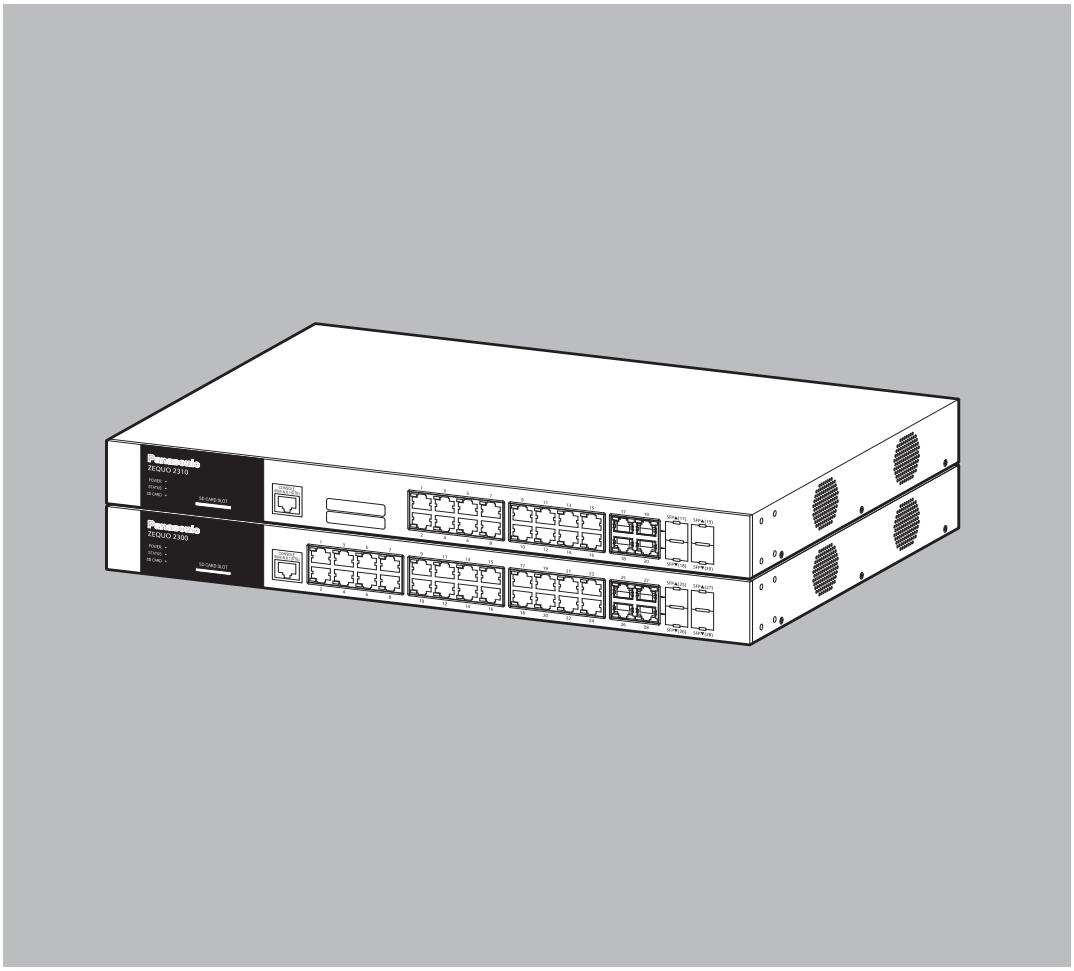
Panasonic

ZEQUO Series

WEB Reference

Model Number: PN26241K/PN26161K



The target model for this WEB reference is as follows.

Model name	Model number	Firmware version
ZEQUO 2300	PN26241K	1.0.0.05 and above
ZEQUO 2310	PN26161K	1.0.0.05 and above

Table of Contents

1 Introduction

The Web User Interface (Web UI) manual is intended for IT professionals who are familiar with Ethernet and Computer Networking principles. This document illustrates and explains the software features available in the Web UI of switches in this series. Switches in this series (**ZEQUO2300** and **ZEQUO2310**) are equipped with an identical set of software features available in the Web UI and will simply be referred to as the 'switch' in this document.

1.1 Related Documentation

The switch can be configured and managed not only through the Web UI, but also through the Command Line Interface (CLI). For more information about the CLI, refer to the *Panasonic ZEQUO2300/2310Command Line Interface Manual*.

2 The Web User Interface (Web UI)

2.1 Connecting to the Web UI

The Web UI of the switch can be accessed using a standard Web browser on any networking node connected to the Ethernet ports of the switch directing or indirectly. Additional security configurations can be made in the Web UI to restrict access to the switch.
The default **IPv4 Address** of the switch is 0.0.0.0 (not configured).
Out of the box, the CLI should be used, through the Console port, to configure the IPv4 address of the switch. Refer to the *Panasonic ZEQUO2300/2310 Command Line Interface Manual* for more information.
Open the Web browser, enter the IPv4 address of the switch into the Uniform Resource Locator (URL) address bar and press **Enter**.

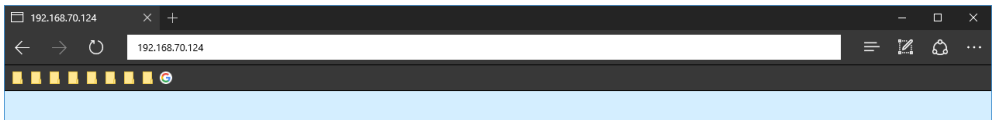


Figure 2-1 Enter IPv4 Address

The default **User Name** and **Password** is 'manager'.
Enter the **User Name** and **Password** in the spaces provided and click the Login button.

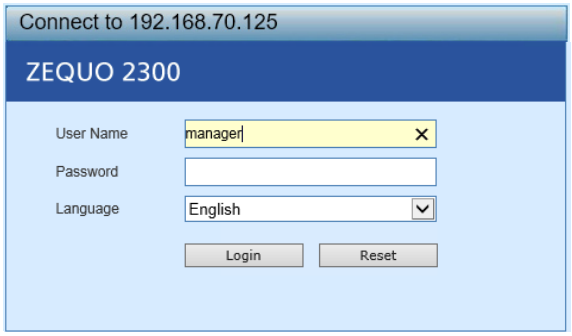


Figure 2-2 Login Window

Access to the Web UI will be given after a successful login.

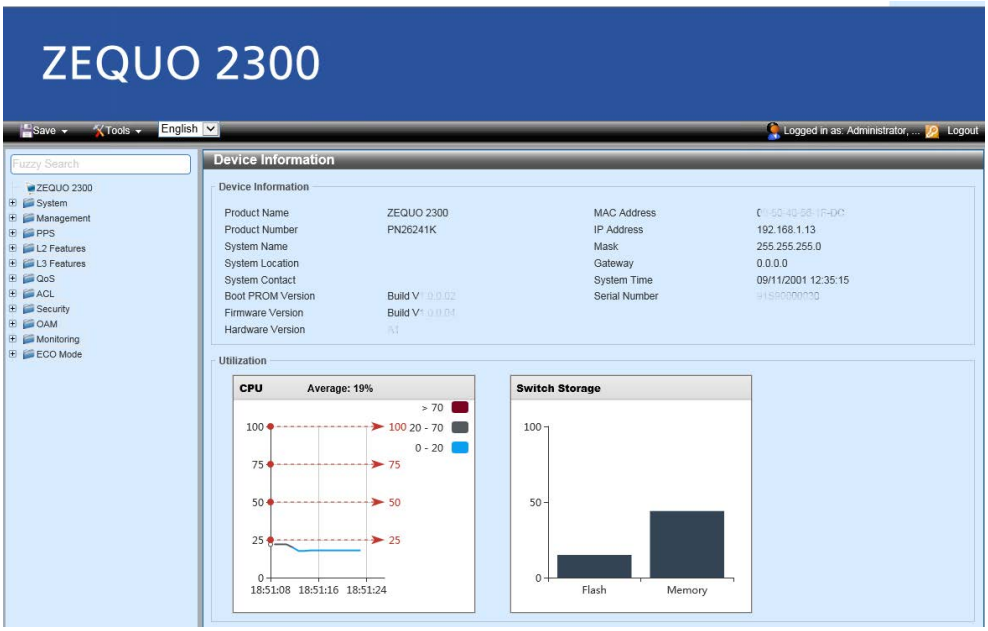


Figure 2-3 Main Web UI Window

2.2 Understanding the Web UI

The Web UI is divided into two main sections (Frame A and Frame B as illustrated in the figure below).

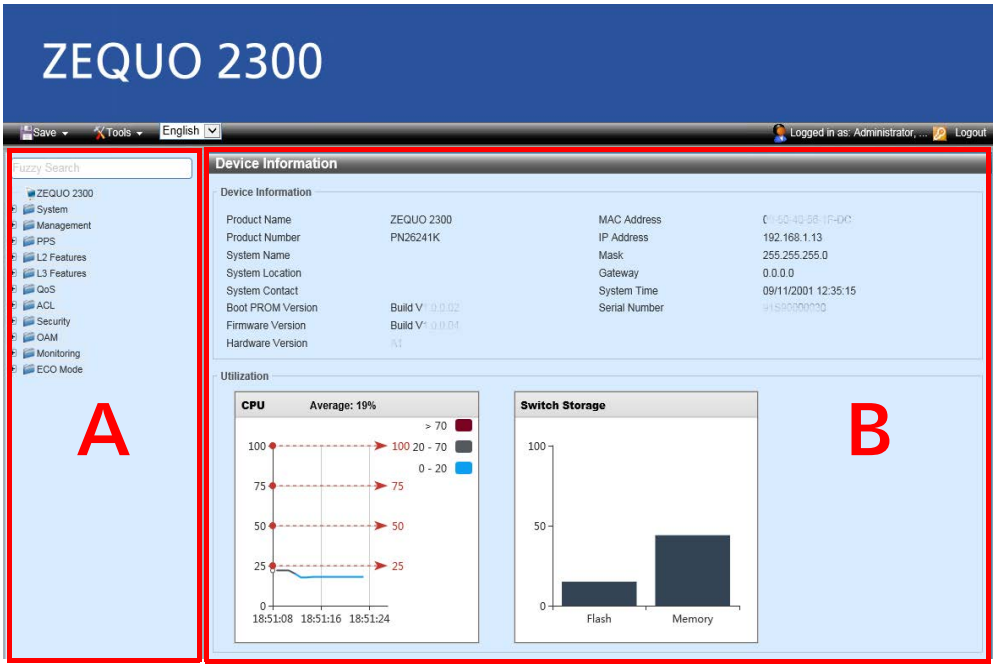


Figure 2-4

All the features available in the Web UI of the switch are grouped into folders in Frame A. In Frame A, click the folder (for example **System**) and then click the feature link (for example **System Information Settings**) to access the configuration window in Frame B. Configuration and management can be done in Frame B.
The following chapters will discuss all the software features in the order they are presented in Frame A.

3 System

3.1 Device Information

This window is used to display general switch information and utilization. This is the first window that will be displayed after logging in to the Web UI of the switch.

Click the **ZEQUO2300** link (in Frame A) to view the following window:

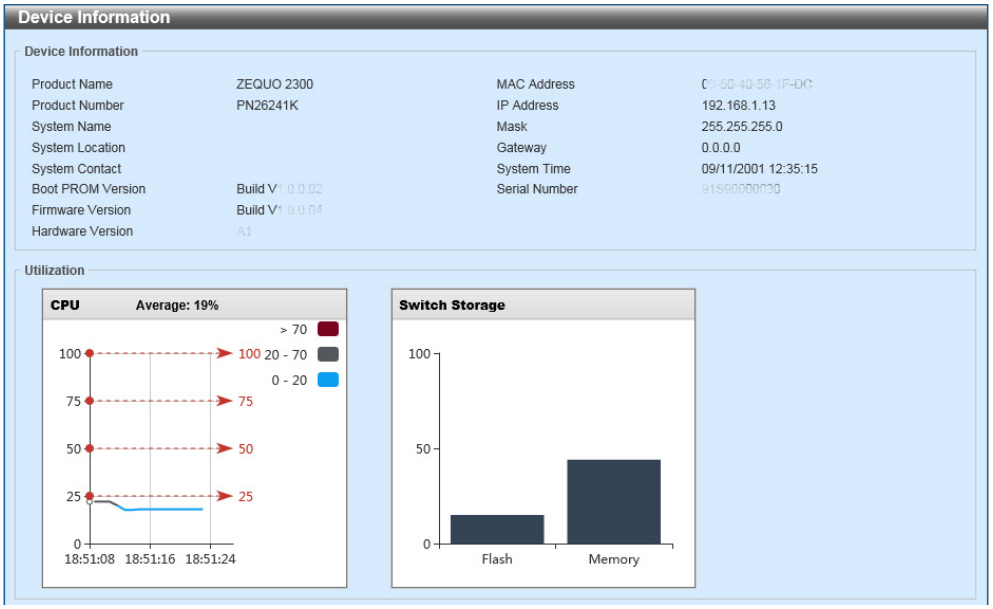


Figure 3-1 Device Information

3.2 System Information Settings

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

Click **System > System Information Settings** to view the following window:

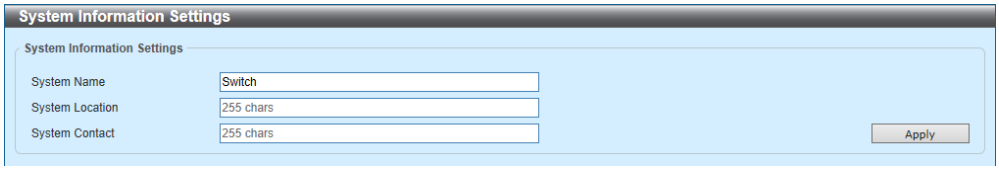


Figure 3-2 System Information Settings

The following parameters can be configured in the **System Information Settings** section:

Parameter	Description
System Name	Enter a system name for the switch. This name can be used to identify the switch in the network.
System Location	Enter the location description of the switch.
System Contact	Enter a contact name for the switch. Generally, this is the name of the person or company responsible for configuring and maintaining the switch.

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

3.3 Peripheral Settings

This window is used to configure and display the peripheral settings.

Click **System > Peripheral Settings** to view the following window:

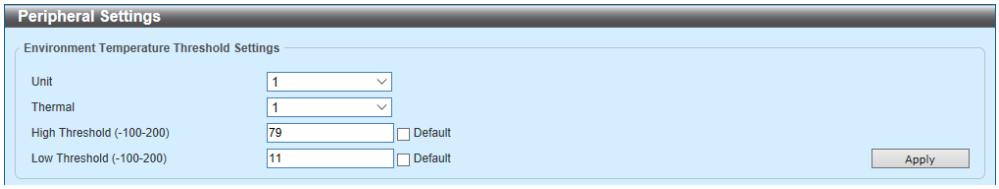


Figure 3-3 Peripheral Settings

The following parameters can be configured in the **Environment Temperature Threshold Settings** section:

Parameter	Description
Unit	Select the unit ID of the switch in the physical stack here.
Thermal	Select the thermal sensor ID.
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.

3.4 Port Configuration

3.4.1 Port Settings

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

Click **System > Port Configuration > Port Settings** to view the following window:

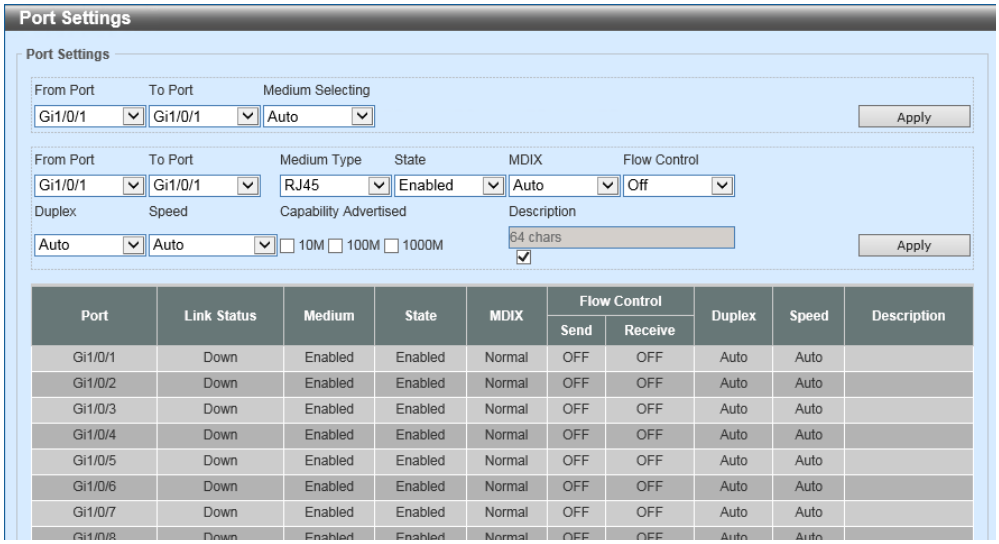


Figure 3-4 Port Settings

The following parameters can be configured in the **Port Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Medium Selecting	Select the port medium type here. Options to choose from are **Auto**, **RJ45** and **SFP**. SFP stands for Small Form-factor Pluggable.
Medium Type	Select the port medium type here. Options to choose from are **RJ45** and **SFP**.
State	Select this option to enable or disabled the physical port here.

Parameter	Description
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 LAN adapter using a straight-through cable or a port (in the MDI mode) on another Switch through a cross-over cable. • **Cross** - Select this option for cross-over 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.
Flow Control	Select to turn flow control **On** or **Off** here. Ports configured for full-duplex use 802.3x flow control and **Auto** ports use an automatic selection of the two.
Duplex	Select the duplex mode used here. Options to choose from are **Auto** and **Full**.
Speed	Select the port speed option here. This option will manually force the connection speed on the selected port to connect only at the speed specified here. 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.

Parameter	Description
Speed	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 10Mbps. This option is only available for 10Mbps copper connections. • **100M** - Specifies to force the port speed to 100Mbps. This option is only available for 100Mbps copper connections. • **1000M** - Specifies to force the port speed to 1Gbps. This option is only available for 1Gbps fiber connections. • **1000M** Master - Specifies to force the port speed to 1Gbps and operates as the master, to facilitate the timing of transmit and receive operations. This option is only available for 1Gbps copper connections. • **1000M** Slave - Specifies to force the port speed to 1Gbps and operates as the slave, to facilitate the timing of transmit and receive operations. This option is only available for 1Gbps copper connections.
Capability Advertised	When the **Speed** is set to **Auto**, these capabilities are advertised during auto-negotiation.
Description	Enter a description for the corresponding port here. This can be up to 64 characters.

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

3.4.2 Port Status

This window is used to display the physical port status and settings on the switch.

Click **System > Port Configuration > Port Status** to view the following window:

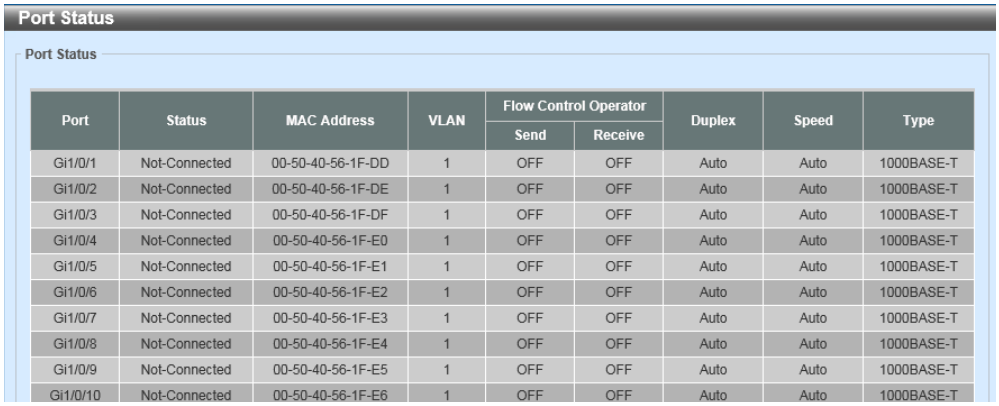


Figure 3-5 Port Status

3.4.3 Port GBIC

This window is used to display information related to the transceivers plugged into the physical ports on the switch. GBIC stands for Gigabit Interface Converter.

Click **System > Port Configuration > Port GBIC** to view the following window:

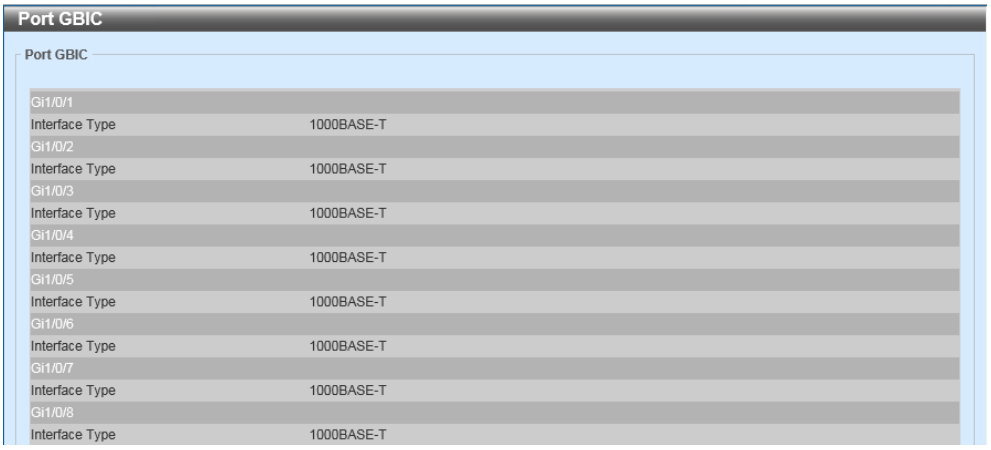


Figure 3-6 Port GBIC

3.4.4 Port Auto Negotiation

This window is used to display the port auto-negotiation table and information.

Click **System > Port Configuration > Port Auto Negotiation** to view the following window:

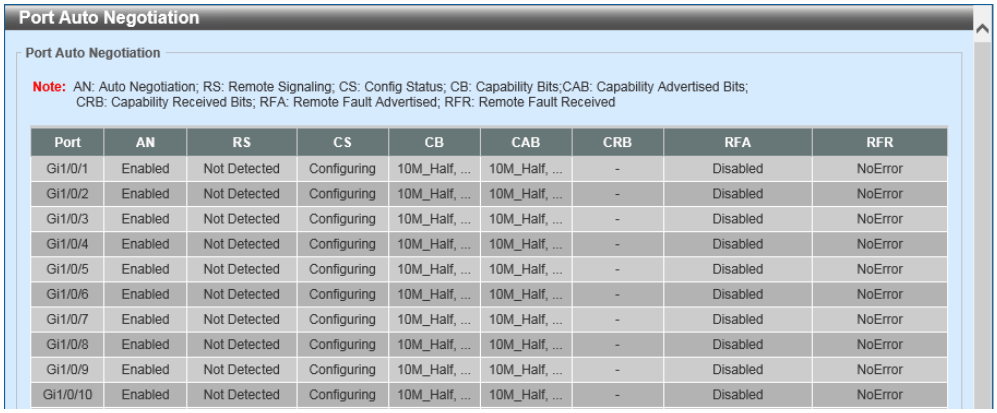


Figure 3-7 Port Auto Negotiation

3.4.5 Error Disable Settings

This window is used to configure and display the settings related to the Error Disable feature.

Click **System > Port Configuration > Error Disable Settings** to view the following window:

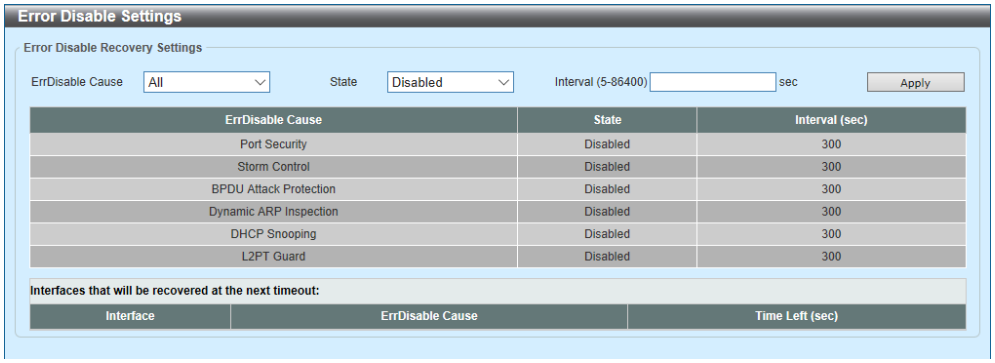


Figure 3-8 Error Disable Settings

The following parameters can be configured in the **Error Disable Recovery Settings** section:

Parameter	Description
ErrDisable Cause	Select the error disabled cause here. Options to choose from are All, Port Security, Storm Control, BPDU Attack Protection, Dynamic ARP Inspection, DHCP Snooping, and L2PT Guard.
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.

3.4.6 Jumbo Frame

This window is used to configure and display the jumbo frame settings. Jumbo frames are Ethernet frames with more than 1518 bytes of payload.

Click **System > Port Configuration > Jumbo Frame** to view the following window:

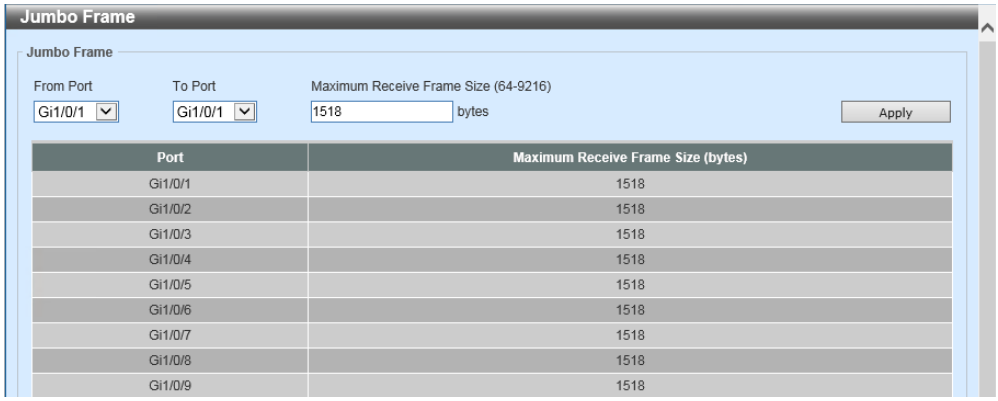


Figure 3-9 Jumbo Frame

The following parameters can be configured in the **Jumbo Frame** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Maximum receive frame size	Receive Frame SizeEnter the maximum receive frame size value here. The range is from 64 to 9216 bytes. By default, this value is 1518 bytes.

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

3.5 System Log

3.5.1 System Log Settings

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

Click **System > System Log > System Log Settings** to view the following window:

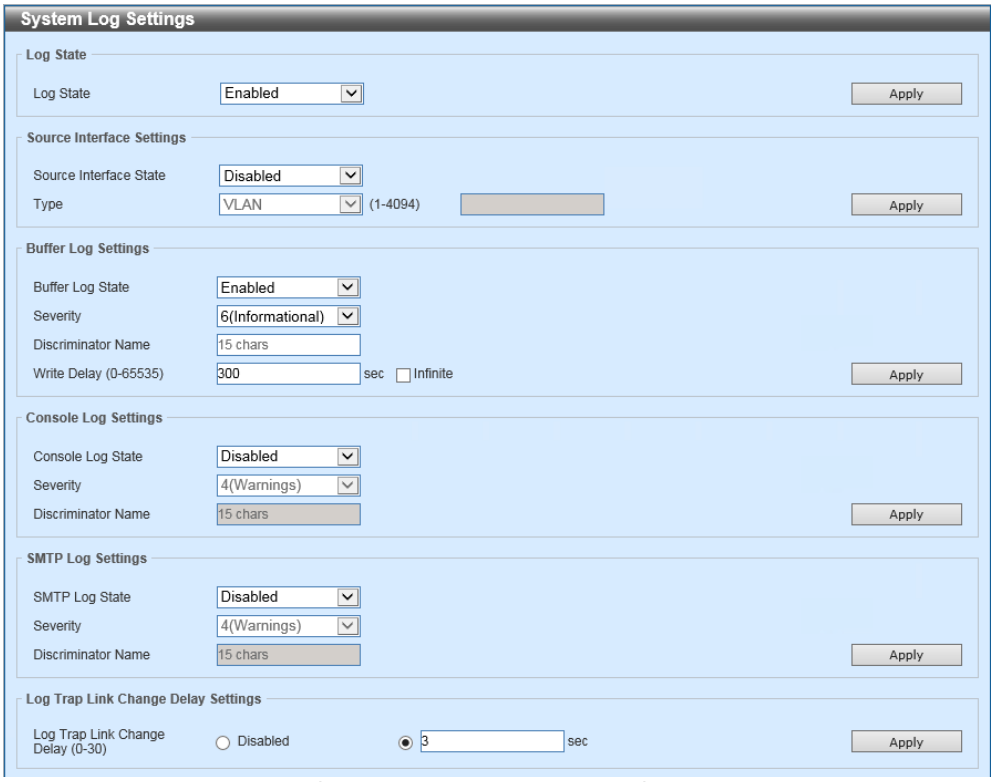


Figure 3-10 System Log Settings

The following parameters can be configured in the **Log State** section:

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 following parameters can be configured in the **Source Interface Settings** section:

Parameter	Description
Source Interface State	Select this option to enable or disable the global source interface state.
Type	Select the type of interface that will be used. Options to choose from are **Loopback** and **VLAN**.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094. The range of loopback interfaces are from 1 to 8.

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

The following parameters can be configured in the **Buffer Log Settings** section:

Parameter	Description
Buffer Log State	Select to enable or disable the global 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 write delay value for the log here. The range is from 0 to 65535 seconds. By default, this value is 300 seconds. Select the **Infinite** option, to disable the write delay feature.

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

The following parameters can be configured in the **Console Log** Settings section:

Parameter	Description
Console Log State	Select to enable or disable the global console log state here.
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 console log messages based on the filtering criteria specified within that profile.

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

The following parameters can be configured in the **SMTP Log Settings** section:

Parameter	Description
SMTP Log State	Select to enable or disable the global Simple Mail Transfer Protocol (SMTP) log state here.
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 SMTP log messages based on the filtering criteria specified within that profile.

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

The following parameters can be configured in the **Log Trap Link Change Delay Settings** section:

Parameter	Description
Log Trap Link Change	Enables issuance delays for system logs and SNMP traps related to the link state of physical ports.The range is from 1 to 30 (seconds). When using the link aggregation on your device, if the system logs and SNMP traps regarding the link status of the physical port cannot be normally transmitted to the SYSLOG server or SNMP server, you may be able to solve issue by using this function. The recommendation value is 5 seconds when using this function.

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

3.5.2 System Log Discriminator Settings

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

Click **System > System Log > System Log Discriminator Settings** to view the following window:

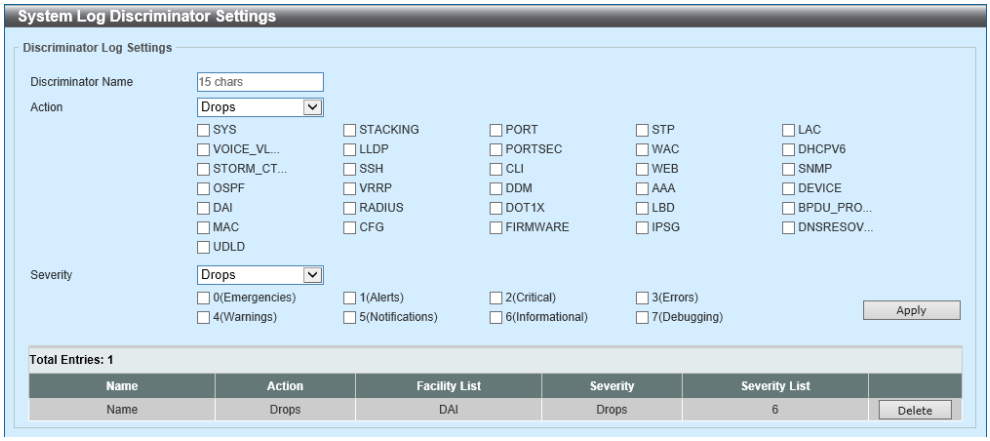


Figure 3-11 System Log Discriminator Settings

The following parameters can be configured in the **Discriminator Log Settings** section:

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 add a new entry based on the information specified.
Click the **Delete** button to delete the entry.

3.5.3 System Log Server Settings

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

Click **System > System Log > System Log Server Settings** to view the following window:

Figure 3-12 System Log Server Settings

The following parameters can be configured in the **Log Server** section:

Parameter	Description
Host IPv4 Address	Enter the IPv4 address for the system log server here.
Host IPv6 Address	Enter the IPv6 address for the system log server here.
UDP Port	Enter the User Datagram Protocol (UDP) port number for the system log server 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)**.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Facility</td><td>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:
<table>
<tr><th>Facility Number</th><th>Facility Name</th><th>Facility Description</th></tr>
<tr><td>1</td><td>user</td><td>User-level messages</td></tr>
<tr><td>2</td><td>mail</td><td>Mail system</td></tr>
<tr><td>3</td><td>daemon</td><td>System daemons</td></tr>
<tr><td>4</td><td>auth1</td><td>Security/authorization messages</td></tr>
<tr><td>5</td><td>syslog</td><td>Messages generated internally by the SYSLOG</td></tr>
<tr><td>6</td><td>lpr</td><td>Line printer sub-system</td></tr>
<tr><td>7</td><td>news</td><td>Network news sub-system</td></tr>
<tr><td>8</td><td>uucp</td><td>UUCP sub-system</td></tr>
<tr><td>9</td><td>clock1</td><td>Clock daemon</td></tr>
<tr><td>10</td><td>auth2</td><td>Security/authorization messages</td></tr>
<tr><td>11</td><td>ftp</td><td>FTP daemon</td></tr>
<tr><td>12</td><td>ntp</td><td>NTP subsystem</td></tr>
<tr><td>13</td><td>logaudit</td><td>Log audit</td></tr>
<tr><td>14</td><td>logalert</td><td>Log alert</td></tr>
<tr><td>15</td><td>clock2</td><td>Clock daemon</td></tr>
<tr><td>16</td><td>local0</td><td>Local use 0 (local0)</td></tr>
<tr><td>17</td><td>local1</td><td>Local use 1 (local1)</td></tr>
<tr><td>18</td><td>local2</td><td>Local use 2 (local2)</td></tr>
<tr><td>19</td><td>local3</td><td>Local use 3 (local3)</td></tr>
<tr><td>20</td><td>local4</td><td>Local use 4 (local4)</td></tr>
<tr><td>21</td><td>local5</td><td>Local use 5 (local5)</td></tr>
<tr><td>22</td><td>local6</td><td>Local use 6 (local6)</td></tr>
<tr><td>23</td><td>local7</td><td>Local use 7 (local7)</td></tr>
</table></td></tr>
<tr><td>Discriminator Name</td><td>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.</td></tr>
</table>

Click the **Apply** button to add a new entry based on the information specified.
Click the **Delete** button to delete the entry.

3.5.4 System Log

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

Click **System > System Log > System Log** to view the following window:

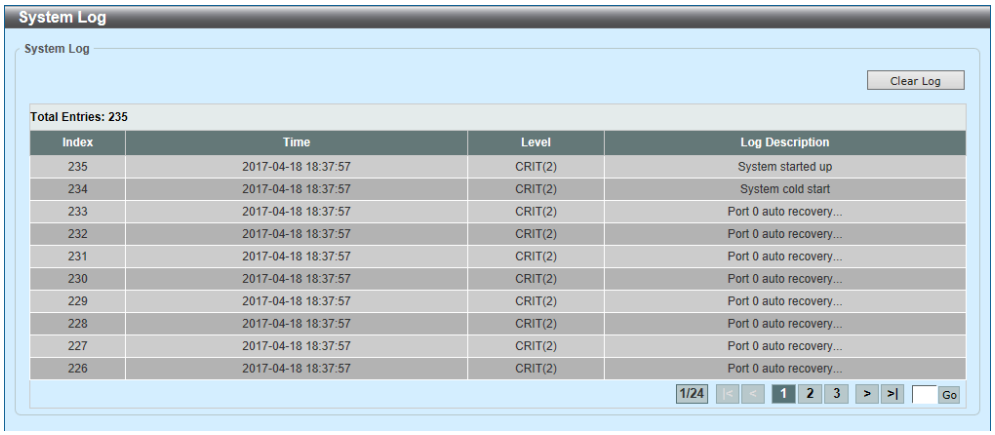


Figure 3-13 System Log

Click the **Clear Log** button to clear the log entries from the table.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

3.5.5 System Attack Log

This window is used to display and clear the system attack log.
Click **System > System Log > System Attack Log** to view the following window:

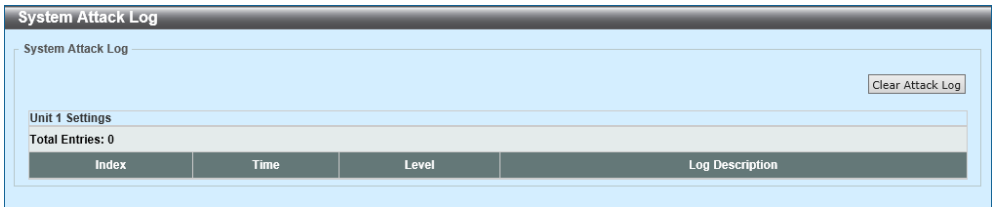


Figure 3-14 System Attack Log

Click the **Clear Attack Log** button to clear the attack log entries from the table.

3.5.6 System Authentication Log

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

Click **System > System Log > System Authentication Log** to view the following window:

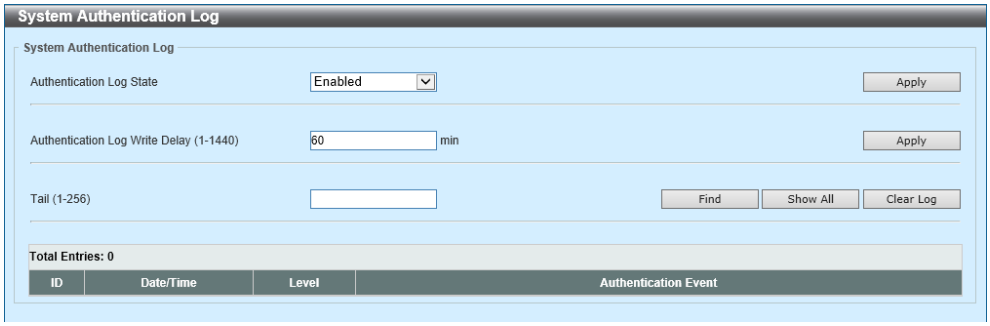


Figure 3-15 System Authentication Log

The following parameters can be configured in the **System Authentication Log** section:

Parameter	Description
Authentication Log State	Select to enable or disable the authentication log here.
Authentication Log Write Delay	Enter the write delay value for the authentication log here. The range is from 1 to 1440 minutes.
Tail	Enter the number of the latest authentication log entries that will be displayed. The range is from 1 to 256.

Click the **Apply** button to accept the changes made.
Click the **Find** button to find and display entries in the table based on the search criteria specified.
Click the **Show All** button to find and display all available entries.
Click the **Clear Log** button to clear the log entries from the table.

3.6 Time and SNTP (Simple Network Time Protocol)

3.6.1 Clock Settings

This window is used to configure and display the time and date settings used by time dependent features on the switch.

Click **System > Time and SNTP > Clock Settings** to view the following window:

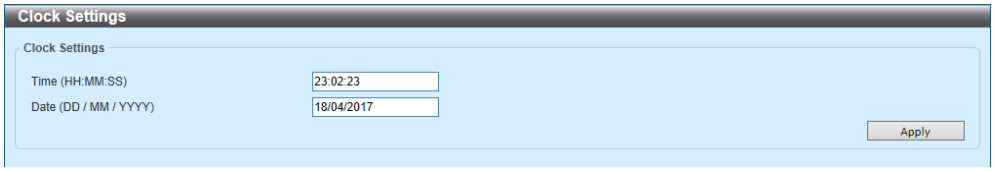


Figure 3-16 Clock Settings

The following parameters can be configured in the **Clock Settings** section:

Parameter	Description
Time	Enter the current time in hours (HH), minutes (MM), and seconds (SS) here. For example, 19:20:20.
Date	Enter the current day (DD), month (MM), and year (YYYY) here. For example, 25/04/2017.

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

3.6.2 Time Zone Settings

This window is used to configure and display the Daylight Savings Time (DST) and Time Zone settings.

Click **System > Time and SNTP > Time Zone Settings** to view the following window:

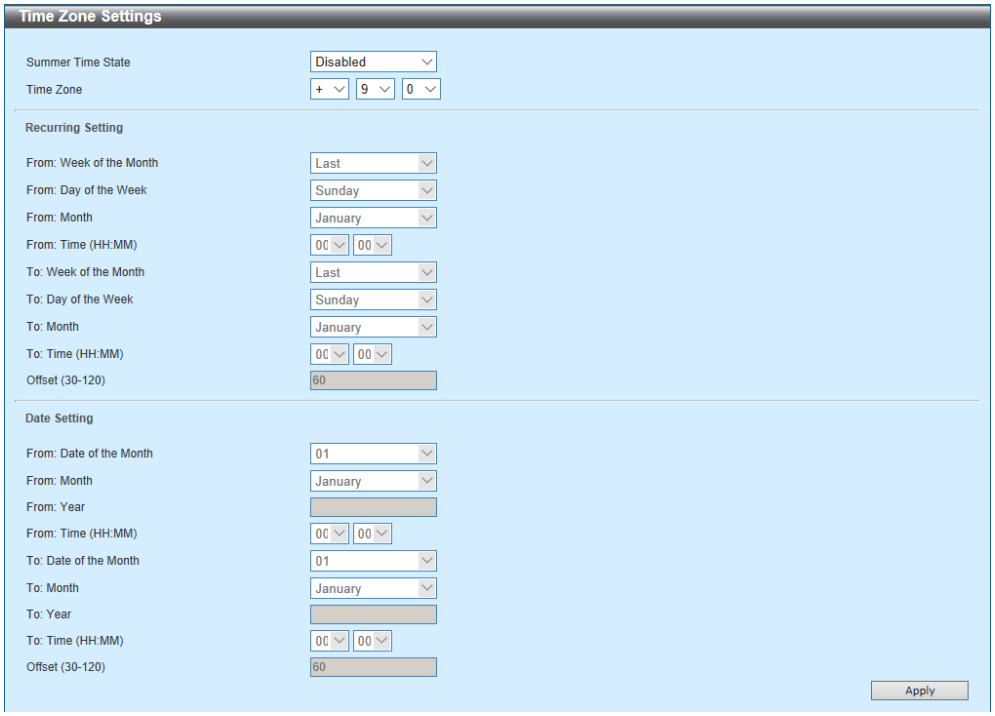


Figure 3-17 Time Zone Settings

The following parameters can be configured in the first section:

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 the local time zone offset from Coordinated Universal Time (UTC).

The following parameters can be configured in the **Recurring Setting** section:

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.
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 30, 60, 90 and 120.

The following parameters can be configured in the **Date Setting** section:

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 30, 60, 90 and 120.

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

3.6.3 SNTP Settings

This window is used to configure and display the Simple Network Time Protocol (SNTP) settings. SNTP is used to synchronize the date and time settings of the switch with the settings hosted by an SNTP server automatically and periodically.

Click **System > Time and SNTP > SNTP Settings** to view the following window:

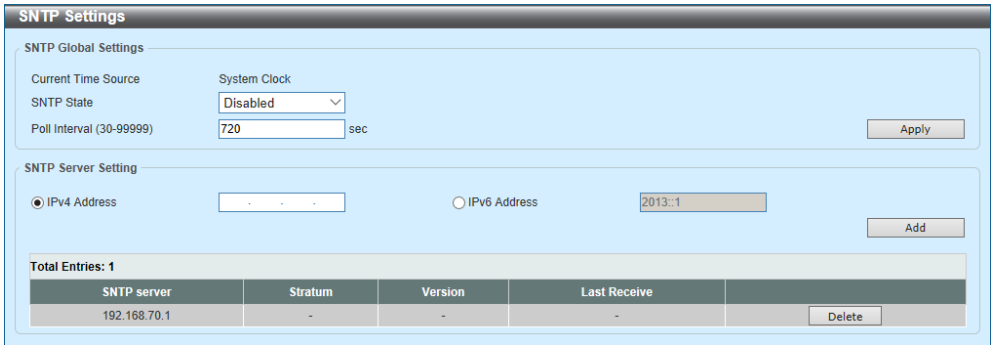


Figure 3-18 SNTP Settings

The following parameters can be configured in the **SNTP Global Settings** section:

Parameter	Description
SNTP State	Select to globally enable or disable SNTP here.
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 following parameters can be configured in the **SNTP Server Setting** section:

Parameter	Description
IPv4 Address	Enter the IPv4 address of the SNTP server here.
IPv6 Address	Enter the IPv6 address of the SNTP server here.

Click the **Add** button to add a new entry based on the information specified.
Click the **Delete** button to delete the entry.

3.7 Time Range

This window is used to configure and display time range profiles.

Click **System > Time Range** to view the following window:

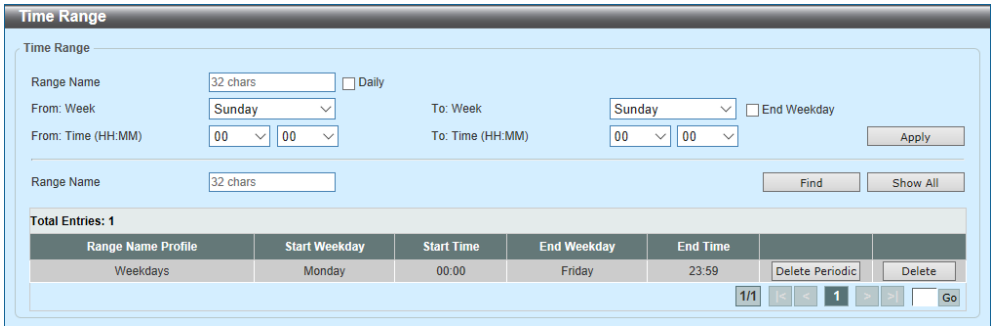


Figure 3-19 Time Range

The following parameters can be configured in the **Time Range** section:

Parameter	Description
Range Name	Enter the name of the time range profile 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 add a new entry based on the information specified.
Click the **Find** button to find and display entries in the table based on the search criteria specified.
Click the **Show All** button to find and display all available entries.
Click the **Delete Periodic** button to delete the periodic entry.
Click the **Delete** button to delete the entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

4 Management

4.1 Command Logging

This window is used to enable or disable the command logging feature. This feature is used to log the CLI commands. Commands that did not change the configuration of the switch will not be logged.

Click **Management > Command Logging** to view the following window:

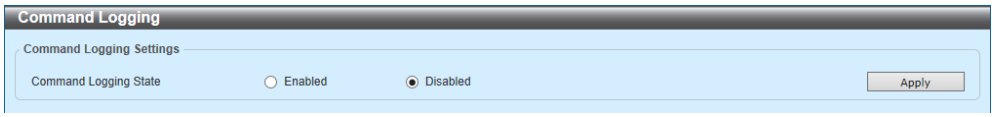


Figure 4-1 Command Logging

The following parameters can be configured in the **Command Logging Settings** section:

Parameter	Description
Command Logging State	Select to enable or disable the command logging function here.

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

4.2 User Accounts Settings

This window is used to configure and display the user account settings. These user accounts are used to log into the software configuration of the switch.

Click **Management > User Accounts Settings** to view the following window:

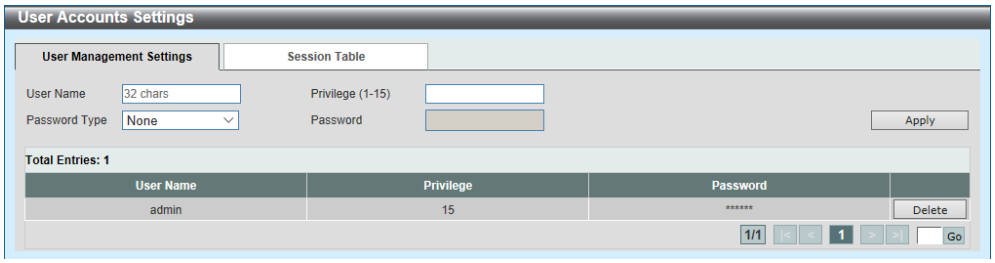


Figure 4-2 User Accounts Settings (User Management Settings)

The following parameters can be configured in the **User Management Settings** section:

Parameter	Description
User Name	Enter the user account name here. This name can be up to 32 characters long.
Privilege	Enter the privilege level for this account here. The range is from 1 to 15.
Password Type	Select the password type for this user account here. Options to choose from are **None**, **Plain Text**, and **Encrypted-SHA1**. SHA stands for Secure Hash Algorithms.
Password	After selecting **Plain Text** or **Encrypted-SHA1** as the password type, enter the password for this user account here.

Click the **Apply** button to add a new entry based on the information specified.
Click the **Delete** button to delete the entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **Session Table** tab to view the following window:

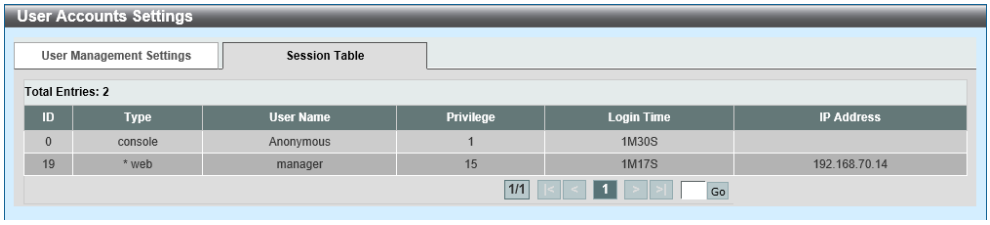


Figure 4-3 User Accounts Settings (Session Table)

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

4.3 User Accounts Encryption

This window is used to enable or disable user account encryption.

Click **Management > User Accounts Encryption** to view the following window:

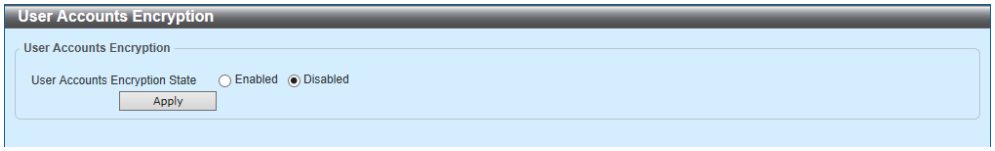


Figure 4-4 User Accounts Encryption

The following parameters can be configured in the **User Accounts Encryption** section:

Parameter	Description
User Accounts Encryption State	Select to enable or disable user account encryption here.

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

4.4 Login Method

This window is used to configure and display the login method for each login application supported on the switch.

Click **Management > Login Method** to view the following window:

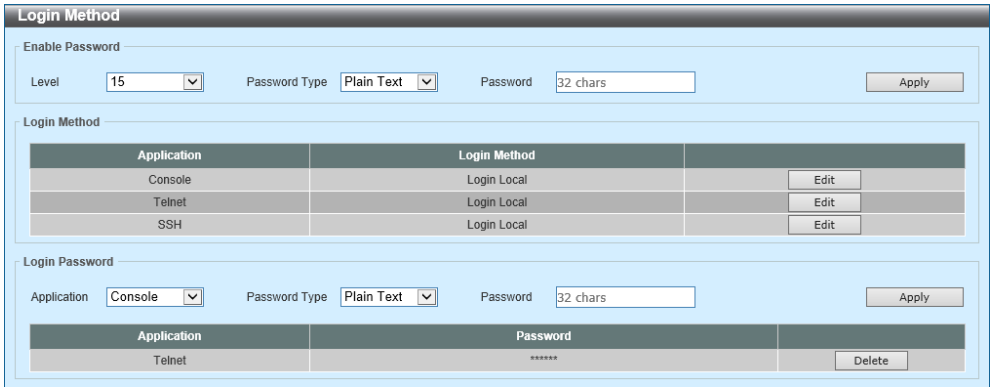


Figure 4-5 Login Method

The following parameters can be configured in the **Enable Password** section:

Parameter	Description
Level	Select the privilege level for the user account here. The range is from 1 to 15.
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.
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.

Click the **Apply** button to accept the changes made.
Click the **Edit** button to edit the settings of the entry.

The following parameters can be configured in the **Login Method** section:

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** - This requires no login authentication to access the specified application. • **Login** - This requires the user to enter a password when trying to access the specified application. • **Login Local** - This requires the user to enter a username and a password to access the specified application.

The following parameters can be configured in the **Login Password** section:

Parameter	Description
Application	Select the application that will be configured here. Options to choose from are **Console**, **Telnet** and Secure Shell (**SSH**).
Password Type	Select the password encryption type that will be used here. Options to choose from are **Plain Text** and **Encrypted**.
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.

Click the **Apply** button to add a new entry based on the information specified.
Click the **Delete** button to delete the entry.

4.5 SNMP (Simple Network Management Protocol)

4.5.1 SNMP Global Settings

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

Click **Management > SNMP > SNMP Global Settings** to view the following window:

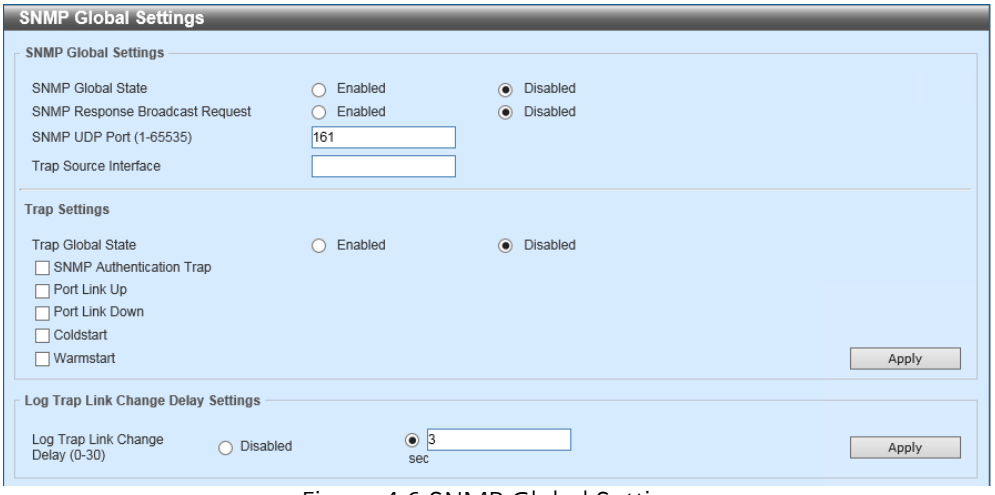


Figure 4-6 SNMP Global Settings

The following parameters can be configured in the **SNMP Global Settings** section:

Parameter	Description
SNMP Global State	Select to globally enable or disable the SNMP feature.
SNMP Response Broadcast Request	Select to enable or disable the server to respond to broadcast SNMP *GetRequest* packets.
SNMP UDP Port	Enter the SNMP UDP port number. The range is from 1 to 65535.
Trap Source Interface	Enter the interface whose IP address will be used as the source address for sending the SNMP trap packet.

The following parameters can be configured in the **Trap Settings** section:

Parameter	Description
Trap Global State	Select to globally enable or disable the sending of all or specific SNMP notifications.
SNMP Authentication Trap	Select 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. For SNMPv3, authentication failure occurs if packets are formed with an incorrect SHA/MD5 authentication key.
Port Link Up	Select 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	Select 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	Select this option to control the sending of SNMP *coldStart* notifications.
Warmstart	Select this option to control the sending of SNMP *warmStart* notifications.

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

The following parameters can be configured in the **Log Trap Link Change Delay Settings** section:

Parameter	Description
Log Trap Link Change	Enables issuance delays for system logs and SNMP traps related to the link state of physical ports.The range is from 1 to 30 (seconds). When using the link aggregation on your device, if the system logs and SNMP traps regarding the link status of the physical port cannot be normally transmitted to the SYSLOG server or SNMP server, you may be able to solve issue by using this function. The recommendation value is 5 seconds when using this function.

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

4.5.2 SNMP Linkchange Trap Settings

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

Click **Management > SNMP > SNMP Linkchange Trap Settings** to view the following window:

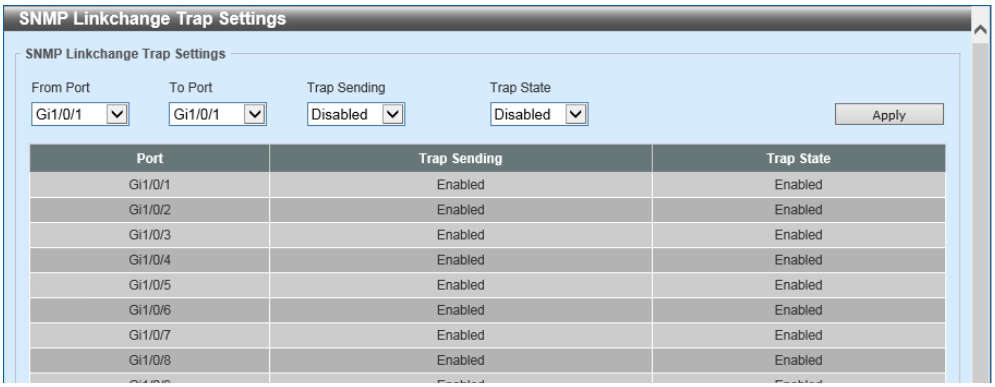


Figure 4-7 SNMP Linkchange Trap Settings

The following parameters can be configured in the **SNMP Linkchange Trap Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Trap Sending	Select to enable or disable the sending of the SNMP notification traps that are generated by the system.
Trap State	Select to enable or disable the SNMP *linkChange* trap.

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

4.5.3 SNMP View Table Settings

This window is used to configure and display the SNMP view table settings. These SNMP view entries define which Management Information Base (MIB) objects can be accessed by a remote SNMP manager. The SNMP Subtree Object Identifier (OID) maps SNMP users to the SNMP views.

Click **Management > SNMP > SNMP View Table Settings** to view the following window:

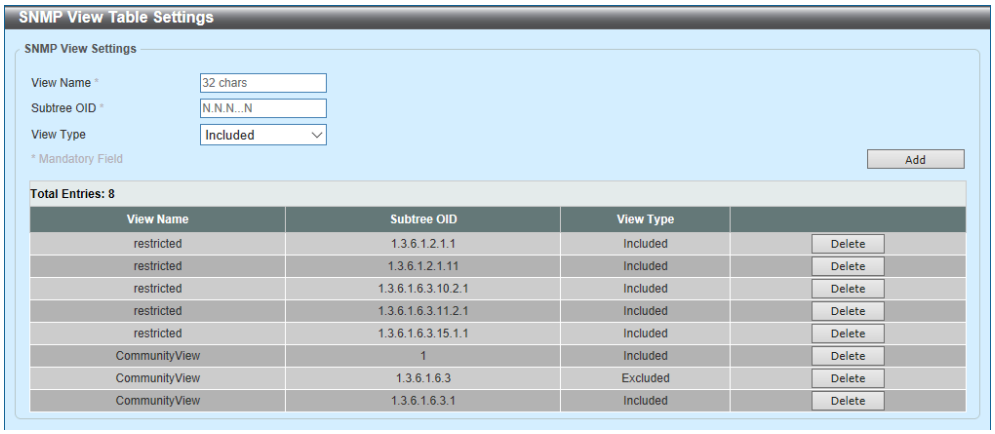


Figure 4-8 SNMP View Table Settings

The following parameters can be configured in the **SNMP View Settings** section:

Parameter	Description
View Name	Enter the SNMP view name here. This is used to identify the new SNMP view being created. This can be up to 32 characters long.
Subtree OID	Enter the OID sub-tree for the view here. 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 specified.
Click the **Delete** button to delete the entry.

4.5.4 SNMP Community Table Settings

This window is used to configure and display SNMP community strings that define the relationship between SNMP managers and SNMP agents. The SNMP community string acts like a password to permit access to the SNMP agent on the switch.
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 SNMP agent of the switch.
- MIB views that define the subset of MIB objects that are accessible to the SNMP community.
- Read-Write or Read-Only permissions for MIB objects accessible to the SNMP community.

Click **Management > SNMP > SNMP Community Table Settings** to view the following window:

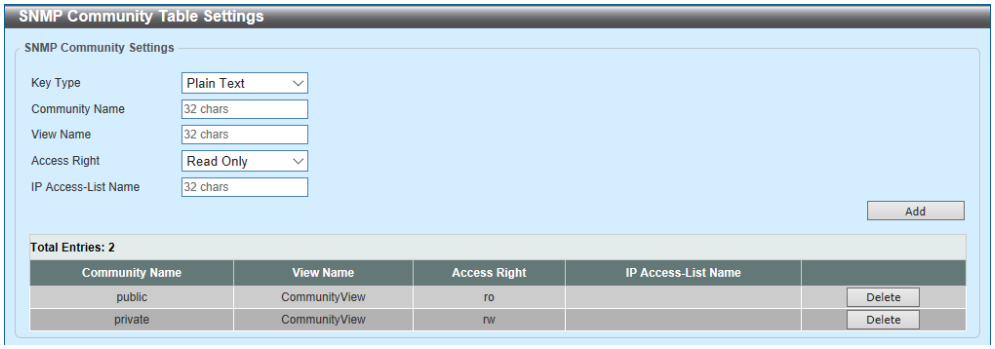


Figure 4-9 SNMP Community Table Settings

The following parameters can be configured in the **SNMP Community Settings** section:

Parameter	Description
Key Type	Select the key type for the SNMP community. Options to choose from are **Plain Text** and **Encrypted**.
Community Name	Enter the SNMP community name here. This 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. This can be up to 32 characters long.
View Name	Enter the SNMP view name here. This 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. This can be up to 32 characters long.

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

4.5.5 SNMP Group Table Settings

This window is used to configure and display the SNMP group table settings. SNMP groups map SNMP users to SNMP views.

Click **Management > SNMP > SNMP Group Table Settings** to view the following window:

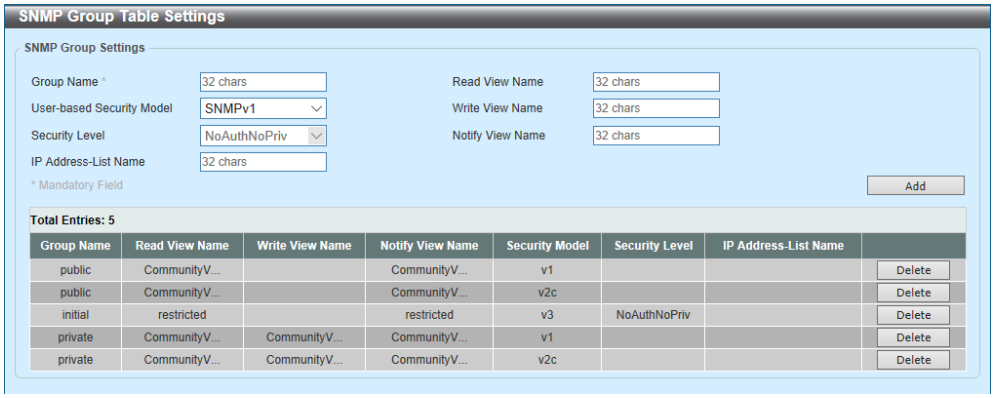


Figure 4-10 SNMP Group Table Settings

The following parameters can be configured in the **SNMP Group Settings** section:

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.

Parameter	Description
Security Level	After selecting to use **SNMPv3** as the **User-based Security Model**, select the security level here. Options to choose from are: • **NoAuthNoPriv** - Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. • **AuthNoPriv** - Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. • **AuthPriv** - Specifies that authorization will be
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 Address-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 specified.
Click the **Delete** button to delete the entry.

4.5.6 SNMP Engine ID Local Settings

This window is used to configure and display the local SNMP engine ID. The engine ID is unique per switch and is used in SNMPv3 (SNMP version 3) implementations.

Click **Management > SNMP > SNMP Engine ID Local Settings** to view the following window:

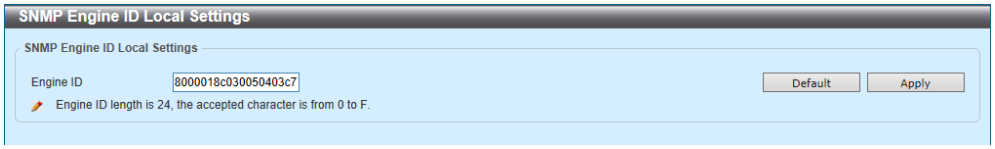


Figure 4-11 SNMP Engine ID Local Settings

The following parameters can be configured in the **SNMP Engine ID Local Settings** section:

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 use the default engine ID.
Click the **Apply** button to accept the changes made.

4.5.7 SNMP User Table Settings

This window is used to configure and display SNMP user settings.

Click **Management > SNMP > SNMP User Table Settings** to view the following window:

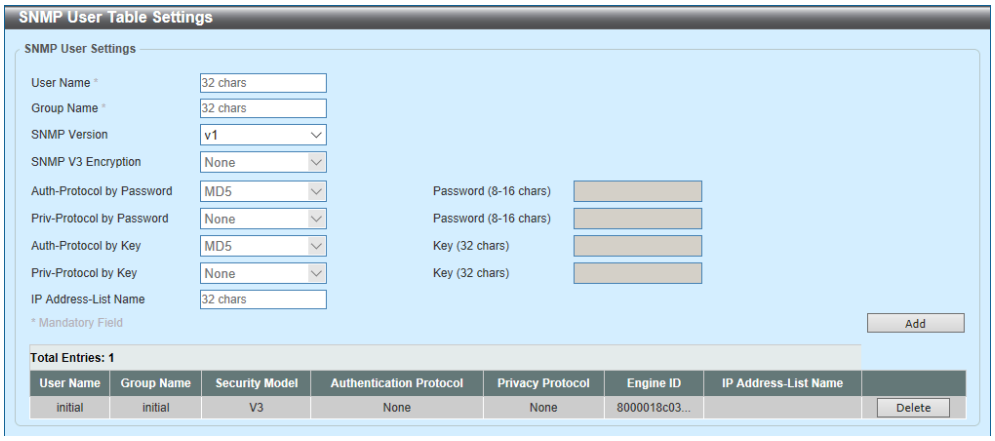


Figure 4-12 SNMP User Table Settings

The following parameters can be configured in the **SNMP User Settings** section:

Parameter	Description
User Name	Enter the SNMP user name here. This is used to identify the SNMP user. This name can be up to 32 characters long.
Group Name	Enter the SNMP group name for the user here. This name can be up to 32 characters long. Spaces are not allowed.
SNMP Version	Select the SNMP version. Options to choose from are **v1**, **v2c**, and **v3**.
SNMP V3 Encryption	After selecting **v3** as the **SNMP Version**, select the SNMPv3 encryption here. Options to choose from are **None**, **Password**, and **Key**.
Auth-Protocol by Password	After selecting **v3** as the **SNMP Version** and **Password** for **SNMP V3 Encryption**, select the authentication protocol for the password here. Options to choose from are: • **MD5** - Specifies to use the HMAC-MD5-96 authentication level. This field will require the user to enter a password or key. • **SHA** - Specifies to use the HMAC-SHA authentication protocol. This field will require the user to enter a password or key.

Parameter	Description
Password	Enter the authentication 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	After selecting **v3** as the **SNMP Version** and **Password** for **SNMP V3 Encryption**, select the private protocol for the password here. Options to choose from are: • **None** - Specifies that no authorization protocol will be used. • **DES56** - Specifies to use Data Encryption Standard (DES) 56-bit encryption, based on the CBC-DES (DES-56) standard. This field requires the user to enter a password or a key.
Password	Enter the private protocol password here. • For none, this field will be disabled. • For DES56, this password must be between 8 and 16 characters long.
Auth-Protocol by Key	After selecting **v3** as the **SNMP Version** and **Key** for **SNMP V3 Encryption** select the authentication protocol for the key here. Options to choose from are: • **MD5** - Specifies to use the HMAC-MD5-96 authentication level. This field will require the user to enter a password or a key. • **SHA** - Specifies to use the HMAC-SHA authentication protocol. This field will require the user to enter a password or a key.
Key	Enter the authentication 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	After selecting **v3** as the **SNMP Version** and **Key** for **SNMP V3 Encryption** select the private protocol for the key here. Options to choose from are: • **None** - Specifies that no authorization protocol will be used. • **DES56** - Specifies to use Data Encryption Standard (DES) 56-bit encryption, based on the CBC-DES (DES-56) standard. This field will require the user to enter a password or a key.
Key	Enter the private protocol key here. • For none, this field will be disabled. • For DES56, this key must be 32 characters long.
IP Address-List Name	Enter the standard IP ACL to associate with the user.

Click the **Add** button to add a new entry based on the information specified.
Click the **Delete** button to delete the entry.

4.5.8 SNMP Host Table Settings

This window is used to configure and display SNMP host settings.

Click **Management > SNMP > SNMP Host Table Settings** to view the following window:

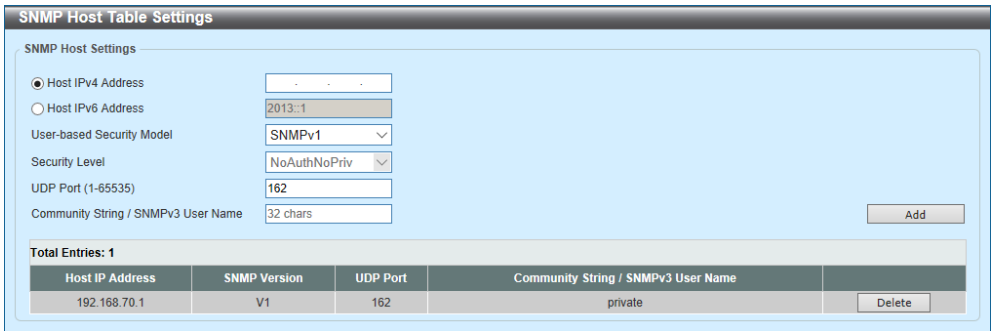


Figure 4-13 SNMP Host Table Settings

The following parameters can be configured in the **SNMP Host Settings** section:

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	After selecting **SNMPv3** as the **User-based Security Model**, select the security level here. Options to choose from are: • **NoAuthNoPriv** - Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. • **AuthNoPriv** - Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. • **AuthPriv** - Specifies that authorization will be
UDP Port	Enter the UDP port number here. The default port number is 162. The range is from 1 to 65535. Some port numbers may conflict with other protocols.

Parameter	Description
Community String / SNMPv3 User Name	Enter the community string to be sent with the notification packet.

Click the **Add** button to add a new entry based on the information specified.
Click the **Delete** button to delete the entry.

4.6 RMON (Remote Monitoring)

4.6.1 RMON Global Settings

This window is used to enable or disable the rising and falling alarm trap states for RMON.

Click **Management > RMON > RMON Global Settings** to view the following window:

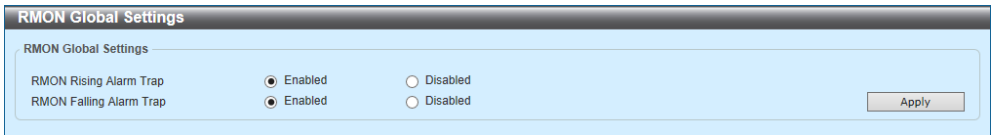


Figure 4-14 RMON Global Settings

The following parameters can be configured in the **RMON Global Settings** section:

Parameter	Description
RMON Rising Alarm Trap	Select to enable or disable the RMON Rising Alarm Trap feature.
RMON Falling Alarm Trap	Select to enable or disable the RMON Falling Alarm Trap feature.

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

4.6.2 RMON Statistics Settings

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

Click **Management > RMON > RMON Statistics Settings** to view the following window:

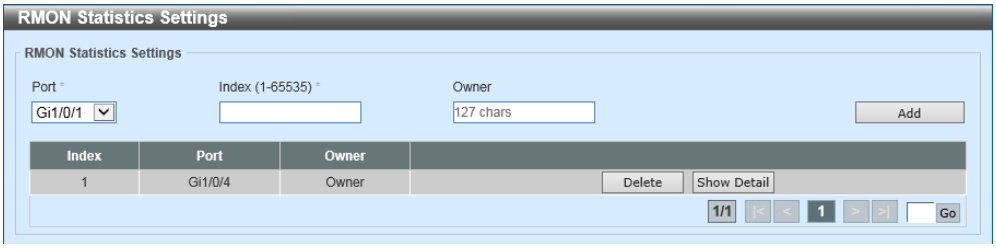


Figure 4-15 RMON Statistics Settings

The following parameters can be configured in the **RMON Statistics Settings** section:

Parameter	Description
Port	Select the port that will be used here.
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 specified.
Click the **Delete** button to delete the entry.
Click the **Show Detail** button to display detailed information related to the entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **Show Detail** button to view the following window:

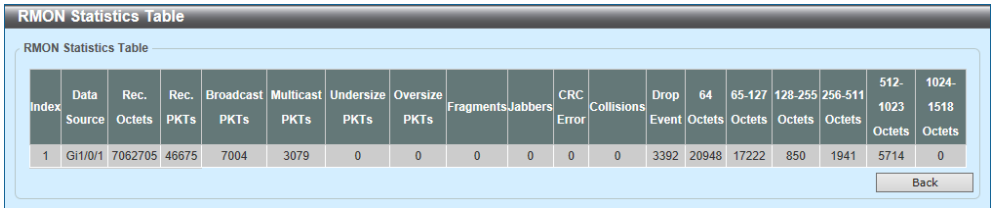


Figure 4-16 RMON Statistics Settings (Show Detail)

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

4.6.3 RMON History Settings

This window is used to configure and display the RMON history settings for the specified port.

Click **Management > RMON > RMON History Settings** to view the following window:

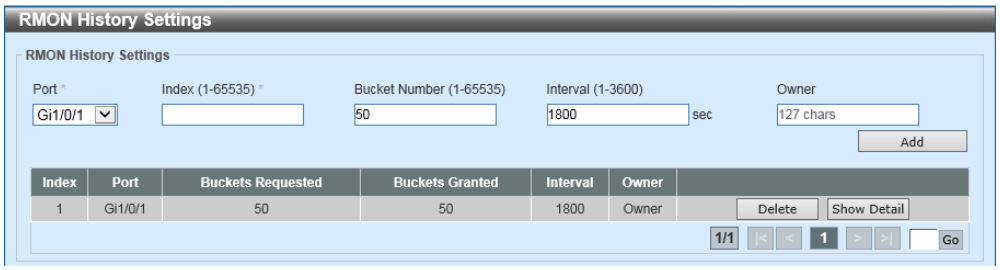


Figure 4-17 RMON History Settings

The following parameters can be configured in the **RMON History Settings** section:

Parameter	Description
Port	Select the port that will be used here.
Index	Enter the index number of the entry in the history group table here. The range 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 interval time for each polling cycle here. The range is from 1 to 3600 seconds.
Owner	Enter the owner string here. The string can be up to 127 characters long.

Click the **Add** button to add a new entry based on the information specified.
Click the **Delete** button to delete the entry.
Click the **Show Detail** button to display detailed information related to the entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **Show Detail** button to view the following window:

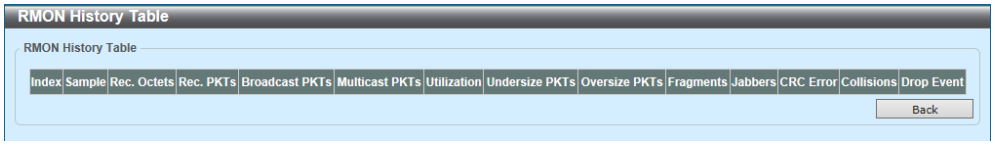


Figure 4-18 RMON History Settings (Show Detail)

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

4.6.4 RMON Alarm Settings

This window is used to configure and display the RMON alarm settings.

Click **Management > RMON > RMON Alarm Settings** to view the following window:

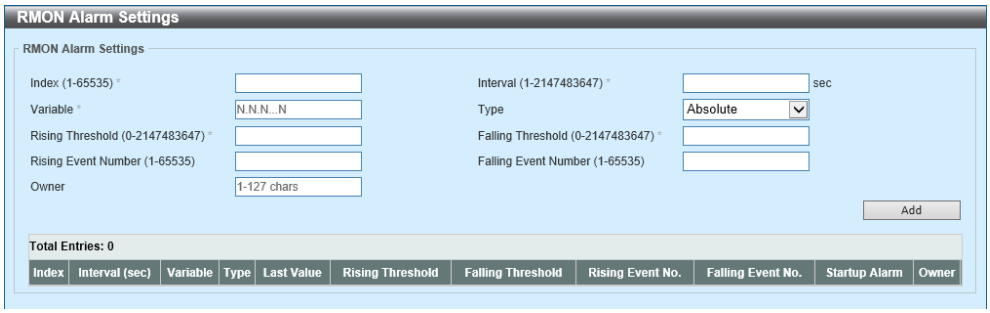


Figure 4-19 RMON Alarm Settings

The following parameters can be configured in the **RMON Alarm Settings** section:

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

4.6.5 RMON Event Settings

This window is used to configure and display the RMON event settings.

