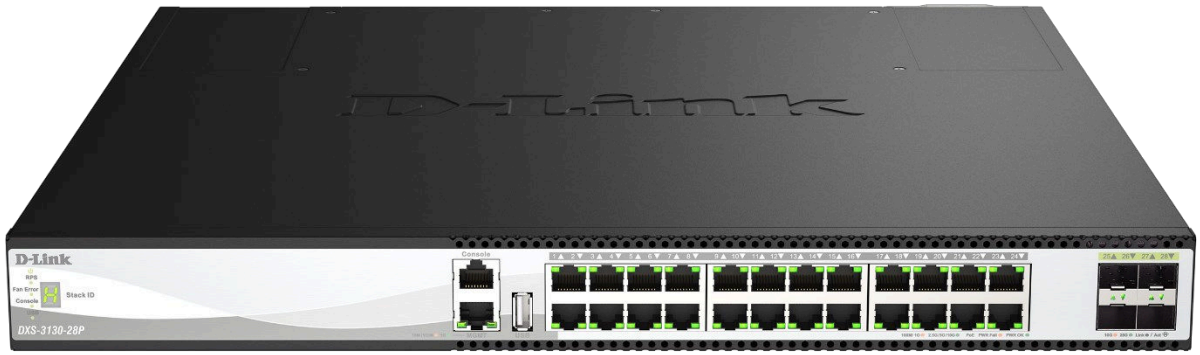
Version 1.00 | 05/09/2024



Web UI manual

Layer 3 Stackable Managed Switch

DXS-3130 Series

Information in this document is subject to change without notice. Reproduction of this document in any manner, without the written permission of the D-Link Corporation, is strictly forbidden.

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

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

© 2024 D-Link Corporation. All rights reserved.

Table of Contents

Table of Contents ..... **i**

1. Introduction **1**
Audience 1
Other Documentation 1
Conventions 1
Notes, Notices, and Cautions 1

2. Web-based Switch Configuration **3**
Management Options 3
Logging into the Web UI 3
Web User Interface (Web UI) 4
Areas of the User Interface 4

3. System **6**
Device Information 6
System Information Settings 7
Peripheral Settings 8
Port Configuration 9
Port Settings 9
Port Status 11
Port GBIC 12
Port Auto Negotiation 12
Error Disable Settings 13
Jumbo Frame 14
Interfaces Description 15
PoE 15
PoE System 16
PoE Status 17
PoE Configuration 18
PoE Statistics 19
PoE Measurement 20
PoE LLDP Classification 20
PoE PD Alive Settings 21
System Log 22
System Log Settings 22
System Log Discriminator Settings 24
System Log Server Settings 25
System Log 27
System Attack Log 27
Time and SNTP 28
Clock Settings 28
Time Zone Settings 28
SNTP Settings 30
Time Range 32
Switch Controller Settings 32

4. Management **34**
Command Logging 34
User Accounts Settings 34
Password Encryption 36
Password Recovery 36
Login Method 37

SNMP 39
SNMP Global Settings 40
SNMP Linkchange Trap Settings 41
SNMP View Table Settings 41
SNMP Community Table Settings 42
SNMP Group Table Settings 43
SNMP Engine ID Local Settings 45
SNMP User Table Settings 45
SNMP Host Table Settings 47
RMON 48
RMON Global Settings 48
RMON Statistics Settings 48
RMON History Settings 49
RMON Alarm Settings 50
RMON Event Settings 51
Telnet/Web 52
Session Timeout 53
DHCP 54
Service DHCP 54
DHCP Class Settings 54
DHCP Server 56
DHCPv6 Server 64
DHCP Relay 68
DHCPv6 Relay 75
DHCP Auto Configuration 80
DNS 80
DNS Global Settings 80
DNS Name Server Settings 81
DNS Host Settings 82
IP Source Interface 83
File System 83
Stacking 85
Physical Stacking 88
Stacking Bandwidth 89
Virtual Stacking (SIM) 89
Single IP Settings 91
Topology 92
Firmware Upgrade 99
Configuration File Backup/Restore 99
Upload Log File 99
D-Link Discovery Protocol 99
SMTP Settings 100
Reboot Schedule Settings 102
PPPoE Circuit ID Insertion Settings 103
SD Card Management 104
SD Card Backup Settings 104
SD Card Execute Settings 104

5. Layer 2 Features 107

FDB 107
Static FDB 107
MAC Address Table Settings 108
MAC Address Table 110

MAC Notification 111
VLAN 113
VLAN Configuration Wizard 113
802.1Q VLAN 113
VLAN Interface 114
802.1v Protocol VLAN 119
GVRP 121
Asymmetric VLAN 125
MAC VLAN 125
Super VLAN 126
Auto Surveillance VLAN 128
Voice VLAN 130
Private VLAN 134
VLAN Tunnel 135
Dot1q Tunnel 135
VLAN Mapping 137
VLAN Mapping Profile 138
STP 144
STP Global Settings 146
STP Port Settings 148
MST Configuration Identification 150
STP Instance 152
MSTP Port Information 152
ERPS (G.8032) 153
ERPS 153
ERPS Profile 158
Loopback Detection 159
Link Aggregation 161
L2 Protocol Tunnel 164
L2 Multicast Control 165
IGMP Snooping 165
MLD Snooping 175
Multicast VLAN 185
Multicast Filtering 188
LLDP 189
LLDP Global Settings 189
LLDP Port Settings 191
LLDP Management Address List 192
LLDP Basic TLVs Settings 192
LLDP Dot1 TLVs Settings 193
LLDP Dot3 TLVs Settings 194
LLDP-MED Port Settings 195
LLDP Statistics Information 196
LLDP Local Port Information 197
LLDP Neighbor Port Information 199

6. Layer 3 Features 201

ARP 201
ARP Elevation 201
ARP Aging Time 201
Static ARP 202
Proxy ARP 202
ARP Table 203

Gratuitous ARP 204
IPv6 Neighbor 205
Interface 205
IPv4 Interface 205
IPv6 Interface 208
Loopback Interface 211
Null Interface 212
UDP Helper 213
IP Forward Protocol 213
IP Helper Address 214
IPv4 Static/Default Route 214
IPv4 Route Table 215
IPv6 Static/Default Route 216
IPv6 Route Table 217
Route Preference 218
ECMP Settings 218
RIP 219
RIP Settings 219
RIP Distribute List 221
RIP Interface Settings 222
RIP Database 223
RIPng 224
RIPng Settings 224
RIPng Interface Settings 225
RIPng Database 226
OSPF 226
OSPFv2 226
OSPFv3 240
IP Multicast Routing Protocol 252
IGMP 252
PIM 256
IPMC 260
IP Route Filter 261
Route Map 261
Policy Route 264
VRRP Settings 265
VRRPv3 Settings 267

7. Quality of Service (QoS) 271

Basic Settings 271
Port Default CoS 271
Port Scheduler Method 271
Queue Settings 273
CoS to Queue Mapping 274
Port Rate Limiting 274
Queue Rate Limiting 275
Advanced Settings 277
DSCP Mutation Map 277
Port Trust State and Mutation Binding 278
DSCP CoS Mapping 278
CoS Color Mapping 279
DSCP Color Mapping 280
Class Map 281

Aggregate Policer 283
Policy Map 286
Policy Binding 290
WRED 291
WRED Profile 291
WRED Queue 292
8. Access Control List (ACL) 294
ACL Configuration Wizard 294
ACL Access List 298
Standard IP ACL 300
Extended IP ACL 302
Standard IPv6 ACL 304
Extended IPv6 ACL 306
Extended MAC ACL 308
Extended Expert ACL 311
ACL Interface Access Group 314
ACL VLAN Access Map 315
ACL VLAN Filter 317
CPU ACL 318
9. Security 322
Port Security 322
Port Security Global Settings 322
Port Security Port Settings 323
Port Security Address Entries 325
802.1X 325
802.1X Global Settings 330
802.1X Port Settings 330
Authentication Sessions Information 332
Authenticator Statistics 332
Authenticator Session Statistics 333
Authenticator Diagnostics 333
AAA 334
AAA Global Settings 334
Application Authentication Settings 335
Application Accounting Settings 335
Authentication Settings 337
Accounting Settings 339
Server RADIUS Dynamic-Author Settings 341
RADIUS 342
RADIUS Global Settings 342
RADIUS Server Settings 344
RADIUS Group Server Settings 344
RADIUS Statistic 346
TACACS 346
TACACS Global Settings 347
TACACS Server Settings 347
TACACS Group Server Settings 348
TACACS Statistic 349
IMPB 349
IPv4 350
IPv6 363
DHCP Server Screening 372

DHCP Server Screening Global Settings 372
DHCP Server Screening Port Settings 373
ARP Spoofing Prevention 374
BPDU Attack Protection 375
MAC Authentication 376
Web-based Access Control 378
Web Authentication 380
WAC Port Settings 381
WAC Customize Page 381
Network Access Authentication 382
Guest VLAN 382
Network Access Authentication Global Settings 383
Network Access Authentication Port Settings 385
Network Access Authentication Sessions Information 386
Safeguard Engine 387
Safeguard Engine Settings 389
CPU Protect Counters 389
CPU Protect Sub-Interface 390
CPU Protect Type 391
Trusted Host 391
Traffic Segmentation Settings 392
Storm Control 393
DoS Attack Prevention Settings 395
SSH 397
SSH Global Settings 397
SSH Algorithm Settings 398
Host Key 398
SSH Server Connection 399
SSH User Settings 400
SSL 401
SSL Global Settings 401
Crypto PKI Trustpoint 402
SSL Service Policy 403
SFTP Server Settings 404
Network Protocol Port Protect 405

10. OAM 406

CFM 406
CFM Settings 406
CFM Port Settings 416
CFM Loopback Test 417
CFM Linktrace Settings 418
CFM Packet Counter 420
CFM Counter CCM 421
CFM MIP CCM Table 421
CFM MEP Fault Table 421
Cable Diagnostics 422
Ethernet OAM 423
Ethernet OAM Settings 423
Ethernet OAM Configuration Settings 424
Ethernet OAM Event Log Table 427
Ethernet OAM Statistics Table 427
Ethernet OAM DULD Settings 428

DDM 430
DDM Settings 430
DDM Temperature Threshold Settings 431
DDM Voltage Threshold Settings 431
DDM Bias Current Threshold Settings 432
DDM TX Power Threshold Settings 433
DDM RX Power Threshold Settings 433
DDM Status Table 434
11. Monitoring 435
VLAN Counter 435
Utilization 436
Port Utilization 436
History Utilization 437
Statistics 438
Port 438
CPU Port 440
Interface Counters 441
Interface History Counters 443
Counters 444
Mirror Settings 446
sFlow 448
sFlow Agent Info-rmation 448
sFlow Receiver Settings 448
sFlow Sampler Settings 449
sFlow Poller Settings 450
Device Environment 451
12. Green 452
Power Saving 452
EEE 453
13. Save and Tools 455
Save Configuration 455
Firmware Upgrade & Backup 455
Firmware Upgrade from HTTP 455
Firmware Upgrade from TFTP 456
Firmware Backup to HTTP 456
Firmware Backup to TFTP 457
Configuration Restore & Backup 458
Configuration Restore from HTTP 458
Configuration Restore from TFTP 458
Configuration Backup to HTTP 459
Configuration Backup to TFTP 459
Log Backup 460
Log Backup to HTTP 460
Log Backup to TFTP 461
Ping 461
Trace Route 464
Reset 466
Reboot System 466
Appendix A - Password Recovery Procedure 468
Appendix B - System Log Entries 469
802.1X 469

AAA ... 469
ARP ... 471
Auto-save ... 471
BPDU Protection ... 472
CFM ... 472
CFM Extension ... 473
Configuration/Firmware ... 474
DAD ... 477
DDM ... 477
DHCPv6 Client ... 478
DHCPv6 Server ... 479
Dynamic ARP Inspection ... 479
ERPS ... 480
Ethernet OAM ... 481
Interface ... 482
IP Directed Broadcast ... 482
LACP ... 482
LBD ... 483
LLDP-MED ... 483
Login/Logout ... 485
MAC ... 486
MSTP Debug Enhancement ... 487
Peripheral ... 489
Port ... 490
Port Security ... 490
Reboot Schedule ... 491
Safeguard ... 491
SNMP ... 491
SSH ... 491
SSL ... 491
Stacking ... 492
Storm Control ... 493
Telnet ... 494
WAC ... 494
Web ... 495

Appendix C - Trap Entries ... 496

802.1X ... 496
802.3ah OAM ... 496
Authentication Fail ... 497
BPDU Protection ... 497
CFM ... 497
CFM Extension ... 497
DDM ... 498
DHCP Server Screen Prevention ... 498
DoS Prevention ... 499
ERPS ... 499
ErrDisable ... 499
Gratuitous ARP ... 500
IP-MAC-Port Binding ... 500
LACP ... 500
LBD ... 501
LLDP-MED ... 501

MAC-based Access Control 502
MAC Notification 502
MSTP 502
Peripheral 503
PoE 503
Port Security 504
Port 504
RMON 505
Safeguard 505
SIM 505
Stacking 507
Start 507
Storm Control 507
System File 508
Upload/Download 508
VRRP 508
WAC 509
Appendix D - RADIUS Attributes Assignment 510
Appendix E - IETF RADIUS Attributes Support 513

1. Introduction

This manual's feature descriptions are based on the software release 1.01.006. The features listed here are the subset of features that are supported by the DXS-3130 Series Switch.

Audience

This reference manual is intended for network administrators and other IT networking professionals responsible for managing the Switch by using the Web User Interface (Web UI). The Web UI is the secondary management interface to the DXS-3130 Series Switch, which will be generally referred to simply as the "**Switch**" within this manual. This manual is written in a way that assumes that you already have the experience and knowledge of Ethernet and modern networking principles for Local Area Networks.

Other Documentation

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

- *DXS-3130 Series Hardware Installation Guide*
- *DXS-3130 Series CLI Reference Guide*

Conventions

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

Notes, Notices, and Cautions

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



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

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

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

2. Web-based Switch Configuration

Management Options
Logging into the Web UI
Web User Interface (Web UI)

Management Options

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

Command Line Interface (CLI)

The Switch can be managed, out-of-band, by using the console port or the MGMT port on the front panel of the Switch. Alternatively, the Switch can also be managed, in-band, by using a Telnet connection to any of the LAN ports on the Switch. The command line interface provides complete access to all Switch management features.

For more detailed information about the CLI, refer to the *DXS-3130 Series CLI Reference Guide*.

SNMP-based Management

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

Web User Interface (Web UI)

The Web UI can be accessed from any computer running web browsing software from its MGMT port or LAN port when it is connected to any of the RJ45 or SFP28/SFP+ ports. The Web UI on the Switch can also be accessed using an HTTPS (SSL) connection.

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



NOTE: The Command Line Interface (CLI) provides the functionality of managing, configuring, and monitoring **all** of the software features that are available on the Switch.

Logging into the Web UI

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



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

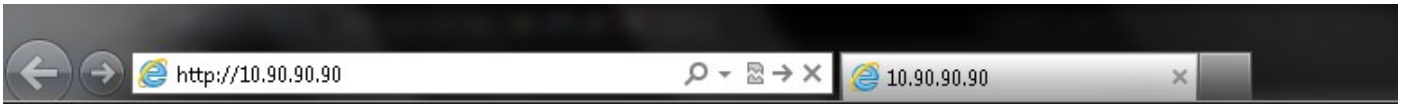


Figure 2-1 Displays entering the IP address in Internet Explorer

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



Figure 2-2 Web UI Login Window

When connecting to the Web UI of the Switch for the first time, leave the **User Name** and **Password** fields blank and click **Login** since there are no login user accounts created by default on the Switch.

NOTE: After a user account was created, login credentials will be required to access the Web UI. During the sending and receiving of the login password to and from the Switch, this information will be protected using TLS/SSL to prevent attackers from snooping this information to gain unauthorized access to the Switch.

Web User Interface (Web UI)

The Web UI provides access to various Switch configuration and management windows. It allows the user to view performance statistics, and permits graphical monitoring of the system's status.

Areas of the User Interface

The figure below shows the user interface. Four distinct areas that divide the user interface, as described in the table.

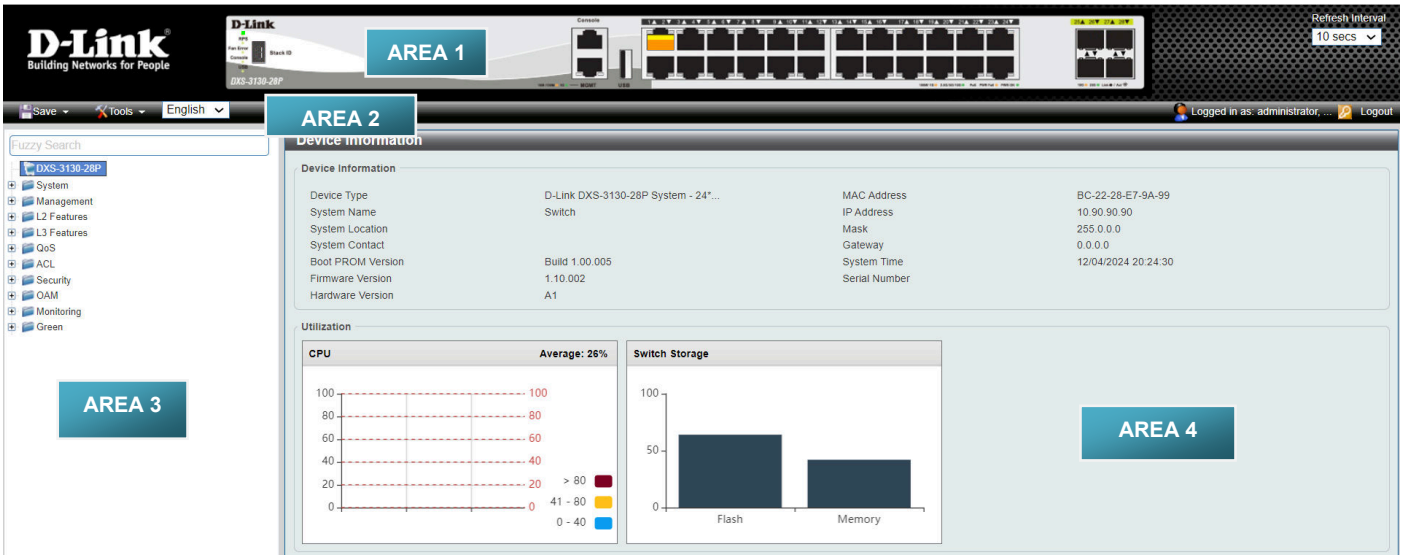


Figure 2-3 Main Web UI Window

Area Number	Description
AREA 1	This area displays a graphical, near real-time image of the front panel of the Switch. This area displays the Switch's ports and expansion modules. It also allows you to select the stack ID to display the ports of the selected switch. It also shows the login user account and allows the user to log out of the management interface. Click the D-Link logo to go to the D-Link website.
AREA 2	This area displays a toolbar used to access **Save** and **Tools** menus.
AREA 3	This area displays a file explorer-type menu tree with all configurable options. Select the folder or window to display. Open folders and click the hyperlinked window buttons and subfolders contained within them to display information pertaining to that category.
AREA 4	In this area, the Switch's configuration page can be found, based on the selection made in **AREA 3**.

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

NOTE: The best screen resolution for viewing the Web UI is 1280 x 1024 pixels.

3. System

Device Information
System Information Settings
Peripheral Settings
Port Configuration
Interfaces Description
PoE
System Log
Time and SNTP
Time Range
Switch Controller Settings

Device Information

In the Device Information section, the user can view a list of basic information regarding the Switch. It appears automatically when you log on to the Switch. To return to the Device Information window after viewing other windows, click the *device name* (e.g. **DXS-3130-28P)** link. The Device Information displays the following information:

Device Type – The type of the switch including the device mode and a description of its ports.

System Name – The name of the device.

System Location – The location of the device. This information can be set in the System Information Settings.

System Contact – The contact person. This information can be set in the System Information Settings.

Boot PROM Version – The boot PROM (programmable read only memory) version.

Firmware Version – The firmware version of the device.

Hardware Version – The hardware version of thd device.

MAC Address – The unique physical address of the device.

IP Address – The IP address of the device. This information can be set in the System Information Settings.

Mask – The subnet mask of the IP address. This information can be set in the System Information Settings.

Gateway – The gateway address. This information can be set in the System Information Settings.

System Time – The current system time. This information can be set in Clock Settings (refer to **System > Time and SNTP > Clock Settings**).

Serial Number – The serial number of the device.

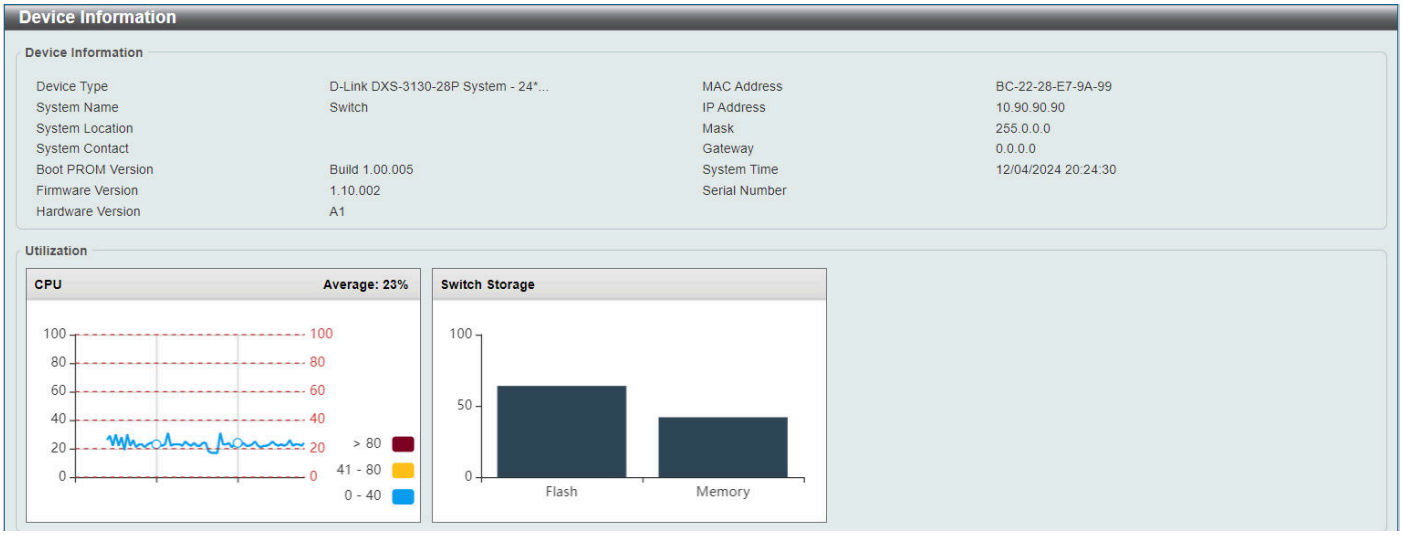


Figure 3-1 Device Information Window

System Information Settings

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

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

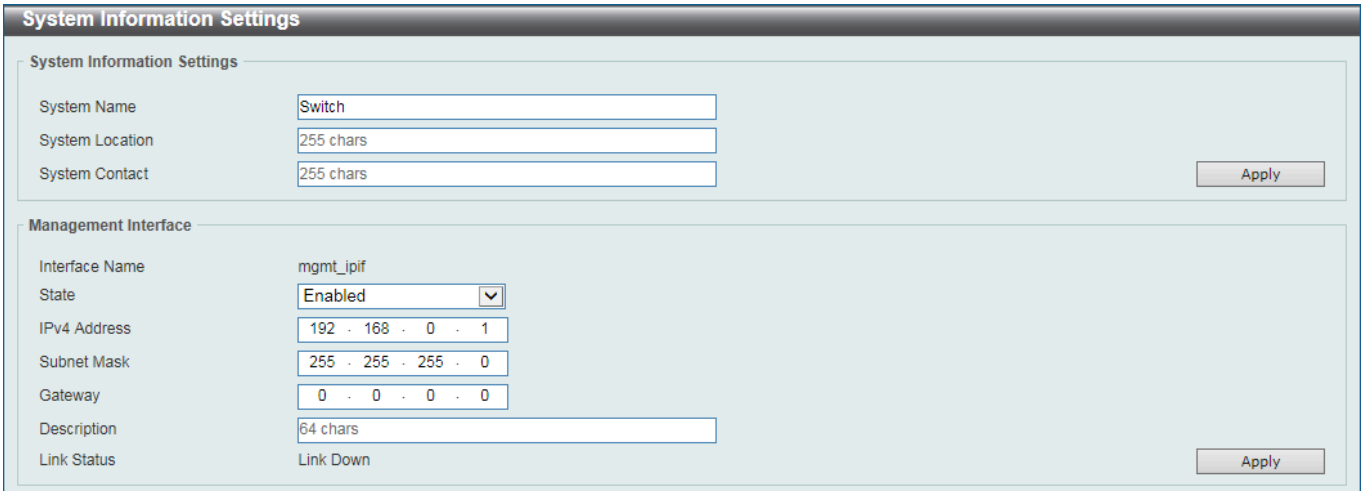


Figure 3-2 System Information Settings Window

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

Parameter	Description
System Name	Enter a system name for the Switch, if so desired. This name will identify it in the Switch network.
System Location	Enter the location of the Switch, if so desired.
System Contact	Enter a contact name for the Switch, if so desired.

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

The fields that can be configured in **Management Interface** are described below:

Parameter	Description
State	Select to enable or disable the state of the management interface here.
IPv4 Address	Enter the IPv4 address for this interface here.
Subnet Mask	Enter the IPv4 subnet mask for this interface here.
Gateway	Enter the gateway IPv4 address for this interface here.
Description	Enter the description for the management interface here. This can be up to 64 characters long.

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

Peripheral Settings

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

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

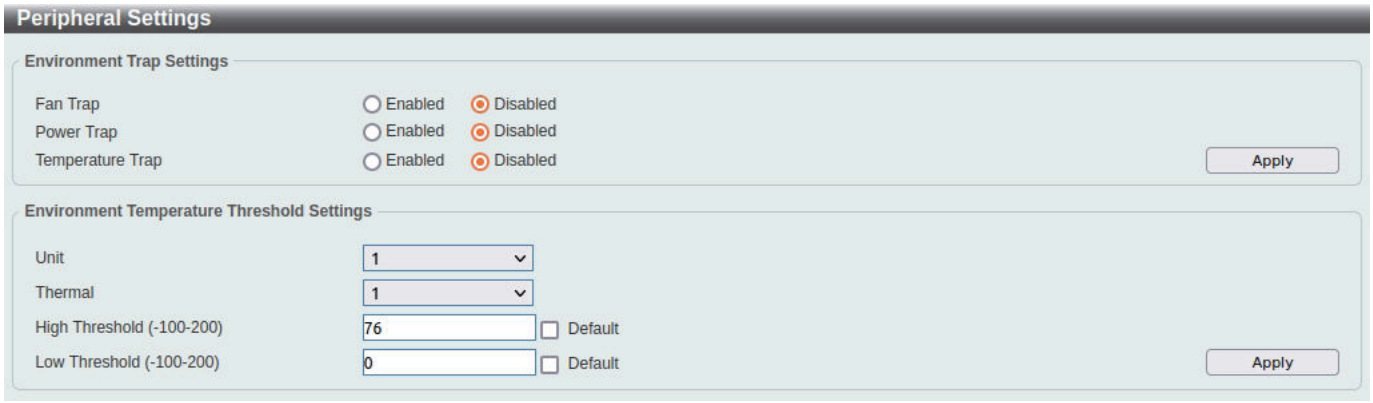


Figure 3-3 Peripheral Settings Window

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

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

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

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

Parameter	Description
Unit	Select the switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
Thermal	Select the thermal sensor ID.

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

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

Port Configuration

Port Settings

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

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

Eth1/0/1 means that the port is numbered Unit 1 (of the stack)/Module 0 (of the system) /Port 1 (physical port number). The port number can be referenced in the diagram displayed in the header above.

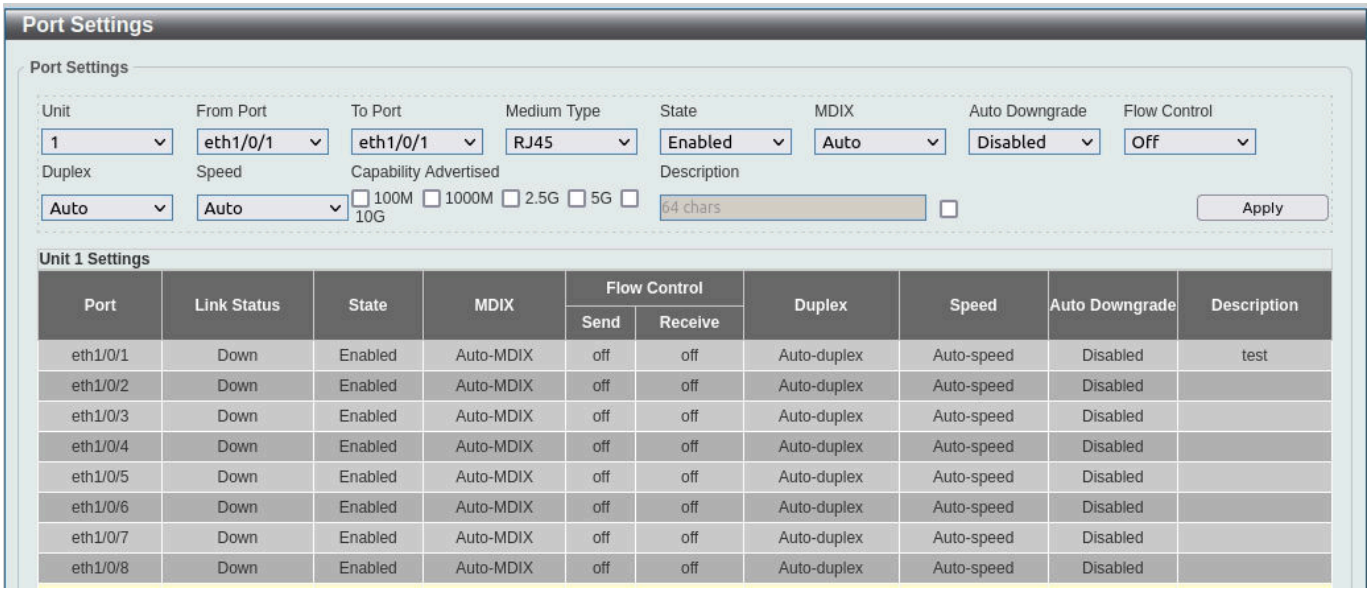


Figure 3-4 Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the stacking unit ID of the Switch that will be configured here. This option is only available when stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here. The port number can be referenced in the diagram displayed in the header above. **NOTE:** Port number specific to fiber optical transceivers will not be available if stacking is enabled (refer to **Management > Stacking**).
Medium Type	Select the port medium type here. Options to choose from are **RJ45** and **SFP**.

Parameter	Description
	NOTE: Selecting the SFP option, which includes the use of SFP28 or optional SFP+ transceivers for 10G/25G connectivity.
State	Select this option to enable or disable the physical port here.
MDIX	Select the Medium Dependent Interface Crossover (MDIX) option here. Options to choose from are: • **Auto** - Select this option for auto-sensing of the optimal type of cabling. • **Normal** - Select this option for normal cabling. If this option is selected, the port is in the MDIX mode and can be connected to a PC NIC using a straight-through cable or a port (in the MDI mode) on another Switch through a 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.
Auto Downgrade	Select to enable or disable the feature to automatically downgrade the advertised speed in the event that a link cannot be established at an available speed.
Flow Control	Select to either 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. **NOTE:** This feature will not work through Switches that are physically stacked.
Duplex	Select the duplex mode used here. Options to choose from are **Auto, Half** and **Full**. **NOTE:** Fiber optic ports support only full-duplex mode.
Speed	Select the port speed option here. This option will manually force the connection speed on the selected port to only connect at the speed specified here. Options to choose from are **Auto**, **100M**, **1000M**, **1000M Master**, **1000M Slave**, **2500M, 2500M Master, 2500M Slave, 5G, 5G Master, 5G Slave, 10G, 10G Master, 10G Slave,** and **25G**. 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. • **Auto** - Specifies that for copper ports, auto-negotiation will start to negotiate the speed and flow control with its link partner. For fiber optic ports, auto-negotiation is not supported. • **100M** - Specifies to force the port speed to 100 Mbps. • **1000M** - Specifies to force the port speed to 1Gbps. • **1000M Master** - Specifies to force the port speed to 1Gbps and operates as the master, to facilitate the timing of transmit and receive operations. • **1000M Slave** - Specifies to force the port speed to 1Gbps and operates as the slave, to facilitate the timing of transmit and receive operations. • **2500M** - Specifies to force the port speed to 2.5 Gbps. • **2500M Master** - Specifies to force the port speed to 2.5 Gbps and operates as the master, to facilitate the timing of transmit and receive operations. • **2500M Slave** - Specifies to force the port speed to 2.5 Gbps and operates as the slave, to facilitate the timing of transmit and receive operations. • **5G** - Specifies to force the port speed to 5 Gbps.

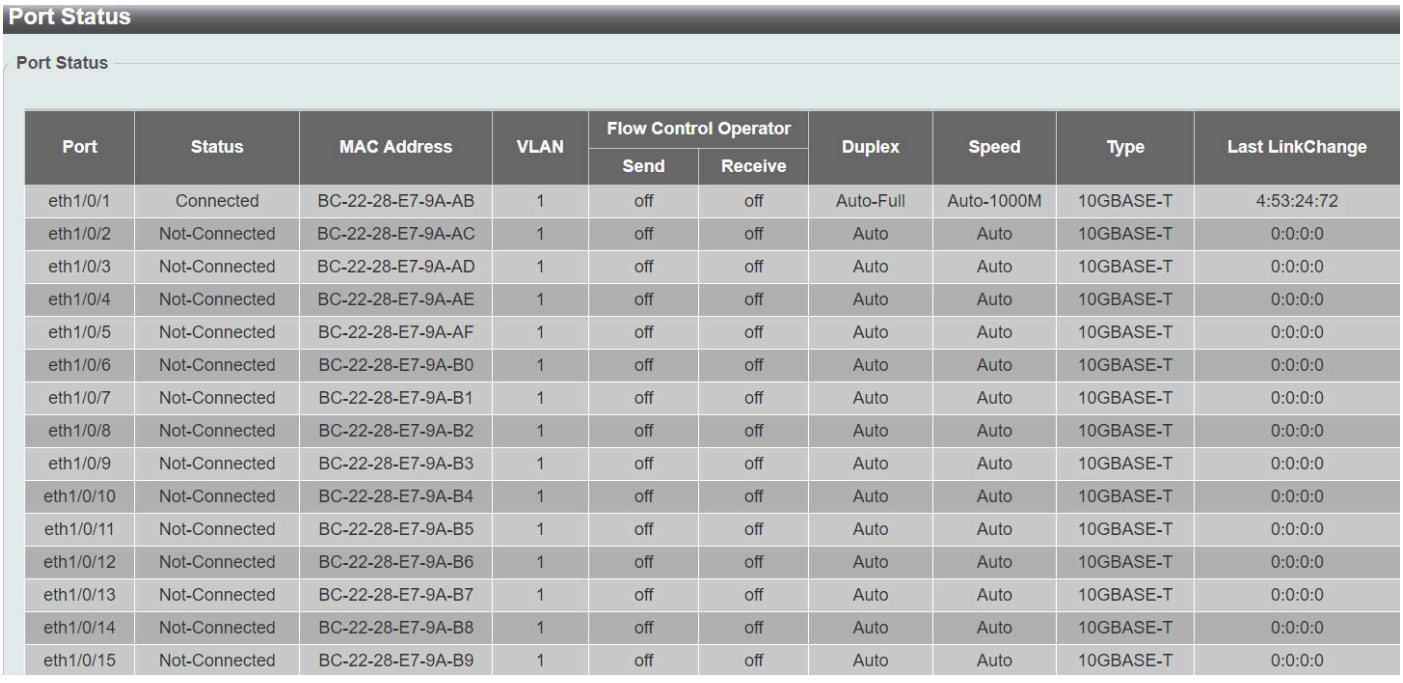
Parameter	Description
	• **5G Master** - Specifies to force the port speed to 5 Gbps and operates as the master, to facilitate the timing of transmit and receive operations. • **5G Slave** - Specifies to force the port speed to 5 Gbps and operates as the slave, to facilitate the timing of transmit and receive operations. • **10G** - Specifies to force the port speed to 10 Gbps. • **10G Master** - Specifies to force the port speed to 10 Gbps and operates as the master, to facilitate the timing of transmit and receive operations. • **10G Slave** - Specifies to force the port speed to 10 Gbps and operates as the slave, to facilitate the timing of transmit and receive operations. • **25G** - Specifies to force the port speed to 25 Gbps. **Notes:** 1. For the support of the speeds on each port, refer to the **DXS-3130-Series HW Installation Guide**. 2. The last 4 fiber optic ports must operate at the same speed.
Capability Advertised	When the **Speed** is set to **Auto**, select the capabilities to be advertised during auto-negotiation.
Description	Check the box to enter a description for the corresponding port here. This can be up to 64 characters.

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

Port Status

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

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



Port	Status	MAC Address	VLAN	Flow Control Operator		Duplex	Speed	Type	Last LinkChange
				Send	Receive				
eth1/0/1	Connected	BC-22-28-E7-9A-AB	1	off	off	Auto-Full	Auto-1000M	10GBASE-T	4:53:24:72
eth1/0/2	Not-Connected	BC-22-28-E7-9A-AC	1	off	off	Auto	Auto	10GBASE-T	0:0:0:0
eth1/0/3	Not-Connected	BC-22-28-E7-9A-AD	1	off	off	Auto	Auto	10GBASE-T	0:0:0:0
eth1/0/4	Not-Connected	BC-22-28-E7-9A-AE	1	off	off	Auto	Auto	10GBASE-T	0:0:0:0
eth1/0/5	Not-Connected	BC-22-28-E7-9A-AF	1	off	off	Auto	Auto	10GBASE-T	0:0:0:0
eth1/0/6	Not-Connected	BC-22-28-E7-9A-B0	1	off	off	Auto	Auto	10GBASE-T	0:0:0:0
eth1/0/7	Not-Connected	BC-22-28-E7-9A-B1	1	off	off	Auto	Auto	10GBASE-T	0:0:0:0
eth1/0/8	Not-Connected	BC-22-28-E7-9A-B2	1	off	off	Auto	Auto	10GBASE-T	0:0:0:0
eth1/0/9	Not-Connected	BC-22-28-E7-9A-B3	1	off	off	Auto	Auto	10GBASE-T	0:0:0:0
eth1/0/10	Not-Connected	BC-22-28-E7-9A-B4	1	off	off	Auto	Auto	10GBASE-T	0:0:0:0
eth1/0/11	Not-Connected	BC-22-28-E7-9A-B5	1	off	off	Auto	Auto	10GBASE-T	0:0:0:0
eth1/0/12	Not-Connected	BC-22-28-E7-9A-B6	1	off	off	Auto	Auto	10GBASE-T	0:0:0:0
eth1/0/13	Not-Connected	BC-22-28-E7-9A-B7	1	off	off	Auto	Auto	10GBASE-T	0:0:0:0
eth1/0/14	Not-Connected	BC-22-28-E7-9A-B8	1	off	off	Auto	Auto	10GBASE-T	0:0:0:0
eth1/0/15	Not-Connected	BC-22-28-E7-9A-B9	1	off	off	Auto	Auto	10GBASE-T	0:0:0:0

Figure 3-5 Port Status Window

Refer to the above **Port Settings** for more information on the status shown here.

The fields that can be configured are described below:

Parameter	Description
Unit	Select the stacking unit ID of the Switch that will be displayed here. This option is available

Port GBIC

This window is used to view active GBIC information found on each applicable physical port of this Switch.

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



Figure 3-6 Port GBIC Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this display here.

Port Auto Negotiation

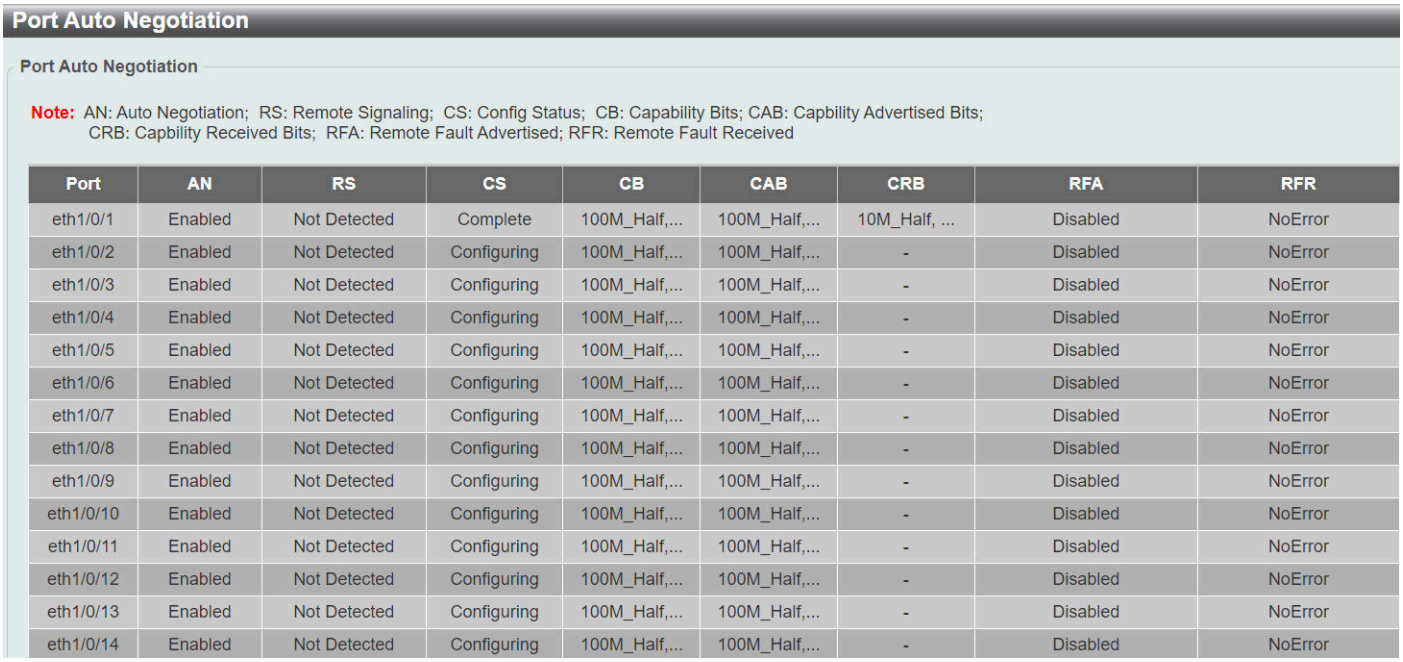
This window is used to view detailed port auto-negotiation information used for deteming the linking mode between link partners.

NOTE: Auto-negotiation is not supported on fiber optic ports.

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

The auto-negotiation information for each port includes the following:

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



Port	AN	RS	CS	CB	CAB	CRB	RFA	RFR
eth1/0/1	Enabled	Not Detected	Complete	100M_Half,...	100M_Half,...	10M_Half, ...	Disabled	NoError
eth1/0/2	Enabled	Not Detected	Configuring	100M_Half,...	100M_Half,...	-	Disabled	NoError
eth1/0/3	Enabled	Not Detected	Configuring	100M_Half,...	100M_Half,...	-	Disabled	NoError
eth1/0/4	Enabled	Not Detected	Configuring	100M_Half,...	100M_Half,...	-	Disabled	NoError
eth1/0/5	Enabled	Not Detected	Configuring	100M_Half,...	100M_Half,...	-	Disabled	NoError
eth1/0/6	Enabled	Not Detected	Configuring	100M_Half,...	100M_Half,...	-	Disabled	NoError
eth1/0/7	Enabled	Not Detected	Configuring	100M_Half,...	100M_Half,...	-	Disabled	NoError
eth1/0/8	Enabled	Not Detected	Configuring	100M_Half,...	100M_Half,...	-	Disabled	NoError
eth1/0/9	Enabled	Not Detected	Configuring	100M_Half,...	100M_Half,...	-	Disabled	NoError
eth1/0/10	Enabled	Not Detected	Configuring	100M_Half,...	100M_Half,...	-	Disabled	NoError
eth1/0/11	Enabled	Not Detected	Configuring	100M_Half,...	100M_Half,...	-	Disabled	NoError
eth1/0/12	Enabled	Not Detected	Configuring	100M_Half,...	100M_Half,...	-	Disabled	NoError
eth1/0/13	Enabled	Not Detected	Configuring	100M_Half,...	100M_Half,...	-	Disabled	NoError
eth1/0/14	Enabled	Not Detected	Configuring	100M_Half,...	100M_Half,...	-	Disabled	NoError

Figure 3-7 Port Auto Negotiation Window

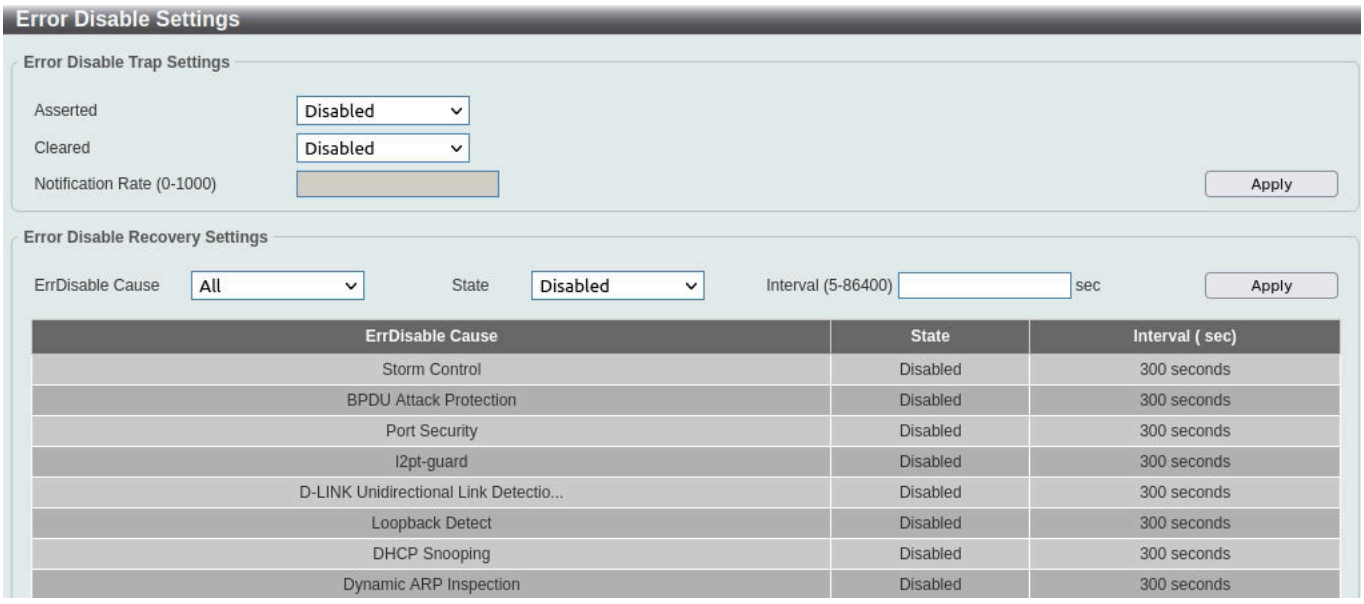
The fields that can be configured are described below:

Parameter	Description
Unit	Select the stacking unit ID of the Switch that will be displayed here. This option is only available when stacking is enabled.

Error Disable Settings

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

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



ErrDisable Cause	State	Interval (sec)
Storm Control	Disabled	300 seconds
BPDU Attack Protection	Disabled	300 seconds
Port Security	Disabled	300 seconds
l2pt-guard	Disabled	300 seconds
D-LINK Unidirectional Link Detectio...	Disabled	300 seconds
Loopback Detect	Disabled	300 seconds
DHCP Snooping	Disabled	300 seconds
Dynamic ARP Inspection	Disabled	300 seconds

Figure 3-8 Error Disable Settings Window

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

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

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

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

Parameter	Description
ErrDisable Cause	Select the error disabled cause here. Options to choose from are **All**, **Port Security, Storm Control, BPDU Attack Protection, Dynamic ARP Inspection, DHCP Snooping, Loopback Detect, L2PT Guard**, and **D-Link Unidirectional Link Detection**.
State	Select to enable or disable the error disabled recovery feature here.
Interval	Enter the time, in seconds, to recover the port from the error state caused by the specified module. The range is from 5 to 86400.

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

Jumbo Frame

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

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



Figure 3-9 Jumbo Frame Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the stacking unit ID of the Switch that will be configured here. This option is only available when stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
Maximum Receive Frame Size	Enter the maximum receive frame size value here. This value must be between 64 and 12,288 bytes. By default, this value is 1536 bytes.

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

Interfaces Description

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

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

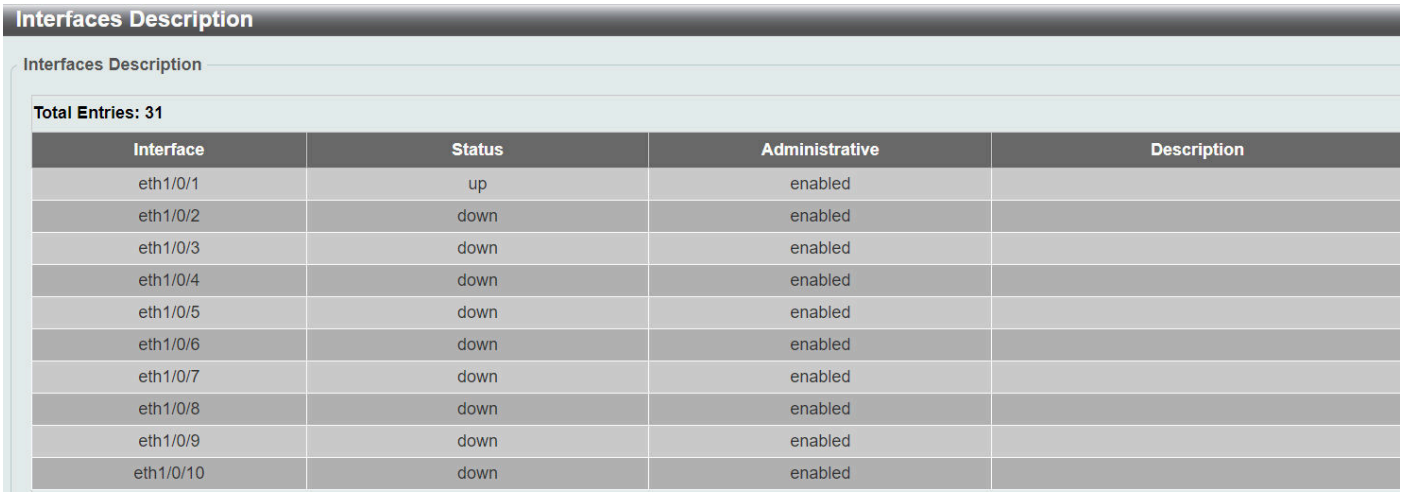


Figure 3-10 Interface Description Window

The description can be set in the **Port Settings**.For detailed information and configuration on the interfaces, refer to **L3 Features > Interface**.

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

PoE

The **DXS-3130-28P** switch supports Power over Ethernet (PoE) as defined by IEEE 802.3bt. All of the 10GBASE-T PoE ports can support PoE up to 60W. The Switch ports can supply a total of 790W (or 1440W when two PSU are installed) and about 54 VDC power to Powered Devices (PDs) over Ethernet cables. The Switch follows the standard Power Sourcing Equipment (PSE) pin-out Alternative A and Alternative B to deliver power over all four pairs of wire. The Switch work with all D-Link 802.3af, 802.3at, 802.3bt capable devices.

The Switch includes the following PoE features:

- Auto-discovery recognizes the connection of a PD and automatically sends power to it.

- The auto-disable feature occurs under two conditions:
  - If the total power consumption exceeds the system power limit
  - If the per-port power consumption exceeds the per port power limit
- Active circuit protection automatically disables the port if there is a short. Other ports will remain active.
- The Switch supports both Fast PoE and Perpetual PoE. By default, the Fast PoE is enabled and cannot be disabled manually, whereas the Perpetual PoE is disabled but can be enabled manually. For Fast PoE, PDs will be powered on without the need for the Swich to boot into the operating system. For Perpetual PoE, PDs will receive power even during system reboot.

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

Class	Maximum power used by the PD	Maximum power supplied by the Switch
1	3.84 Watts	4 Watts
2	6.49 Watts	7 Watts
3	13 Watts	15.4 Watts
4	25.5 Watts	30 Watts
5	40 Watts	45 Watts
6	51 Watts	60 Watts

PoE System

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

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

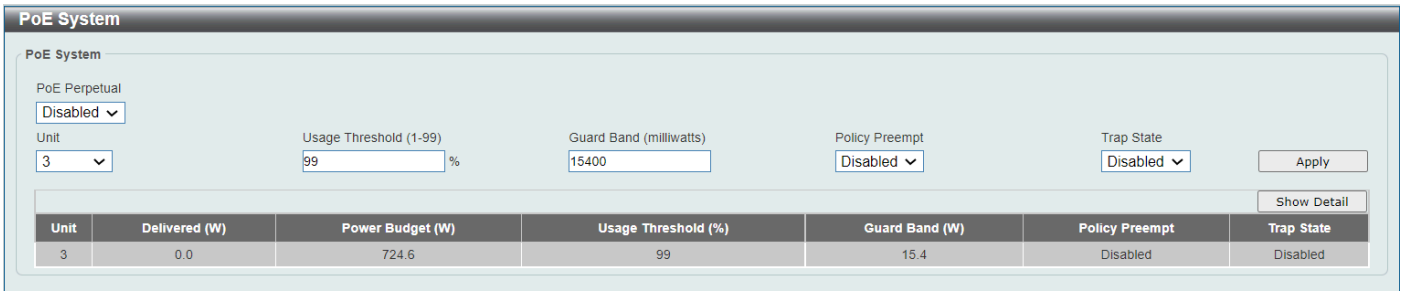


Figure 3-11 PoE System Window

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

Parameter	Description
PoE Perpetual	The POE Perpetual provides power to connected powered devices (PD) during system reboot. Disabling this option will not turn off the PoE. To enable or disable PoE on port basis, refer to **System > PoE > PoE Configuration.**
Unit	Select the stacking unit ID of the Switch that will be configured here. This option is only available when stacking is enabled.
Usage Threshold	Enter the usage threshold to generate a log and send the corresponding standard notification. The range is from 1 to 99 percent.
Guard Band	Specify the amount of power to be preserved for guard band protection. The range of valid setting is from 0 to 15400 milliwatts.

Parameter	Description
Policy Preempt	Select this option to enable or disable the disconnection of the Powered Device (PD) which is power provisioned with a lower priority in order to release the power to the newly connected PD with higher priority under power shortage conditions.
Trap State	Select this option to enable or disable the sending of PoE trap notifications.

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

Click the **Show Detail** button to see the PoE system Parameters table at the bottom of the window. After clicking the **Show Detail** button, the following information on PoE System Parameters will appear.

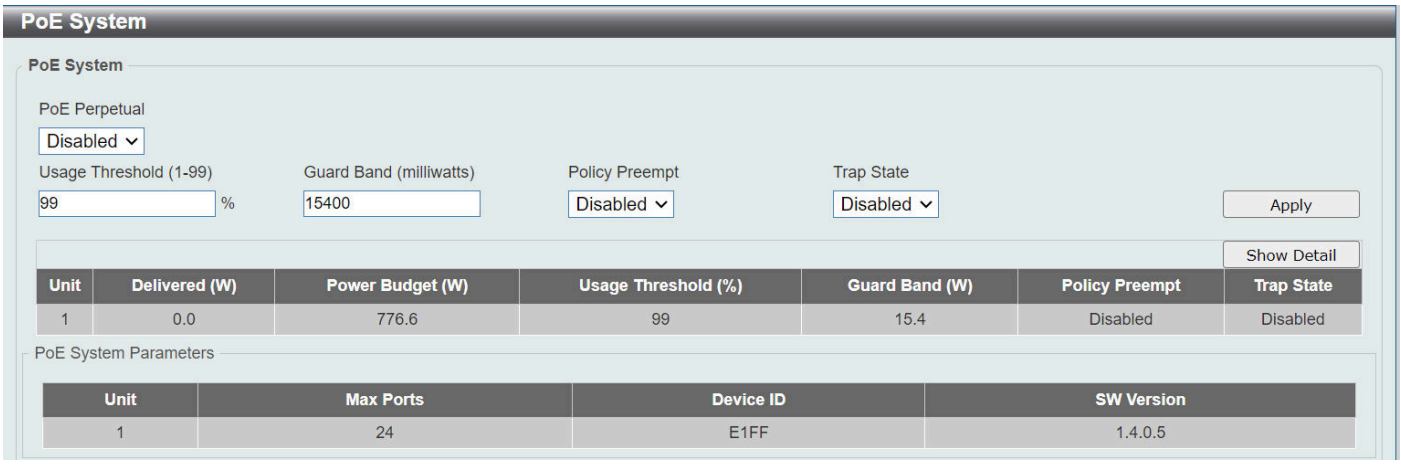


Figure 3-12 PoE System (Show Detail) Window

PoE Status

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

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

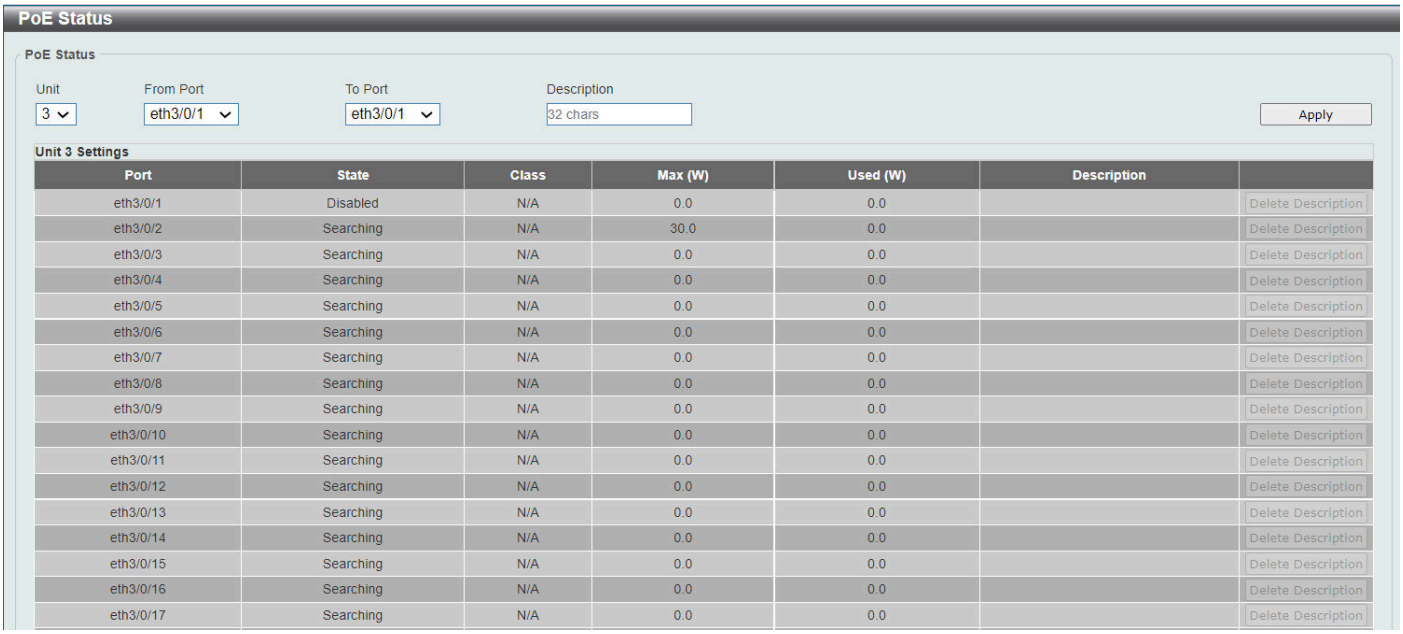


Figure 3-13 PoE Status Window

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

Parameter	Description
Unit	Select the stacking unit ID of the Switch that will be configured here. This option is only available when stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
Description	Enter the text that describes the PD connected to a PoE interface. The maximum length is 32 characters.

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

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

PoE Configuration

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

NOTE: If the Switch failed to supply power to the IEEE 802.3bt Powered Device (PD),

- Check if the PD connected to the port supports the 802.3bt standard.
- Manually configure the PoE power limit value to 60 Watts for the PoE ports. For information about PoE ports, refer to DXS-3130 Series HW Installation Guide.
- Disable **Power Via MDI** (refer to LLDP Dot3 TLVs Settings), which is disabled by default.

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

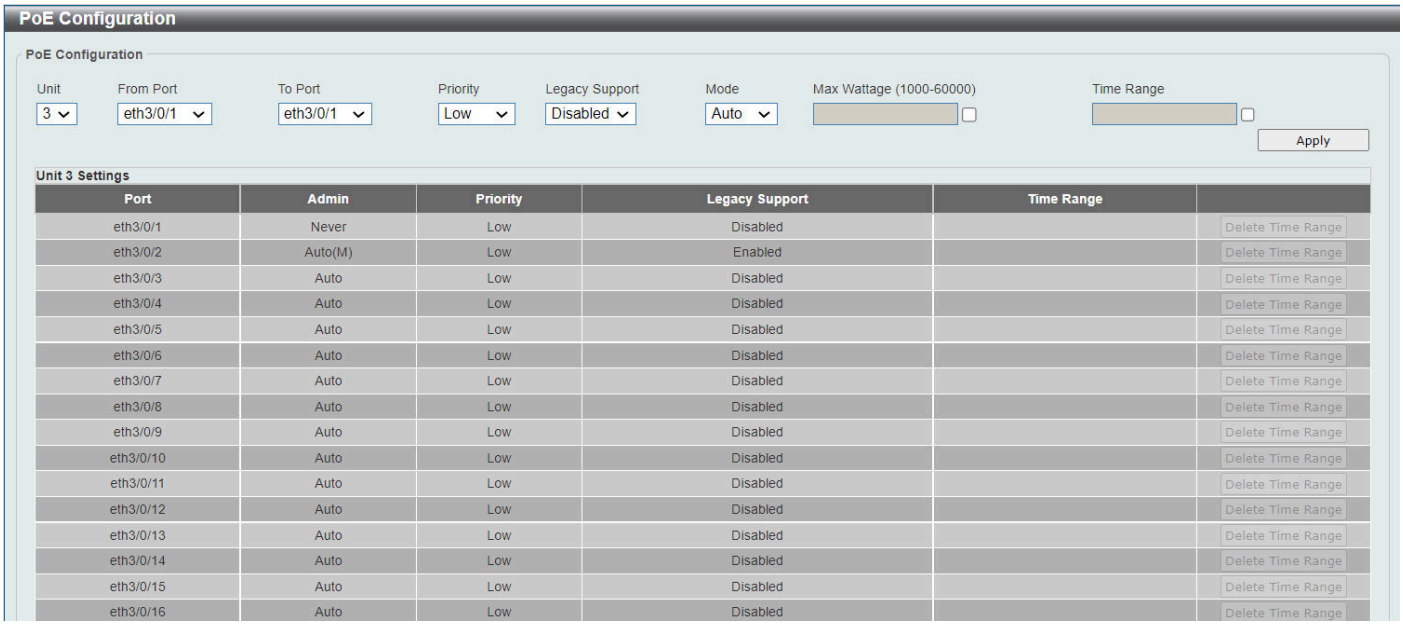


Figure 3-14 PoE Configuration Window

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

Parameter	Description
Unit	Select the stacking unit ID of the Switch that will be configured here. This option is only available when stacking is enabled.

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Priority	Select the priority for provisioning power to the port. Options to choose from are **Critical**, **High** and **Low**. A low priority means that the port can stop supplying power to connected PDs under power shortage conditions.
Legacy Support	Select this option to enable or disable the support of legacy PD.
Mode	Select the power management mode for the PoE ports. Options to choose from are **Auto** and **Never**.
Max Wattage	When selecting **Auto** in the **Mode** drop-down list, this option appears. Tick the check box and enter the maximum wattage of power that can be provisioned to the auto-detected PD. If the value is not entered, the class of the PD automatically determines the maximum wattage which can be provisioned. The valid range for maximum wattage is between 1000 mW and 60000 mW (milliwatt). One milliwatt equals to 0.001 watts.
Time Range	When selecting **Auto** in the **Mode** drop-down list, this option appears. Tick the check box and enter the name of the time range to determine the activation period. Refer to **System > Time** Range**.**

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

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

PoE Statistics

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

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

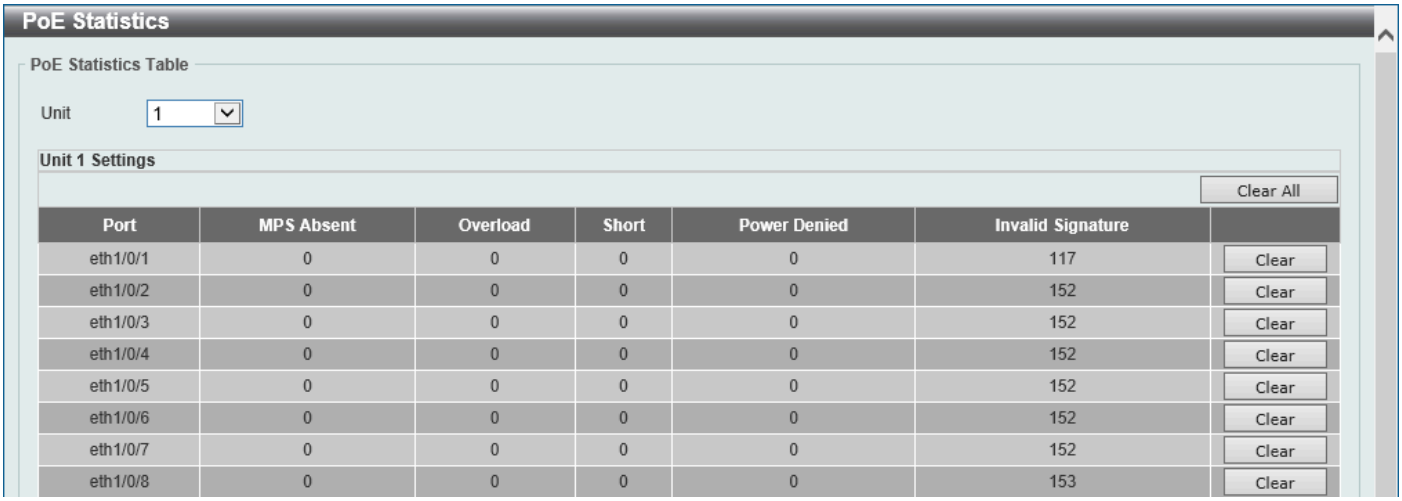


Figure 3-15 PoE Statistics Window

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

Parameter	Description
Unit	Select the stacking unit ID of the Switch that will be used here. This option is only available if stacking is enabled.

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

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

PoE Measurement

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

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

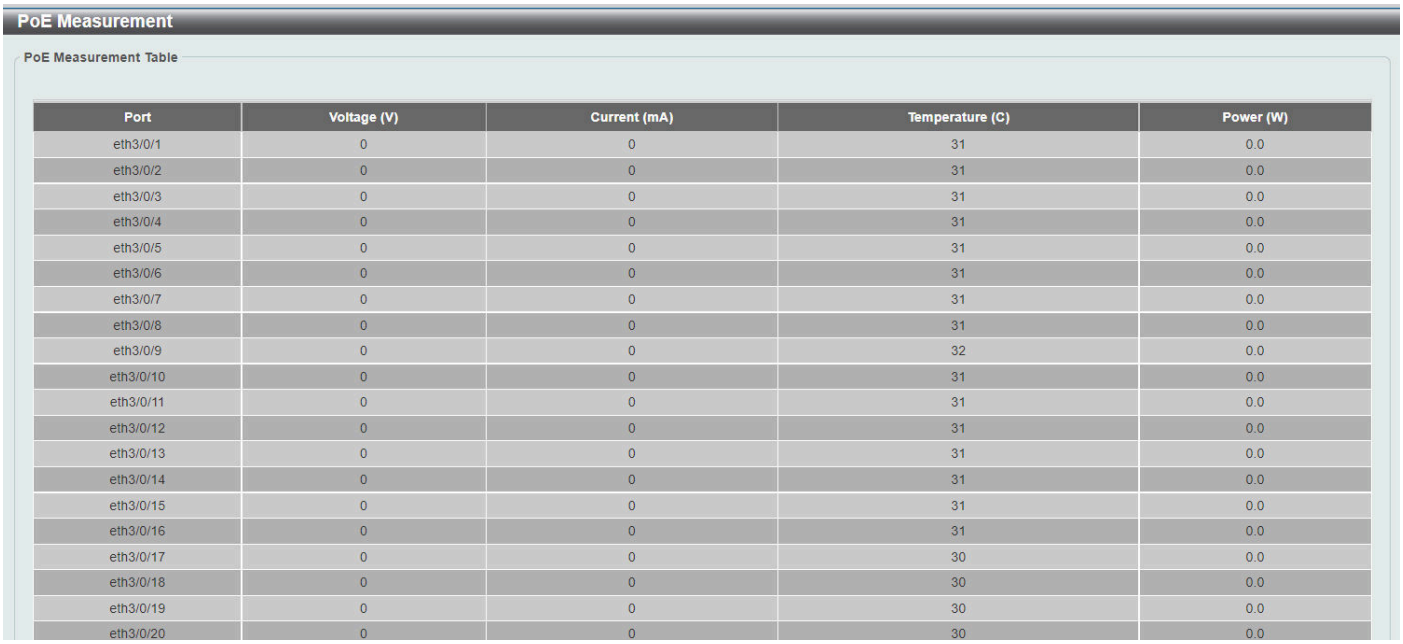


Figure 3-16 PoE Measurement Window

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

Parameter	Description
Unit	Select the stacking unit ID of the Switch that will be used here. This option is only available when stacking is enabled.

