the action that will be taken here. Options to choose from are **Permit** and **Deny**.
IP	Select the type of sender IP address that will be used here. Options to choose from are **Any**, **Host**, and **IP with Mask**.
Sender IP	After selecting the **Host** or **IP with Mask** options as the type of **IP**, enter the sender IP address used here.
Sender IP Mask	After selecting the **IP with Mask** option as the type of **IP**, enter the sender IP mask used here.
MAC	Select the type of sender MAC address that will be used here. Options to choose from are **Any**, **Host**, and **MAC with Mask**.
Sender MAC	After selecting the **Host** or **MAC with Mask** options as the type of **MAC**, enter the sender MAC address used here.
Sender MAC Mask	After selecting the **MAC with Mask** option as the type of **MAC**, enter the sender MAC mask used here.

Click the **Back** button to return to the previous page.

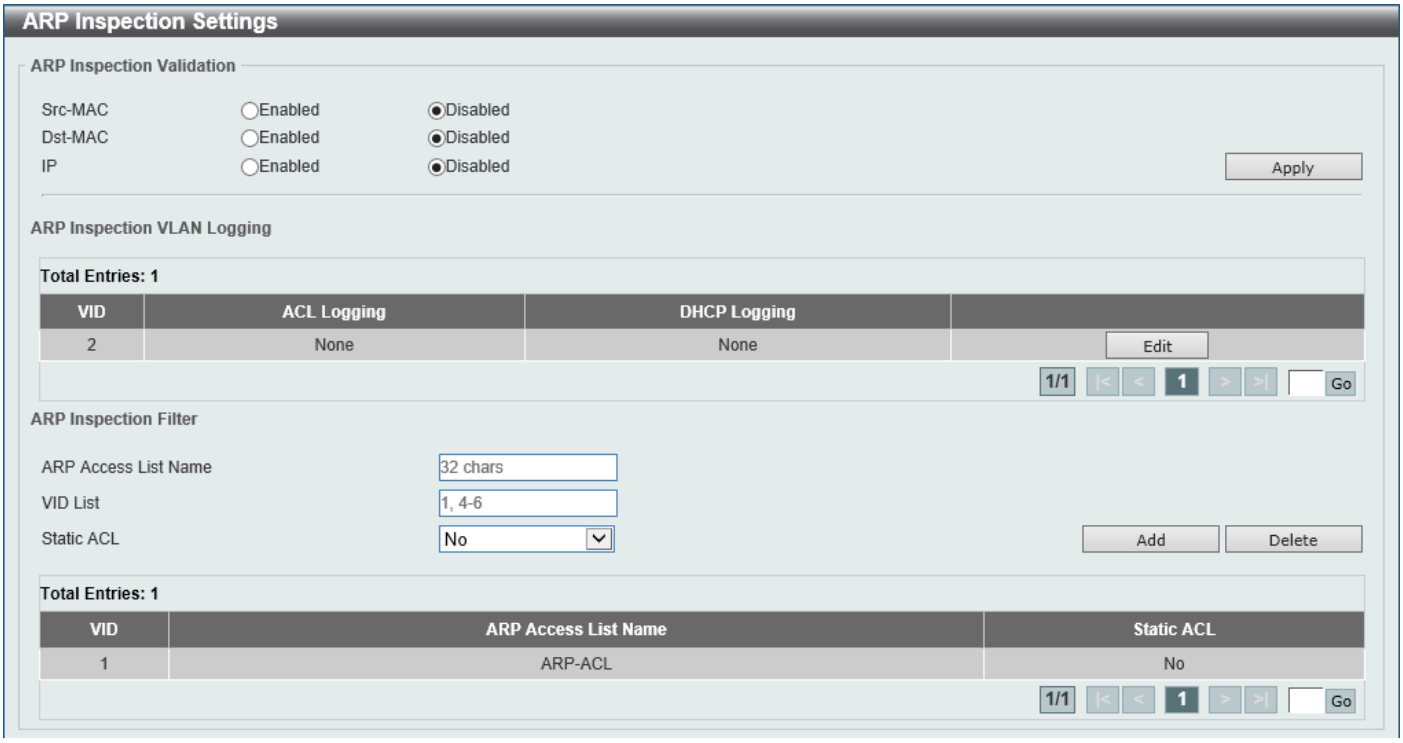
Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

ARP Inspection Settings

This window is used to display and configure the ARP inspection settings.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Settings**, as shown below:



ARP Inspection Settings

ARP Inspection Validation

Src-MAC ○Enabled ●Disabled

Dst-MAC ○Enabled ●Disabled

IP ○Enabled ●Disabled

ARP Inspection VLAN Logging

Total Entries: 1

VID	ACL Logging	DHCP Logging	
2	None	None	Edit

ARP Inspection Filter

ARP Access List Name: 32 chars

VID List: 1, 4-6

Static ACL: No

Total Entries: 1

VID	ARP Access List Name	Static ACL
1	ARP-ACL	No

Figure 9-39 ARP Inspection Settings Window

The fields that can be configured in **ARP Inspection Validation** are described below:

Parameter	Description
Src-MAC	Select to enable or disable the source MAC option here. This option specifies to check for ARP requests and response packets and the consistency of the source MAC address in the Ethernet header against the sender MAC address in the ARP payload.
Dst-MAC	Select to enable or disable the destination MAC option here. This option specifies to check for ARP response packets and the consistency of the destination MAC address in the Ethernet header against the target MAC address in the ARP payload.
IP	Select to enable or disable the IP option here. This option specifies to check the ARP body for invalid and unexpected IP addresses. It also specifies to check the validity of IP address in the ARP payload. The sender IP in both the ARP request and response and target IP in the ARP response are validated. Packets destined for the IP addresses 0.0.0.0, 255.255.255.255, and all IP multicast addresses are dropped. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses.

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

Click the **Edit** button to configure the ARP inspection VLAN logging settings.

After clicking the **Edit** button the following fields can be configured:

Parameter	Description
ACL Logging	Select the ACL logging action here. This specifies the logging criteria for packets that are dropped or permitted based on ACL matches. Options to choose from are: • **Deny** - Specifies logging when denied by the configured ACL. • **Permit** - Specifies logging when permitted by the configured ACL. • **All** - Specifies logging when permitted or denied by the configured ACL. • **None** - Specifies that ACL-matched packets are not logged.
DHCP Logging	Select the DHCP logging action here. This specifies the logging criteria for packets dropped or permitted based on matches against the DHCP bindings. Options to choose from are: • **Deny** - Specifies logging when denied by DHCP bindings. • **Permit** - Specifies logging when permitted by DHCP bindings. • **All** - Specifies logging when permitted or denied by DHCP bindings. • **None** - Specifies to prevent the logging of all packets permitted or denied by DHCP bindings.

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

The fields that can be configured in **ARP Inspection Filter** are described below:

Parameter	Description
ARP Access List Name	Enter the ARP access list name used here. This name can be up to 32 characters long.
VID List	Enter the VLAN ID list used here.
Static ACL	Select whether to use a static ACL or not here by either selecting **Yes** or **No**.

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

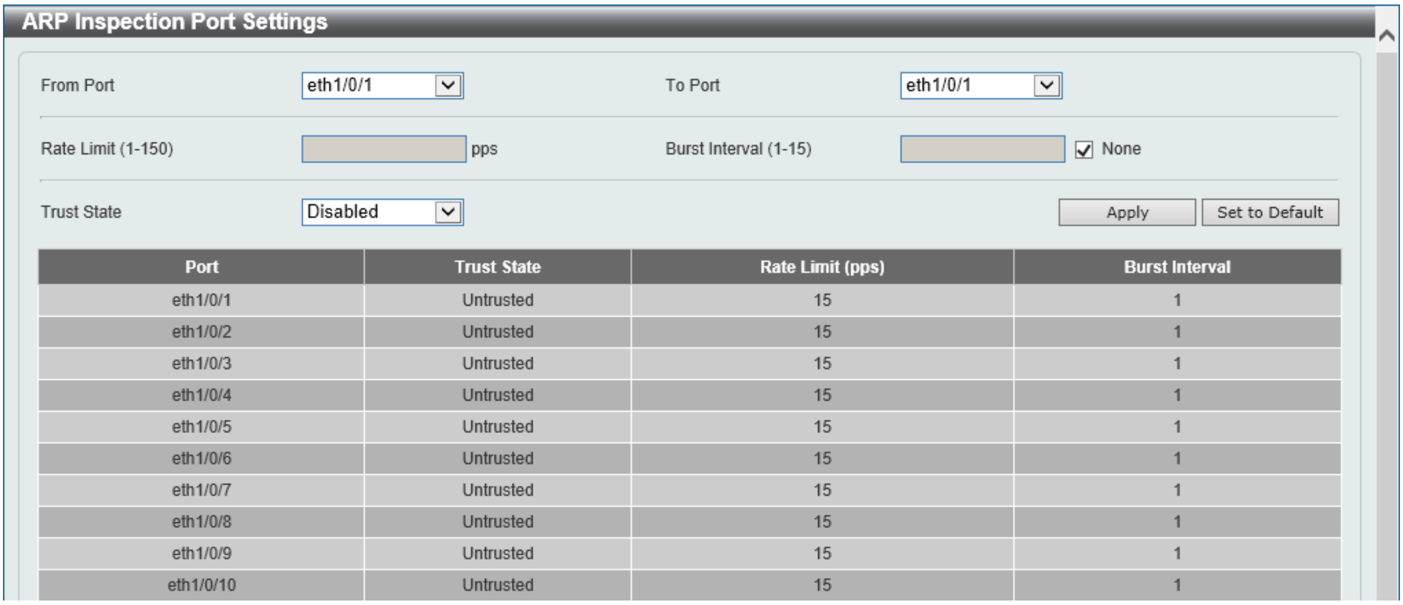
Click the **Delete** button to remove an entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

ARP Inspection Port Settings

This window is used to display and configure the ARP inspection port settings.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Port Settings**, as shown below:



ARP Inspection Port Settings

From Port: eth1/0/1 To Port: eth1/0/1

Rate Limit (1-150): pps Burst Interval (1-15): ☑ None

Trust State: Disabled

Port	Trust State	Rate Limit (pps)	Burst Interval
eth1/0/1	Untrusted	15	1
eth1/0/2	Untrusted	15	1
eth1/0/3	Untrusted	15	1
eth1/0/4	Untrusted	15	1
eth1/0/5	Untrusted	15	1
eth1/0/6	Untrusted	15	1
eth1/0/7	Untrusted	15	1
eth1/0/8	Untrusted	15	1
eth1/0/9	Untrusted	15	1
eth1/0/10	Untrusted	15	1

Figure 9-40 ARP Inspection Port Settings Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Rate Limit	Enter the rate limit value here. This value must be between 1 and 150 packets per seconds.
Burst Interval	Enter the burst interval value here. This value must be between 1 and 15. Tick the **None** option to disable the option.
Trust State	Select to enable or disable the trust state here.

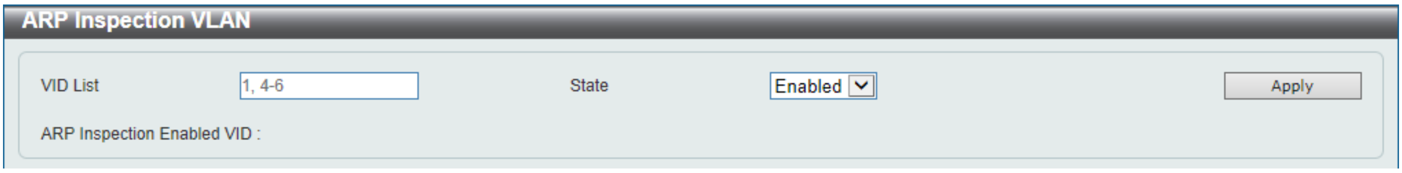
Click the **Apply** button to accept the changes made.

Click the **Set to Default** button to change the information to the default values.

ARP Inspection VLAN

This window is used to display and configure the ARP inspection VLAN settings.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection VLAN**, as shown below:



ARP Inspection VLAN

VID List: 1, 4-6 State: Enabled

ARP Inspection Enabled VID :

Figure 9-41 ARP Inspection VLAN Window

The fields that can be configured are described below:

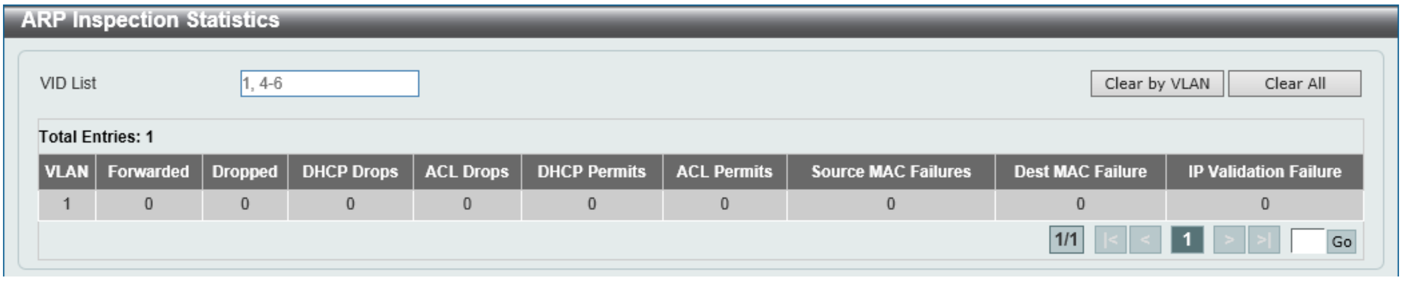
Parameter	Description
VID List	Enter the VLAN ID list used here.
State	Select to enable or disable the ARP inspection option's state for the specified VLAN here.

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

ARP Inspection Statistics

This window is used to view and clear the ARP inspection statistics information.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Statistics**, as shown below:



ARP Inspection Statistics

VID List: 1, 4-6

Total Entries: 1

VLAN	Forwarded	Dropped	DHCP Drops	ACL Drops	DHCP Permits	ACL Permits	Source MAC Failures	Dest MAC Failure	IP Validation Failure
1	0	0	0	0	0	0	0	0	0

Figure 9-42 ARP Inspection Statistics Window

The fields that can be configured are described below:

Parameter	Description
VID List	Enter the VLAN ID list used here.

Click the **Clear by VLAN** button to clear the information based on the VLAN ID(s) entered.

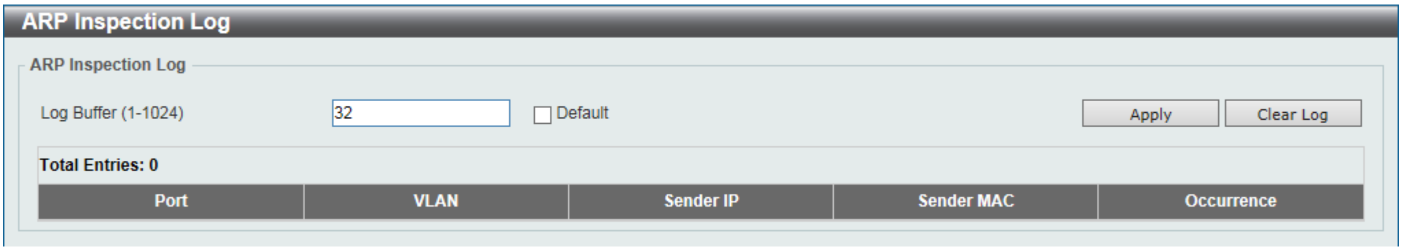
Click the **Clear All** button to clear all the information in this table.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

ARP Inspection Log

This window is used to view, configure, and clear the ARP inspection log information.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Log**, as shown below:



ARP Inspection Log

ARP Inspection Log

Log Buffer (1-1024): 32 □ Default

Total Entries: 0

Port	VLAN	Sender IP	Sender MAC	Occurrence

Figure 9-43 ARP Inspection Log Window

The fields that can be configured are described below:

Parameter	Description
Log Buffer	Enter the log buffer value used here. This value must be between 1 and 1024. By default, this value is 32. Tick the **Default** option to restore value to the default setting.

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

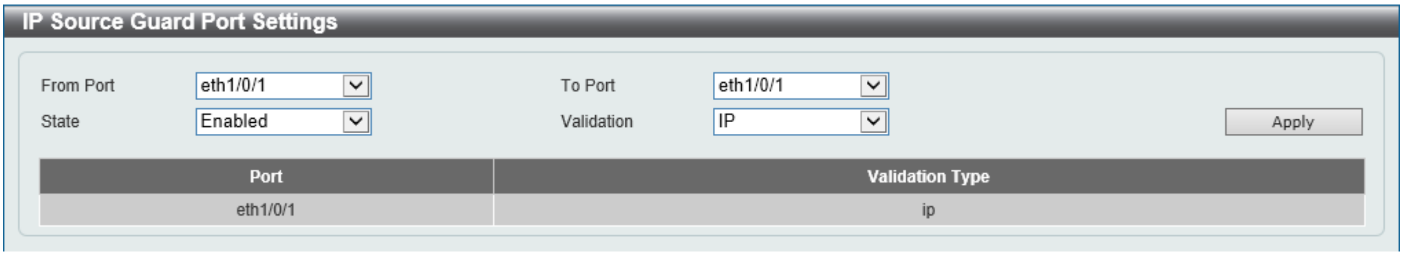
Click the **Clear Log** button to clear the log.

IP Source Guard

IP Source Guard Port Settings

This window is used to display and configure the IP Source Guard (IPSG) port settings.

To view the following window, click **Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Port Settings**, as shown below:



IP Source Guard Port Settings

From Port: eth1/0/1
To Port: eth1/0/1
State: Enabled
Validation: IP

Port	Validation Type
eth1/0/1	ip

Figure 9-44 IP Source Guard Port Settings Window

The fields that can be configured are described below:

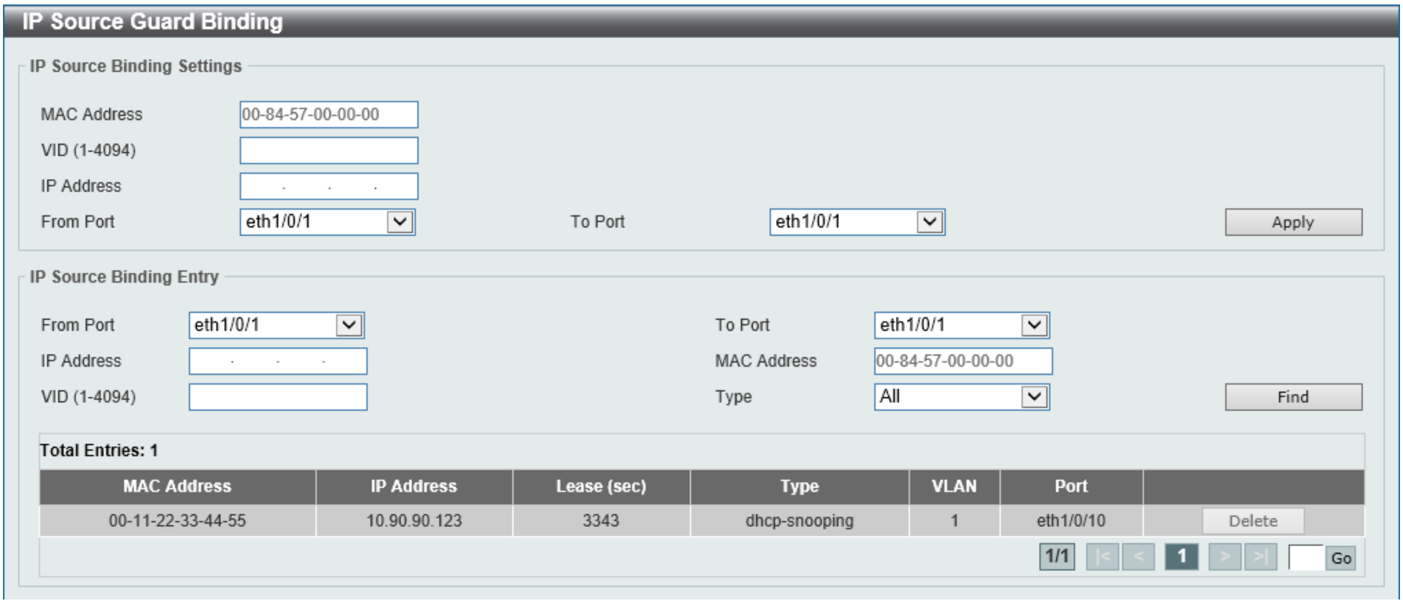
Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the IPSG's state for the specified port(s) here.
Validation	Select the validation method used here. Options to choose from are **IP** and **IP-MAC**. Selecting **IP** means that the IP address of the received packets will be checked. Selecting **IP-MAC** means that the IP address and the MAC address of the received packets will be checked.

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

IP Source Guard Binding

This window is used to display and configure the IPSG binding settings.

To view the following window, click **Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Binding**, as shown below:



Total Entries: 1

MAC Address	IP Address	Lease (sec)	Type	VLAN	Port	
00-11-22-33-44-55	10.90.90.123	3343	dhcp-snooping	1	eth1/0/10	Delete

Figure 9-45 IP Source Guard Binding Window

The fields that can be configured in **IP Source Binding Settings** are described below:

Parameter	Description
MAC Address	Enter the MAC address of the binding entry here.
VID	Enter the VLAN ID of the binding entry here.
IP Address	Enter the IP address of the binding entry here.
From Port - To Port	Select the appropriate port range used for the configuration here.

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

The fields that can be configured in **IP Source Binding Entry** are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the query here.
IP Address	Enter the IP address of the binding entry here.
MAC Address	Enter the MAC address of the binding entry here.
VID	Enter the VLAN ID of the binding entry here.
Type	Select the type of binding entry to find here. Options to choose from are: • **All** - Specifies that all the DHCP binding entries will be displayed. • **DHCP Snooping** - Specifies to display the IP-source guard binding entry learned by DHCP binding snooping. • **Static** - Specifies to display the IP-source guard binding entry that is manually configured.

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

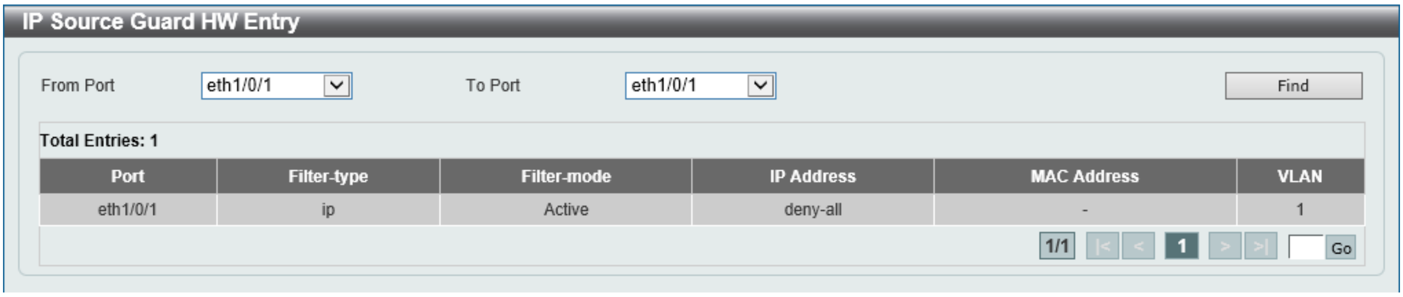
Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IP Source Guard HW Entry

This window is used to view the IPSG hardware entries.

To view the following window, click **Security > IMPB > IPv4 > IP Source Guard > IP Source Guard HW Entry**, as shown below:



IP Source Guard HW Entry

From Port: eth1/0/1 To Port: eth1/0/1

Total Entries: 1

Port	Filter-type	Filter-mode	IP Address	MAC Address	VLAN
eth1/0/1	ip	Active	deny-all	-	1

Figure 9-46 IP Source Guard HW Entry Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the query here.

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

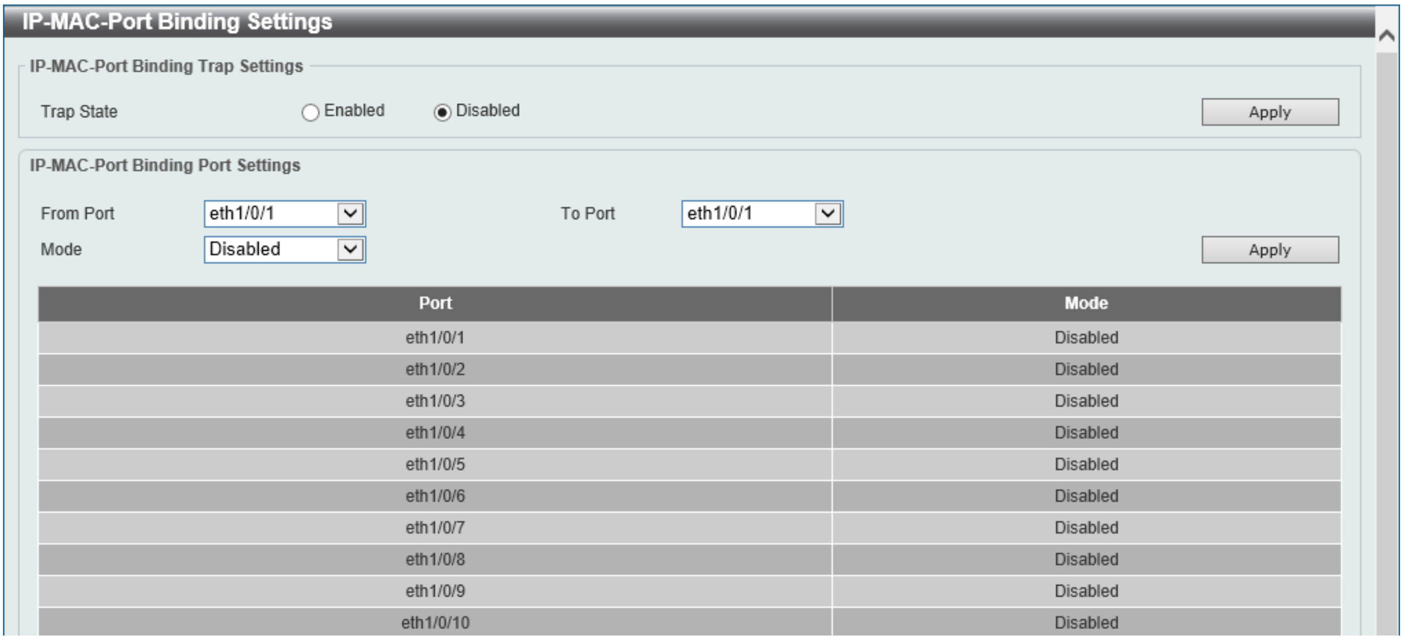
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Advanced Settings

IP-MAC-Port Binding Settings

This window is used to display and configure the IP-MAC-Port binding settings.

To view the following window, click **Security > IMPB > IPv4 > Advanced Settings > IP-MAC-Port Binding Settings**, as shown below:



IP-MAC-Port Binding Settings

IP-MAC-Port Binding Trap Settings

Trap State ○ Enabled ● Disabled

IP-MAC-Port Binding Port Settings

From Port: eth1/0/1 To Port: eth1/0/1

Mode: Disabled

Port	Mode
eth1/0/1	Disabled
eth1/0/2	Disabled
eth1/0/3	Disabled
eth1/0/4	Disabled
eth1/0/5	Disabled
eth1/0/6	Disabled
eth1/0/7	Disabled
eth1/0/8	Disabled
eth1/0/9	Disabled
eth1/0/10	Disabled

Figure 9-47 IP-MAC-Port Binding Settings Window

The fields that can be configured in **IP-MAC-Port Binding Trap Settings** are described below:

Parameter	Description
Trap State	Select the enable or disable the IP-MAC-Port binding option's trap state.

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

The fields that can be configured in **IP-MAC-Port Binding Port Settings** are described below:

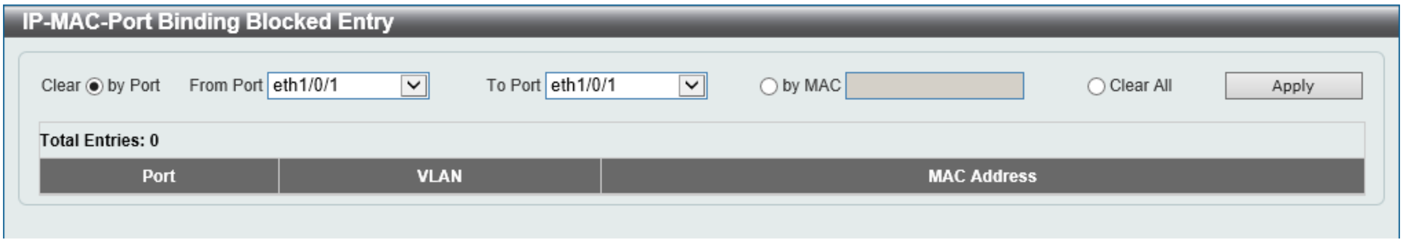
Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Mode	Select the mode of access control that will be used here. Options to choose from are **Disabled**, **Strict**, and **Loose**. When a port is enabled for IMPB strict-mode access control, a host can only access the port after the host sends ARP or IP packets and the ARP packet or IP packet sent by the host passes the binding check. To pass the binding check, the source IP address, source MAC address, VLAN ID, and arrival port number must match any of the entries defined by either the IPSG static binding entry or the DHCP snooping learned dynamic binding entry. When a port is enabled for IMPB loose-mode access control, a host will be denied to access the port after the host sends ARP or IP packets and the ARP packet or IP packet sent by the host does not pass the binding check. To pass the binding check, the source IP address, source MAC address, VLAN ID, and arrival port must match any of the entries defined by either the IPSG static binding entry or the DHCP snooping learned dynamic binding entry.

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

IP-MAC-Port Binding Blocked Entry

This window is used to view and clear the IP-MAC-Port binding blocked entry table.

To view the following window, click **Security > IMPB > IPv4 > Advanced Settings > IP-MAC-Port Binding Blocked Entry**, as shown below:


IP-MAC-Port Binding Blocked Entry

Clear ● by Port   From Port eth1/0/1   To Port eth1/0/1   ○ by MAC   ○ Clear All

Total Entries: 0

Port	VLAN	MAC Address

Figure 9-48 IP-MAC-Port Binding Blocked Entry Window

The fields that can be configured are described below:

Parameter	Description
Clear by Port	Select this option to clear the entry table based on the port(s) selected.
From Port - To Port	Select the appropriate port range that will be cleared here.
Clear by MAC	Select this option to clear the entry table based on the MAC address entered. Enter the MAC address that will be cleared in the space provided.
Clear All	Select this option to clear all entries that contain MAC addresses.

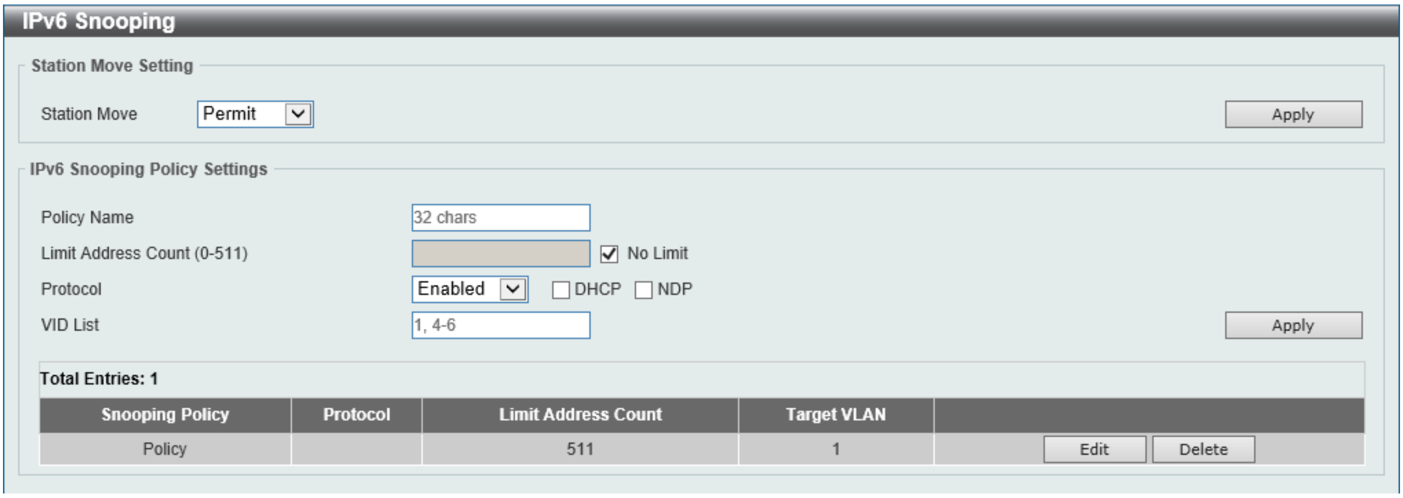
Click the **Apply** button to accept the changes made.

IPv6

IPv6 Snooping

This window is used to display and configure the IPv6 snooping settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 Snooping**, as shown below:



IPv6 Snooping

Station Move Setting

Station Move: Permit

IPv6 Snooping Policy Settings

Policy Name: 32 chars

Limit Address Count (0-511): ☑ No Limit

Protocol: Enabled ☐ DHCP ☐ NDP

VID List: 1, 4-6

Total Entries: 1

Snooping Policy	Protocol	Limit Address Count	Target VLAN	
Policy		511	1	Edit Delete

Figure 9-49 IPv6 Snooping Window

The fields that can be configured in **Station Move Setting** are described below:

Parameter	Description
Station Move	Select the station move options here. Options to choose from are **Permit** and **Deny**.

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

The fields that can be configured in **IPv6 Snooping Policy Settings** are described below:

Parameter	Description
Policy Name	Enter the IPv6 snooping policy name used here. This name can be up to 32 characters long.
Limit Address Count	Enter the address count limit value used here. This value must be between 0 and 511. Tick the **No Limit** option to disable this option.
Protocol	Select the protocol state here. Options to choose from are **Enabled** and **Disabled**. • **DHCP** - Specifies that addresses should be snooped in DHCPv6 packets. • **NDP** - Specifies that addresses should be snooped in NDP packets. DHCPv6 snooping sniffs the DHCPv6 packets sent between the DHCPv6 client and server in the address assigning procedure. When a DHCPv6 client successfully got a valid IPv6 address, DHCPv6 snooping creates its binding database. ND Snooping is designed for a stateless auto-configuration assigned IPv6 address and manually configured IPv6 address. Before assigning an IPv6 address, the host must perform Duplicate Address Detection first. ND snooping detects DAD messages (DAD Neighbor Solicitation (NS) and DAD Neighbor Advertisement (NA)) to build its binding database. The NDP packet (NS and NA) is also used to detect whether a host is still reachable and determine whether to delete a binding or not.
VID List	Enter the VLAN ID list used here.

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

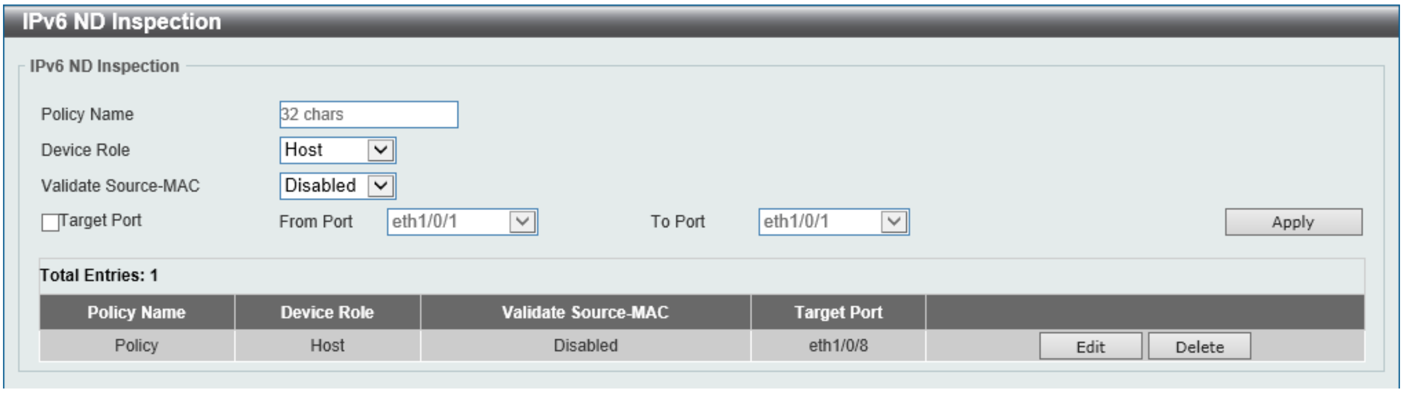
Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

IPv6 ND Inspection

This window is used to display and configure the IPv6 ND inspection settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 ND Inspection**, as shown below:



IPv6 ND Inspection

IPv6 ND Inspection

Policy Name: 32 chars

Device Role: Host

Validate Source-MAC: Disabled

□ Target Port   From Port: eth1/0/1   To Port: eth1/0/1

Total Entries: 1

Policy Name	Device Role	Validate Source-MAC	Target Port	
Policy	Host	Disabled	eth1/0/8	Edit Delete

Figure 9-50 IPv6 ND Inspection Window

The fields that can be configured are described below:

Parameter	Description
Policy Name	Enter the policy name used here. This name can be up to 32 characters long.
Device Role	Select the device role here. Options to choose from are **Host** and **Router**. By default, the device's role is set as host and inspection for NS and NA messages are performed. If the device role is set as router, the NS and NA inspection is not performed. When performing NS/NA inspection, the message will be verified against the dynamic binding table learned from the ND protocol or from the DHCP.
Validate Source-MAC	Select to enable or disable the validation of the source MAC address option here. When the Switch receives an ND message that contains a link-layer address, the source MAC address is checked against the link-layer address. The packet will be dropped if the link-layer address and the MAC addresses are different from each other.
Target Port	Tick this option to specify the target port.
From Port - To Port	Select the appropriate port range used for the configuration here.

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

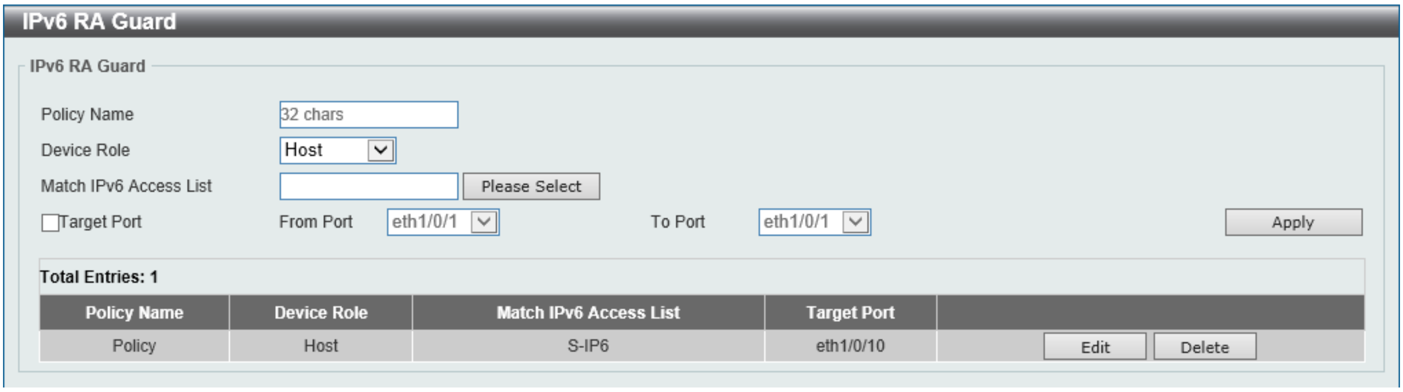
Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

IPv6 RA Guard

This window is used to display and configure the IPv6 Router Advertisement (RA) guard settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 RA Guard**, as shown below:



IPv6 RA Guard

IPv6 RA Guard

Policy Name: 32 chars

Device Role: Host

Match IPv6 Access List: [Please Select]

□ Target Port From Port: eth1/0/1 To Port: eth1/0/1 [Apply]

Total Entries: 1

Policy Name	Device Role	Match IPv6 Access List	Target Port	
Policy	Host	S-IP6	eth1/0/10	Edit Delete

Figure 9-51 IPv6 RA Guard Window

The fields that can be configured are described below:

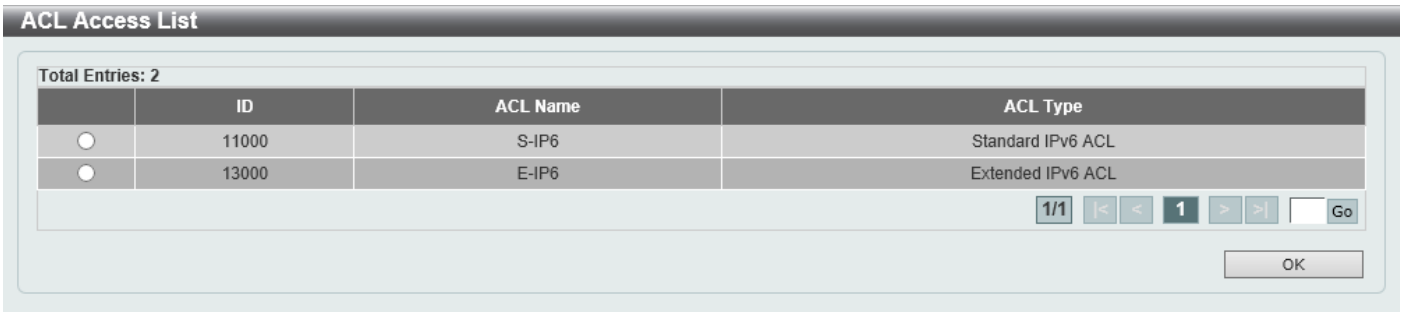
Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Device Role	Select the device role here. Options to choose from are **Host** and **Router**. By default, the device's role is **Host**, which will block all the RA packets. If the device's role is **Router**, RA packets will be forwarded according to the port's bound ACL.
Match IPv6 Access List	Enter or select the IPv6 access list to match here. Click the **Please Select** button to select an existing ACL from the list.
Target Port	Tick this option to specify the target port.
From Port - To Port	Select the appropriate port range used for the configuration here.

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

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

Click the **Delete** button to remove the specified entry.

After clicking the **Please Select** button, the following window will appear:



ACL Access List

Total Entries: 2

	ID	ACL Name	ACL Type
○	11000	S-IP6	Standard IPv6 ACL
○	13000	E-IP6	Extended IPv6 ACL

Figure 9-52 ACL Access List Window

Select the radio button next to the entry to use that ACL in the configuration.

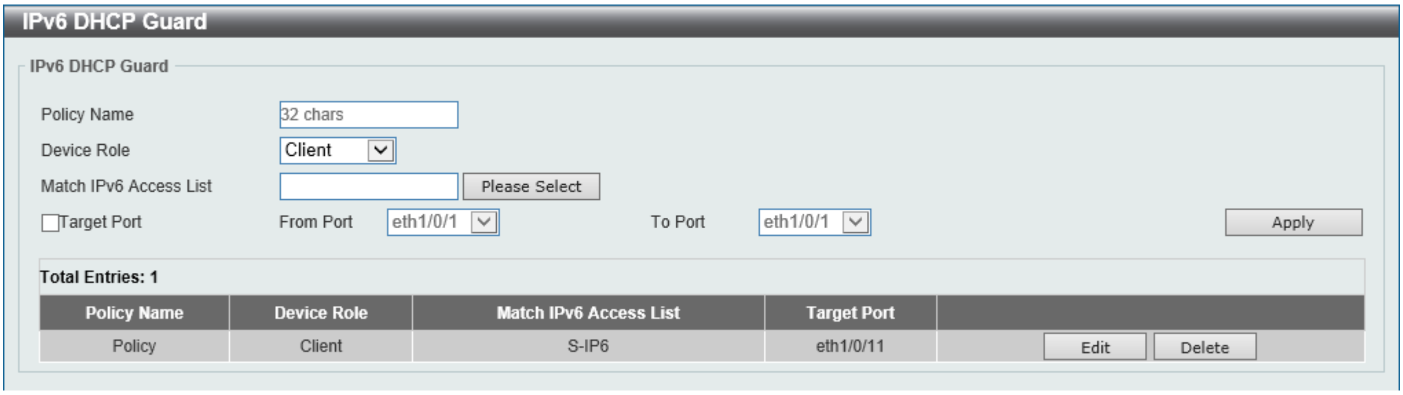
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **OK** button to accept the selection made.

IPv6 DHCP Guard

This window is used to display and configure the IPv6 DHCP guard settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 DHCP Guard**, as shown below:



IPv6 DHCP Guard

IPv6 DHCP Guard

Policy Name: 32 chars

Device Role: Client

Match IPv6 Access List: [Please Select]

□ Target Port   From Port: eth1/0/1   To Port: eth1/0/1   [Apply]

Total Entries: 1

Policy Name	Device Role	Match IPv6 Access List	Target Port	
Policy	Client	S-IP6	eth1/0/11	Edit Delete

Figure 9-53 IPv6 DHCP Guard Window

The fields that can be configured are described below:

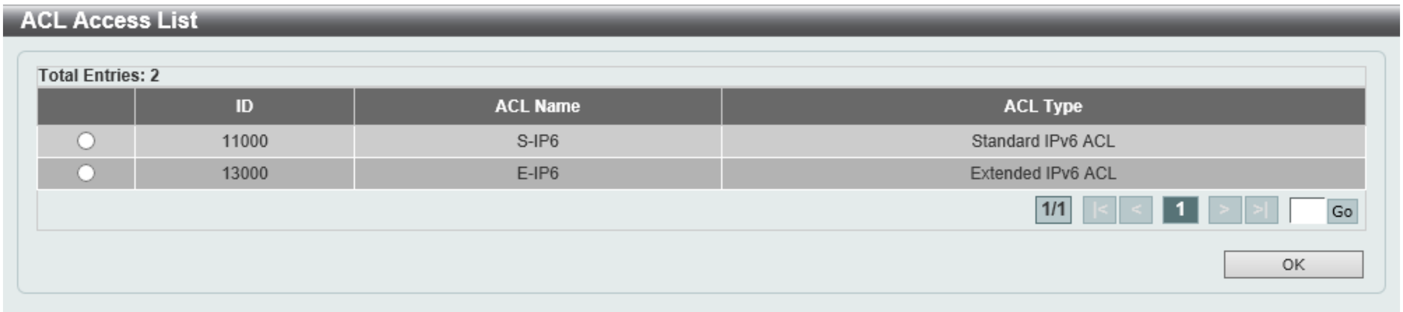
Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Device Role	Select the device role here. Options to choose from are **Client** and **Server**. By default, the device's role is set as **Client**, which will block all the DHCPv6 packets from the DHCPv6 Server. If the device's role is set as **Server**, DHCPv6 Server packets will be forwarded according to the port's bound ACL.
Match IPv6 Access List	Enter or select the IPv6 access list to match here. Click the **Please Select** button to select an existing ACL from the list.
Target Port	Tick this option to specify the target port.
From Port - To Port	Select the appropriate port range used for the configuration here.

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

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

Click the **Delete** button to remove the specified entry.

After clicking the **Please Select** button, the following window will appear:



ACL Access List

Total Entries: 2

	ID	ACL Name	ACL Type
○	11000	S-IP6	Standard IPv6 ACL
○	13000	E-IP6	Extended IPv6 ACL

Figure 9-54 ACL Access List Window

Select the radio button next to the entry to use that ACL in the configuration.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

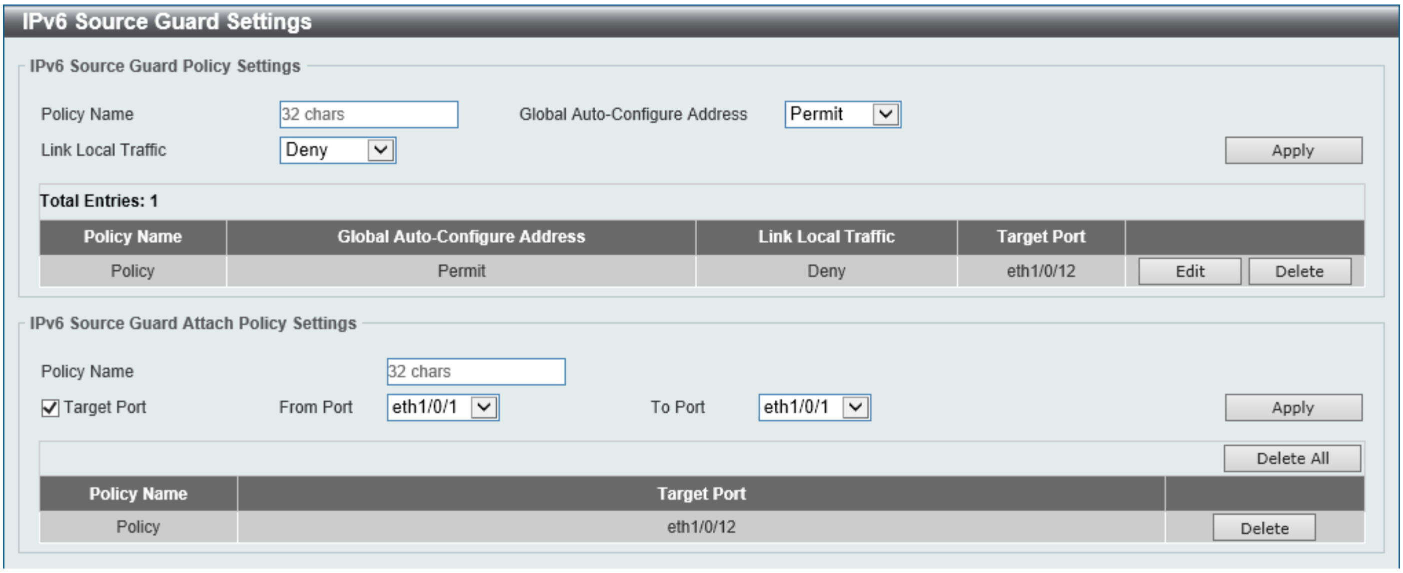
Click the **OK** button to accept the selection made.

IPv6 Source Guard

IPv6 Source Guard Settings

This window is used to display and configure the IPv6 source guard settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 Source Guard > IPv6 Source Guard Settings**, as shown below:



IPv6 Source Guard Settings

IPv6 Source Guard Policy Settings

Policy Name: 32 chars
Global Auto-Configure Address: Permit
Link Local Traffic: Deny

Total Entries: 1

Policy Name	Global Auto-Configure Address	Link Local Traffic	Target Port	
Policy	Permit	Deny	eth1/0/12	Edit Delete

IPv6 Source Guard Attach Policy Settings

Policy Name: 32 chars
☑ Target Port From Port: eth1/0/1 To Port: eth1/0/1

Policy Name	Target Port	
Policy	eth1/0/12	Delete

Figure 9-55 IPv6 Source Guard Settings Window

The fields that can be configured in **IPv6 Source Guard Policy Settings** are described below:

Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Global Auto-Configure Address	Select to **Permit** of **Deny** data traffic from the auto-configured global address. It is useful when all global addresses on a link are assigned by DHCP and the administrator that wants to block hosts with self-configured addresses from sending traffic. By default, **Permit** is used.
Link Local Traffic	Select to **Permit** of **Deny** hardware permitted data traffic send by the link-local address. By default, **Deny** is used.