Click **Management > RMON > RMON Event Settings** to view the following window:

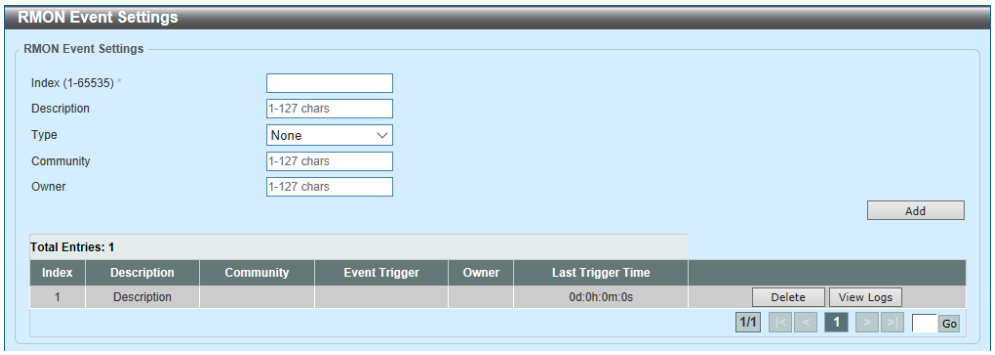


Figure 4-20 RMON Event Settings

The following parameters can be configured in the **RMON Event Settings** section:

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 specified.
Click the **Delete** button to delete the entry.
Click the **View Logs** button to display the log entries associated with the specified entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **View Logs** button to view the following window:

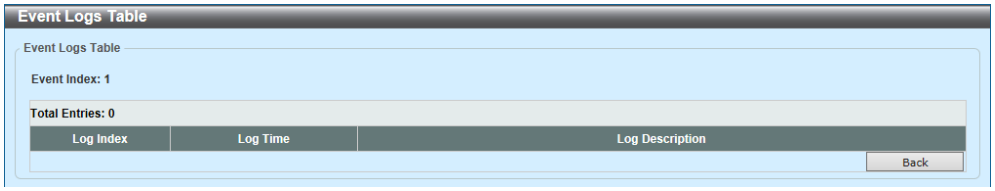


Figure 4-21 RMON Event Settings (View Logs)

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

4.7 Telnet/Web

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

Click **Management > Telnet/Web** to view the following window:

Figure 4-22 Telnet/Web

The following parameters can be configured in the **Telnet Settings** section:

Parameter	Description
Telnet State	Select to enable or disable the Telnet server feature here.
Port	Enter the Transmission Control Protocol (TCP) port number used for Telnet management of the Switch. The well-known TCP port for the Telnet protocol is 23.

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

The following parameters can be configured in the **Web Settings** section:

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

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

4.8 Session Timeout

This window is used to configure and display the session timeout settings for Web, Console, Telnet, and SSH connections.

Click **Management > Session Timeout** to view the following window:

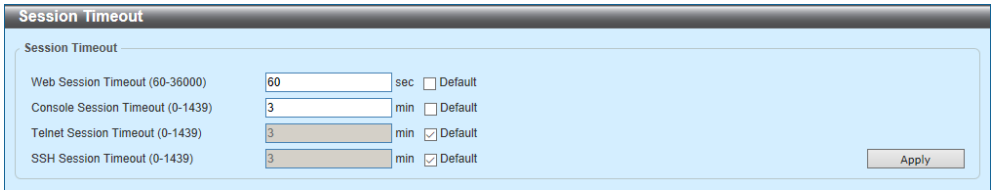


Figure 4-23 Session Timeout

The following parameters can be configured in the **Session Timeout** section:

Parameter	Description
Web Session Timeout	Enter the time in seconds of the web session timeout. Tick the **Default** check box to return to the default setting. The value is from 60 to 36000 seconds. The default value is 180 seconds.
Console Session Timeout	Enter the time in minutes of the console session timeout. Tick the **Default** check box to return to the default setting. The value is from 0 to 1439 minutes. Enter 0 to disable the timeout. The default value is 3 minutes.
Telnet Session Timeout	Enter the time in minutes of the Telnet session timeout. Tick the **Default** check box to return to the default setting. The value is from 0 to 1439 minutes. Enter 0 to disable the timeout. The default value is 3 minutes.
SSH Session Timeout	Enter the time in minutes of the SSH session timeout. Tick the **Default** check box to return to the default setting. The value is from 0 to 1439 minutes. Enter 0 to disable the timeout. The default value is 3 minutes.

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

4.9 DHCP Auto Configuration

This window is used to enable or disable the DHCP auto-configuration feature.

Click **Management > DHCP Auto Configuration** to view the following window:

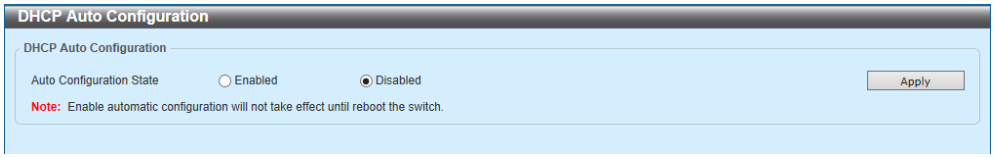


Figure 4-24 DHCP Auto Configuration

The following parameters can be configured in the **DHCP Auto Configuration** section:

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

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

4.10 DNS (Domain Name System)

4.10.1 DNS Global Settings

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

Click **Management > DNS > DNS Global Settings** to view the following window:

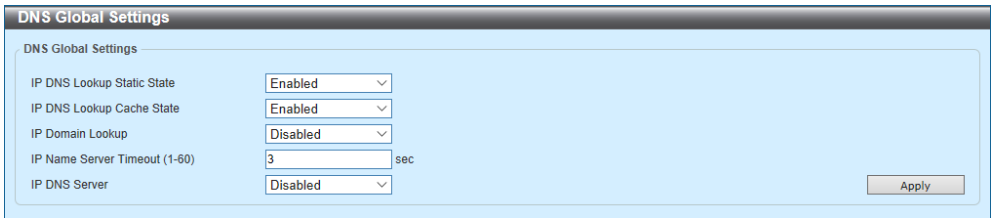


Figure 4-25 DNS Global Settings

The following parameters can be configured in the **DNS Global Settings** section:

Parameter	Description
IP DNS Lookup Static State	Select to enable or disable the IP DNS lookup static state here.
IP DNS Lookup Cache State	Select to enable or disable the IP DNS lookup cache state here.
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.
IP DNS Server	Select to globally enable or disable the DNS server feature here.

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

4.10.2 DNS Name Server Settings

This window is used to configure and display DNS name server settings.

Click **Management > DNS > DNS Name Server Settings** to view the following window:

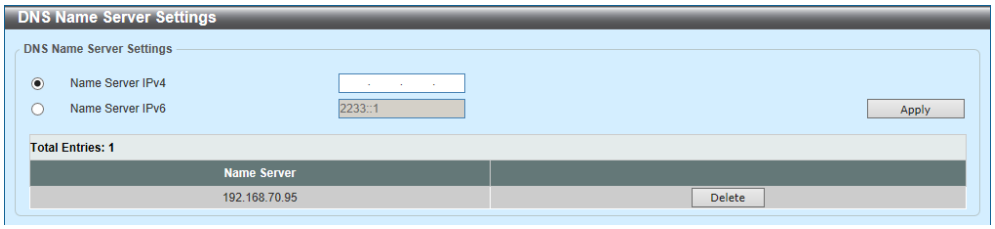


Figure 4-26 DNS Name Server Settings

The following parameters can be configured in the **DNS Name Server Settings** section:

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 add a new entry based on the information specified.
Click the **Delete** button to delete the entry.

4.10.3 DNS Host Settings

This window is used to configure and display DNS host settings.

Click **Management > DNS > DNS Host Settings** to view the following window:

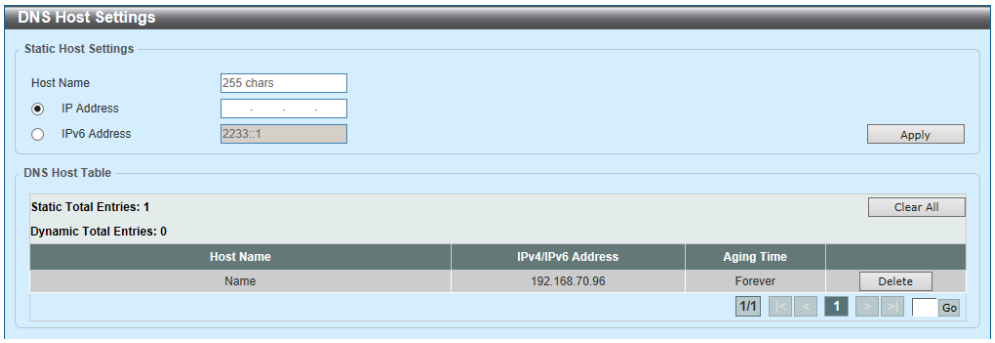


Figure 4-27 DNS Host Settings

The following parameters can be configured in the **Static Host Settings** section:

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

Click the **Apply** button to add a new entry based on the information specified.
Click the **Clear All** button to remove all the dynamic entries from the table.
Click the **Delete** button to delete the entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

4.11 File System

This window is used to configure and display the file system of the switch.

Click **Management > File System** to view the following window:

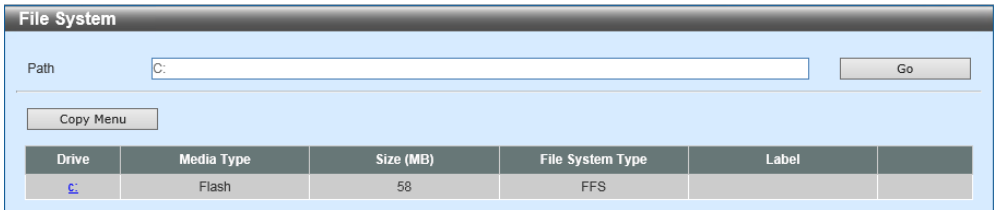


Figure 4-28 File System

The following parameters can be configured:

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 file system.
Click the Drive Link (c:) to navigate the C: drive

Click the Drive Link (c:) to view the following window:

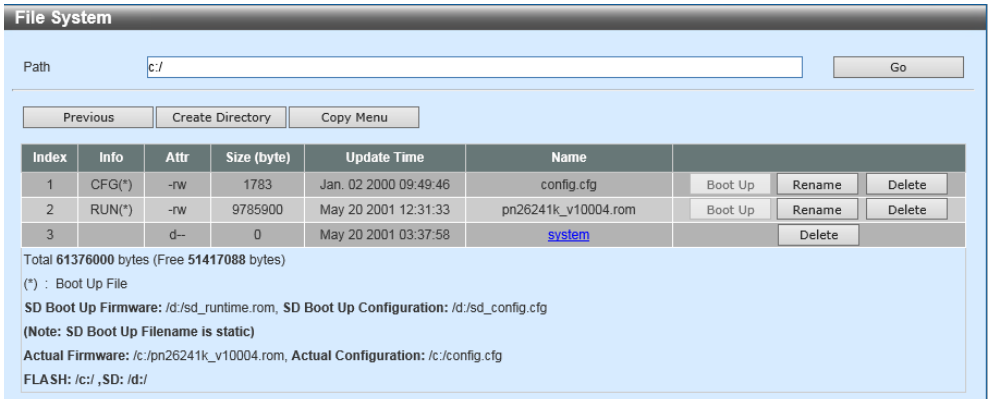


Figure 4-29 File System (c:)

Click the **Previous** button to return to the previous window.
Click the **Create Directory** button to create a new directory in the file system.
Click the **Boot Up** button to use the file(s) in the boot-up sequence. Only one configuration file and one firmware file can be used in the boot-up sequence.
Click the **Rename** button to rename a specific file name.
Click the **Delete** button to remove the file or folder from the file system.

Click the **Copy Menu** button to view the following window:

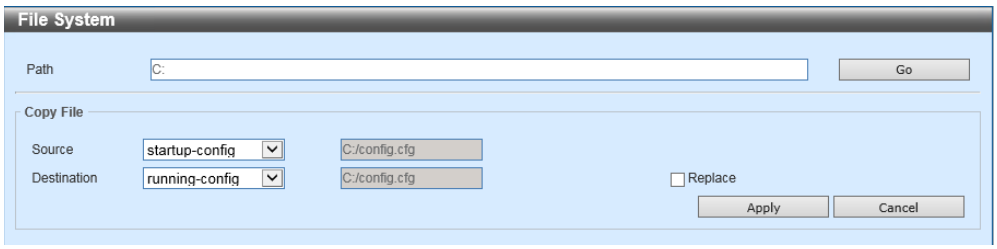


Figure 4-30 File System (Copy)

The following parameters can be configured:

Parameter	Description
Source	Select the type of source file that will be copied here. Options to choose from are **startup-config** and **Source File**. Only after selecting the **Source File** option can the source file path and filename be entered in the space provided.
Destination	Select the type of destination file that will be copied here. Options to choose from are **startup-config**, **running-config**, and **Destination File**. Only after selecting the **Destination File** option can the destination file path and filename be entered in the space provided. Select the **Replace** check box to replace the current running configuration with the indicated configuration file.

Click the **Apply** button to copy the source configuration/file to the destination configuration/file.
Click the **Cancel** button the cancel the copy.

4.12 SMTP Settings

This window is used to configure and display the Simple Mail Transfer Protocol (SMTP) settings.

Click **Management > SMTP Settings** to view the following window:

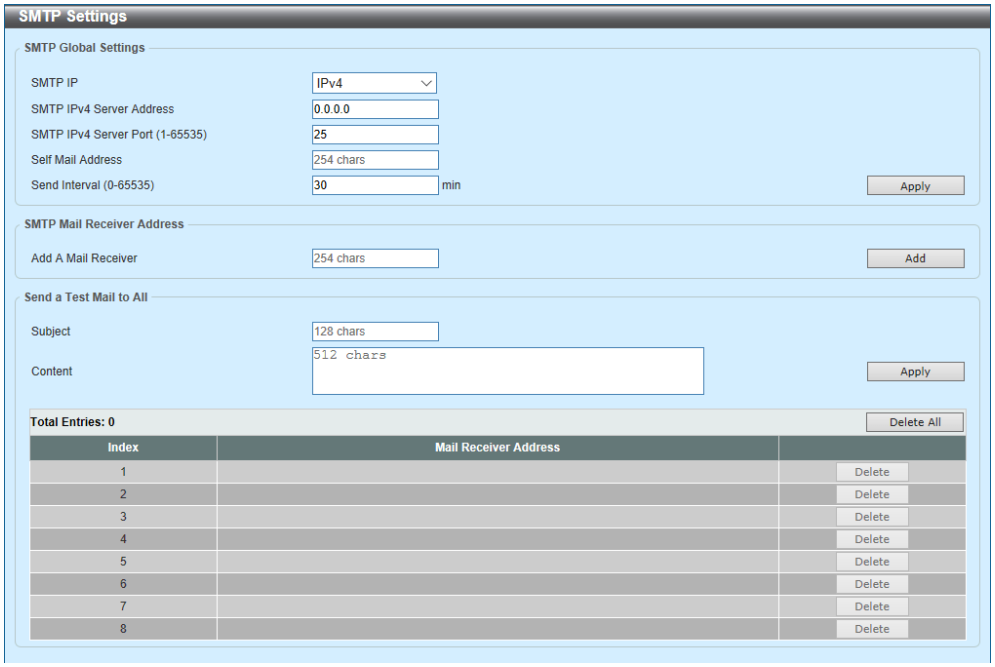


Figure 4-31 SMTP Settings

The following parameters can be configured in the **SMTP Global Settings** section:

Parameter	Description
SMTP IP	Select the SMTP server IP address type here. Options to choose from are **IPv4** and **IPv6**.
SMTP IPv4 Server Address	After selecting **IPv4** as the **SMTP IP** type enter the SMTP server IPv4 address here.
SMTP IPv6 Server Address	After selecting **IPv6** as the **SMTP IP** type enter the SMTP server IPv6 address here.
SMTP IPv4 Server Port	After selecting **IPv4** as the **SMTP IP** type enter the SMTP server port number here. The range is from 1 to 65535. By default, this value is 25.
SMTP IPv6 Server Port	After selecting **IPv6** as the **SMTP IP** type enter the SMTP server port number here. The range is from 1 to 65535. By default, this value is 25.
Self Mail Address	Enter the email address that represents the Switch here. This string can be up to 254 characters long.

Parameter	Description
Send Interval	Enter the sending interval value here. The range is from 0 to 65535 minutes. By default, this value is 30 minutes.

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

The following parameters can be configured in the **SMTP Mail Receiver Address** section:

Parameter	Description
Add A Mail Receiver	Enter the email address of the receiver here. This string can be up to 254 characters long.

The following parameters can be configured in the **Send a Test Mail to All** section:

Parameter	Description
Subject	Enter the subject of the email here. This string can be up to 128 characters long.
Content	Enter the content of the email here. This string can be up to 512 characters long.

Click the **Add** button to add a new entry based on the information specified.
Click the **Apply** button to accept the changes made.
Click the **Delete All** button to remove all the receiver mail addresses from all the entries.
Click the **Delete** button to remove the receiver mail address from the specified entry.

4.13 NLB FDB Settings

This window is used to configure and display the Network Load Balancing (NLB) File Database (FDB) settings on the specified port(s).

Click **Management > NLB FDB Settings** to view the following window:

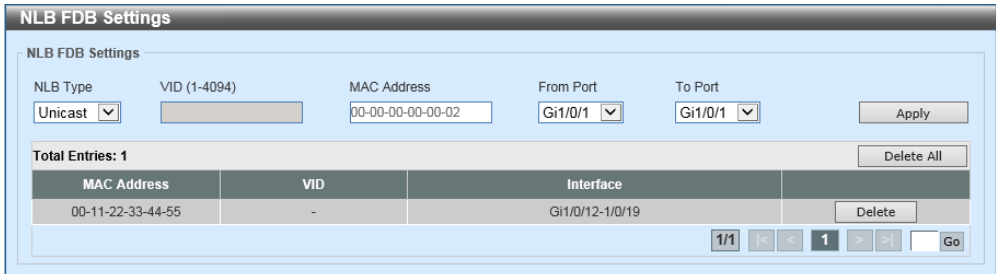


Figure 4-32 NLB FDB Settings

The following parameters can be configured in the **NLB FDB Settings** section:

Parameter	Description
NLB Type	Select the NLB type here. Options to choose from are **Unicast** and **Multicast**.
VID	After selecting **Multicast** as the **NLB Type**, enter the VLAN ID that will be used here. The range is from 1 to 4094.
MAC Address	Enter the unicast or multicast MAC address of the entry here. If a received packet contains a destination MAC address that matches the specified MAC address, it will be forwarded to the specified interface.
From Port - To Port	Select the port(s) that will be used here.

Click the **Apply** button to accept the changes made.
Click the **Delete All** button to delete all the entries.
Click the **Delete** button to delete the entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

4.14 IP Setup

4.14.1 IP Setup Settings

This window is used to enable or disable the IP setup interface feature.

Click **Management > IP Setup > IP Setup Settings** to view the following window:

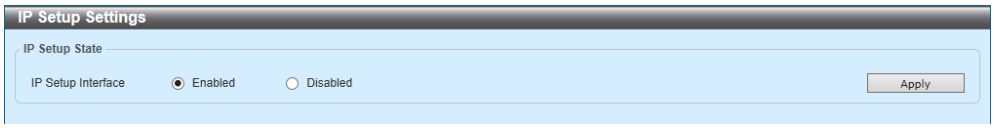


Figure 4-33 IP Setup Settings

The following parameters can be configured in the **IP Setup State** section:

Parameter	Description
IP Setup Interface	Select to enable or disable the IP setup interface feature here.

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

5 L2 Features

5.1 FDB (File Database)

5.1.1 Static FDB

5.1.1.1 Unicast Static FDB

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

Click **L2 Features > FDB > Static FDB > Unicast Static FDB** to view the following window:

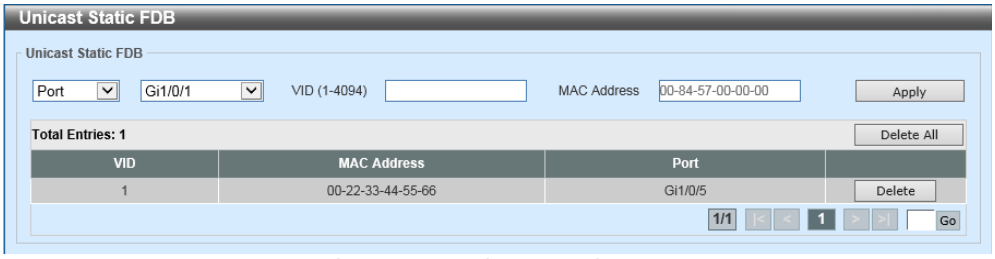


Figure 5-1 Unicast Static FDB

The following parameters can be configured in the **Unicast Static FDB** section:

Parameter	Description
Port/Drop	Select the **Port** option to use the port on which the MAC address entered resides. Select the **Drop** option to drop the MAC address from the unicast static FDB.
Port Number	After selecting the **Port** option, select the port that will be used here.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.
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 add a new entry based on the information specified.
Click the **Delete All** button to delete all the entries.

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

5.1.1.2 Multicast Static FDB

This window is used to configure and display the multicast static FDB settings.

Click **L2 Features > FDB > Static FDB > Multicast Static FDB** to view the following window:

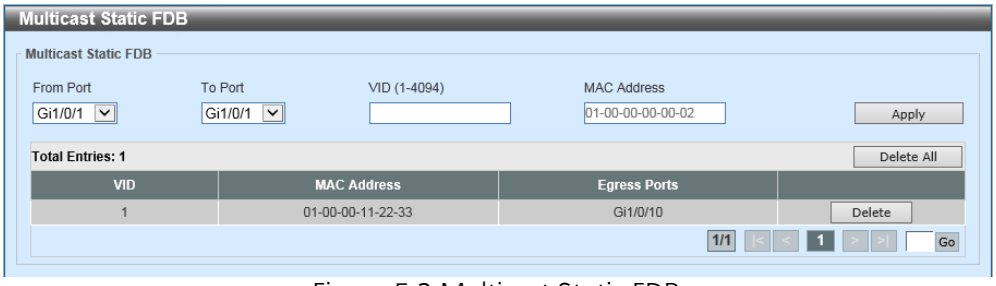


Figure 5-2 Multicast Static FDB

The following parameters can be configured in the **Multicast Static FDB** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.
MAC Address	Enter the static destination MAC address of the multicast packets. This must be a multicast MAC address.

Click the **Apply** button to add a new entry based on the information specified.
Click the **Delete All** button to delete all the entries.
Click the **Delete** button to delete the entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

5.1.2 MAC Address Table Settings

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

Click **L2 Features > FDB > MAC Address Table Settings** to view the following window:

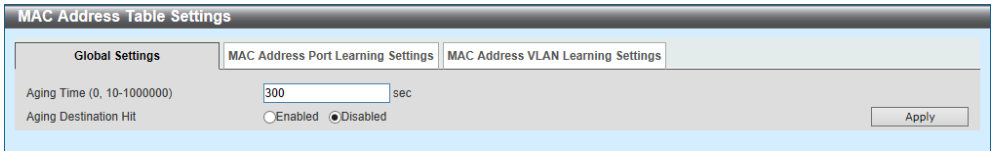


Figure 5-3 MAC Address Table Settings (Global Settings)

The following parameters can be configured in the **Global Settings** section:

Parameter	Description
Aging Time	Enter the MAC address table aging time here. The range is from 10 to 1000000 seconds. Entering 0 will disable MAC address aging. By default, this value is 300 seconds.
Aging Destination Hit	Select to enable or disable the aging destination hit function.

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

Click the **MAC Address Port Learning Settings** tab to view the following window:

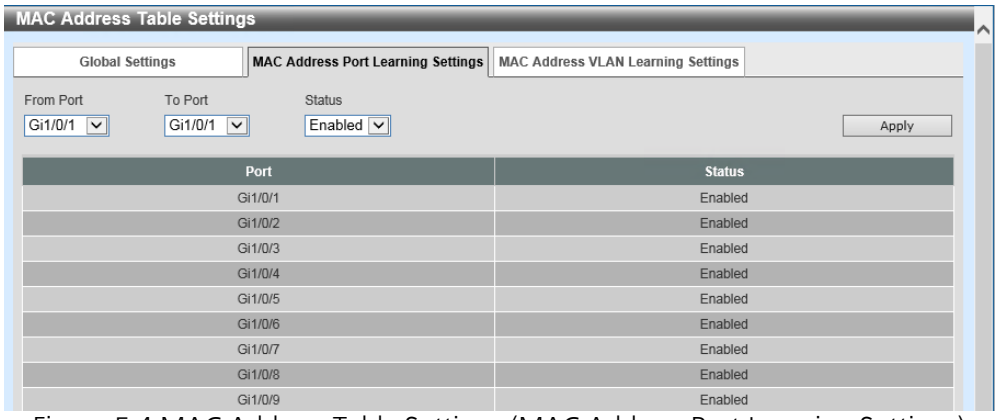


Figure 5-4 MAC Address Table Settings (MAC Address Port Learning Settings)

The following parameters can be configured in the **MAC Address Port Learning Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used 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.

Click the **MAC Address VLAN Learning Settings** tab to view the following window:

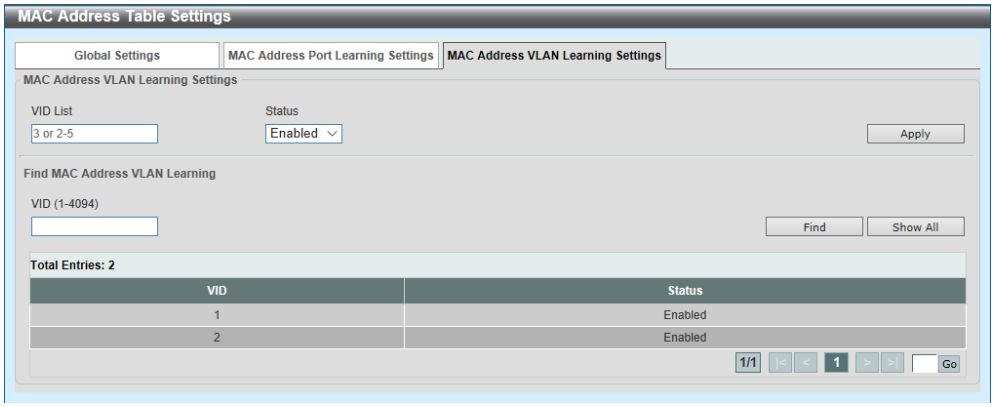


Figure 5-5 MAC Address Table Settings (MAC Address VLAN Learning Settings)

The following parameters can be configured in the **MAC Address VLAN Learning Settings** section:

Parameter	Description
VID List	Enter the VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.
Status	Select to enable or disable the MAC address learning function on the VLAN(s) specified here.

Click the **Apply** button to add a new entry based on the information specified.

The following parameters can be configured in the **Find MAC Address VLAN Learning** section:

Parameter	Description
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

Click the **Find** button to find and display entries in the table based on the search criteria specified.
Click the **Show All** button to find and display all available entries.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

5.1.3 MAC Address Table

This window is used to display and clear MAC address table entries.

Click **L2 Features > FDB > MAC Address Table** to view the following window:

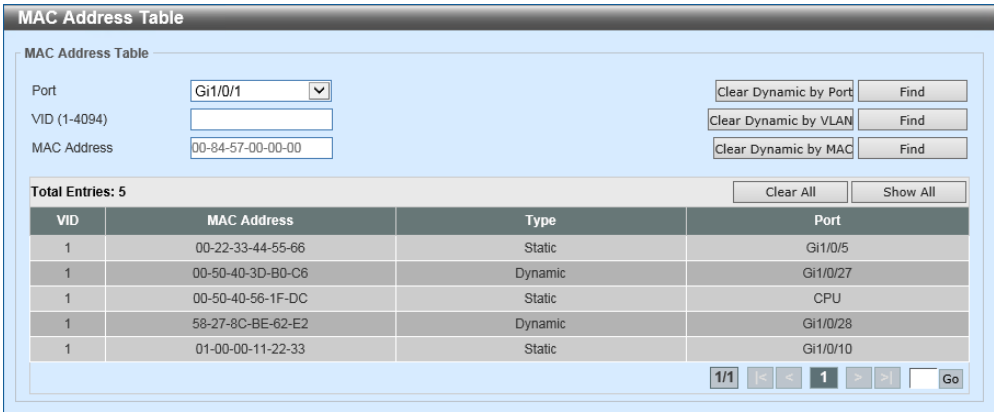


Figure 5-6 MAC Address Table

The following parameters can be configured in the **MAC Address Table** section:

Parameter	Description
Port	Select the port number of the Switch that will be configured here.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.
MAC Address	Enter the MAC address that will be used for this configuration here.

Click the **Clear Dynamic by Port** button to clear all the dynamic MAC addresses associated with the port specified.
Click the **Clear Dynamic by VLAN** button to clear all the dynamic MAC addresses associated with the VLAN specified.
Click the **Clear Dynamic by MAC** button to clear the specified dynamic MAC address from the table.
Click the **Find** button to find and display entries in the table based on the search criteria specified.
Click the **Clear All** button to remove all the entries from the table.
Click the **Show All** button to find and display all available entries.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

5.1.4 MAC Notification

This window is used to configure and display the global MAC notification settings and the MAC notification settings on the specified port(s).

Click **L2 Features > FDB > MAC Notification** to view the following window:

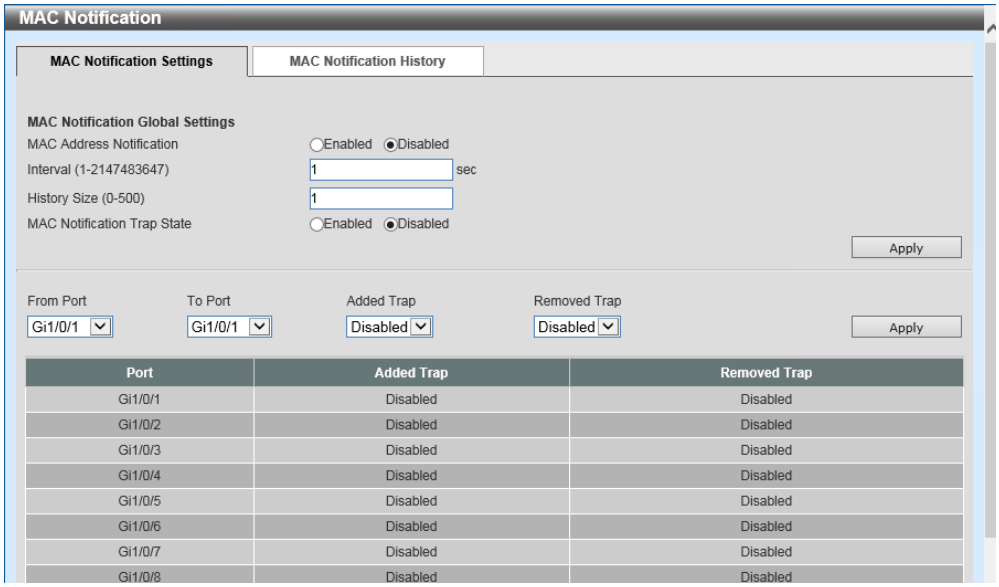


Figure 5-7 MAC Notification (MAC Notification Settings)

The following parameters can be configured in the **MAC Notification Global Settings** section:

Parameter	Description
MAC Address Notification	Select to enable or disable MAC notification globally on the Switch.
Interval	Enter the time value between notifications. The range is from 1 to 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. The range is from 0 to 500. By default, this value is 1.
MAC Notification Trap State	Select to enable or disable the MAC notification trap state.
From Port - To Port	Select the port(s) that will be used 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.

Click the **MAC Notification History** tab to view the following window:

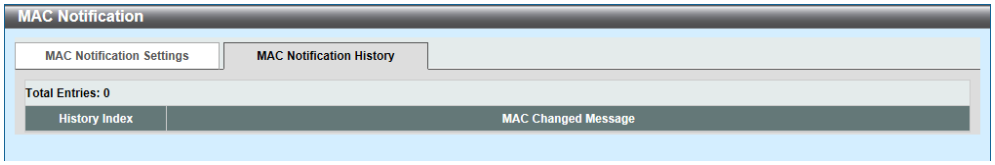


Figure 5-8 MAC Notification (MAC Notification History)

5.2 Link Aggregation

This window is used to configure and display the link aggregation settings.

Click **L2 Features > Link Aggregation** to view the following window:

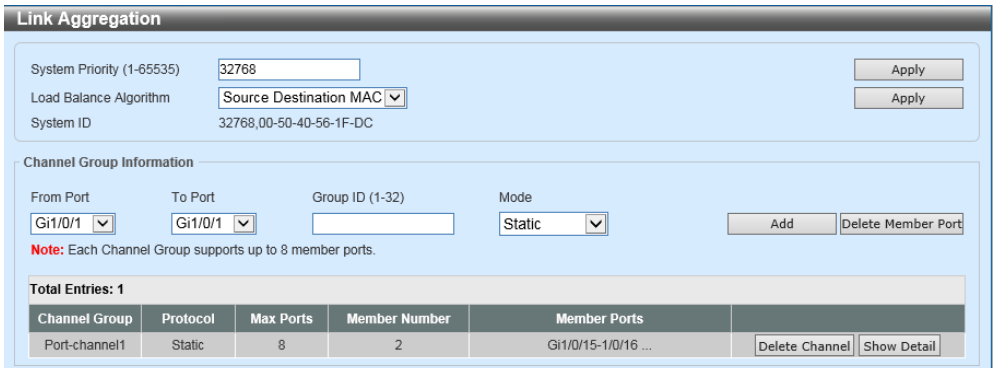


Figure 5-9 Link Aggregation

The following parameters can be configured in the first section:

Parameter	Description
System Priority	Enter the system priority value used here. The range is from 1 to 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 balance algorithm that will be used here. Options to choose from are **Source MAC**, **Destination MAC**, **Source Destination MAC**, **Source IP**, **Destination IP**, **Source Destination IP**, **Source L4 Port**, **Destination L4 Port**, and **Source Destination L4 Port**. By default, this option is **Source Destination MAC**.

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

The following parameters can be configured in the **Channel Group Information** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Group ID	Enter the channel group number here. The range is from 1 to 32. 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.

Parameter	Description
Mode	Select the mode option here. Options to choose from are **Static**, **Active**, and **Passive**. If the mode **Static** is specified, the channel group type is static. If the mode **Active** or **Passive** is specified, the channel group type is the Link Aggregation Control Protocol (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 entry based on the information specified.
Click the **Delete Member Port** button to delete the member ports from the specified port-channel.
Click the **Delete Channel** button to delete the entry.
Click the **Show Detail** button to display detailed information related to the entry.

Click the **Show Detail** button to view the following window:

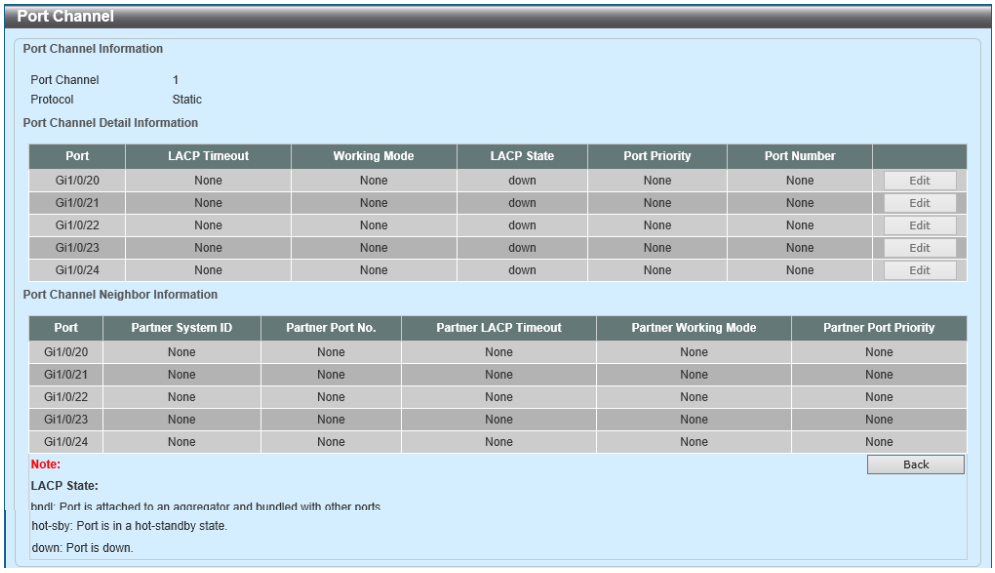


Figure 5-10 Link Aggregation (Show Detail)

Click the **Edit** button to edit the settings of the entry.
Click the **Back** button to return to the previous window.

5.3 VLAN (Virtual Local Area Network)

5.3.1 802.1Q VLAN

This window is used to configure and display the IEEE 802.1Q VLAN settings.

Click **L2 Features > VLAN > 802.1Q VLAN** to view the following window:

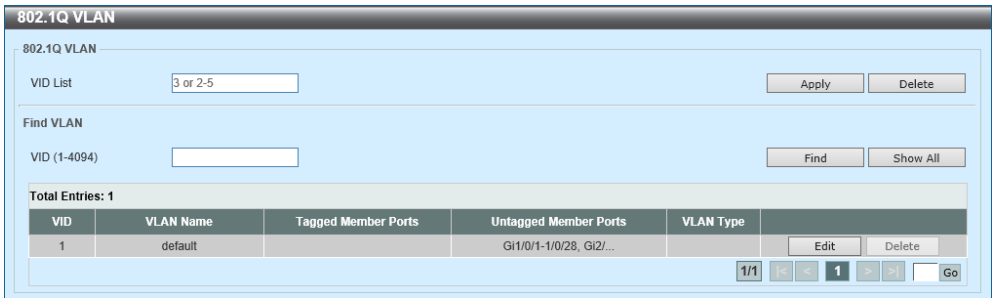


Figure 5-11 802.1Q VLAN

The following parameters can be configured in the **802.1Q VLAN** section:

Parameter	Description
VID List	Enter the VLAN ID(s) that will be created or deleted here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.

Click the **Apply** button to add a new entry based on the information specified.
Click the **Delete** button to delete an entry based on the information specified.

The following parameters can be configured in the **Find VLAN** section:

Parameter	Description
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

Click the **Find** button to find and display entries in the table based on the search criteria specified.
Click the **Show All** button to find and display all available entries.
Click the **Edit** button to edit the settings of the entry.
Click the **Delete** button to delete the entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

5.3.2 802.1v Protocol VLAN

5.3.2.1 Protocol VLAN Profile

This window is used to configure and display IEEE 802.1v protocol VLAN settings. Multiple VLANs are supported for each protocol. Untagged ports can be configured for different protocols on the same physical port.

Click **L2 Features > VLAN > 802.1v Protocol VLAN > Protocol VLAN Profile** to view the following window:

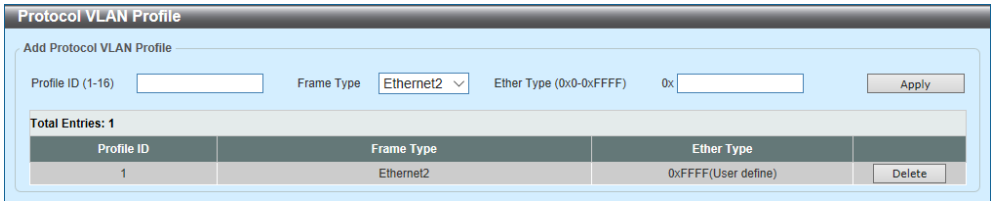


Figure 5-12 Protocol VLAN Profile

The following parameters can be configured in the **Add Protocol VLAN Profile** section:

Parameter	Description
Profile ID	Enter the 802.1v protocol VLAN profile ID here. The range is from 1 to 16.
Frame Type	Select the frame type option here. This function maps packets to protocol-defined VLANs by examining the type octet within the packet header to discover the type of protocol associated with it. Options to choose from are **Ethernet 2**, **SNAP**, and **LLC**. SNAP stands for Subnetwork Access Protocol. LLC stands for Logical Link Control.
Ether Type	Enter the Ethernet type value for the group here. The protocol value is used to identify a protocol of the frame type specified. The range is from 0x0 to 0xFFFF. Depending on the frame type, the octet string will have one of the following values: • For **Ethernet 2**, this is a 16-bit (2-octet) hex value. For example, IPv4 is 0800, IPv6 is 86DD, ARP is 0806, etc. • For IEEE802.3 **SNAP**, this is a 16-bit (2-octet) hex value. • For IEEE802.3 **LLC**, this is a 2-octet IEEE 802.2 Link

Click the **Apply** button to add a new entry based on the information specified.
Click the **Delete** button to delete the entry.

5.3.2.2 Protocol VLAN Profile Interface

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

Click **L2 Features > VLAN > 802.1v Protocol VLAN > Protocol VLAN Profile Interface** to view the following window:

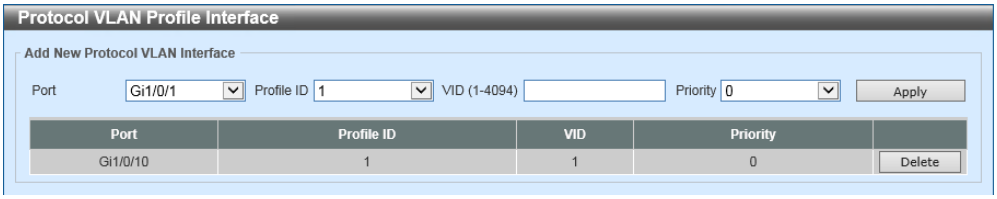


Figure 5-13 Protocol VLAN Profile Interface

The following parameters can be configured in the **Add New Protocol VLAN Interface** section:

Parameter	Description
Port	Select the port number of the Switch that will be configured here.
Profile ID	Select the 802.1v protocol VLAN profile ID here.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.
Priority	Select the priority value used here. This value is between 0 and 7. This parameter is specified to re-write the 802.1p default priority previously set in the Switch, which is used to determine the Class of Service (CoS) queue that packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously.

Click the **Apply** button to add a new entry based on the information specified.
Click the **Delete** button to delete the entry.

5.3.3 GVRP

5.3.3.1 GVRP Global

This window is used to configure and display the global GARP VLAN Registration Protocol (GVRP) settings. GARP stands for Generic Attribute Registration Protocol.

Click **L2 Features > VLAN > GVRP > GVRP Global** to view the following window:

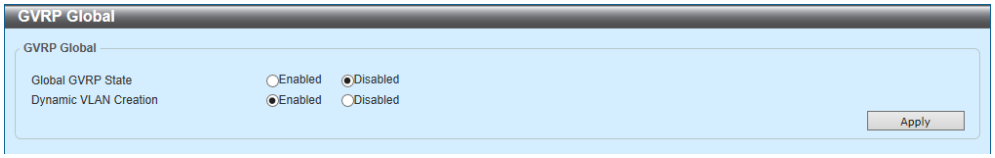


Figure 5-14 GVRP Global

The following parameters can be configured in the **GVRP Global** section:

Parameter	Description
Global GVRP State	Select to enable or disable the global GVRP state here.
Dynamic VLAN Creation	Select to enable or disable the dynamic VLAN creation function here.

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

5.3.3.2 GVRP Port

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

Click **L2 Features > VLAN > GVRP > GVRP Port** to view the following window:

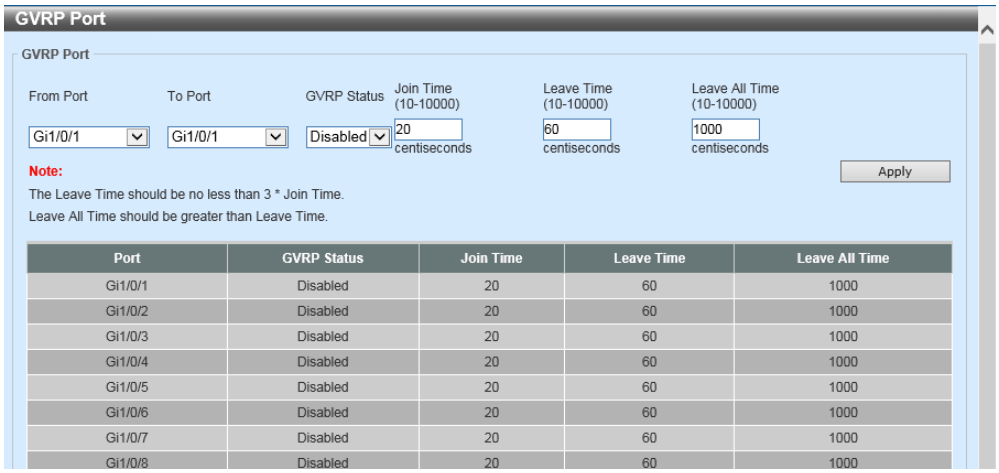


Figure 5-15 GVRP Port

The following parameters can be configured in the **GVRP Port** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
GVRP Status	Select the enable or disable the GVRP port status. This enables the port to become a member of a VLAN dynamically. By default, this option is disabled.
Join Time	Enter the Join Time value here. The range is from 10 to 10000 centiseconds. By default, this value is 20 centiseconds.
Leave Time	Enter the Leave Time value here. The range is from 10 to 10000 centiseconds. By default, this value is 60 centiseconds.
Leave All Time	Enter the Leave All Time value here. The range is from 10 to 10000 centiseconds. By default, this value is 1000 centiseconds.

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

5.3.3.3 GVRP Advertise VLAN

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

Click **L2 Features > VLAN > GVRP > GVRP Advertise VLAN** to view the following window:

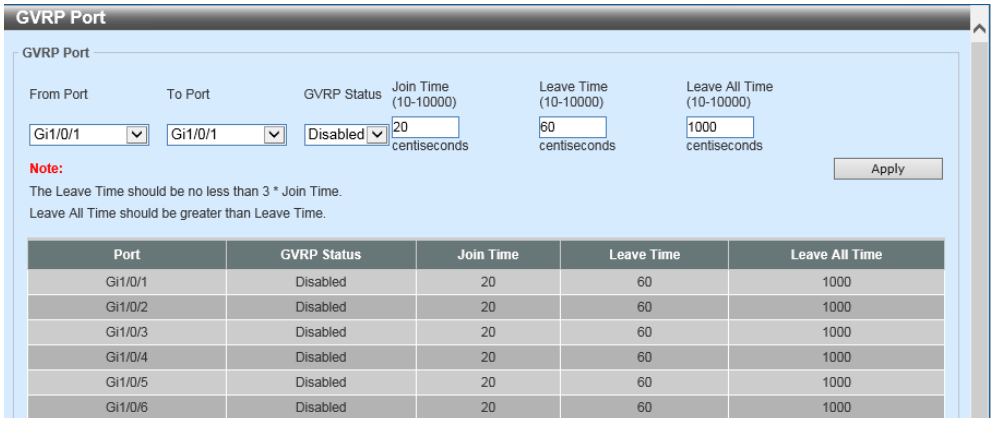


Figure 5-16 GVRP Advertise VLAN

The following parameters can be configured in the **GVRP Advertise VLAN** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Action	Select the advertised VLAN to port mapping action here. Options to choose from are **All**, **Add**, **Remove**, and **Replace**. When selecting **All**, all the advertised VLANs will be used.
Advertise VID List	Enter the VLAN ID(s) that will be advertised used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.

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

5.3.3.4 GVRP Forbidden VLAN

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

Click **L2 Features > VLAN > GVRP > GVRP Forbidden VLAN** to view the following window:

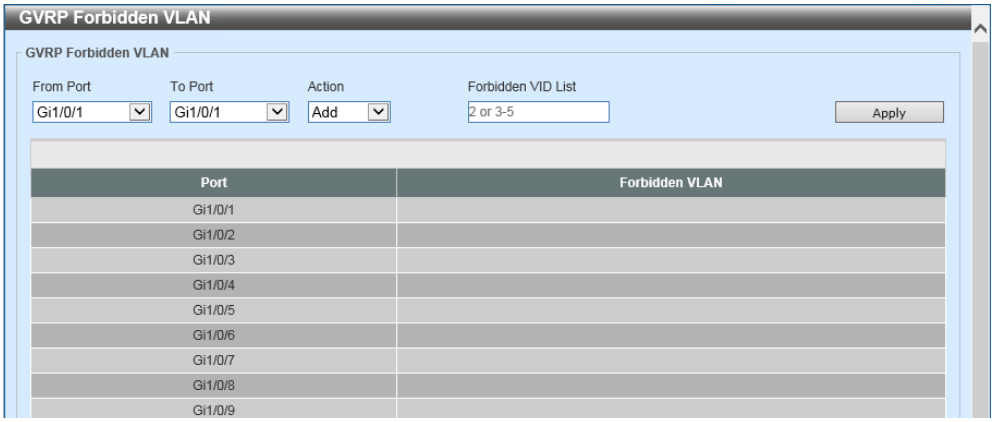


Figure 5-17 GVRP Forbidden VLAN

The following parameters can be configured in the **GVRP Forbidden VLAN** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Action	Select the forbidden VLAN to port mapping action that will be taken here. Options to choose from are **All**, **Add**, **Remove**, and **Replace**. When selecting **All**, all the forbidden VLANs will be used.
Forbidden VID List	Enter the VLAN ID(s) that will be forbidden used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.

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

5.3.3.5 GVRP Statistics Table

This window is used to display and clear the GVRP statistics.

Click **L2 Features > VLAN > GVRP > GVRP Statistics Table** to view the following window:

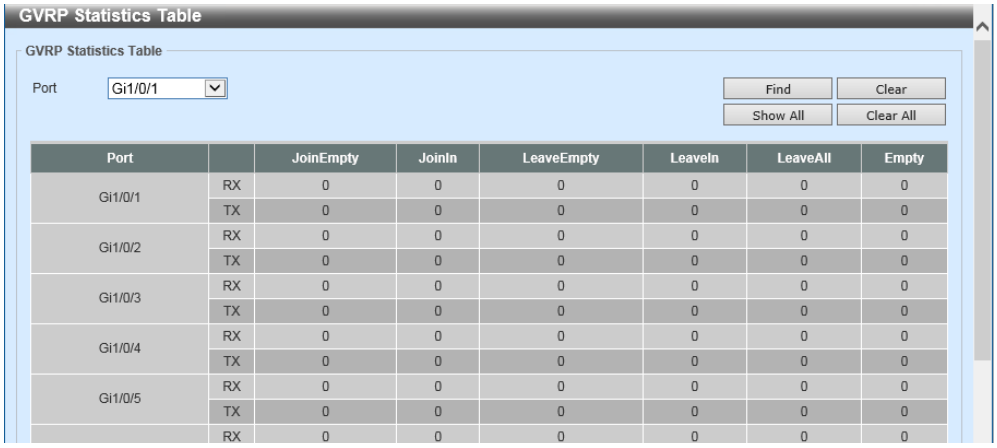


Figure 5-18 GVRP Statistics Table

The following parameters can be configured in the **GVRP Statistics Table** section:

Parameter	Description
Port	Select the port that will be used here.

Click the **Find** button to find and display entries in the table based on the search criteria specified.
Click the **Clear** button to clear the statistics information from the port specified.
Click the **Show All** button to find and display all available entries.
Click the **Clear All** button to clear all the statistics information from all the ports.

5.3.4 Asymmetric VLAN

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

Click **L2 Features > VLAN > Asymmetric VLAN** to view the following window:

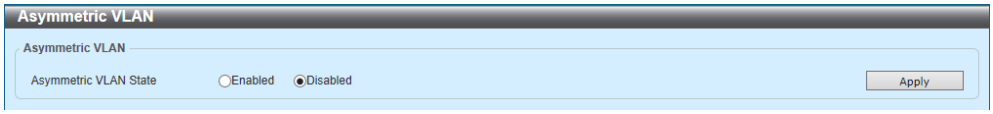


Figure 5-19 Asymmetric VLAN

The following parameters can be configured in the **Asymmetric VLAN** section:

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

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

5.3.5 MAC VLAN

This window is used to configure and display the MAC-based VLAN settings. VLAN operating on a port will change when a static MAC-based VLAN entry is configured and associated to that port.

Click **L2 Features > VLAN > MAC VLAN** to view the following window:

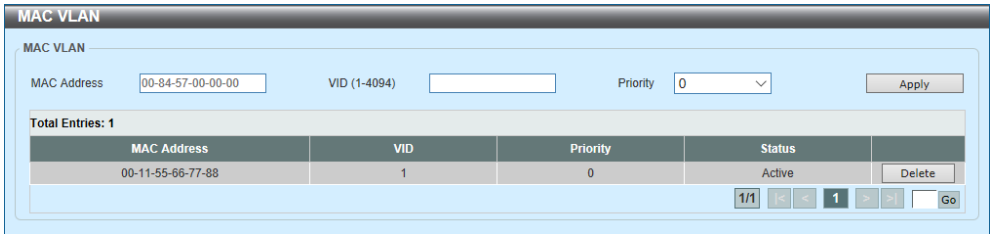


Figure 5-20 MAC VLAN

The following parameters can be configured in the **MAC VLAN** section:

Parameter	Description
MAC Address	Enter the unicast MAC address.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.
Priority	Select the priority that is assigned to untagged packets. This value is between 0 and 7.

Click the **Apply** button to add a new entry based on the information specified.
Click the **Delete** button to delete the entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

5.3.6 VLAN Interface

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

Click **L2 Features > VLAN > VLAN Interface** to view the following window:

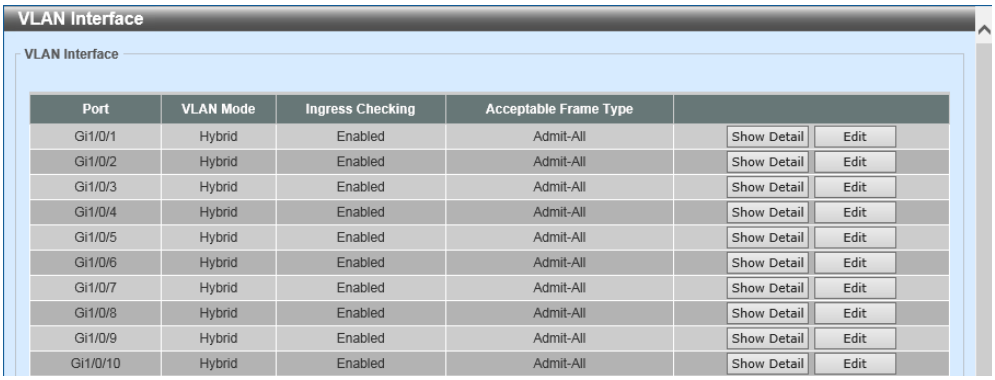


Figure 5-21 VLAN Interface

Click the **Show Detail** button to display detailed information related to the entry.
Click the **Edit** button to edit the settings of the entry.

Click the **Show Detail** button to view the following window:

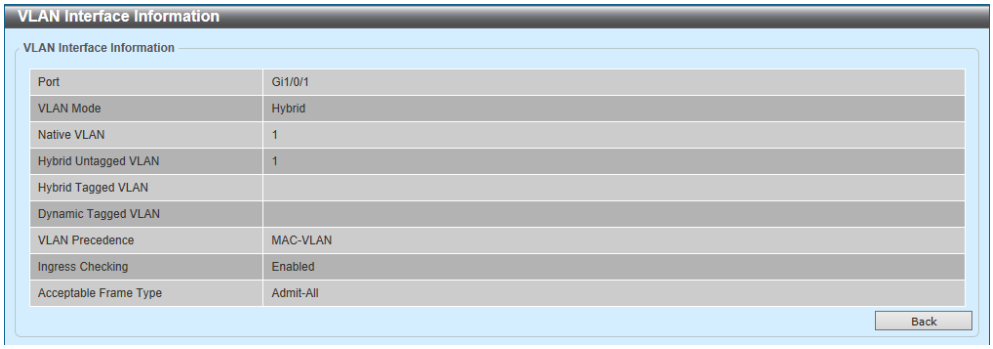


Figure 5-22 VLAN Interface (Show Detail)

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

Click the **Edit** button to view the following window:

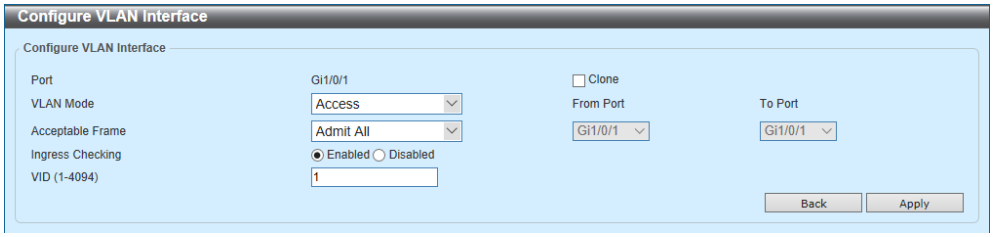


Figure 5-23 VLAN Interface (Edit, Access)

The following parameters can be configured in the **Configure VLAN Interface** section:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are **Access**, **Hybrid**, **Trunk**, **Promiscuous**, and **Host**.
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.
VLAN ID	Enter the VLAN ID used for this configuration here. The range is from 1 to 4094.
Clone	Select this option to enable the clone feature.
From Port - To Port	Select the port(s) that will be used here.

Click the **Apply** button to accept the changes made.
Click the **Back** button to return to the previous window.

Select **Hybrid** as the **VLAN Mode** to view the following window:

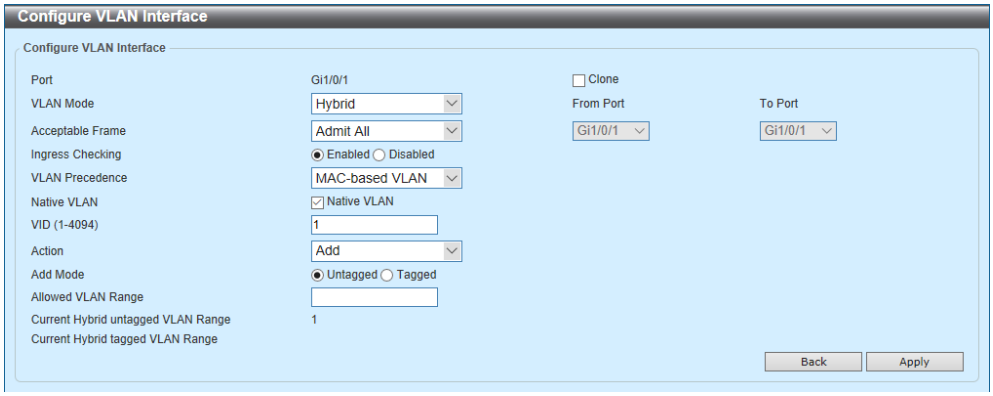


Figure 5-24 VLAN Interface (Edit, Hybrid)

The following parameters can be configured in the **Configure VLAN Interface** section:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are **Access**, **Hybrid**, **Trunk**, **Promiscuous**, and **Host**.
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.
VLAN Precedence	Select the VLAN precedence option here. Options to choose from are **MAC-based VLAN** and **Subnet-based VLAN**.
Native VLAN	Tick this option to enable the native VLAN function.
VID	After ticking the **Native VLAN** option, this parameter will be available. Enter the VLAN ID that will be used here. The range is from 1 to 4094.
Action	Select the action that will be taken here. Options to choose from are **None**, **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 port(s) that will be used here.

Click the **Apply** button to accept the changes made.
Click the **Back** button to return to the previous window.

Select **Trunk** as the **VLAN Mode** to view the following window:

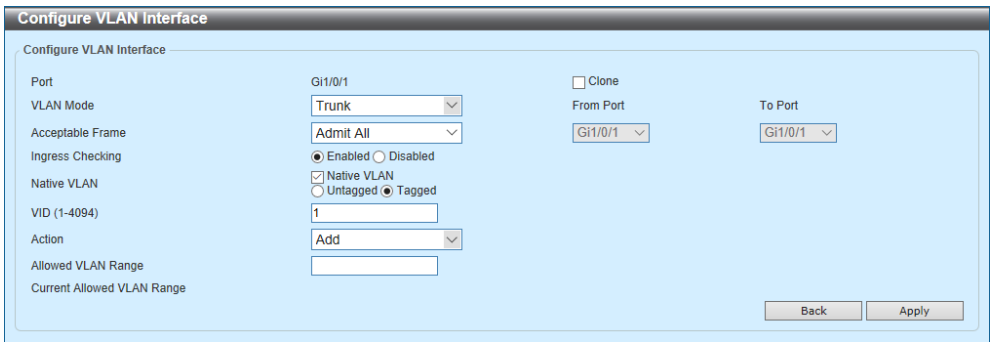


Figure 5-25 VLAN Interface (Edit, Trunk)

The following parameters can be configured in the **Configure VLAN Interface** section:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are **Access**, **Hybrid**, **Trunk**, **Promiscuous**, and **Host**.
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, this parameter will be available. Enter the VLAN ID that will be used here. The range is from 1 to 4094.
Action	Select the action that will be taken here. Options to choose from are **None**, **All**, **Add**, **Remove**, **Except**, and **Replace**.
Allowed VLAN Range	Enter the allowed VLAN range here.
Clone	Select this option to enable the clone feature.
From Port - To Port	Select the port(s) that will be used here.

Click the **Apply** button to accept the changes made.
Click the **Back** button to return to the previous window.

Select **Promiscuous** as the **VLAN Mode** to view the following window:

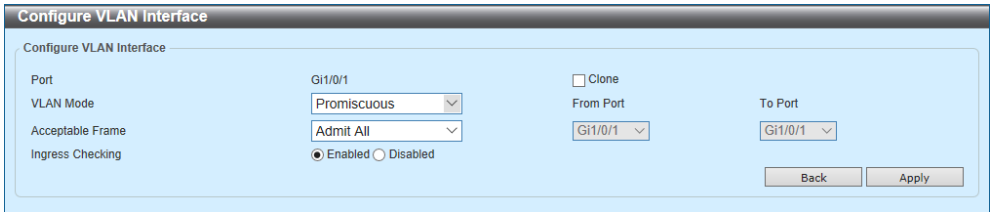


Figure 5-26 VLAN Interface (Edit, Promiscuous)

The following parameters can be configured in the **Configure VLAN Interface** section:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are **Access**, **Hybrid**, **Trunk**, **Promiscuous**, and **Host**.
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.
Clone	Select this option to enable the clone feature.
From Port - To Port	Select the port(s) that will be used here.

Click the **Apply** button to accept the changes made.
Click the **Back** button to return to the previous window.

Select **Host** as the **VLAN Mode** to view the following window:

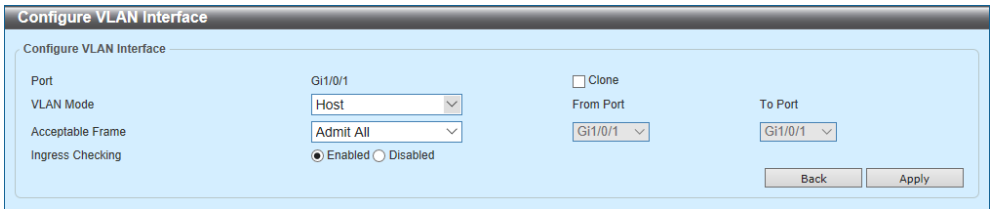


Figure 5-27 VLAN Interface (Edit, Host)

The following parameters can be configured in the **Configure VLAN Interface** section:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are **Access**, **Hybrid**, **Trunk**, **Promiscuous**, and **Host**.
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.
Clone	Select this option to enable the clone feature.
From Port - To Port	Select the port(s) that will be used here.

Click the **Apply** button to accept the changes made.
Click the **Back** button to return to the previous window.

5.3.7 Subnet VLAN

This window is used to configure and display the subnet VLAN settings. If an untagged or priority-tagged IP packet is received on a port, its source IP address will be used to match the subnet VLAN entries. If the source IP is in the subnet of an entry, the packet will be classified to the VLAN defined for this subnet.

Click **L2 Features > VLAN > Subnet VLAN** to view the following window:

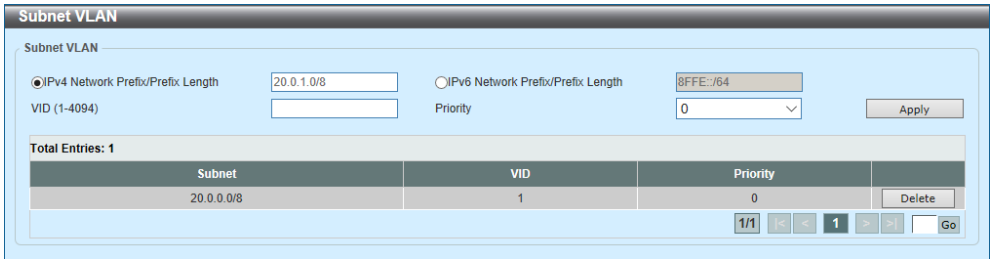


Figure 5-28 Subnet VLAN

The following parameters can be configured in the **Subnet VLAN** section:

Parameter	Description
IPv4 Network Prefix / Prefix Length	Select and enter the IPv4 address and prefix length value for the subnet VLAN here.
IPv6 Network Prefix / Prefix Length	Select and enter the IPv6 address and prefix length value for the subnet VLAN here.
VID	Enter the subnet VLAN ID that will be used here. The range is from 1 to 4094.
Priority	Select the priority value used here. This value is between 0 and 7. A lower value takes higher priority.

Click the **Apply** button to add a new entry based on the information specified.
Click the **Delete** button to delete the entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

5.3.8 Voice VLAN

5.3.8.1 Voice VLAN Global

This window is used to configure and display the global voice VLAN settings. This is used to globally enable or disable the voice VLAN feature and to specify the voice VLAN on the switch. Only one voice VLAN can be specified on the switch.

Click **L2 Features > VLAN > Voice VLAN > Voice VLAN Global** to view the following window:

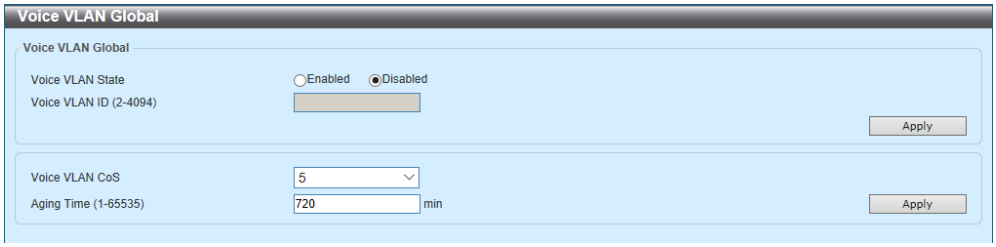


Figure 5-29 Voice VLAN Global

The following parameters can be configured in the **Voice VLAN Global** section:

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.

5.3.8.2 Voice VLAN Port

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

Click **L2 Features > VLAN > Voice VLAN > Voice VLAN Port** to view the following window:

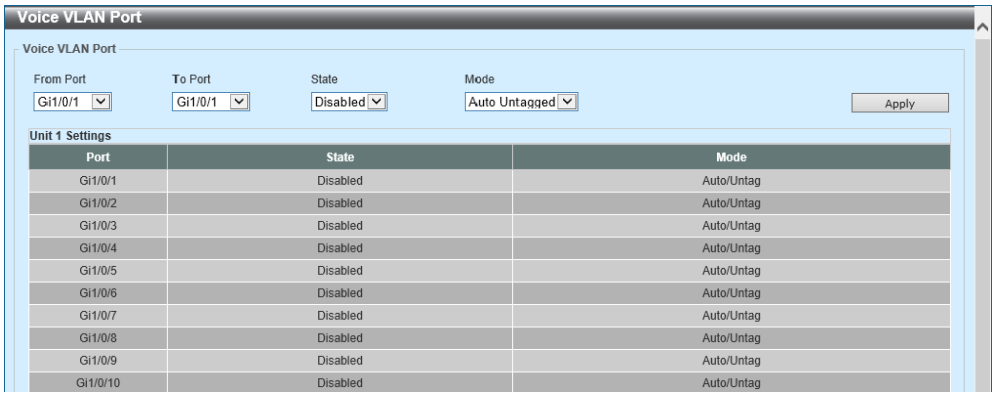


Figure 5-30 Voice VLAN Port

The following parameters can be configured in the **Voice VLAN Port** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used 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 address of the packet complies with the OUI addresses.

Parameter	Description
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

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

5.3.8.3 Voice VLAN OUI

This window is used to configure and display the voice VLAN OUI settings. A user-defined OUI can be associated with a voice VLAN. If the source MAC address of the received packet matches any of the OUI patterns, the received packet is determined as a voice packet. Default OUIs cannot be deleted or duplicated.

Click **L2 Features > VLAN > Voice VLAN > Voice VLAN OUI** to view the following window:

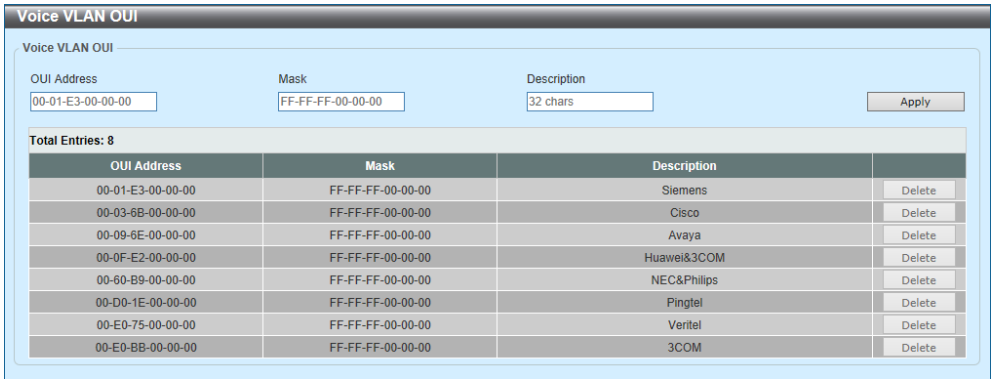


Figure 5-31 Voice VLAN OUI

The following parameters can be configured in the **Voice VLAN OUI** section:

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 add a new entry based on the information specified.
Click the **Delete** button to delete the entry.

5.3.8.4 Voice VLAN Device

This window is used to display the voice VLAN device table and information.

Click **L2 Features > VLAN > Voice VLAN > Voice VLAN Device** to view the following window:

Figure 5-32 Voice VLAN Device

5.3.8.5 Voice VLAN LLDP-MED Device

This window is used to display the voice VLAN LLDP-MED device table and information.

Click **L2 Features > VLAN > Voice VLAN > Voice VLAN LLDP-MED Device** to view the following window:

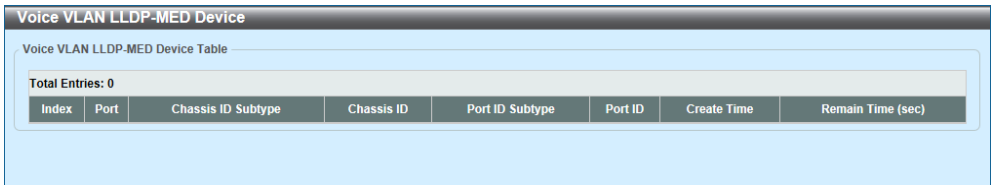


Figure 5-33 Voice VLAN LLDP-MED Device

5.3.9 Private VLAN

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

Click **L2 Features > VLAN > Private VLAN** to view the following window:

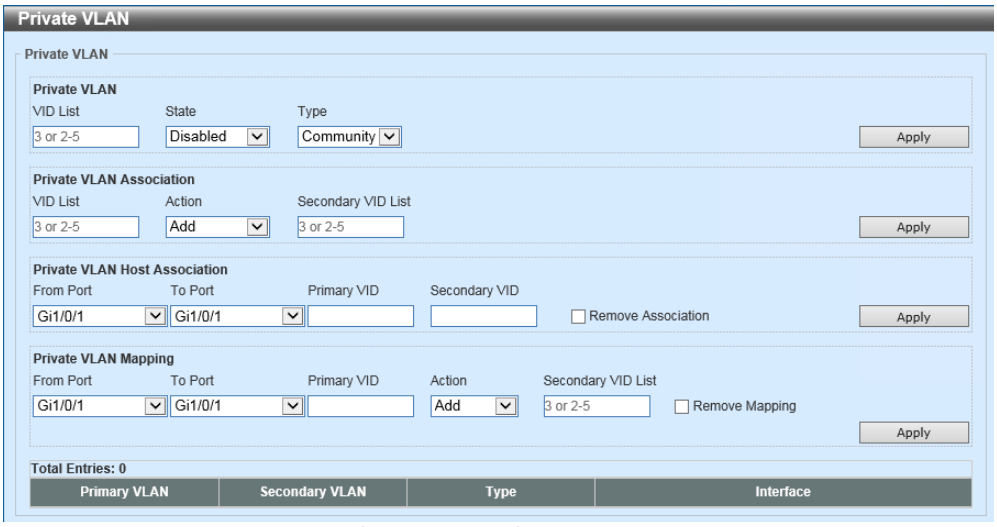


Figure 5-34 Private VLAN

The following parameters can be configured in the **Private VLAN** section:

Parameter	Description
VID List	Enter the private VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.
State	Select to enable or disable the private VLAN state here.
Type	Select the type of private VLAN that will be created here. Options to choose from are **Community**, **Isolated**, and **Primary**.

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

The following parameters can be configured in the **Private VLAN Association** section:

Parameter	Description
VID List	Enter the private VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.
Action	Select the action that will be taken for the private VLAN here. Options to choose from are **Add**, **Remove**, and **Disabled**.

Parameter	Description
Secondary VID List	Enter the secondary private VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.

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

The following parameters can be configured in the **Private VLAN Host Association** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Primary VID	Enter the primary VLAN ID that will be used here. The range is from 1 to 4094.
Secondary VID	Enter the secondary VLAN ID that will be used here. The range is from 1 to 4094. When ticking the **Remove Association** option, specifies that this configuration will not be enabled.

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

The following parameters can be configured in the **Private VLAN Mapping** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Primary VID	Enter the primary VLAN ID that will be used here. The range is from 1 to 4094.
Action	Select **Add** to add a new entry based in the information entered. Select **Remove** to remove an entry based in the information entered.
Secondary VID List	Enter the secondary VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094. When ticking the **Remove Mapping** option, this specifies that this configuration will not be enabled.

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

5.4 STP (Spanning Tree Protocol)

5.4.1 STP Global Settings

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

Click **L2 Features > STP > STP Global Settings** to view the following window:

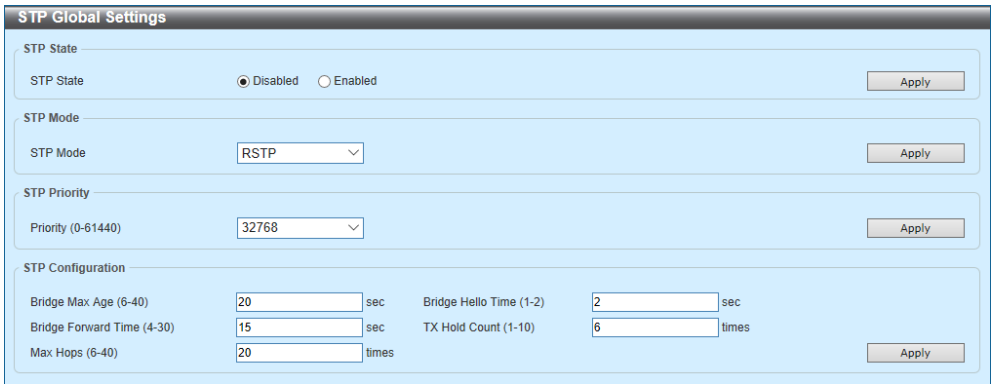


Figure 5-35 STP Global Settings

The following parameters can be configured in the **STP State** section:

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

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

The following parameters can be configured in the **STP Mode** section:

Parameter	Description
STP Mode	Select the STP mode used here. Options to choose from are MSTP, RSTP, and STP. MSTP stands for Multiple Spanning Tree Protocol. RSTP stands for Rapid Spanning Tree Protocol. STP stands for Spanning Tree Protocol.

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

The following parameters can be configured in the **STP Priority** section:

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

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

The following parameters can be configured in the **STP Configuration** section:

Parameter	Description
Bridge Max Age	Enter the bridge maximum age value here. The range is from 6 to 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. The range is from 1 to 2 seconds. By default, this value is 2 seconds. This is the interval between two transmissions of Bridge Protocol Data Unit (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 Rapid Spanning Tree Protocol (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. The range is from 4 to 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. The range is from 1 to 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. The range is from 6 to 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.

5.4.2 STP Port Settings

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

Click **L2 Features > STP > STP Port Settings** to view the following window:

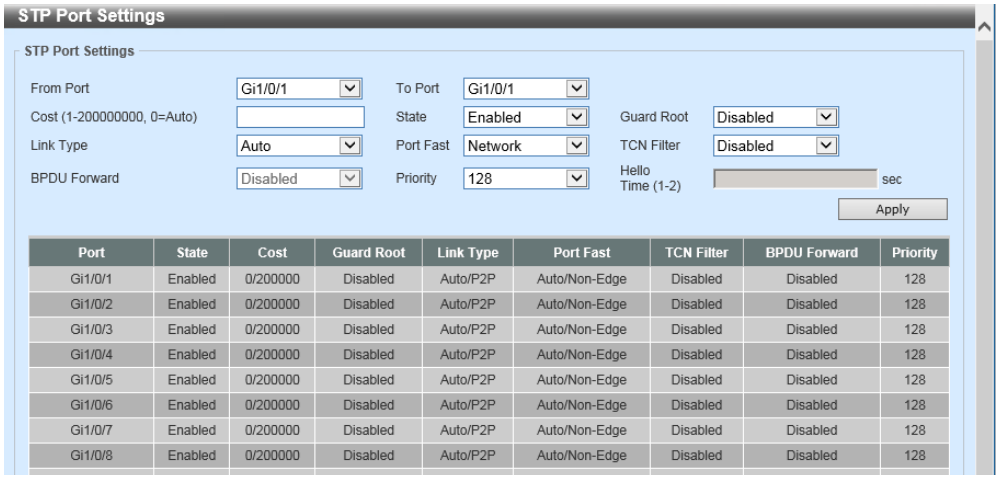


Figure 5-36 STP Port Settings

The following parameters can be configured in the **STP Port Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Cost	Enter the cost value here. The range is from 1 to 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 option here. Options to choose from are **Auto**, **P2P**, and **Shared**. A full-duplex port is considered to have a Point-to-Point (P2P) connection. Alternatively, a half-duplex port is considered to have a Shared connection. The port cannot transit into the forwarding state rapidly by setting the link type to **Shared**. By default, this option is **Auto**.