PoE LLDP Classification

The PoE LLDP Classification displays PoE messages between the PD and PSE negotiated over LLDP. For PSE, it shows information such as power priority and allocated power value (refer to the above sections on PoE related configuration). For PD related information, it shows information such as power priority and requested power value as shown in the following table:

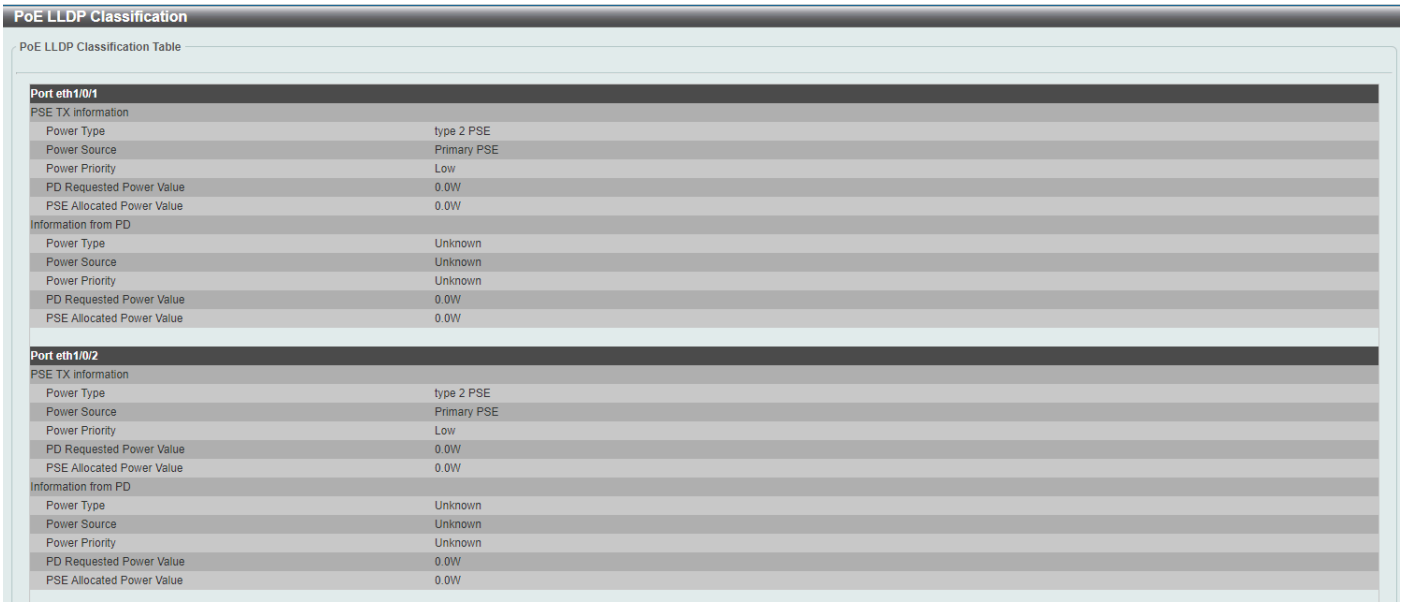


Figure 3-17 PoE LLDP Classification Table

PoE PD Alive Settings

This window is used to display and configure the PoE PD alive settings. The PoE alive feature provides the notification and reset mechanism when PD devices stop working or are not responding using the ping mechanism.

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

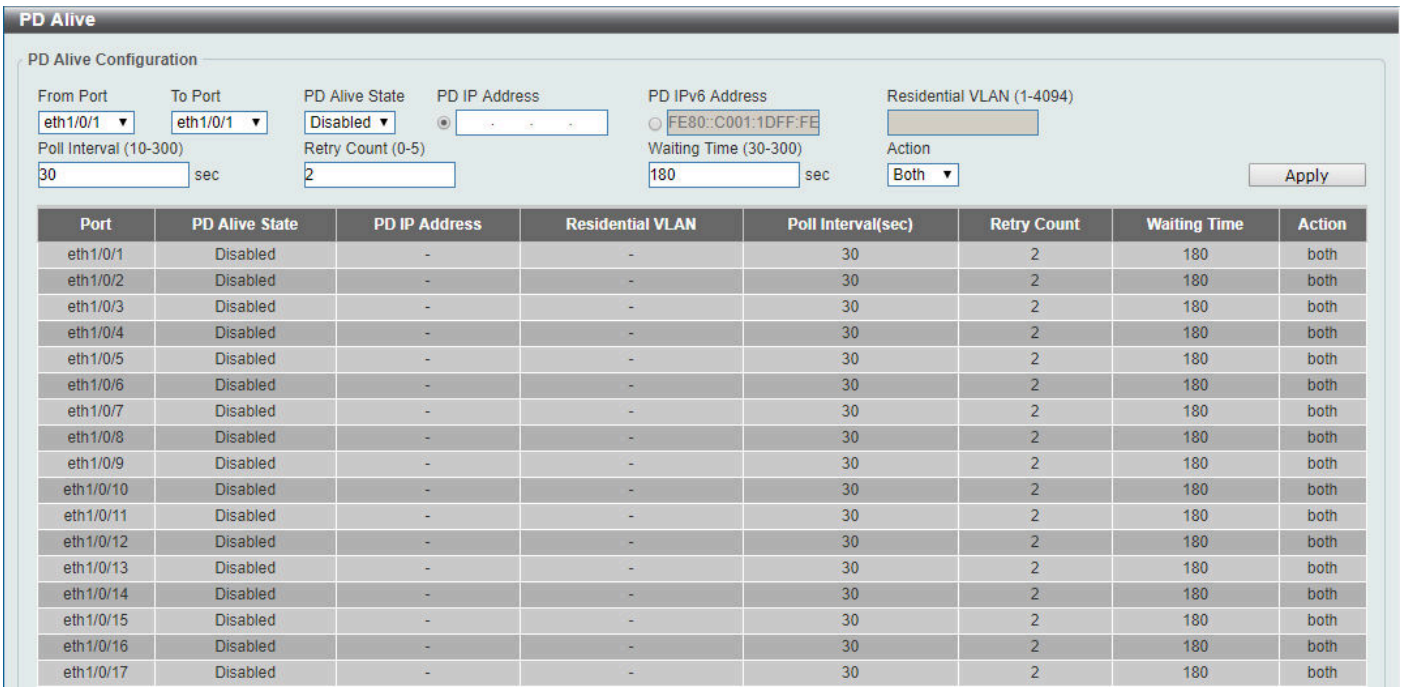


Figure 3-18 PD Alive Window

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

Parameter	Description
Unit	Select the stacking unit ID of the Switch that will be configured here. This option is only available if stacking is enabled.

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
PD Alive State	Select to enable or disable the state of the PoE alive function on the specified port(s) here.
PD IP Address	Enter the IPv4 address of the target PD here.
PD IPv6 Address	Enter the IPv6 address of the target PD here.
Residential VLAN (1-4094)	The VLAN ID assigned to the designated ports.
Poll Interval (sec)	Enter the poll interval value here. The range is from 10 to 300 seconds. This is the interval at which ping requests will be sent to the target PD to check the status.
Retry Count	Enter the retry count value here. The range is from 0 to 5. This is the number of times that the ping request will be resend if the target PD does not respond.
Waiting Time (30-300)	Enter the waiting time value here. The range is from 30 to 300 seconds. This is the time the Switch will wait for the PD to recover from rebooting.
Action	Select the action that will be taken here. Options to choose from are: • **Reset** - Specifies to reset the PoE port state. • **Notify** - Specifies to send logs and traps to notify the administrator. • **Both** - Specifies to send logs and traps and then to reset the PoE port state.

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

System Log

System Log Settings

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

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

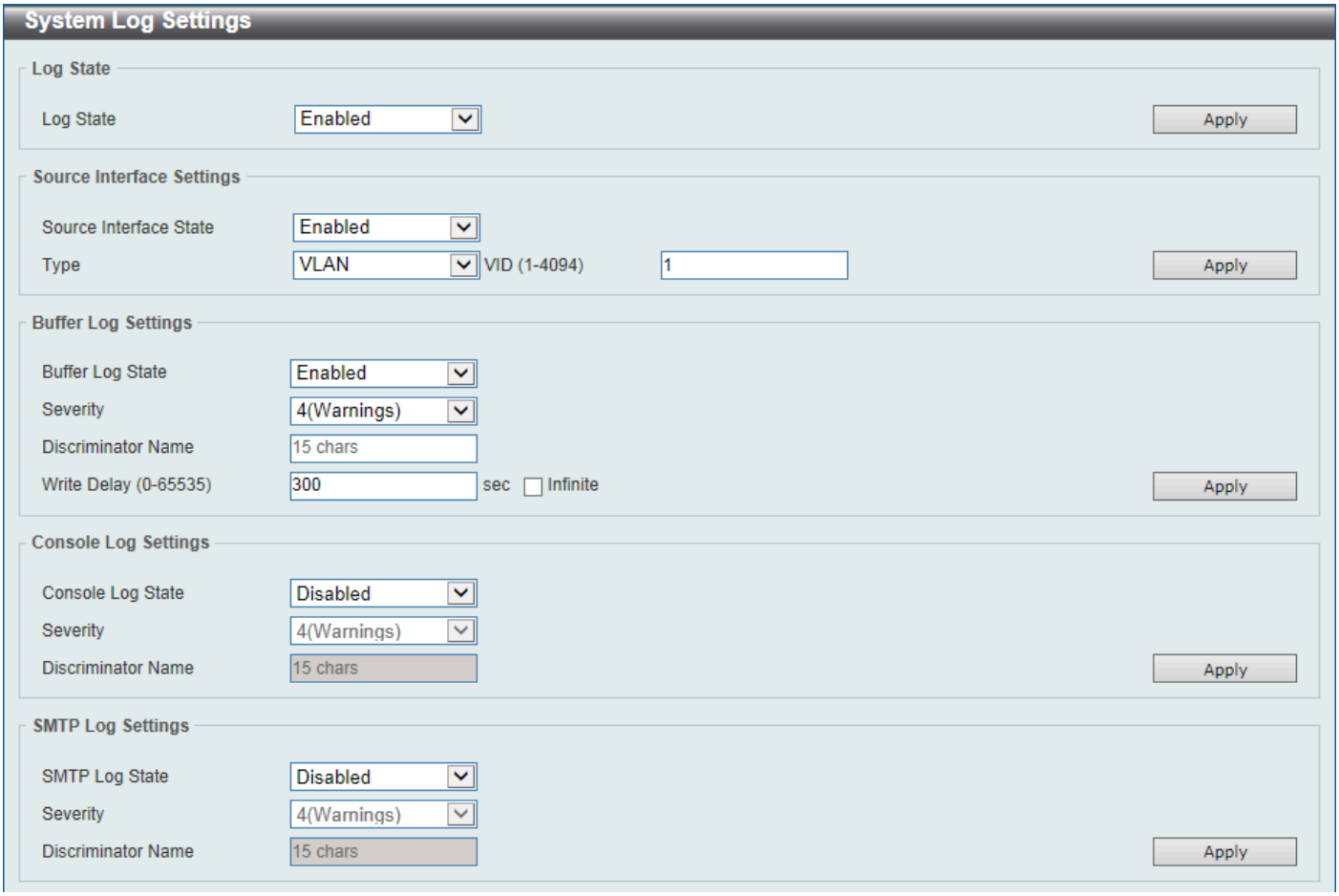


Figure 3-19 System Log Settings Window

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

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

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

The fields that can be configured for **Source Interface Settings** are described below:

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. The options are **Loopback**, **Mgmt**, and **VLAN**.
Interface ID (1-4094)	Enter the interface VID used here. For loopback interfaces this ID can be from 1 to 8. For the management (Mgmt) interface this value is always 0. For VLAN interfaces this value is from 1 to 4094.

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

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

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

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

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

Parameter	Description
Console Log State	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. Refer to **System Log Discriminator Settings** for more information.

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

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

Parameter	Description
SMTP Log State	Enable or disable the global 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. Refer to **System Log Discriminator Settings** for more information.

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

System Log Discriminator Settings

This window is used to display and configure the system log discriminator settings. It allows you to filter logs generated based on the facility types.

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

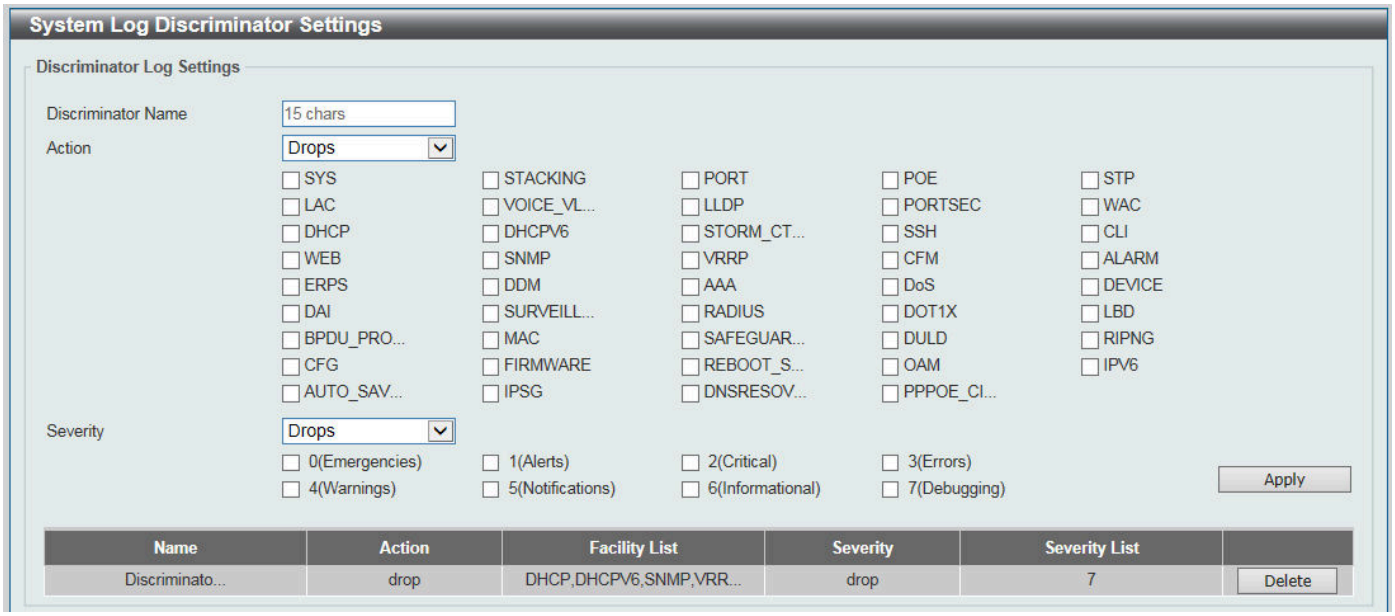


Figure 3-20 System Log Discriminator Settings Window

The fields that can be configured are described below:

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

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

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

System Log Server Settings

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

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

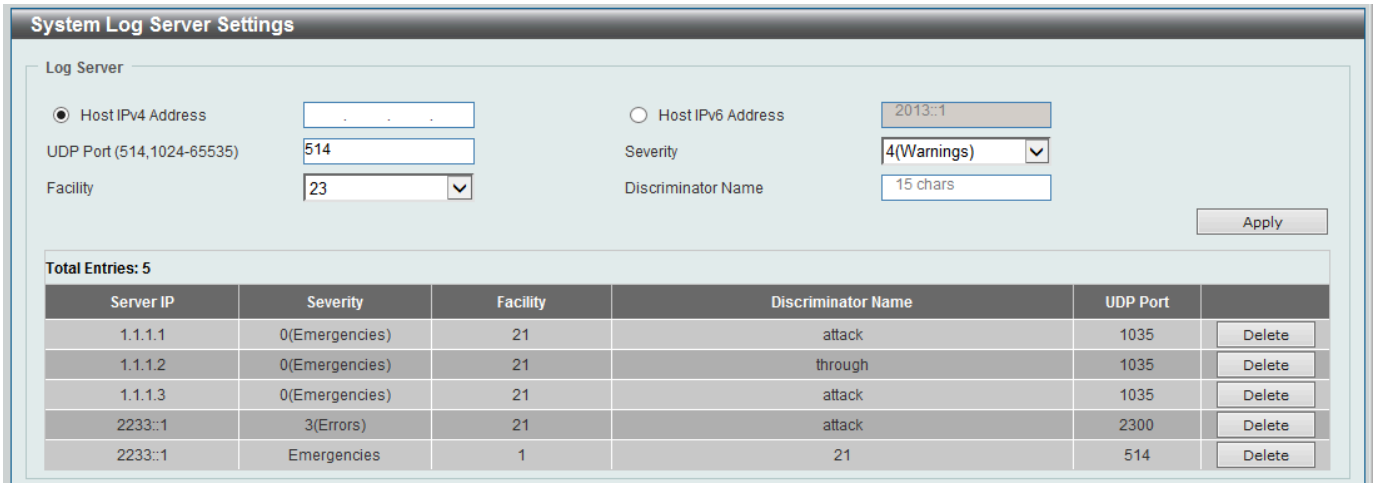


Figure 3-21 System Log Server Settings Window

The fields that can be configured are described below:

Parameter	Description
Host IPv4 Address	Enter the system log server IPv4 address here.
Host IPv6 Address	Enter the system log server IPv6 address here.
UDP Port	Enter the system log server UDP port number here. This value must be either 514 or between 1024 and 65535. By default, this value is 514.
Severity	Select the severity value of the type of information that will be logged. Options to choose from are **0 (Emergencies), 1 (Alerts), 2 (Critical), 3 (Errors), 4 (Warnings), 5 (Notifications), 6 (Informational)**, and **7 (Debugging).**
Facility	Select the facility number that will be logged here. The range is from 0 to 23. Each facility number is associated with a specific facility. See the table below:

Facility Number	Facility Name	Facility Description
0	kern	Kernel messages
1	user	User-level messages
2	mail	Mail system
3	daemon	System daemons
4	auth1	Security/authorization messages
5	syslog	Messages generated internally by the SYSLOG
6	lpr	Line printer sub-system
7	news	Network news sub-system
8	uucp	UUCP sub-system
9	clock1	Clock daemon
10	auth2	Security/authorization messages
11	ftp	FTP daemon
12	ntp	NTP subsystem
13	logaudit	Log audit
14	logalert	Log alert
15	clock2	Clock daemon

Parameter	Description		
	16	local0	Local use 0 (local0)
	17	local1	Local use 1 (local1)
	18	local2	Local use 2 (local2)
	19	local3	Local use 3 (local3)
	20	local4	Local use 4 (local4)
	21	local5	Local use 5 (local5)
	22	local6	Local use 6 (local6)
	23	local7	Local use 7 (local7)
Discriminator Name	Enter the name of the discriminator that will be used to filter messages sent to the log server here. This name can be up to 15 characters long. Refer to **System Log Discriminator Settings** for more information.		

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

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

System Log

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

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

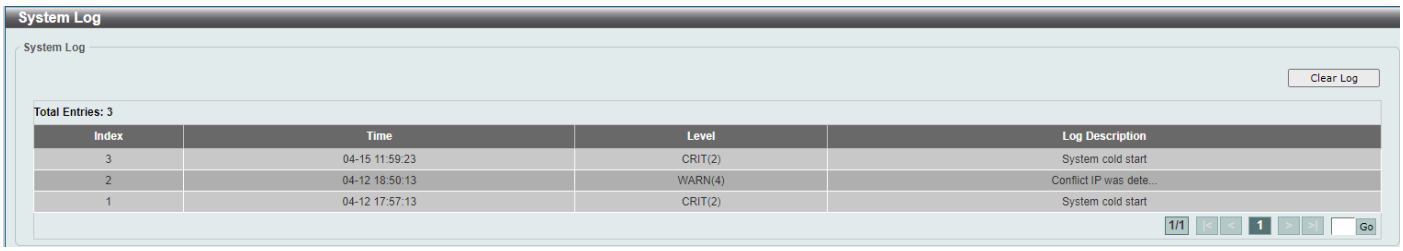


Figure 3-22 System Log Window

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

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

System Attack Log

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

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



Figure 3-23 System Attack Log Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the stacking unit ID of the Switch that will be displayed here. This option is only available when stacking is enabled.

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

Time and SNTP

Clock Settings

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

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

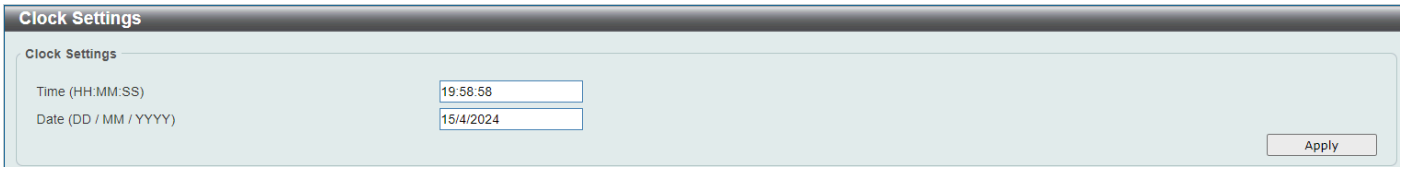


Figure 3-24 Clock Settings Window

The fields that can be configured are described below:

Parameter	Description
Time	Enter the current time in hours (HH) in 24-hour clock notation, minutes (MM), and seconds (SS) here. For example, 18:30:30.
Date	Enter the current day (DD), month (MM), and year (YYYY) here. For example, 30/04/2015.

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

Time Zone Settings

This window is used to display and configure time zones and Daylight Savings Time settings for Simple Network Time Protocol (SNTP).

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

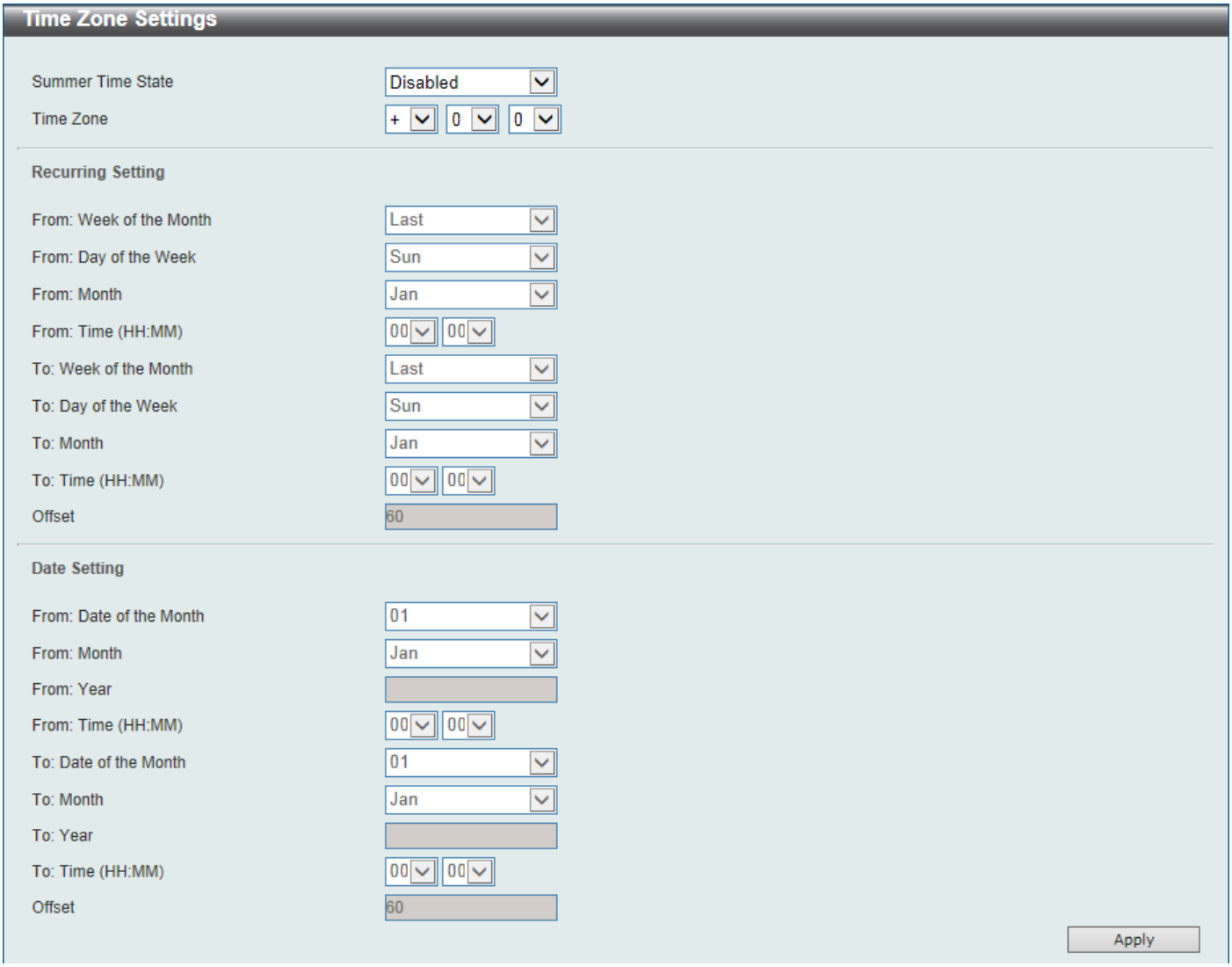


Figure 3-25 Time Zone Settings Window

The fields that can be configured are described below:

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

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

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

Parameter	Description
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 (HH:MM)	Select the time of the day that summer time will start in 24-hour clock.
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 (HH:MM)	Select the time of the day that summer time will end.
Offset	Enter the number of minutes to add during summer time.

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

Parameter	Description
From: Date of the Month	Select date of the month that summer time will start.
From: Month	Select the month that summer time will start.
From: Year	Enter the year that the summer time will start.
From: Time (HH:MM)	Select the time of the day that summer time will start in 24-hour clock notation.
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 (HH:MM)	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.

SNTP Settings

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

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

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

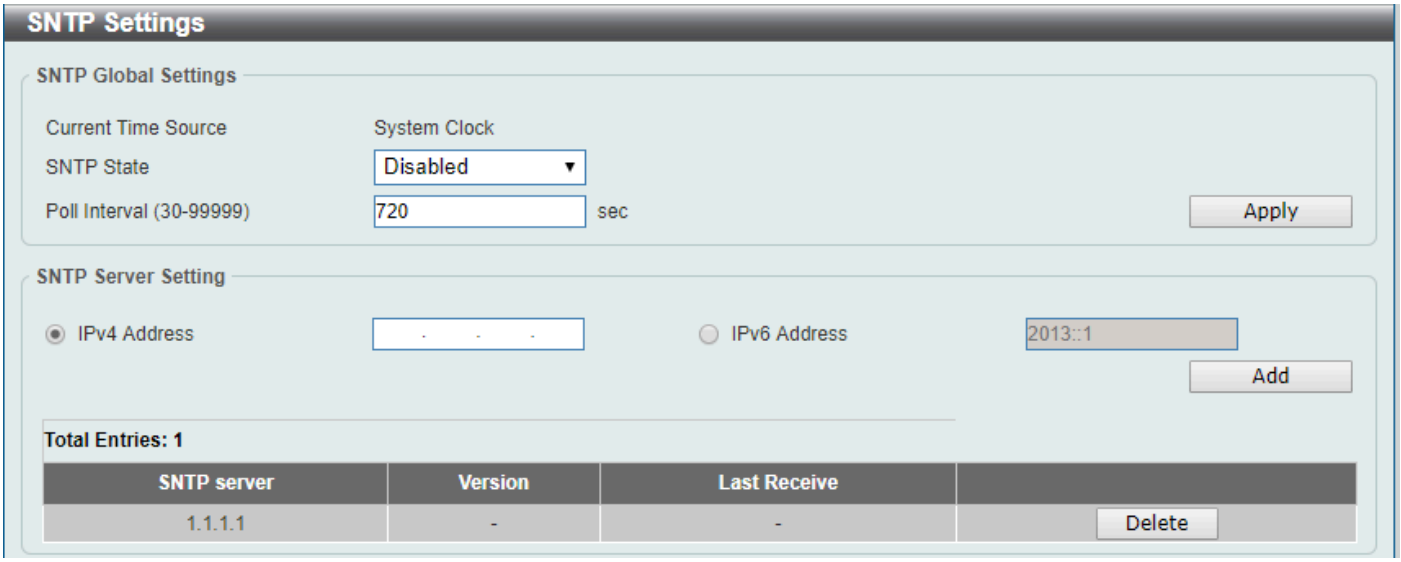


Figure 3-26 SNTP Settings Window

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

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

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

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

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

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

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

Time Range

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

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

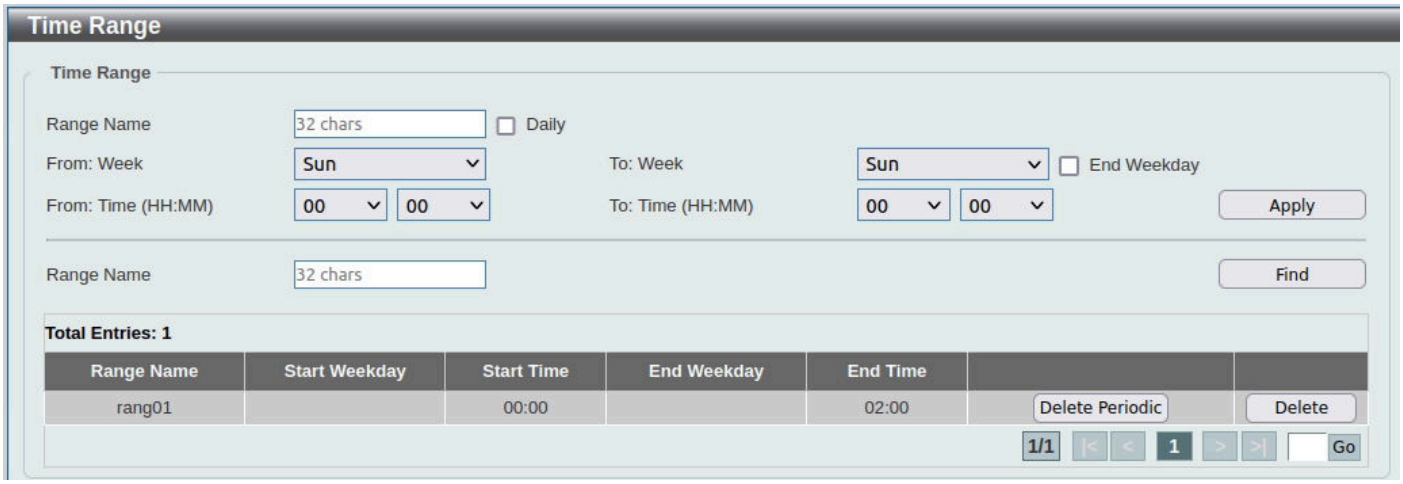


Figure 3-27 Time Range Window

The fields that can be configured are described below:

Parameter	Description
Range Name	Enter the time profile range name here. This name can be up to 32 characters long. Note that you can define multiple schedules for a single range profile.
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 Weekday** option to use this time profile from the starting day of the week until the end of the week.
From Time ~ To Time	Select the starting and ending time of the day that will be used for this time profile. The first drop-down menu selects the hour and the second drop-down menu selects the minute.

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

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

Click the **Delete Periodic** button to delete the periodic entry for multiple schedules of a ranlge profile.

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

Switch Controller Settings

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

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



Figure 3-28 Switch Controller Settings Window

The fields that can be configured are described below:

Parameter	Description
HoL Prevention State	Select to enable or disable the HoL (Head of Line) Prevention function here.

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

4. Management

Command Logging
User Accounts Settings
Password Encryption
Password Recovery
Login Method
SNMP
RMON
Telnet/Web
Session Timeout
DHCP
DHCP Auto Configuration
DNS
IP Source Interface
File System
Stacking
Virtual Stacking (SIM)
D-Link Discovery Protocol
SMTP Settings
Reboot Schedule Settings
PPPoE Circuit ID Insertion Settings
SD Card Management

Command Logging

This window is used to display and configure the command logging function. The command logging function is used to log the commands that have successfully been configured on the Switch via the command line interface. The command, along with information about the user that entered the command, is included in the system log. Commands that do not cause a change in the Switch configuration or operation (such as 'show' commands) are not logged.

To view the following window, click **Management > Command Logging**, as shown below:

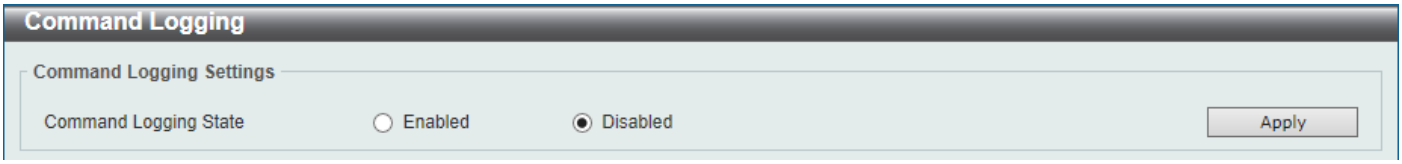


Figure 4-1 Command Logging Window

The fields that can be configured are described below:

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

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

User Accounts Settings

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

There are several configuration options available in the Web User Interface (Web UI). The set of configuration options available to the user depends on the account's **Privilege Level**.

NOTE: By default, there are no user accounts created on the Switch.

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

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

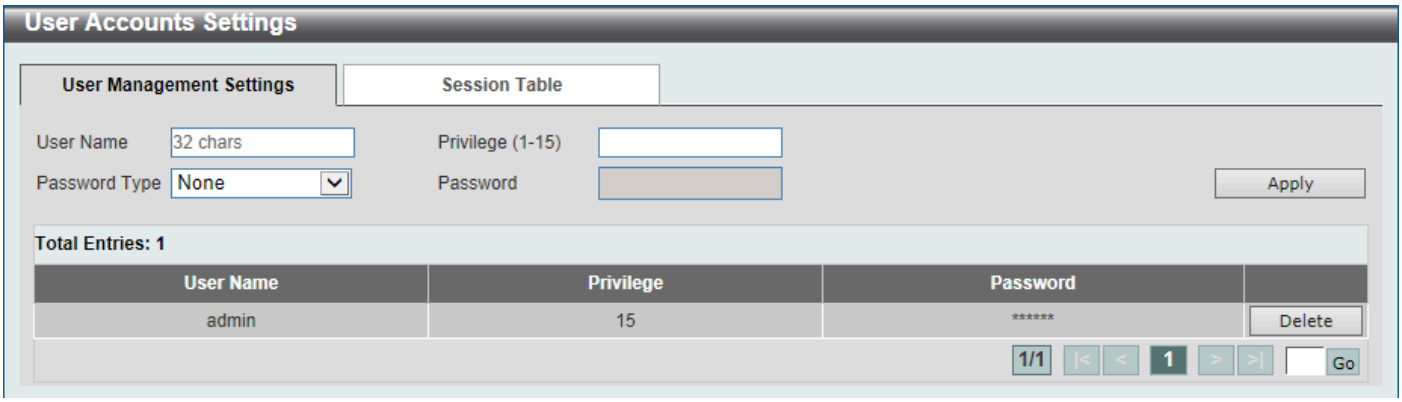


Figure 4-2 User Accounts Settings Window

The fields that can be configured are described below:

Parameter	Description
User Name	Enter the user account name here. This name can be up to 32 characters long and is case sensitive.
Privilege	Enter the privilege level for this account here. The range is from 1 to 15. Privilege levels define what commands users can execute. The range is from 1 to 15. Level 1 is the lowest level which can only view settings and access to limited commands; level 15 has full administrative access.
Password Type	Select the password type for this user account here. Options are **None, Plain Text, Encrypted-SHA1**, and **Encrypted-MD5**.
Password	After selecting **Plain Text, Encrypted-SHA1**, or **Encrypted-MD5** as the password type, enter the password for this user account here. In the plain-text form, the password must contain 8-30 characters and include at least one uppercase and lowercase letter, one number, and one symbol, such as @!&*. It must not be identical to the username and must not contain adjacent identical characters or digits or the default IP address. In the encrypted SHA1 form, the password must be 35 characters long and contain *@& in the beginning. In the encrypted MD5 form, the password must be 31 characters long and contain *@$ in the beginning.

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

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

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

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

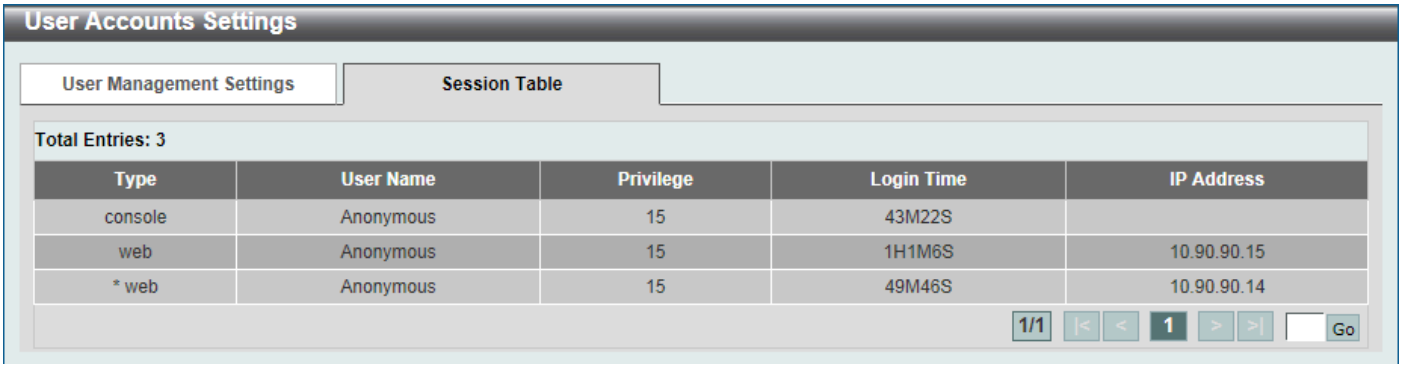


Figure 4-3 Session Table Window

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

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

Password Encryption

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

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

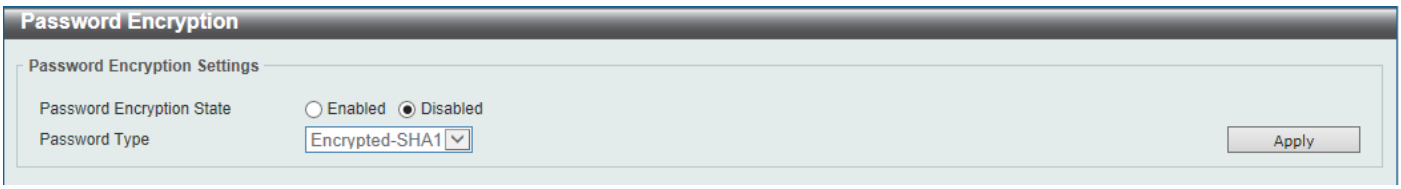


Figure 4-4 Password Encryption Window

The fields that can be configured are described below:

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

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

Password Recovery

This window is used to display and configure the password recovery settings. For example, the administrator may need to update a user account because the password has been forgotten.

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

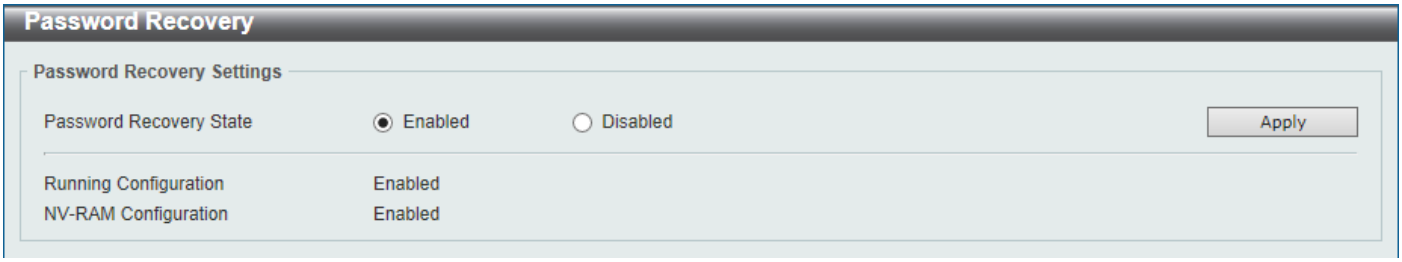


Figure 4-5 Password Recovery Window

The fields that can be configured are described below:

Parameter	Description
Password Recovery State	Select to enable or disable the password recovery feature here. Enabling this feature allows access to the reset configuration mode in the CLI. From the reset configuration mode, user accounts can be updated, the enable password feature can be updated for administrator privilege levels, and the AAA feature can be disabled to allow local authentication. The running configuration can then be saved as the startup configuration. A reboot is required.

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

Login Method

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

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

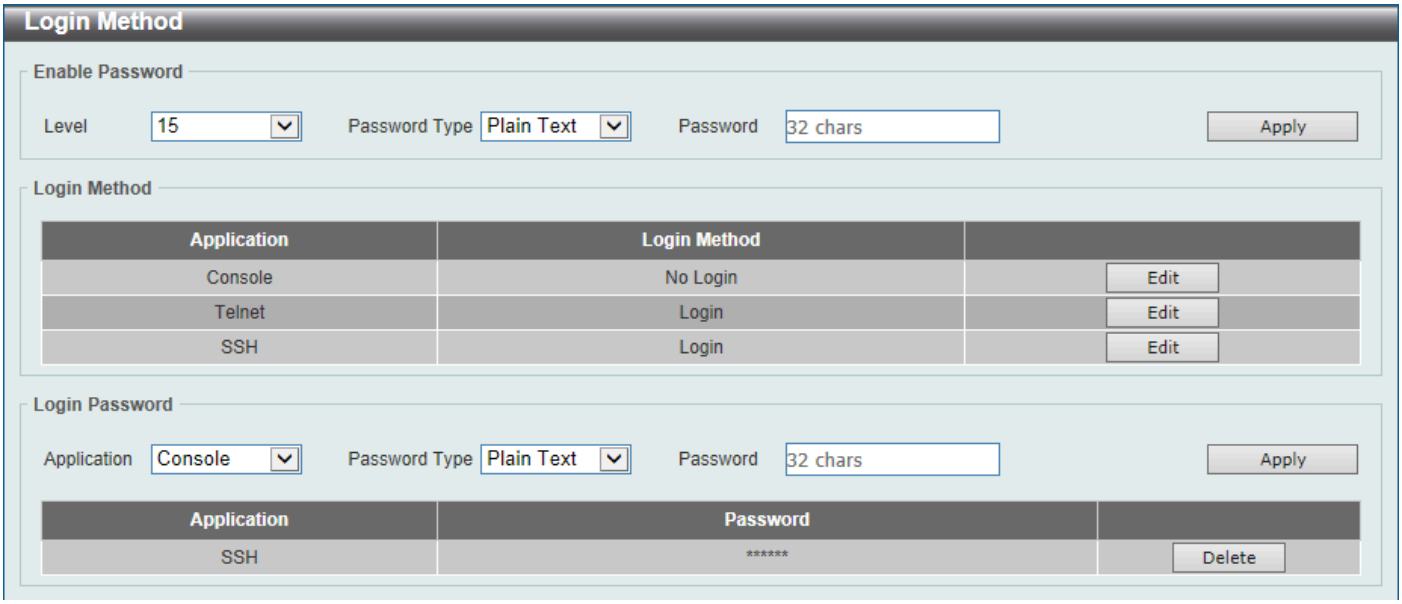


Figure 4-6 Login Method Window

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

Parameter	Description
Level	Specify the privilege level for privileged mode. The range is from 1 to 15.

Parameter	Description
Password Type	Select the password type for the user here. Options to choose from are: • **Plain Text** - Specifies that the password will be in plain text. This is the default option. • **Encrypted-SHA1** - Specifies that the password will be encrypted based on SHA-1. • **Encrypted-MD5** - Specifies that the password will be encrypted based on MD5.
Password	Specify the password to enable the privilege level. In the plain-text form, the password can be up to 32 characters long and is case sensitive. In the encrypted SHA1 form, the password must be 35 characters long and contain *@& in the beginning. In the encrypted MD5 form, the password must be 31 characters long and contain *@$ in the beginning.

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

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

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

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

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

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

Parameter	Description
Application	Select the application that will be configured here. Options to choose from are **Console**, **Telnet** and **SSH**.
Password Type	Select the password encryption type that will be used here. Options to choose from are **Plain Text, Encrypted**, and **Encrypted-MD5.**
Password	Enter the password for the selected application here. This password will be used when the **Login Method** for the specified application is set as **Login**. In the plain-text form, the password can be up to 32 characters long and is case sensitive. In the encrypted SHA1 form, the password must be 35 characters long and contains *@& in the beginning. In the encrypted MD5 form, the password must be 31 characters long and contains *@$ in the beginning.

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

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

SNMP

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

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

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

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

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

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

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

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

MIBs

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

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

Traps

Traps are messages that alert network personnel of events that occur on the Switch. The events can be as serious as a reboot (someone accidentally turned the Switch off/unplugged the Switch), or less serious like a port status change.

The Switch generates traps and sends them to the trap recipient (or network manager). Typical traps include trap messages for Authentication Failure, Topology Change and Broadcast/Multicast Storm.

SNMP Global Settings

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

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

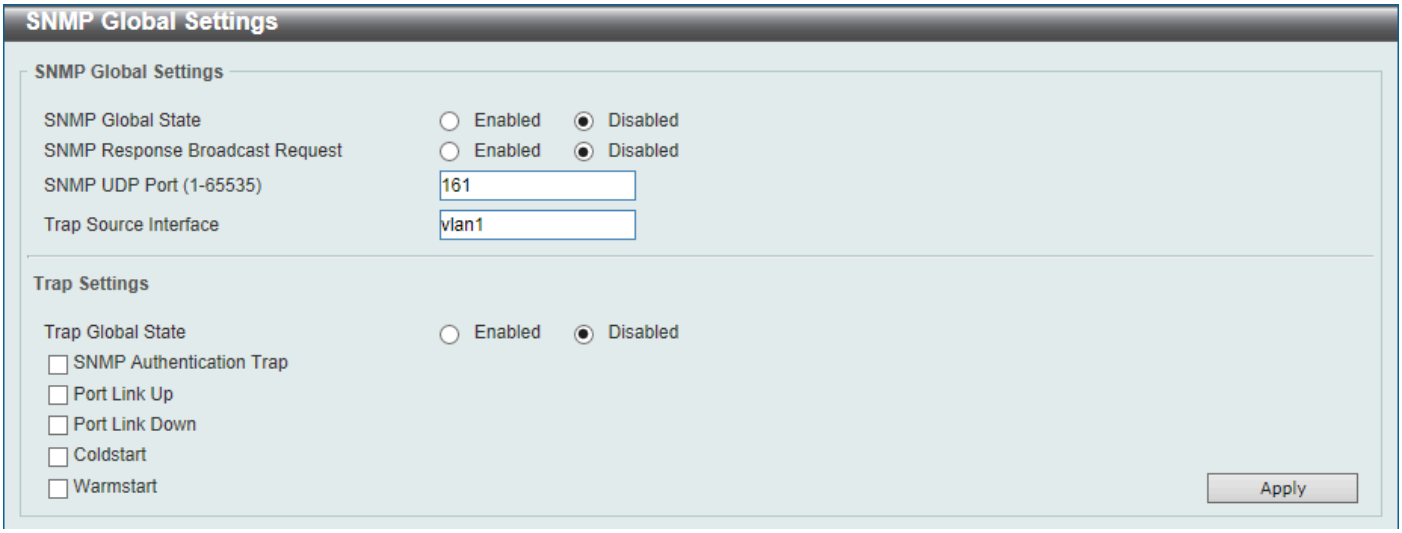


Figure 4-7 SNMP Global Settings Window

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

Parameter	Description
SNMP Global State	Select this option to enable or disable the SNMP feature.
SNMP Response Broadcast Request	Select this option to enable or disable the server to response to broadcast SNMP GetRequest packets.
SNMP UDP Port	Enter the SNMP UDP port number (1-65535).
Trap Source Interface	Enter the interface whose IP address will be used as the source address for sending the SNMP trap packet.

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

Parameter	Description
Trap Global State	Select this option to enable or disable the sending of all or specific SNMP notifications.
SNMP Authentication Trap	Tick this option to control the sending of SNMP authentication failure notifications. An *authenticationFailuretrap* trap is generated when the device receives an SNMP message that is not properly authenticated. The authentication method depends on the version of SNMP being used. For SNMPv1 or SNMPv2c, authentication failure occurs if packets are formed with an incorrect community string. For SNMPv3, authentication failure occurs if packets are formed with an incorrect SHA/MD5 authentication key.
Port Link Up	Tick this option to control the sending of port link up notifications. A *linkUp* trap is generated when the device recognizes that one of the communication links has come up.

Parameter	Description
Port Link Down	Tick this option to control the sending of port link down notifications. A *linkDown* trap is generated when the device recognizes that one of the communication links is down.
Coldstart	Tick this option to control the sending of SNMP *coldStart* notifications.
Warmstart	Tick this option to control the sending of SNMP *warmStart* notifications.

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

SNMP Linkchange Trap Settings

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

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

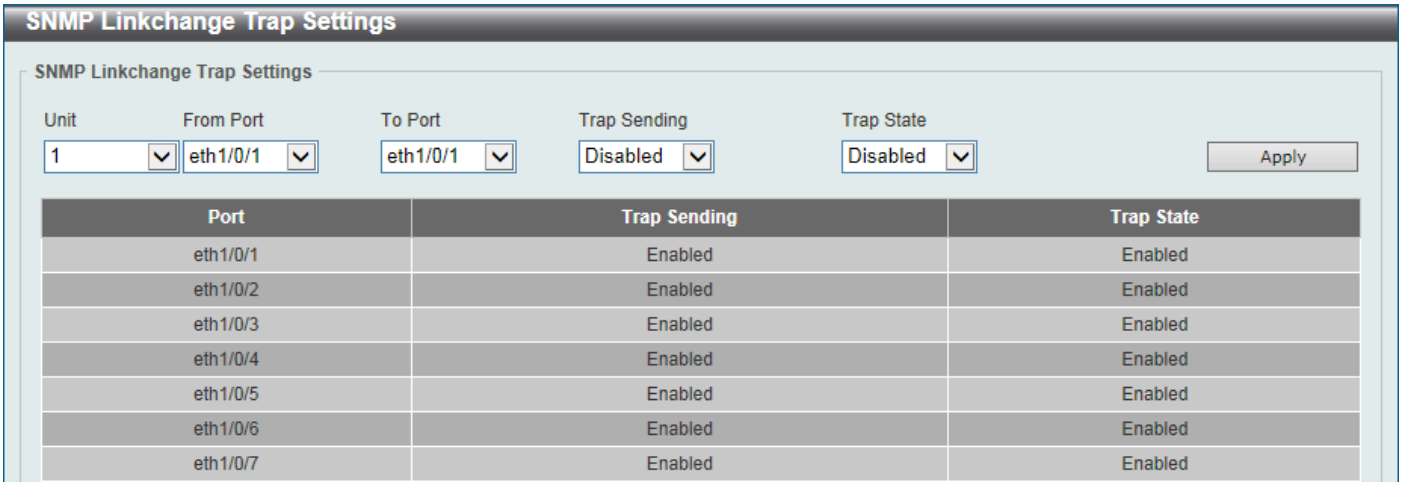


Figure 4-8 SNMP Linkchange Trap Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
Trap Sending	Select this option to enable or disable the sending of the SNMP notification traps that are generated by the system.
Trap State	Select this option to enable or disable the SNMP *linkChange* trap.

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

SNMP View Table Settings

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

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

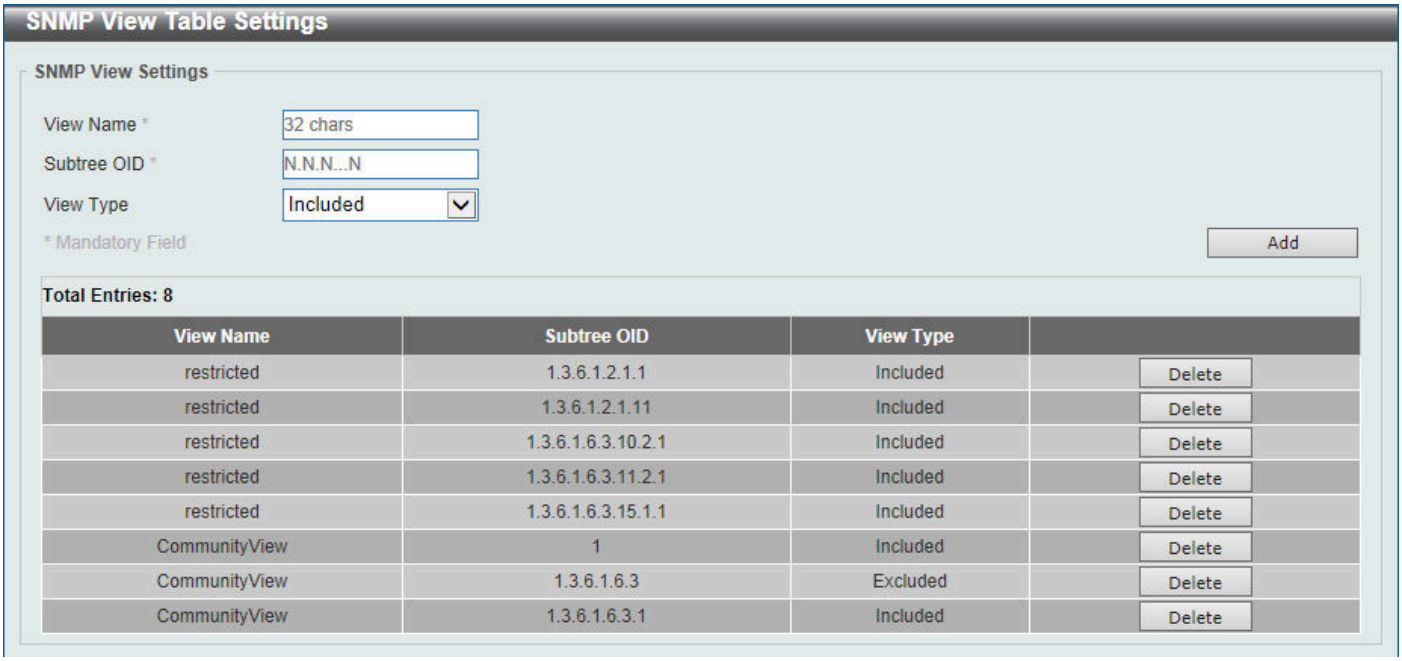


Figure 4-9 SNMP View Table Settings Window

The fields that can be configured are described below:

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

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

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

SNMP Community Table Settings

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

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

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

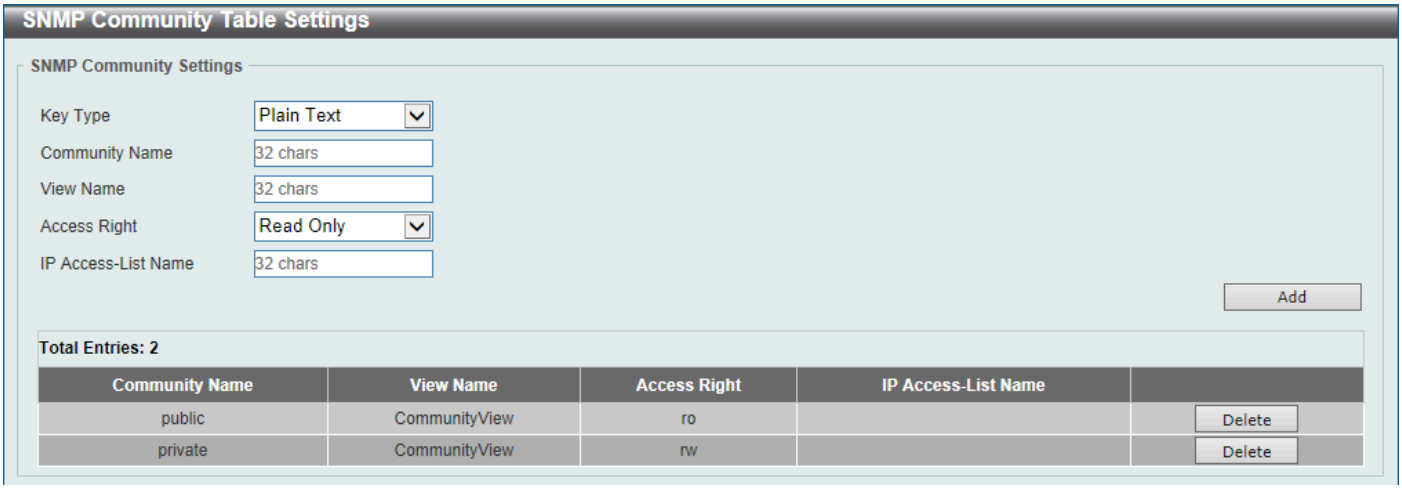


Figure 4-10 SNMP Community Table Settings Window

The fields that can be configured are described below:

Parameter	Description
Key Type	Select the key type for the SNMP community. Options to choose from are **Plain Text**, and **Encrypted**.
Community Name	Enter an alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.
View Name	Enter an alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. The view name must exist in the SNMP View Table.
Access Right	Select the access right here. Options to choose from are **Read Only** and **Read Write**. • **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 or 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. **Refer to ACL > ACL Access List**.

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

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

SNMP Group Table Settings

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

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

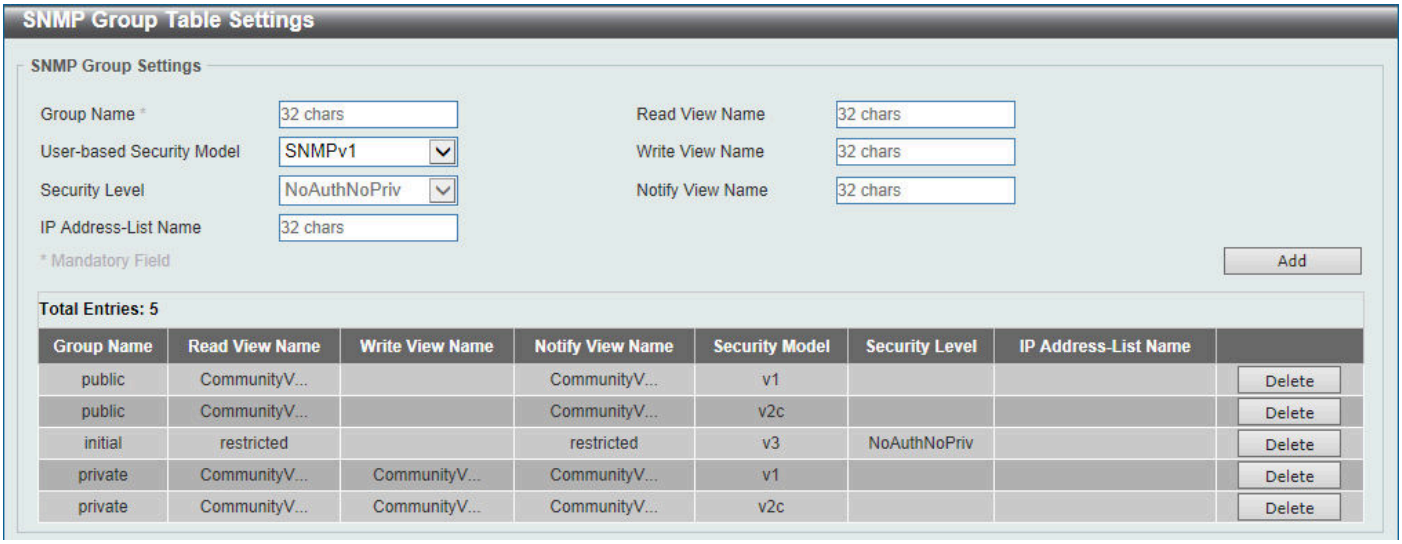


Figure 4-11 SNMP Group Table Settings Window

The fields that can be configured are described below:

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

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

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

SNMP Engine ID Local Settings

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

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

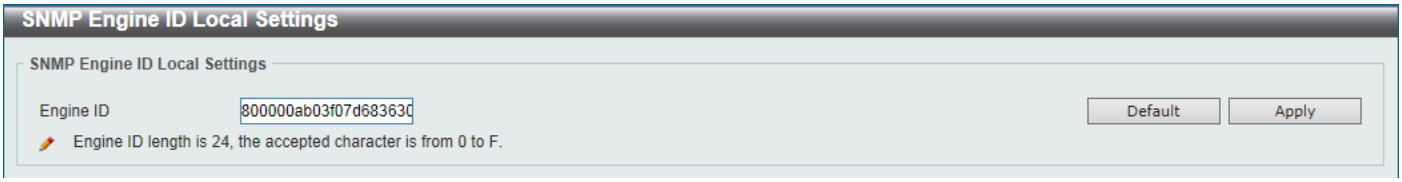


Figure 4-12 SNMP Engine ID Local Settings Window

The fields that can be configured are described below:

Parameter	Description
Engine ID	Enter the SNMP engine ID string here. It can accept up to 24 hexadecimal characters.

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

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

SNMP User Table Settings

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

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

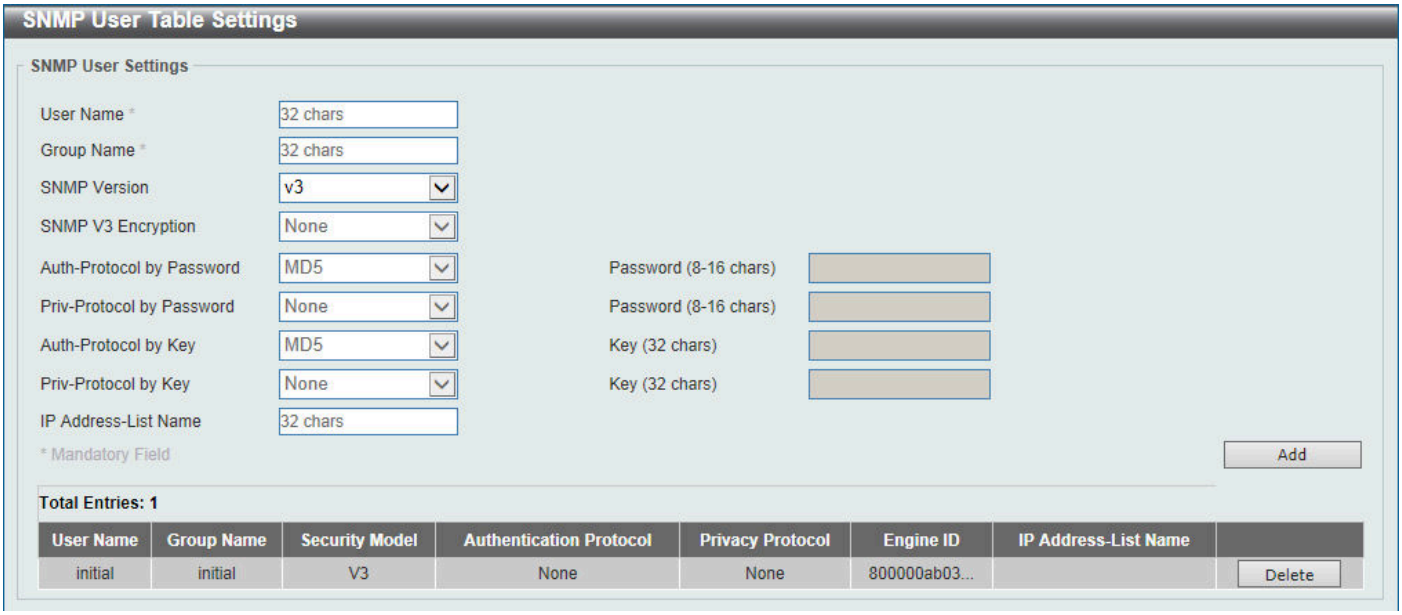


Figure 4-13 SNMP User Table Settings Window

The fields that can be configured are described below:

Parameter	Description
User Name	Enter SNMP user name here. This name can be up to 32 characters long. This is used to identify the SNMP user.

Parameter	Description
Group Name	Enter the SNMP group name to which the user belongs. This name can be up to 32 characters long. Spaces are not allowed.
SNMP Version	Select the SNMP version. Options to choose from are **v1, v2c**, and **v3**.
SNMP V3 Encryption	When selecting **v3** in the **SNMP Version** drop-down list, this option is available. Options to choose from are **None, Password**, and **Key**.
Auth-Protocol by Password	When selecting **v3** in the **SNMP Version** drop-down list, and selecting **Password** in the SNMP V3 Encryption drop-down list, this option is available. Select the authentication level. Options to choose from are the following: • **MD5** - Select to use the HMAC-MD5-96 authentication level. This field will require the user to enter a password or key. • **SHA** - Specify that the HMAC-SHA authentication protocol will be used. This field will require the user to enter a password or key.
Password	Enter the **Auth-Protocol** password here. For **MD5** this password must be between 8 and 16 characters long. For **SHA** this password must be between 8 and 20 characters long.
Priv-Protocol by Password	When selecting **v3** in the **SNMP Version** drop-down list, and selecting **Password** in the SNMP V3 Encryption drop-down list, this option is available. Select the private protocol. Options to choose from are the following: • **None** - Specify that no authorization protocol is in use. • **DES56** - Specify that DES 56-bit encryption is in use, based on the CBC-DES (DES-56) standard. This field will require the user to enter a password or a key. • **AES128** - Specify that Advanced Encryption Standard (AES) encryption is in use. This field will require the user to enter a password or a key.
Password	Enter the **Priv-Protocol** password here. For **none**, this field will be disabled. For **DES56** and **AES128** this password must be between 8 and 16 characters long.
Auth-Protocol by Key	When selecting **v3** in the **SNMP Version** drop-down list, and selecting **Key** in the SNMP V3 Encryption drop-down list, this option is available. Select the authentication level. Options to choose from are the following: • **MD5** - Select to use the HMAC-MD5 authentication level. This field will require the user to enter a password or a key. • **SHA** - Specify that the HMAC-SHA authentication protocol will be used. This field will require the user to enter a password or a key.
Key	Enter the **Auth-Protocol** key here. For **MD5** this key must be 32 characters long. For **SHA** this key must be 40 characters long.
Priv-Protocol by Key	When selecting **v3** in the **SNMP Version** drop-down list, and selecting **Key** in the SNMP V3 Encryption drop-down list, this option is available. Select the private protocol. Options to choose from are the following: • **None** - Specify that no authorization protocol is in use. • **DES56** - Specify that DES 56-bit encryption is in use, based on the CBC-DES (DES-56) standard. This field will require the user to enter a password or a key. • **AES128** - Specify that AES encryption is in use. This field will require the user to enter a password or a key.
Key	Enter the **Priv-Protocol** key here. For **none**, this field will be disabled. For **DES56** and **AES128** this key must be 32 characters long.
IP Address-List Name	Enter the standard IP access control list (ACL) to associate with the user. **Refer to ACL > ACL Access List**.

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

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

SNMP Host Table Settings

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

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

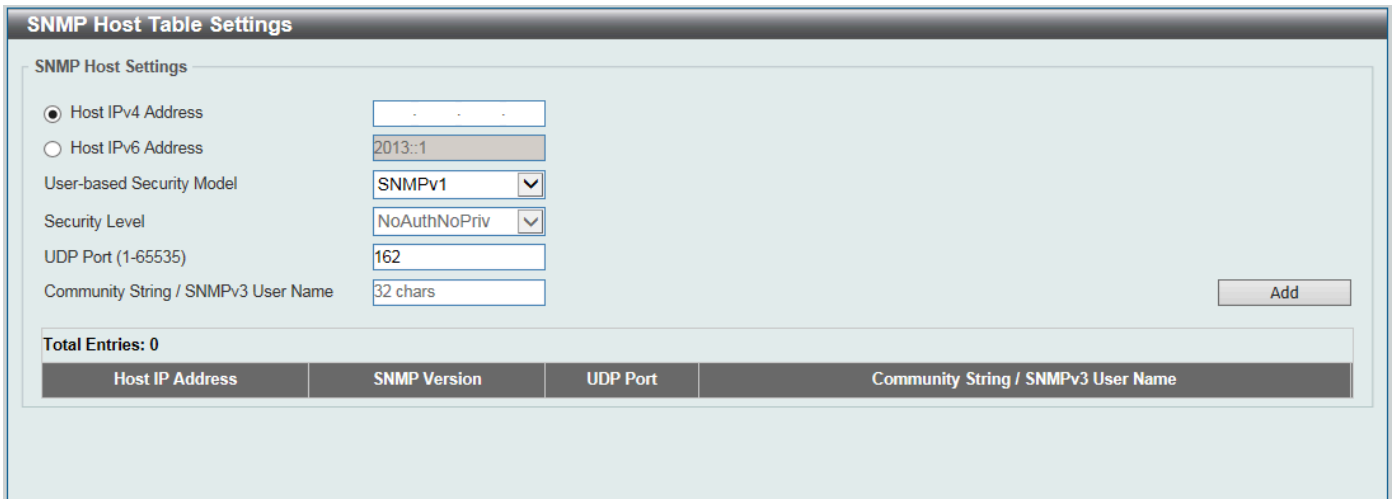


Figure 4-14 SNMP Host Table Settings Window

The fields that can be configured are described below:

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

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

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

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

RMON

RMON Global Settings

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

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

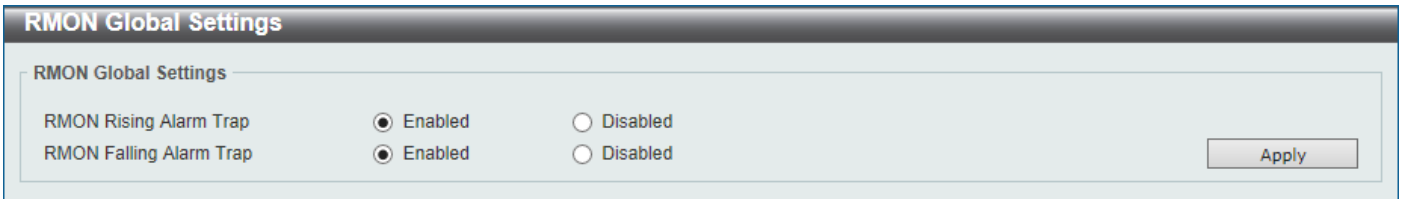


Figure 4-15 RMON Global Settings Window

The fields that can be configured are described below:

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

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

RMON Statistics Settings

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

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

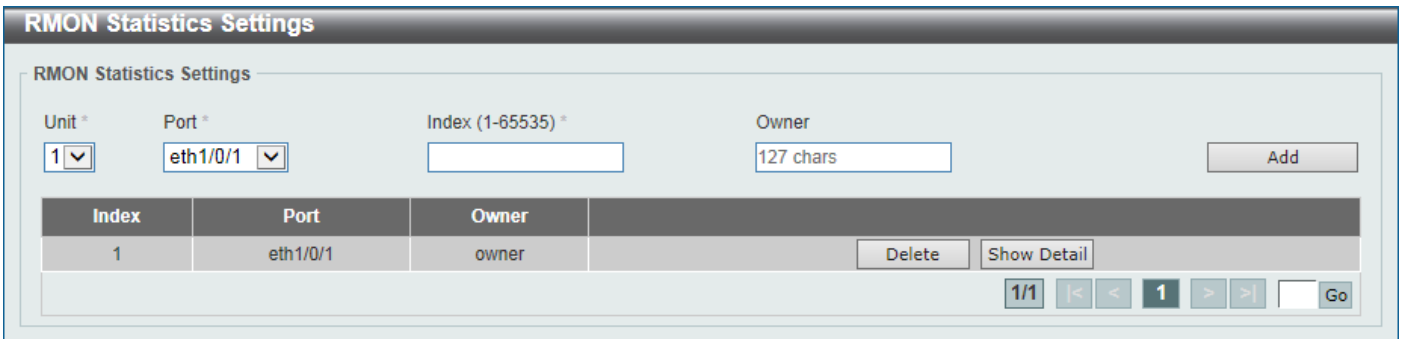


Figure 4-16 RMON Statistics Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
Port	Select to choose the port.
Index	Enter the RMON table index. The value is from 1 to 65535.
Owner	Enter the owner string. The string can be up to 127 characters.