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

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

Click the **Delete** button to remove the specified entry.

The fields that can be configured in **IPv6 Source Guard Attach Policy Settings** are described below:

Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Target Port	Select this option to specify the target port.
From Port - To Port	Select the appropriate port range used for the configuration here.

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

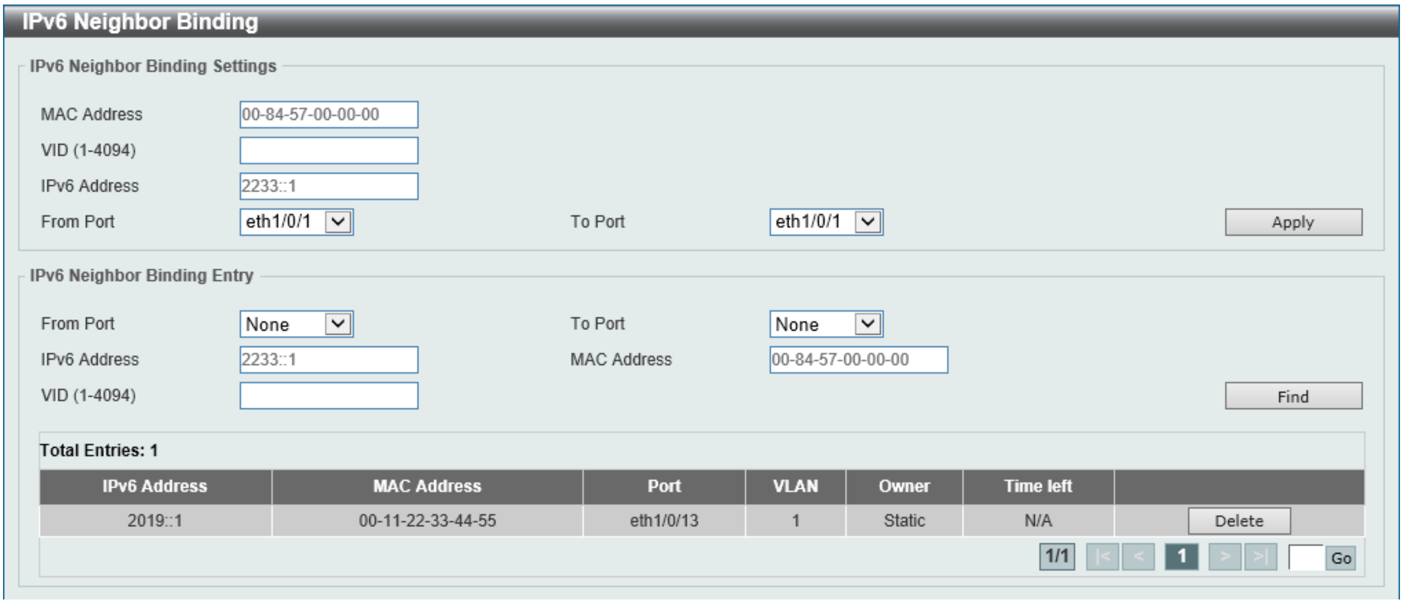
Click the **Delete All** button to remove all the entries.

Click the **Delete** button to remove the specified entry.

IPv6 Neighbor Binding

This window is used to display and configure the IPv6 neighbor binding settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 Source Guard > IPv6 Neighbor Binding**, as shown below:



IPv6 Neighbor Binding Settings

MAC Address: 00-84-57-00-00-00
VID (1-4094):
IPv6 Address: 2233::1
From Port: eth1/0/1
To Port: eth1/0/1

IPv6 Neighbor Binding Entry

From Port: None
To Port: None
IPv6 Address: 2233::1
MAC Address: 00-84-57-00-00-00
VID (1-4094):

Total Entries: 1

IPv6 Address	MAC Address	Port	VLAN	Owner	Time left	
2019::1	00-11-22-33-44-55	eth1/0/13	1	Static	N/A	Delete

Figure 9-56 IPv6 Neighbor Binding Window

The fields that can be configured in **IPv6 Neighbor Binding Settings** are described below:

Parameter	Description
MAC Address	Enter the MAC address used here.
VID	Enter the VLAN ID used here. This value must be between 1 and 4094.
IPv6 Address	Enter the IPv6 address used here.
From Port - To Port	Select the appropriate port range used for the configuration here.

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

The fields that can be configured in **IPv6 Neighbor Binding Entry** are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the search here.
IPv6 Address	Enter the IPv6 address to find here.
MAC Address	Enter the MAC address to find here.
VID	Enter the VLAN ID to find here.

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

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

DHCP Server Screening

This function allows users to not only to restrict all DHCP server packets but also to receive any specified DHCP server packet by any specified DHCP client. It is useful when one or more DHCP servers are present on the network and both provide DHCP services to different distinct groups of clients.

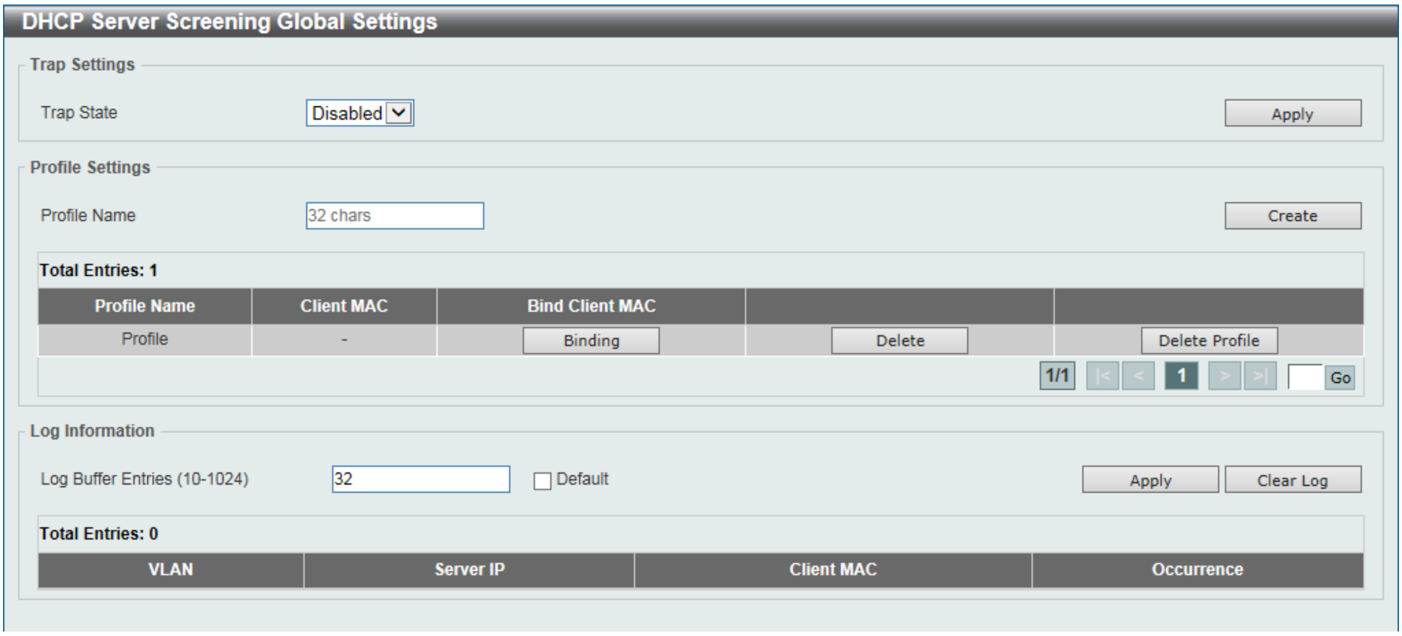
When the DHCP Server Screening function is enabled on a port, all DHCP server packets received on this ports will be redirected to the CPU for a software-based check. Legal DHCP server packets will be forwarded out and illegal DHCP server packets will be dropped.

When DHCP Server Screening function is enabled, all DHCP Server packets will be filtered from a specific port.

DHCP Server Screening Global Settings

This window is used to display and configure the global DHCP server screening settings.

To view the following window, click **Security > DHCP Server Screening > DHCP Server Screening Global Settings**, as shown below:



DHCP Server Screening Global Settings

Trap Settings

Trap State: Disabled

Profile Settings

Profile Name: 32 chars

Total Entries: 1

Profile Name	Client MAC	Bind Client MAC		
Profile	-	Binding	Delete	Delete Profile

Log Information

Log Buffer Entries (10-1024): 32 □ Default

Total Entries: 0

VLAN	Server IP	Client MAC	Occurrence

Figure 9-57 DHCP Server Screening Global Settings Window

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

Parameter	Description
Trap State	Select to enable or disable the DHCP server screening trap here.

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

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

Parameter	Description
Profile Name	Enter the DHCP server screening profile name here. This name can be up to 32 characters long.

Click the **Create** button to create a new profile.

Click the **Binding** button to configure the client MAC address in the profile.

Click the **Delete** button to remove the specified entry.

Click the **Delete Profile** button to remove the specified profile.

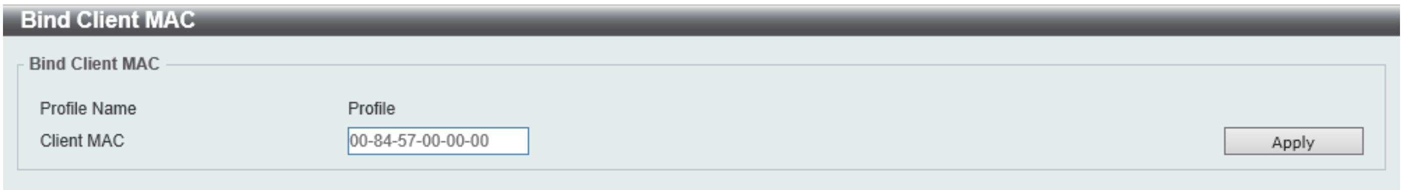
The fields that can be configured in **Log Information** are described below:

Parameter	Description
Log Buffer Entries	Enter the logged buffer entries value here. This value must be between 10 and 1024. By default, this value is 32.

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

Click the **Clear Log** button to clear the log.

After clicking the **Binding** button, the following window will appear:



Bind Client MAC

Bind Client MAC

Profile Name: Profile

Client MAC: 00-84-57-00-00-00

Figure 9-58 Bind Client MAC Window

The fields that can be configured are described below:

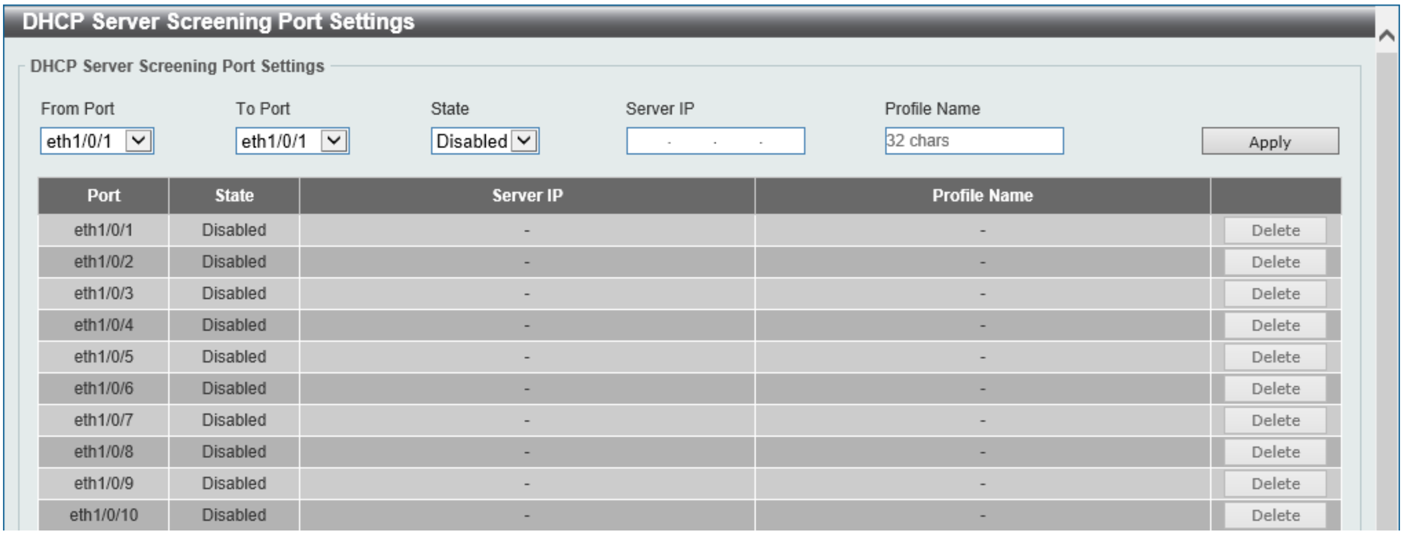
Parameter	Description
Client MAC	Enter the MAC address used here.

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

DHCP Server Screening Port Settings

This window is used to display and configure the DHCP server screening port settings.

To view the following window, click **Security > DHCP Server Screening > DHCP Server Screening Port Settings**, as shown below:



DHCP Server Screening Port Settings

DHCP Server Screening Port Settings

From Port: eth1/0/1 | To Port: eth1/0/1 | State: Disabled | Server IP: . . . | Profile Name: 32 chars

Port	State	Server IP	Profile Name	
eth1/0/1	Disabled	-	-	Delete
eth1/0/2	Disabled	-	-	Delete
eth1/0/3	Disabled	-	-	Delete
eth1/0/4	Disabled	-	-	Delete
eth1/0/5	Disabled	-	-	Delete
eth1/0/6	Disabled	-	-	Delete
eth1/0/7	Disabled	-	-	Delete
eth1/0/8	Disabled	-	-	Delete
eth1/0/9	Disabled	-	-	Delete
eth1/0/10	Disabled	-	-	Delete

Figure 9-59 DHCP Server Screening Port Settings Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the DHCP server screening function on the port(s) specified.

Parameter	Description
Server IP	Enter the DHCP server IP address here.
Profile Name	Enter the DHCP server screening profile that will be used for the port(s) specified here.

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

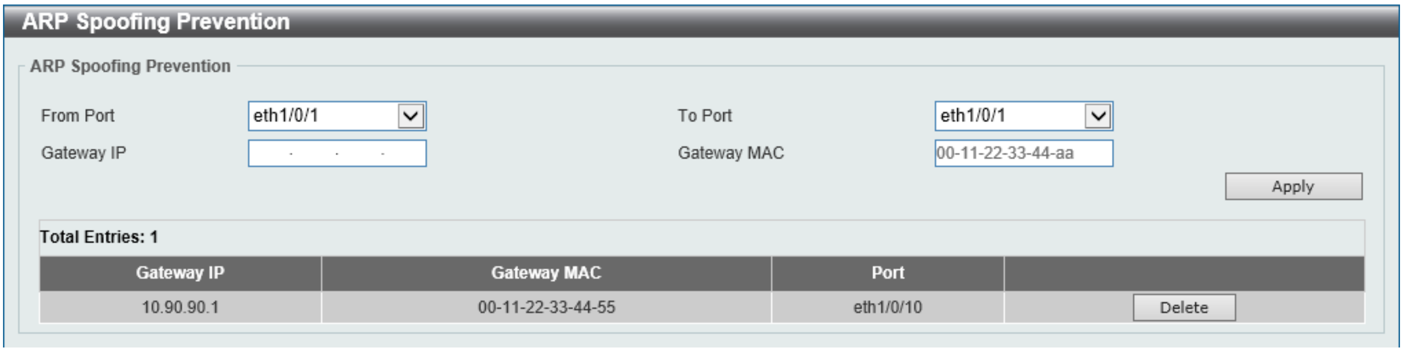
Click the **Delete** button to remove the specified entry.

ARP Spoofing Prevention

This window is used to display and configure the ARP spoofing prevention settings. When an entry is created, ARP packets whose sender IP address matches the gateway IP address, of an entry, but its sender MAC address field does not match the gateway MAC address, of the entry, will be dropped by the system. The ASP will bypass the ARP packets whose sender IP address doesn’t match the configured gateway IP address.

If an ARP address matches a configured gateway’s IP address, MAC address, and port list, then bypass the Dynamic ARP Inspection (DAI) check no matter if the receiving port is ARP trusted or untrusted.

To view the following window, click **Security > ARP Spoofing Prevention**, as shown below:



ARP Spoofing Prevention

ARP Spoofing Prevention

From Port: eth1/0/1
To Port: eth1/0/1
Gateway IP: . . .
Gateway MAC: 00-11-22-33-44-aa

Total Entries: 1

Gateway IP	Gateway MAC	Port	
10.90.90.1	00-11-22-33-44-55	eth1/0/10	Delete

Figure 9-60 ARP Spoofing Prevention Window

The fields that can be configured in **ARP Spoofing Prevention** are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Gateway IP	Enter the gateway IP address used here.
Gateway MAC	Enter the gateway MAC address used here.

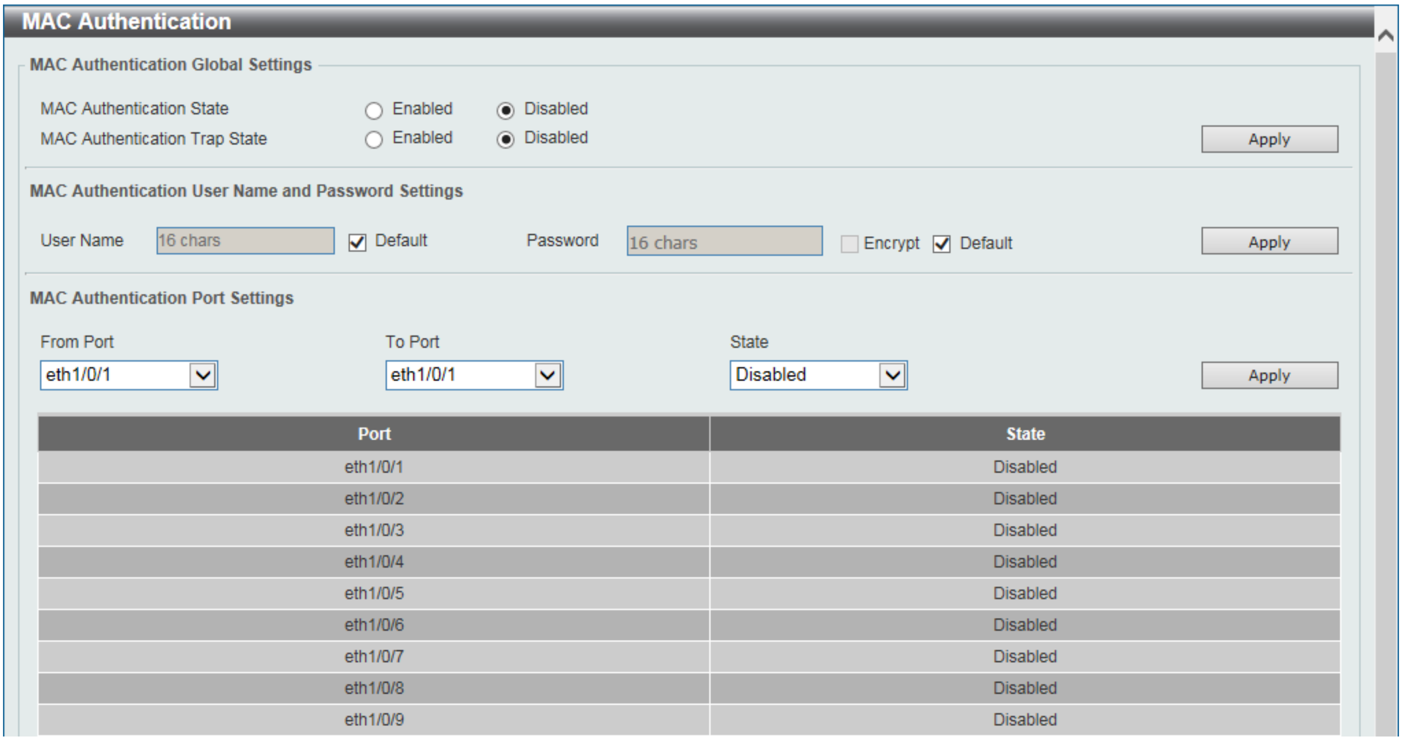
Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

MAC Authentication

This window is used to display and configure the MAC authentication settings. MAC authentication is a feature designed to authenticate a user by MAC address when the user is trying to access the network via the Switch. The Switch itself can perform the authentication based on a local database or be a RADIUS client and perform the authentication process via the RADIUS protocol with a remote RADIUS server.

To view the following window, click **Security > MAC Authentication**, as shown below:



MAC Authentication

MAC Authentication Global Settings

MAC Authentication State ○ Enabled ● Disabled

MAC Authentication Trap State ○ Enabled ● Disabled

MAC Authentication User Name and Password Settings

User Name: 16 chars ☑ Default — Password: 16 chars □ Encrypt ☑ Default

MAC Authentication Port Settings

From Port: eth1/0/1 — To Port: eth1/0/1 — State: Disabled

Port	State
eth1/0/1	Disabled
eth1/0/2	Disabled
eth1/0/3	Disabled
eth1/0/4	Disabled
eth1/0/5	Disabled
eth1/0/6	Disabled
eth1/0/7	Disabled
eth1/0/8	Disabled
eth1/0/9	Disabled

Figure 9-61 MAC Authentication Window

The fields that can be configured in **MAC Authentication Global Settings** are described below:

Parameter	Description
MAC Authentication State	Select to enable or disable the global MAC authentication state.
MAC Authentication Trap State	Select to enable or disable the MAC authentication trap state.

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

The fields that can be configured in **MAC Authentication User Name and Password Settings** are described below:

Parameter	Description
User Name	Enter the username used for MAC authentication here. This name can be up to 16 characters long. Tick the **Default** option to restore the username to the client MAC address here.
Password	Enter the password used for MAC authentication here. Tick the **Encrypt** option save this password in the encrypted form. Tick the **Default** option to restore the password to the client MAC address here.

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

The fields that can be configured in **MAC Authentication Port Settings** are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable MAC authentication for the port(s) specified here.

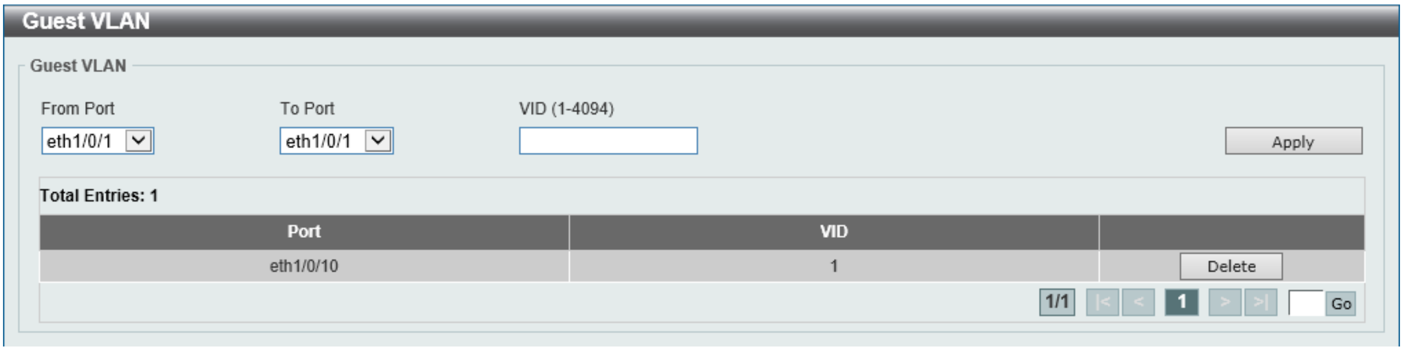
Click the **Apply** button to accept the changes made.

Network Access Authentication

Guest VLAN

This window is used to display and configure the network access authentication guest VLAN settings.

To view the following window, click **Security > Network Access Authentication > Guest VLAN**, as shown below:



Total Entries: 1

Port	VID	
eth1/0/10	1	Delete

Figure 9-62 Guest VLAN Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
VID	Enter the VLAN ID used here. This value must be between 1 and 4094.

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

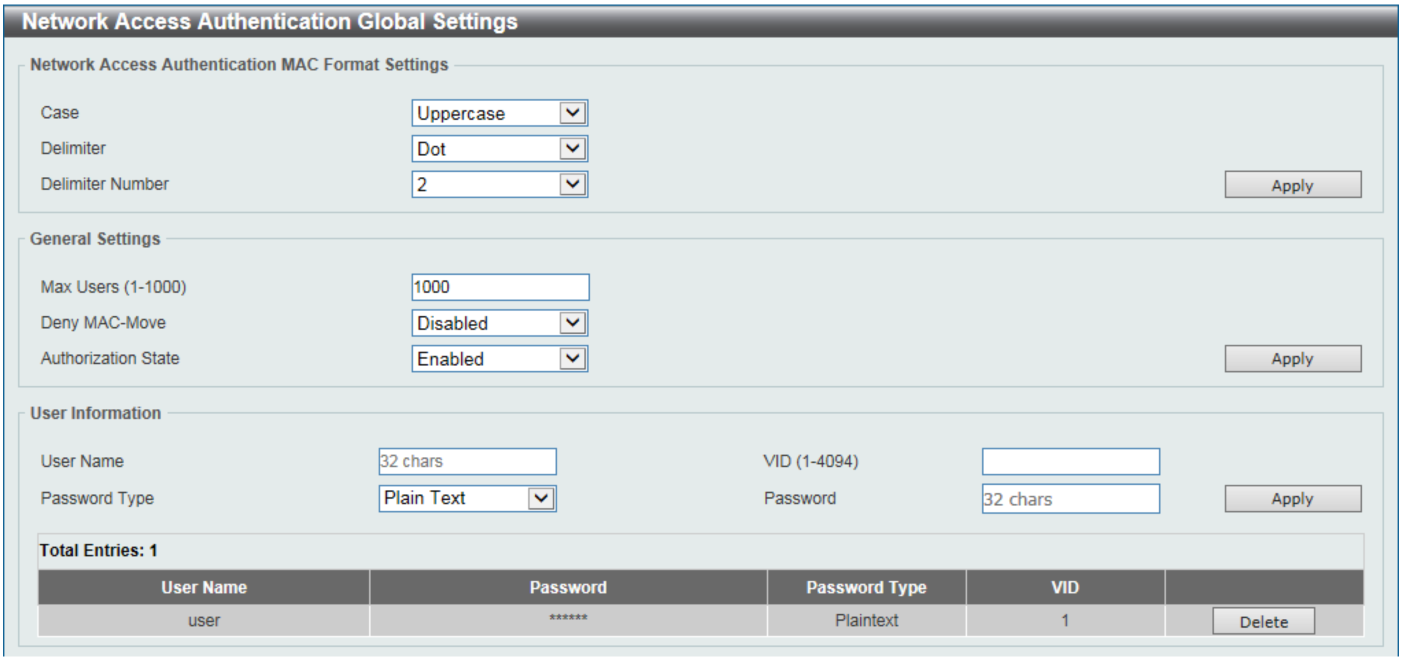
Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Network Access Authentication Global Settings

This window is used to display and configure the global Network Access Authentication settings.

To view the following window, click **Security > Network Access Authentication > Network Access Authentication Global Settings**, as shown below:



Network Access Authentication Global Settings

Network Access Authentication MAC Format Settings

Case: Uppercase
Delimiter: Dot
Delimiter Number: 2

General Settings

Max Users (1-1000): 1000
Deny MAC-Move: Disabled
Authorization State: Enabled

User Information

User Name: 32 chars
VID (1-4094):
Password Type: Plain Text
Password: 32 chars

Total Entries: 1

User Name	Password	Password Type	VID	
user	******	Plaintext	1	Delete

Figure 9-63 Network Access Authentication Global Settings Window

The fields that can be configured in **Network Access Authentication MAC Format Settings** are described below:

Parameter	Description
Case	Select the case format that will be used for the network access authentication MAC address here. Options to choose from are **Lowercase** and **Uppercase**.
Delimiter	Select the delimiter that will be used for the network access authentication MAC address here. Options to choose from are **Hyphen**, **Colon**, **Dot**, and **None**.
Delimiter Number	Select the delimiter number option here. Options to choose from are **1**, **2**, and **5**.

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

The fields that can be configured for **General Settings** are described below:

Parameter	Description
Max Users	Enter the maximum amount of users allowed here. This value must be between 1 and 1000. The default value is 1000.
Deny MAC-Move	Select to enable or disable the deny MAC-move feature here. This option controls whether to allow authenticated hosts to do roaming across different Switch ports and only controls whether a host, which is authenticated at a port set to the multi-authenticate mode, is allowed to move to another port. If a station is allowed to move, there are two situations. It may either need to be re-authenticated or directly moved to the new port without re-authentication based on the following rule. If the new port has the same authentication configuration as the original port, re-authentication is not needed. The host will inherit the same authorization attributes with new port. The authenticated host can do roaming from port 1 to port 2, and inherit the authorization attributes without re-authentication. If the new port has the different authentication configuration as the original port, re-authentication is needed. The authenticated host on port 1 can

Parameter	Description
	move and re-authenticated by port 2. If the new port has no authentication method enabled, the station is directly moved to the new port. The session with the original port is removed. The authenticated host on port 1 can be moved to port 2. If this feature is disabled and an authenticated host moves to another port, this is treated as a violation error.
Authorization State	Select to enable or disable the authorized state here. The option is used to enable or disable the acceptance of an authorized configuration. When authorization is enabled for authentication, the authorized attributes (for example, VLAN) assigned by the RADIUS server will be accepted if the authorization status is enabled.

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

The fields that can be configured in **User Information** are described below:

Parameter	Description
User Name	Enter the user name used here. This name can be up to 32 characters long.
VID	Enter the VLAN ID used here.
Password Type	Select the password type option here. Options to choose from are **Plain Text** and **Encrypted**.
Password	Enter the password used here. This can be up to 32 characters long.

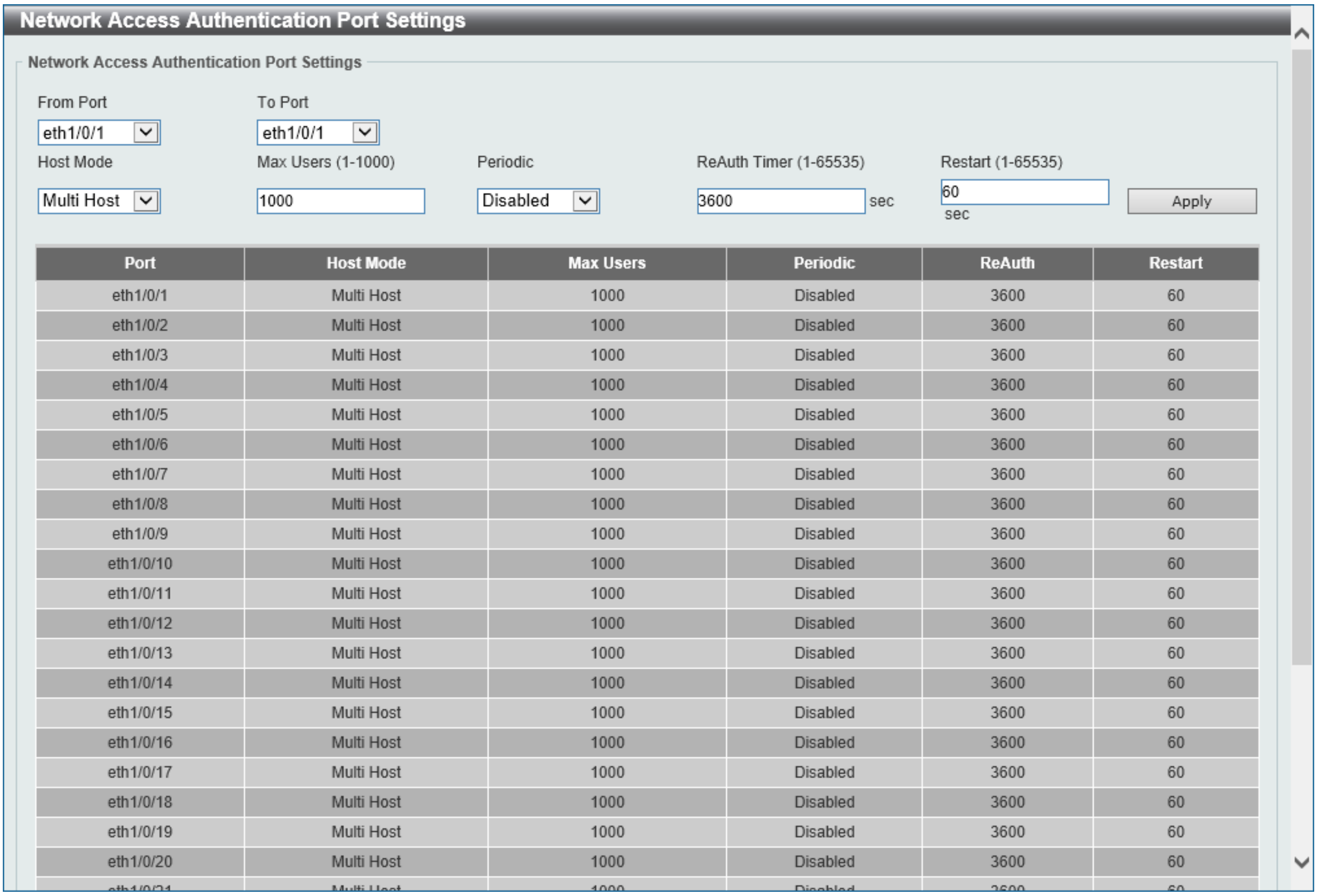
Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Network Access Authentication Port Settings

This window is used to display and configure the network access authentication port settings.

To view the following window, click **Security > Network Access Authentication > Network Access Authentication Port Settings**, as shown below:



Network Access Authentication Port Settings

From Port: eth1/0/1
To Port: eth1/0/1
Host Mode: Multi Host
Max Users (1-1000): 1000
Periodic: Disabled
ReAuth Timer (1-65535): 3600 sec
Restart (1-65535): 60 sec

Port	Host Mode	Max Users	Periodic	ReAuth	Restart
eth1/0/1	Multi Host	1000	Disabled	3600	60
eth1/0/2	Multi Host	1000	Disabled	3600	60
eth1/0/3	Multi Host	1000	Disabled	3600	60
eth1/0/4	Multi Host	1000	Disabled	3600	60
eth1/0/5	Multi Host	1000	Disabled	3600	60
eth1/0/6	Multi Host	1000	Disabled	3600	60
eth1/0/7	Multi Host	1000	Disabled	3600	60
eth1/0/8	Multi Host	1000	Disabled	3600	60
eth1/0/9	Multi Host	1000	Disabled	3600	60
eth1/0/10	Multi Host	1000	Disabled	3600	60
eth1/0/11	Multi Host	1000	Disabled	3600	60
eth1/0/12	Multi Host	1000	Disabled	3600	60
eth1/0/13	Multi Host	1000	Disabled	3600	60
eth1/0/14	Multi Host	1000	Disabled	3600	60
eth1/0/15	Multi Host	1000	Disabled	3600	60
eth1/0/16	Multi Host	1000	Disabled	3600	60
eth1/0/17	Multi Host	1000	Disabled	3600	60
eth1/0/18	Multi Host	1000	Disabled	3600	60
eth1/0/19	Multi Host	1000	Disabled	3600	60
eth1/0/20	Multi Host	1000	Disabled	3600	60

Figure 9-64 Network Access Authentication Port Settings Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the port(s) for the configuration here.
Host Mode	Select the host mode option that will be associated with the selected port(s) here. Options to choose from are **Multi Host** and **Multi Auth**. If the port is operated in the multi-host mode, and if one of the hosts is authenticated, then all other hosts are allowed to access the port. According to 802.1X authentication, if the re-authentication fails or the authenticated user logs off, the port will be blocked for a quiet period. The port restores the processing of EAPOL packets after the quiet period. If the port is operated in the **Multi Auth** mode, each host needs to be authenticated individually to access the port. A host is represented by its MAC address. Only the authorized host is allowed to access.
Max Users	Enter the maximum users value used here. This value must be between 1 and 1000.
Periodic	Select to enable or disable periodic re-authentication for the selected port here. This parameter only affects the 802.1X protocol.
ReAuth Timer	Enter the re-authentication timer value here. The range is from 1 to 65535 seconds. By default, this value is 3600 seconds.

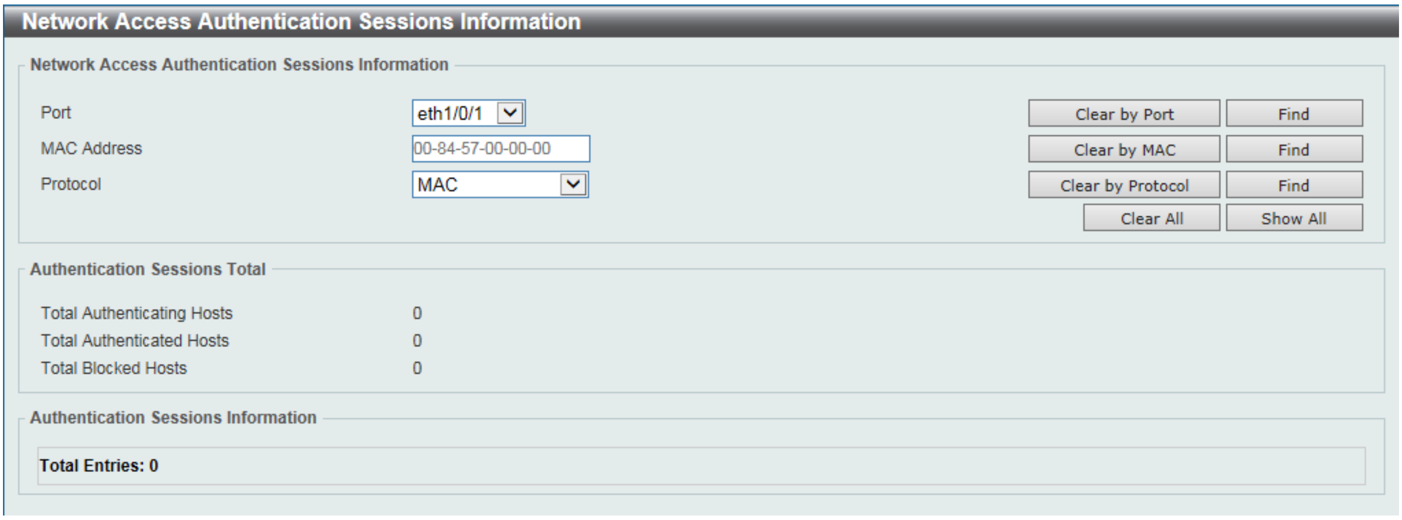
Parameter	Description
Restart	Enter the restart time value used here. The range is from 1 to 65535 seconds. By default, this value is 60 seconds.

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

Network Access Authentication Sessions Information

This window is used to view and clear the network access authentication session information.

To view the following window, click **Security > Network Access Authentication > Network Access Authentication Sessions Information**, as shown below:


Network Access Authentication Sessions Information

Network Access Authentication Sessions Information

Port: eth1/0/1

MAC Address: 00-84-57-00-00-00

Protocol: MAC

Authentication Sessions Total

Total Authenticating Hosts 0

Total Authenticated Hosts 0

Total Blocked Hosts 0

Authentication Sessions Information

Total Entries: 0

Figure 9-65 Network Access Authentication Sessions Information Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the port for the query here.
MAC Address	Enter the MAC address used here.
Protocol	Select the protocol option used here. Options to choose from are **MAC** and **DOT1X**.

Click the **Clear by Port** button to the clear the information based on the port selected.

Click the **Clear by MAC** button to the clear the information based on the MAC address entered.

Click the **Clear by Protocol** button to the clear the information based on the protocol selected.

Click the **Clear All** button to clear all the information in this table.

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

Click the **Show All** button to locate and display all the entries.

Safeguard Engine

Periodically, malicious hosts on the network will attack the Switch by utilizing packet flooding (ARP Storm) or other methods. These attacks may increase the Switch’s CPU load beyond its capability. To alleviate this problem, the Safeguard Engine function was added to the Switch’s software.

The Safeguard Engine can help the overall operability of the Switch by minimizing the workload of the Switch while the attack is ongoing, thus making it capable to forward essential packets over its network in a limited bandwidth.

If the CPU load rises above the rising threshold value, the Safeguard Engine function will be activated and the Switch will enter the exhausted mode. In the exhausted mode, the Switch will limit the bandwidth available for ARP and broadcast IP packets. If the CPU load falls below the falling threshold value, the Safeguard Engine will be deactivated and the Switch will exit the exhausted mode and enter the normal mode.

Packets that are destined to the CPU can be classified into three groups. These groups, otherwise known as sub-interfaces, are logical interfaces that the CPU will use to identify certain types of traffic. The three groups are **Protocol**, **Manage**, and **Route**.

Generally, the **Protocol** group should receive the highest priority when the Switch's CPU processes received packets and the **Route** group should receive the lowest priority as the Switch's CPU usually does get involved in the processing of routing packets. In the **Protocol** group, packets are protocol control packets identified by the router. In the **Manage** group, packets are destined to any router or system network management interface by means of interactive access protocols, like Telnet and SSH. In the **Route** group, packets are identified as traversing routing packets that is generally processed by the router CPU.

In the following table a list of supported protocols are displayed with their respective sub-interfaces (groups):

Protocol Name	Sub-interface (Group)	Description
802.1X	Protocol	Port-based Network Access Control
ARP	Protocol	Address resolution Protocol
DHCP	Protocol	Dynamic Host Configuration Protocol
DNS	Protocol	Domain Name System
ICMPv4	Protocol	Internet Control Message Protocol
ICMPv6-Neighbor	Protocol	IPv6 Internet Control Message Protocol Neighbor Discovery Protocol (NS/NA/RS/RA)
ICMPv6-Other	Protocol	IPv6 Internet Control Message Protocol except Neighbor Discovery Protocol (NS/NA/RS/RA)
IGMP	Protocol	Internet Group Management Protocol
LACP	Protocol	Link Aggregation Control Protocol
SNMP	Manage	Simple Network Management Protocol
SSH	Manage	Secure Shell
STP	Protocol	Spanning Tree Protocol
Telnet	Manage	Telnet
TFTP	Manage	Trivial File Transfer Protocol
Web	Manage	Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS)

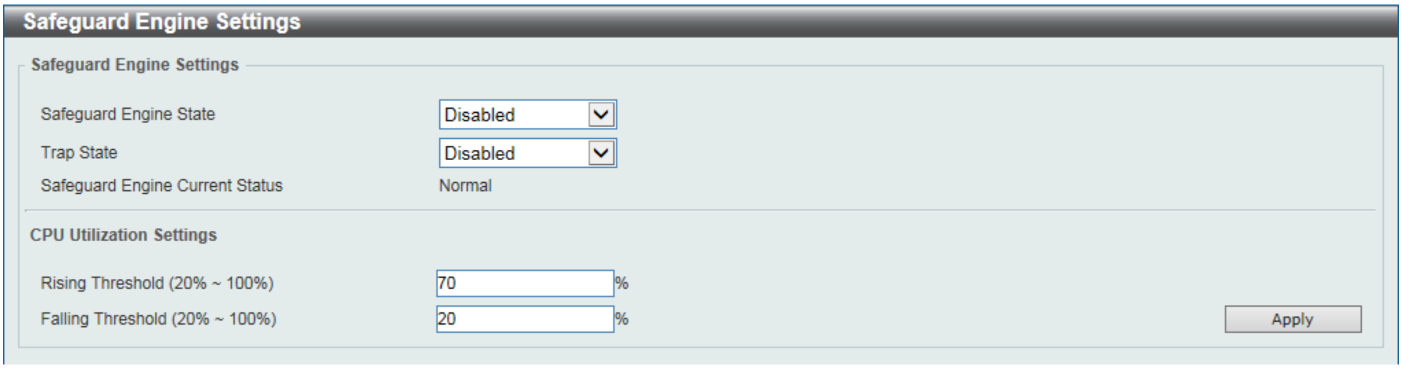
A customized rate limit (in packets per second) can be assigned to the Safeguard Engine's sub-interfaces as a whole or to individual protocols specified by the user in the management interface. Be careful when customizing the rate limit for individual protocols, using this function, as improper rate limits can cause the Switch to process packets abnormally.

NOTE: When Safeguard Engine is enabled, the Switch will allot bandwidth to various traffic flows (ARP, IP) using the FFP (Fast Filter Processor) metering table to control the CPU utilization and limit traffic. This may limit the speed of routing traffic over the network.

Safeguard Engine Settings

This window is used to display and configure the safeguard engine settings.

To view the following window, click **Security > Safeguard Engine > Safeguard Engine Settings**, as shown below:



Safeguard Engine Settings

Safeguard Engine Settings

Safeguard Engine State: Disabled

Trap State: Disabled

Safeguard Engine Current Status: Normal

CPU Utilization Settings

Rising Threshold (20% ~ 100%): 70 %

Falling Threshold (20% ~ 100%): 20 %

Figure 9-66 Safeguard Engine Settings Window

The fields that can be configured in **Safeguard Engine Settings** are described below:

Parameter	Description
Safeguard Engine State	Select to enable or disable the safeguard engine feature here.
Trap State	Select to enable or disable the safeguard engine trap state here.

The fields that can be configured in **CPU Utilization Settings** are described below:

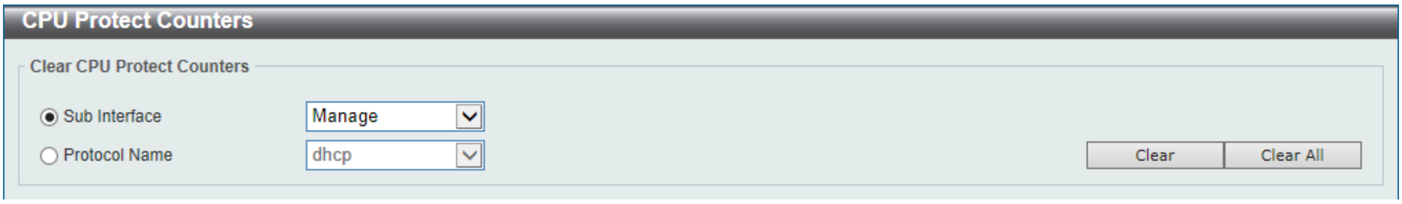
Parameter	Description
Rising Threshold	Enter the rising threshold value here. This value must be between 20% and 100%. This value is used to configure the acceptable level of CPU utilization before the Safeguard Engine mechanism is enabled. Once the CPU utilization reaches this percentage level, the Switch will move into Exhausted mode, based on the parameters provided in this window.
Falling Threshold	Enter the falling threshold value here. This value must be between 20% and 100%. This value is used to configure the acceptable level of CPU utilization as a percentage, where the Switch leaves the Safeguard Engine state and returns to normal mode.

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

CPU Protect Counters

This window is used to view and clear the CPU protection counter information.

To view the following window, click **Security > Safeguard Engine > CPU Protect Counters**, as shown below:



CPU Protect Counters

Clear CPU Protect Counters

● Sub Interface: Manage

○ Protocol Name: dhcp

Figure 9-67 CPU Protect Counters Window

The fields that can be configured are described below:

Parameter	Description
Sub Interface	Select the sub-interface option here. Options to choose from are **Manage**, **Protocol**, **Route**, and **All**. This option specifies to clear the CPU protect related counters of sub-interfaces.
Protocol Name	Select the protocol name option here.

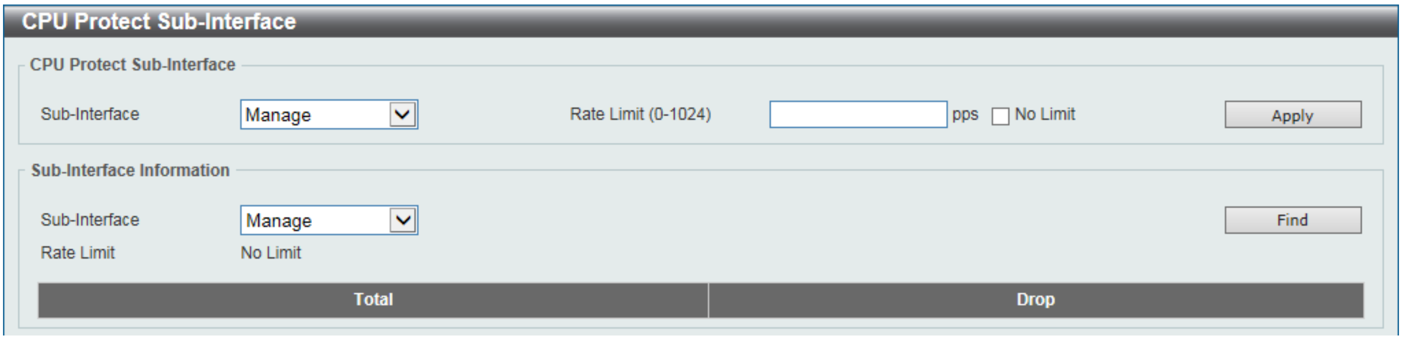
Click the **Clear** button to clear the information based on the selections made.

Click the **Clear All** button to clear all the information in this table.

CPU Protect Sub-Interface

This window is used to display and configure the CPU protection sub-interface settings.

To view the following window, click **Security > Safeguard Engine > CPU Protect Sub-Interface**, as shown below:



CPU Protect Sub-Interface

CPU Protect Sub-Interface

Sub-Interface: Manage

Rate Limit (0-1024): pps □ No Limit

Sub-Interface Information

Sub-Interface: Manage

Rate Limit: No Limit

Total	Drop

Figure 9-68 CPU Protect Sub-Interface Window

The fields that can be configured in **CPU Protect Sub-Interface** are described below:

Parameter	Description
Sub-Interface	Select the sub-interface option here. Options to choose from are **Manage**, **Protocol**, and **Route**.
Rate Limit	Enter the rate limit value used here. This value must be between 0 and 1024 packets per second. Tick the **No Limit** option to disable the rate limit.