Parameter	Description
Port Fast	Select the Port Fast option here. Options to choose from are: • **Network** - 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. • **Disabled** - 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. • **Edge** - 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. By default, this option is **Network**.
TCN Filter	Select to enable or disable the Topology Change Notification (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. The range is from **1** to **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.

5.4.3 MST Configuration Identification

This window is used to configure and display the MST configuration identification settings. These settings are used to identify Multiple Spanning Tree Instances (MSTIs) configured on the switch. The default Common Internal Spanning Tree (CIST) can be modified but cannot be deleted and the MSTI ID cannot be changed.

Click **L2 Features > STP > MST Configuration Identification** to view the following window:

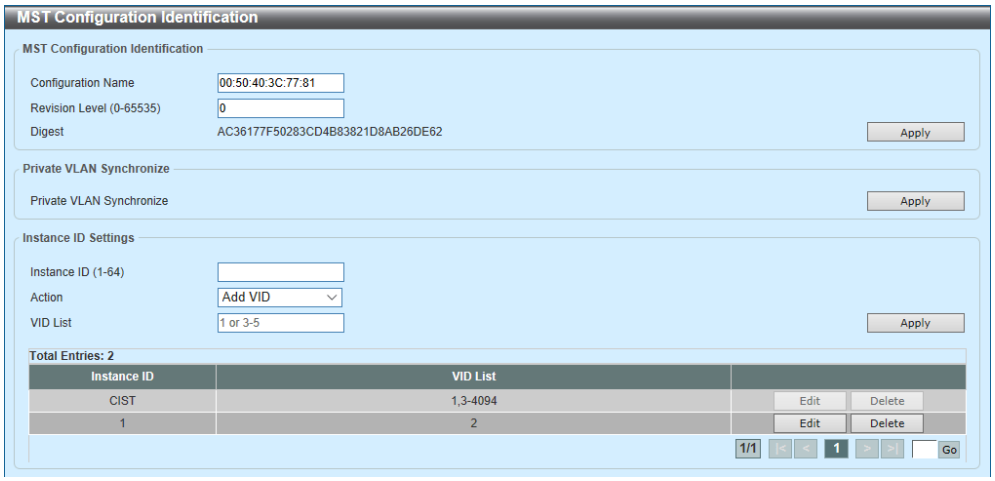


Figure 5-37 MST Configuration Identification

The following parameters can be configured in the **MST Configuration Identification** section:

Parameter	Description
Configuration Name	Enter the MST. This name uniquely identifies the MSTI. If the 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. The range is from 0 to 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 following parameters can be configured in the **Instance ID Settings** section:

Parameter	Description
Instance ID	Enter the instance ID here. The range is from 1 to 64.
Action	Select the action that will be taken here. Options to choose from are **Add VID** and **Remove VID**.
VID List	Enter the VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.

Click the **Apply** button to accept the changes made.
Click the **Edit** button to edit the settings of the entry.
Click the **Delete** button to delete the entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

5.4.4 STP Instance

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

Click **L2 Features > STP > STP Instance** to view the following window:

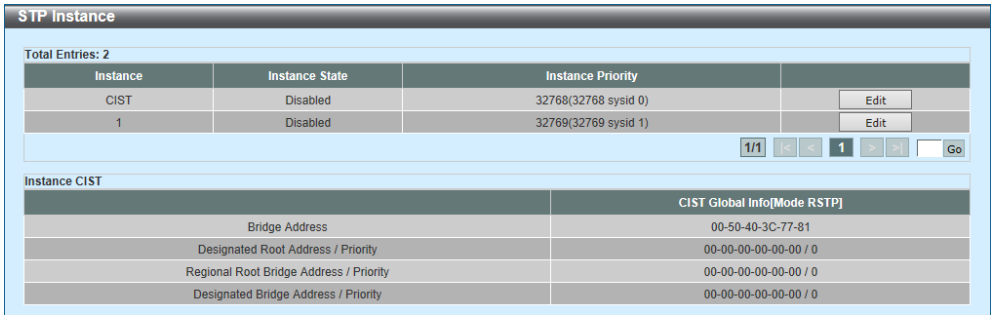


Figure 5-38 STP Instance

The following parameters can be configured in the **STP Instance** section:

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

5.4.5 MSTP Port Information

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

Click **L2 Features > STP > MSTP Port Information** to view the following window:

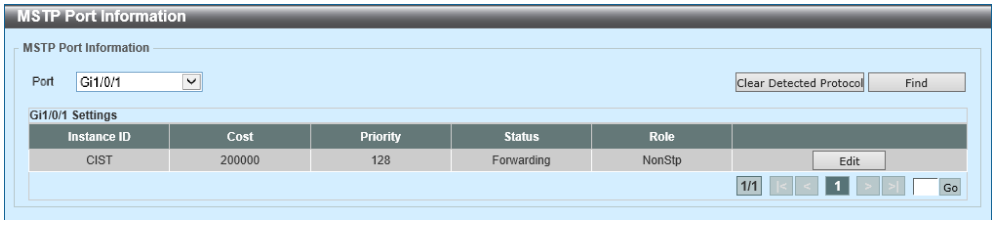


Figure 5-39 MSTP Port Information

The following parameters can be configured in the **MSTP Port Information** section:

Parameter	Description
Port	Select the port that will be used here.
Cost	After clicking the **Edit** button, enter the cost value here. The range is from 1 to 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 128. A lower value has higher priority.

Click the **Clear Detected Protocol** button to remove the detected protocol association from the port specified.
Click the **Find** button to find and display entries in the table based on the search criteria specified.
Click the **Edit** button to edit the settings of the entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

5.5 Line Loopback

5.5.1 Line Loopback Settings

This window is used to configure and display the line loopback settings.

Click **L2 Features > Line Loopback > Line Loopback Settings** to view the following window:

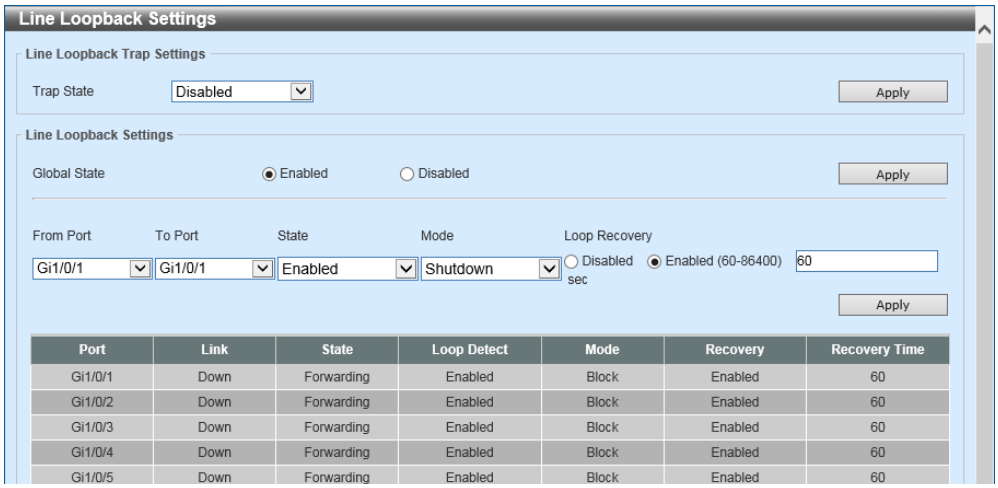


Figure 5-40 Line Loopback Settings

The following parameters can be configured in the **Line Loopback Settings** section:

Parameter	Description
Global State	Select to globally enable or disable the line loopback feature.
From Port - To Port	Select the port(s) that will be used here.
State	Select to enable or disable the line loopback feature on the specified port(s).
Mode	Select the line loopback mode that will be used on the specified port(s). Options to choose from are: • **Shutdown** - Specifies to first set the port(s) to the shutdown state and then to the blocking state when a loop occurs. • **Block** - Specifies to set the port(s) to the blocking state directly when a loop occurs.
Loop Recovery	Select to enable or disable the loop recovery feature here. When enabled, the port(s) will be recovered to the normal state after the timeout value has expired. Enter the timeout value in the space provided. The range is from 60 to 86400 seconds.

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

5.5.2 Line Loopback Log

This window is used to display and clear the line loopback log.

Click **L2 Features > Line Loopback > Line Loopback Log** to view the following window:

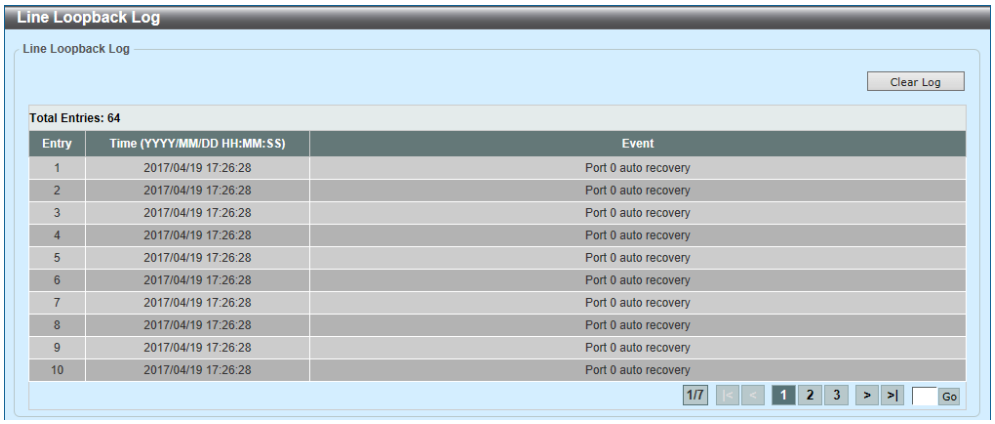


Figure 5-41 Line Loopback Log

Click the **Clear Log** button to clear the log entries from the table.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

5.6 L2 Protocol Tunnel

This window is used to configure and display the Layer 2 protocol tunnel settings.

Click **L2 Features > L2 Protocol Tunnel** to view the following window:

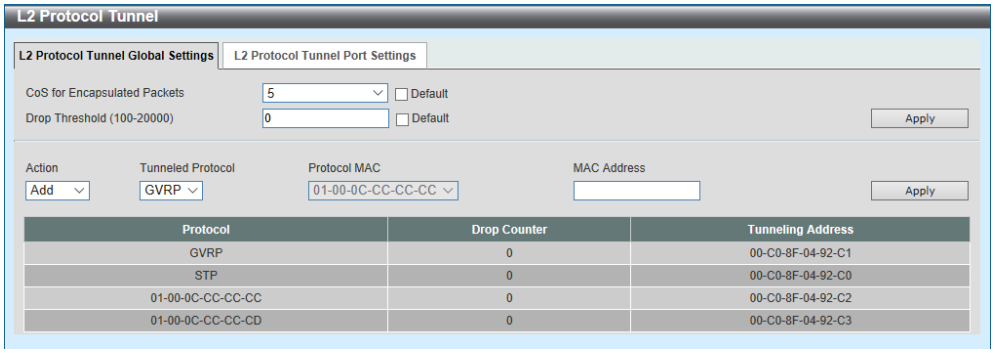


Figure 5-42 L2 Protocol Tunnel (L2 Protocol Tunnel Global Settings)

The following parameters can be configured in the **L2 Protocol Tunnel Global Settings** section:

Parameter	Description
CoS for Encapsulated Packets	Select the CoS value for encapsulated packets here. This value is between 0 and 7. Select the **Default** option to use the default value.
Drop Threshold	Enter the drop threshold value here. The range is from 100 to 20000. By default, this value is 0. The tunneling of the Layer 2 protocol packets will consume CPU processing power in encapsulating, decapsulating, and forwarding of the packet. Use this option to restrict the CPU processing bandwidth consumed by specifying a threshold on the number of all Layer 2 protocol packets that can be processed by the system. When the maximum number of packets is exceeded, the excessive protocol packets are dropped. Select the **Default** option to use the default value.
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**. This is used to add or delete a Layer 2 Protocol Tunneling (L2PT) tunneling multicast address to or from the specified protocol.

Parameter	Description
Tunneled Protocol	Select the tunneled protocol here. Options to choose from are: • **GVRP** - Specifies that GVRP packets will be tunneled to the configured address. • **STP** - Specifies that STP packets will be tunneled to the configured address. • **MAC** - Specifies that protocol packets with the specified destination address will be tunneled to the configured address. • **All** - Specifies that all packets will be tunneled to the configured address.
Protocol MAC	After selecting the **MAC** option as the **Tunneled Protocol**, select the destination address that will be tunneled to the configured address here. Options to choose from are **01-00-0C-CC-CC-CC** and **01-00-0C-CC-CC-CD**.
MAC Address	Enter the MAC address of which the specified protocol will be tunneled to here. This MAC address should not be an address reserved or used by other protocols.

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

Click the **L2 Protocol Tunnel Port Settings** tab to view the following window:

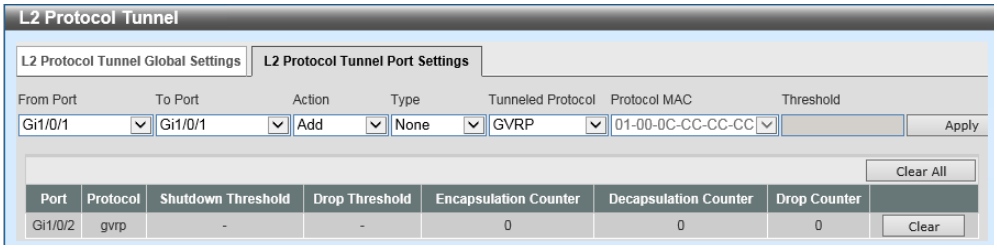


Figure 5-43 L2 Protocol Tunnel (L2 Protocol Tunnel Port Settings)

The following parameters can be configured in the **L2 Protocol Tunnel Port Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Action	Select **Add** to add a new entry based in the information entered. Select **Delete** to delete an entry based in the information entered.
Type	Select the type option here. Options to choose from are **None**, **Shutdown**, and **Drop**.

Parameter	Description
Tunneled Protocol	Select the tunneled protocol option here. Options to choose from are **GVRP**, **STP**, **Protocol MAC**, and **All**.
Protocol MAC	After selecting the **Protocol MAC** option as the **Tunneled Protocol**, the following option will be available. Select the protocol MAC option here. Options to choose from are **01-00-0C-CC-CC-CC** and **01-00-0C-CC-CC-CD**.
Threshold	After selecting the **Shutdown** or **Drop** option in the **Type** field, the following parameter will be available. Enter the threshold value here. The range is from 1 to 4096.

Click the **Apply** button to add a new entry based on the information specified.
Click the **Clear All** button to clear the information from all the entries.
Click the **Clear** button to clear the information from the entry.

5.7 L2 Multicast Control

5.7.1 IGMP Snooping

5.7.1.1 IGMP Snooping Settings

This window is used to configure and display the Internet Group Management Protocol (IGMP) snooping settings.

Click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Settings** to view the following window:

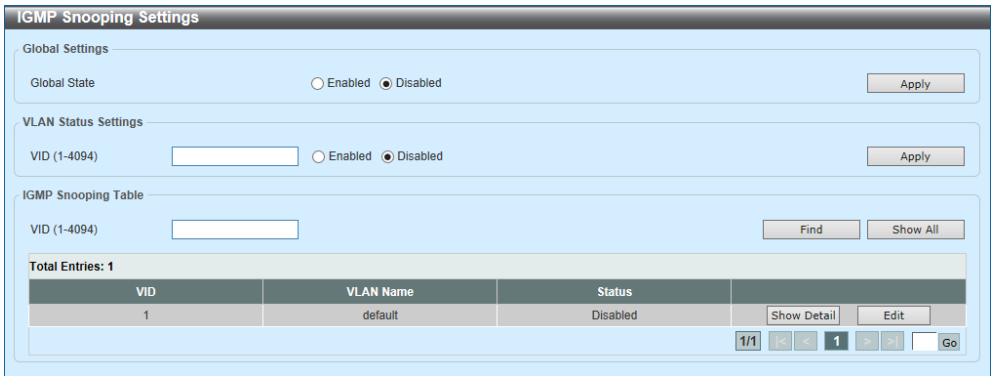


Figure 5-44 IGMP Snooping Settings

The following parameters can be configured in the **Global Settings** section:

Parameter	Description
Global State	Select this option to globally enable or disable IGMP snooping.

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

The following parameters can be configured in the **VLAN Status Settings** section:

Parameter	Description
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

Click the **Apply** button to add a new entry based on the information specified.

The following parameters can be configured in the **IGMP Snooping Table** section:

Parameter	Description
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

Click the **Find** button to find and display entries in the table based on the search criteria specified.
Click the **Show All** button to find and display all available entries.
Click the **Show Detail** button to display detailed information related to the entry.
Click the **Edit** button to edit the settings of the entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **Show Detail** button to view the following window:

Figure 5-45 IGMP Snooping Settings (Show Detail)

Click the **Modify** button to edit the settings.
Click the **Edit** or **Modify** button to view the following window:

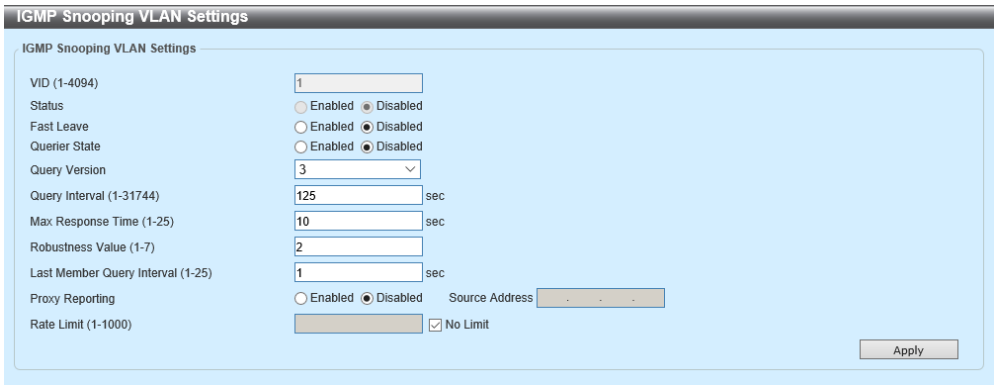


Figure 5-46 IGMP Snooping Settings (Edit, Modify)

The following parameters can be configured in the **IGMP Snooping VLAN Settings** section:

Parameter	Description
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 leave message.
Querier State	Select this option to enable or disable the querier state.
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.
Las 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.
Proxy Reporting	Select this option to enable or disable the proxy-reporting function.
Source Address	Enter the source IP of proxy reporting. This is available when **Enabled** is selected in **Proxy Reporting**.
Rate Limit	Enter the rate limit value here. The range is from 1 to 1000. Tick the **No Limit** option to apply no rate limit on this profile.

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

5.7.1.2 IGMP Snooping Groups Settings

This window is used to configure and display the IGMP snooping group settings.

Click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Groups Settings** to view the following window:

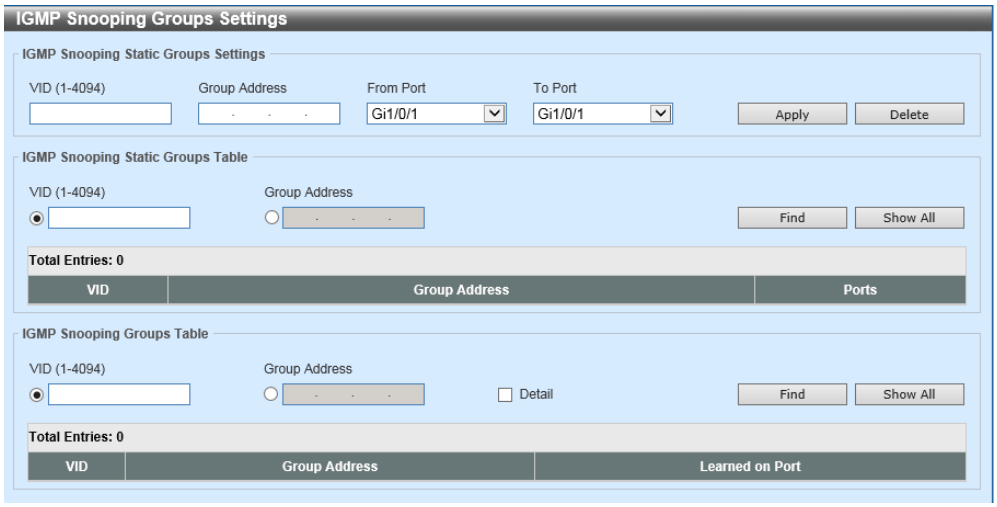


Figure 5-47 IGMP Snooping Groups Settings

The following parameters can be configured in the **IGMP Snooping Static Groups Settings** section:

Parameter	Description
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.
Group Address	Enter an IP multicast group address.
From Port - To Port	Select the port(s) that will be used here.

Click the **Apply** button to add a new entry based on the information specified.
Click the **Delete** button to delete an entry based on the information specified.

The following parameters can be configured in the **IGMP Snooping Static Groups Table** section:

Parameter	Description
VID	Select and enter the VLAN ID that will be used here. The range is from 1 to 4094.
Group Address	Click the radio button and enter an IP multicast group address.

Click the **Find** button to find and display entries in the table based on the search criteria specified.
Click the **Show All** button to find and display all available entries.

The following parameters can be configured in the **IGMP Snooping Groups Table** section:

Parameter	Description
VID	Select and enter the VLAN ID that will be used here. The range is from 1 to 4094.
Group Address	Click the radio button and enter an IP multicast group address.
Detail	Select this option to display the IGMP group detail information.

Click the **Find** button to find and display entries in the table based on the search criteria specified.
Click the **Show All** button to find and display all available entries.

5.7.1.3 IGMP Snooping Filter Settings

This window is used to configure and display the IGMP snooping filter settings.

Click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Filter Settings** to view the following window:

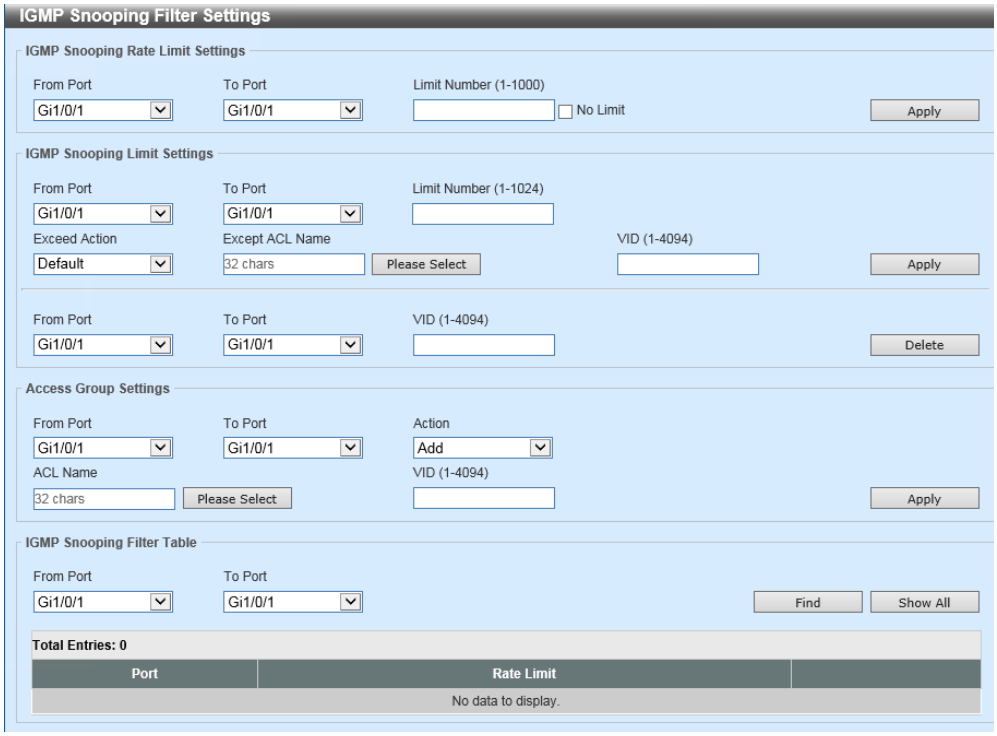


Figure 5-48 IGMP Snooping Filter Settings

The following parameters can be configured in the **IGMP Snooping Rate Limit Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here. This is only available if the Port option was selected as the action below.
Limit Number	Enter the limit number here. This is to configure the rate of IGMP control packets that the Switch can process on a specific interface. The range is from 1 to 1000 packets per second. Select the **No Limit** option to remove the limitation.

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

The following parameters can be configured in the **IGMP Snooping Limit Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Limit Number	Enter the limit number here. This is used to set the limitation on the number of IGMP cache entries that can be created. The range is from 1 to 4096.
Exceed Action	Select the exceed action here. This parameter specifies the action for handling newly learned groups when the limitation is exceeded. Options to choose from are: • **Default** - Specifies that the default action will be taken. • **Drop** - Specifies that the new group will be dropped. • **Replace** - Specifies that the new group will replace the oldest group.
Except ACL Name	Enter the standard IP access list name here. The group (*,G), or channel (S,G) permitted by the access list will be excluded from the limit. To permit a channel (S,G), specify S in the source address field and G in the destination address field of the access list entry. To permit a group (*,G), specify “any” in the source address field and G in the destination address field of the access list entry. This name can be up to 32 characters long. Alternatively, click the **Please Select** button to find and select any of the exiting access lists configured on this Switch to be used in this configuration.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

Click the **Apply** button to add a new entry based on the information specified.
Click the **Delete** button to delete an entry based on the information specified.

The following parameters can be configured in the **Access Group Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Action	Select **Add** to add a new entry based in the information entered. Select **Delete** to delete an entry based in the information entered.
ACL Name	Enter the standard IP access list name here. This is used to permit users to join a group (*, G), specify "any" in source address field and G in destination address field of the access list entry. This name can be up to 32 characters long. Alternatively, click the **Please Select** button to find and select any of the exiting access lists configured on this Switch to be used in this configuration.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

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

The following parameters can be configured in the **IGMP Snooping Filter Table** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.

Click the **Find** button to find and display entries in the table based on the search criteria specified.
Click the **Show All** button to find and display all available entries.
Click the **Show Detail** button to display detailed information related to the entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **Show Detail** button to view the following window:

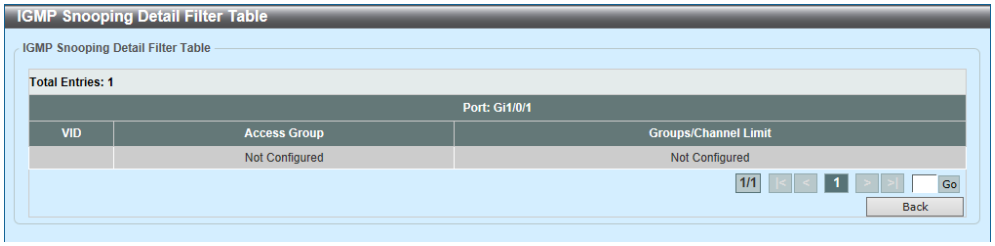


Figure 5-49 IGMP Snooping Filter Settings (Show Detail)

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.
Click the **Back** button to return to the previous window.

5.7.1.4 IGMP Snooping Multicast Router Information

This window is used to configure and display the IGMP Snooping multicast router settings.

Click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Multicast Router Information** to view the following window:

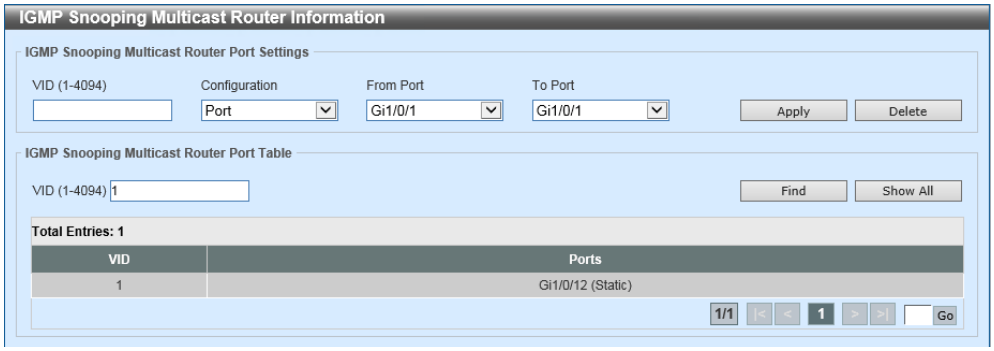


Figure 5-50 IGMP Snooping Multicast Router Information

The following parameters can be configured in the **IGMP Snooping Multicast Router Port Settings** section:

Parameter	Description
VID	Enter the VLAN ID that will be 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 port(s) that will be used here.

Click the **Apply** button to add a new entry based on the information specified.
Click the **Delete** button to delete an entry based on the information specified.

The following parameters can be configured in the **IGMP Snooping Multicast Router Port Table** section:

Parameter	Description
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

Click the **Find** button to find and display entries in the table based on the search criteria specified.
Click the **Show All** button to find and display all available entries.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

5.7.1.5 IGMP Snooping Statistics Settings

This window is used to display and clear IGMP snooping statistics.

Click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Statistics Settings** to view the following window:

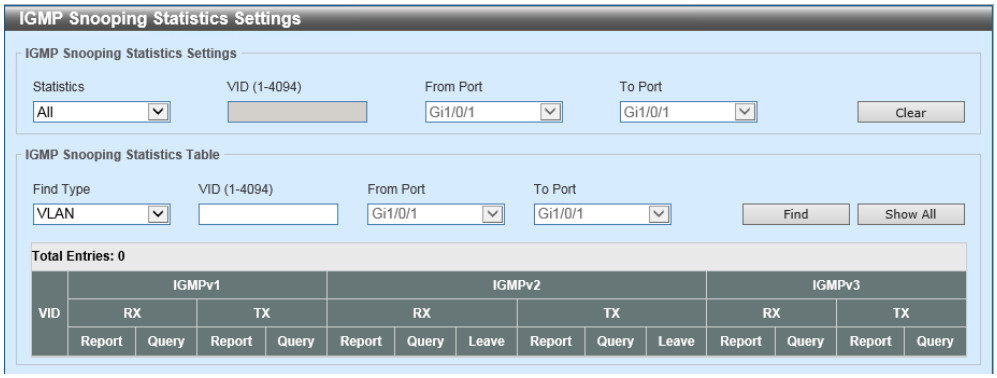


Figure 5-51 IGMP Snooping Statistics Settings

The following parameters can be configured in the **IGMP Snooping Statistics Settings** section:

Parameter	Description
Statistics	Select the interface here. Options to choose from are **All**, **VLAN**, and **Port**.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094. This is available when **VLAN** is selected in the **Statistics** drop-down list.
From Port - To Port	Select the port(s) that will be used here. This is available when **Port** is selected in the **Statistics** drop-down list.

Click the **Clear** button to clear the statistics information based on the criteria specified.

The following parameters can be configured in the **IGMP Snooping Statistics Table** section:

Parameter	Description
Find Type	Select the interface type. Options to choose from are **VLAN**, and **Port**.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094. This is available when **VLAN** is selected in the **Find Type** drop-down list.
From Port - To Port	Select the port(s) that will be used here. This is available when **Port** is selected in the **Find Type** drop-down list.

Click the **Find** button to find and display entries in the table based on the search criteria specified.
Click the **Show All** button to find and display all available entries.

5.7.2 MLD Snooping

5.7.2.1 MLD Snooping Settings

This window is used to configure and display the Multicast Listener Discovery (MLD) snooping settings.

Click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Settings** to view the following window:

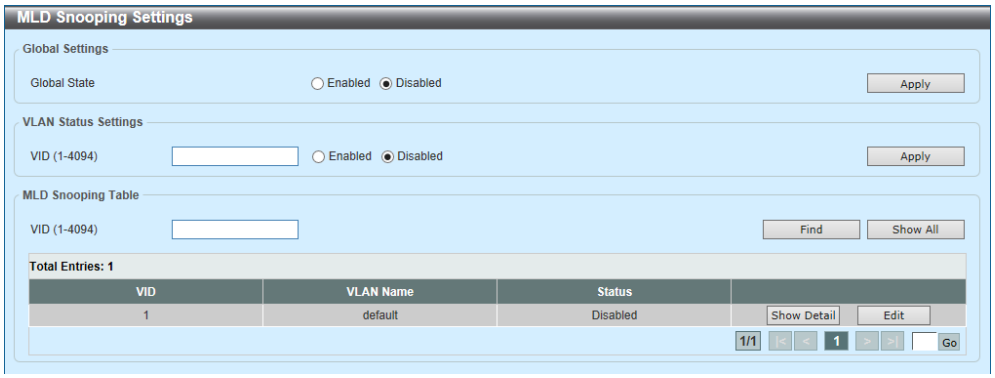


Figure 5-52 MLD Snooping Settings

The following parameters can be configured in the **Global Settings** section:

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 following parameters can be configured in the **VLAN Status Settings** section:

Parameter	Description
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

Click the **Apply** button to add a new entry based on the information specified.

The following parameters can be configured in the **MLD Snooping Table** section:

Parameter	Description
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

Click the **Find** button to find and display entries in the table based on the search criteria specified.
Click the **Show All** button to find and display all available entries.
Click the **Show Detail** button to display detailed information related to the entry.
Click the **Edit** button to edit the settings of the entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **Show Detail** button to view the following window:

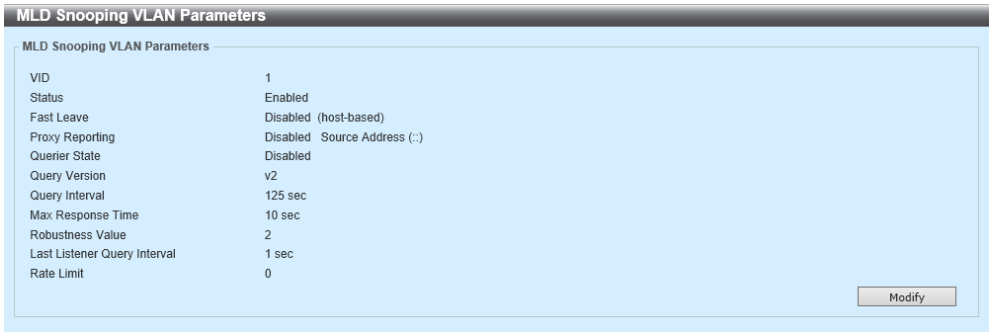


Figure 5-53 MLD Snooping Settings (Show Detail)

Click the **Modify** button to edit the settings.

Click the **Edit** or **Modify** button to view the following window:

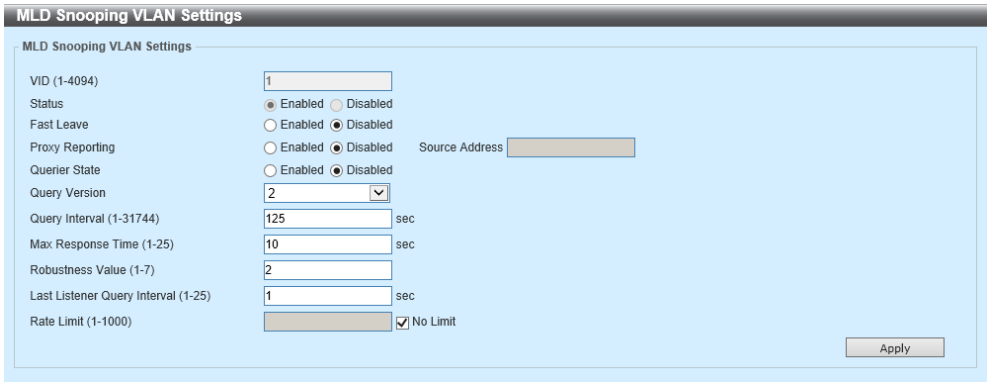


Figure 5-54 MLD Snooping Settings (Edit, Modify)

The following parameters can be configured in the **IGMP Snooping VLAN Settings** section:

Parameter	Description
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 leave message.
Proxy Reporting	Select this option to enable or disable the proxy-reporting function.
Source Address	Enter the source IP of proxy reporting. This is available when **Enabled** is selected in **Proxy Reporting**.
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.
Rate Limit	Enter the rate limit value here. The range is from 1 to 1000. Tick the **No Limit** option to apply no rate limit on this profile.

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

5.7.2.2 MLD Snooping Groups Settings

This window is used to configure and display the MLD snooping group settings.

Click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Groups Settings** to view the following window:

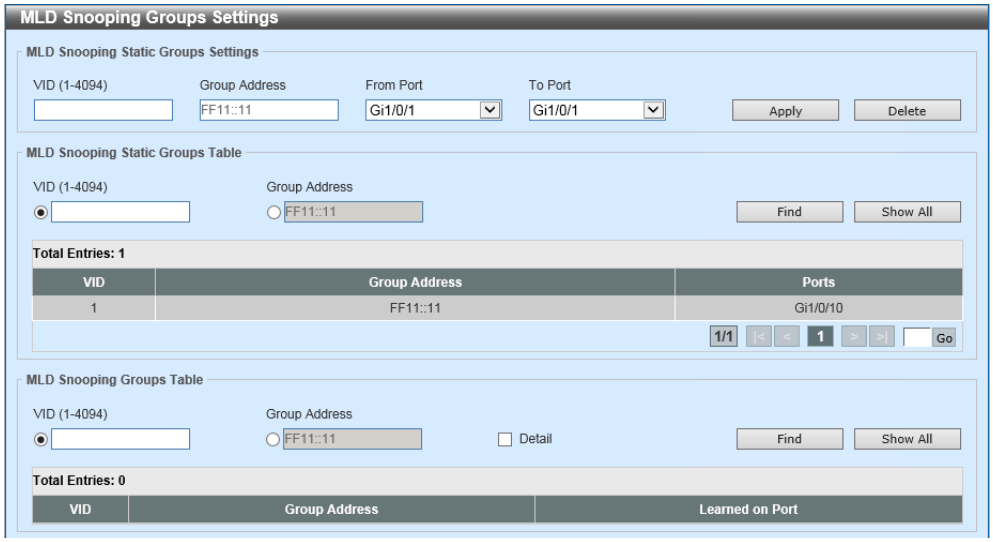


Figure 5-55 MLD Snooping Groups Settings

The following parameters can be configured in the **MLD Snooping Static Groups Settings** section:

Parameter	Description
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.
Group Address	Enter the IPv6 multicast group address here.
From Port - To Port	Select the port(s) that will be used here.

Click the **Apply** button to add a new entry based on the information specified.
Click the **Delete** button to delete an entry based on the information specified.

The following parameters can be configured in the **MLD Snooping Static Groups Table** section:

Parameter	Description
VID	Select and enter the VLAN ID that will be used here. The range is from 1 to 4094.
Group Address	Click the radio button and enter an IPv6 multicast group address.

Click the **Find** button to find and display entries in the table based on the search criteria specified.
Click the **Show All** button to find and display all available entries.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

The following parameters can be configured in the **MLD Snooping Groups Table** section:

Parameter	Description
VID	Select and enter the VLAN ID that will be used here. The range is from 1 to 4094.
Group Address	Click the radio button and enter an IPv6 multicast group address.
Detail	Select this option to display the MLD group detail information.

Click the **Find** button to find and display entries in the table based on the search criteria specified.
Click the **Show All** button to find and display all available entries.

5.7.2.3 MLD Snooping Filter Settings

This window is used to configure and display the MLD snooping filter settings.

Click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Filter Settings** to view the following window:

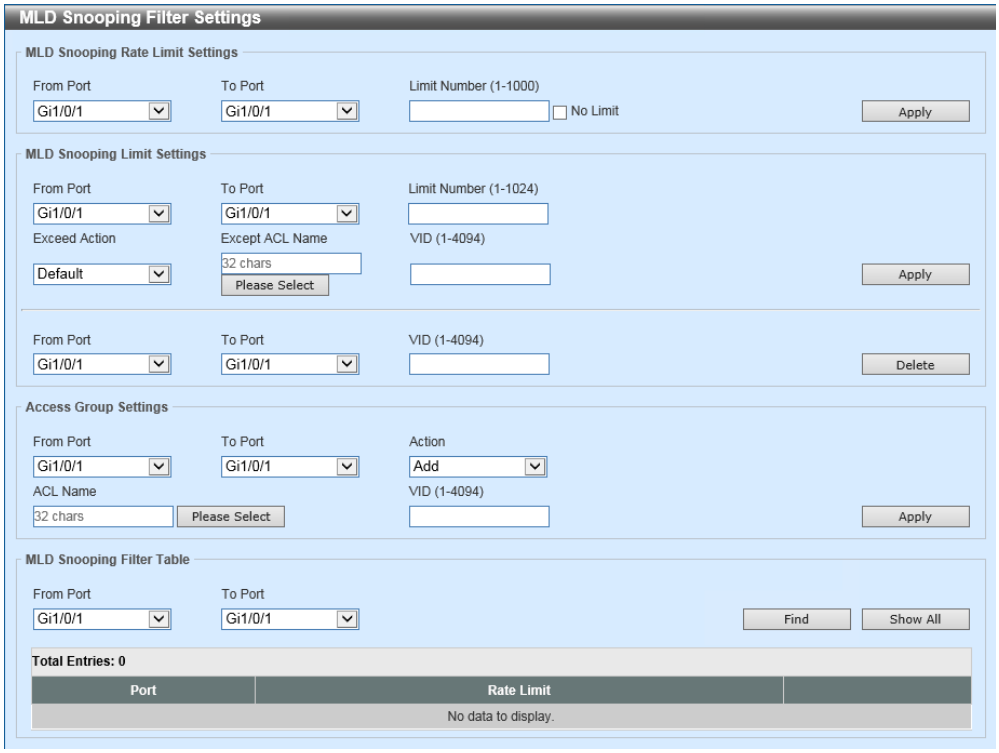


Figure 5-56 MLD Snooping Filter Settings

The following parameters can be configured in the **MLD Snooping Rate Limit Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here. This is only available if the **Port** option was selected as the action below.
Limit Number	Enter the limit number here. This number is used to configure the rate of MLD control packets that the Switch can process on a specific interface. The range is from 1 to 1000 packets per second. Select the **No Limit** option to remove the limitation.

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

The following parameters can be configured in the **MLD Snooping Limit Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Limit Number	Enter the limit number here. This is used to set the limitation on the number of MLD cache entries that can be created. The range is from 1 to 2048.
Exceed Action	Select the exceed action here. This parameter specifies the action for handling newly learned groups when the limitation is exceeded. Options to choose from are: • **Default** - Specifies that the default action will be taken. • **Drop** - Specifies that the new group will be dropped. • **Replace** - Specifies that the new group will replace the oldest group.
Except ACL Name	Enter the standard IP access list name here. The group (*,G), or channel (S,G) permitted by the access list will be excluded from the limit. To permit a channel (S,G), specify S in the source address field and G in the destination address field of the access list entry. To permit a group (*,G), specify “any” in the source address field and G in the destination address field of the access list entry. This name can be up to 32 characters long. Alternatively, click the **Please Select** button to find and select any of the exiting access lists configured on this Switch to be used in this configuration.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

Click the **Apply** button to add a new entry based on the information specified.
Click the **Delete** button to delete an entry based on the information specified.

The following parameters can be configured in the **Access Group Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Action	Select **Add** to add a new entry based in the information entered. Select **Delete** to delete an entry based in the information entered.

Parameter	Description
ACL Name	Enter the standard IP access list name here. This is used to permit users to join a group (*, G), specify "any" in source address field and G in destination address field of the access list entry. This name can be up to 32 characters long. Alternatively, click the **Please Select** button to find and select any of the exiting access lists configured on this Switch to be used in this configuration.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

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

The following parameters can be configured in the **MLD Snooping Filter Table** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.

Click the **Find** button to find and display entries in the table based on the search criteria specified.
Click the **Show All** button to find and display all available entries.
Click the **Show Detail** button to display detailed information related to the entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **Show Detail** button to view the following window:

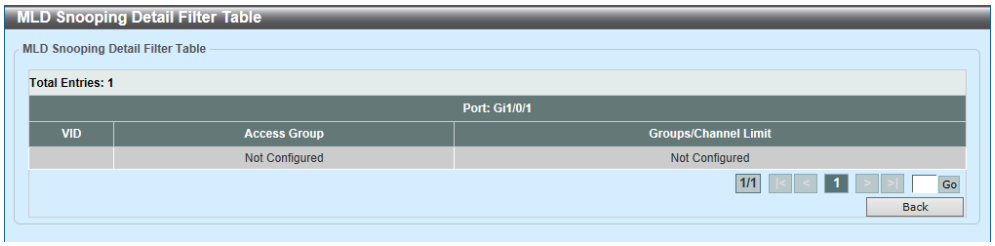


Figure 5-57 MLD Snooping Filter Settings (Show Detail)

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.
Click the **Back** button to return to the previous window.

5.7.2.4 MLD Snooping Multicast Router Information

This window is used to configure and display the MLD snooping multicast router settings.

Click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Multicast Router Information** to view the following window:

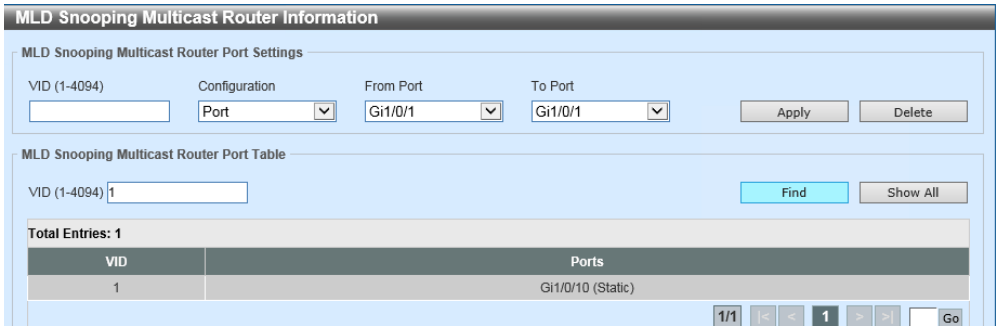


Figure 5-58 MLD Snooping Multicast Router Information

The following parameters can be configured in the **MLD Snooping Multicast Router Port Settings** section:

Parameter	Description
VID	Enter the VLAN ID that will be 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 as being connected to multicast-enabled routers. • **Forbidden Port** - Select to have the configured ports as being not connected to multicast-enabled routers.
From Port - To Port	Select the port(s) that will be used here.

Click the **Apply** button to add a new entry based on the information specified.
Click the **Delete** button to delete an entry based on the information specified.

The following parameters can be configured in the **MLD Snooping Multicast Router Port Table** section:

Parameter	Description
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

Click the **Find** button to find and display entries in the table based on the search criteria specified.
Click the **Show All** button to find and display all available entries.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

5.7.2.5 MLD Snooping Statistics Settings

This window is used to display and clear MLD snooping statistics.

Click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Statistics Settings** to view the following window:

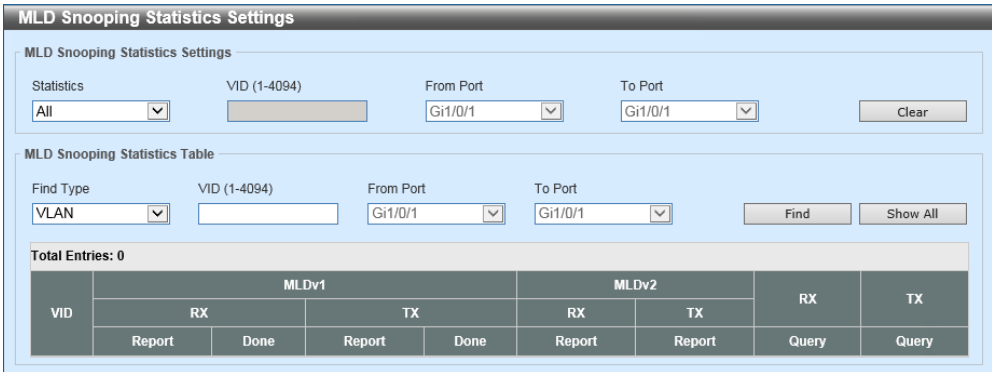


Figure 5-59 MLD Snooping Statistics Settings

The following parameters can be configured in the **MLD Snooping Statistics Settings** section:

Parameter	Description
Statistics	Select the interface here. Options to choose from are **All**, **VLAN**, and **Port**.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094. This is available when **VLAN** is selected in the **Statistics** drop-down list.
From Port - To Port	Select the port(s) that will be used here. This is available when **Port** is selected in the **Statistics** drop-down list.

Click the **Clear** button to clear the statistics information based on the criteria specified.

The following parameters can be configured in the **MLD Snooping Statistics Table** section:

Parameter	Description
Find Type	Select the interface type. Options to choose from are **VLAN** and **Port**.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094. This is available when **VLAN** is selected in the **Find Type** drop-down list.
From Port - To Port	Select the port(s) that will be used here. This is available when **Port** is selected in the **Find Type** drop-down list.

Click the **Find** button to find and display entries in the table based on the search criteria specified.
Click the **Show All** button to find and display all available entries.

5.7.3 Multicast Filtering Mode

This window is used to configure and display the multicast filtering mode.

Click **L2 Features > L2 Multicast Control > Multicast Filtering Mode** to view the following window:

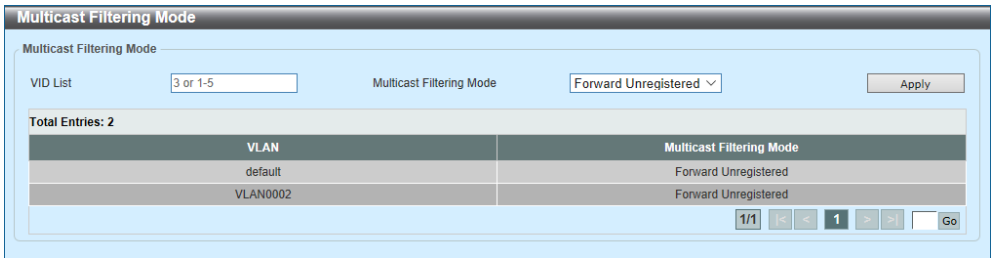


Figure 5-60 Multicast Filtering Mode

The following parameters can be configured in the **Multicast Filtering Mode** section:

Parameter	Description
VID List	Enter the VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.
Multicast Filter Mode	Select the multicast filter mode here. Options to choose from are: • **Forward Unregistered** - 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** - All multicast packets will be flooded based on the VLAN domain. • **Filter Unregistered** - Registered packets will be forwarded based on the forwarding table and all unregistered multicast packets will be filtered.

Click the **Apply** button to add a new entry based on the information specified.

5.8 LLDP (Link Layer Discovery Protocol)

5.8.1 LLDP Global Settings

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

Click **L2 Features > LLDP > LLDP Global Settings** to view the following window:

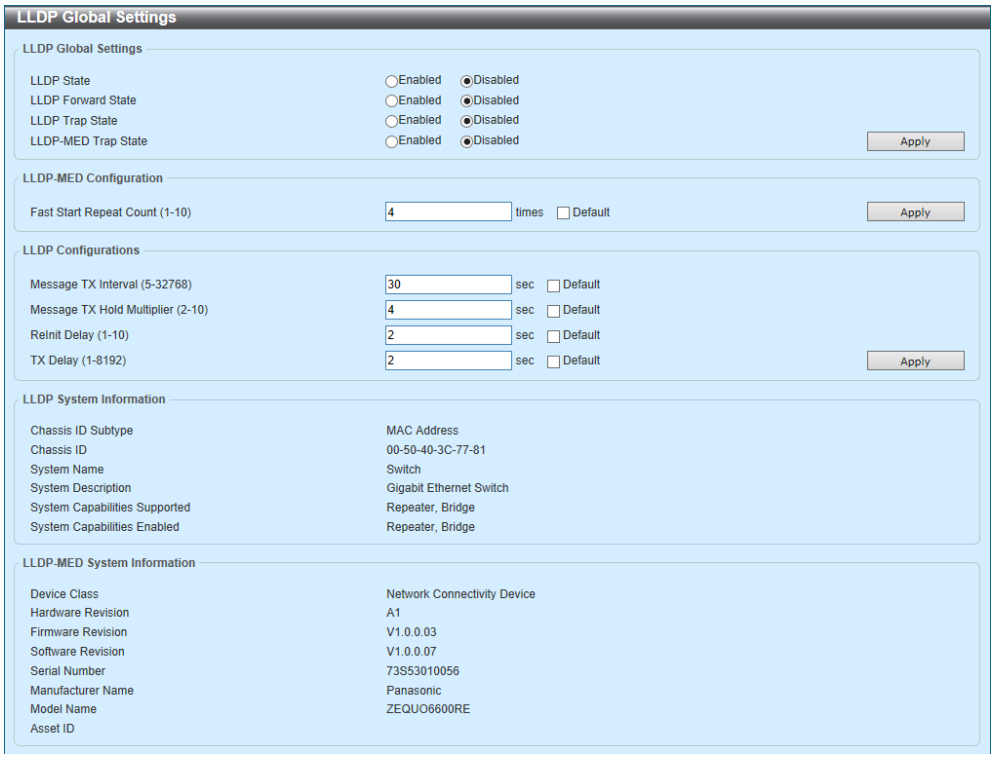


Figure 5-61 LLDP Global Settings

The following parameters can be configured in the **LLDP Global Settings** section:

Parameter	Description
LLDP State	Select this option to enable or disable the LLDP feature
LLDP Forward State	Select this option to enable or disable LLDP forward state. When the **LLDP State** is disabled and **LLDP Forward State** is enabled, the received LLDP Data Unit (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 Media Endpoint Discovery (LLDP-MED) trap state.

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

The following parameters can be configured in the **LLDP-MED Configuration** section:

Parameter	Description
Fast Start Repeat Count	Enter the LLDP-MED fast start repeat count value. The range is from 1 to 10. Select the **Default** option to use the default value.

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

The following parameters can be configured in the **LLDP Configurations** section:

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. Select the **Default** option to use the default value.
Message TX Hold Multiplier	Enter the multiplier on the LLDPDUs transmission interval that used to calculate the Time-To-Live (TTL) value of an LLDPDU. The range is from 2 to 10. Select the **Default** option to use the default value.
ReInit Delay	Enter the delay value for LLDP initialization on an interface. The range is from 1 to 10 seconds. Select the **Default** option to use the default value.
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. Select the **Default** option to use the default value.

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

5.8.2 LLDP Port Settings

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

Click **L2 Features > LLDP > LLDP Port Settings** to view the following window:

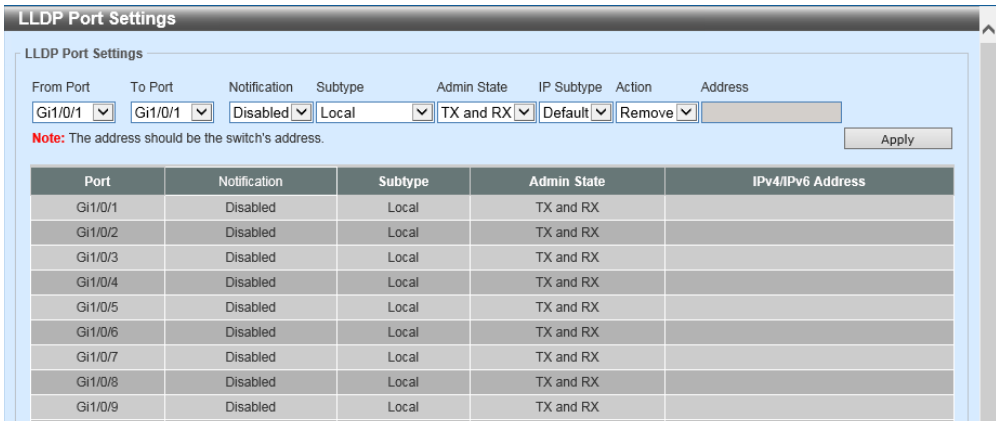


Figure 5-62 LLDP Port Settings

The following parameters can be configured in the **LLDP Port Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Notification	Select to enable or disable the notification feature here.
Subtype	Select the subtype of LLDP Type-Length-Value (TLV) here. 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. • **Disabled** - The local LLDP agent can neither transmit nor receive LLDP frames. The default option is **TX** and **RX**.
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.

5.8.3 LLDP Management Address List

This window is used to display the LLDP management address list and information.

Click **L2 Features > LLDP > LLDP Management Address List** to view the following window:

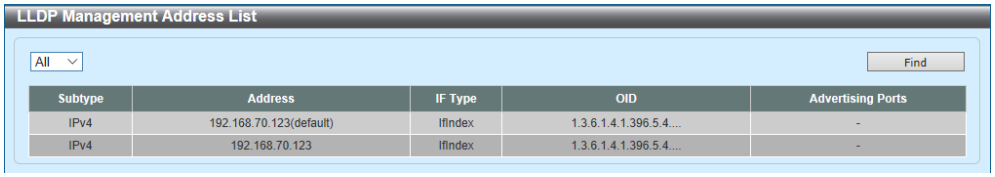


Figure 5-63 LLDP Management Address List

The following parameters can be configured:

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 find and display entries in the table based on the search criteria specified.

5.8.4 LLDP Basic TLVs Settings

This window is used to configure and display the basic LLDP TLV settings.

Click **L2 Features > LLDP > LLDP Basic TLVs Settings** to view the following window:

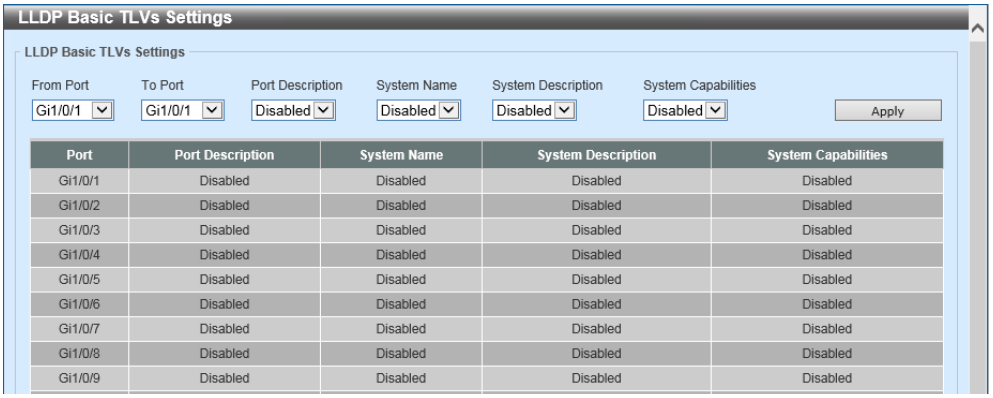


Figure 5-64 LLDP Basic TLVs Settings

The following parameters can be configured in the **LLDP Basic TLVs Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Port Description	Select to enable or disable the sending of the port description TLV.
System Name	Select to enable or disable the sending of the system name TLV.
System Description	Select to enable or disable the sending of the system description TLV.
System Capabilities	Select to enable or disable the sending of the system capabilities TLV.

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

5.8.5 LLDP Dot1 TLVs Settings

This window is used to configure and display the IEEE 802.1 LLDP TLV settings.

Click **L2 Features > LLDP > LLDP Dot1 TLVs Settings** to view the following window:

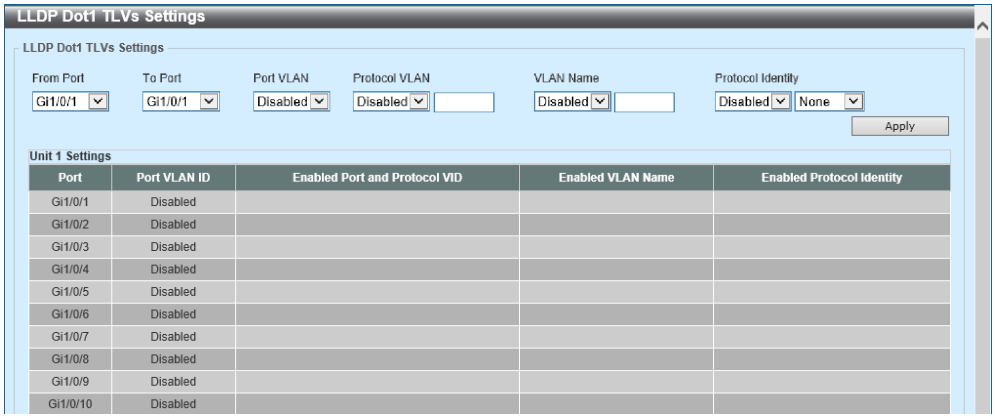


Figure 5-65 LLDP Dot1 TLVs Settings

The following parameters can be configured in the **LLDP Dot1 TLVs Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Port VLAN	Select to enable or disable the sending of the port VLAN ID TLV.
Protocol VLAN	Select to enable or disable the sending of the port and protocol VLAN ID (PPVID) TLV. Enter the ID of the protocol VLAN in the space provided.
VLAN Name	Select to enable or disable the sending of the VLAN name TLV. Enter the ID of the VLAN in the space provided.
Protocol Identity	Select to enable or disable the sending of the protocol identity TLV. Options for protocol name to choose from are **None**, **EAPOL**, **LACP**, **GVRP**, **STP**, and **All**.

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

5.8.6 LLDP Dot3 TLVs Settings

This window is used to configure and display the IEEE 802.3 LLDP TLV settings.

Click **L2 Features > LLDP > LLDP Dot3 TLVs Settings** to view the following window:

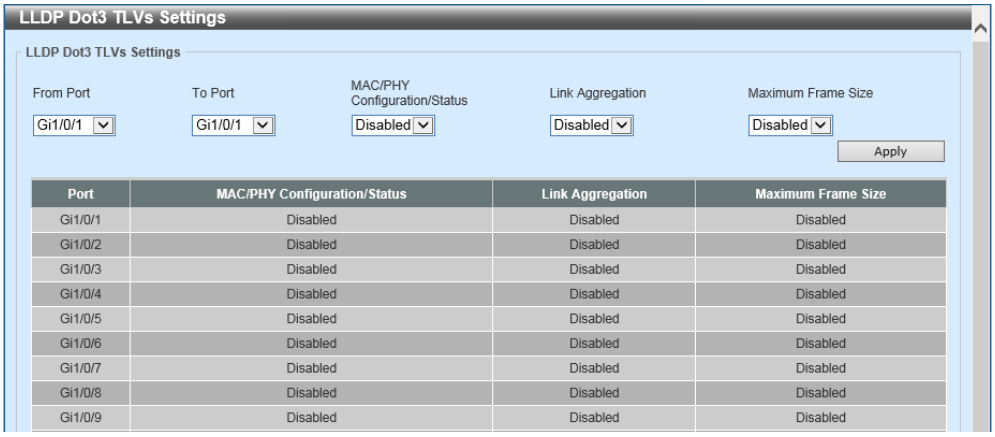


Figure 5-66 LLDP Dot3 TLVs Settings

The following parameters can be configured in the **LLDP Dot3 TLVs Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
MAC/PHY Configuration/Status	Select to enable or disable the sending of the MAC/PHY configuration/status TLV.
Link Aggregation	Select to enable or disable the sending of the link aggregation TLV.
Maximum Frame Size	Select to enable or disable the sending of the maximum frame size TLV.

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

5.8.7 LLDP-MED Port Settings

This window is used to configure and display the LLDP-MED port settings.

Click **L2 Features > LLDP > LLDP-MED Port Settings** to view the following window:

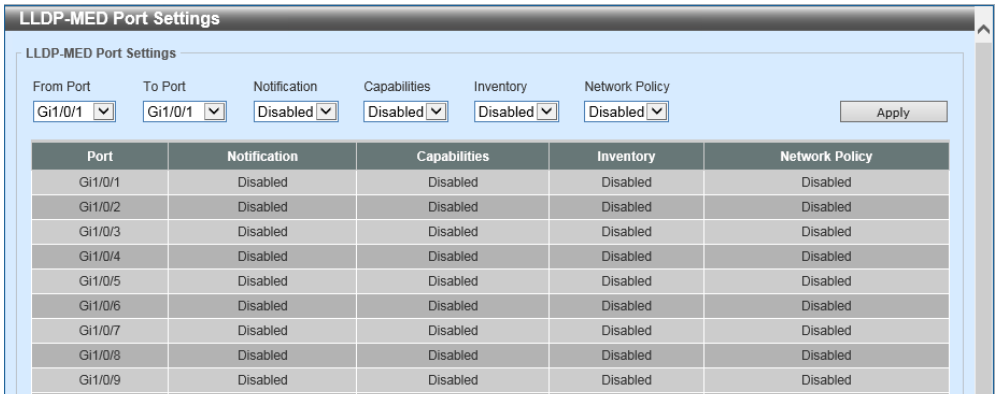


Figure 5-67 LLDP-MED Port Settings

The following parameters can be configured in the **LLDP-MED Port Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Notification	Select to enable or disable the sending of the LLDP-MED notification TLV.
Capabilities	Select to enable or disable the sending of the LLDP-MED capabilities TLV.
Inventory	Select to enable or disable the sending of the LLDP-MED inventory management TLV.
Network Policy	Select to enable or disable the sending of the LLDP-MED network policy TLV.

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

5.8.8 LLDP Statistics Information

This window is used to display and clear the LLDP statistics.

Click **L2 Features > LLDP > LLDP Statistics Information** to view the following window:

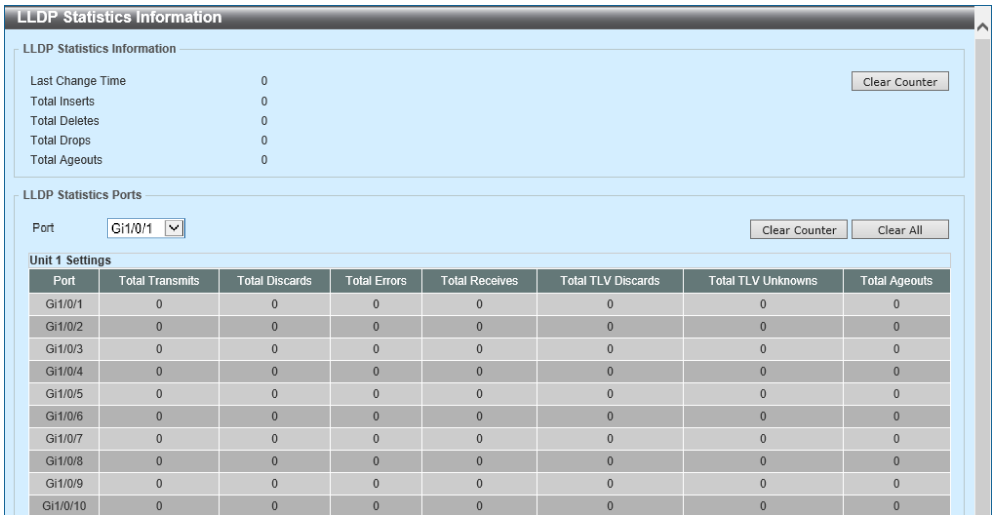


Figure 5-68 LLDP Statistics Information

The following parameters can be configured in the **LLDP Statistics Ports** section:

Parameter	Description
Port	Select the port that will be used here.

Click the **Clear** button to clear the counter information.
Click the **Clear All** button to clear the counter information for all the ports.

5.8.9 LLDP Local Port Information

This window is used to display local LLDP port information.

Click **L2 Features > LLDP > LLDP Local Port Information** to view the following window:

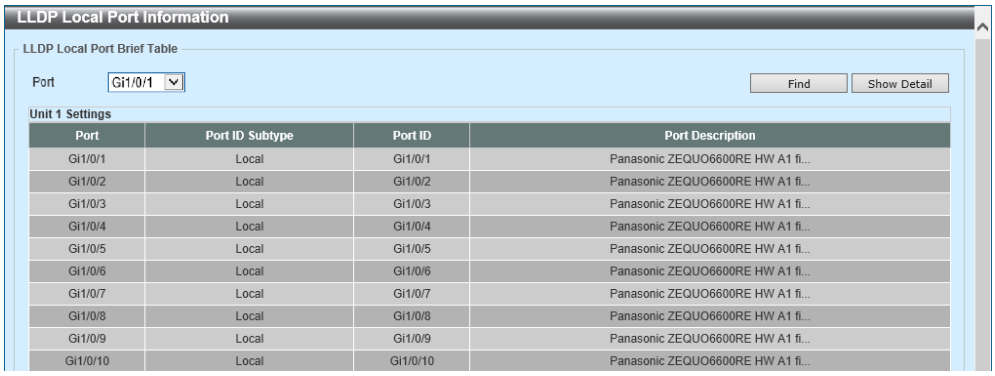


Figure 5-69 LLDP Local Port Information

The following parameters can be configured in the **LLDP Local Port Brief Table** section:

Parameter	Description
Port	Select the port that will be used here.

Click the **Find** button to find and LLDP local port information associated with the specified port
Click the **Show Detail** button to display detailed LLDP local port information associated with the specified port

Click the **Show Detail** button to view the following window:

Figure 5-70 LLDP Local Port Information (Show Detail)

Click each individual link to display detailed information related to the specified feature in the table.
Click the **Back** button to return to the previous window.

5.8.10 LLDP Neighbor Port Information

This window is used to display neighboring LLDP port information.

Click **L2 Features > LLDP > LLDP Neighbor Port Information** to view the following window:

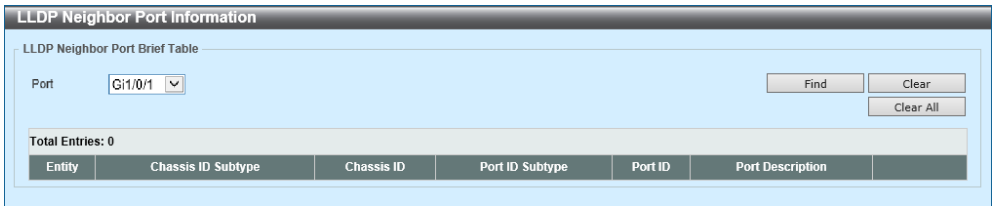


Figure 5-71 LLDP Neighbor Port Information

The following parameters can be configured in the **LLDP Neighbor Port Brief Table** section:

Parameter	Description
Port	Select the port that will be used here.

Click the **Find** button to find and LLDP neighbor port information associated with the specified port
Click the **Clear** button to clear LLDP neighbor port information associated with the specified port.
Click the **Clear All** button to clear all LLDP neighbor port information.

5.9 UDLD (Unidirectional Link Detection)

Use the following window, and then implement the UDLD settings to display the settings and condition.

Choose **L2 Features** > **UDLD** to display the following window.

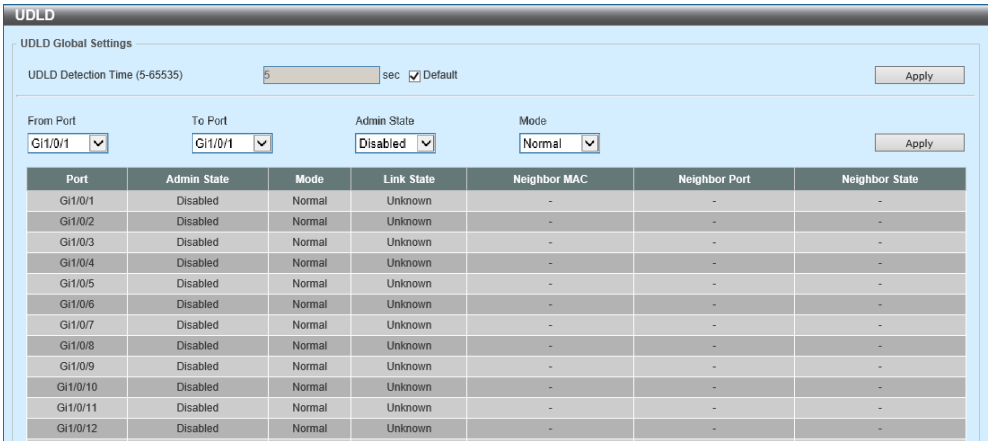


図 5-72 UDLD

In the **UDLD Global Settings** section, you can configure the following parameters.

Parameter	Description
UDLD Detection Time	Configure the unidirectional connection detection time (seconds). The range of the configuration is from 5 to 65,535 seconds. The factory default settings is five (5) seconds.
From Port - To Port	Choose the port you use.
Administration State	Enable or disable the UDLD function of the port specified. The factory default settings is Enabled.
Mode	Choose the UDLD mode to be used on the port specified. The factory default settings is Normal. The options (or values) available are as follows: • [Normal] - If you detect the unidirectional connection, relay the link of the corresponding port to record an event on the system log. • [Shutdown] - If you detect the unidirectional connection, execute to shutdown the corresponding ports to record an event on the system log.

Click **Apply** to reflect the change.

NOTE You can use this function among our products.

5.10 RRP (Ring Redundant Protocol)

This window is used to configure and display the RRP settings.

Click **L2 Features > RRP** to view the following window:

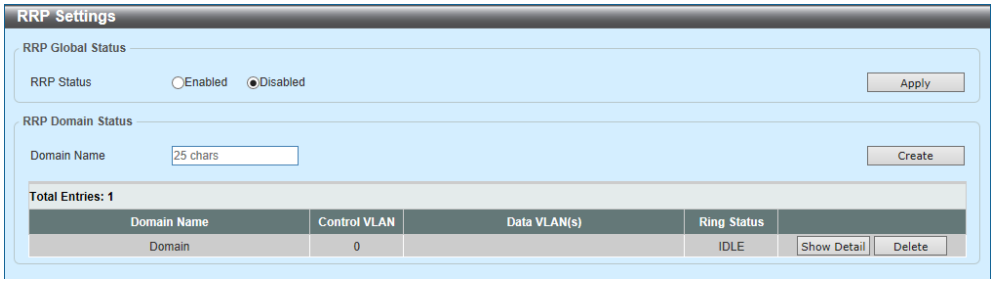


Figure 5-73 RRP

The following parameters can be configured in the **RRP Global Status** section:

Parameter	Description
RRP Status	Select to enable or disable the RRP feature here.

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

The following parameters can be configured in the **RRP Domain Status** section:

Parameter	Description
Domain Name	Enter the RRP domain name here. This can be up to 25 characters long. The domain represents the physical ring.

Click the **Create** button to create a new RRP domain.
Click the **Show Detail** button to display detailed information related to the entry.
Click the **Delete** button to delete the entry.

Click the **Show Detail** button to view the following window:

Figure 5-74 RRP (Show Detail)

Click the **Edit** button to edit the settings.
Click the **Back** button to return to the previous window.

Click the **Edit** button to view the following window:

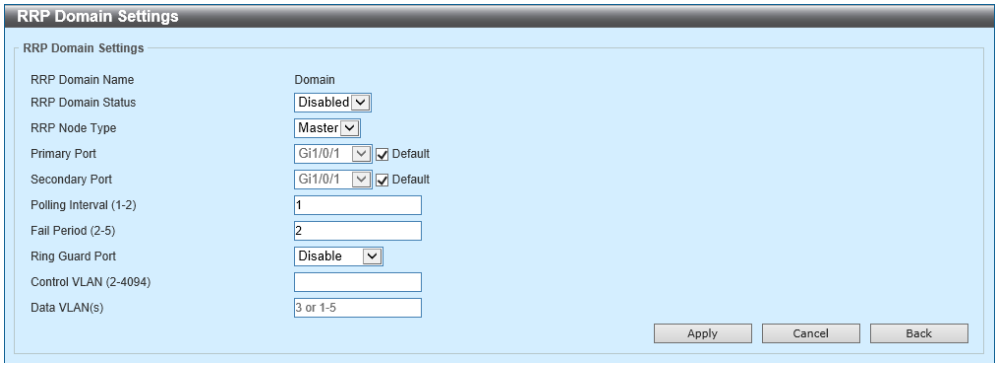


Figure 5-75 RRP (Edit)

The following parameters can be configured in the **RRP Domain Settings** section:

Parameter	Description
RRP Domain Status	Select the enable or disable the RRP domain here.
RRP Node Type	Select the RRP node type here. Options to choose from are: • **Master** - Specifies the node as the master node in the domain. Only one master node can be specified in an RRP domain. Responsibilities of the master node include ring polling and ring restoration. • **Transit** - Specifies the node as a transit node in the domain. Many transit nodes can be specified in an RRP domain. Responsibilities of a transit node include link down alerts.

Parameter	Description
Primary Port	Select the primary switch unit and port here. This port will be the first port in the RRP domain. Select the **Default** option to clear current settings.
Secondary Port	Select the secondary switch unit and port here. This port will be the second port in the RRP domain. Select the **Default** option to clear current settings.
Polling Interval	Enter the hello-packet polling interval here. The range is from 1 to 2 seconds. The polling interval should be shorter than the fail period.
Fail Period	Enter the fail period here. The range is from 2 to 5 seconds. The fail period should be longer than the polling interval.
Ring Guard Port	Select to status of the guard port in the RRP ring here. Options to choose from are: • **Primary** - Specifies use the primary port as the ring guard-enabled port. • **Secondary** - Specifies the secondary port as the ring guard-enabled port. • **Both** - Specifies both the primary and secondary ports as ring guard-enabled ports. • **Disable** - Specifies to disable this feature.
Control VLAN	Enter the ID of the control VLAN here. The range is from 2 to 4094.
Data VLAN	Enter the ID(s) of the data VLAN(s) here. The range is from 1 to 4094.

Click the **Apply** button to accept the changes made.
Click the **Cancel** button to discard the changes made.
Click the **Back** button to return to the previous window.

6 L3 Features

6.1 ARP (Address Resolution Protocol)

6.1.1 ARP Control Settings

This window is used to enable or disable the ARP refresh before timeout feature.