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

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

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

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

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

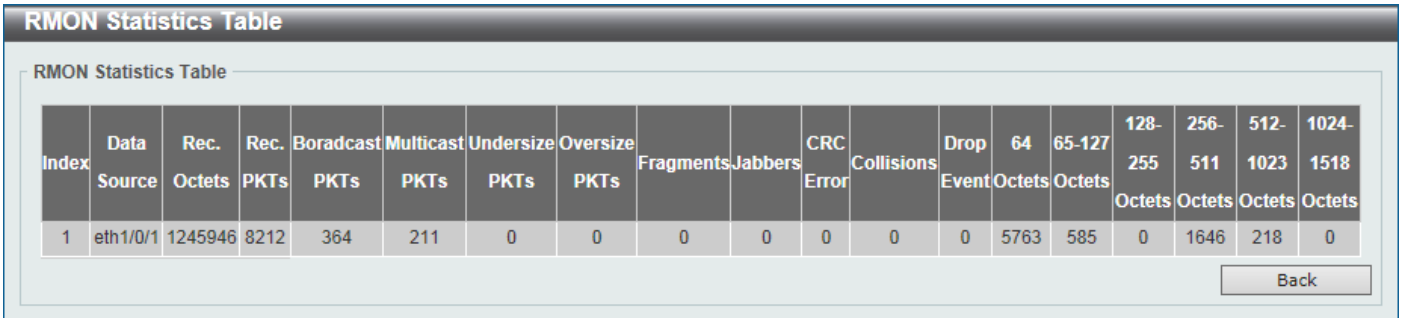


Figure 4-17 RMON Statistics Settings (Show Detail) Window

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

RMON History Settings

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

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

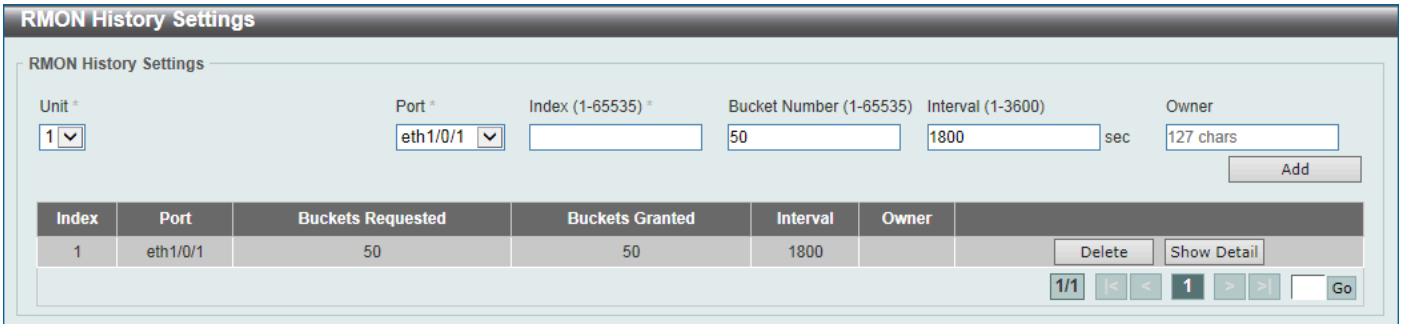


Figure 4-18 RMON History Settings Window

The fields that can be configured are described below:

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

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

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

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

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

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

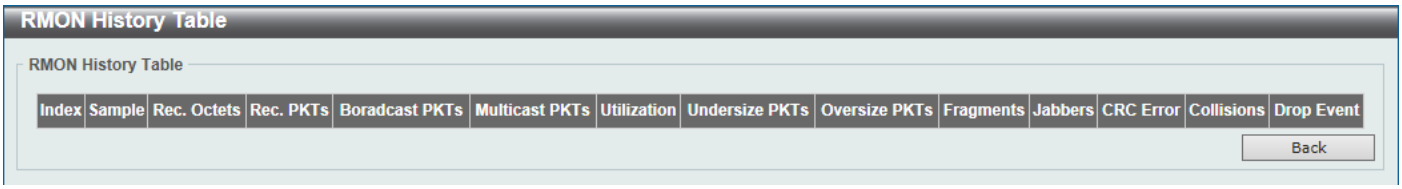


Figure 4-19 RMON History Settings (Show Detail) Window

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

RMON Alarm Settings

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

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

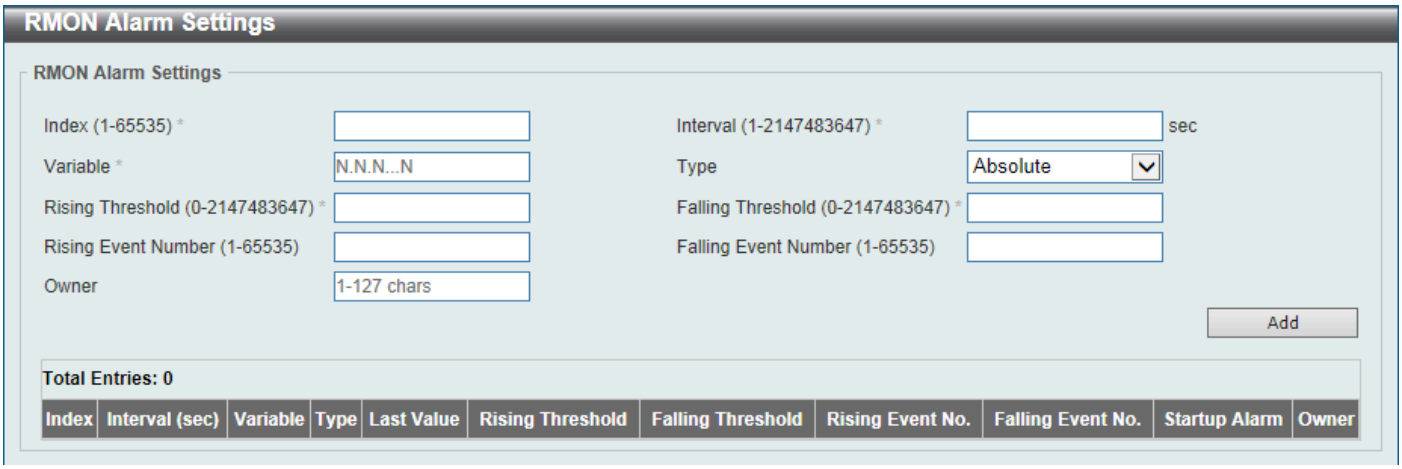


Figure 4-20 RMON Alarm Settings Window

The fields that can be configured are described below:

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

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

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

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

RMON Event Settings

This window is used to display and configure event entries.

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

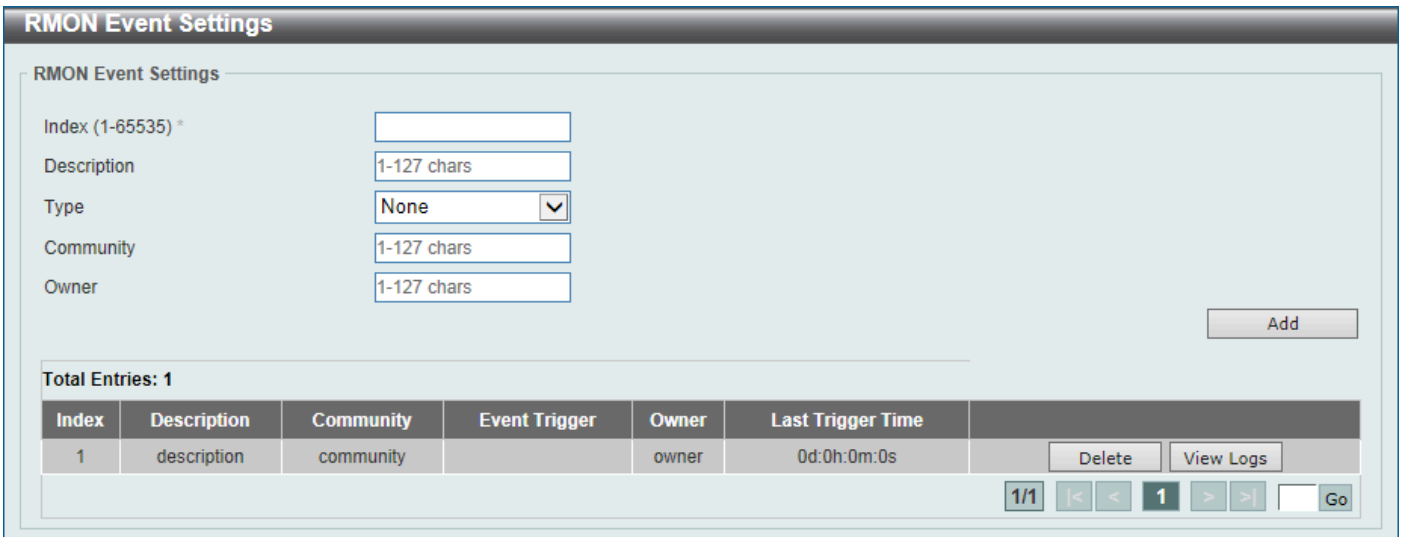


Figure 4-21 RMON Event Settings Window

The fields that can be configured are described below:

Parameter	Description
Index	Enter the index value of the alarm entry here. The range is from 1 to 65535.

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

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

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

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

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

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



Figure 4-22 RMON Event Settings (View Logs) Window

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

Telnet/Web

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

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

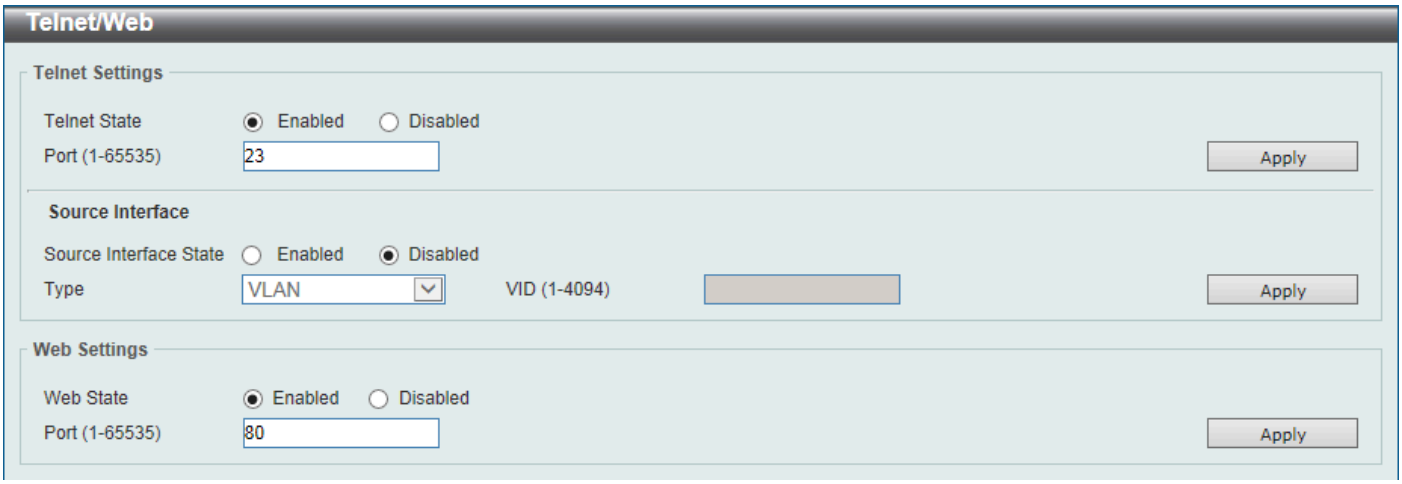


Figure 4-23 Telnet/Web Window

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

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

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

The fields that can be configured in **Source Interface** are described below:

Parameter	Description
Source Interface State	Select to enable or disable the source interface's state here.
Type	Select the type of source interface that will be used here. Options to choose from are Loopback, Mgmt, and VLAN.
VID	Enter the interface ID here. For loopback interfaces the range is from 1 to 8. For the management (Mgmt) interface this value can only be 0. For VLAN interfaces the range is from 1 to 4094.

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

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

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

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

Session Timeout

This window is used to display and configure the session timeout settings.

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

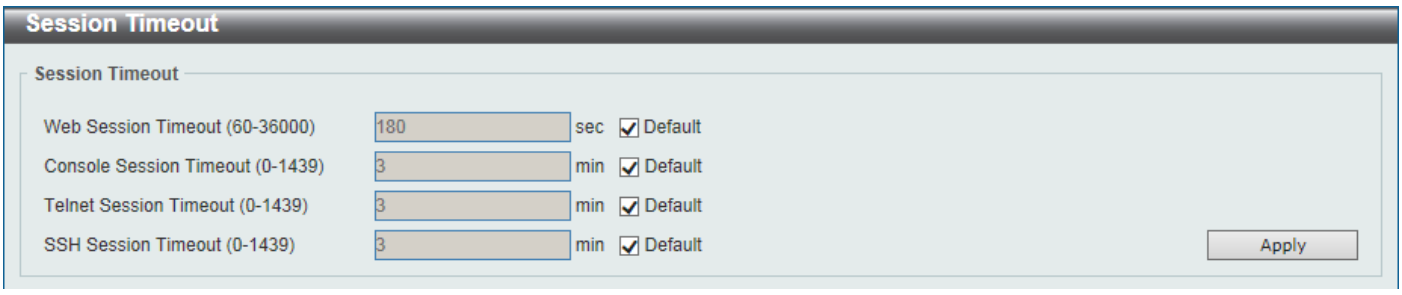


Figure 4-24 Session Timeout Window

The fields that can be configured are described below:

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.

Parameter	Description
Console Session Timeout	Enter the time in minutes of the web 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.

DHCP

Service DHCP

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

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



Figure 4-25 Service DHCP Window

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

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

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

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

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

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

DHCP Class Settings

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

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

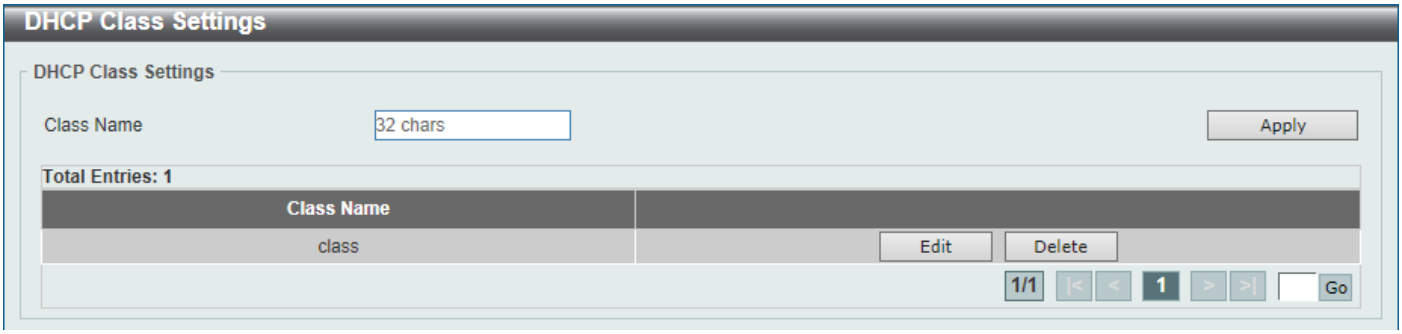


Figure 4-26 DHCP Class Settings Window

The fields that can be configured are described below:

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

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

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

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

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

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

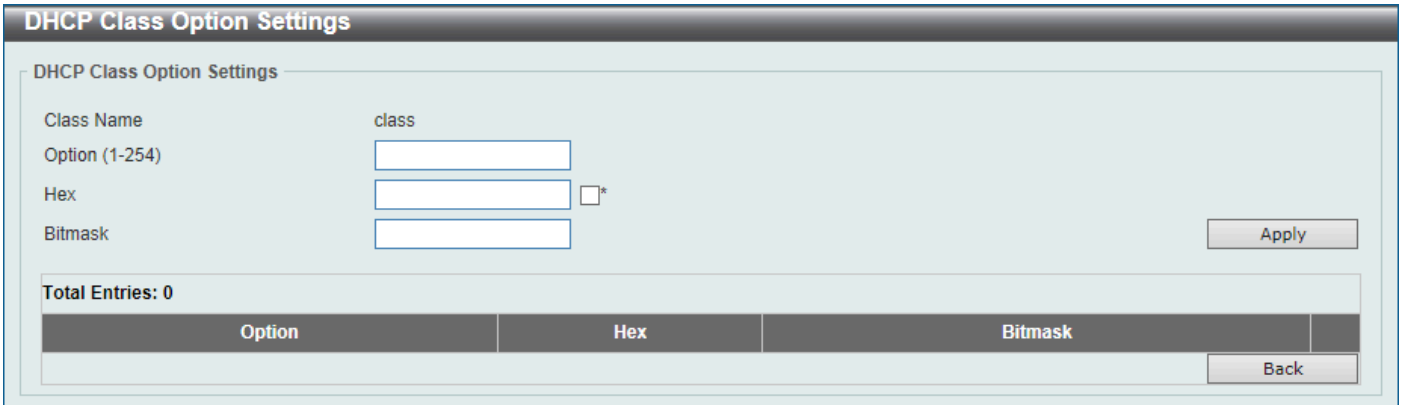


Figure 4-27 DHCP Class Settings (Edit) Window

The fields that can be configured are described below:

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

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

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

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

DHCP Server

The Dynamic Host Configuration Protocol (DHCP) allows the Switch to designate IP addresses, subnet masks, default gateways and other IP parameters to devices that request this information. This occurs when a DHCP enabled device is booted on or attached to the locally attached network. This device is known as the DHCP client and when enabled, it will emit query messages on the network before any IP parameters are set. When the DHCP server receives this request, it will allocate an IP address to the client. The DHCP client may be then utilize the IP address allocated by the DHCP server as its local configuration.

The user can configure many DHCP related parameters that it will utilize on its locally attached network, to control and limit the IP settings of clients desiring an automatic IP configuration, such as the lease time of the allocated IP address, the range of IP addresses that will be allowed in its DHCP pool, the ability to exclude various IP addresses within the range so as not to make identical entries on its network, or to assign the IP address of an important device (such as a DNS server or the IP address of the default route) to another device on the network.

Users also have the ability to bind IP addresses within the DHCP pool to specific MAC addresses in order to assign the same IP addresses to important devices.

DHCP Server Global Settings

This window is used to display and configure the global DHCP server parameters.

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

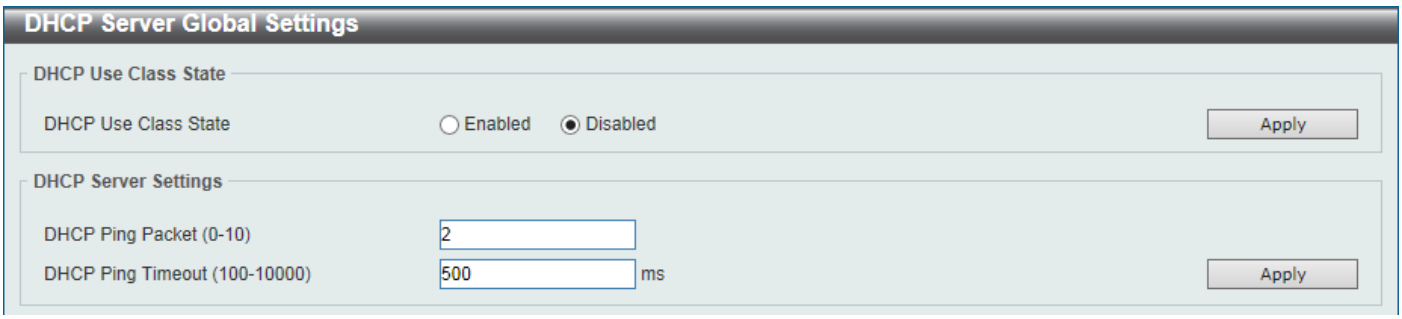


Figure 4-28 DHCP Server Global Settings Window

The fields that can be configured in **DHCP Use Class State** are described below:

Parameter	Description
DHCP Use Class State	Select to enable or disable the DHCP Use Class State here. When enabled, the DHCP server will use DHCP classes for address allocation.

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

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

Parameter	Description
DHCP Ping Packet	Enter the number of ping packets that the Switch will send out on the network containing the IP address to be allotted. If the ping request is not returned, the IP address is considered unique to the local network and then allotted to the requesting client. A value of 0 means there is no ping test. The range is from 0 to 10. The default value is 2.
DHCP Ping Timeout	Enter the amount of time the DHCP server must wait before timing out a ping packet. The range is from 100 to 10000 milliseconds. The default value is 500 milliseconds.

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

DHCP Server Pool Settings

This window is used to display and configure the DHCP server pool settings.

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

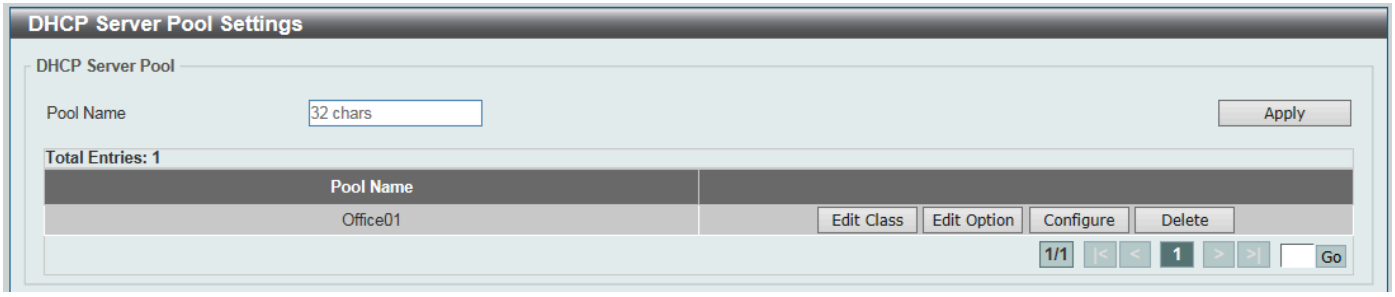


Figure 4-29 DHCP Server Pool Settings Window

The fields that can be configured are described below:

Parameter	Description
Pool Name	Enter the DHCP server pool name here. This name can be up to 32 characters long.

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

Click the **Edit Class** button to configure the DHCP class.

Click the **Edit Option** button to configure the DHCP server pool option settings.

Click the **Configure** button to configure the DHCP server pool settings.

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

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

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

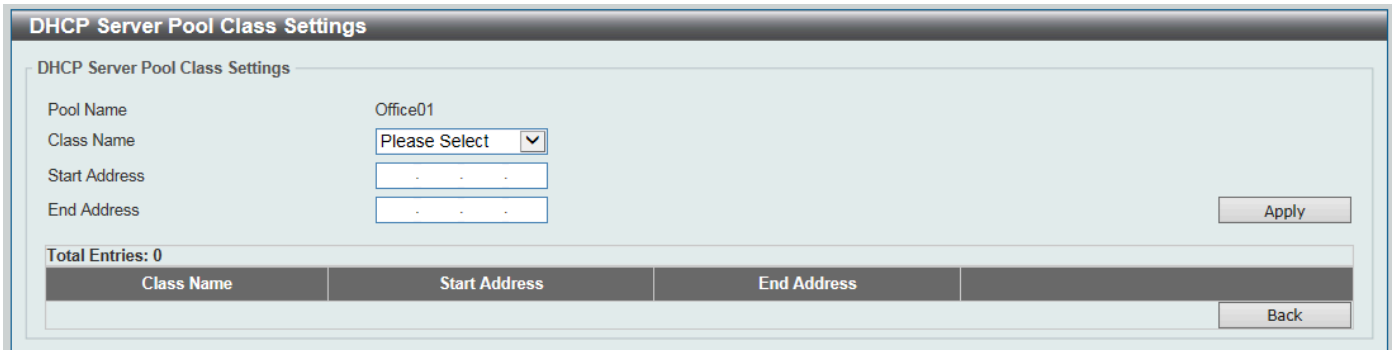


Figure 4-30 DHCP Server Pool Settings (Edit Class) Window

The fields that can be configured are described below:

Parameter	Description
Class Name	Select an existing DHCP class name here that will be associated with this DHCP pool.

Parameter	Description
Start Address	Enter the starting IPv4 address that will be associated with the DHCP class in the DHCP pool here.
End Address	Enter the ending IPv4 address that will be associated with the DHCP class in the DHCP pool here.

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

Click the **Delete by Name** button to remove the DHCP class association by name.

Click the **Delete by Address** button to remove the DHCP class association by address.

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

After clicking the **Edit Option** button, the following page will appear.



Figure 4-31 DHCP Server Pool Settings (Edit Option) Window

The fields that can be configured are described below:

Parameter	Description
Option	Enter the DHCP option number here. The range is from 1 to 254.
Type	Select the DHCP option type here. Options to choose from are **ASCII**, **HEX**, and **IP**. After selecting **ASCII**, enter the ASCII string in the space provided. This string can be up to 255 characters long. After selecting **HEX**, enter the hexadecimal string in the space provided. This string can be up to 254 characters long. Select the **None** option to specify a zero-length hexadecimal string. After selecting **IP**, enter the IPv4 address(es) in the space(s) provided. Up to 8 IPv4 address can be entered.

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

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

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

After clicking the **Configure** button, the following page will appear.

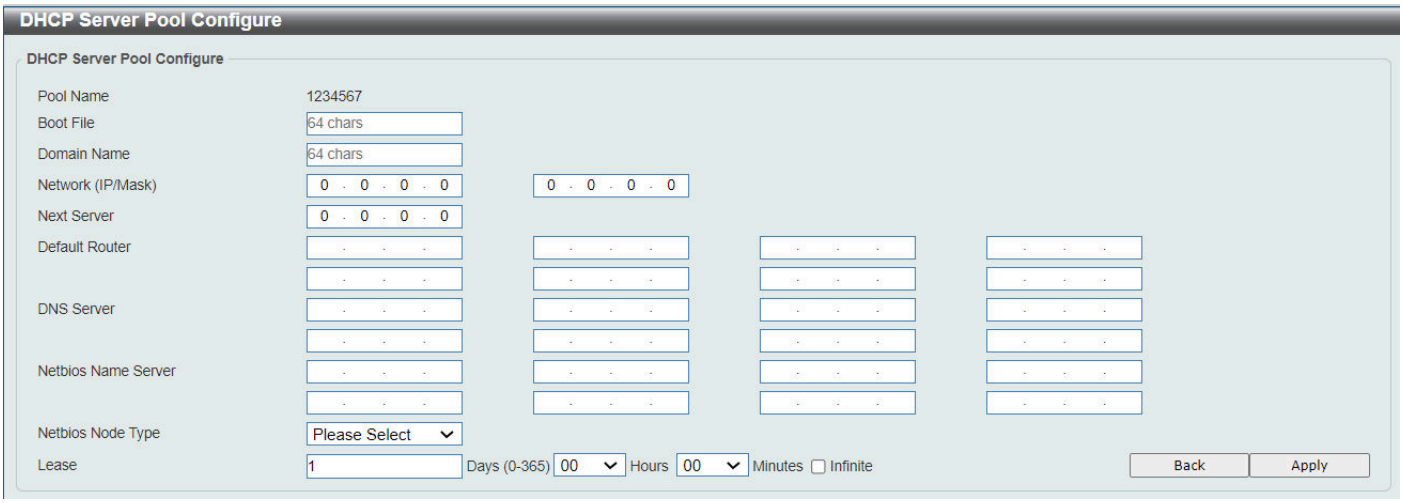


Figure 4-32 DHCP Server Pool Settings (Configure) Window

The fields that can be configured are described below:

Parameter	Description
Boot File	Enter the boot file name here. This can be up to 64 characters long.
Domain Name	Enter the domain name for the DHCP client here. This can be up to 64 characters long.
Network (IP/Mask)	Enter the network IPv4 address and subnet mask for the DHCP client here.
Next Server	Enter the next server IPv4 address here. The boot image file is stored on this server and can be retrieved by DHCP clients using this IP address. The server is typically a TFTP server. Only one next server IP address can be specified.
Default Router	Enter the IPv4 address of the default router for the DHCP client here. Up to 8 IPv4 address can be entered here. The IP address of the router should be on the same subnet as the client's subnet. Routers are listed in the order of preference. If default routers are already configured, the default routers configured later will be added to the default interface list.
DNS Server	Enter the IPv4 address to be used by the DHCP client as the DNS server here. Up to 8 IPv4 address can be entered here. Servers are listed in the order of preference. If DNS servers are already configured, the DNS servers configured later will be added to the DNS server list.
Netbios Name Server	Enter the WINS name server IPv4 address for the DHCP client here. Up to 8 IPv4 address can be entered here. Servers are listed in the order of preference. If name servers are already configured, the name server configured later will be added to the default interface list.
Netbios Node Type	Select the NetBIOS node type for Microsoft DHCP clients here. The node type determines the method that NetBIOS uses to register and resolve names. Options to choose from are **Broadcast, Peer To Peer, Mixed**, and **Hybrid**. A **Broadcast** system uses broadcasts. A Peer To Peer (p-node) system uses only point-to-point name queries to a name server (WINS). A **Mixed** (m-node) system broadcasts first, and then queries the name server. A **Hybrid** (h-node) system queries the name server first, and then broadcasts. The **Hybrid** type is recommended.
Lease	Enter and select the lease time for an IPv4 address that is assigned from the address pool here. Enter the **Days** in the range from 0 to 365. Select the **Hours** and **Minutes** from the drop-down menus. Alternatively, the **Infinite** option can be selected to specify that the lease time is unlimited.

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

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

DHCP Server Exclude Address

This window is used to view and exclude a range of IPv4 addresses from being allocated to the DHCP client. The DHCP server automatically allocates addresses in DHCP address pools to DHCP clients. All the addresses except the interface's IP address on the router and the excluded address (es) specified here are available for allocation. Multiple ranges of addresses can be excluded. To remove a range of excluded addresses, administrators must specify the exact range of addresses previously configured.

To view the following window, click **Management > DHCP > DHCP Server > DHCP Server Exclude Address**, as shown below:



Figure 4-33 DHCP Server Exclude Address Window

The fields that can be configured are described below:

Parameter	Description
Begin Address	Enter the first IPv4 address of a range of addresses to be excluded here.
End Address	Enter the last IPv4 address of a range of addresses to be excluded here.

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

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

DHCP Server Manual Binding

This window is used to display and configure the DHCP server manual binding settings. With a manual binding entry, the IP address can be either be bound with a client-identifier or bound with the hardware address of the host.

To view the following window, click **Management > DHCP > DHCP Server > DHCP Server Manual Binding**, as shown below:

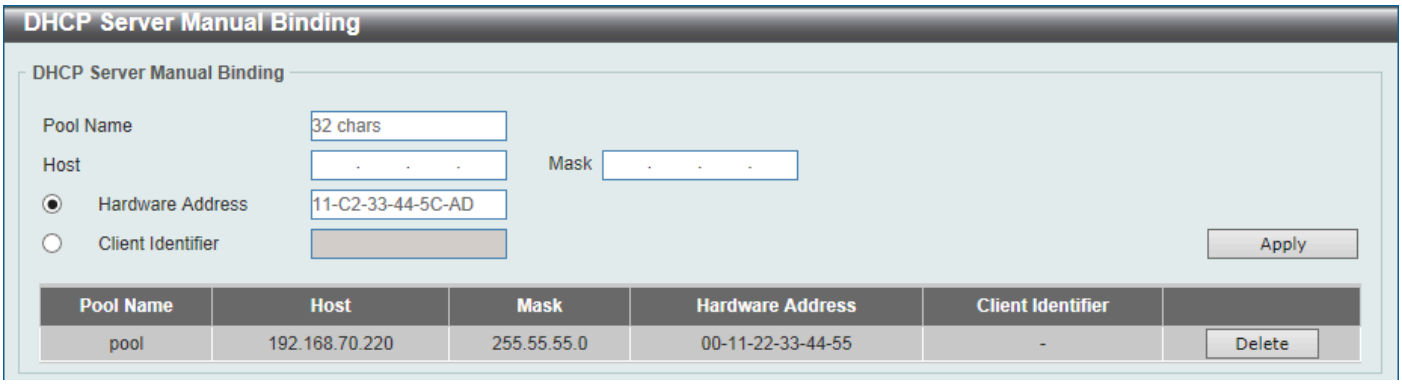


Figure 4-34 DHCP Server Manual Binding Window

The fields that can be configured are described below:

Parameter	Description
Pool Name	Enter the DHCP server pool name here. This name can be up to 32 characters long.
Host	Enter the DHCP host IPv4 address here.
Mask	Enter the DHCP host network subnet mask here.
Hardware Address	Enter the DHCP host MAC address here.
Client Identifier	Enter the DHCP host identifier in hexadecimal notation here. The client identifier is formatted by the media type and the MAC address.

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

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

DHCP Server Manual Binding Ext

This window is used to display and configure the DHCP server manual binding settings. With a manual binding entry, the IP address can be either be bound with a client-identifier or bound with the hardware address of the host.

To view the following window, click **Management > DHCP > DHCP Server > DHCP Server Manual Binding Ext**, as shown below:

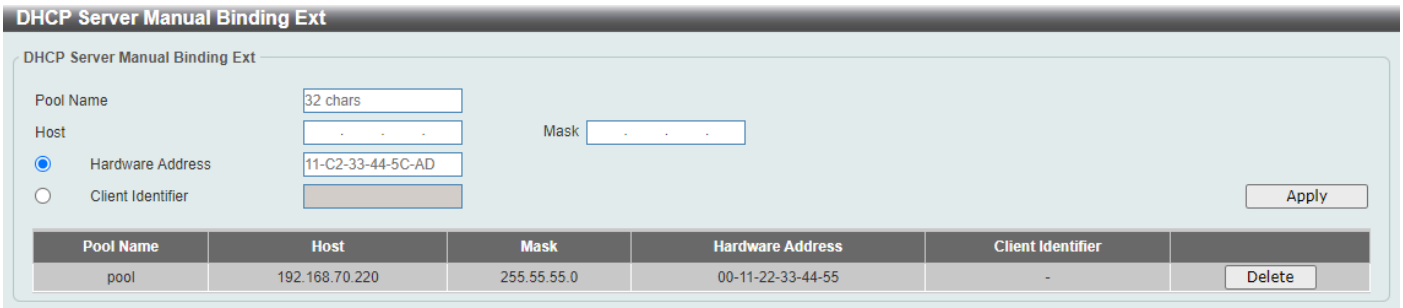


Figure 4-35 DHCP Server Manual Binding Window

The fields that can be configured are described below:

Parameter	Description
Pool Name	Enter the DHCP server pool name here. This name can be up to 32 characters long.
Host	Enter the DHCP host IPv4 address here.
Mask	Enter the DHCP host network subnet mask here.
Hardware Address	Enter the DHCP host MAC address here.
Client Identifier	Enter the DHCP host identifier in hexadecimal notation here. The client identifier is formatted by the media type and the MAC address.

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

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

DHCP Server Dynamic Binding

This window is used to view and clear the DHCP server dynamic binding entries.

To view the following window, click **Management > DHCP > DHCP Server > DHCP Server Dynamic Binding**, as shown below:

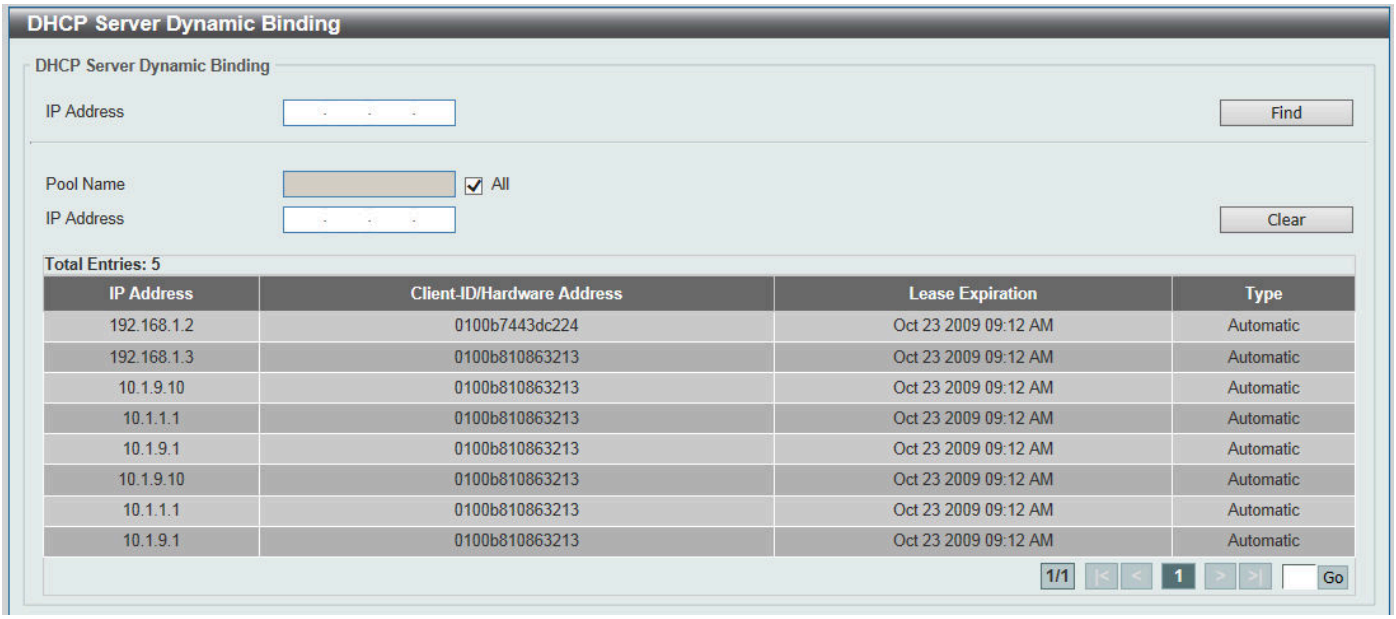


Figure 4-36 DHCP Server Dynamic Binding Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the binding entry IPv4 address here.
Pool Name	Enter the DHCP server pool name here. This name can be up to 32 characters long. Select the **All** option to clear the binding entries for all pools.

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

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

DHCP Server IP Conflict

This window is used to view and clear the DHCP conflict entries from the DHCP server database.

To view the following window, click **Management > DHCP > DHCP Server > DHCP Server IP Conflict**, as shown below:

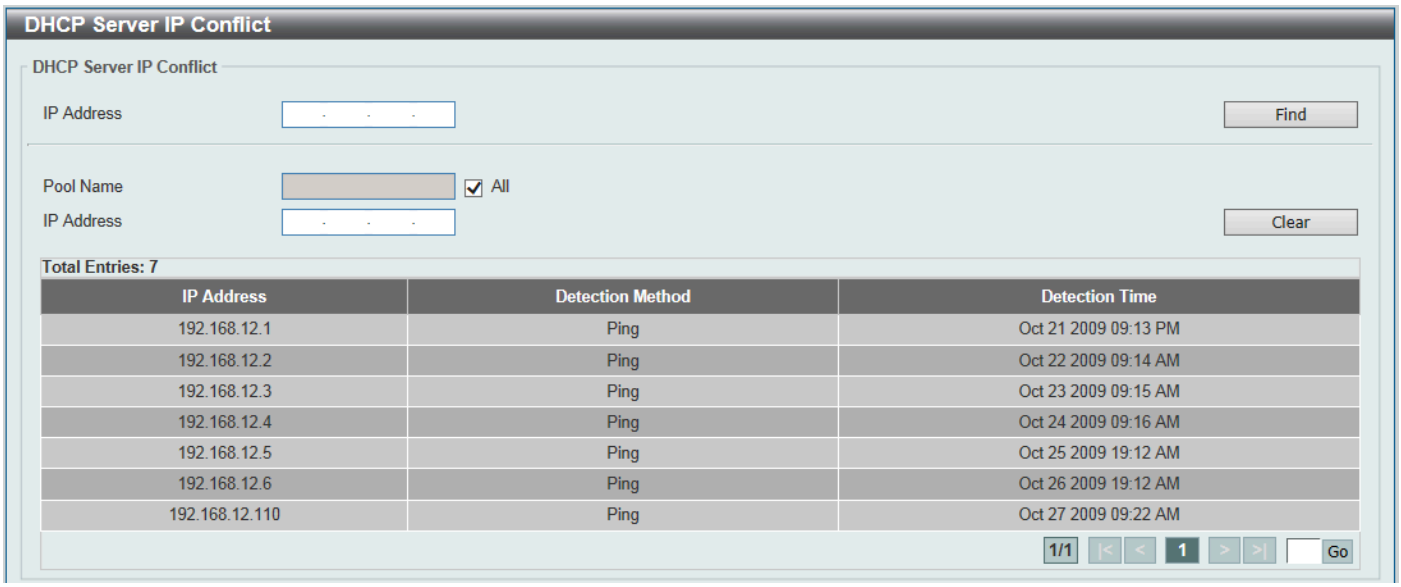


Figure 4-37 DHCP Server IP Conflict Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the IPv4 address of the conflict entry to be located or cleared.
Pool Name	Enter the DHCP server pool name here. This name can be up to 32 characters long. Select the **All** option to clear the conflict entries for all pools.

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

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

DHCP Server Statistic

This window is used to display DHCP server statistic information.

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

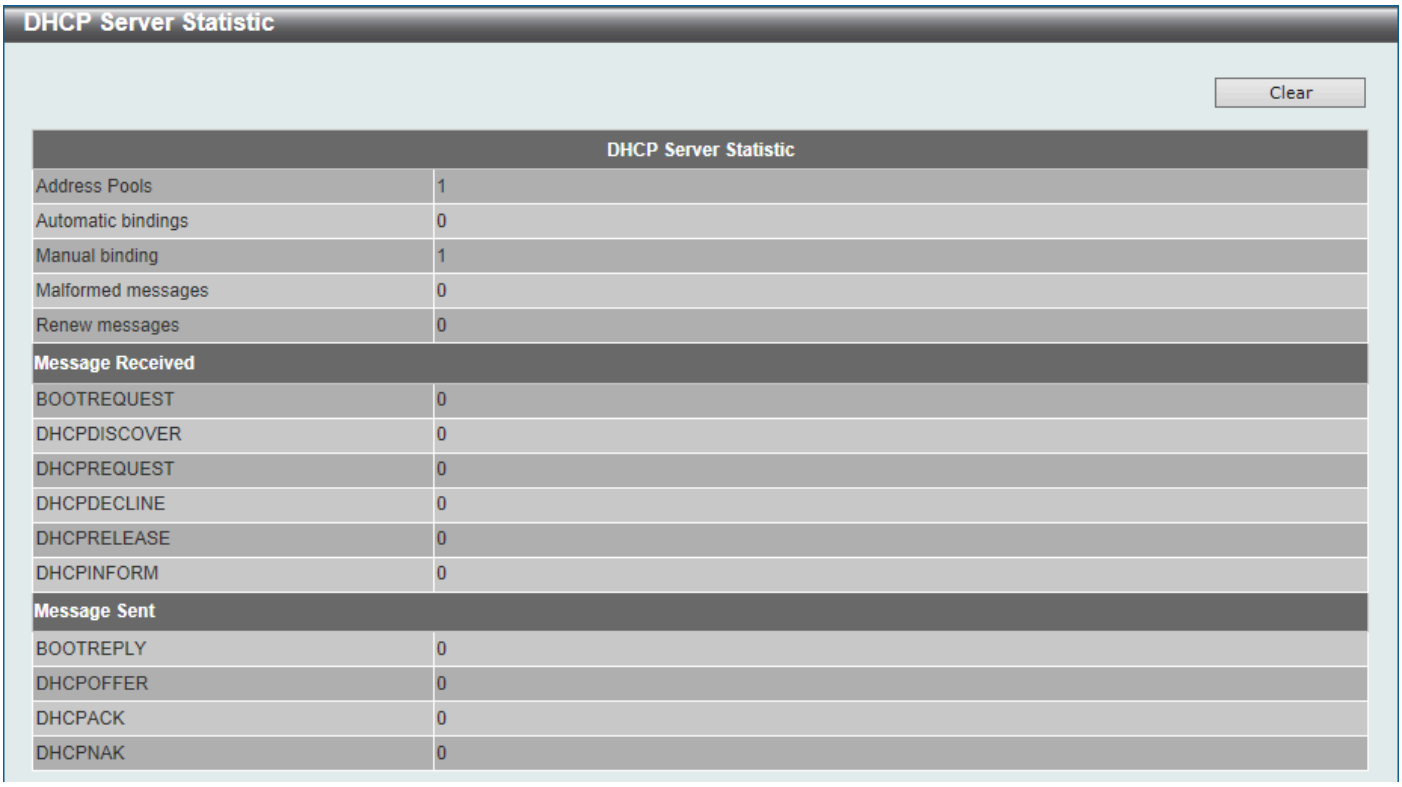


Figure 4-38 DHCP Server Statistic Window

Click the **Clear** button to clear the statistics information displayed here.

DHCPv6 Server

DHCPv6 Server Pool Settings

This window is used to display and configure the DHCPv6 server pool settings.

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

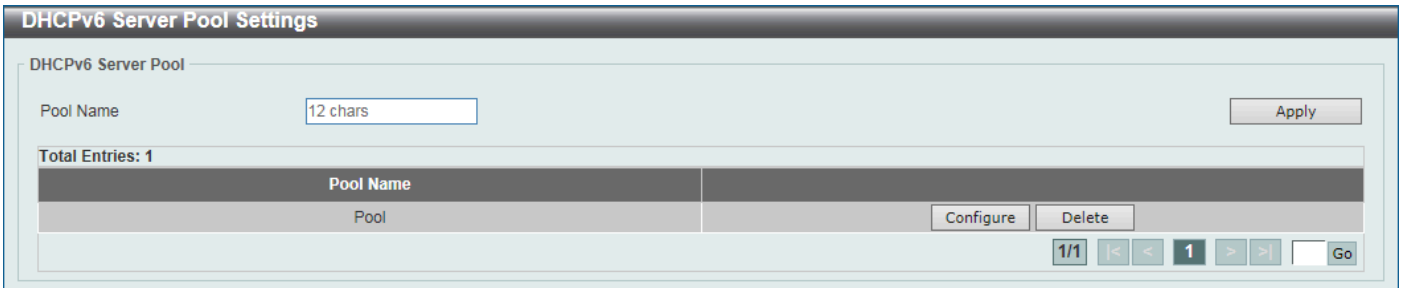


Figure 4-39 DHCPv6 Server Pool Settings Window

The fields that can be configured are described below:

Parameter	Description
Pool Name	Enter the DHCPv6 server pool name here. This name can be up to 12 characters long.

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

Click the **Configure** button to configure the DHCPv6 server pool settings.

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

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

After clicking the **Configure** button, the following page will appear.

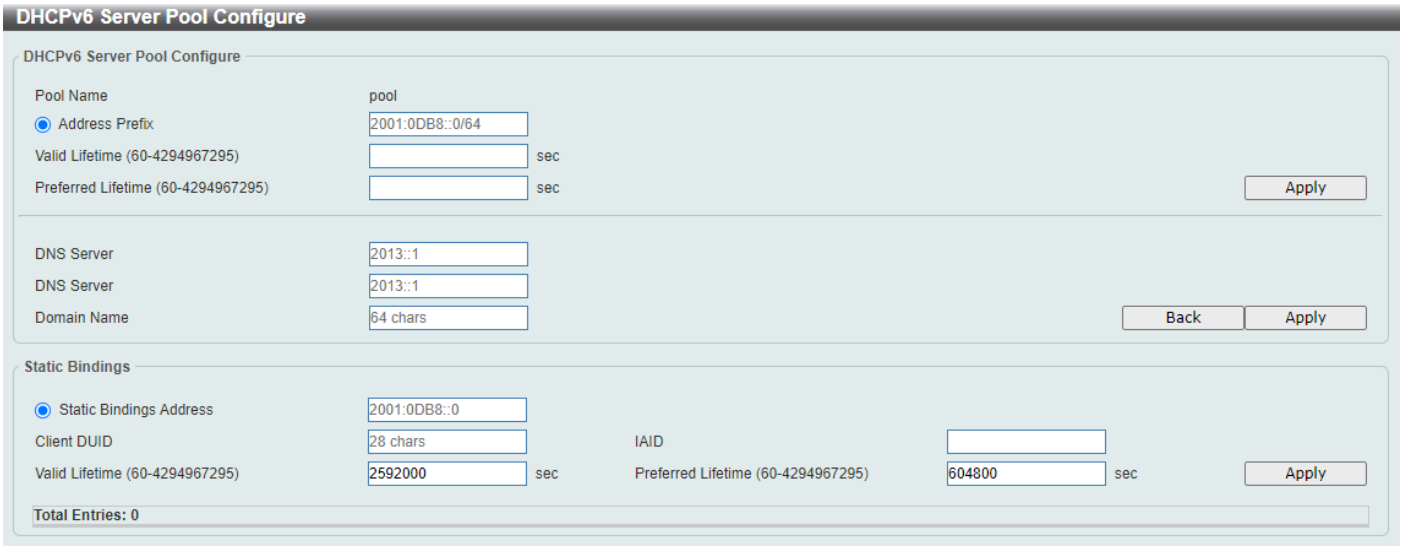


Figure 4-40 DHCPv6 Server Pool Settings (Configure) Window

The fields that can be configured in **DHCPv6 Server Pool Configure** are described below:

Parameter	Description
Address Prefix	Select and enter the DHCPv6 server pool IPv6 network address and prefix length here. For example, 2015::0/64.
Valid Lifetime	Enter the valid lifetime value here. The range is from 60 to 4294967295 seconds. The valid lifetime should be greater than preferred lifetime. If this value is not specified, then the default valid lifetime will be 2592000 seconds (30 days).
Preferred Lifetime	Enter the preferred lifetime value here. The range is from 60 to 4294967295 seconds. If this value is not specified, then the default preferred lifetime will be 604800 seconds (7 days).
DNS Server	Enter the DNS server IPv6 address to be assigned to requesting DHCPv6 clients here.
Domain Name	Enter the domain name to be assigned to requesting DHCPv6 clients here.

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

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

The fields that can be configured in **Static Bindings** are described below:

Parameter	Description
Static Bindings Address	Enter the static binding IPv6 address assign to the specific client here.
Client DUID	Enter the client DHCP Unique Identifier (DUID) here. This string can be up to 28 characters long.
IAID	Enter the Identity Association Identifier (IAID) here. The IAID here uniquely identifies a collection of non-temporary addresses (IANA) assigned on the client.
Valid Lifetime	Enter the valid lifetime value here. The valid lifetime should be greater than the preferred lifetime. The range is from 60 to 4294967295 seconds. By default, this value is 2592000 seconds (30 days).
Preferred Lifetime	Enter the preferred lifetime value here. The range is from 60 to 4294967295 seconds. By default, this value is 604800 seconds (7 days).

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

DHCPv6 Server Exclude Address

This window is used to specify IPv6 addresses that a DHCPv6 server should not assign to DHCPv6 clients. The DHCPv6 server assumes that all addresses (excluding the Switch's IPv6 address) can be assigned to clients. Use this window to exclude a single IPv6 address or a range of IPv6 addresses. The excluded addresses are only applied to the pool(s) for address assignment.

To view the following window, click **Management > DHCP > DHCPv6 Server > DHCPv6 Server Exclude Address**, as shown below:



Figure 4-41 DHCPv6 Server Exclude Address Window

The fields that can be configured are described below:

Parameter	Description
Low IPv6 Address	Enter the excluded IPv6 address or first IPv6 address in the excluded address range here.
High IPv6 Address	Enter the last IPv6 address in the excluded address range here (optional).

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

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

DHCPv6 Server Binding

This window is used to view and clear the DHCPv6 server binding entries.

To view the following window, click **Management > DHCP > DHCPv6 Server > DHCPv6 Server Binding**, as shown below:

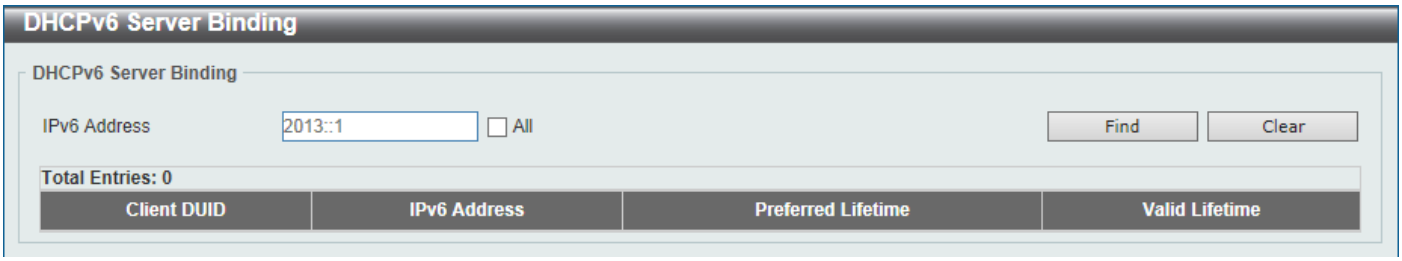


Figure 4-42 DHCPv6 Server Binding Window

The fields that can be configured are described below:

Parameter	Description
IPv6 Address	Enter the binding entry IPv6 address to be displayed or cleared here. Select the All option to display or clear all DHCPv6 client prefix bindings in or from the binding table.

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

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

DHCPv6 Server Interface Settings

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

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

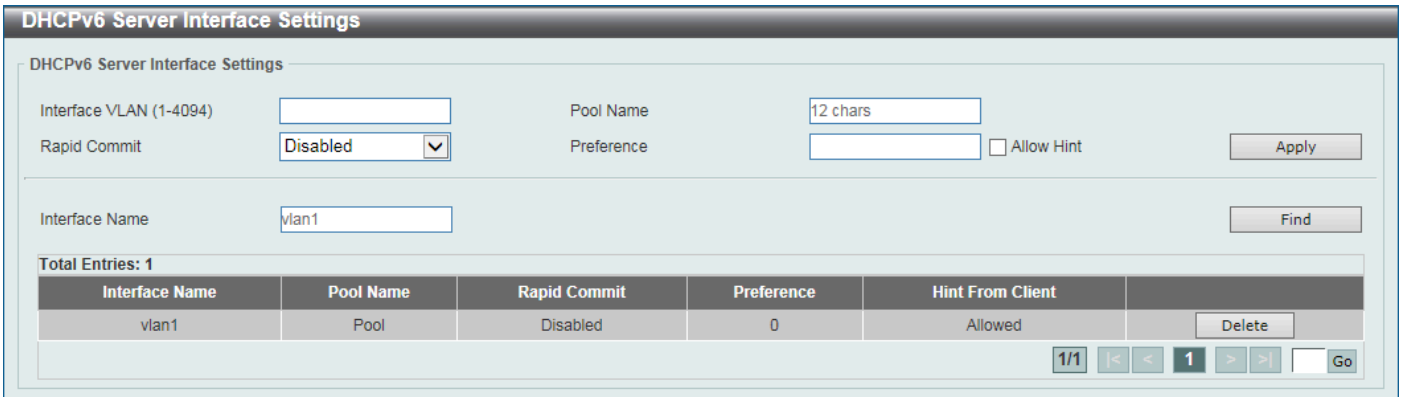


Figure 4-43 DHCPv6 Server Interface Settings Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the interface VLAN ID here. The range is from 1 to 4094.
Pool Name	Enter the DHCPv6 server pool name here. This name can be up to 12 characters long.
Rapid Commit	Select to enable or disable two-message exchange here. By default, two-message exchange is not allowed.
Preference	Enter the preference value here.

Parameter	Description
Interface Name	Enter the interface name here.

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

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

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

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

DHCPv6 Server Operational Information

This window is used to display the DHCPv6 server pool information. Refer to **DHCPv6 Server Pool Settings** for more information.

To view the following window, click **Management > DHCP > DHCPv6 Server > DHCPv6 Server Operational Information**, as shown below:



Figure 4-44 DHCPv6 Server Operational Information Window

DHCP Relay

DHCP Relay Global Settings

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

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

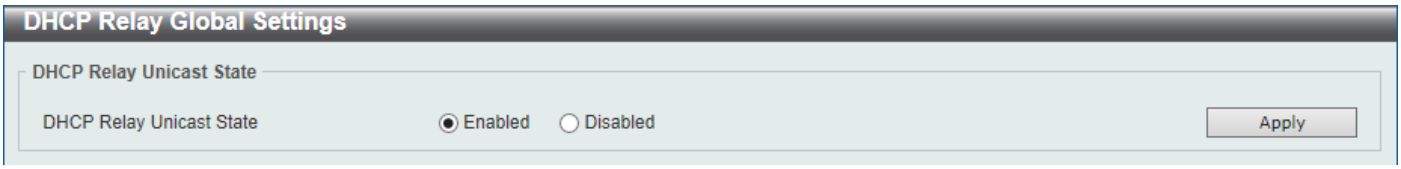


Figure 4-45 DHCP Relay Global Settings Window

The fields that can be configured are described below:

Parameter	Description
DHCP Relay Unicast State	Select to globally enable or disable the DHCP relay unicast state here.

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

DHCP Relay Pool Settings

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

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

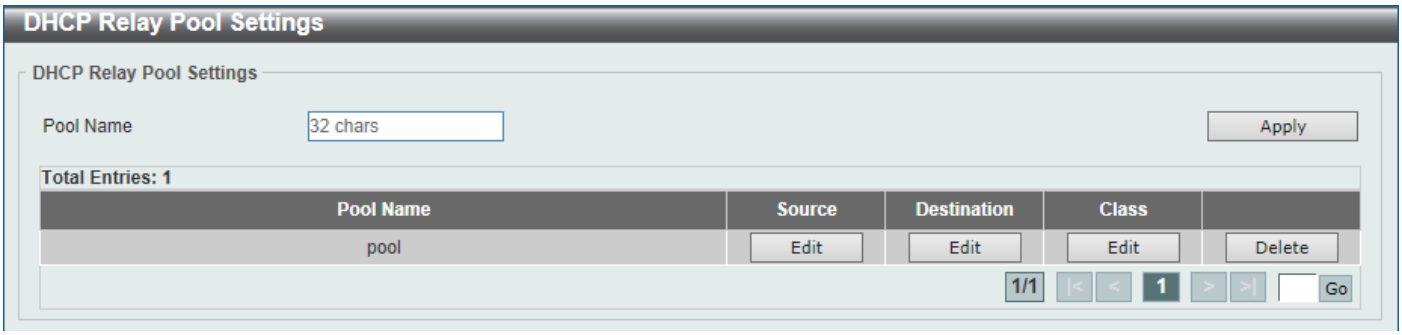


Figure 4-46 DHCP Relay Pool Settings Window

The fields that can be configured are described below:

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

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

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

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

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

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

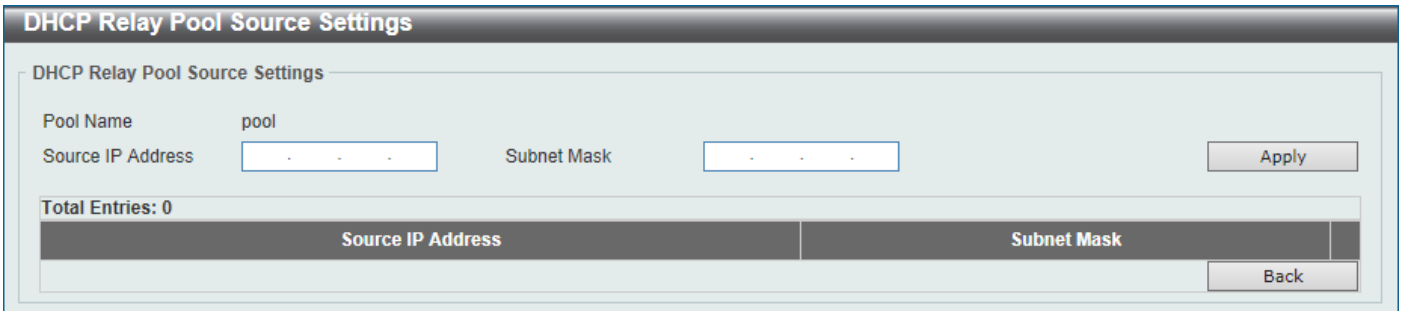


Figure 4-47 DHCP Relay Pool Settings (Source Edit) Window

The fields that can be configured are described below:

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

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

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

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

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

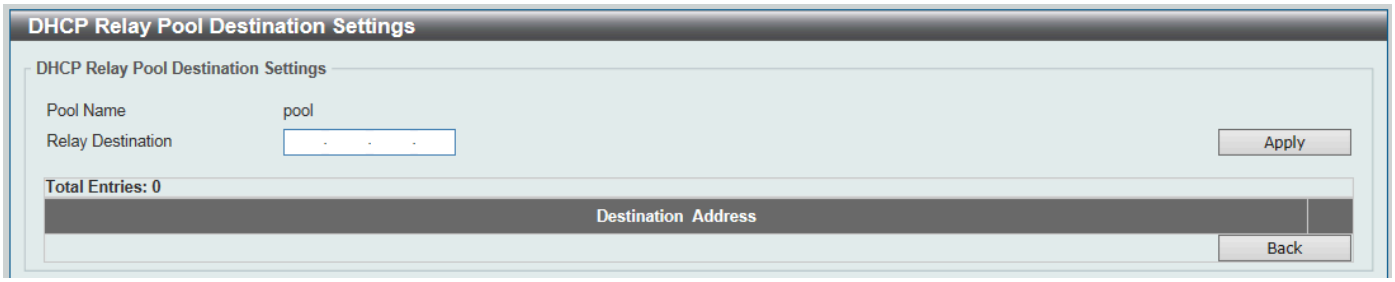


Figure 4-48 DHCP Relay Pool Settings (Destination Edit) Window

The fields that can be configured are described below:

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

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

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

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

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

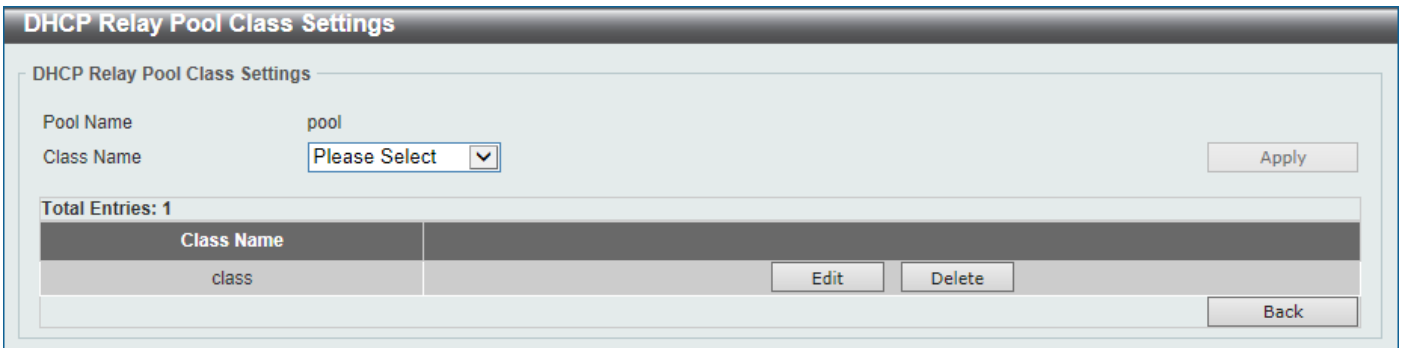


Figure 4-49 DHCP Relay Pool Settings (Class Edit) Window

To edit a class, select it then click **Apply** to display its information below.

The fields that can be configured are described below:

Parameter	Description
Class Name	Select the DHCP class name.

To edit a class, select it then click **Apply** to display its information below.

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

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

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

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

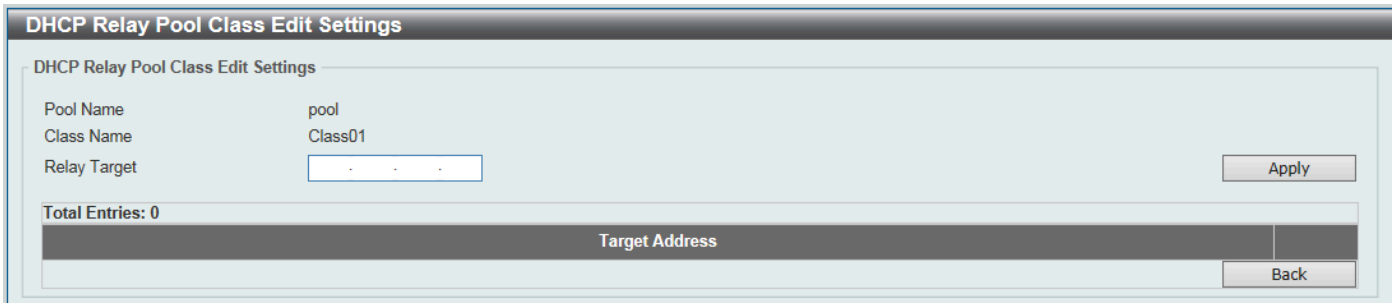


Figure 4-50 DHCP Relay Pool Settings (Class Edit, Edit) Window

The fields that can be configured are described below:

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

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

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

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

DHCP Relay Information Settings

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

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

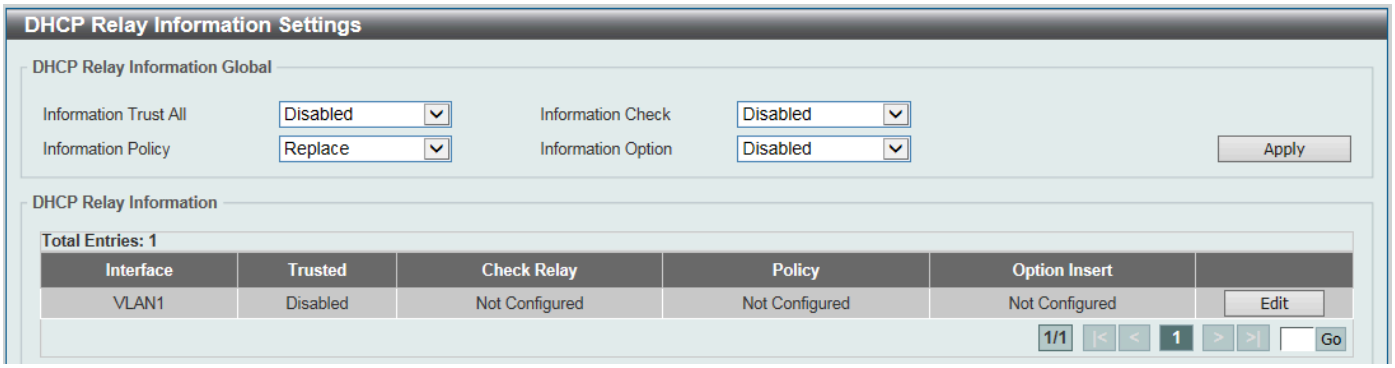


Figure 4-51 DHCP Relay Information Settings Window

The fields that can be configured are described below:

Parameter	Description
Information Trust All	Select this option to enable or disable the DHCP relay agent to trust the IP DHCP relay information for all interfaces.
information Check	Select this option to enable or disable the DHCP relay agent to validate and remove the relay agent information option in the received DHCP reply packet.
Information Policy	Select the Option 82 re-forwarding policy for the DHCP relay agent. Options to choose from are **Keep**, **Drop**, and **Replace**. • **Keep** - Select to keep the packet that already has the relay option. The packet is left unchanged and directly relayed to the DHCP server. • **Drop** - Select to discard the packet that already has the relay option.

Parameter	Description
	• **Replace** - Select to replace the packet that already has the relay option. The packet will be replaced with a new option.
Information Option	Select this option to enable or disable the insertion of relay agent information (Option 82) during the relay of DHCP request packets.

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

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

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

DHCP Relay Information Option Format Settings

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

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

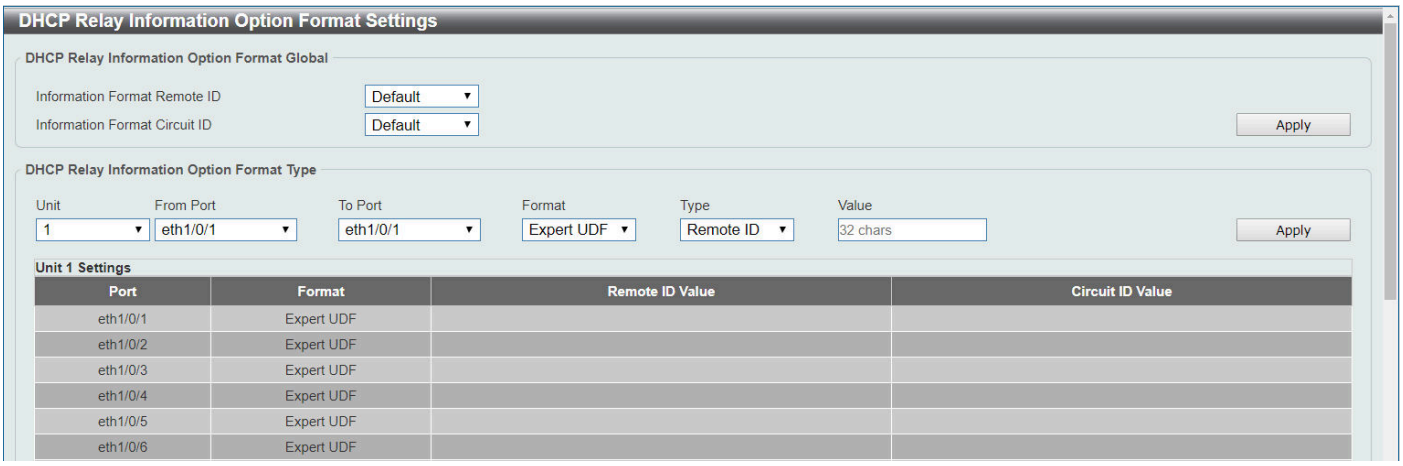


Figure 4-52 DHCP Relay Information Option Format Settings Window

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

Parameter	Description
Information Format Remote ID	Select the DHCP information remote ID sub-option. Options to choose from are: • **Default** - Select to use the Switch's system MAC address as the remote ID. • **User Define** - Select to use a user-defined remote ID. Enter the user-defined string with the maximum of 32 characters in the text box. • **Vendor2** - Select to use vendor 2 as the remote ID. • **Expert UDF** - Select to use the expert UDF remote ID. Select the stand-alone unit format after this selection here.
Information Format Circuit ID	Select the DHCP information circuit ID sub-option. Options to choose from are: • **Default** - Select to use the default circuit ID sub-option. • **User Define** - Select to use a user-defined circuit ID. Enter the user-defined string with the maximum of 32 characters in the text box. • **Vendor1** - Select to use vendor 1 as the circuit ID. • **Expert UDF** - Select to use the expert UDF circuit ID. Select the stand-alone unit format after this selection here.