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

The fields that can be configured in **Sub-Interface Information** are described below:

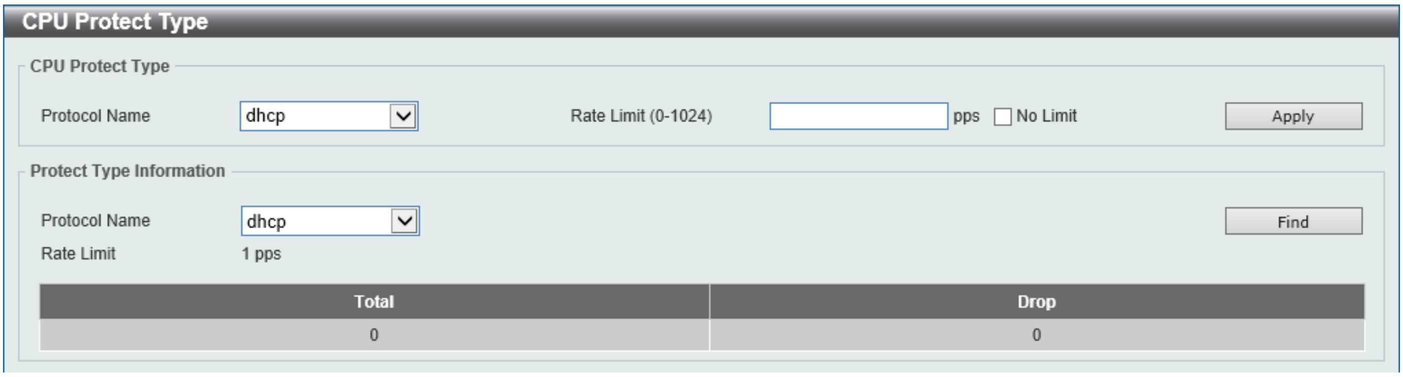
Parameter	Description
Sub-Interface	Select the sub-interface option here. Options to choose from are **Manage**, **Protocol**, and **Route**.

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

CPU Protect Type

This window is used to display and configure the CPU protection type settings.

To view the following window, click **Security > Safeguard Engine > CPU Protect Type**, as shown below:



CPU Protect Type

CPU Protect Type

Protocol Name: dhcp

Rate Limit (0-1024): pps □ No Limit

Protect Type Information

Protocol Name: dhcp

Rate Limit: 1 pps

Total	Drop
0	0

Figure 9-69 CPU Protect Type Window

The fields that can be configured in **CPU Protect Type** are described below:

Parameter	Description
Protocol Name	Select the protocol name option here.
Rate Limit	Enter the rate limit value used here. This value must be between 0 and 1024 packets per second. Tick the **No Limit** option to disable the rate limit.

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

The fields that can be configured in **Protect Type Information** are described below:

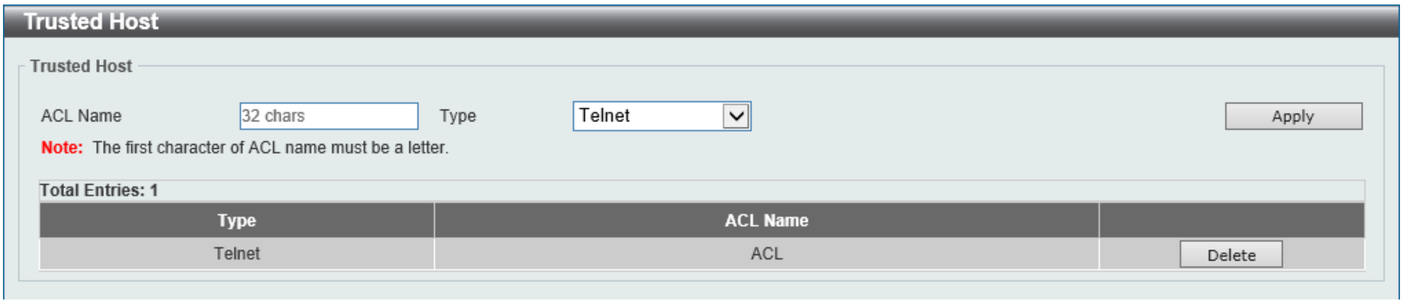
Parameter	Description
Protocol Name	Select the protocol name here. After selecting the protocol name, the **Rate Limit** assigned to the protocol type will be displayed.

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

Trusted Host

This window is used to display and configure the trusted host settings.

To view the following window, click **Security > Trusted Host**, as shown below:



Trusted Host

Trusted Host

ACL Name: 32 chars

Type: Telnet

Note: The first character of ACL name must be a letter.

Total Entries: 1

Type	ACL Name	
Telnet	ACL	Delete

Figure 9-70 Trusted Host Window

The fields that can be configured are described below:

Parameter	Description
ACL Name	Enter the access class' name here. This name can be up to 32 characters long.
Type	Select the trusted host type here. Options to choose from are **Telnet**, **SSH**, **Ping**, **HTTP**, and **HTTPS**.

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

Click the **Delete** button to remove the specific entry.

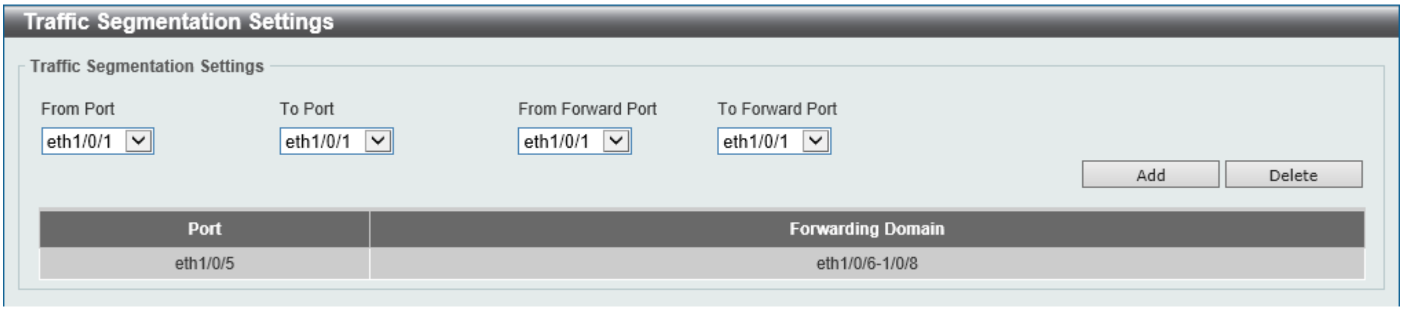
Traffic Segmentation Settings

This window is used to display and configure the traffic segmentation settings. When the traffic segmentation forwarding domain is specified, packets received by the port will be restricted in Layer 2 packet forwarding to interfaces within the domain. When the forwarding domain of a port is empty, Layer 2 forwarding for packets received by the port is not restricted.

The traffic segmentation member list can be comprised of different interface types, for example port and port-channel in the same forwarding domain. If the interfaces specified by the command include a port-channel, all the member ports of this port-channel will be included in the forwarding domain.

If the forwarding domain of an interface is empty, then there is no restriction on Layer 2 forwarding of packets received by the port.

To view the following window, click **Security > Traffic Segmentation Settings**, as shown below:



Traffic Segmentation Settings

Traffic Segmentation Settings

From Port: eth1/0/1

To Port: eth1/0/1

From Forward Port: eth1/0/1

To Forward Port: eth1/0/1

Port	Forwarding Domain
eth1/0/5	eth1/0/6-1/0/8

Figure 9-71 Traffic Segmentation Settings Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the receiving port range used for the configuration here.
From Forward Port - To Forward Port	Select the forward port range used for the configuration here.

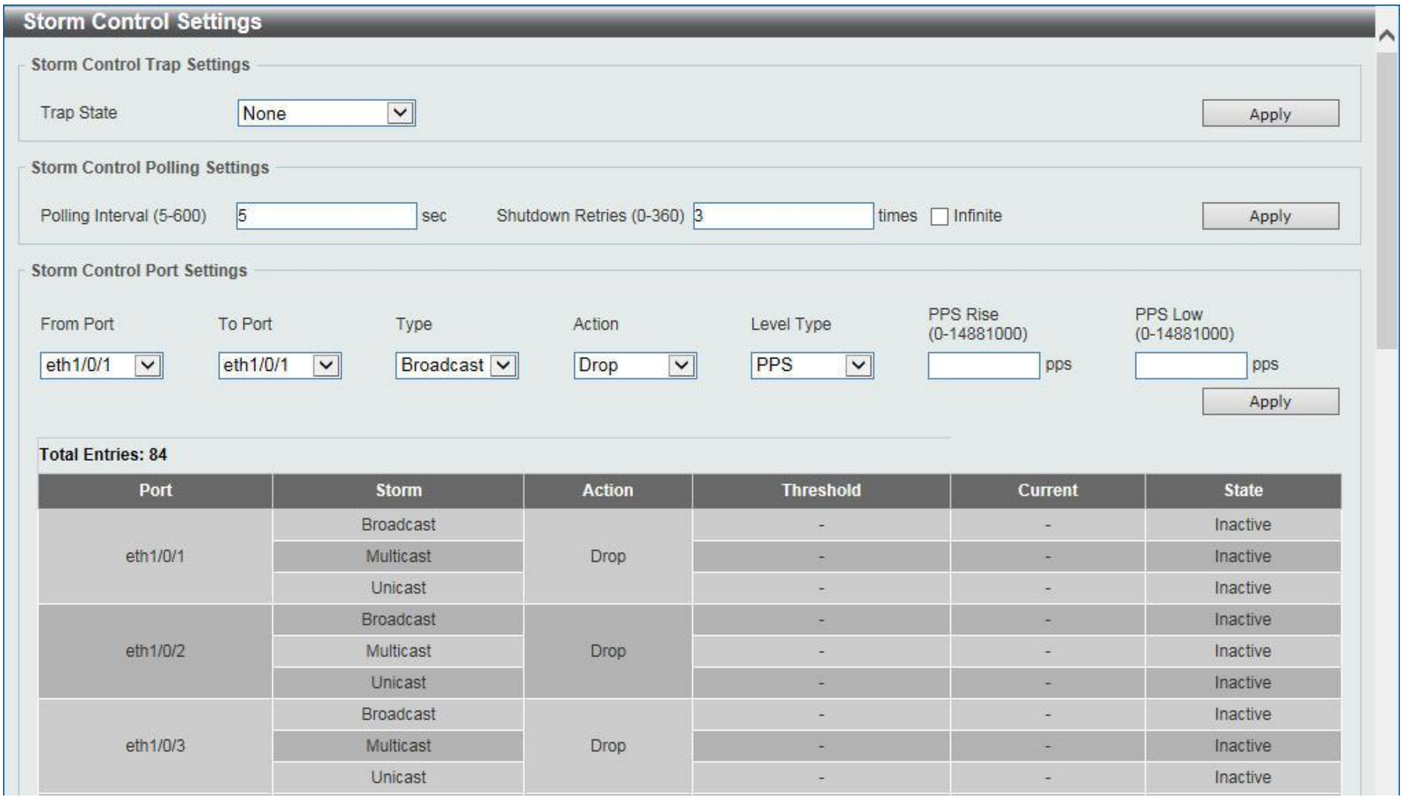
Click the **Add** button to add a new entry based on the information entered.

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

Storm Control Settings

This window is used to display and configure the storm control settings.

To view the following window, click **Security > Storm Control Settings**, as shown below:



Storm Control Settings

Storm Control Trap Settings

Trap State: None

Storm Control Polling Settings

Polling Interval (5-600): 5 sec

Shutdown Retries (0-360): 3 times □ Infinite

Storm Control Port Settings

From Port	To Port	Type	Action	Level Type	PPS Rise (0-14881000)	PPS Low (0-14881000)
eth1/0/1	eth1/0/1	Broadcast	Drop	PPS	pps	pps

Total Entries: 84

Port	Storm	Action	Threshold	Current	State
eth1/0/1	Broadcast	Drop	-	-	Inactive
	Multicast		-	-	Inactive
	Unicast		-	-	Inactive
eth1/0/2	Broadcast	Drop	-	-	Inactive
	Multicast		-	-	Inactive
	Unicast		-	-	Inactive
eth1/0/3	Broadcast	Drop	-	-	Inactive
	Multicast		-	-	Inactive
	Unicast		-	-	Inactive

Figure 9-72 Storm Control Settings Window

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

Parameter	Description
Trap State	Select the storm control trap option here. Options to choose from are: • **None** - Specifies that no traps will be sent. • **Storm Occur** - Specifies that a trap notification is sent when a storm event is detected. • **Storm Clear** - Specifies that a trap notification is sent when a storm event is cleared. • **Both** - Specifies that a trap notification is sent when a storm event is detected and/or cleared.

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

The fields that can be configured in **Storm Control Polling Settings** are described below:

Parameter	Description
Polling Interval	Enter the interval value used here. This value must be between 5 and 600 seconds. By default, this value is 5 seconds.
Shutdown Retries	Enter the shutdown retries value used here. This value must be between 0 and 360. By default, this value is 3. Tick the **Infinite** option to disable this feature.

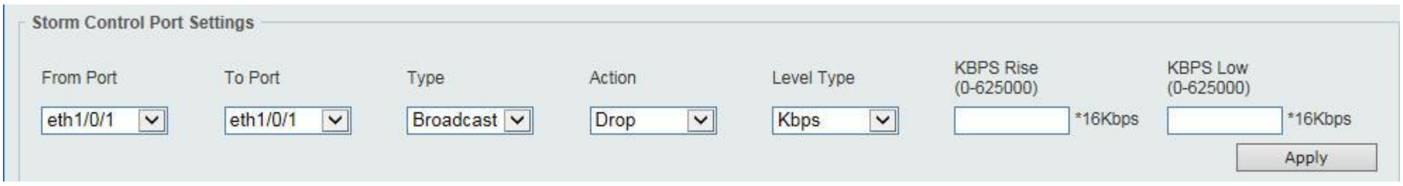
Click the **Apply** button to accept the changes made.

The fields that can be configured in **Storm Control Port Settings** are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Type	Select the type of storm attack that will be controlled here. Options to choose from are **Broadcast**, **Multicast**, and **Unicast**. When the action is configured as the shutdown mode, the unicast refers to both known and unknown unicast packets; that is, if the known and unknown unicast packets hit the specified threshold, the port will be shutdown. Otherwise, unicast refers to unknown unicast packets.
Action	Select the action that will be taken here. Options to choose from are: • **None** - Specifies not to filter the storm packets. • **Shutdown** - Specifies to shut down the port when the value specified for rise threshold is reached. • **Drop** - Specifies to discards packets that exceed the risen threshold.
Level Type	Select the level type option here. Options to choose from are **PPS**, **Kbps**, and **Level**.
PPS Rise	Enter the rise packets per second value here. This option specifies the rise threshold value in packets count per second. This value must be between 0 and 14881000 packets per second. If the low PPS value is not specified, the default value is 80% of the specified risen PPS.
PPS Low	Enter the low packets per second value here. This option specifies the low threshold value in packets count per second. This value must be between 0 and 14881000 packets per second. If the low PPS value is not specified, the default value is 80% of the specified risen PPS.

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

After selecting the **Kbps** option as the **Level Type**, the following parameters are available.



Storm Control Port Settings

From Port	To Port	Type	Action	Level Type	KBPS Rise (0-625000)	KBPS Low (0-625000)
eth1/0/1	eth1/0/1	Broadcast	Drop	Kbps	*16Kbps	*16Kbps

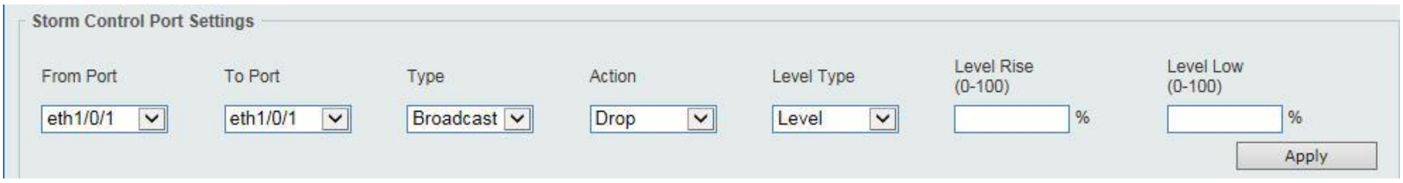
Figure 9-73 Storm Control Settings (Level Type - Kbps) Window

The additional fields that can be configured in **Storm Control Port Settings** are described below:

Parameter	Description
KBPS Rise	Enter the rise KBPS value used here. This option specifies the rise threshold value as a rate of 16 kbps per unit at which traffic is received on the port. This value must be between 0 and 625000.
KBPS Low	Enter the low KBPS value used here. This option specifies the low threshold value as a rate of 16 kbps per unit at which traffic is received on the port. This value must be between 0 and 625000. If the low KBPS is not specified, the default value is 80% of the specified risen KBPS.

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

After selecting the **Level** option as the **Level Type**, the following parameters are available.



Storm Control Port Settings

From Port	To Port	Type	Action	Level Type	Level Rise (0-100)	Level Low (0-100)
eth1/0/1	eth1/0/1	Broadcast	Drop	Level	%	%

Figure 9-74 Storm Control Settings (Level Type - Level) Window

The additional fields that can be configured in **Storm Control Port Settings** are described below:

Parameter	Description
Level Rise	Enter the rise level value used here. This option specifies the rise threshold value as a percentage of the total bandwidth per port at which traffic is received on the port. This value must be between 0% and 100%.
Level Low	Enter the low level value used here. This option specifies the low threshold value as a percentage of the total bandwidth per port at which traffic is received on the port. This value must be between 0% and 100%. If the low level is not specified, the default value is 80% of the specified risen level.

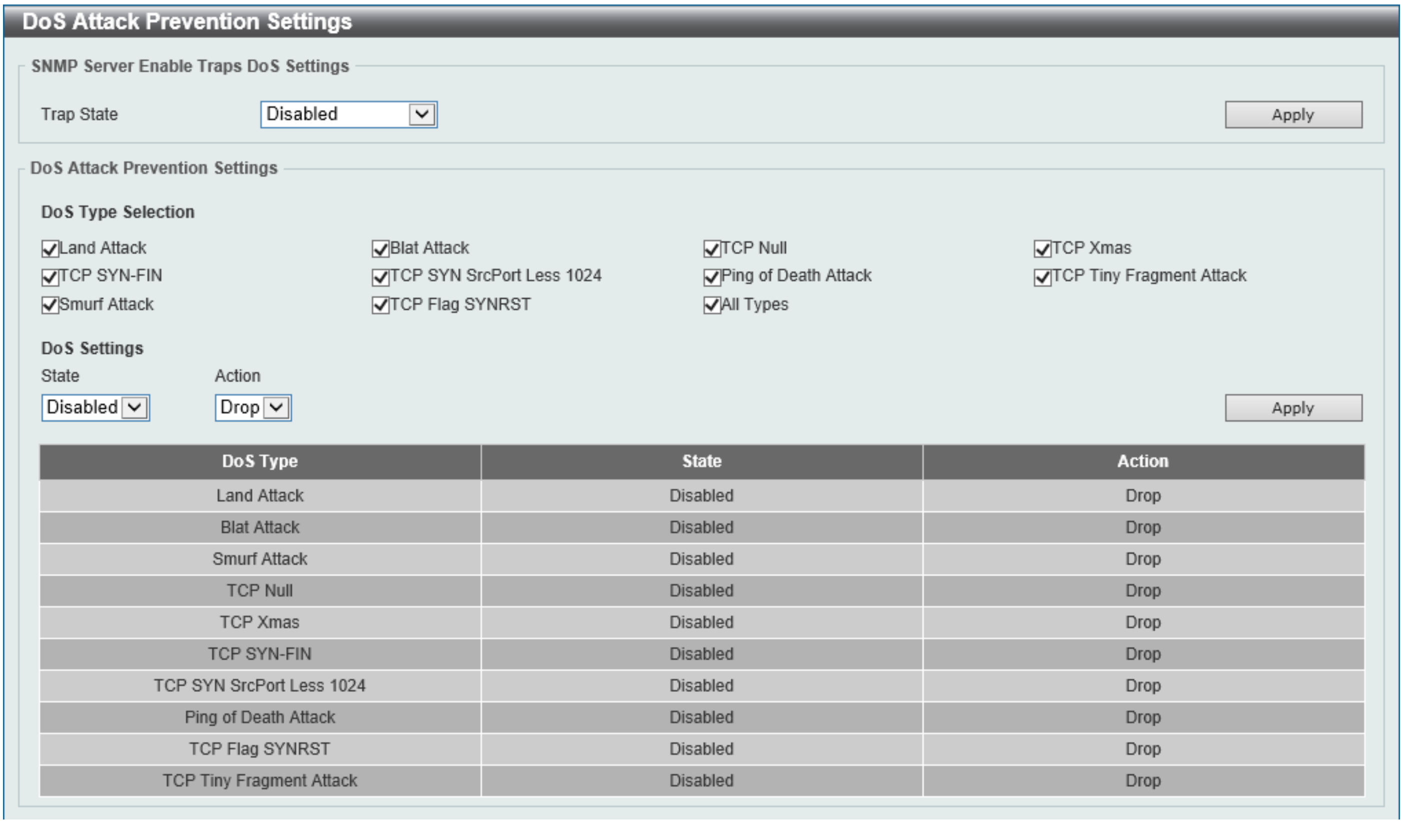
Click the **Apply** button to accept the changes made.

DoS Attack Prevention Settings

This window is used to display and configure the Denial-of-Service (DoS) attack prevention settings. The following well-known DoS types that can be detected by most Switches:

- **Land Attack:** This type of attack involves IP packets where the source and destination address are set to the address of the target device. It may cause the target device to reply to itself continuously.
- **Blat Attack**: This type of attack will send packets with the TCP/UDP source port equal to the destination port of the target device. It may cause the target device to respond to itself.
- **TCP-Null:** This type of attack involves port scanning by using specific packets that contain a sequence number of 0 and no flags.
- **TCP-Xmas:** This type of attack involves port scanning by using specific packets that contain a sequence number of 0 and the Urgent (URG), Push (PSH), and FIN flags.
- **TCP SYN-FIN:** This type of attack involves port scanning by using specific packets that contain SYN and FIN flags.
- **TCP SYN SrcPort Less 1024:** This type of attack involves port scanning by using specific packets that contain source port 0 to 1023 and SYN flag.
- **Ping of Death Attack:** A ping of death is a type of attack on a computer that involves sending a malformed or otherwise a malicious ping to a computer. A ping is normally 64 bytes in size (many computers cannot handle a ping larger than the maximum IP packet size which is 65535 bytes). The sending of a ping of this size can crash the target computer. Traditionally, this bug has been relatively easy to exploit. Generally, sending a 65536 byte ping packet is illegal according to networking protocol, but a packet of such a size can be sent if it is fragmented; when the target computer reassembles the packet, a buffer overflow can occur, which often causes a system crash.
- **TCP Tiny Fragment Attack:** The Tiny TCP Fragment attacker uses IP fragmentation to create extremely small fragments and force the TCP header information into a separate packet fragment to pass through the check function of the router and issue an attack.
- **Smurf Attack:** Smurf is a Distributed Denial of Service (DDoS) attack that enables and executes the DDoS.Smurf malware. Smurf attacks are in a way similar to ping floods, as both are carried out by sending a lot of ICMP Echo request packets. Smurf, however, is an amplification attack vector that boosts its damage potential by exploiting the characteristics of broadcast networks.
- **TCP Flag SYN RST** - The TCP SYN/RESET flood is a DDoS attack that exploits part of the normal TCP three-way handshake to consume more resources on targeted nodes to render them unresponsive. TCP connection requests are sent faster than the targeted machine can process, resulting in network traffic saturation.
- **All Types:** All of above types.

To view the following window, click **Security > DoS Attack Prevention Settings**, as shown below:



DoS Attack Prevention Settings

SNMP Server Enable Traps DoS Settings

Trap State: Disabled

DoS Attack Prevention Settings

DoS Type Selection

☑Land Attack ☑Blat Attack ☑TCP Null ☑TCP Xmas
☑TCP SYN-FIN ☑TCP SYN SrcPort Less 1024 ☑Ping of Death Attack ☑TCP Tiny Fragment Attack
☑Smurf Attack ☑TCP Flag SYNRST ☑All Types

DoS Settings

State: Disabled

Action: Drop

DoS Type	State	Action
Land Attack	Disabled	Drop
Blat Attack	Disabled	Drop
Smurf Attack	Disabled	Drop
TCP Null	Disabled	Drop
TCP Xmas	Disabled	Drop
TCP SYN-FIN	Disabled	Drop
TCP SYN SrcPort Less 1024	Disabled	Drop
Ping of Death Attack	Disabled	Drop
TCP Flag SYNRST	Disabled	Drop
TCP Tiny Fragment Attack	Disabled	Drop

Figure 9-75 DoS Attack Prevention Settings Window

The fields that can be configured in **SNMP Server Enable Traps DoS Settings** are described below:

Parameter	Description
Trap State	Select to enable or disable the DoS attack prevention trap state here.

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

The fields that can be configured in **DoS Attack Prevention Settings** are described below:

Parameter	Description
DoS Type Selection	Tick the DoS type option that will be prevented here.
State	Select to enable or disable the global DoS attack prevention state here.
Action	Select the action that will be taken when the DoS attack was detected here. The only option to select here is **Drop**.

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

SSH

Secure Shell (SSH) 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.

The steps required to use the SSH protocol for secure communication between a remote PC (the SSH client) and the Switch (the SSH server) are as follows:

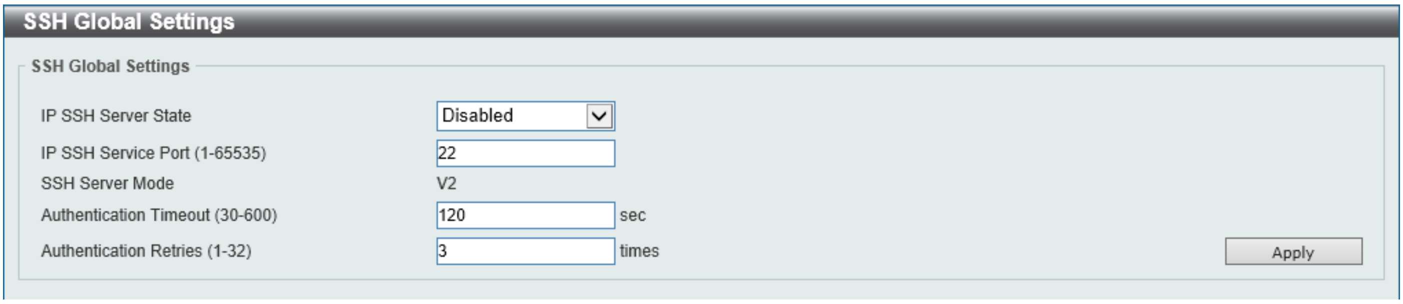
- Create a user account with admin-level access using the User Accounts window. This is identical to creating any other admin-level User Account on the Switch, including specifying a password. This password is used to logon to the Switch, once a secure communication path has been established using the SSH protocol.
- Configure the User Account to use a specified authorization method to identify users that are allowed to establish SSH connections with the Switch using the SSH User Authentication Mode window. There are three choices as to the method SSH will use to authorize the user, which are Host Based, Password, and Public Key.
- Configure the encryption algorithm that SSH will use to encrypt and decrypt messages sent between the SSH client and the SSH server, using the SSH Authentication Method and Algorithm Settings window.
- Finally, enable SSH on the Switch using the SSH Configuration window.

After completing the preceding steps, a SSH Client on a remote PC can be configured to manage the Switch using a secure, in band connection.

SSH Global Settings

This window is used to display and configure the global SSH settings.

To view the following window, click **Security > SSH > SSH Global Settings**, as shown below:



SSH Global Settings

SSH Global Settings

IP SSH Server State: Disabled

IP SSH Service Port (1-65535): 22

SSH Server Mode: V2

Authentication Timeout (30-600): 120 sec

Authentication Retries (1-32): 3 times

Figure 9-76 SSH Global Settings Window

The fields that can be configured are described below:

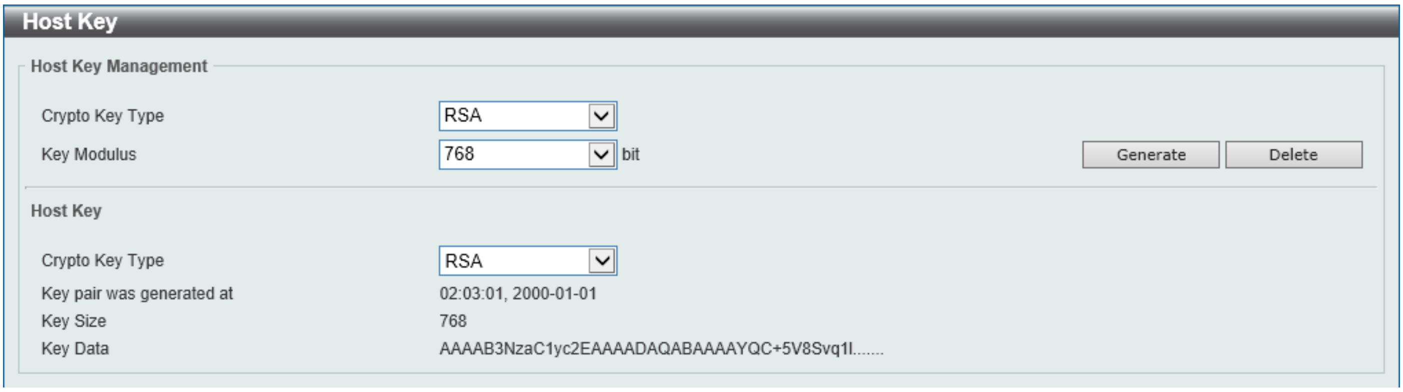
Parameter	Description
IP SSH Server State	Select to enable or disable the global SSH server state.
IP SSH Service Port	Enter the SSH service port number used here. This value must be between 1 and 65535. By default, this number is 22.
Authentication Timeout	Enter the authentication timeout value here. This value must be between 30 and 600 seconds. By default, this value is 120 seconds.
Authentication Retries	Enter the authentication retries value here. This value must be between 1 and 32. By default, this value is 3.

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

Host Key

This window is used to view and generate the SSH host key.

To view the following window, click **Security > SSH > Host Key**, as shown below:



Host Key

Host Key Management

Crypto Key Type: RSA

Key Modulus: 768 bit

Host Key

Crypto Key Type: RSA

Key pair was generated at: 02:03:01, 2000-01-01

Key Size: 768

Key Data: AAAAB3NzaC1yc2EAAAADAQABAAAAYQC+5V8Svq1l.......

Figure 9-77 Host Key Window

The fields that can be configured in **Host Key Management** are described below:

Parameter	Description
Crypto Key Type	Select the crypto key type used here. Options to choose from are the Rivest Shamir Adleman (**RSA**) key type and the Digital Signature Algorithm (**DSA**) key type.
Key Modulus	Select the key modulus value here. Options to choose from are **360**, **512**, **768**, **1024**, and **2048** bit.

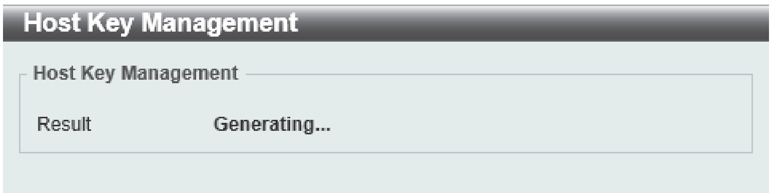
Click the **Generate** button to generate a host key based on the selections made.

Click the **Delete** button to remove a host key based on the selections made.

The fields that can be configured in **Host Key** are described below:

Parameter	Description
Crypto Key Type	Select the crypto key type used here. Options to choose from are the Rivest Shamir Adleman (**RSA**) key type and the Digital Signature Algorithm (**DSA**) key type.

After clicking the **Generate** button, the following window will appear:



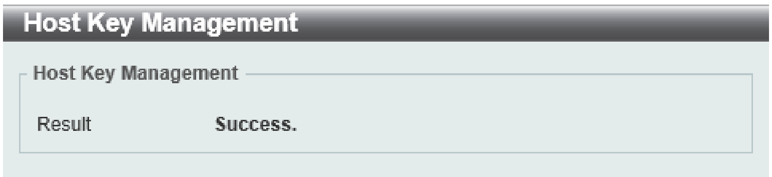
Host Key Management

Host Key Management

Result: Generating...

Figure 9-78 Host Key (Generating) Window

After the key was successfully generated, the following window will appear.



Host Key Management

Host Key Management

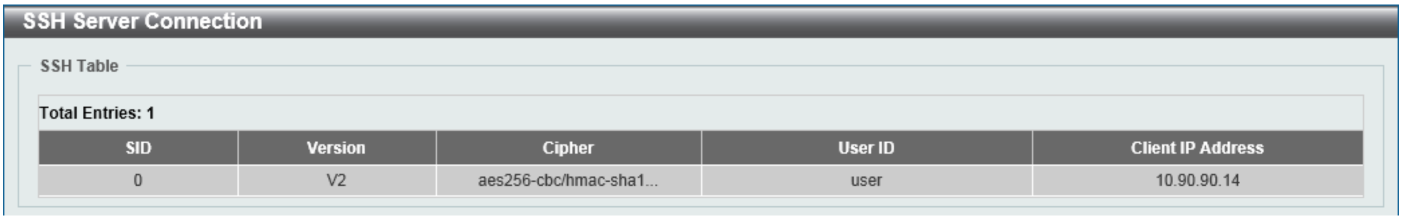
Result: Success.

Figure 9-79 Host Key (Generating, Success) Window

SSH Server Connection

This window is used to view the SSH server connections table.

To view the following window, click **Security > SSH > SSH Server Connection**, as shown below:



Total Entries: 1

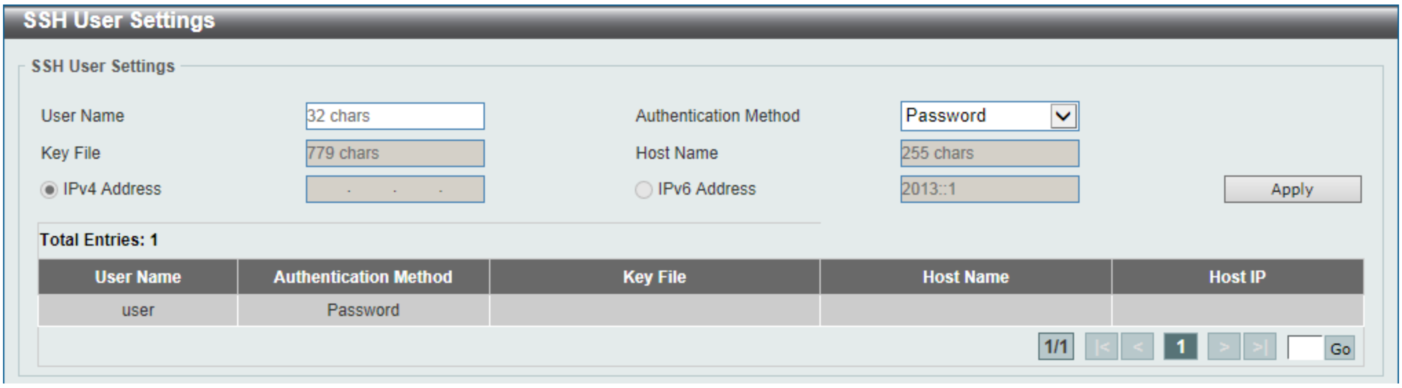
SID	Version	Cipher	User ID	Client IP Address
0	V2	aes256-cbc/hmac-sha1...	user	10.90.90.14

Figure 9-80 SSH Server Connection Window

SSH User Settings

This window is used to display and configure the SSH user settings.

To view the following window, click **Security > SSH > SSH User Settings**, as shown below:



User Name	32 chars	Authentication Method	Password
Key File	779 chars	Host Name	255 chars
● IPv4 Address	. . .	○ IPv6 Address	2013::1

Total Entries: 1

User Name	Authentication Method	Key File	Host Name	Host IP
user	Password			

Figure 9-81 SSH User Settings Window

The fields that can be configured are described below:

Parameter	Description
User Name	Enter the SSH user’s username used here. This name can be up to 32 characters long.
Authentication Method	Select the authentication methods used here. Options to choose from are **Password**, **Public Key**, and **Host-based**.
Key File	After selecting the **Public Key** or **Host-based** option as the **Authentication Method**, enter the public key here.
Host Name	After selecting the **Host-based** option as the **Authentication Method**, enter the host name here.
IPv4 Address	After selecting the **Host-based** option as the **Authentication Method**, select and enter the IPv4 address here.
IPv6 Address	After selecting the **Host-based** option as the **Authentication Method**, select and enter the IPv6 address here.

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

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

SSL

Secure Sockets Layer (SSL) is a security feature that will provide a secure communication path between a server and client through the use of authentication, digital signatures, and encryption. These security functions are implemented through the use of a cipher suite, which is a security string that determines the exact cryptographic parameters, specific encryption algorithms, and key sizes to be used for an authentication session and consists of three levels:

- **Key Exchange:** The first part of the cipher suite string specifies the public key algorithm to be used. This Switch utilizes the Rivest Shamir Adleman (RSA) public key algorithm and the Digital Signature Algorithm (DSA), specified here as the DHE DSS Diffie-Hellman (DHE) public key algorithm. This is the first authentication process between client and server as they "exchange keys" in looking for a match and therefore authentication to be accepted to negotiate encryptions on the following level.
- **Encryption:** The second part of the cipher suite that includes the encryption used for encrypting the messages sent between client and host. The Switch supports two types of cryptology algorithms:
  - **Stream Ciphers** - There are two types of stream ciphers on the Switch, RC4 with 40-bit keys, and RC4 with 128-bit keys. These keys are used to encrypt messages and need to be consistent between client and host for optimal use.
  - **CBC Block Ciphers** - CBC refers to Cipher Block Chaining, which means that a portion of the previously encrypted block of encrypted text is used in the encryption of the current block. The Switch supports the 3DES EDE encryption code defined by the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) to create the encrypted text.
- **Hash Algorithm:** This part of the cipher suite allows the user to choose a message digest function that will determine a Message Authentication Code. This Message Authentication Code will be encrypted with a sent message to provide integrity and prevent against replay attacks. The Switch supports three hash algorithms, MD5 (Message Digest 5), SHA (Secure Hash Algorithm), and SHA256.

These three parameters are uniquely assembled in four choices on the Switch to create a three-layered encryption code for secure communication between the server and the client. The user may implement any one or combination of the cipher suites available, yet different cipher suites will affect the security level and the performance of the secured connection. The information included in the cipher suites is not included with the Switch and requires downloading from a third source in a file form called a certificate. This function of the Switch cannot be executed without the presence and implementation of the certificate file and can be downloaded to the Switch by utilizing a TFTP server or the Switch file system. The Switch supports TLS 1.0, TLS 1.1, and TLS 1.2. Other versions of SSL may not be compatible with this Switch and may cause problems upon authentication and transfer of messages from client to server.

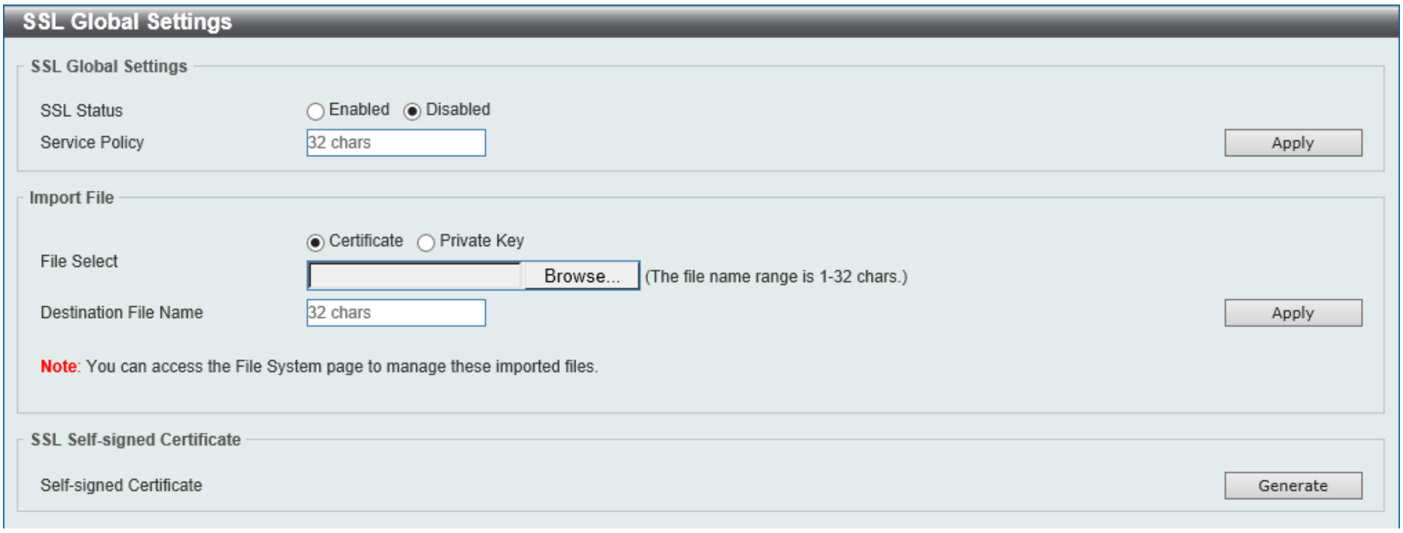
When the SSL function has been enabled, the web will become disabled. To manage the Switch through the web-based management while utilizing the SSL function, the web browser must support SSL encryption and the header of the URL must begin with https:// (Ex. https://xx.xx.xx.xx). Any other method will result in an error and no access can be authorized for the web-based management.

Users can 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. Currently, the Switch comes with a certificate pre-loaded though the user may need to download more, depending on user circumstances.

SSL Global Settings

This window is used to display and configure the global SSL settings.

To view the following window, click **Security > SSL > SSL Global Settings**, as shown below:



SSL Global Settings

SSL Global Settings

SSL Status ○ Enabled ● Disabled

Service Policy 32 chars

Import File

File Select ● Certificate ○ Private Key

(The file name range is 1-32 chars.)

Destination File Name 32 chars

Note: You can access the File System page to manage these imported files.

SSL Self-signed Certificate

Self-signed Certificate

Figure 9-82 SSL Global Settings Window

The fields that can be configured in **SSL Global Settings** are described below:

Parameter	Description
SSL Status	Select to enable or disable the global SSL status here.
Service Policy	Enter the service policy name here. This name can be up to 32 characters long.

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

The fields that can be configured in **Import File** are described below:

Parameter	Description
File Select	Select the file type that will be loaded here. Options to choose from are **Certificate** and **Private Key**. After selecting the file type, browse to the appropriate file, located on the local computer, by pressing the **Browse** button.
Destination File Name	Enter the destination file name used here. This name can be up to 32 characters long.

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

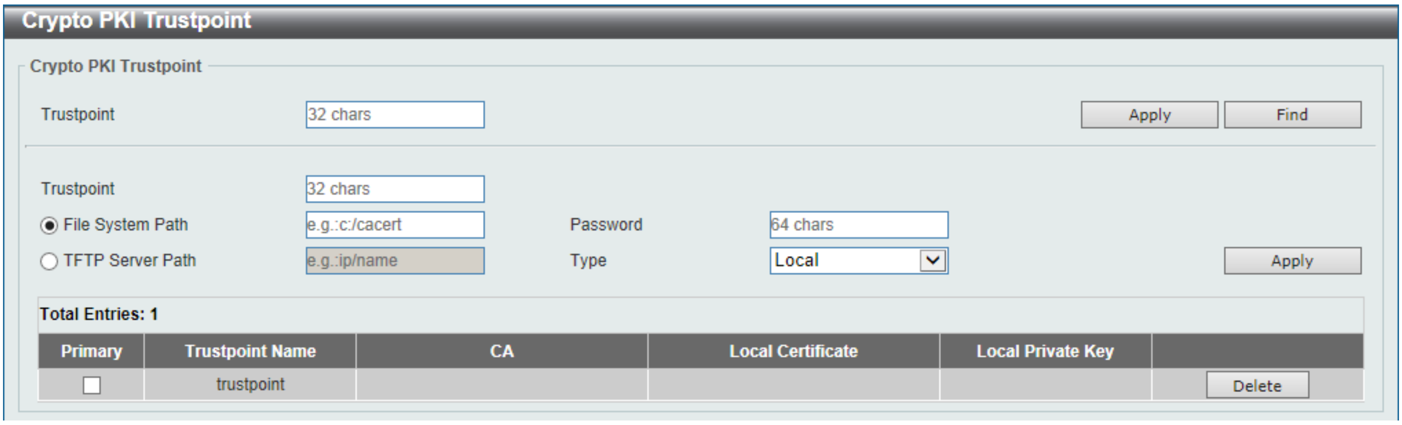
Click the **Generate** button in the **SSL-Self-signed Certificate** section to generate a new self-signed certificate, regardless if there is a built-in self-signed certificate or not. The certificate generated does not affect the user-downloaded certificates.

NOTE: The SSL self-signed certificate only supports self-signature RSA certificates with a key length of 2048 bits.

Crypto PKI Trustpoint

This window is used to display and configure the crypto PKI trust point settings.

To view the following window, click **Security > SSL > Crypto PKI Trustpoint**, as shown below:



Crypto PKI Trustpoint

Crypto PKI Trustpoint

Trustpoint: 32 chars [Apply] [Find]

Trustpoint: 32 chars

● File System Path: e.g.:c:/cacert   Password: 64 chars

○ TFTP Server Path: e.g.:ip/name   Type: Local [Apply]

Total Entries: 1

Primary	Trustpoint Name	CA	Local Certificate	Local Private Key	
□	trustpoint				Delete

Figure 9-83 Crypto PKI Trustpoint Window

The fields that can be configured are described below:

Parameter	Description
Trustpoint	Enter the name of the trust-point that is associated with the imported certificates and key pairs here. This name can be up to 32 characters long.
File System Path	Enter the file system path for certificates and key pairs here.
Password	Enter the encrypted password phrase that is used to undo encryption when the private keys are imported here. The password phrase is a string of up to 64 characters. If the password phrase is not specified, the NULL string will be used.
TFTP Server Path	Enter the TFTP server path here.
Type	Select the type of certificate that will be imported here. Options to choose from are: • **Both** - Specifies to import the CA certificate, local certificate, and key pairs. • **CA** - Specifies to import the CA certificate only. • **Local** - Specifies to import local certificate and key pairs only.
Primary	Select the **Primary** checkbox to specify which entry is the primary trustpoint (when multiple entries exist). After the checkbox is selected, a 'Success' confirmation window will appear.

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

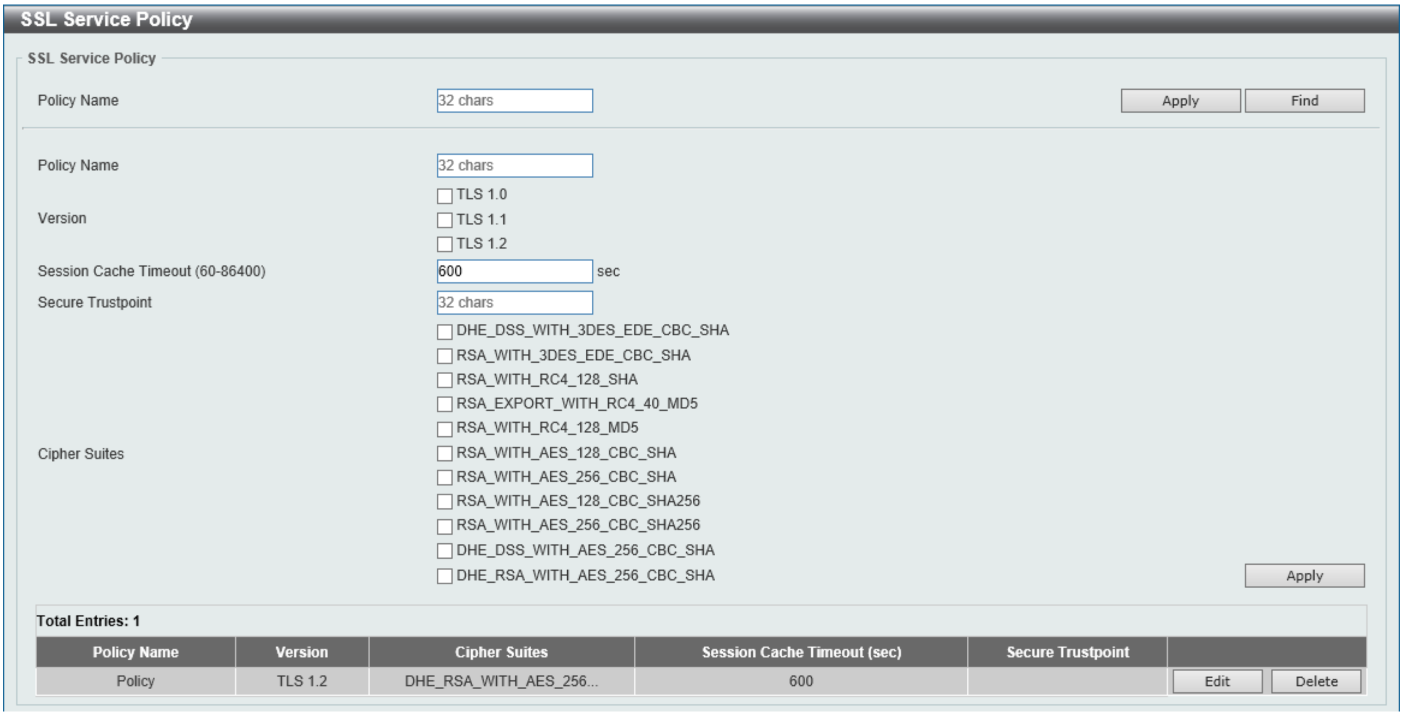
Click the **Find** button to locate a specific entry based on the information entered.

Click the **Delete** button to remove the specified entry.

SSL Service Policy

This window is used to display and configure the SSL service policy settings.

To view the following window, click **Security > SSL > SSL Service Policy**, as shown below:



SSL Service Policy

SSL Service Policy

Policy Name: 32 chars

Policy Name: 32 chars

Version: □ TLS 1.0 □ TLS 1.1 □ TLS 1.2

Session Cache Timeout (60-86400): 600 sec

Secure Trustpoint: 32 chars

Cipher Suites:
□ DHE_DSS_WITH_3DES_EDE_CBC_SHA
□ RSA_WITH_3DES_EDE_CBC_SHA
□ RSA_WITH_RC4_128_SHA
□ RSA_EXPORT_WITH_RC4_40_MD5
□ RSA_WITH_RC4_128_MD5
□ RSA_WITH_AES_128_CBC_SHA
□ RSA_WITH_AES_256_CBC_SHA
□ RSA_WITH_AES_128_CBC_SHA256
□ RSA_WITH_AES_256_CBC_SHA256
□ DHE_DSS_WITH_AES_256_CBC_SHA
□ DHE_RSA_WITH_AES_256_CBC_SHA

Total Entries: 1

Policy Name	Version	Cipher Suites	Session Cache Timeout (sec)	Secure Trustpoint	
Policy	TLS 1.2	DHE_RSA_WITH_AES_256...	600		Edit Delete

Figure 9-84 SSL Service Policy Window

The fields that can be configured are described below:

Parameter	Description
Policy Name	Enter the SSL service policy name here. This name can be up to 32 characters long.
Version	Select the Transport Layer Security (TLS) version here. Options to choose from are **TLS 1.0**, **TLS 1.1**, and **TLS 1.2**.
Session Cache Timeout	Enter the session cache timeout value used here. This value must be between 60 and 86400 seconds. By default, this value is 600 seconds.
Secure Trustpoint	Enter the secure trust point name here. This name can be up to 32 characters long.
Cipher Suites	Select the cipher suites that will be associated with this profile here.