Click **L3 Features > ARP > ARP Control Settings** to view the following window:

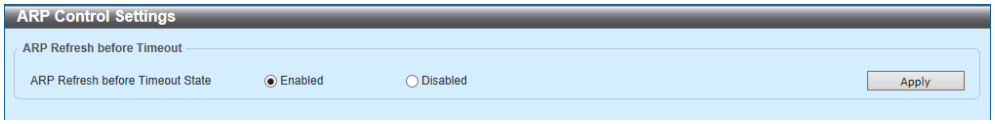


Figure 6-1 ARP Control Settings

The following parameters can be configured in the **ARP Refresh before Timeout** section:

Parameter	Description
ARP Refresh before Timeout State	Select to enable or disable the ARP refresh before timeout feature here.

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

6.1.2 ARP Aging Time

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

Click **L3 Features > ARP > ARP Aging Time** to view the following window:

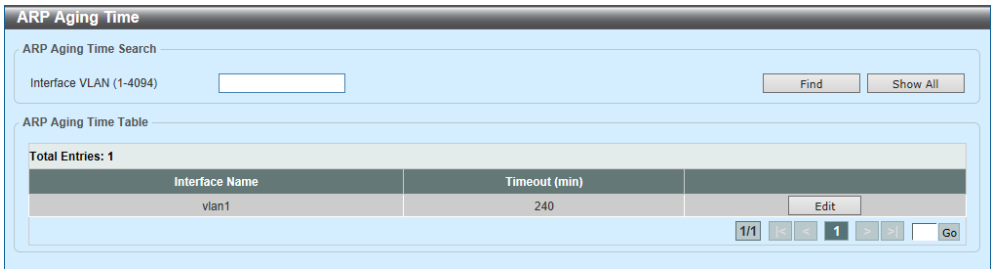


Figure 6-2 ARP Aging Time

The following parameters can be configured in the **ARP Aging Time Search** section:

Parameter	Description
Interface VLAN	Enter the VLAN ID here. The range is from 1 to 4094.
Timeout	After clicking the **Edit** button, enter the timeout value here. The range is from 0 to 65535 minutes.

Click the **Find** button to find and display entries based on the search criteria specified.
Click the **Show All** button to find and display all available entries.
Click the **Edit** button to edit the settings of the entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

6.1.3 Static ARP

This window is used to configure and display the static ARP settings.

Click **L3 Features > ARP > Static ARP** to view the following window:

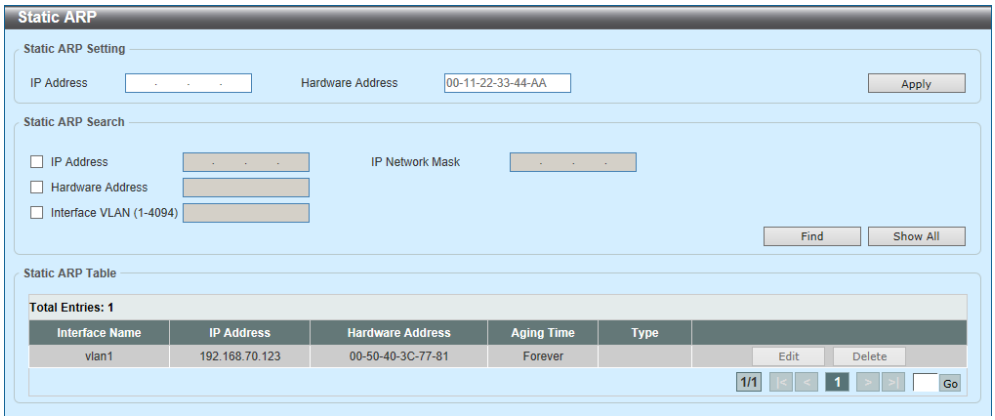


Figure 6-3 Static ARP

The following parameters can be configured in the **Static ARP Setting** section:

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 add a new Static ARP entry.

The following parameters can be configured in the **Static ARP Search** section:

Parameter	Description
IP Address	Select and enter the IP address of the entry here.
IP Network Mask	Select and enter the subnet mask for the IP address here.
Hardware Address	Select and enter the MAC address of the entry here.
Interface VLAN	Select and enter the VLAN ID here. The range is from 1 to 4094.

Click the **Find** button to find and display entries based on the search criteria specified.
Click the **Show All** button to find and display all available entries.
Click the **Edit** button to edit the settings of the entry.
Click the **Delete** button to delete the entry.

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

6.1.4 ARP Table

This window is used to display and clear the ARP entries in the table.

Click **L3 Features > ARP > ARP Table** to view the following window:

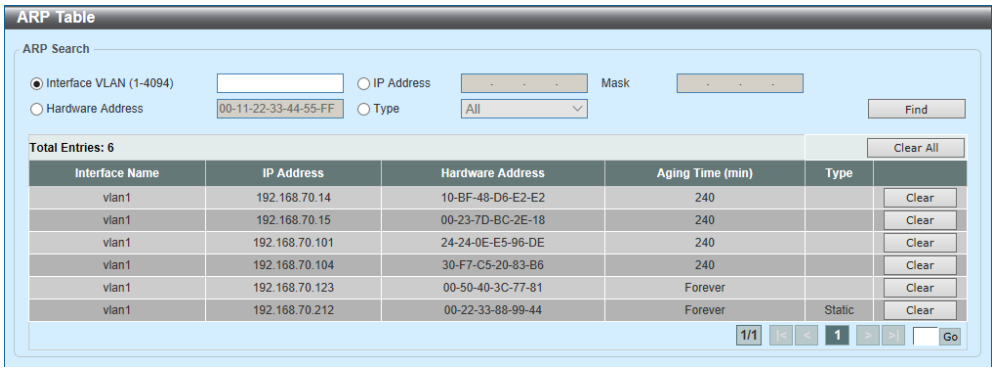


Figure 6-4 ARP Table

The following parameters can be configured in the **ARP Search** section:

Parameter	Description
Interface VLAN	Select and enter the VLAN ID of the interface here. This range is from 1 to 4094.
IP Address	Select and enter the IP address to display here.
Mask	Select and enter the subnet mask 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 find and display entries based on the search criteria specified.
Click the **Clear All** button to remove all the entries from the table.
Click the **Clear** 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.

6.2 Gratuitous ARP

This window is used to configure and display the gratuitous ARP settings. A gratuitous ARP request packet is an ARP request packet where the source and the destination IP address are both set to the IP address of the sending device and the destination MAC address is the broadcast address. A device uses a gratuitous ARP request packet to discover whether the IP address is duplicated by other hosts or to preload or reconfigure the ARP cache entry of hosts connected to the interface.

Click **L3 Features > Gratuitous ARP** to view the following window:

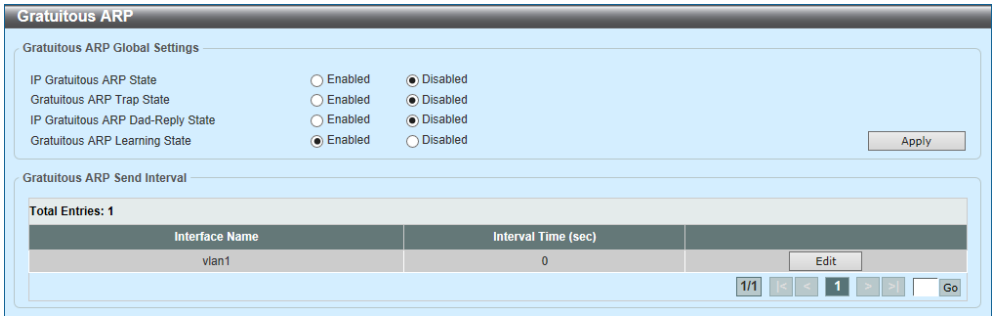


Figure 6-5 Gratuitous ARP

The following parameters can be configured in the **Gratuitous ARP Global Settings** section:

Parameter	Description
IP Gratuitous ARP State	Select to enable or disable the transmission of gratuitous ARP request packets.
Gratuitous ARP Trap State	Select to enable or disable the gratuitous ARP feature trap state here.
IP Gratuitous ARP Dad-Reply State	Select to enable or disable the IP gratuitous ARP Dad-reply state.
Gratuitous ARP Learning State	Select to enable or disable the gratuitous ARP learning state. Normally, the system will only learn ARP entries from ARP reply packets or a normal ARP request packet that asks for the MAC address of the Switch IP address. This option used to enable or disable the learning of ARP entries based on received gratuitous ARP packets. The gratuitous ARP packet is sent by a source IP address and is identical to the IP that the packet is querying.

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

The following parameters can be configured in the **Gratuitous ARP Send Interval** section:

Parameter	Description
Interval Time	After clicking the **Edit** button, enter the gratuitous ARP sending interval time, in seconds, here.

Click the **Edit** button to edit the settings of the entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

6.3 IPv6 Neighbor

This window is used to configure and display the IPv6 neighbor settings.

Click **L3 Features > IPv6 Neighbor** to view the following window:

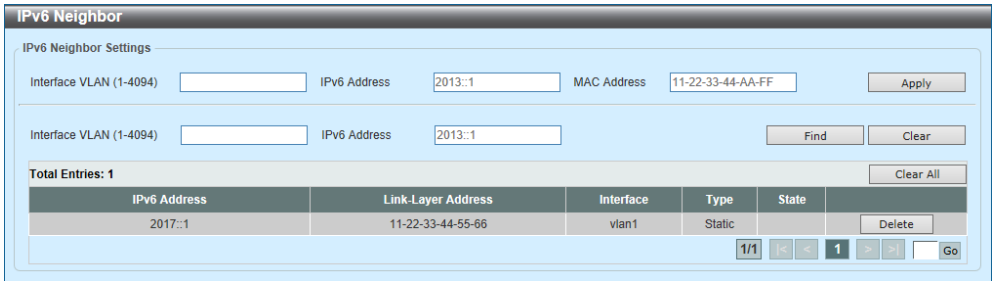


Figure 6-6 IPv6 Neighbor

The following parameters can be configured in the **IPv6 Neighbor Settings** section:

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 add a new entry.
Click the **Find** button to find and display entries based on the search criteria specified.
Click the **Clear** button to clear the information based on the criteria specified.
Click the **Clear All** button to remove all the dynamic entries.
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.

6.4 Interface

6.4.1 IPv4 Interface

This window is used to configure and display the IPv4 interface settings.

Click **L3 Features > Interface > IPv4 Interface** to view the following window:

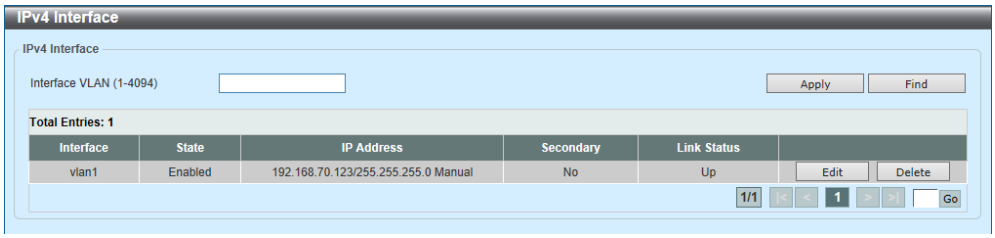


Figure 6-7 IPv4 Interface

The following parameters can be configured in the **IPv4 Interface** section:

Parameter	Description
Interface VLAN	Enter the interface VLAN ID here. The range is from 1 to 4094.

Click the **Apply** button to add a new entry.
Click the **Find** button to find and display entries based on the search criteria specified.
Click the **Edit** button to edit the settings of the specified 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.

Click the **Edit** button to view the following window:

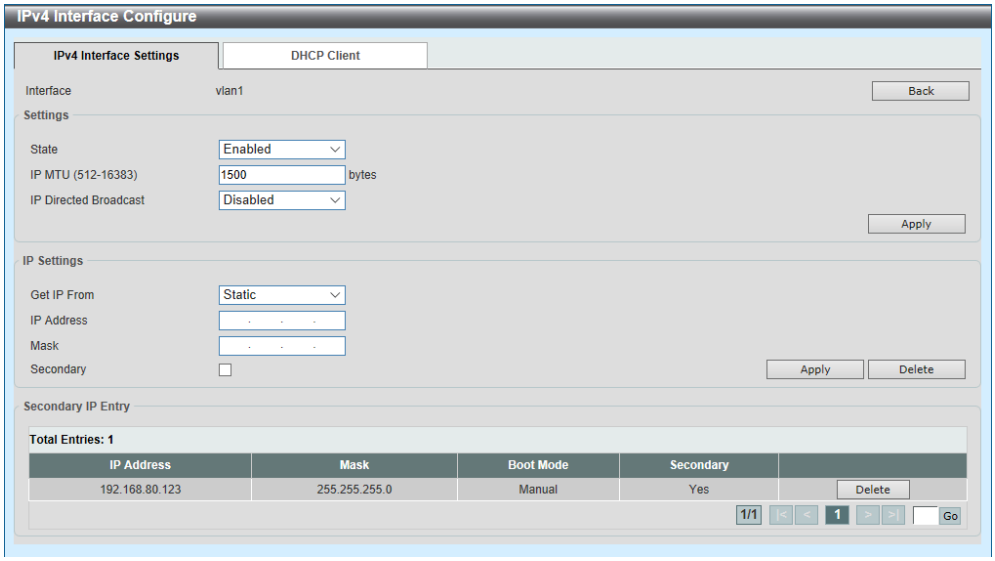


Figure 6-8 IPv4 Interface (Edit, IPv4 Interface Settings)

The following parameters can be configured in the **Settings** section:

Parameter	Description
State	Select to enable or disable the IPv4 interface global state.
IP MTU	Enter the Maximum Transmission Unit (MTU) value here. The range is from 512 to 16383 bytes. By default, this value is 1500 bytes.
IP Directed Broadcast	Select to enable or disable the IP directed broadcast feature here. This parameter is used to enable or disable the conversion of IP directed broadcasts received by the interface to physical broadcasts when the destination network is directly connected to the Switch.

Click the **Back** button to return to the previous window.
Click the **Apply** button to accept the changes made.

The following parameters can be configured in the **IP Settings** section:

Parameter	Description
Get IP From	Select the get IP from option here. Options to choose from are: • **Static** - Enter the IPv4 address settings of this interface manually in the fields provided. • **DHCP** - This interface will obtain IPv4 settings automatically from the DHCP server located on the local network.
IP Address	Enter the IPv4 address for this interface here.

Parameter	Description
Mask	Enter the IPv4 subnet mask for this interface here.
Secondary	Tick this option to use the IPv4 address and mask as the secondary interface configuration.

Click the **Apply** button to add a new 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.

Click the **DHCP Client** tab to view the following window:

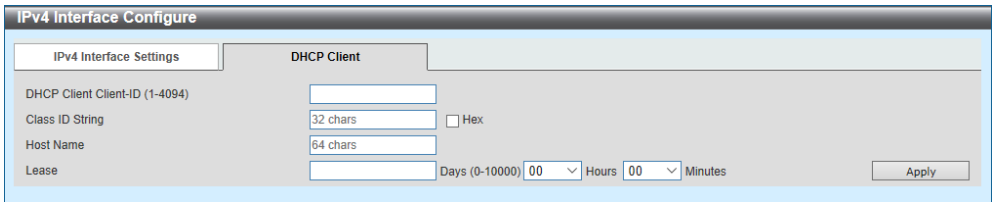


Figure 6-9 IPv4 Interface (Edit, DHCP Client)

The following parameters can be configured in the **DHCP Client** section:

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.
Host Name	Enter the host name here. This string can be up to 64 characters long. This parameter is used to specify the value of the host name option to be sent with the DHCP discover message.
Lease	Enter and optionally select the DHCP client lease time here. In the textbox, 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.

6.4.2 IPv6 Interface

This window is used to configure and display the IPv6 interface settings.

Click **L3 Features > Interface > IPv6 Interface** to view the following window:

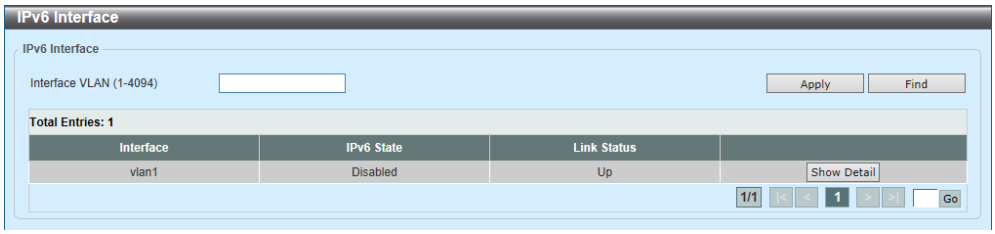


Figure 6-10 IPv6 Interface

The following parameters can be configured in the **IPv6 Interface** section:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID that will be associated with the IPv6 entry.

Click the **Apply** button to add a new entry.
Click the **Find** button to find and display entries based on the search criteria specified.
Click the **Show Detail** button to display detailed information related to the entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **Show Detail** button to view the following window:

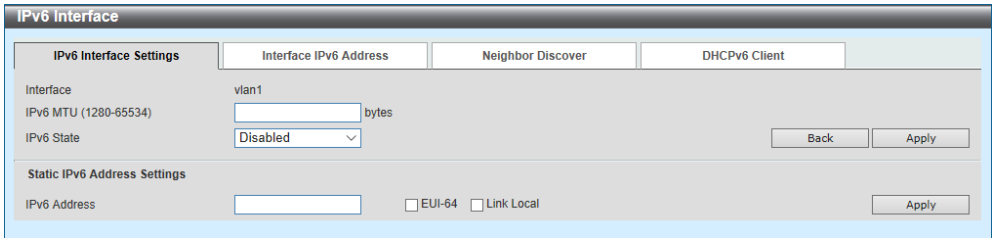


Figure 6-11 IPv6 Interface (Show Detail, IPv6 Interface Settings)

The following parameters can be configured in the **IPv6 Interface Settings** section:

Parameter	Description
IPv6 MTU	Enter the IPv6 MTU value here. The range is from 1280 to 65534 bytes. By default, this value is 1500 bytes. This parameter is used to configure the MTU to be advertised in Router Advertisement (RA) messages.
IPv6 State	Select to enable or disable the IPv6 interface global state here.

Click the **Back** button to return to the previous window.
Click the **Apply** button to accept the changes made.

The following parameters can be configured in the **Static IPv6 Address Settings** section:

Parameter	Description
IPv6 Address	Enter the IPv6 address for this IPv6 interface here. • Select the Extended Unique Identifier 64-bit (**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.

Click the **Interface IPv6 Address** tab to view the following window:

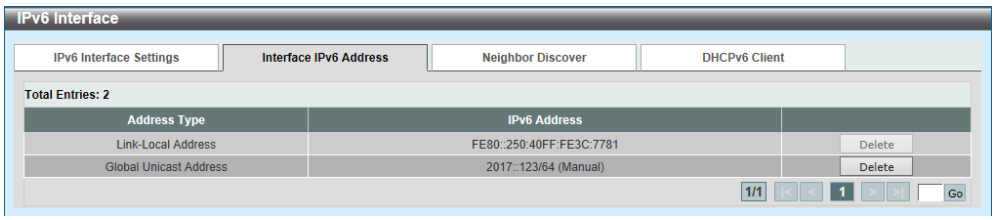


Figure 6-12 IPv6 Interface (Show Detail, Interface IPv6 Address)

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.

Click the **Neighbor Discover** tab to view the following window:

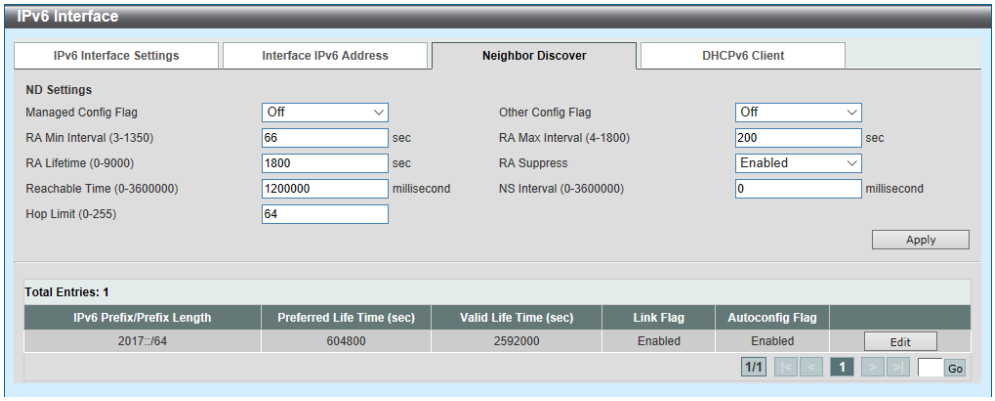


Figure 6-13 IPv6 Interface (Show Detail, Neighbor Discover)

The following parameters can be configured in the **ND Settings** section:

Parameter	Description
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.
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 1200 (unspecified) in the RA message. The Reachable Time is used by the IPv6 node in determining the reachability of the neighbor nodes.
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 use 1 second.

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.

Click the **Apply** button to add a new entry.
Click the **Edit** button to edit the settings of the specified entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **DHCPv6 Client** tab to view the following window:

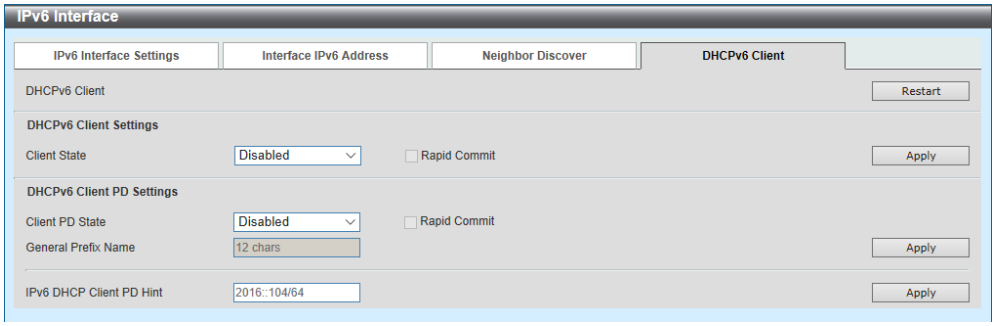


Figure 6-14 IPv6 Interface (Show Detail, DHCPv6 Client)

Click the **Restart** button to restart the DHCPv6 client feature.

The following parameters can be configured in the **DHCPv6 Client Settings** section:

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.

The following parameters can be configured in the **DHCPv6 Client PD Settings** section:

Parameter	Description
Client PD State	Select to enable or disable the DHCPv6 client process that requests a Prefix Delegation (PD) through a specified interface. Select the **Rapid Commit** option to proceed with two-message exchange for prefix delegation. The rapid-commit option will be included in the Solicit message to request a two-message handshake.

Parameter	Description
General Prefix Name	Enter the IPv6 general prefix name here. This name can be up to 12 characters long.
IPv6 DHCP Client PD Hint	Enter the IPv6 prefix to be sent in the message as a hint here.

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

6.5 IPv4 Default Route

Use the following window to implement the settings on an IPv4 default route and display its settings.

Choose **L3 Features > IPv4 Default Route** to display the following window.

Figure 6-15 IPv4 efault Route

In these section of **IPv4 Default Route**, you can configure the following parameter.

Parameter	Overview
Gateway	Enter a gateway address of this route.

Click **Apply** to add a new entry.

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

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

6.6 IPv4 Route Table

Use the following window to display the IPv4 route table and its information.

Choose **L3 Feature > IPv4 Route Table** to display the following window.

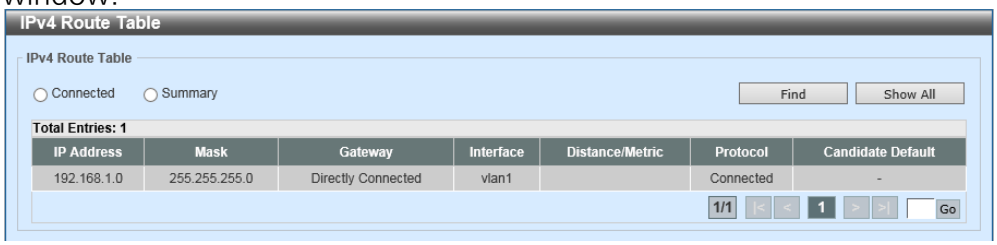


Figure 6-16 IPv4 Route Table

In the section of the **IPv4 Route Table**, you can configure the following parameters.

Parameter	Overview
IP Address	Choose and enter a single IPv4 address.
Network Address	Choose and enter an IPv4 network address. Enter a network prefix on the first (left-side) entry-field. Then enter a network mask on the second entry-field (right side).

Click **Find** to search and display the entries based on the search condition specified.

Click **See All** to search and display all the entries available.

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

Click the **Summary** option to view the following window:

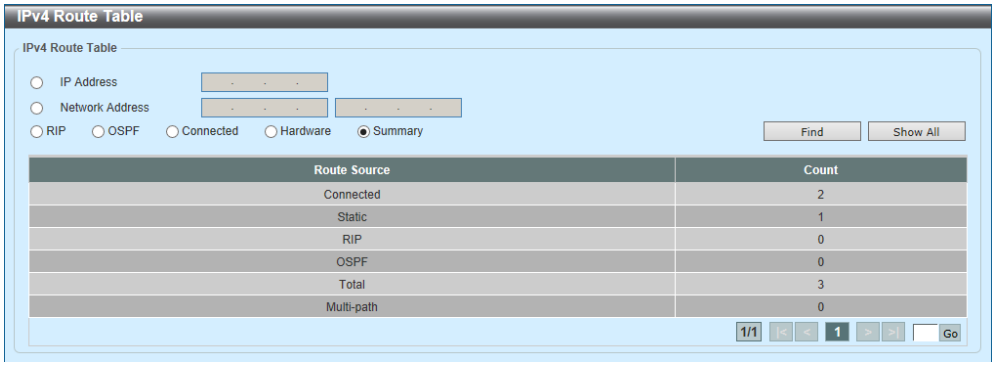


Figure 6-17 IPv4 Route Table (Summary)

6.7 IPv6 Default Route

Use the following window to implement the settings on an IPv6 default route and display its settings.

Choose **L3 Features > IPv6 Default Route** to display the following window.

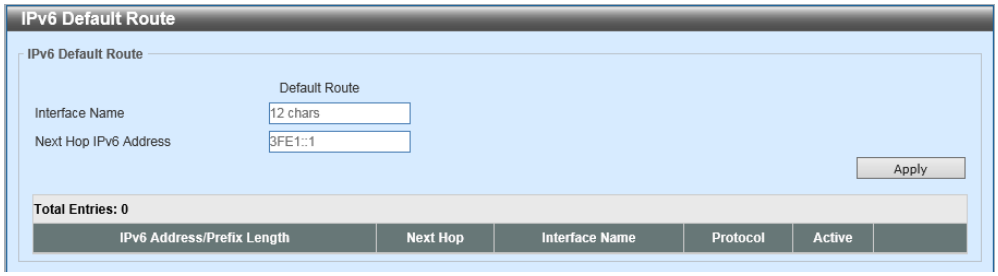


Figure 6-18 IPv6 Default Route

In the section of **IPv6 Default Route**, you can configure the following parameters.

Parameter	Overview
IPv6 Address/ Prefix Length	Enter an IPv6 address and prefix-length for this route. If you set **Default Route** to on, use this route for a default route.
Interface Name	Enter an interface name to be associated with this route.
Next Hop IPv6 Address	Enter an IPv6 address of the next hop.
Distance	Enter the distance for the static route management. The range is from 1 to 254. The lower the value, the better route will be. If not specified, the distance becomes 1 for managing a static-route (by default).

Click **Apply** to add a new entry.

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

If two or more pages exist, enter the page numbers. Then click **Go** to move to a specific page.

6.8 IPv6 Route Table

Use the following window to display the IPv6 route table and its information.

Choose **L3 Features > IPv6 Route Table** to display the following window.

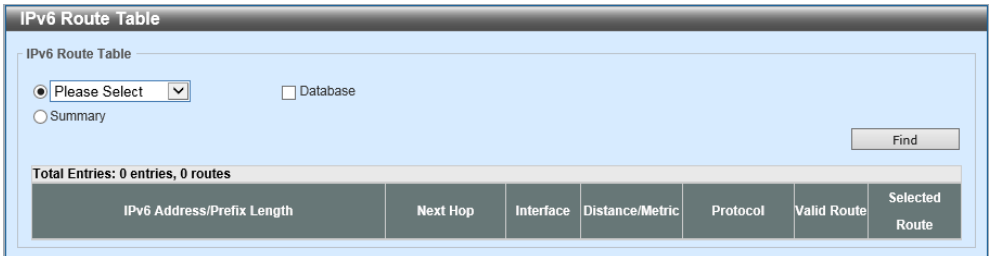


Figure 6-19 IPv6 Route Table

In the section of the **IPv6 Route Table**, you can configure the following parameters.

Parameter	Overview
IPv6 Address	Choose and enter an IPv6 address to be displayed.
IPv6 Address/ Prefix Length	Choose and enter an IPv6 address and prefix-length to be displayed. If you choose **Longer Prefixes**, a route and all the concrete routes are displayed.
Interface Name	Choose and enter an interface name to be displayed.

Click **Find** to search and display the entries based on the search condition specified.

If two or more pages exist, enter the page numbers. Then click Go to move to a specific page.

Click the **Summary** option to view the following window:

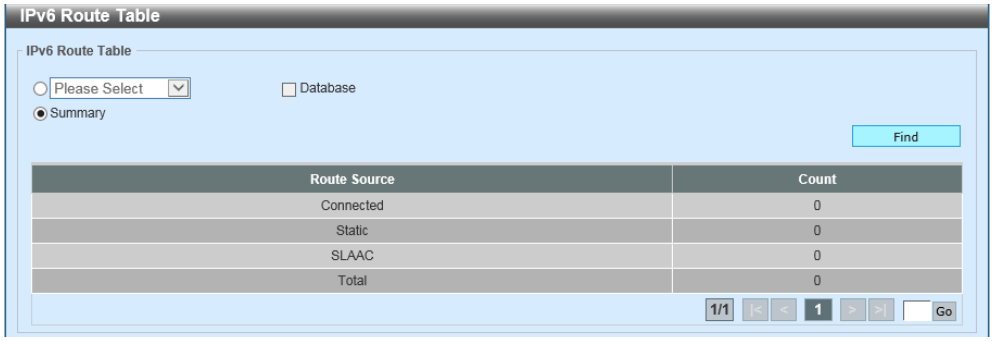


Figure 6-20 IPv6 Route Table (Summary)

6.9 IPv6 General Prefix

This window is used to configure and display the general IPv6 prefixes.

Click **L3 Features > IPv6 General Prefix** to view the following window:

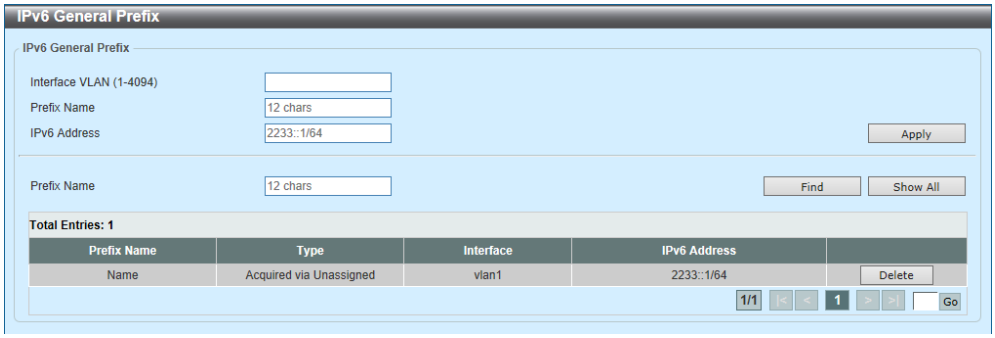


Figure 6-21 IPv6 General Prefix

The following parameters can be configured in the **IPv6 General Prefix** section:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID used here. The range is from 1 to 4094.
Prefix Name	Enter the IPv6 general prefix entry name here. This name can be up to 12 characters long.
IPv6 Address	Enter the IPv6 address and prefix length here. The prefix length of the IPv6 address is also the local subnet on the VLAN interface.

Click the **Apply** button to add a new entry.
Click the **Find** button to find and display entries based on the search criteria specified.
Click the **Show All** button to find and display all available entries.
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.

6.9.0.1 IP Multicast Forwarding Cache

This window is used to display IP multicast forwarding cache information.

Click **L3 Features > IP Multicast Routing Protocol > IPMC > IP Multicast Forwarding Cache** to view the following window:

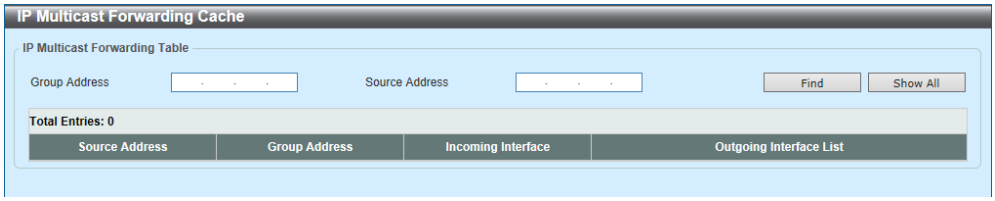


Figure 6-22 IP Multicast Forwarding Cache

The following parameters can be configured in the **IP Multicast Forwarding Table** section:

Parameter	Description
Group Address	Enter the multicast group IP address here.
Source Address	Enter the multicast source IP address here.

Click the **Find** button to find and display entries based on the search criteria specified.
Click the **Show All** button to find and display all available entries.

6.9.0.2 IPv6 Multicast Routing Forwarding Cache Table

This window is used to display IPv6 multicast routing forwarding cache information.

Click **L3 Features > IP Multicast Routing Protocol > IPv6MC > IPv6 Multicast Routing Forwarding Cache Table** to view the following window:

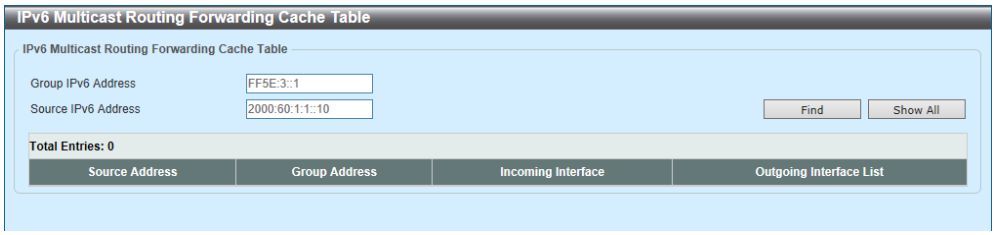


Figure 6-23 IPv6 Multicast Routing Forwarding Cache Table

The following parameters can be configured in the **IPv6 Multicast Routing Forwarding Cache Table** section:

Parameter	Description
Group IPv6 Address	Enter the multicast group IPv6 address here.
Source IPv6 Address	Enter the multicast source IPv6 address here.

Click the **Find** button to find and display entries based on the search criteria specified.
Click the **Show All** button to find and display all available entries.

7 QoS (Quality of Service)

7.1 Basic Settings

7.1.1 Port Default CoS

This window is used to configure and display the default Class of Service (CoS) settings per port interface.

Click **QoS > Basic Settings > Port Default CoS** to view the following window:

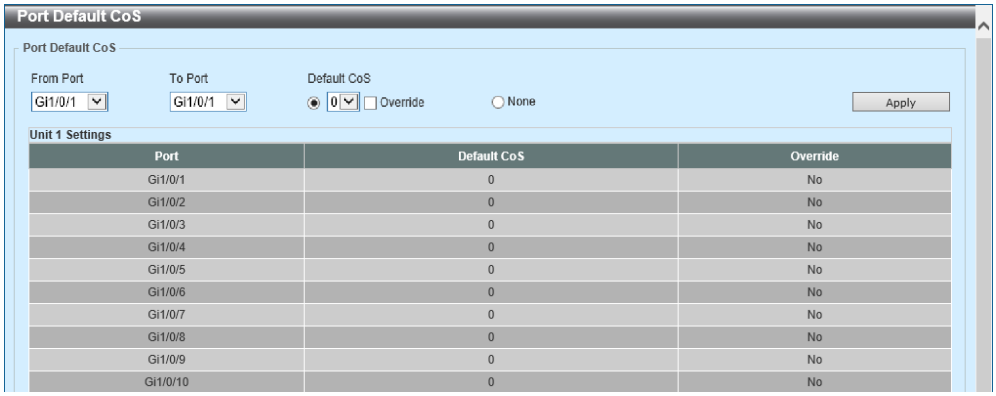


Figure 7-1 Port Default CoS

The following parameters can be configured in the **Port Default CoS** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used 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.

7.1.2 Port Scheduler Method

This window is used to configure and display the method settings related to the port scheduler feature.

Click **QoS > Basic Settings > Port Scheduler Method** to view the following window:

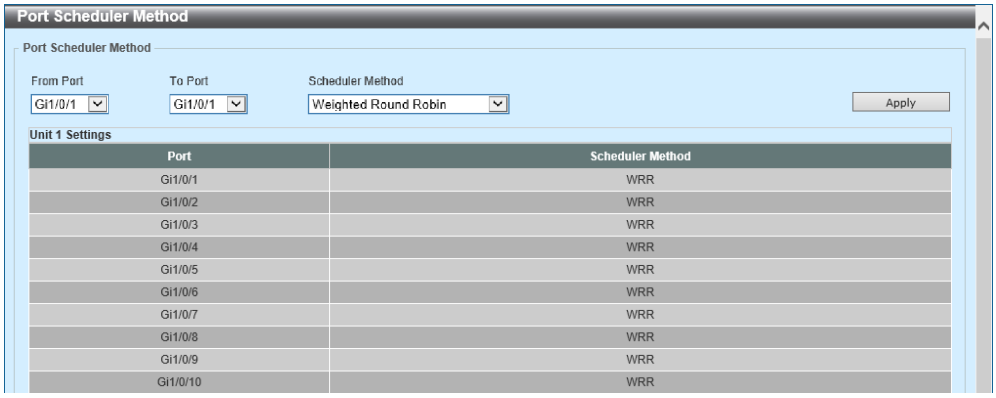


Figure 7-2 Port Scheduler Method

The following parameters can be configured in the **Port Scheduler Method** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.

Parameter	Description
Scheduler Method	Select the scheduler method that will be applied to the specified port(s). Options to choose from are: • **Strict Priority (SP)** - Specifies that all queues use strict priority scheduling. It provides strict priority access to the queues from the highest CoS queue to the lowest. • **Round Robin (RR)** - 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. • **Weighted Round Robin (WRR)** - Operates by transmitting 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. • **Weighted Deficit Round Robin (WDRR)** - Operates by serving 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.

7.1.3 Queue Settings

This window is used to configure and display the QoS queue settings.

Click **QoS > Basic Settings > Queue Settings** to view the following window:

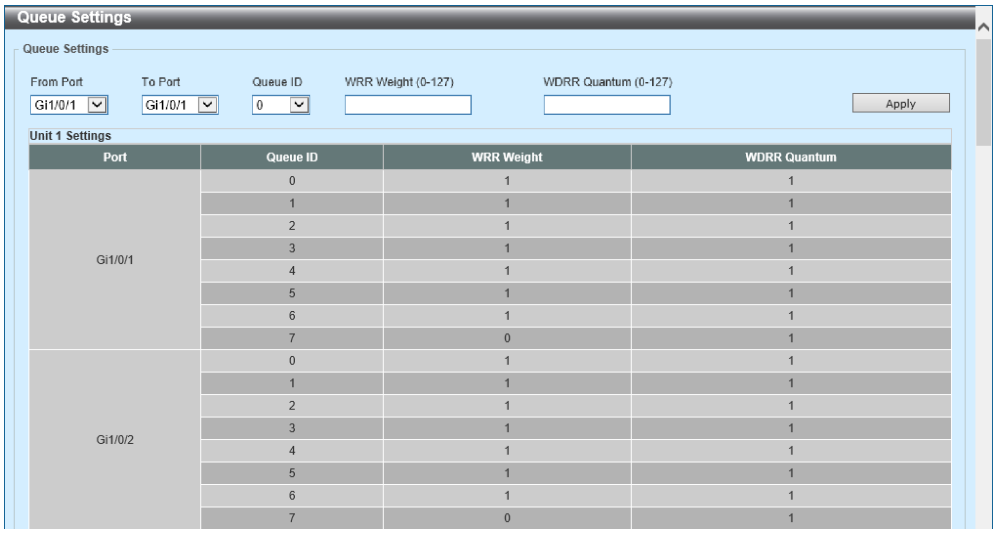


Figure 7-3 Queue Settings

The following parameters can be configured in the **Queue Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Queue ID	Enter the queue ID value here. The range is from 0 to 7.
WRR Weight	Enter the WRR weight value here. The range is from 0 to 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. The weight of the last queue should be zero while the Differentiate Service is supported.
WDRR Quantum	Enter the WDRR quantum value here. The range is from 0 to 127.

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

7.1.4 CoS to Queue Mapping

This window is used to configure and display the CoS-to-Queue mapping settings.

Click **QoS > Basic Settings > CoS to Queue Mapping** to view the following window:

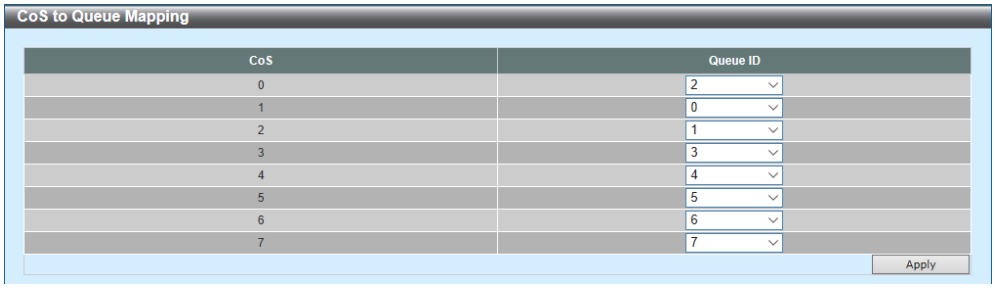


Figure 7-4 CoS to Queue Mapping

The following parameters can be configured:

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.

7.1.5 Port Rate Limiting

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

Click **QoS > Basic Settings > Port Rate Limiting** to view the following window:

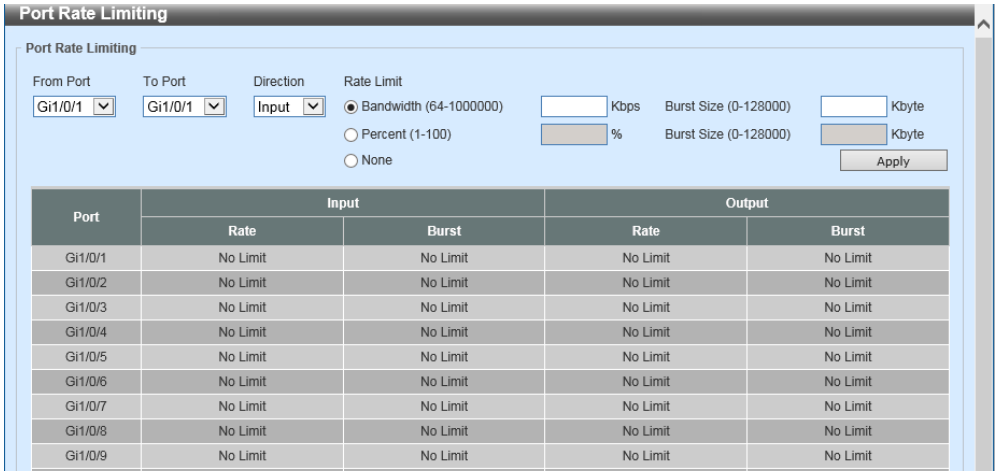


Figure 7-5 Port Rate Limiting

The following parameters can be configured in the **Port Rate Limiting** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used 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.

Parameter	Description
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. The range is from 8 to 40000000 kbps. Enter the **Burst Size** value in the space provided. The range is from 0 to 128000 kilobytes. • When **Percent** is selected, enter the input/output bandwidth percentage value used in the space provided. The range is from 1 and 100 percent. Enter the **Burst Size** value in the space provided. The range is from 0 to 128000 kilobytes. • When **None** is selected, the rate limit on the specified port(s) will be removed. 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.

7.1.6 Queue Rate Limiting

This window is used to configure and display the queue rate limiting settings.

Click **QoS > Basic Settings > Queue Rate Limiting** to view the following window:

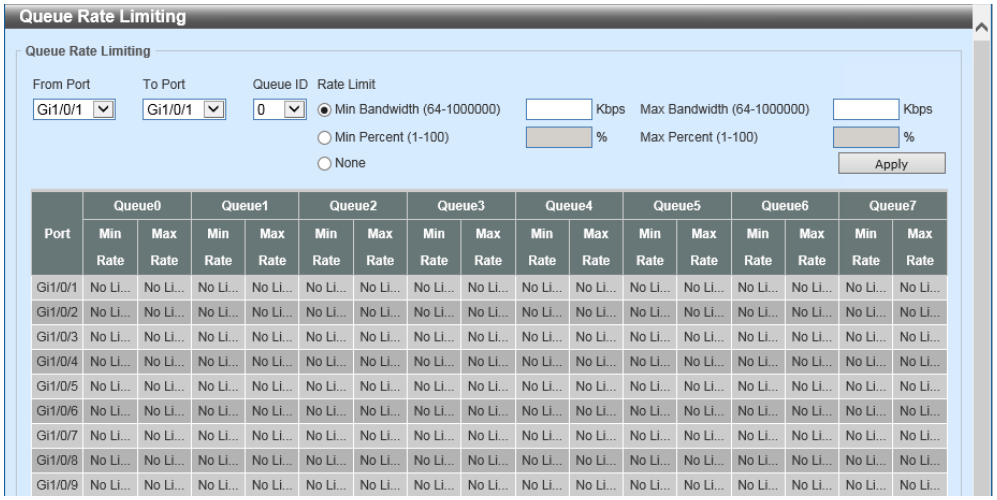


Figure 7-6 Queue Rate Limiting

The following parameters can be configured in the **Queue Rate Limiting** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
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 rate limit settings of the queue here. • When the **Min Bandwidth** option is selected, enter the minimum bandwidth rate limit in the space provided. The range is from 8 to 40000000 kbps. Enter the maximum bandwidth (**Max Bandwidth**) rate limit in the space provided. The range is from 8 to 40000000 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. The range is from 1 to 100 percent (%). Enter the maximum percentage value (**Max Percent**) in the space provided. The range is from 1 to 100 percent (%). • When **None** is selected, then no rate limit will be assigned to the specified port(s).

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

7.2 Advanced Settings

7.2.1 DSCP Mutation Map

This window is used to configure and display the Differentiated Services Code Point (DSCP) mutation map settings.

Click **QoS > Advanced Settings > DSCP Mutation Map** to view the following window:

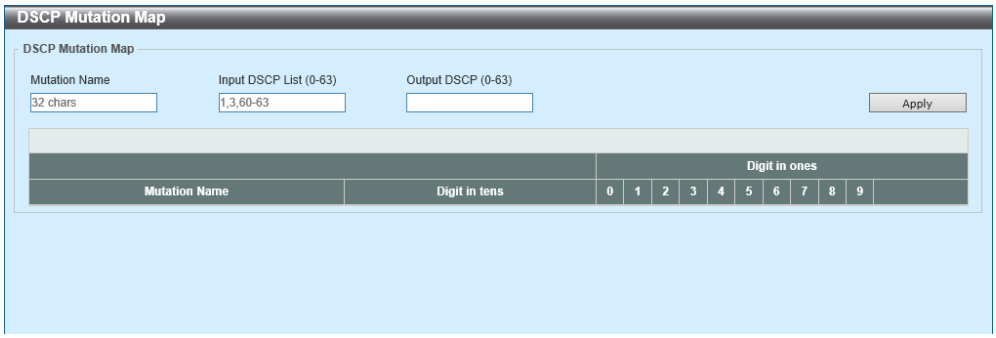


Figure 7-7 DSCP Mutation Map

The following parameters can be configured in the **DSCP Mutation Map** section:

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. The range is from 0 to 63.
Output DSCP List	Enter the output DSCP list value here. The range is from 0 to 63.

Click the **Apply** button to add a new 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.

7.2.2 Port Trust State and Mutation Binding

This window is used to configure and display the port trust state and mutation binding settings.

Click **QoS > Advanced Settings > Port Trust State and Mutation Binding** to view the following window:

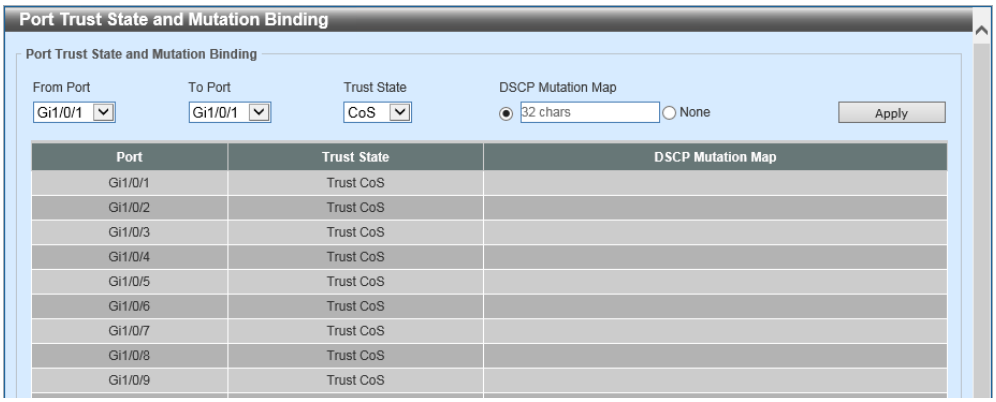


Figure 7-8 Port Trust State and Mutation Binding

The following parameters can be configured in the **Port Trust State** and **Mutation Binding** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Trust State	Select the port trust state 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 not to allocate a DSCP mutation map to the port(s).

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

7.2.3 DSCP CoS Mapping

This window is used to configure and display the DSCP CoS mapping settings.

Click **QoS > Advanced Settings > DSCP CoS Mapping** to view the following window:

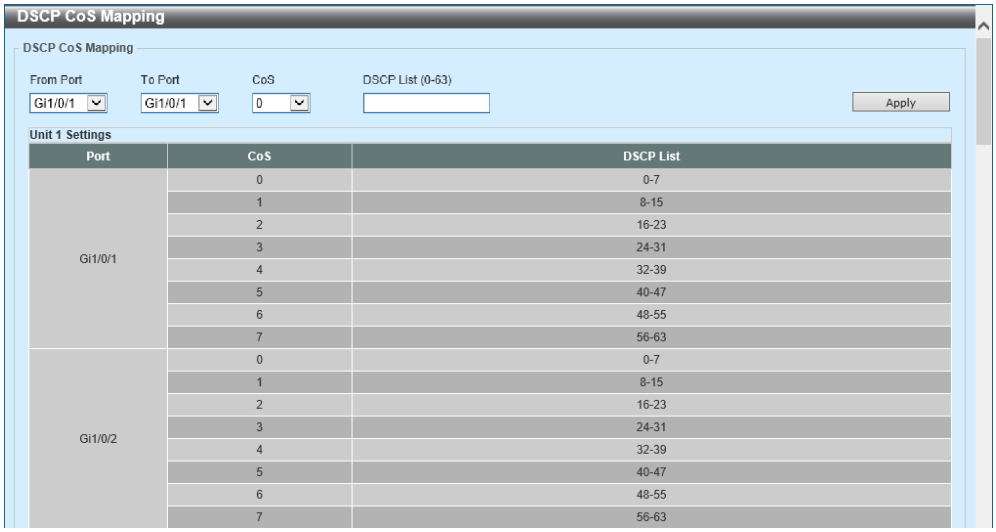


Figure 7-9 DSCP CoS Mapping

The following parameters can be configured in the **DSCP CoS Mapping** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used 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. The range is from 0 to 63.

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

7.2.4 CoS Color Mapping

This window is used to configure and display the CoS color mapping settings.

Click **QoS > Advanced Settings > CoS Color Mapping** to view the following window:

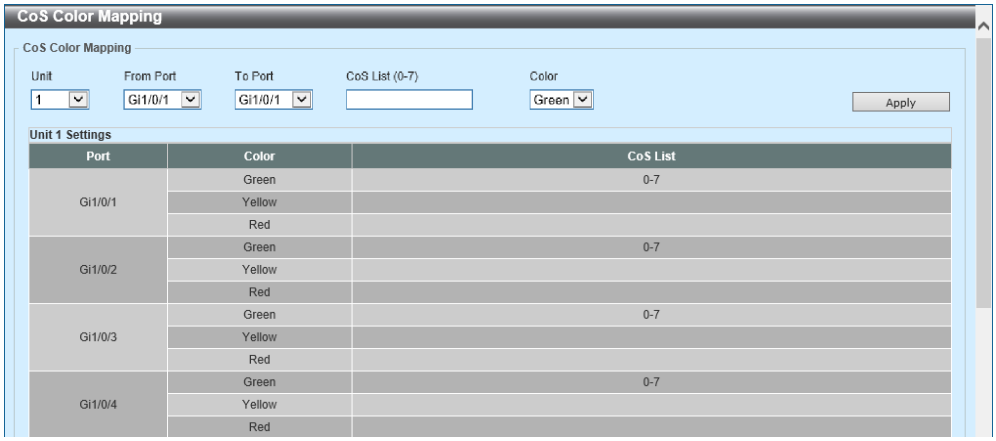


Figure 7-10 CoS Color Mapping

The following parameters can be configured in the **CoS Color Mapping** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
CoS List	Enter the CoS value that will be mapped to the color. The range is from 0 to 7.
Color	Select the color option that will be mapped to the CoS value. Options to choose from are **Green**, **Yellow**, and **Red**.

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

7.2.5 DSCP Color Mapping

This window is used to configure and display the DSCP color mapping settings.

Click **QoS > Advanced Settings > DSCP Color Mapping** to view the following window:

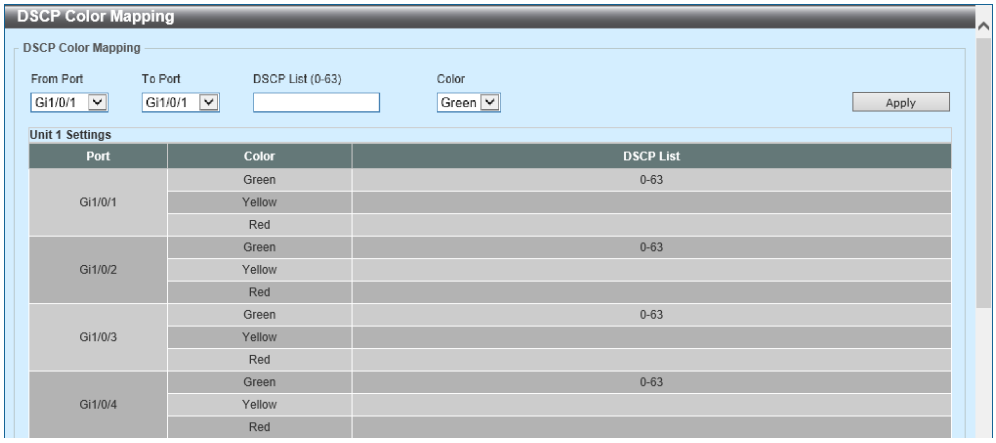


Figure 7-11 DSCP Color Mapping

The following parameters can be configured in the **DSCP Color Mapping** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
DSCP List	Enter the DSCP list value here that will be mapped to a color. The range is from 0 to 63.
Color	Select the color option that will be mapped to the DSCP value. Options to choose from are **Green**, **Yellow**, and **Red**.

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

7.2.6 Class Map

This window is used to configure and display the class map settings.

Click **QoS > Advanced Settings > Class Map** to view the following window:

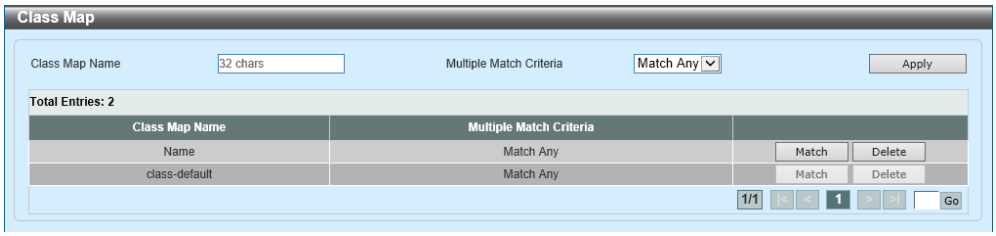


Figure 7-12 Class Map

The following parameters can be configured:

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 add a new entry.
Click the Match button to configure the match rule settings for the specified 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.

Click the **Match** button to view the following window:

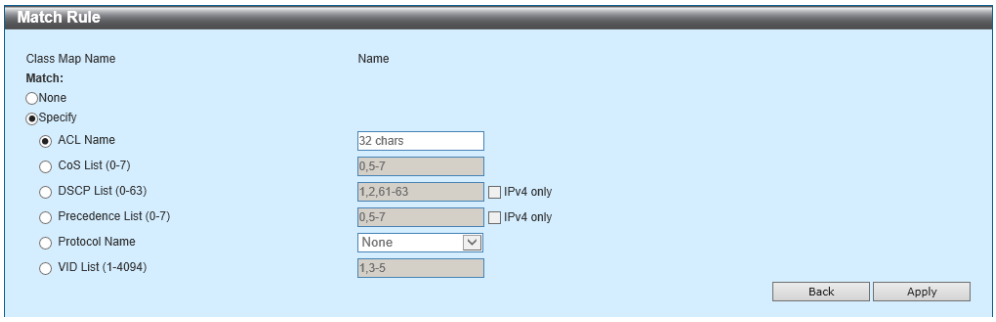


Figure 7-13 Class Map (Match)

The following parameters can be configured:

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. The range is from 0 to 7.
DSCP List	Select and enter the DSCP list value that will be matched with this class map here. The range is from 0 to 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. The range is from 0 to 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**.
VID List	Select and enter the VLAN ID(s) that will be matched with the class map here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.

Click the **Apply** button to accept the changes made.
Click the **Back** button to return to the previous window.

7.2.7 Aggregate Policer

This window is used to configure and display the aggregate policer settings.

Click **QoS > Advanced Settings > Aggregate Policer** to view the following window:

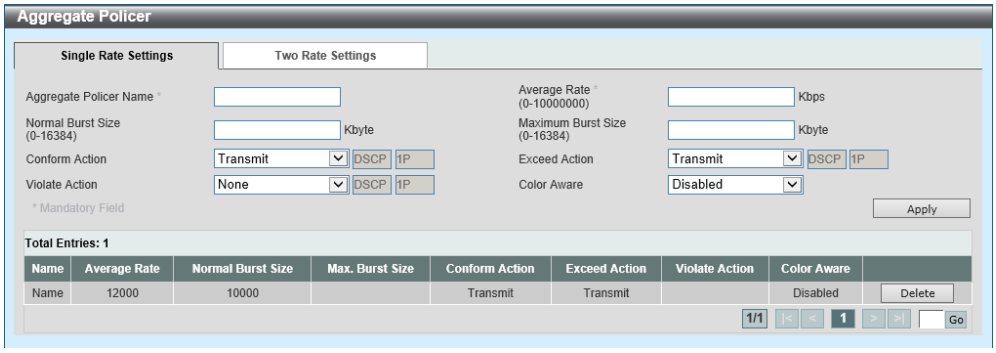


Figure 7-14 Aggregate Policer (Single Rate Settings)

The following parameters can be configured in the **Single Rate Settings** section:

Parameter	Description
Aggregate Policer Name	Enter the aggregate policer name here.
Average Rate	Enter the average rate value here. The range is from 0 to 10000000 kbps.
Normal Burst Size	Enter the normal burst size value here. The range is from 0 to 16384 Kbytes.
Maximum Burst Size	Enter the maximum burst size value here. The range is from 0 to 16384 Kbytes.

Parameter	Description
Confirm Action	Select the confirm action here. The confirm action specifies the action to take on green color packets. If the confirm action is not specified, the default action is to **Transmit**. Options to choose from are: • **Drop** - Specifies that the packet will be dropped. • **Set-DSCP-Transmit** - Specifies to configure and transmit the packet with the new DSCP value. Enter the DSCP value in the space provided. • **Set-1P-Transmit** - Specifies to configure and transmit the packet with the new IEEE 802.1p value. Enter the IEEE 802.1p value in the space provided. • **Transmit** - Specifies that the packet will be transmitted unaltered. • **Set-DSCP-1P** - Specifies to configure and transmit the packet with the new DSCP and IEEE 802.1p values. Enter the DSCP and IEEE 802.1p values in the spaces provided.
Exceed Action	Select the exceed action here. The exceed action specifies the action to take on packets that exceed the rate limit. For a two rate policer, if the exceed action is not specified, the default action is **Drop**. Options to choose from are: • **Drop** - Specifies that the packet will be dropped. • **Set-DSCP-Transmit** - Specifies to configure and transmit the packet with the new DSCP value. Enter the DSCP value in the space provided. • **Set-1P-Transmit** - Specifies to configure and transmit the packet with the new IEEE 802.1p value. Enter the IEEE 802.1p value in the space provided. • **Transmit** - Specifies that the packet will be transmitted unaltered. • **Set-DSCP-1P** - Specifies to configure and transmit the packet with the new DSCP and IEEE 802.1p values. Enter the DSCP and IEEE 802.1p values in the spaces provided.

Parameter	Description
Violate Action	Select the violate action here. The violate action specifies the action to take on packets that violate the normal and maximum burst sizes for singe rate policing. It specifies the action to take for those packets that did not conform to both CIR and PIR. For a single rate policer, if the violate action is not specified, it will create a single-rate two-color policer. For a two-rate policer, if the violation action is not specified, the default action is equal to the exceed action. Options to choose from are: • **None** - Specifies that no action will be taken. • **Drop** - Specifies that the packet will be dropped. • **Set-DSCP-Transmit** - Specifies to configure and transmit the packet with the new DSCP value. Enter the DSCP value in the space provided. • **Set-1P-Transmit** - Specifies to configure and transmit the packet with the new IEEE 802.1p value. Enter the IEEE 802.1p value in the space provided. • **Transmit** - Specifies that the packet will be transmitted unaltered. • **Set-DSCP-1P** - Specifies to configure and transmit the packet with the new DSCP and IEEE 802.1p values. Enter the DSCP and IEEE 802.1p values in the spaces provided.
Color Aware	Select to enable or disable the color aware feature here. • When color aware is **Enabled**, the policer works in the color aware mode. • When color aware is **Disabled**, the policer works in the color blind mode.

Click the **Apply** button to add a new 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.

Click the **Two Rate Settings** tab to view the following window:

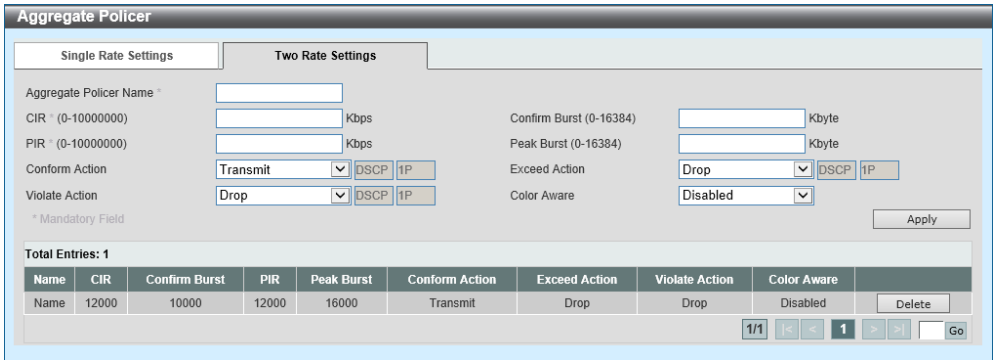


Figure 7-15 Aggregate Policer (Two Rate Settings)

The following parameters can be configured in the **Two Rate Settings** section:

Parameter	Description
Aggregate Policer Name	Enter the aggregate policer name here.
CIR	Enter the Committed Information Rate (CIR) value here. The range is from 0 to 10000000 kbps. The committed packet rate is the first token bucket for the two-rate metering.
Confirm Burst	Enter the confirm burst value here. The range is from 0 to 16384 Kbytes. The confirm burst value specifies the burst size for the first token bucket in kbps.
PIR	Enter the Peak Information Rate (PIR) value here. The range is from 0 to 10000000 kbps. The peak information rate is the second token bucket for the two-rate metering.
Peak Burst	Enter the peak burst value here. The range is from 0 to 16384 Kbytes. The peak burst value is the burst size for the second token bucket in kilobytes.

Parameter	Description
Confirm Action	Select the confirm action here. The confirm action specifies the action to take on green color packets. If the confirm action is not specified, the default action is to **Transmit**. Options to choose from are: • **Drop** - Specifies that the packet will be dropped. • **Set-DSCP-Transmit** - Specifies to configure and transmit the packet with the new DSCP value. Enter the DSCP value in the space provided. • **Set-1P-Transmit** - Specifies to configure and transmit the packet with the new IEEE 802.1p value. Enter the IEEE 802.1p value in the space provided. • **Transmit** - Specifies that the packet will be transmitted unaltered. • **Set-DSCP-1P** - Specifies to configure and transmit the packet with the new DSCP and IEEE 802.1p values. Enter the DSCP and IEEE 802.1p values in the spaces provided.
Exceed Action	Select the exceed action here. The exceed action specifies the action to take on packets that exceed the rate limit. For a two rate policer, if the exceed action is not specified, the default action is **Drop**. Options to choose from are: • **Drop** - Specifies that the packet will be dropped. • **Set-DSCP-Transmit** - Specifies to configure and transmit the packet with the new DSCP value. Enter the DSCP value in the space provided. • **Set-1P-Transmit** - Specifies to configure and transmit the packet with the new IEEE 802.1p value. Enter the IEEE 802.1p value in the space provided. • **Transmit** - Specifies that the packet will be transmitted unaltered. • **Set-DSCP-1P** - Specifies to configure and transmit the packet with the new DSCP and IEEE 802.1p values. Enter the DSCP and IEEE 802.1p values in the spaces provided.

Parameter	Description
Violate Action	Select the violate action here. The violate action specifies the action to take on packets that violate the normal and maximum burst sizes for singe rate policing. It specifies the action to take for those packets that did not conform to both CIR and PIR. • For a single rate policer, if the violate action is not specified, it will create a single-rate two-color policer. • For a two-rate policer, if the violation action is not specified, the default action is equal to the exceed action. Options to choose from are: • **Drop** - Specifies that the packet will be dropped. • **Set-DSCP-Transmit** - Specifies to configure and transmit the packet with the new DSCP value. Enter the DSCP value in the space provided. • **Set-1P-Transmit** - Specifies to configure and transmit the packet with the new IEEE 802.1p value. Enter the IEEE 802.1p value in the space provided. • **Transmit** - Specifies that the packet will be transmitted unaltered. • **Set-DSCP-1P** - Specifies to configure and transmit the packet with the new DSCP and IEEE 802.1p values. Enter the DSCP and IEEE 802.1p values in the spaces provided.
Color Aware	Select to enable or disable the color aware feature here. • When color aware is **Enabled**, the policer works in the color-aware mode. • When color aware is **Disabled**, the policer works in the color-blind mode.

Click the **Apply** button to add a new 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.

7.2.8 Policy Map

This window is used to configure and display the policy map settings.

Click **QoS > Advanced Settings > Policy Map** to view the following window:

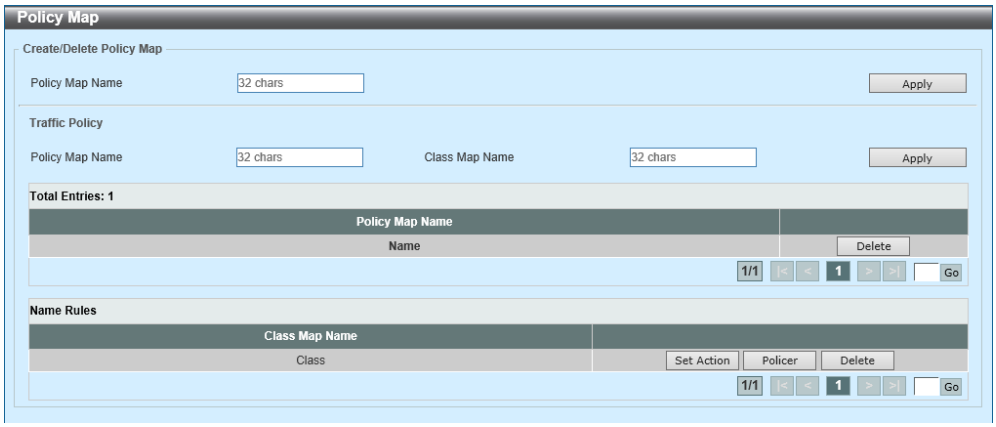


Figure 7-16 Policy Map

The following parameters can be configured in the **Create/Delete Policy Map** section:

Parameter	Description
Policy Map Name	Enter the policy map name here that will be created or deleted. This name can be up to 32 characters long.

Click the **Apply** button to add a new 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.

The following parameters can be configured in the **Traffic Policy** section:

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 add a new entry.
Click the **Set Action** button to configure the set action settings for the specified entry.
Click the **Policer** button to configure the police action settings for the specified 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.

Click the **Set Action** button to view the following window:

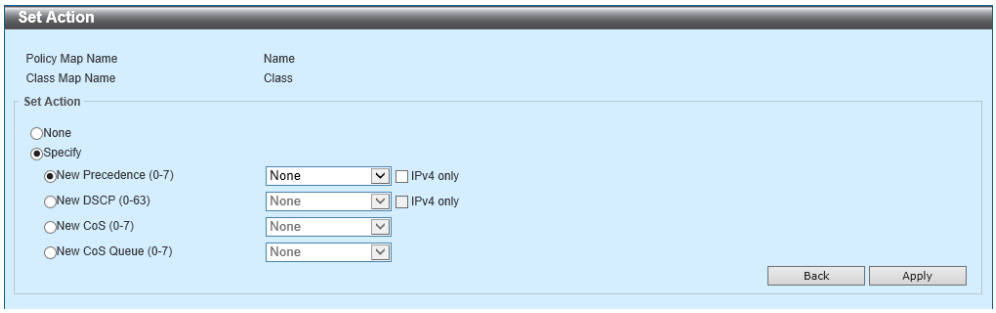


Figure 7-17 Policy Map (Set Action)

The following parameters can be configured in the **Set Action** section:

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.
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 selected, then both the IPv4 and IPv6 DSCP will be marked.
New CoS	Select the new CoS value to the packet here. The range is from 0 to 7.
New Cos Queue	Select the new CoS queue value to the packets here. This will overwrite the original CoS queue selection. Setting the CoS queue will not take effect if the policy map is applied for the egress flow on the interface.

Click the **Apply** button to accept the changes made.
Click the **Back** button to return to the previous window.

Click the **Policer** button and specify the police action as **Police** to view the following window:

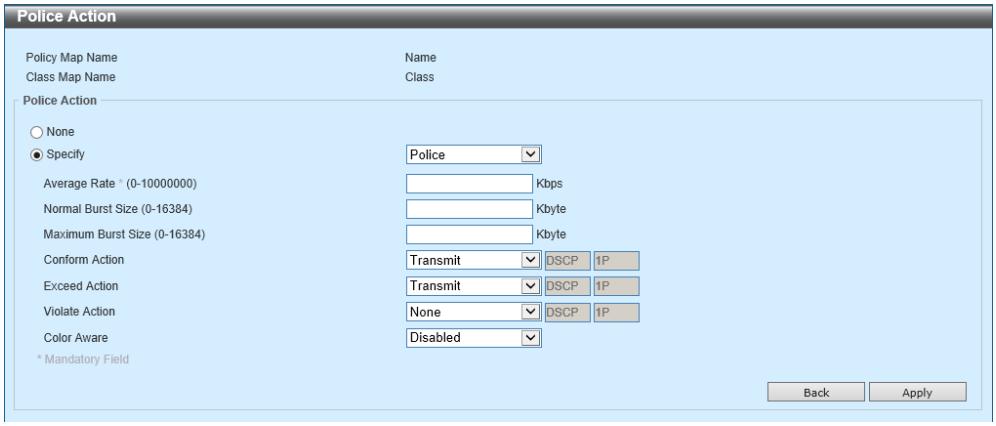


Figure 7-18 Policy Map (Policer, Police)

The following parameters can be configured in the **Police Action** section:

Parameter	Description
None	Select this option to specify that no policer settings will be configured for this entry.
Specify	Select this option to specify that the following policer settings will be applied to this entry.
Average Rate	Enter the average rate value here. The range is from 0 to 10000000 Kbps.
Normal Burst Size	Enter the normal burst size value here. The range is from 0 to 16384 Kbps.
Maximum Burst Size	Enter the maximum burst size value here. The range is from 0 to 16384 Kbps.
Conform Action	Select the conform action that will be taken here. This action will be taken on green color packets. Option to choose from are: • **Drop** - Specifies that the packet will be dropped. • **Set-DSCP-Transmit** - Specifies to configure and transmit the packet with the new DSCP value. Enter the DSCP value in the space provided. • **Set-1P-Transmit** - Specifies to configure and transmit the packet with the new IEEE 802.1p value. Enter the IEEE 802.1p value in the space provided. • **Transmit** - Specifies that the packet will be transmitted unaltered. • **Set-DSCP-1P** - Specifies to configure and transmit the packet with the new DSCP and IEEE 802.1p values. Enter the DSCP and IEEE 802.1p values in the spaces provided.

Parameter	Description
Exceed Action	Select the exceed action that will be taken here. This action will be taken on yellow color packets that exceed the rate limit. Option to choose from are: • **Drop** - Specifies that the packet will be dropped. • **Set-DSCP-Transmit** - Specifies to configure and transmit the packet with the new DSCP value. Enter the DSCP value in the space provided. • **Set-1P-Transmit** - Specifies to configure and transmit the packet with the new IEEE 802.1p value. Enter the IEEE 802.1p value in the space provided. • **Transmit** - Specifies that the packet will be transmitted unaltered. • **Set-DSCP-1P** - Specifies to configure and transmit the packet with the new DSCP and IEEE 802.1p values. Enter the DSCP and IEEE 802.1p values in the spaces provided.
Violate Action	Select the violate action that will be taken here. This action will be taken on red color packets. Option to choose from are: • **None** - Specifies that no violate action will be taken. • **Drop** - Specifies that the packet will be dropped. • **Set-DSCP-Transmit** - Specifies to configure and transmit the packet with the new DSCP value. Enter the DSCP value in the space provided. • **Set-1P-Transmit** - Specifies to configure and transmit the packet with the new IEEE 802.1p value. Enter the IEEE 802.1p value in the space provided. • **Transmit** - Specifies that the packet will be transmitted unaltered. • **Set-DSCP-1P** - Specifies to configure and transmit the packet with the new DSCP and IEEE 802.1p values. Enter the DSCP and IEEE 802.1p values in the spaces provided.
Color Aware	Select to enable or disable the color aware feature here. • When **Enabled**, the policer works in the color-aware mode. • •When **Disabled**, the policer works in the color-blind mode.

Click the **Apply** button to accept the changes made.
Click the **Back** button to return to the previous window.

Click the **Policer** button and specify the police action as **Police CIR** to view the following window:

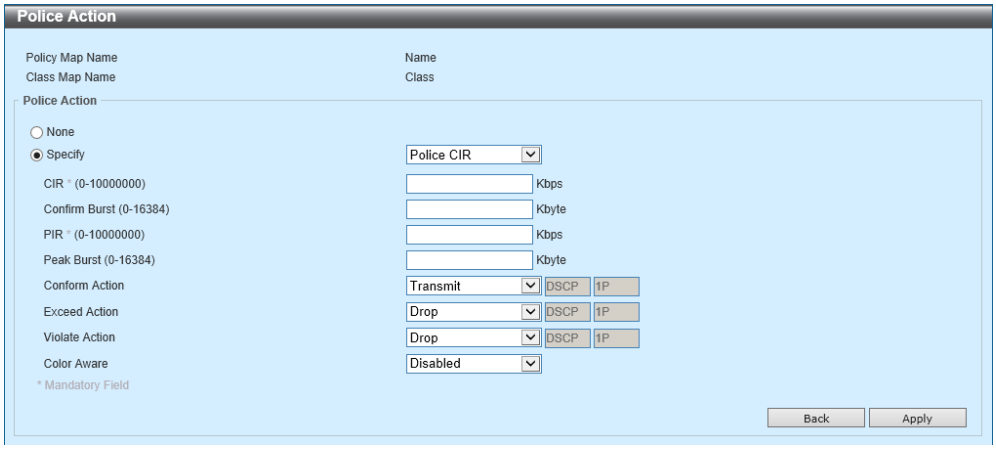


Figure 7-19 Policy Map (Policer, Police CIR)

The following parameters can be configured in the **Police Action** section:

Parameter	Description
None	Select this option to specify that no policer settings will be configured for this entry.
Specify	Select this option to specify that the following policer settings will be applied to this entry.
CIR	Enter the Committed Information Rate (CIR) value here. This is the first token bucket for two-rate metering. The range is from 0 to 10000000 kbps.
Confirm Burst	Enter the confirm burst value here. This is the size of the first token bucket. The range is from 0 to 16384 kilobytes.
PIR	Enter the Peak Information Rate (PIR) value here. This is the second token bucket for two-rate metering. The range is from 0 to 10000000.
Peak Burst	Enter the peak burst value here. This is the size of the second token bucket. The range is from 0 to 16384 kilobytes.