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

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

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

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

DHCP Relay Information Profile Settings

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

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

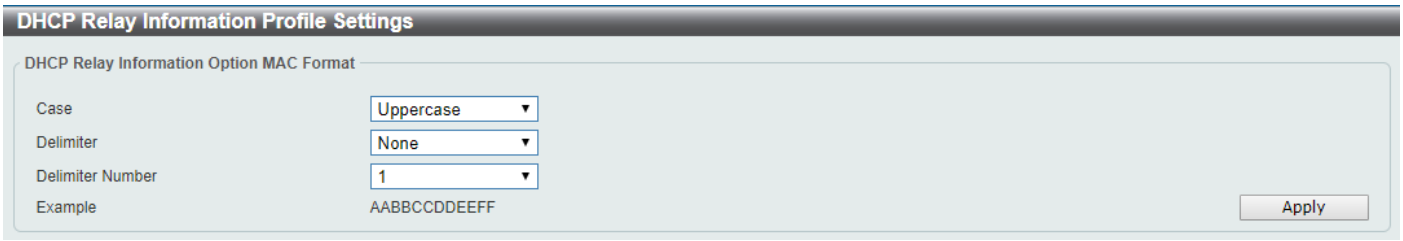


Figure 4-53 DHCP Relay Information Profile Settings Window

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

Parameter	Description
Case	Select the case that will be used here. Options to choose from are: • **Lowercase** - Specifies that when using the lowercase format, the Option 82 MAC address for the user-defined profile will be formatted as: aa-bb-cc-dd-ee-ff. • **Uppercase** - Specifies that when using the uppercase format, the Option 82 MAC address for the user-defined profile username will be formatted as: AA-BB-CC-DD-EE-FF.
Delimiter	Select the delimiter that will be used here. Options to choose from are: • **Hyphen** - Specifies that the format will be AA-BB-CC-DD-EE-FF. • **Colon** - Specifies that the format will be AA:BB:CC:DD:EE:FF. • **Dot** - Specifies that the format will be AA.BB.CC.DD.EE.FF. • **None** - Specifies that when not using any delimiter, the format will be AABBCCDDEEFF.
Delimiter Number	Select the delimiter number here. Options to choose from are: • **1** - Single delimiter, the format is: AABBCC.DDEEFF. • **2** - Double delimiters, the format is: AABB.CCDD.EEFF.

Parameter	Description
	• **5** - Multiple delimiters, the format is: AA.BB.CC.DD.EE.FF.

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

DHCP Relay Port Settings

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

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

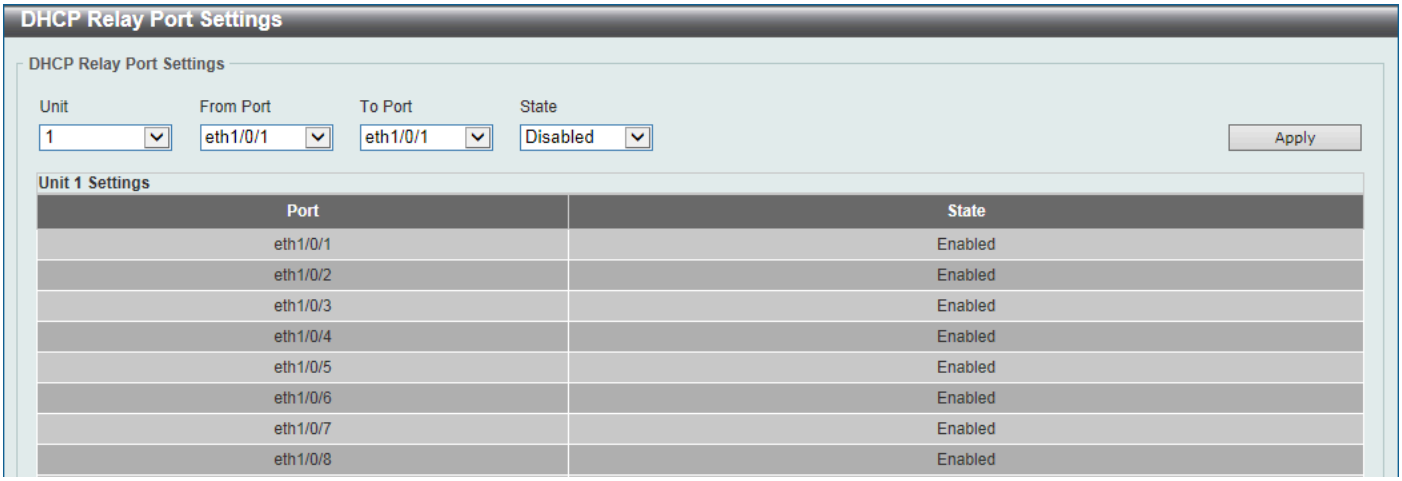


Figure 4-54 DHCP Relay Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration here.
State	Select to enable or disable the DHCP Relay feature on the specified port(s).

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

DHCP Local Relay VLAN

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

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

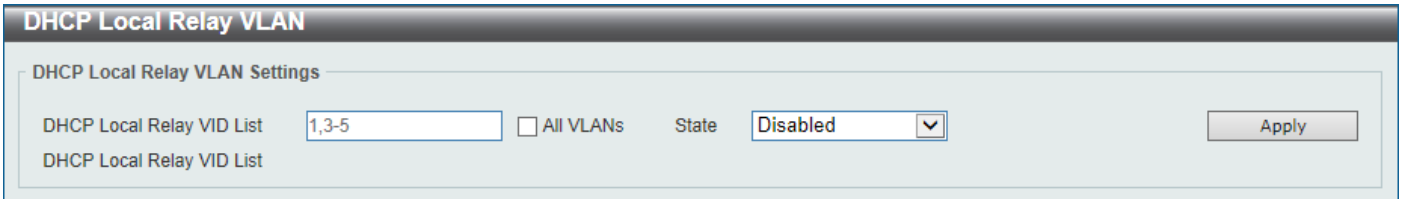


Figure 4-55 DHCP Local Relay VLAN Window

The fields that can be configured are described below:

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

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

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

DHCPv6 Relay

DHCPv6 Relay Global Settings

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

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

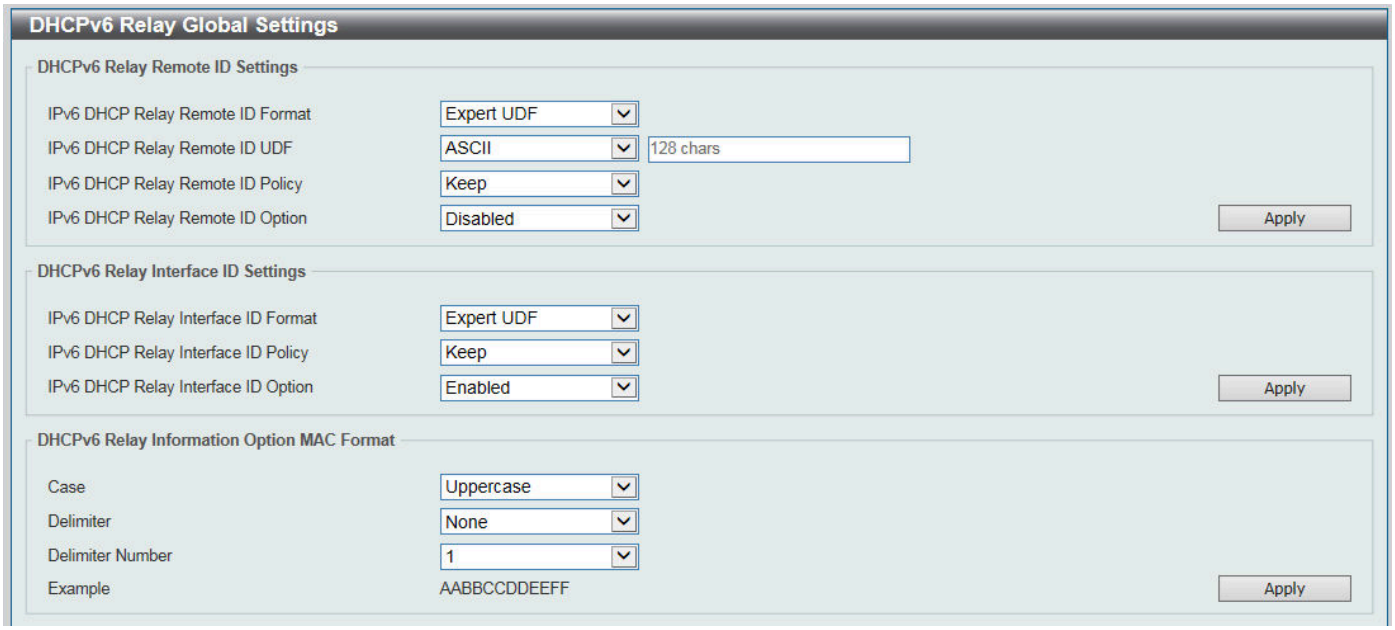


Figure 4-56 DHCPv6 Relay Global Settings Window

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

Parameter	Description
IPv6 DHCP Relay Remote ID Format	Select the IPv6 DHCP Relay remote ID format that will be used here. Options to choose from are **Default, CID with User Define,** and **User Define**.
IPv6 DHCP Relay Remote ID UDF	Select to choose the User Define Field (UDF) for remote ID. Options to choose from are **ASCII**, and **Hex**. • **ASCII** - Select to enter the ASCII string with a maximum of 128 characters in the text box.

Parameter	Description
	• **HEX** - Select to enter the hexadecimal string with a maximum of 256 characters in the text box.
IPv6 DHCP Relay Remote ID Policy	Select to choose Option 37 forwarding policy for the DHCPv6 relay agent. Options to choose from are **Keep**, and **Drop**. • **Keep** - Select that the DHCPv6 request packet that already has the relay agent Remote-ID option is left unchanged and directly relayed to the DHCPv6 server. • **Drop** - Select to discard the packet that already has the relay agent Remote-ID Option 37.
IPv6 DHCP Relay Remote ID Option	Select this option to enable or disable the insertion of the relay agent remote ID Option 37 during the relay of DHCP for IPv6 request packets.

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

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

Parameter	Description
IPv6 DHCP Relay Interface ID Format	Select the IPv6 DHCP relay interface ID format that will be used here. Options to choose from are **Default, CID,** and **Vendor1**.
IPv6 DHCP Relay Interface ID Policy	Select the Option 18 re-forwarding policy for the DHCPv6 relay agent here. Options to choose from are: • **Keep** - Specifies that the DHCPv6 request packets that already contain the relay agent interface ID option are left unchanged and directly relay to the DHCPv6 server. • **Drop** - Specifies to discard the packets that already contain the relay agent interface ID Option 18.
IPv6 DHCP Relay Interface ID Option	Select to enable or disable the insertion of the relay agent interface ID Option 18 during the relay of DHCP for IPv6 request packets.

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

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

Parameter	Description
Case	Select the case that will be used here. Options to choose from are: • **Lowercase** - Specifies that the MAC format will be lowercase. For example: aa-bb-cc-dd-ee-ff. • **Uppercase** - Specifies that the MAC format will be uppercase. For example: AA-BB-CC-DD-EE-FF.
Delimiter	Select the delimiter that will be used here. Options to choose from are: • **Hyphen** - Specifies that the MAC address format will contain hyphens. For example: AA-BB-CC-DD-EE-FF. • **Colon** - Specifies that the MAC address format will contain colons. For example: AA:BB:CC:DD:EE:FF. • **Dot** - Specifies that the MAC address format will contain dots. For example: AA.BB.CC.DD.EE.FF. • **None** - Specifies that the MAC address format will contain no delimiters. For example: AABBCCDDEEFF.
Delimiter Number	Specifies the delimiter number that will be used in the MAC address format here. Options to choose from are:

Parameter	Description
	• **1** - Specifies to use a single delimiter. For example: AABBCC.DDEEFF. • **2** - Specifies to use two delimiters. For example: AABB.CCDD.EEFF • **5** - Specifies to use multiple delimiters. For example: AA.BB.CC.DD.EE.FF

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

DHCPv6 Relay Interface Settings

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

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

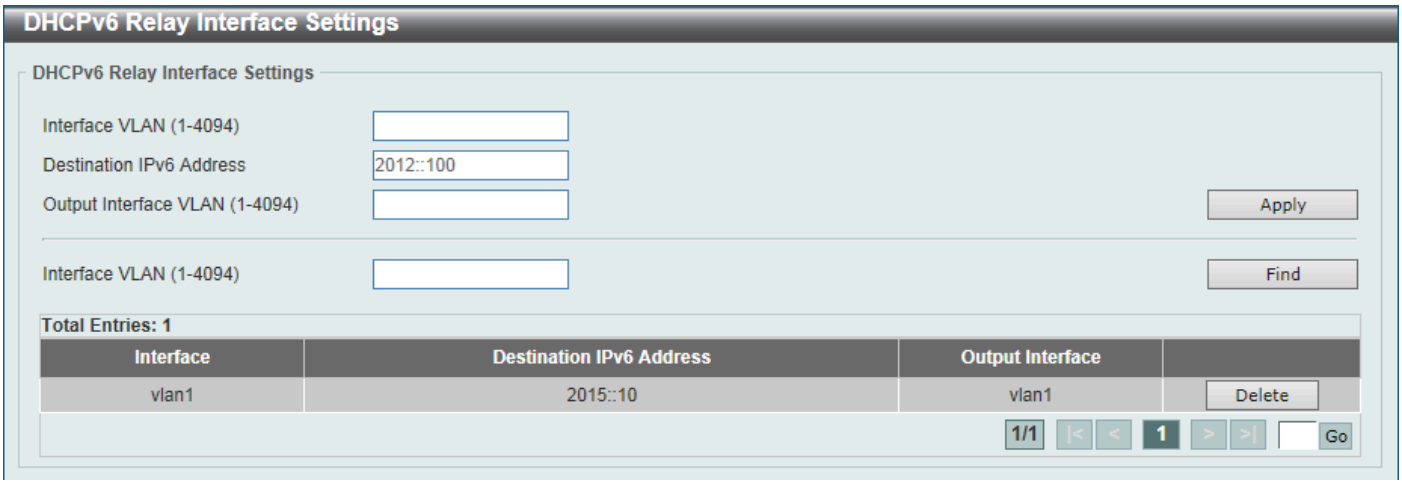


Figure 4-57 DHCPv6 Relay Interface Settings Window

The fields that can be configured are described below:

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

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

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

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

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

DHCPv6 Relay Format Type Settings

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

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

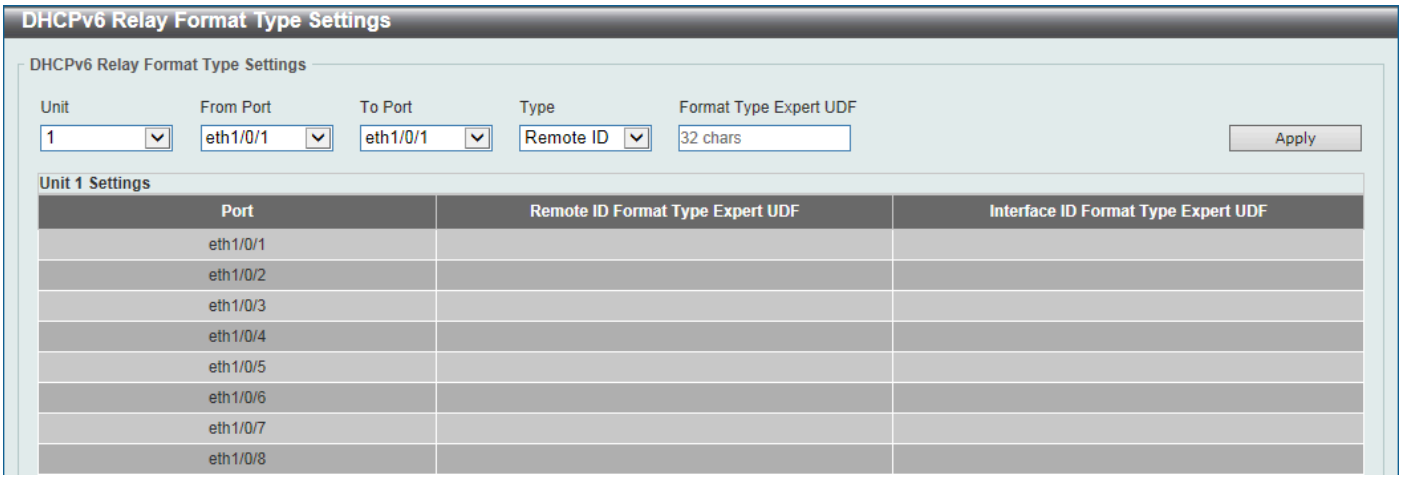


Figure 4-58 DHCPv6 Relay Format Type Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Type	Select the type here. Options to choose from are: • **Remote ID** - Specifies to configure the Expert UDF format type string for DHCPv6 Option 37. • **Interface ID** - Specifies to configure the Expert UDF format type string for DHCPv6 Option 18.
Format Type Expert UDF	Enter the format type expert UDF string that will be used on the specified port(s) here.

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

DHCPv6 Relay Port Settings

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

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



Figure 4-59 DHCPv6 Relay Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration here.
State	Select to enable or disable the DHCPv6 relay port feature on the specified port(s) here.

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

DHCPv6 Local Relay VLAN

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

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

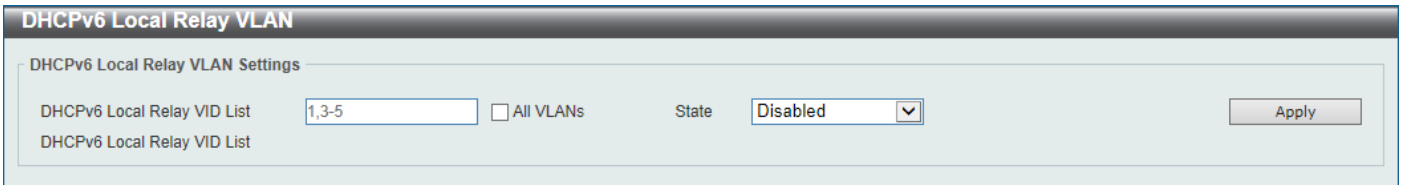


Figure 4-60 DHCPv6 Local Relay VLAN Window

The fields that can be configured are described below:

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

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

NOTE: When the state of the DHCPv6 relay port is disabled, the port will not relay or locally relay received DHCPv6 packets.

DHCP Auto Configuration

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

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

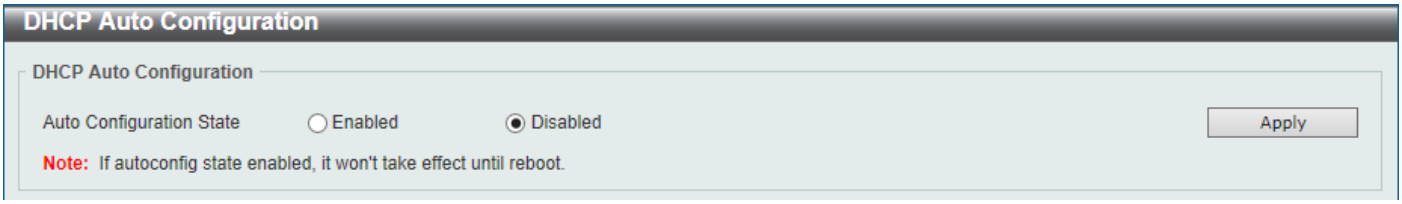


Figure 4-61 DHCP Auto Configuration Window

The fields that can be configured are described below:

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

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

DNS

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

DNS Global Settings

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

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

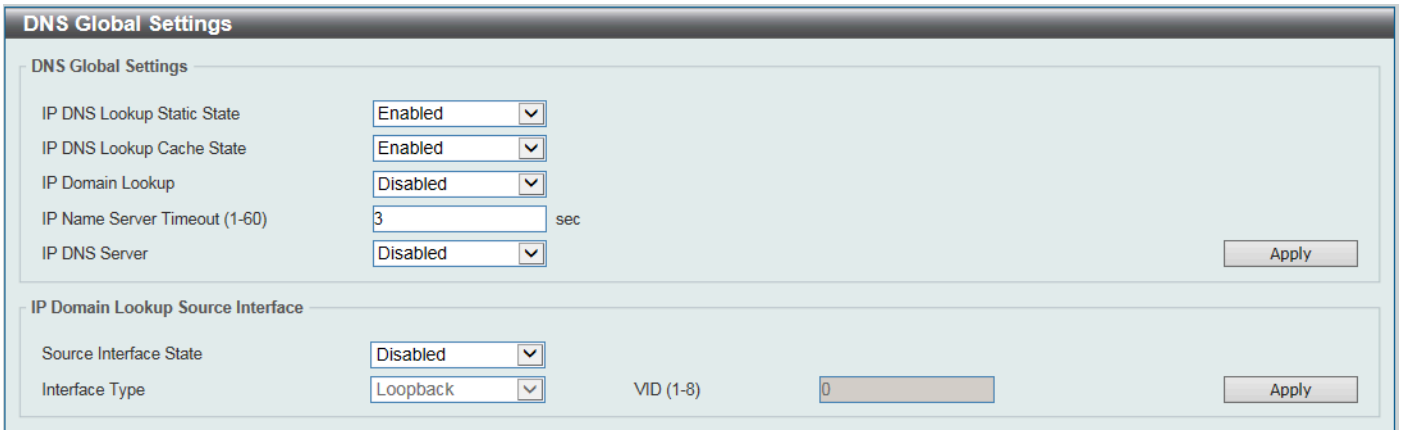


Figure 4-62 DNS Global Settings Window

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

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.

The fields that can be configured in **IP Domain Lookup Source Interface** are described below:

Parameter	Description
Source Interface State	Select to enable or disable the source interface state here.
Interface Type	Select the source interface type here. Options to choose from are **Loopback**, **Mgmt**, and **VLAN**.
Interface ID	If VLAN is selected, enter the VLAN ID (1-4094) of the source interface here. If Mgmt is selected, enter 0. If Loopback is selected, enter 1-8.

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

DNS Name Server Settings

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

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



Figure 4-63 DNS Name Server Settings Window

The fields that can be configured are described below:

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

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

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

DNS Host Settings

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

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



Figure 4-64 DNS Host Settings Window

The fields that can be configured are described below:

Parameter	Description
Host Name	Enter the host name (up to 255 characters) of the equipment.
IP Address	Select and enter the IPv4 address of the network equipment.
IPv6 Address	Select and enter the IPv6 address of the network equipment.

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

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

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

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

IP Source Interface

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

To view the following window, click **Management > IP Source Interface**, as shown below:

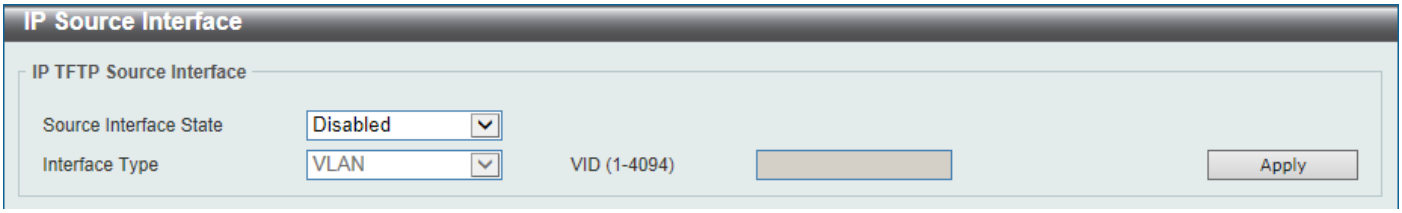


Figure 4-65 IP Source Interface Window

The fields that can be configured in **IP TFTP Source Interface** are described below:

Parameter	Description
Source Interface State	Select to enable or disable the IP TFTP source interface state here.
Interface Type	After enabling the Source Interface State option, select the interface type here. Options to choose from are Loopback, Mgmt, and VLAN.
VID	Enter the interface ID here. For loopback interfaces this value is from 1 to 8. For the management interface (Mgmt) this value can only be 0. For VLAN interfaces this value is from 1 to 4094.

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

File System

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

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

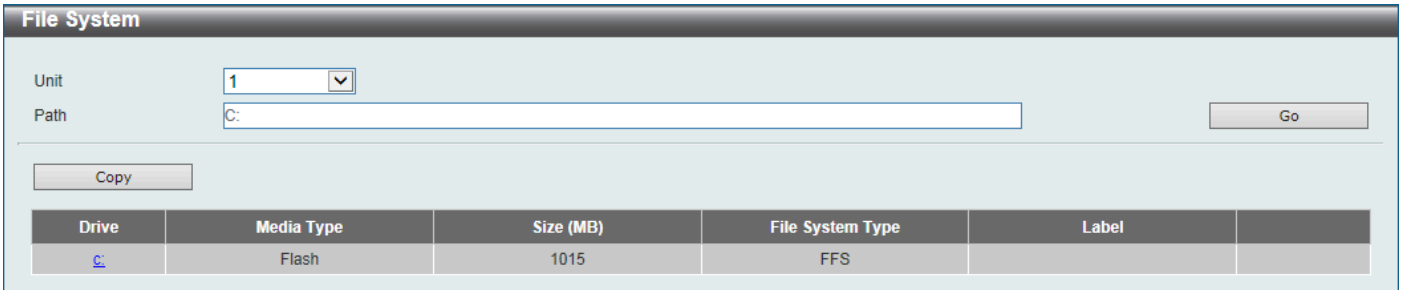


Figure 4-66 File System Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
Path	Enter the path string and click **Go** to navigate the C drive.

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

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

Click the **c:** hyperlinkto navigate the C: drive

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

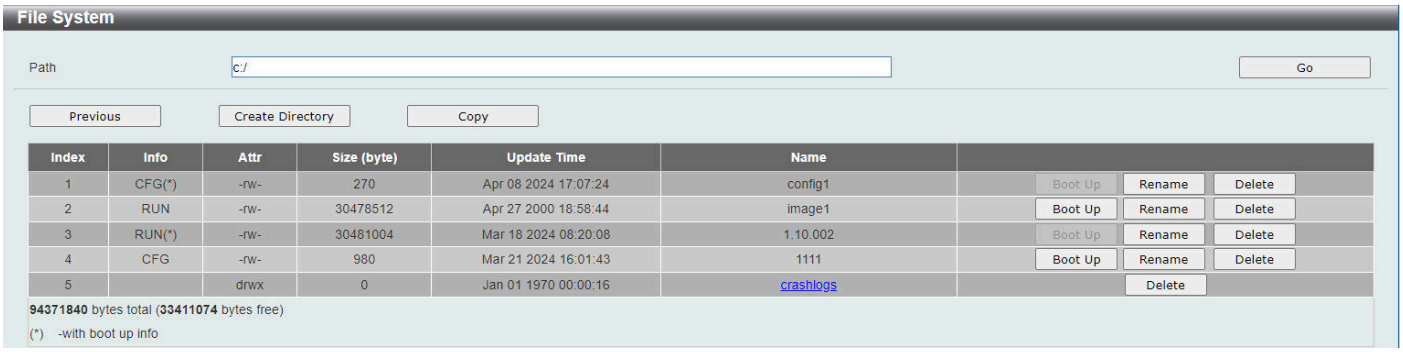


Figure 4-67 File System (Drive) Window

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

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

Click the **Create Directory** to create a new directory within the file system of the Switch.

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

Click the **Boot Up** button to set a specific runtime image as the boot up image.

Click the **Rename** button to rename a specific file name.

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

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

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

Click the **Copy** button to see the following window.

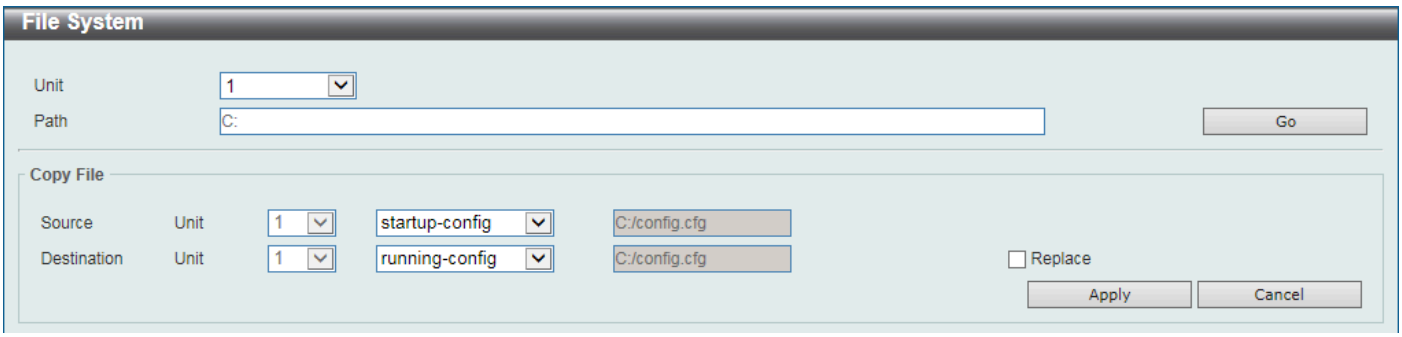


Figure 4-68 File System (Copy) Window

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

Parameter	Description
Source	Select the source Switch **Unit** ID and type of source file that will be copied here. Options to choose from are **startup-config** and **Source File**. Only after

Parameter	Description
	selecting the **Source File** option can the source file path and filename be entered in the space provided.
Destination	Select the destination Switch **Unit** ID and 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. Tick the **Replace** check box to replace the current running configuration with the indicated configuration file.

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

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

Stacking

The Switch supports stacking 9 Switches together while being managed by one console connection to the console port on the master Switch, or by an IP address through the MGMT port, or by multiple IP addresses through any of the ports using Telnet, the Web User Interface, and SNMP. This cost-effective Switch provides an affordable solution for administrators to upgrade their networks using the SFP28 ports to scale and stack the Switches. This increases overall reliability, serviceability, and availability of the network.

- **Duplex Chain** - The Duplex Chain topology stacks Switches together in a chain-link format. Using this method, data transfer is only possible in one direction and if there is a break in the chain, then data transfer will be affected.
- **Duplex Ring** - The Duplex Ring stacks Switches in a ring or circle format where data can be transferred in two directions. This topology is very resilient because if there is a break in the ring, data can still be transferred through the stacking cables between Switches in the stack.



NOTE: When stacking is enabled, the last 4 SFP28 ports are dedicated stacking ports and cannot be used for any other purposes. Only these ports connected using optical fiber cables or Direct Attached Cables (DAC) can perform stacking and they must operate at the same speed: 25 Gbps; any other types of optical modules cannot be used for stacking.



NOTE: Using Duplex Ring topology is strongly recommended.

Physical stacking needs to be enabled and can be configured to support 4-port stacking configuration. When the 4-port stacking configuration is used through the 25G SFP28 ports, a full-duplex speed of up to 200 Gbps will be available between two Switches.

The figure below illustrates how switches can be stacked in Duplex Ring formation.

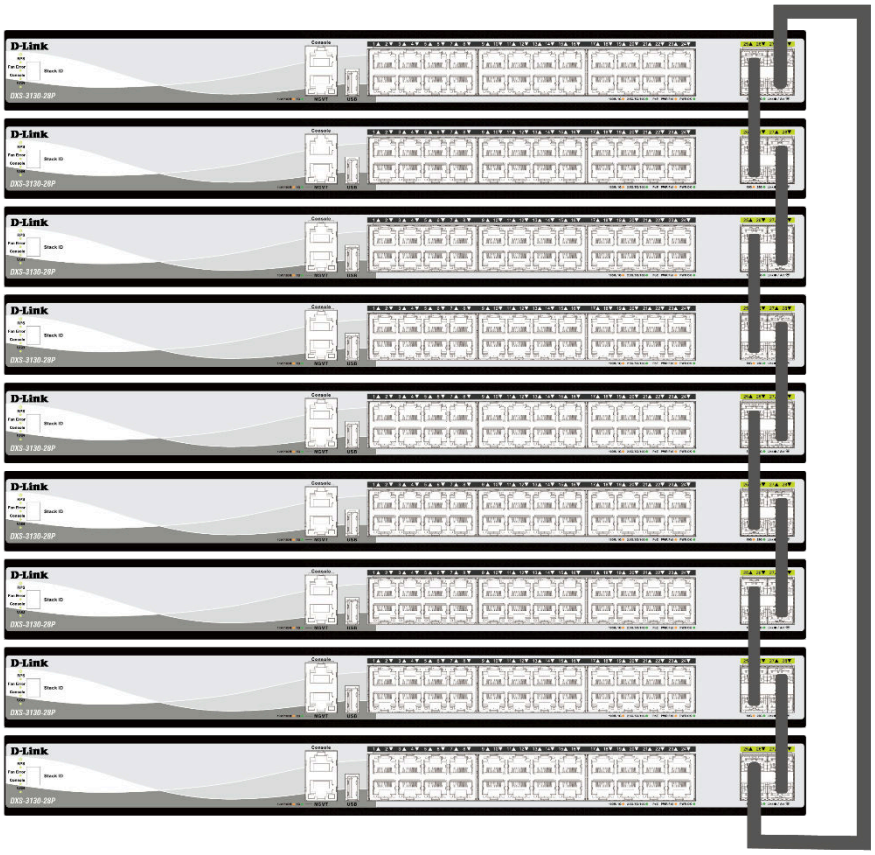


Figure 4-69 Duplex Ring stacking topology (SFP28 ports)

NOTE: For more stacking topologies, please refer to Switch Stacking section in DXS-3130-Series HW Installation Guide.

Switch Roles in a Stack

Within each of these topologies, each Switch plays a role in the Switch stack. These roles can be set by the user per individual Switch, or if desired, can be automatically determined by the Switch stack. Three possible roles exist when stacking with the Switch.

Primary Master - The Primary Master is the leader of the stack. It will maintain normal operations, monitor operations and the running topology of the Stack. This Switch will also assign Stack Unit IDs, synchronize configurations and transmit commands to remaining Switches in the Switch stack. The Primary Master can be manually set by assigning this Switch the highest priority (a lower number denotes a higher priority) before physically assembling the stack, or it can be determined automatically by the stack through an election process. This determines the lowest MAC address and then will assign that Switch as the Primary Master if all priorities are the same. The Primary master is physically displayed by the seven segment LED on the front panel of the Switch where the LED will flash between its given Box ID and ‘H’.

Backup Master - The Backup Master is the backup to the Primary Master and will take over the functions of the Primary Master if the Primary Master fails or is removed from the Stack. It also monitors the status of neighboring Switches in the stack, will perform commands assigned to it by the Primary Master and will monitor the running status of the Primary Master. The Backup Master can be set by the user by assigning this Switch the second highest priority (a lower number denotes a higher priority) before physically assembling the stack, or it can be determined automatically by the stack through an election process. This determines the second lowest MAC address and then will

assign that Switch as the Backup Master if all priorities are the same. The Backup master is physically displayed by the seven segment LED on the front panel of the Switch where the LED will flash between its given Box ID and 'h'.

Slave - Slave Switches constitute the rest of the Switch stack and although not Primary or Backup Masters, they can be placed into these roles when these other two roles fail or are removed from the stack. Slave Switches perform operations requested by the master, monitor the status of the stack topology, and adhere to the Backup Master's commands once it becomes the Primary Master. Slave Switches will do a self-check to determine if they are to become the Backup Master if the Backup Master is promoted to the Primary Master, or if the Backup Master fails or is removed from the Switch stack. If both Primary and Backup masters fail, or are removed from the Switch stack, the Switch will determine if it is to become the Primary Master. These roles will be determined by priority and if this is the same, by the value of the MAC addresses.

Once Switches have been assembled in the topology desired by the user and powered on, the stack will undergo three processes until it reaches a functioning state.

- **Initialization State** - This is the first state of the stack, where the runtime codes are set and initialized, and the system conducts a peripheral diagnosis to determine each individual Switch is functioning properly.
- **Master Election State** - Once the runtime codes are loaded and initialized, the stack will undergo the Master Election State where it will discover the type of topology used, elect a Primary Master and then a Backup Master.
- **Synchronization State** - Once the Primary Master and the Backup Master have been established, the Primary Master will assign Stacking Unit IDs to Switches in the stack, synchronize configurations for all Switches and then transmit commands to the rest of the Switches based on the configuration of the Primary Master.

Once these steps have been completed, the Switch stack will enter a normal operating mode.

Stack Switch Swapping

The stacking feature of the Switch supports hot swapping of Switches in and out of the running stack. Users may remove or add Switches to the stack without powering down or largely affecting the transfer of data between Switches in the stack, as long as some basic rules are adhered to.

When Switches are 'hot inserted' into the running stack, the new Switch may take on the Primary Master, Backup Master or Slave role, depending on configuration set on the newly added Switch, such as priority or MAC address. Yet, if adding two stacks together that have both previously undergone the election process, and therefore both have a Primary Master and a Backup master, a new Primary Master will be elected from one of the already existing Primary Masters, based on priority or MAC address. This Primary Master will take over all of the Primary Master's roles for all new Switches that were hot inserted. This process is done using discovery packets that circulate through the Switch stack every 1.5 seconds until the discovery process has been completed.

The 'hot remove' action means removing a device from the stack while the stack is still running. The hot removal is detected by the stack when it fails to receive heartbeat packets during its specified interval from a device, or when one of the stacking ports links is down. Once the device has been removed, the remaining Switches will update their stacking topology database to reflect the change. Any one of the three roles, Primary Master, Backup Master or Slave, may be removed from the stack, yet a different process occurs for each specific device removal.

If a Slave device has been removed, the Primary Master will inform other Switches of the hot remove of this device through the use of unit leave messages. Switches in the stack will clear the configuration of the unit removed, and dynamically learned databases, such as ARP, will also be cleared.

If the Backup Master has been hot removed, a new Backup Master will be chosen through the election process previously described. Switches in the stack will clear the configuration of the unit removed, and dynamically learned databases, such as ARP, will also be cleared. Then the Backup Master will begin backing up the Primary Master when the database synchronization has been completed by the stack.

If the Primary Master is removed, the Backup Master will assume the Primary Master's role and a new Backup Master will be chosen using the election process. Switches in the stack will clear the configuration of the unit removed, and dynamically learned databases, such as ARP, will also be cleared. The new Primary Master will inherit the MAC and IP address of the previous Primary Master to avoid conflict within the stack and the network itself.

If both the Primary Master and the Backup Master are removed, the election process is immediately initiated, and a new Primary Master and Backup Master are elected. Switches in the stack will clear the configuration of the units that have been removed, and dynamically learned databases, such as ARP, will also be cleared. Static Switch configuration still remains in the database of the remaining Switches in the stack and those functions will not be affected.

NOTE: If there is a Box ID conflict when the stack is in the discovery phase, the device will enter a special standalone topology mode. Users can only get device information, configure Box IDs, save and reboot. All stacking ports will be disabled and an error message will be produced on the local console port of each device in the stack. Users must reconfigure Box IDs and reboot the stack to rectify the problem.

NOTE: When constructing a stacking with different switch models, static box_id setting is recommended. If a new inserted switch box_id's device type is different from the configuration file box_id's device type, the new inserted switch will use default configurations.

Physical Stacking

This window is used to display and configure the physical stacking settings.

To view the following window, click **Management > Stacking > Physical Stacking**, as shown below:

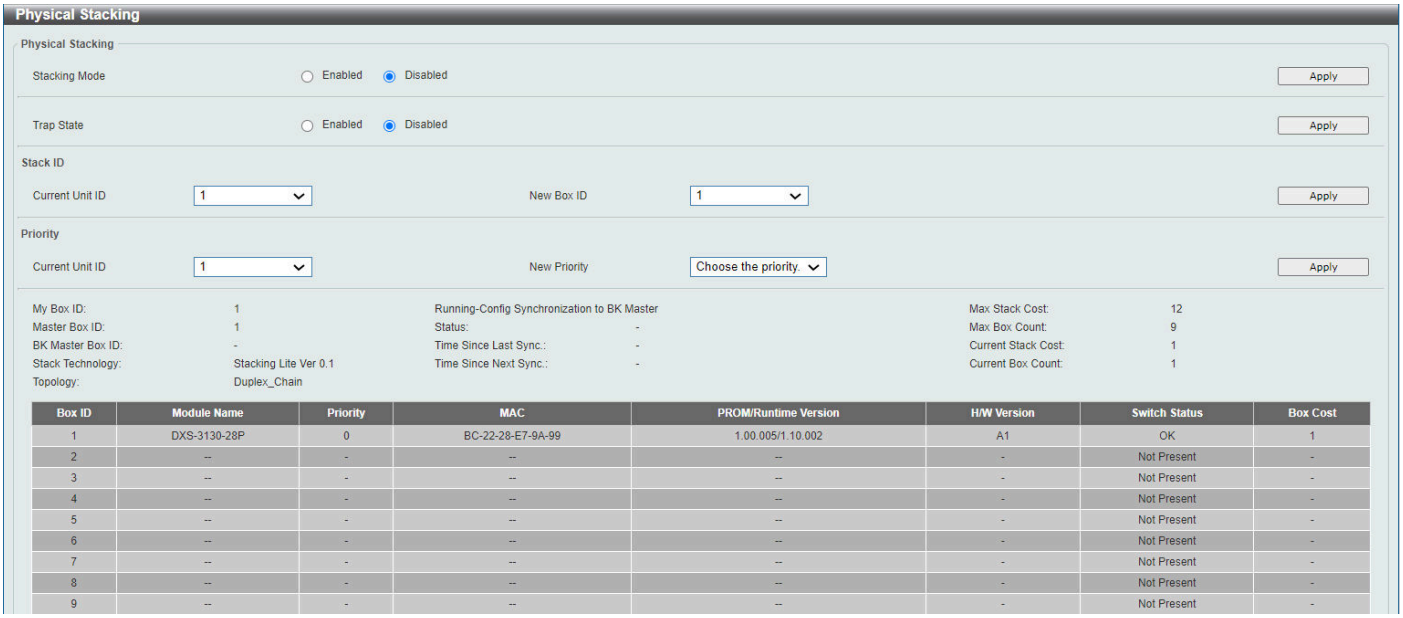


Figure 4-70 Physical Stacking Window

The fields that can be configured in **Physical Stacking** are described below:

Parameter	Description
Stacking Mode	Select this option to enable or disable the stacking mode.
Trap State	Select this option to enable or disable stacking related SNMP traps.

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

The fields that can be configured in **Stack ID** are described below:

Parameter	Description
Current Unit ID	Select the unit ID of the Switch in the stack.

Parameter	Description
New Box ID	Select the new box ID for the Switch that is selected in the **Current Unit ID** field. The user may choose any number between 1 and 9 to identify the Switch in the switch stack.

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

Parameter	Description
Current Unit ID	Select the unit ID of the Switch in the stack.
New Priority	Enter the priority of the Switch stacking unit. The range is from 0 to 15. A higher number means a higher priority and 0 indicates unassigned.

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

Stacking Bandwidth

This window is used to display and configure the stacking bandwidth settings. Physical stacking needs to be enabled and can be configured to support 4-port stacking configuration.

- With the 4-port-SFP28 stacking configuration, the **DXS-3130-28P** will use only physical ports 25, 26, 27, and 28 for 4-port stacking for a full-duplex speed of up to 200 Gbps.

NOTE: The stacking bandwidth must be configured before the Switch can be stacked with other Switches.

To view the following window, click **Management > Stacking > Stacking Bandwidth**, as shown below:

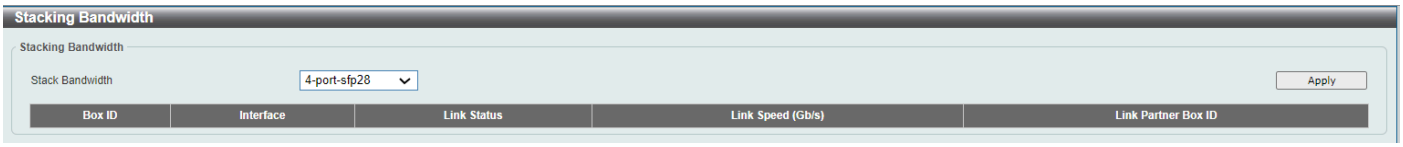


Figure 4-71 Stacking Bandwidth Window

The fields that can be configured are described below:

Parameter	Description
Stack Bandwidth	Select the stacking bandwidth here: • **4-port-SFP28** - Specifies 4 SFP28 ports to be used for stacking.

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

Virtual Stacking (SIM)

D-Link Single IP Management (SIM) is a concept that will stack Switches together over Ethernet instead of using stacking ports or modules. There are some advantages in implementing the Single IP Management feature:

- SIM can simplify management of small workgroups or wiring closets while scaling the network to handle increased bandwidth demand.

- SIM can reduce the number of IP address needed in your network.
- SIM can eliminate any specialized cables for stacking connectivity and remove the distance barriers that typically limit your topology options when using other stacking technology.

Switches using D-Link Single IP Management (labeled here as SIM) must conform to the following rules:

- SIM is an optional feature on the Switch and can easily be enabled or disabled through the Command Line Interface or Web Interface. SIM grouping has no effect on the normal operation of the Switch in the network.
- There are three classifications for Switches using SIM. The **Commander Switch (CS)**, which is the master Switch of the group, **Member Switch (MS)**, which is a Switch that is recognized by the CS as a member of a SIM group, and a **Candidate Switch (CaS)**, which is a Switch that has a physical link to the SIM group but has not been recognized by the CS as a member of the SIM group.
- A SIM group can only have one Commander Switch (CS).
- A SIM group accepts up to 32 Switches (numbered 1-32), not including the Commander Switch (numbered 0).
- Members of a SIM group must be in the same Layer 2 network.
- There is no limit to the number of SIM groups in the same IP subnet (broadcast domain); however, a single Switch can only belong to one group.
- If multiple VLANs are configured, the SIM group will only utilize the management VLAN on any Switch.
- SIM allows intermediate devices that do not support SIM. This enables the user to manage Switches that are more than one hop away from the CS.

The SIM group is a group of Switches that are managed as a single entity. The Switch may take on three different roles:

1. **Commander Switch (CS)** - This is a Switch that has been manually configured as the controlling device for a group, and takes on the following characteristics:
    - It has an IP Address.
    - It is not a CS or member Switch of another SIM group.
    - It is connected to the member Switches through its management VLAN.
2. **Member Switch (MS)** - This is a Switch that has joined a SIM group and is accessible from the CS, and it takes on the following characteristics:
    - It is not a CS or MS of another SIM group.
    - It is connected to the CS through the CS management VLAN.
3. **Candidate Switch (CaS)** - This is a Switch that is ready to join a SIM group but is not yet a member of the SIM group. The Candidate Switch may join the SIM group of the Switch by manually configuring it to be a MS of a SIM group. A Switch configured as a CaS is not a member of a SIM group and will take on the following characteristics:
    - It is not a CS or MS of another Single IP group.
    - It is connected to the CS through the CS management VLAN.

The following rules also apply to the above roles:

- Each device begins in a CaS state.
- A CS must change its role to CaS and then to MS, to become a MS of a SIM group. Thus, the CS cannot directly be converted to a MS.
- The user can manually configure a CS to become a CaS.
- A MS can become a CaS by:
    - Being configured as a CaS through the CS.
    - If report packets from the CS to the MS time out.
- The user can manually configure a CaS to become a CS

- The CaS can be configured through the CS to become a MS.

After configuring one Switch to operate as the CS of a SIM group, additional Switches may join the group by manually configuring the Switch to be a MS. The CS will then serve as the in-band entry point for access to the MS. The CS's IP address will become the path to all MSs in the group and the CS's administrator password, and/or authentication will control access to all MSs in the SIM group.

With SIM enabled, the applications in the CS will redirect the packets instead of executing packets. The applications will decode the packet from the administrator, modify some data, and then send it to the MS. After execution, the CS may receive a response packet from the MS, which it will encode and send it back to the administrator.

When a CaS becomes a MS, it automatically becomes a member of the first SNMP community (includes read/write and read only) to which the CS belongs. However, if a MS has its own IP address, it can belong to SNMP communities to which other switches in the group, including the CS, do not belong.

Single IP Settings

This window is used to display and configure the SIM settings. The Switch is set as a Candidate (CaS) as the factory default configuration and Single IP Management is disabled.

To view the following window, click **Management > Virtual Stacking (SIM) > Single IP Settings**, as shown below:

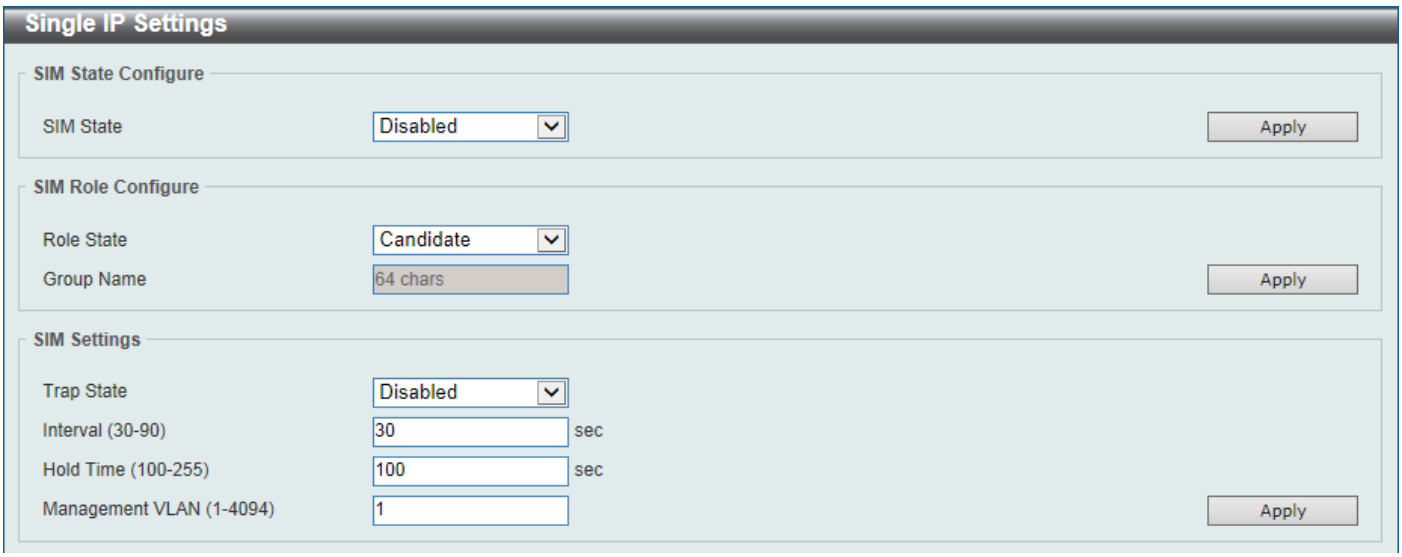


Figure 4-72 Single IP Settings Window

The fields that can be configured in **SIM State Configure** are described below:

Parameter	Description
SIM State	Select this option to enable or disable the SIM state on the Switch. Select **Disabled** to disable SIM on the Switch.

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

The fields that can be configured in **SIM Role Configure** are described below:

Parameter	Description
Role State	Select to change the SIM role of the Switch. Options to choose from are **Candidate** and **Commander**. • **Candidate** - A Candidate Switch (CaS) is not the member of a SIM group but is connected to a Commander Switch. This is the default setting for the SIM role of the Switch.

Parameter	Description
	• **Commander** - Select to make the Switch a Commander Switch (CS). The user may join other Switches to this Switch, over Ethernet, to be part of the SIM group. Choosing this option will also enable the Switch to be configured for SIM.
Group Name	Enter a group name if commander is selected for the SIM role. This is optional. This name is used to segment Switches into different SIM groups.

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

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

Parameter	Description
Trap State	Select to enable or disable the SIM trap state here.
Interval	Enter the interval in seconds. The range is from 30 to 90.
Hold Time	Enter the hold-time in seconds. The range is from 100 to 255.
Management VLAN	Enter the single IP management message VLAN ID (1-4094).

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

After enabling the Switch to be a Commander Switch (CS), the **Single IP Management** folder will then contain four added links to aid in configuring SIM through the Web UI, including **Topology**, **Firmware Upgrade**, **Configuration File Backup/Restore** and **Upload Log File**.

Topology

This window is used to view, manage and configure the Switch within the SIM group and requires Java to function properly on your computer.

To view the following window, click **Management > Virtual Stacking (SIM) > Topology**, as shown below:

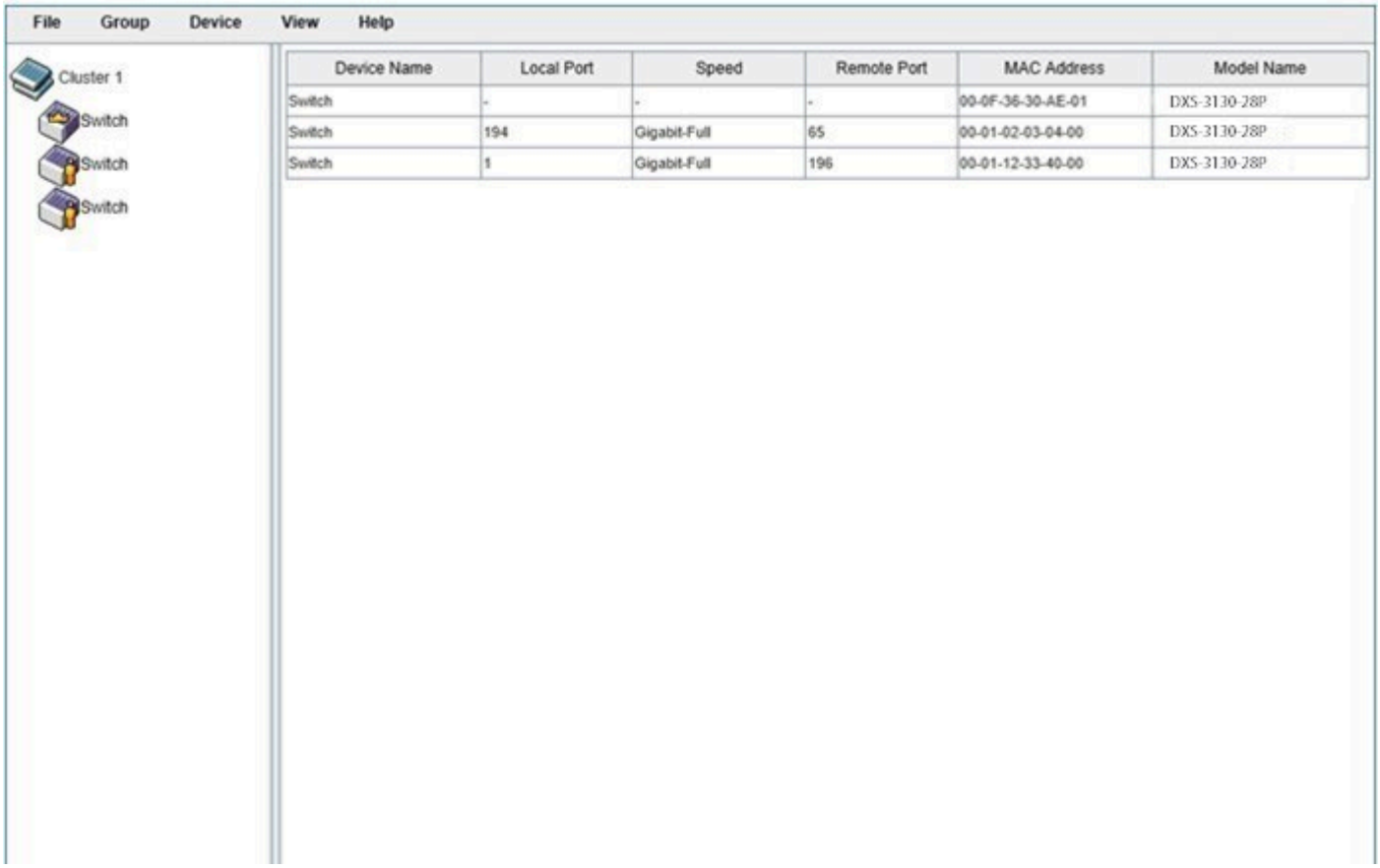


Figure 4-73 Topology Window

There is a menu bar at the top of the window containing **File**, **Group**, **Device**, **View**, and **Help**.

File

Print Topology

Select this option to print the SIM topology map to any of the printers configured on the PC accessing the Web UI.

Preference

Select this option to configure the display properties for the SIM topology map.

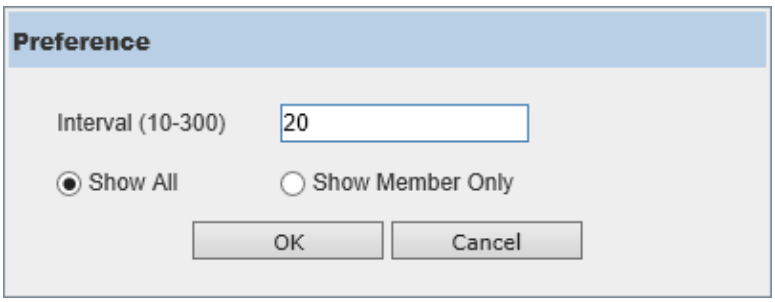


Figure 4-74 Preference

The fields that can be configured are described below:

Parameter	Description
Interval	Enter the SIM topology display refresh interval value here. The range is from 10 to 300.
Show All	Select this option to display all available SIM devices in the topology.
Show Member Only	Select this option to only display SIM member devices in the topology.

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

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

Group

Add to Group

Select a Candidate Switch (CaS) from the list and then select this option (**Add to Group**) to add the selected CaS to the SIM group. Password authentication is required when a CaS is added to the SIM group.

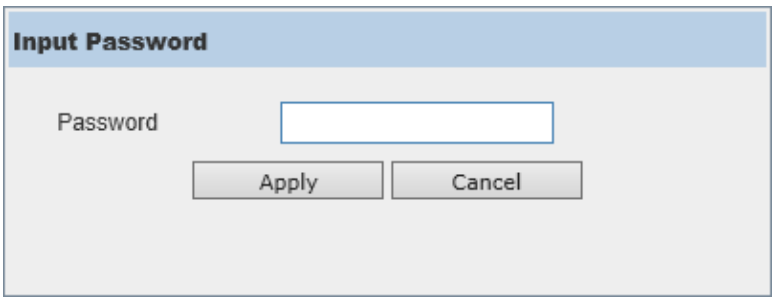


Figure 4-75 Add to Group (Input Password)

Enter the **Password** and click the **Apply** button to add the CaS to the SIM group.

Click the **Cancel** button to discard the addition and return to the Topology window.

Remove from Group

Select a Member Switch (MS) from the list and then select this option (**Remove from Group**) to remove the selected MS from the SIM group.

Device

Configure

Select a device from the list and then select this option (**Configure**) to connect to the Web User Interface (if available) on the selected device.

View

Refresh

Select this option to refresh the items displayed in the page.

Topology

Under **View**, select **Topology** to view the following:

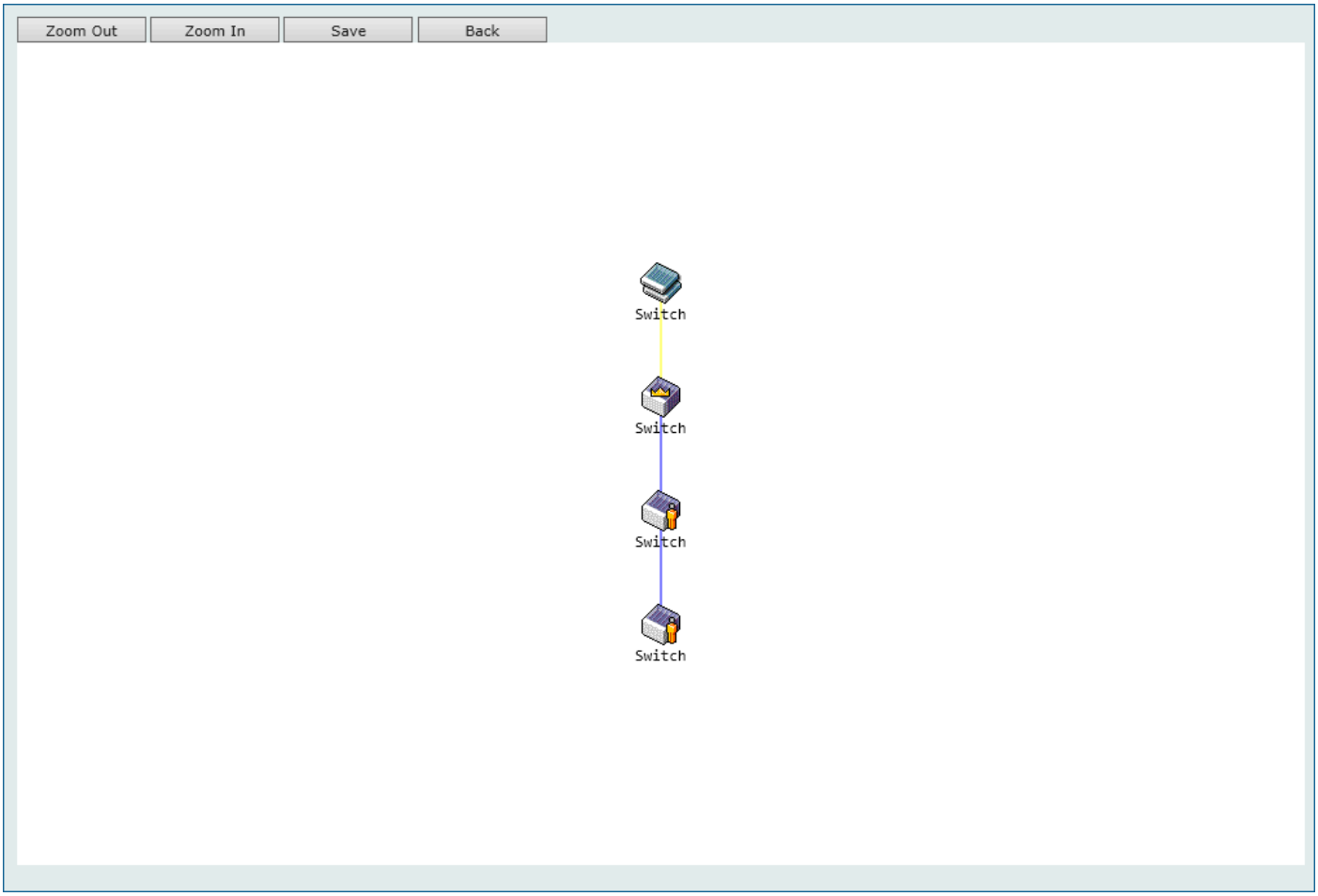


Figure 4-76 View > Topology

Click the **Zoom In** button enlarge the size of the displayed items.

Click the **Zoom Out** button reduce the size of the displayed items.

Click the **Save** button to save the display.

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

This window will display how the devices within the SIM Group connect to other groups and devices. Possible icons on this window are as follows:

Icon	Description	Icon	Description
	Group		Layer 3 Member Switch

Icon	Description	Icon	Description
	Layer 2 Commander Switch		Member Switch of other group
	Layer 3 Commander Switch		Layer 2 Candidate Switch
	Commander Switch of other group		Layer 3 Candidate Switch
	Layer 2 Member Switch		Unknown device

Tool Tips

In the Topology view window, the mouse plays an important role in configuration and in viewing device information. Hover the mouse pointer over a specific device in the Topology window to display more information about the device

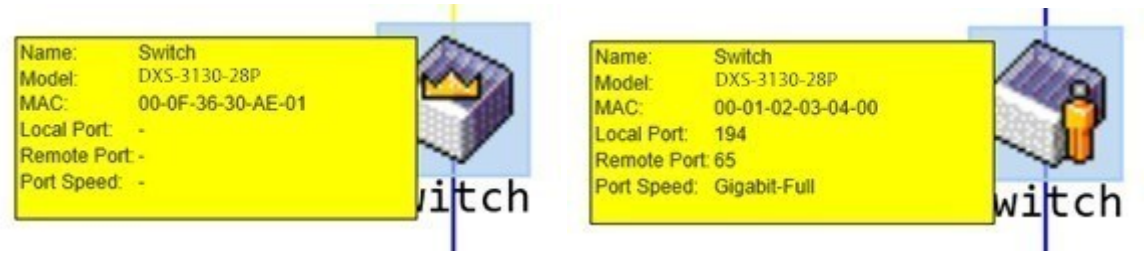


Figure 4-77 Device Information Utilizing the Tool Tip

Hover the mouse pointer over a line between two devices to display the **connection speed** between the two devices.

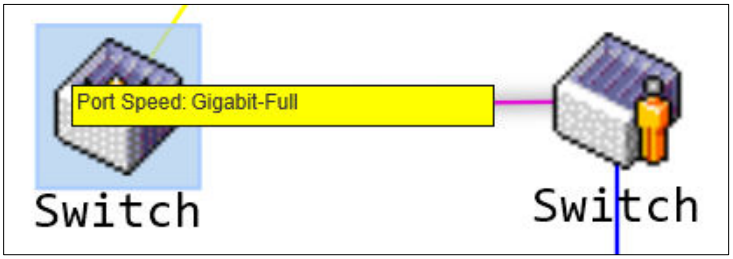
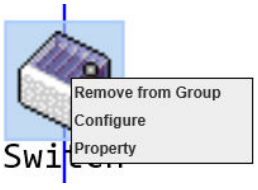
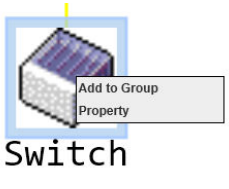


Figure 4-78 Port Speed Utilizing the Tool Tip

Right-Click

Right-click on a device to allow the user to perform various functions, depending on the role of the Switch in the SIM group and the icon associated with it.

Group	Commander Switch	Member Switch	Candidate Switch
			

The fields that can be configured are described below:

Parameter	Description
Property	Specifies to display more information about the device.
Configure	(Member Switch Only) Specifies to connect to the Web User Interface (if available) on the selected device.
Add to Group	(Candidate Switch Only) Specifies to add the selected CaS to the SIM group. Password authentication is required when a CaS is added to the SIM group.
Remove from Group	(Member Switch Only) Specifies to remove the selected MS from the SIM group.

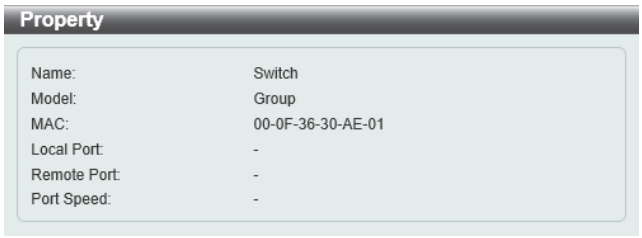


Figure 4-79 Group Property



Figure 4-80 Commander Switch Property



Figure 4-81 Member Switch Property



Figure 4-82 Candidate Switch Property

The fields displayed are described below:

Parameter	Description
Name	Displays the Device Name of the Switches in the SIM group configured. If the device is not configured with a name, it will be given the name default and tagged with the last six digits of the MAC address to identify it.
Module	Displays the full module name of the Switch.
MAC Address	Displays the MAC address of the Switch.
Local Port	Displays the number of the physical port on the CS that the MS or CaS is connected to. The CS will have no entry in this field.
Remote Port	Displays the number of the physical port on the MS or CaS that the CS is connected to. The CS will have no entry in this field.
Port Speed	Displays the connection speed between the CS and the MS or CaS.

Help

About

Select this option to display the SIM Copyright information and release date.

Firmware Upgrade

The Firmware Upgrade tab allows you to download firmware from a TFTP server. To obtain firmware files from a TFTP server, enter the following information:

Field	Description
TFTP Server IP	The IP address of a TFTP server.
Path\ Filename	Enter the directory and name of the firmware file stored on the TFTP server.

Click **Download** to download the firmware file to the selected member Switch.

Configuration File Backup/Restore

The Configuration File Backup/Restore tab allows you to restore the Switch to a previous state or back up the current configuration file to a TFTP server.

Field	Description
TFTP Server IP	The IP address of a TFTP server.
Path\ Filename	Enter the directory and name of the configuration file stored on the TFTP server.

Click **Restore** to the apply the configure file to the selected member Switch or **Backup** to upload the configuration file to the designated TFTP server.

Upload Log File

The Upload Log File allows you to upload log files to a log (TFTP) server.

Field	Description
TFTP Server IP	The IP address of a TFTP server.
Path\ Filename	Enter the directory of the TFTP server for storing log files.

Click **Upload** to upload log files of the selected member Switch to the designated TFTP server.

D-Link Discovery Protocol

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

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

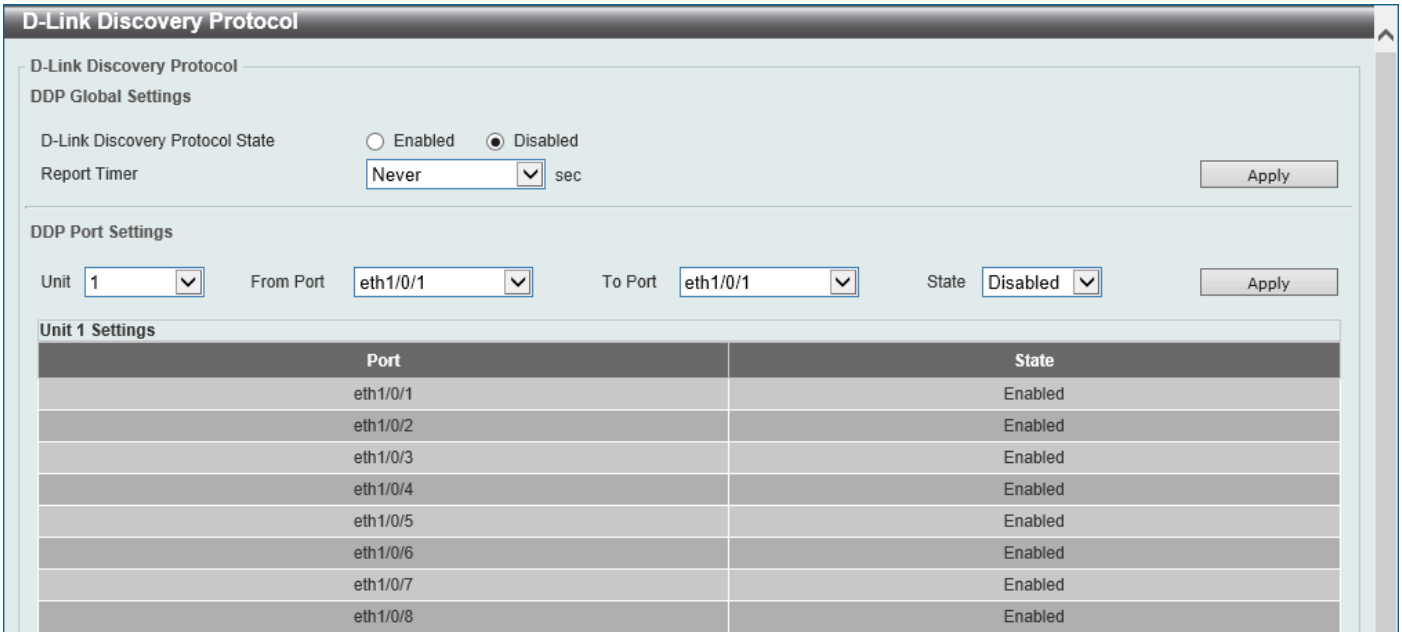


Figure 4-83 D-Link Discovery Protocol Window

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

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

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

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

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration here.
State	Select to enable or disable the DDP feature on the specified port(s) here.