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

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

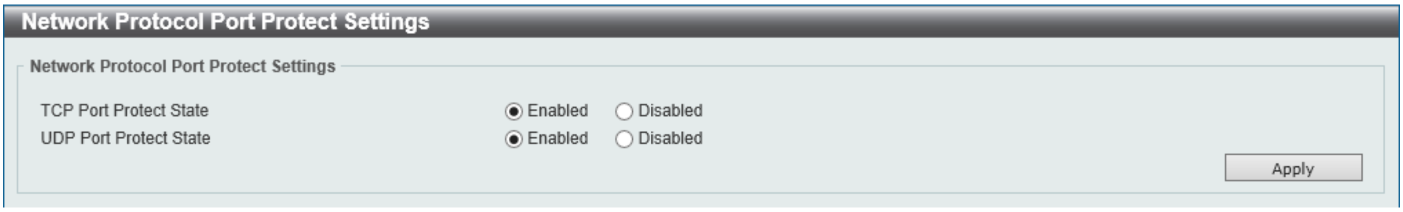
Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

Network Protocol Port Protect Settings

This window is used to display and configure the network protocol port protection settings.

To view the following window, click **Security > Network Protocol Port Protect Settings**, as shown below:



Network Protocol Port Protect Settings

Network Protocol Port Protect Settings

TCP Port Protect State ● Enabled ○ Disabled

UDP Port Protect State ● Enabled ○ Disabled

Figure 9-85 Network Protocol Port Protect Settings Window

The fields that can be configured are described below:

Parameter	Description
TCP Port Protect State	Select to enable or disable the TCP port network protocol protection function here.
UDP Port Protect State	Select to enable or disable the UDP port network protocol protection function here.

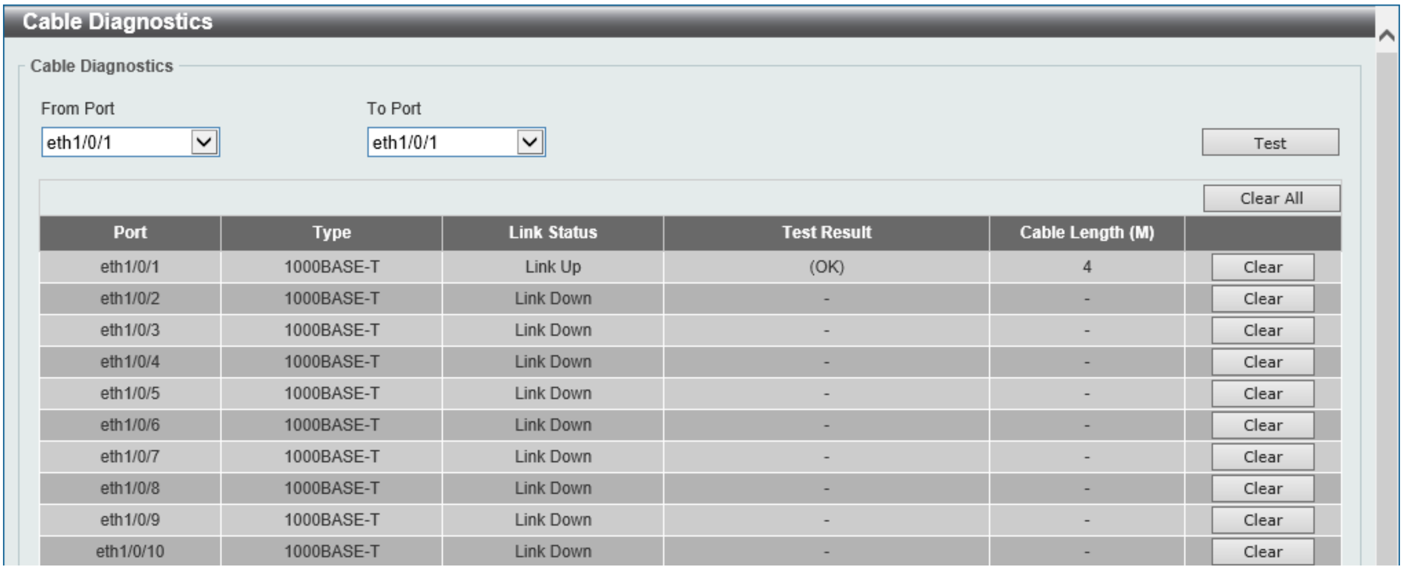
Click the **Apply** button to accept the changes made.

10. OAM

Cable Diagnostics

The cable diagnostics feature is designed primarily for administrators or customer service representatives to verify and test copper cables; it can rapidly determine the quality of the cables and the types of error.

To view the following window, click **OAM > Cable Diagnostics**, as shown below:



From Port: eth1/0/1
To Port: eth1/0/1

Port	Type	Link Status	Test Result	Cable Length (M)	
eth1/0/1	1000BASE-T	Link Up	(OK)	4	Clear
eth1/0/2	1000BASE-T	Link Down	-	-	Clear
eth1/0/3	1000BASE-T	Link Down	-	-	Clear
eth1/0/4	1000BASE-T	Link Down	-	-	Clear
eth1/0/5	1000BASE-T	Link Down	-	-	Clear
eth1/0/6	1000BASE-T	Link Down	-	-	Clear
eth1/0/7	1000BASE-T	Link Down	-	-	Clear
eth1/0/8	1000BASE-T	Link Down	-	-	Clear
eth1/0/9	1000BASE-T	Link Down	-	-	Clear
eth1/0/10	1000BASE-T	Link Down	-	-	Clear

Figure 10-1 Cable Diagnostics Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.

Click the **Test** button to test the specific port.

Click the **Clear** button to clear all the information for the specific port.

Click the **Clear All** button to clear all the information in this table.

NOTE: For this test, the supported cable length is from 10 to 130 meters and wire speed is at 100/1000 Mbps. Testing at 10 Mbps is not supported.

NOTE: The distance deviation of cable length detection on 100/1000 Mbps ports are:

- ± 25 meters on cables that are 40 meters and shorter.
- ± 20 meters on cables that are between 40 and 100 meters.

NOTE: The distance deviation on a link-down detection is:

- ± 15 meters on cables that are 30 meters and shorter.
- ± 7 meters on cables that are between 30 and 110 meters.

- ± 15 meters on cables that are between 110 and 130 meters.

NOTE: For more accurate test results, use the TIA/EIA-568B pin assignment on the RJ45 connectors.

Test Result messages:

- **Open** - The cable in the error pair does not have a connection at the specified position.
- **Short** - The cable in the error pair has a short problem at the specified position.
- **Crosstalk** - The cable in the error pair has a crosstalk problem at the specified position.
- **Mismatch** - An impedance mismatch in each differential pair.
- **PairBusy** - The remote partner interfered the test. Start the test again.
- **Shutdown** - The remote partner is powered off.
- **Unknown** - The test got an unknown status.
- **OK** - The pair or cable has no error.
- **No cable** - The port does not have any cable connection to the remote partner.

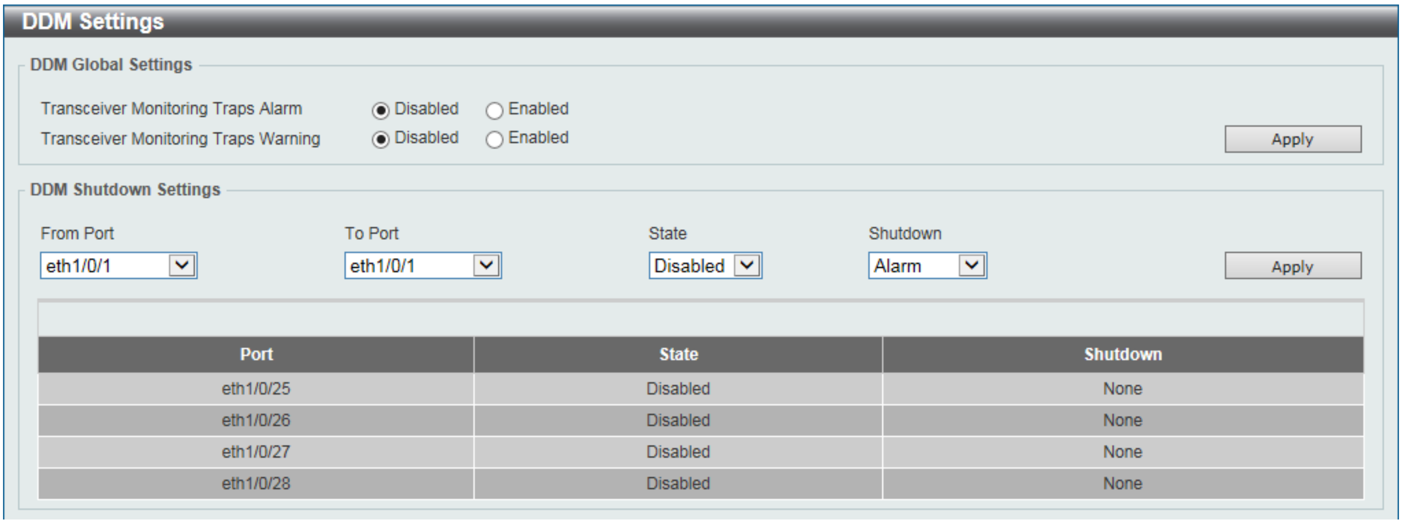
DDM

This folder contains windows that perform Digital Diagnostic Monitoring (DDM) functions on the Switch. There are windows that allow the user to view the digital diagnostic monitoring status of SFP/SFP+ modules inserting to the Switch and to configure alarm settings, warning settings, temperature threshold settings, voltage threshold settings, bias current threshold settings, Tx power threshold settings, and Rx power threshold settings.

DDM Settings

The window is used to view and configure the action that will occur for specific ports when an exceeding alarm threshold or warning threshold event is encountered.

To view the following window, click **OAM > DDM > DDM Settings**, as shown below:



DDM Settings

DDM Global Settings

Transceiver Monitoring Traps Alarm ● Disabled ○ Enabled

Transceiver Monitoring Traps Warning ● Disabled ○ Enabled

DDM Shutdown Settings

From Port: eth1/0/1

To Port: eth1/0/1

State: Disabled

Shutdown: Alarm

Port	State	Shutdown
eth1/0/25	Disabled	None
eth1/0/26	Disabled	None
eth1/0/27	Disabled	None
eth1/0/28	Disabled	None

Figure 10-2 DDM Settings Window

The fields that can be configured in **DDM Global Settings** are described below:

Parameter	Description
Transceiver Monitoring Traps Alarm	Select to enable or disable the transceiver monitoring traps alarm feature here.

Parameter	Description
Transceiver Monitoring Traps Warning	Select to enable or disable the transceiver monitoring traps warning feature here.

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

The fields that can be configured in **DDM Shutdown Settings** are described below:

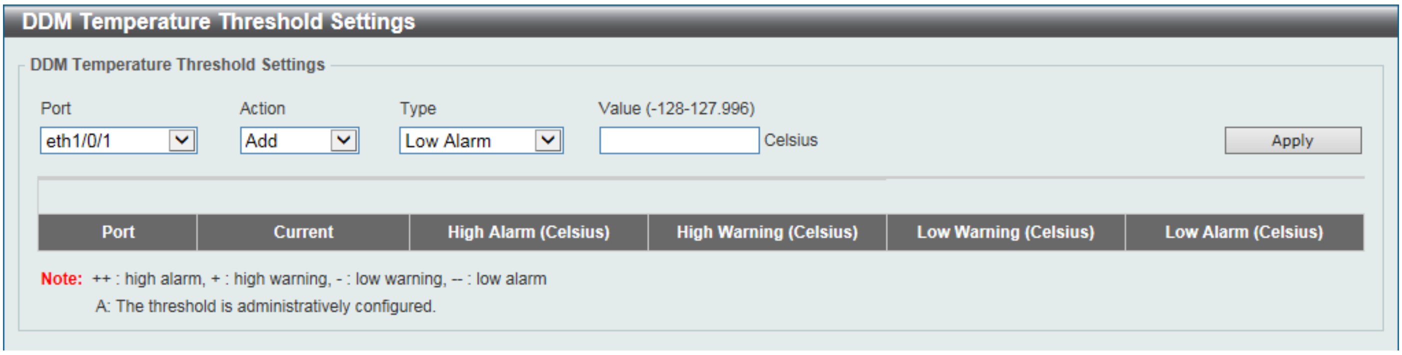
Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Use the drop-down menu to enable or disable the DDM state.
Shutdown	Specify whether to shut down the port, when the operating parameter exceeds the Alarm or Warning threshold. • **Alarm** - Shutdown the port when the configured alarm threshold range is exceeded. • **Warning** - Shutdown the port when the configured warning threshold range is exceeded. • **None** - The port will never shutdown regardless if the threshold ranges are exceeded or not. This is the default.

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

DDM Temperature Threshold Settings

This window is used to display and configure the DDM Temperature Threshold Settings for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM Temperature Threshold Settings**, as shown below:



DDM Temperature Threshold Settings

DDM Temperature Threshold Settings

Port: eth1/0/1
Action: Add
Type: Low Alarm
Value (-128-127.996): Celsius

Port	Current	High Alarm (Celsius)	High Warning (Celsius)	Low Warning (Celsius)	Low Alarm (Celsius)

Note: ++ : high alarm, + : high warning, - : low warning, -- : low alarm
A: The threshold is administratively configured.

Figure 10-3 DDM Temperature Threshold Settings Window

The fields that can be configured are described below:

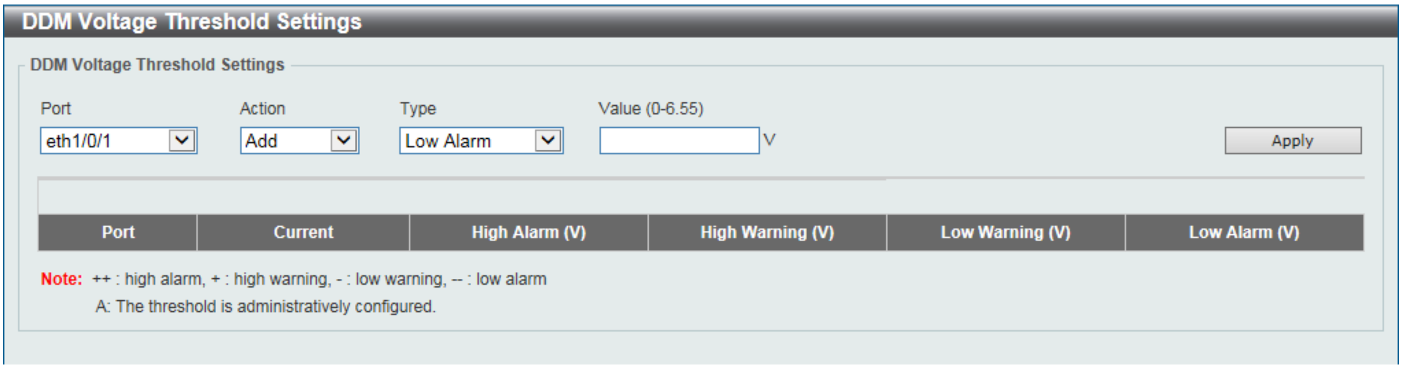
Parameter	Description
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**.
Type	Select the type of temperature threshold. Options to choose from are **Low Alarm**, **Low Warning**, **High Alarm**, and **High Warning**.
Value	Enter the threshold value. This value must be between -128 and 127.996 °C.

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

DDM Voltage Threshold Settings

This window is used to display and configure the DDM Voltage Threshold Settings for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM Voltage Threshold Settings**, as shown below:



Note: ++ : high alarm, + : high warning, - : low warning, -- : low alarm
A: The threshold is administratively configured.

Figure 10-4 DDM Voltage Threshold Settings Window

The fields that can be configured are described below:

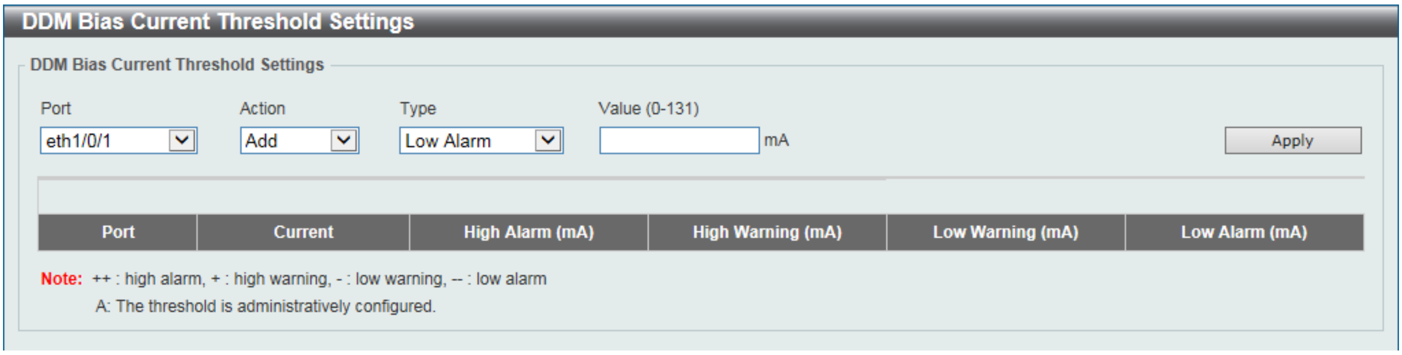
Parameter	Description
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**.
Type	Select the type of voltage threshold. Options to choose from are **Low Alarm**, **Low Warning**, **High Alarm**, and **High Warning**.
Value	Enter the threshold value. This value must be between 0 and 6.55 Volt.

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

DDM Bias Current Threshold Settings

This window is used to display and configure the threshold of the bias current for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM Bias Current Threshold Settings**, as shown below:



Note: ++ : high alarm, + : high warning, - : low warning, -- : low alarm
A: The threshold is administratively configured.

Figure 10-5 DDM Bias Current Threshold Settings Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the port used for the configuration here.

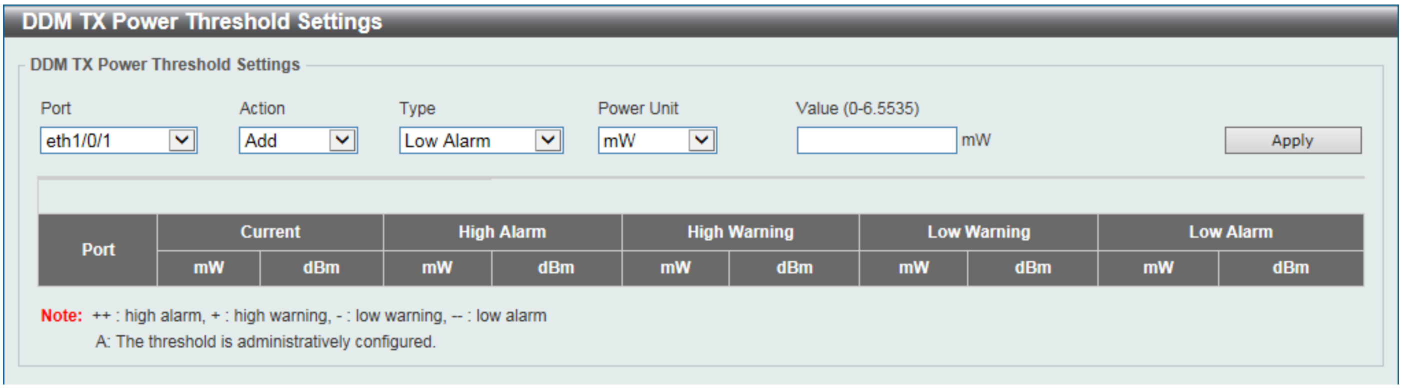
Parameter	Description
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**.
Type	Select the type of bias current threshold. Options to choose from are **Low Alarm**, **Low Warning**, **High Alarm**, and **High Warning**.
Value	Enter the threshold value. This value must be between 0 and 131 mA.

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

DDM TX Power Threshold Settings

This window is used to display and configure the threshold of TX power for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM TX Power Threshold Settings**, as shown below:



DDM TX Power Threshold Settings

DDM TX Power Threshold Settings

Port: eth1/0/1
Action: Add
Type: Low Alarm
Power Unit: mW
Value (0-6.5535): mW

Port	Current		High Alarm		High Warning		Low Warning		Low Alarm	
	mW	dBm	mW	dBm	mW	dBm	mW	dBm	mW	dBm

Note: ++ : high alarm, + : high warning, - : low warning, -- : low alarm
A: The threshold is administratively configured.

Figure 10-6 DDM TX Power Threshold Settings Window

The fields that can be configured are described below:

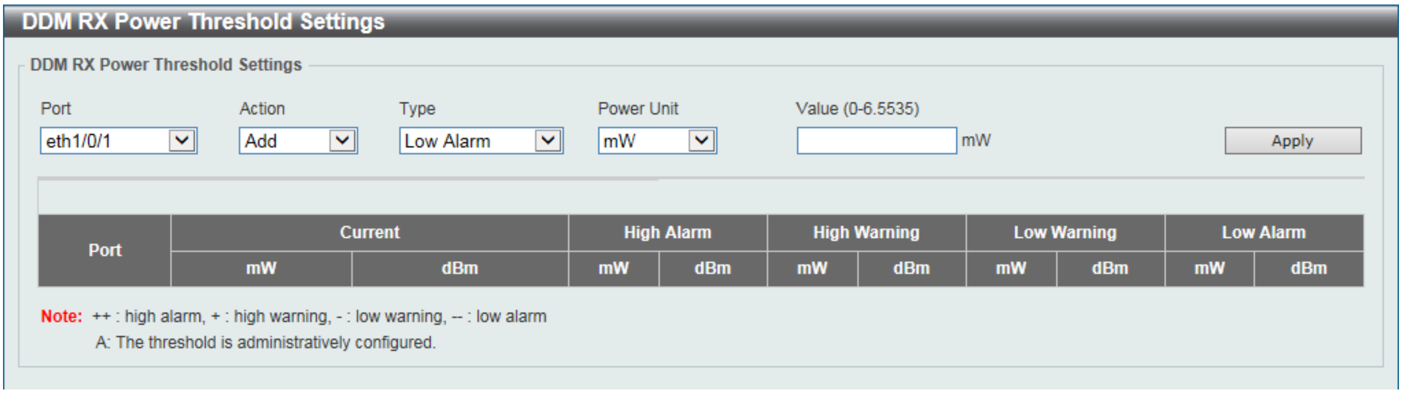
Parameter	Description
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**.
Type	Select the type of TX power threshold. Options to choose from are **Low Alarm**, **Low Warning**, **High Alarm**, and **High Warning**.
Power Unit	Select the power unit here. Options to choose from are **mW** and **dBm**.
Value	Enter the threshold value either in **mW** or **dBm** here. • When selecting **mW** in the **Power Unit** drop-down list, this value must be between 0 and 6.5535. • When selecting **dBm** in the **Power Unit** drop-down list, this value must be between -40 and 8.1647.

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

DDM RX Power Threshold Settings

This window is used to display and configure the threshold of RX power for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM RX Power Threshold Settings**, as shown below:



DDM RX Power Threshold Settings

DDM RX Power Threshold Settings

Port: eth1/0/1 · Action: Add · Type: Low Alarm · Power Unit: mW · Value (0-6.5535): mW

Port	Current		High Alarm		High Warning		Low Warning		Low Alarm	
	mW	dBm	mW	dBm	mW	dBm	mW	dBm	mW	dBm

Note: ++ : high alarm, + : high warning, - : low warning, -- : low alarm

A: The threshold is administratively configured.

Figure 10-7 DDM RX Power Threshold Settings Window

The fields that can be configured are described below:

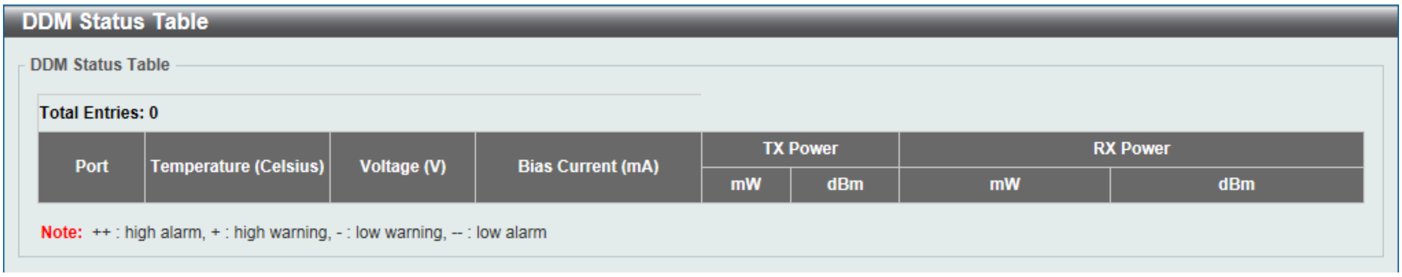
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**.
Type	Select the type of RX power threshold. Options to choose from are **Low Alarm**, **Low Warning**, **High Alarm**, and **High Warning**.
Power Unit	Select the power unit here. Options to choose from are **mW** and **dBm**.
Value	Enter the threshold value either in **mW** or **dBm** here. • When selecting **mW** in the **Power Unit** drop-down list, this value must be between 0 and 6.5535. • When selecting **dBm** in the **Power Unit** drop-down list, this value must be between -40 and 8.1647.

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

DDM Status Table

This window is used to display the current operating digital diagnostic monitoring parameters and their values on the SFP module for specified ports.

To view the following window, click **OAM > DDM > DDM Status Table**, as shown below:



DDM Status Table

DDM Status Table

Total Entries: 0

Port	Temperature (Celsius)	Voltage (V)	Bias Current (mA)	TX Power		RX Power	
				mW	dBm	mW	dBm

Note: ++ : high alarm, + : high warning, - : low warning, -- : low alarm

Figure 10-8 DDM Status Table Window

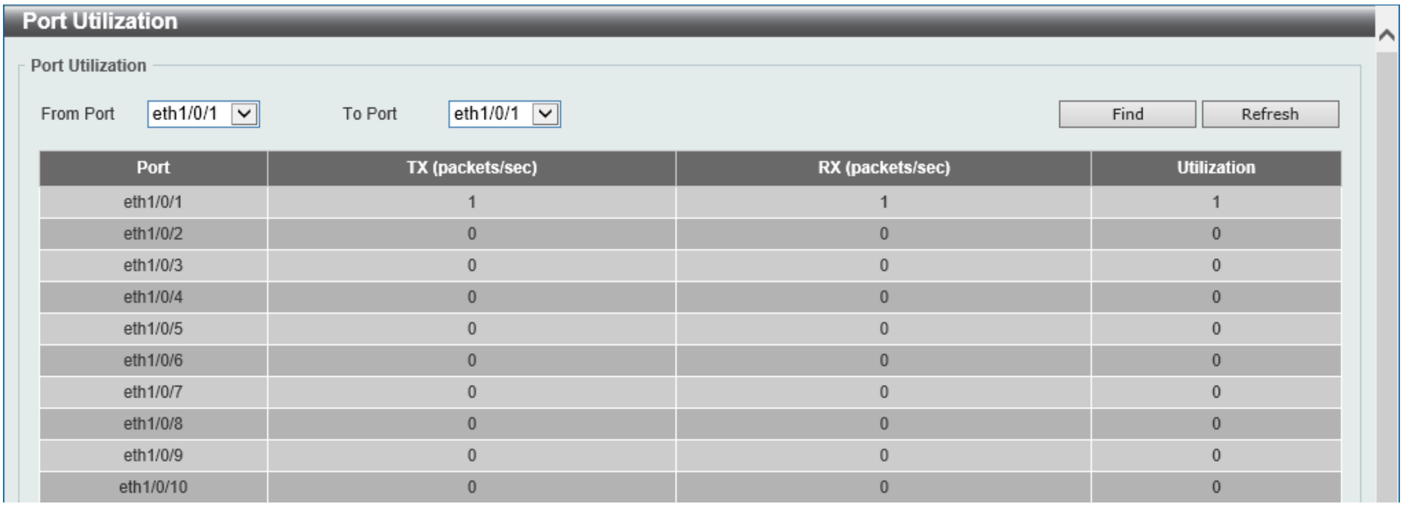
11. Monitoring

Utilization

Port Utilization

This window is used to view the port utilization table.

To view the following window, click **Monitoring > Utilization > Port Utilization**, as shown below:



Port Utilization

Port Utilization

From Port: eth1/0/1

To Port: eth1/0/1

Port	TX (packets/sec)	RX (packets/sec)	Utilization
eth1/0/1	1	1	1
eth1/0/2	0	0	0
eth1/0/3	0	0	0
eth1/0/4	0	0	0
eth1/0/5	0	0	0
eth1/0/6	0	0	0
eth1/0/7	0	0	0
eth1/0/8	0	0	0
eth1/0/9	0	0	0
eth1/0/10	0	0	0

Figure 11-1 Port Utilization Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the range of ports that will be used here.

Click the **Find** button to display entries in the table based on the information entered/selected.

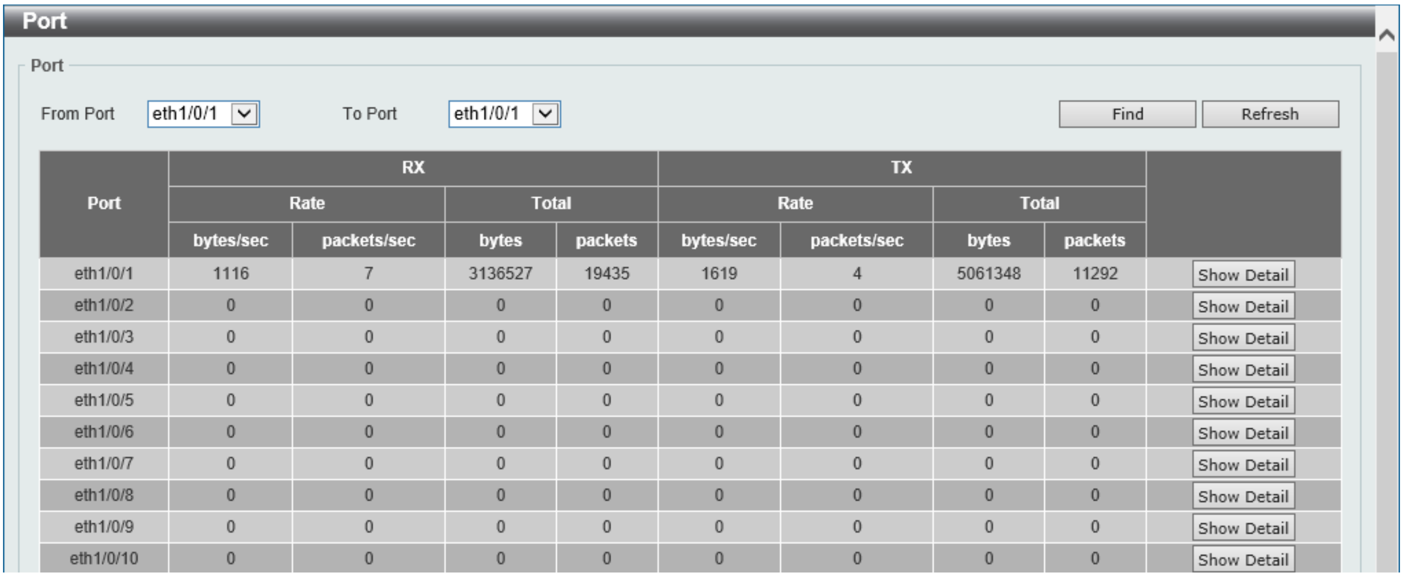
Click the **Refresh** button to refresh the information displayed in the table.

Statistics

Port

This window is used to view the port statistics information.

To view the following window, click **Monitoring > Statistics > Port**, as shown below:



Port

From Port eth1/0/1 To Port eth1/0/1

Port	RX				TX				
	Rate		Total		Rate		Total		
	bytes/sec	packets/sec	bytes	packets	bytes/sec	packets/sec	bytes	packets	
eth1/0/1	1116	7	3136527	19435	1619	4	5061348	11292	Show Detail
eth1/0/2	0	0	0	0	0	0	0	0	Show Detail
eth1/0/3	0	0	0	0	0	0	0	0	Show Detail
eth1/0/4	0	0	0	0	0	0	0	0	Show Detail
eth1/0/5	0	0	0	0	0	0	0	0	Show Detail
eth1/0/6	0	0	0	0	0	0	0	0	Show Detail
eth1/0/7	0	0	0	0	0	0	0	0	Show Detail
eth1/0/8	0	0	0	0	0	0	0	0	Show Detail
eth1/0/9	0	0	0	0	0	0	0	0	Show Detail
eth1/0/10	0	0	0	0	0	0	0	0	Show Detail

Figure 11-2 Port Window

The fields that can be configured are described below:

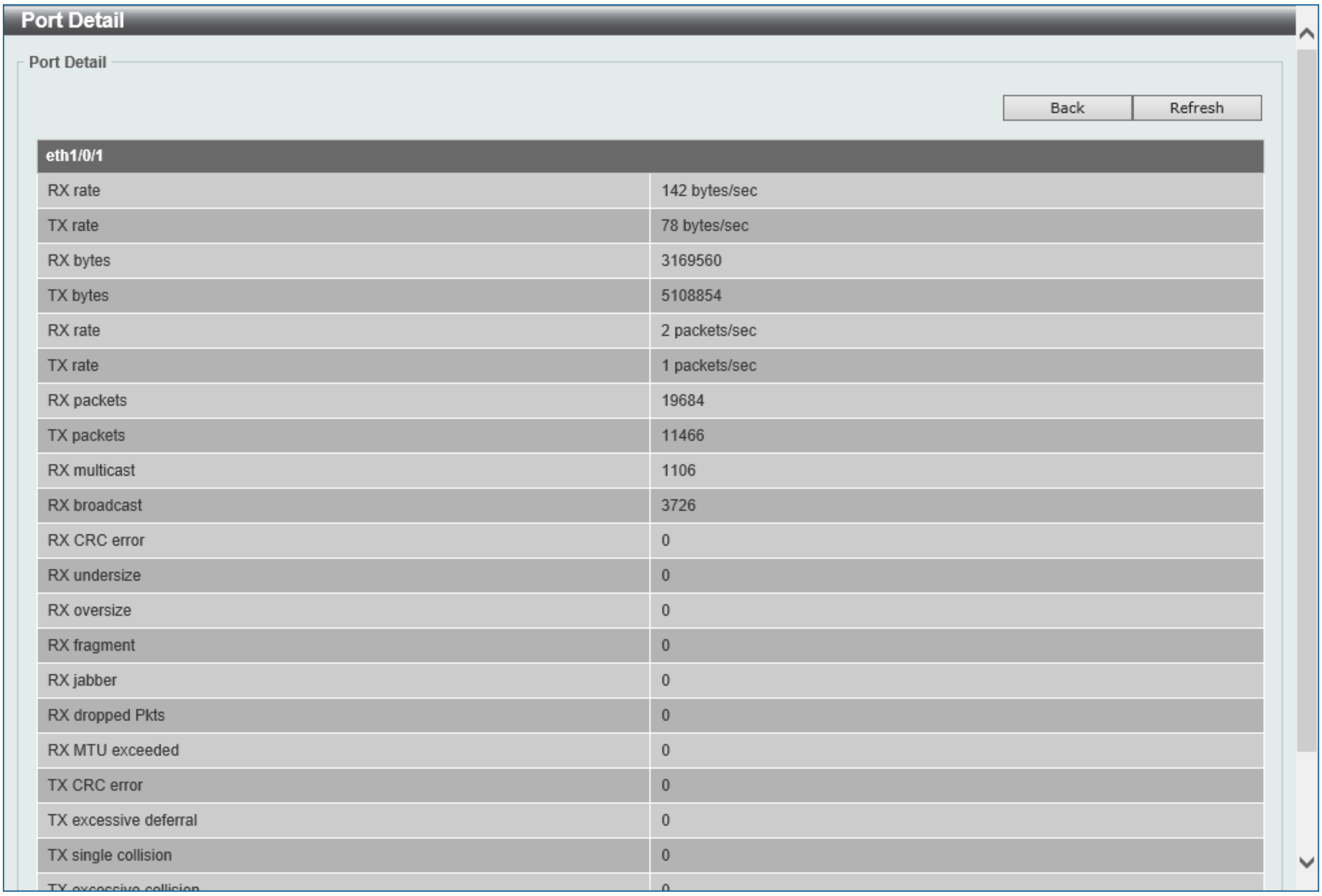
Parameter	Description
From Port - To Port	Select the range of ports that will be used in this display here.

Click the **Find** button to display entries in the table based on the information selected.

Click the **Refresh** button to refresh the information displayed in the table.

Click the **Show Detail** button to view more detailed statistics information on the specified port.

After clicking the **Show Detail** button, the following window will appear:



eth1/0/1	
RX rate	142 bytes/sec
TX rate	78 bytes/sec
RX bytes	3169560
TX bytes	5108854
RX rate	2 packets/sec
TX rate	1 packets/sec
RX packets	19684
TX packets	11466
RX multicast	1106
RX broadcast	3726
RX CRC error	0
RX undersize	0
RX oversize	0
RX fragment	0
RX jabber	0
RX dropped Pkts	0
RX MTU exceeded	0
TX CRC error	0
TX excessive deferral	0
TX single collision	0
TX excessive collision	0

Figure 11-3 Port (Show Detail) Window

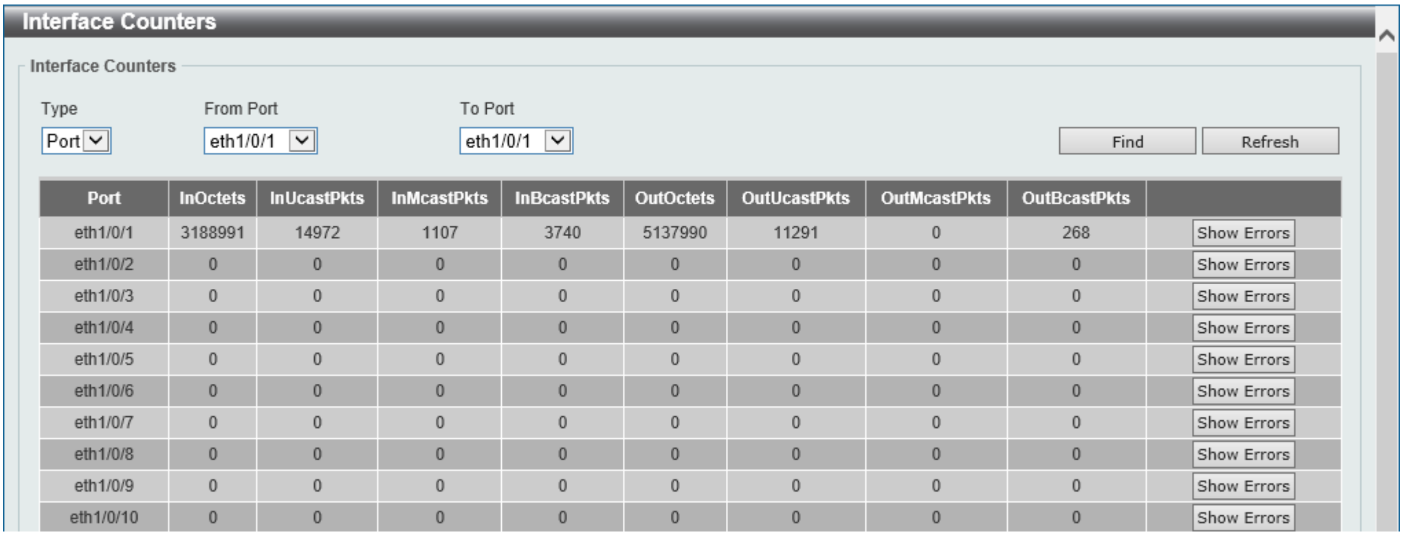
Click the **Back** button to return to the previous window.

Click the **Refresh** button to refresh the information displayed in the table.

Interface Counters

This window is used to view the interface counter information.

To view the following window, click **Monitoring > Statistics > Interface Counters**, as shown below:



Type: Port
From Port: eth1/0/1
To Port: eth1/0/1

Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts	
eth1/0/1	3188991	14972	1107	3740	5137990	11291	0	268	Show Errors
eth1/0/2	0	0	0	0	0	0	0	0	Show Errors
eth1/0/3	0	0	0	0	0	0	0	0	Show Errors
eth1/0/4	0	0	0	0	0	0	0	0	Show Errors
eth1/0/5	0	0	0	0	0	0	0	0	Show Errors
eth1/0/6	0	0	0	0	0	0	0	0	Show Errors
eth1/0/7	0	0	0	0	0	0	0	0	Show Errors
eth1/0/8	0	0	0	0	0	0	0	0	Show Errors
eth1/0/9	0	0	0	0	0	0	0	0	Show Errors
eth1/0/10	0	0	0	0	0	0	0	0	Show Errors

Figure 11-4 Interface Counters (Port) Window

The fields that can be configured are described below:

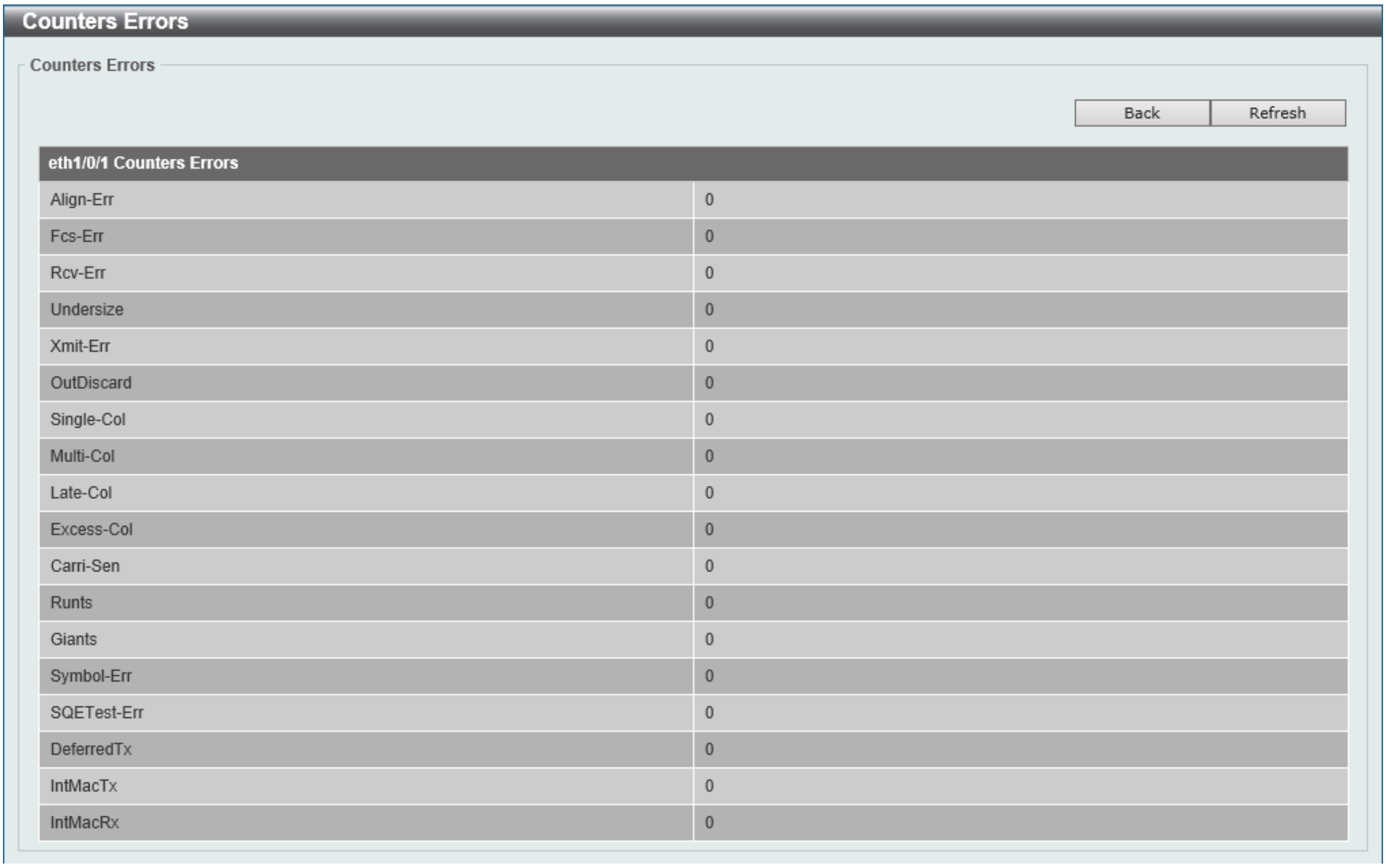
Parameter	Description
Type	Specifies that the type is **Port**.
From Port - To Port	Select the range of ports that will be used in this display here.

Click the **Find** button to display entries in the table based on the information selected.

Click the **Refresh** button to refresh the information displayed in the table.

Click the **Show Errors** button to view more detailed error information on the specified port.

After clicking the **Show Errors** button, the following window will appear:



eth1/0/1 Counters Errors	
Align-Err	0
Fcs-Err	0
Rcv-Err	0
Undersize	0
Xmit-Err	0
OutDiscard	0
Single-Col	0
Multi-Col	0
Late-Col	0
Excess-Col	0
Carri-Sen	0
Runts	0
Giants	0
Symbol-Err	0
SQETest-Err	0
DeferredTx	0
IntMacTx	0
IntMacRx	0

Figure 11-5 Interface Counters (Show Errors) Window

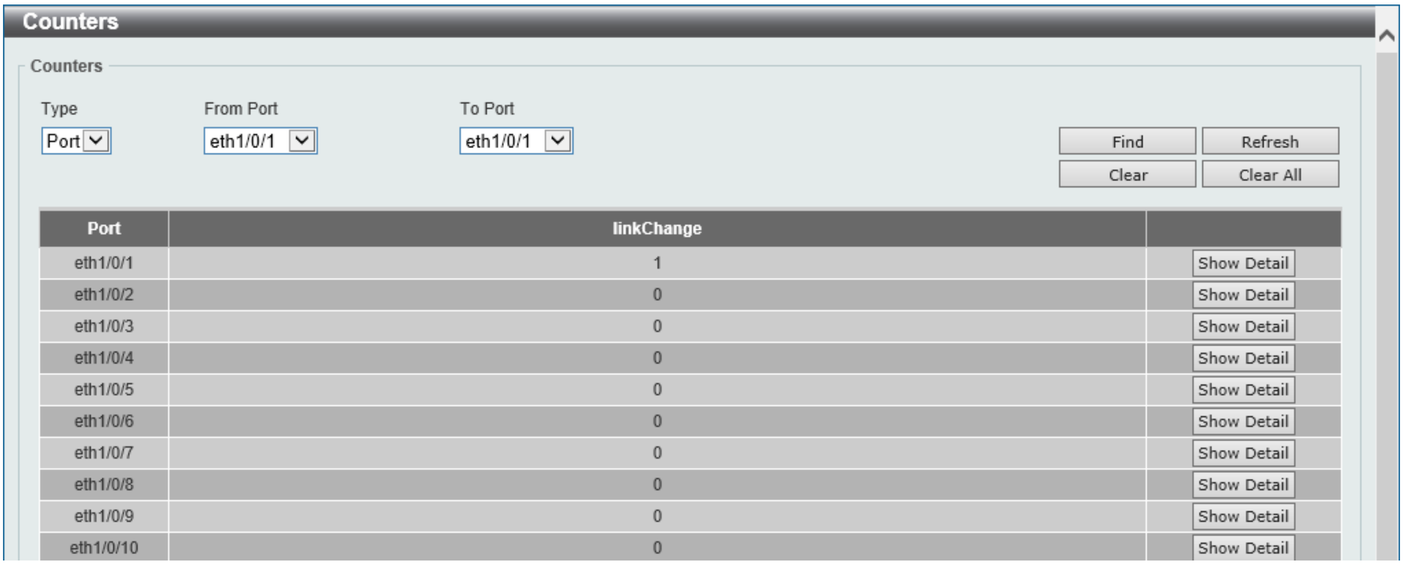
Click the **Back** button to return to the previous window.

Click the **Refresh** button to refresh the information displayed in the table.

Counters

This window is used to view and clear counter information.

To view the following window, click **Monitoring > Statistics > Counters**, as shown below:



Counters

Counters

Type: Port

From Port: eth1/0/1

To Port: eth1/0/1

Port	linkChange	
eth1/0/1	1	Show Detail
eth1/0/2	0	Show Detail
eth1/0/3	0	Show Detail
eth1/0/4	0	Show Detail
eth1/0/5	0	Show Detail
eth1/0/6	0	Show Detail
eth1/0/7	0	Show Detail
eth1/0/8	0	Show Detail
eth1/0/9	0	Show Detail
eth1/0/10	0	Show Detail

Figure 11-6 Counters (Port) Window

The fields that can be configured are described below:

Parameter	Description
Type	Specifies that the type is **Port**.
From Port - To Port	Select the range of ports that will be used in this display here.

Click the **Find** button to display entries in the table based on the information selected.

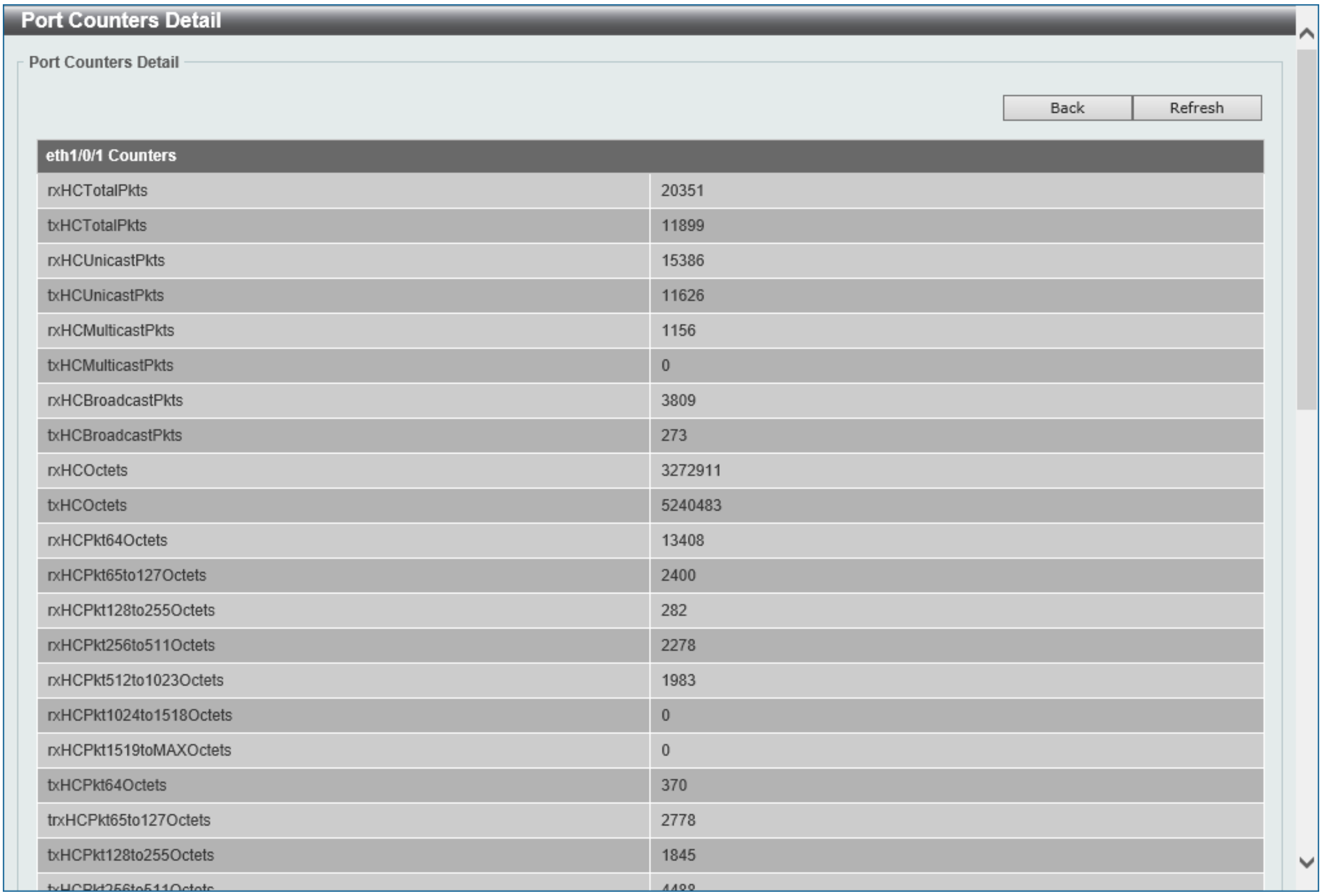
Click the **Refresh** button to refresh the counter information displayed in the table.