Parameter	Description
Conform Action	Select the conform action that will be taken here. This action will be taken on green color packets. Option to choose from are: • **Drop** - Specifies that the packet will be dropped. • **Set-DSCP-Transmit** - Specifies to configure and transmit the packet with the new DSCP value. Enter the DSCP value in the space provided. • **Set-1P-Transmit** - Specifies to configure and transmit the packet with the new IEEE 802.1p value. Enter the IEEE 802.1p value in the space provided. • **Transmit** - Specifies that the packet will be transmitted unaltered. • **Set-DSCP-1P** - Specifies to configure and transmit the packet with the new DSCP and IEEE 802.1p values. Enter the DSCP and IEEE 802.1p values in the spaces provided.
Exceed Action	Select the exceed action that will be taken here. This action will be taken on yellow color packets that exceed the rate limit. Option to choose from are: • **Drop** - Specifies that the packet will be dropped. • **Set-DSCP-Transmit** - Specifies to configure and transmit the packet with the new DSCP value. Enter the DSCP value in the space provided. • **Set-1P-Transmit** - Specifies to configure and transmit the packet with the new IEEE 802.1p value. Enter the IEEE 802.1p value in the space provided. • **Transmit** - Specifies that the packet will be transmitted unaltered. • **Set-DSCP-1P** - Specifies to configure and transmit the packet with the new DSCP and IEEE 802.1p values. Enter the DSCP and IEEE 802.1p values in the spaces provided.

Parameter	Description
Violate Action	Select the violate action that will be taken here. This action will be taken on red color packets. Option to choose from are: • **None** - Specifies that no violate action will be taken. • **Drop** - Specifies that the packet will be dropped. • **Set-DSCP-Transmit** - Specifies to configure and transmit the packet with the new DSCP value. Enter the DSCP value in the space provided. • **Set-1P-Transmit** - Specifies to configure and transmit the packet with the new IEEE 802.1p value. Enter the IEEE 802.1p value in the space provided. • **Transmit** - Specifies that the packet will be transmitted unaltered. • **Set-DSCP-1P** - Specifies to configure and transmit the packet with the new DSCP and IEEE 802.1p values. Enter the DSCP and IEEE 802.1p values in the spaces provided.
Color Aware	Select to enable or disable the color aware feature here. • When **Enabled**, the policer works in the color-aware mode. • When **Disabled**, the policer works in the color-blind mode.

Click the **Apply** button to accept the changes made.
Click the **Back** button to return to the previous window.

Click the **Policer** button and specify the police action as **Police Aggregate** to view the following window:

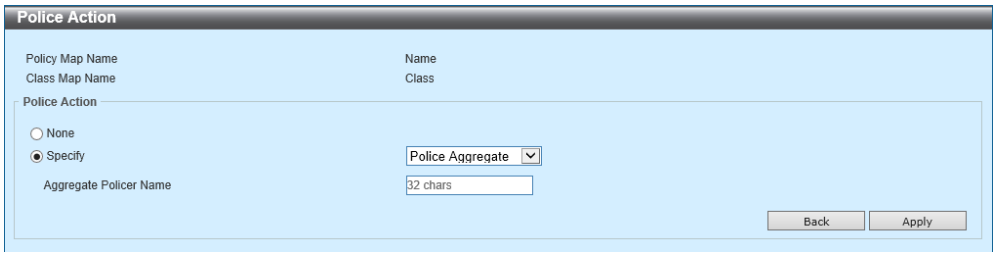


Figure 7-20 Policy Map (Policer, Police Aggregate)

The following parameters can be configured in the **Police Action** section:

Parameter	Description
None	Select this option to specify that no policer settings will be configured for this entry.
Specify	Select this option to specify that the following policer settings will be applied to this entry.

Parameter	Description
Aggregate Policer Name	Enter the name for the aggregate policing rule here. This can be up to 32 characters long.

Click the **Apply** button to accept the changes made.
Click the **Back** button to return to the previous window.

7.2.9 Policy Binding

This window is used to configure and display the policy binding settings.

Click **QoS > Advanced Settings > Policy Binding** to view the following window:

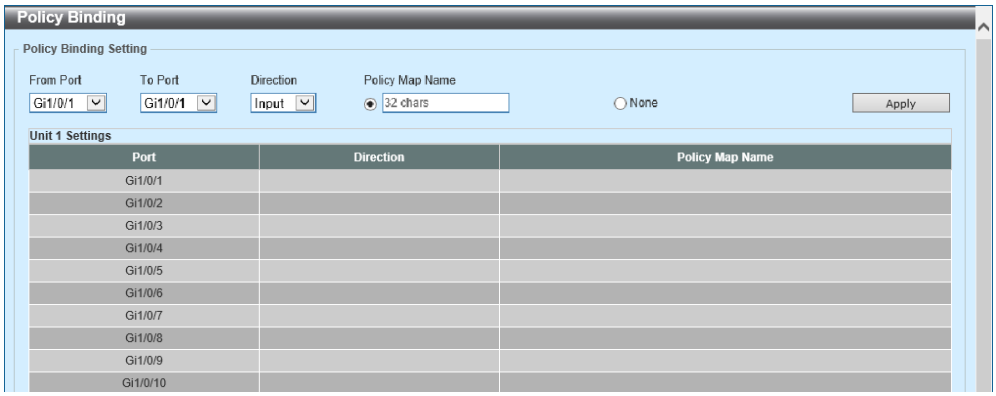


Figure 7-21 Policy Binding

The following parameters can be configured in the **Policy Binding Setting** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Direction	Select the direction option here. Options to choose from are **Input** and **Output**. Input specified ingress traffic and output specifies egress traffic.
Policy Map Name	Enter the policy map name here. This name can be up to 32 characters long. • Select the **None** option not to tie a policy map to this entry.

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

7.3 WRED (Weighted Random Early Detection)

7.3.1 WRED Profile

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

Click **QoS > WRED > WRED Profile** to view the following window:

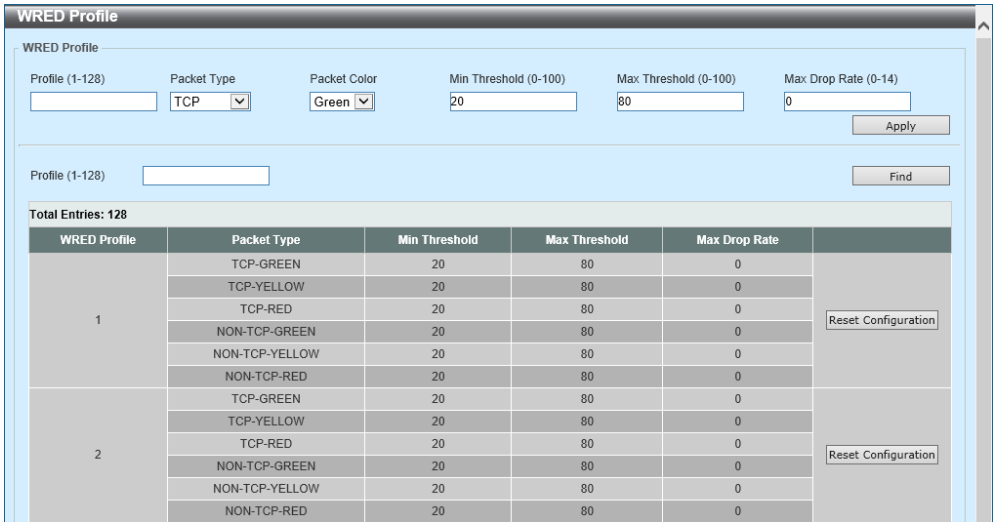


Figure 7-22 WRED Profile

The following parameters can be configured in the **WRED Profile** section:

Parameter	Description
Profile	Enter the WRED profile ID here. The range is from 1 to 128.
Packet Type	Select the packet type here. Options to choose from are: • **TCP** - Specifies the WRED drop parameters for the TCP packets to be set. • **Non-TCP** - Specifies the WRED drop parameters for non-TCP packets to be set.
Packet Color	Select the packet color here. Options to choose from are: • **Green** - Specifies the WRED drop parameters for green packets to be set. • **Yellow** - Specifies the WRED drop parameters for yellow packets to be set. • **Red** - Specifies the WRED drop parameters for red packets to be set.
Min Threshold	Enter the minimum threshold value here that will be used to start WRED dropping. The range is from 0 to 100.

Parameter	Description
Max Threshold	Enter the maximum threshold value here over which WRED will drop all packets destined for this queue. The range is from 0 to 100.
Max Drop Rate	Enter the maximum drop-rate value here. The range is from 0 to 14. This feature specifies the drop probability when the average queue size reaches the maximum threshold. When this value is zero, then the packet will not be dropped or remarked for ECN.

Click the **Apply** button to accept the changes made.
Click the **Find** button to find and display entries based on the search criteria specified.
Click the **Reset Configuration** button to reset the configuration for the specified entry.

7.3.2 WRED Queue

This window is used to configure and display the WRED queue settings.

Click **QoS > WRED > WRED Queue** to view the following window:

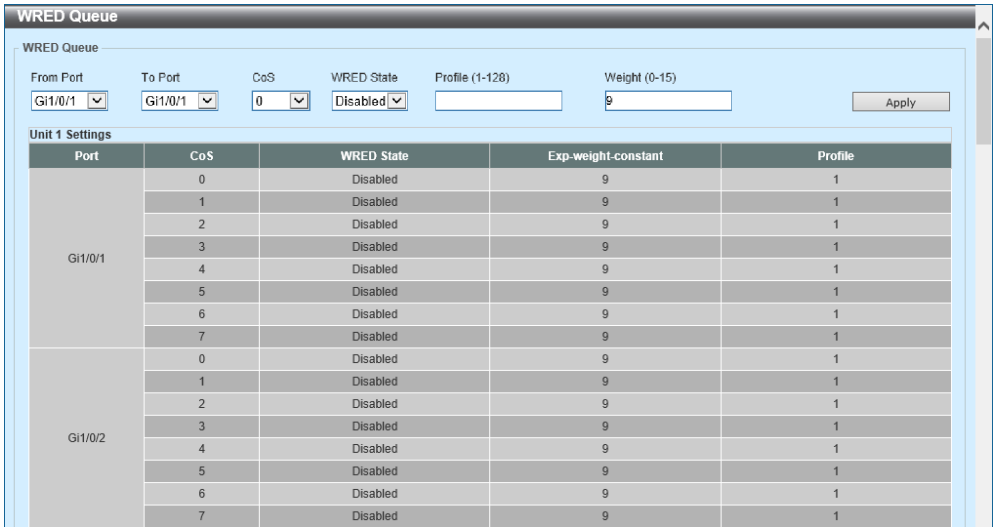


Figure 7-23 WRED Queue

The following parameters can be configured in the **WRED Queue** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
CoS	Select the CoS value here. The range is from 0 to 7.
WRED State	Select to enable or disable the WRED feature state on the specified port(s) here.
Profile	Enter the WRED profile ID here. The range is from 1 to 128.
Weight	Enter the exponential weight value here. The range is from 0 to 15. This feature is used to configure the WRED exponential weight factor for the average queue size calculation for the queue.

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

7.4 Egress Buffer Settings

Use the following window to configure the threshold of output buffering and display the threshold specified. Regarding the threshold of output buffering, operating with the default configuration is recommended. Egress Buffer changes the status to "High" regarding the environment where the traffics instantaneously exceeding the maximum quantity of communications for a port occur frequently.

Choose **QoS > Egress Buffer Settings** to display the following window.

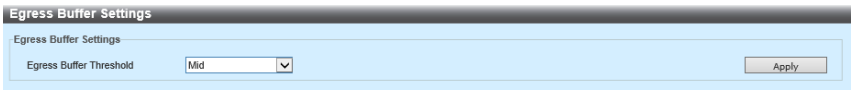


Figure 7-24 Egress Buffer Settings

In the section of **Egress Buffer Settings**, you can configure the following parameter.

Parameter	Overview
Threshold Settings for Egress Buffer	Choose the threshold of an output buffering. The options (values) available are **Mid** and **High**. If the value is configured in advance, the threshold is displayed. The default (or initial) value is **Mid**.

Click **Apply** to reflect the change.

8 ACL (Access Control List)

8.1 ACL Configuration Wizard

This window is used to configure new and existing ACLs using the ACL Configuration Wizard.

Click **ACL > ACL Configuration Wizard** to view the following window:

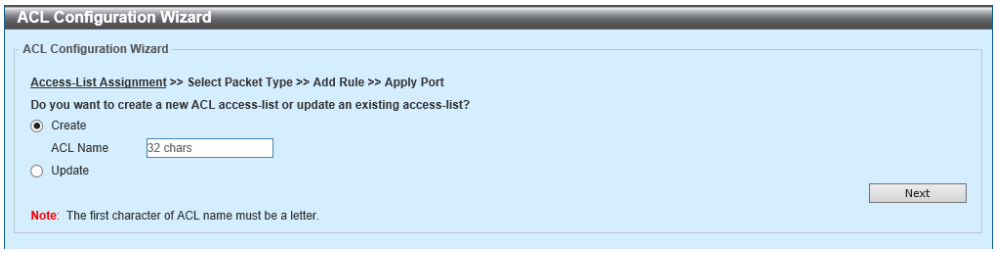


Figure 8-1 ACL Configuration Wizard (Create)

Click the **Update** option to view the following window:

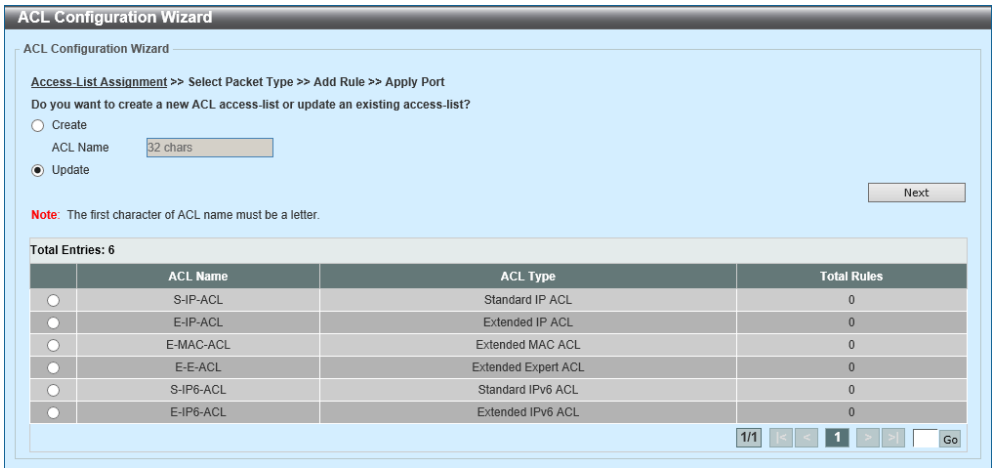


Figure 8-2 ACL Configuration Wizard (Update)

The following parameters can be configured:

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 proceed to the next step in the wizard.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After select to **Create** an ACL and clicking the **Next** button, the following window will be displayed:

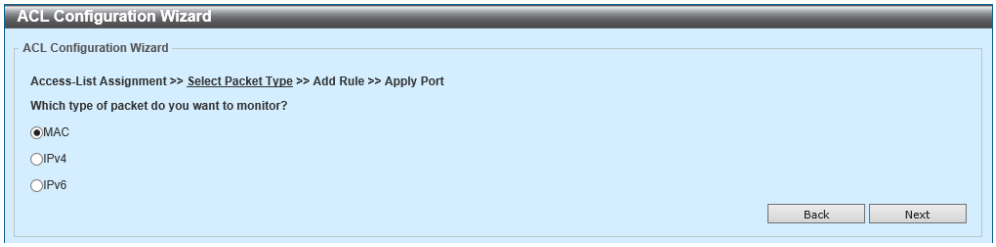


Figure 8-3 ACL Configuration Wizard (Select ACL Type)

The following parameters can be configured:

Parameter	Description
MAC	Select this option to create a MAC ACL.
IPv4	Select this option to create an IPv4 ACL.
IPv6	Select this option to create an IPv6 ACL.

Click the **Next** button to proceed to the next step in the wizard.
Click the **Back** button to return to the previous step in the wizard.

8.1.1 MAC ACL

After selecting to **Create/Update** a **MAC ACL**, the following window will be displayed:

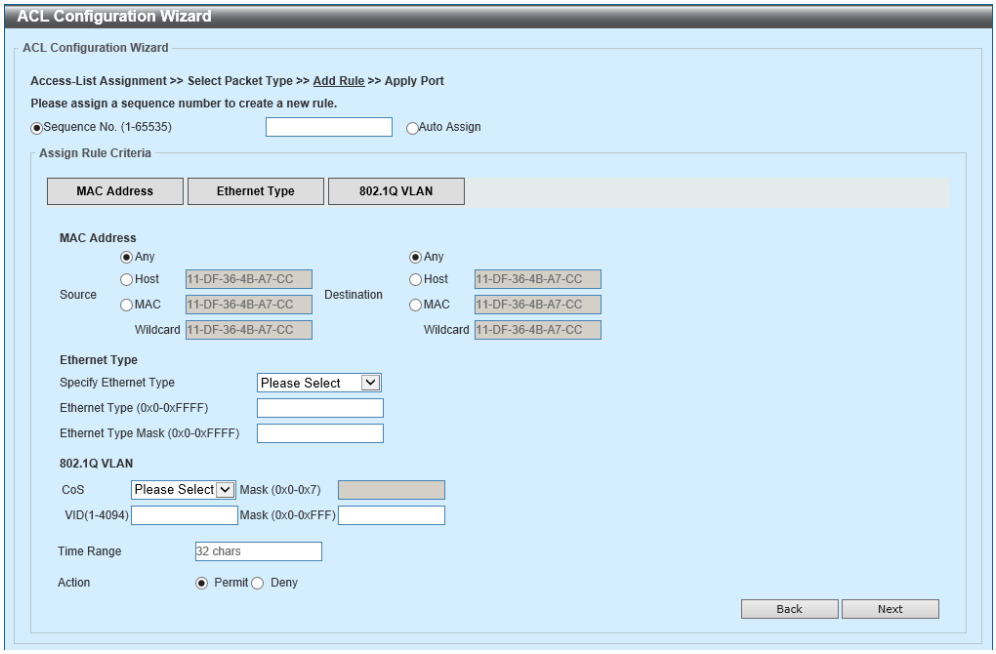


Figure 8-4 ACL Configuration Wizard (Configure MAC ACL)

The following parameters can be configured:

Parameter	Description
Sequence No.	Enter the ACL rule number here. The range is from 1 to 65535. Select **Auto Assign** to generate an ACL rule number automatically for this entry.
Source	Select and enter the source MAC address information here. Options to choose from are: • **Any** - Specifies that any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host MAC address here. • **MAC** - 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** - Specifies that any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host MAC address here. • **MAC** - 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. The range is from 0x600 to 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. The range is from 0x0 to 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. • **Mask** - Enter the CoS mask value here. The range is from 0x0 to 0x7.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094. • **Mask** - Enter the VLAN ID mask value here. The range is from 0x0 to 0xFFF.
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, Deny and Deny CPU.

Click the **Next** button to proceed to the next step in the wizard.
Click the **Back** button to return to the previous step in the wizard.

After clicking the **Next** button (in the previous step), the following window will be displayed:

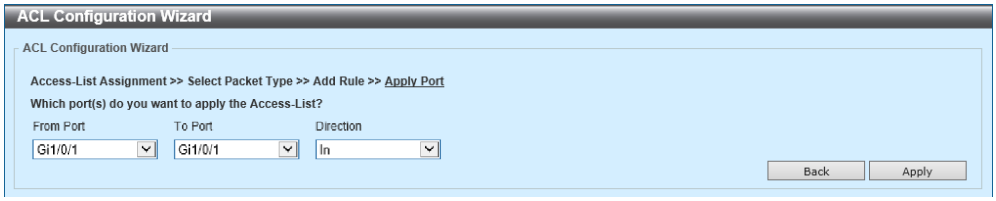


Figure 8-5 ACL Configuration Wizard (Select Ports and Direction)

The following parameters can be configured:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Direction	Select the direction here. Options to choose from are In and Out.

Click the **Apply** button to accept the changes made and return to the **ACL Configuration Wizard** window.
Click the **Back** button to return to the previous step in the wizard.

8.1.2 IPv4

After selecting to **Update** a **Standard IP ACL**, the following window will be displayed:

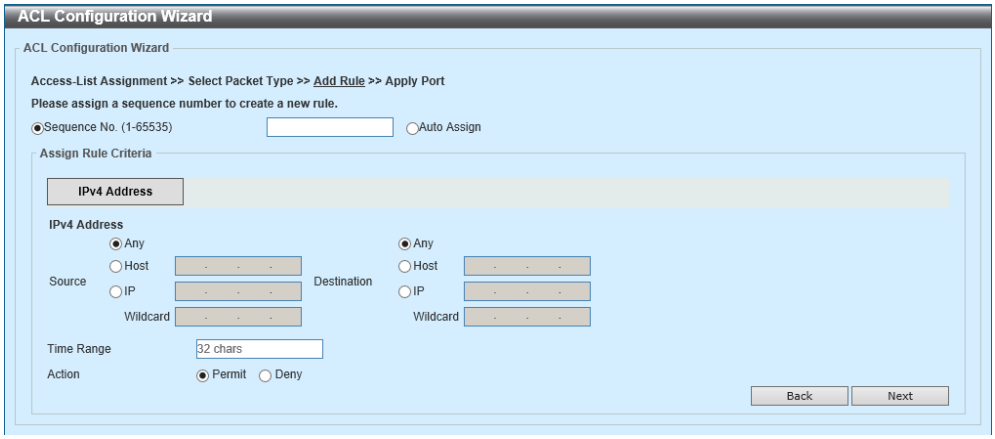


Figure 8-6 ACL Configuration Wizard (Configure Standard IP ACL)

After selecting to **Update** an **Extended IP ACL** or to **Create** an **IPv4 ACL**, the following window will be displayed:

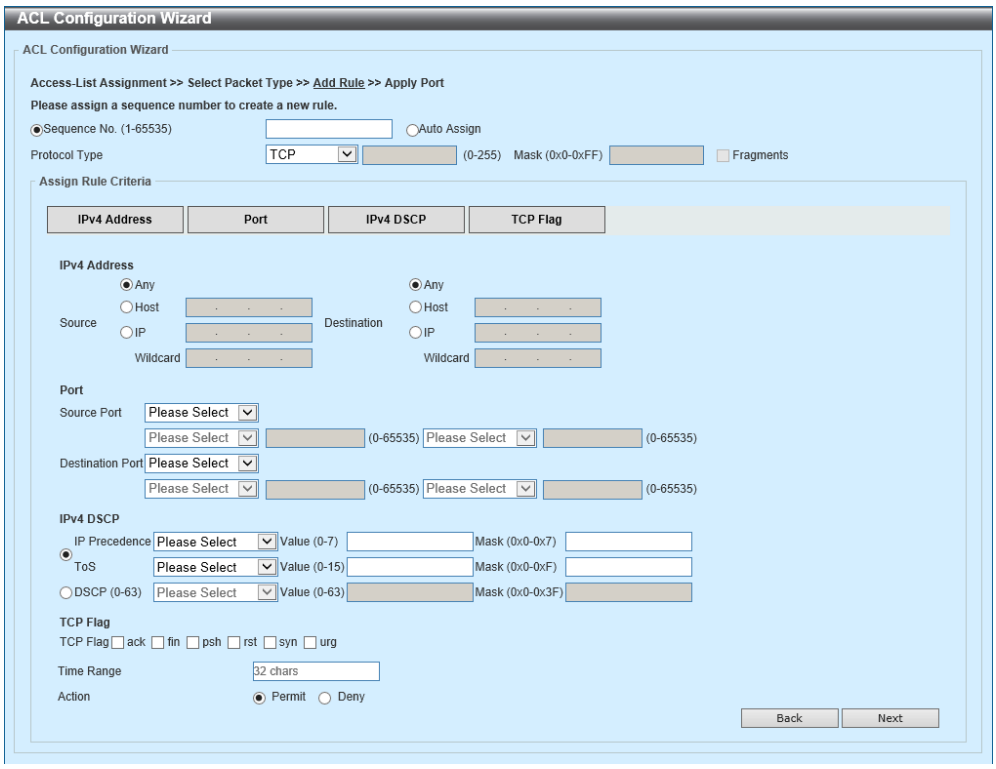


Figure 8-7 ACL Configuration Wizard (Configure Extended IP ACL)

The following parameters can be configured:

Parameter	Description
Sequence No.	Enter the ACL rule number here. The range is from 1 to 65535. Select **Auto Assign** to generate an ACL rule number automatically 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. • **Mask** - After selecting the Protocol ID option, manually enter the protocol mask value here. The range is from 0x0 to 0xFF. • **Fragments** - Select this option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are: • **Any** - Specifies that any source traffic will be evaluated according to the conditions of this rule. • **Host** - Specifies to use and enter a source host IP address here. • **IP** - Specifies to use and enter a 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** - Specifies that any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Specifies to use and enter a destination host IP address here. • **IP** - Specifies to use and enter a 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
Source Port	Select and enter the source port value here. Options to choose from are: • **=** - The ACL will use the port number specified only. • **>** - The ACL will use all ports greater than the port number specified. • **<** - The ACL will use all ports smaller than the port number specified. • ≠ - The ACL will use all ports except the port number specified. • **Range** - The ACL will use the ports specified within the range. • **Mask** - The ACL will use the ports within the range of the mask specified. Enter the port mask value in the space provided. The range is from 0x0 to 0xFFFF. This parameter is only available when **TCP** or **UDP** is selected as the **Protocol Type**.
Destination Port	Select and enter the destination port value here. Options to choose from are: • **=** - The ACL will use the port number specified only. • **>** - The ACL will use all ports greater than the port number specified. • **<** - The ACL will use all ports smaller than the port number specified. • ≠ - The ACL will use all ports except the port number specified. • **Range** - The ACL will use the ports specified within the range. • **Mask** - The ACL will use the ports within the range of the mask specified. Enter the port mask value in the space provided. The range is from 0x0 to 0xFFFF. This parameter is only available when **TCP** or **UDP** is selected as the **Protocol Type**.
Specify ICMP Message Type	Select the ICMP message type used here. This parameter is only available when **ICMP** is selected as the **Protocol Type**.
ICMP Message Type	When the **ICMP Message Type** is not specified, 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 when **ICMP** is selected as the **Protocol Type**.

Parameter	Description
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 when **ICMP** is selected as the **Protocol Type**.
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. • **Mask** - Enter the IP precedence mask value here. The range is from 0x0 to 0x7.
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. • **Mask** - Enter the ToS mask value here. The range is from 0x0 to 0xF.
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. • **Mask** - Enter the DSCP mask value here. The range is from 0x0 to 0x3F.
TCP Flag	Select the TCP flag that will be evaluated in this ACL here. Options to choose from are **ack**, **fin**, **psh**, **rst**, **syn**, and **urg**. This parameter is only available when **TCP** is selected as the **Protocol Type**.
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 **Next** button to proceed to the next step in the wizard.
Click the **Back** button to return to the previous step in the wizard.

After clicking the **Next** button (in the previous step), the following window will be displayed:

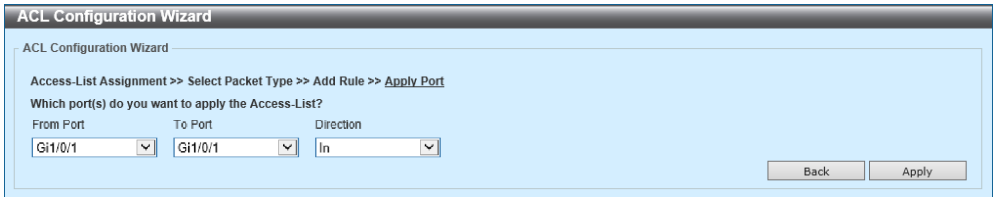


Figure 8-8 ACL Configuration Wizard (IPv4, Step 3)

The following parameters can be configured:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Direction	Select the direction here. Options to choose from are In and Out.

Click the **Apply** button to accept the changes made and return to the ACL Configuration Wizard window.
Click the **Back** button to return to the previous step in the wizard.

8.1.3 IPv6

After selecting to **Update** a **Standard IPv6 ACL**, the following window will be displayed:

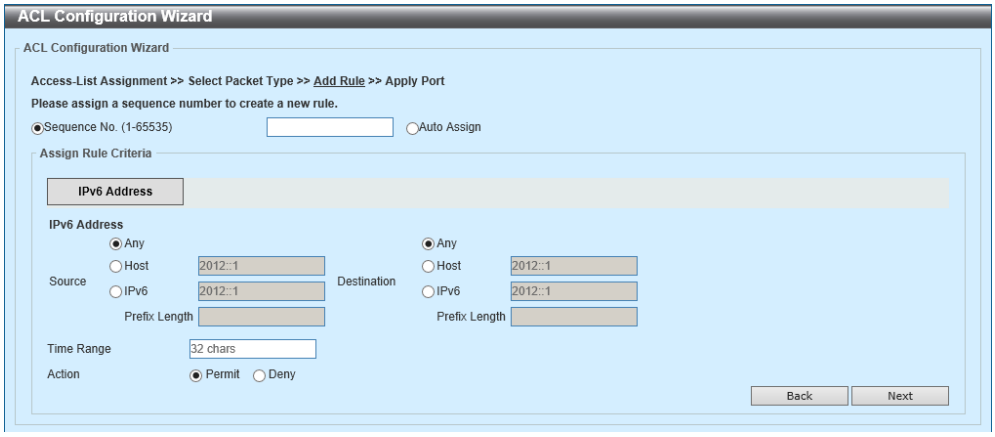


Figure 8-9 ACL Configuration Wizard (Configure Standard IPv6 ACL)

After selecting to **Update** an **Extended IPv6 ACL** or to **Create** an **IPv6 ACL**, the following window will be displayed:

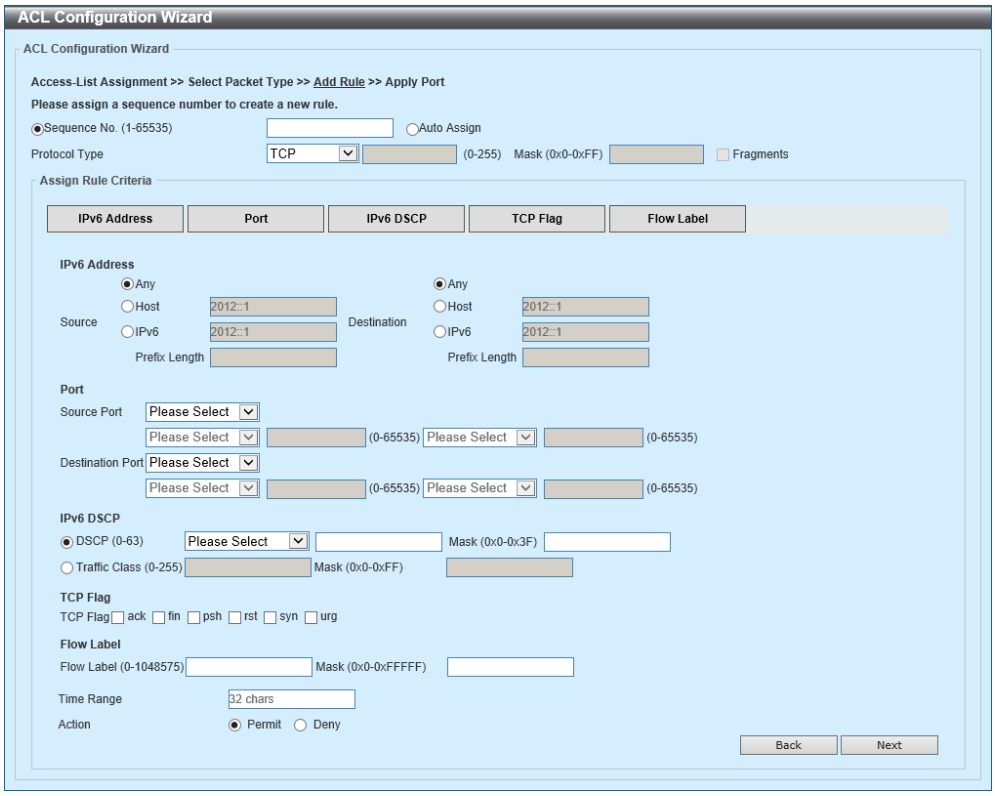


Figure 8-10 ACL Configuration Wizard (Configure Extended IPv6 ACL)

The following parameters can be configured:

Parameter	Description
Sequence No.	Enter the ACL rule number here. The range is from 1 to 65535. Select **Auto Assign** to generate an ACL rule number automatically 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. • **Mask** - After selecting the Protocol ID option, manually enter the protocol mask value here. The range is from 0x0 to 0xFF. • **Fragments** - Select this option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are: • **Any** - Specifies that any source traffic will be evaluated according to the conditions of this rule. • **Host** - Specifies to use and enter the source host IPv6 address here. • **IPv6** - Specifies to use and 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** - Specifies that any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Specifies to use and enter the destination host IPv6 address here. • **IPv6** - Specifies to use and enter the destination IPv6 address and **Prefix Length** value in the spaces provided.

Parameter	Description
Source Port	Select and enter the source port value here. Options to choose from are: • **=** - The ACL will use the port number specified only. • **>** - The ACL will use all ports greater than the port number specified. • **<** - The ACL will use all ports smaller than the port number specified. • ≠ - The ACL will use all ports except the port number specified. • **Range** - The ACL will use the ports specified within the range. • **Mask** - The ACL will use the ports within the range of the mask specified. Enter the port mask value in the space provided. The range is from 0x0 to 0xFFFF. This parameter is only available when **TCP** or **UDP** is selected as the **Protocol Type**.
Destination Port	Select and enter the destination port value here. Options to choose from are: • **=** - The ACL will use the port number specified only. • **>** - The ACL will use all ports greater than the port number specified. • **<** - The ACL will use all ports smaller than the port number specified. • ≠ - The ACL will use all ports except the port number specified. • **Range** - The ACL will use the ports specified within the range. • **Mask** - The ACL will use the ports within the range of the mask specified. Enter the port mask value in the space provided. The range is from 0x0 to 0xFFFF. This parameter is only available when **TCP** or **UDP** is selected as the **Protocol Type**.
Specify ICMP Message Type	Select the ICMP message type used here. This parameter is only available when **ICMP** is selected as the **Protocol Type**.
ICMP Message Type	When the **ICMP Message Type** is not specified, 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 when **ICMP** is selected as the **Protocol Type**.

Parameter	Description
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 when **ICMP** is selected as the **Protocol Type**.
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. • **Mask** - Enter the DSCP mask value here. The range is from 0x0 to 0x3F.
Traffic Class	Select and enter the traffic class value here. The range is from 0 to 255. • **Mask** - Enter the traffic class mask value here. The range is from 0x0 to 0xFF.
TCP Flag	Select the TCP flag that will be evaluated in this ACL here. Options to choose from are **ack**, **fin**, **psh**, **rst**, **syn**, and **urg**. This parameter is only available when **TCP** is selected as the **Protocol Type**.
Flow Label	Enter the flow label value here. The range is from 0 to 1048575. • **Mask** - Enter the flow label mask here. The range is from 0x0 to 0xFFFFF.
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 **Next** button to proceed to the next step in the wizard.
Click the **Back** button to return to the previous step in the wizard.

After clicking the **Next** button (in the previous step), the following window will be displayed:

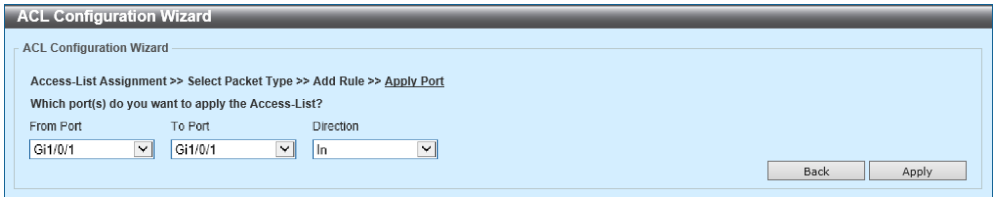


Figure 8-11 ACL Configuration Wizard (IPv6, Step 3)

The following parameters can be configured:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Direction	Select the direction here. Options to choose from are In and Out.

Click the **Apply** button to accept the changes made and return to the ACL Configuration Wizard window.
Click the **Back** button to return to the previous step in the wizard.

8.2 ACL Access List

This window is used to configure and display the ACLs, ACL rules and settings.

Click **ACL > ACL Access List** to view the following window:

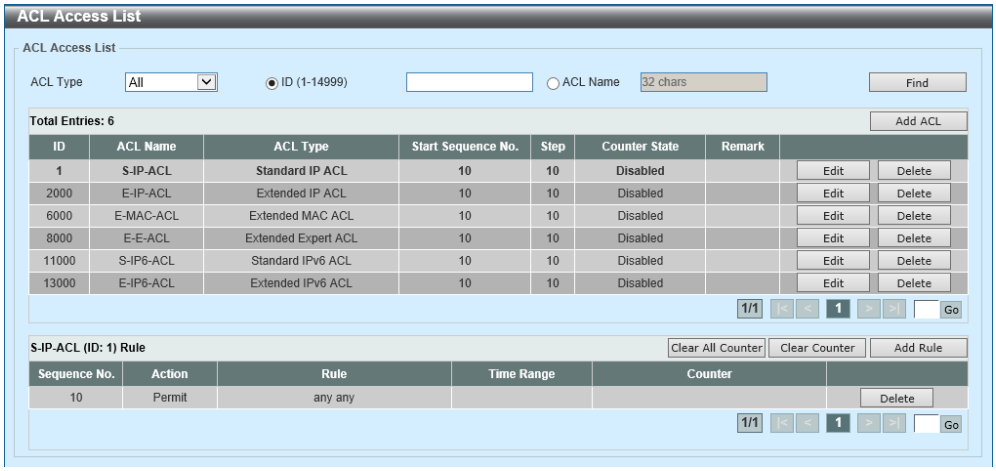


Figure 8-12 ACL Access List

The following parameters can be configured in the **ACL Access List** section:

Parameter	Description
ACL Type	Select the ACL type to find here. Options to choose from are **All**, **IP ACL**, **IPv6 ACL**, **MAC ACL**, and **Expert 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 find and display entries based on the search criteria specified.
Click the **Add ACL** button to add a new ACL profile entry.
Click the **Edit** button to edit the settings of the specified entry.
Click the **Delete** button to delete the specified entry.
Click the **Clear All Counter** button to clear all the counter information.
Click the **Clear Counter** button to clear the counter information related to the selected ACL profile.
Click the **Add Rule** button to add a new ACL rule entry for the selected ACL profile.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click **Edit** button to view the following window:

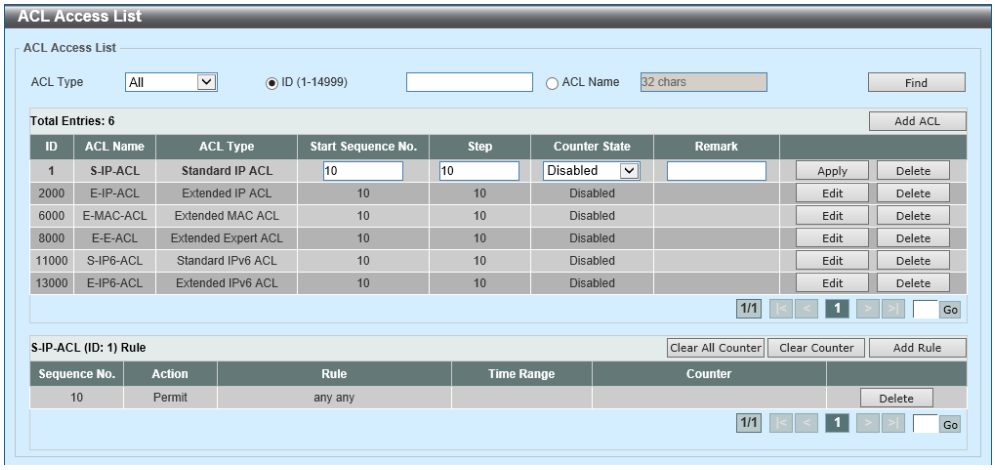


Figure 8-13 ACL Access List (Edit)

The following parameters can be configured in the **ACL Access List** section:

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.

8.2.1 Standard IP ACL

Click the **Add ACL** button (in the **ACL Access List** window) to view the following window:

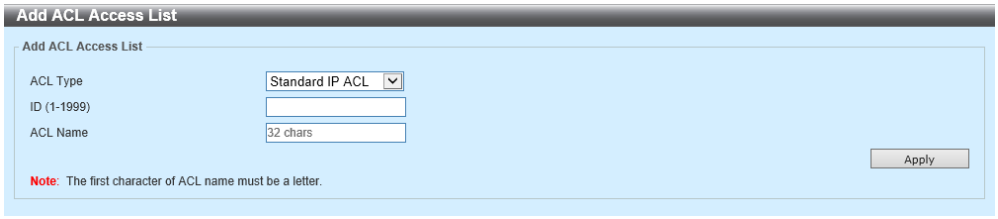


Figure 8-14 ACL Access List (Add ACL, Standard IP ACL)

The following parameters can be configured in the **Add ACL Access List** section:

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**, **Extended MAC ACL**, and **Extended Expert ACL**. This section discusses how the **Standard IP ACL**.
ID	Enter the ID for the Standard IP ACL here. The range is from 1 to 1999.
ACL Name	Enter the name of the ACL here. This name can be up to 32 characters long.

Click the **Apply** button to add the new ACL profile.

Select a **Standard IP ACL** profile and click the **Add Rule** button (in the **ACL Access List** window) to view the following window:

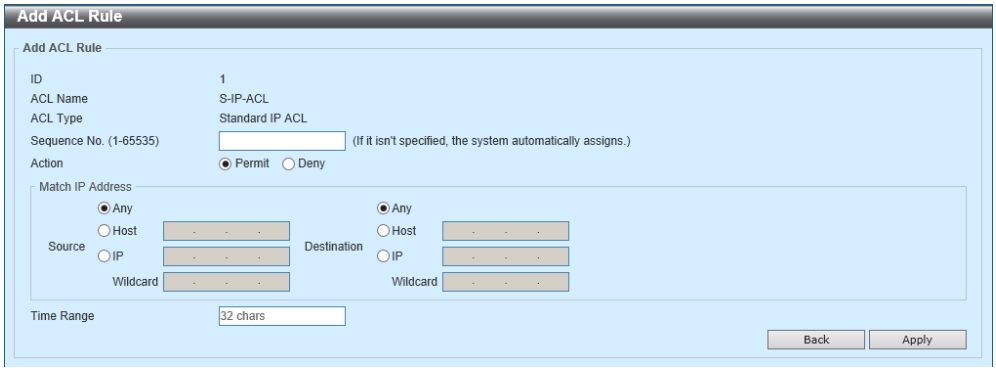


Figure 8-15 ACL Access List (Add Rule, Standard IP ACL)

The following parameters can be configured in the **Add ACL Rule** section:

Parameter	Description
Sequence No.	Enter the ACL rule number here. The range is from 1 to 65535. This number will be generated automatically if not specified.
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** - Specifies that any source traffic will be evaluated according to the conditions of this rule. • **Host** - Specifies to use and enter a source host IP address here. • **IP** - Specifies to use and enter a 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** - Specifies that any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Specifies to use and enter a destination host IP address here. • **IP** - Specifies to use and enter a 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.
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 add the new ACL rule.
Click the **Back** button to return to ACL Access List window.

8.2.2 Extended IP ACL

Click the **Add ACL** button (in the **ACL Access List** window) to view the following window:

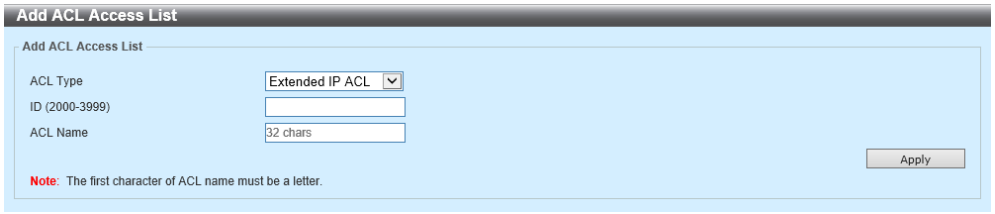


Figure 8-16 ACL Access List (Add ACL, Extended IP ACL)

The following parameters can be configured in the **Add ACL Access List** section:

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**, **Extended MAC ACL**, and **Extended Expert ACL**. This section discusses how the **Extended IP ACL**.
ID	Enter the ID for the Extended IP ACL here. The range is from 2000 to 3999.
ACL Name	Enter the name of the ACL here. This name can be up to 32 characters long.

Click the **Apply** button to add the new ACL profile.

Select an **Extended IP ACL** profile and click the **Add Rule** button (in the **ACL Access List** window) to view the following window:

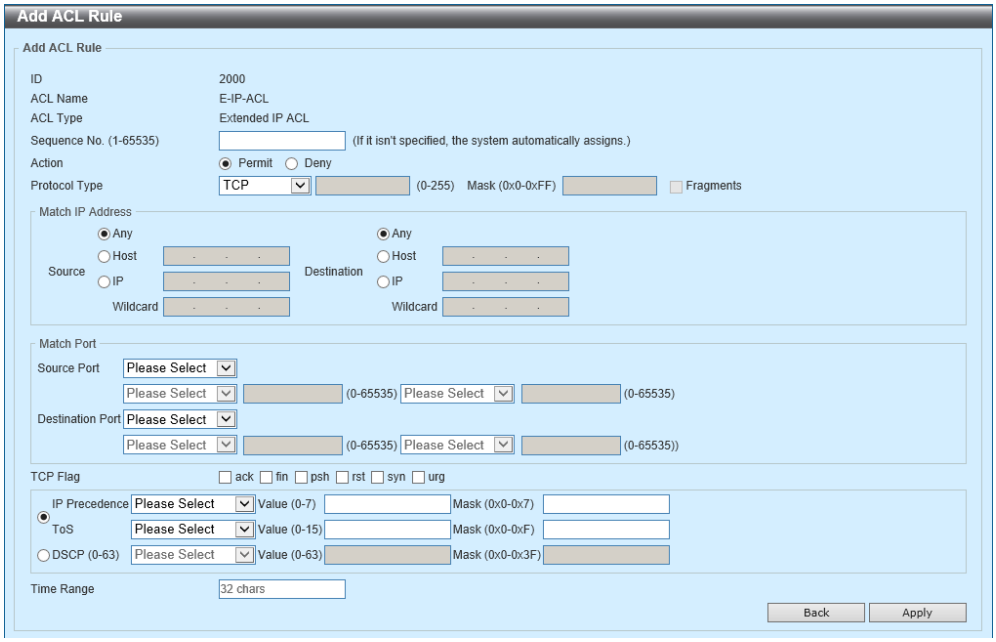


Figure 8-17 ACL Access List (Add Rule, Extended IP ACL)

The following parameters can be configured in the **Add ACL Rule** section:

Parameter	Description
Sequence No.	Enter the ACL rule number here. The range is from 1 to 65535. This number will be generated automatically if not specified.
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. • **Mask** - After selecting the Protocol ID option, manually enter the protocol mask value here. The range is from 0x0 to 0xFF. • **Fragments** - Select this option to include packet fragment filtering.

Parameter	Description
Source	Select and enter the source information here. Options to choose from are: • **Any** - Specifies that any source traffic will be evaluated according to the conditions of this rule. • **Host** - Specifies to use and enter a source host IP address here. • **IP** - Specifies to use and enter a 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** - Specifies that any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Specifies to use and enter a destination host IP address here. • **IP** - Specifies to use and enter a 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: • **=** - The ACL will use the port number specified only. • **>** - The ACL will use all ports greater than the port number specified. • **<** - The ACL will use all ports smaller than the port number specified. • ≠ - The ACL will use all ports except the port number specified. • **Range** - The ACL will use the ports specified within the range. • **Mask** - The ACL will use the ports within the range of the mask specified. Enter the port mask value in the space provided. The range is from 0x0 to 0xFFFF. This parameter is only available when **TCP** or **UDP** is selected as the **Protocol Type**.

Parameter	Description
Destination Port	Select and enter the destination port value here. Options to choose from are: • **=** - The ACL will use the port number specified only. • **>** - The ACL will use all ports greater than the port number specified. • **<** - The ACL will use all ports smaller than the port number specified. • ≠ - The ACL will use all ports except the port number specified. • **Range** - The ACL will use the ports specified within the range. • **Mask** - The ACL will use the ports within the range of the mask specified. Enter the port mask value in the space provided. The range is from 0x0 to 0xFFFF. This parameter is only available when **TCP** or **UDP** is selected as the **Protocol Type**.
TCP Flag	Select the TCP flag that will be evaluated in this ACL here. Options to choose from are **ack**, **fin**, **psh**, **rst**, **syn**, and **urg**. This parameter is only available when **TCP** is selected as the **Protocol Type**.
Specify ICMP Message Type	Select the ICMP message type used here. This parameter is only available when **ICMP** is selected as the **Protocol Type**.
ICMP Message Type	When the **ICMP Message Type** is not specified, 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 when **ICMP** is selected as the **Protocol Type**.
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 when **ICMP** is selected as the **Protocol Type**.
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. • **Mask** - Enter the IP precedence mask value here. The range is from 0x0 to 0x7.

Parameter	Description
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. • **Mask** - Enter the ToS mask value here. The range is from 0x0 to 0xF.
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. • **Mask** - Enter the DSCP mask value here. The range is from 0x0 to 0x3F.
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 add the new ACL rule.
Click the **Back** button to return to ACL Access List window.

8.2.3 Standard IPv6 ACL

Click the **Add ACL** button (in the **ACL Access List** window) to view the following window:

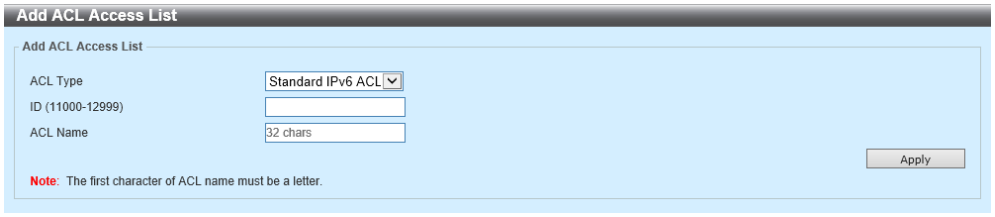


Figure 8-18 ACL Access List (Add ACL, Standard IPv6 ACL)

The following parameters can be configured in the **Add ACL Access List** section:

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**, **Extended MAC ACL**, and **Extended Expert ACL**. This section discusses how the **Standard IPv6 ACL**.
ID	Enter the ID for the Standard IPv6 ACL here. The range is from 11000 to 12999.
ACL Name	Enter the name of the ACL here. This name can be up to 32 characters long.

Click the **Apply** button to add the new ACL profile.

Select a **Standard IPv6 ACL** profile and click the **Add Rule** button (in the **ACL Access List** window) to view the following window:

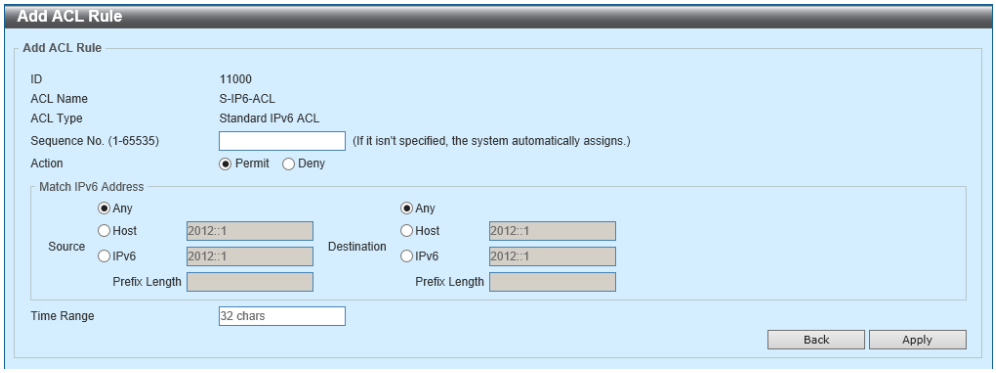


Figure 8-19 ACL Access List (Add Rule, Standard IPv6 ACL)

The following parameters can be configured in the **Add ACL Rule** section:

Parameter	Description
Sequence No.	Enter the ACL rule number here. The range is from 1 to 65535. This number will be generated automatically if not specified.
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** - Specifies that any source traffic will be evaluated according to the conditions of this rule. • **Host** - Specifies to use and enter the source host IPv6 address here. • **IPv6** - Specifies to use and 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** - Specifies that any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Specifies to use and enter the destination host IPv6 address here. • **IPv6** - Specifies to use and 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 add the new ACL rule.
Click the **Back** button to return to ACL Access List window.

8.2.4 Extended IPv6 ACL

Click the **Add ACL** button (in the **ACL Access List** window) to view the following window:

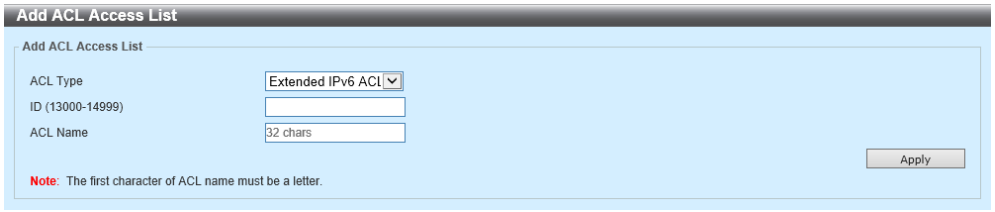


Figure 8-20 ACL Access List (Add ACL, Extended IPv6 ACL)

The following parameters can be configured in the **Add ACL Access List** section:

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**, **Extended MAC ACL**, and **Extended Expert ACL**. This section discusses how the **Extended IPv6 ACL**.
ID	Enter the ID for the Extended IPv6 ACL here. The range is from 13000 to 14999.
ACL Name	Enter the name of the ACL here. This name can be up to 32 characters long.

Click the **Apply** button to add the new ACL profile.

Select an **Extended IPv6 ACL** profile and click the **Add Rule** button (in the **ACL Access List** window) to view the following window:

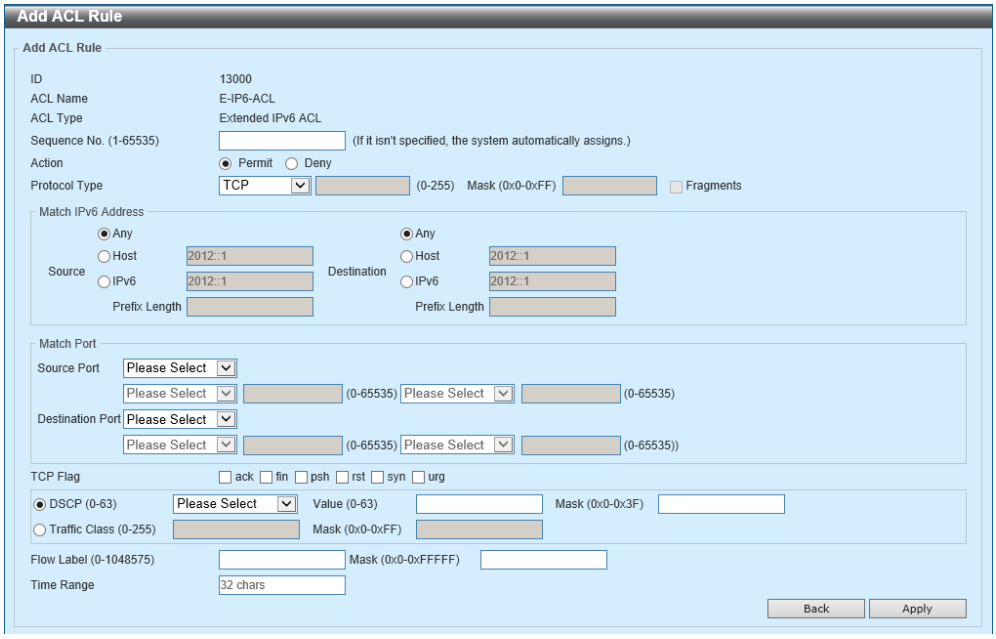


Figure 8-21 ACL Access List (Add Rule, Extended IPv6 ACL)

The following parameters can be configured in the **Add ACL Rule** section:

Parameter	Description
Sequence No.	Enter the ACL rule number here. The range is from 1 to 65535. This number will be generated automatically if not specified.
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. • **Mask** - After selecting the Protocol ID option, manually enter the protocol mask value here. The range is from 0x0 to 0xFF. • **Fragments** - Select this option to include packet fragment filtering.

Parameter	Description
Source	Select and enter the source information here. Options to choose from are: • **Any** - Specifies that any source traffic will be evaluated according to the conditions of this rule. • **Host** - Specifies to use and enter the source host IPv6 address here. • **IPv6** - Specifies to use and 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** - Specifies that any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Specifies to use and enter the destination host IPv6 address here. • **IPv6** - Specifies to use and 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: • **=** - The ACL will use the port number specified only. • **>** - The ACL will use all ports greater than the port number specified. • **<** - The ACL will use all ports smaller than the port number specified. • ≠ - The ACL will use all ports except the port number specified. • **Range** - The ACL will use the ports specified within the range. • **Mask** - The ACL will use the ports within the range of the mask specified. Enter the port mask value in the space provided. The range is from 0x0 to 0xFFFF. This parameter is only available when **TCP** or **UDP** is selected as the **Protocol Type**.

Parameter	Description
Destination Port	Select and enter the destination port value here. Options to choose from are: • **=** - The ACL will use the port number specified only. • **>** - The ACL will use all ports greater than the port number specified. • **<** - The ACL will use all ports smaller than the port number specified. • ≠ - The ACL will use all ports except the port number specified. • **Range** - The ACL will use the ports specified within the range. • **Mask** - The ACL will use the ports within the range of the mask specified. Enter the port mask value in the space provided. The range is from 0x0 to 0xFFFF. This parameter is only available when **TCP** or **UDP** is selected as the **Protocol Type**.
TCP Flag	Select the TCP flag that will be evaluated in this ACL here. Options to choose from are **ack**, **fin**, **psh**, **rst**, **syn**, and **urg**. This parameter is only available when **TCP** is selected as the **Protocol Type**.
Specify ICMP Message Type	Select the ICMP message type used here. This parameter is only available when **ICMP** is selected as the **Protocol Type**.
ICMP Message Type	When the **ICMP Message Type** is not specified, 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 when **ICMP** is selected as the **Protocol Type**.
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 when **ICMP** is selected as the **Protocol Type**.

Parameter	Description
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. • **Mask** - Enter the DSCP mask value here. The range is from 0x0 to 0x3F.
Traffic Class	Select and enter the traffic class value here. The range is from 0 to 255. • **Mask** - Enter the traffic class mask value here. The range is from 0x0 to 0xFF.
Flow Label	Enter the flow label value here. The range is from 0 to 1048575. • **Mask** - Enter the flow label mask here. The range is from 0x0 to 0xFFFFF.
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 add the new ACL rule.
Click the **Back** button to return to ACL Access List window.

8.2.5 Extended MAC ACL

Click the **Add ACL** button (in the **ACL Access List** window) to view the following window:

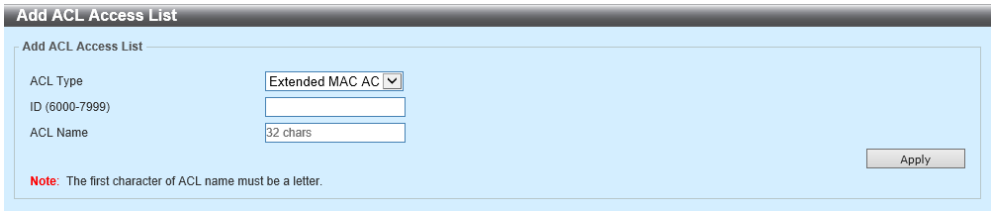


Figure 8-22 ACL Access List (Add ACL, Extended MAC ACL)

The following parameters can be configured in the **Add ACL Access List** section:

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**, **Extended MAC ACL**, and **Extended Expert ACL**. This section discusses how the **Extended MAC ACL.**
ID	Enter the ID for the Extended MAC ACL here. The range is from 6 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 add the new ACL profile.

Select an **Extended MAC ACL** profile and click the **Add Rule** button (in the **ACL Access List** window) to view the following window:

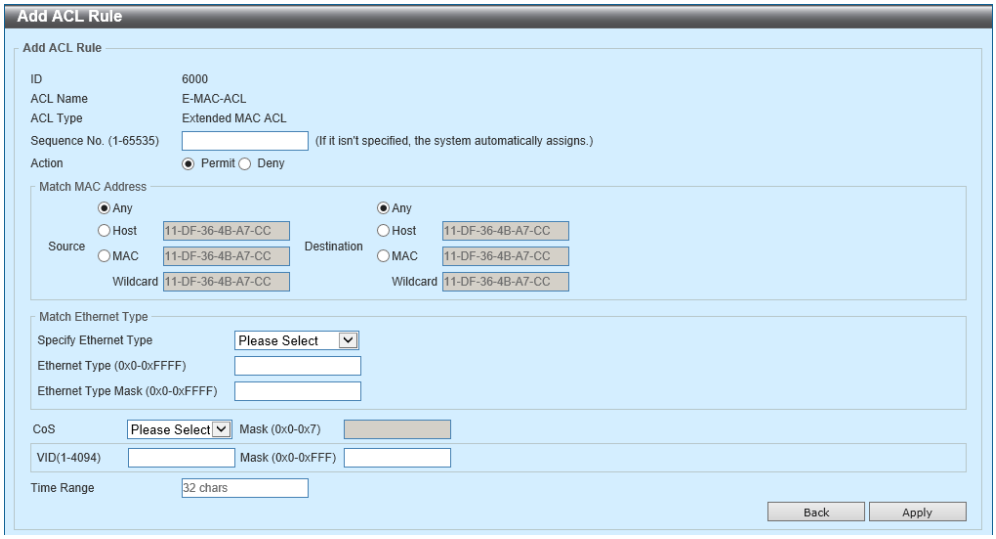


Figure 8-23 ACL Access List (Add Rule, Extended MAC ACL)

The following parameters can be configured in the **Add ACL Rule** section:

Parameter	Description
Sequence No.	Enter the ACL rule number here. The range is from 1 to 65535. This number will be generated automatically if not specified.
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** - Specifies that any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host MAC address here. • **MAC** - 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** - Specifies that any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host MAC address here. • **MAC** - 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. The range is from 0x600 to 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. The range is from 0x0 to 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. • **Mask** - Enter the CoS mask value here. The range is from 0x0 to 0x7.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094. • **Mask** - Enter the VLAN ID mask value here. The range is from 0x0 to 0xFFF.

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 add the new ACL rule.
Click the **Back** button to return to ACL Access List window.

8.2.6 Extended Expert ACL

Click the **Add ACL** button (in the **ACL Access List** window) to view the following window:

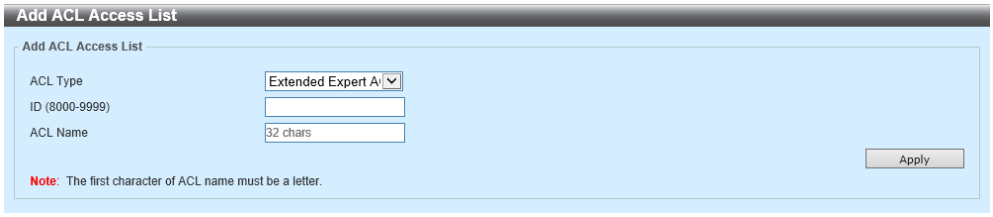


Figure 8-24 ACL Access List (Add ACL, Extended Expert ACL)

The following parameters can be configured in the **Add ACL Access List** section:

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**, **Extended MAC ACL**, and **Extended Expert ACL**. This section discusses how the **Extended Expert ACL**.
ID	Enter the ID for the Extended Expert ACL here. The range is from 8000 to 9999.
ACL Name	Enter the name of the ACL here. This name can be up to 32 characters long.

Click the **Apply** button to add the new ACL profile.

Select an **Extended Expert ACL** profile and click the **Add Rule** button (in the **ACL Access List** window) to view the following window:

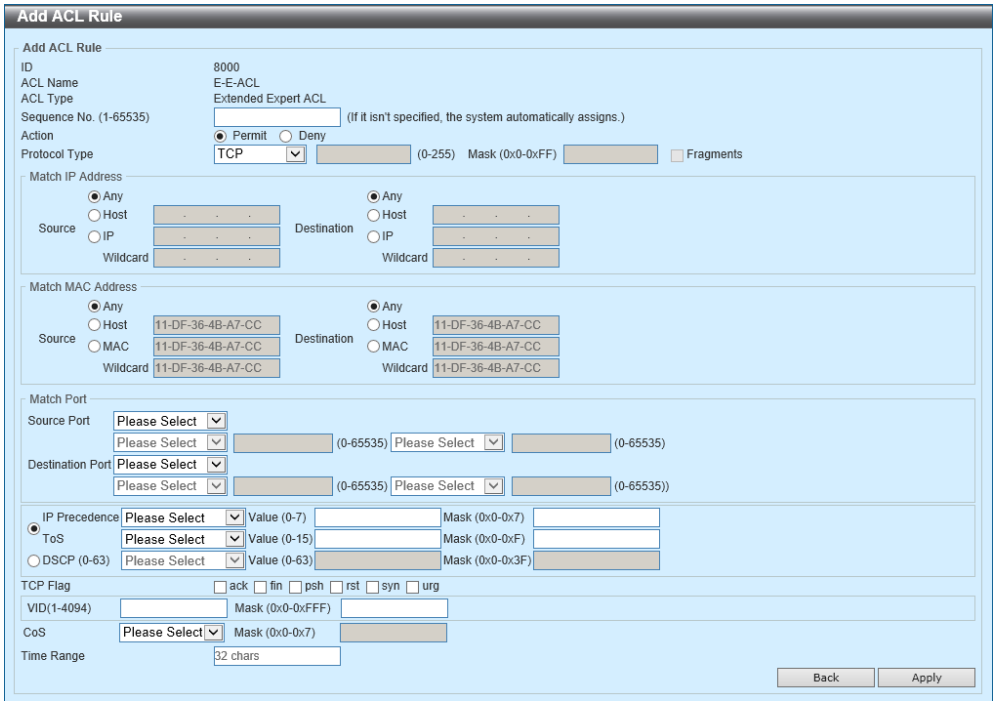


Figure 8-25 ACL Access List (Add Rule, Extended Expert ACL)

The following parameters can be configured in the **Add ACL Rule** section:

Parameter	Description
Sequence No.	Enter the ACL rule number here. The range is from 1 to 65535. This number will be generated automatically if not specified.
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. • **Mask** - After selecting the Protocol ID option, manually enter the protocol mask value here. The range is from 0x0 to 0xFF. • **Fragments** - Select this option to include packet fragment filtering.

Parameter	Description
Source (IP Address)	Select and enter the source information here. Options to choose from are: • **Any** - Specifies that any source traffic will be evaluated according to the conditions of this rule. • **Host** - Specifies to use and enter a source host IP address here. • **IP** - Specifies to use and enter a 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 (IP Address)	Select and enter the destination information here. Options to choose from are: • **Any** - Specifies that any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Specifies to use and enter a destination host IP address here. • **IP** - Specifies to use and enter a 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 (MAC Address)	Select and enter the source MAC address information here. Options to choose from are: • **Any** - Specifies that any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host MAC address here. • **MAC** - Enter the source MAC address and **Wildcard** value in the spaces provided.
Destination (MAC Address)	Select and enter the destination MAC address information here. Options to choose from are: • **Any** - Specifies that any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host MAC address here. • **MAC** - Enter the destination MAC address and **Wildcard** value in the spaces provided.

Parameter	Description
Source Port	Select and enter the source port value here. Options to choose from are: • **=** - The ACL will use the port number specified only. • **>** - The ACL will use all ports greater than the port number specified. • **<** - The ACL will use all ports smaller than the port number specified. • ≠ - The ACL will use all ports except the port number specified. • **Range** - The ACL will use the ports specified within the range. • **Mask** - The ACL will use the ports within the range of the mask specified. Enter the port mask value in the space provided. The range is from 0x0 to 0xFFFF. This parameter is only available when **TCP** or **UDP** is selected as the **Protocol Type**.
Destination Port	Select and enter the destination port value here. Options to choose from are: • **=** - The ACL will use the port number specified only. • **>** - The ACL will use all ports greater than the port number specified. • **<** - The ACL will use all ports smaller than the port number specified. • ≠ - The ACL will use all ports except the port number specified. • **Range** - The ACL will use the ports specified within the range. • **Mask** - The ACL will use the ports within the range of the mask specified. Enter the port mask value in the space provided. The range is from 0x0 to 0xFFFF. This parameter is only available when **TCP** or **UDP** is selected as the **Protocol Type**.
Specify ICMP Message Type	Select the ICMP message type used here. This parameter is only available when **ICMP** is selected as the **Protocol Type**.
ICMP Message Type	When the **ICMP Message Type** is not specified, 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 when **ICMP** is selected as the **Protocol Type**.

Parameter	Description
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 when **ICMP** is selected as the **Protocol Type**.
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. • **Mask** - Enter the IP precedence mask value here. The range is from 0x0 to 0x7.
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. • **Mask** - Enter the ToS mask value here. The range is from 0x0 to 0xF.
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. • **Mask** - Enter the DSCP mask value here. The range is from 0x0 to 0x3F.
TCP Flag	Select the TCP flag that will be evaluated in this ACL here. Options to choose from are **ack**, **fin**, **psh**, **rst**, **syn**, and **urg**. This parameter is only available when **TCP** is selected as the **Protocol Type**.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094. • **Mask** - Enter the VLAN ID mask value here. The range is from 0x0 to 0xFFF.

Parameter	Description
CoS	Select the CoS value that will be used here. The range is from 0 to 7. • **Mask** - Enter the CoS mask value here. The range is from 0x0 to 0x7.
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 add the new ACL rule.
Click the **Back** button to return to ACL Access List window.

8.3 ACL Interface Access Group

This window is used to configure and display the ACL access group settings on the specified port(s).

Click **ACL > ACL Interface Access Group** to view the following window:

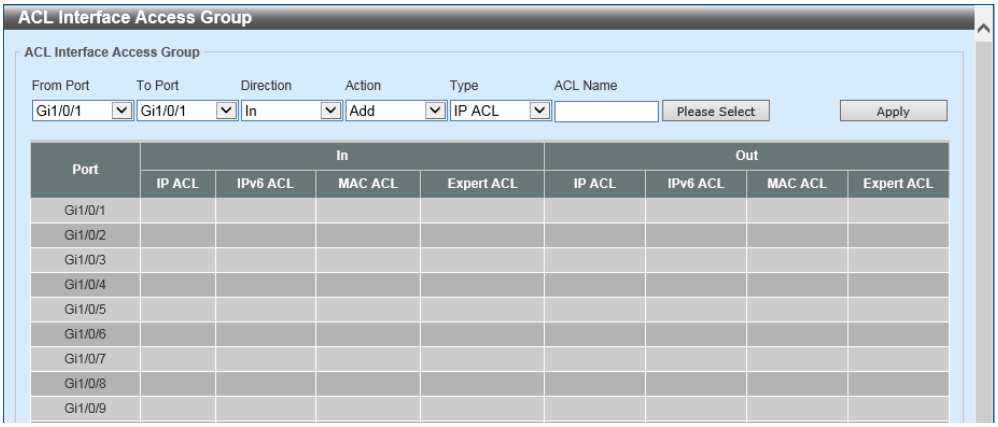


Figure 8-26 ACL Interface Access Group

The following parameters can be configured in the **ACL Interface Access Group** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Direction	Select the direction here. Options to choose from are **In** and **Out**.
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**, **MAC ACL**, and **Expert 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.
Click the **Please Select** button to display the configured access control lists that can be used in this window.

Click the **Please Select** button to view the following window:

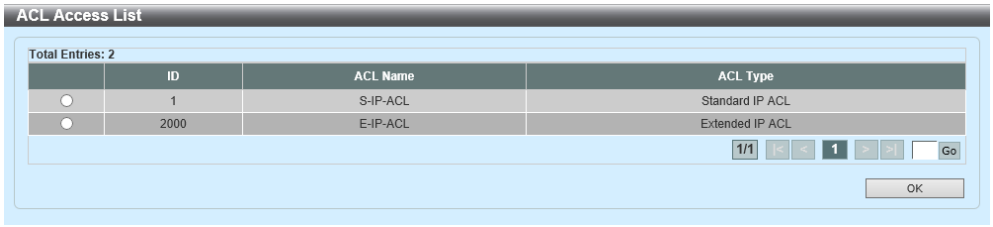


Figure 8-27 ACL Interface Access Group (Please Select)

Click the **OK** button to use the selected access control list.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

8.4 ACL VLAN Access Map

This window is used to configure and display the ACL VLAN access map settings.

Click **ACL > ACL VLAN Access Map** to view the following window:

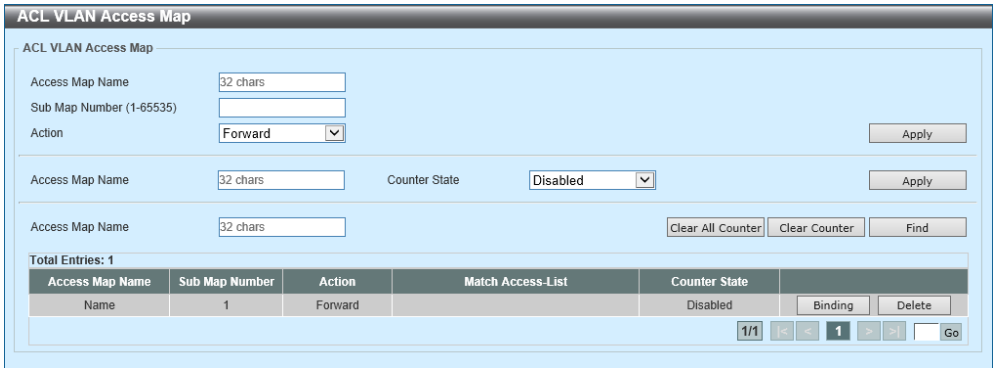


Figure 8-28 ACL VLAN Access Map

The following parameters can be configured in the **ACL VLAN Access Map** section:

Parameter	Description
Access Map Name	Enter the access map name here. This name can be up to 32 characters long.
Sub Map Number	Enter the sub-map number here. The range is from 1 to 65535.
Action	Select the action that will be taken here. Options to choose from are **Forward**, **Drop**, and **Redirect**. When the **Redirect** option is selected, select the redirected interface from the drop-down list.
Counter State	Select whether to enable or disable the counter state.

Click the **Apply** button to add a new entry.
Click the **Clear All Counter** button to clear all the counter information.
Click the **Clear Counter** button to clear the counter information related to the specified access map.
Click the **Find** button to find and display entries based on the search criteria specified.
Click the Binding button to configure the binding settings for the specified 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.

Click the **Binding** button to view the following window:

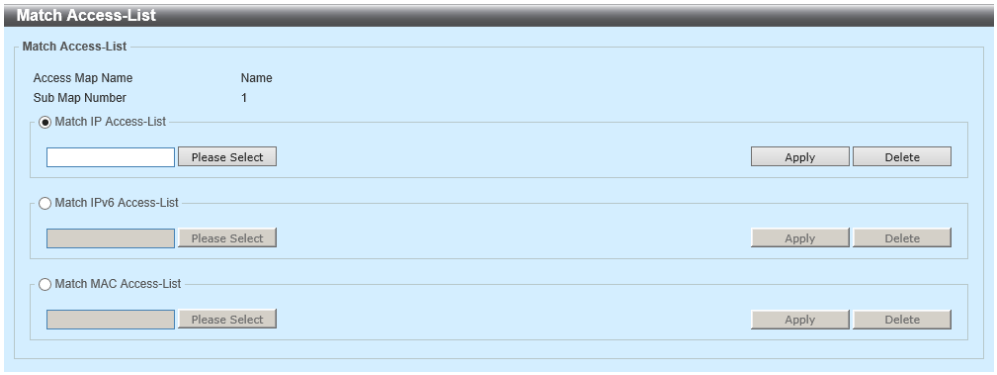


Figure 8-29 ACL VLAN Access Map (Binding)

The following parameters can be configured in the **Match Access List** section:

Parameter	Description
Match IP Access-List	Here the IP access list that will be matched will be displayed.
Match IPv6 Access-List	Here the IPv6 access list that will be matched will be displayed.
Match MAC Access-List	Here the MAC access list that will be matched will be displayed.

Click the **Please Select** button to display the configured access control lists that can be used in this window.
Click the **Apply** button to accept the changes made.
Click the **Delete** button to delete the specified binding.