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

SMTP Settings

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

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

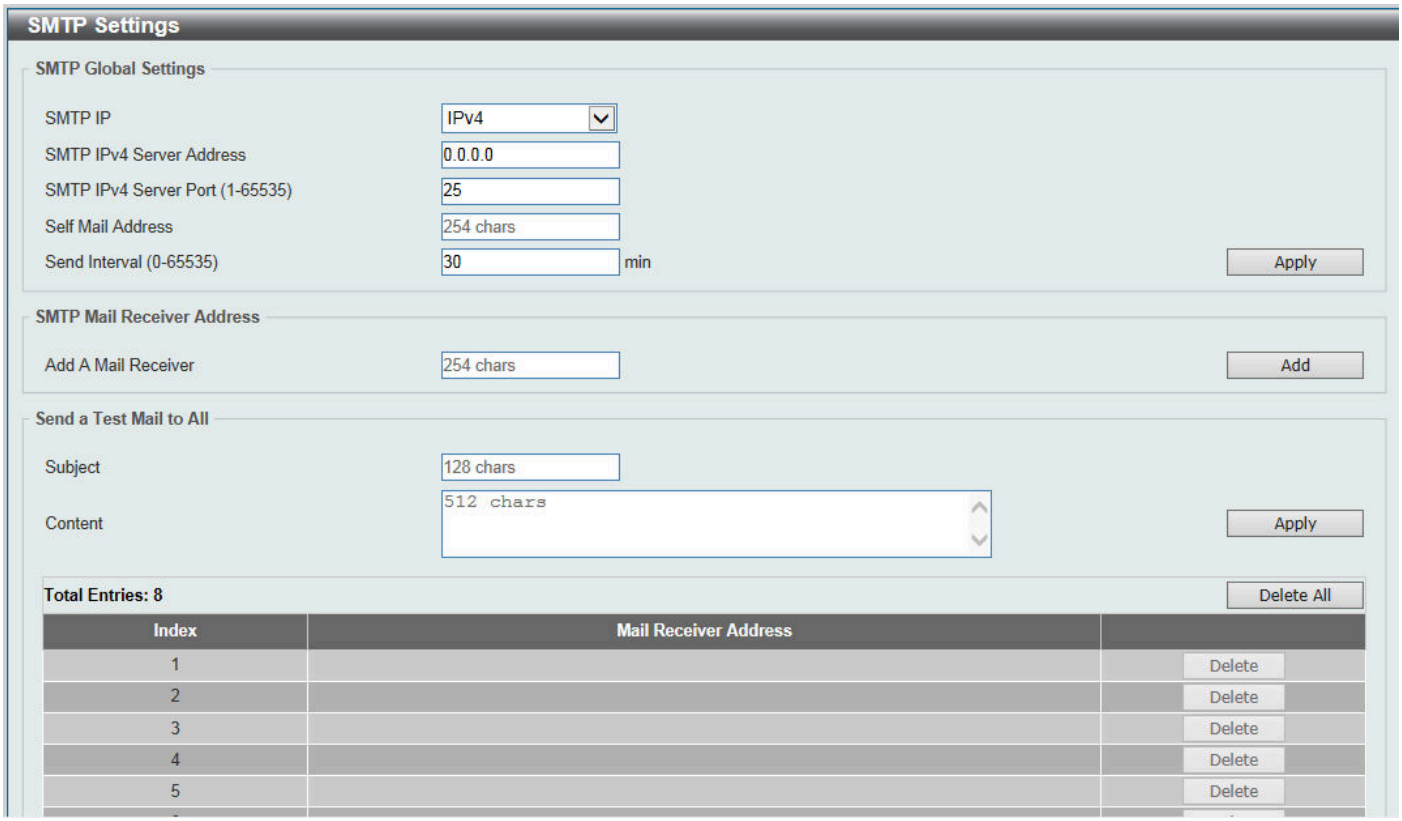


Figure 4-84 SMTP Settings Window

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

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 in the format: x.x.x.x (x is a number between 0 and 255).
SMTP IPv6 Server Address	After selecting **IPv6** as the SMTP IP type enter the SMTP server IPv6 address here in the format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (x is a hexadecimal digit)
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.
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 fields that can be configured in **SMTP Mail Receiver Address** are described below:

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

Click the **Add** button to add a new SMTP email recipient.

The fields that can be configured in **Send a Test Mail to All** are described below:

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

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

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

Reboot Schedule Settings

This window is used to display and configure the reboot schedule settings. Use this window to configure the reboot schedule of the Switch. The reboot schedule must take effect within 30 days. After the reboot schedule has taken effect and the Switch is restarted, it will generate a log message to identify that the Switch has been restarted using the reboot schedule. After a reboot or a shutdown, the reboot schedule will be deleted automatically. If the Switch was manually rebooted or powered off, before the reboot schedule could take effect, the specified reboot schedule will be cancelled.

To view the following window, click **Management > Reboot Schedule Settings**, as shown below:

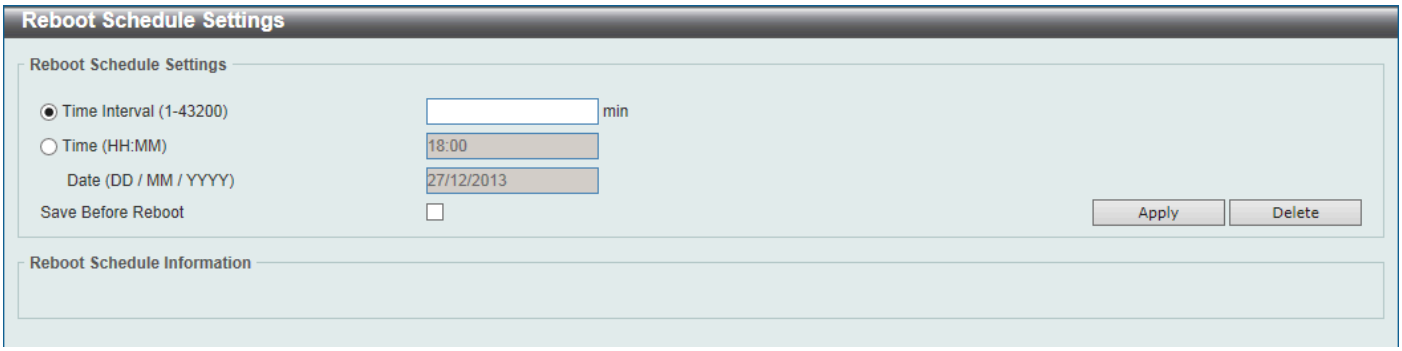


Figure 4-85 Reboot Schedule Settings Window

The fields that can be configured are described below:

Parameter	Description
Time Interval	Select and enter the reboot schedule time interval value here. The reboot will be initiated after the specified time interval has passed. The range is from 1 to 43200 minutes (30 days).
Time	Select and enter the time at which the reboot should be initiated here. This time uses the 24-hour format, for example, 21:30. If the date was not specified, the reboot will be initiated when the system clock reaches the time specified within the next 24 hours.

Parameter	Description
Date	Select and enter the date at which the reboot should be initiated here. This date uses the following format: DD/MM/YYYY. For example, 23/12/2015. The reboot schedule can only be initiated within 30 days of configuration.
Save Before Reboot	Select this option to save all configuration changes made before the reboot is initiated.

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

Click the **Delete** button to remove the specified reboot schedule.

PPPoE Circuit ID Insertion Settings

This window is used to display and configure the PPPoE Circuit ID Insertion Settings.

To view the following window, click **Management > PPPoE Circuit ID Insertion Settings**, as shown below:

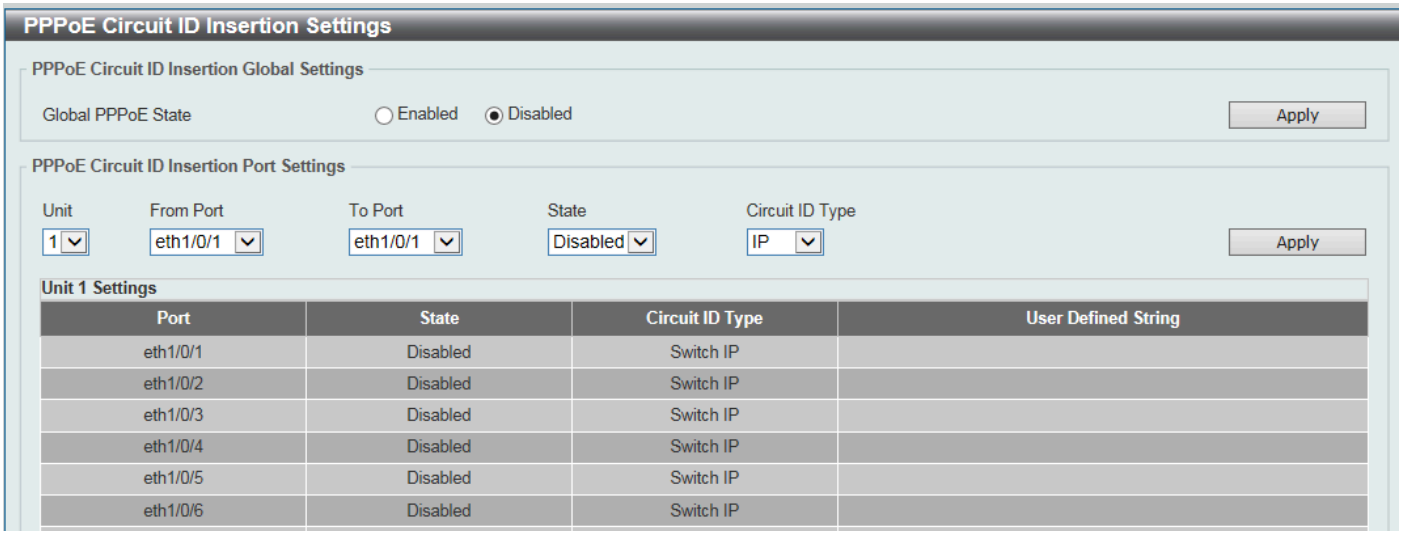


Figure 4-86 PPPoE Circuit ID Insertion Global Settings Window

The fields that can be configured in **PPPoE Circuit ID Insertion Settings** are described below:

Parameter	Description
Global PPPoE State	Select this option to enable or disable the PPPoE Circuit ID Insertion on the Switch. Select Disabled to disable PPPoE Circuit ID Insertion on the Switch.

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

The fields that can be configured in **PPPoE Circuit ID Insertion Port Settings** are described below:

Parameter	Description
Unit	Select the stacking unit ID of the Switch that will be configured here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration here.
State	Select to enable or disable the PPPoE Circuit ID Insertion Port state here.
Circuit ID Type	Specifies that the IP, MAC, or expert UDF format will be used.

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

SD Card Management

This section refers to the configuration associated with removable devices which includes USB driver storage.

SD Card Backup Settings

This window is used to display and configure the SD card backup settings. This is used to create or modify an SD card management backup schedule entry.

To view the following window, click **Management > SD Card Management > SD Card Backup Settings**, as shown below:

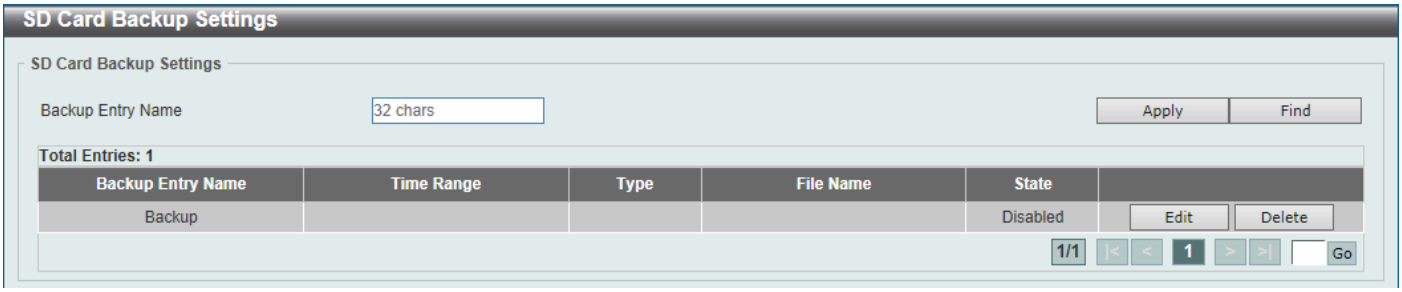


Figure 4-87 SD Card Backup Settings Window

The fields that can be configured are described below:

Parameter	Description
Backup Entry Name	Enter the name of the SD card management backup schedule here. This string can be up to 32 characters long.
Time Range	After clicking the **Edit** button, enter the time range schedule that will be used here (refer to **System > Time Range**).
Type	After clicking the Edit button, select the backup type here. Options to choose from are: • **Configuration** - Specifies that this schedule is used to back up the configuration. • **Log** - Specifies that this schedule is used to back up the system log.
File Name	After clicking the **Edit** button, enter the destination file path and name here.
State	After clicking the **Edit** button, select to enable or disable this schedule here.

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

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

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

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

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

SD Card Execute Settings

This window is used to display and configure the SD card execution settings. This is used to execute the configuration from the SD card to the Switch file system manually.

To view the following window, click **Management > SD Card Management > SD Card Execute Settings**, as shown below:

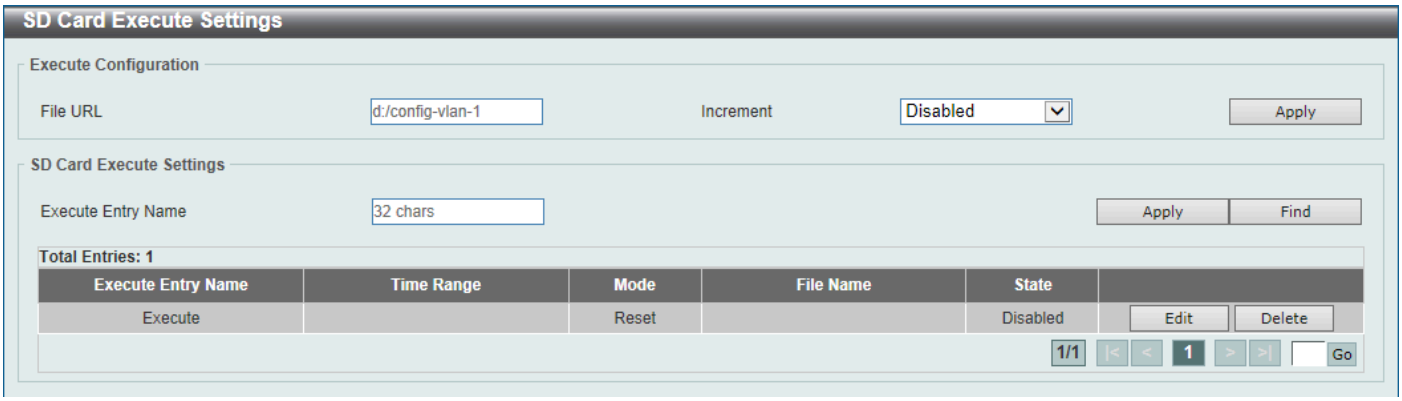


Figure 4-88 SD Card Execute Settings Window

The fields that can be configured in **Execute Configuration** are described below:

Parameter	Description
File URL	Enter the URL of the file here. If the current directory is not the directory of SD card file system, then the full file path must be entered, for example, d:/path_name/file_name.
Increment	Select to enable or disable the increment feature here. • When enabled, the current configuration will not be cleared before executing the configuration. • When disabled, the current configuration will be cleared before executing the configuration.

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

The fields that can be configured in **SD Card Execute Settings** are described below:

Parameter	Description
Execute Entry Name	Enter the name of the execution entry here. This string can be up to 32 characters long.
Time Range	After clicking the **Edit** button, enter the time range schedule that will be used here. Refer to **System >** Time Range**.**
Mode	After clicking the **Edit** button, select the mode here. Options to choose from are: • **Increase** - Specifies that the current configuration will not be cleared before executing the configuration. • **Reset** - Specifies that the current configuration will be cleared before executing the configuration.
File Name	After clicking the **Edit** button, enter the source file path and name that will be executed here.
State	After clicking the **Edit** button, select to enable or disable this schedule here.

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

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

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

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

5. Layer 2 Features

FDB
VLAN
VLAN Tunnel
STP
ERPS (G.8032)
Loopback Detection
Link Aggregation
L2 Protocol Tunnel
L2 Multicast Control
LLDP

FDB

Static FDB

This section configures the FDB (forwarding database) table used by the Switch.

Unicast Static FDB

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

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

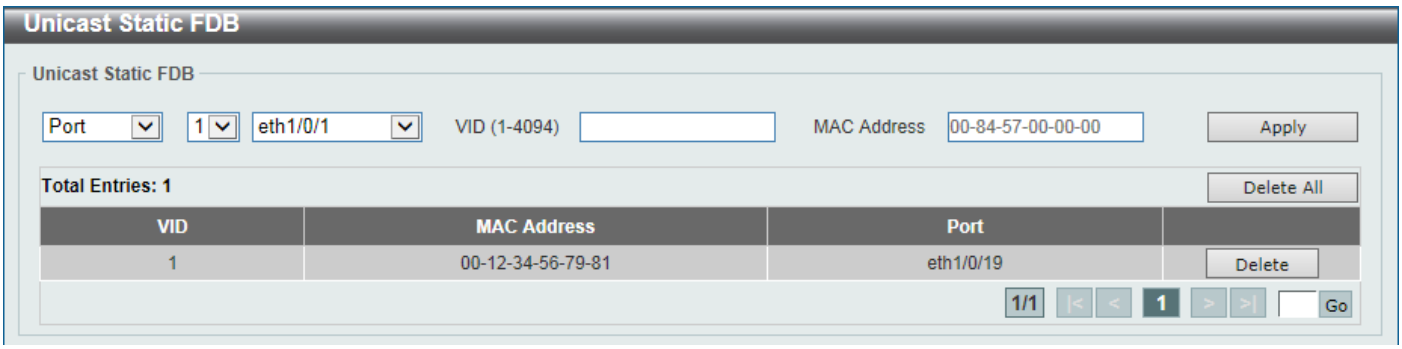


Figure 5-1 Unicast Static FDB Window

The fields that can be configured are described below:

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

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

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

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

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

Multicast Static FDB

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

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

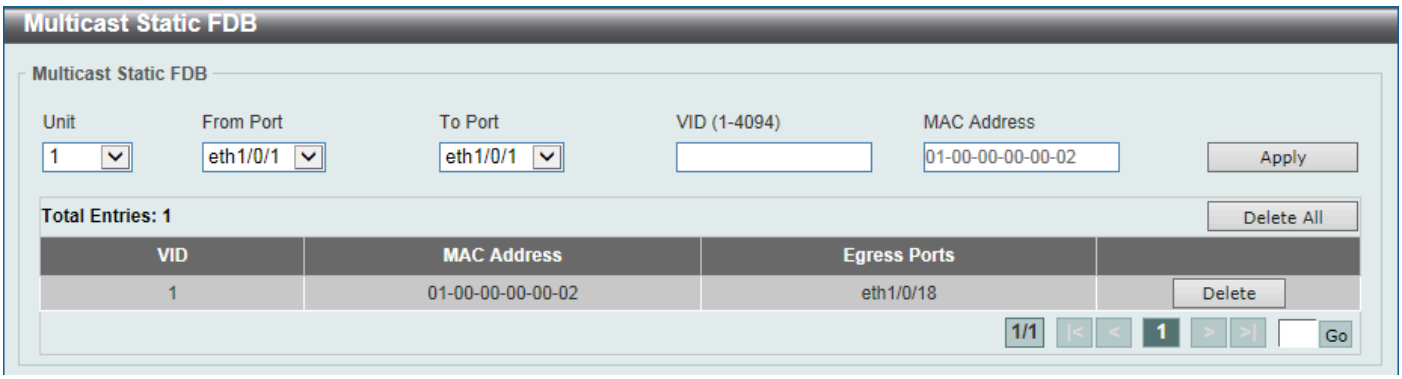


Figure 5-2 Multicast Static FDB Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the stacking unit ID of the Switch that will be configured here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration here.
VID	Enter the VLAN ID of the VLAN the corresponding MAC address belongs to.
MAC Address	Enter the static destination MAC address of the multicast packets. This must be a multicast MAC address. The format of the destination MAC address is: *x*1-*xx-xx-xx-xx-xx* *x*5-*xx-xx-xx-xx-xx* *x*9-*xx-xx-xx-xx-xx* *x*D-*xx-xx-xx-xx-xx* (where X is a hexadecimal character).

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

Click the **Delete All** button to remove all the entries.

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

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

MAC Address Table Settings

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

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

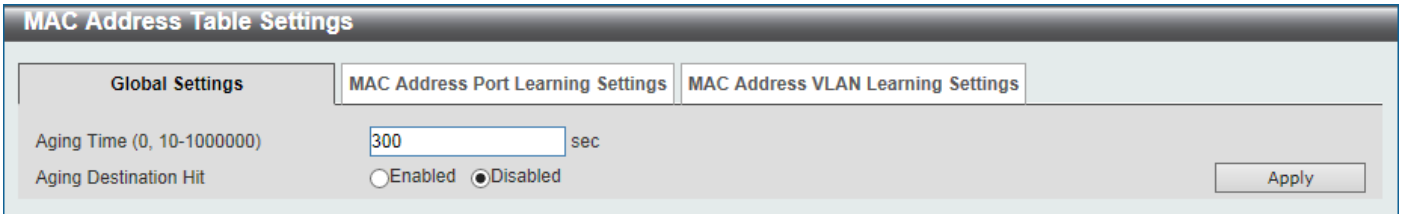


Figure 5-3 MAC Address Table Settings (Global Settings) Window

The fields that can be configured are described below:

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

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

After selecting the **MAC Address Port Learning Settings** tab option, at the top of the page, the following page will be available.

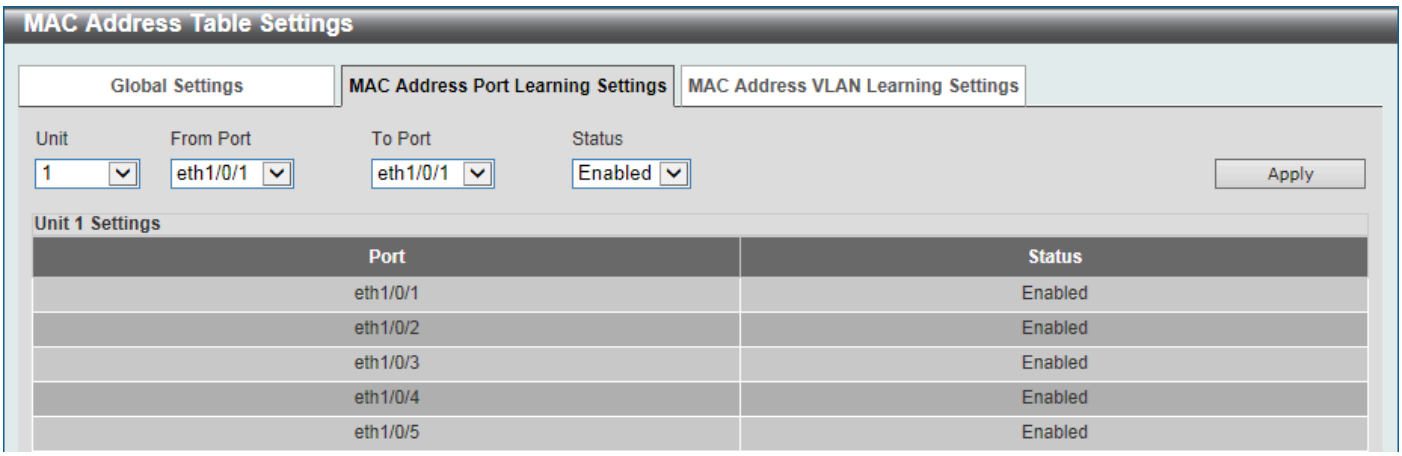


Figure 5-4 MAC Address Table Settings (MAC Address Port Learning Settings) Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the stacking unit ID of the Switch that will be configured here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Status	Select to enable or disable the MAC address learning function on the ports specified here.

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

After selecting the **MAC Address VLAN Learning Settings** tab option, at the top of the page, the following page will be available.

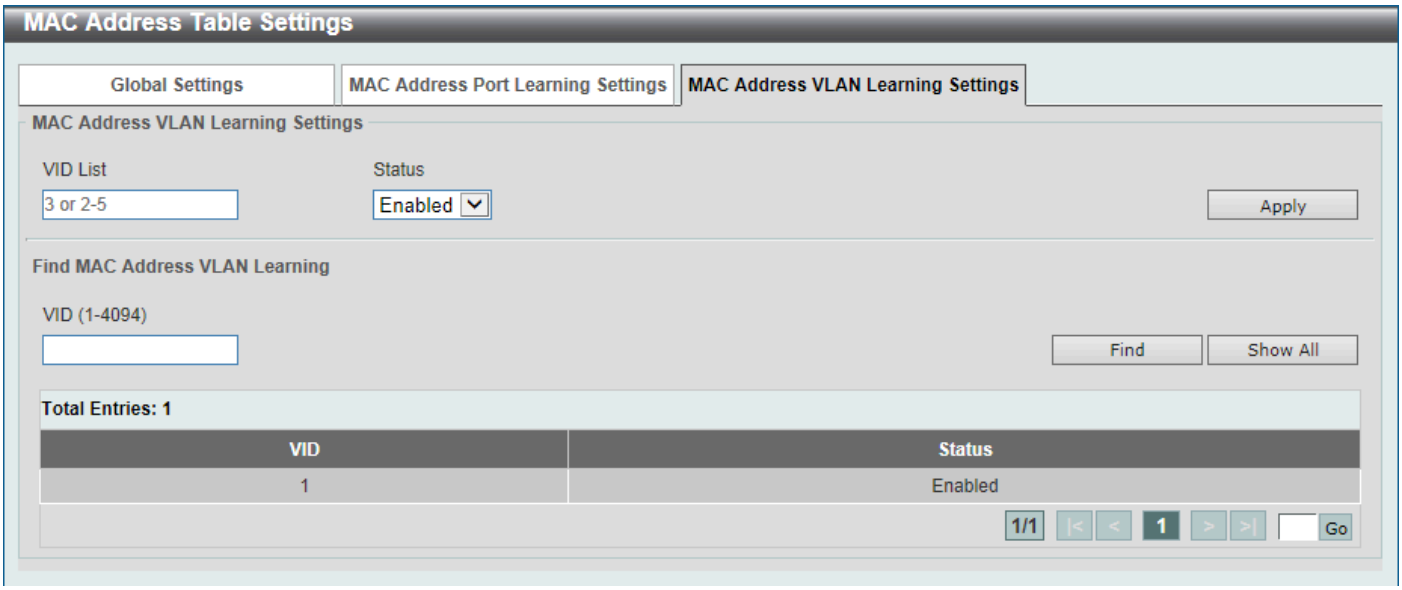


Figure 5-5 MAC Address Table Settings (MAC Address VLAN Learning Settings) Window

The fields that can be configured are described below:

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

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

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

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

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

MAC Address Table

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

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

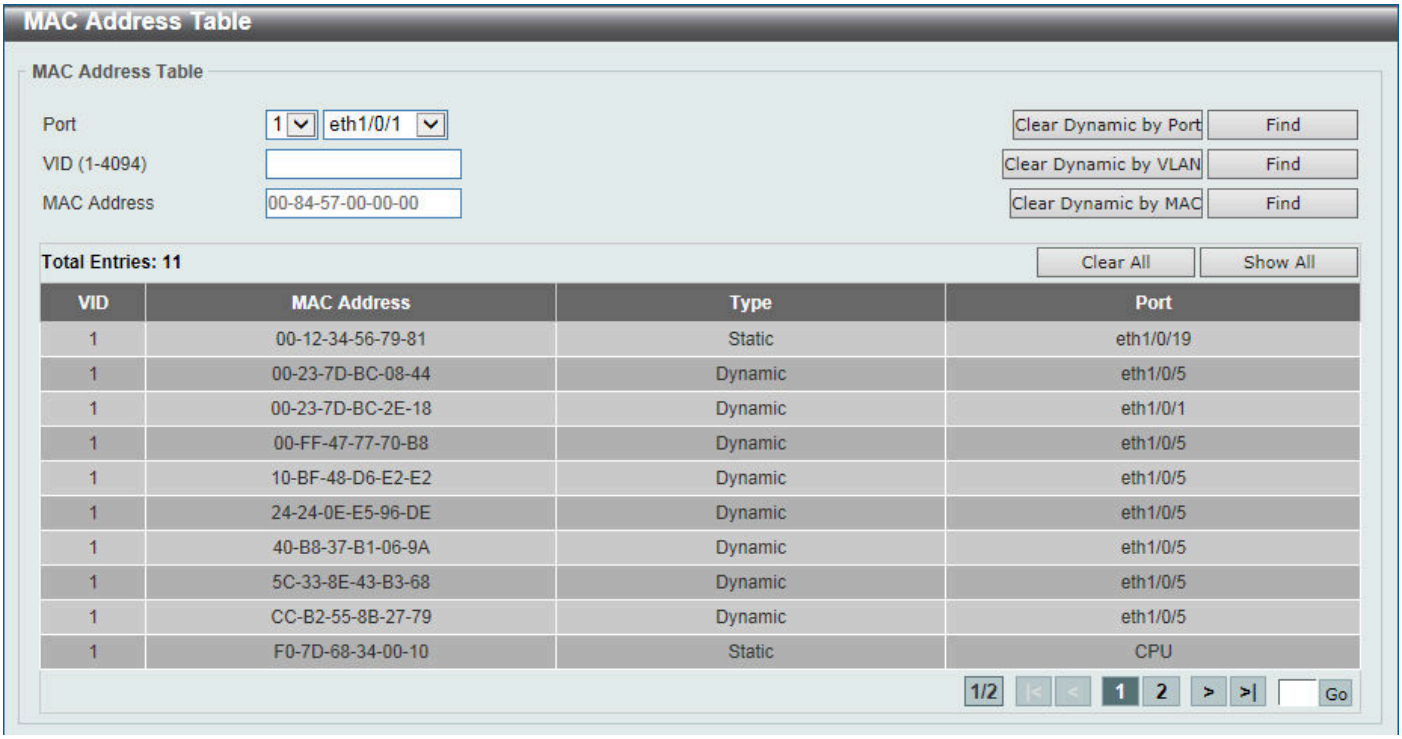


Figure 5-6 MAC Address Table Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the stacking unit ID and the port number of the Switch that will be configured here. The unit ID option is only available when stacking is enabled.
VID	Enter the VLAN ID that will be used for this configuration here.
MAC Address	Enter the MAC address that will be used for this configuration here.

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

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

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

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

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

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

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

MAC Notification

This window is used to display and configure MAC notification.

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

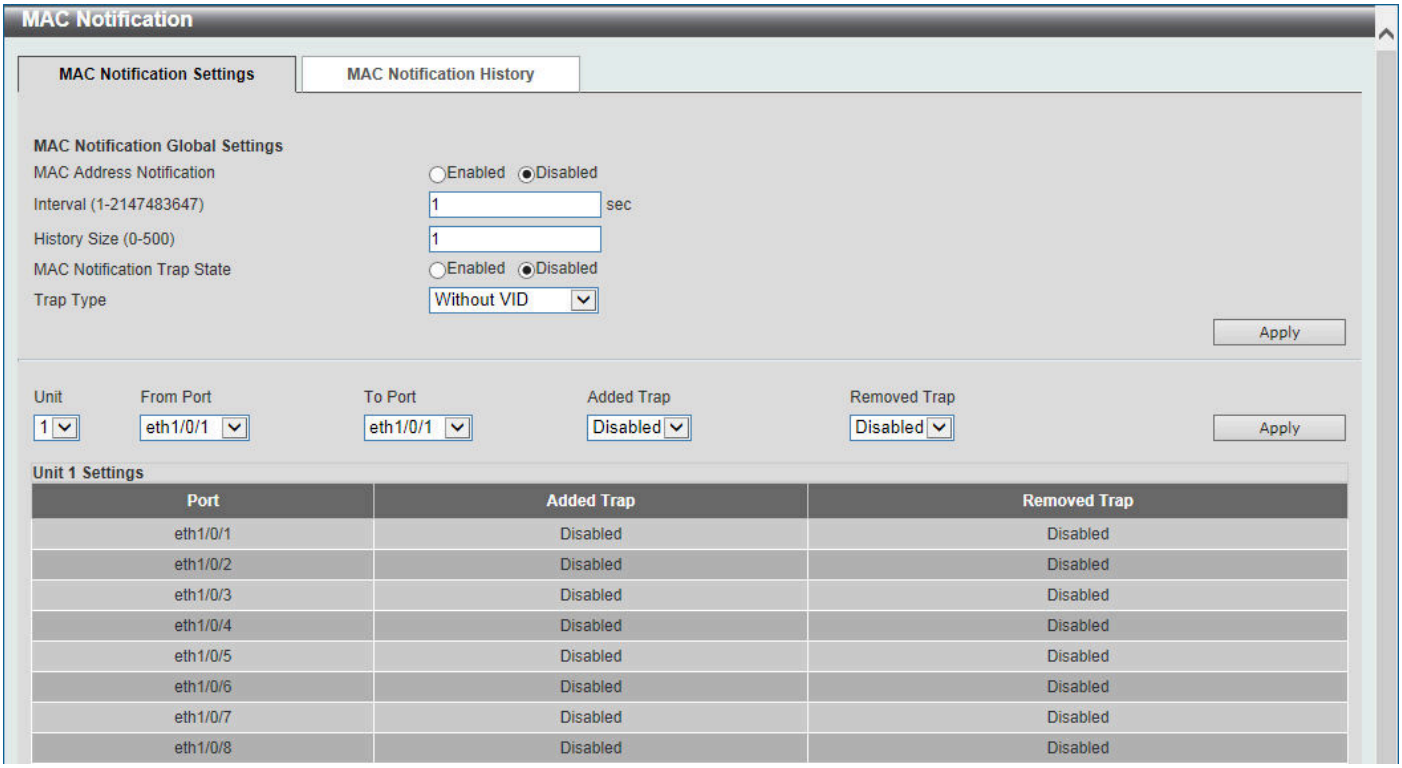


Figure 5-7 MAC Notification (MAC Notification Settings) Window

The fields that can be configured are described below:

Parameter	Description
MAC Address Notification	Select to enable or disable MAC notification globally on the Switch
Interval	Enter the time value between notifications. This value must be between 1 and 2147483647 seconds. By default, this value is 1 second.
History Size	Enter the maximum number of entries listed in the history log used for notification. This value must be between 0 and 500. By default, this value is 1. Refer to below **MAC Notification History**.
MAC Notification Trap State	Select to enable or disable the MAC notification trap state.
Trap Type	Select the trap type here. Options to choose from are: • **Without VID** - Specifies the trap information without the VLAN ID. • **With VID** - Specifies the trap information with the VLAN ID.
Unit	Select the stacking unit ID of the Switch that will be configured here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Added Trap	Select to enable or disable the added trap for the port(s) selected.
Removed Trap	Select to enable or disable the removed trap for the port(s) selected.

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

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

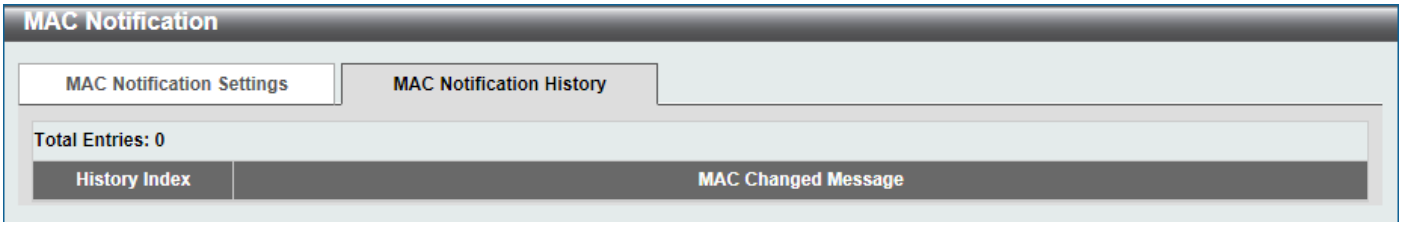


Figure 5-8 MAC Notification (MAC Notification History) Window

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

VLAN

VLAN Configuration Wizard

Use the following procedure to create a VLAN with the wizard:

1. Select **Create VLAN** to create a new VLAN or **Configure VLAN** to configure an existing VLAN. Then enter a **VID (1-4094)** for VLAN creation or configuration. Click **Next** to continue.
2. Enter a **VLAN name** for this VLAN. For each port, configure its VLAN type from one of the following:

   Tagged: a tagged member of the VLAN.

   Untagged: an untagged member of the VLAN.

   Not Member: not a member of this VLAN.

   Native VLAN (PVID): Whether this VLAN will be the port's native VLAN. If not, the default is VLAN 1.
3. Click **Apply** to save your settings. You can click **View Allowed VLAN** to view currently configured VLANs.

802.1Q VLAN

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

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

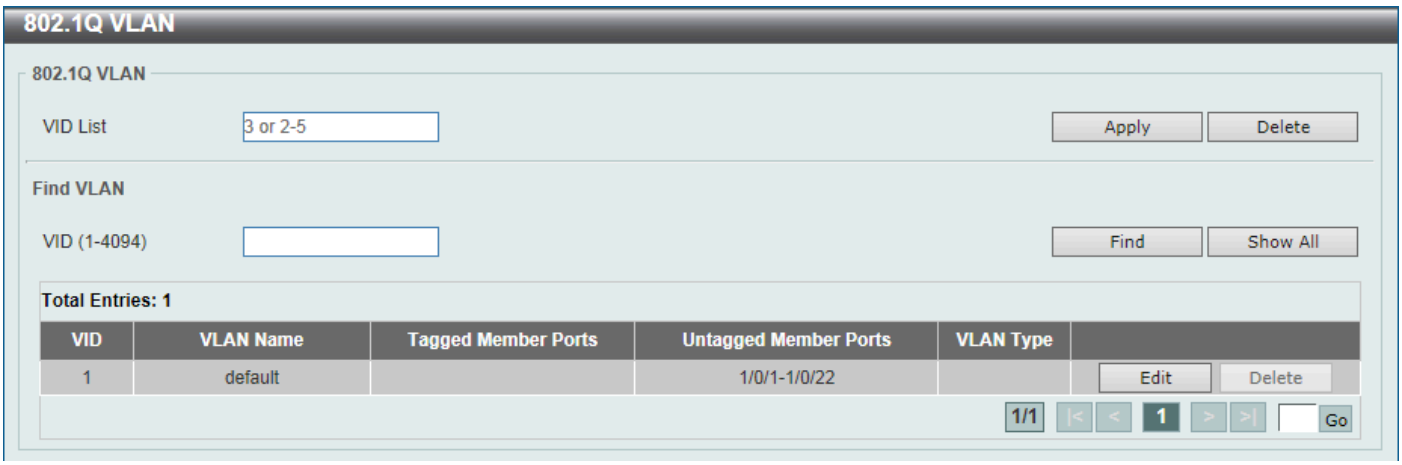


Figure 5-9 802.1Q VLAN Window

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

Parameter	Description
VID List	Enter the VLAN ID list that will be created here. Use "-" to specify a range of VIDs and "," to separate multiple VIDs. For example, 2,4-6.

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

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

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

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

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

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

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

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

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

VLAN Interface

The VLAN Interface tab allows you to view and configure existing VLANs. For each port, click **Show Detail** to display detailed information about the configured VLAN: VLAN Mode, Native VLAN, Hybrid Untagged/untagged VLAN, Dynamic tagged VLAN, Ingress Checking enabled/disabled, and Acceptable Frame Type. You can also click **Edit** to edit the current VLAN setting on each port.

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

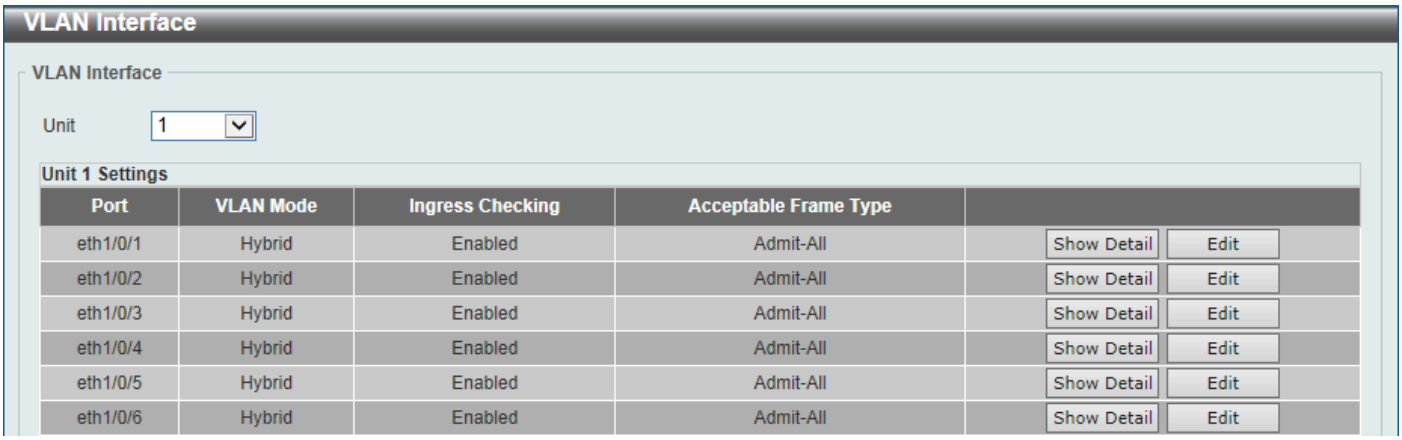


Figure 5-10 VLAN Interface Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.

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

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

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

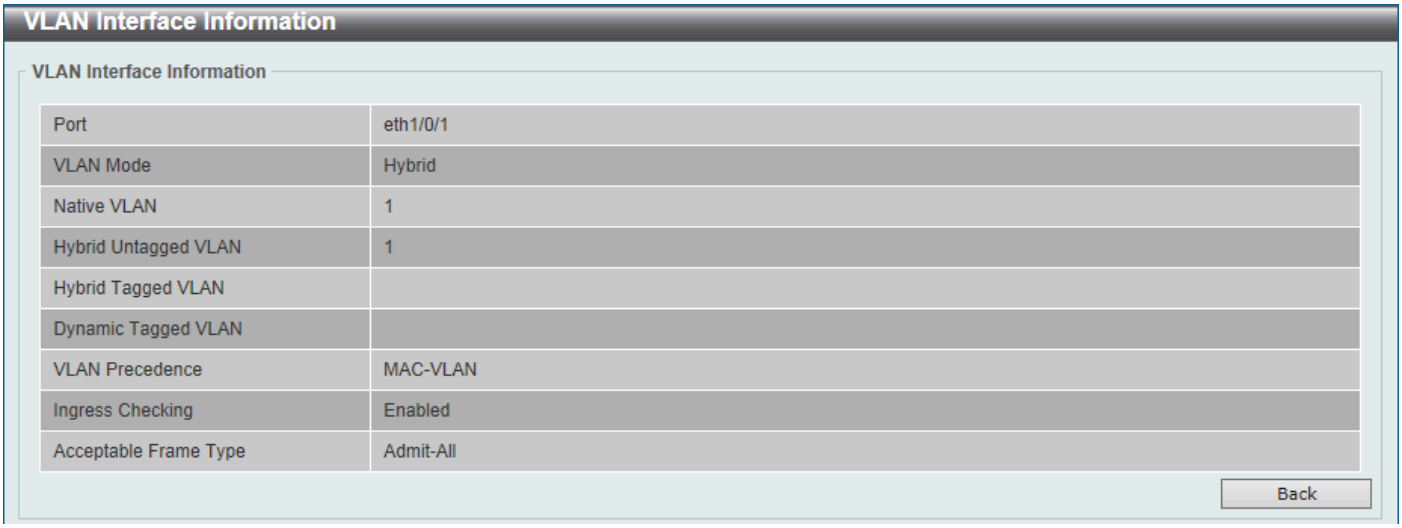


Figure 5-11 VLAN Interface (VLAN Detail) Window

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

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

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

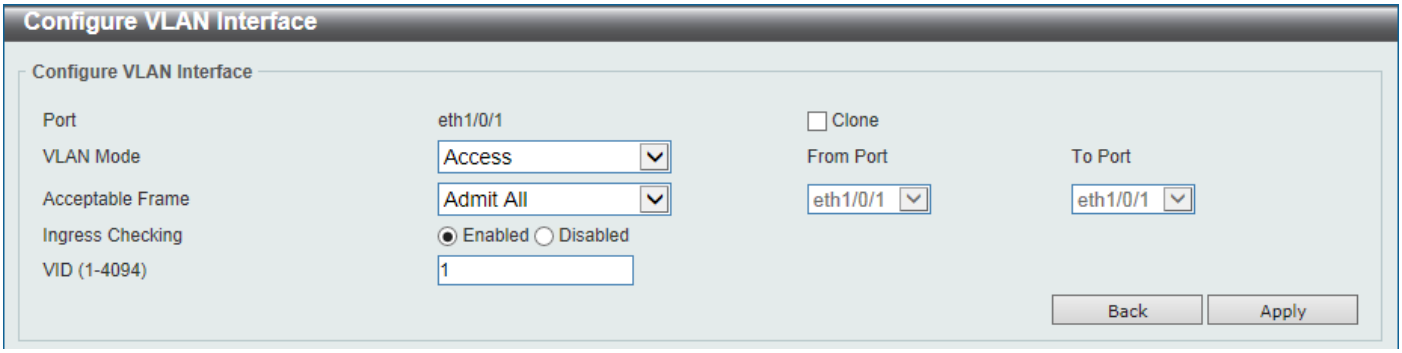


Figure 5-12 VLAN Interface (Access) Window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select one of the following VLAN mode: **Hybrid, Access, Trunk, 802.1Q-Tunnel, Promiscuous,** or **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 whether the frames should be checked for its acceptance when entering the port.
VID	Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.
Clone	Select this option to clone the configured information to the selected ports. Specify the **From Port** and **To Port** for the port range.

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

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

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

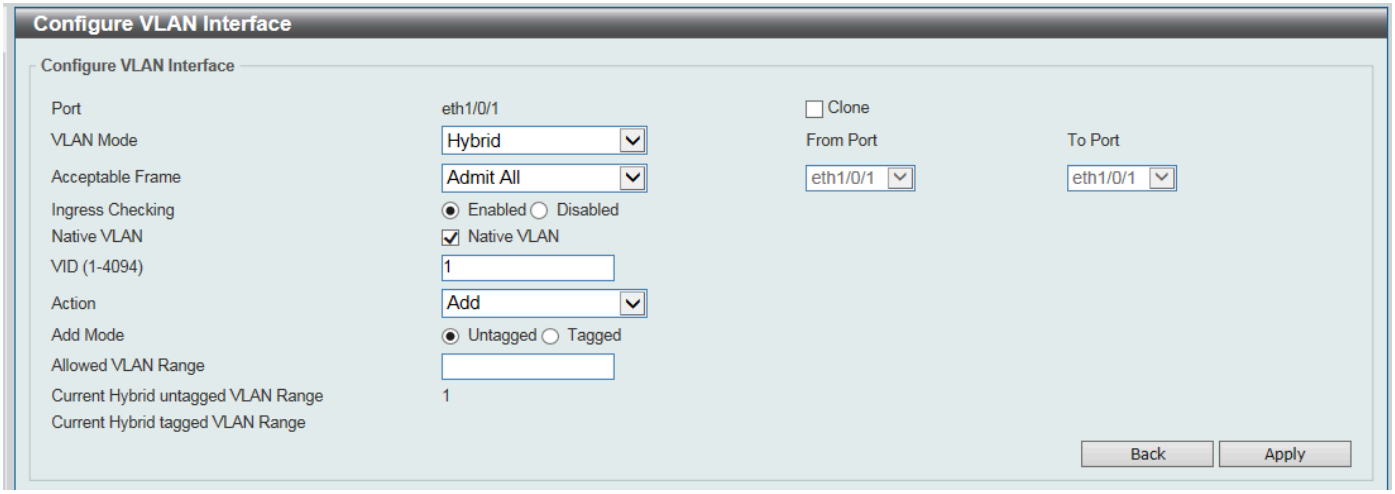


Figure 5-13 VLAN Interface (Hybrid) Window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select one of the following VLAN mode: **Hybrid, Access, Trunk, 802.1Q-Tunnel, Promiscuous,** or **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 whether the frames should be checked for its acceptance when entering the port.
Native VLAN	Tick this option to enable the native VLAN function.
VID	After ticking the **Native VLAN** option the following parameter will be available. Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.
Action	Select how the frames should be processed for this VLAN: **Add**, **Remove**, **Tagged** or **Untagged**. For **Add**, enter the VLAN range to add the port to and specify whether it is tagged or untagged. For **Remove**, enter the VLAN range to remove the port from this VLAN. For **Tagged** or Untagged, enter the VLAN range in **Allowed VLAN Range** with which the port should be an untagged or tagged VLAN member.
Clone	Select this option to clone the configured information to the selected ports. Specify the **From Port** and **To Port** for the port range.

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

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

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

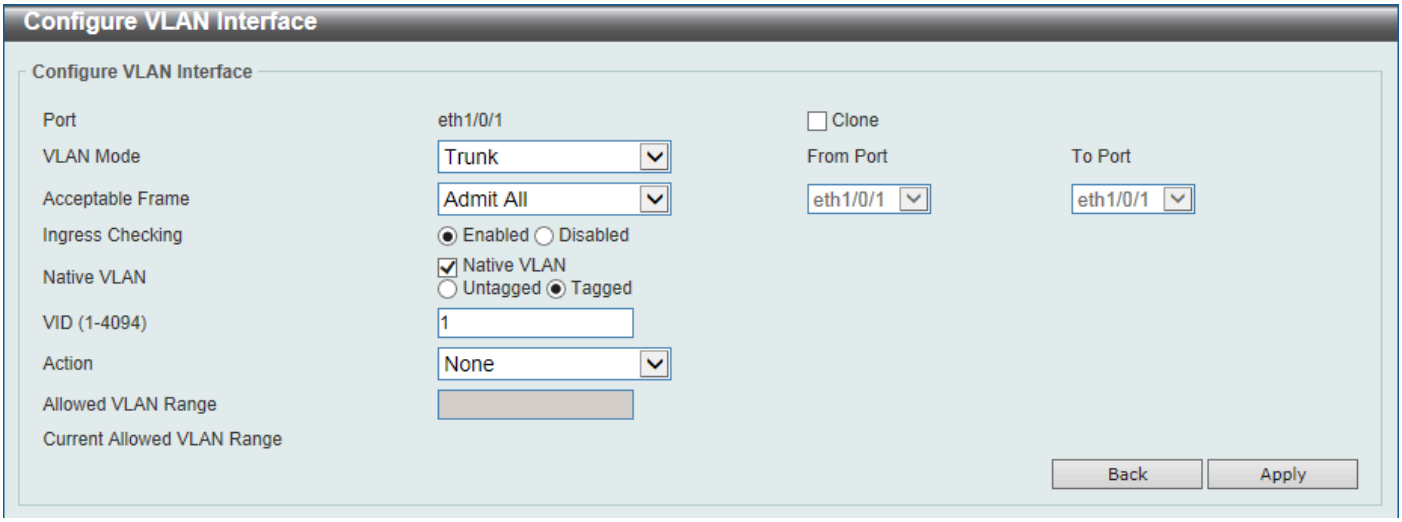


Figure 5-14 VLAN Interface (Trunk) Window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select one of the following VLAN mode: **Hybrid, Access, Trunk, 802.1Q-Tunnel, Promiscuous,** or **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 whether the frames should be checked for its acceptance when entering the port.
Native VLAN	Tick this option to enable the native VLAN function. Also select if this VLAN supports **Untagged** or **Tagged** frames.
VID	After ticking the **Native VLAN** option the following parameter will be available. Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.
Action	Select how the frames should be processed for this VLAN: **None**, **All, Add**, **Remove**, **Except, Replace**. For **Add, Remove, Except,** and **Replace**, enter the VLAN range in **Allowed VLAN Range** to perform the selected operation.
Clone	Select this option to clone the configured information to the selected ports. Specify the **From Port** and **To Port** for the port range.

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

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

When **802.1Q-Tunnel** was selected as the **VLAN Mode**, the following page will appear.

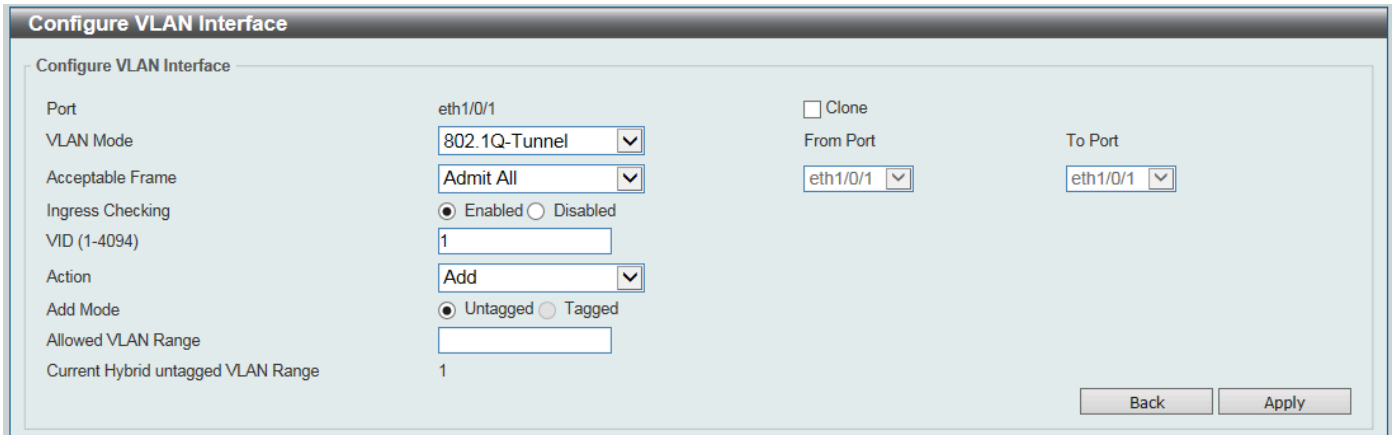


Figure 5-15 VLAN Interface (802.1Q-Tunnel) Window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are **Access, Hybrid, Trunk, 802.1Q-Tunnel, Promiscuous, Host, Trunk Promiscuous**, and **Trunk Secondary.**
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are **Tagged Only, Untagged Only**, and **Admit All**.
Ingress Checking	Select whether the frames should be checked for its acceptance when entering the port.
VID	Enter the VLAN ID used for this configuration here. This value must be between 1 and 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. If Add is selected, enter the VLAN range in **Allowed VLAN Range** to add the port to and specify whether it is tagged or untagged member of the VLAN.
Clone	Select this option to clone the configured information to the selected ports. Specify the **From Port** and **To Port** for the port range.

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

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

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

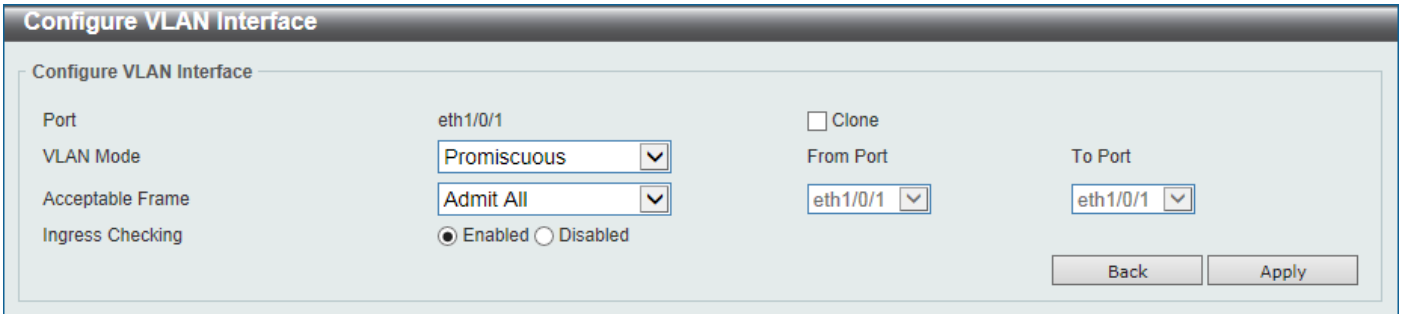


Figure 5-16 VLAN Interface (Promiscuous) Window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select one of the following VLAN mode: **Hybrid, Access, Trunk, 802.1Q-Tunnel, Promiscuous,** or **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 whether the frames should be checked for its acceptance when entering the port.
Clone	Select this option to clone the configured information to the selected ports. Specify the **From Port** and **To Port** for the port range.

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

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

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

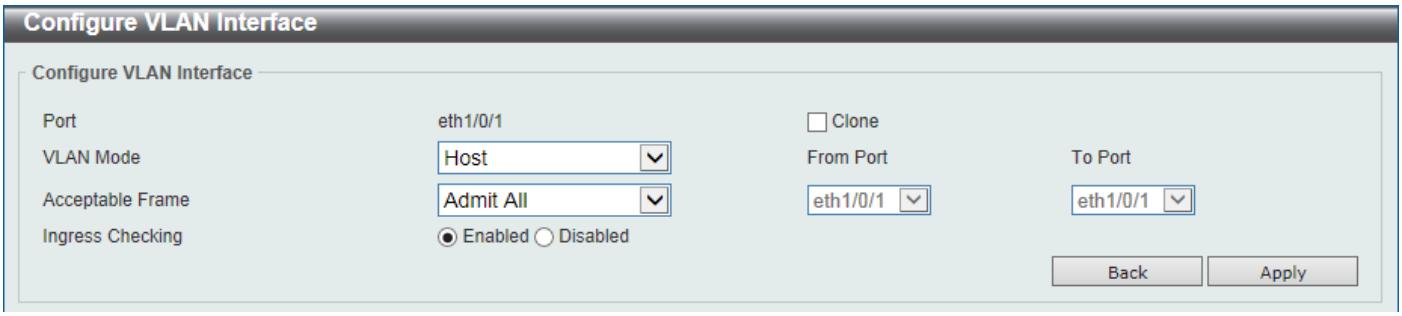


Figure 5-17 VLAN Interface (Host) Window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select one of the following VLAN mode: **Hybrid, Access, Trunk, 802.1Q-Tunnel, Promiscuous,** or **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 whether the frames should be checked for its acceptance when entering the port.
Clone	Select this option to clone the configured information to the selected ports. Specify the **From Port** and **To Port** for the port range.

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

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

After saving your changes, you may click the **Port Summary** tab to view your current VLAN configurations listed by ports.

802.1v Protocol VLAN

Protocol VLAN Profile

This window is used to display and configure 802.1v protocol VLAN profiles. The 802.1v Protocol VLAN group settings support multiple VLANs for each protocol and allow the user to configure untagged ports of different protocols on the

same physical port. For example, it allows the user to configure an 802.1Q and 802.1v untagged port on the same physical port.

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

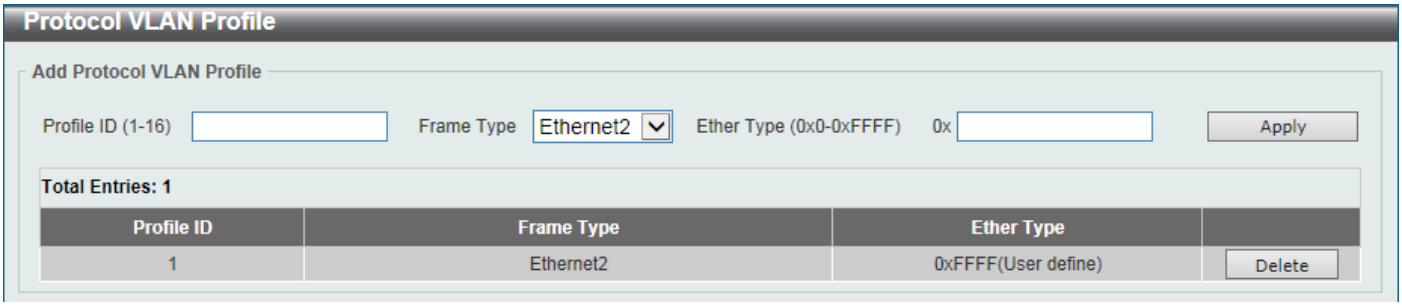


Figure 5-18 Protocol VLAN Profile Window

The fields that can be configured are described below:

Parameter	Description
Profile ID	Enter the 802.1v protocol VLAN profile ID here. This value must be between 1 and 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**.
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 of values are 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 Service Access Point (LSAP) pair. The first octet is for Destination Service Access Point (DSAP) and the second octet is for Source.

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

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

Protocol VLAN Profile Interface

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

To view the following window, click **L2 Features > VLAN > 802.1v Protocol VLAN > Protocol VLAN Profile Interface**, as shown below:

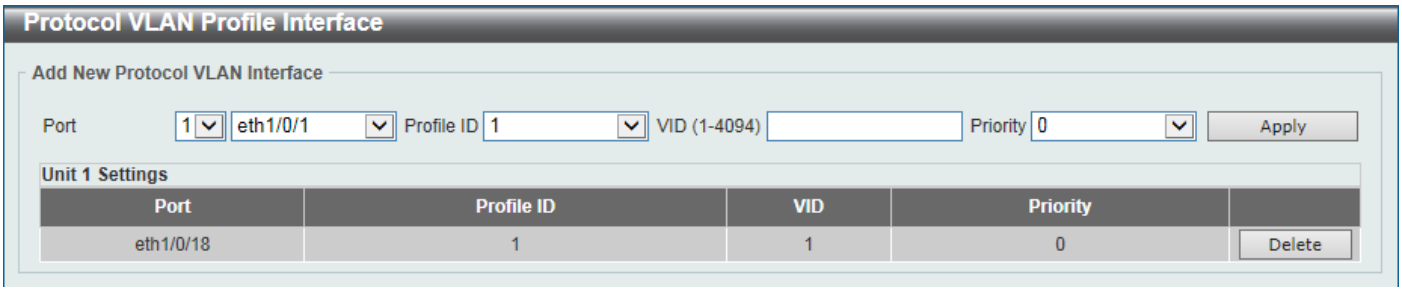


Figure 5-19 Protocol VLAN Profile Interface Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the stacking unit ID and the port number of the Switch that will be configured here. This option is only available when stacking is enabled.
Profile ID	Select the 802.1v protocol VLAN profile ID here.
VID	Enter the VLAN ID (1-4094) used here.
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 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 accept the changes made.

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

GVRP

GVRP Global

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

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



Figure 5-20 GVRP Global Window

The fields that can be configured are described below:

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

Parameter	Description
Dynamic VLAN Creation	Select to enable or disable the dynamic VLAN creation function here.
NNI BPDU Address	Select the NNI BPDU address option here. This option is used to determine the BPDU protocol address for GVRP in customer networks. It can use 802.1d GVRP address or 802.1ad service provider GVRP address. Options to choose from are Dot1d and Dot1ad.

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

GVRP Port

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

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

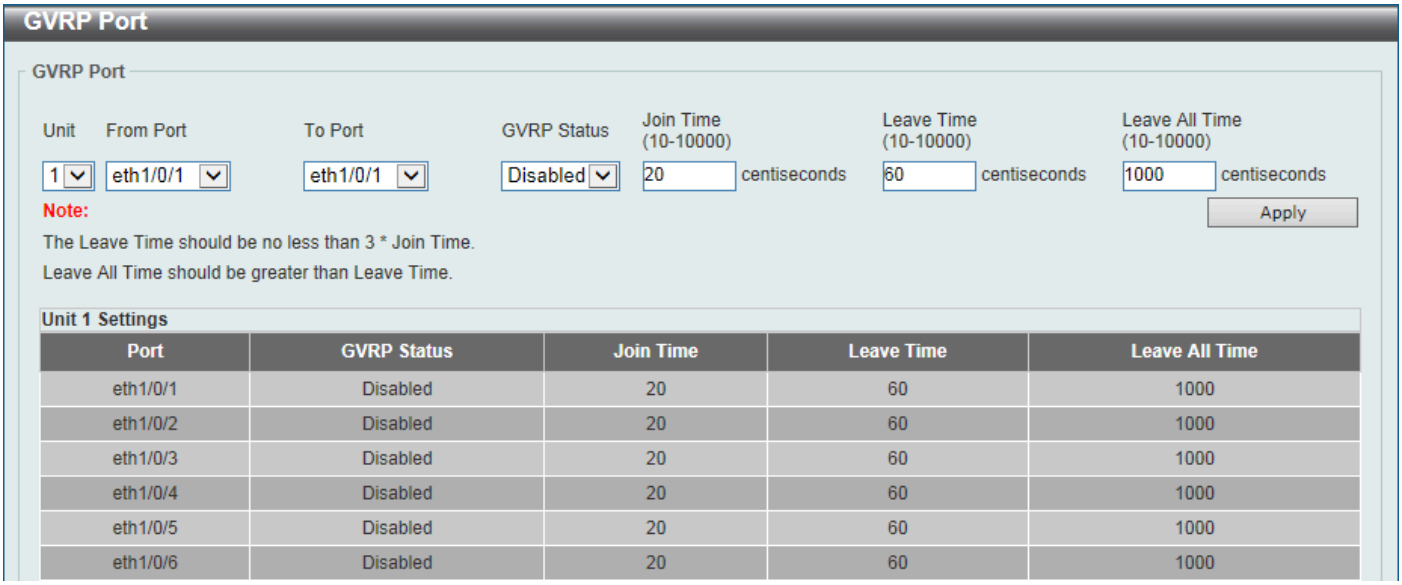


Figure 5-21 GVRP Port Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the range osf ports that will be used for this configuration here.
GVRP Status	Select the enable or disable the GVRP port status. This enables the port to dynamically become a member of a VLAN. By default, this option is disabled.
Join Time	Enter the Join Time value in centiseconds (0.01 second). This value must be between 10 and 10000 centiseconds. By default, this value is 20 centiseconds.
Leave Time	Enter the Leave Time value in centiseconds (0.01 second). This value must be between 10 and 10000 centiseconds. By default, this value is 60 centiseconds.
Leave All Time	Enter the Leave All Time value in centiseconds. This value must be between 10 and 10000 centiseconds. By default, this value is 1000 centiseconds.

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

GVRP Advertise VLAN

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

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

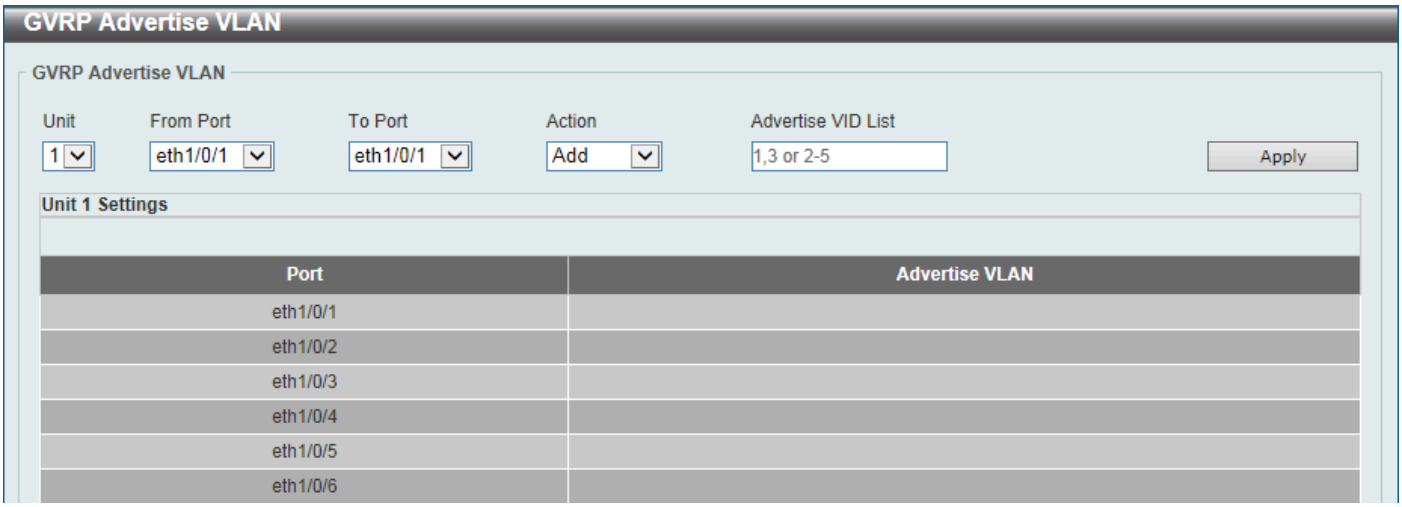


Figure 5-22 GVRP Advertise VLAN Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration 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 advertised VLAN ID list here.

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

GVRP Forbidden VLAN

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

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

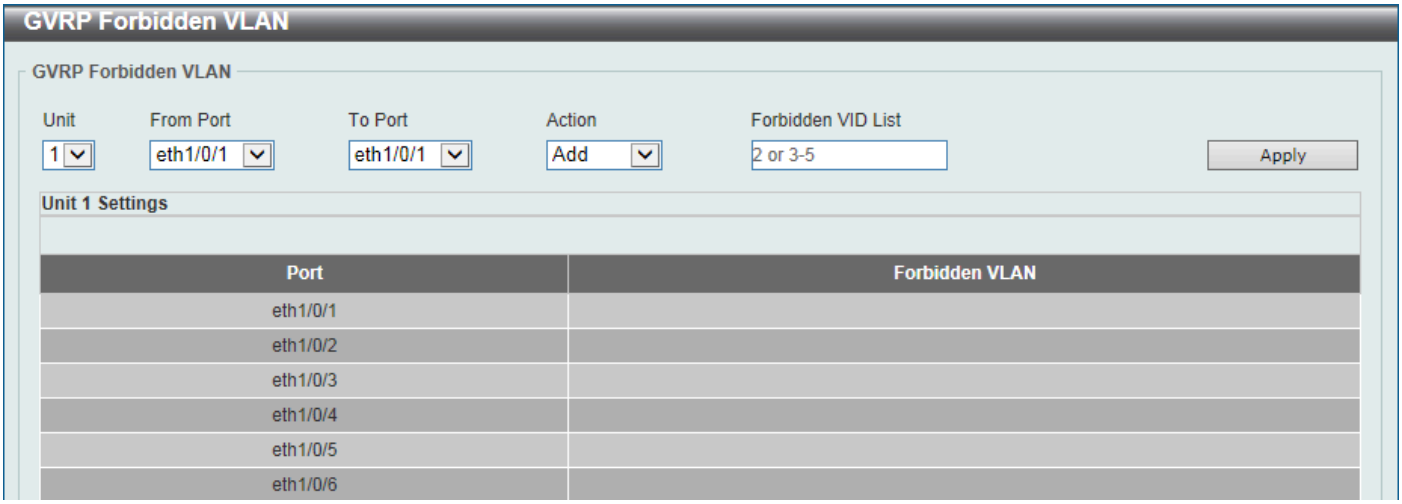


Figure 5-23 GVRP Forbidden VLAN Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Action	Select the forbidden VLAN to port mapping action that will be taken here. Options to choose from are **All, Add**, and **Remove** and **Replace**. When selecting **All**, all the forbidden VLANs will be used.
Forbidden VID List	Enter the forbidden VLAN ID list here.

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

GVRP Statistics Table

This window is used to view GVRP statistics information.