Click the **Clear** button clear the counter information displayed in the table based on the information selected.

Click the **Clear All** button clear all the counter information displayed in the table.

Click the **Show Detail** button to view detailed counter information on the specified port.

After clicking the **Show Detail** button, the following window will appear:



eth1/0/1 Counters	
rxHCTotalPkts	20351
txHCTotalPkts	11899
rxHCUnicastPkts	15386
txHCUnicastPkts	11626
rxHCMulticastPkts	1156
txHCMulticastPkts	0
rxHCBroadcastPkts	3809
txHCBroadcastPkts	273
rxHCOctets	3272911
txHCOctets	5240483
rxHCPkt64Octets	13408
rxHCPkt65to127Octets	2400
rxHCPkt128to255Octets	282
rxHCPkt256to511Octets	2278
rxHCPkt512to1023Octets	1983
rxHCPkt1024to1518Octets	0
rxHCPkt1519toMAXOctets	0
txHCPkt64Octets	370
trxHCPkt65to127Octets	2778
txHCPkt128to255Octets	1845
txHCPkt256to511Octets	4488

Figure 11-7 Counters (Show Detail) Window

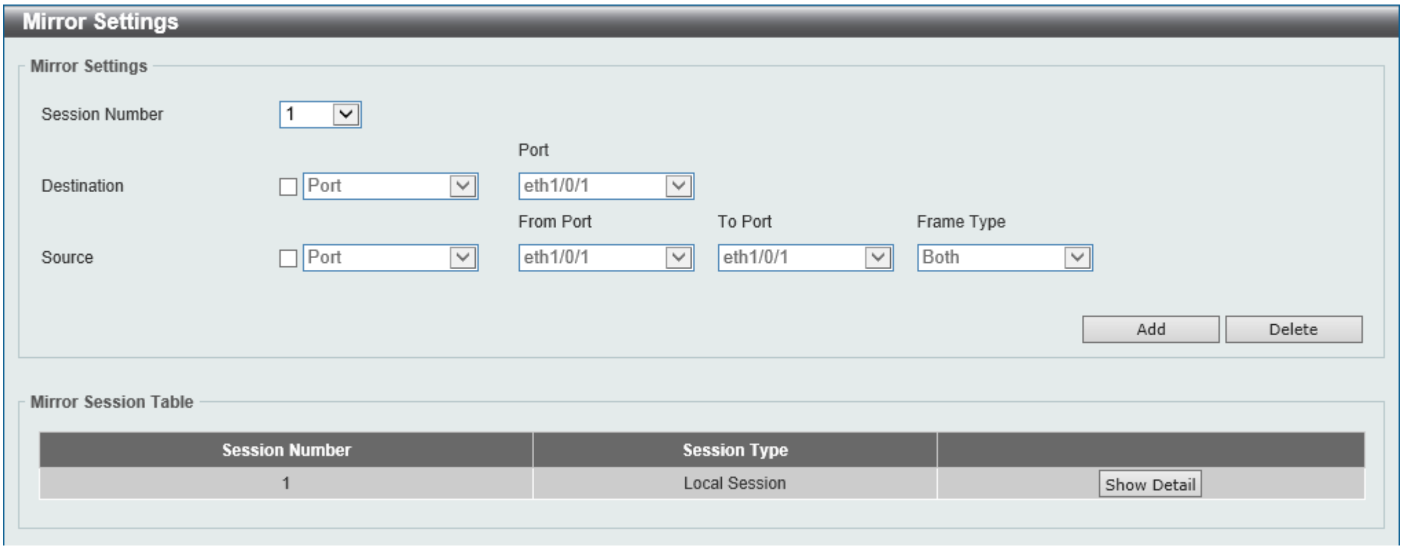
Click the **Back** button to return to the previous window.

Click the **Refresh** button to refresh the information displayed in the table.

Mirror Settings

This window is used to display and configure the mirror feature’s settings. The Switch allows users to copy frames transmitted and received on a port and redirect the copies to another port. Attach a monitoring device to the mirroring port, such as a sniffer or an RMON probe, to view details about the packets passing through the first port. This is useful for network monitoring and troubleshooting purposes.

To view the following window, click **Monitoring > Mirror Settings**, as shown below:



Mirror Settings

Mirror Settings

Session Number: 1

Destination: □ Port — Port: eth1/0/1

Source: □ Port — From Port: eth1/0/1 — To Port: eth1/0/1 — Frame Type: Both

Mirror Session Table

Session Number	Session Type	
1	Local Session	Show Detail

Figure 11-8 Mirror Settings Window

The fields that can be configured for **Mirror Settings** are described below:

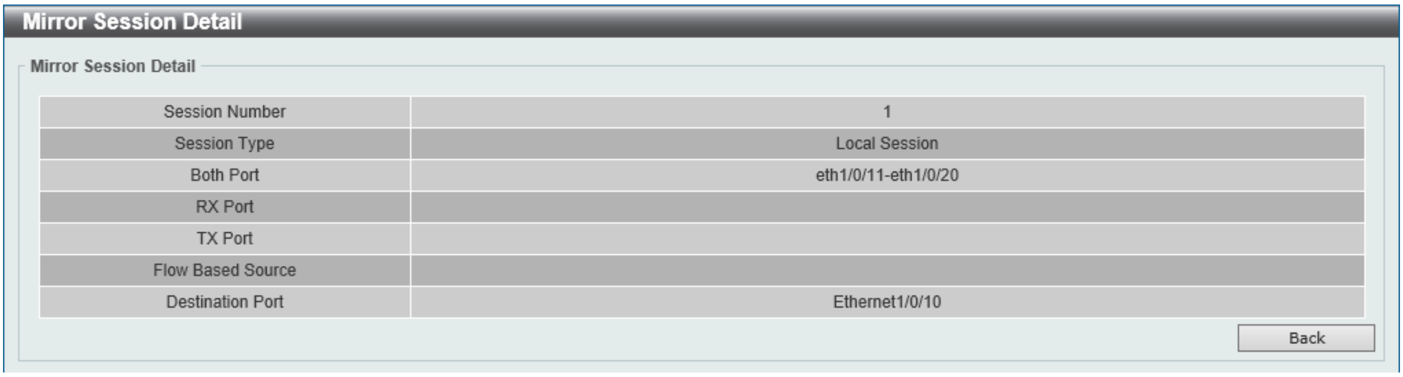
Parameter	Description
Session Number	Select the mirror session number for this entry here.
Destination	Tick the checkbox and select the destination port number here.
Source	Tick the checkbox and select the source for this port mirror entry. In the first drop-down menu, select the source type option. Options to choose from are: • **Port** - After selecting this option, select the **From Port** and **To Port** numbers from the drop-down menus. Lastly select the **Frame Type** option from the last drop-down menu. Options to choose from are: ○ **Both** - Specifies that traffic in both the incoming and outgoing directions will be mirrored. ○ **RX** - Specifies that traffic in only the incoming direction will be mirrored. ○ **TX** - Specifies that traffic in only the outgoing direction will be mirrored.

Click the **Add** button to add the newly configured mirror entry based on the information entered.

Click the **Delete** button to delete an existing mirror entry based on the information entered.

Click the **Show Detail** button to view detailed information about the mirror session.

After clicking the **Show Detail** button, the following window will appear:



Mirror Session Detail

Mirror Session Detail

Session Number	1
Session Type	Local Session
Both Port	eth1/0/11-eth1/0/20
RX Port	
TX Port	
Flow Based Source	
Destination Port	Ethernet1/0/10

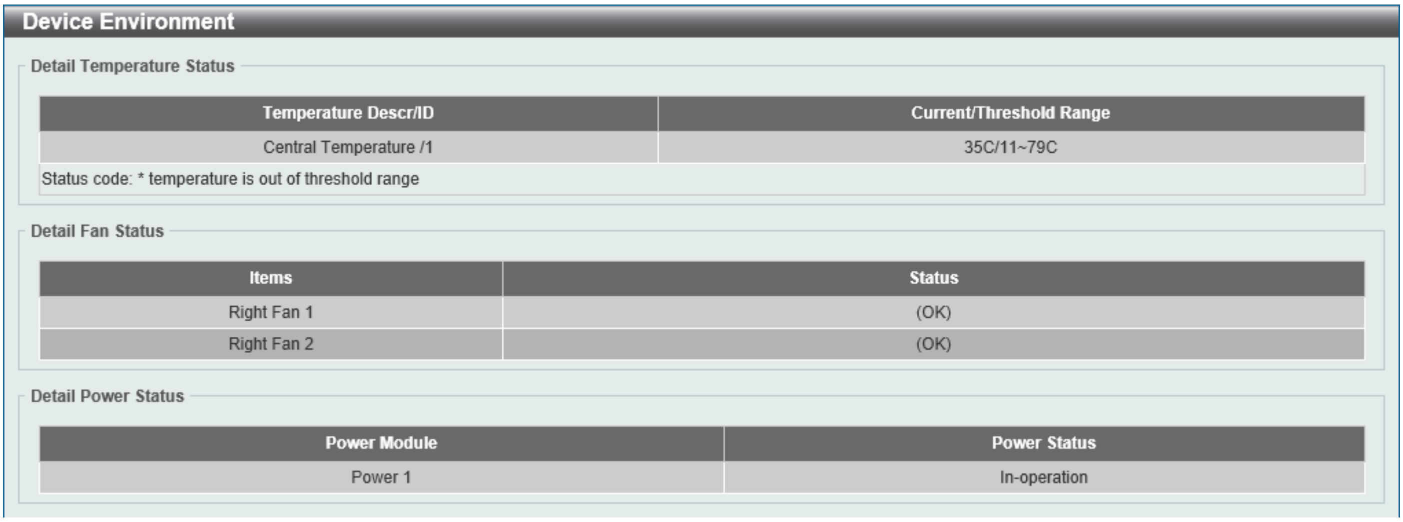
Figure 11-9 Mirror Settings (Show Detail) Window

Click the **Back** button to return to the previous page.

Device Environment

The device environment feature displays the Switch internal temperature status.

To view the following window, click **Monitoring > Device Environment**, as shown below:



Device Environment

Detail Temperature Status

Temperature Descr/ID	Current/Threshold Range
Central Temperature /1	35C/11~79C

Status code: * temperature is out of threshold range

Detail Fan Status

Items	Status
Right Fan 1	(OK)
Right Fan 2	(OK)

Detail Power Status

Power Module	Power Status
Power 1	In-operation

Figure 11-10 Device Environment Window

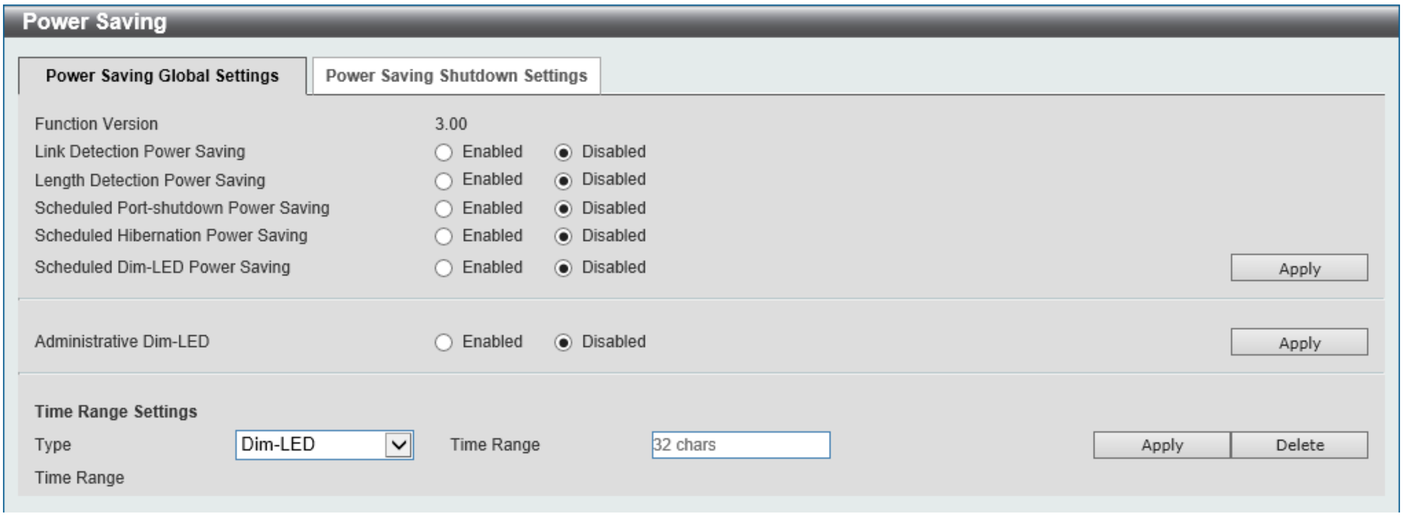
12. Green

Power Saving
EEE

Power Saving

This window is used to display and configure the power saving settings of the Switch.

To view the following window, click **Green > Power Saving**, as shown below:



Function Version 3.00
Link Detection Power Saving ○ Enabled ● Disabled
Length Detection Power Saving ○ Enabled ● Disabled
Scheduled Port-shutdown Power Saving ○ Enabled ● Disabled
Scheduled Hibernation Power Saving ○ Enabled ● Disabled
Scheduled Dim-LED Power Saving ○ Enabled ● Disabled

Administrative Dim-LED ○ Enabled ● Disabled

Time Range Settings
Type Dim-LED Time Range 32 chars
Time Range

Figure 12-1 Power Saving Global Settings Window

The fields that can be configured in **Power Saving Global Settings** are described below:

Parameter	Description
Link Detection Power Saving	Select to enable or disable the link detection power saving function here. When enabled, a port that has a link down status will be turned off to save power to the Switch. This will not affect the port's capabilities when the port status is link up.
Length Detection Power Saving	Select to enable or disable the cable length detection power saving function here. This feature will allow the Switch to automatically detect the cable length connected to the port and increase or reduce the required power to this port accordingly to save power.
Scheduled Port-shutdown Power Saving	Select to enable or disable the scheduled port-shutdown power saving function here.
Scheduled Hibernation Power Saving	Select to enable or disable the scheduled hibernation power saving function here.
Scheduled Dim-LED Power Saving	Select to enable or disable the scheduled dimming of LEDs to save power function here.
Administrative Dim-LED	Select this option to enable or disable the port LED function.

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

The fields that can be configured in **Time Range Settings** are described below:

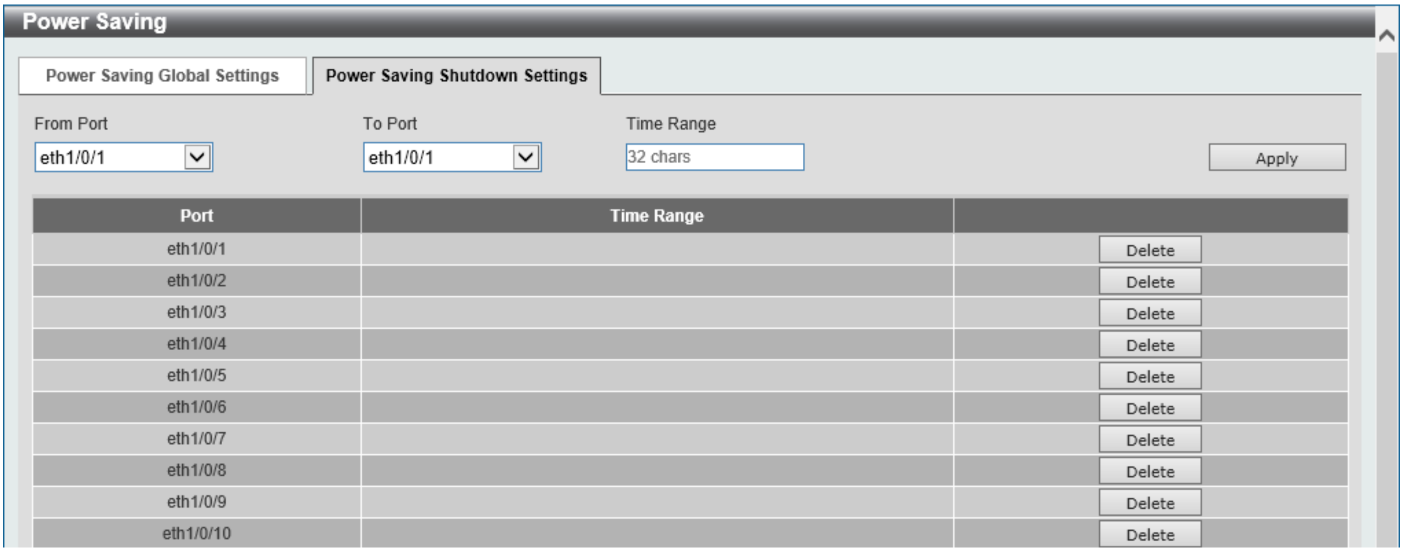
Parameter	Description
Type	Select the power saving type here. Options to choose from are: • **Dim-LED** - Specifies to add or delete a time range profile for the dim LED schedule. When the schedule is up, all the port LEDs are turned off.

Parameter	Description
	• **Hibernation** - Specifies to add or delete a time range profile for the system hibernation schedule. When the system enters the hibernation mode, the Switch goes into a low powered state and idle. It shuts down all the ports and LEDs, all network functions is disabled, and only the console connection works through the RS232 port. If the Switch is an endpoint PSE, power is not provided through the ports.
Time Range	Enter the name of the time range to associate with the power saving type.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Delete** button to remove the specified entry.

After clicking the **Power Saving Shutdown Settings** tab, the following page will appear.



From Port: eth1/0/1

To Port: eth1/0/1

Time Range: 32 chars

Port	Time Range	
eth1/0/1		Delete
eth1/0/2		Delete
eth1/0/3		Delete
eth1/0/4		Delete
eth1/0/5		Delete
eth1/0/6		Delete
eth1/0/7		Delete
eth1/0/8		Delete
eth1/0/9		Delete
eth1/0/10		Delete

Figure 12-2 Power Saving Shutdown Settings Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Time Range	Enter the name of the time range to associate with the ports.

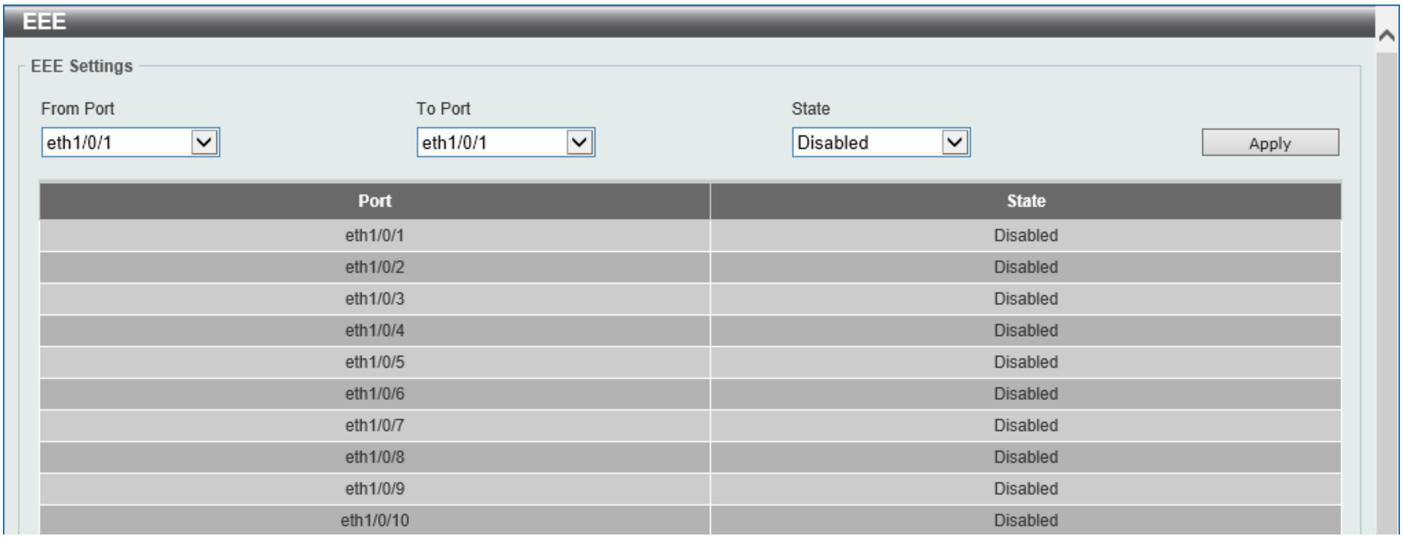
Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

EEE

Energy Efficient Ethernet (EEE) is defined in IEEE 802.3az. It is designed to reduce the energy consumption of a link when no packets are being sent.

To view the following window, click **Green > EEE**, as shown below:



EEE

EEE Settings

From Port: eth1/0/1

To Port: eth1/0/1

State: Disabled

Port	State
eth1/0/1	Disabled
eth1/0/2	Disabled
eth1/0/3	Disabled
eth1/0/4	Disabled
eth1/0/5	Disabled
eth1/0/6	Disabled
eth1/0/7	Disabled
eth1/0/8	Disabled
eth1/0/9	Disabled
eth1/0/10	Disabled

Figure 12-3 EEE Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select this option to enable or disable the state of this feature here.

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

13. Toolbar

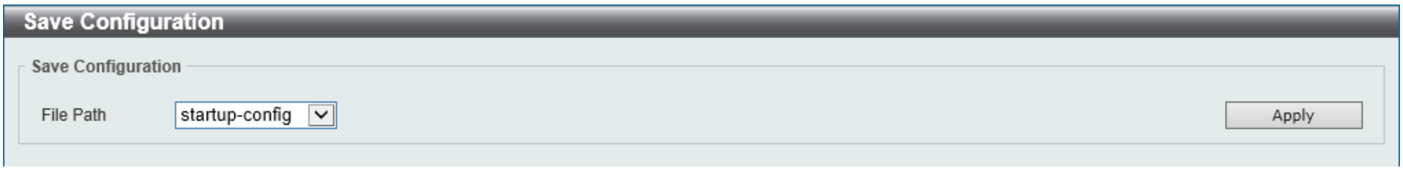
Save
Tools
Wizard
Online Help
Surveillance Mode
Logout

Save

Save Configuration

This window is used to save the running configuration to the start-up configuration. This is to prevent the loss of configuration in the event of a power failure.

To view the following window, click **Save > Save Configuration**, as shown below:



Save Configuration

Save Configuration

File Path: startup-config

Figure 13-1 Save Configuration Window

The fields that can be configured are described below:

Parameter	Description
File Path	Select the destination where the configuration will be saved here. Options to choose from are **startup-config**, **Configuration 1**, and **Configuration 2**.

Click the **Apply** button to save the configuration.

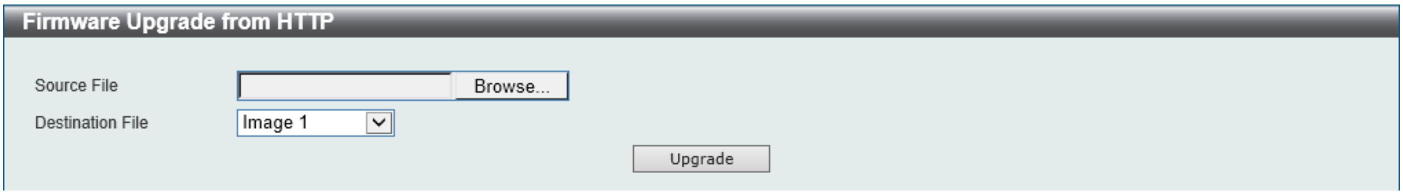
Tools

Firmware Upgrade & Backup

Firmware Upgrade from HTTP

This window is used to initiate a firmware upgrade from a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP**, as shown below:



Firmware Upgrade from HTTP

Source File:

Destination File: Image 1

Figure 13-2 Firmware Upgrade from HTTP Window

The fields that can be configured are described below:

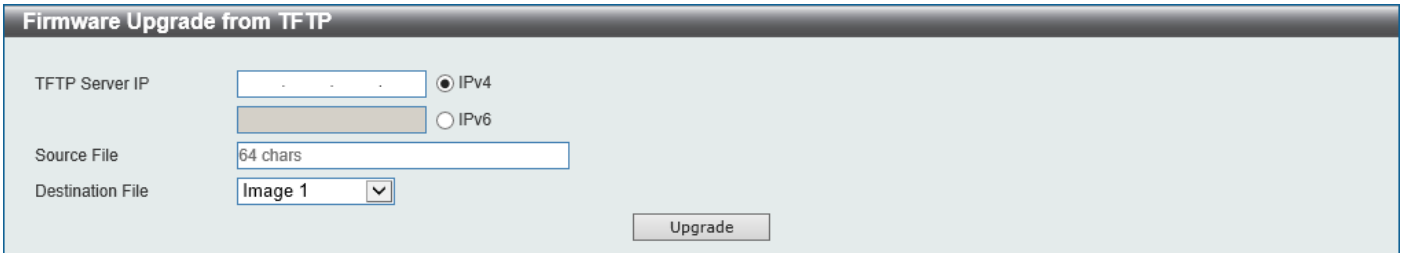
Parameter	Description
Source File	Click the **Browse** button and navigate to the firmware file on the local PC here. This file will be uploaded to the Switch.
Destination File	Select the destination where the firmware file will be saved on the Switch here. Options to choose from are **Image 1** and **Image 2**.

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Upgrade from TFTP

This window is used to initiate a firmware upgrade from a TFTP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from TFTP**, as shown below:



Firmware Upgrade from TFTP

TFTP Server IP: . . . ● IPv4 ○ IPv6

Source File: 64 chars

Destination File: Image 1

Figure 13-3 Firmware Upgrade from TFTP Window

The fields that can be configured are described below:

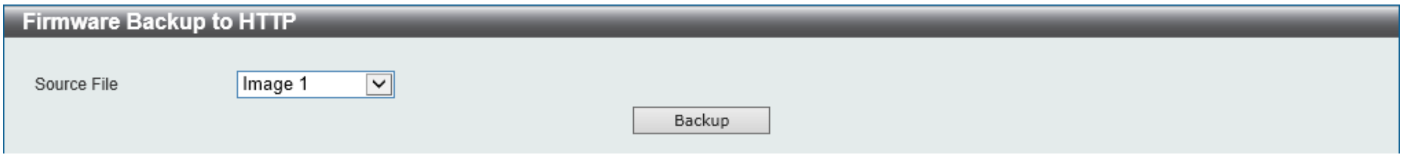
Parameter	Description
TFTP Server IP	Select and enter the IP address of the TFTP server here. • **IPv4** - Specifies to select and enter the IPv4 address of the TFTP server. • **IPv6** - Specifies to select and enter the IPv6 address of the TFTP server.
Source File	Enter the filename and path of the firmware file on the TFTP server here. This will be uploaded to the Switch. This field can be up to 64 characters long.
Destination File	Select the destination where the firmware file will be saved on the Switch here. Options to choose from are **Image 1** and **Image 2**.

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Backup to HTTP

This window is used to initiate a firmware backup to a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to HTTP**, as shown below:



Firmware Backup to HTTP

Source File: Image 1

Figure 13-4 Firmware Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source File	Select the firmware on the Switch that will be backed up to the local PC here. Options to choose from are **Image 1** and **Image 2**.

Click the **Backup** button to initiate the firmware backup.

Firmware Backup to TFTP

This window is used to initiate a firmware backup to a TFTP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to TFTP**, as shown below:

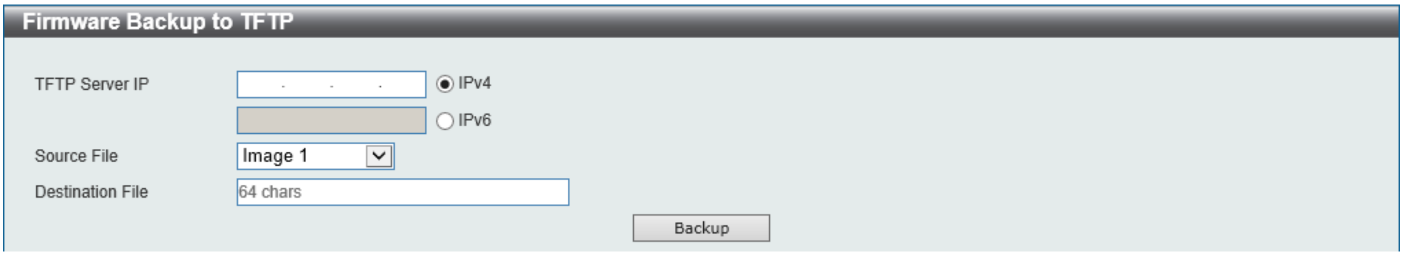


Figure 13-5 Firmware Backup to TFTP Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Select and enter the IP address of the TFTP server here. • **IPv4** - Specifies to select and enter the IPv4 address of the TFTP server. • **IPv6** - Specifies to select and enter the IPv6 address of the TFTP server.
Source File	Select the firmware file on the Switch that will be backed up to the TFTP server here. Options to choose from are **Image 1** and **Image 2**.
Destination File	Enter the filename and path of the firmware file that will be stored on the TFTP server here. This field can be up to 64 characters long.

Click the **Backup** button to initiate the firmware backup.

Configuration Restore & Backup

Configuration Restore from HTTP

This window is used to initiate a configuration restore from a local PC using HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from HTTP**, as shown below:

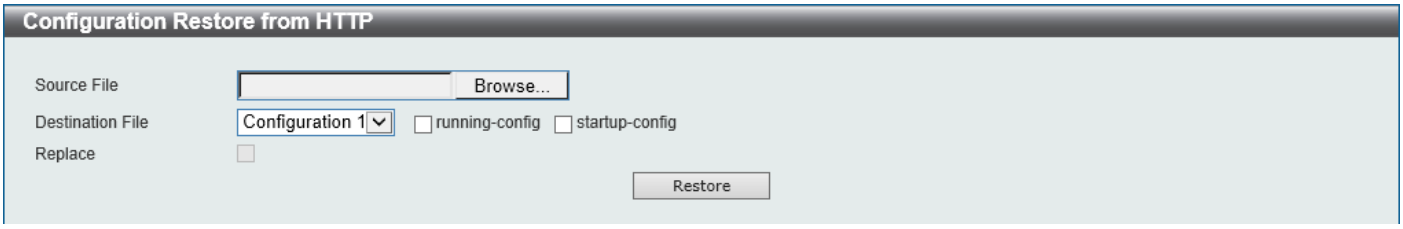


Figure 13-6 Configuration Restore from HTTP Window

The fields that can be configured are described below:

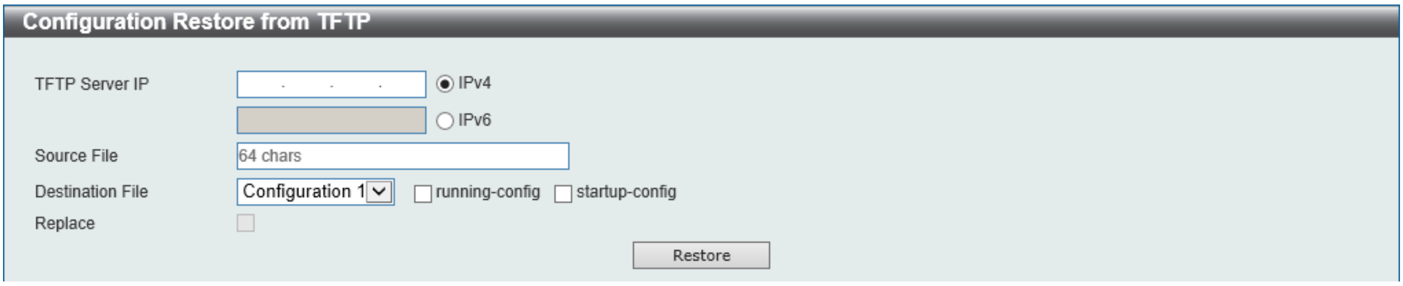
Parameter	Description
Source File	Click the **Browse** button and navigate to the configuration file on the local PC here. This file will be uploaded to the Switch.
Destination File	Select the destination for the configuration file on the Switch here. Options to choose from are: • **Configuration 1** - Select this option to use configuration 1 as the destination. • **Configuration 2** - Select this option to use configuration 2 as the destination. • **running-config** - Select this option to use the running configuration as the destination. • **startup-config** - Select this option to use the start-up configuration as the destination.
Replace	Select this option to replace the running configuration on the Switch with this one.

Click the **Restore** button to initiate the configuration restore.

Configuration Restore from TFTP

This window is used to initiate a configuration restore from a TFTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from TFTP**, as shown below:



Configuration Restore from TFTP

TFTP Server IP [. . .] ● IPv4
[ ] ○ IPv6

Source File [64 chars]

Destination File [Configuration 1 ▾] □ running-config □ startup-config

Replace □

Figure 13-7 Configuration Restore from TFTP Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Select and enter the IP address of the TFTP server here. • **IPv4** - Specifies to select and enter the IPv4 address of the TFTP server. • **IPv6** - Specifies to select and enter the IPv6 address of the TFTP server.
Source File	Enter the filename and path of the configuration file on the TFTP server here. This will be uploaded to the Switch. This field can be up to 64 characters long.
Destination File	Select the destination for the configuration file on the Switch here. Options to choose from are: • **Configuration 1** - Select this option to use configuration 1 as the destination. • **Configuration 2** - Select this option to use configuration 2 as the destination. • **running-config** - Select this option to use the running configuration as the destination. • **startup-config** - Select this option to use the start-up configuration as the destination.

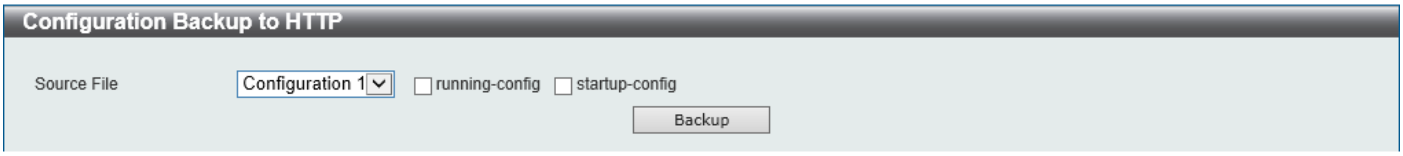
Parameter	Description
Replace	Select this option to replace the running configuration on the Switch with this one.

Click the **Restore** button to initiate the configuration restore.

Configuration Backup to HTTP

This window is used to initiate a configuration file backup to a local PC using HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to HTTP**, as shown below:



Configuration Backup to HTTP

Source File: Configuration 1 □ running-config □ startup-config

Figure 13-8 Configuration Backup to HTTP Window

The fields that can be configured are described below:

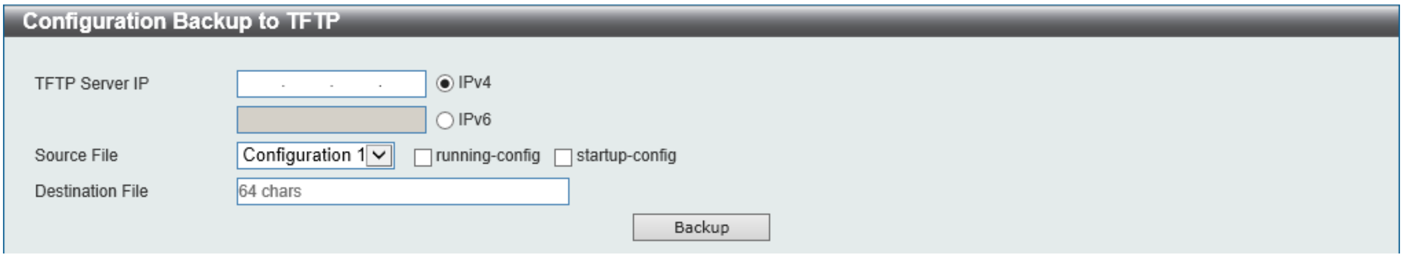
Parameter	Description
Source File	Select the configuration on the Switch that will be backed up to the local PC here. Options to choose from are: • **Configuration 1** - Select this option to backup configuration 1. • **Configuration 2** - Select this option to backup configuration 2. • **running-config** - Select this option to backup the running configuration. • **startup-config** - Select this option to backup the start-up configuration.

Click the **Backup** button to initiate the configuration file backup.

Configuration Backup to TFTP

This window is used to initiate a configuration file backup to a TFTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to TFTP**, as shown below:



Configuration Backup to TFTP

TFTP Server IP: . . . ● IPv4

○ IPv6

Source File: Configuration 1 □ running-config □ startup-config

Destination File: 64 chars

Figure 13-9 Configuration Backup to TFTP Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Select and enter the IP address of the TFTP server here. • **IPv4** - Specifies to select and enter the IPv4 address of the TFTP server. • **IPv6** - Specifies to select and enter the IPv6 address of the TFTP server.

Parameter	Description
Source File	Select the configuration on the Switch that will be backed up to the TFTP server here. Options to choose from are: • **Configuration 1** - Select this option to backup configuration 1. • **Configuration 2** - Select this option to backup configuration 2. • **running-config** - Select this option to backup the running configuration. • **startup-config** - Select this option to backup the start-up configuration.
Destination File	Enter the filename and path of the configuration file that will be stored on the TFTP server here. This field can be up to 64 characters long.

Click the **Backup** button to initiate the configuration file backup.

Certificate & Key Restore & Backup

Certificate & Key Restore from HTTP

This window is used to initiate a certificate and key restore from a local PC using HTTP.

To view the following window, click **Tools > Certificate & Key Restore & Backup > Certificate & Key Restore from HTTP**, as shown below:

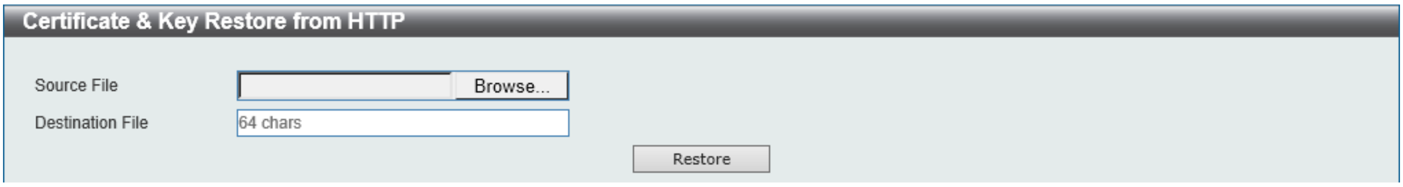


Figure 13-10 Certificate & Key Restore from HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source File	Click the **Browse** button and navigate to the certificate and key file on the local PC here. This will be uploaded to the Switch.
Destination File	Enter the filename and path of the certificate and key file that will be stored on the Switch here. This field can be up to 64 characters long.

Click the **Restore** button to initiate the certificate and key restore.

Certificate & Key Restore from TFTP

This window is used to initiate a certificate and key restore from a TFTP server.

To view the following window, click **Tools > Certificate & Key Restore & Backup > Certificate & Key Restore from TFTP**, as shown below:

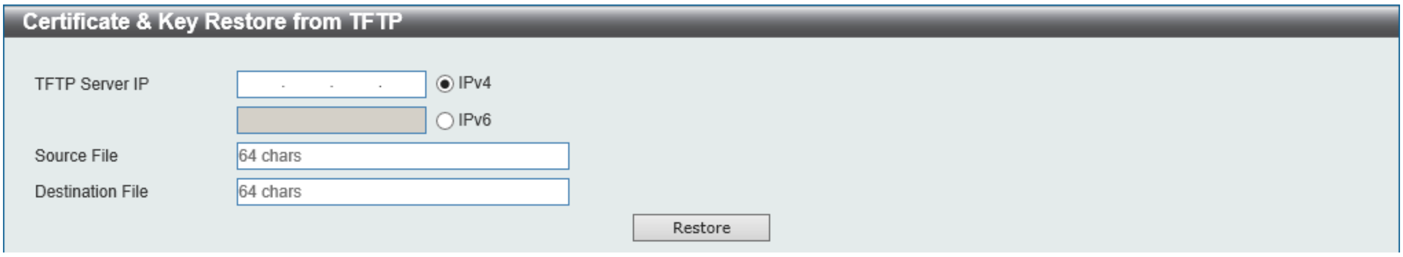


Figure 13-11 Certificate & Key Restore from TFTP Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Select and enter the IP address of the TFTP server here. • **IPv4** - Specifies to select and enter the IPv4 address of the TFTP server. • **IPv6** - Specifies to select and enter the IPv6 address of the TFTP server.
Source File	Enter the filename and path of the certificate and key file on the TFTP server here. This will be uploaded to the Switch. This field can be up to 64 characters long.
Destination File	Enter the filename and path of the certificate and key file that will be stored on the Switch here. This field can be up to 64 characters long.

Click the **Restore** button to initiate the certificate and key restore.

Public Key Backup to HTTP

This window is used to initiate a certificate and key backup to a local PC using HTTP.

To view the following window, click **Tools > Certificate & Key Upgrade & Backup > Public Key Backup to HTTP**, as shown below:

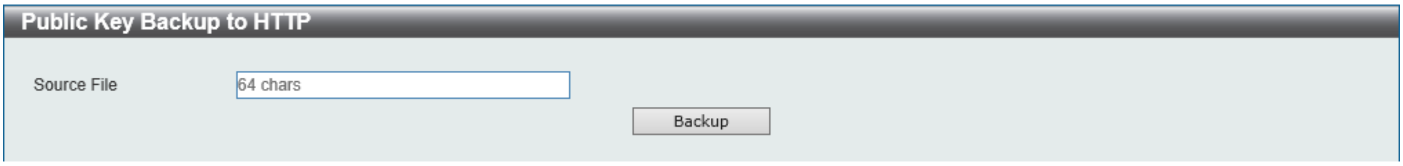


Figure 13-12 Public Key Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source File	Enter the filename and path of the certificate and key file on the Switch here. This will be downloaded to the local PC using HTTP. This field can be up to 64 characters long.

Click the **Backup** button to initiate the certificate and key backup.

Public Key Backup to TFTP

This window is used to initiate a certificate and key backup to a TFTP server.

To view the following window, click **Tools > Certificate & Key Upgrade & Backup > Public Key Backup to TFTP**, as shown below:

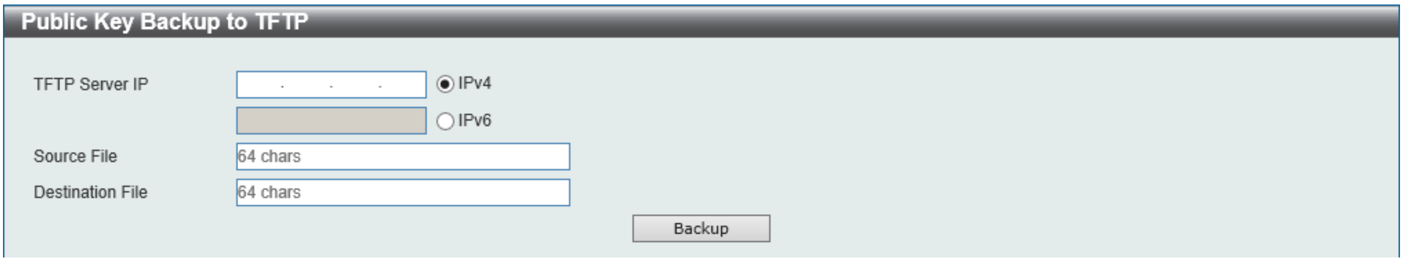


Figure 13-13 Public Key Backup to TFTP Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Select and enter the IP address of the TFTP server here. • **IPv4** - Specifies to select and enter the IPv4 address of the TFTP server. • **IPv6** - Specifies to select and enter the IPv6 address of the TFTP server.
Source File	Enter the filename and path of the certificate and key file on the Switch here. This will be downloaded to the TFTP server. This field can be up to 64 characters long.
Destination File	Enter the filename and path of the certificate and key file that will be stored on the TFTP sever here. This field can be up to 64 characters long.

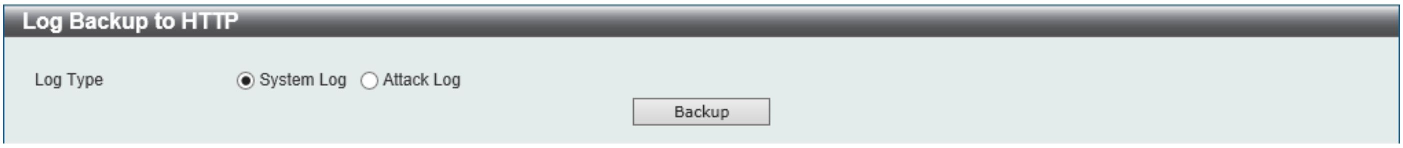
Click the **Backup** button to initiate the certificate and key backup.

Log Backup

Log Backup to HTTP

This window is used to initiate a system log backup to a local PC using HTTP.

To view the following window, click **Tools > Log Backup > Log Backup to HTTP**, as shown below:



Log Type ● System Log ○ Attack Log

Figure 13-14 Log Backup to HTTP Window

The fields that can be configured are described below:

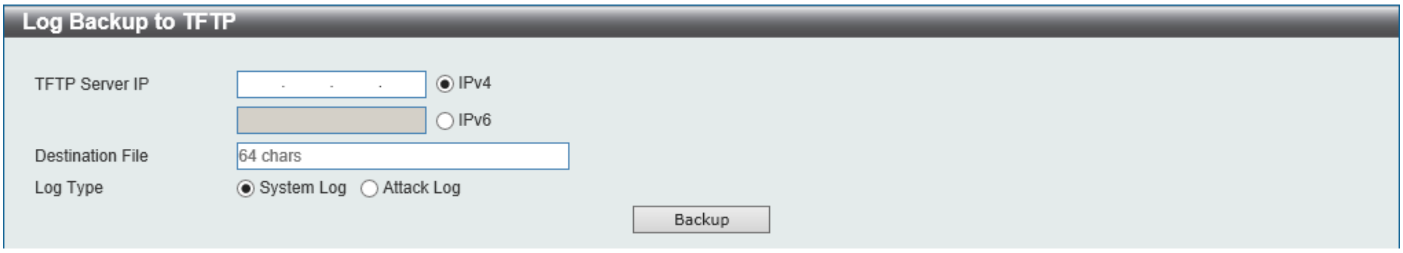
Parameter	Description
Log Type	Select the log type on the Switch that will be backed up to the local PC here. Options to choose from are **System Log** and **Attack Log**.

Click the **Backup** button to initiate the system log backup.

Log Backup to TFTP

This window is used to initiate a system log backup to a TFTP server.

To view the following window, click **Tools > Log Backup > Log Backup to TFTP**, as shown below:



TFTP Server IP . . . ● IPv4
○ IPv6
Destination File 64 chars
Log Type ● System Log ○ Attack Log

Figure 13-15 Log Backup to TFTP Window

The fields that can be configured are described below:

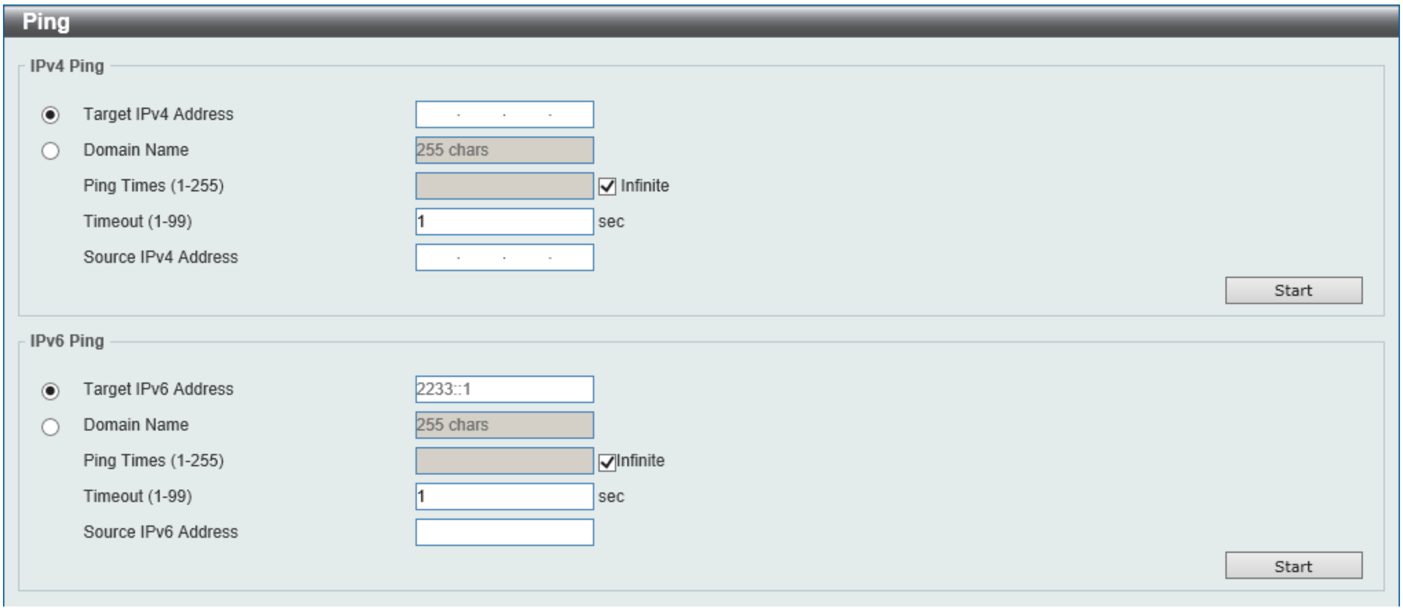
Parameter	Description
TFTP Server IP	Select and enter the IP address of the TFTP server here. • **IPv4** - Specifies to select and enter the IPv4 address of the TFTP server. • **IPv6** - Specifies to select and enter the IPv6 address of the TFTP server.
Destination File	Enter the filename and path of the log file that will be stored on the TFTP sever here. This field can be up to 64 characters long.
Log Type	Select the log type on the Switch that will be backed up to the TFTP server here. Options to choose from are **System Log** and **Attack Log**.