Click the **Please Select** button to view the following window:

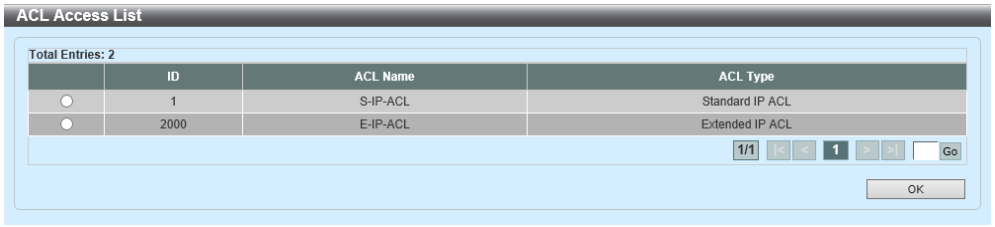


Figure 8-30 ACL VLAN Access Map (Binding, Please Select)

Click the **OK** button to use the selected access control list.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

8.5 ACL VLAN Filter

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

Click **ACL > ACL VLAN Filter** to view the following window:

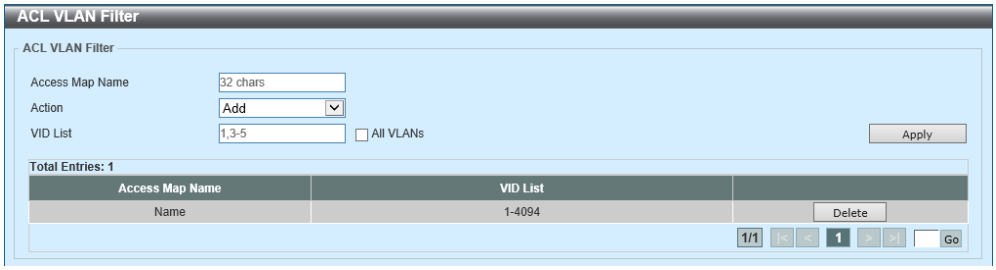


Figure 8-31 ACL VLAN Filter

The following parameters can be configured in the **ACL VLAN Filter** section:

Parameter	Description
Access Map Name	Enter the access map name here. This name can be up to 32 characters long.
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**.
VID List	Enter the VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094. Select the **All VLANs** option to apply this configuration to all the VLANs configured on this Switch.

Click the **Apply** button to add a new 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.

9 Security

9.1 Port Security

9.1.1 Port Security Global Settings

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

Click **Security > Port Security > Port Security Global Settings** to view the following window:

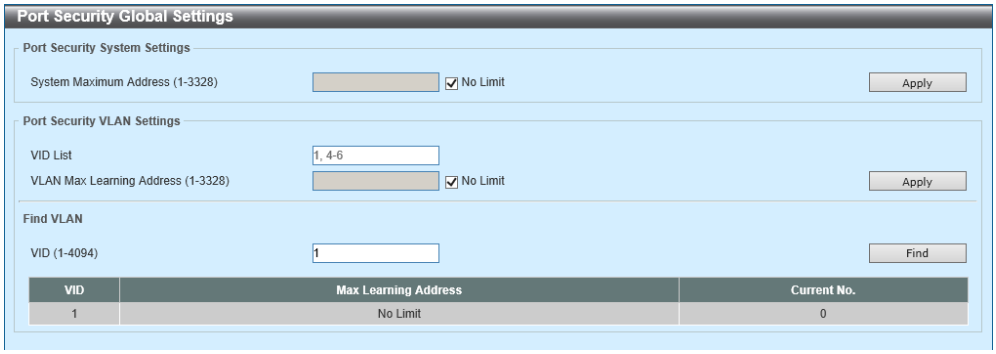


Figure 9-1 Port Security Global Settings

The following parameters can be configured in the **Port Security System Settings** section:

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. Select **No Limit** to allow the maximum number of secure MAC address.

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

The following parameters can be configured in the **Port Security VLAN Settings** section:

Parameter	Description
VID List	Enter the VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.
VLAN Max Learning Address	Enter the maximum number of allowed MAC addresses that can be learned on the specified VLAN(s) here. The range is from 1 to 3328. Select **No Limit** to allow the maximum number of secure MAC address.

Click the **Apply** button to add a new entry based on the information specified.

The following parameters can be configured in the **Find VLAN** section:

Parameter	Description
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

Click the **Find** button to find and display entries based on the search criteria specified.

9.1.2 Port Security Port Settings

This window is used to configure and display the port security settings on the specified port(s).

Click **Security > Port Security > Port Security Port Settings** to view the following window:

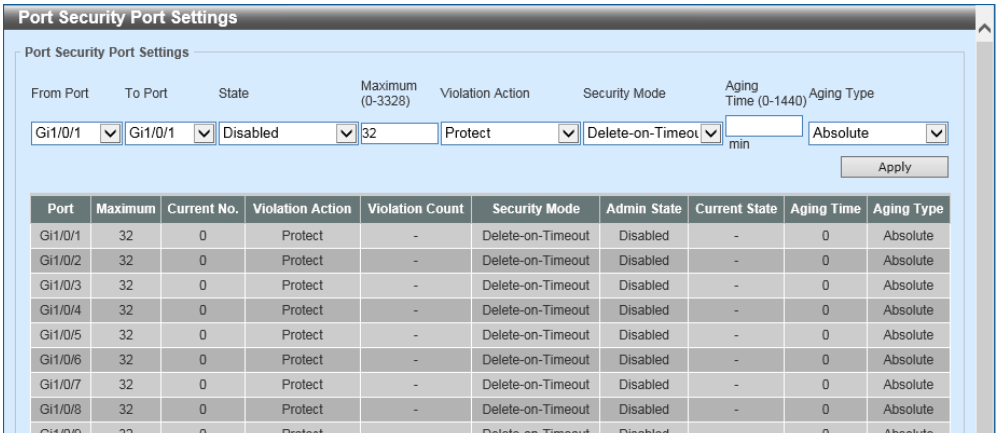


Figure 9-2 Port Security Port Settings

The following parameters can be configured in the **Port Security Port Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used 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. The range is from 0 to 3328. 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 insecure hosts at the port-security process level, but does not increment the security-violation count. • **Restrict** - Specifies to drop all packets from 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.

Parameter	Description
Security Mode	Select the security mode option here. Options to choose from are: • **Permanent** - Specifies that all learned MAC addresses will not be purged out unless the user manually deletes those entries. • **Delete-on-Timeout** - Specifies that all learned MAC addresses will 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. The range is from 0 to 1440 minutes.
Aging Type	Select the aging type here. Options to choose from are: • **Absolute** - Specifies that all secure addresses on this port will age out, exactly after the time specified, and is removed from the secure address list. This is the default type. • **Inactivity** - Specifies that the secure addresses on this port age out only if there is no data traffic from the secure source address for the specified period.

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

9.1.3 Port Security Address Entries

This window is used to configure and display the MAC address entries for port security.

Click **Security > Port Security > Port Security Address Entries** to view the following window:

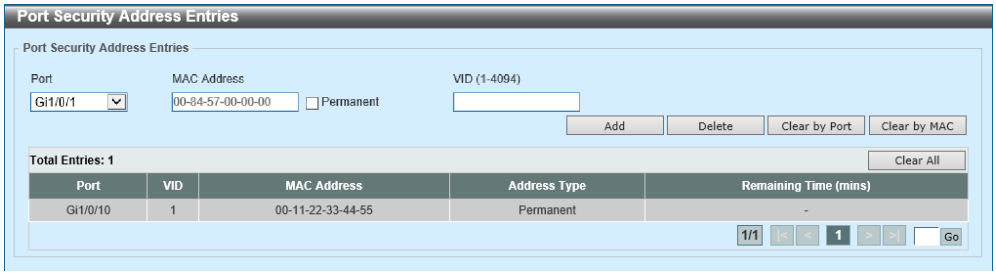


Figure 9-3 Port Security Address Entries

The following parameters can be configured in the **Port Security Address Entries** section:

Parameter	Description
Port	Select the port that will be used here.
MAC Address	Enter the MAC address here. Select the **Permanent** option to specify that all learned MAC addresses will not be purged out unless the user manually deletes those entries.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.

Click the **Add** button to add a new entry.
Click the **Delete** button to delete the specified entry.
Click the **Clear by Port** button to remove all the MAC addresses secured to the specified ports.
Click the **Clear by MAC** button to remove the specified MAC address secured to any of the ports.
Click the **Clear All** button to remove all the MAC addresses secured to ports.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

9.2 802.1X

9.2.1 802.1X Global Settings

This window is used to configure and display the global IEEE 802.1X settings.

Click **Security > 802.1X > 802.1X Global Settings** to view the following window:

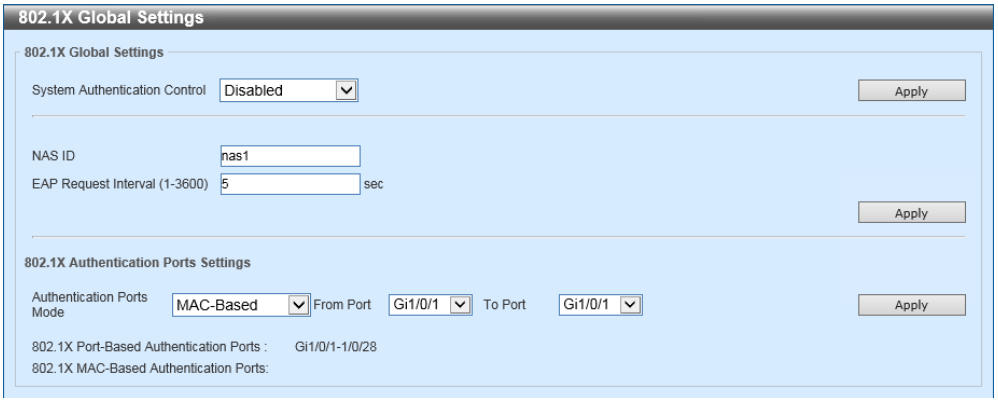


Figure 9-4 802.1X Global Settings

The following parameters can be configured in the **802.1X Global Settings** section:

Parameter	Description
System Authentication Control	Select to enable or disable system authentication control here. This feature will restrict access to unauthorized hosts to the network.
NAS ID	Enter the ID of the Network Access Server (NAS) here.
EAP Request Interval	Enter the Extensible Authentication Protocol (EAP) request interval here. The range is from 1 to 3600 seconds.

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

The following parameters can be configured in the **802.1X Authentication Port Settings** section:

Parameter	Description
Authentication Ports Mode	Select the authentication mode that will be used on the specified port(s) here. Options to choose from are **Port-Based** and **MAC-Based**.
From Port - To Port	Select the port(s) that will be used here.

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

9.2.2 802.1X Forced Authorized MAC Settings

This window is used to configure and display the IEEE 802.1X forced authorized MAC settings.

Click **Security > 802.1X > 802.1X Forced Authorized MAC Settings** to view the following window:

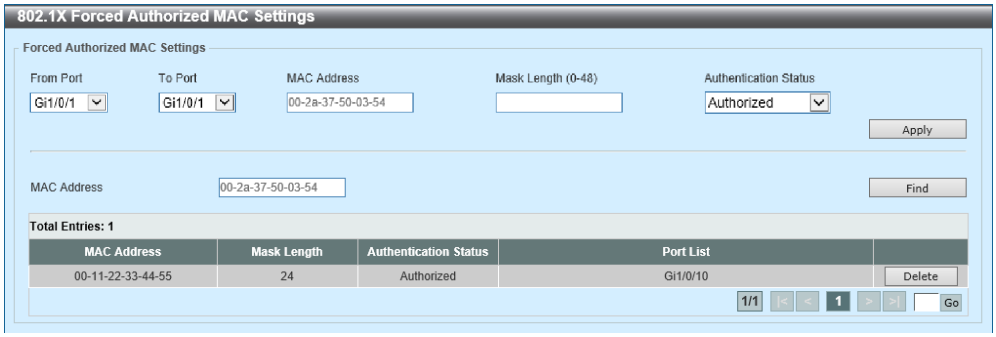


Figure 9-5 802.1X Forced Authorized MAC Settings

The following parameters can be configured in the **Forced Authorized MAC Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
MAC Address	Enter the MAC address of the supplicant here.
Mask Length	Enter the MAC mask bit length here. The range is from 0 to 48.
Authentication Status	Select the authentication status here. Options to choose from are: • **Authorized** - Select this option to force an authorized state. • **Unauthorized** - Select this option to force an unauthorized state.

Click the **Apply** button to add a new entry.
Click the **Find** button to find and display entries based on the search criteria specified.
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.

9.2.3 802.1X Unauthorized MAC Settings

This window is used to configure and display the IEEE 802.1X unauthorized MAC settings.

Click **Security > 802.1X > 802.1X Unauthorized MAC Settings** to view the following window:

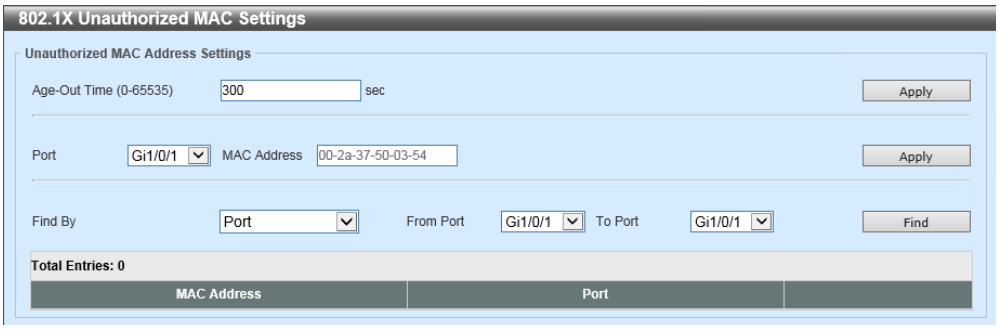


Figure 9-6 802.1X Unauthorized MAC Settings

The following parameters can be configured in the **Unauthorized MAC Address Settings** section:

Parameter	Description
Age-Out Time	Enter the age-out time value here. This time is used in aging out static unauthorized hosts. The range is from 0 to 65535 seconds.
From Port - To Port	Select the port(s) that will be used here.
MAC Address	Enter the MAC address of the unauthorized host here.
Find By MAC	Select this option to find and display configured and dynamic unauthorized hosts, sorted by MAC address.
Find By Port	Select to find and display configured and dynamic unauthorized hosts on the specified port(s). • **From Port / To Port** - Select the port(s) that will be used here.

Click the **Apply** button to accept the changes made.
Click the **Find** button to find and display entries based on the search criteria specified.

9.2.4 802.1X Port Settings

This window is used to configure and display the IEEE 802.1X port-based and MAC-based access control settings on the specified port(s).

Click **Security > 802.1X > 802.1X Port Settings** to view the following window:

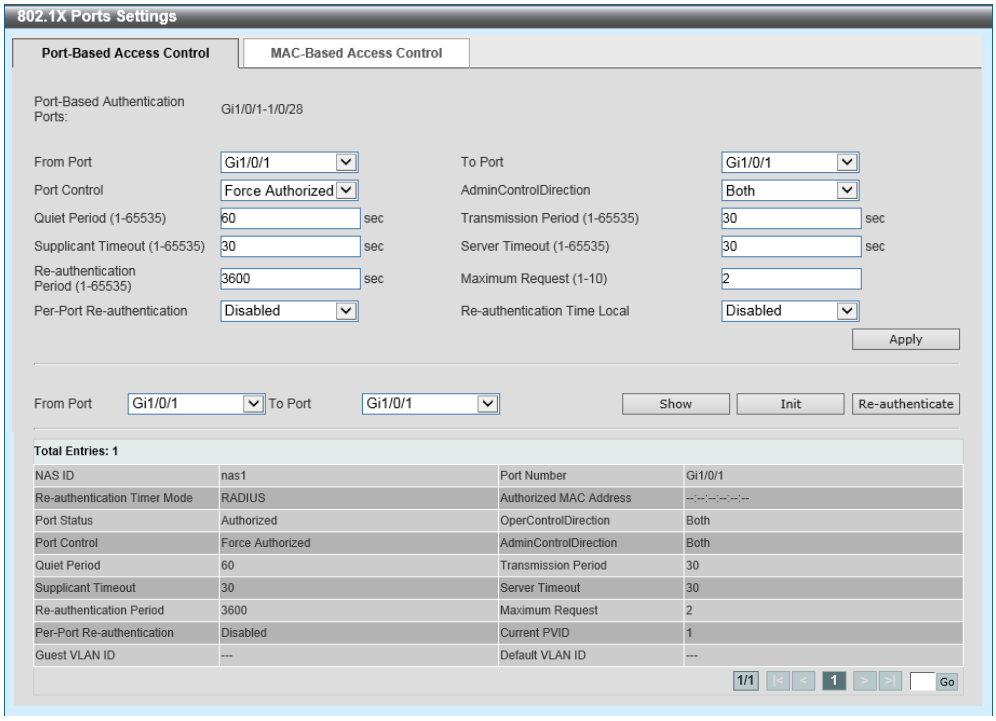


Figure 9-7 802.1X Port Settings (Port-Based Access Control)

The following parameters can be configured in the **Port-Based Access Control** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Port Control	Select the authorization state of the port(s) here. Options to choose from are: • **Auto** - Specifies to enable IEEE 802.1X authentication on the port(s). • **Force Authorized** - Specifies to force an authorized state on the port(s). • **Force Unauthorized** - Specifies to force an unauthorized state on the port(s).

Parameter	Description
Admin Control Direction	Select the control direction of traffic on the port(s) here. Options to choose from are: • **Both** - Specifies to control traffic in a bidirectional direction. • **In** - Specifies to control traffic in an inbound direction only.
Quiet Period	Enter the quiet period here. This is the number or seconds that the switch will remain in the quiet state after a failed authentication process. The range is from 1 to 65535 seconds.
Transmission Period	Enter the transmission period here. This is the number of seconds that the switch will wait for an EAP-request or identity frame from the supplicant before retransmitting the request. The range is from 1 to 65535 seconds.
Supplicant Timeout	Enter the supplicant timeout value here. This is the number of seconds the switch will wait for a response from the supplicant before timing out the supplicant message. This does not apply to the EAP request ID. The range is from 1 to 65535 seconds.
Server Timeout	Enter the server timeout value here. This is the number of seconds the switch will wait for a response from the authentication server before timing out the connection. The range is from 1 to 65535 seconds.
Re-authentication Period	Enter the re-authentication period here. This is the number of seconds between re-authentication attempts. The range is from 1 to 65535 seconds.
Maximum Request	Enter the maximum number of EAP requests that will be allowed from a backend authentication machine here before the authentication process is restarted. The range is from 1 to 10.
Per-Port Re-authentication	Select to enable or disable periodic re-authentication on the port(s) here.
Re-authentication Time Local	Select to enable or disable the use of the local settings for the timer to re-authenticate a session here.

Click the **Apply** button to accept the changes made.
Click the **Show** button to display the port-based access control settings associated to the specified port(s).
Click the **Init** button to initiate the port-based access control settings on the specified port(s).
Click the **Re-authenticate** button to re-authenticate all the connections to the specified port(s).

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

Click the **MAC-Based Access Control** tab to view the following window:

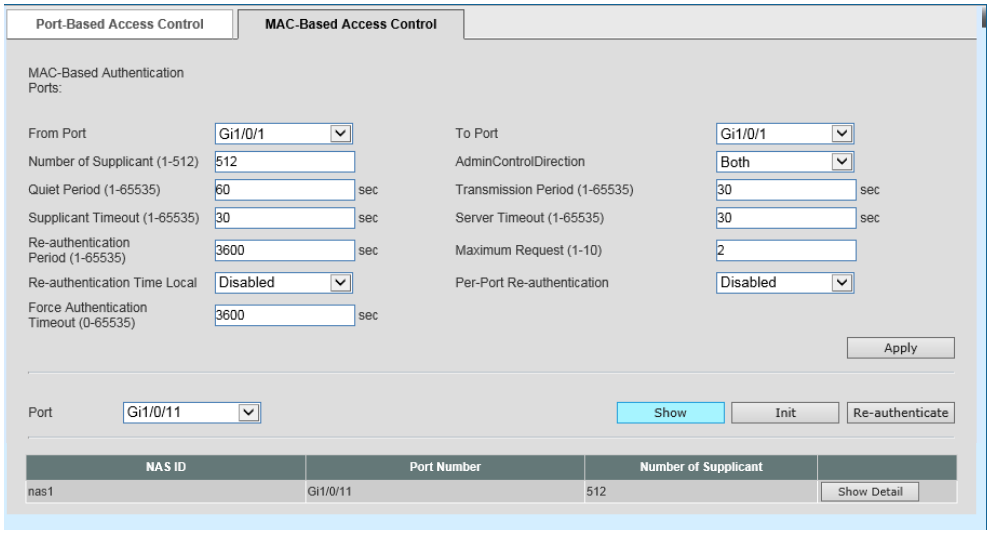


Figure 9-8 802.1X Port Settings (MAC-Based Access Control)

The following parameters can be configured in the **MAC-Based Access Control** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Number of Supplicant	Enter the maximum number of authenticated users that will be allowed on the port(s) here. The range is from 1 to 512.
Admin Control Direction	Select the control direction of traffic on the port(s) here. Options to choose from are: • **Both** - Specifies to control traffic in a bidirectional direction. • **In** - Specifies to control traffic in an inbound direction only.
Quiet Period	Enter the quiet period here. This is the number or seconds that the switch will remain in the quiet state after a failed authentication process. The range is from 1 to 65535 seconds.
Transmission Period	Enter the transmission period here. This is the number of seconds that the switch will wait for an EAP-request or identity frame from the supplicant before retransmitting the request. The range is from 1 to 65535 seconds.

Parameter	Description
Supplicant Timeout	Enter the supplicant timeout value here. This is the number of seconds the switch will wait for a response from the supplicant before timing out the supplicant message. This does not apply to the EAP request ID. The range is from 1 to 65535 seconds.
Server Timeout	Enter the server timeout value here. This is the number of seconds the switch will wait for a response from the authentication server before timing out the connection. The range is from 1 to 65535 seconds.
Re-authentication Period	Enter the re-authentication period here. This is the number of seconds between re-authentication attempts. The range is from 1 to 65535 seconds.
Maximum Request	Enter the maximum number of EAP requests that will be allowed from a backend authentication machine here before the authentication process is restarted. The range is from 1 to 10.
Re-authentication Time Local	Select to enable or disable the use of the local settings for the timer to re-authenticate a session here.
Per-Port Re-authentication	Select to enable or disable periodic re-authentication on the port(s) here.
Force Authentication Timeout	Enter the forced authentication timeout value here. This is the number of seconds the switch will wait before timing out a forced authorized/unauthorized entry. The range is from 0 to 65535 seconds. Enter 0 to never timeout an entry.

Click the **Apply** button to accept the changes made.
Click the **Show** button to display the MAC-based access control settings associated to the specified port.
Click the **Init** button to initiate the MAC-based access control settings on the specified port.
Click the **Re-authenticate** button to re-authenticate all the connections to the specified port.
Click the **Show Detail** button to display detailed information related to the entry.

Click the **Show Detail** button to view the following window:

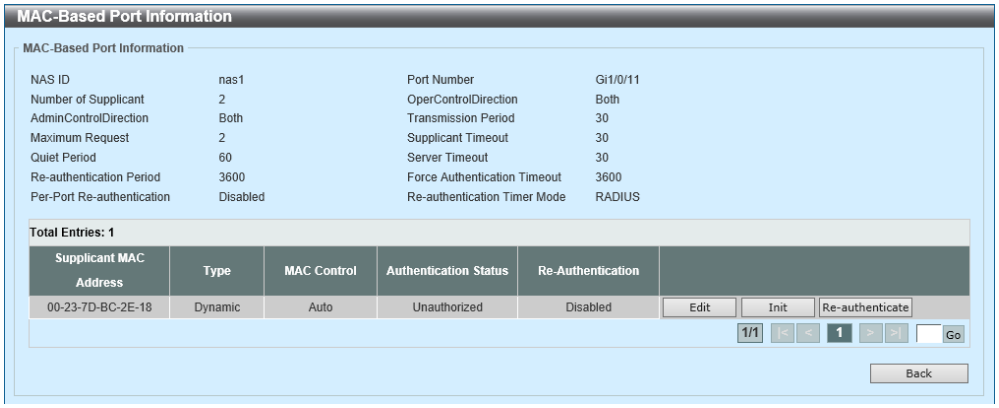


Figure 9-9 802.1X Port Settings (MAC-Based Access Control, Show Detail)

Click the **Edit** button to enable or disable the re-authentication function.
Click the **Init** button to initiate the MAC-based access control settings on the specified port.
Click the **Re-authenticate** button to re-authenticate the specified supplicant MAC address connection.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.
Click the **Back** button to return to the previous window.

9.2.5 EAP Port Config

This window is used to configure and display the EAP settings on the specified port(s).

Click **Security > 802.1X > EAP Port Config** to view the following window:

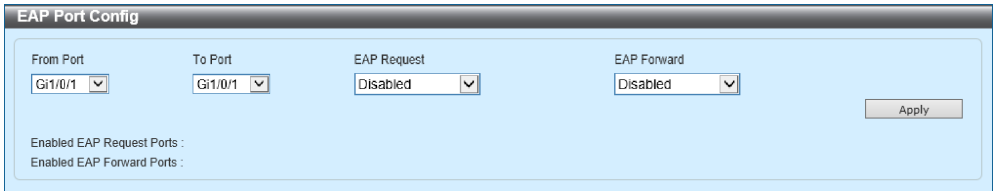


Figure 9-10 EAP Port Config

The following parameters can be configured:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
EAP Request	Select to enable or disable the EAP request function on the specified port(s) here.
EAP Forward	Select to enable or disable the EAP forward function on the specified port(s) here. This is used to enable/disable the forwarding of IEEE 802.1X Protocol Data Units (PDUs).

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

9.2.6 802.1X Authenticator Statistics

This window is used to display and clear IEEE 802.1X authenticator statistics on the specified port.

Click **Security > 802.1X > 802.1X Authenticator Statistics** to view the following window:

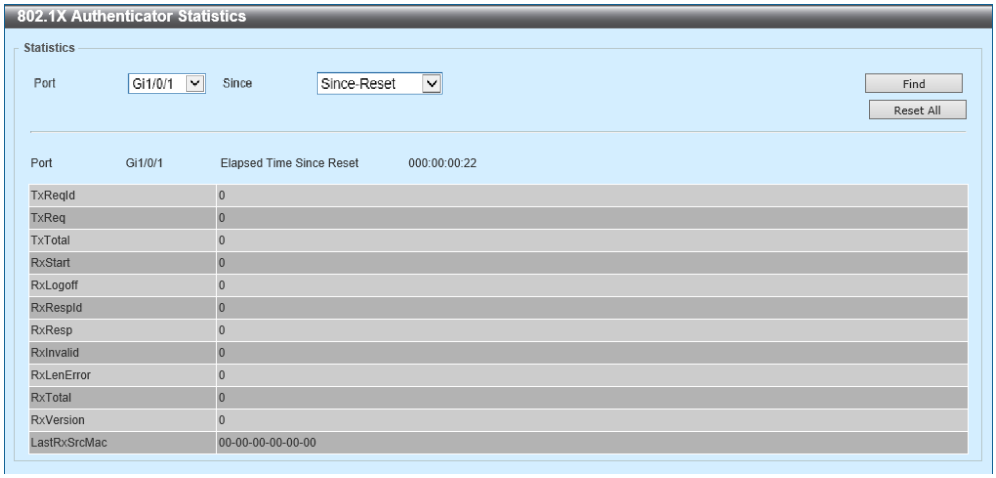


Figure 9-11 802.1X Authenticator Statistics

The following parameters can be configured in the **Statistics** section:

Parameter	Description
Port	Select the port that will be used here.
Since	Select the time range here. Options to choose from are: • **Since-Reset** - Specifies to display statistics since the last switch reset. • **Since-Up** - Specifies to display statistics since the last time the switch was booted up.

Click the **Find** button to display the information based on the search criteria specified.
Click the **Reset All** button to reset all the statistics information.

9.3 AAA (Authentication, Authorization, and Accounting)

9.3.1 AAA Global Settings

This window is used to globally enable or disable the AAA feature.

Click **Security > AAA > AAA Global Settings** to view the following window:

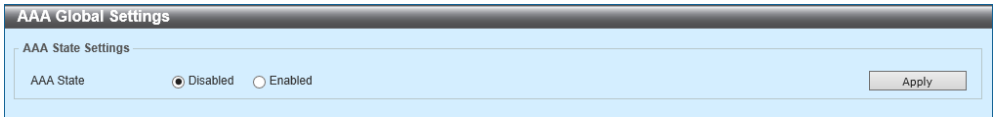


Figure 9-12 AAA Global Settings

The following parameters can be configured in the **AAA State Settings** section:

Parameter	Description
AAA State	Select to globally enable or disable the AAA feature here.

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

9.3.2 AAA Authentication Settings

This window is used to configure and display the AAA authentication settings.

Click **Security > AAA > AAA Authentication Settings** to view the following window:

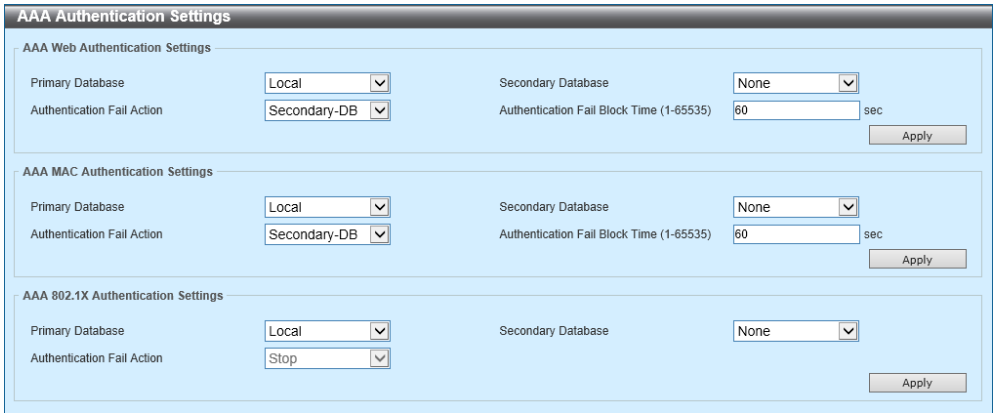


Figure 9-13 AAA Authentication Settings

The following parameters can be configured in the **AAA Web Authentication Settings** section:

Parameter	Description
Primary Database	Select the primary database that will be used for web authentication here. Options to choose from are: • **RADIUS** - Specifies to use the database on the RADIUS server as the primary database. • **Local** - Specifies to use local database on the switch as the primary database.
Secondary Database	Select the secondary database that will be used for web authentication here. Options to choose from are: • **None** - Authentication on the secondary database is treated as approved. • **RADIUS** - Specifies to use the database on the RADIUS server as the secondary database. • **Local** - Specifies to use local database on the switch as the secondary database.

Parameter	Description
Authentication Fail Action	Select the action to take when web authentication fails here. Options to choose from are: • **Stop** - Specifies to stop authentication when web authentication failed using the primary database. However the secondary database applies if it cannot communicate with the RADIUS server which is the primary database • **Secondary-DB** - Specifies to initiate authentication using the secondary database when web authentication failed using the primary database.
Authentication Fail Block Time	Enter the amount of seconds that a host will be blocked after web authentication failed. The range is from 1 to 65535 seconds.

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

The following parameters can be configured in the **AAA MAC Authentication Settings** section:

Parameter	Description
Primary Database	Select the primary database that will be used for MAC authentication here. Options to choose from are: • **RADIUS** - Specifies to use the database on the RADIUS server as the primary database. • **Local** - Specifies to use local database on the switch as the primary database.
Secondary Database	Select the secondary database that will be used for MAC authentication here. Options to choose from are: • **None** - Authentication on the secondary database is treated as approved. • **RADIUS** - Specifies to use the database on the RADIUS server as the secondary database. • **Local** - Specifies to use local database on the switch as the secondary database.
Authentication Fail Action	Select the action to take when MAC authentication fails here. Options to choose from are: • **Stop** - Specifies to stop authentication when MAC authentication failed using the primary database. However the secondary database applies if it cannot communicate with the RADIUS server which is the primary database • **Secondary-DB** - Specifies to initiate authentication using the secondary database when MAC authentication failed using the primary database.

Parameter	Description
Authentication Fail Block Time	Enter the amount of seconds that a host will be blocked after MAC authentication failed. The range is from 1 to 65535 seconds.

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

The following parameters can be configured in the **AAA 802.1X Authentication Settings** section:

Parameter	Description
Primary Database	Select the primary database that will be used for IEEE 802.1X authentication here. Options to choose from are: • **RADIUS** - Specifies to use the database on the RADIUS server as the primary database. • **Local** - Specifies to use local database on the switch as the primary database.
Secondary Database	Select the secondary database that will be used for IEEE 802.1X authentication here. Options to choose from are: • **None** - Specifies that no secondary database will be used. • **Local** - Specifies to use local database on the switch as the secondary database.

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

9.3.3 AAA Authentication User Settings

This window is used to configure and display the AAA authentication user settings.

Click **Security > AAA > AAA Authentication User Settings** to view the following window:

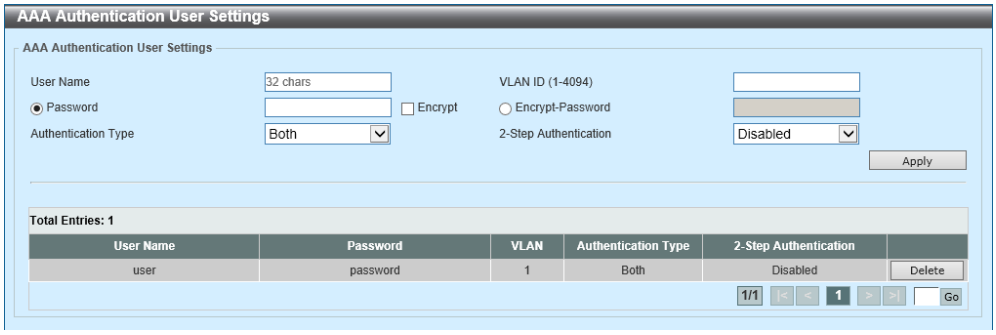


Figure 9-14 AAA Authentication User Settings

The following parameters can be configured in the **AAA Authentication User Settings** section:

Parameter	Description
User Name	Enter the username for the local authentication account here. This can be up to 32 characters long.
VLAN ID	Enter the target VLAN ID for the local authentication account here. The range is from 1 to 4094.
Password	Select and enter the clear-text password for the local authentication account here. Select the **Encrypt** option to enable password encryption for this account. The clear-text password will be saved in the encrypted form on the switch.
Encrypt Password	Select and enter the encrypted password for the local authentication account here.
Authentication Type	Select the authentication type here. Options to choose from are: • **Both** - Specifies that the local authentication account will be used for IEEE 802.1X and web authentication. • **Web** - Specifies that the local authentication account will be used for web authentication only. • **Dot1X** - Specifies that the local authentication account will be used for IEEE 802.1X authentication only.
2-Step Authentication	Select to enable or disable two-step authentication here.

Click the **Apply** button to add a new 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.

9.3.4 AAA Authentication MAC Settings

This window is used to configure and display the AAA authentication MAC settings.

Click **Security > AAA > AAA Authentication MAC Settings** to view the following window:

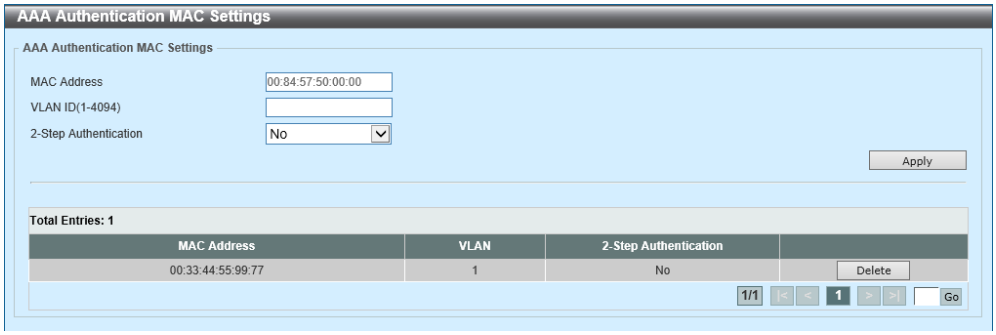


Figure 9-15 AAA Authentication MAC Settings

The following parameters can be configured in the **AAA Authentication MAC Settings** section:

Parameter	Description
MAC Address	Enter the MAC address for the local authentication account here. This will be used in MAC authentication.
VLAN ID	Enter the target VLAN ID for the local authentication account here. The range is from 1 to 4094.
2-Step Authentication	Select to enable or disable two-step authentication here. Options to choose from are: • **No** - Specifies to disable two-step authentication for the local authentication account. • **Web** - Specifies to enable two-step authentication and use web authentication as the second authentication method. • **802.1X** - Specifies to enable two-step authentication and use IEEE 802.1X authentication as the second authentication method. • **Any** - Specifies to enable two-step authentication and use IEEE 802.1X and web authentication as the second authentication methods.

Click the **Apply** button to add a new 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.

9.3.5 Application Authentication Settings

This window is used to configure and display the application authentication settings.

Click **Security > AAA > Application Authentication Settings** to view the following window:

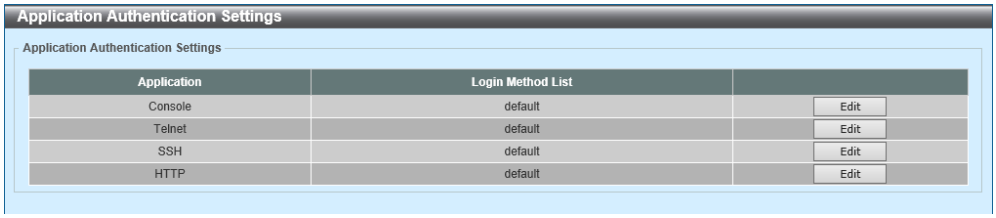


Figure 9-16 Application Authentication Settings

Click the **Edit** button to view the following window:

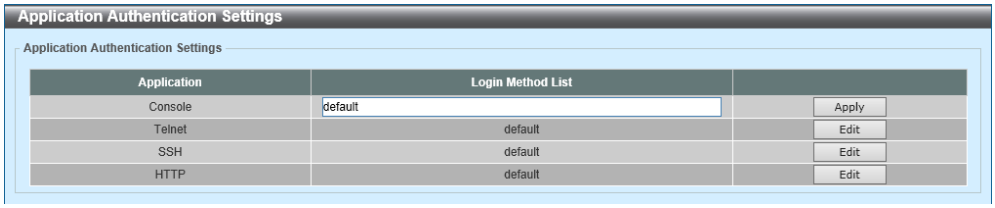


Figure 9-17 Application Authentication Settings (Edit)

The following parameters can be configured in the **Application Authentication Settings** section:

Parameter	Description
Login Method List	Enter the name for the login method list here.

Click the **Edit** button to edit the settings of the specified entry.
Click the **Apply** button to accept the changes made.

9.3.6 Application Accounting Settings

This window is used to configure and display the application accounting settings.

Click **Security > AAA > Application Accounting Settings** to view the following window:

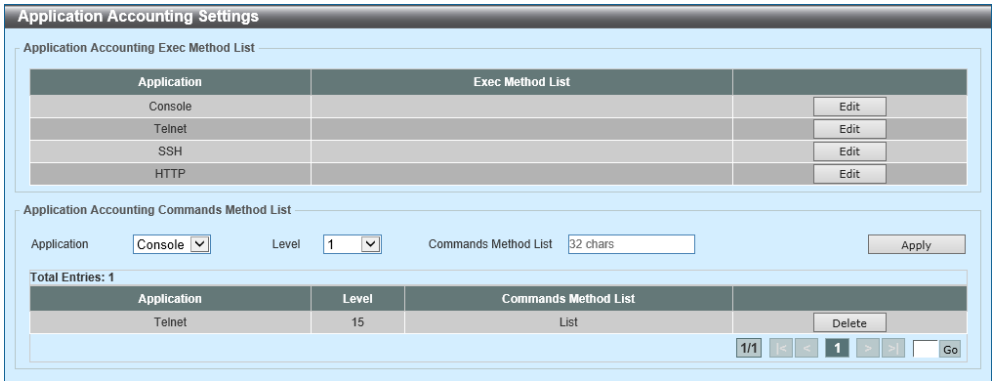


Figure 9-18 Application Accounting Settings

Click the **Edit** button to view the following window:

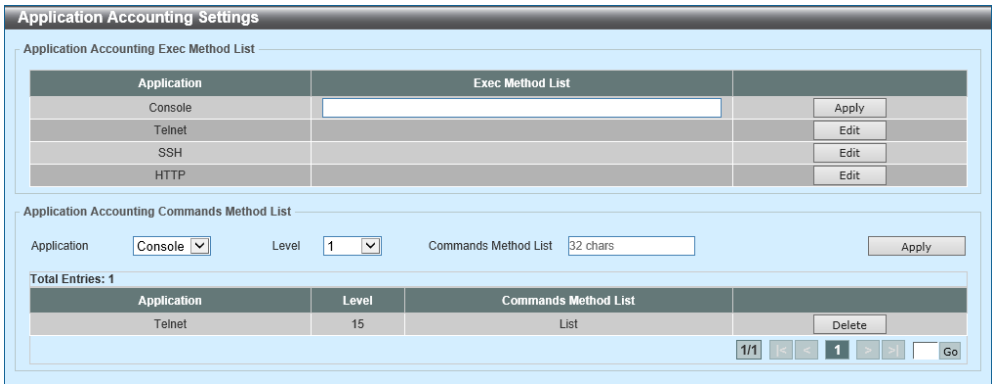


Figure 9-19 Application Accounting Settings (Edit)

The following parameters can be configured in the **Application Accounting Exec Method List** section:

Parameter	Description
Exec Method List	Enter the name for the EXEC method list here.

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

The following parameters can be configured in the **Application Accounting Method List** section:

Parameter	Description
Application	Select the application used here. Options to choose from are **Console**, **Telnet**, and **SSH**.
Level	Select the privilege level used here. Options to choose from are levels 1 to 15.
Commands Method List	Enter the commands method list name used here.

Click the **Apply** button to add a new 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.

Click the **AAA Accounting Commands** tab to view the following window:

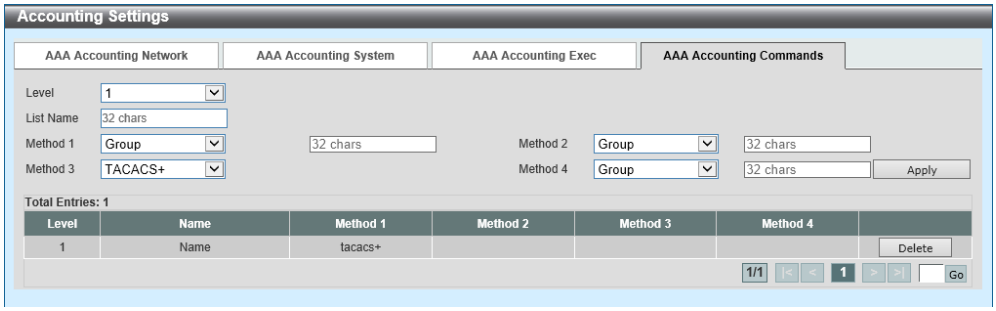


Figure 9-20 Accounting Settings (AAA Accounting Commands)

The following parameters can be configured in the **AAA Accounting Commands** section:

Parameter	Description
Level	Select the privilege level used here. Options to choose from are levels 1 to 15.
List Name	Enter the method list name that will be used with the AAA accounting commands option here.
Method 1 – Method 4	Select the method lists that will be used for this configuration here. Options to choose from are **None**, **Group**, and **TACACS+**. The **None** option is only available for Method 1.

Click the **Apply** button to add a new 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.

9.3.7 Authentication EXEC Settings

This window is used to configure and display the authentication execution settings.

Click **Security > AAA > Authentication EXEC Settings** to view the following window:

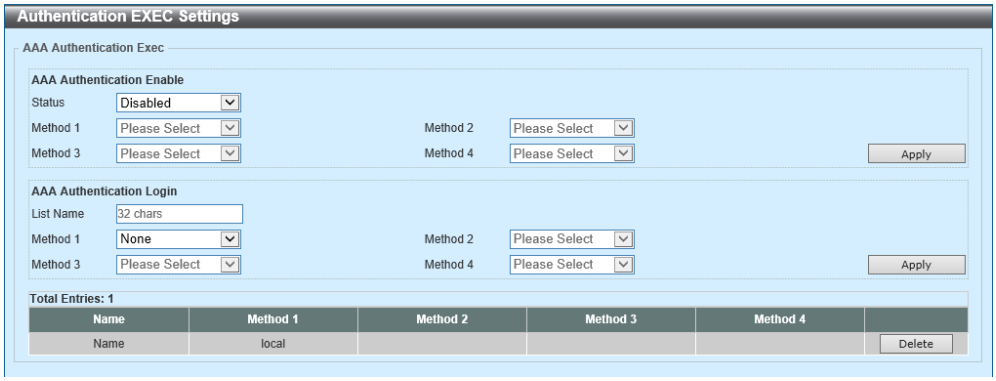


Figure 9-21 Authentication EXEC Settings

The following parameters can be configured in the **AAA Authentication Enable** section:

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** - Specifies that the user will pass the authentication if it is not denied by previous method authentication. Normally, the method is listed as the last method. • **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 following parameters can be configured in the **AAA Authentication Login** section:

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: • **None** - Specifies that the user will pass authentication if it is not denied by previous method's authentication. Normally, the method is listed as the last method. • **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 add a new entry.
Click the **Delete** button to delete the specified entry.

9.3.8 Accounting Settings

This window is used to configure and display the AAA accounting settings.

Click **Security > AAA > Accounting Settings** to view the following window:

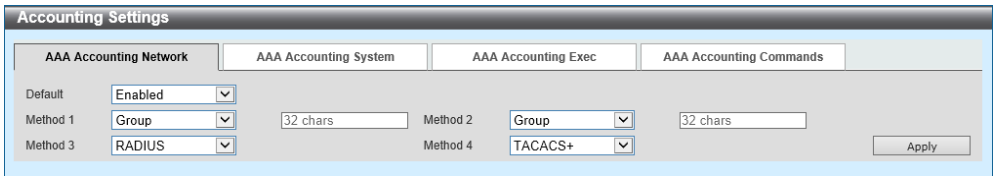


Figure 9-22 Accounting Settings (AAA Accounting Network)

The following parameters can be configured in the **AAA Accounting Network** section:

Parameter	Description
Default	Select to enable or disable the use of the default method list here.
Method 1 – Method 4	Select the method lists that will be used for this configuration here. Options to choose from are **None**, **Group**, **RADIUS**, and **TACACS+**. The **None** option is only available for Method 1.

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

Click the **AAA Accounting System** tab to view the following window:

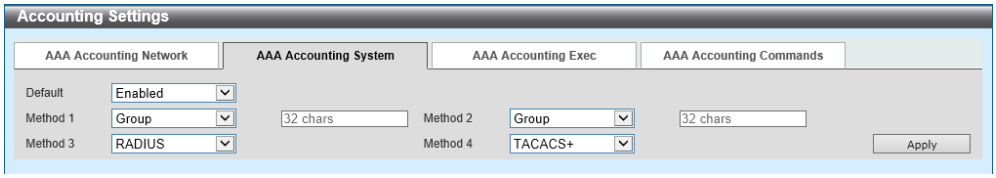


Figure 9-23 Accounting Settings (AAA Accounting System)

The following parameters can be configured in the **AAA Accounting System** section:

Parameter	Description
Default	Select to enable or disable the use of the default method list here.
Method 1 – Method 4	Select the method lists that will be used for this configuration here. Options to choose from are **None**, **Group**, **RADIUS**, and **TACACS+**. The **None** option is only available for Method 1.

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

Click the **AAA Accounting Exec** tab to view the following window:

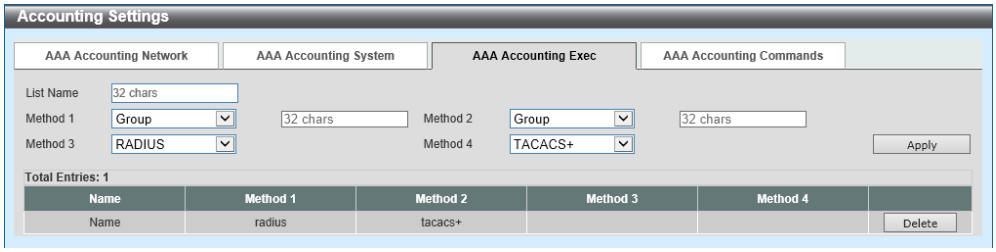


Figure 9-24 Accounting Settings (AAA Accounting Exec)

The following parameters can be configured in the **AAA Accounting Exec** section:

Parameter	Description
List Name	Enter the method list name that will be used with the AAA accounting EXEC option here.
Method 1 – Method 4	Select the method lists that will be used for this configuration here. Options to choose from are **None**, **Group**, **RADIUS**, and **TACACS+**. The **None** option is only available for Method 1.

Click the **Apply** button to add a new entry.
Click the **Delete** button to delete the specified entry.

9.4 Authentication

9.4.1 Authentication Dynamic VLAN Settings

This window is used to configure and display the dynamic VLAN settings used in authentication.

Click **Security > Authentication > Authentication Dynamic VLAN Settings** to view the following window:

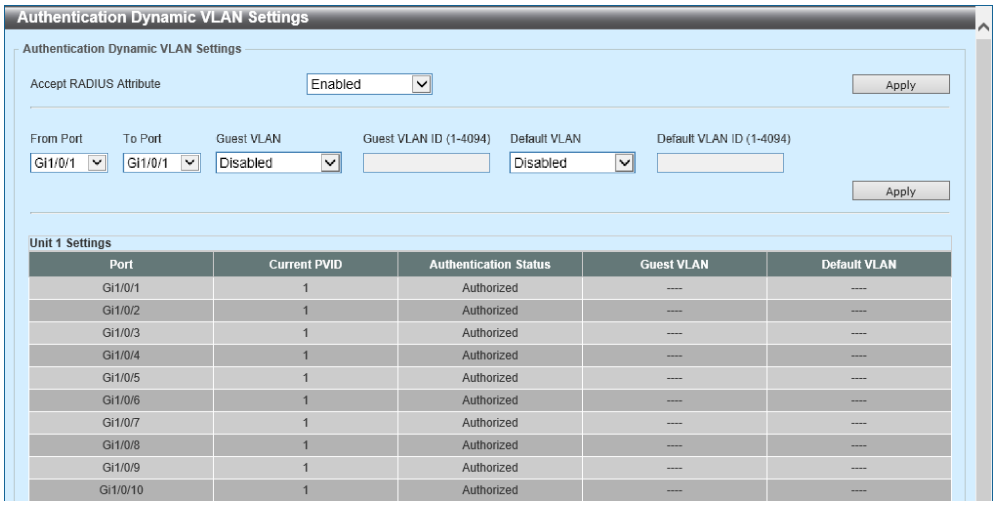


Figure 9-25 Authentication Dynamic VLAN Settings

The following parameters can be configured in the **Authentication Dynamic VLAN Settings** section:

Parameter	Description
Accept RADIUS Attribute	Select to enable or disable the acceptance of RADIUS attributes here.
From Port - To Port	Select the port(s) that will be used here.
Guest VLAN	Select to enable or disable the guest VLAN here. When this is enabled, hosts will be allowed access to the guest VLAN without the need for authentication.
Guest VLAN ID	Enter the guest VLAN ID here. The range is from 1 to 4094.
Default VLAN	Select to enable or disable the default VLAN here. After hosts were successfully authenticated, they will be assigned to the default VLAN if the dynamic VLAN feature is disabled or the target VLAN for the host is invalid.
Default VLAN ID	Enter the default VLAN ID here. The range is from 1 to 4094.

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

9.4.2 Authentication Status Table

This window is used to display the authentication status table and information. Additionally, the authentication aging time can also be configured in this window.

Click **Security > Authentication > Authentication Status Table** to view the following window:

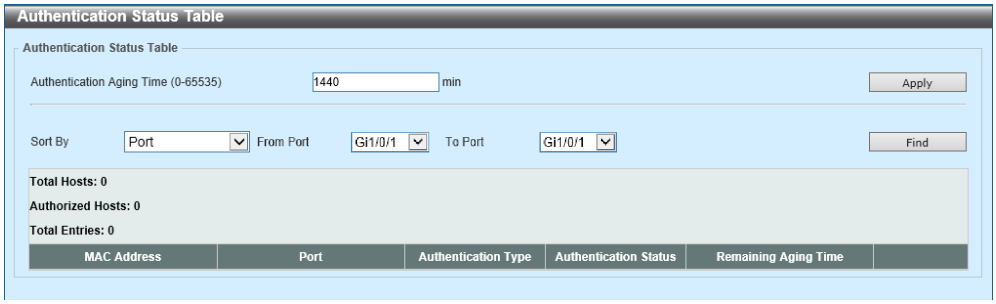


Figure 9-26 Authentication Status Table

The following parameters can be configured in the **Authentication Status Table** section:

Parameter	Description
Authentication Aging Time	Enter the timeout value for MAC/Web authentication sessions here. The range is from 0 to 65535 minutes.
Sort By MAC	Select this option to display authentication sessions, sorted by MAC address.
Sort By Port	Select this option to display authentication sessions on the specified port(s). • **From Port / To Port** - Select the port(s) that will be used here.

Click the **Apply** button to accept the changes made.
Click the **Find** button to find and display entries based on the search criteria specified.

9.4.3 2-Step Authentication Settings

This window is used to configure and display the 2-step authentication settings on the specified port(s).

Click **Security > Authentication > 2-Step Authentication Settings** to view the following window:

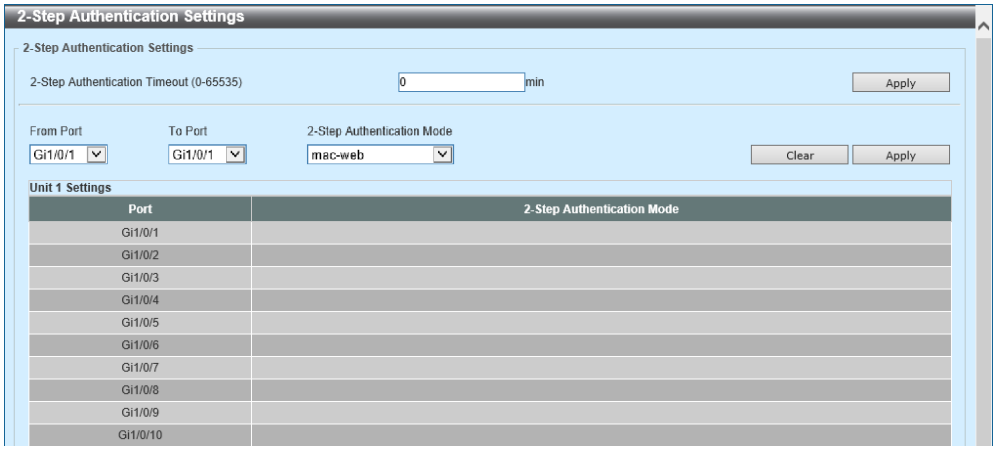


Figure 9-27 2-Step Authentication Settings

The following parameters can be configured in the **2-Step Authentication Settings** section:

Parameter	Description
2-Step Authentication Timeout	Enter the timeout value after which the second step of authentication will be attempted. The range is from 0 to 65535 minutes.
From Port - To Port	Select the port(s) that will be used here.
2-Step Authentication Mode	Select the two-step authentication mode here. Options to choose from are: • **MAC-Web** - Specifies that MAC and Web authentication will both be used in the first step in the two-step authentication method. • **MAC-Dot1X** - Specifies that MAC and IEEE 802.1X authentication will both be used in the first step in the two-step authentication method. • **Dot1X-Web** - Specifies that IEEE 802.1X and Web authentication will both be used in the first step in the two-step authentication method.

Click the **Apply** button to accept the changes made.
Click the **Clear** button to clear the information based on the criteria specified.

9.5 RADIUS (Remote Authentication Dial-In User Service)

9.5.1 RADIUS Global Settings

This window is used to configure and display the global settings associated with the RADIUS feature.

Click **Security > RADIUS > RADIUS Global Settings** to view the following window:

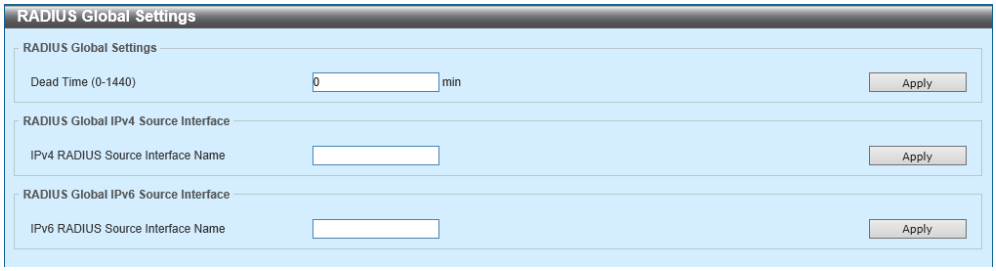


Figure 9-28 RADIUS Global Settings

The following parameters can be configured in the **RADIUS Global Settings** section:

Parameter	Description
Dead Time	Enter the dead time value here. 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. The range is from 1 to 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.

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

The following parameters can be configured in the **RADIUS Global IPv4 Source Interface** section:

Parameter	Description
IPv4 RADIUS Source Interface Name	Enter the name of the IPv4 RADIUS source interface here.

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

The following parameters can be configured in the **RADIUS Global IPv6 Source Interface** section:

Parameter	Description
IPv6 RADIUS Source Interface Name	Enter the name of the IPv6 RADIUS source interface here.

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

9.5.2 RADIUS Server Settings

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

Click **Security > RADIUS > RADIUS Server Settings** to view the following window:

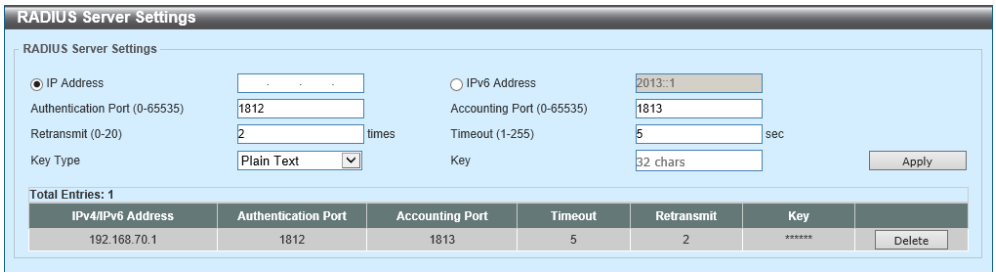


Figure 9-29 RADIUS Server Settings

The following parameters can be configured in the **RADIUS Server Settings** section:

Parameter	Description
IP Address	Enter the IPv4 address of the RADIUS server here.
IPv6 Address	Enter the IPv6 address of the RADIUS server here.
Authentication Port	Enter the authentication port number used here. The range is from 0 to 65535. By default, this value is 1812. If no authentication is used, use the value 0.
Accounting Port	Enter the accounting port number used here. The range is from 0 to 65535. By default, this value is 1813. If no accounting is used, use the value 0.
Retransmit	Enter the retransmit value used here. The range is from 0 to 20. By default, this value is 3. To disable this option, enter the value 0.
Timeout	Enter the timeout value used here. The range is from 1 to 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 add a new entry.
Click the **Delete** button to delete the specified entry.

9.5.3 RADIUS Group Server Settings

This window is used to configure and display the RADIUS group server settings.

Click **Security > RADIUS > RADIUS Group Server Settings** to view the following window:

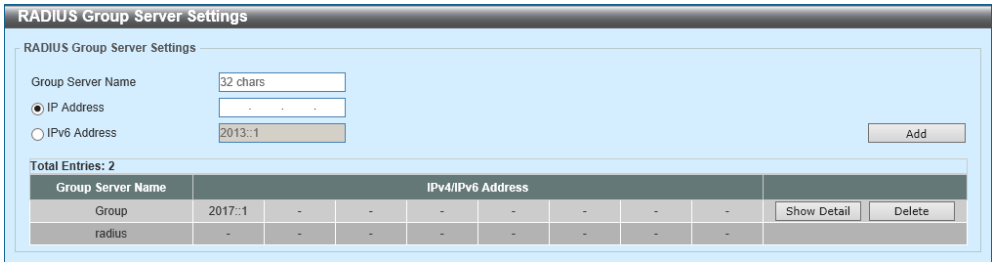


Figure 9-30 RADIUS Group Server Settings

The following parameters can be configured in the **RADIUS Group Server Settings** section:

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 IPv4 address of the RADIUS group server here.
IPv6 Address	Enter the IPv6 address of the RADIUS group server here.

Click the **Add** button to add a new entry.
Click the **Show Detail** button to display detailed information related to the entry.
Click the **Delete** button to delete the specified entry.

Click the **Show Detail** button to view the following window:

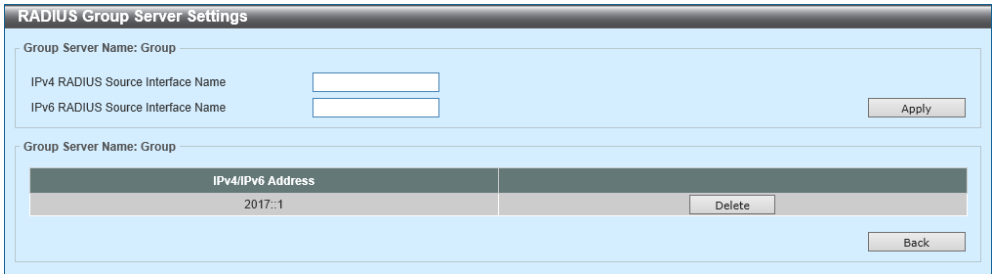


Figure 9-31 RADIUS Group Server Settings (Show Detail)

The following parameters can be configured:

Parameter	Description
IPv4 RADIUS Source Interface Name	Enter the name of the source IPv4 RADIUS interface here.
IPv6 RADIUS Source Interface Name	Enter the name of the source IPv6 RADIUS interface here.

Click the **Apply** button to add a new entry.
Click the **Delete** button to delete the specified entry.
Click the **Back** button to return to the previous window.

9.5.4 RADIUS Statistics

This window is used to display and clear the RADIUS statistics information.

Click **Security > RADIUS > RADIUS Statistics** to view the following window:

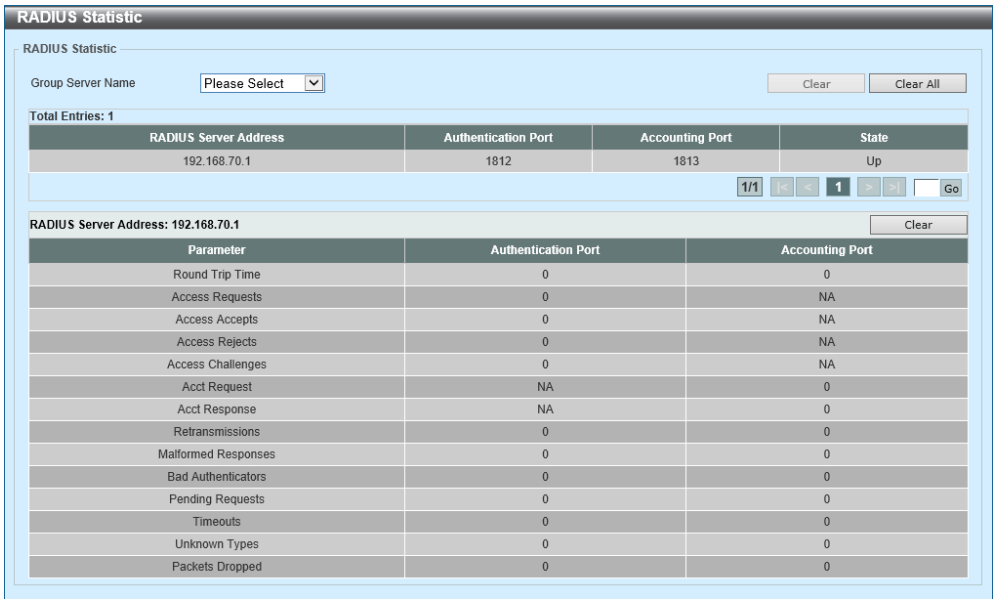


Figure 9-32 RADIUS Statistics

The following parameters can be configured in the **RADIUS Statistic** section:

Parameter	Description
Group Server Name	Select the RADIUS group server name from this list here.

Click the first **Clear** button to clear the statistics information based on the criteria specified.
Click the **Clear All** button to clear all the statistics information.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.
Click the second **Clear** button to clear the statistics information in the table.

9.6 TACACS+ (Terminal Access Controller Access-Control System Plus)

9.6.1 TACACS+ Global Settings

This window is used to configure and display the global settings associated with the TACACS+ feature.

Click **Security > TACACS+ > TACACS+ Global Settings** to view the following window:

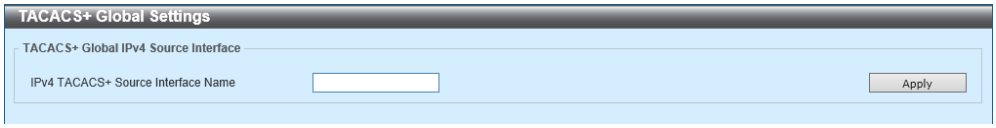


Figure 9-33 TACACS+ Global Settings

The following parameters can be configured in the **TACACS+ Global IPv4 Source Interface** section:

Parameter	Description
IPv4 TACACS+ Source Interface Name	Enter the name of the IPv4 TACACS+ source interface here.

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

9.6.2 TACACS+ Server Settings

This window is used to configure and display the TACACS+ server settings.

Click **Security > TACACS+ > TACACS+ Server Settings** to view the following window:

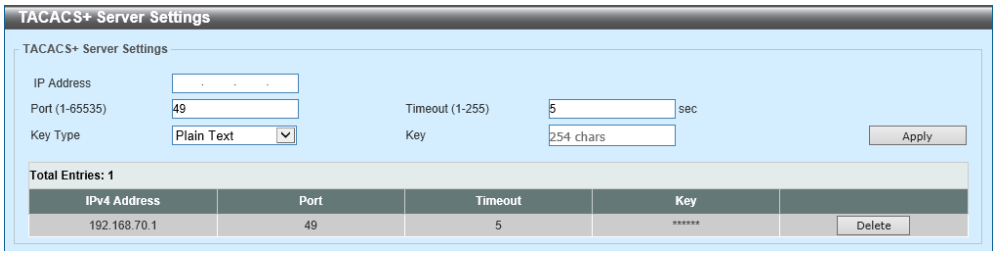


Figure 9-34 TACACS+ Server Settings

The following parameters can be configured in the **TACACS+ Server Settings** section:

Parameter	Description
IP Address	Enter the IPv4 address of the TACACS+ server here.
Port	Enter the port number used here. The range is from 1 to 65535. By default, this value is 49.
Timeout	Enter the timeout value here. The range is from 1 to 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 add a new entry.
Click the **Delete** button to delete the specified entry.

9.6.3 TACACS+ Group Server Settings

This window is used to configure and display the TACACS+ group server settings.

Click **Security > TACACS+ > TACACS+ Group Server Settings** to view the following window:

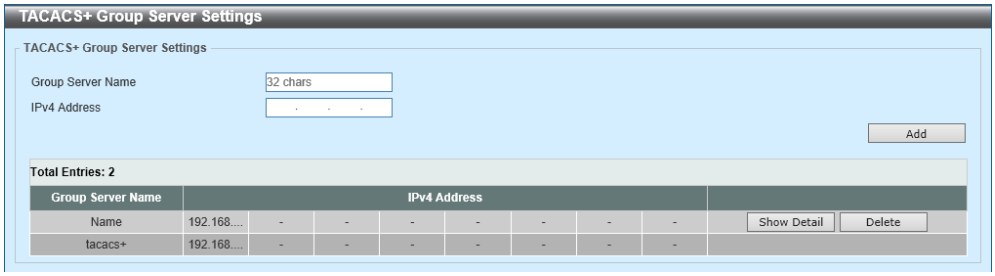


Figure 9-35 TACACS+ Group Server Settings

The following parameters can be configured in the **TACACS+ Group Server Settings** section:

Parameter	Description
Group Server Name	Enter the TACACS+ group server name here. This name can be up to 32 characters long.
IPv4 IP Address	Enter the IPv4 address of the TACACS+ group server here.

Click the **Add** button to add a new entry.
Click the **Show Detail** button to display detailed information related to the entry.
Click the **Delete** button to delete the specified entry.

Click the **Show Detail** button to view the following window:

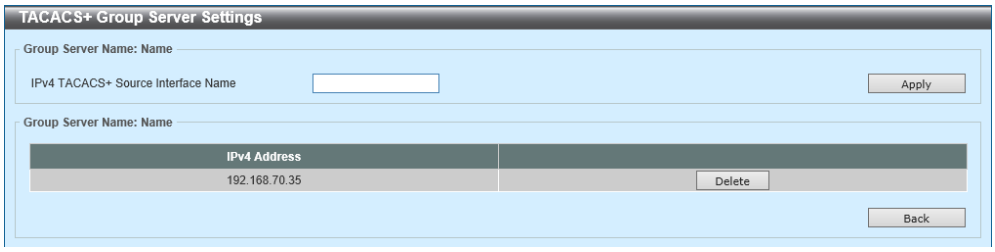


Figure 9-36 TACACS+ Group Server Settings (Show Detail)

The following parameters can be configured in the **TACACS+ Group Server Settings** section:

Parameter	Description
IPv4 TACACS+ Source Interface Name	Enter the name of the source IPv4 TACACS+ interface here.

Click the **Apply** button to add a new entry.
Click the **Delete** button to delete the specified entry.
Click the **Back** button to return to the previous window.

9.6.4 TACACS+ Statistics

This window is used to display and clear the TACACS+ statistics information.

Click **Security > TACACS+ > TACACS+ Statistics** to view the following window:

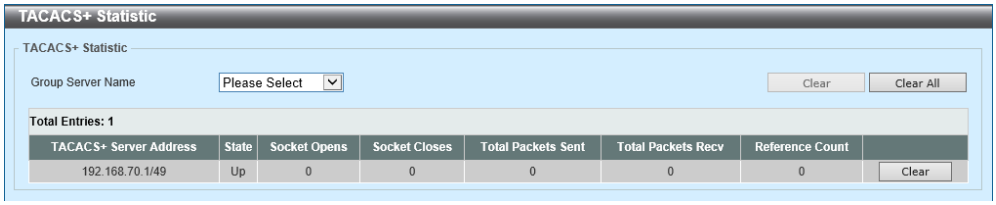


Figure 9-37 TACACS+ Statistics

The following parameters can be configured in the **TACACS+ Statistic** section:

Parameter	Description
Group Server Name	Select the TACACS+ group server name from this list here.

Click the first **Clear** button to clear the statistics information based on the criteria specified.
Click the **Clear All** button to clear all the statistics information.
Click the second **Clear** button to clear the statistics information for the specified entry.

9.7 SAVI (Source Address Validation Improvements)

9.7.1 IPv4

9.7.1.1 DHCPv4 Snooping

9.7.1.1.1 DHCP Snooping Global Settings

This window is used to configure and display the global settings associated with the DHCP snooping feature.

Click **Security > SAVI > IPv4 > DHCPv4 Snooping > DHCP Snooping Global Settings** to view the following window:

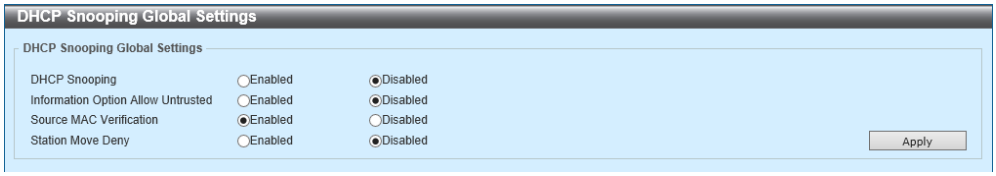


Figure 9-38 DHCP Snooping Global Settings

The following parameters can be configured in the **DHCP Snooping Global Settings** section:

Parameter	Description
DHCP Snooping	Select to globally enable or disable DHCP snooping here.
Information Option Allow Untrusted	Select to globally enable or disable the option to 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.

9.7.1.1.2 DHCP Snooping Port Settings

This window is used to configure and display the DHCP snooping settings on the specified port(s).

Click **Security > SAVI > IPv4 > DHCPv4 Snooping > DHCP Snooping Port Settings** to view the following window:

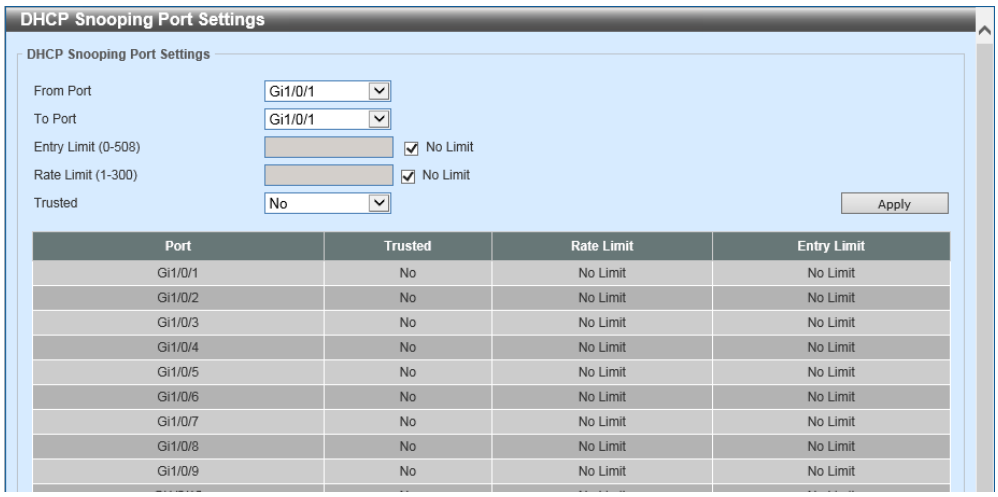


Figure 9-39 DHCP Snooping Port Settings

The following parameters can be configured in the **DHCP Snooping Port Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Entry Limit	Enter the entry limit value here. The range is from 0 to 508. Tick the **No Limit** option to disable the function.
Rate Limit	Enter the rate limit value here. The range is from 1 to 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 trusted interfaces. The ports connected to DHCP clients should be configured as untrusted interfaces. DHCP snooping will act as a firewall between untrusted interfaces and DHCP servers.

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

9.7.1.1.3 DHCP Snooping VLAN Settings

This window is used to configure and display the DHCP snooping settings on the specified VLAN(s).

Click **Security > SAVI > IPv4 > DHCPv4 Snooping > DHCP Snooping VLAN Settings** to view the following window:

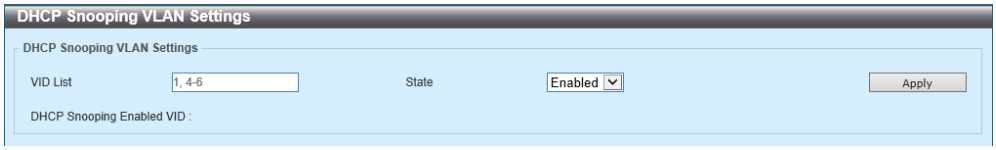


Figure 9-40 DHCP Snooping VLAN Settings

The following parameters can be configured in the **DHCP Snooping VLAN Settings** section:

Parameter	Description
VID List	Enter the VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.
State	Select to enable or disable the DHCP snooping VLAN setting here.

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

9.7.1.1.4 DHCP Snooping Database

This window is used to configure and display the DHCP snooping database settings.

Click **Security > SAVI > IPv4 > DHCPv4 Snooping > DHCP Snooping Database** to view the following window:

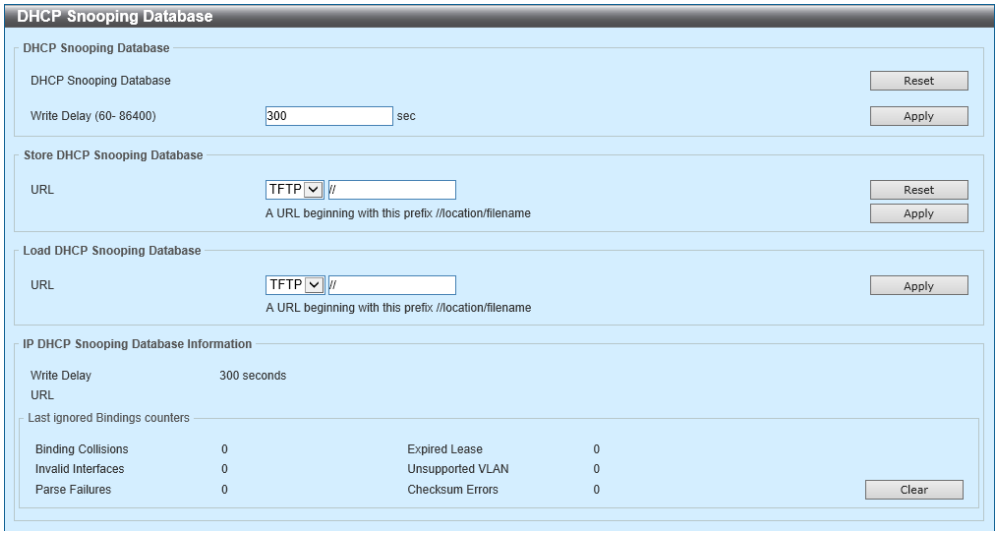


Figure 9-41 DHCP Snooping Database

The following parameters can be configured in the **DHCP Snooping Database** section:

Parameter	Description
Write Delay	Enter the write delay time here. The range is from 60 to 86400 seconds. By default, this value is 300 seconds.

Click the **Reset** button to reset the DHCP snooping database.
Click the **Apply** button to accept the changes made.

The following parameters can be configured in the **Store DHCP Snooping Database** section:

Parameter	Description
URL	Select the location from the drop-down list and enter the URL where the DHCP snooping database will be stored to here. Locations to choose from are **TFTP**, **FTP**, and **Local**.

Click the **Reset** button to reset the stored DHCP snooping database.
Click the **Apply** button to store the DHCP snooping database.

The following parameters can be configured in the **Load DHCP Snooping Database** section:

Parameter	Description
URL	Select the location from the drop-down list and enter the URL where the DHCP snooping database will be loaded from here. Locations to choose from are **TFTP**, **FTP**, and **Local**.