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

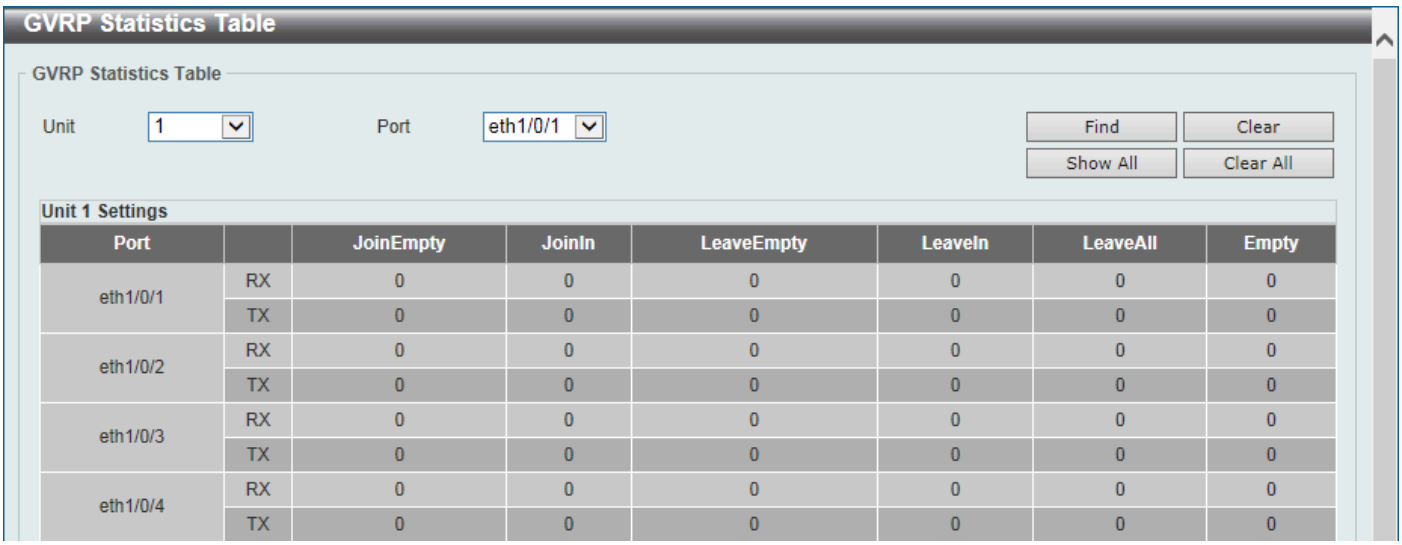


Figure 5-24 GVRP Statistics Table Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit to be displayed here. This option is only available when stacking is enabled.
Port	Select the port number to display GVRP statistic information.

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

Click the **Clear** button to clear all the information for the specific port.

Click the **Show All** button to view all GVRP statistic information.

Click the **Clear All** button to clear all the information in this table.

Asymmetric VLAN

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

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

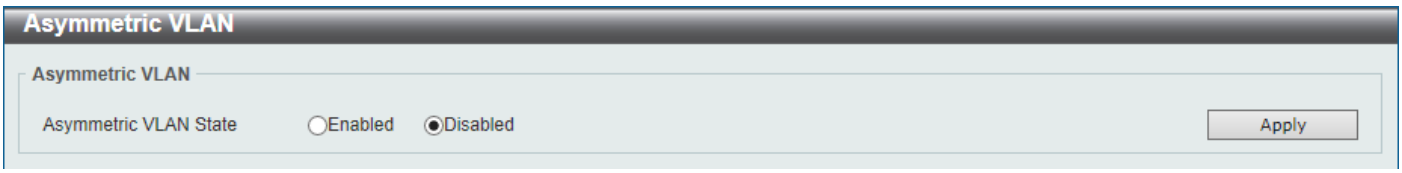


Figure 5-25 Asymmetric VLAN Window

The fields that can be configured are described below:

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

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

MAC VLAN

This window is used to display and configure the MAC-based VLAN information. When a static MAC-based VLAN entry is configured, the VLAN operating on the port will be changed.

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

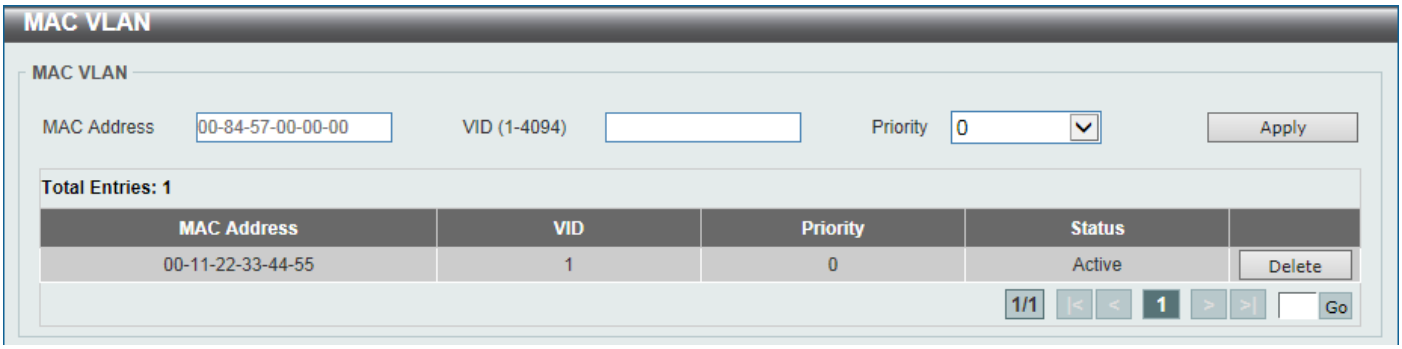


Figure 5-26 MAC VLAN Window

The fields that can be configured are described below:

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

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

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

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

Super VLAN

This window is used to display and configure the super VLAN settings. This is used to specify a VLAN as a super VLAN. Super VLANs are used to aggregate multiple sub-VLANs (Layer 2 broadcast domains) into an IP subnet. A super VLAN cannot have any physical member port. A super VLAN cannot be a sub-VLAN at the same time. Once an IP interface is bound to a super VLAN, the proxy ARP will be enabled automatically on the interface for communication between its sub-VLANs. Multiple super VLANs can be configured and each super VLAN can consist of multiple sub-VLANs.

Private VLAN and super VLAN are mutually exclusive. A private VLAN cannot be configured as a super VLAN. Layer 3 routing protocols, multicast protocols, and the IPv6 protocol cannot run on a super VLAN interface.

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

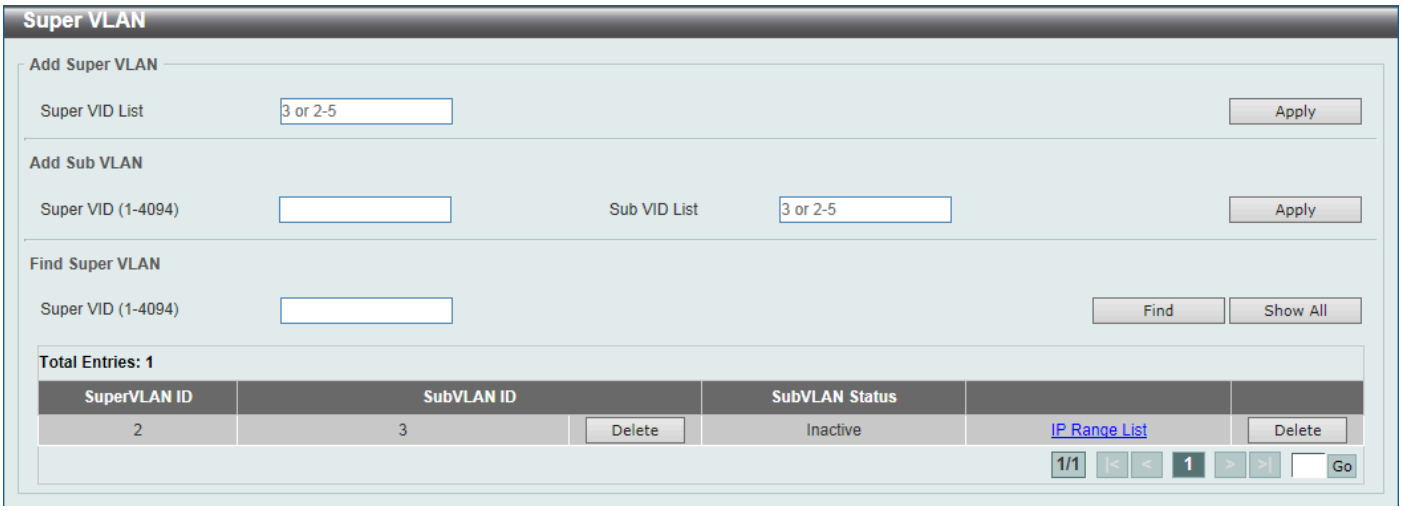


Figure 5-27 Super VLAN Window

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

Parameter	Description
Super VID List	Enter the super VLAN ID(s) that will be created here.

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

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

Parameter	Description
Super VID	Enter the super VLAN ID that will be associated with the sub-VLAN(s) here. The range is from 1 to 4094.

Parameter	Description
Sub VID List	Enter the sub-VLAN ID(s) that will be associated with the super VLAN here.

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

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

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

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

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

Click the **Delete** button to remove the specific entry or to remove the sub-VLAN from the super VLAN.

Click the IP Range List link to add an IP range to the sub-VLAN.

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

After clicking the IP Range List link, the following page will be available.

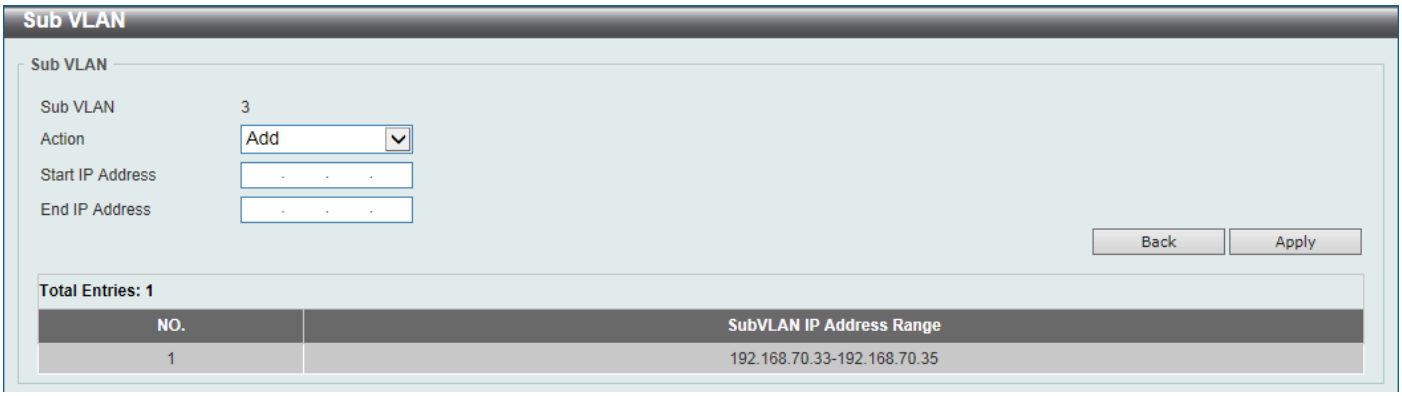


Figure 5-28 Super VLAN (IP Range List) Window

The fields that can be configured are described below:

Parameter	Description
Action	Select the action that will be taken here. Options to choose from are **Add** and **Remove**.
Start IP Address	Enter the starting IP address in the range of this sub-VLAN here.
End IP Address	Enter the ending IP address in the range of this sub-VLAN here.

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

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

Auto Surveillance VLAN

Auto Surveillance Properties

The Auto Surveillance VLAN can group surveillance devices into a VLAN. This window is used to display and configure the auto surveillance VLAN properties.To view the following window, click **L2 Features > VLAN > Auto Surveillance VLAN > Auto Surveillance Properties**, as shown below:

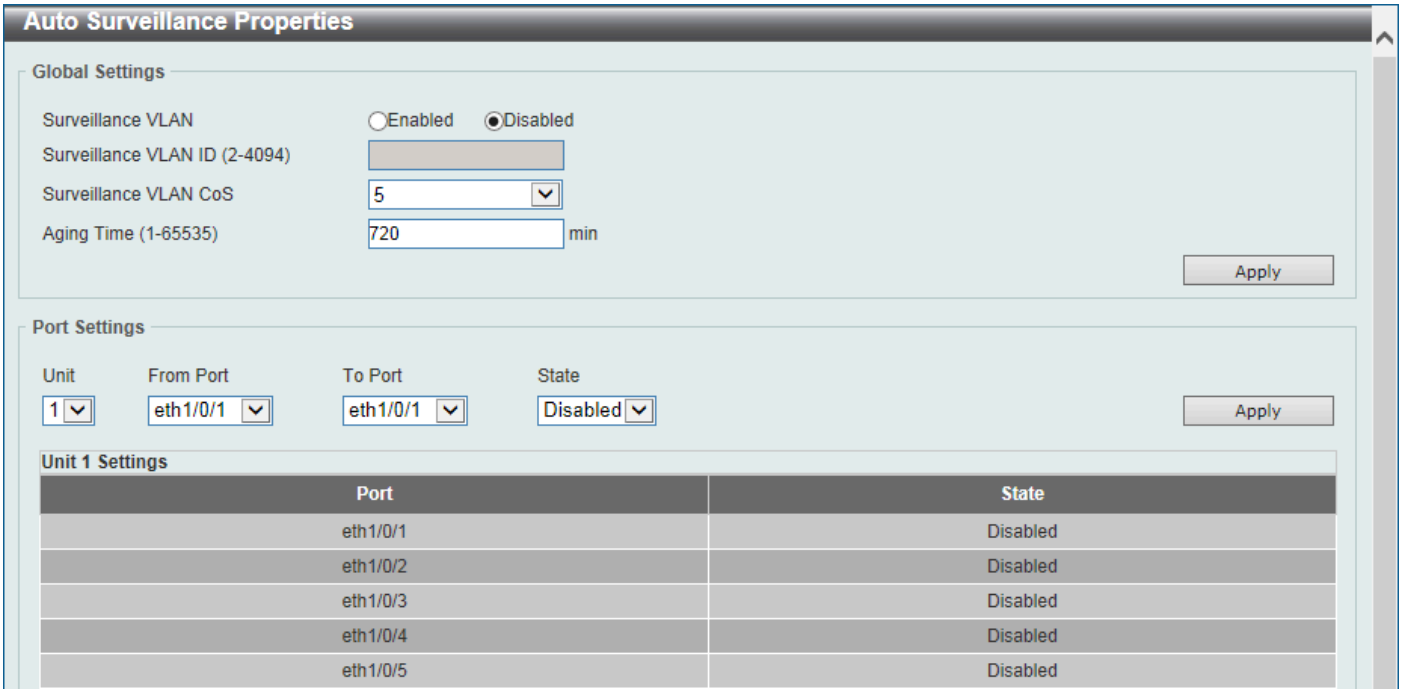


Figure 5-29 Auto Surveillance Properties Window

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

Parameter	Description
Surveillance VLAN	Select to enable or disable the surveillance VLAN feature here.
Surveillance VLAN ID	Enter the VLAN ID of the surveillance VLAN here. The range is from 2 to 4094. A normal VLAN needs to be created before assigning the VLAN as a surveillance VLAN.
Surveillance VLAN CoS	Enter the Class of Service (CoS) value for the surveillance VLAN here. The surveillance packets arriving at the surveillance VLAN enabled port are marked with the CoS specified here. The remarking of CoS allows the surveillance VLAN traffic to be distinguished from data traffic in quality of service. The range is from 0 to 7.
Aging Time	Enter the aging time value here. This is used to configure the aging time for aging out the surveillance VLAN dynamic member ports. The range is from 1 to 65535 minutes. When the last surveillance device connected to the port stops sending traffic and the MAC address of this surveillance device is aged out, the surveillance VLAN aging timer will be started. The port will be removed from the surveillance VLAN after expiration of surveillance VLAN aging timer. If the surveillance traffic resumes during the aging time, the aging timer will be cancelled.

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

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

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

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

MAC Settings and Surveillance Device

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

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

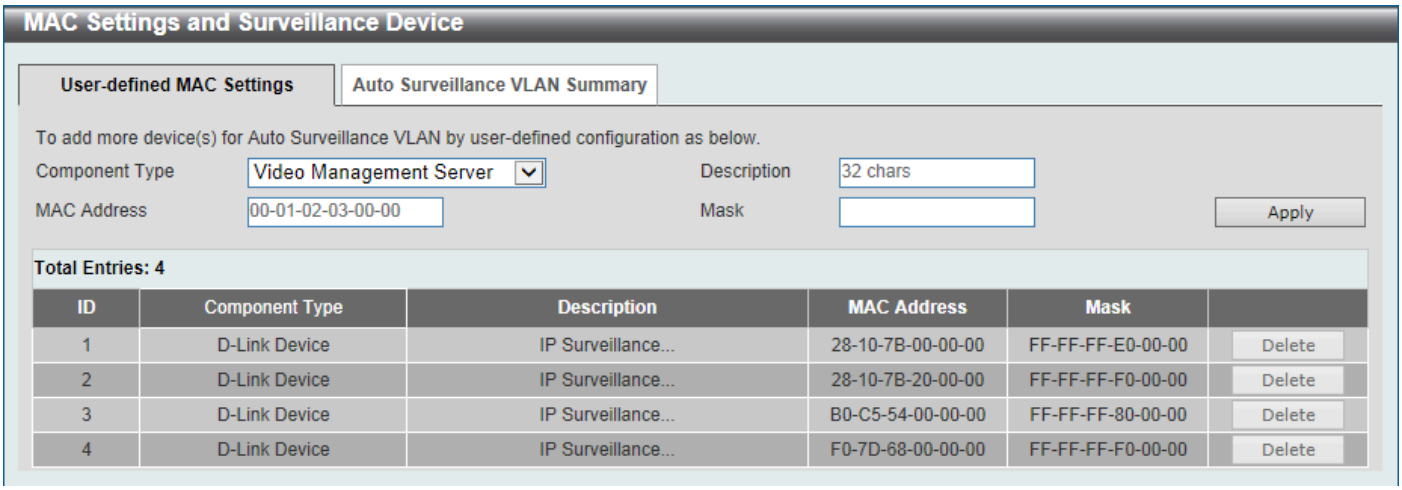


Figure 5-30 MAC Settings and Surveillance Device Window

The fields that can be configured are described below:

Parameter	Description
Component Type	Select the component type here. Option to choose from are: • **Video Management server** - Specifies the surveillance device type as Video Management Server (VMS). • **VMS Client/Remote Viewer** - Specifies the surveillance device type as VMS client. • **Video Encoder** - Specifies the surveillance device type as Video Encoder. • **Network Storage** - Specifies the surveillance device type as Network Storage. • **Other IP Surveillance Device** - Specifies the surveillance device type as other IP Surveillance Devices.
Description	Enter the description for the user-defined OUI here. This string can be up to 32 characters long.

Parameter	Description
MAC Address	Enter the OUI MAC address here. If the source MAC addresses of the received packet matches any of the OUI pattern, the received packet is determined as a surveillance packet.
Mask	Enter the matching bitmask for the OUI MAC address here.

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

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

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

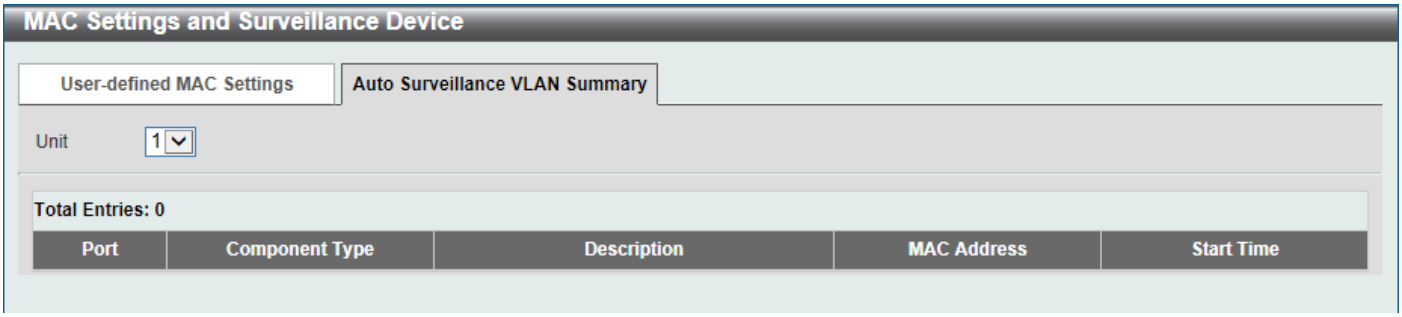


Figure 5-10 MAC Settings and Surveillance Device (Auto Surveillance VLAN Summary) Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the stacking unit ID of the Switch that will be used in this display here.

Voice VLAN

Voice VLAN Global

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

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

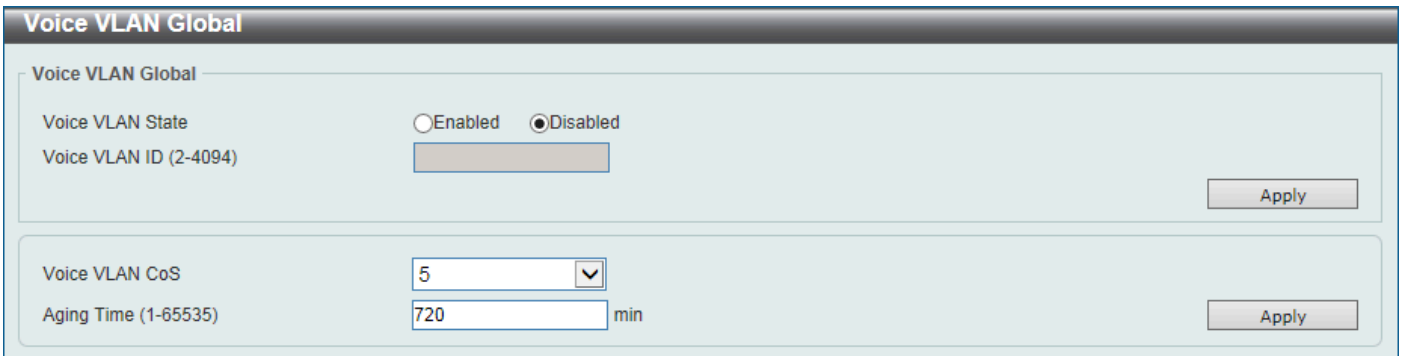


Figure 5-32 Voice VLAN Global Window

The fields that can be configured are described below:

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

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

Voice VLAN Port

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

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

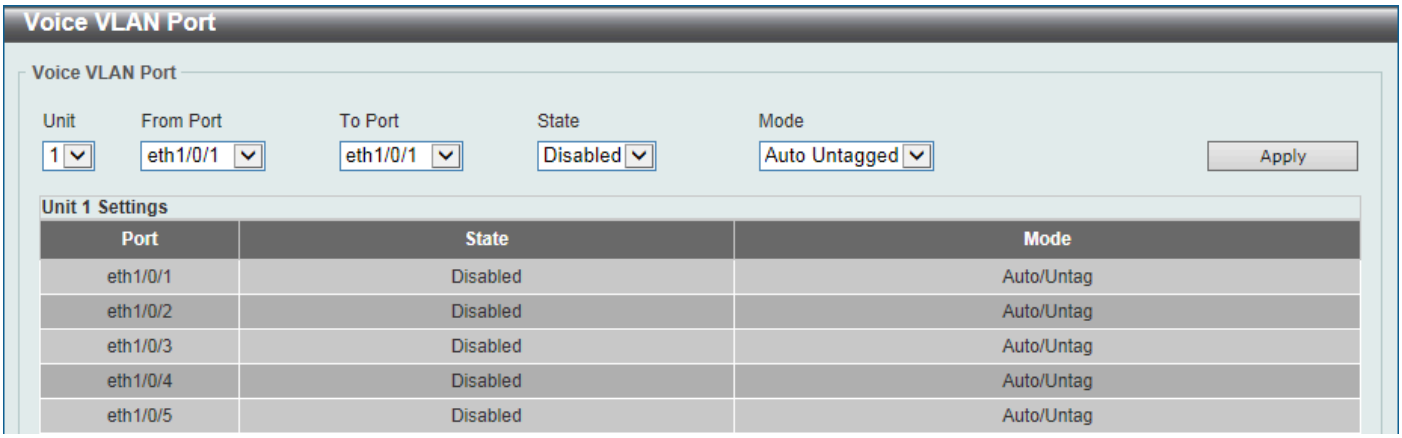


Figure 5-33 Voice VLAN Port Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration here.
State	Select to enable or disable the voice VLAN feature on the specified port(s) here. When the voice VLAN is enabled for a port, the received voice packets will be forwarded in the voice VLAN. The received packets are determined as voice packets if the source MAC addresses of packets complies with the OUI addresses.

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 device through the device's OUI, it will join the voice VLAN as a tagged member automatically. When the voice device sends tagged packets, the Switch will change its priority. When the voice device sends untagged packets, it will forward them in the Port VLAN ID (PVID). When the port is working in auto-untagged mode, and the port captures a voice device through the device's OUI, it will join the voice VLAN as an untagged member automatically. When the voice device sends tagged packets, the Switch will change its priority. When the voice device sends untagged packets, it will forward them in the voice VLAN. When the Switch receives LLDP-MED packets, it checks the VLAN ID, tagged flag, and priority flag. The Switch should follow the tagged flag and priority setting.

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

Voice VLAN OUI

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

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

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

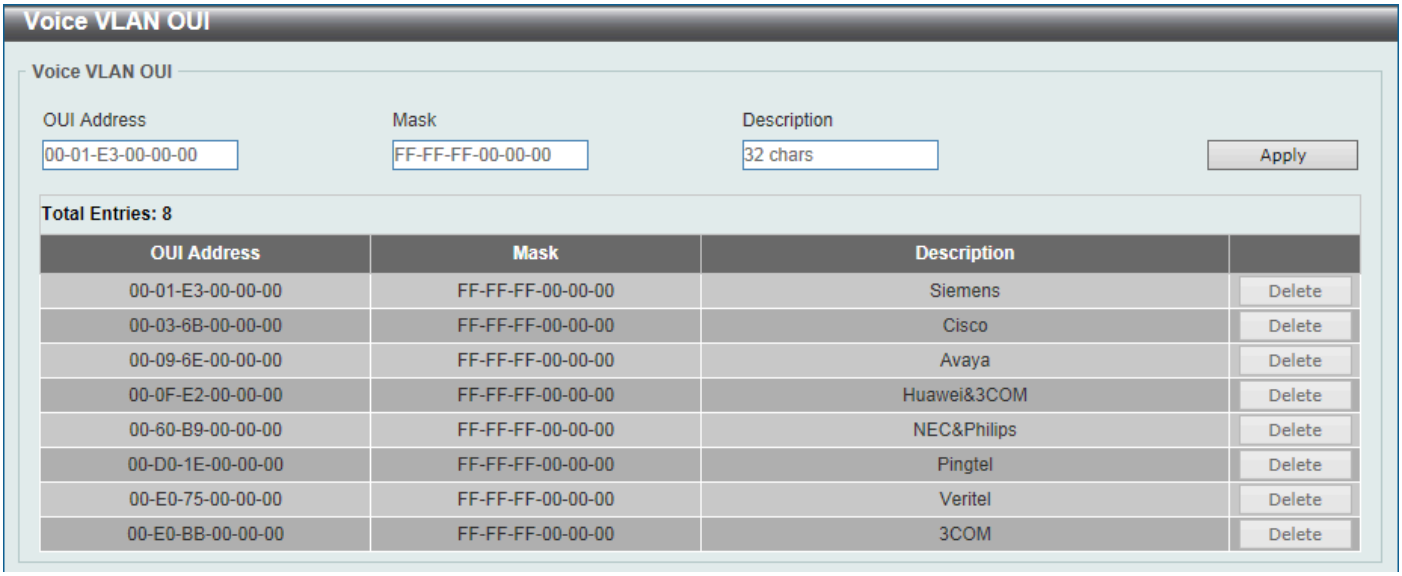


Figure 5-34 Voice VLAN OUI Window

The fields that can be configured are described below:

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

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

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

Voice VLAN Device

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

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

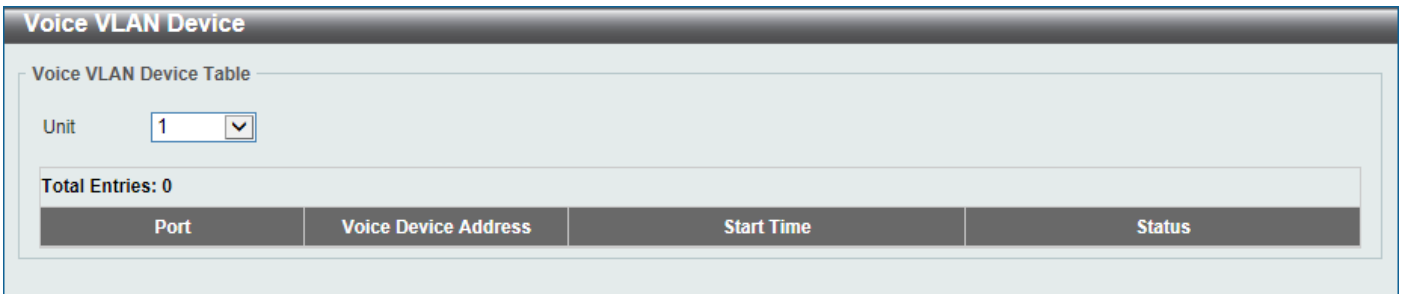


Figure 5-35 Voice VLAN Device Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used in this display here. This option is only available when stacking is enabled.

Voice VLAN LLDP-MED Device

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

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

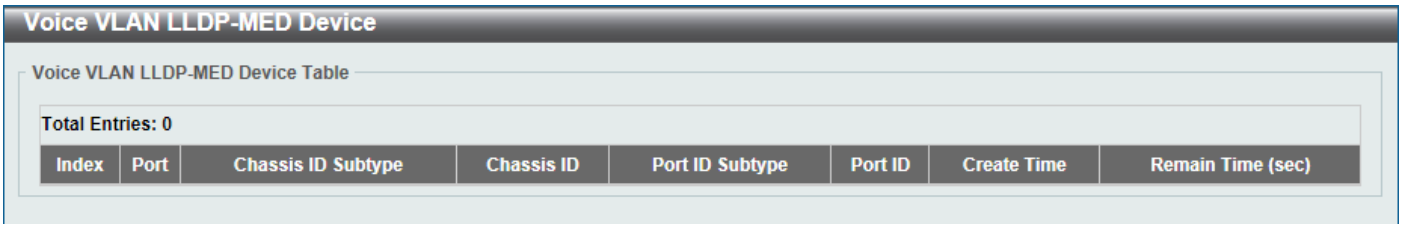


Figure 5-36 Voice VLAN LLDP-MED Device Window

Private VLAN

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

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

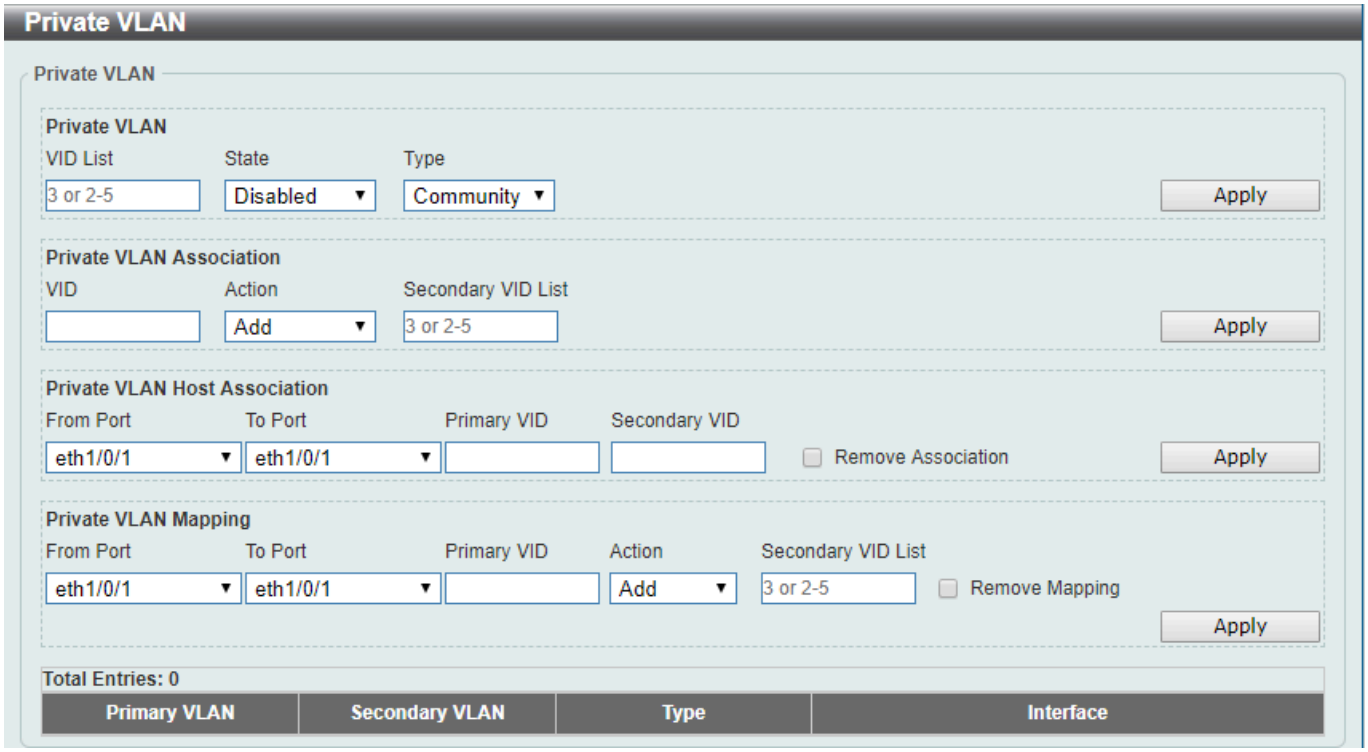


Figure 5-37 Private VLAN Window

The fields that can be configured for **Private VLAN** are described below:

Parameter	Description
VID List	Enter the private VLAN ID list here. Use "-" to specify a range of VIDs and "," to separate multiple VIDs. For example, 2,4-6.
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 fields that can be configured for **Private VLAN Association** are described below:

Parameter	Description
VID List	Enter the private VLAN ID list here.
Action	Select the action that will be taken for the private VLAN here. Options to choose from are **Add** and **Remove**.
Secondary VID List	Enter the secondary private VLAN ID here.

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

The fields that can be configured for **Private VLAN Host Association** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Primary VID	Enter the primary private VLAN ID here.
Secondary VID	Enter the secondary private VLAN ID here. When ticking the **Remove Association** option, this specifies that this configuration will not be enabled.

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

The fields that can be configured for **Private VLAN Mapping** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Primary VID	Enter the primary private VLAN ID here.
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 private VLAN ID here. When ticking the **Remove Mapping** option, this specifies that this configuration will not be enabled.

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

VLAN Tunnel

Dot1q Tunnel

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

An 802.1Q tunnel port behaves as a User Network Interface (UNI) port of a service VLAN. The trunk ports which are tagged members of the service VLAN behave as the Network Node Interface (NNI) ports of the service VLAN.

Only configure the 802.1Q tunneling Ethernet type on ports that are connected to the provider bridge network, which receives and transmits the service VLAN tagged frames. If the tunnel Ethernet type is configured, the specified value will be the Tag Protocol ID (TPID) in the outer VLAN tag of the transmitted frames of the port. The specified TPID is also used to identify the service VLAN tag for the received frame on this port.

To view the following window, click **L2 Features > VLAN Tunnel > Dot1q Tunnel**, as shown below:

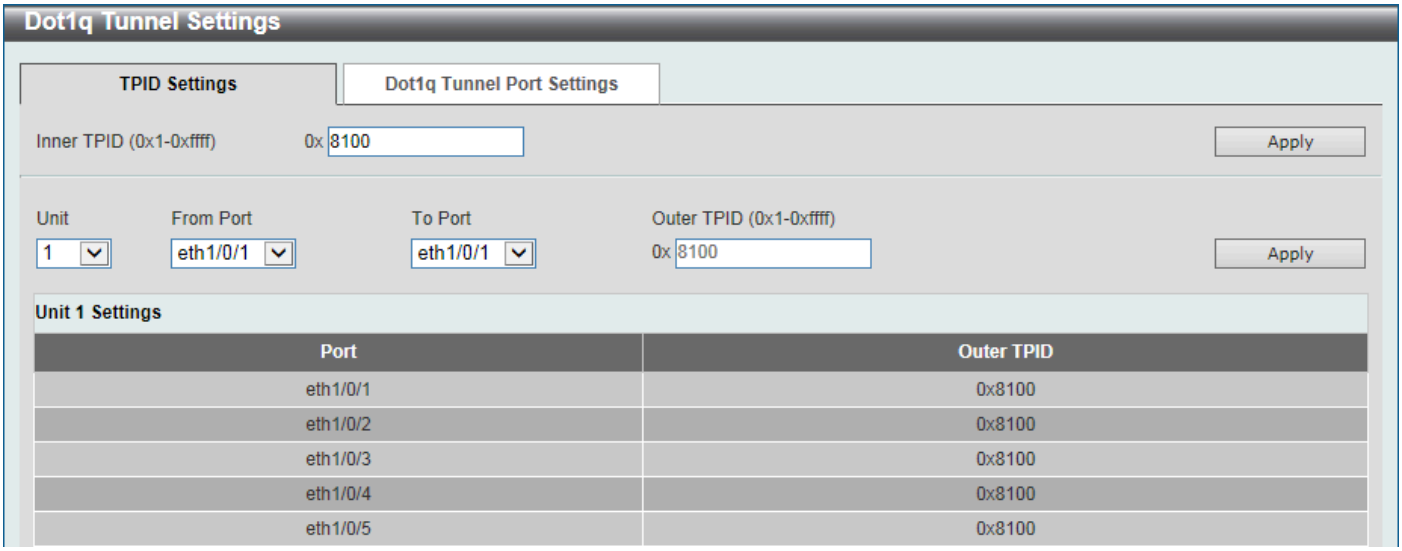


Figure 5-38 Dot1q Tunnel Window

The fields that can be configured are described below:

Parameter	Description
Inner TPID	Enter the inner TPID value here. This value is in the hexadecimal form. The range is from 0x1 to 0xFFFF. The inner TPID is used to decide if the ingress packet is C-tagged. The inner TPID can be configured per system.
Unit	Select the Switch unit ID that will be used here. This option is only available when stacking is enabled.
From Port - To Port	Select the port range that will be used here.
Outer TPID	Enter the outer TPID value here. This value is in the hexadecimal form. The range is from 0x1 to 0xFFFF.

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

After clicking the **Dot1q Tunnel Port Settings** tab, the following page will appear:

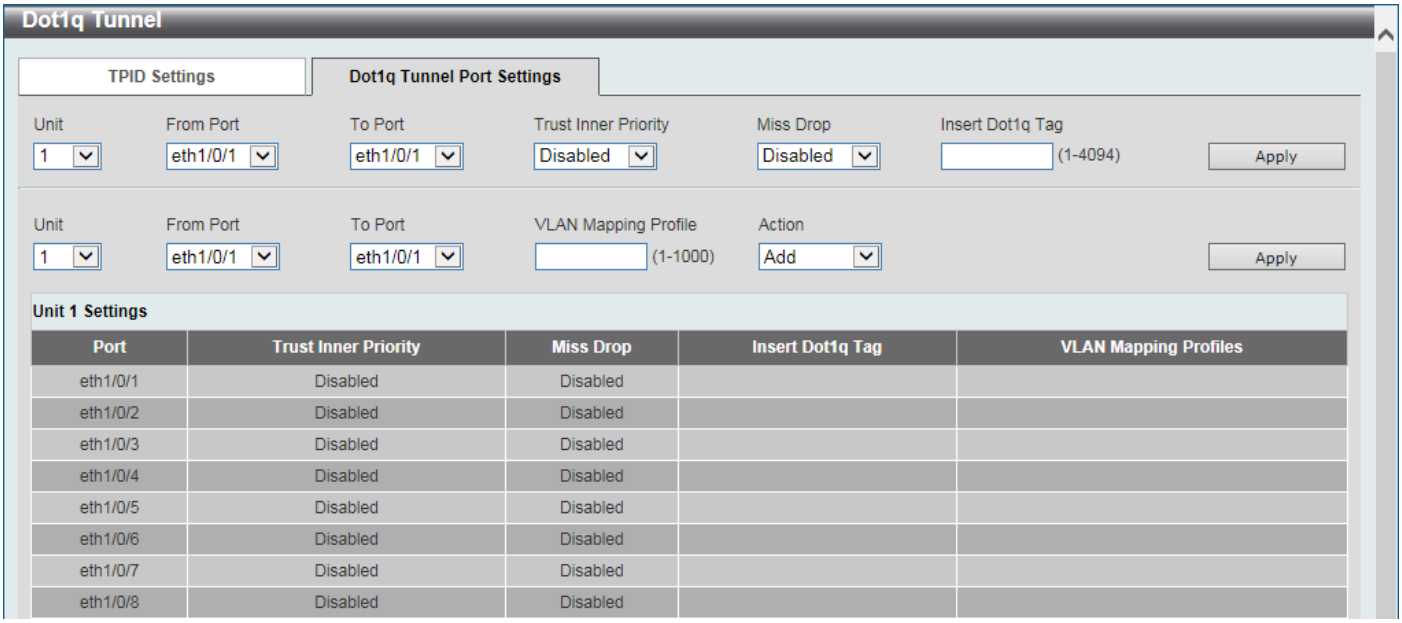


Figure 5-39 Dot1q Tunnel Settings (Dot1q Tunnel Port Settings) Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit ID that will be used here. This option is only available when stacking is enabled.
From Port - To Port	Select the port range that will be used here.
Trust Inner Priority	Select to enable or disable the 802.1Q Inner Trust Priority feature here. When the trusting priority option is enabled on an 802.1Q tunnel port, the priority of the VLAN tag in the received packets will be copied to the service VLAN tag.
Miss Drop	Select to enable or disable the Miss Drop feature here. If the VLAN mapping Miss Drop option is enabled on the receiving port, when the original VLAN of the received packets cannot match the VLAN mapping entries or rules on this port, the received packets will be dropped.
Insert Dot1q Tag	Enter the 802.1Q VLAN ID that is inserted to the untagged packets which are received on the 802.1Q tunnel port(s) here. The range is from 1 to 4094.
VLAN Mapping Profile	Enter the ID of the VLAN mapping profile here. A lower ID has a higher priority. The ID range is from 1 to 1000.
Action	Select **Add** to add a new entry based in the information entered. Select **Remove** to remove an entry based in the information entered.

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

VLAN Mapping

This window is used to display and configure the VLAN mapping settings. If a profile is applied on an interface, the Switch matches the incoming packets according to the rules of the profile. If the packet matches a rule, the action of the rule will be taken. This action may be adding or replacing the outer-VID, specifying the priority of the new outer-TAG or specifying the packet's new inner-VID.

The match order depends on the rule's sequence number in the profile and stopped when first matched. If the sequence number is not specified, it will be allocated automatically. The sequence number begins from 10 and increments 10. Multiple different types of profiles can be configured on one interface.

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

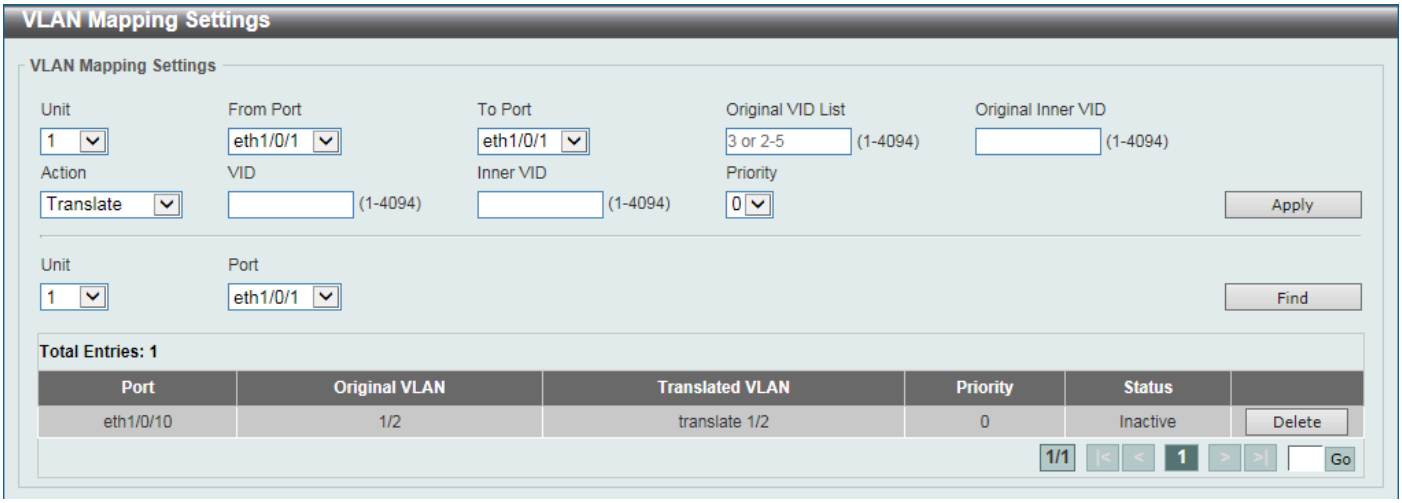


Figure 5-40 VLAN Mapping Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit ID that will be used here. This option is only available when stacking is enabled.
From Port - To Port	Select the port range that will be used here.
Port	Select the port that will be used for the search here.
Original VID List	Enter the original VLAN ID list here. The range is from 1 to 4094.
Original Inner VID	Enter the original inner VLAN ID here. The range is from 1 to 4094.
Action	Select the action that will be taken here. Options to choose from are **Translate** and **Dot1q-tunnel**. • **Translate** - Specifies that the VID will replace the VID of the matched packets. • **Dot1q-tunnel** - Specifies that the outer-VID will be added for matched packets.
VID	Enter the VLAN ID to be translated here. The range is from 1 to 4094.
Inner VID	Enter the inner VLAN ID to be translated here. The range is from 1 to 4094.
Priority	Select the 802.1p priority value here. The range is from 0 to 7. A higher value has a higher priority.

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

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

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

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

VLAN Mapping Profile

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

To view the following window, click **L2 Features > VLAN Tunnel > VLAN Mapping Profile**, after clicking an entry of the VLAN Mapping **Profile**, the rules of Profile 1 will appear.

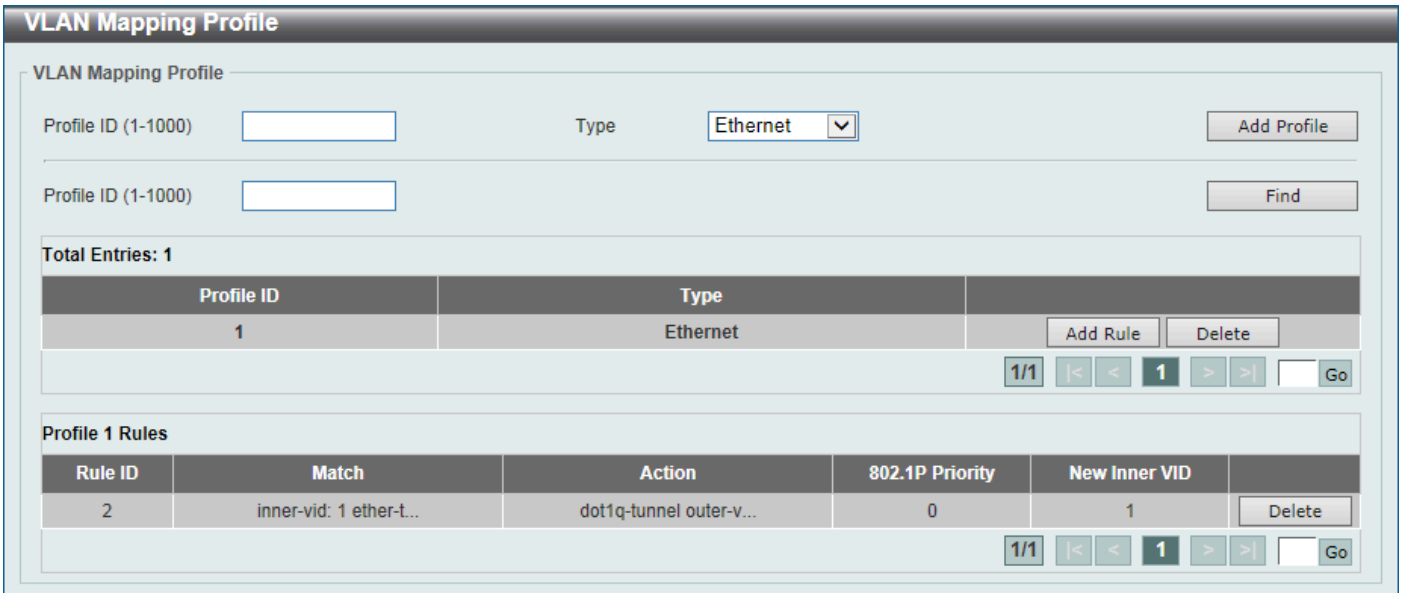


Figure 5-41 VLAN Mapping Profile Window

The fields that can be configured are described below:

Parameter	Description
Profile ID	Enter the ID of the VLAN mapping profile here. A lower ID has a higher priority. The ID range is from 1 to 1000.
Type	Select the profile type here. Different profiles can match different fields. Options to choose from are **Ethernet**, **IP**, **IPv6**, and **Ethernet-IP**. • **Ethernet** - The profile can match Layer 2 fields. • **IP** - The profile can match Layer 3 IP fields. • **IPv6** - The profile can match IPv6 destination or source addresses. • **Ethernet-IP** - The profile can match Layer 2 and Layer 3 IP fields.

Click the **Add Profile** button to add a new VLAN mapping profile.

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

Click the **Add Rule** button to create a new rule.

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

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

After clicking the **Add Rule** button next to an **Ethernet** type profile, the following page will appear.

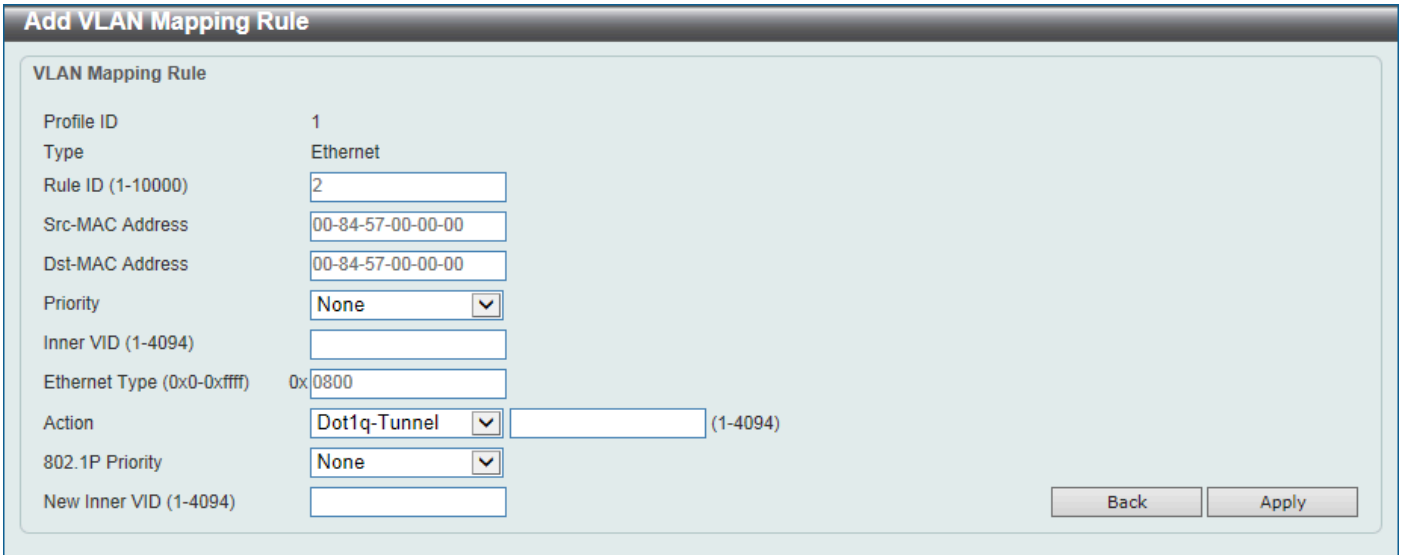


Figure 5-42 VLAN Mapping Profile (Ethernet, Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Rule ID	Enter the VLAN mapping rule ID here. If not specified, the rule ID begins from 10 and is incremented by 10 for every new rule. The range is from 1 to 10000.
Src-MAC Address	Enter the source MAC address here.
Dst-MAC Address	Enter the destination MAC address here.
Priority	Select the 802.1p priority value here. The range is from 0 to 7. A higher value has a higher priority.
Inner VID	Enter the inner VLAN ID here. The range is from 1 to 4094.
Ethernet Type	Enter the Ethernet type value here. The range is from 0x0 to 0xFFFF.
Action	Select the action that will be taken here. Options to choose from are **Dot1q-Tunnel** and **Translate**. • **Dot1q-Tunnel** - Specifies that the outer-VID will be added for matched packets. • **Translate** - Specifies that the outer-VID will replace the outer-VID of the matched packets.
New Outer VID	Enter the new outer VLAN ID here. The range is from 1 to 4094.
802.1P Priority	Select the 802.1p priority value here. The range is from 0 to 7. A higher value has a higher priority.
New Inner VID	After selecting Dot1q-Tunnel as the action, enter the new inner VLAN ID here. The range is from 1 to 4094. This option is only available when Dot1q-Tunnel is selected as the action.

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

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

After clicking the **Add Rule** button next to an **IP** type profile, the following page will appear.

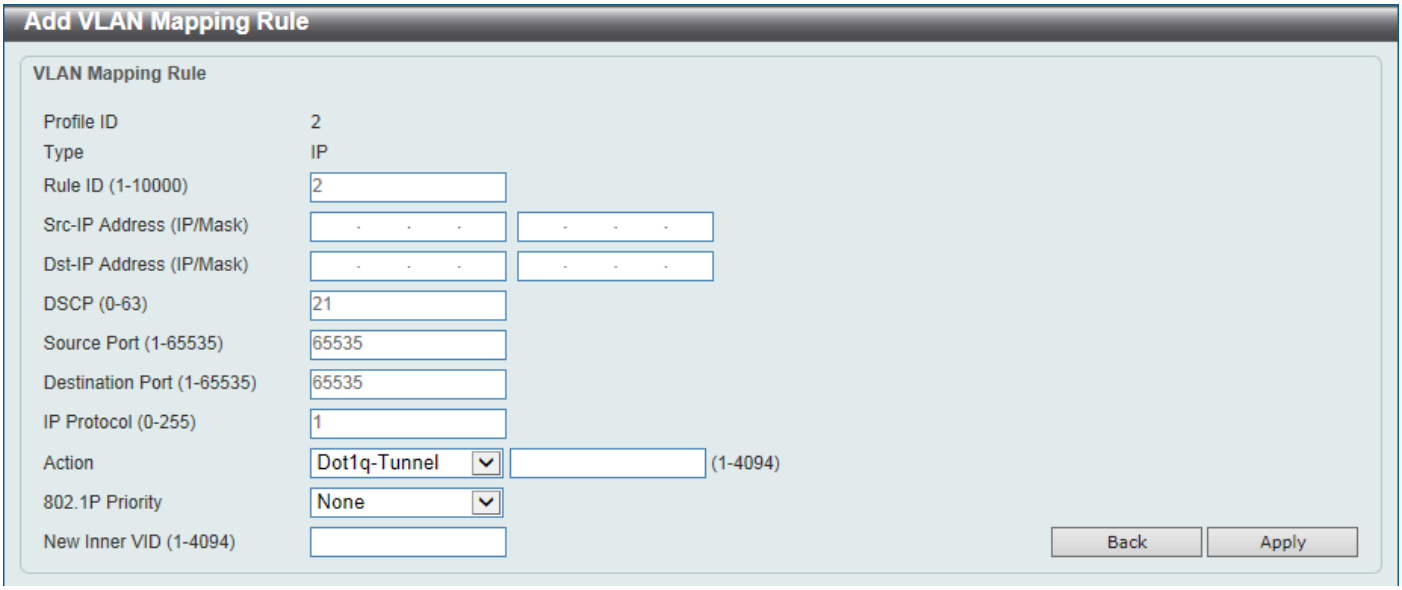


Figure 5-43 VLAN Mapping Profile (IP, Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Rule ID	Enter the VLAN mapping rule ID here. If not specified, the rule ID begins from 10 and is incremented by 10 for every new rule. The range is from 1 to 10000.
Src-IP Address (IP/Mask)	Enter the source IPv4 address and subnet mask here.
Dst-IP Address (IP/Mask)	Enter the destination IPv4 address and subnet mask here.
DSCP	Enter the differentiated services code point (DSCP) value here. The range is from 0 to 63.
Source Port	Enter the source TCP/UDP port number here. The range is from 1 to 65535.
Destination Port	Enter the destination TCP/UDP port number here. The range is from 1 to 65535.
IP Protocol	Enter the Layer 3 IP protocol value here. The range is from 0 to 255.
Action	Select the action that will be taken here. Options to choose from are **Dot1q-Tunnel** and **Translate**. • **Dot1q-Tunnel** - Specifies that the VID will be added for matched packets. • **Translate** - Specifies that the outer-VID will replace the outer-VID of the matched packets.
New Outer VID	Enter the new outer VLAN ID here. The range is from 1 to 4094.
802.1P Priority	Select the 802.1p priority value here. The range is from 0 to 7. A higher value has a higher priority.
New Inner VID	After selecting Dot1q-Tunnel as the action, enter the new inner VLAN ID here. The range is from 1 to 4094. This option is only available when Dot1q-Tunnel is selected as the action.

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

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

After clicking the **Add Rule** button next to an **IPv6** type profile, the following page will appear.

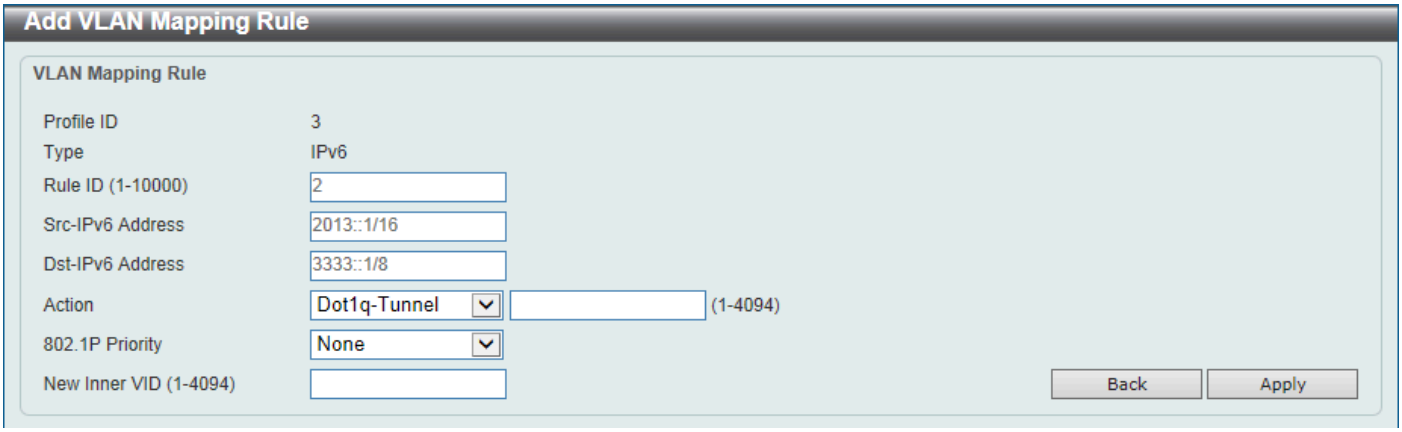


Figure 5-44 VLAN Mapping Profile (IPv6, Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Rule ID	Enter the VLAN mapping rule ID here. If not specified, the rule ID begins from 10 and is incremented by 10 for every new rule. The range is from 1 to 10000
Src-IPv6 Address	Enter the source IPv6 address and prefix length here.
Dst-IPv6 Address	Enter the destination IPv6 address and prefix length here.
Action	Select the action that will be taken here. Options to choose from are **Dot1q-Tunnel** and **Translate**. • **Dot1q-Tunnel** - Specifies that the outer-VID will be added for matched packets. • **Translate** - Specifies that the outer-VID will replace the outer-VID of the matched packets.
New Outer VID	Enter the new outer VLAN ID here. The range is from 1 to 4094.
802.1P Priority	Select the 802.1p priority value here. The range is from 0 to 7. A higher value has a higher priority.
New Inner VID	After selecting Dot1q-Tunnel as the action, enter the new inner VLAN ID here. The range is from 1 to 4094. This option is only available when Dot1q-Tunnel was selected as the action.

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

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

After clicking the **Add Rule** button next to an **Ethernet-IP** type profile, the following page will appear.

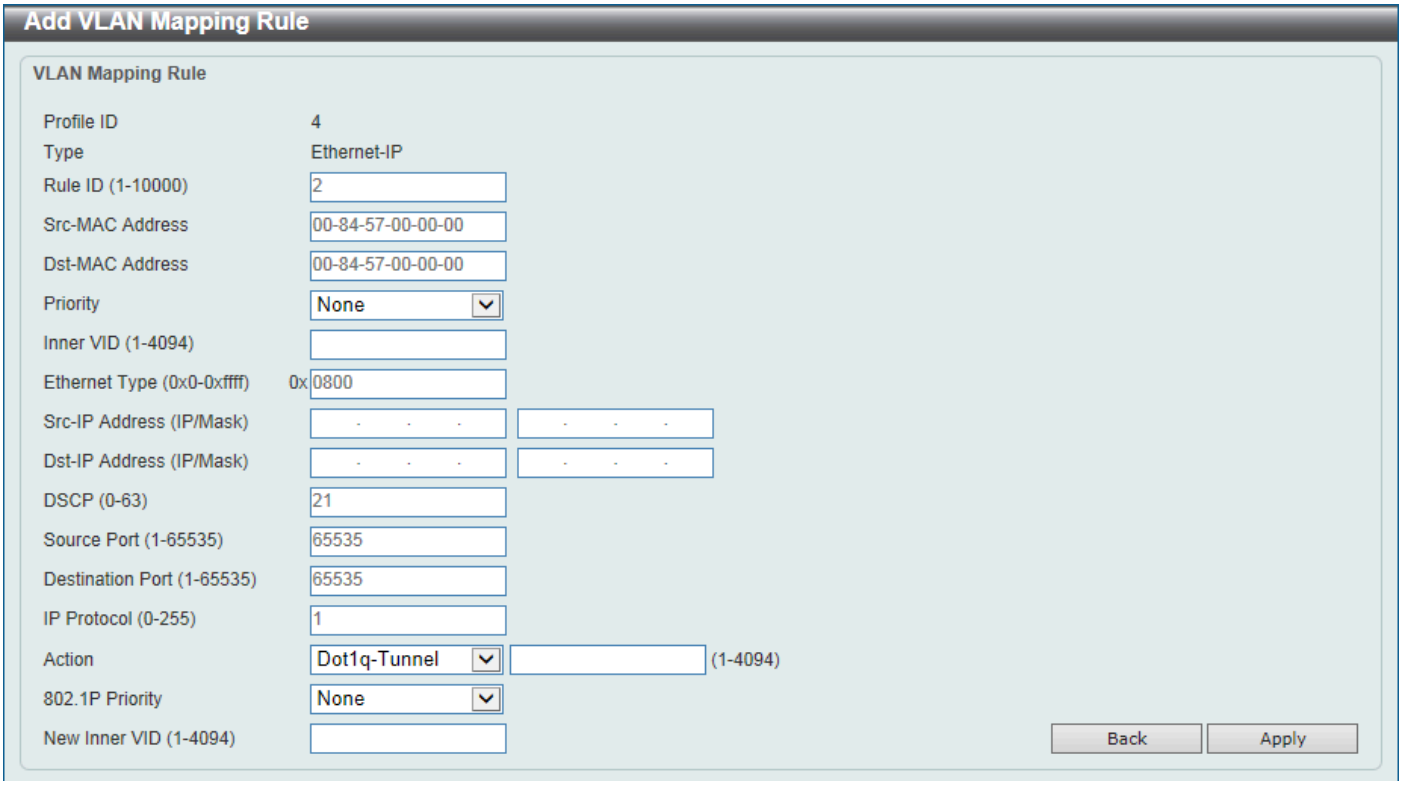


Figure 5-45 VLAN Mapping Profile (Ethernet-IP, Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Rule ID	Enter the VLAN mapping rule ID here. If not specified, the rule ID begins from 10 and is incremented by 10 for every new rule. The range is from 1 to 10000
Src-MAC Address	Enter the source MAC address here.
Dst-MAC Address	Enter the destination MAC address here.
Priority	Select the 802.1p priority value here. The range is from 0 to 7. A higher value has a higher priority.
Inner VID	Enter the inner VLAN ID here. The range is from 1 to 4094.
Ethernet Type	Enter the Ethernet type value here. The range is from 0x0 to 0xFFFF.
Src-IP Address	Enter the source IPv4 address and subnet mask here.
Dst-IP Address	Enter the destination IPv4 address and subnet mask here.
DSCP	Enter the differentiated services code point (DSCP) value here. The range is from 0 to 63.
Source Port	Enter the source TCP/UDP port number here. The range is from 1 to 65535.
Destination Port	Enter the destination TCP/UDP port number here. The range is from 1 to 65535.
IP Protocol	Enter the Layer 3 IP protocol value here. The range is from 0 to 255.
Action	Select the action that will be taken here. Options to choose from are **Dot1q-Tunnel** and **Translate**. • **Dot1q-Tunnel** - Specifies that the outer-VID will be added for matched packets.

Parameter	Description
	• **Translate** - Specifies that the outer-VID will replace the outer-VID of the matched packets.
New Outer VID	Enter the new outer VLAN ID here. The range is from 1 to 4094.
802.1P Priority	Select the 802.1p priority value here. The range is from 0 to 7. A higher value has a higher priority.
New Inner VID	After selecting Dot1q-Tunnel as the action, enter the new inner VLAN ID here. The range is from 1 to 4094. This option is only available when **Dot1q-Tunnel** was selected as the action.

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

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

STP

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

802.1Q-2005 MSTP

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

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

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

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

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

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

- The Switch must be set to the MSTP setting (found in the **STP Global Settings** window in the **STP Mode** field).

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

802.1D-2004 Rapid Spanning Tree

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

Port Transition States

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

All three protocols calculate a stable topology in the same way. Every segment will have a single path to the root bridge. All bridges listen for BPDU packets. However, BPDU packets are sent more frequently, with every Hello packet. BPDU packets are sent even if a BPDU packet was not received. Therefore, each link between bridges is sensitive to the status of the link. Ultimately this difference results in faster detection of failed links, and therefore faster topology adjustment. A drawback of IEEE 802.1D-1998 is this absence of immediate feedback from adjacent bridges.

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

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

Edge Port

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

P2P Port

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

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

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

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

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

STP Global Settings

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

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

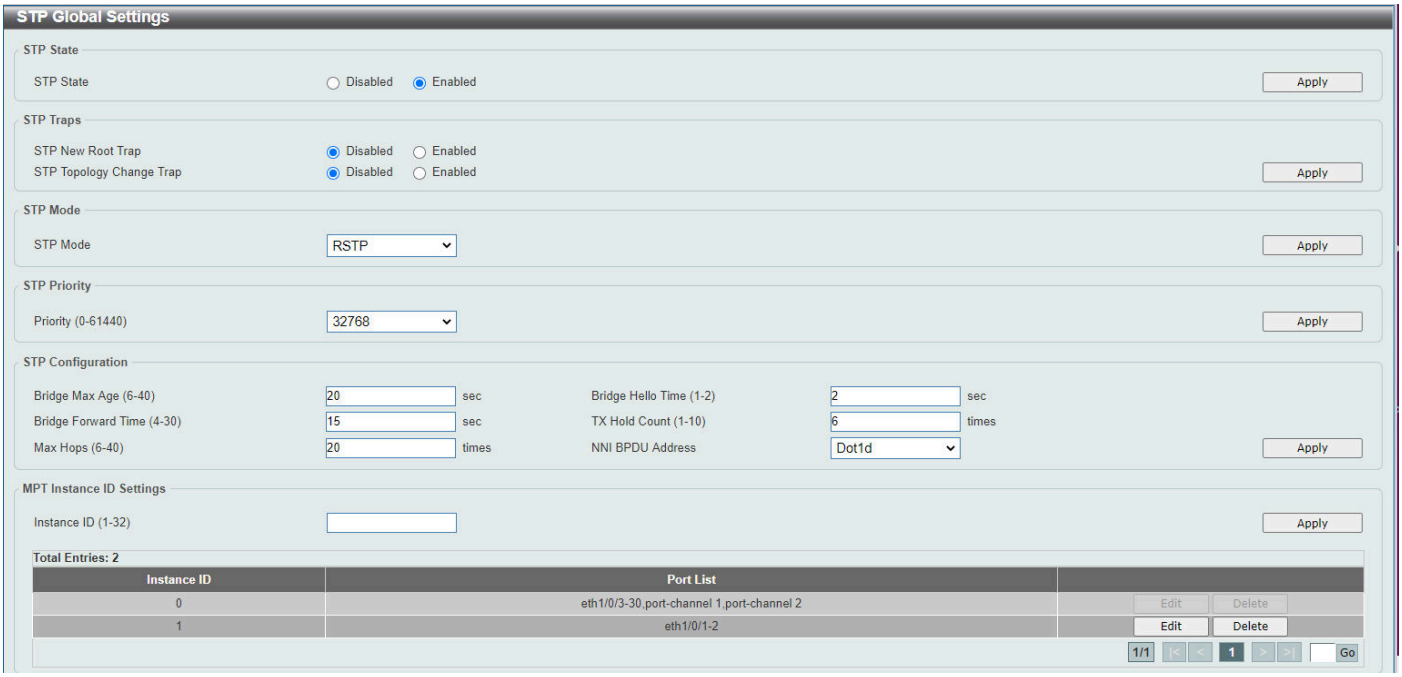


Figure 5-46 STP Global Settings Window

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

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

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

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

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

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

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

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

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

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

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

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

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

Parameter	Description
Bridge Max Age	Enter the bridge Maximum Age value here. This value must be between 6 and 40 seconds. By default, this value is 20 seconds. The Maximum Age value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN.
Bridge Hello Time	After selecting **RSTP/STP** as the **Spanning Tree Mode**, this parameter will be available. Enter the bridge Hello Time value here. This value must be between 1 and 2 seconds. By default, this value is 2 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge. This field will only appear here when STP or RSTP is selected for the STP version. For MSTP, the Hello Time must be set on a port per-port basis.
Bridge Forward Time	Enter the bridge Forwarding Time value here. This value must be between 4 and 30 seconds. By default, this value is 15 seconds. Every port on the Switch spends this time in the Listening state while moving from the Blocking state to the Forwarding state.
TX Hold Count	Enter the Transmit Hold Count value here. This value must be between 1 and 10 times. By default, this value is 6 times. This value is used to set the maximum number of Hello packets transmitted per interval.
Max Hops	Enter the maximum number of hops that are allowed. This value must be between 6 and 40 hops. By default, this value is 20 hops. This value is used to set the number of hops between devices in a spanning tree region before the Bridge Protocol Data Unit (BPDU) packet sent by the Switch will be discarded. Each Switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BDPU packet and the information held for the port will age out.
NNI BPDU Address	Select the NNI BPDU Address option here. Options to choose from are **Dot1d** and **Dot1ad**. By default, this option is **Dot1d**. This parameter is used to determine the BPDU protocol address for STP in the service provider network. It can use an 802.1d STP address and an 802.1ad service provider STP address.