Click the **Backup** button to initiate the system log backup.

Ping

Ping is a small program that sends ICMP Echo packets to the IP address you specify. The destination node then responds to or "echoes" the packets sent from the Switch. This is very useful to verify connectivity between the Switch and other nodes on the network.

To view the following window, click **Tools > Ping**, as shown below:



Ping

IPv4 Ping

● Target IPv4 Address: . . .
○ Domain Name: 255 chars
Ping Times (1-255): ☑ Infinite
Timeout (1-99): 1 sec
Source IPv4 Address: . . .

Start

IPv6 Ping

● Target IPv6 Address: 2233::1
○ Domain Name: 255 chars
Ping Times (1-255): ☑ Infinite
Timeout (1-99): 1 sec
Source IPv6 Address:

Start

Figure 13-16 Ping Window

The fields that can be configured in **IPv4 Ping** are described below:

Parameter	Description
Target IPv4 Address	Select and enter an IP address to be pinged.
Domain Name	Select and enter the domain name of the system to discover.
Ping Times	Enter the number of times desired to attempt to Ping the IPv4 address configured in this window. Users may enter a number of times between 1 and 255. Tick the **Infinite** check box to keep sending ICMP Echo packets to the specified IP address until the program is stopped.
Timeout	Select a timeout period between 1 and 99 seconds for this Ping message to reach its destination. If the packet fails to find the IP address in this specified time, the Ping packet will be dropped.
Source IPv4 Address	Enter the source IPv4 address. If the current Switch has more than one IP address, you can enter one of them to this field. When entered, this IPv4 address

Parameter	Description
	will be used as the packets' source IP address sent to the remote host, or as primary IP address.

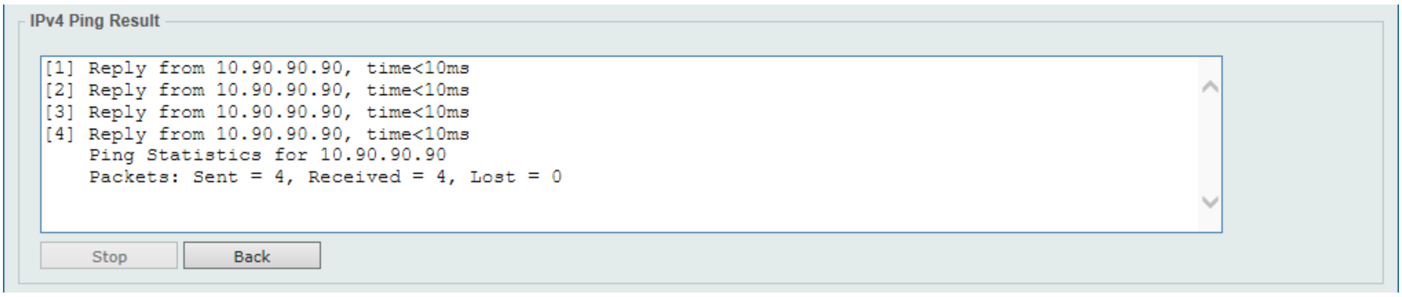
Click the **Start** button to initiate the Ping Test for each individual section.

The fields that can be configured in **IPv6 Ping** are described below:

Parameter	Description
Target IPv6 Address	Enter an IPv6 address to be pinged.
Domain Name	Select and enter the domain name of the system to discover.
Ping Times	Enter the number of times desired to attempt to Ping the IPv6 address configured in this window. Users may enter a number of times between 1 and 255. Tick the **Infinite** check box to keep sending ICMPv6 Echo packets to the specified IPv6 address until the program is stopped.
Timeout	Select a timeout period between 1 and 99 seconds for this Ping message to reach its destination. If the packet fails to find the IPv6 address in this specified time, the Ping packet will be dropped.
Source IPv6 Address	Enter the source IPv6 address. If the current Switch has more than one IPv6 address, you can enter one of them to this field. When entered, this IPv6 address will be used as the packets' source IPv6 address sent to the remote host, or as primary IPv6 address.

Click the **Start** button to initiate the Ping Test for each individual section.

After clicking the **Start** button in **IPv4 Ping** section, the following **IPv4 Ping Result** section will appear:



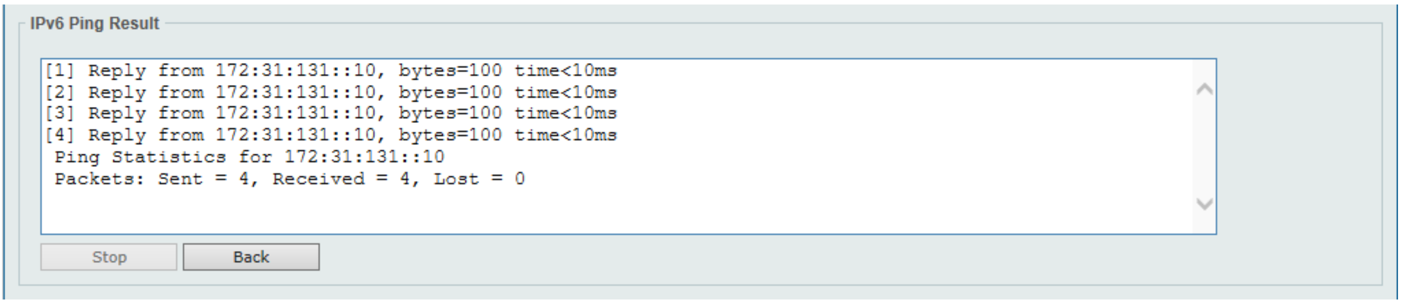
```
[1] Reply from 10.90.90.90, time<10ms
[2] Reply from 10.90.90.90, time<10ms
[3] Reply from 10.90.90.90, time<10ms
[4] Reply from 10.90.90.90, time<10ms
    Ping Statistics for 10.90.90.90
    Packets: Sent = 4, Received = 4, Lost = 0
```

Figure 13-17 IPv4 Ping (Start) Window

Click the **Stop** button to halt the Ping Test.

Click the **Back** button to return to the IPv4 Ping section.

After clicking the **Start** button in **IPv6 Ping** section, the following **IPv6 Ping Result** section will appear:



```
[1] Reply from 172:31:131::10, bytes=100 time<10ms
[2] Reply from 172:31:131::10, bytes=100 time<10ms
[3] Reply from 172:31:131::10, bytes=100 time<10ms
[4] Reply from 172:31:131::10, bytes=100 time<10ms
 Ping Statistics for 172:31:131::10
 Packets: Sent = 4, Received = 4, Lost = 0
```

Figure 13-18 IPv6 Ping (Start) Window

Click the **Stop** button to halt the Ping Test.

Click the **Back** button to return to the IPv6 Ping section.

Language Management

This window is used to install the language file to the Switch.

To view the following window, click **Tools > Language Management**, as shown below:

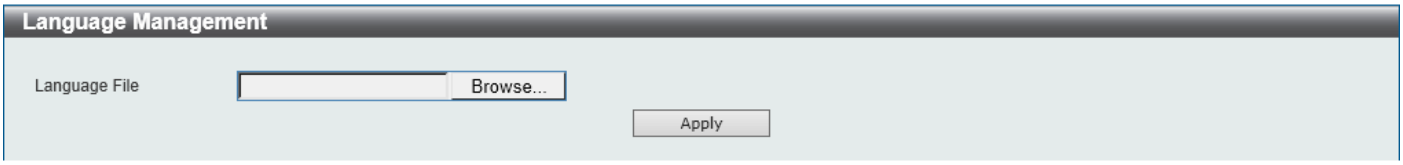


Figure 13-19 Language Management Window

The fields that can be configured are described below:

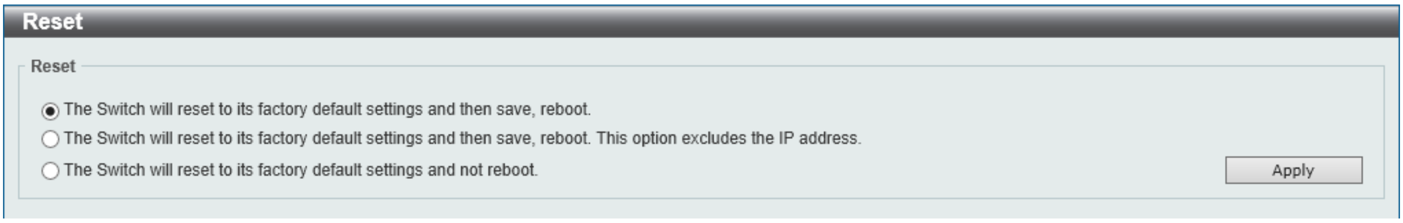
Parameter	Description
Language File	Click the **Browse** button and navigate to the language pack file on the local PC here. This file will be uploaded to the Switch.

Click the **Apply** button to initiate the language pack upload and installation.

Reset

This window is used to reset the Switch's configuration to the factory default settings.

To view the following window, click **Tools > Reset**, as shown below:



● The Switch will reset to its factory default settings and then save, reboot.

○ The Switch will reset to its factory default settings and then save, reboot. This option excludes the IP address.

○ The Switch will reset to its factory default settings and not reboot.

Figure 13-20 Reset Window

Select one of the following options:

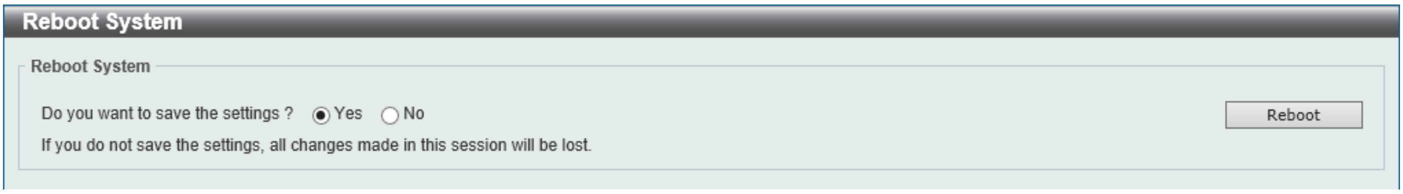
- The Switch will reset to its factory default settings and then save, reboot.
- The Switch will reset to its factory default settings and then save, reboot. This option excludes the IP address.
- The Switch will reset to its factory default settings and not reboot.

Click the **Apply** button to initiate the reset.

Reboot System

This window is used to reboot the Switch and alternatively save the configuration before doing so.

To view the following window, click **Tools > Reboot System**, as shown below:



Reboot System

Reboot System

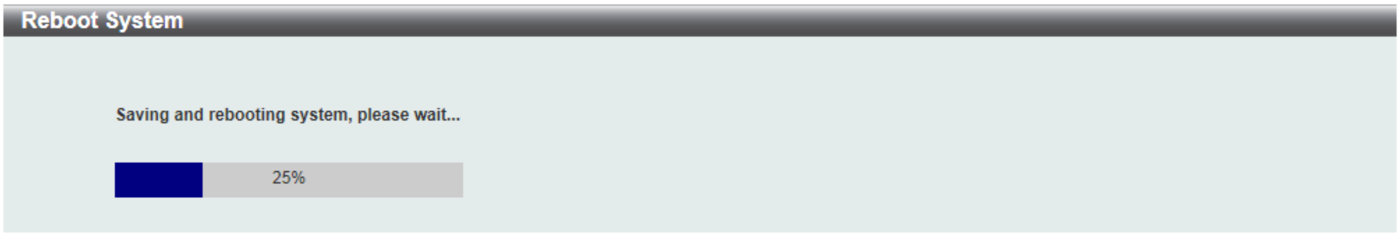
Do you want to save the settings ? ● Yes ○ No

If you do not save the settings, all changes made in this session will be lost.

Figure 13-21 Reboot System Window

When rebooting the Switch, any configuration changes that was made during this session, will be lost unless the **Yes** option is selected when asked to save the settings.

Click the **Reboot** button to alternatively save the settings and reboot the Switch.



Reboot System

Saving and rebooting system, please wait...

Figure 13-22 Reboot System (Rebooting) Window

Wizard

Click this option to start the Smart Wizard. For more information about the Smart Wizard, refer to **Smart Wizard** on page 5.

Online Help

D-Link Support Site

Click this option to connect to the D-Link support website. An Internet connection is required.

User Guide

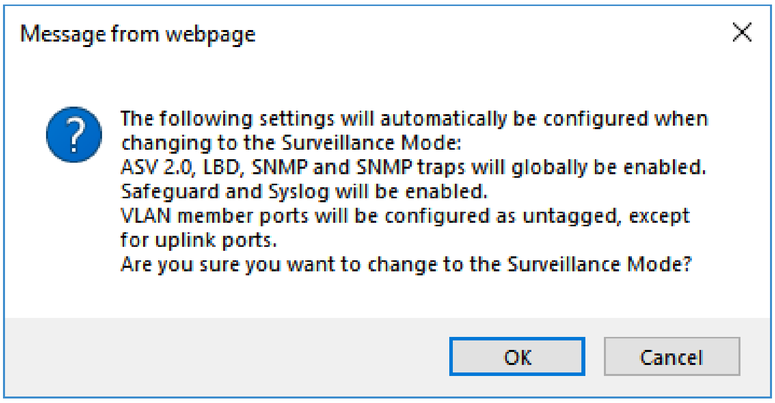
Click this option to connect to the online user guide for the Switch. An Internet connection is required.

Surveillance Mode

Click this option to change the Web UI mode and style from the **Standard Mode** to the **Surveillance Mode**. An unsuccessful change will display a warning message.

NOTE: All active Web UI user sessions can only access the same Web UI mode at the same time. The mode can only be changed when one user session is active. The mode cannot be changed when another user session is connected to the Web UI.

After clicking the **Surveillance Mode** option in the **Toolbar**, the following window will appear.



Message from webpage

The following settings will automatically be configured when changing to the Surveillance Mode:
ASV 2.0, LBD, SNMP and SNMP traps will globally be enabled.
Safeguard and Syslog will be enabled.
VLAN member ports will be configured as untagged, except for uplink ports.
Are you sure you want to change to the Surveillance Mode?

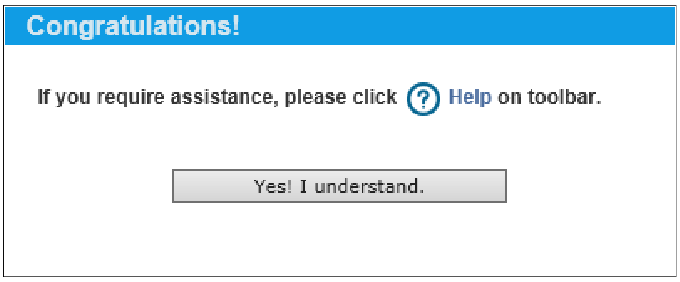
Figure 13-23 Surveillance Mode Confirmation Message

The window above displays a message that the abovementioned configurations need to be changed when access to the Surveillance Mode is given.

Click the **OK** button to continue.

Click the **Cancel** button to return to the **Standard Mode**.

After successfully switching to the Surveillance Mode on the Web UI of the Switch, the following window will appear.



Congratulations!

If you require assistance, please click ? Help on toolbar.

Figure 13-24 Surveillance Mode 'Congratulations' Message

Click the **Yes! I understand** button to continue.

Logout

Click this option to log out of the Web UI of the Switch

14. Surveillance Mode

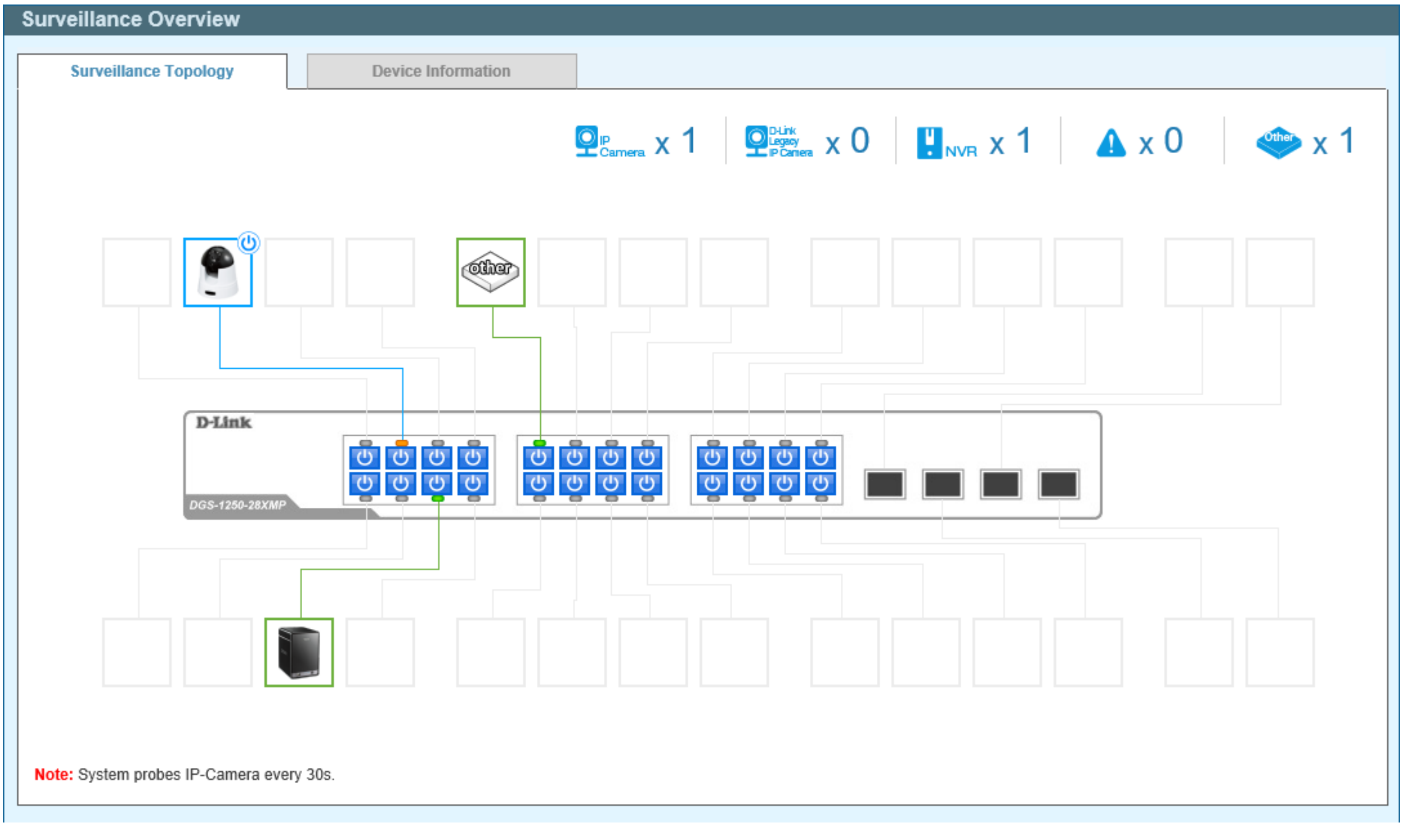
Surveillance Overview

In this window, the **Surveillance Topology** and **Device Information** are displayed. It appears automatically when you access the Surveillance Mode in the Web UI of the Switch.

Surveillance Topology

This window provides more information about what is connected to each port. Hover with the mouse pointer over each device icon to get more information about the recognized device (such as the number of devices, device type, IP address, power consumption, link speed, and errors).

To return to the Surveillance Overview window after viewing other windows, click the **DGS-1250-28XMP** link.



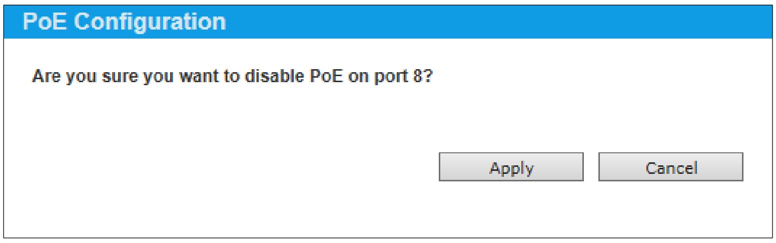
Note: System probes IP-Camera every 30s.

Figure 14-1 Surveillance Overview Window

The following icons are available in this window and are described below:

Icon	Description
IP Camera x 1	This displays the total amount of ONVIF IP cameras connected to the Ethernet ports on the Switch.
D-Link Legacy IP Camera x 0	This displays the total amount of D-Link legacy IP cameras (detected by ASV 1.0) connected to the Ethernet ports on the Switch.
NVR x 1	This displays the total amount of Network Video Recorders (NVRs) connected to the Ethernet ports on the Switch.
⚠ x 0	This displays the amount of surveillance warnings generated on the Switch.
Other x 1	This displays the amount of other devices connected to the Ethernet ports on the Switch.
	This displays the device connected to the Ethernet port on the Switch. The green border around the image indicates that the device is a non-PoE device.
	This displays the device connected to the Ethernet port on the Switch. The blue border around the image indicates that the device is a PoE device and is receiving power from the Switch using PoE. The PD Alive function can be used on this device.
⏻	Click this icon to disable PoE on the port.
⏻	Click this icon to enable PoE on the port.

After clicking the ⏻ icon, the following window will appear:

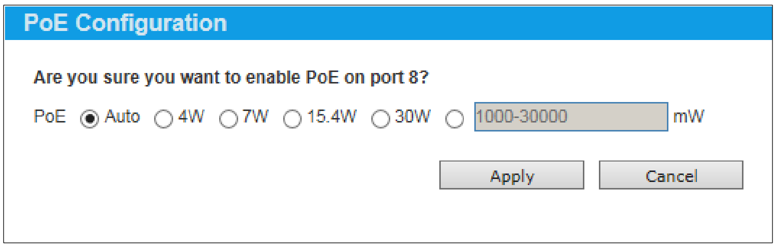


PoE Configuration

Are you sure you want to disable PoE on port 8?

Figure 14-2 PoE Configuration (To Disable) Window

After clicking the ⏻ icon, the following window will appear:



PoE Configuration

Are you sure you want to enable PoE on port 8?

PoE ● Auto ○ 4W ○ 7W ○ 15.4W ○ 30W ○ 1000-30000 mW

Figure 14-2 PoE Configuration (To Enable) Window

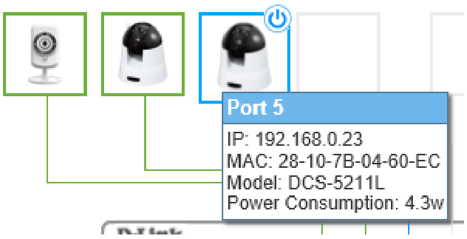
The fields that can be configured are described below:

Parameter	Description
PoE	Select the maximum power that will be supplied on the PoE port. Options to choose from are **Auto**, **4W**, **7W**, **15.4W**, **30W**, and a configurable value from 1000 mW to 30000 mW. The unit is either in watt or milliwatt.

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

Click the **Cancel** button to discard the changes made.

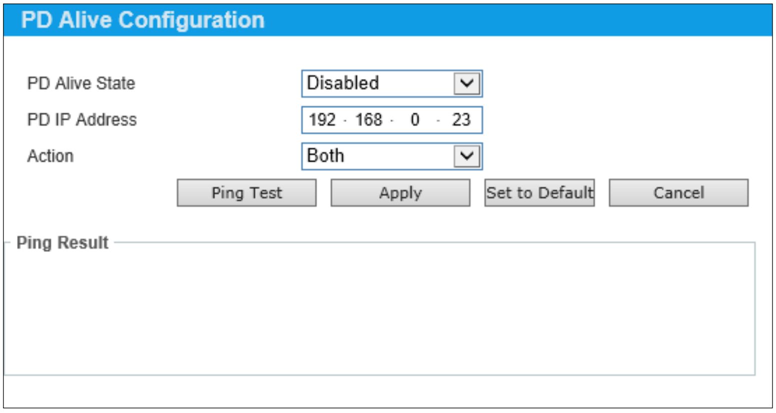
After hovering (with the mouse pointer) over the network device icon, the following additional information will be displayed:



Port 5
IP: 192.168.0.23
MAC: 28-10-7B-04-60-EC
Model: DCS-5211L
Power Consumption: 4.3w

Figure 14-2 Additional Device Information

After clicking (left-click) the network device icon, the following window will appear.



PD Alive Configuration

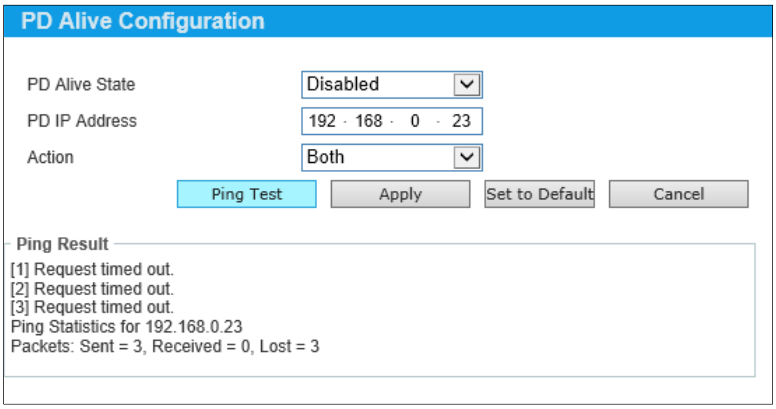
PD Alive State: Disabled
PD IP Address: 192 . 168 . 0 . 23
Action: Both

Figure 14-2 PD Alive Configuration Window

The fields that can be configured are described below:

Parameter	Description
PD Alive State	Select to enable or disable the PD Alive function here.
PD IP Address	Enter the IP address of the PD here.
Action	Select the action that will be taken here. Options to choose from are: • **Reset** - Specifies to reset the PoE port state (turn PoE off and on). • **Notify** - Specifies to send logs and traps to notify the administrator. • **Both** - Specifies to send logs and traps to notify the administrator and to reset the PoE port state (turn PoE off and on).

After clicking **Ping Test** button, the following window will appear.



PD Alive Configuration

PD Alive State: Disabled
PD IP Address: 192 . 168 . 0 . 23
Action: Both

Ping Result

```
[1] Request timed out.
[2] Request timed out.
[3] Request timed out.
Ping Statistics for 192.168.0.23
Packets: Sent = 3, Received = 0, Lost = 3
```

Figure 14-2 PD Alive Configuration Window (Ping Result)

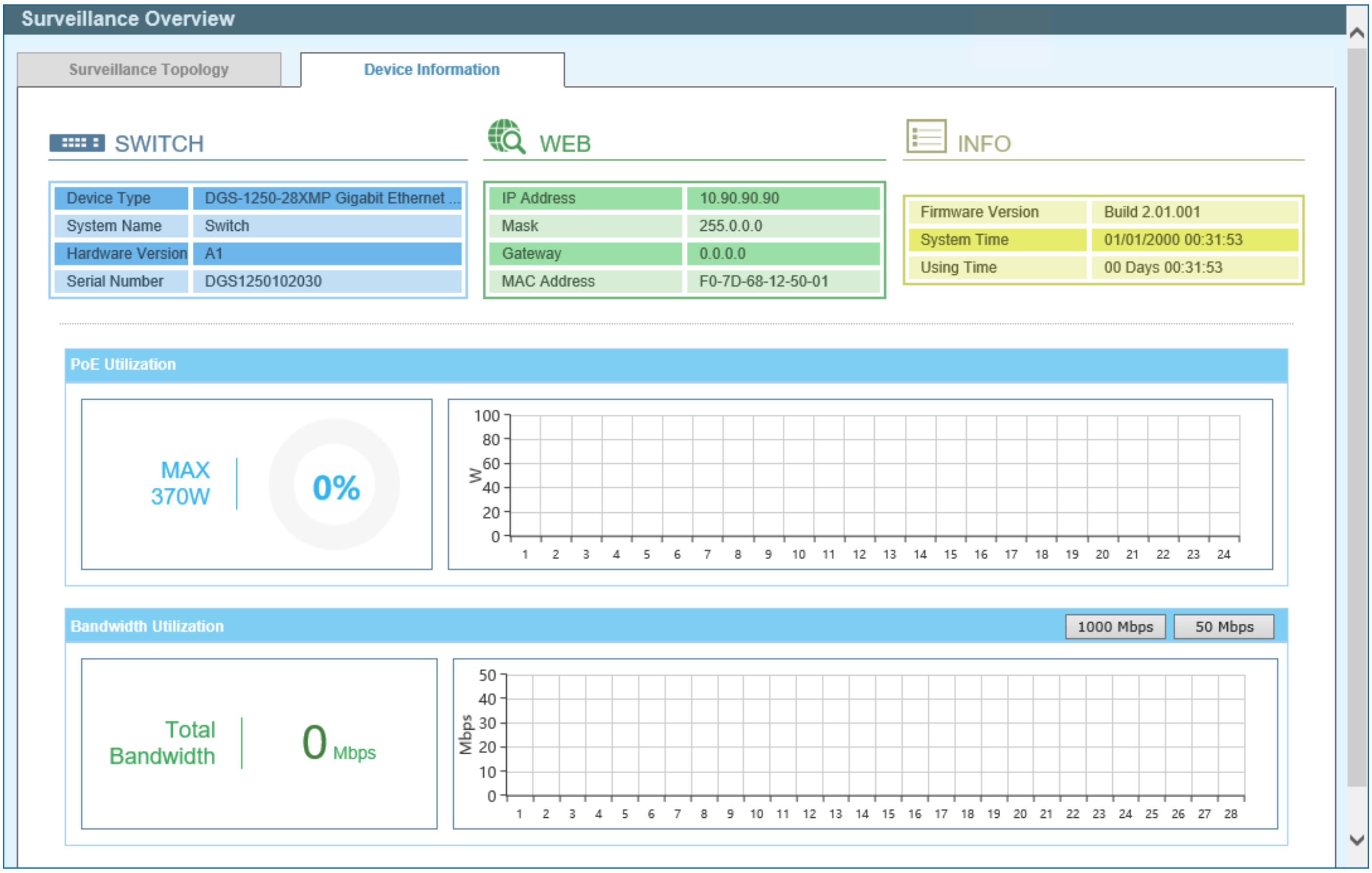
The **Ping Result** will be displayed.

NOTE: A breakdown of the device icons can be found by clicking the **Help** menu in the toolbar.

NOTE: The Switch uses ONVIF traffic to monitor the status of the surveillance device, but some third party devices do not fully comply with the ONVIF standard. If you are having problems with surveillance devices not being detected, please check ONVIF compatibility with the manufacturer of the original surveillance device.

Device Information

After clicking the **Device Information** tab, the following window will appear.



Surveillance Overview

SWITCH

Device Type	DGS-1250-28XMP Gigabit Ethernet ...
System Name	Switch
Hardware Version	A1
Serial Number	DGS1250102030

WEB

IP Address	10.90.90.90
Mask	255.0.0.0
Gateway	0.0.0.0
MAC Address	F0-7D-68-12-50-01

INFO

Firmware Version	Build 2.01.001
System Time	01/01/2000 00:31:53
Using Time	00 Days 00:31:53

Figure 14-6 Device Information Window

Click the **1000 Mbps** button to change the maximum bandwidth displayed in the **Bandwidth Utilization** chart to 1 Gbps.

Click the **50 Mbps** button to change the maximum bandwidth displayed in the **Bandwidth Utilization** chart to 50 Mbps.

Port Information

This window is used to display port information like throughput, distance of the network cable, PoE provisioning status, power consumption; loopback detection status, group, and how many IP cameras, NVRs, and other devices are connected to the ports.

To view the following window, click **Port Information**, as shown below:

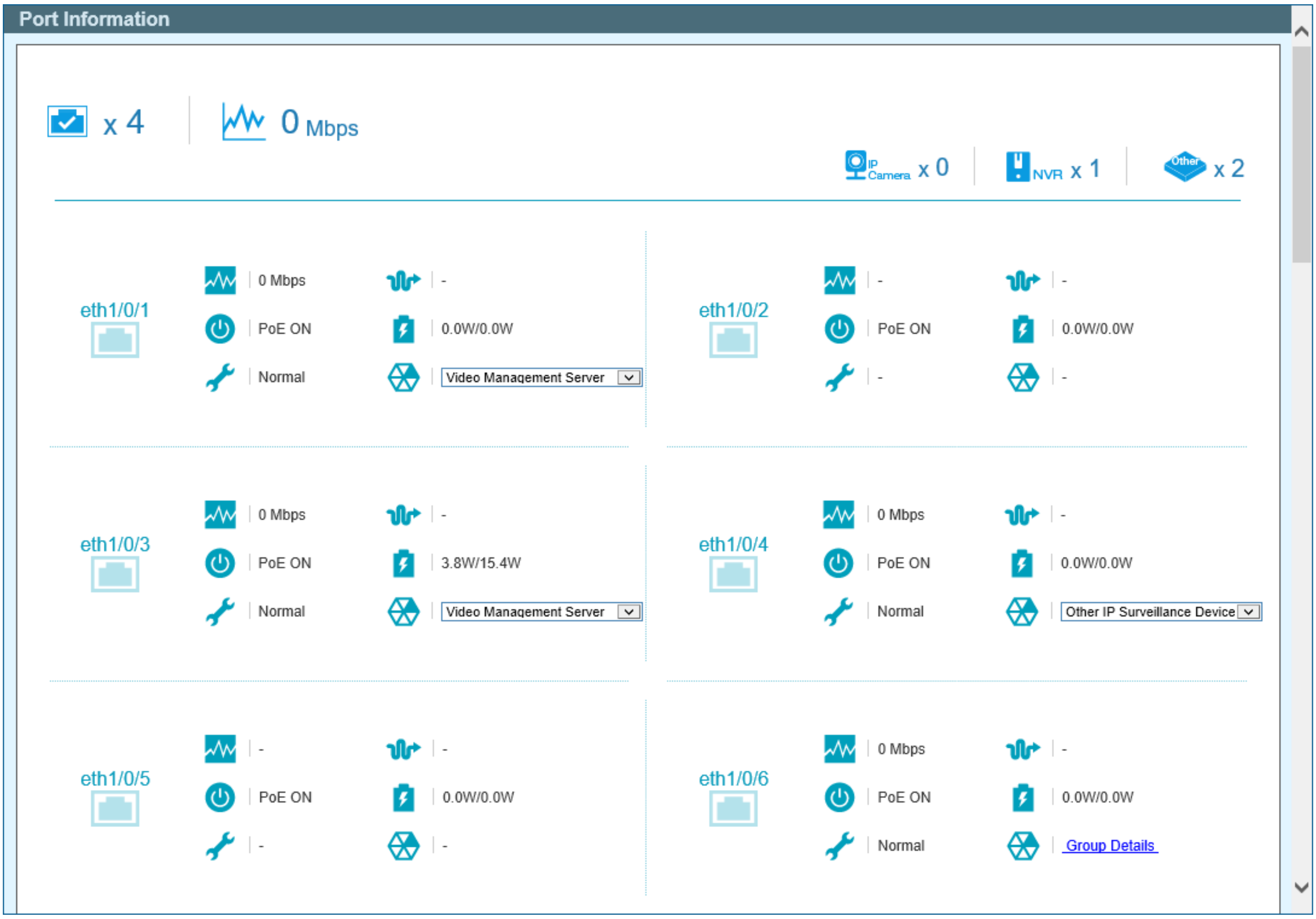


Figure 14-7 Port Information Window

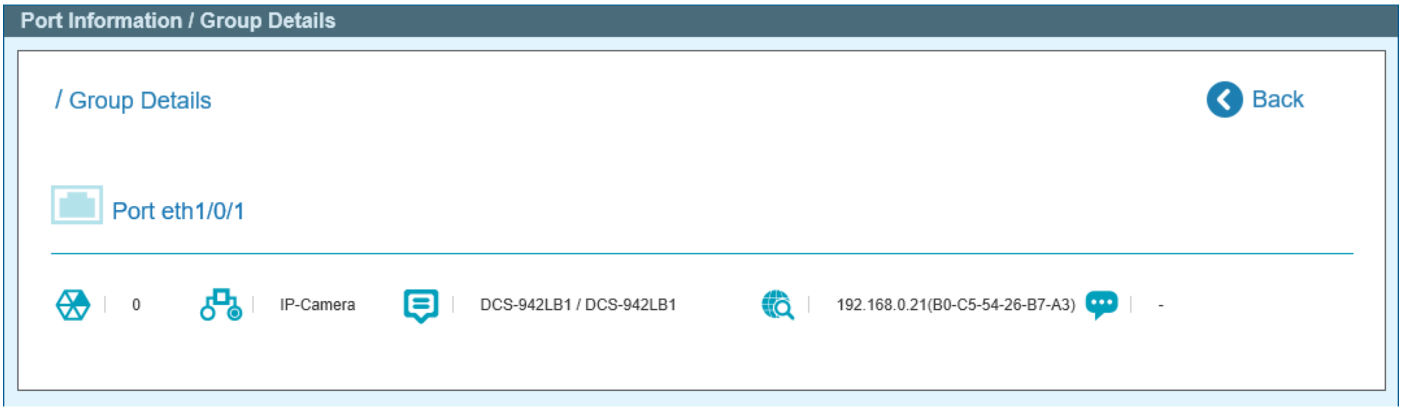
The following icons are available in this window and are described below:

Icon	Description
x 5	This displays the total amount of Ethernet devices connected to the Ethernet ports on the Switch.
6 Mbps	The displays the total amount of inbound bandwidth that is being used by the Ethernet devices connected to the Ethernet ports on the Switch.
IP Camera x 3	This displays the total amount of ONVIF IP cameras connected to the Ethernet ports on the Switch.
NVR x 1	This displays the total amount of NVRs connected to the Ethernet ports on the Switch.
Other x 1	This displays the total amount of other Ethernet devices connected to the Ethernet ports on the Switch.
eth1/0/1	This displays the Ethernet port number on the Switch.
0 Mbps	This displays the amount of inbound bandwidth that is being used by the Ethernet device connected to the respective Ethernet port.

Icon	Description
-	This displays the Ethernet cable length between the device and the Ethernet port on the Switch.
PoE ON	This displays the PoE status on the port.
3.9W/15.4W	This displays the power consumption and power class of the PD connected to the Ethernet port.
Normal Loop	This displays the Loopback Detection status on the Ethernet port. • **Normal** - Specifies that there are no loops in the network. • **Loop** - Specifies that there is a loop in the network. Click the **Loop** link to navigate to the **Health Diagnostic** window.
Group Details	If an ONVIF IP camera or NVR is connected to the port, the **Group Details** link will be available. Select the **Group Details** link to access the Group Details window.
Video Management Server ▾	If a network device is connected to the port that is neither an ONVIF IP camera nor NVR, the device type can be selected. Options to choose from are **Video Management Server**, **VMS Client/Remote Viewer**, **Video Encoder**, **Network Storage**, and **Other IP Surveillance Device**.

Group Details

After clicking **Group Details** link, the following window will appear.



Port Information / Group Details

/ Group Details

Back

Port eth1/0/1

0 | IP-Camera | DCS-942LB1 / DCS-942LB1 | 192.168.0.21(B0-C5-54-26-B7-A3) | -

Figure 14-8 Port Information / Group Details Window

The following icons are available in this window and are described below:

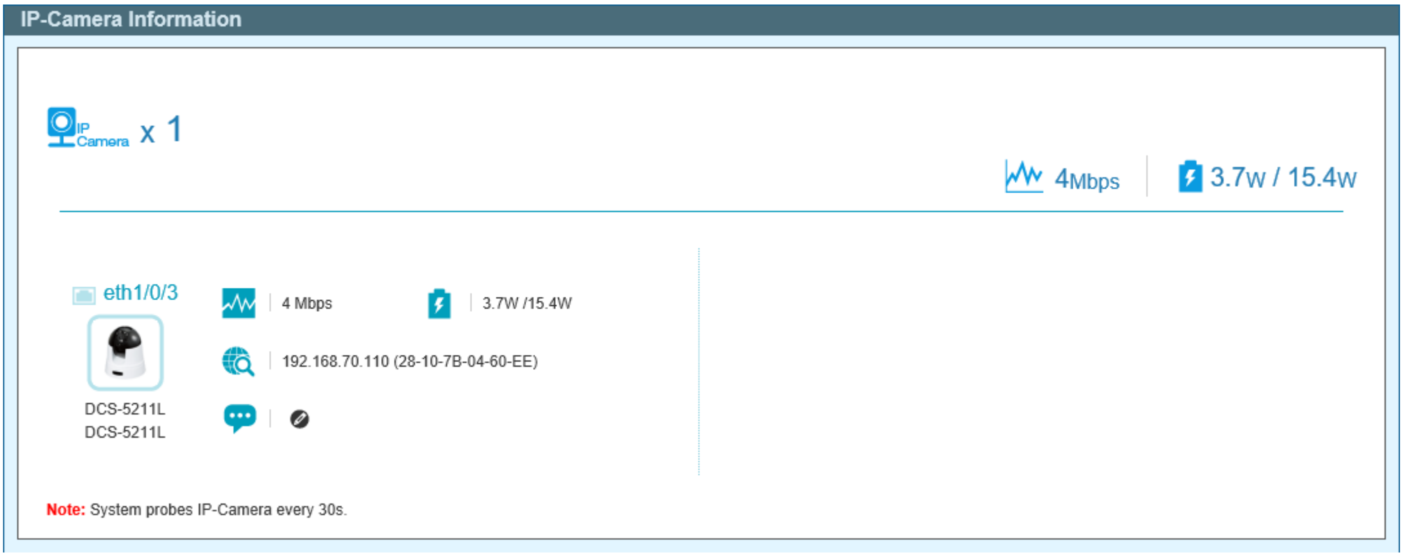
Icon	Description
Port eth1/0/5	This displays the Ethernet port number on the Switch.
0	This displays the group ID of the IP camera or NVR on the port.
IP-Camera	This displays the type of device connected to the port. The can be either **IP-Camera** or **NVR**.
DCS-5211L / DCS-5211L	This displays the model name of the IP camera.
192.168.0.23(28-10-7B-04-60-EC)	This displays the IP Address and MAC Address of the IP camera or NVR.
DCS-942LB1	This displays the description of the device connected to the port.

Click the **< Back** option to return to the previous window.

IP-Camera Information

This window is used to display IP camera information.

To view the following window, click **IP-Camera Information**, as shown below:



IP-Camera Information

IP Camera x 1

4Mbps

3.7w / 15.4w

eth1/0/3

4 Mbps

3.7W /15.4W

192.168.70.110 (28-10-7B-04-60-EE)

DCS-5211L
DCS-5211L

Note: System probes IP-Camera every 30s.

Figure 14-9 IP-Camera Information Window

The following icons are available in this window and are described below:

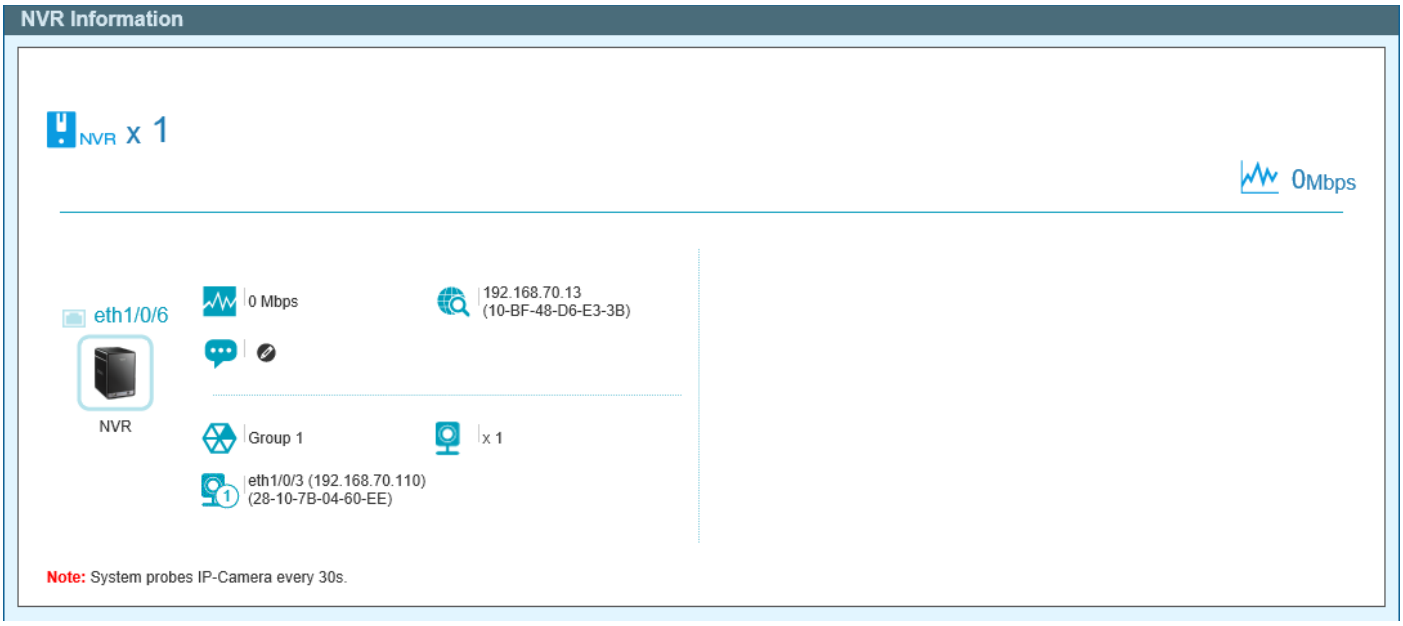
Icon	Description
IP Camera x 3	This displays the total amount of ONVIF IP cameras connected to the Ethernet ports on the Switch.
0Mbps	The displays the total amount of inbound bandwidth that is being used by the ONVIF IP cameras connected to the Ethernet ports on the Switch.
4.4w / 15.4w	The displays the total power consumption and power class (of PDs) used by the ONVIF IP cameras connected to the Ethernet ports on the Switch.
eth1/0/1	This displays the Ethernet port number on the Switch.
 DCS-942LB1 DCS-942LB1	This displays a photo, manufacturer, and model name of the IP camera connected to the port. D-Link IP cameras will display the photo of the specific model connected to the port. Non-D-Link camera will display a generic IP camera photo.
0 Mbps	This displays the amount of inbound bandwidth that is being used by the IP camera.
4.4W /15.4W	This displays the power consumption and power class of the IP camera.
192.168.0.21 (B0-C5-54-26-B7-A3)	This displays the IP address and MAC address of the IP camera.
DCS-942LB1 ✎	This displays the description for the IP camera. Click the ✎ icon to modify the description.

Icon	Description
💬 | ▭ ✓	Enter the description for the IP camera here. Click the ✓ icon to apply the modified description.

NVR Information

This window is used to display NVR information.

To view the following window, click **NVR Information**, as shown below:



Note: System probes IP-Camera every 30s.

Figure 14-10 NVR Information Window

The following icons are available in this window and are described below:

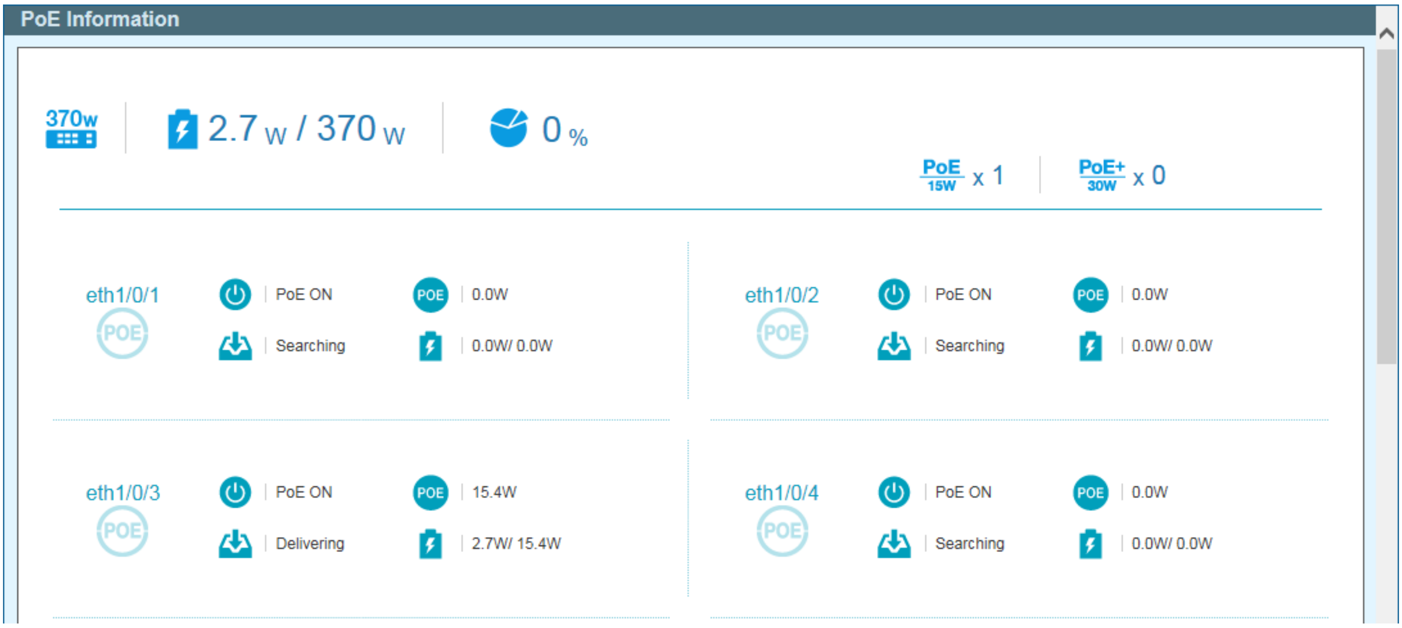
Icon	Description
NVR x 1	This displays the total amount of NVRs connected to the Ethernet ports on the Switch.
0Mbps	The displays the total amount of inbound bandwidth that is being used by the NVRs connected to the Ethernet ports on the Switch.
eth1/0/2	This displays the Ethernet port number on the Switch.
NVR	This displays a generic photo of the NVR connected to the port.
0 Mbps	This displays the amount of inbound bandwidth that is being used by the NVR.
192.168.0.202 (B8-70-F4-B0-42-A1)	This displays the IP address and MAC address of the NVR.
💬 | ✎	This displays the description for the NVR. Click the ✎ icon to modify the description.
💬 | ▭ ✓	Enter the description for the NVR here. Click the ✓ icon to apply the modified description.

Icon	Description
Group 1	This displays the group ID of the NVR.
x 3	This displays the number of ONVIF IP cameras managed by this NVR.
1 eth1/0/5 (192.168.0.23) (28-10-7B-04-60-EC)	This displays information about the ONVIF IP camera that is managed by this NVR.