Click the **Apply** button to load the DHCP snooping database.
Click the **Clear** button to clear the counter information.

9.7.1.1.5 DHCP Snooping Binding Entry

This window is used to configure and display DHCP snooping binding entries.

Click **Security > SAVI > IPv4 > DHCPv4 Snooping > DHCP Snooping Binding Entry** to view the following window:

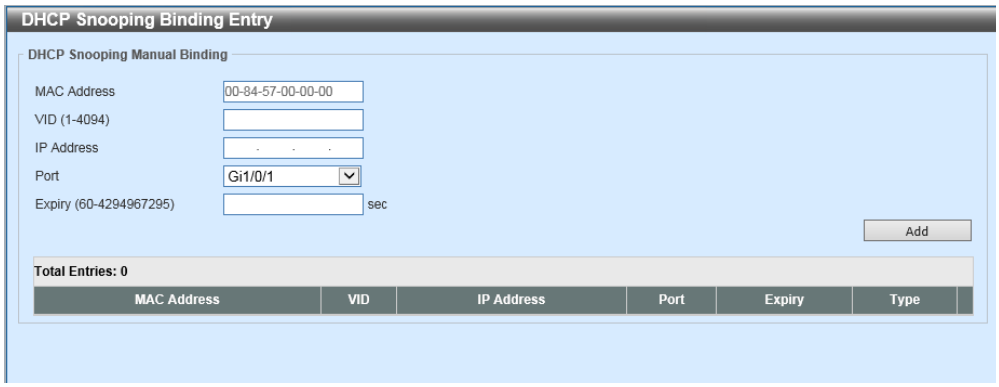


Figure 9-42 DHCP Snooping Binding Entry

The following parameters can be configured in the **DHCP Snooping Manual Binding** section:

Parameter	Description
MAC Address	Enter the MAC address of the DHCP snooping binding entry here.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.
IP Address	Enter the IP address of the DHCP snooping binding entry here.
Port	Select the port that will be used here.
Expiry	Enter the expiry time value used here. The range is from 60 to 4294967295 seconds.

Click the **Add** button to add a new 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.

9.7.1.2 Dynamic ARP Inspection

9.7.1.2.1 ARP Access List

This window is used to configure and display the ARP access list settings used in dynamic ARP inspection.

Click **Security > SAVI > IPv4 > Dynamic ARP Inspection > ARP Access List** to view the following window:

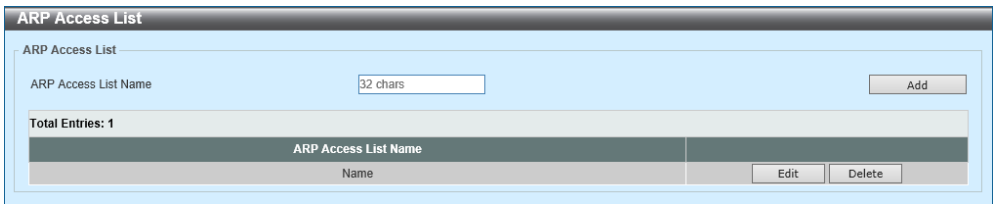


Figure 9-43 ARP Access List

The following parameters can be configured in the **ARP Access List** section:

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.
Click the **Edit** button to edit the settings of the specified entry.
Click the **Delete** button to delete the specified entry.

Click the **Edit** button to view the following window:

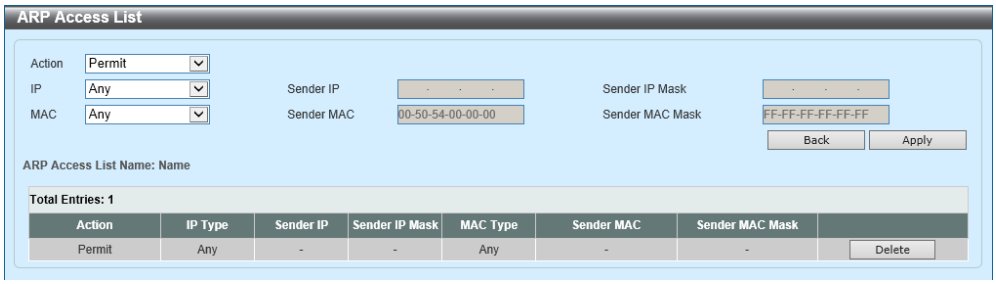


Figure 9-44 ARP Access List (Edit)

The following parameters can be configured:

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 **Apply** button to add a new entry.
Click the **Back** button to return to the previous window.
Click the **Delete** button to delete the specified entry.

9.7.1.2.2 ARP Inspection Settings

This window is used to configure and display the dynamic ARP inspection settings.

Click **Security > SAVI > IPv4 > Dynamic ARP Inspection > ARP Inspection Settings** to view the following window:

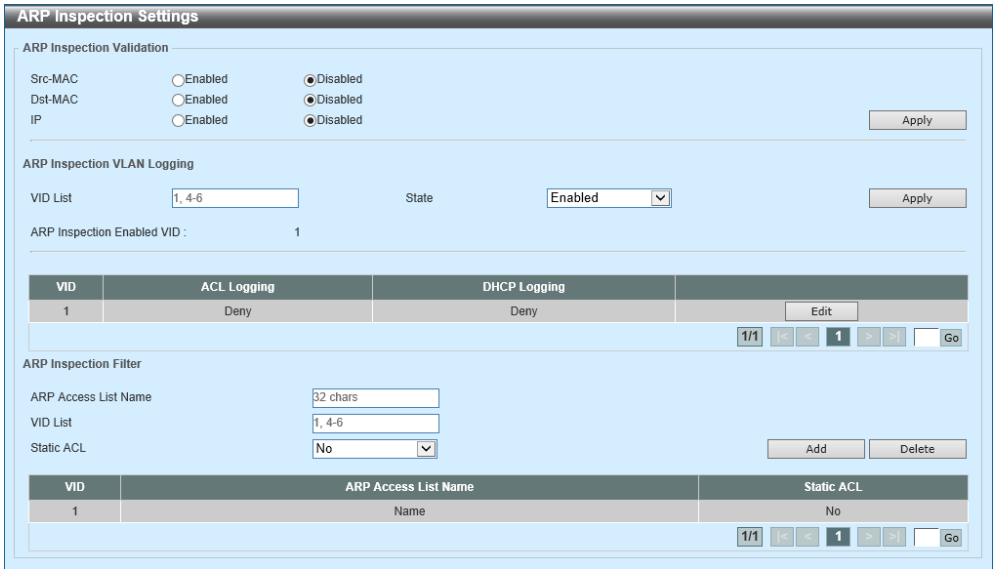


Figure 9-45 ARP Inspection Settings

The following parameters can be configured in the **ARP Inspection Validation** section:

Parameter	Description
Src-MAC	Select to enable or disable the source MAC option here. This option specifies to check for ARP request 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.

Parameter	Description
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. Target IP addresses are checked only in ARP responses.

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

The following parameters can be configured in the **ARP Inspection VLAN Logging** section:

Parameter	Description
VID List	Enter the VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.
State	Select to enable or disable ARP inspection VLAN logging of the specified VLAN(s) here.

Click the **Apply** button to add a new entry.
Click the **Edit** button to edit the settings of the specified entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

The following parameters can be configured in the **ARP Inspection Filter** section:

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(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.
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.
Click the **Delete** button to delete an entry based on the information specified.

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

9.7.1.2.3 ARP Inspection Port Settings

This window is used to configure and display the dynamic ARP inspection settings on the specified port(s).

Click **Security > SAVI > IPv4 > Dynamic ARP Inspection > ARP Inspection Port Settings** to view the following window:

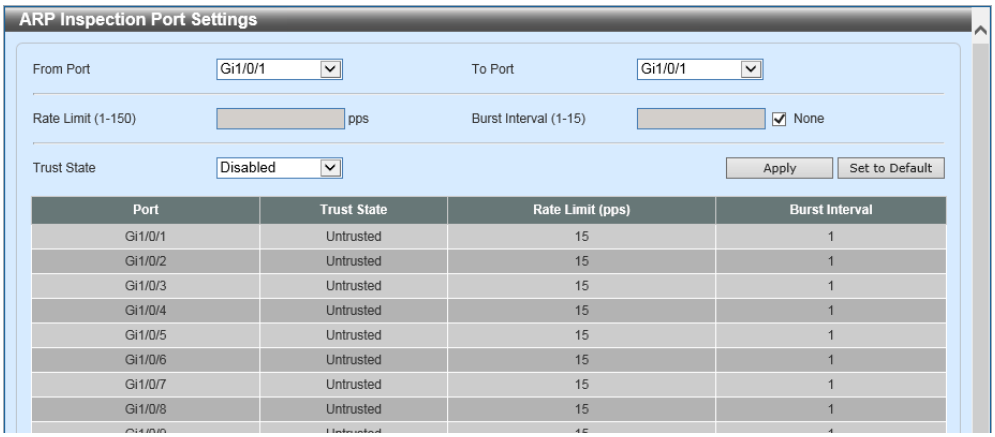


Figure 9-46 ARP Inspection Port Settings

The following parameters can be configured:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Rate Limit	Enter the rate limit value here. The range is from 1 to 150 packets per seconds.
Burst Interval	Enter the burst interval value here. The range is from 1 to 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 the set the trust state to the default setting.

9.7.1.2.4 ARP Inspection Statistics

This window is used to display and clear the dynamic ARP inspection statistics information.

Click **Security > SAVI > IPv4 > Dynamic ARP Inspection > ARP Inspection Statistics** to view the following window:

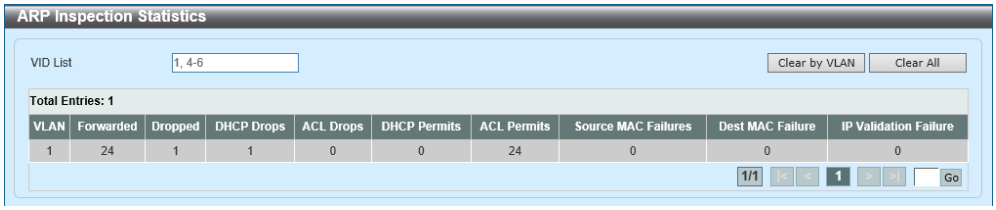


Figure 9-47 ARP Inspection Statistics

The following parameters can be configured:

Parameter	Description
VID List	Enter the VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 1 to 4094.

Click the **Clear by VLAN** button to clear the statistics information related to the specified VLAN.
Click the **Clear All** button to clear all the statistics information.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

9.7.1.2.5 ARP Inspection Log

This window is used to display and clear the dynamic ARP inspection log information. The log buffer value can also be configured in this window.

Click **Security > SAVI > IPv4 > Dynamic ARP Inspection > ARP Inspection Log** to view the following window:

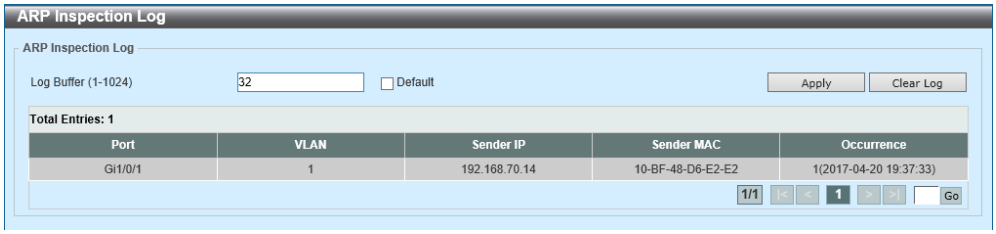


Figure 9-48 ARP Inspection Log

The following parameters can be configured in the **ARP Inspection Log** section:

Parameter	Description
Log Buffer	Enter the size of the log buffer here. The range is from 1 to 1024. By default, this value is 32. Select the **Default** option to use the default value.

Click the **Apply** button to accept the changes made.
Click the **Clear Log** button to clear the ARP inspection log.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

9.7.1.3 IP Source Guard

9.7.1.3.1 IP Source Guard Port Settings

This window is used to configure and display the IP source guard settings on the specified port(s).

Click **Security > SAVI > IPv4 > IP Source Guard > IP Source Guard Port Settings** to view the following window:

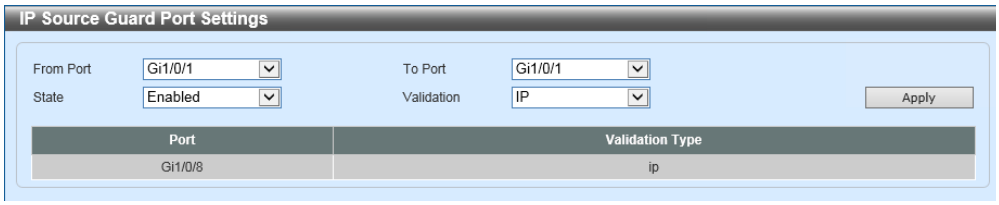


Figure 9-49 IP Source Guard Port Settings

The following parameters can be configured:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
State	Select to enable or disable the IP source guard's state for the specified port(s) here.
Validation	Select the validation method used here. Options to choose from are: • **IP** - Specifies that the IP address of the received packets will be checked. • **IP-MAC** - Specifies that the IP address and the MAC address of the received packets will be checked.

Click the **Apply** button to add a new entry.

9.7.1.3.2 IP Source Guard Binding

This window is used to configure and display the IP source guard binding settings.

Click **Security > SAVI > IPv4 > IP Source Guard > IP Source Guard Binding** to view the following window:

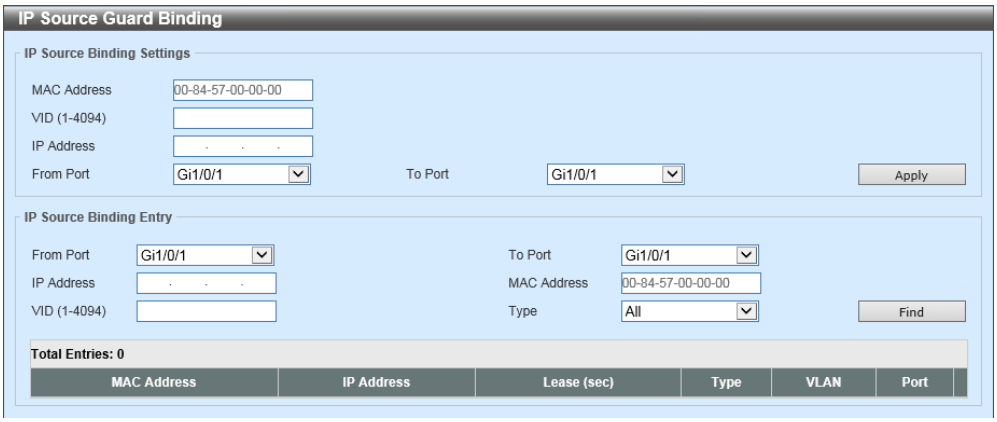


Figure 9-50 IP Source Guard Binding

The following parameters can be configured in the **IP Source Binding Settings** section:

Parameter	Description
MAC Address	Enter the MAC address of the binding entry here.
VID	Enter the VLAN ID that will be used here. The range is from 1 to 4094.
IP Address	Enter the IP address of the binding entry here.
From Port - To Port	Select the port(s) that will be used here.

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

The following parameters can be configured in the **IP Source Binding Entry** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used 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 that will be used here. The range is from 1 to 4094.
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 find and display entries based on the search criteria specified.
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.

9.7.1.3.3 IP Source Guard HW Entry

This window is used to display the IP source guard, hardware entries on the specified port(s).

Click **Security > SAVI > IPv4 > IP Source Guard > IP Source Guard HW Entry** to view the following window:

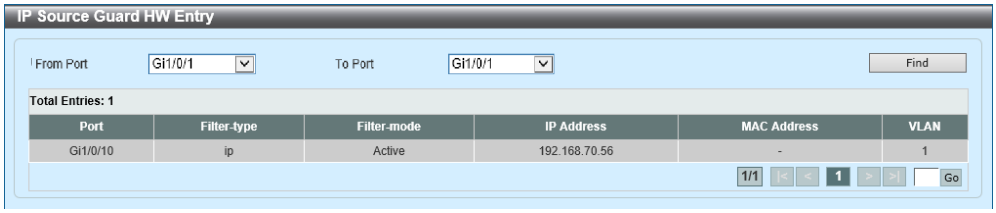


Figure 9-51 IP Source Guard HW Entry

The following parameters can be configured:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.

Click the **Find** button to find and display entries based on the search criteria specified.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

9.8 DHCP Server Protect

9.8.1 DHCP Server Protect Global Settings

This window is used to configure and display the global settings associated with the DHCP server protect feature.

Click **Security > DHCP Server Protect > DHCP Server Protect Global Settings** to view the following window:

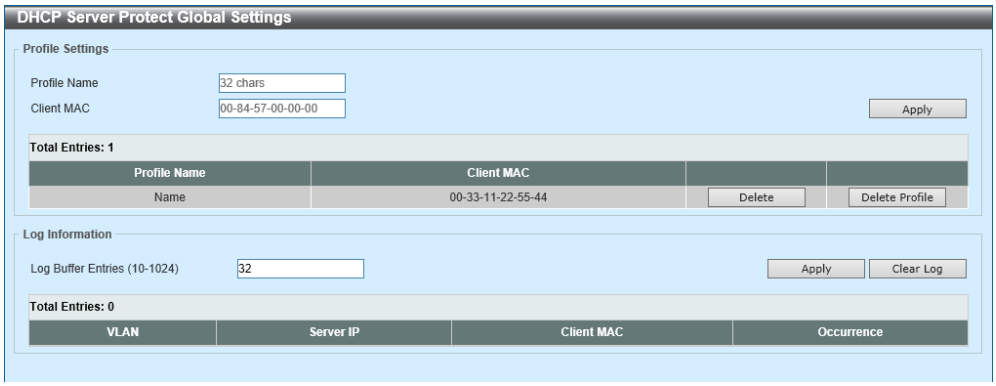


Figure 9-52 DHCP Server Protect Global Settings

The following parameters can be configured in the **Profile Settings** section:

Parameter	Description
Profile Name	Enter the DHCP Server Protect profile name here. This name can be up to 32 characters long.
Client MAC	Enter the MAC address used here.

Click the **Apply** button to add a new entry.
Click the **Delete** button to remove the MAC address from the specified profile.
Click the **Delete Profile** button to delete the profile.

The following parameters can be configured in the **Log Information** section:

Parameter	Description
Log Buffer Entries	Enter the amount of entries that will be logged here. The range is from 10 to 1024. By default, this value is 32.

9.8.2 DHCP Server Protect Port Settings

This window is used to configure and display the DHCP server protect settings on the specified port(s).

Click **Security > DHCP Server Protect > DHCP Server Protect Port Settings** to view the following window:

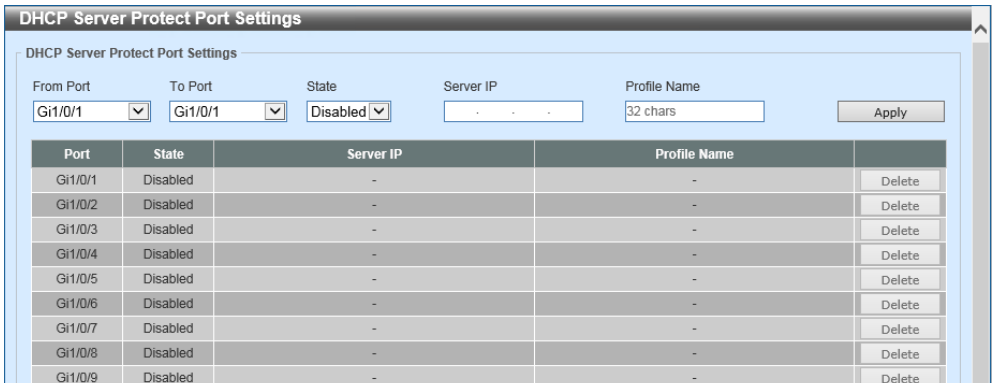


Figure 9-53 DHCP Server Protect Port Settings

The following parameters can be configured in the **DHCP Server Protect Port Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
State	Select to enable or disable the DHCP Server Protect function on the port(s) specified.
Server IP	Enter the DHCP server IP address here.
Profile Name	Enter the DHCP Server Protect 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 server IP address and profile name from the specified port.

9.9 BPDU Guard

This window is used to configure and display the state of the BPDU guard feature and the BPDU guard settings on the specified port(s).

Click **Security > BPDU Guard** to view the following window:

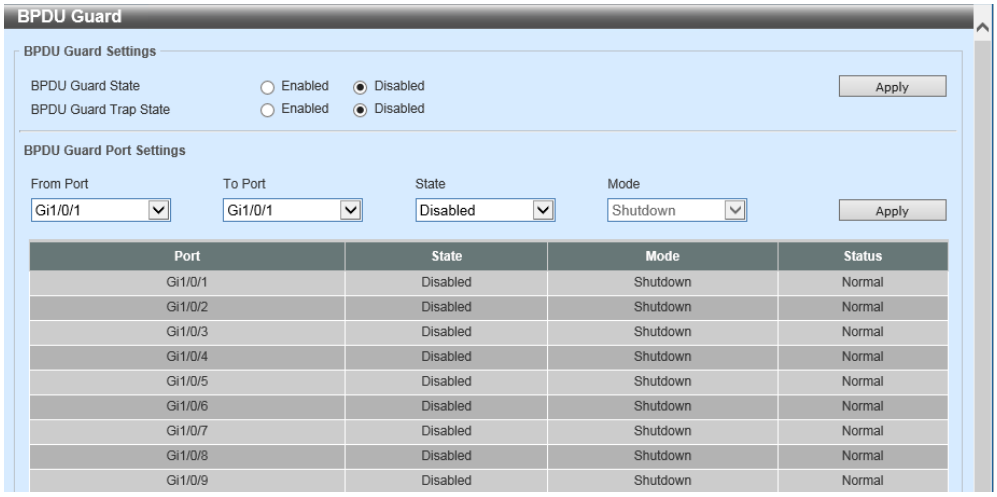


Figure 9-54 BPDU Guard

The following parameters can be configured in the **BPDU Guard Settings** section:

Parameter	Description
BPDU Guard State	Select to globally enable or disable the BPDU Guard feature here.
BPDU Guard Trap State	Select to enable or disable the BPDU Guard trap state here.

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

The following parameters can be configured in the **BPDU Guard Port Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
State	Select to enable or disable BPDU Guard on the port(s) specified.
Mode	Select the BPDU Guard mode that will be applied to the specified port(s). Options to choose from are: • **Drop** - Drop all received BPDU packets when the port enters under attack state. • **Block** - Drop all packets (include BPDU and normal packets) when the port enters under attack state. • **Shutdown** - Shut down the port when the port enters under attack state.

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

9.10 NetBIOS Filtering

This window is used to configure and display the NetBIOS filtering settings on the specified port(s).

Click **Security > NetBIOS Filtering** to view the following window:

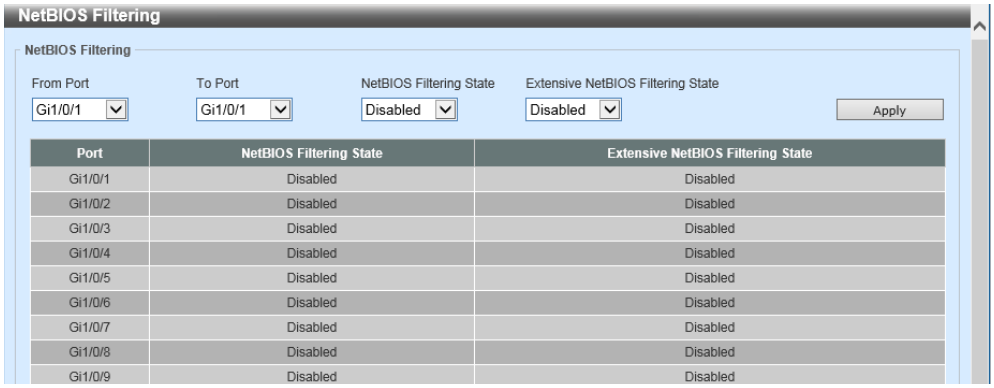


Figure 9-55 NetBIOS Filtering

The following parameters can be configured in the **NetBIOS Filtering** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
NetBIOS Filtering State	Select to enable or disable the NetBIOS filtering state on the specified port(s). This is used to permit or deny NetBIOS packets on physical ports.
Extensive NetBIOS Filtering State	Select to enable or disable the extensive NetBIOS filtering state on the specified port(s). This is used to permit or deny NetBIOS packets over 802.3 frames on physical ports.

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

9.11 MAC Authentication

This window is used to configure and display the MAC authentication settings.

Click **Security > MAC Authentication** to view the following window:

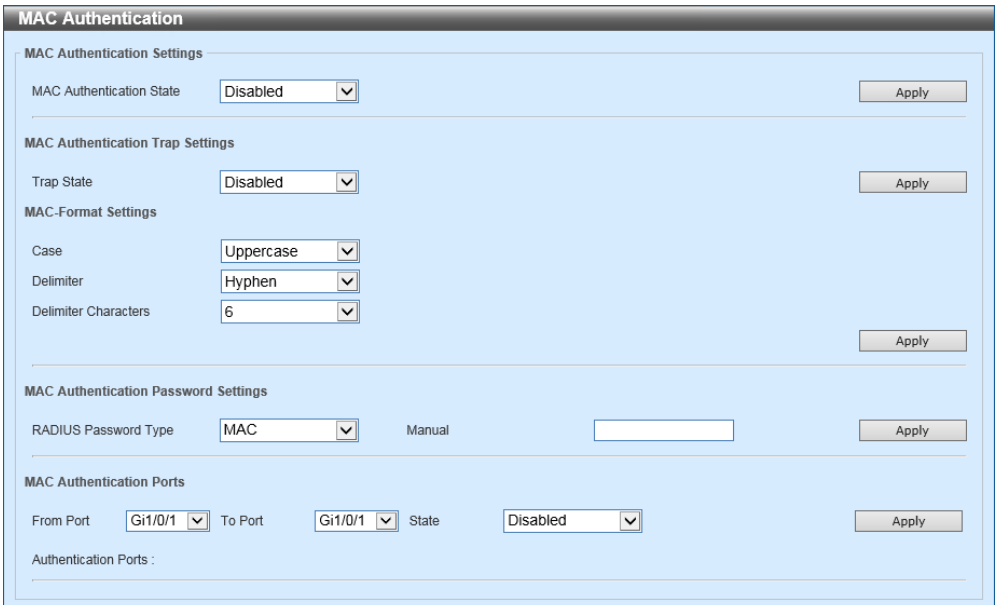


Figure 9-56 MAC Authentication

The following parameters can be configured in the **MAC Authentication Settings** section:

Parameter	Description
MAC Authentication State	Select to globally enable or disable the MAC Authentication feature here.

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

The following parameters can be configured in the **MAC Format Settings** section:

Parameter	Description
Case	Select the letter case that will be used in the MAC address. Options to choose from are: • **Upper Case** - Specifies the use the uppercase format for the MAC address. For example, AA-BB-CC-DD-EE-FF. • **Lower Case** - Specifies the use the lowercase format for the MAC address. For example, aa-bb-cc-dd-ee-ff.

Parameter	Description
Delimiter	Select the type of delimiters that will be used in the MAC address. Options to choose from are: • **Hyphen** - Specifies to use hyphens as delimiters in the MAC address. For example, AA-BB-CC-DD-EE-FF. • **Colon** - Specifies to use colons as delimiters in the MAC address. For example, AA:BB:CC:DD:EE:FF. • **Dot** - Specifies to use dots as delimiters in the MAC address. For example, AA.BB.CC.DD.EE.FF. • **None** - Specifies not to use delimiters in the MAC address. For example, AABBCCDDEEFF.
Delimiter Characters	Select the number of delimiters that will be used in the MAC address. Options to choose from are: • **2** - Specifies to use a single delimiter in the MAC address. For example, AABBCC-DDEEFF. • **4** - Specifies to use two delimiters in the MAC address. For example, AABB-CCDD-EEFF. • **6** - Specifies to use five delimiters in the MAC address. For example, AA-BB-CC-DD-EE-FF.

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

The following parameters can be configured in the **MAC Authentication Password Settings** section:

Parameter	Description
RADIUS Password Type	Select the RADIUS password type here. Options to choose from are: • **MAC Address** - Specifies to use the MAC address as the RADIUS password. • **Manual** - Specifies to use a manual string as the RADIUS password.
Manual	Enter the RADIUS password for the MAC authentication account here.

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

The following parameters can be configured in the **MAC Authentication Ports** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
State	Select to enable or disable MAC authentication for the port(s) specified here.

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

9.12 Web Authentication

9.12.1 Web Authentication Settings

This window is used to configure and display the Web authentication settings.

Click **Security > Web Authentication > Web Authentication Settings** to view the following window:

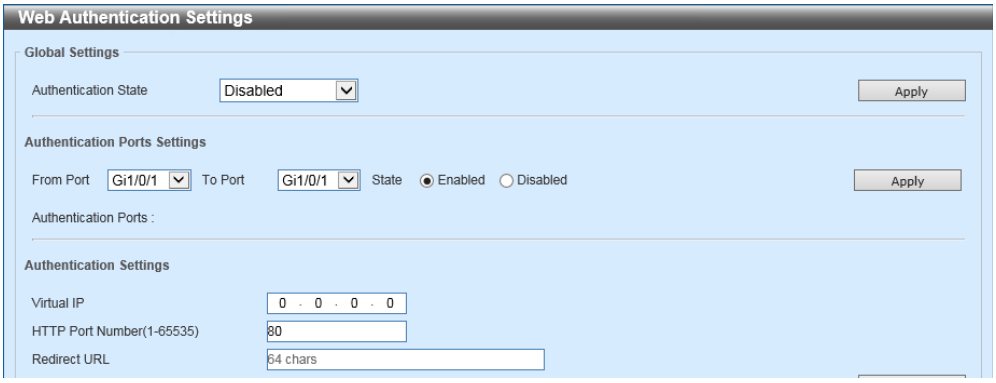


Figure 9-57 Web Authentication Settings

The following parameters can be configured in the **Global Settings** section:

Parameter	Description
Authentication State	Select to globally enable or disable the Web authentication feature.

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

The following parameters can be configured in the **Authentication Port Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
State	Select to enable or disable the Web authentication feature on the specified port(s).

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

The following parameters can be configured in the **Authentication Settings** section:

Parameter	Description
Virtual IP	Enter the virtual IPv4 address used here. All web authentication processes communicate with this virtual IP address, however, the virtual IP does not respond to any ICMP packets or ARP requests. The virtual IPv4 address and the IPv4 address of the switch must use different subnets. The virtual IPv4 address is an essential component for successful web authentication.
HTTP Port Number	Enter the HTTP TCP/UDP port number here. The range is from 1 to 65535. By default, this value is 80. HTTP stands for the Hypertext Transfer Protocol.
Redirect URL	Enter the redirection URL here. This can be up to 64 characters long.

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

9.12.2 Web Page Contents Settings

This window is used to configure and display the Web page content settings.

Click **Security > Web Authentication > Web Page Contents Settings** to view the following window:

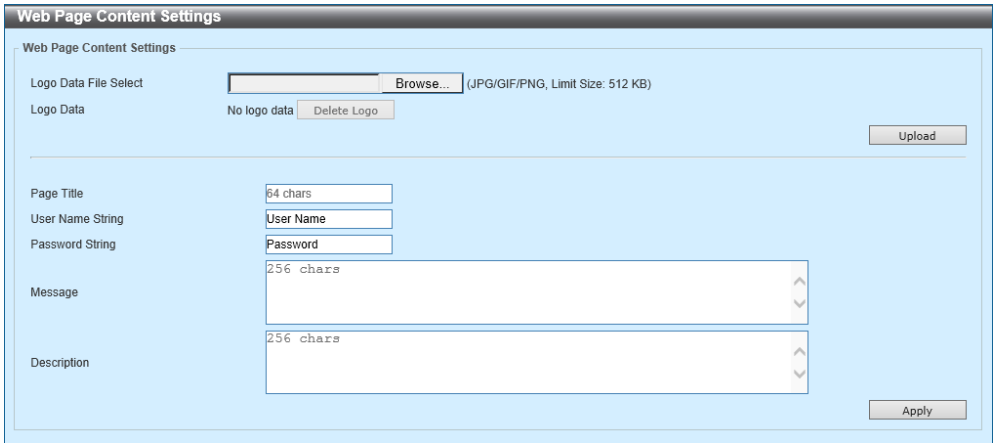


Figure 9-58 Web Page Contents Settings

The following parameters can be configured in the **Web Page Content Settings** section:

Parameter	Description
Logo Data File Select	Click the **Browse** button and navigate to the image file (JPG/GIF/PNG) that will be uploaded here.
Logo Data	This displays the uploaded image file (in use). Click the **Delete Logo** button to delete the existing image file.
Page Title	Enter a custom page title message here. This can be up to 64 characters long.
User Name String	Enter a custom username title here. This can be up to 32 characters long.
Password String	Enter a custom password title here. This can be up to 32 characters long.
Message	Enter a custom message here. This can be up to 256 characters long.
Description	Enter a custom description message here. This can be up to 256 characters long.

Click the **Upload** button to upload the new logo.
Click the **Apply** button to accept the changes made.

9.13 Trusted Host

This window is used to configure and display the trusted host settings.

Click **Security > Trusted Host** to view the following window:

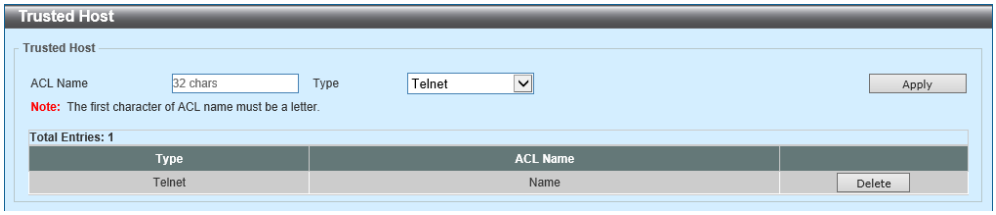


Figure 9-59 Trusted Host

The following parameters can be configured in the **Trusted Host** section:

Parameter	Description
ACL Name	Enter the name of the ACL 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 Hyper Text Transfer Protocol Secure (**HTTPS**).

Click the **Apply** button to add a new entry.
Click the **Delete** button to delete the specified entry.

9.14 Traffic Segmentation Settings

This window is used to configure and display the traffic segmentation settings on the specified port(s).

Click **Security > Traffic Segmentation Settings** to view the following window:

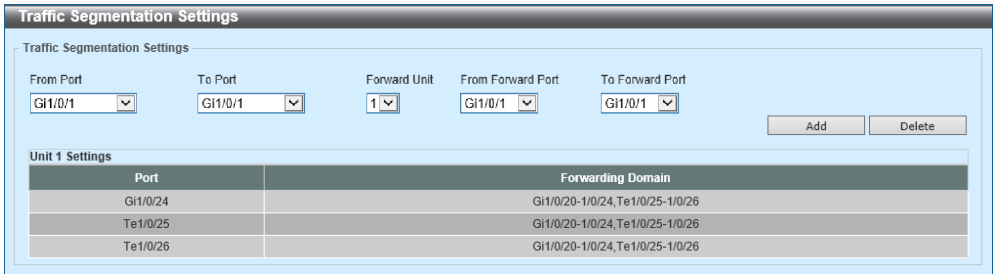


Figure 9-60 Traffic Segmentation Settings

The following parameters can be configured in the **Traffic Segmentation Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will receive packets.
From Forward Port – To Forward Port	Select the port(s) that will forward packets.

Click the **Add** button to add a new entry.
Click the **Delete** button to delete an entry based on the information specified.

9.15 Storm Control

This window is used to configure and display the storm control settings.

Click **Security > Storm Control** to view the following window:

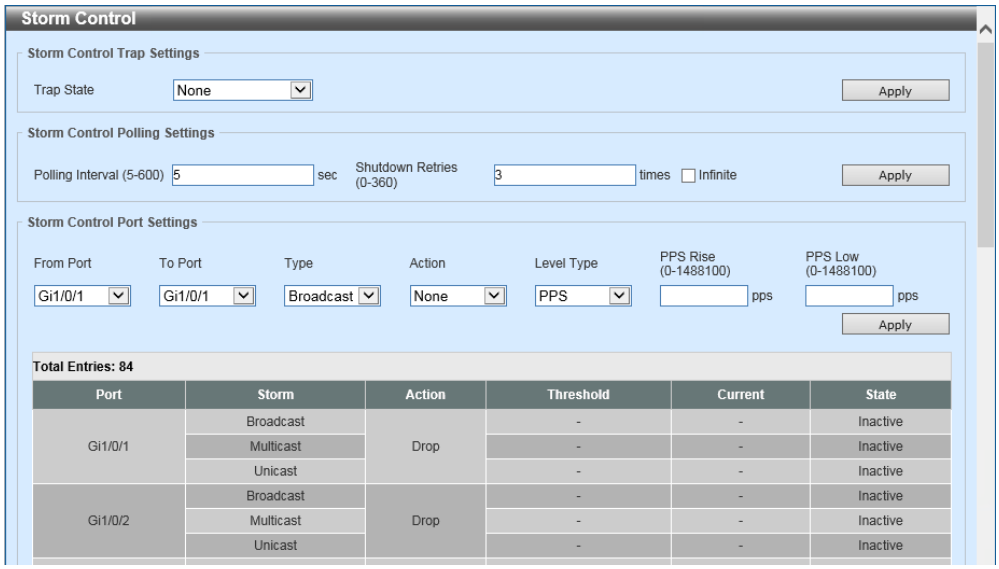


Figure 9-61 Storm Control (Level Type, PPS)

The following parameters can be configured in the **Storm Control Polling Settings** section:

Parameter	Description
Polling Interval	Enter the polling interval value used here. The range is from 5 to 600 seconds. By default, this value is 5 seconds.
Shutdown Retries	Enter the shutdown retries value used here. The range is from 0 to 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 following parameters can be configured in the **Storm Control Port Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used 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 **Shutdown**, 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 discard packets that exceed the risen threshold.
Level Type	Select the level type option here. Options to choose from are Packets Per Second (**PPS**), **Kbps**, and **Level**.
PPS Rise	Enter the PPS rise value here. This option specifies the rise threshold value in packets count per second. The range is from 1 to 255000 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 PPS low value here. This option specifies the low threshold value in packets count per second. The range is from 1 to 255000 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.

Select **Kbps** as the **Level Type** to view the following window:

Figure 9-62 Storm Control (Level Type, Kbps)

The following additional parameters can be configured:

Parameter	Description
KBPS Rise	Enter the KBPS rise value here. This option specifies the rise threshold value as a rate of kilobits per second at which traffic is received on the port. The range is from 1 to 2147483647 Kbps.
KBPS Low	Enter the KBPS low value here. This option specifies the low threshold value as a rate of kilobits per second at which traffic is received on the port. The range is from 1 to 2147483647 Kbps. 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.

Select **Level** as the **Level Type** to view the following window:

Figure 9-63 Storm Control (Level Type, Level)

The following additional parameters can be configured:

Parameter	Description
Level Rise	Enter the level rise value 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. The range is from 1 to 100 percent.
Level Low	Enter the level low value 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. The range is from 1 to 100 percent. 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.

9.16 SSH (Secure Shell)

9.16.1 SSH Global Settings

This window is used to configure and display the global settings associated with the SSH feature.

Click **Security > SSH > SSH Global Settings** to view the following window:

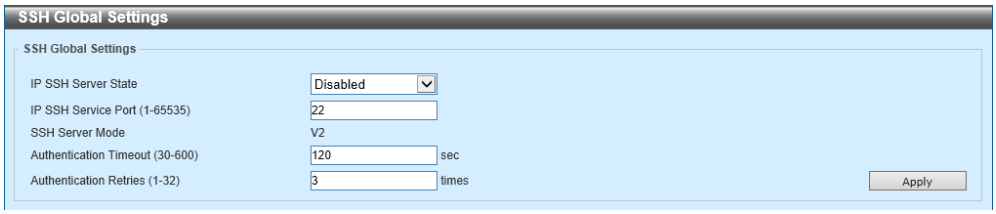


Figure 9-64 SSH Global Settings

The following parameters can be configured in the **SSH Global Settings** section:

Parameter	Description
IP SSH Server State	Select to globally enable or disable the SSH server here.
IP SSH Service Port	Enter the SSH service port number used here. The range is from 1 to 65535. By default, this number is 22.
Authentication Timeout	Enter the authentication timeout value here. The range is from 30 to 600 seconds. By default, this value is 120 seconds.
Authentication Retries	Enter the authentication retries value here. The range is from 1 to 32. By default, this value is 3.

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

9.16.2 Host Key

This window is used to configure and display the SSH host key settings.

Click **Security > SSH > Host Key** to view the following window:

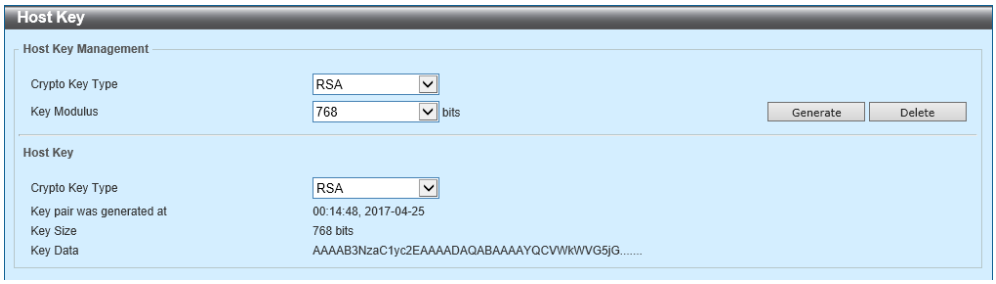


Figure 9-65 Host Key

The following parameters can be configured in the **Host Key Management** section:

Parameter	Description
Crypto Key Type	Select the cryptographic 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 following parameters can be configured in the **Host Key** section:

Parameter	Description
Crypto Key Type	Select the cryptographic key type used here. Options to choose from are RSA and DSA.

9.16.3 SSH Server Connection

This window is used to display the SSH server connection table and information.

Click **Security > SSH > SSH Server Connection** to view the following window:

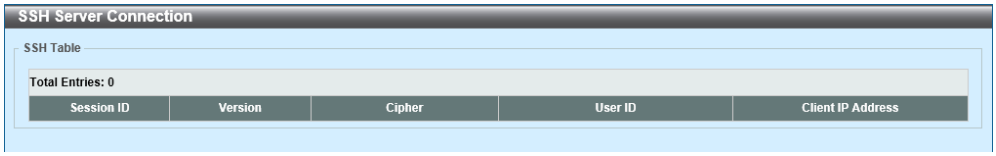


Figure 9-66 SH Server Connection

9.16.4 SSH User Settings

This window is used to configure and display the SSH user settings.

Click **Security > SSH > SSH User Settings** to view the following window:

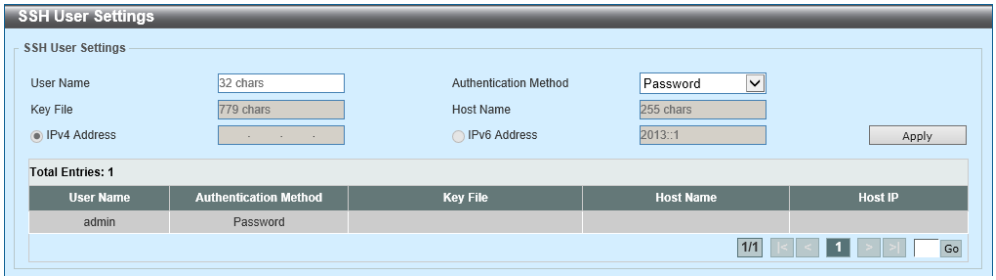


Figure 9-67 SSH User Settings

The following parameters can be configured in the **SSH User Settings** section:

Parameter	Description
User Name	Enter the username for the SSH user account used here. This can be up to 32 characters long.
Authentication Method	Select the SSH authentication method here. Options to choose from are **Password**, **Public Key**, and **Host-based**.
Key File	After selecting **Public Key** or **Host-based**, enter the public key here. This can be up to 779 characters long.
Host Name	After selecting **Host-based**, enter the host name here. This can be up to 255 characters long.
IPv4 Address	After selecting **Host-based**, select and enter the IPv4 address of the SSH user account here.
IPv6 Address	After selecting **Host-based**, select and enter the IPv6 address of the SSH user account here.

Click the **Apply** button to add a new entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

9.17 SSL (Secure Sockets Layer)

9.17.1 SSL Global Settings

This window is used to configure and display the global settings associated with the SSL feature.

Click **Security > SSL > SSL Global Settings** to view the following window:

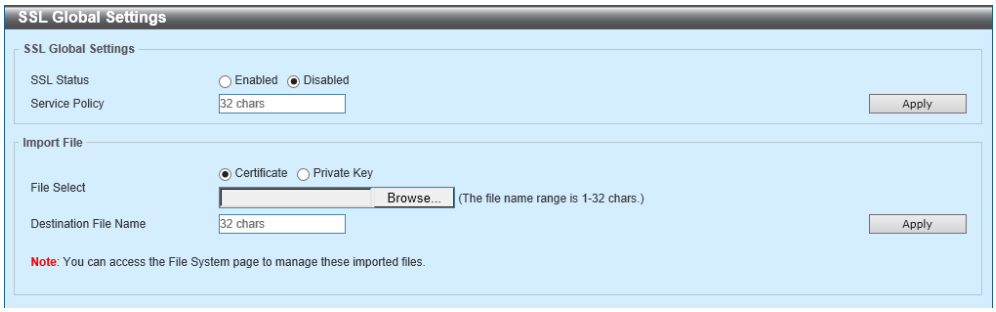


Figure 9-68 SSL Global Settings

The following parameters can be configured in the **SSL Global Settings** section:

Parameter	Description
SSL Status	Select to globally enable or disable the SSL feature 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 following parameters can be configured in the **Import File** section:

Parameter	Description
File Select	Select the file type that will be uploaded here. Options to choose from are **Certificate** and **Private Key**. After selecting the file type, browse to the 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 import the SSL file.

9.17.2 Crypto PKI Trustpoint

This window is used to configure and display the SSL cryptographic Public Key Infrastructure (PKI) trust-point settings.

Click **Security > SSL > Crypto PKI Trustpoint** to view the following window:

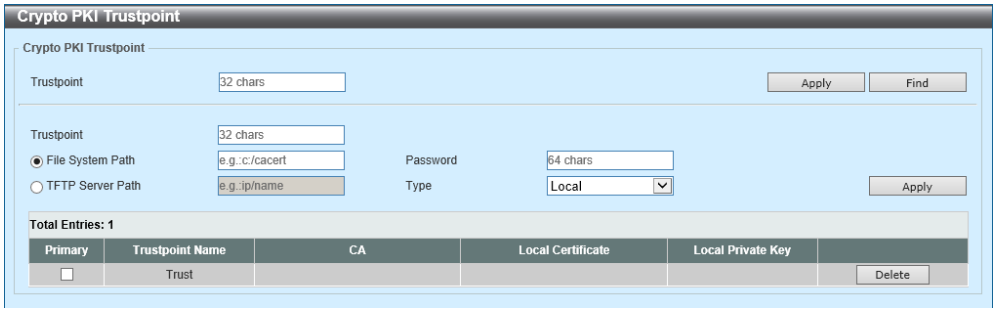


Figure 9-69 Crypto PKI Trustpoint

The following parameters can be configured in the **Crypto PKI Trustpoint** section:

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 Certificate Authority (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.

Click the **Apply** button to add a new entry.
Click the **Find** button to find and display entries based on the search criteria specified.
Click the **Delete** button to delete the specified entry.

9.17.3 SSL Service Policy

This window is used to configure and display the SSL service policy settings.

Click **Security > SSL > SSL Service Policy** to view the following window:

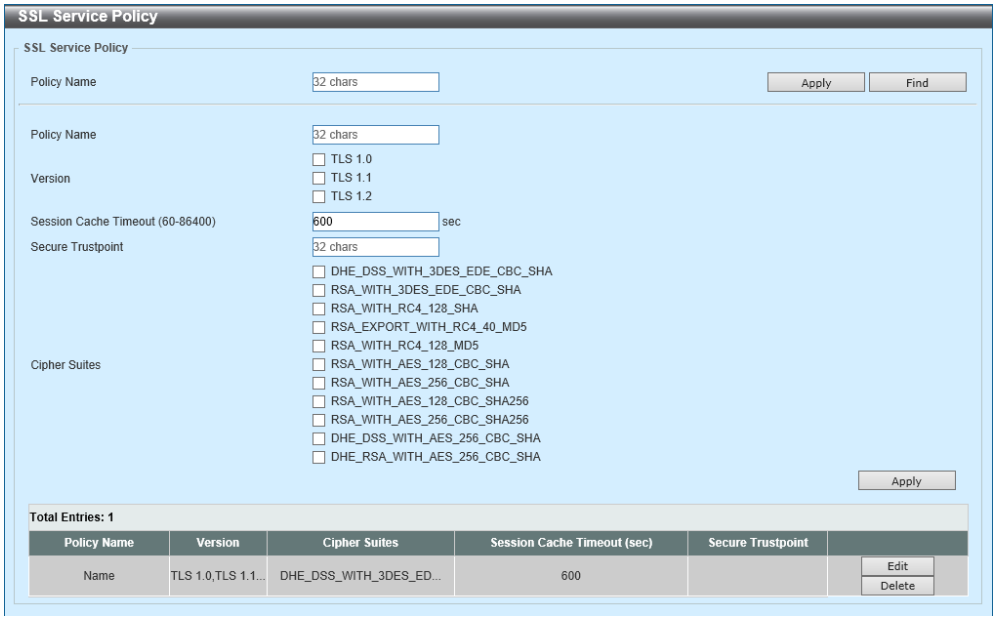


Figure 9-70 SSL Service Policy

The following parameters can be configured in the **SSL Service Policy** section:

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 timeout value for session cache here. The range is from 60 to 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 add a new entry.
Click the **Find** button to find and display entries based on the search criteria specified.
Click the **Edit** button to edit the settings of the specified entry.
Click the **Delete** button to delete the specified entry.

10 OAM (Operations, Administration & Management)

10.1 Cable Diagnostics

This window is used to initiate and display the cable diagnostics test and results on the specified port(s).

Click **OAM > Cable Diagnostics** to view the following window:

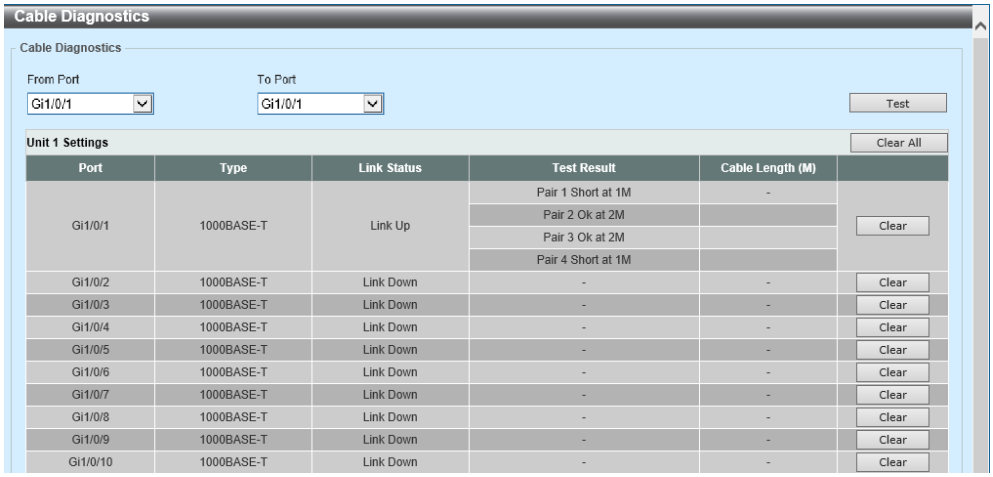


Figure 10-1 Cable Diagnostics

The following parameters can be configured in the **Cable Diagnostics** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.

Click the **Test** button to start the cable diagnostics test on the specified port(s).
Click the **Clear All** button to clear all the cable diagnostics results.
Click the **Clear** button to clear the cable diagnostics results on the specified port.

10.2 1DDM (Digital Diagnostic Monitoring)

10.2.1 DDM Settings

This window is used to configure and display the global settings associated with the DDM feature and the DDM shutdown settings on the specified port(s).

Click **DDM > DDM Settings** to view the following window:

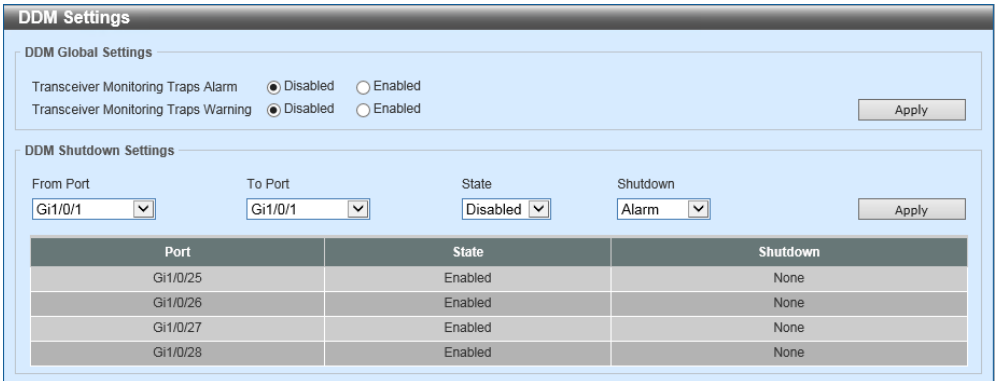


Figure 10-2 DDM Settings

The following parameters can be configured in the **DDM Global Settings** section:

Parameter	Description
Transceiver Monitoring Traps Alarm	Select to enable or disable the sending of transceiver monitoring alarm traps here.
Transceiver Monitoring Traps Warning	Select to enable or disable the sending of transceiver monitoring warning traps here.

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

The following parameters can be configured in the **DDM Shutdown Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
State	Select to enable or disable the DDM feature on the specified port(s) here.
Shutdown	Select the shutdown behavior here. Options to choose from are: • **Alarm** - Specifies to shut down the port when the configured alarm threshold range is exceeded. • **Warning** - Specifies to shut down the port when the configured warning threshold range is exceeded. • **None** - Specifies that the port will never be shut down regardless if the threshold ranges were exceeded or not. This is the default option.

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

10.2.2 DDM Temperature Threshold Settings

This window is used to configure and display the DDM temperature threshold settings on the specified port(s).

Click **DDM > DDM Temperature Threshold Settings** to view the following window:

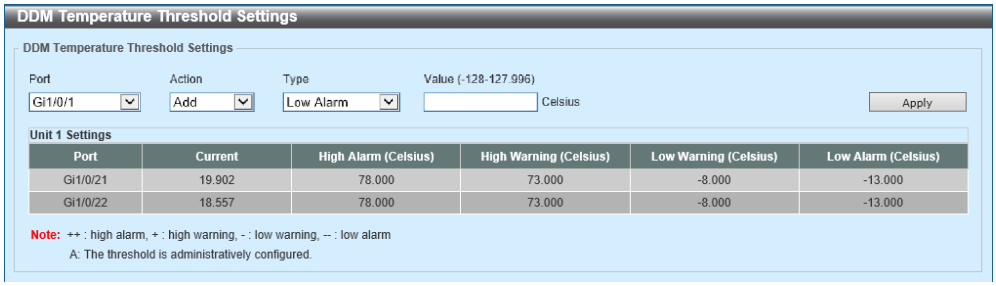


Figure 10-3 DDM Temperature Threshold Settings

The following parameters can be configured in the **DDM Temperature Threshold Settings** section:

Parameter	Description
Port	Select the port that will be used 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. The range is from -128 to 127.996 °C.

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

10.2.3 DDM Voltage Threshold Settings

This window is used to configure and display the DDM voltage threshold settings on the specified port(s).

Click **DDM > DDM Voltage Threshold Settings** to view the following window:

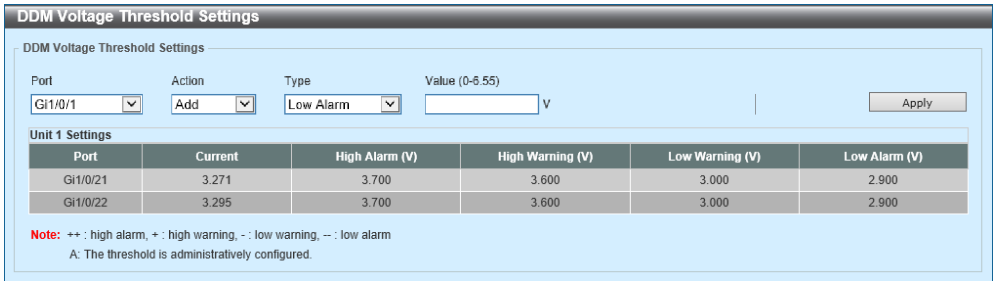


Figure 10-4 DDM Voltage Threshold Settings

The following parameters can be configured in the **DDM Voltage Threshold Settings** section:

Parameter	Description
Port	Select the port that will be used 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. The range is from 0 to 6.55 Volt.

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

10.2.4 DDM Bias Current Threshold Settings

This window is used to configure and display the DDM bias current threshold settings on the specified port(s).

Click **DDM > DDM Bias Current Threshold Settings** to view the following window:

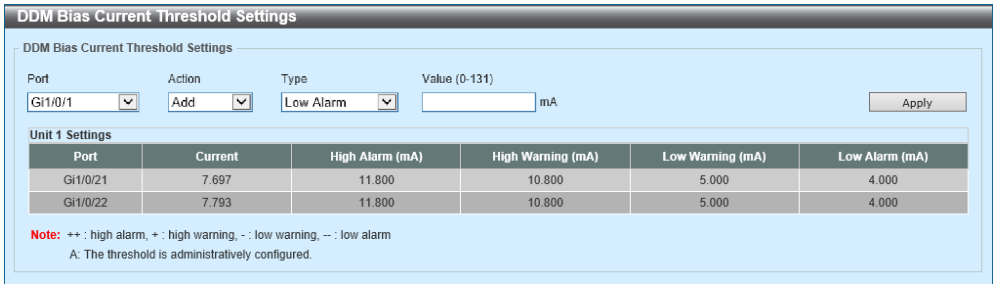


Figure 10-5 DDM Bias Current Threshold Settings

The following parameters can be configured in the **DDM Bias Current Threshold Settings** section:

Parameter	Description
Port	Select the port that will be used here.
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. The range is from 0 to 131 mA.

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

10.2.5 DDM TX Power Threshold Settings

This window is used to configure and display the DDM TX power threshold settings on the specified port(s).

Click **DDM > DDM TX Power Threshold Settings** to view the following window:

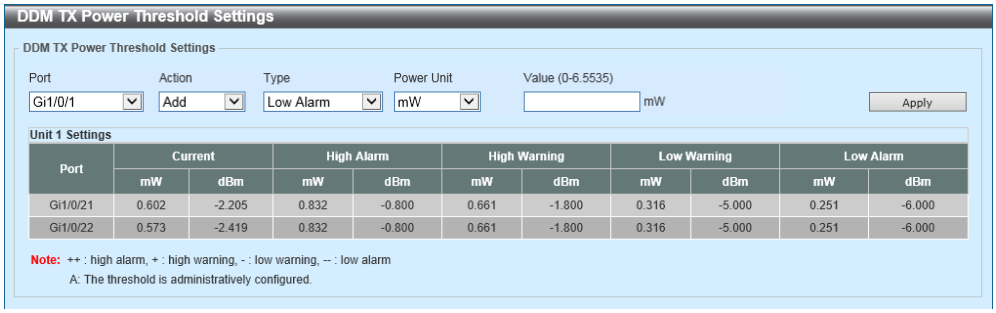


Figure 10-6 DDM TX Power Threshold Settings

The following parameters can be configured in the **DDM TX Power Threshold Settings** section:

Parameter	Description
Port	Select the port that will be used 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 here. • When selecting to specify the threshold value in **mW**, the range is from 0 to 6.5535 mW. • When selecting to specify the threshold value in **dBm**, the range is from -40 to 8.1647 dBm.

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

10.2.6 DDM RX Power Threshold Settings

This window is used to configure and display the DDM RX power threshold settings on the specified port(s).

Click **DDM > DDM RX Power Threshold Settings** to view the following window:

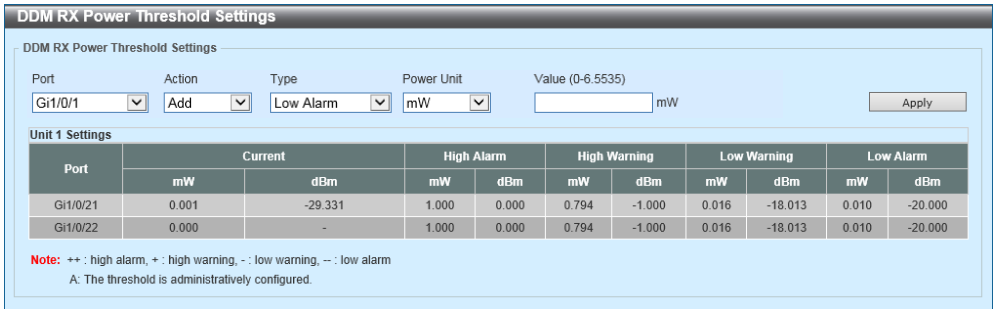


Figure 10-7 DDM RX Power Threshold Settings

The following parameters can be configured in the **DDM RX Power Threshold Settings** section:

Parameter	Description
Port	Select the port that will be used 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 here. • When selecting to specify the threshold value in **mW**, the range is from 0 to 6.5535 mW. • When selecting to specify the threshold value in **dBm**, the range is from -40 to 8.1647 dBm.

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

10.2.7 DDM Status Table

This window is used to display the DDM status table and information.

Click **DDM > DDM Status Table** to view the following window:

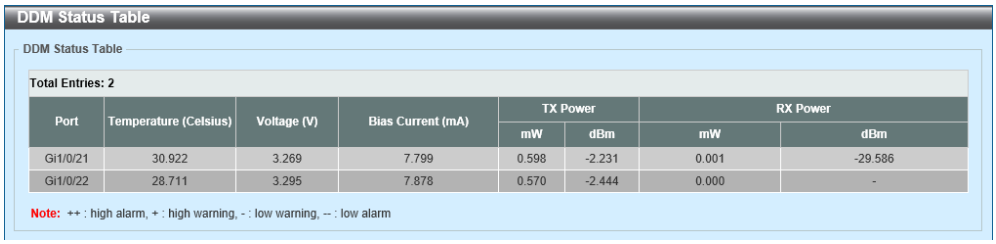


Figure 10-8 DDM Status Table

11 Monitoring

11.1 Utilization

11.1.1 Port Utilization

This window is used to display the port utilization table and information.

Click **Monitoring > Utilization > Port Utilization** to view the following window:

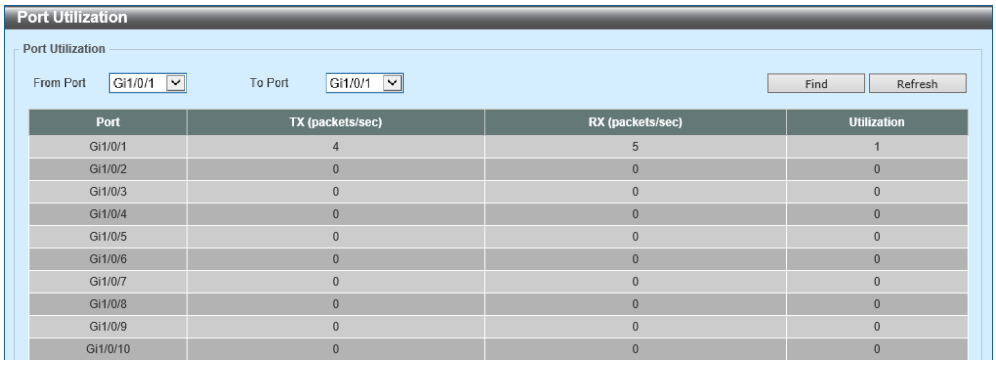


Figure 11-1 Port Utilization

The following parameters can be configured in the **Port Utilization** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.

Click the **Find** button to display the port utilization information related to the specified port(s).
Click the **Refresh** button to refresh the information displayed in the table.

11.2 Statistics

11.2.1 Port

This window is used to display the port RX/TX statistics and information.

Click **Monitoring > Statistics > Port** to view the following window:

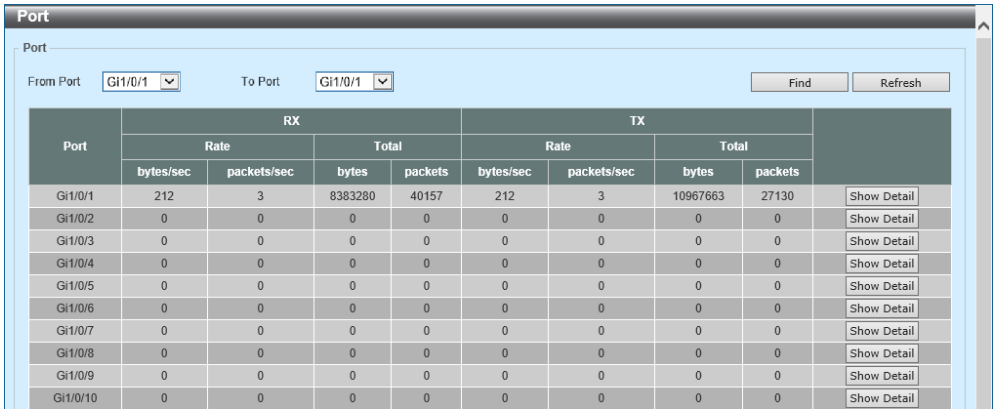


Figure 11-2 Port

The following parameters can be configured in the **Port** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.

Click the **Find** button to display the port statistics information related to the specified port(s).
Click the **Refresh** button to refresh the information displayed in the table.
Click the **Show Detail** button to display detailed information related to the entry.

Click the **Show Detail** button to view the following window:

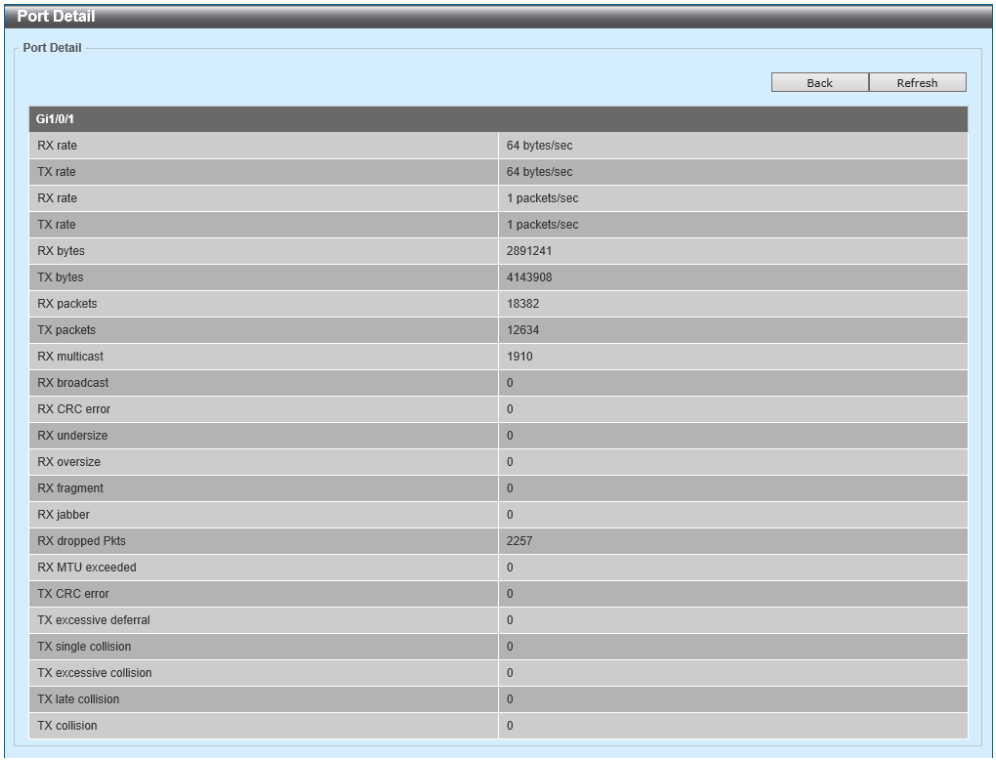


Figure 11-3 Port (Show Detail)

Click the **Back** button to return to the previous window.
Click the **Refresh** button to refresh the information displayed in the table.

11.2.2 Interface Counters

This window is used to display the interface counters statistics and information.

Click **Monitoring > Statistics > Interface Counters** to view the following window:

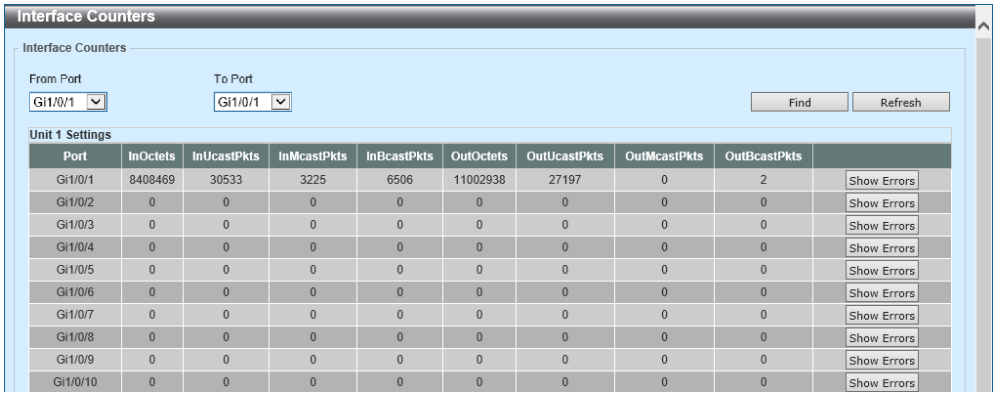


Figure 11-4 Interface Counters

The following parameters can be configured in the **Interface Counters** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.

Click the **Find** button to display the interface counters related to the specified port(s).
Click the **Refresh** button to refresh the information displayed in the table.
Click the **Show Errors** button to display detailed error information related to the entry.

Click the **Show Errors** button to view the following window:

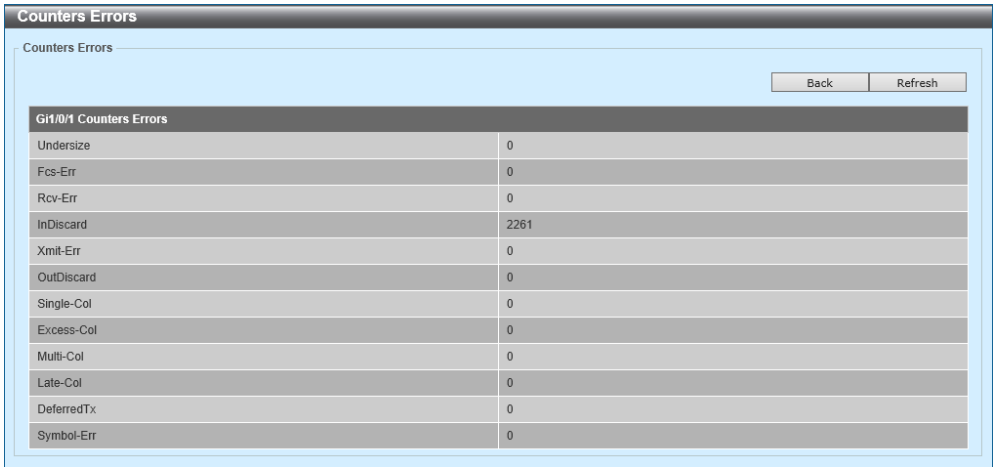


Figure 11-5 Interface Counters (Show Errors)

Click the **Back** button to return to the previous window.
Click the **Refresh** button to refresh the information displayed in the table.

11.2.3 Counters

This window is used to display and clear the link-change counters on the specified port(s).

Click **Monitoring > Statistics > Counters** to view the following window:

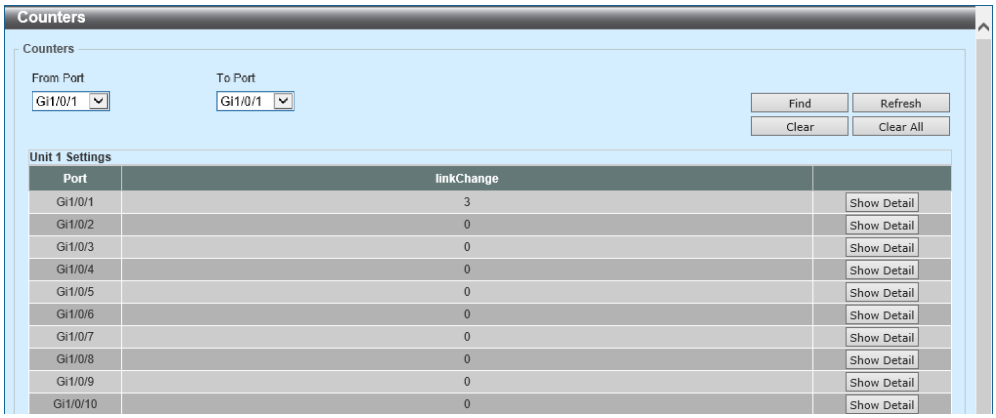


Figure 11-6 Counters

The following parameters can be configured in the **Counters** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.

Click the **Find** button to display the link-change counter information related to the specified port(s).
Click the **Refresh** button to refresh the information displayed in the table.
Click the **Clear** button to clear the link-change counter information related to the specified port(s).
Click the **Clear All** button to clear all the link-change counter information.
Click the **Show Detail** button to display detailed information related to the entry.

Click the **Show Detail** button to view the following window:

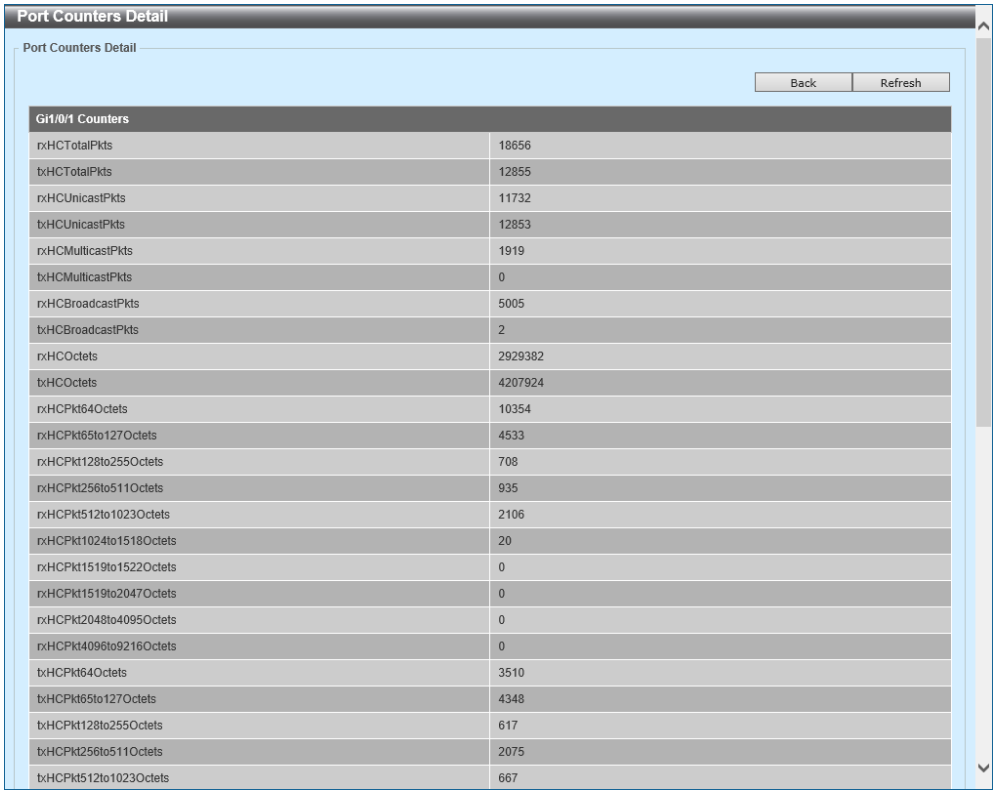


Figure 11-7 Counters (Show Detail)

Click the **Back** button to return to the previous window.
Click the **Refresh** button to refresh the information displayed in the table.

11.3 Mirror Settings

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

Click **Monitoring > Mirror Settings** to view the following window:

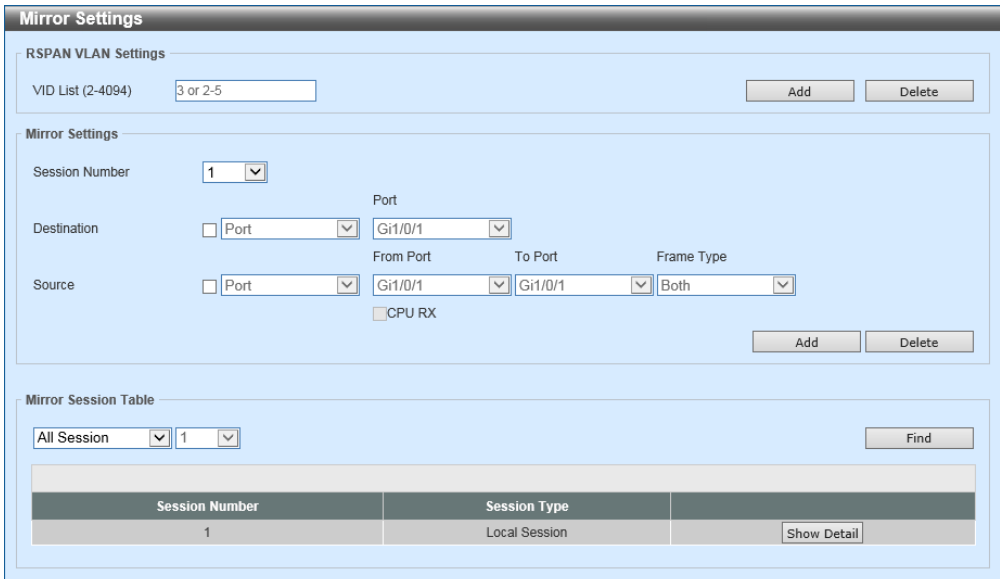


Figure 11-8 Mirror Settings

The following parameters can be configured in the **RSPAN VLAN Settings** section:

Parameter	Description
VID List	Enter the RSPAN VLAN ID(s) that will be used here. A series of VLAN IDs can be entered separated by commas or a range of VLAN IDs can be entered separated by a hyphen. The range is from 2 to 4094.