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

The fields that can be configured for **MPT Instance ID Settings** are described below:

Parameter	Description
Instance ID	Enter a new instance ID.

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

This window is used to display and configure the MPT instance setting. Click **Edit** to modify the MPT instance setting and click **Delete** to delete an MPT instance.

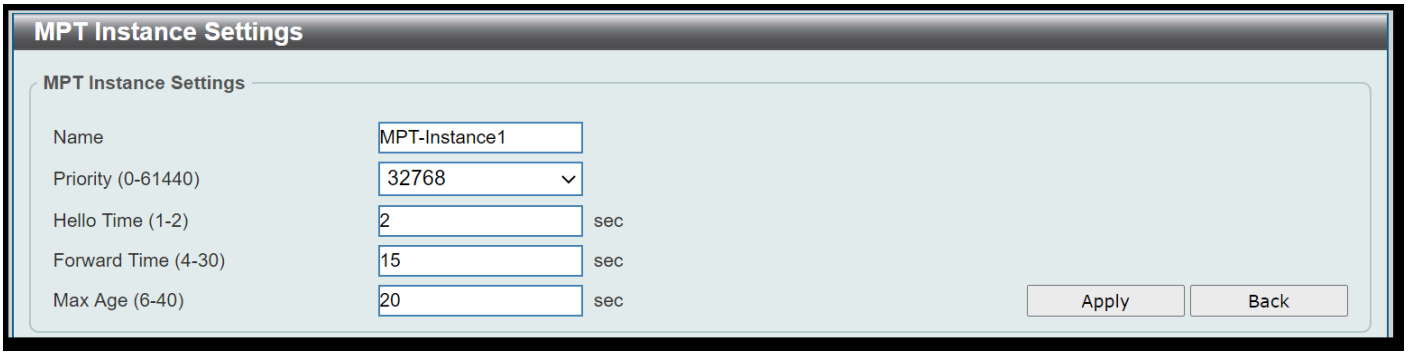


Figure 5-47 MPT Instance Settings Window

The fields that can be configured for **MPT Instance** are described below:

Parameter	Description
Name	Enter the MPT instance name here.
Priority	Select the instance priority here.
Hello Time	Enter the bridge Hello Time value here. This value must be between 1 and 2 seconds. By default, this value is 2 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge. This field will only appear here when STP or RSTP is selected for the STP version. For MSTP, the Hello Time must be set on a port per-port basis.
Forward Time	Enter the bridge Forwarding Time value here. This value must be between 4 and 30 seconds. By default, this value is 15 seconds. Every port on the Switch spends this time in the Listening state while moving from the Blocking state to the Forwarding state.
Max Age	Enter the bridge Maximum Age value here. This value must be between 6 and 40 seconds. By default, this value is 20 seconds. The Maximum Age value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN.

Click the **Apply** button to accept the changes made and click **Back** to return to the **STP Global Setting** window.

STP Port Settings

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

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

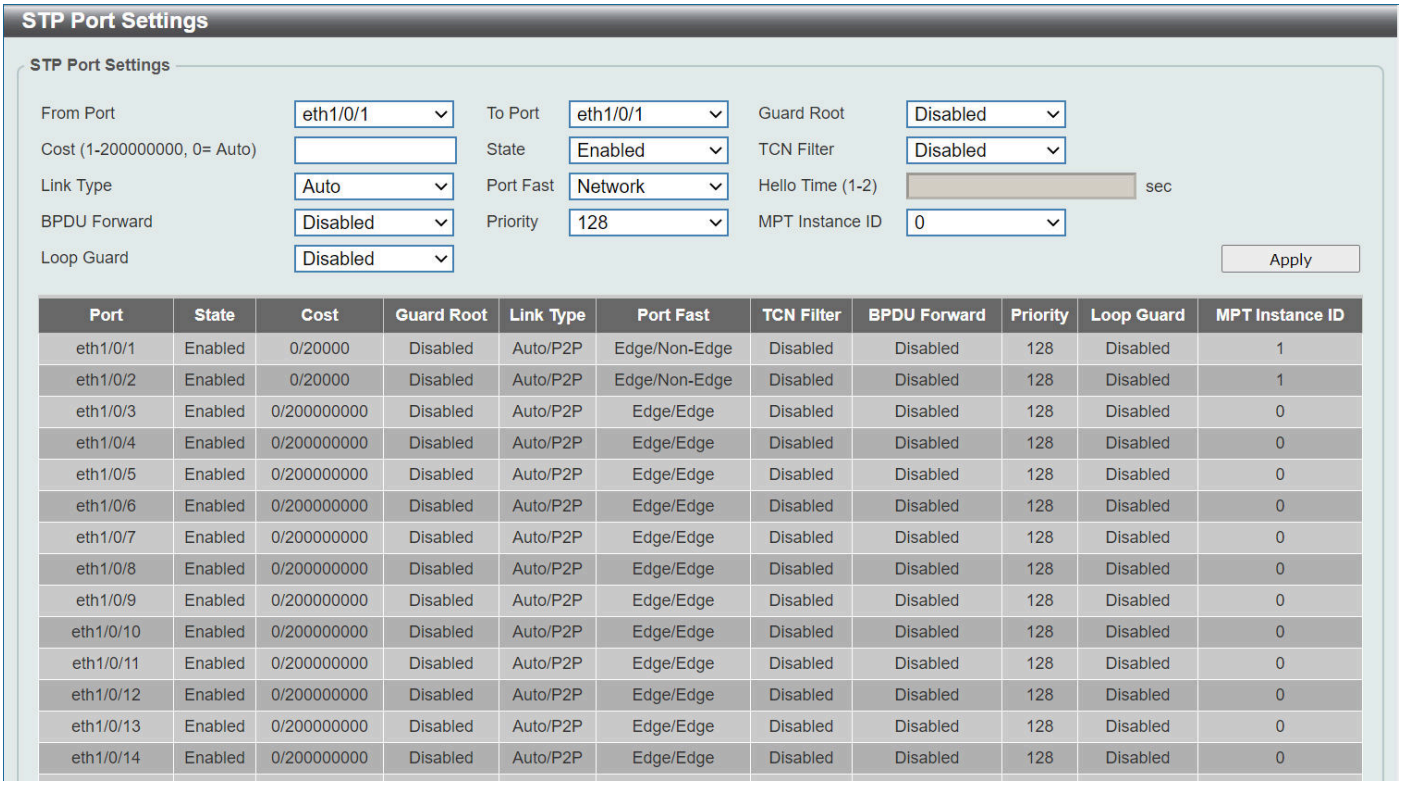


Figure 5-48 STP Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Cost	Enter the cost value here. This value must be between 1 and 200000000. This value defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is 0 (auto). Setting 0 for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. The default port cost for a 100Mbps port is 200000, a Gigabit port is 20000, and a 10 Gigabit port is 2000. The lower the number, the greater the probability the port will be chosen to forward packets.
State	Select to enable or disable the STP port state.
Guard Root	Select to enable or disable the Guard Root function.
Link Type	Select the Link Type 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**.
Port Fast	Select the Port Fast option here. Options to choose from are **Network**, **Disabled**, and **Edge**. • In the **Network** mode the port will remain in the non-port-fast state for three seconds. The port will change to the port-fast state if no BPDU is received and changes to the forwarding state. If the port received the BPDU later, it will change to the non-port-fast state.

Parameter	Description
	• In the **Disabled** mode, the port will always be in the non-port-fast state. It will always wait for the forward-time delay to change to the forwarding state. • In the **Edge** mode, the port will directly change to the spanning-tree forwarding state when a link-up occurs without waiting for the forward-time delay. If the interface receives a BPDU later, its operation state changes to the non-port-fast state. By default, this option is **Network**.
TCN Filter	Select to enable or disable the TCN Filter option. When a port is set to the TCN filter mode, the TC event received by the port will be ignored. By default, this option is **Disabled**.
BPDU Forward	Select to enable or disable BPDU forwarding. If enabled, the received STP BPDU will be forwarded to all VLAN member ports in the untagged form. By default, this option is **Disabled**.
Priority	Select the priority value here. Options to choose from are **0** to **240**. By default this option is 128. A lower value has higher priority.
Hello Time	Enter the hello time value here. This value must be between **1** and **2** seconds. This value specifies the interval that a designated port will wait between the periodic transmissions of each configuration message.
Loop Guard	Select to enable or disable the Loop Guard feature on the specified port(s) here. The STP Loop Guard feature provides additional protection against Layer 2 forwarding loops (STP loops). An STP loop is created when an STP blocking port in a redundant topology erroneously transitions to the Forwarding state. This usually happens because one of the ports in a physically redundant topology (not necessarily the STP blocking port) no longer receives STP BPDUs. In its operation, STP relies on continuous reception or transmission of BPDUs based on the port role. The designated port transmits BPDUs, and the non-designated port receives BPDUs. When one of the ports in a physically redundant topology no longer receives BPDUs, the STP considers the topology to be loop free. Eventually, an alternate port that was previously a Blocking or Backup port becomes Designated and moves to a Forwarding state. This situation creates a loop.
MPT instance ID	Select MPT instance ID here.

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

MST Configuration Identification

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

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

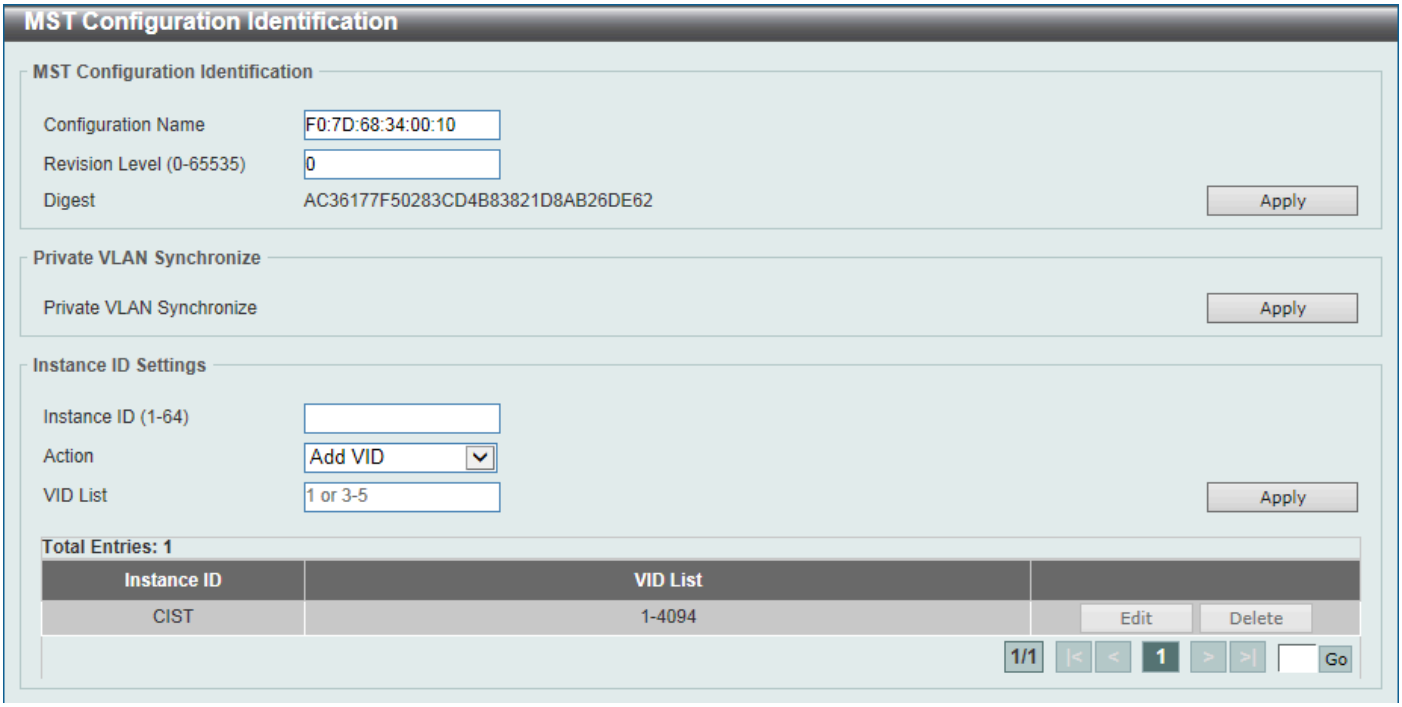


Figure 5-49 MST Configuration Identification Window

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

Parameter	Description
Configuration Name	Enter the MST. This name uniquely identifies the MSTI (Multiple Spanning Tree Instance). If a Configuration Name is not set, this field will show the MAC address to the device running MSTP.
Revision Level	Enter the revision level value here. This value must be between 0 and 65535. By default, this value is 0. This value, along with the Configuration Name, identifies the MSTP region configured on the Switch.

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

In the **Private VLAN Synchronize** section, the user can click the **Apply** button to synchronize the private VLANs.

The fields that can be configured for **Instance ID Settings** are described below:

Parameter	Description
Instance ID	Enter the instance ID here. This value must be between 1 and 64.
Action	Select the action that will be taken here. Options to choose from are **Add VID** and **Remove VID**.
VID List	Enter the VID list value here. This field is used to specify the VID range from configured VLANs set on the Switch. Use "-" to specify a range of VIDs and "," to separate multiple VIDs. For example, 6,8-10.

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

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

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

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

STP Instance

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

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

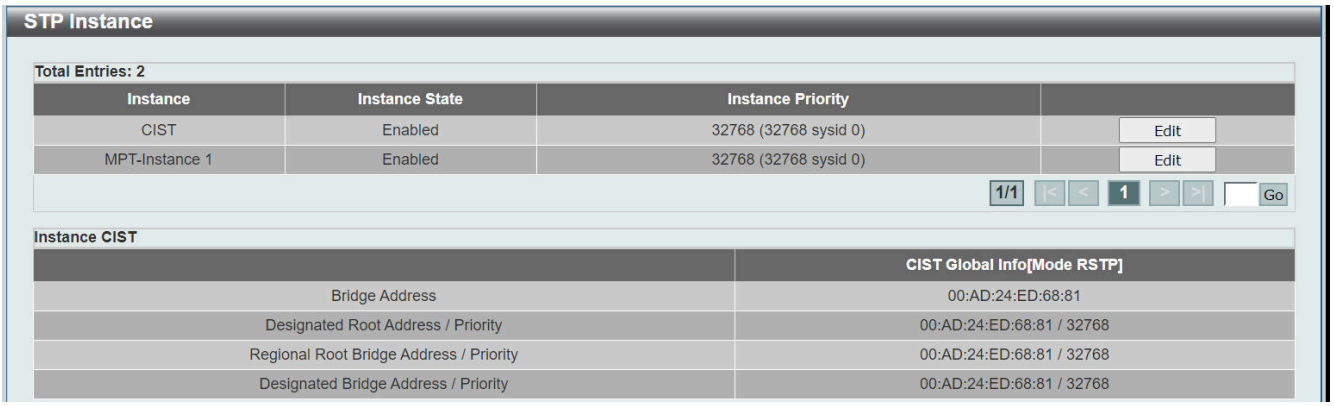


Figure 5-50 STP Instance Window

The fields that can be configured are described below:

Parameter	Description
Instance Priority	After clicking the **Edit** button, enter the Instance Priority value here. The range is from 0 to 61440.

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

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

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

MSTP Port Information

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

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

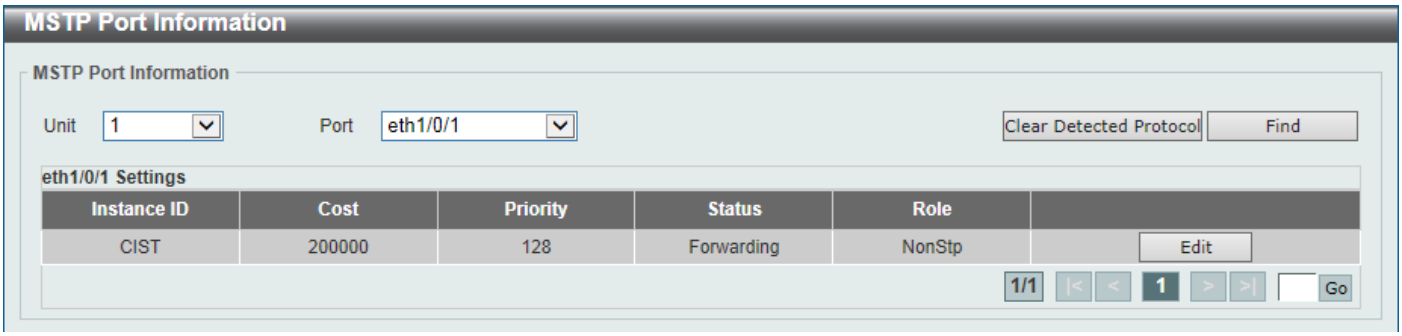


Figure 5-51 MSTP Port Information Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this display here.

Parameter	Description
Port	Select the port number that will be cleared here. This option is only available when stacking is enabled.
Cost	After clicking the **Edit** button, enter the cost value here. This value must be between 1 and 200000000.
Priority	After clicking the **Edit** button, select the priority value here. Options to choose from are **0** to **240**. A lower value has higher priority.

Click the **Clear Detected Protocol** button to clear the detected protocol settings for the port selected.

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

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

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

ERPS (G.8032)

Ethernet Ring Protection Switching (ERPS) (ITU-T G.8032) integrates mature Ethernet Operations, Administration, and Maintenance (OAM) functions and a simple Automatic Protection Switching (APS) protocol to provide sub-50ms protection for Ethernet traffic in a ring topology. It ensures that there are no loops formed at the Ethernet layer.

One link within a ring will be blocked to avoid a Loop (RPL, Ring Protection Link). When the failure happens, protection switching blocks the failed link and unblocks the RPL. When the failure clears, protection switching blocks the RPL again and unblocks the link on which the failure is cleared.

ERPS

This window is used to display and configure the Ethernet Ring Protection Switching (ERPS) settings. STP and Loopback Detection (LBD) should be disabled on the ring ports before enabling ERPS. The ERPS cannot be enabled before the R-APS VLAN ring ports, RPL port, and RPL owner are configured.

NOTE: Be aware that changing the ERPS version will lead to the restart of the running protocol.

To view the following window, click **L2 Features > ERPS (G.8032) > ERPS**, as shown below:

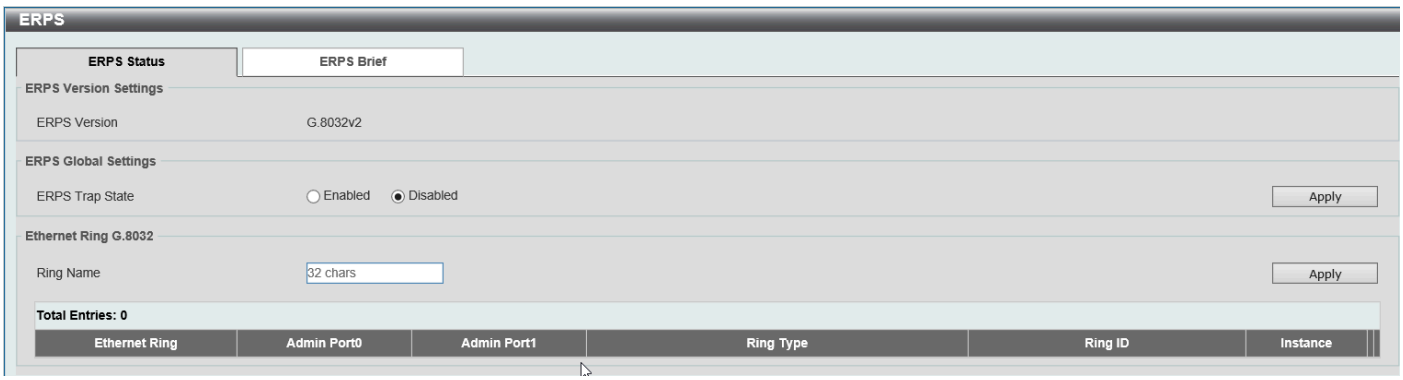


Figure 5-52 ERPS Window

More information about the **ERPS Version Settings**:

Parameter	Description
ERPS Version	G.8032v2 provides the following functions: • Supports multi-instance in a physical ring. • Supports operation commands: manual, force, and clear. • Supports to configure the sending of the R-APS PDU destination address with the RING-ID of the physical ring. If Ethernet ring nodes running ITU-T G.8032v1 and ITU-T G.8032v2 co-exist on an Ethernet ring, the following configurations should be made on the G.8032v2 device: • All physical ring IDs must have the default value of 1. • The major ring instance and sub-ring instance of the interconnection node must have different R-APS VLAN IDs. • Manual switch or force switch command must not exist. • The physical ring must have only one instance.

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

Parameter	Description
ERPS Trap State	Enable or disable trap function for ERPS events.

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

The fields that can be configured in **Ethernet Ring G.8032** are described below:

Parameter	Description
Ring Name	Enter the Ethernet Ring Protection (ERP) instance name here. This name can be up to 32 characters long.

Click the **Apply** button to create an ITU-T G.8032 ERP physical ring.

Click the **Edit Ring** button to modify an ITU-T G.8032 ERP physical ring.

Click the **Show Detail** button to view the ITU-T G.8032 ERP physical ring status information.

Click the **Delete** button to delete the specified ITU-T G.8032 ERP physical ring.

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

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

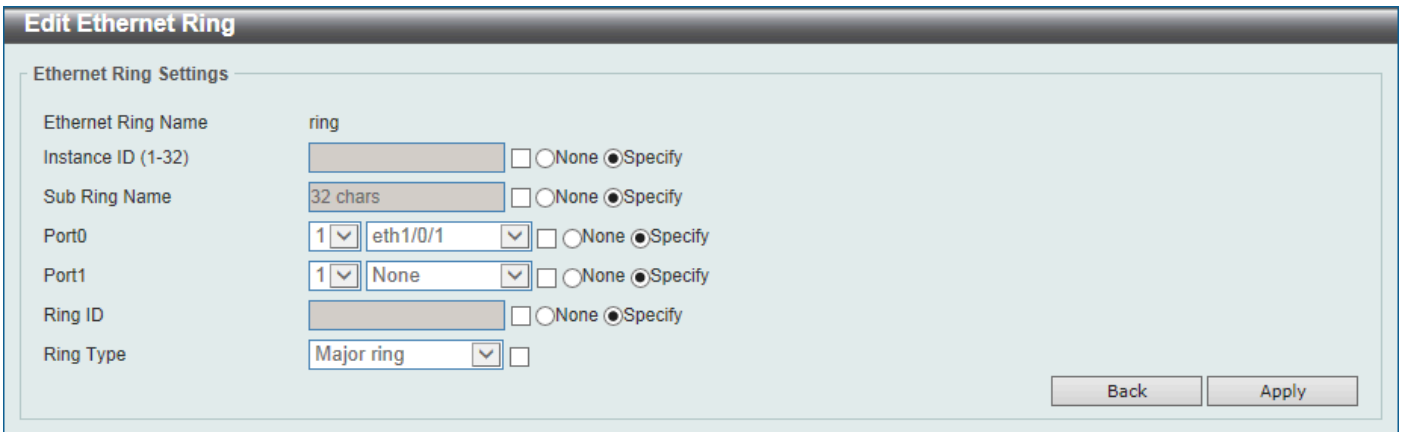


Figure 5-53 ERPS (Edit Ring) Window

The fields that can be configured are described below:

Parameter	Description
Instance ID	Select the checkbox and enter the ERP instance number here. This value must be between 1 and 32. Select the **Specify** radio button to configure this parameter as normal. Select the **None** radio button to revert this parameter to the default setting.
Sub Ring Name	Select the checkbox and enter the physical ring's sub-ring name here. This name can be up to 32 characters long. Select the **Specify** radio button to configure this parameter as normal. Select the **None** radio button to revert this parameter to the default setting.
Port0	Select the checkbox and then select the Switch unit ID and the port number that will be the first ring port of the physical ring. Select the **Specify** radio button to configure this parameter as normal. Select the **None** radio button to revert this parameter to the default setting.
Port1	Select the checkbox and then select the Switch unit ID and the port number that will be the second ring port of the physical ring. Select the **None** option, from the drop-down menu, specifies that the inter-connected node is a local node endpoint of an open ring. Select the **Specify** radio button to configure this parameter as normal. Select the **None** radio button to revert this parameter to the default setting.
Ring ID	Select the checkbox and enter the ring ID here. The range is from 1 to 239. Select the **Specify** radio button to configure this parameter as normal. Select the **None** radio button to revert this parameter to the default setting.
Ring Type	Select the checkbox and then select the ring type here. Options to choose from are **Major Ring** and **Sub Ring**.

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

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

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

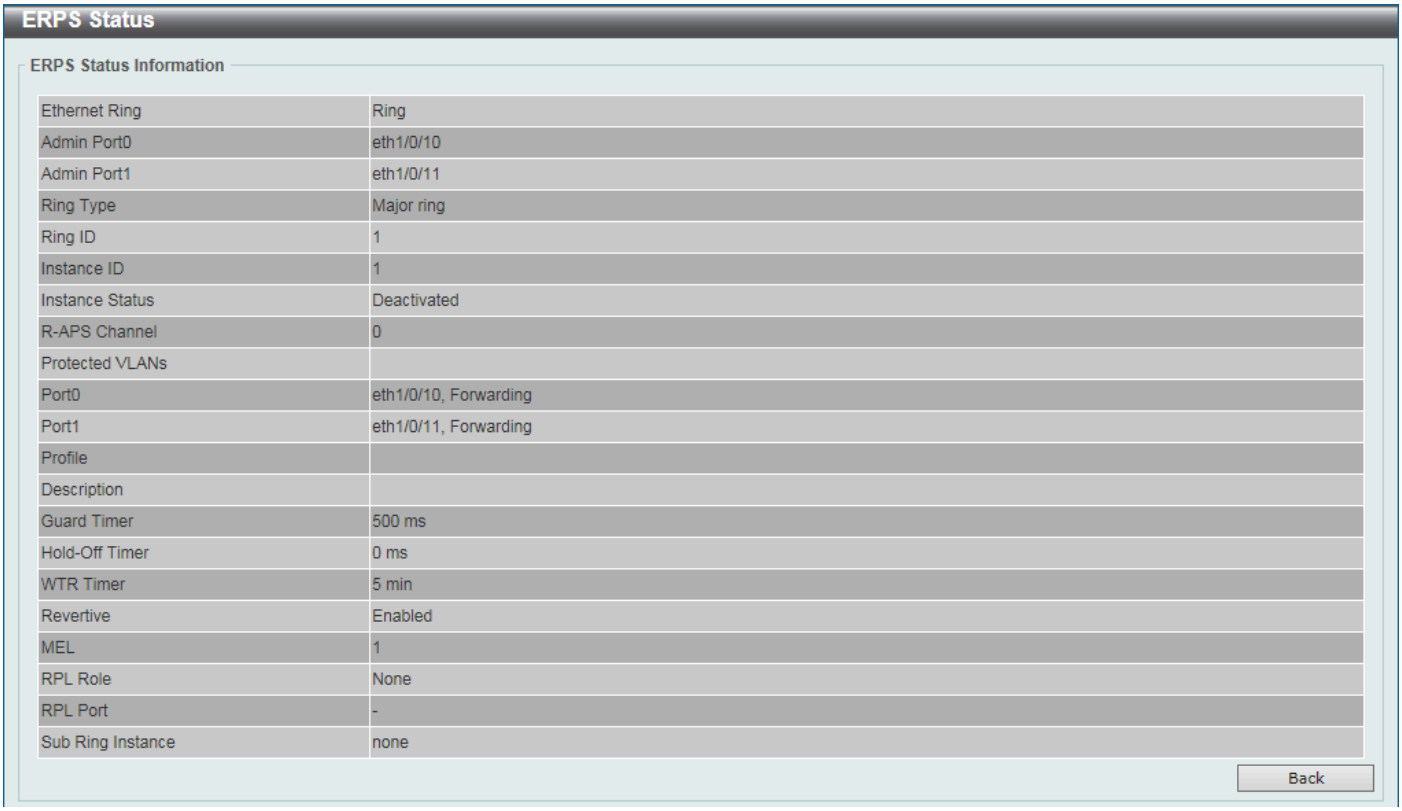


Figure 5-54 ERPS (View Detail) Window

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

After selecting the **ERPS Brief** tabs option, at the top of the page, the following page will be available.

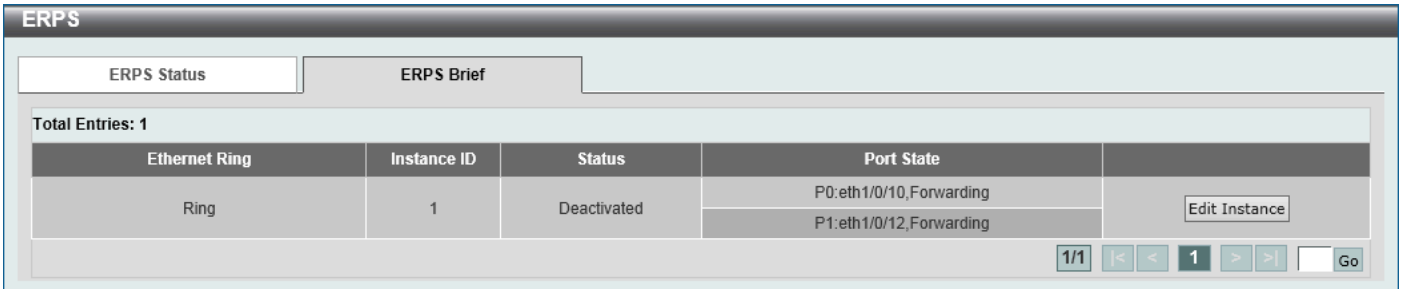


Figure 5-55 ERPS (ERPS Brief) Window

Click the **Edit Instance** button to configure the ERP instance.

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

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

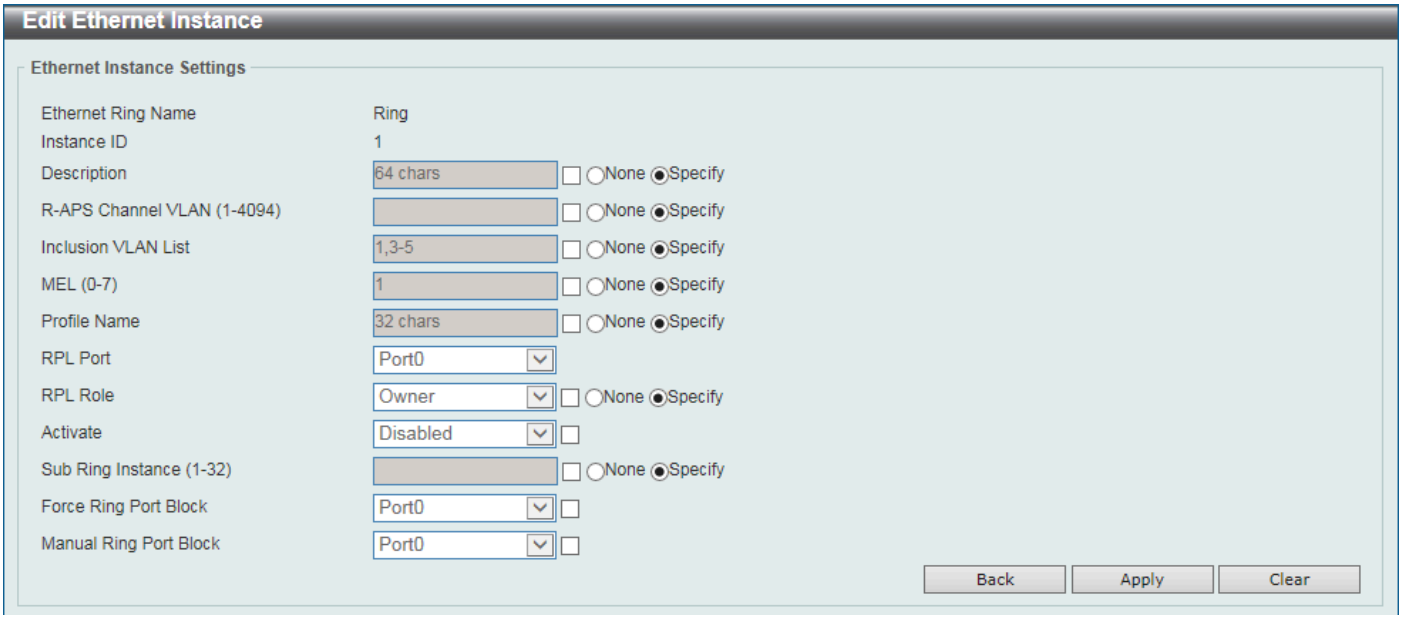


Figure 5-56 ERPS (ERPS Brief, Edit Instance) Window

The fields that can be configured are described below:

Parameter	Description
Description	Select the checkbox and enter the ERP instance description here. This description can be up to 64 characters long. Select the **Specify** radio button to configure this parameter as normal. Select the **None** radio button to revert this parameter to the default setting.
R-APS Channel VLAN	Select the checkbox and enter the R-APS channel VLAN ID for the ERP instance here. The APS channel VLAN of a sub-ring instance is also the virtual channel of the sub-ring. This value must be between 1 and 4094. Select the **Specify** radio button to configure this parameter as per normal. Select the **None** radio button to revert this parameter to the default setting.
Inclusion VLAN List	Select the checkbox and enter the inclusion VLAN list here. A range is identified when a hyphen (-) is used. For example VLANs 1 to 5 can be entered as 1-5. A list is identified when commas (,) are used. For example, use VLANs 1,3,5. The VLANs specified here will be protected by the ERP mechanism. Select the **Specify** radio button to configure this parameter as normal. Select the **None** radio button to revert this parameter to the default setting.
MEL	Select the checkbox and enter the ring MEL value of the ERP instance here. This value must be between 0 and 7. The configured MEL value of all ring nodes that participate in the same ERP instance should be identical. Select the **Specify** radio button to configure this parameter as normal. Select the **None** radio button to revert this parameter to the default setting.
Profile Name	Select the checkbox and enter the G.8032 profile name here that will be associated with this ERP instance. Multiple ERP instances can be associated with the same G.8032 profile. The instances associated with the same profile protect the same set of VLANs, or the VLANs protected by one instance are a subset of LANs protected by another instance. This name can be up to 32 characters long. Select the **Specify** radio button to configure this parameter as normal. Select the **None** radio button to revert this parameter to the default setting.
RPL Port	Select the checkbox and then select the RPL port option here. Options to choose from are **Port0** and **Port1**. The option selected will be configured as the RPL port.

Parameter	Description
RPL Role	Select the checkbox and then select whether this node is the RPL owner or neighbor. Options to choose from are **Owner** and **Neighbor**. Select the Specify radio button to configure this parameter as normal. Select the None radio button to revert this parameter to the default setting.
Activate	Select the checkbox and then select whether or not to active this ERP instance. Options to choose from are **Enabled** and **Disabled**. Enabling this option will active this ERP instance.
Sub Ring Instance	Select the checkbox and enter the identifier of the ERP instance here. This is used to specify the sub-ring instance of a physical ring instance. The range is from 1 to 32. Select the **Specify** radio button to configure this parameter as normal. Select the **None** radio button to revert this parameter to the default setting.
Force Ring Port Block	Select the checkbox and select the ERP instance port that will be blocked here. This forcibly blocks an instance port immediately after force is configured, irrespective of whether link failures have occurred. Options to choose from are **Port0** and **Port1**.
Manual Ring Port Block	Select the checkbox and select the ERP instance port that will be blocked here. This forcibly blocks a port on which MS is configured when link failures and FS conditions are absent. Options to choose from are **Port0** and **Port1**.

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

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

Click the **Clear** button to clear the forced or manual configuration associated with this entry.

ERPS Profile

This window is used to display and configure the Ethernet Ring G.8032 Profile settings.

To view the following window, click **L2 Features > ERPS (G.8032) > ERPS Profile**, as shown below:

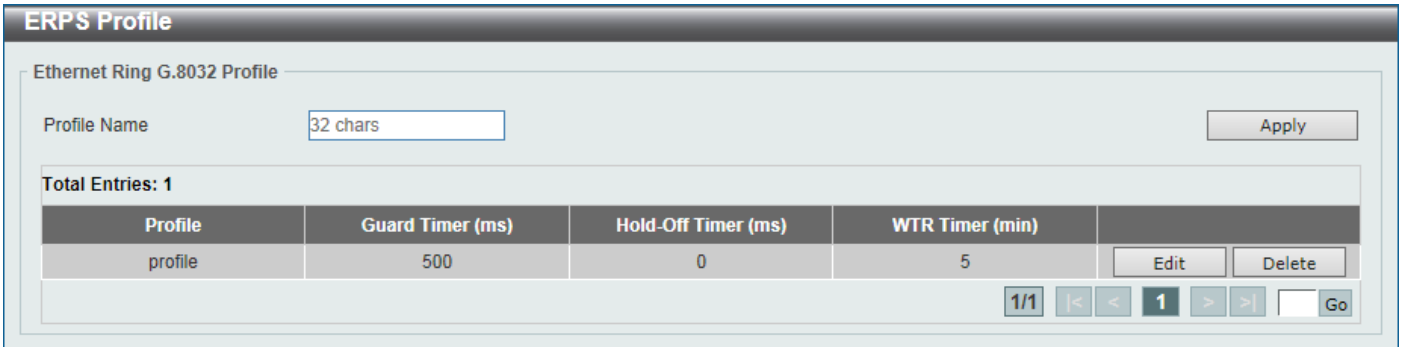


Figure 5-57 ERPS Profile Window

The fields that can be configured are described below:

Parameter	Description
Profile Name	Enter the G.8032 profile name here. This name can be up to 32 characters long. Multiple ERP instances can be associated with the same G.8032 profile. The instances associated with the same profile protect the same set of VLANs, or the VLANs protected by one instance are a subset of LANs protected by another instance.

Click the **Apply** button to associate the G.8032 profile with the ERP instance created.

Click the **Edit** button to modify the specified G.8032 profile.

Click the **Delete** button to disassociate the G.8032 profile.

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

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

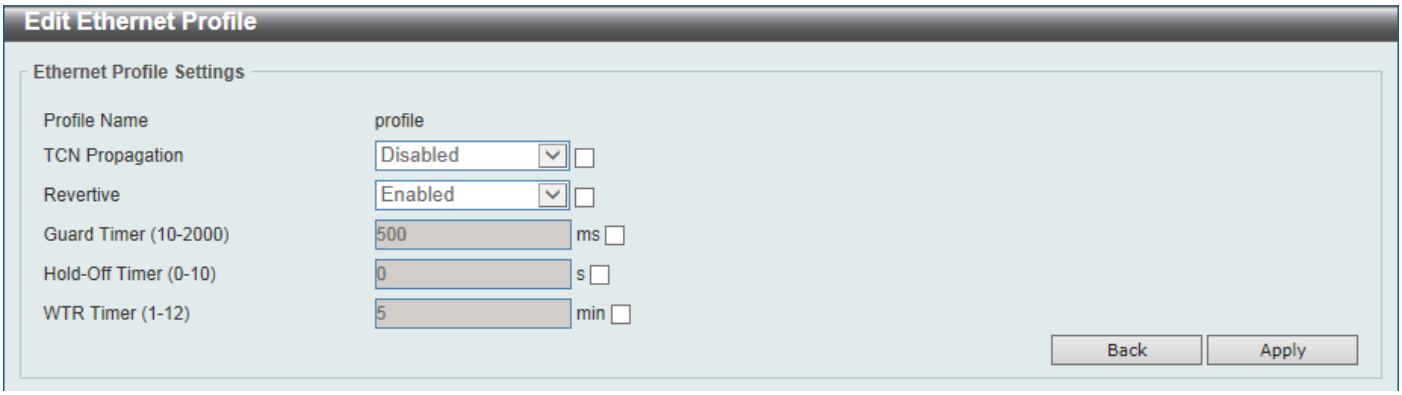


Figure 5-58 ERPS Profile (Edit) Window

The fields that can be configured are described below:

Parameter	Description
TCN Propagation	Select the checkbox and then select the TCN propagation state. Options to choose from are **Enable** and **Disabled**. This function is used to enable the propagation of the topology change notifications from the sub-ERP instance to the major instance.
Revertive	Select the checkbox and then select the revertive state. Options to choose from are **Enable** and **Disabled**. This function is used to revert back to the working transport entity, for example, when the RPL is blocked.
Guard Timer	Select the checkbox and enter the guard timer value here. This value must be between 10 and 2000 milliseconds. By default, this value is 500 milliseconds.
Hold-Off Timer	Select the checkbox and enter hold-off timer value here. This value must be between 0 and 10 seconds. By default, this value is 0 seconds.
WTR Timer	Select the checkbox and enter the Wait To Restore (WTR) timer value here. This value must be between 1 and 12 minutes. By default, this value is 5 minutes.

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

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

Loopback Detection

The Loopback Detection (LBD) function is used to detect the loop created by a specific port. This feature is used to temporarily shut down a port on the Switch when a CTP (Configuration Testing Protocol) packet has been looped back to the Switch. When the Switch detects CTP packets received from a port or a VLAN, this signifies a loop on the network. The Switch will automatically block the port or the VLAN and send an alert to the administrator. The Loopback Detection port will restart (change to normal state) when the Loopback Detection Recover Time times out. The Loopback Detection function can be implemented on a range of ports at a time. The user may enable or disable this function using the drop-down menu.

To view the following window, click **L2 Features > Loopback Detection**, as shown below:

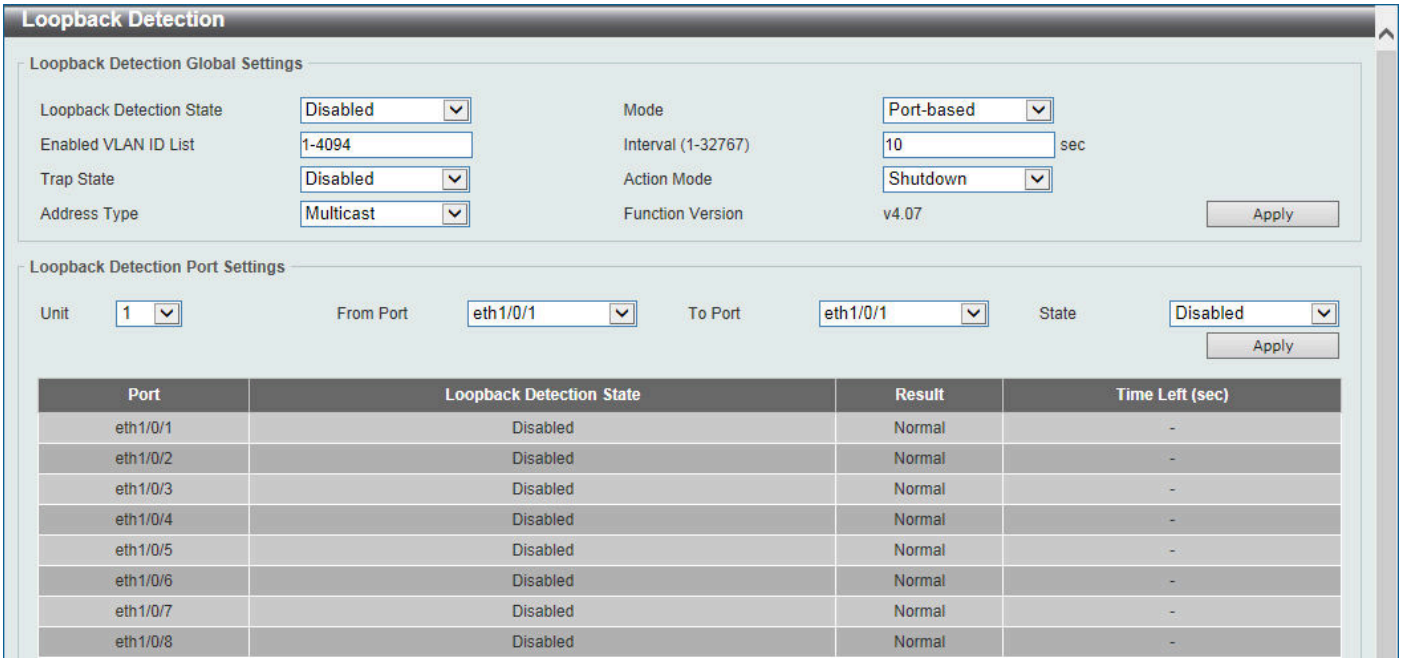


Figure 5-59 Loopback Detection Window

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

Parameter	Description
Loopback Detection State	Select to enable or disable loopback detection. The default is **Disabled**.
Mode	Select the loopback detection mode. Options to choose from are **Port-based** and **VLAN-based**.
Enabled VLAN ID List	Enter the VLAN ID for loop detection. Use "-" to specify a range of VIDs and "," to separate multiple VIDs.
Interval	Enter the interval in seconds that the device will use to transmit Configuration Test Protocol (CTP) packets to detect a loopback event. The valid range is from 1 to 32767 seconds. The default setting is 10 seconds.
Trap State	Select to enable or disable the loopback detection trap state.
Action Mode	Select the action mode here. Option to choose from are: • **Shutdown** - Specifies to shut down the port in the port-based mode or block traffic on the specific VLAN in the VLAN-based mode when a loop has been detected. • **None** - Specifies not to shut down the port in the port-based mode or block traffic on the specific VLAN in the VLAN-based mode when a loop has been detected.
Address Type	Select the address type here. Options to choose from are **Multicast** and **Broadcast**.
NOTE: You can configure errdisable trap and recovery settings in **System > Port Configuration > Error Disable Settings**.	

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

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

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select this option to enable or disable the state of the port.

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

Link Aggregation

Understanding Port Trunk Groups

Port trunk groups are used to combine a number of ports together to make a single high-bandwidth data pipeline. The Switch supports up to 32 port trunk groups with up to 8 ports in each group.

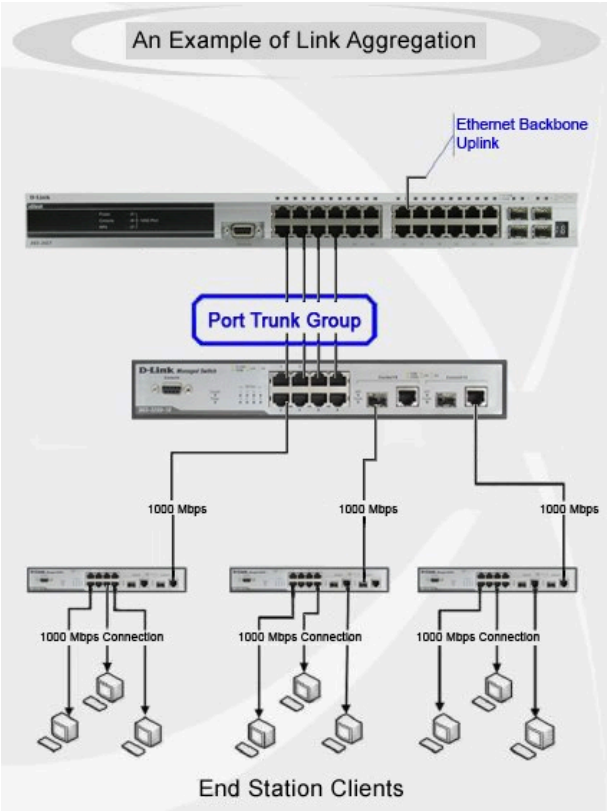


Figure 5-60 Example of Port Trunk Group

The Switch treats all ports in a trunk group as a single port. Data transmitted to a specific host (destination address) will always be transmitted over the same port in a trunk group. This allows packets in a data stream to arrive in the same order they were sent.

Link aggregation allows several ports to be grouped together and to act as a single link. This results in a bandwidth that is a multiple of a single link's bandwidth.

Link aggregation is most commonly used to link bandwidth intensive network devices, such as servers, to the backbone of a network.

The Switch allows the creation of up to 32 link aggregation groups, each group consisting of up to 8 links (ports). Each port can only belong to a single link aggregation group.

Load balancing is automatically applied to the ports in the aggregated group, and a link failure within the group causes the network traffic to be directed to the remaining links in the group.

The Spanning Tree Protocol will treat a link aggregation group as a single link. If two redundant link aggregation groups are configured on the Switch, STP will block one entire group; in the same way STP will block a single port that has a redundant link.

NOTE: If any ports within the trunk group become disconnected, packets intended for the disconnected port will be load shared among the other linked ports of the link aggregation group.

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

To view the following window, click **L2 Features > Link Aggregation**, as shown below:

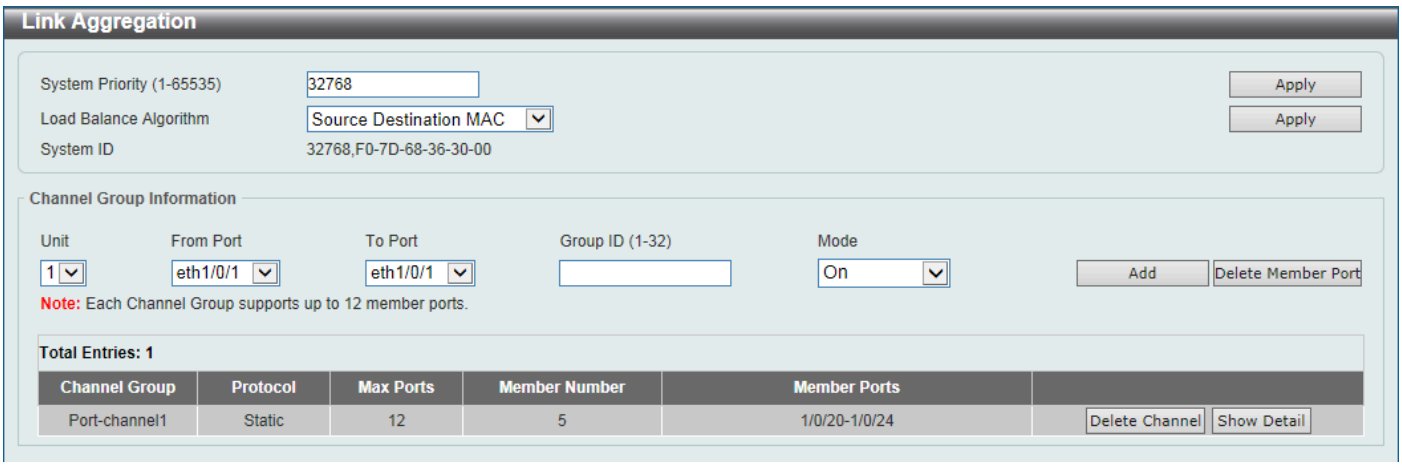


Figure 5-61 Link Aggregation Window

The fields that can be configured for **Link Aggregation** are described below:

Parameter	Description
System Priority	Enter the system priority value used here. This value must be between **1** and **65535**. By default, this value is **32768**. The system priority determines which ports can join a port-channel and which ports are put in the stand-alone mode. The lower value has a higher priority. If two or more ports have the same priority, the port number determines the priority.
Load Balance Algorithm	Select the load balancing algorithm that will be used here. Options to choose from are **Source MAC, Destination MAC, Source Destination MAC, Source IP, Destination IP, 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 fields that can be configured for **Channel Group Information** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the list of ports that will be associated with this configuration here.
Group ID	Enter the channel group number here. This value must be between **1** and **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 **On**, **Active**, and **Passive**. If the mode **On** is specified, the channel group type is static. If the mode **Active** or **Passive** is specified, the channel group type is LACP. A channel group can only consist of either static members or LACP members. Once the type of channel group has been determined, other types of interfaces cannot join the channel group.

Click the **Add** button to add a new channel group.

Click the **Delete Member Port** button, to delete the member port(s) specified from the group.

Click the **Delete Channel** button to delete the specified channel group.

Click the **Show Detail** button to view more detailed information about the channel.

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

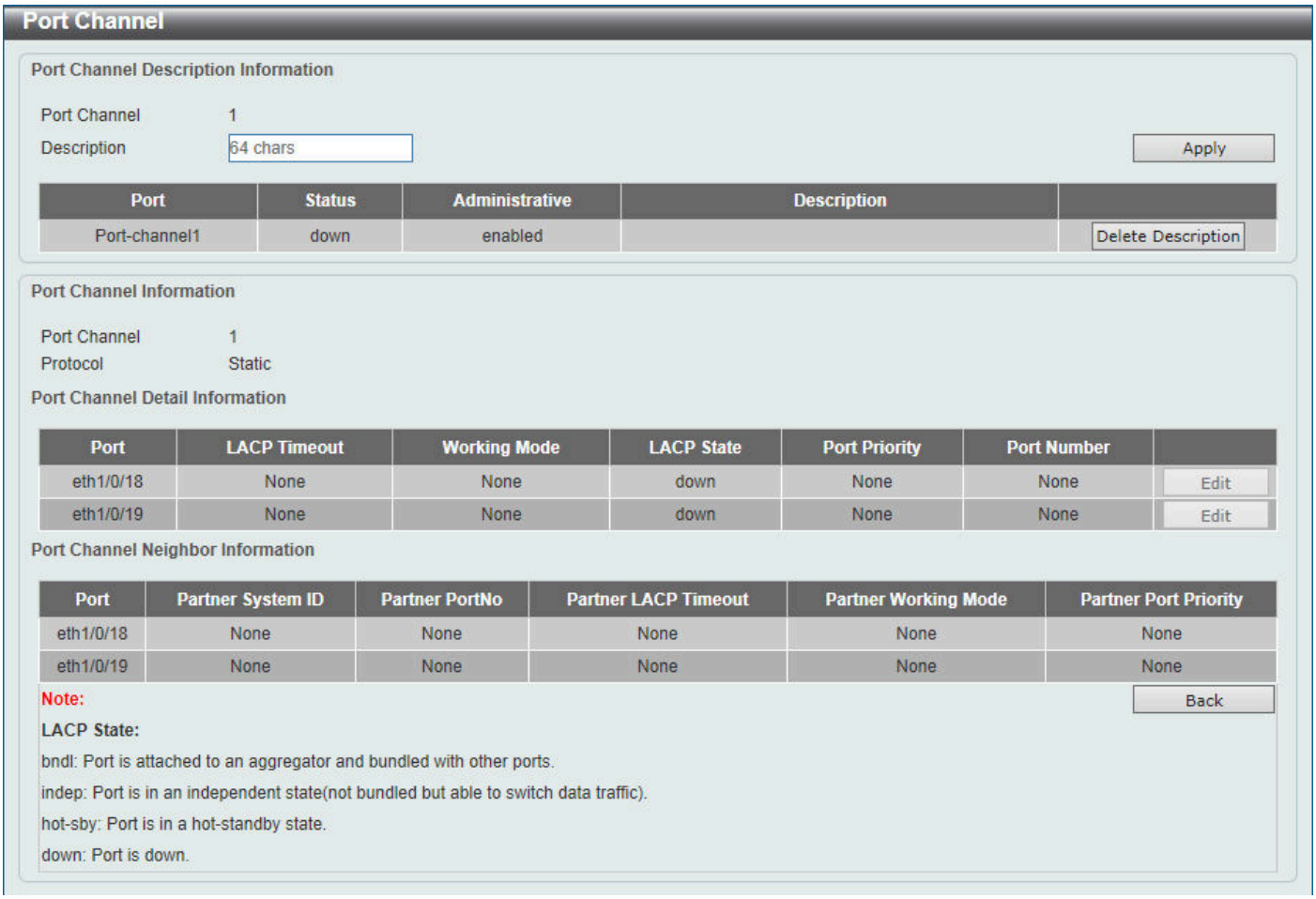


Figure 5-62 Link Aggregation (Show Detail) Window

The fields that can be configured are described below:

Parameter	Description
Description	Enter the description for the port channel here. This string can be up to 64 characters long.

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

Click the **Delete Description** button to delete the description for the port channel.

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

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

L2 Protocol Tunnel

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

To view the following window, click **L2 Features > L2 Protocol Tunnel**, as shown below:

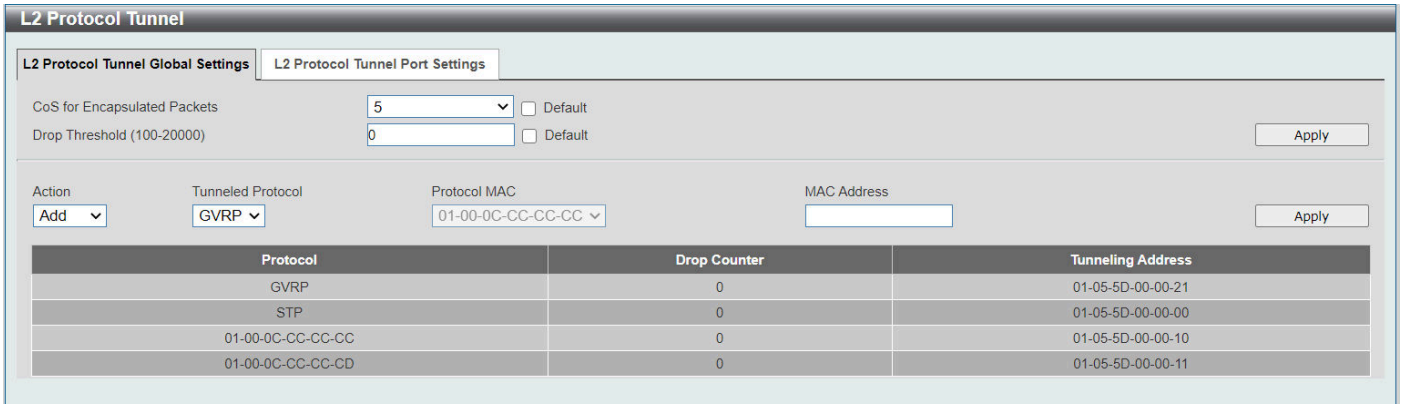


Figure 5-63 L2 Protocol Tunnel (L2 Protocol Tunnel Global Setting) Window

The fields that can be configured are described below:

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. This value must be between 100 and 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 an L2PT tunneling multicast address to or from the specified protocol.
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 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.

After selecting the **L2 Protocol Tunnel Port Settings** tab option, at the top of the page, the following page will be available.

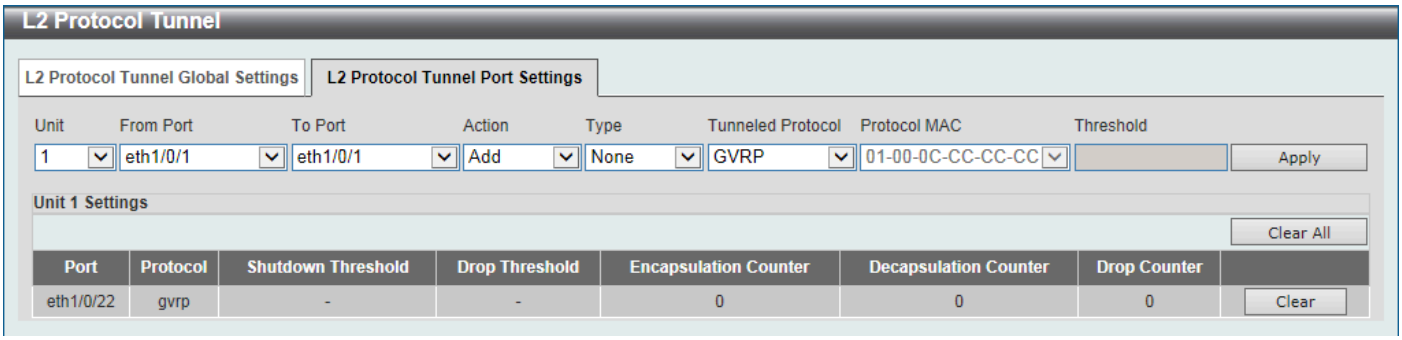


Figure 5-64 L2 Protocol Tunnel (L2 Protocol Tunnel Port Setting) Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration 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**.
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 and Add in the Action field, the following parameter will be available. Enter the threshold value here. This value must be between **1** and **4096**.
You can configure errdisable trap and recovery settings in **System > Port Configuration > Error Disable Settings**.	

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

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

Click the **Clear** button to clear all the counter information of the specific entry.

L2 Multicast Control

IGMP Snooping

Internet Group Management Protocol (IGMP) snooping allows the Switch to recognize IGMP queries and reports sent between network stations or devices and an IGMP host.

IGMP Snooping Settings

In order to use IGMP Snooping it must first be enabled for the entire Switch under **IGMP Global Settings** at the top of the window. You may then fine-tune the settings for each VLAN by clicking the corresponding **Edit** button. When enabled for IGMP snooping, the Switch can open or close a port to a specific multicast group member based on IGMP messages sent from the device to the IGMP host or vice versa. The Switch monitors IGMP messages and discontinues forwarding multicast packets when there are no longer hosts requesting that they continue.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Settings**, as shown below:

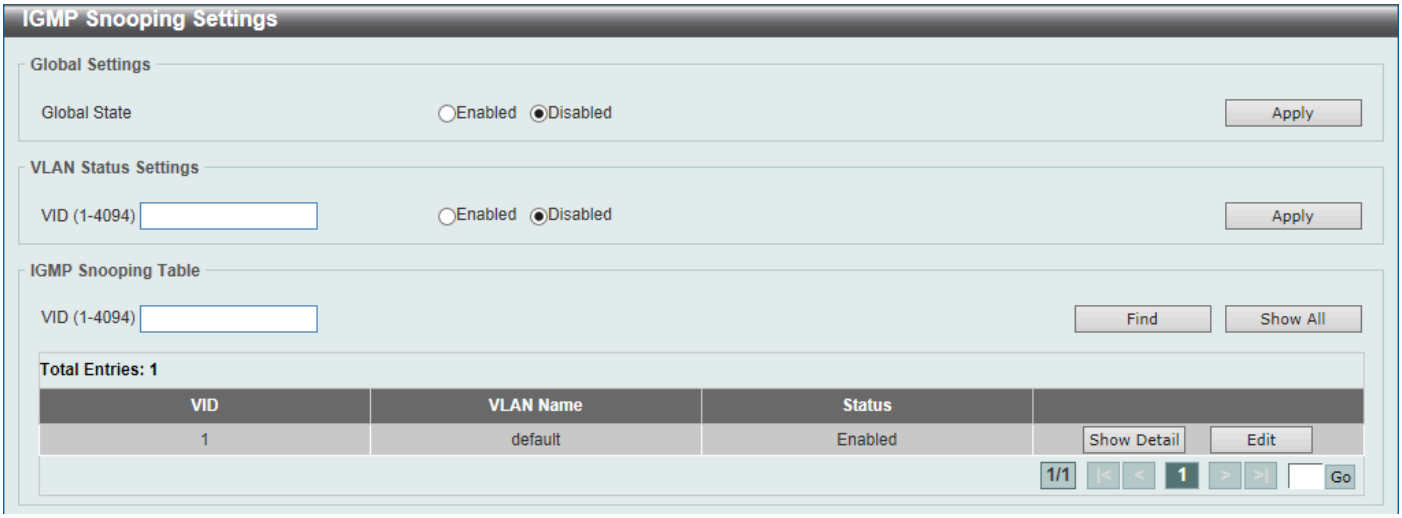


Figure 5-65 IGMP Snooping Settings Window

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

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

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

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

Parameter	Description
VID	Enter a single VLAN ID from 1 to 4094 and select to enable or disable IGMP snooping on the VLAN.

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

The fields that can be configured in **IGMP Snooping Table** are described below:

Parameter	Description
VID	Enter a VLAN ID from 1 to 4094.

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

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

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

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

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

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

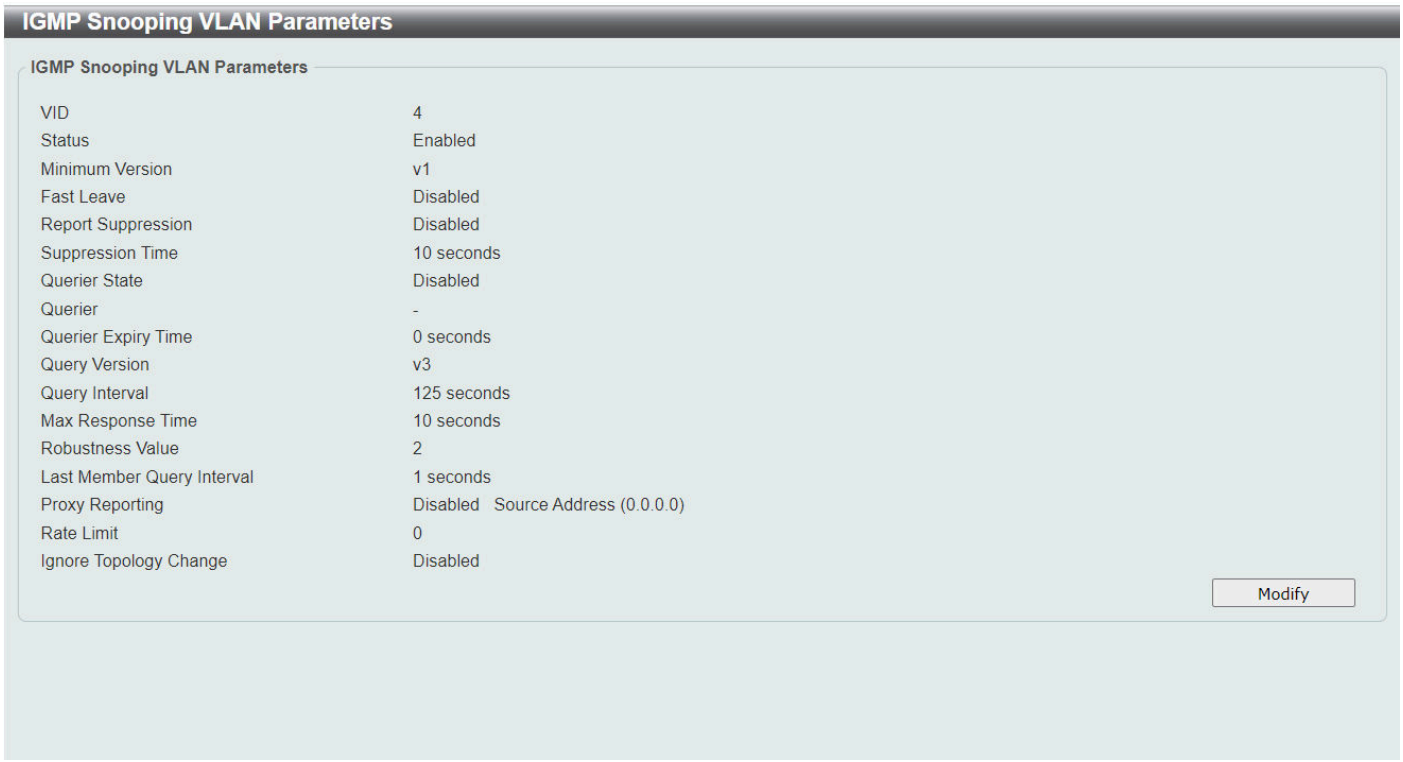


Figure 5-66 IGMP Snooping Settings (Show Detail) Window

The window displays the detail information about IGMP snooping VLAN.

Click the **Modify** button to edit the information in the following window.

After clicking the **Modify** or **Edit** button in IGMP Snooping Settings window, the following window will appear.

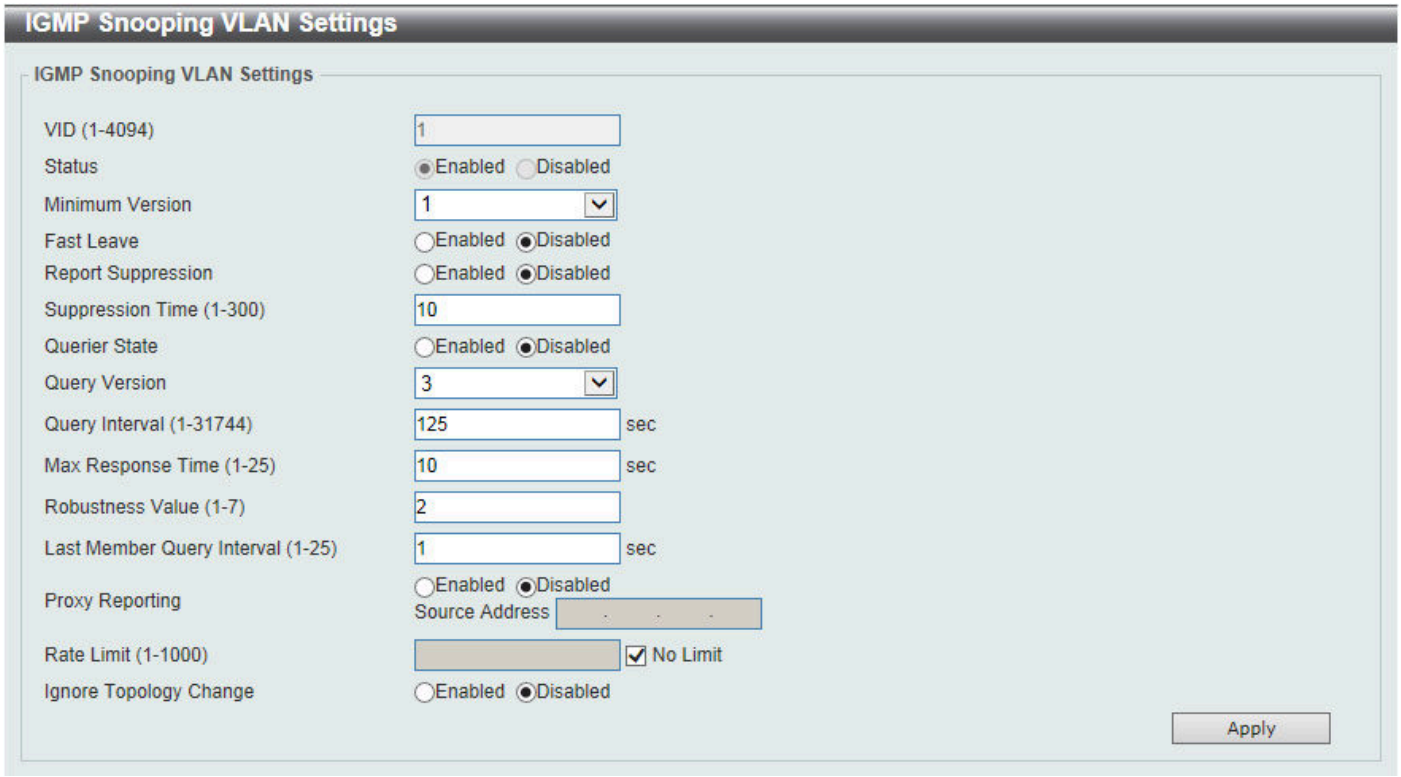


Figure 5-67 IGMP Snooping Settings (Modify, Edit) Window

The fields that can be configured are described below:

Parameter	Description
Minimum Version	Select the minimum IGMP host version that is allowed on the VLAN. Options to choose from are **1**, **2**, and **3**.
Fast Leave	Select this option to enable or disable the IGMP snooping Fast Leave function. If enabled, the membership is immediately removed when the system receives the IGMP leave message.
Report Suppression	Select this option to enable or disable the report suppression. The report suppression function only works for IGMPv1 and IGMPv2 traffic. When report suppression is enabled, the Switch suppresses the duplicate reports sent by hosts. The suppression for the same group report or leave will continue until the suppression time expires. For report or leave messages to the same group, only one report or leave message is forwarded. The remaining report and leave messages are suppressed.
Suppression Time	Enter the interval of suppressing duplicate IGMP reports or leaves. The range is from 1 to 300.
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.
Last Member Query Interval	Enter the interval at which the IGMP snooping querier sends IGMP group-specific or group-source-specific (channel) query messages. The range is from 1 to 25.
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.
Ignore Topology Change	Select to enable or disable the Ignore Topology Change feature here.