PoE Information

This window is used to display Power-over-Ethernet (PoE) information.

To view the following window, click **PoE Information**, as shown below:



PoE Information

370w | 2.7 W / 370 W | 0 %

PoE 15W x 1 | PoE+ 30W x 0

eth1/0/1 POE | PoE ON | Searching | POE 0.0W | 0.0W/ 0.0W

eth1/0/2 POE | PoE ON | Searching | POE 0.0W | 0.0W/ 0.0W

eth1/0/3 POE | PoE ON | Delivering | POE 15.4W | 2.7W/ 15.4W

eth1/0/4 POE | PoE ON | Searching | POE 0.0W | 0.0W/ 0.0W

Figure 14-11 PoE Information Window

The following icons are available in this window and are described below:

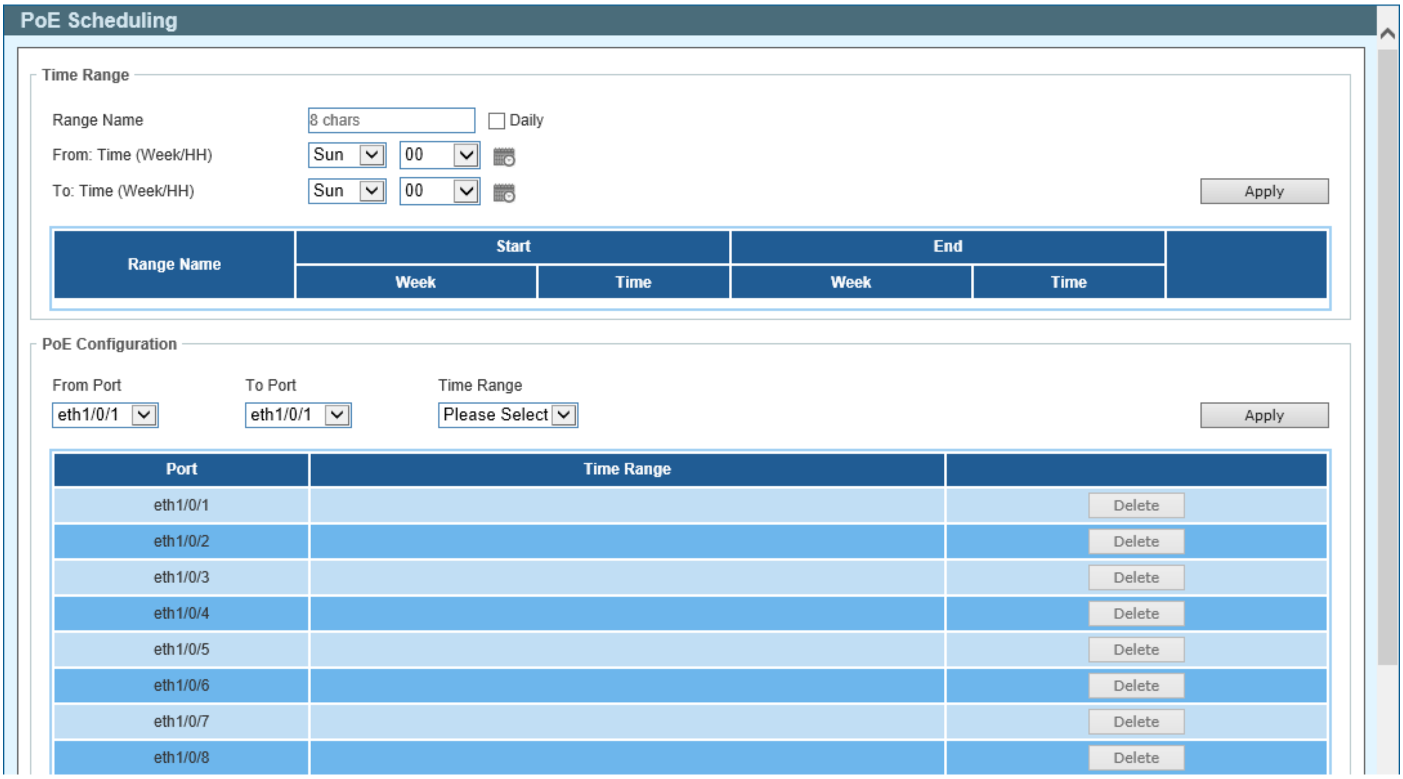
Icon	Description
370w	This displays the maximum PoE budget that can be provided by the Switch.
3.7 W / 370 W	This displays the total PoE consumption and power class of PDs connected to the Switch.
22 %	This displays the current PoE utilization (in percentage).
PoE 15W x 1	This displays the number of PoE devices connected to the Switch that is using 15 Watts of power per port.
PoE+ 30W x 0	This displays the number of PoE devices connected to the Switch that is using 30 Watts of power per port.
eth1/0/5 POE	This displays the Ethernet port number on the Switch.
PoE ON	This displays the PoE state on the port. This can be either **PoE ON** or **PoE OFF**.

Icon	Description
POE | 15.4W	This displays the maximum PoE budget available on this port.
Delivering Power Denied	This displays the current PoE status on the port. This status can be one of the following: **Disabled**, **Requesting**, **Searching**, **Delivering**, **MPS (Maintain Power Signature) Absent**, **PD Short**, **Overload**, **Power Denied**, **Thermal Shutdown**, **Startup Failure**, or **Classification Failure**. When the **Power Denied** message is displayed, click on the link to redirect the **Health Diagnostic** window for more information.
3.5W/ 15.4W	This displays the PoE consumption and power class of the PD connected to the port.

PoE Scheduling

This window is used to display and configure the PoE scheduling settings.

To view the following window, click **PoE Scheduling**, as shown below:



PoE Scheduling

Time Range

Range Name: 8 chars □ Daily

From: Time (Week/HH): Sun 00

To: Time (Week/HH): Sun 00

Apply

Range Name	Start		End		
	Week	Time	Week	Time	

PoE Configuration

From Port: eth1/0/1

To Port: eth1/0/1

Time Range: Please Select

Apply

Port	Time Range	
eth1/0/1		Delete
eth1/0/2		Delete
eth1/0/3		Delete
eth1/0/4		Delete
eth1/0/5		Delete
eth1/0/6		Delete
eth1/0/7		Delete
eth1/0/8		Delete

Figure 14-12 PoE Scheduling Window

The fields that can be configured in the **Time Range** section are described below:

Parameter	Description
Range Name	Enter the name of the time range schedule here. Tick the **Daily** option to use this schedule for every day of the week.
From: Time (Week/HH)	Select the starting day and hour in the time range schedule here. Alternatively, click the 📅 icon to open a calendar for easy day and hour selection.
To: Time (Week/HH)	Select the ending day and hour in the time range schedule here. The schedule will end at the end of the selected hour.

Parameter	Description
	Alternatively, click the 📅 icon to open a calendar for easy day and hour selection.

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

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

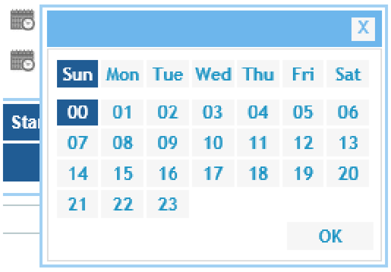
The fields that can be configured in the **PoE Configuration** section are described below:

Parameter	Description
From Port / To Port	Select the port range that will be used here.
Time Range	Select the time range schedule that will be applied to the selected port(s) here.

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

Click the **Delete** button to remove the time range schedule from the specified port.

After clicking the 📅 icon, the following window will appear:



Sun	Mon	Tue	Wed	Thu	Fri	Sat
00	01	02	03	04	05	06
07	08	09	10	11	12	13
14	15	16	17	18	19	20
21	22	23				

Figure 14-13 Day and Hour Window

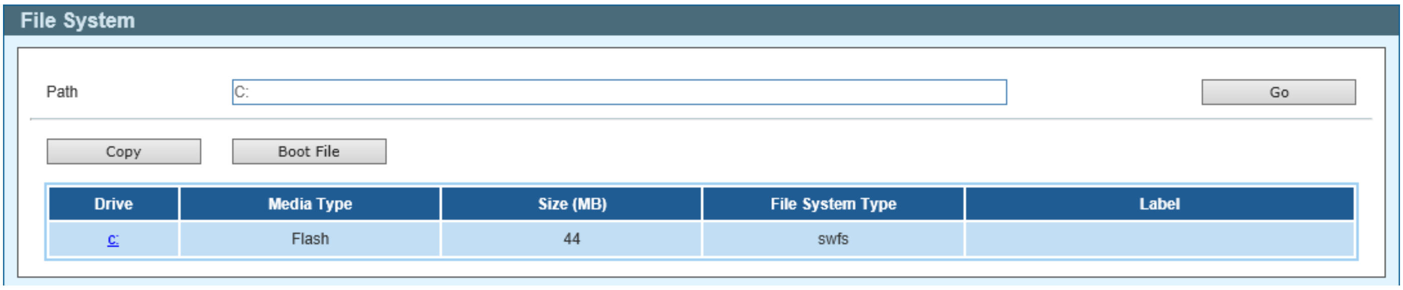
Click the **OK** button to use the Day and Hour selected.

Management

File System

This window is used to display and configure the file system settings.

To view the following window, click **Management > File System**, as shown below:



File System

Path: C:

Drive	Media Type	Size (MB)	File System Type	Label
c:	Flash	44	swfs	

Figure 14-14 File System Window

The fields that can be configured are described below:

Parameter	Description
Path	Enter the path string here.

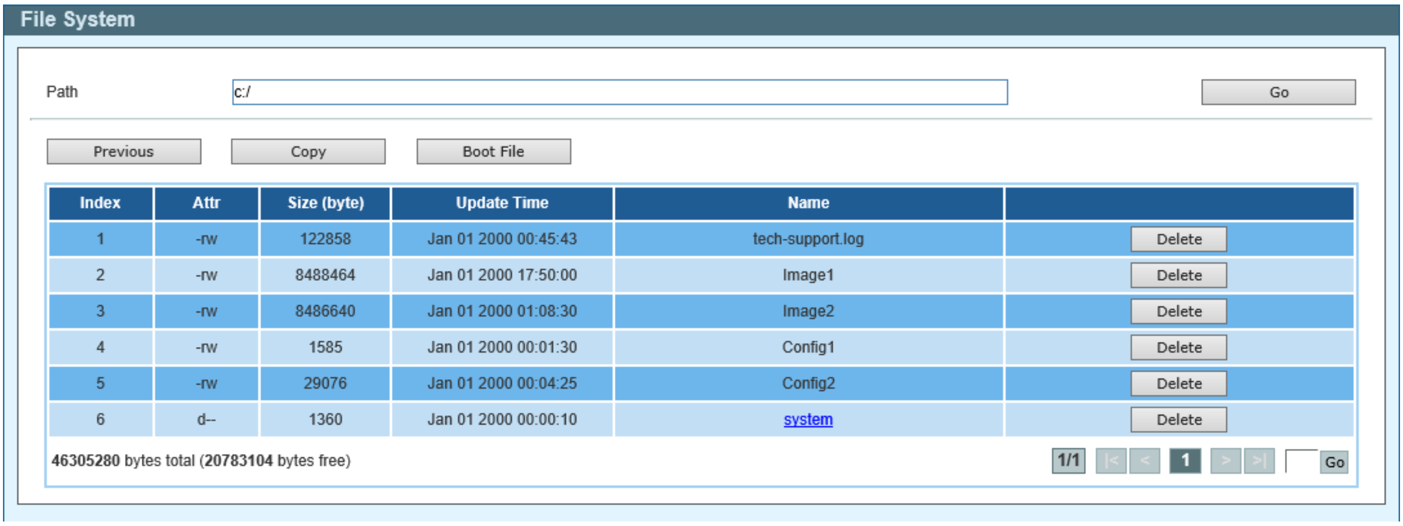
Click the **Go** button to navigate to the path entered.

Click the **Copy** button to copy a specific file to the Switch.

Click the **Boot File** button to configure the bootup image and configuration file settings.

Click the c: hyperlink to navigate the C: drive

After clicking the c: hyperlink, the following window will appear.



File System

Path: c:/

Index	Attr	Size (byte)	Update Time	Name	
1	-rw	122858	Jan 01 2000 00:45:43	tech-support.log	Delete
2	-rw	8488464	Jan 01 2000 17:50:00	Image1	Delete
3	-rw	8486640	Jan 01 2000 01:08:30	Image2	Delete
4	-rw	1585	Jan 01 2000 00:01:30	Config1	Delete
5	-rw	29076	Jan 01 2000 00:04:25	Config2	Delete
6	d--	1360	Jan 01 2000 00:00:10	system	Delete

46305280 bytes total (**20783104** bytes free)

Figure 14-15 File System (c:) Window

Click the **Go** button to navigate to the path entered.

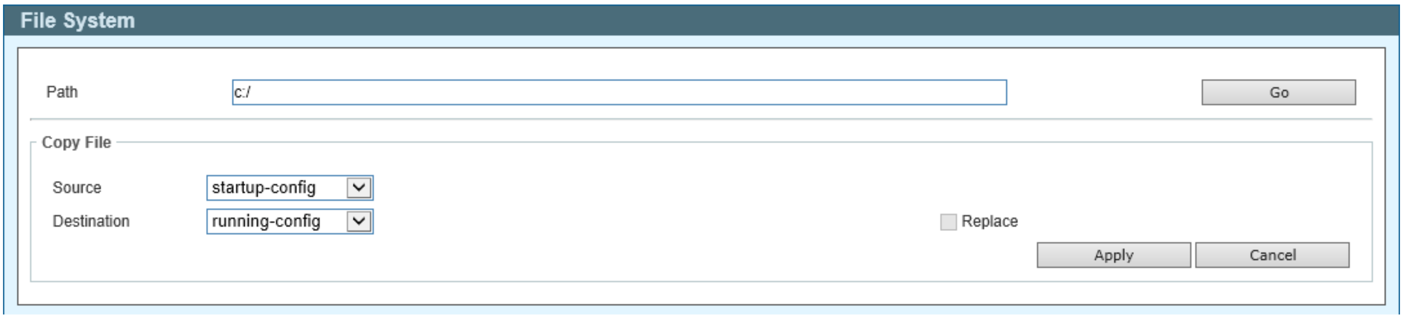
Click the **Previous** button to return to the previous window.

Click the **Copy** button to copy a specific file to the Switch.

Click the **Boot File** button to configure the bootup image and configuration file settings.

Click the **Delete** button to remove a specific file from the file system.

After clicking the **Copy** button, the following windows will appear.



File System

Path: c:/

Copy File

Source: startup-config

Destination: running-config

□ Replace

Figure 14-16 File System (Copy) Window

The fields that can be configured are described below:

Parameter	Description
Source	Select the source for the copy here. Options to choose from are: • **startup-config** - Specifies to copy the startup configuration as the source. • **Image 1** - Specifies to copy firmware "**Image 1**" as the source.

Parameter	Description
	• **Image 2** - Specifies to copy firmware "**Image 2**" as the source. • **Configuration 1** - Specifies to copy "**Configuration 1**" as the source. • **Configuration 2** - Specifies to copy "**Configuration 2**" as the source.
Destination	Select the destination for the copy here. Options to choose from are: • **running-config** - Specifies to overwrite the running configuration with the source. • **startup-config** - Specifies to overwrite the start-up configuration with the source. • **Image 1** - Specifies to overwrite "**Image 1**" with the source. • **Image 2** - Specifies to overwrite "**Image 2**" with the source. • **Configuration 1** - Specifies to overwrite "**Configuration 1**" with the source. • **Configuration 2** - Specifies to overwrite "**Configuration 2**" with the source.
Replace	Specifies to replace the current running configuration with the indicated configuration file.

Click the **Apply** button to initiate the copy.

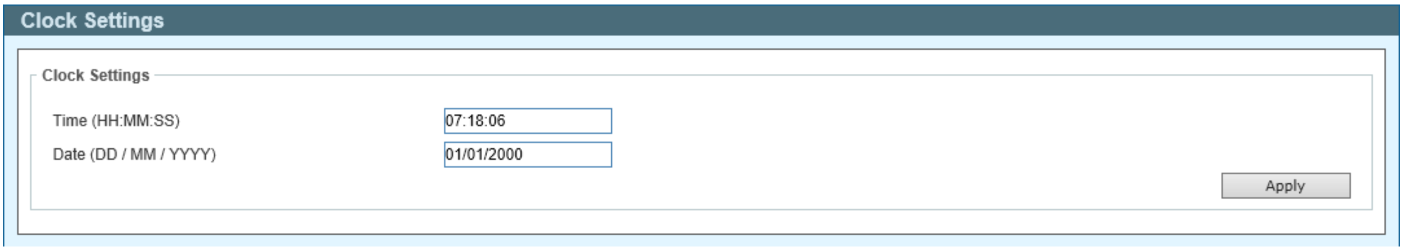
Click the **Cancel** button the discard the process.

Time

Clock Settings

This window is used to display and configure the time settings on the Switch.

To view the following window, click **Time > Clock Settings**, as shown below:



Clock Settings

Clock Settings

Time (HH:MM:SS) 07:18:06

Date (DD / MM / YYYY) 01/01/2000

Figure 14-17 Clock Settings Window

The fields that can be configured are described below:

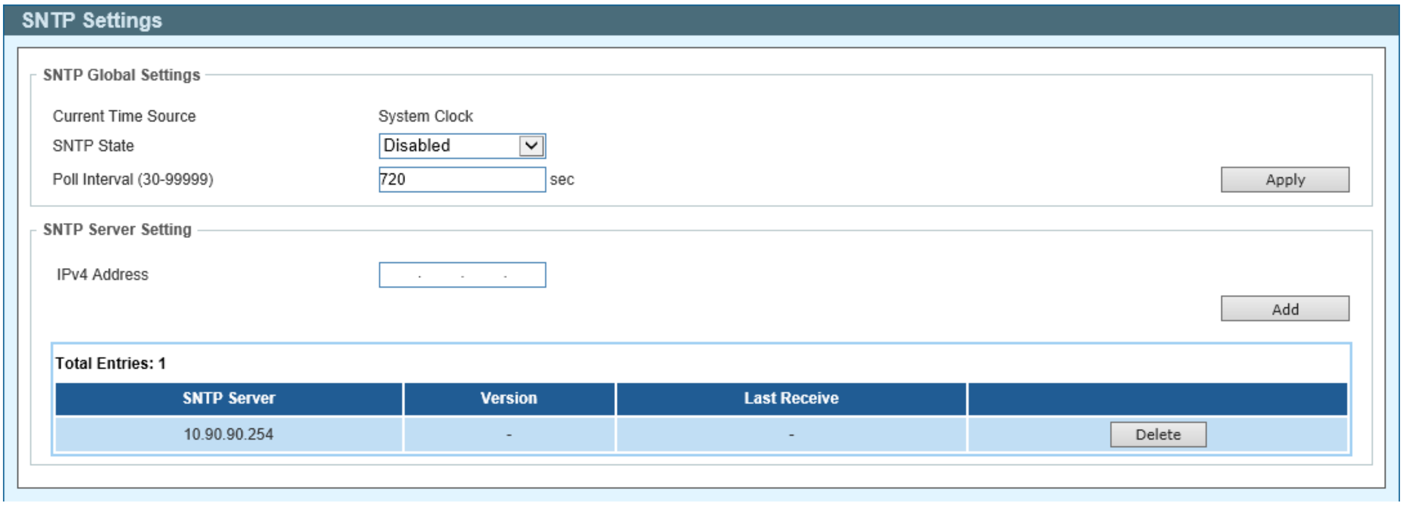
Parameter	Description
Time (HH:MM:SS)	Enter the current time in hours, minutes, and seconds.
Date (DD/MM/YYYY)	Enter the current day, month, and year to update the system clock.

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

SNTP Settings

This window is used to display and configure the Simple Network Time Protocol (SNTP) settings.

To view the following window, click **Time > SNTP Settings**, as shown below:



SNTP Settings

SNTP Global Settings

Current Time Source: System Clock

SNTP State: Disabled

Poll Interval (30-99999): 720 sec

SNTP Server Setting

IPv4 Address: . . .

Total Entries: 1

SNTP Server	Version	Last Receive	
10.90.90.254	-	-	Delete

Figure 14-18 SNTP Settings Window

The fields that can be configured in the **SNTP Global Settings** section are described below:

Parameter	Description
SNTP State	Select to enable or disable the SNTP feature here.
Poll Interval	Enter the poll interval value here. The range is from 30 to 99999 seconds. By default, this value is 720 seconds.

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

The fields that can be configured in the **SNTP Server Setting** section are described below:

Parameter	Description
IPv4 Address	Enter the IPv4 address of the SNTP server here.

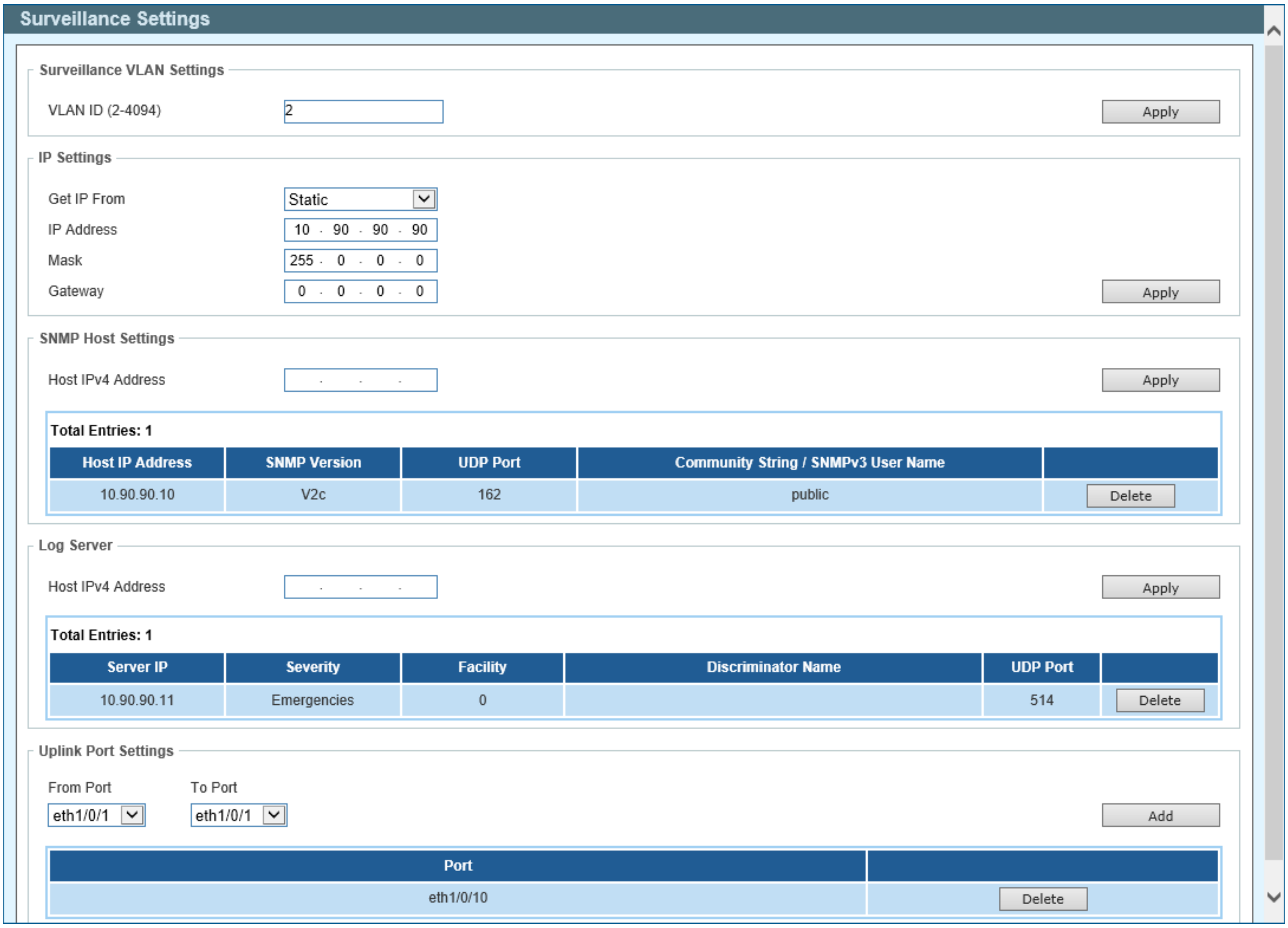
Click the **Add** button to add the SNTP server to the configuration.

Click the **Delete** button to remove the SNTP server from the configuration.

Surveillance Settings

This window is used to display and configure the surveillance settings. The Switch has only one Surveillance VLAN. This surveillance VLAN also supports to recognize the surveillance devices, like IP Cameras (IPC) and Network Video Recorders (NVR), using the ONVIF protocol.

To view the following window, click **Surveillance Settings**, as shown below:



Surveillance Settings

Surveillance VLAN Settings

VLAN ID (2-4094): 2

IP Settings

Get IP From: Static

IP Address: 10 . 90 . 90 . 90

Mask: 255 . 0 . 0 . 0

Gateway: 0 . 0 . 0 . 0

SNMP Host Settings

Host IPv4 Address: . . .

Total Entries: 1

Host IP Address	SNMP Version	UDP Port	Community String / SNMPv3 User Name	
10.90.90.10	V2c	162	public	Delete

Log Server

Host IPv4 Address: . . .

Total Entries: 1

Server IP	Severity	Facility	Discriminator Name	UDP Port	
10.90.90.11	Emergencies	0		514	Delete

Uplink Port Settings

From Port: eth1/0/1

To Port: eth1/0/1

Port	
eth1/0/10	Delete

Figure 14-19 Surveillance Settings Window

The fields that can be configured in the **Surveillance VLAN Settings** section are described below:

Parameter	Description
VLAN ID	Enter the ID of the surveillance VLAN here. The range is from 2 to 4094.

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

The fields that can be configured in the **IP Settings** section are described below:

Parameter	Description
Get IP From	Select the method used to configure the IP address settings on the Switch here. Options to choose from are: • **Static** - Specifies that the IP address settings will be manually configured. • **DHCP** - Specifies that the IP address settings will be automatically obtained from a DHCP server on the network.
IP Address	Enter the IPv4 address of the Switch here.
Mask	Enter the IPv4 subnet mask of the Switch here.

Parameter	Description
Gateway	Enter the IPv4 address of the default gateway here.

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

The fields that can be configured in the **SNMP Host Settings** section are described below:

Parameter	Description
Host IPv4 Address	Enter the IPv4 address of the SNMP host here.

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

Click the **Delete** button to remove the specified entry.

The fields that can be configured in the **Log Server** section are described below:

Parameter	Description
Host IPv4 Address	Enter the IPv4 address of the SNMP server here.

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

Click the **Delete** button to remove the specified entry.

The uplink ports join all surveillance VLANs since they forward surveillance traffic to other switches. It is recommended to connect uplink ports to the other switches because the discovery process is disabled on these ports.

The fields that can be configured in the **Uplink Port Settings** section are described below:

Parameter	Description
From Port / To Port	Select the uplink port range that will be used here.

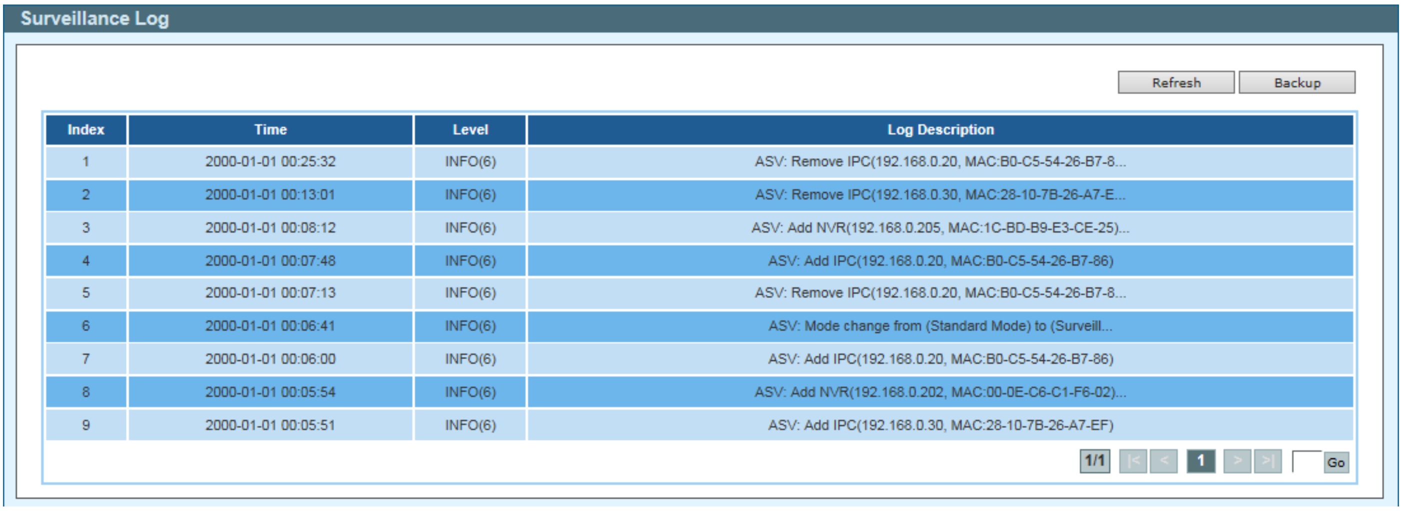
Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Surveillance Log

This window is used to display the surveillance log.

To view the following window, click **Surveillance Log**, as shown below:



Index	Time	Level	Log Description
1	2000-01-01 00:25:32	INFO(6)	ASV: Remove IPC(192.168.0.20, MAC:B0-C5-54-26-B7-8...
2	2000-01-01 00:13:01	INFO(6)	ASV: Remove IPC(192.168.0.30, MAC:28-10-7B-26-A7-E...
3	2000-01-01 00:08:12	INFO(6)	ASV: Add NVR(192.168.0.205, MAC:1C-BD-B9-E3-CE-25)...
4	2000-01-01 00:07:48	INFO(6)	ASV: Add IPC(192.168.0.20, MAC:B0-C5-54-26-B7-86)
5	2000-01-01 00:07:13	INFO(6)	ASV: Remove IPC(192.168.0.20, MAC:B0-C5-54-26-B7-8...
6	2000-01-01 00:06:41	INFO(6)	ASV: Mode change from (Standard Mode) to (Surveill...
7	2000-01-01 00:06:00	INFO(6)	ASV: Add IPC(192.168.0.20, MAC:B0-C5-54-26-B7-86)
8	2000-01-01 00:05:54	INFO(6)	ASV: Add NVR(192.168.0.202, MAC:00-0E-C6-C1-F6-02)...
9	2000-01-01 00:05:51	INFO(6)	ASV: Add IPC(192.168.0.30, MAC:28-10-7B-26-A7-EF)

Figure 14-20 Surveillance Log Window

Click the **Refresh** button to refresh the information displayed in the table.

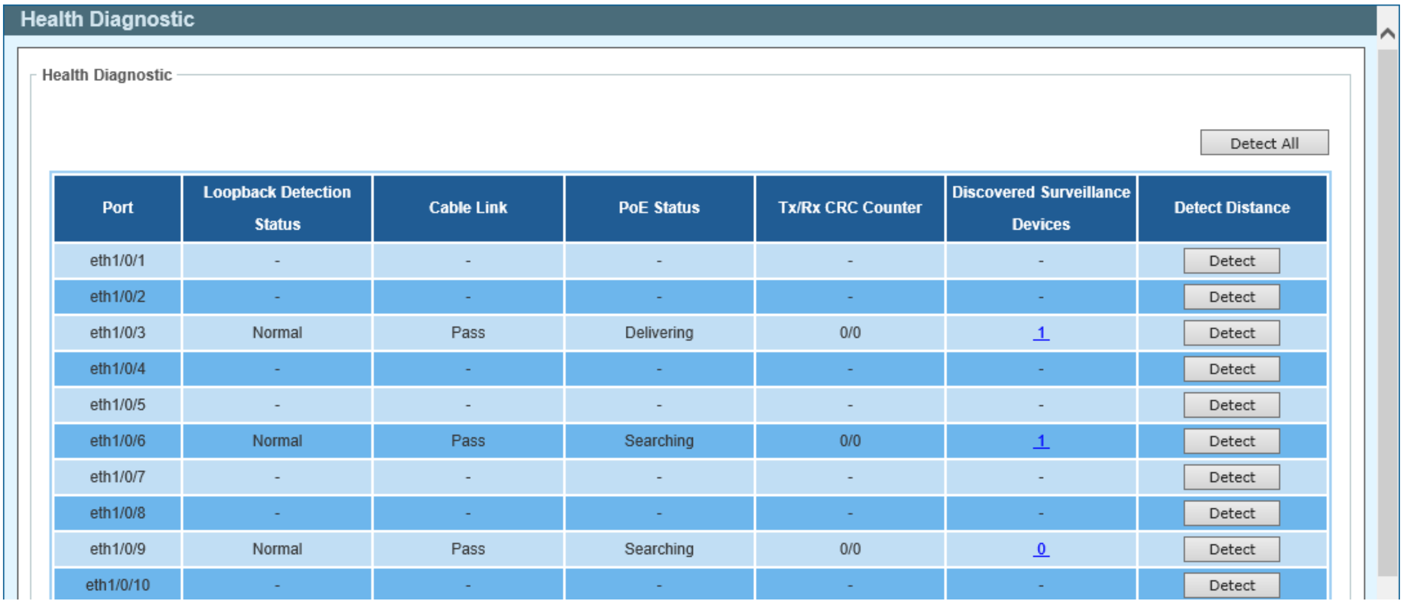
Click the **Backup** button to upload the surveillance log to the PC using HTTP.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Health Diagnostic

This window is used to display Health Diagnostics information, Discovered Surveillance Devices information, and initiate a cable distance test on all or selected ports on the Switch. For each link-up port, the system will check the link status, PoE status and error counters periodically. This page will refresh every 30s.

To view the following window, click **Health Diagnostic**, as shown below:



Port	Loopback Detection Status	Cable Link	PoE Status	Tx/Rx CRC Counter	Discovered Surveillance Devices	Detect Distance
eth1/0/1	-	-	-	-	-	Detect
eth1/0/2	-	-	-	-	-	Detect
eth1/0/3	Normal	Pass	Delivering	0/0	1	Detect
eth1/0/4	-	-	-	-	-	Detect
eth1/0/5	-	-	-	-	-	Detect
eth1/0/6	Normal	Pass	Searching	0/0	1	Detect
eth1/0/7	-	-	-	-	-	Detect
eth1/0/8	-	-	-	-	-	Detect
eth1/0/9	Normal	Pass	Searching	0/0	0	Detect
eth1/0/10	-	-	-	-	-	Detect

Figure 14-21 Health Diagnostic Window

The fields that are displayed in the table are described below:

Parameter	Description
Port	This field displays the Ethernet port number.
Loopback Detection Status	This field displays the Loopback Detection status on the Ethernet port. It can be one of the following: • **Normal** - No loop is detected on the port. • **Loop** - A loop is detected on the port.
Cable Link	This field displays the cable link status. It can be one of the following: • **Pass** - The port link is up and operating in the full-duplex mode. • **10M Half** - The port link is up and operating at 10 Mbps speed and in the half-duplex mode. • **100M Half** - The port link is up and operating at 100 Mbps speed and in the half-duplex mode.
PoE Status	This field displays the PoE status. It can be one of the following: **Delivering**, **Searching**, **Pass**, **MPS (Maintain Power Signature) Absent**, **PD Short**, **Overload**, **Power Denied**, **Thermal Shutdown**, **Startup Failure**, or **Classification Failure**.
Tx/Rx CRC Counter	This field displays the TX/RX CRC counter.

Parameter	Description
Discovered Surveillance Devices	This field displays the number of ONVIF IP cameras and NVRs discovered on the port. Click the hyperlink (1) to view the group details associated with IP camera or NVR connected to the port.
Detect Distance	Click the **Detect** button to initiate a cable distance test on the specified port.

Click the **Detect All** button to initiate a cable distance test on all the ports of the Switch.

Toolbar

Wizard

Click this option to start the Smart Wizard. For more information about the Smart Wizard, refer to **Smart Wizard** on page 5.

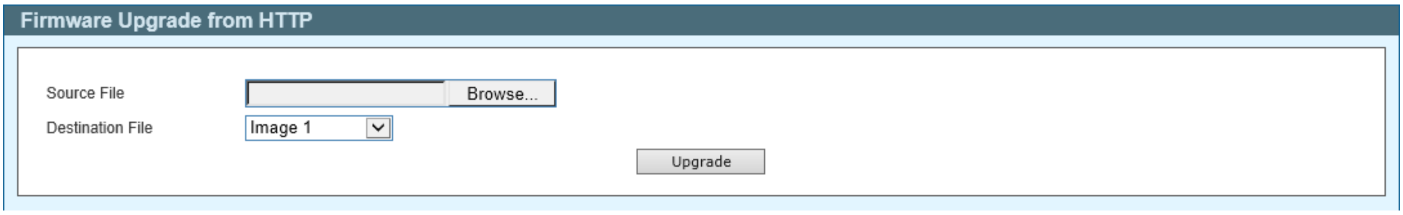
Tools

Firmware Upgrade & Backup

Firmware Upgrade from HTTP

This window is used to initiate a firmware upgrade from a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP**, as shown below:


Firmware Upgrade from HTTP

Source File

Destination File: Image 1

Figure 14-22 Firmware Upgrade from HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source File	Click the **Browse** button and navigate to the firmware file on the local PC here. This file will be uploaded to the Switch.
Destination File	Select the destination where the firmware file will be saved on the Switch here. Options to choose from are **Image 1** and **Image 2**.

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Backup to HTTP

This window is used to initiate a firmware backup to a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to HTTP**, as shown below:

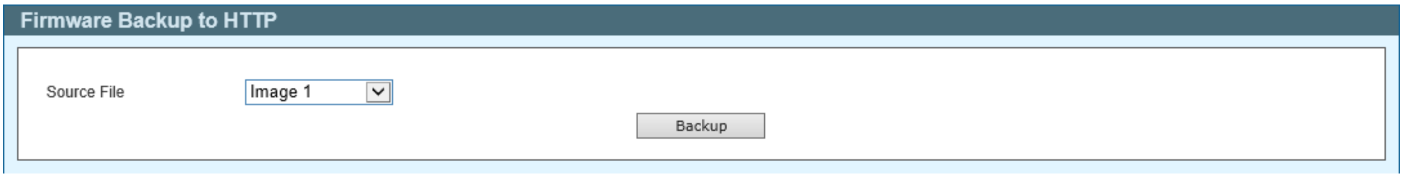


Figure 14-23 Firmware Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source File	Select the firmware on the Switch that will be backed up to the local PC here. Options to choose from are **Image 1** and **Image 2**.

Click the **Backup** button to initiate the firmware backup. Wait for the Web browser to prompt where to save the file on the local PC.

Configuration Restore & Backup

Configuration Restore from HTTP

This window is used to initiate a configuration restore from a local PC using HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from HTTP**, as shown below:

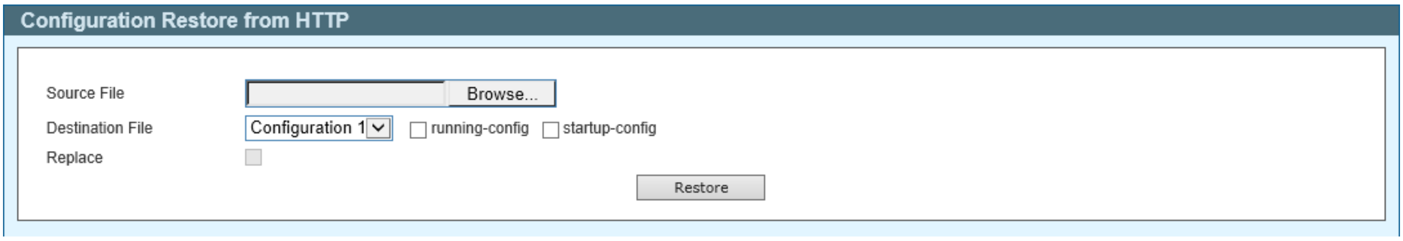


Figure 14-24 Configuration Restore from HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source File	Click the **Browse** button and navigate to the configuration file on the local PC here. This file will be uploaded to the Switch.
Destination File	Select the destination for the configuration file on the Switch here. Options to choose from are: • **Configuration 1** - Select this option to use configuration 1 as the destination. • **Configuration 2** - Select this option to use configuration 2 as the destination. • **running-config** - Select this option to use the running configuration as the destination. • **startup-config** - Select this option to use the start-up configuration as the destination.

Parameter	Description
Replace	Select this option to replace the running configuration on the Switch with this one.

Click the **Restore** button to initiate the configuration restore.

Configuration Backup to HTTP

This window is used to initiate a configuration file backup to a local PC using HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to HTTP**, as shown below:

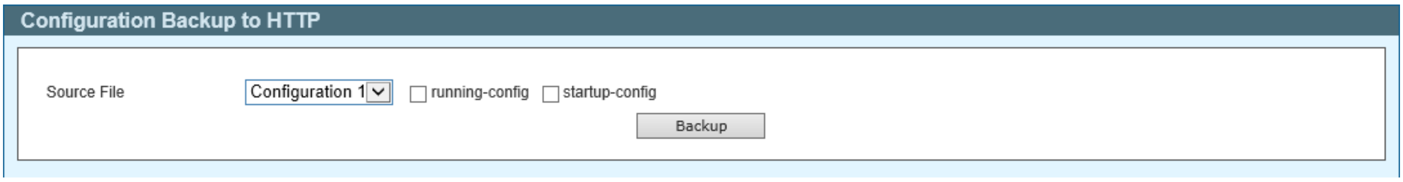


Figure 14-25 Configuration Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source File	Select the configuration on the Switch that will be backed up to the local PC here. Options to choose from are: • **Configuration 1** - Select this option to backup configuration 1. • **Configuration 2** - Select this option to backup configuration 2. • **running-config** - Select this option to backup the running configuration. • **startup-config** - Select this option to backup the start-up configuration.

Click the **Backup** button to initiate the configuration file backup. Wait for the Web browser to prompt where to save the file on the local PC.

Language Management

This window is used to install the language file to the Switch.

To view the following window, click **Tools > Language Management**, as shown below:

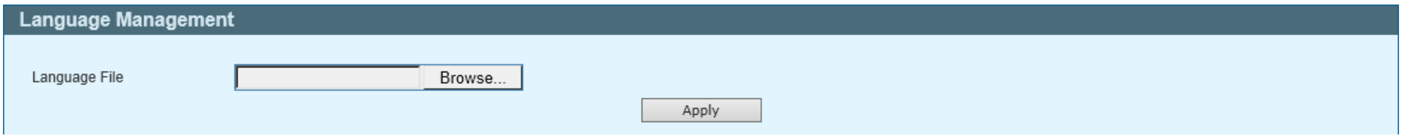


Figure 14-26 Language Management Window

The fields that can be configured are described below:

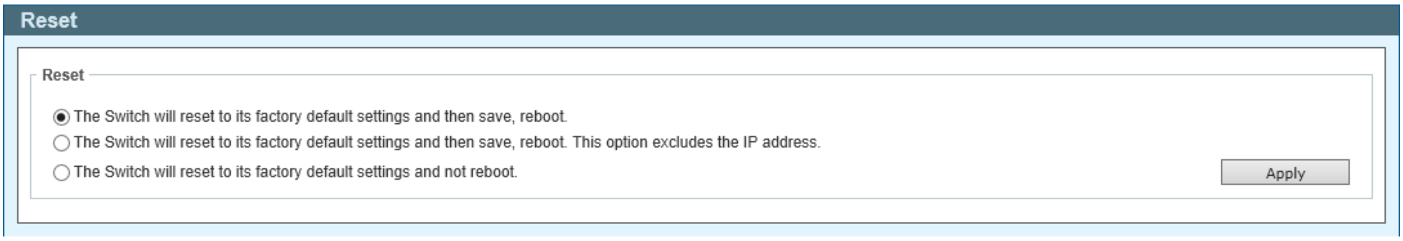
Parameter	Description
Language File	Click the **Browse** button and navigate to the language pack file on the local PC here. This file will be uploaded to the Switch.

Click the **Apply** button to initiate the language pack upload and installation.

Reset

This window is used to reset the Switch's configuration to the factory default settings.

To view the following window, click **Tools > Reset**, as shown below:



Reset

Reset

● The Switch will reset to its factory default settings and then save, reboot.

○ The Switch will reset to its factory default settings and then save, reboot. This option excludes the IP address.

○ The Switch will reset to its factory default settings and not reboot.

Figure 14-27 Reset Window

Select one of the following options:

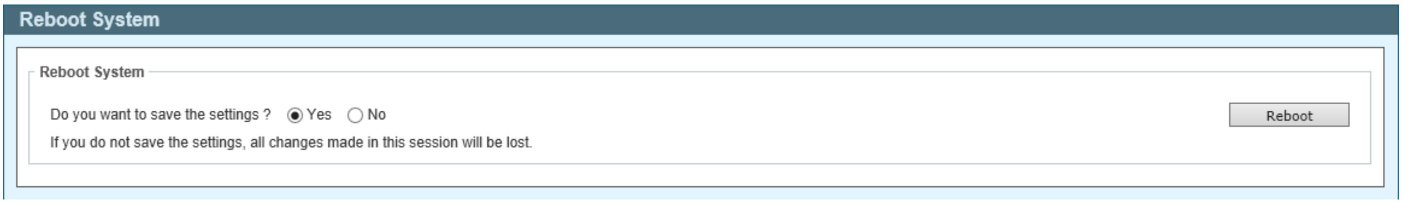
- The Switch will reset to its factory default settings and then save, reboot.
- The Switch will reset to its factory default settings and then save, reboot. This option excludes the IP address.
- The Switch will reset to its factory default settings and not reboot.

Click the **Apply** button to initiate the reset.

Reboot System

This window is used to reboot the Switch and alternatively save the configuration before doing so.

To view the following window, click **Tools > Reboot System**, as shown below:



Reboot System

Reboot System

Do you want to save the settings ? ● Yes ○ No

If you do not save the settings, all changes made in this session will be lost.

Figure 14-28 Reboot System Window

When rebooting the Switch, any configuration changes that was made during this session, will be lost unless the **Yes** option is selected when asked to save the settings.

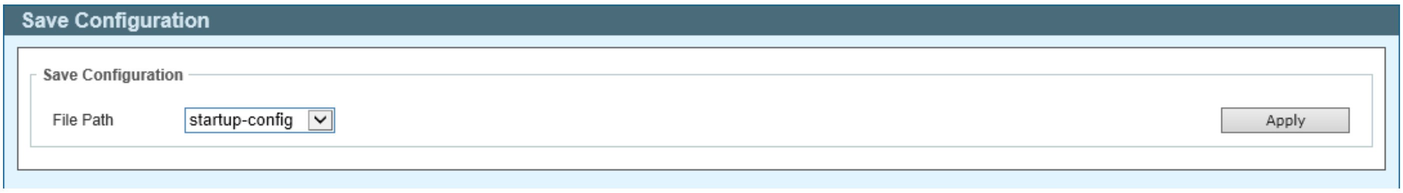
Click the **Reboot** button to alternatively save the settings and reboot the Switch.

Save

Save Configuration

This window is used to save the running configuration to the start-up configuration. This is to prevent the loss of configuration in the event of a power failure.

To view the following window, click **Save > Save Configuration**, as shown below:



Save Configuration

Save Configuration

File Path: startup-config

Figure 14-29 Save Configuration Window

The fields that can be configured are described below:

Parameter	Description
File Path	Select the destination where the configuration will be saved here. Options to choose from are **startup-config**, **Configuration 1**, and **Configuration 2**.

Click the **Apply** button to save the configuration.

Help

Click this option to access the built-in Surveillance Help window.

After clicking the **Help** option, the following window will appear.