Click the **Apply** button to add a new entry.
Click the **Delete** button to delete an entry based on the information specified.

The following parameters can be configured in the **Mirror Settings** section:

Parameter	Description
Session Number	Select the mirror session number for this entry here. This number is between 1 and 4.
Destination	Select and configure the destination settings for this port mirror entry here. Select the destination **Port** or **Remote VLAN**. • **Port** - Select the Destination **Port** number. • **Remote VLAN** - Select the Destination **Port** number. Enter the VID in the space provided. The **VID** range is from 2 to 4094.
Source	Select and configure the source settings for this port mirror entry here. Select the source **Port**, **ACL** or **Remote VLAN**. • **Port** - Select the **From Port** and **To Port** numbers. Select the **Frame Type**. Frame type options to choose from are: o**Both** - Specifies that traffic in both the incoming and outgoing directions will be mirrored. o**RX** - Specifies that traffic in only the incoming direction will be mirrored. o**TX** - Specifies that traffic in only the outgoing direction will be mirrored. o**CPU RX** - Specifies to monitor CPU RX traffic. • **ACL** - Enter the **ACL Name** in the space provided. This can be up to 32 characters long. • **Remote VLAN** - Enter the remote VID in the space provided. The range is from 2 to 4094.

Click the **Apply** button to add a new entry.
Click the **Delete** button to delete an entry based on the information specified.

The following parameters can be configured in the **Mirror Session Table** section:

Parameter	Description
Mirror Session Type	Select the mirror session type of information that will be displayed here. Options to choose from are **All Session**, **Session Number**, **Remote Session**, and **Local Session**. After selecting the **Session Number** option, select the session number from the drop-down menu. The range is from 1 to 4.

Click the **Find** button to find and display entries based on the search criteria specified.
Click the **Show Detail** button to display detailed information related to the entry.

Click the **Show Detail** button to view the following window:

Figure 11-9 Mirror Settings (Show Detail)

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

11.4 Device Environment

This window is used to display the current temperature reading, fan status and power module status of the switch.

Click **Monitoring > Device Environment** to view the following window:

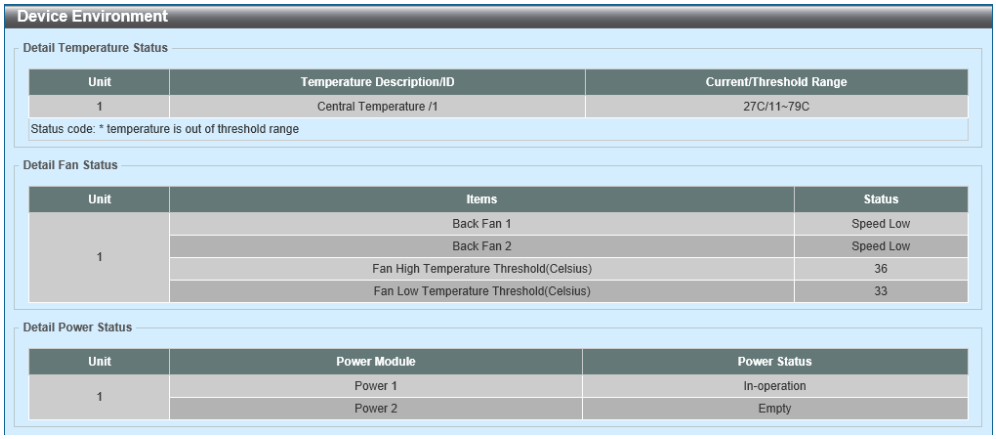


Figure 11-10 Device Environment

12 Eco Mode

12.1 Power Saving

This window is used to configure and display the power saving settings on the specified port(s).

Click **Eco Mode > Power Saving** to view the following window:

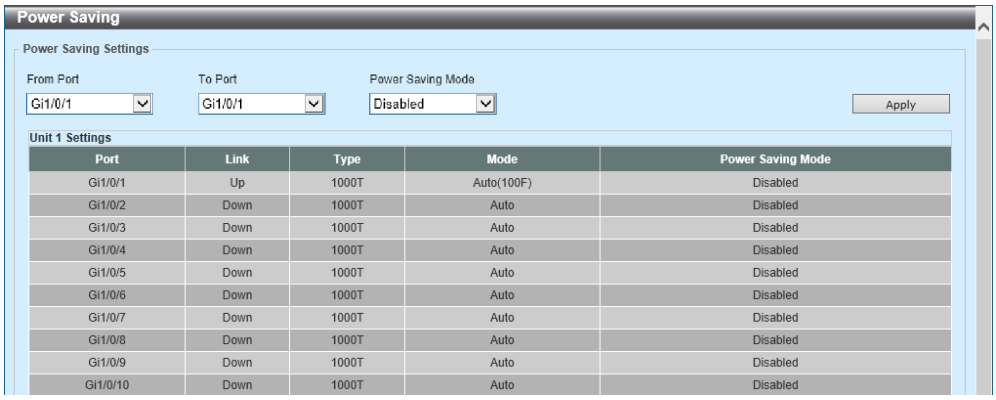


Figure 12-1 Power Saving

The following parameters can be configured in the **Power Saving Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
Power Saving Mode	Select the power saving mode that will be used on the specified port(s). Options to choose from are: • **Disabled** - Specifies to disable the power saving function. • **Full** - Specifies to use the power saving function to its full capacity. • **Half** - Specifies to use half of the power saving function capacity only. This is generally anything between zero and full capacity.

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

12.2 EEE (Energy Efficient Ethernet)

This window is used to configure and display the EEE settings on the specified port(s).

Click **Eco Mode > EEE** to view the following window:

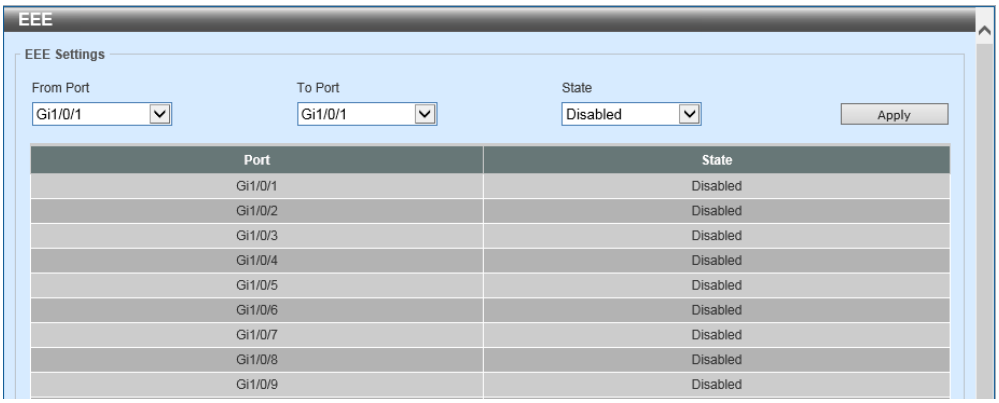


Figure 12-2 EEE

The following parameters can be configured in the **EEE Settings** section:

Parameter	Description
From Port - To Port	Select the port(s) that will be used here.
State	Select to enable or disable the EEE feature on the specified port(s).

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

13 Toolbar

13.1 Save

13.1.1 Save Configuration

This window is used to save the running configuration as the start-up configuration. This is to prevent the loss of configuration in the event of a power failure.

Click **Save > Save Configuration** in the toolbar to view the following window:

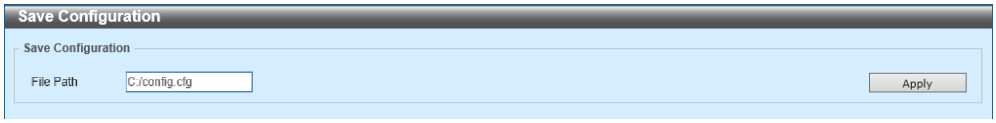


Figure 13-1 Save Configuration

The following parameters can be configured in the **Save Configuration** section:

Parameter	Description
File Path	Enter the filename and path in the space provided.

Click the **Apply** button to save the configuration.

13.2 Tools

13.2.1 Firmware Upgrade & Backup

13.2.1.1 Firmware Upgrade from HTTP

This window is used to upgrade the firmware on the switch from a local PC using HTTP.

Click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP** in the toolbar to view the following window:

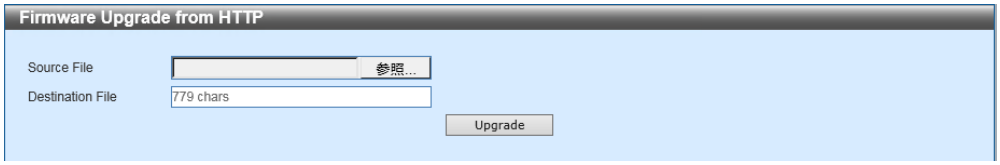


Figure 13-2 Firmware Upgrade from HTTP

The following parameters can be configured:

Parameter	Description
Source File	Click the **Browse** button and navigate to the firmware file (on the local PC) that will be used in this upgrade.
Destination File	Enter the destination path and location where the new firmware should be stored on the Switch. This field can be up to 64 characters long.

Click the **Upgrade** button to start the upgrade.

13.2.1.2 Firmware Upgrade from TFTP

This window is used to upgrade the firmware on the switch from a TFTP server.

Click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from TFTP** in the toolbar to view the following window:

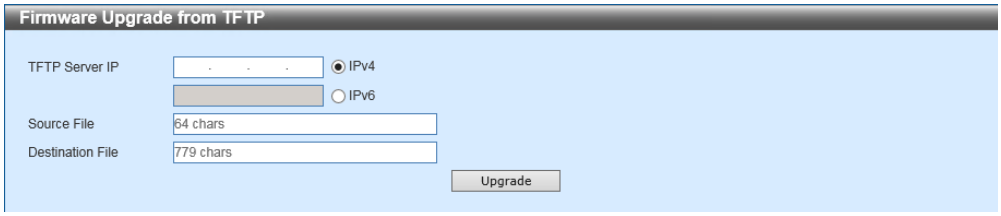


Figure 13-3 Firmware Upgrade from TFTP

The following parameters can be configured:

Parameter	Description
TFTP Server IP	Enter the IP address of the TFTP server here. • **IPv4** - Select and enter the IPv4 address of the TFTP server here. • **IPv6** - Select and enter the IPv6 address of the TFTP server here.
Source File	Enter the source filename and path of the firmware file located on the TFTP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the new firmware should be stored on the Switch. This field can be up to 64 characters long.

Click the **Upgrade** button to start the upgrade.

13.2.1.3 Firmware Upgrade from RCP

This window is used to upgrade the firmware on the switch from an RCP server.

Click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from RCP** in the toolbar to view the following window:

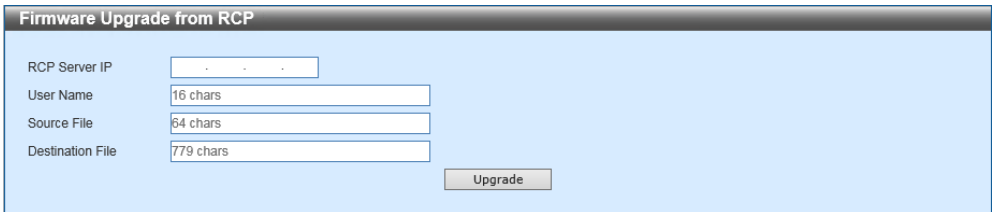


Figure 13-4 Firmware Upgrade from RCP

The following parameters can be configured:

Parameter	Description
RCP Server IP	Enter the IP address of the RCP server here.
User Name	Enter the user name for the RCP connection here. This name can be up to 32 characters long.
Source File	Enter the source filename and path of the firmware file located on the RCP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the new firmware should be stored on the Switch. This field can be up to 64 characters long.

Click the **Upgrade** button to start the upgrade.

13.2.1.4 Firmware Backup to HTTP

This window is used to save a backup copy of the firmware on the switch to a local PC using HTTP.

Click **Tools > Firmware Upgrade & Backup > Firmware Backup to HTTP** in the toolbar to view the following window:

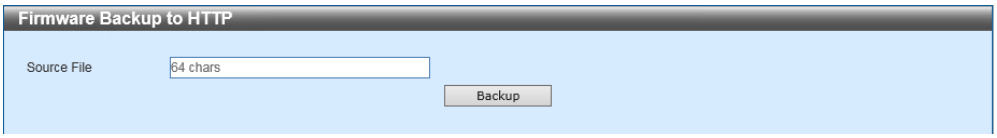


Figure 13-5 Firmware Backup to HTTP

The following parameters can be configured:

Parameter	Description
Source File	Enter the source filename and path of the firmware file located on the Switch here. This field can be up to 64 characters long.

Click the **Backup** button to start the backup.

13.2.1.5 Firmware Backup to TFTP

This window is used to save a backup copy of the firmware on the switch to a TFTP server.

Click **Tools > Firmware Upgrade & Backup > Firmware Backup to TFTP** in the toolbar to view the following window:

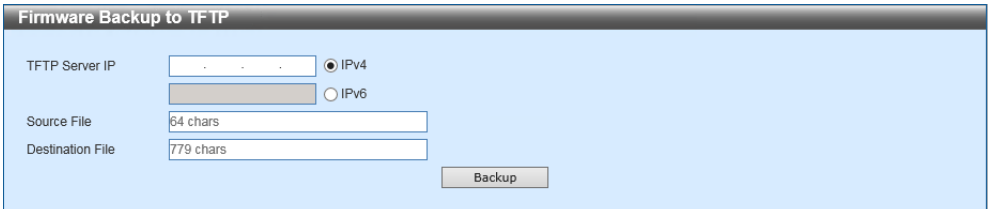


Figure 13-6 Firmware Backup to TFTP

The following parameters can be configured:

Parameter	Description
TFTP Server IP	Enter the IP address of the TFTP server here. • **IPv4** - Select and enter the IPv4 address of the TFTP server here. • **IPv6** - Select and enter the IPv6 address of the TFTP server here.
Source File	Enter the source filename and path of the firmware file located on the Switch here. This field can be up to 64 characters long.
Destination File	Enter the destination filename and path of the firmware file to be backed up to the TFTP server here. This field can be up to 64 characters long.

Click the **Backup** button to start the backup.

13.2.1.6 Firmware Backup to RCP

This window is used to save a backup copy of the firmware on the switch to an RCP server.

Click **Tools > Firmware Upgrade & Backup > Firmware Backup to RCP** in the toolbar to view the following window:

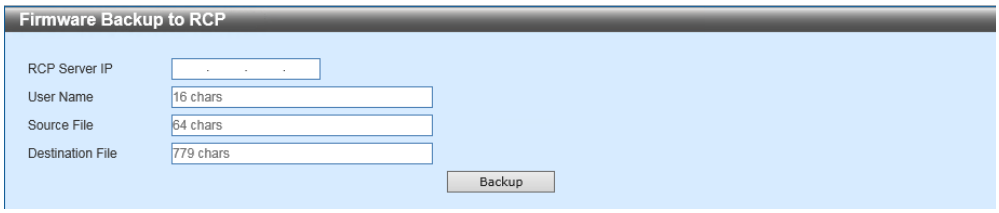


Figure 13-7 Firmware Backup to RCP

The following parameters can be configured:

Parameter	Description
RCP Server IP	Enter the IP address of the RCP server here.
User Name	Enter the user name for the RCP connection here. This name can be up to 32 characters long.
Source File	Enter the source filename and path of the firmware file located on the Switch here. This field can be up to 64 characters long.
Destination File	Enter the destination filename and path of the firmware file to be backed up to the RCP server here. This field can be up to 64 characters long.

Click the **Backup** button to start the backup.

13.2.2 Configuration Restore & Backup

13.2.2.1 Configuration Restore from HTTP

This window is used to restore the configuration on the switch from the local PC using HTTP.

Click **Tools > Configuration Restore & Backup > Configuration Restore from HTTP** in the toolbar to view the following window:

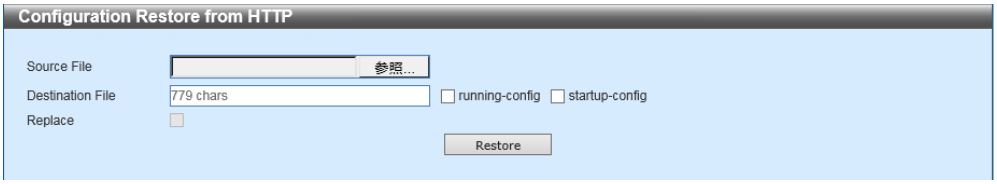


Figure 13-8 Configuration Restore from HTTP

The following parameters can be configured:

Parameter	Description
Source File	Click the **Browse** button and navigate to the configuration file (on the local PC) that will be used in this restore.
Destination File	Enter the destination path and location where the configuration file should be stored on the Switch. This field can be up to 64 characters long. • Select the **running-config** option to restore and overwrite the running configuration file on the Switch. • Select the **startup-config** option to restore and overwrite the start-up configuration file on the Switch.
Replace	Select this option to replace the configuration file on the Switch with this one.

Click the **Restore** button to start the restore.

13.2.2.2 Configuration Restore from TFTP

This window is used to restore the configuration on the switch from a TFTP server.

Click **Tools > Configuration Restore & Backup > Configuration Restore from TFTP** in the toolbar to view the following window:

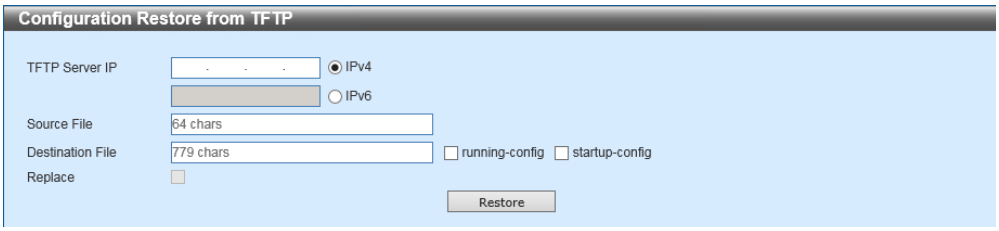


Figure 13-9 Configuration Restore from TFTP

The following parameters can be configured:

Parameter	Description
TFTP Server IP	Enter the IP address of the TFTP server here. • **IPv4** - Select and enter the IPv4 address of the TFTP server here. • **IPv6** - Select and enter the IPv6 address of the TFTP server here.
Source File	Enter the source filename and path of the configuration file located on the TFTP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the configuration file should be stored on the Switch. This field can be up to 64 characters long. • Select the **running-config** option to restore and overwrite the running configuration file on the Switch. • Select the **startup-config** option to restore and overwrite the start-up configuration file on the Switch.
Replace	Select this option to replace the configuration file on the Switch with this one.

Click the **Restore** button to start the restore.

13.2.2.3 Configuration Restore from RCP

This window is used to restore the configuration on the switch from an RCP server.

Click **Tools > Configuration Restore & Backup > Configuration Restore from RCP** in the toolbar to view the following window:

Figure 13-10 Configuration Restore from RCP

The following parameters can be configured:

Parameter	Description
RCP Server IP	Enter the IP address of the RCP server here.
User Name	Enter the user name for the RCP connection here. This name can be up to 32 characters long.
Source File	Enter the source filename and path of the configuration file located on the RCP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the configuration file should be stored on the Switch. This field can be up to 64 characters long. • Select the **running-config** option to restore and overwrite the running configuration file on the Switch. • Select the **startup-config** option to restore and overwrite the start-up configuration file on the Switch.
Replace	Select this option to replace the configuration file on the Switch with this one.

Click the **Restore** button to start the restore.

13.2.2.4 Configuration Backup to HTTP

This window is used to save a backup copy of the configuration on the switch to a local PC using HTTP.

Click **Tools > Configuration Restore & Backup > Configuration Backup to HTTP** in the toolbar to view the following window:

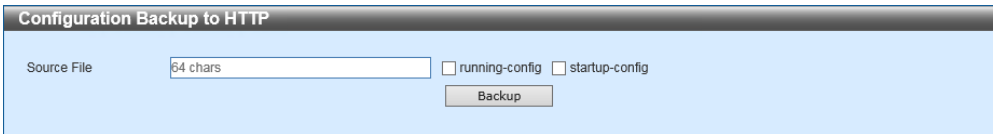


Figure 13-11 Configuration Backup to HTTP

The following parameters can be configured:

Parameter	Description
Source File	Enter the source filename and path of the configuration file located on the Switch here. This field can be up to 64 characters long. • Select the **running-config** option to back up the running configuration file from the Switch. • Select the **startup-config** option to back up the start-up configuration file from the Switch.

Click the **Backup** button to start the backup.

13.2.2.5 Configuration Backup to TFTP

This window is used to save a backup copy of the configuration on the switch to a TFTP server.

Click **Tools > Configuration Restore & Backup > Configuration Backup to TFTP** in the toolbar to view the following window:

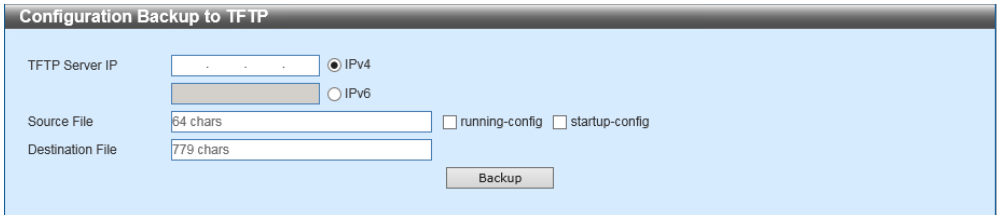


Figure 13-12 Configuration Backup to TFTP

The following parameters can be configured:

Parameter	Description
TFTP Server IP	Enter the IP address of the TFTP server here. • **IPv4** - Select and enter the IPv4 address of the TFTP server here. • **IPv6** - Select and enter the IPv6 address of the TFTP server here.
Source File	Enter the source filename and path of the configuration file located on the Switch here. This field can be up to 64 characters long. • Select the **running-config** option to back up the running configuration file from the Switch. • Select the **startup-config** option to back up the start-up configuration file from the Switch.
Destination File	Enter the destination path and location where the configuration file should be stored on the TFTP server. This field can be up to 64 characters long.

Click the **Backup** button to start the backup.

13.2.2.6 Configuration Backup to RCP

This window is used to save a backup copy of the configuration on the switch to an RCP server.

Click **Tools > Configuration Restore & Backup > Configuration Backup to RCP** in the toolbar to view the following window:

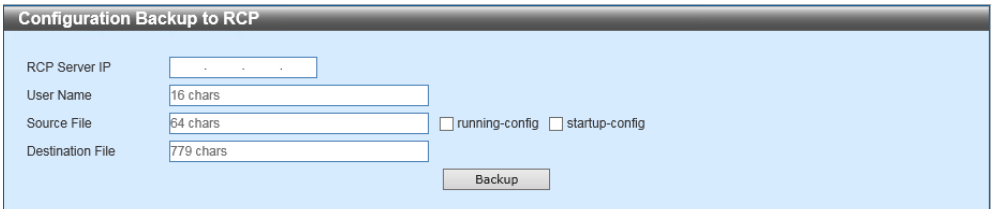


Figure 13-13 Configuration Backup to RCP

The following parameters can be configured:

Parameter	Description
RCP Server IP	Enter the IP address of the RCP server here.
User Name	Enter the user name for the RCP connection here. This name can be up to 32 characters long.
Source File	Enter the source filename and path of the configuration file located on the Switch here. This field can be up to 64 characters long. • Select the **running-config** option to back up the running configuration file from the Switch. • Select the **startup-config** option to back up the start-up configuration file from the Switch.
Destination File	Enter the destination path and location where the configuration file should be stored on the RCP server. This field can be up to 64 characters long.

Click the **Backup** button to start the backup.

13.2.3 Log Backup

13.2.3.1 Log Backup to HTTP

This window is used to save a copy of the system log or the attack log on the switch to a local PC using HTTP.

Click **Tools > Log Backup > Log Backup to HTTP** in the toolbar to view the following window:

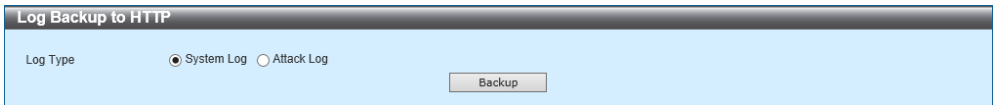


Figure 13-14 Log Backup to HTTP

The following parameters can be configured:

Parameter	Description
Log Type	Select the log type that will be backed up to the local PC using HTTP. • **System Log** - Specifies that the system log will be backed up. • **Attack Log** - Specifies that the attack log will be backed up.

Click the **Backup** button to start the backup.

13.2.3.2 Log Backup to TFTP

This window is used to save a copy of the system log or the attack log on the switch to a TFTP server.

Click **Tools > Log Backup > Log Backup to TFTP** in the toolbar to view the following window:

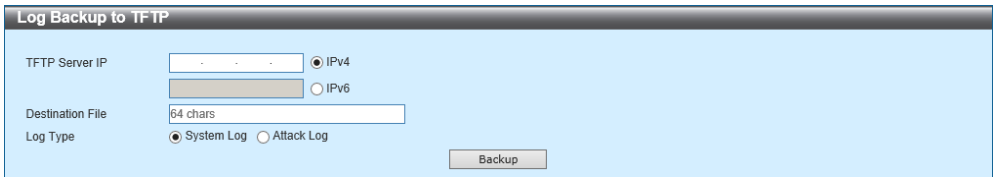


Figure 13-15 Log Backup to TFTP

The following parameters can be configured:

Parameter	Description
TFTP Server IP	Enter the IP address of the TFTP server here. • **IPv4** - Select and enter the IPv4 address of the TFTP server here. • **IPv6** - Select and enter the IPv6 address of the TFTP server here.
Destination File	Enter the destination path and location where the log file should be stored on the TFTP server. This field can be up to 64 characters long.
Log Type	Select the log type that will be backed up to the TFTP server. • **System Log** - Specifies that the system log will be backed up. • **Attack Log** - Specifies that the attack log will be backed up.

Click the **Backup** button to start the backup.

13.2.3.3 Log Backup to RCP

This window is used to save a copy of the system log or the attack log on the switch to an RCP server.

Click **Tools > Log Backup > Log Backup to RCP** in the toolbar to view the following window:

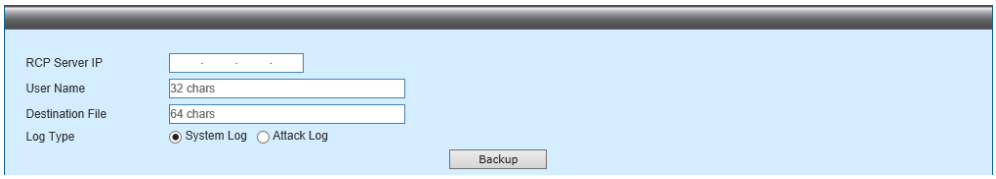


Figure 13-16 Log Backup to RCP

The following parameters can be configured:

Parameter	Description
RCP Server IP	Enter the IP address of the RCP server here.
User Name	Enter the user name for the RCP connection here. This name can be up to 32 characters long.
Destination File	Enter the destination path and location where the log file should be stored on the RCP server. This field can be up to 64 characters long.
Log Type	Select the log type that will be backed up to the RCP server. • **System Log** - Specifies that the system log will be backed up. • **Attack Log** - Specifies that the attack log will be backed up.

Click the **Backup** button to start the backup.

13.2.4 Ping

This window is used to ping a destination IPv4/IPv6 address or domain name to test network connectivity. An access list can be applied to the ping request.

Click **Tools > Ping** in the toolbar to view the following window:

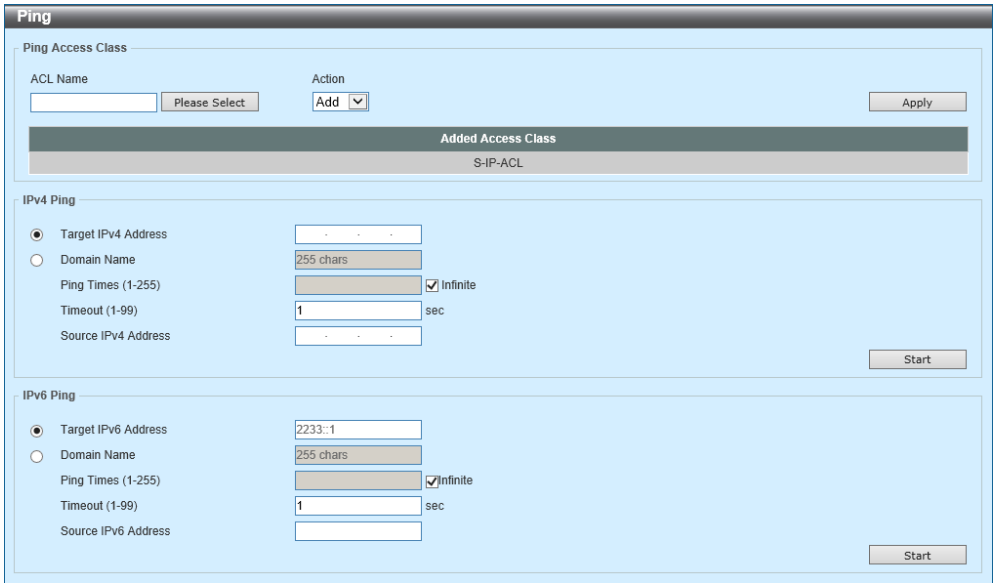


Figure 13-17 Ping

The following parameters can be configured in the **Ping Access Class** section:

Parameter	Description
ACL Name	Enter the name of the ACL that will be used here. This name can be up to 32 characters long. Click the **Please Select** button to select an existing ACL from the list.
Action	Select the action to be taken here. Options to choose from are **Add** and **Clear**.

Click the **Apply** button to use the selected access control list.

The following parameters can be configured in the **IPv4 Ping** section:

Parameter	Description
Target IPv4 Address	Select and enter the destination IPv4 address here.
Domain Name	Select and enter the destination domain name here. This can be up to 255 characters long.
Ping Times	Enter the number of times desired to attempt to Ping the IPv4 address configured in this window. The range is from 1 to 255. Tick the **Infinite** check box to keep sending ICMP Echo packets to the specified IPv4 address until the program is stopped.
Timeout	Enter the timeout period for Ping messages. If the packet fails to find the IPv4 address in this specified time, the Ping packet will be dropped. The range is from 1 to 99 seconds.
Source IPv4 Address	Enter the source IPv4 address. If the Switch has more than one IPv4 address, one of them can be entered here. When entered, this IPv4 address will be used as the source IPv4 address of the packets sent to the remote host.

Click the **Start** button to start the IPv4 ping.

The following parameters can be configured in the **IPv6 Ping** section:

Parameter	Description
Target IPv6 Address	Select and enter the destination IPv6 address here.
Domain Name	Select and enter the destination domain name here. This can be up to 255 characters long.
Ping Times	Enter the number of times desired to attempt to Ping the IPv6 address configured in this window. The range is from 1 to 255. Tick the **Infinite** check box to keep sending ICMP Echo packets to the specified IPv6 address until the program is stopped.
Timeout	Enter the timeout period for Ping messages. If the packet fails to find the IPv6 address in this specified time, the Ping packet will be dropped. The range is from 1 to 99 seconds.
Source IPv6 Address	Enter the source IPv6 address. If the Switch has more than one IPv6 address, one of them can be entered here. When entered, this IPv6 address will be used as the source IPv6 address of the packets sent to the remote host.

Click the **Start** button to start the IPv6 ping.

Select and enter the **IPv4 Ping** parameters and click the **Start** button to view the following window:

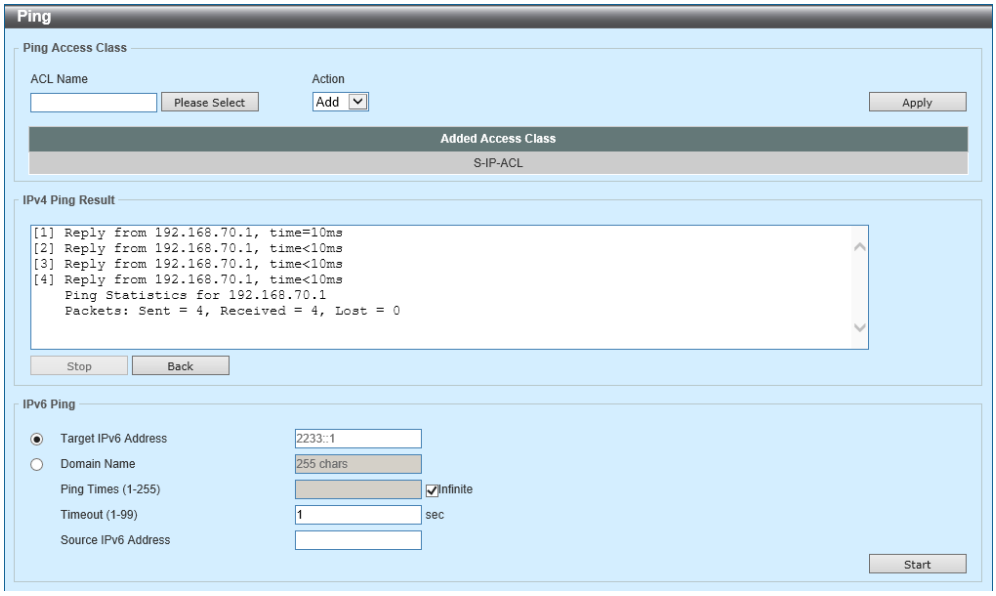


Figure 13-18 Ping (Results)

Click the **Stop** button to stop the pinging process.
Click the **Back** button to return to the original Ping window.

Click the **Please Select** button to view the following window:

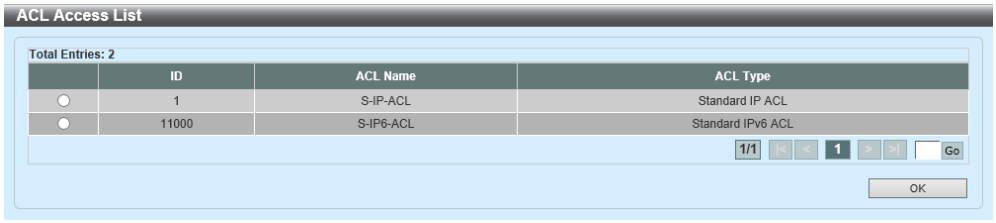


Figure 13-19 Ping (Please Select)

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.
Click the **OK** button to use the selected access control list.

13.2.5 Trace Route

This window is used to trace a route to a destination IPv4/IPv6 address or domain name to test network connectivity.

Click **Tools > Trace Route** in the toolbar to view the following window:

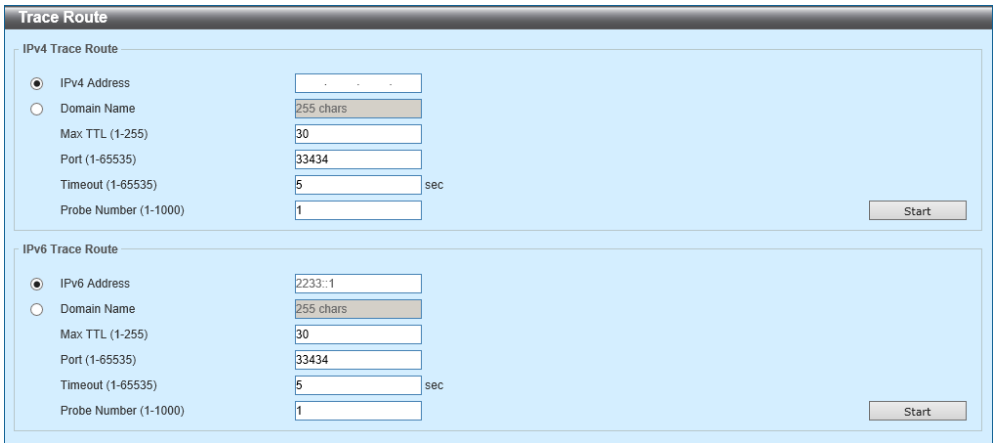


Figure 13-20 Trace Route

The following parameters can be configured in the **IPv4 Trace Route** section:

Parameter	Description
IPv4 Address	Select and enter the destination IPv4 address here.
Domain Name	Select and enter the destination domain name here. This can be up to 255 characters long.
Max TTL	Enter the maximum Time-To-Live (TTL) value of the trace route request here. This is the maximum number of routers that a trace route packet can pass. The trace route option will cross while seeking the network path between two devices. The range is from 1 to 255 hops.
Port	Enter the port number here. The range is from 1 to 65535.
Timeout	Enter the timeout period while waiting for a response from the remote device here. The range is from 1 to 65535 seconds. The default is 5 seconds.
Probe Number	Enter the probe time number here. The range is from 1 to 1000. The default value is 1.

Click the **Start** button to start the IPv4 trace route.

The following parameters can be configured in the **IPv6 Trace Route** section:

Parameter	Description
IPv6 Address	Select and enter the destination IPv6 address here.
Domain Name	Select and enter the destination domain name here. This can be up to 255 characters long.
Max TTL	Enter the maximum TTL value of the trace route request here. This is the maximum number of routers that a trace route packet can pass. The trace route option will cross while seeking the network path between two devices. The range is from 1 to 255 hops.
Port	Enter the port number here. The range is from 1 to 65535.
Timeout	Enter the timeout period while waiting for a response from the remote device here. The range is from 1 to 65535 seconds. The default is 5 seconds.
Probe Number	Enter the probe time number here. The range is from 1 to 1000. The default value is 1.

Click the **Start** button to start the IPv6 trace route.

Select and enter the **IPv4 Trace Route** parameters and click the **Start** button to view the following window:

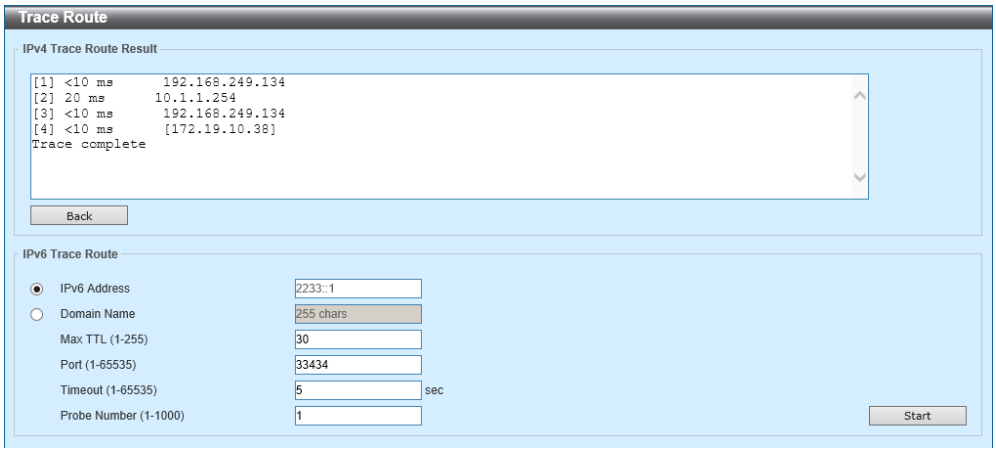


Figure 13-21 Trace Route (Results)

Click the **Back** button to return to the original Trace Route window.

13.2.6 Reset

This window is used initiate a factory reset of the software configuration on the switch.

Click **Tools > Reset** in the toolbar to view the following window:

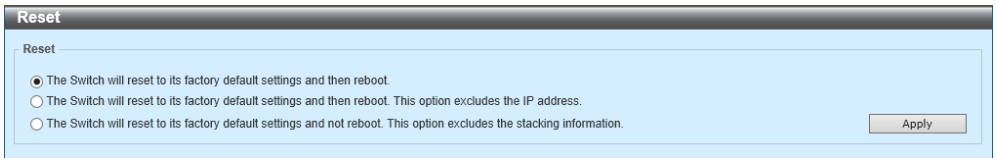


Figure 13-22 Reset

The following parameters can be configured:

Parameter	Description
Reset	Select one of the following reset options: • The Switch will reset to its factory default settings and then reboot. • The Switch will reset to its factory default settings and then reboot. This option excludes the IP address. • The Switch will reset to its factory default settings and not reboot.

Click the **Apply** button to start the factory reset.

13.2.7 Reboot System

This window is used to initiate a reboot of the switch. Any new configuration changes made since the last reboot or power-up will be lost if the changes were not saved.

Click **Tools > Reboot System** in the toolbar to view the following window:

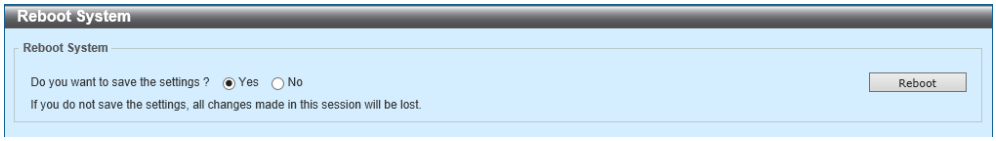


Figure 13-23 Reboot System

Select the **Yes** option to save the new configurations made before the reboot.
Select the **No** option to discard the new configurations made before the reboot.
Click the **Reboot** button to start the reboot.

13.3 Language

Select the language of the Web UI here. By default, English and Japanese can be selected.

Select the language in the toolbar as illustrated below:

Figure 13-24 Language

13.4 Logout

Click the **Logout** option, in the toolbar, to log out of the Web UI of the switch.

Figure 13-25 Logout

14 Appendix - System Log Entries

14.1 802.1X

ID	Log Description	Severity
1.	Event Description: 802.1X Authentication successful. Log Message: [802.1X](<method>) Authorized user <username> (<macaddr>) on Port <portNum> to VLAN <vid> Parameters Description: method: Indicates local or RADIUS. username: The user that is being authenticated. macaddr: The MAC address of the authenticated device. portNum: The switch port number. vid: The authorized VLAN ID.	Informational
2.	Event Description: 802.1X Authentication failure. Log Message: [802.1X](<method>)Rejected user <username> (<macaddr>) on Port <portNum> Parameters Description: method: local or RADIUS. username: TIndicateshe user that is being authenticated. macaddr: The MAC address of the authenticated device. portNum: The switch port number.	Notice
3.	Event Description: The 802.1X authentication table full, cannot authenticate new address. Log Message: [802.1X]Rejected <macaddr> on Port <portNum> (auth table was full) Parameters Description: macaddr: The MAC address of the authenticated device. portNum: The switch port number.	Notice

14.2 AAA

ID	Log Description	Severity
1.	Event Description: Successful login. Log Message: Successful login through <Console | Telnet | SSH>(Username: <username>, IP: <ipaddr | ipv6address>) Parameters Description: ipaddr: The IP address. username: The user name. ipv6address: The IPv6 address.	Informational
2.	Event Description: Login failed. Log Message: Login failed through <Console | Telnet | SSH> (Username: <username>, IP: <ipaddr | ipv6address>) Parameters Description: ipaddr: The IP address. username: The user name. ipv6address: The IPv6 address.	Warning
3.	Event Description: Logout. Log Message: Logout through <Console | Telnet | SSH> (Username: <username>, IP: <ipaddr | ipv6address>) Parameters Description: ipaddr: The IP address. username: The user name. ipv6address: The IPv6 address.	Informational
4.	Event Description: Session timed out. Log Message: <Console | Telnet > session timed out (Username: <username>, IP: <ipaddr | ipv6address>) Parameters Description: ipaddr: The IP address. username: The user name. ipv6address: The IPv6 address.	Informational
5.	Event Description: SSH server is enabled. Log Message: SSH server is enabled	Informational
6.	Event Description: SSH server is disabled. Log Message: SSH server is disabled	Informational
7.	Event Description: Authentication Policy is enabled. Log Message: Authentication Policy is enabled (Module: AAA)	Informational
8.	Event Description: Authentication Policy is disabled. Log Message: Authentication Policy is disabled (Module: AAA)	Informational
9.	Event Description: Login failed due to AAA server timeout or improper configuration. Log Message: Login failed through <Console | Telnet | SSH> from <ipaddr | ipv6address> due to AAA server <ipaddr | ipv6address> timeout or improper configuration (Username: <username>) Parameters Description: ipaddr: The IP address. ipv6address: The IPv6 address. username: The user name.	Warning

ID	Log Description	Severity
10.	Event Description: Successful Enable Admin authenticated by AAA local or none or server. Log Message: Successful Enable Admin through <Console | Telnet | SSH> from <ipaddr | ipv6address> authenticated by AAA <local | none | server <ipaddr | ipv6address>> (Username: <username>) Parameters Description: local: Enable admin by AAA local method. none: Enable admin by AAA none method. server: Enable admin by AAA server method. ipaddr: The IP address. ipv6address: The IPv6 address. username: The user name.	Informational
11.	Event Description: Enable Admin failed due to AAA server timeout or improper configuration. Log Message: Enable Admin failed through <Console | Telnet | SSH> from <ipaddr | ipv6address> due to AAA server <ipaddr | ipv6address> timeout or improper configuration (Username: <username>) Parameters Description: ipaddr: The IP address. ipv6address: The IPv6 address. username: The user name.	Warning
12.	Event Description: Enable Admin failed authenticated by AAA local or server. Log Message: Enable Admin failed through <Console | Telnet | SSH> from <ipaddr | ipv6address> authenticated by AAA < local | server <ipaddr | ipv6address>> (Username: <username>) Parameters Description: local: Enable admin by AAA local method. server: Enable admin by AAA server method. ipaddr: The IP address. ipv6address: The IPv6 address. username: The user name.	Warning
13.	Event Description: Successful login authenticated by AAA local or none or server. Log Message: Successful login through <Console | Telnet | SSH> from < ipaddr | ipv6address > authenticated by AAA <local | none | server <ipaddr | ipv6address>> (Username: <username>) Parameters Description: local: Specify AAA local method. none: Specify none method. server: Specify AAA server method. ipaddr: The IP address. ipv6address: The IPv6 address. username: The user name.	Informational
14.	Event Description: Login failed authenticated by AAA local or server. Log Message: Login failed through <Console | Telnet | SSH> from <ipaddr | ipv6address> authenticated by AAA <local | server <ipaddr | ipv6address>> (Username: <username>) Parameters Description: local: Specify AAA local method. server: Specify AAA server method. ipaddr: The IP address. ipv6address: The IPv6 address. username: The user name.	Warning

14.3 ARP

ID	Log Description	Severity
1.	Event Description: Gratuitous ARP detected duplicate IP. Log Message: Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>, Interface: <ipif_name>) Parameters Description: ipaddr: The IP address which is duplicated with our device. macaddr: The MAC address of the device that has duplicated IP address as our device. portNum: 1.Interger value; 2.Represent the logic port number of the device. ipif_name: The name of the interface of the switch which has the conflict IP address.	Warning

14.4 Authentication (2-step)

ID	Log Description	Severity
1.	Event Description: 2-step Authentication successful. Log Message: [<step-mode>] (<method>) Authorized user <username> (<macaddr>) on Port <portNum> to VLAN <vid> Parameters Description: step-mode: Indicates 2-step authentication mode. method: Indicates local or RADIUS. username: The user that is being authenticated. macaddr: The MAC address of the authenticated device. portNum: The switch port number. vid: The authorized VLAN ID.	Informational
2.	Event Description: MAC-WEB Authentication failures. Log Message: [MAC-WEB] (<method>) Rejected at MAC auth <macaddr>) on Port <portNum> Parameters Description: method: Indicates local or RADIUS. macaddr: The MAC address of the authenticated device. portNum: The switch port number.	Notice
3.	Event Description: MAC-WEB Authentication failures. Log Message: [MAC-WEB] (<method>) Rejected at WEB auth user <username> (<macaddr>) on Port <portNum> Parameters Description: method: Indicates local or RADIUS. username: The user that is being rejected. macaddr: The MAC address of the authenticated device. portNum: The switch port number.	Notice
4.	Event Description: MAC-802.1X Authentication failures. Log Message: [MAC-802.1X] (<method>) Rejected at MAC auth <macaddr>) on Port <portNum> Parameters Description: method: Indicates local or RADIUS. macaddr: The MAC address of the authenticated device. portNum: The switch port number.	Notice
5.	Event Description: MAC-802.1X Authentication failures. Log Message: [MAC-802.1X] (<method>) Rejected at 802.1X auth user <username> (<macaddr>) on Port <portNum> Parameters Description: method: Indicates local or RADIUS. username: The user that is being rejected. macaddr: The MAC address of the authenticated device. portNum: The switch port number.	Notice
6.	Event Description: 802.1 X-WEB Authentication failures. Log Message: [802.1X-WEB] (<method>) Rejected at 802.1X auth user <username> (<macaddr>) on Port <portNum> Parameters Description: method: Indicates local or RADIUS. username: The user that is being rejected. macaddr: The MAC address of the authenticated device. portNum: The switch port number.	Notice

ID	Log Description	Severity
7.	Event Description: 802.1 X-WEB Authentication failures. Log Message: [802.1X-WEB] (<method>) Rejected at WEB auth user <username> (<macaddr>) on Port <portNum> Parameters Description: method: Indicates local or RADIUS. username: The user that is being rejected. macaddr: The MAC address of the authenticated device. portNum: The switch port number.	Notice

14.5 BPDU Guard

ID	Log Description	Severity
1.	Event Description: BPDU attack happened. Log Message: Port<portNum> enter BPDU under attacking state (mode: drop / block / shutdown) Parameters Description: portNum: The port number. mode: The BPDU current state.	Informational
2.	Event Description: BPDU attack automatically recover. Log Message: Port <portNum> recover from BPDU under attacking state automatically Parameters Description: portNum: The port number.	Informational
3.	Event Description: BPDU attack manually recover. Log Message: Port<portNum> recover from BPDU under attacking state manually Parameters Description: portNum: The port number.	Informational

14.6 Command

ID	Log Description	Severity
1.	Event Description: Command Logging Log Message: “<command-str>” executed by <username> from <line>[, IP: <ip-address>] Parameters Description: username: The account name which executed this command. command-str: The command string which was executed successfully and cause a change in switch configuration. line: This parameter indicates the line mode which this command is executed from. (e.g. console, telnet, SSH) ip-address: (Optional) If the command is inputted from remote terminal (e.g. telnet, SSH), this parameter is needed.	Informational

14.7 Configuration/Firmware

ID	Log Description	Severity
1.	Event description: Firmware upgraded successfully. 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.	Informational
2.	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.	Warning
3.	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.	Informational
4.	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.	Warning

ID	Log Description	Severity
5.	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. macaddr : Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server.	Informational
6.	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.	Warning
7.	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.	Informational
8.	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.	Warning
9.	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.	Warning

ID	Log Description	Severity
10.	Event description: Log message uploaded successfully. 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.	Informational
11.	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.	Informational

14.8 DAD

ID	Log Description	Severity
1.	Event description: When DUT receives Neighbor Solicitation (NS) message with reduplicated address in the DAD duration, DUT will add a log. Log Message: Duplicate address <ipv6address > on <interface-id> via receiving Neighbor Solicitation Messages Parameters description: ipv6address : ipv6 address in Neighbor Solicitation Messages. interface-id : port interface ID.	Warning
2.	Event description: When DUT receives Neighbor Advertisement (NA) message with reduplicated address in the DAD duration, DUT will add a log. Log Message: Duplicate address <ipv6address > on <interface-id> via receiving Neighbor Advertisement Messages Parameters description: ipv6address : ipv6 address in Neighbor Advertisement Messages. interface-id : port interface ID.	Warning

14.9 DDM

ID	Log Description	Severity
1.	Event description: when the any of SFP parameters exceeds from the warning threshold. Log Message: Optical transceiver <interface-id> <component> <high-low> warning threshold exceeded Parameters description: interface-id: port interface ID. component: DDM threshold type. It can be one of the following types: temperature supply voltage bias current TX power RX power high-low: High or low threshold.	Warning
2.	Event description: when the any of SFP parameters exceeds from the alarm threshold. Log Message: Optical transceiver <interface-id> <component> <high-low> alarm threshold exceeded Parameters description: interface-id: port interface ID. component: DDM threshold type. It can be one of the following types: temperature supply voltage bias current TX power RX power high-low: High or low threshold.	Critical
3.	Event description: when the any of SFP parameters recovers from the warning threshold. Log Message: Optical transceiver <interface-id> <component> back to normal Parameters description: interface-id: port interface ID. component: DDM threshold type. It can be one of the following types: temperature supply voltage bias current TX power RX power	Warning

14.10 Debug Error

ID	Log Description	Severity
1.	Event description: system fatal error lead to reboot system. Log Message: System re-start reason: system fatal error	Emergencies
2.	Event description: CPU exception lead to reboot system. Log Message: System re-start reason: CPU exception	Emergencies

14.11 DHCPv6 Client

ID	Log Description	Severity
1.	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
2.	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: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
3.	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: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
4.	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: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
5.	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: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
6.	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: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
7.	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: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational

ID	Log Description	Severity
8.	Event description: DHCPv6 client PD interface administrator state changed. Log Message: DHCPv6 client PD on interface <intf-name> changed state to <enabled | disabled> Parameters description: intf-name: Name of the DHCPv6 client PD interface.	Informational
9.	Event description: DHCPv6 client PD obtains an IPv6 prefix from a delegation router. Log Message: DHCPv6 client PD obtains an ipv6 prefix < ipv6networkaddr> on interface <intf-name> Parameters description: ipv6networkaddr: ipv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
10.	Event description: The IPv6 prefix obtained from a delegation router starts renewing. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts renewing Parameters description: ipv6networkaddr: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
11.	Event description: The IPv6 prefix obtained from a delegation router renews success. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> renews success Parameters description: ipv6anetworkaddr: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
12.	Event description: The IPv6 prefix obtained from a delegation router starts rebinding. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts rebinding Parameters description: ipv6address: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
13.	Event description: The IPv6 prefix obtained from a delegation router rebinds success. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> rebinds success Parameters description: ipv6address: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
14.	Event description: The IPv6 prefix from a delegation router was deleted. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> was deleted Parameters description: ipv6address: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational

14.12 Dynamic ARP

ID	Log Description	Severity
1.	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. ip-address: IP address. mac-address: MAC address. vlan-id: VLAN ID. interface-id : The interface number.	Warning
2.	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. ip-address: IP address. mac-address: MAC address. vlan-id: VLAN ID. interface-id : The interface number.	Informational

14.13 Interface

ID	Log Description	Severity
1.	Event description: Port link up. Log Message: Port <port> link up, <nway> Parameters description: port: Represents the logical port number. nway: Represents the speed and duplex of link.	Informational
2.	Event description: Port link down. Log Message: Port <port> link down Parameters description: port: Represents the logical port number.	Informational

14.14 IP Source Guard Verify

ID	Log Description	Severity
1.	Event description: This message indicates that no hardware rule resource to set DHCP Snooping entry into IPSG table. Log Message: Failed to set IPSG entry due to no hardware rule resource. (IP: <IPADDR>, MAC: <MACADDR>, VID: <VLANID>, Interface <INTERFACE-ID>) Parameters description: IPADDR: IP address MACADDR: MAC address VLANID: The VLAN VID INTERFACE-ID : The interface number	Warning

14.15 LACP

ID	Log Description	Severity
1.	Event description: Link Aggregation Group link up. Log Message: Link Aggregation Group < group_id > link up Parameters description: group_id: The group id of the link up aggregation group.	Informational
2.	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
3.	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
4.	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

14.16 LLDP-MED

ID	Log Description	Severity
1.	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>) Parameters description: portNum: The port number. chassisType: 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: chassis ID. portType: 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: port ID. deviceClass: LLDP-MED device type.	Notice

ID	Log Description	Severity
2.	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: 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: chassis ID. portType: 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: port ID. deviceClass: LLDP-MED device type.	Notice
3.	Event description: Incompatible LLDP-MED TLV set detected. 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: 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: chassis ID. portType: 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: port ID. deviceClass: LLDP-MED device type.	Notice

14.17 Loop Detection

ID	Log Description	Severity
1.	Event description: The loop detected between 2 ports or 2 LACP interfaces. Log Message: The loop detected between port/port-channel <portNum> and <portNum> Parameters description: portNum: The port number or LACP interface id.	Warning
2.	Event description: The loop detected on 1 port or 1 LACP interface. Log Message: The loop detected on port/port-channel <portNum> Parameters description: portNum: The port number or LACP interface id.	Warning
3.	Event description: The loop detected between 1 port and 1 LACP interface. Log Message: The loop detected between port/port-channel <portNum> and port/port-channel <portNum> Parameters description: portNum: The port number or port-channel number.	Warning
4.	Event description: Looped port or LACP interface auto recovery. Log Message: Port/Port-channel <portNum> auto recovery Parameters description: portNum: The port number or LACP interface id.	Informational

14.18 MAC-based Access Control

ID	Log Description	Severity
1.	Event description: MAC authentication successful. Log Message: [MAC](<method>)Authorized <macaddr> on Port <portNum> to VLAN <vid> Parameters description: method: Indicates local or RADIUS. macaddr: The MAC address of the authenticated device. portNum: The switch port number. vid: The authorized VLAN ID.	Informational
2.	Event description: MAC authentication failure. Log Message: [MAC](<method>)Rejected <macaddr> on Port <portNum> Parameters description: method: Indicates local or RADIUS. macaddr: The MAC address of the authenticated device. portNum: The switch port number.	Notice
3.	Event description: The MAC authentication table full, cannot authenticate new address. Log Message: [MAC]Rejected <macaddr> on Port <portNum> (auth table was full) Parameters description: macaddr: The MAC address of the authenticated device. portNum: The switch port number.	Notice

14.19 MSTP Debug Enhancement

ID	Log Description	Severity
1.	Event description: Topology changed. Log Message: Topology changed (Instance : <Instance-id>,<interface-id>, MAC:<macaddr>) Parameters description: Instance-id: Instance ID. interface-id: Port ID. macaddr: MAC address.	Notice
2.	Event description: Spanning Tree new Root Bridge. Log Message: [CIST | CIST Regional | MSTI Regional] New Root bridge selected ([Instance: <Instance-id>] MAC: <macaddr> Priority :< priority>) Parameters description: Instance-id : Instance ID. macaddr: MAC address. priority: Priority value.	Notice
3.	Event description: Spanning Tree new Root Bridge. Log Message: [CIST | CIST Regional | MSTI Regional] New Root bridge selected ([Instance: <Instance-id>] MAC: <macaddr> Priority :< priority>) Parameters description: Instance-id : Instance ID. macaddr: MAC address. priority: Priority value.	Informational
4.	Event description: Spanning Tree Protocol is disabled. Log Message: Spanning Tree Protocol is disabled	Informational
5.	Event description: New root port. Log Message: New root port selected (Instance:<instance-id>, <interface-id >) Parameters description: instance-id: Instance ID. interface-id: Port ID.	Notice
6.	Event description: Spanning Tree port status changed. Log Message: Spanning Tree port status change (Instance :< instance-id>, <interface-id>) <old-status> -> <new-status> Parameters description: instance-id: Instance ID. interface-id: Port ID. old_status: Old status. new_status: New status.	Notice
7.	Event description: Spanning Tree port role changed. Log Message: Spanning Tree port role change (Instance :< instance-id>, <interface-id>) <old-role> -> <new-role> Parameters description: instance-id: Instance ID. interface-id: Port ID. old_role: Old role. new_status: New role.	Informational
8.	Event description: Spanning Tree instance created. Log Message: Spanning Tree instance created. (Instance :< instance-id>) Parameters description: instance-id: Instance ID.	Informational

ID	Log Description	Severity
9.	Event description: Spanning Tree instance deleted. Log Message: Spanning Tree instance deleted. (Instance :< instance-id >) Parameters description: instance-id: Instance ID.	Informational
10.	Event description: Spanning Tree Version changed. Log Message: Spanning Tree version change (new version :< new-version>) Parameters description: new_version: New STP version.	Informational
11.	Event description: Spanning Tree MST configuration ID name and revision level changed. Log Message: Spanning Tree MST configuration ID name and revision level change (name :< name>, revision level <revision-level>) Parameters description: name : New name. revision_level: New revision level.	Informational
12.	Event description: Spanning Tree MST configuration ID VLAN mapping table deleted. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: < instance-id > delete vlan <startvlanid> [- <endvlanid>]) Parameters description: instance-id: Instance ID. startvlanid-endvlanid: VLAN list.	Informational
13.	Event description: Spanning Tree MST configuration ID VLAN mapping table added. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: < instance-id > add vlan <startvlanid> [- <endvlanid>]) Parameters description: instance-id: Instance ID. startvlanid-endvlanid: VLAN list.	Informational
14.	Event description: Spanning Tree role changed due to the guard root function. Log Message: Spanning Tree port role change (Instance : < instance-id >, <interface-id>) to alternate port due to the guard root Parameters description: instance-id: Instance ID. interface-id: Port ID.	Informational

14.20 Port Security

ID	Log Description	Severity
1.	Event description: Address full on a port Log Message: MAC address <mac-address> causes port security violation on <interface-id> Parameters description: macaddr: The violation MAC address. interface-id: The interface on which the violation occur.	Warning
2.	Event description: Address full on system. Log Message : Limit on system entry number has been exceeded	Warning

14.21 RADIUS

ID	Log Description	Severity
1.	Event description: This log will be generated when RADIUS assigned a valid VLAN ID attributes. Log Message: RADIUS server <server-ip> assigned VID: <vid> to port <interface-id> (Username: <username>) Parameters description: server-ip: It indicates the RADIUS server IP address. vid: The assign VLAN ID that authorized by from RADIUS server. interface-id: It indicates the port number of the client authenticated. username: It indicates the username for authentication.	Informational
2.	Event description: This log will be generated when RADIUS assigned a valid bandwidth attributes. Log Message: RADIUS server <server-ip> assigned <direction> bandwidth: <threshold> to port < interface-id> (Username: <username>) Parameters description: server-ip: It indicates the RADIUS server IP address. direction: It indicates the direction for bandwidth control, e.g.: ingress or egress. threshold: The assign threshold of bandwidth that authorized by from RADIUS server. interface-id: It indicates the port number of the client authenticated. username: It indicates the username for authentication.	Informational
3.	Event description: This log will be generated when RADIUS assigned a valid priority attributes. Log Message: RADIUS server <server-ip> assigned 802.1p default priority: <priority> to port < interface-id> (Username: <username>) Parameters description: server-ip: It indicates the RADIUS server IP address. priority: The assign priority that authorized by from RADIUS server. interface-id: It indicates the port number of the client authenticated. username: It indicates the username for authentication.	Informational
4.	Event description: This log will be generated when RADIUS assigned ACL script but fails to apply to the system due to insufficient resource. Log Message: RADIUS server <server-ip> assigns <username> ACL failure at port < interface-id> (<acl-script>) Parameters description: server-ip: It indicates the RADIUS server IP address. username: It indicates the username for authentication. interface-id: It indicates the port number of the client authenticated. acl-script: The assign ACL script that authorized by from RADIUS server.	Warning
5.	Event description: This log will be generated when fail to assign access-list number. Log Message: Local assigns [USERNAME] filter-id ID failure at port INTERFACE-ID Parameters description: username: It indicates the username for authentication. filter-id: It indicates access-list number. interface-id: It indicates the port number of the client authenticated.	Warning

14.22 RRP

ID	Log Description	Severity
1.	Event description: The status in “Master Node” changes from “Failed” to “Complete. Log Message: Ring topology was recovered to complete	Notice
2.	Event description: The status in “Master Node” changes from “Complete” to “Failed. Log Message: Ring topology was failed	Warning
3.	Event description: Master or Transit node flush its Forwarding Database based on RRP packets or state machine. Log Message: FDB was flushed	Informational
4.	Event description: The RRP status in “Transit Node” changes to “Link-Up. Log Message: RRP ring status was changed to Link-Up	Warning
5.	Event description: The RRP status in “Transit Node” changes to “Link-Down. Log Message: RRP ring status was changed to Link-Down	Notice
6.	Event description: The RRP status in “Transit Node” changes to “Pre-Forwarding”. Log Message: RRP ring status was changed to Pre-Forwarding	Informational
7.	Event description: Worked ring guard function at the specific domain and port. Log Message: Ring Guard was activated on “<domain-name>” domain at port <port> Parameters description: <domain name>: target domain name. <port num>: target port number worked ring guard function.	Informational

14.23 SNMP

ID	Log Description	Severity
1.	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

14.24 System

ID	Log Description	Severity
1.	Event description: System start up. Log Message: System started up	Critical
2.	Event description: Save current configuration to flash. Log Message: Configuration saved to flash by console (Username: <username>) Parameters description: username: The user name.	Informational
3.	Event description: Save system configuration from remote. Log Message: Configuration saved to flash (Username: <username>, IP: <ipaddr>) Parameters description: username: The user name. ipaddr: The ip address.	Informational
4.	Event description: System power up and start up. Log Message: System cold start	Critical
5.	Event description: System reboot and start up. Log Message: System warm start	Critical

14.25 Telnet

ID	Log Description	Severity
1.	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 user name that used to login telnet server.	Informational
2.	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 user name that used to login telnet server.	Warning
3.	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 user name that used to login telnet server.	Informational
4.	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 user name that used to login telnet server.	Informational

14.26 Temperature

ID	Log Description	Severity
1.	Event description: Temperature sensor enters alarm state. Log Message: Uint <unitID> Sensor:<sensorID> detects abnormal temperature <temperature> Parameters description: unitID: The unit ID. sensorID: The sensor ID. temperature: The current temperature of the sensor.	Critical
2.	Event description: Temperature recovers to normal. Log Message: Uint <unitID> Sensor:<sensorID> temperature back to normal Parameters description: unitID: The unit ID. sensorID: The sensor ID. temperature: The temperature.	Critical

14.27 Traffic Control

ID	Log Description	Severity
1.	Event description: Broadcast, Multicast or Unicast storm occurrence. Log Message: Broadcast | Multicast | Unicast> storm is occurring on <interface-id> Parameters description: interface-id: The interface ID on which a storm is occurring.	Warning
2.	Event description: Broadcast, Multicast or Unicast storm cleared. Log Message: <Broadcast | Multicast | Unicast> storm is cleared on <interface-id> Parameters description: interface-id: The interface ID on which a storm is cleared.	Informational
3.	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.	Warning

14.28 UDLD

ID	Log Description	Severity
1.	Event description: A unidirectional link is detected on this port. Log Message: Unidirectional link detection on <INTERFACE-ID> Parameters description: INTERFACE-ID: The interface name.	Warning

14.29 Voice VLAN

ID	Log Description	Severity
1.	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
2.	Event description: When an interface which is in auto voice VLAN mode joins the voice VLAN. Log Message: < interface-id > add into voice VLAN <vid > Parameters description: interface-id: Interface name.s vid: VLAN ID.	Informational
3.	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: Interface name. vid: LAN ID.	Informational

14.30 WAC

ID	Log Description	Severity
1.	Event description: When a client host fails to authenticate. Log Message: [WEB](RADIUS/Local) Rejected user <string> (<macaddr>) on Port <portNum> Parameters description: string: User name. macaddr: MAC address. portNum : The port number.	Warning
2.	Event description: When a client host authenticated successful. Log Message: [WEB](RADIUS/Local)Authorized user <string> (<macaddr>) on Port <portNum> to VLAN <vlanNum> Parameters description: string: User name. macaddr: MAC address. portNum : The port number. vlanNum : The VLAN number.	Informational
3.	Event description: When client table full. Log Message: [WEB]Rejected <macaddr> on Port <portNum> (auth table was full) Parameters description: macaddr: MAC address. portNum : The port number.	Notice

14.31 Web

ID	Log Description	Severity
1.	Event description: Successful login via web. Log Message: "Successful login through Web (Username: <username>, IP: <ipaddr>)" Parameters description: username: user name. ipaddr: IP address from where user access the switch via web.	Informational
2.	Event description: Login failed via web. Log Message: Login failed through Web (Username: <username>, IP: <ipaddr>)" Parameters description: username: user name. ipaddr: IP address from where user access the switch via web.	Warning
3.	Event description: Successful login from HTTPS. Log Message: Successful login through Web(SSL) (Username: <username>, IP: <ipaddr>) Parameters description: username: user name. ipaddr: IP address from where user access the switch via secure web.	Informational
4.	Event description: login failed via secure web. Log Message: Login failed through Web(SSL) (Username: <username>, IP: <ipaddr>) Parameters description: username: user name. ipaddr: IP address from where user access the switch via secure web.	Warningsssss ssss
5.	Event description: Log upload successfully. Log Message: Log message uploaded by WEB successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <ipaddr>, File Name: <filename>) Parameters description: username: user name. ipaddr: IP address from where user access the switch. macaddr: MAC address of client. server IP: TFTP server IP address. filename: the log file name.	Informational
6.	Event description: Log upload unsuccessfully. Log Message: Log message uploaded by WEB unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <ipaddr>, File Name: <filename>) Parameters description: username: user name. ipaddr: IP address from where user access the switch. macaddr: MAC address of client. server IP: TFTP server IP address. filename: the log file name.	Informational

15 Appendix - System Trap Entries

15.1 BPDU Guard

ID	Trap Name	Trap Description	OID
1.	mnoBpduProtectionUnderAttackingTrap	BPDU attack happened, enter drop / block / shutdown mode. Binding objects: mnoBpduProtectionPortIndex The port interface. (2) mnoBpduProtectionPortMode Drop / block / shutdown mode.	1.3.6.1.4.1.396.5.5.3.4.0.1
2.	mnoBpduProtectionRecoveryTrap	BPDU attack automatically recover. Binding objects: mnoBpduProtectionPortIndex The port interface. mnoBpduProtectionRecoveryMethod Auto/manual recovers.	1.3.6.1.4.1.396.5.5.3.4.0.2

15.2 DDM

ID	Trap Name	Trap Description	OID
1.	mnoDdmAlarmTrap	The trap is sent when any parameter value exceeds the alarm threshold value or recovers to normal status depending on the configuration of the trap action. Binding objects: mnoDdmPort The port number mnoDdmThresholdType The ddm threshold type temperature/voltage/bias/txpower/rxpower mnoDdmThresholdExceedType The threshold that was exceeded was a high alarm threshold or a low alarm threshold (4) mnoDdmThresholdExceedOrRecover The GBIC is exceeding its ddm threshold or recover to normal status	1.3.6.1.4.1.396.5.5.1.4.0.1
2.	mnoDdmWarningTrap	The trap is sent when any parameter value exceeds the warning threshold value or recovers to normal status depending on the configuration of the trap action. Binding objects: mnoDdmPort The port number mnoDdmThresholdType The ddm threshold type temperature/voltage/bias/txpower/rxpower mnoDdmThresholdExceedType The threshold that was exceeded was a high warning threshold or a low warning threshold (4) mnoDdmThresholdExceedOrRecover The GBIC is exceeding its ddm threshold or recover to normal status	1.3.6.1.4.1.396.5.5.1.4.0.2

15.3 DHCP Server Protect

ID	Trap Name	Trap Description	OID
1.	mnoFilterDetectedTrap	Send trap when an illegal DHCP server is detected. The same illegal DHCP server IP address detected is just sent once to the trap receivers within the log ceasing unauthorized duration. Binding objects: mnoFilterDetectedIP The illegal DHCP server IP address. mnoFilterDetectedport The port interface.	1.3.6.1.4.1.396.5.5.3.7.0.1

15.4 Gratuitous ARP

ID	Trap Name	Trap Description	OID
1.	mnoAgentGratuitousARPTrap	The trap is sent when IP address conflicted. Binding objects: agentGratuitousARPIpAddr The conflicted IP address received in the gratuitous ARP packet. agentGratuitousARPMacAddr The sender's MAC address in the gratuitous ARP packet. agentGratuitousARPPortNumber The switch's port number who received the gratuitous ARP packet. agentGratuitousARPInterfaceName The switch's IP interface name who received the gratuitous ARP.	1.3.6.1.4.1.396.5.5.3.6.0.1

15.5 LLDP-MED

ID	Trap Name	Trap Description	OID
1.	lldpRemTablesChange	A lldpRemTablesChange notification is sent when the value of lldpStatsRemTableLastChangeTime changes. Binding objects: (1) lldpStatsRemTablesInserts (2) lldpStatsRemTablesDeletes (3) lldpStatsRemTablesDrops (4) lldpStatsRemTablesAgeouts	1.0.8802.1.1.2.0.0.1
2.	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	1.0.8808.1.1.2.1.5.4795.0.1

15.6 Loop Detect

ID	Trap Name	Trap Description	OID
1.	mnoLoopDetectNotification	Indicates the network loop occurred.	1.3.6.1.4.1.396.5.5.2.1
2.	mnoLoopRecoveryNotification	Indicates the network loop resolved.	1.3.6.1.4.1.396.5.5.2.2

15.7 MAC-based Access Control

ID	Trap Name	Trap Description	OID
1.	mnoMacBasedAccessControlLoggedSuccess	The trap is sent when a MAC-based Access Control host is successfully logged in. Binding objects: mnoMacBasedAuthInfoMacIndex The host MAC addresses. mnoMacBasedAuthInfoPortIndex The port interface. mnoMacBasedAuthVID The VLAN ID.	1.3.6.1.4.1.396.5.5.3.2.0.1
2.	mnoMacBasedAccessControlLoggedFail	The trap is sent when a MAC-based Access Control host login fails. Binding objects: mnoMacBasedAuthInfoMacIndex The host MAC addresses. mnoMacBasedAuthInfoPortIndex The port interface. mnoMacBasedAuthVID The VLAN ID.	1.3.6.1.4.1.396.5.5.3.2.0.2
3.	mnoMacBasedAccessControlAgesOut	The trap is sent when a MAC-based Access Control host ages out. Binding objects: mnoMacBasedAuthInfoMacIndex The host MAC addresses. (2) mnoMacBasedAuthInfoMacIndex The port interface. (3) mnoMacBasedAuthVID The VLAN ID.	1.3.6.1.4.1.396.5.5.3.2.0.3

15.8 MAC Notification

ID	Trap Name	Trap Description	OID
1.	mnoL2macNotification	This trap indicates the MAC addresses variation in address table Binding objects: mnoL2macNotifyInfo Devices MAC address change information. And the detailed information include : Operation Code + MAC address + Box ID + Interface ID + Zero. Operation Code: 1, 2 1 means learned a new MAC address 2 means deleted an old MAC address. Box ID: The switch box ID Interface ID: The Interface ID learned or deleted on the box. Zero: Used to separate each message (Operate Code + MAC address + Box ID + Port Number).	1.3.6.1.4.1.396 .5.5.3.1.0.1

15.9 MSTP

ID	Trap Name	Trap Description	OID
1.	newRoot	The newRoot 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, e.g., 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
2.	topologyChange	A topologyChange 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 ofthis trap is optional	1,3,6,1,2,1,17.0.2

15.10 Port Security

ID	Trap Name	Trap Description	OID
1.	mnoL2PortSecurityViolationTrap	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: mnoPortSecPortIndex The port interface. mnoL2PortSecurityViolationMac The host MAC addresses.	1.3.6.1.4.1.396.5.5.3.3.0.1

15.11 Port

ID	Trap Name	Trap Description	OID
1.	linkUp	A notification is generated when port linkup. Binding objects: (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6. 3.1.1.5.4
2.	linkDown	A notification is generated when port linkdown. Binding objects: (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6. 3.1.1.5.3

15.12 RMON

ID	Trap Name	Trap Description	OID
1.	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
2.	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

15.13 SNMP Authentication

ID	Trap Name	Trap Description	OID
1.	authenticationFailure	An authenticationFailure 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

15.14 System

ID	Trap Name	Trap Description	OID
1.	coldStart	A coldStart 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
2.	warmStart	A warmStart 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

15.15 Temperature

ID	Trap Name	Trap Description	OID
1.	mnoTemperatureRising Alarm	This notification will send out when current temperature more than high threshold.	1.3.6.1.4.1.396. 5.5.1.2.1
2.	mnoTemperatureFalling Alarm	This notification will send out when current temperature falling from high threshold.	1.3.6.1.4.1.396. 5.5.1.2.2

15.16 Traffic Control

ID	Trap Name	Trap Description	OID
1.	mnoPktStormOccurred	When packet storm is detected by packet storm mechanism and take shutdown as action. Binding objects: mnoPktStormCtrlPortIndex The port interface.	1.3.6.1.4.1.396.5.5.3.5.0.1
2.	mnoPktStormCleared	When the packet storm is clear. Binding objects: mnoPktStormCtrlPortIndex The port interface.	1.3.6.1.4.1.396.5.5.3.5.0.2
3.	mnoPktStormDisablePort	When the port is disabled by the packet storm mechanism. Binding objects: mnoPktStormCtrlPortIndex The port interface.	1.3.6.1.4.1.396.5.5.3.5.0.3

Panasonic Electric Works Networks Co., Ltd.

2-12-7, Higashi-Shimbashi, Minato-ku, Tokyo Japan, 105-0021
URL: https://panasonic.co.jp/ew/pewnw/english/index.html

P0222-3062