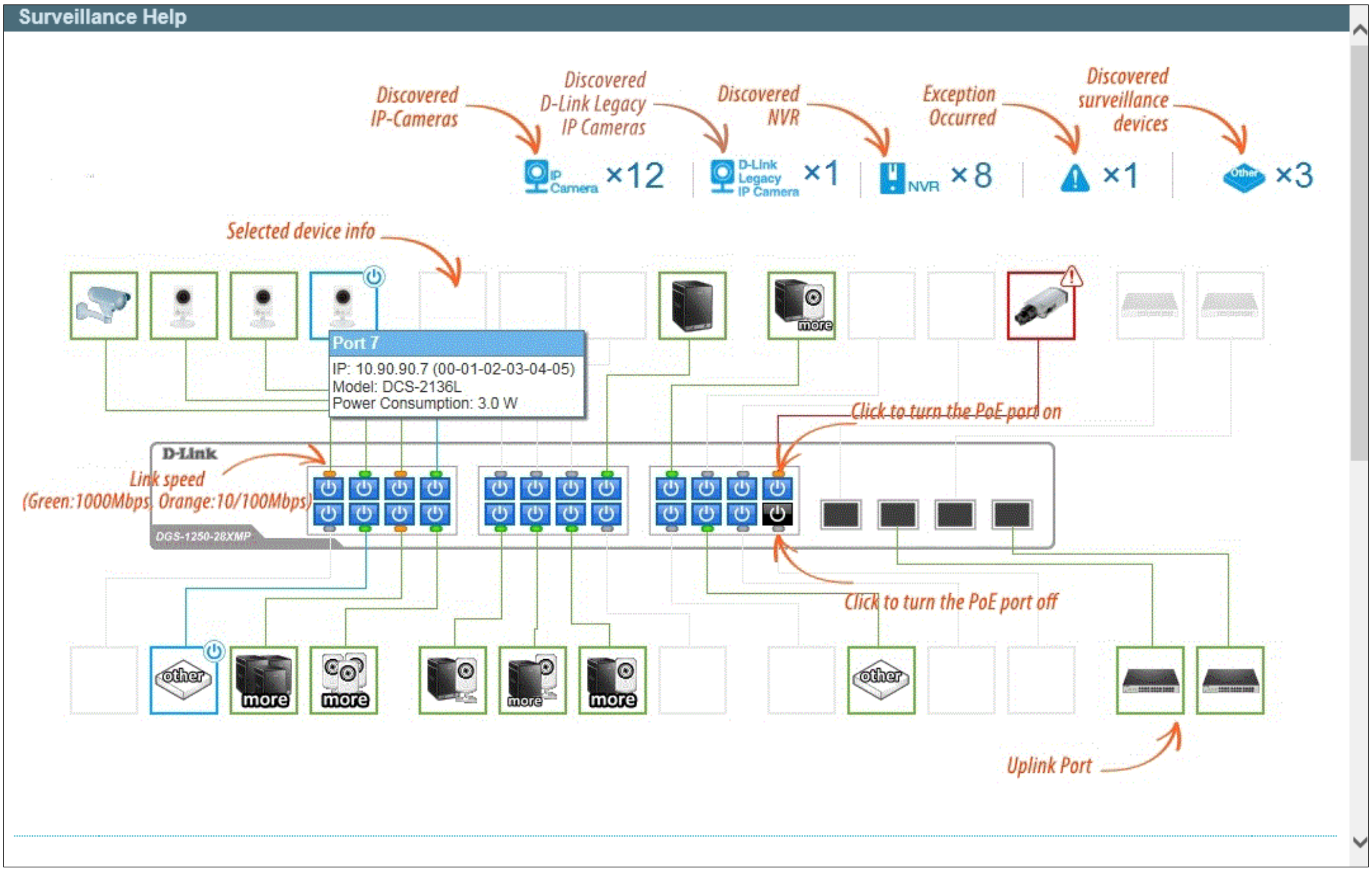
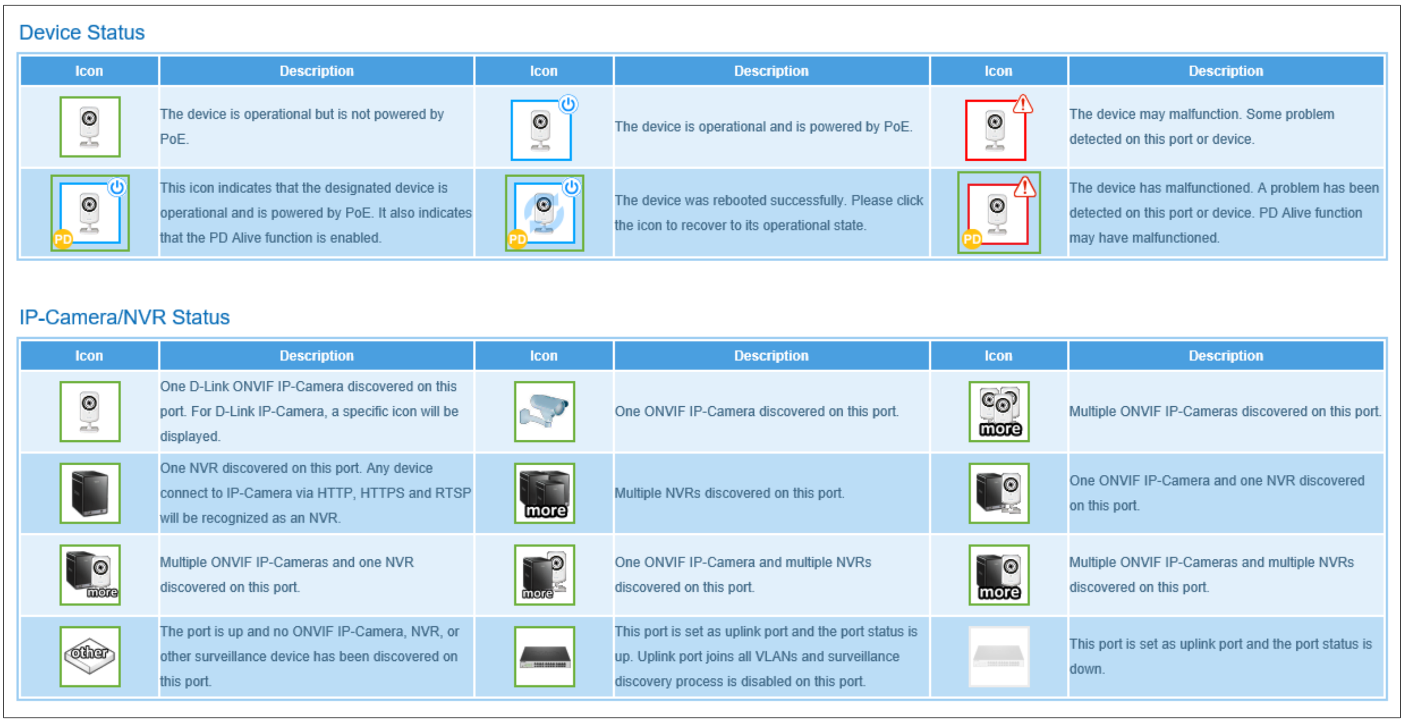

Surveillance Help
Discovered IP-Cameras
Discovered D-Link Legacy IP Cameras
Discovered NVR
Exception Occurred
Discovered surveillance devices
IP Camera ×12
D-Link Legacy IP Camera ×1
NVR ×8
×1
Other ×3
Selected device info
Port 7
IP: 10.90.90.7 (00-01-02-03-04-05)
Model: DCS-2136L
Power Consumption: 3.0 W
more
Click to turn the PoE port on
D-Link
Link speed
(Green:1000Mbps, Orange:10/100Mbps)
DGS-1250-28XMP
Click to turn the PoE port off
other
more
Uplink Port

Figure 14-30 Help (Diagram) Window



Device Status

Icon	Description	Icon	Description	Icon	Description
	The device is operational but is not powered by PoE.		The device is operational and is powered by PoE.		The device may malfunction. Some problem detected on this port or device.
PD	This icon indicates that the designated device is operational and is powered by PoE. It also indicates that the PD Alive function is enabled.	PD	The device was rebooted successfully. Please click the icon to recover to its operational state.	PD	The device has malfunctioned. A problem has been detected on this port or device. PD Alive function may have malfunctioned.

IP-Camera/NVR Status

Icon	Description	Icon	Description	Icon	Description
	One D-Link ONVIF IP-Camera discovered on this port. For D-Link IP-Camera, a specific icon will be displayed.		One ONVIF IP-Camera discovered on this port.	more	Multiple ONVIF IP-Cameras discovered on this port.
	One NVR discovered on this port. Any device connect to IP-Camera via HTTP, HTTPS and RTSP will be recognized as an NVR.	more	Multiple NVRs discovered on this port.		One ONVIF IP-Camera and one NVR discovered on this port.
more	Multiple ONVIF IP-Cameras and one NVR discovered on this port.	more	One ONVIF IP-Camera and multiple NVRs discovered on this port.	more	Multiple ONVIF IP-Cameras and multiple NVRs discovered on this port.
other	The port is up and no ONVIF IP-Camera, NVR, or other surveillance device has been discovered on this port.		This port is set as uplink port and the port status is up. Uplink port joins all VLANs and surveillance discovery process is disabled on this port.		This port is set as uplink port and the port status is down.

Figure 14-31 Help (Table) Window

Online Help

D-Link Support Site

Click this option to connect to the D-Link support website. An Internet connection is required.

User Guide

Click this option to connect to the online user guide for the Switch. An Internet connection is required.

Standard Mode

Click the **Standard Mode** button in the toolbar to change the Web UI mode and style from Surveillance Mode to Standard Mode.

NOTE: All active Web UI user sessions can only access the same Web UI mode at the same time. The mode can only be changed when one user session is active. The mode cannot be changed when another user session is connected to the Web UI.

Logout

Click this option to log out of the Web UI of the Switch

Appendix A - System Log Entries

The following table lists all possible entries and their corresponding meanings that will appear in the System Log of this Switch.

802.1X

Log Description	Severity
Event Description: 802.1X Authentication failure. Log Message: 802.1X authentication fail [due to <reason>] from (Username: <username>, <interface-id>, MAC: <mac-address>) Parameters Description: reason: The reason for the failed authentication. The possible reason may be: (1) user authentication failure (2) no server(s) responding (3) no servers configured (4) no resources (5) user timeout expired username: The user that is being authenticated. interface-id: The switch interface number. mac-address: The MAC address of the authenticated device.	Critical
Event Description: 802.1X Authentication successful. Log Message: 802.1X authentication success (Username: <username>, <interface-id>, MAC: <mac-address>) Parameters Description: username: The user that is being authenticated. interface-id: The interface name. mac-address: The MAC address of the authenticated device.	Informational

AAA

Log Description	Severity
Event Description: This log will be generated when AAA global state is enabled or disabled. Log Message: AAA is <status> Parameters Description: status: The status indicates the AAA enabled or disabled.	Informational
Event Description: This log will be generated when login successfully. Log Message: Successful login through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>) Parameters Description: exec-type: It indicates the EXEC types. For example, Console, Telnet, SSH, Web, and Web (SSL). client-ip: It indicates the client’s IP address if valid through IP protocol. aaa-method: It indicates the authentication method. For example, none, local, and server. server-ip: It indicates the AAA server IP address if authentication method is remote server. Username: It indicates the username for authentication. Note: For console, there will be no client IP information for logging.	Informational
Event Description: This log will be generated when login failure.	Warning

Log Description	Severity
Log Message: Login failed through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>). Parameters Description: exec-type: It indicates the EXEC types. For example, Console, Telnet, SSH, Web, and Web (SSL). client-ip: It indicates the client's IP address if valid through IP protocol. aaa-method: It indicates the authentication method. For example, local. server-ip: It indicates the AAA server IP address if authentication method is remote server. username: It indicates the username for authentication. Note: For console, there will be no client IP information for logging.	
Event Description: This log will be generated when the remote server does not respond to the login authentication request. Log Message: Login failed through <exec-type> <from client-ip> due to AAA server <server-ip> timeout (Username: <username>) Parameters Description: exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, and Web(SSL). client-ip: It indicates the client's IP address if valid through IP protocol. server-ip: It indicates the AAA server IP address if authentication method is remote server. username: It indicates the username for authentication. Note: For console, there will be no client IP information for logging.	Warning
Event Description: This log will be generated when enable privilege successfully. Log Message: Successful enable privilege through <exec-type> <from client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>) Parameters Description: exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL). client-ip: It indicates the client's IP address if valid through IP protocol. aaa-method: It indicates the authentication method, e.g.: local, server. server-ip: It indicates the AAA server IP address if authentication method is remote server. username: It indicates the username for authentication.	Informational
Event Description: This log will be generated when enable privilege failure. Log Message: Enable privilege failed through <exec-type> <from client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>) Parameters Description: exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL). client-ip: It indicates the client's IP address if valid through IP protocol. aaa-method: It indicates the authentication method, e.g.: local, server. server-ip: It indicates the AAA server IP address if authentication method is remote server. username: It indicates the username for authentication.	Warning
Event Description: This log will be generated when the remote server does not respond to the enable password authentication request. Log Message: Enable privilege failed through <exec-type> <from client-ip> due to AAA server <server-ip> timeout (Username: <username>) Parameters Description: exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL). client-ip: It indicates the client's IP address if valid through IP protocol. server-ip: It indicates the AAA server IP address if authentication method is remote server. username: It indicates the username for authentication.	Warning

Auto Surveillance VLAN

Log Description	Severity
Event Description: When a new surveillance device is detected on an interface. Log Message: New surveillance device detected (<interface-id>, MAC: <mac-address>) Parameters Description: interface-id: The interface name. mac-address: Surveillance device MAC address.	Informational
Event Description: When an interface that is enabled surveillance, VLAN joins the surveillance VLAN automatically. Log Message: <interface-id> add into surveillance VLAN <vid> Parameters Description: interface-id: The interface name. vid: The VLAN ID.	Informational
Event Description: When an interface leaves the surveillance VLAN and at the same time, no surveillance device is detected in the aging interval for that interface, the log message will be sent. Log Message: <interface-id> remove from surveillance VLAN <vid> Parameters Description: interface-id: The interface name. vid: The VLAN ID.	Informational
Event Description: When an IPC is added in the surveillance VLAN, the log message will be sent. Log Message: ASV: Add IPC(<ipaddr>, MAC: <mac-address>) Parameters Description: ipaddr: Represent the IP address of the IPC.	Informational
Event Description: When an IPC is removed from the surveillance VLAN, the log message will be sent. Log Message: ASV: Remove IPC(<ipaddr>, MAC: <mac-address>) Parameters Description: ipaddr: Represent the IP address of the IPC.	Informational
Event Description: When an NVR is added in the surveillance VLAN, the log message will be sent. Log Message: ASV: Add NVR(<ipaddr>, MAC: <mac-address>) Parameters Description: ipaddr: Represent the IP address of the NVR.	Informational
Event Description: When an NVR is removed from the surveillance VLAN, the log message will be sent. Log Message: ASV: Remove NVR(<ipaddr>, MAC: <mac-address>) Parameters Description: ipaddr: Represent the IP address of the NVR.	Informational
Event Description: When the mode of ASV 2.0 is changed by Web GUI, the log message will be sent. Log Message: ASV: Mode change from <mode> to <mode> Parameters Description: mode: Represent the mode of ASV 2.0. The mode can be standard or surveillance.	Informational

Configuration/Firmware

Log Description	Severity
Event Description: Firmware upgraded successfully.	Informational

Log Description	Severity
Log Message: Firmware upgraded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters Description: session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server. Note: For console, there will be no IP and MAC information for logging.	
Event Description: Firmware upgraded unsuccessfully. Log Message: Firmware upgraded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters Description: session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server. Note: For console, there will be no IP and MAC information for logging.	Warning
Event Description: Firmware uploaded successfully. Log Message: Firmware uploaded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters Description: session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server. Note: For console, there will be no IP and MAC information for logging.	Informational
Event Description: Firmware uploaded unsuccessfully. Log Message: Firmware uploaded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters Description: session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server. Note: For console, there will be no IP and MAC information for logging.	Warning
Event Description: Configuration downloaded successfully. Log Message: Configuration downloaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters Description: session: The user's session. username: Represent current login user. ipaddr: Represent client IP address.	Informational

Log Description	Severity
macaddr: Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server. Note: For console, there will be no IP and MAC information for logging.	
Event Description: Configuration downloaded unsuccessfully. Log Message: Configuration downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters Description: session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server. Note: For console, there will be no IP and MAC information for logging.	Warning
Event Description: Configuration uploaded successfully. Log Message: Configuration uploaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters Description: session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server. Note: For console, there will be no IP and MAC information for logging.	Informational
Event Description: Configuration uploaded unsuccessfully. Log Message: Configuration uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters Description: session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server. Note: For console, there will be no IP and MAC information for logging.	Warning
Event Description: Configuration saved to flash by console. Log Message: Configuration saved to flash by console (Username: <username>) Parameters Description: username: Represent current login user.	Informational
Event Description: Configuration saved to flash by remote. Log Message: Configuration saved to flash (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event Description: Log message uploaded successfully.	Informational

Log Description	Severity
Log Message: Log message uploaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>]) Parameters Description: session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr: Represent client MAC address. Note: For console, there will be no IP and MAC information for logging.	
Event Description: Log message uploaded unsuccessfully. Log Message: Log message uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>]) Parameters Description: session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr: Represent client MAC address. Note: For console, there will be no IP and MAC information for logging.	Warning
Event Description: Unknown type files downloaded unsuccessfully. Log Message: Downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters Description: session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server. Note: For console, there will be no IP and MAC information for logging.	Warning

NOTE:

1. The user's session indicates Console, Web, SNMP, Telnet, or SSH.
2. If update configuration/firmware through Console, there will be no IP and MAC information for logging.

DAI

Log Description	Severity
Event Description: This log will be generated when DAI detect invalid ARP packet. Log Message: Illegal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>) Parameters Description: type: The type of ARP packet, it indicates that ARP packet is request or ARP response.	Warning
Event Description: This log will be generated when DAI detect valid ARP packet. Log Message: Legal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>) Parameters Description: type: The type of ARP packet, it indicates that ARP packet is request or ARP response.	Informational

DDM

Log Description	Severity
Event Description: This log is generated when the any of SFP parameters exceeds from the predefined threshold. Log Message: Optical transceiver <interface-id> <component> <high-low> <type> threshold exceeded Parameters Description: interface-id: The port interface ID. component: DDM threshold type. It can be one of the following types: temperature, supply voltage, bias current, TX power, or RX power high-low: High or low threshold. violate-type: Warning or alarm.	Warning
Event Description: This log is generated when the any of SFP parameters fall below the corresponding warning threshold. Log Message: Optical transceiver <interface-id> <component> back to normal Parameters Description: interface-id: The port interface ID. component: DDM threshold type. It can be one of the following types: temperature, supply voltage, bias current, TX power, or RX power.	Warning

DDP

Log Description	Severity
Event Description: This message means that configuration is automatically saved due to setting changes from DDP. Log Message: CONFIG-6-DDPSAVECONFIG: Configuration automatically saved to flash due to configuring from DDP(Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent the user who executed this function. IP: Represent client IP address.	Informational

DHCPv6 Client

Log Description	Severity
Event Description: DHCPv6 client interface administrator state changed. Log Message: DHCPv6 client on interface <ipif-name> changed state to [enabled | disabled] Parameters Description: ipif-name: Name of the DHCPv6 client interface.	Informational
Event Description: DHCPv6 client obtains an IPv6 address from a DHCPv6 server. Log Message: DHCPv6 client obtains an ipv6 address <ipv6address> on interface <ipif-name> Parameters Description: ipv6address: The IPv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
Event Description: The IPv6 address obtained from a DHCPv6 server starts renewing. Log Message: The IPv6 address <ipv6address> on interface <ipif-name> starts renewing Parameters Description: ipv6address: The IPv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational

Log Description	Severity
Event Description: The IPv6 address obtained from a DHCPv6 server renews success. Log Message: The IPv6 address <ipv6address> on interface <ipif-name> renews success Parameters Description: ipv6address: The IPv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
Event Description: The IPv6 address obtained from a DHCPv6 server starts rebinding. Log Message: The IPv6 address <ipv6address> on interface <ipif-name> starts rebinding Parameters Description: ipv6address: The IPv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
Event Description: The IPv6 address obtained from a DHCPv6 server rebinds success. Log Message: The IPv6 address <ipv6address> on interface <ipif-name> rebinds success Parameters Description: ipv6address: The IPv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
Event Description: The IPv6 address from a DHCPv6 server was deleted. Log Message: The IPv6 address <ipv6address> on interface <ipif-name> was deleted Parameters Description: ipv6address: The IPv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational

DHCPv6 Relay

Log Description	Severity
Event Description: DHCPv6 relay on a specify interface’s administrator state changed. Log Message: DHCPv6 relay on interface <ipif-name> changed state to [enabled | disabled] Parameters Description: ipif-name: Name of the DHCPv6 relay agent interface.	Informational

DNS Resolver

Log Description	Severity
Event Description: Duplicate Domain name cache added, leads a dynamic domain name cache be deleted. Log Message: [DNS-RESOLVER(1):]Duplicate Domain name case name: <domain-name>, static IP: <ipaddr>, dynamic IP:<ipaddr> Parameters Description: domain-name: The domain name string. ipaddr: The IP address.	Informational

DoS Prevention

Log Description	Severity
Event Description: Detect DOS attack. Log Message: <dos-type> is dropped from (IP: <ip-address> Port <interface-id>) Parameters Description:	Notice

Log Description	Severity
dos-type: DOS attack type. ip-address: IP address. interface-id: Interface name.	

Interface

Log Description	Severity
Event Description: When port is down. Log Message: Port <port-type><interface-id> link down Parameters Description: port-type: The port type. interface-id: Interface name.	Informational
Event Description: When port is up. Log Message: Port <port-type><interface-id> link up, <link-speed> Parameters Description: port-type: The port type. interface-id: The interface name. link-speed: The port link speed.	Informational
Event Description: Port is linked on half-duplex mode. Log Message: ASV: Port <interface-id> Half duplex detected Parameters Description: interface-id: Interface name.	Warning

IPv6 Duplicate Address

Log Description	Severity
Event Description: This log will be generated when DUT receives Neighbor Solicitation (NS) message with reduplicated address in the DAD duration. Log Message: Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Solicitation Messages Parameters Description: ipv6address: ipv6 address in Neighbor Solicitation Messages interface-id: Interface name	Warning
Event Description: This log will be generated when DUT receives Neighbor Advertisement (NA) message with reduplicated address in the DAD duration. Log Message: Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Advertisement Messages Parameters Description: ipv6address: ipv6 address in Neighbor Advertisement Messages interface-id: Interface name	Warning

LACP

Log Description	Severity
Event Description: Link Aggregation Group link up. Log Message: Link Aggregation Group <group-id> link up Parameters Description:	Informational

Log Description	Severity
group-id: The group ID of the link down aggregation group.	
Event Description: Link Aggregation Group link down. Log Message: Link Aggregation Group <group-id> link down Parameters Description: group-id: The group ID of the link down aggregation group.	Informational
Event Description: Member port attach to Link Aggregation Group. Log Message: <ifname> attach to Link Aggregation Group <group-id> Parameters Description: ifname: The interface name of the port that attach to aggregation group. group-id: The group ID of the aggregation group that port attach to.	Informational
Event Description: Member port detach from Link Aggregation Group. Log Message: <ifname> detach from Link Aggregation Group <group-id> Parameters Description: ifname: The interface name of the port that detach from aggregation group. group-id: The group ID of the aggregation group that port detach from.	Informational

LBD

Log Description	Severity
Event Description: Record the event when an interface detect loop. Log Message: <interface-id> LBD loop occurred Parameters Description: interface-id: Interface on which loop is detected.	Critical
Event Description: Record the event when an interface detect loop. Log Message: <interface-id> VLAN <vlan-id> LBD loop occurred Parameters Description: interface-id: Interface on which loop is detected. vlan-id: VLAN on which loop is detected.	Critical
Event Description: Record the event when an interface loop recovered. Log Message: <interface-id> LBD loop recovered Parameters Description: interface-id: Interface on which loop is detected.	Critical
Event Description: Record the event when an interface loop recovered. Log Message: <interface-id> VLAN <vlan-id> LBD loop recovered Parameters Description: interface-id: Interface on which loop is detected. vlan-id: VLAN on which loop is detected.	Critical
Event Description: Record the event when the number of VLANs that loop back has occurred exceeds a reserved number. Log Message: Loop VLAN numbers overflow	Critical

LLDP/LLDP-MED

Log Description	Severity
Event Description: LLDP-MED topology change detected Log Message: LLDP-MED topology change detected (on port <portNum>. chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>)	Notice

Log Description	Severity
Parameters Description: portNum: The port number. chassisType: The chassis ID subtype. Value list: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: The chassis ID. portType: The port ID subtype. Value list: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: The port ID. deviceClass: The LLDP-MED device type.	
Event Description: Conflict LLDP-MED device type detected. Log Message: Conflict LLDP-MED device type detected (on port <portNum>, chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>) Parameters Description: portNum: The port number. chassisType: The chassis ID subtype. Value list: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: The chassis ID. portType: The port ID subtype. Value list: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: The port ID. deviceClass: The LLDP-MED device type.	Notice
Event Description: Incompatible LLDP-MED TLV set detected.	Notice

Log Description	Severity
Log Message: Incompatible LLDP-MED TLV set detected (on port <portNum>, chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>) Parameters Description: portNum: The port number. chassisType: The chassis ID subtype. Value list: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: The chassis ID. portType: The port ID subtype. Value list: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: The port ID. deviceClass: The LLDP-MED device type.	

Login/Logout

Log Description	Severity
Event Description: Login through console successfully. Log Message: Successful login through Console (Username: <username>) Parameters Description: username: Represent current login user.	Informational
Event Description: Login through console unsuccessfully. Log Message: Login failed through Console (Username: <username>) Parameters Description: username: Represent current login user.	Warning
Event Description: Console session timed out. Log Message: Console session timed out (Username: <username>) Parameters Description: username: Represent current login user.	Informational
Event Description: Logout through console. Log Message: Logout through Console (Username: <username>) Parameters Description: username: Represent current login user.	Informational
Event Description: Login through Telnet successfully. Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user.	Informational

Log Description	Severity
ipaddr: Represent client IP address.	
Event Description: Login through Telnet unsuccessfully. Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Warning
Event Description: Telnet session timed out. Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event Description: Logout through Telnet. Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event Description: Login through SSH successfully. Log Message: Successful login through SSH (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event Description: Login through SSH unsuccessfully. Log Message: Login failed through SSH (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Critical
Event Description: The SSH session timed out. Log Message: SSH session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event Description: Logout through SSH. Log Message: Logout through SSH (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational

MAC-based Access Control

Log Description	Severity
Event Description: A host has passed the authentication. Log Message: MAC-based Access Control host login success (MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Parameters Description: mac-address: The host MAC address. interface-id: The interface on which the host is authenticated. vlan-id: The VLAN ID on which the host exists.	Informational
Event Description: A host has aged out.	Informational

Log Description	Severity
Log Message: MAC-based Access Control host aged out (MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Parameters Description: mac-address: The host MAC address. interface-id: The interface on which the host is authenticated. vlan-id: The VLAN ID on which the host exists.	
Event Description: A host failed to pass the authentication. Log Message: MAC-based Access Control host login fail (MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Parameters Description: mac-address: The host MAC address. interface-id: The interface on which the host is authenticated. vlan-id: The VLAN ID on which the host exists.	Critical
Event Description: The authorized user number on the whole device has reached the maximum user limit. Log Message: MAC-based Access Control enters stop learning state	Warning
Event Description: The authorized user number on the whole device is below the maximum user limit in a time interval. Log Message: MAC-based Access Control recovers from stop learning state	Warning
Event Description: The authorized user number on an interface has reached the maximum user limit. Log Message: <interface-id> enters MAC-based Access Control stop learning state Parameters Description: interface-id: The interface on which the host is authenticated.	Warning
Event Description: The authorized user number on an interface is below the maximum user limit in a time interval. Log Message: <interface-id> recovers from MAC-based Access Control stop learning state Parameters Description: interface-id: The interface on which the host is authenticated.	Warning

MSTP Debug Enhancement

Log Description	Severity
Event Description: Used to record the event that Spanning Tree Protocol is enabled. Log Message: Spanning Tree Protocol is enabled	Informational
Event Description: Used to record the event that Spanning Tree Protocol is disabled. Log Message: Spanning Tree Protocol is disabled	Informational
Event Description: Used to record MSTP instance topology change event. Log Message: Topology changed (Instance: <Instance-id>,<interface-id>, MAC:<macaddr>) Parameters Description: Instance-id: The MST instance ID. Instance 0 represents for default instance, CIST. interface-id: The port number that detect or receive topology change information. macaddr: The system of bridge MAC address.	Notice
Event Description: Used to record MSTP instance new root bridge selected. Log Message: [CIST | CIST Region | MSTI Region] New Root bridge selected ([Instance: <Instance-id>] MAC: <macaddr> Priority:<priority>) Parameters Description:	Informational

Log Description	Severity
Instance-id: The MST instance ID. Instance 0 represents for default instance, CIST. macaddr: The system of bridge MAC address. priority: The bridge priority value must be divisible by 4096.	
Event Description: Used to record MSTP instance new root port selected. Log Message: New root port selected (Instance:<Instance-id>, <interface-id>) Parameters Description: Instance-id: The MST instance ID. Instance 0 represents for default instance, CIST. interface-id: The port number that detect or receive topology change information.	Notice
Event Description: Used to record MSTP instance port state change event. Log Message: Spanning Tree port status change (Instance:<Instance-id>, <interface-id>) <old-status> -> <new-status> Parameters Description: Instance-id: The MST instance ID. Instance 0 represents for default instance, CIST. interface-id: The port number that detect or receive topology change information. old-status: The old status. new-status: The new status. The port of STP state. The value may be Disable, Discarding, Learning, or Forwarding.	Notice
Event Description: Used to record MSTP instance port role change event. Log Message: Spanning Tree port role change (Instance:<Instance-id>, <interface-id>) <old-role> -> <new-role> Parameters Description: Instance-id: The MST instance ID. Instance 0 represents for default instance, CIST. Interface-id: The port number that detect or receive topology change information. old-role: The old role. new-role: The new role. The port role of STP. The value may be DisabledPort, AlternatePort, BackupPort, RootPort, DesignatedPort, or MasterPort.	Informational
Event Description: Use to record action to create an MST instance. Log Message: Spanning Tree instance created (Instance:<Instance-id>) Parameters Description: Instance-id: The MST instance ID. Instance 0 represents for default instance, CIST.	Informational
Event Description: Use to record action to delete an MST instance. Log Message: Spanning Tree instance deleted (Instance:<Instance-id>) Parameters Description: Instance-id: The MST instance ID. Instance 0 represents for default instance, CIST.	Informational
Event Description: Use to record action to change the STP version. Log Message: Spanning Tree version change (new version:<new-version>) Parameters Description: new-version: Running under which version of STP.	Informational
Event Description: Used to record the configuration name and revision level changed in the MST Configuration Identification. Log Message: Spanning Tree MST configuration ID name and revision level change (name: <name> revision level <revision-level>) Parameters Description: name: The name given for a specified MST region. revision-level: Switches using the same given name but with a different revision level are considered members of different MST regions.	Informational
Event Description: Use to record action to maps a VLAN(s) to an MST instance. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <Instance-id> add vlan <startvlanid> [- <endvlanid>])	Informational

Log Description	Severity
Parameters Description: Instance-id: The MST instance ID. Instance 0 represents for default instance, CIST. startvlanid: The start VID of add VLAN range. endvlanid: The end VID of add VLAN range.	
Event Description: Use to record action to delete a VLAN(s) from an MST instance. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <Instance-id> delete vlan <startvlanid> [- <endvlanid>]) Parameters Description: Instance-id: The MST instance ID. Instance 0 represents for default instance, CIST. startvlanid: The start VID of delete VLAN range. endvlanid: The end VID of delete VLAN range.	Informational
Event Description: Used to record the event that port role change to alternate due to guard root. Log Message: Spanning Tree port role change (Instance:<instance-id>, <interface-id>) to alternate port due to the guard root Parameters Description: Instance-id: The MST instance ID. Instance 0 represents for default instance, CIST. Interface-id: The port number that detect the event.	Informational

Peripheral

Log Description	Severity
Event Description: Fan Recovered. Log Message: <fan-descr> back to normal Parameters Description: fan-descr: The FAN ID and position.	Critical
Event Description: Fan Failed. Log Message: <fan-descr> failed Parameters Description: fan-descr: The FAN ID and position.	Critical
Event Description: Temperature sensor enters alarm state. Log Message: <thermal-sensor-descr> detects abnormal temperature <degree> Parameters Description: thermal-sensor-descr: The sensor ID and position. degree: The current temperature.	Critical
Event Description: Temperature recovers to normal. Log Message: <thermal-sensor-descr> temperature back to normal Parameters Description: thermal-sensor-descr: The sensor ID and position.	Critical
Event Description: Power failed. Log Message: <power-descr> failed Parameters Description: power-descr: The power position and ID.	Critical
Event Description: Power is recovered. Log Message: <power-descr> back to normal Parameters Description: power-descr: The power position and ID.	Critical
Event Description: Press the factory reset button.	Critical

Log Description	Severity
Log Message: Factory reset button pressed	

PoE

Log Description	Severity
Event Description: Total power usage threshold is exceeded. Log Message: Usage threshold <percentage> is exceeded Parameters Description: percentage: The usage threshold.	Warning
Event Description: Total power usage threshold is recovered. Log Message: Usage threshold <percentage> is recovered Parameters Description: percentage: The usage threshold.	Warning
Event Description: PD doesn't reply the ping request. Log Message: ASV: PD alive check failed. (Port: <portNum>, PD: <ipaddr>) Parameters Description: portNum: The port number. ipaddr: The IP address of PD.	Warning

Port Security

Log Description	Severity
Event Description: Address full on a port. Log Message: MAC address <macaddr> causes port security violation on <interface-id> Parameters Description: macaddr: The violation MAC address. interface-id: The interface ID.	Warning
Event Description: Address full on system. Log Message: Limit on system entry number has been exceeded	Warning

Safeguard

Log Description	Severity
Event Description: The host enters the exhausted mode. Log Message: Safeguard Engine enters EXHAUSTED mode	Warning
Event Description: The host enters the normal mode. Log Message: Safeguard Engine enters NORMAL mode	Informational

SNMP

Log Description	Severity
Event Description: SNMP request received with invalid community string. Log Message: SNMP request received from <ipaddr> with invalid community string Parameters Description: ipaddr: The IP address.	Informational

SSH

Log Description	Severity
Event Description: The SSH server is enabled. Log Message: SSH server is enabled	Informational
Event Description: The SSH server is disabled. Log Message: SSH server is disabled	Informational

Storm Control

Log Description	Severity
Event Description: Storm occurrence. Log Message: <Broadcast | Multicast | Unicast> storm is occurring on <interface-id> Parameters Description: Broadcast: Storm is resulted by broadcast packets (DA = FF:FF:FF:FF:FF:FF). Multicast: Storm is resulted by multicast packets, including unknown L2 multicast, known L2 multicast, unknown IP multicast, and known IP multicast. Unicast: Storm is resulted by unicast packets, including both known and unknown unicast packets. interface-id: The interface ID on which a storm is occurring.	Warning
Event Description: Storm cleared. Log Message: <Broadcast | Multicast | Unicast> storm is cleared on <interface-id> Parameters Description: Broadcast: Broadcast storm is cleared. Multicast: Multicast storm is cleared. Unicast: Unicast storm (including both known and unknown unicast packets) is cleared. interface-id: The interface ID on which a storm is cleared.	Informational
Event Description: Port shut down due to a packet storm. Log Message: <interface-id> is currently shut down due to the <Broadcast | Multicast | Unicast> storm Parameters Description: interface-id: The interface ID on which is error-disabled by storm. Broadcast: The interface is disabled by broadcast storm. Multicast: The interface is disabled by multicast storm. Unicast: The interface is disabled by unicast storm (including both known and unknown unicast packets).	Warning

System

Log Description	Severity
Event Description: This log will be generated when system warm start. Log Message: System warm start	Critical
Event Description: This log will be generated when system cold start. Log Message: System cold start	Critical
Event Description: This log will be generated when system start up. Log Message: System started up	Critical

Telnet

Log Description	Severity
Event Description: Successful login through Telnet. Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: ipaddr: The IP address of Telnet client. username: The username that used to login Telnet server.	Informational
Event Description: Login failed through Telnet. Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: ipaddr: The IP address of Telnet client. username: The username that used to login Telnet server.	Warning
Event Description: Logout through Telnet. Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: ipaddr: The IP address of Telnet client. username: The username that used to login Telnet server.	Informational
Event Description: Telnet session timed out. Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: ipaddr: The IP address of Telnet client. username: The username that used to login Telnet server.	Informational

Voice VLAN

Log Description	Severity
Event Description: When a new voice device is detected on an interface. Log Message: New voice device detected (<interface-id>, MAC: <mac-address>) Parameters Description: interface-id: Interface name. mac-address: Voice device MAC address.	Informational
Event Description: When an interface that is in auto voice VLAN mode joins the voice VLAN. Log Message: <interface-id> add into voice VLAN <vid> Parameters Description: interface-id: The interface name. vid: The VLAN ID.	Informational
Event Description: When an interface leaves the voice VLAN and at the same time, no voice device is detected in the aging interval for that interface, the log message will be sent. Log Message: <interface-id> remove from voice VLAN <vid> Parameters Description: interface-id: The interface name. vid: The VLAN ID.	Informational

Web

Log Description	Severity
Event Description: Successful login through Web. Log Message: Successful login through Web (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational
Event Description: Login failed through Web. Log Message: Login failed through Web (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username that used to login HTTP server. ipaddr: The IP address of HTTP client.	Warning
Event Description: Web session timed out. Log Message: Web session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational
Event Description: Logout through Web. Log Message: Logout through Web (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational
Event Description: Successful login through Web (SSL). Log Message: Successful login through Web (SSL) (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username that used to login SSL server. ipaddr: The IP address of SSL client.	Informational
Event Description: Login failed through Web (SSL). Log Message: Login failed through Web (SSL) (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username that used to login SSL server. ipaddr: The IP address of SSL client.	Warning
Event Description: Web (SSL) session timed out. Log Message: Web (SSL) session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username that used to login SSL server. ipaddr: The IP address of SSL client.	Informational
Event Description: Logout through Web (SSL). Log Message: Logout through Web (SSL) (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username that used to login SSL server. ipaddr: The IP address of SSL client.	Informational

Appendix B - Trap Entries

The following table lists the trap log entries and their corresponding meanings that will appear in the Switch.

802.1X

Trap Name	Description	OID
dDot1xExtLoggedSuccess	This trap is sent when a host has successfully logged in (passed 802.1X authentication). Binding objects: (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName	1.3.6.1.4.1.171.11.165.1000.30.0.1
dDot1xExtLoggedFail	This trap is sent when a host failed to pass IEEE 802.1X authentication (login failed). Binding objects: (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName (5) dDot1xExtNotifyFailReason	1.3.6.1.4.1.171.11.165.1000.30.0.2

Authentication Fail

Trap Name	Description	OID
authenticationFailure	This trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.	1.3.6.1.6.3.1.1.5.5

DDM

Trap Name	Description	OID
swDdmAlarmTrap	A notification is generated when an abnormal alarm situation occurs, or recovers from an abnormal alarm situation to normal status. Binding objects: (1) dDdmNotifyInfoIfIndex (2) dDdmNotifyInfoComponent (3) dDdmNotifyInfoAbnormalLevel (4) dDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.171.11.165.1000.72.0.1
swDdmWarningTrap	A notification is generated when an abnormal warning situation occurs, or recovers from an abnormal warning situation to normal status. Binding objects: (1) dDdmNotifyInfoIfIndex (2) dDdmNotifyInfoComponent (3) dDdmNotifyInfoAbnormalLevel	1.3.6.1.4.1.171.11.165.1000.72.0.2

Trap Name	Description	OID
	(4) dDdmNotifyInfoThresholdExceedOrRecover	

DHCP Server Screen Prevention

Trap Name	Description	OID
dDhcpFilterAttackDetected	When DHCP Server Screen is enabled, if the switch received the forge DHCP Server packet, the switch will trap the event if any attacking packet is received. Binding objects: (1) dDhcpFilterLogBufServerIpAddr (2) dDhcpFilterLogBufClientMacAddr (3) dDhcpFilterLogBufferVlanId (4) dDhcpFilterLogBufferOccurTime	1.3.6.1.4.1.171.11.165.1000.133.0.1

DoS Prevention

Trap Name	Description	OID
dDosPreveAttackDetectedPacket	This trap is sent when detect DOS attack. Binding objects: (1) dDoSPrevCtrlAttackType (2) dDosPrevNotiInfoDropIpAddr (3) dDosPrevNotiInfoDropPortNumber	1.3.6.1.4.1.171.11.165.1000.59.0.2

ErrDisable

Trap Name	Description	OID
dErrDisNotifyPortDisabledAssert	This trap is sent when a port enters into error-disabled state. Binding objects: (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.171.11.165.1000.45.0.1
dErrDisNotifyPortDisabledClear	The trap is sent when a port loop restarts after the interval time. Binding objects: (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.171.11.165.1000.45.0.2

General Management

Trap Name	Description	OID
dGenMgmtLoginFail	This trap is sent when the user login failed to the switch. Binding objects: (1) dGenMgmtNotifyInfoLoginType (2) dGenMgmtNotifyInfoUserName	1.3.6.1.4.1.171.11.165.1000.165.0.1

Gratuitous ARP Trap

Trap Name	Description	OID
agentGratuitousARPTrap	This trap is sent when IP address conflicted. Binding objects: (1) ipaddr (2) macaddr (3) portNumber (4) agentGratuitousARPInterfaceName	1.3.6.1.4.1.171.11.165.1000.75.0.1

IMPB

Trap Name	Description	OID
dImpbViolationTrap	This notification is generated when IP-MAC-Port binding address violation is detected. Binding objects: (1) ifIndex (2) dImpbViolationIpAddrType (3) dImpbViolationIpAddress (4) dImpbViolationMacAddress	1.3.6.1.4.1.171.11.165.1000.22.0.1

LACP

Trap Name	Description	OID
linkUp	This trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus. Binding objects: (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.4
linkDown	This trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus. Binding objects: (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.3

LBD

Trap Name	Description	OID
dLbdLoopOccurred	This trap is sent when an interface loop occurs. Binding objects: (1) dLbdNotifyInfoIfIndex	1.3.6.1.4.1.171.11.165.1000.46.0.1

Trap Name	Description	OID
dLbdLoopRestart	This trap is sent when an interface loop restarts after the interval time. Binding objects: (1) dLbdNotifyInfoIfIndex	1.3.6.1.4.1.171.11.165.1000.46.0.2
dLbdVlanLoopOccurred	This trap is sent when an interface with a VID loop occurs. Binding objects: (1) dLbdNotifyInfoIfIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.171.11.165.1000.46.0.3
dLbdVlanLoopRestart	This trap is sent when an interface loop with a VID restarts after the interval time. Binding objects: (1) dLbdNotifyInfoIfIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.171.11.165.1000.46.0.4

LLDP

Trap Name	Description	OID
lldpRemTablesChange	This notification is sent when the value of lldpStatsRemTableLastChangeTime changes. It can be utilized by an NMS to trigger LLDP remote systems table maintenance polls. Binding objects: (1) lldpStatsRemTablesInserts (2) lldpStatsRemTablesDeletes (3) lldpStatsRemTablesDrops (4) lldpStatsRemTablesAgeouts	1.0.8802.1.1.2.0.0.1
lldpXMedTopologyChangeDetected	A notification generated by the local device sensing a change in the topology that indicates that a new remote device attached to a local port, or a remote device disconnected or moved from one port to another. Binding objects: (1) lldpRemChassisIdSubtype (2) lldpRemChassisId (3) lldpXMedRemDeviceClass	1.0.8802.1.1.2.1.5.4795.0.1

MAC-based Access Control

Trap Name	Description	OID
dMacAuthLoggedSuccess	The trap is sent when a MAC-based Access Control host is successfully logged in. Binding objects: (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.171.11.165.1000.153.0.1
dMacAuthLoggedFail	The trap is sent when a MAC-based Access Control host login fails. Binding objects: (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.171.11.165.1000.153.0.2

Trap Name	Description	OID
dMacAuthLoggedAgesOut	The trap is sent when a MAC-based Access Control host ages out. Binding objects: (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.171.11.165.1000.153.0.3

MAC Notification

Trap Name	Description	OID
dL2FdbMacNotification	This trap indicate the MAC addresses variation in the address table. Binding objects: (1) dL2FdbMacChangeNotifyInfo	1.3.6.1.4.1.171.11.165.1000.3.0.1

MSTP

Trap Name	Description	OID
newRoot	This trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root. For example, upon expiration of the Topology Change Timer, immediately subsequent to its election. Implementation of this trap is optional.	1.3.6.1.2.1.17.0.1
topologyChange	This trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional.	1.3.6.1.2.1.17.0.2

PD Alive

Trap Name	Description	OID
dPoeIfPdAliveFailOccurNotification	This trap indicates if the PD reply the ping request. At least 500 ms must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethMainPseGroupIndex (2) pethPsePortIndex (3) dPoeIfPdAliveCfgPdIpType (4) dPoeIfPdAliveCfgPdIpAddr	1.3.6.1.4.1.171.14.24.0.4

Peripheral

Trap Name	Description	OID
dEntityExtFanStatusChg	Fan status change notification. Binding objects: (1) dEntityExtEnvFanIndex (2) dEntityExtEnvFanStatus	1.3.6.1.4.1.171.11.165.1000.5.0.1

Trap Name	Description	OID
dEntityExtThermalStatusChg	Temperature status change notification. Binding objects: (1) dEntityExtEnvTempIndex (2) dEntityExtEnvTempStatus	1.3.6.1.4.1.171.11.165.1000.5.0.2
dEntityExtFactoryResetButton	Press the factory reset button.	1.3.6.1.4.1.171.11.165.1000.5.0.5

PoE

Trap Name	Description	OID
pethMainPowerUsageOnNotification	This trap indicates PSE Threshold usage indication is on, the usage power is above the threshold. At least 500 ms must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethMainPseConsumptionPower	1.3.6.1.2.1.105.0.2
pethMainPowerUsageOffNotification	This trap indicates PSE Threshold usage indication is off; the usage power is below the threshold. At least 500 ms must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethMainPseConsumptionPower	1.3.6.1.2.1.105.0.3
dPoeIfPowerDeniedNotification	This notification indicates if PSE state diagram enters the state POWER_DENIED. At least 500 ms must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethPsePortPowerDeniedCounter	1.3.6.1.4.1.171.11.165.1000.24.0.1
dPoeIfPowerOverLoadNotification	This trap indicates if PSE state diagram enters the state ERROR_DELAY_OVER. At least 500 ms must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethPsePortOverLoadCounter	1.3.6.1.4.1.171.11.165.1000.24.0.2
dPoeIfPowerShortCircuitNotification	This trap indicates if PSE state diagram enters the state ERROR_DELAY_SHORT. At least 500 ms must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethPsePortShortCounter	1.3.6.1.4.1.171.11.165.1000.24.0.3

Port

Trap Name	Description	OID
linkUp	This notification is generated when the port link is up. Binding objects: (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.4
linkDown	This notification is generated when the port link is down. Binding objects: (1) ifIndex (2) ifAdminStatus	1.3.6.1.6.3.1.1.5.3

Trap Name	Description	OID
	(3) ifOperStatus	

Port Security

Trap Name	Description	OID
dPortSecMacAddrViolation	When the port security trap is enabled, new MAC addresses that violate the pre-defined port security configuration will trigger trap messages to be sent out. Binding objects: (1) ifIndex (2) dPortSecIfCurrentStatus (3) dPortSecIfLastMacAddress	1.3.6.1.4.1.171.11.165.1000.8.0.1

RMON

Trap Name	Description	OID
risingAlarm	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps. Binding objects: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmRisingThreshold	1.3.6.1.2.1.16.0.1
fallingAlarm	The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps. Binding objects: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmFallingThreshold	1.3.6.1.2.1.16.0.2

Safeguard

Trap Name	Description	OID
dSafeguardChgToExhausted	This trap indicates System change operation mode from normal to exhaust. Binding objects: (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.171.11.165.1000.19.1.1.0.1
dSafeguardChgToNormal	This trap indicates system change operation mode from exhausted to normal. Binding objects: (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.171.11.165.1000.19.1.1.0.2

Start

Trap Name	Description	OID
coldStart	This trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.	1.3.6.1.6.3.1.1.5.1
warmStart	This trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.	1.3.6.1.6.3.1.1.5.2

Storm Control

Trap Name	Description	OID
dStormCtrlOccurred	This trap is sent when dStormCtrlNotifyEnable is 'stormOccurred' or 'both' and a storm is detected. Binding objects: (1) ifIndex (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.171.11.165.1000.25.0.1
dStormCtrlStormCleared	This trap is sent when dStormCtrlNotifyEnable is 'stormCleared' or 'both' and a storm is cleared. Binding objects: (1) ifIndex (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.171.11.165.1000.25.0.2

System File

Trap Name	Description	OID
dsfUploadImage	The notification is sent when the user uploads image file successfully.	1.3.6.1.4.1.171.11.165.1000.14.0.1
dsfDownloadImage	The notification is sent when the user downloads image file successfully.	1.3.6.1.4.1.171.11.165.1000.14.0.2
dsfUploadCfg	The notification is sent when the user uploads configuration file successfully.	1.3.6.1.4.1.171.11.165.1000.14.0.3
dsfDownloadCfg	The notification is sent when the user downloads configuration file successfully.	1.3.6.1.4.1.171.11.165.1000.14.0.4
dsfSaveCfg	The notification is sent when the user saves configuration file successfully.	1.3.6.1.4.1.171.11.165.1000.14.0.5

Appendix C - RADIUS Attributes Assignment

The RADIUS Attributes Assignment on the Switch is used in the following modules: Console, Telnet, SSH, Web, 802.1X and MAC-based Access Control.

The description that follows explains the following RADIUS Attributes Assignment types:

- Privilege Level
- VLAN

To assign the **Privilege Level** by the RADIUS server, the proper parameters should be configured on the RADIUS server. The table below shows the parameters for the privilege level.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	1	Required
Attribute-Specific Field	Used to assign the privilege level of the user to operate the Switch.	Range (1-15)	Required

If the user has configured the privilege level attribute of the RADIUS server (for example, level 15) and the Console, Telnet, SSH, and Web authentication is successful, the device will assign the privilege level (according to the RADIUS server) to this access user. However, if the user does not configure the privilege level attribute and authenticates successfully, the device will not assign any privilege level to the access user. If the privilege level is configured less than the minimum supported value or greater than the maximum supported value, the privilege level will be ignored.

To assign the **VLAN** by the RADIUS server, the proper parameters should be configured on the RADIUS server. To use VLAN assignment, RFC 3580 defines the following tunnel attributes in RADIUS packets.

The table below shows the parameters for a VLAN:

RADIUS Tunnel Attribute	Description	Value	Usage
Tunnel-Type	This attribute indicates the tunneling protocol(s) to be used (in the case of a tunnel initiator) or the tunneling protocol in use (in the case of a tunnel terminator).	13 (VLAN)	Required
Tunnel-Medium-Type	This attribute indicates the transport medium being used.	6 (802)	Required
Tunnel-Private-Group-ID	This attribute indicates group ID for a particular tunneled session.	A string (VID)	Required

A summary of the Tunnel-Private-Group-ID Attribute format is shown below.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |     Tag       |   String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The table below shows the definition of Tag field (different with RFC 2868):

Tag field value	String field format
0x01	VLAN name (ASCII)
0x02	VLAN ID (ASCII)
Others (0x00, 0x03 ~ 0x1F, >0x1F)	When the Switch receives the VLAN setting string, it will think it is the VLAN ID first. In other words, the Switch will check all existing VLAN IDs and check if there is one matched. If the Switch can find one matched, it will move to that VLAN. If the Switch cannot find the matched VLAN ID, it will think the VLAN setting string as a "VLAN Name". Then it will check that it can find out a matched VLAN Name.

NOTE: A tag field of greater than 0x1F is interpreted as the first octet of the following field.

If the user has configured the VLAN attribute of the RADIUS server (for example, VID 3) and the 802.1X, or MAC based Access Control is successful, the port will be assigned to VLAN 3. However, if the user does not configure the VLAN attributes, when the port is not guest VLAN member, it will be kept in its current authentication VLAN, and when the port is guest VLAN member, it will be assigned to its original VLAN.

Appendix D - IETF RADIUS Attributes Support

Remote Authentication Dial-In User Service (RADIUS) attributes carry specific authentication, authorization, information, and configuration details for the request and reply. This appendix lists the RADIUS attributes currently supported by the Switch.

RADIUS attributes are supported by the IETF standard and Vendor-Specific Attribute (VSA). VSA allows the vendor to create an additionally owned RADIUS attribute. For more information about D-Link VSA, refer to **Appendix C - RADIUS Attributes Assignment**.

IETF standard RADIUS attributes are defined in the RFC 2865 Remote Authentication Dial-In User Service (RADIUS), RFC 2866 RADIUS Accounting, and RFC 2868 RADIUS Attributes for Tunnel Protocol Support, and RFC 2869 RADIUS Extensions.

The following table lists the IETF **RADIUS Authentication Attributes** supported by the D-Link Switch.

Number	IETF Attribute
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
7	Framed-Protocol
8	Framed-IP-Address
12	Framed-MTU
18	Reply-Message
24	State
26	Vendor-Specific
27	Session-Timeout
29	Termination-Action
30	Called-Station-ID
31	Calling-Station-ID
32	NAS-Identifier
60	CHAP-Challenge
61	NAS-Port-Type
64	Tunnel-Type
65	Tunnel-Medium-Type
77	Connect-Info
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID
85	Acct-Interim-Interval
87	NAS-Port-ID
95	NAS-IPv6-Address