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

IGMP Snooping AAA Settings

This window is used to display and configure the IGMP snooping AAA settings.To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping AAA Settings**, as shown below:

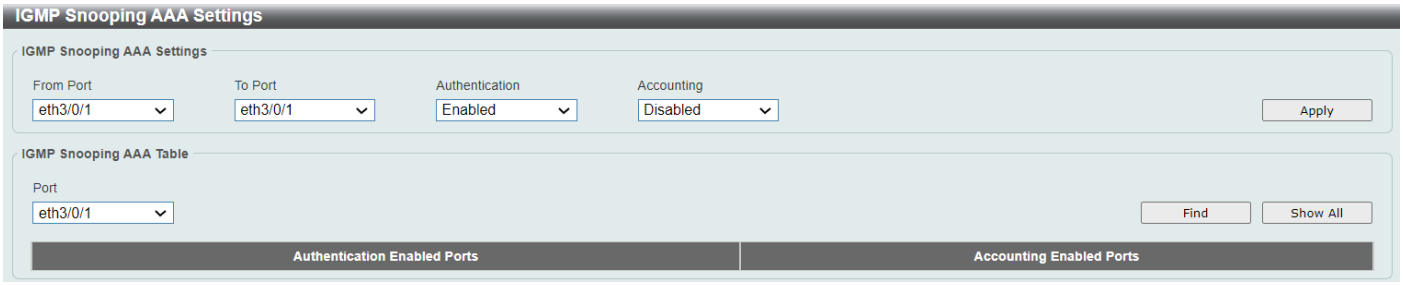


Figure 5-68 IGMP Snooping AAA Settings Window, accounting

The fields that can be configured in **IGMP Snooping AAA Settings** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Authentication	Select to enable or disable authentication here. This is used to enable or disable the authentication function for IGMP join messages. When enabled and the client wants to join a group, the system will perform authentication first.
Accounting	Select to enable or disable accounting here. This is used to enable or disable the accounting function for IGMP join messages. When enabled and the client wants to join a group, the system will perform accounting first.

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

The fields that can be configured in **IGMP Snooping AAA Table** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this display here.
From Port - To Port	Select the range of ports that will be used for this display here.

Click the **Find** button to generate the display based on the selections made.

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

IGMP Snooping Groups Settings

This window is used to display and configure the IGMP snooping static group, and view IGMP snooping group.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Groups Settings**, as shown below:

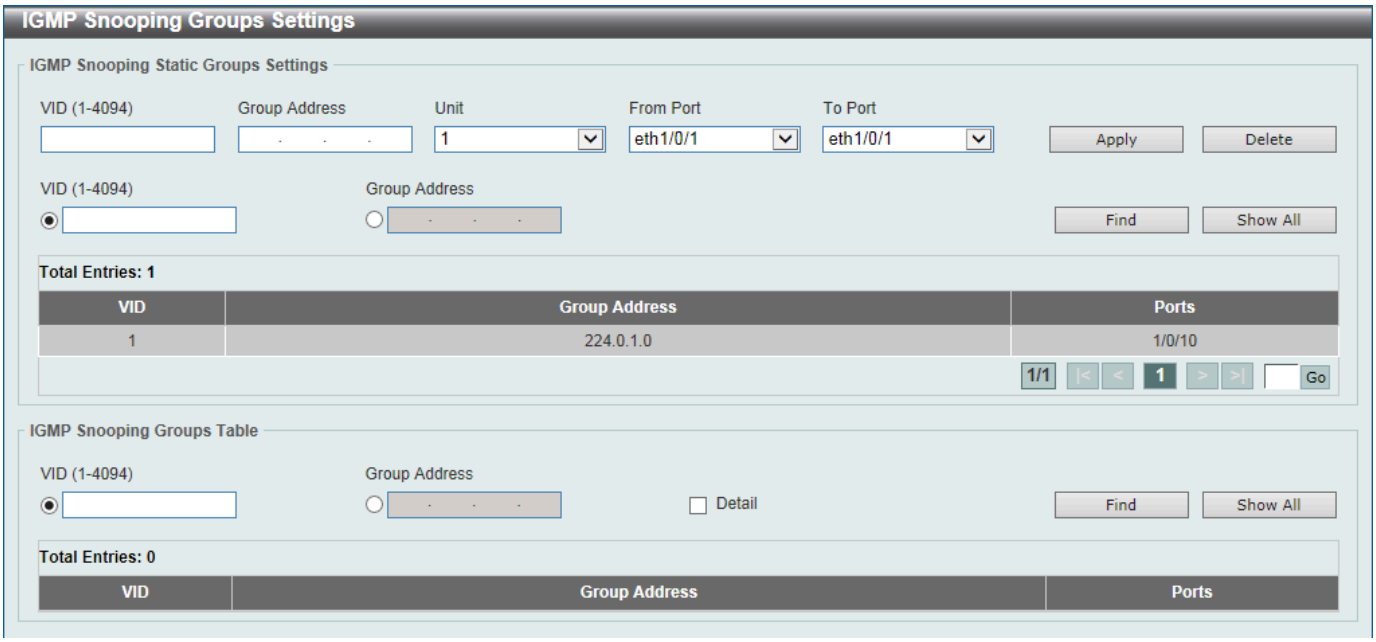


Figure 5-69 IGMP Snooping Groups Settings Window

The fields that can be configured in **IGMP Snooping Static Groups Settings** are described below:

Parameter	Description
VID	Enter a VLAN ID of the multicast group. The range is from 1 to 4094.
Group Address	Enter an IP multicast group address. Valid address range is from 224.0.0.0 to 239.255.255.255.
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
VID	Click the radio button and enter a VLAN ID of the multicast group. The range is from 1 to 4094.
Group Address	Click the radio button and enter an IP multicast group address.

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

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

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

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

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

The fields that can be configured in **IGMP Snooping Groups Table** are described below:

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

Click the **Find** button to locate a specific entry based on the information entered. Click the **Show All** button to view all the entries.

IGMP Snooping Filter Settings

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

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Filter Settings** as shown below:

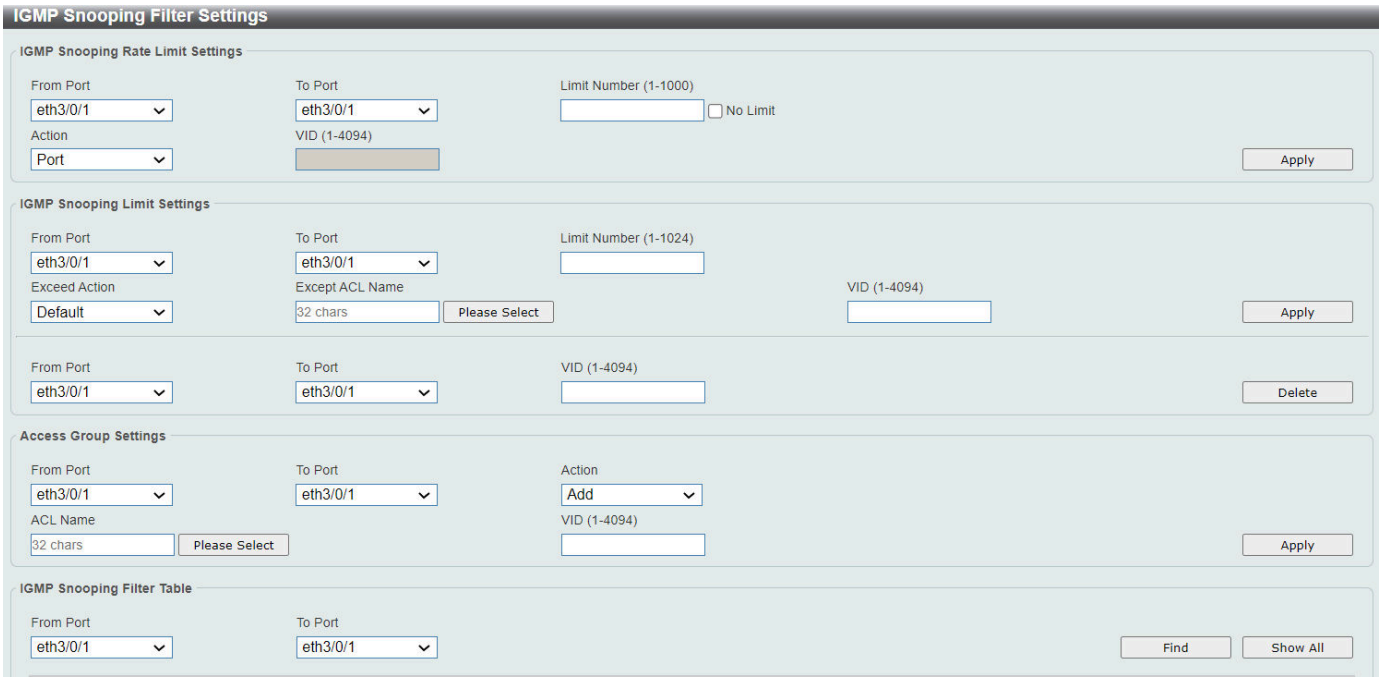


Figure 5-70 IGMP Snooping Filter Settings Window

The fields that can be configured in **IGMP Snooping Rate Limit Settings** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
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 (1-1000). Select **No Limit** to not restrict this value.
Action	Select **VLAN** or **Port** to force the restriction based on the specify VLAN ID or port range. If VLAN is selected, enter the VLAN ID in VID. If Port is selected, select the above port range.
VID	Enter the VLAN ID here. This is the Layer 2 VLAN on a trunk port and applies the filter to packets that arrive on that VLAN. The range is from 1 to 4094. This is only available if the **VLAN** option was selected as the action.

The fields that can be configured in **IGMP Snooping Limit Settings** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
Limit Number	Set a limit for the number of multicast groups (1-1024). Select **No Limit** to not restrict this value.

Parameter	Description
Exceed Action	Select Drop, Default, or Replace when the the number of IGMP multicast groups exceeds the above limit to specify the action for handling newly learned groups. Options to choose from are **Default**, **Drop** and **Replace**. • **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. Also enter the VLAN ID in VID when Replace is selected.
Except ACL Name	Enter the standard IP access list name here. The group (*,G) permitted by the access list will be excluded from the limit. 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 Layer 2 VLAN ID on a trunk port here. This applies the filter to packets that arrive on that VLAN. The range is from 1 to 4094.

Click **Apply** to save your changes. Or click **Delete** to delete a VLAN ID of the entered information of the above fields.

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

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the appropriate port range used for the access group configuration here. The Access Group allows you to define different IGMP snooping limit settings for a port that belongs to multiple VLANs or Access Control List.
Action	Select **Add** or **Delete** to add or delete the entered information of an access group.
ACL Name	Enter the standard IP access list name here if Add is selected in the **Action** field. 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 used for this configuration here. The range is from 1 to 4094.

The fields that can be configured in **IGMP Snooping Filter Table** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the appropriate port range used for display here.

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

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

Click Show Detail to view detail information of a specific entry.

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

IGMP Snooping Mrouter Settings

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

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Mrouter Settings**, as shown below:

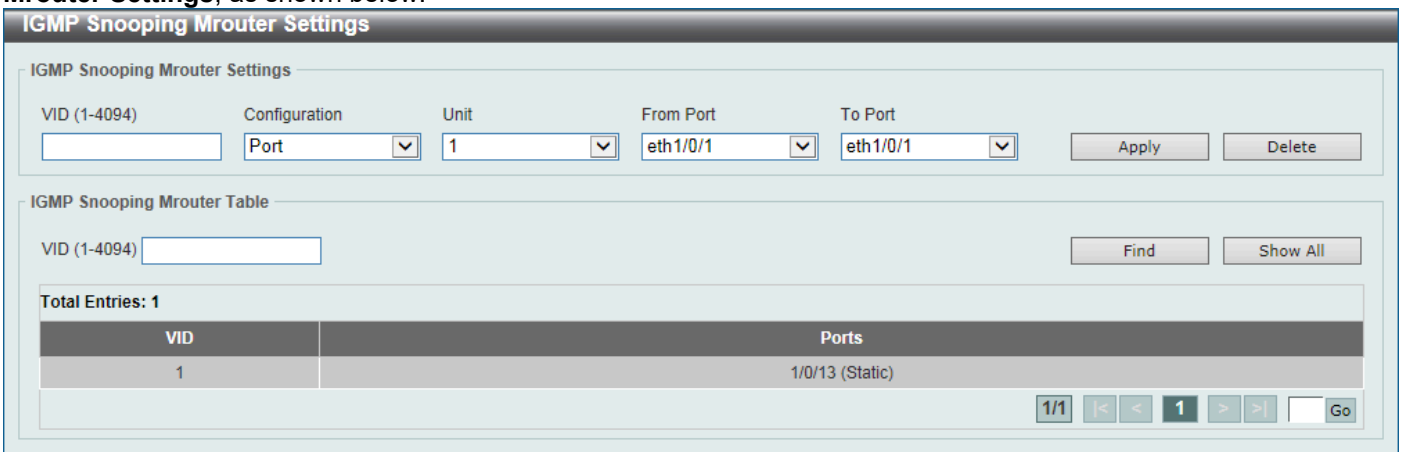


Figure 5-71 IGMP Snooping Mrouter Settings Window

The fields that can be configured in **IGMP Snooping Mrouter Settings** are described below:

Parameter	Description
VID	Enter the VLAN ID used here. The range is from 1 to 4094.
Configuration	Select the port configuration. Options to choose from are **Port**, and **Forbidden Port**. • **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.
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.

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

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

The fields that can be configured in **IGMP Snooping Mrouter Table** are described below:

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

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

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

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

IGMP Snooping Statistics Settings

This window is used to view and clear the IGMP snooping related statistics.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Statistics Settings**, as shown below:

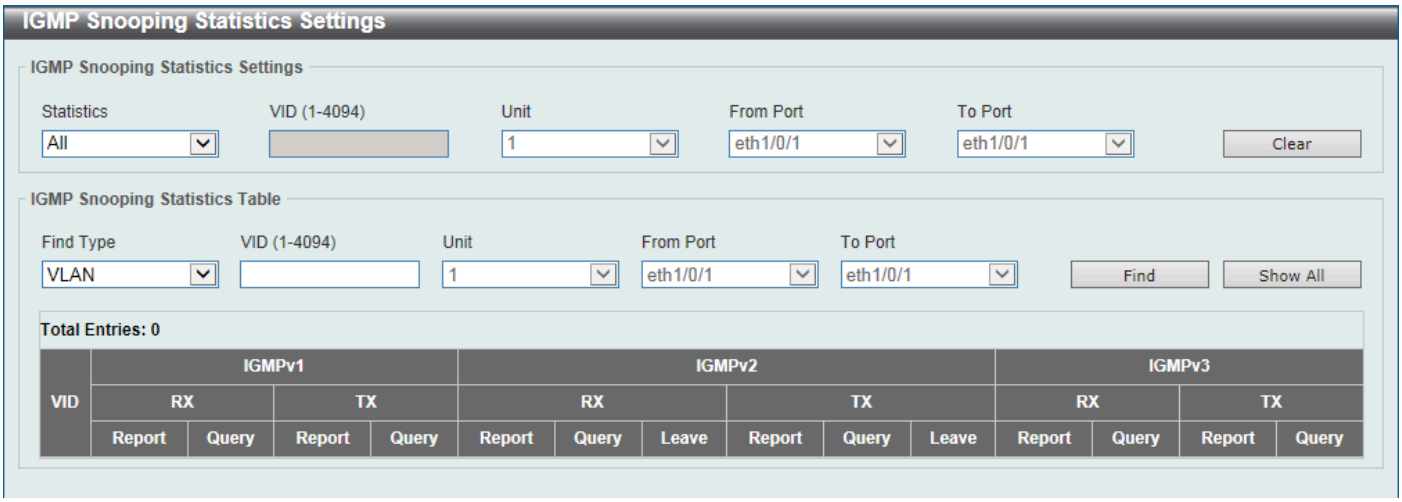


Figure 5-72 IGMP Snooping Statistics Settings Window

The fields that can be configured in **IGMP Snooping Statistics Settings** are described below:

Parameter	Description
Statistics	Select the interface here. Options to choose from are **All, VLAN**, and **Port**.
VID	Enter a VLAN ID between 1 and 4094. This is available when **VLAN** is selected in the **Statistics** drop-down list.
Unit	Select the Switch unit that will be used for this configuration here. This is available when **Port** is selected in the **Statistics** drop-down list and stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here. This is available when **Port** is selected in the **Statistics** drop-down list.

Click the **Clear** button to clear the IGMP snooping related statistics.

The fields that can be configured in **IGMP Snooping Statistics Table** are described below:

Parameter	Description
Find Type	Select the interface type. Options to choose from are **VLAN** and **Port**.
VID	Enter a VLAN ID between 1 and 4094. This is available when **VLAN** is selected in the **Find Type** drop-down list.
Unit	Select the Switch unit that will be used for this configuration here. This is available when **Port** is selected in the **Find Type** drop-down list.
From Port - To Port	Select the appropriate port range used for the configuration here. This is available when **Port** is selected in the **Find Type** drop-down list.

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

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

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

MLD Snooping

Multicast Listener Discovery (MLD) Snooping is an IPv6 function used similarly to IGMP snooping in IPv4. It is used to discover ports on a VLAN that are requesting multicast data. Instead of flooding all ports on a selected VLAN with multicast traffic, MLD snooping will only forward multicast data to ports that wish to receive this data through the use of queries and reports produced by the requesting ports and the source of the multicast traffic.

MLD snooping is accomplished through the examination of the layer 3 part of an MLD control packet transferred between end nodes and a MLD router. When the Switch discovers that this route is requesting multicast traffic, it adds the port directly attached to it into the correct IPv6 multicast table and begins the process of forwarding multicast traffic to that port. This entry in the multicast routing table records the port, the VLAN ID, and the associated multicast IPv6 multicast group address, and then considers this port to be an active listening port. The active listening ports are the only ones to receive multicast group data.

MLD Control Messages

These types of messages are transferred between devices using MLD snooping. These messages are all defined by four ICMPv6 packet headers, labeled 130, 131, 132, and 143.

- **Multicast Listener Query** - Similar to the IGMPv2 Host Membership Query for IPv4, and labeled as 130 in the ICMPv6 packet header, this message is sent by the router to ask if any link is requesting multicast data. There are two types of MLD query messages emitted by the router: the General Query, which is used to advertise all multicast addresses that are ready to send multicast data to all listening ports, and the Multicast Specific query, which is used to advertise a specific multicast address that is also ready. These two types of messages are distinguished by a multicast destination address located in the IPv6 header and a multicast address in the Multicast Listener Query Message.
- **Multicast Listener Report, Version 1** - Comparable to the Host Membership Report in IGMPv2, and labeled as 131 in the ICMP packet header, this message is sent by the listening port to the Switch stating that it is interested in receiving multicast data from a multicast address in response to the Multicast Listener Query message.
- **Multicast Listener Done** - Similar to the Leave Group Message in IGMPv2, and labeled as 132 in the ICMPv6 packet header, this message is sent by the multicast listening port stating that it is no longer interested in receiving multicast data from a specific multicast group address, therefore stating that it is “done” with the multicast data from this address. Once this message is received by the Switch, it will no longer forward multicast traffic from a specific multicast group address to this listening port.
- **Multicast Listener Report, Version 2** - Comparable to the Host Membership Report in IGMPv3, and labeled as 143 in the ICMP packet header, this message is sent by the listening port to the Switch stating that it is interested in receiving multicast data from a multicast address in response to the Multicast Listener Query message.

MLD Snooping Settings

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

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Settings**, as shown below:

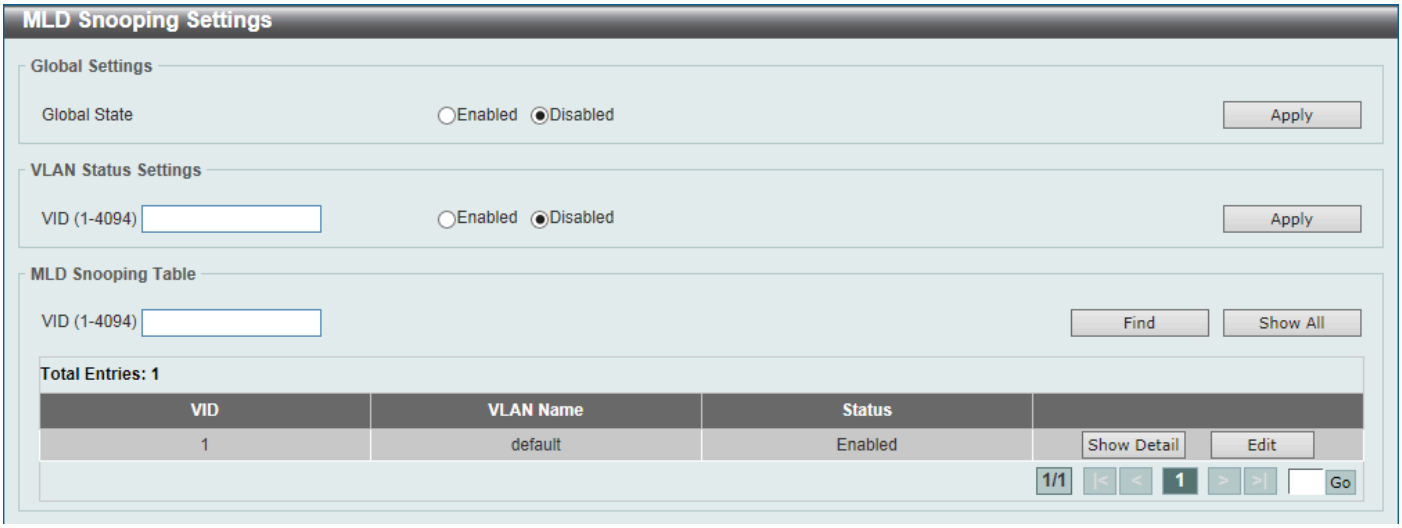


Figure 5-73 MLD Snooping Settings Window

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

Parameter	Description
Global State	Select this option to enable or disable the global MLD snooping state.

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

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

Parameter	Description
VID	Enter a VLAN ID from 1 to 4094 and select to enable or disable MLD snooping on the VLAN.

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

The fields that can be configured in **MLD Snooping Table** are described below:

Parameter	Description
VID	Enter a VLAN ID from 1 to 4094.

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

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

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

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

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

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

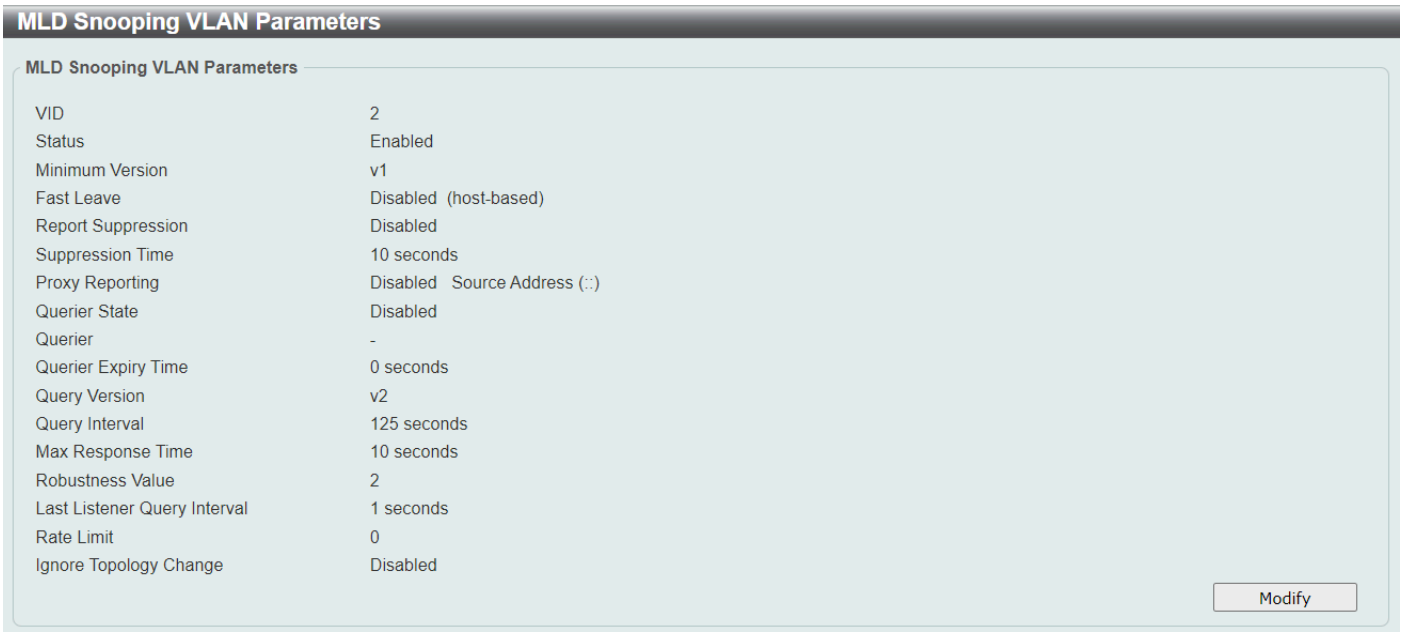


Figure 5-74 MLD Snooping Settings (Show Detail) Window

The window displays the detail information about MLD snooping VLAN.

Click the **Modify** button to edit the information in the following window. After clicking the **Modify** or **Edit** button in MLD Snooping Settings window, the following window will appear.

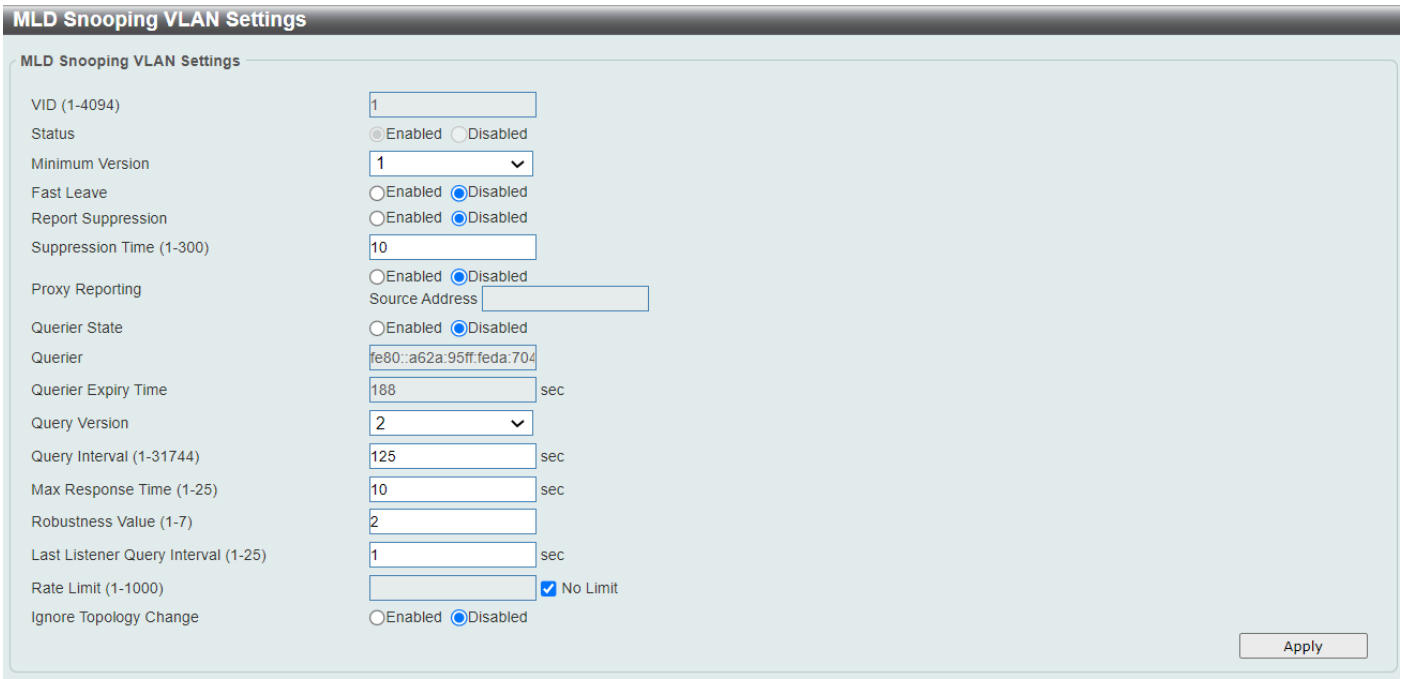


Figure 5-75 MLD Snooping Settings (Modify, Edit) Window

The fields that can be configured are described below:

Parameter	Description
Minimum Version	Select the minimum version of MLD hosts that is allowed on the VLAN. Options to choose from are **1** and **2**.
Fast Leave	Select this option to enable or disable the MLD snooping Fast Leave function. If enabled, the membership is immediately removed when the system receives the MLD leave message.
Report Suppression	Select this option to enable or disable the report suppression.
Suppression Time	Enter the interval of suppressing duplicate MLD reports or leaves. The range is from 1 to 300.
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.
Ignore Topology Change	Select to enable or disable the Ignore Topology Change feature here.

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

MLD Snooping Groups Settings

This window is used to display and configure the MLD snooping static group, and view MLD snooping group.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Groups Settings**, as shown below:

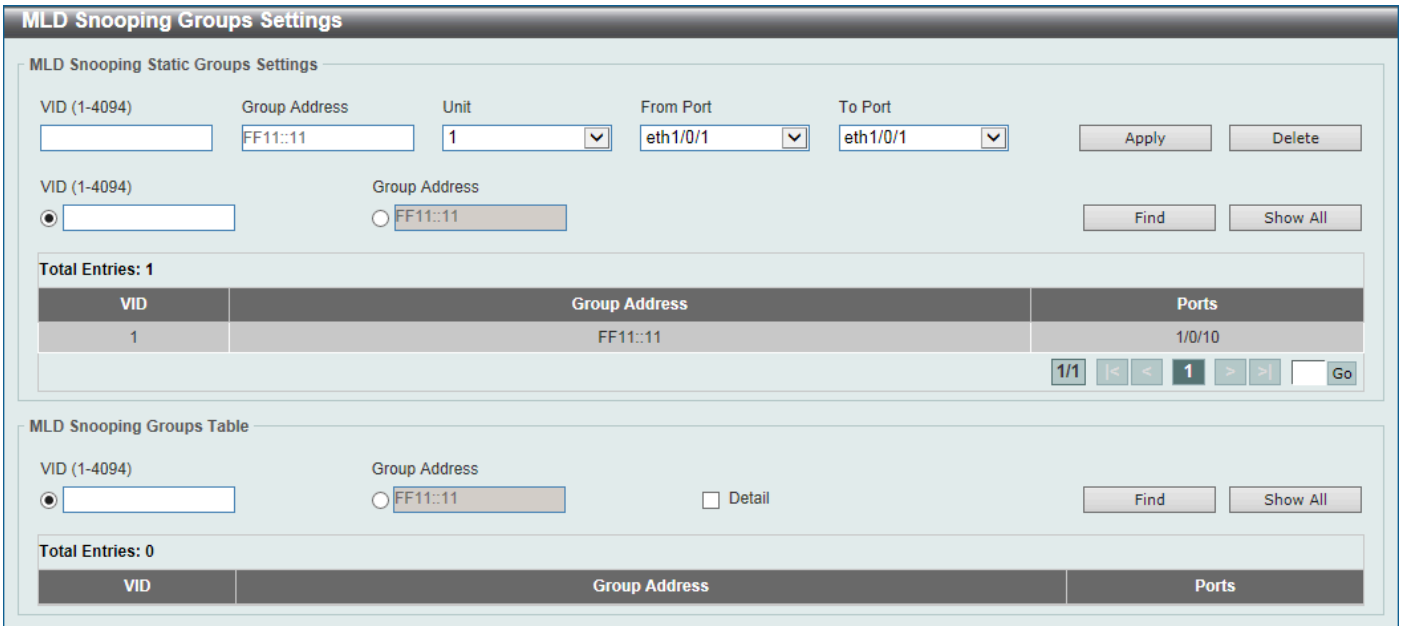


Figure 5-76 MLD Snooping Groups Settings Window

The fields that can be configured in **MLD Snooping Static Groups Settings** are described below:

Parameter	Description
VID	Enter the VLAN ID of the multicast group here. The range is from 1 to 4094.
Group Address	Enter the IPv6 multicast group address here. Valid IPv6 multicast addresses have the prefix ff00::/8.
Unit	Select the Switch unit that will be used for this configuration here. This option is only available if stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
VID	For search criteria, click the radio button and enter a VLAN ID of the multicast group. The range is from 1 to 4094.
Group Address	For search criteria, click the radio button and enter an IP multicast group address.

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

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

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

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

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

The fields that can be configured in **MLD Snooping Groups Table** are described below:

Parameter	Description
VID	Click the radio button and enter a VLAN ID of the multicast group. The range is from 1 to 4094.
Group Address	Click the radio button and enter an IP multicast group address.
Detail	Select this option to display the MLD group detail information.

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

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

MLD Snooping Filter Settings

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

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Filter Settings**, as shown below:

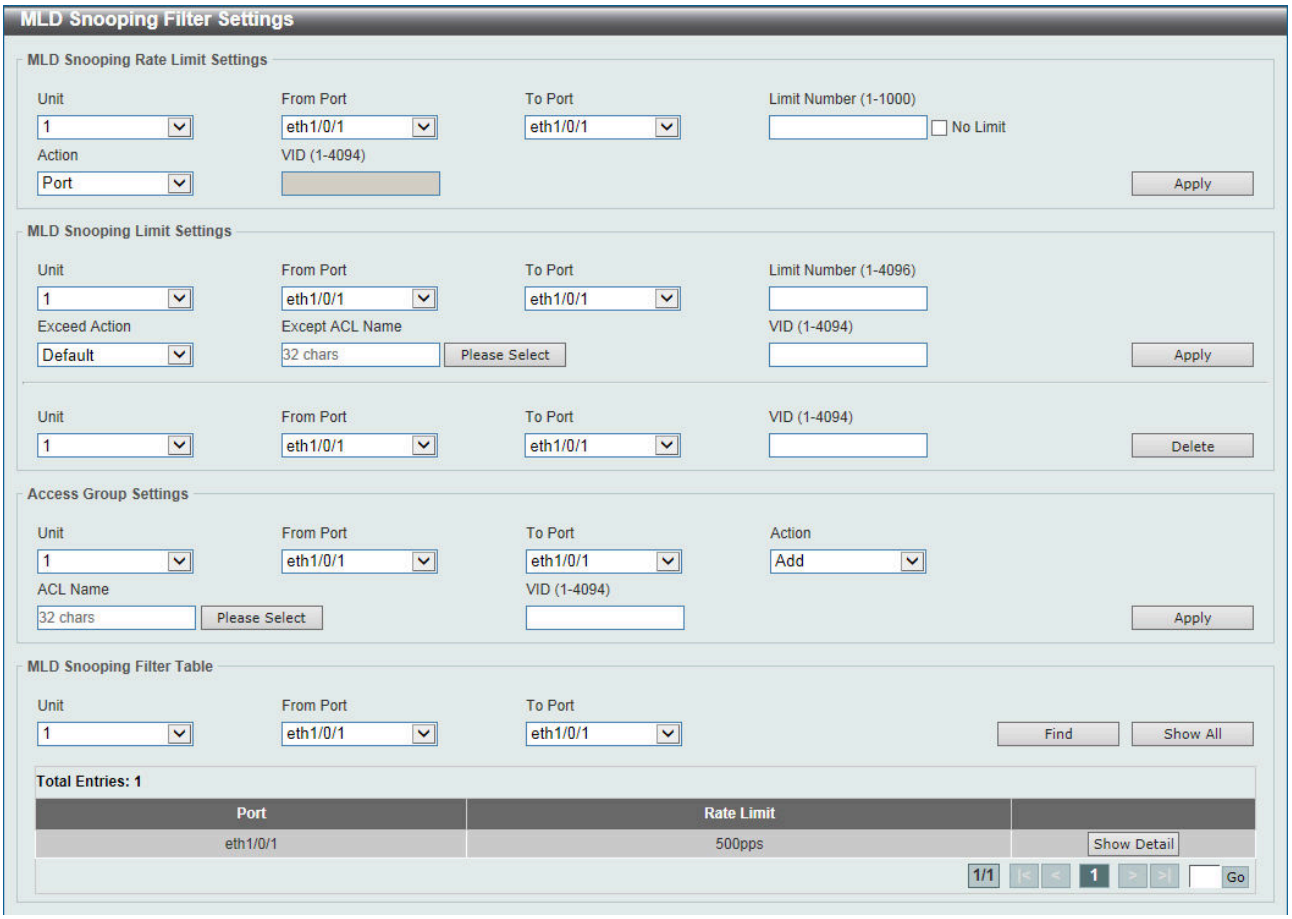


Figure 5-77 MLD Snooping Filter Settings Window

The fields that can be configured in **MLD Snooping Rate Limit Settings** are described below:

Parameter	Description
Unit	Select the Switch unit ID that will be used here.This option is only available when stacking enabled.
From Port - To Port	Select the Switch port range 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 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.
Action	Select the action that will be taken here. Options to choose from are **Port** and **VLAN**.

Parameter	Description
VID	Enter the VLAN ID here. This is the Layer 2 VLAN on a trunk port and applies the filter to packets that arrive on that VLAN. The range is from 1 to 4094. This is only available if the **VLAN** option was selected as the action.

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

The fields that can be configured in **MLD Snooping Limit Settings** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.This option is only available when stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration 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 1024.
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**, **Drop** and **Replace**. • **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) permitted by the access list will be excluded from the limit. 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 Layer 2 VLAN ID on a trunk port here. This applies the filter to packets that arrive on that VLAN. The range is from 1 to 4094.

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

Click the **Delete** button to delete an entry based on the information entered.

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

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration 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 used for this configuration here. The range is from 1 to 4094.

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

The fields that can be configured in **MLD Snooping Filter Table** are described below:

Parameter	Description
Unit	Select the Switch unit ID that will be used here. This option is only available when stacking is enabled.
From Port - To Port	Select the Switch port range that will be used here.

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

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

Click the **Show Detail** button to view more detailed information about the entry.

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

After clicking the **Please Select** button, the following page will appear.

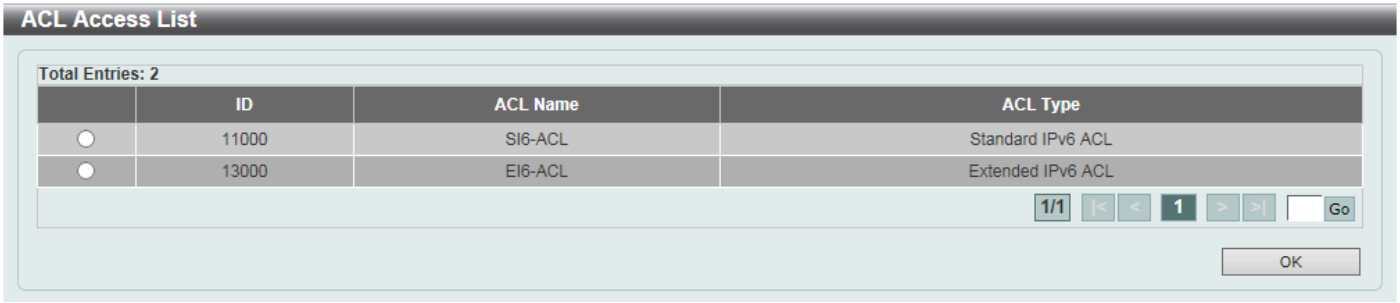


Figure 5-78 MLD Snooping Filter Settings (Please Select) Window

Select the ACL and click the **OK** button to use the selected access list.

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

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



Figure 5-79 MLD Snooping Filter Settings (Show Detail) Window

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

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

MLD Snooping Mrouter Settings

This window is used to display and configure the specified interface(s) as the router ports or forbidden to be IPv6 multicast router ports on the VLAN interface on the Switch.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Mrouter Settings**, as shown below:

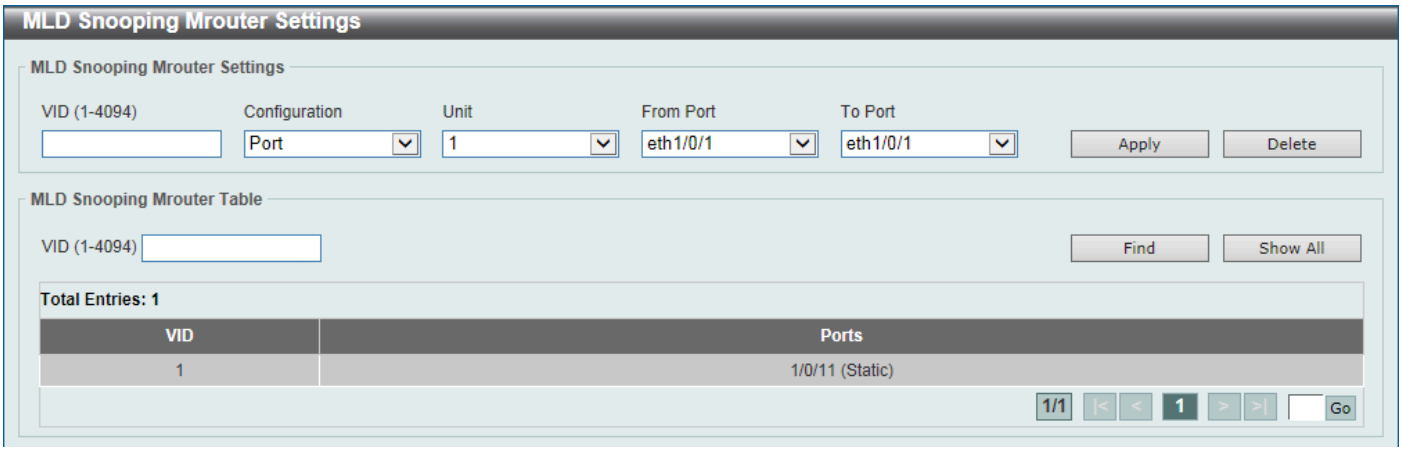


Figure 5-80 MLD Snooping Mrouter Settings Window

The fields that can be configured in **MLD Snooping Mrouter Settings** are described below:

Parameter	Description
VID	Enter a VLAN ID between 1 and 4094.
Configuration	Select the port configuration. Options to choose from are **Port**, **Forbidden Port**, and **Learn pimv6**. • **Port** - Select to have the configured ports as being connected to multicast-enabled routers. • **Forbidden Port** - Select to have the configured ports as being not connected to multicast-enabled routers. • **Learn pimv6** - Select to enable dynamic learning of multicast router port.
Unit	Select the Switch unit that will be used for this configuration here.This option is only available if stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.

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

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

The fields that can be configured in **MLD Snooping Mrouter Table** are described below:

Parameter	Description
VID	Enter a VLAN ID between 1 and 4094.

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

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

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

MLD Snooping Statistics Settings

This window is used to view and clear the MLD snooping related statistics.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Statistics Settings**, as shown below:

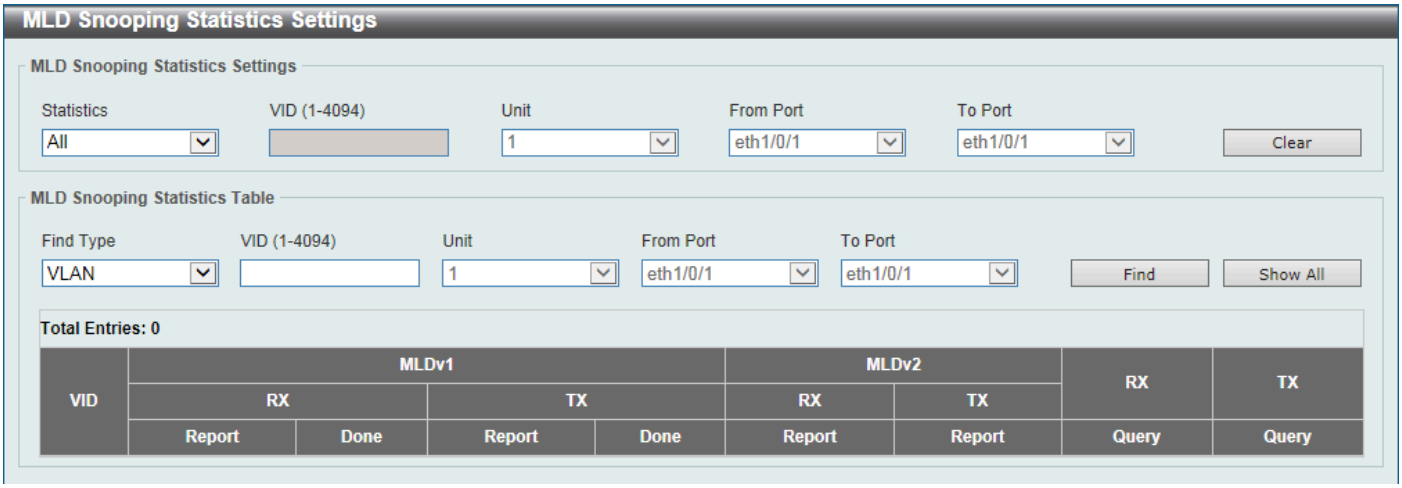


Figure 5-81 MLD Snooping Statistics Settings Window

The fields that can be configured in **MLD Snooping Statistics Settings** are described below:

Parameter	Description
Statistics	Select the interface here. Options to choose from are **All, VLAN**, and **Port**.
VID	Enter a VLAN ID between 1 and 4094. This is available when **VLAN** is selected in the **Statistics** drop-down list.
Unit	Select the Switch unit that will be used for this configuration here. This is available when **Port** is selected in the **Statistics** drop-down list and stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here. This is available when **Port** is selected in the **Statistics** drop-down list.

Click the **Clear** button to clear the MLD snooping related statistics.

The fields that can be configured in **MLD Snooping Statistics Table** are described below:

Parameter	Description
Find Type	Select the interface type. Options to choose from are **VLAN**, and **Port**.
VID	Enter a VLAN ID between 1 and 4094. This is available when **VLAN** is selected in the **Find Type** drop-down list.
Unit	Select the Switch unit that will be used for this configuration here. This is available when **Port** is selected in the **Statistics** drop-down list and stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here. This is available when **Port** is selected in the **Find Type** drop-down list.

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

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

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

Multicast VLAN

Multicast VLAN Settings

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

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

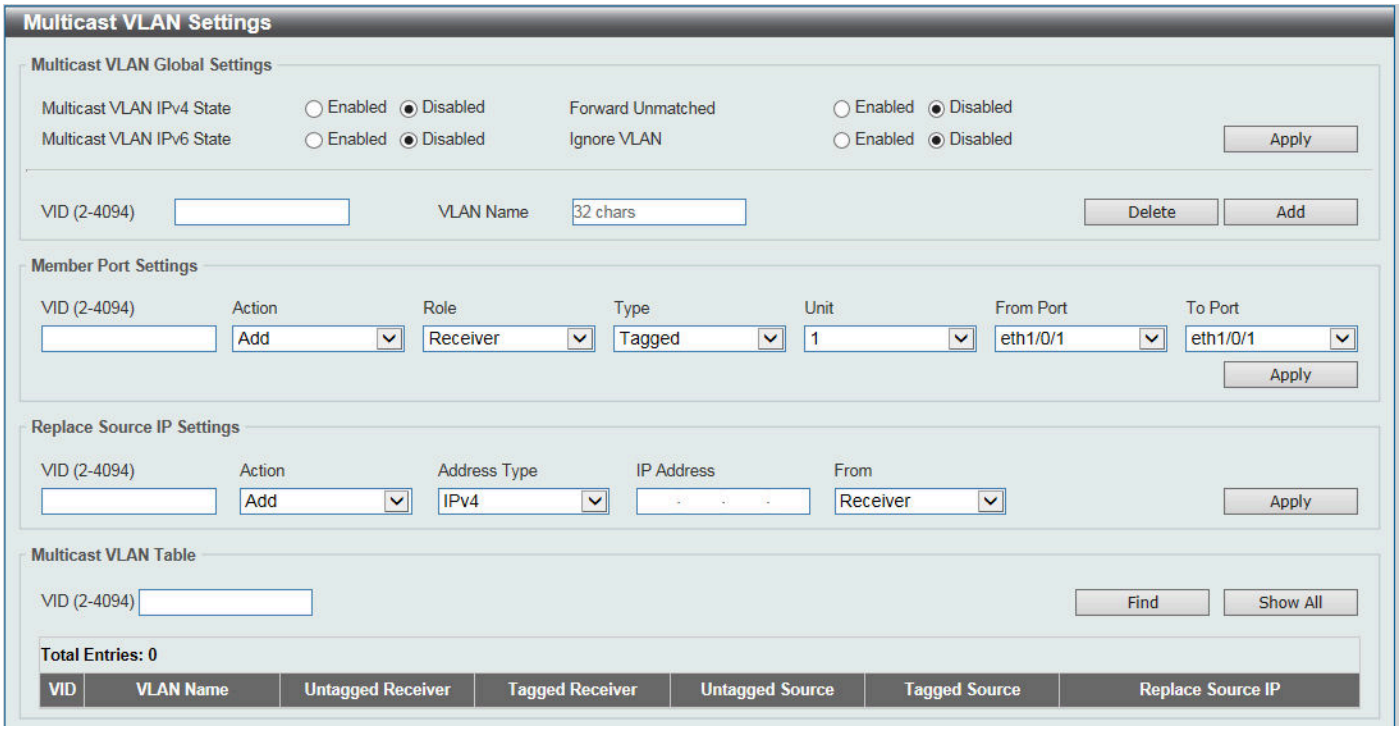


Figure 5-82 Multicast VLAN Settings Window

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

Parameter	Description
Multicast VLAN IPv4 State	Select to enable or disable the IPv4 IGMP control packet process in multicast VLANs.
Forward Unmatched	Select the enable or disable the Forward Unmatched feature here. This specifies that if the received IGMP or MLD control packet is untagged, does not match any profile, and the associated default VLAN is a multicast VLAN, or is tagged with a multicast VLAN, but does not match the associated profile, then the packet will be forwarded or dropped based on this setting. By default, the packet will be dropped.
Multicast VLAN IPv6 State	Select to enable or disable the IPv6 MLD control packet process in multicast VLANs.
Ignore VLAN	Select the enable or disable the ignore VLAN feature here. This specifies the setting for tagged IGMP or MLD control packets. If enabled, then the packet's VLAN is ignored and taken to match the profile to find its multicast VLAN. When this option is enabled, the Switch will ignore the VLAN of the receiving IGMP or MLD control packet and try to find a match profile.
VID	Enter the VLAN ID of the multicast VLAN that will be created or deleted here. The range is 2 to 4094.
VLAN Name	Enter the VLAN name of the multicast VLAN that will be created or deleted here.

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

Click the **Delete** button to delete an entry based on the information entered.

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

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

Parameter	Description
VID	Enter the multicast VLAN ID that will be used here. The range is 2 to 4094.
Action	Select **Add** to add a new entry based in the information entered. Select **Delete** to delete an entry based in the information entered.
Role	Select the role here. Options to choose from are **Receiver** and **Source**. • **Receiver** - Specifies to configure the port as a subscriber port that can only receive multicast data in the multicast VLAN. • **Source** - Specifies to configure the port as an uplink port that can send multicast data in the multicast VLAN.
Type	Select the type here. Options to choose from are **Tagged** and **Untagged**. • **Tagged** - Specifies that if a port is a tagged member, the packets sent from the port are tagged with the Multicast VLAN ID. • **Untagged** - Specifies that if the port is an untagged member, then the packets will be forwarded in the untagged form.
Unit	Select the Switch unit ID that will be used here.This option is only available if stacking is enabled.
From Port - To Port	Select the Switch port range that will be used here.

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

The fields that can be configured in **Replace Source IP Settings** are described below:

Parameter	Description
VID	Enter the multicast VLAN ID that will be used here. The range is 2 to 4094.
Action	Select **Add** to add a new entry based in the information entered. Select **Delete** to delete an entry based in the information entered.
Address Type	Select the address type here. Options to choose from are **IPv4** and **IPv6**. • **IPv4** - Specifies to enter the source IPv4 address for IGMP control packet reporting. • **IPv6** - Specifies to enter the source IPv6 address for MLD control packet reporting.
IP Address	Enter the IPv4/IPv6 address here.
From	Select the “from” option here. Options to choose from are **Receiver**, **Source**, and **Both**. • **Receiver** - Specifies that the source IPv4/IPv6 address of the IGMP/MLD report/leave packet received on any multicast VLAN receiver port will be replaced. • **Source** - Specifies that the source IPv4/IPv6 address of the IGMP/MLD report/leave packet received on any multicast VLAN source port will be replaced. • **Both** - Specifies that the source IPv4/IPv6 address of the IGMP/MLD report/leave packet received on any port in the multicast VLAN will be replaced.

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

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

Parameter	Description
VID	Enter the multicast VLAN ID that will be used here. The range is 2 to 4094.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to view all the entries.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Multicast VLAN Group Settings

This widow is used to view and configure the multicast VLAN group settings.

To view the following window, click **L2 Features > L2 Multicast Control > Multicast VLAN > Multicast VLAN Group Settings**, as shown below:

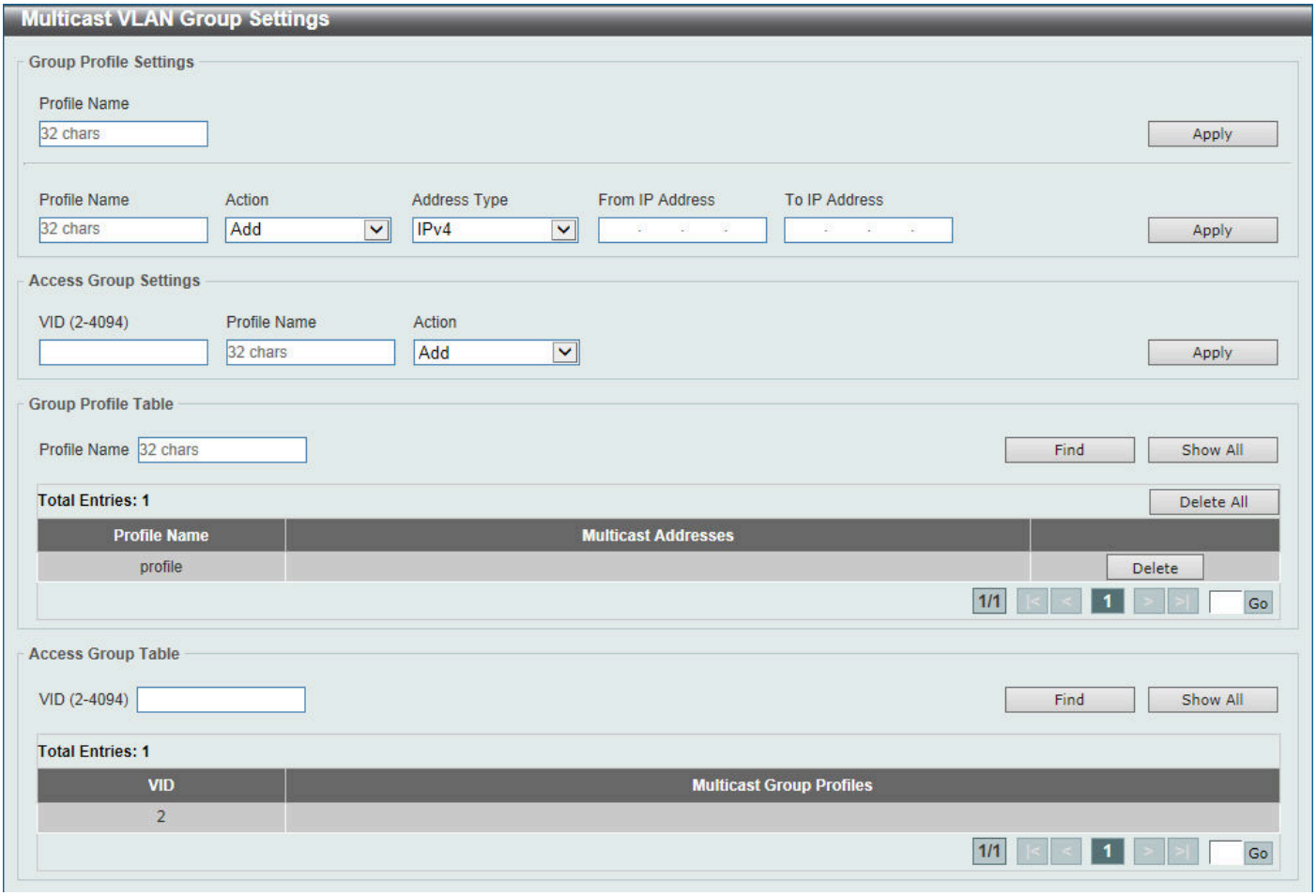


Figure 5-83 Multicast VLAN Group Settings Window

The fields that can be configured in **Group Profile Settings** are described below:

Parameter	Description
Profile Name	Enter the group profile name for the multicast VLAN feature here. This name can be up to 32 characters long.

Parameter	Description
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**. Multiple ranges can be added to a multicast VLAN profile. The IP address ranges, specified in a single profile, must be of the same address family.
Address Type	Select the address type here. Options to choose from are **IPv4** and **IPv6**. • **IPv4** - Specifies to use IPv4 multicast addresses in the range. • **IPv6** - Specifies to use IPv6 multicast addresses in the range.
From IP Address	Enter the source IPv4/IPv6 address here.
To IP Address	Enter the destination IPv4/IPv6 address here.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Access Group Settings** are described below:

Parameter	Description
VID	Enter the multicast VLAN ID that will be used here. The range is 2 to 4094.
Profile Name	Enter the group profile name for the multicast VLAN feature 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**. This is to add or delete the multicast group entirely.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Group Profile Table** are described below:

Parameter	Description
Profile Name	Enter the group profile name for the multicast VLAN feature here. This name can be up to 32 characters long.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to display all the entries.

Click the **Delete All** button to delete all the entries found in the display table.

Click the **Delete** button to delete the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

The fields that can be configured in **Access Group Table** are described below:

Parameter	Description
VID	Enter the multicast VLAN ID that will be used here. The range is 2 to 4094.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to display all the entries.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Multicast Filtering

This window is used to display and configure the Layer 2 multicast filtering settings.

To view the following window, click **L2 Features > L2 Multicast Control > Multicast Filtering**, as shown below:

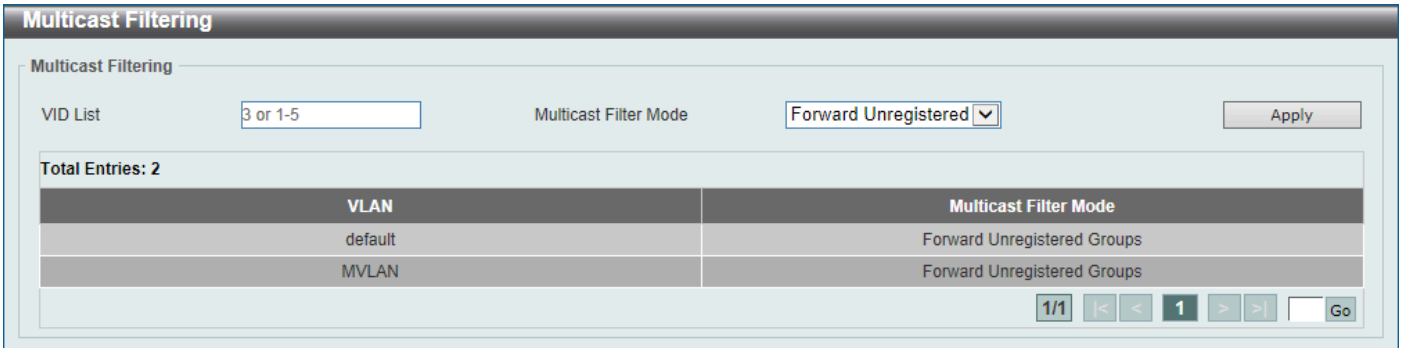


Figure 5-84 Multicast Filtering Window

The fields that can be configured are described below:

Parameter	Description
VID List	Enter the VLAN ID list that will be used for this configuration here.
Multicast Filter Mode	Select the multicast filter mode here. Options to choose from are **Forward Unregistered**, **Forward All**, and **Filter Unregistered**. • When selecting the **Forward Unregistered** option, registered multicast packets will be forwarded based on the forwarding table and all unregistered multicast packets will be flooded based on the VLAN domain. • When selecting the **Forward All** option, all multicast packets will be flooded based on the VLAN domain. • When selecting the **Filter Unregistered** option, registered packets will be forwarded based on the forwarding table and all unregistered multicast packets will be filtered.

Click the **Apply** button to accept the changes made.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

LLDP

LLDP Global Settings

This window is used to display and configure the global LLDP settings.

To view the following window, click **L2 Features > LLDP > LLDP Global Settings**, as shown below:

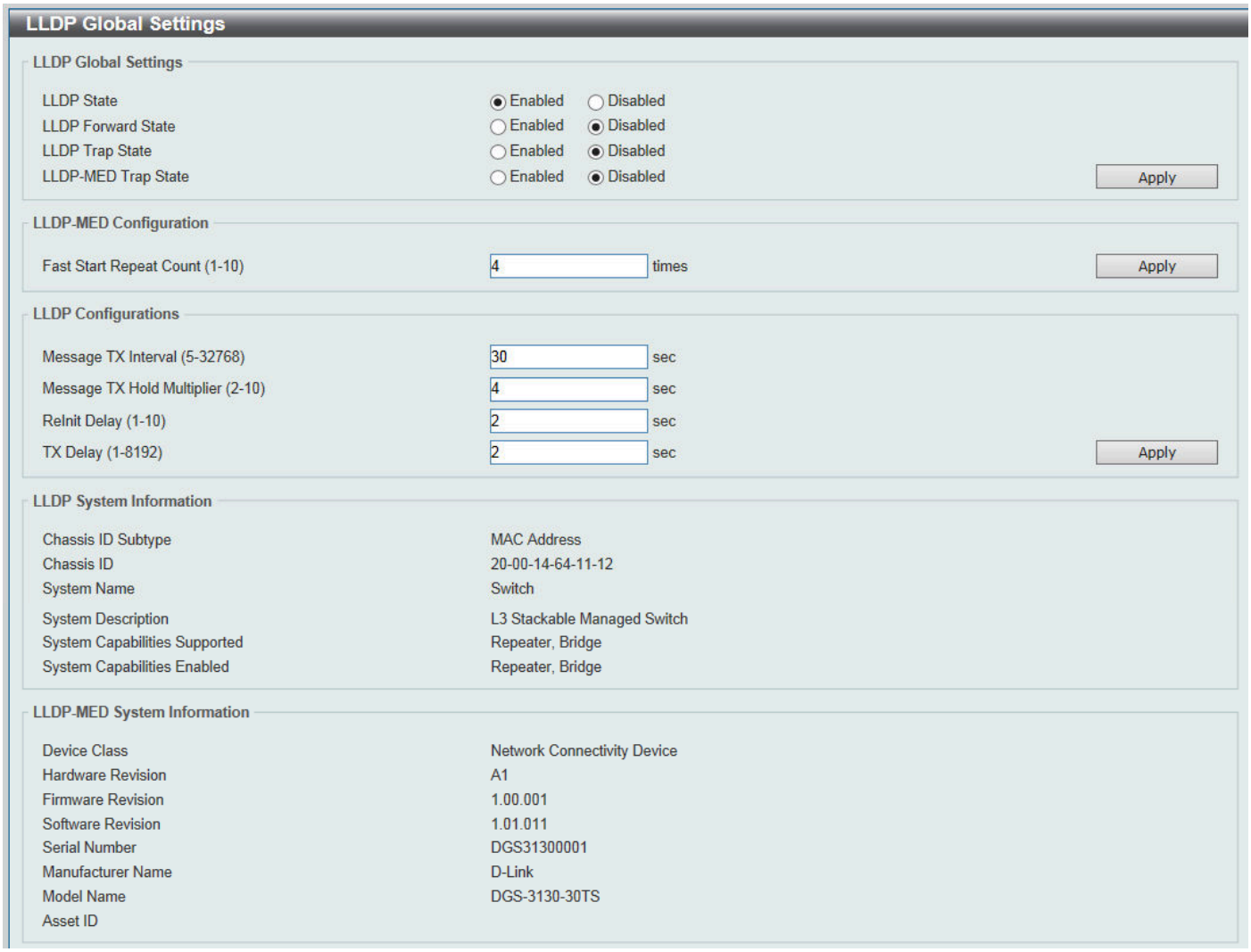


Figure 5-85 LLDP Global Settings Window

The fields that can be configured in **LLDP Global Settings** are described below:

Parameter	Description
LLDP State	Select this option to enable or disable the LLDP feature
LLDP Forward State	Select this option to enable or disable LLDP forward state. When the **LLDP State** is disabled and **LLDP Forward Sate** is enabled, the received LLDPDU packet will be forwarded.
LLDP Trap State	Select this option to enable or disable the LLDP trap state.
LLDP-MED Trap State	Select this option to enable or disable the Link Layer Discovery Protocol-Media Endpoint Discover (LLDP-MED) trap state.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **LLDP-MED Settings** are described below:

Parameter	Description
Fast Start Repeat Count	Enter the LLDP-MED fast start repeat count value. This value must be between 1 and 10.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **LLDP Configurations** are described below:

Parameter	Description
Message TX Interval	Enter the interval between consecutive transmissions of LLDP advertisements on each physical interface. The range is from 5 to 32768 seconds.
Message TX Hold Multiplier	Enter the multiplier on the LLDPDUs transmission interval that used to calculate the TTL value of an LLDPDU. This value must be between 2 and 10.
ReInit Delay	Enter the delay value for LLDP initialization on an interface. This value must be between 1 and 10 seconds.
TX Delay	Enter the delay value for sending successive LLDPDUs on an interface. The valid values are from 1 to 8192 seconds and should not be greater than one-fourth of the transmission interval timer.

Click the **Apply** button to accept the changes made.

LLDP Port Settings

This window is used to display and configure the LLDP port settings.

To view the following window, click **L2 Features > LLDP > LLDP Port Settings**, as shown below:

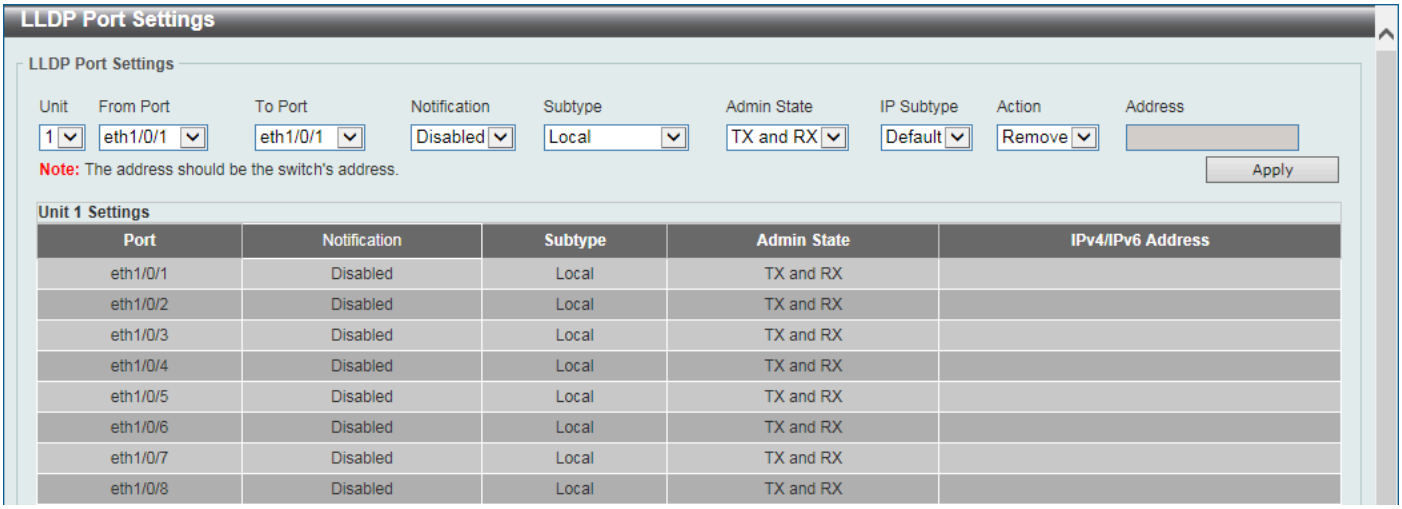


Figure 5-86 LLDP Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
Notification	Select to enable or disable the notification feature here.
Subtype	Select the subtype of LLDP TLV(s). Options to choose from are **MAC Address**, and **Local**.
Admin State	Select the local LLDP agent and allow it to send and receive LLDP frames on the port. Options to choose from are **TX**, **RX**, **TX and RX**, and **Disabled**. • **TX** - The local LLDP agent can only transmit LLDP frames. • **RX** - The local LLDP agent can only receive LLDP frames.

Parameter	Description
	• **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 value 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**. The default indicates that no IP address information will be included.
Action	Select the action that will be taken here. Options to choose from are **Remove** and **Add**.
Address	Enter the switch's management IP address for the corresponding IP Subtype selected.

Click the **Apply** button to accept the changes made.

NOTE: The IPv4 or IPv6 address entered here should be an existing LLDP management IP address.

LLDP Management Address List

This window is used to view the LLDP management address list.

To view the following window, click **L2 Features > LLDP > LLDP Management Address List**, as shown below:



Figure 5-87 LLDP Management Address List Window

The fields that can be configured are described below:

Parameter	Description
Subtype	Select the subtype. Options to choose from are **All**, **IPv4** and **IPv6**. After selecting the **IPv4** option, enter the IPv4 address in the space provided. After selecting the **IPv6** option, enter the IPv6 address in the space provided.

Click the **Find** button to locate a specific entry based on the selection made.

LLDP Basic TLVs Settings

The Type-Length-Value (TLV) field allows specific information to be sent within LLDP packets. This window is used to configure basic TLV settings. An active LLDP port on the Switch always includes mandatory data in its outbound advertisements. There are four optional data types that can be configured to exclude one or more of these data types from outbound LLDP advertisements. The mandatory data type includes four basic types of TLVs: end of LLDPDU TLV, chassis ID TLV, port ID TLV, and TTL TLV. The mandatory data types cannot be disabled. There are also four

data types which can be optionally selected. These include: Port Description, System Name, System Description and System Capability.

To view the following window, click **L2 Features > LLDP > LLDP Basic TLVs Settings**, as shown below:

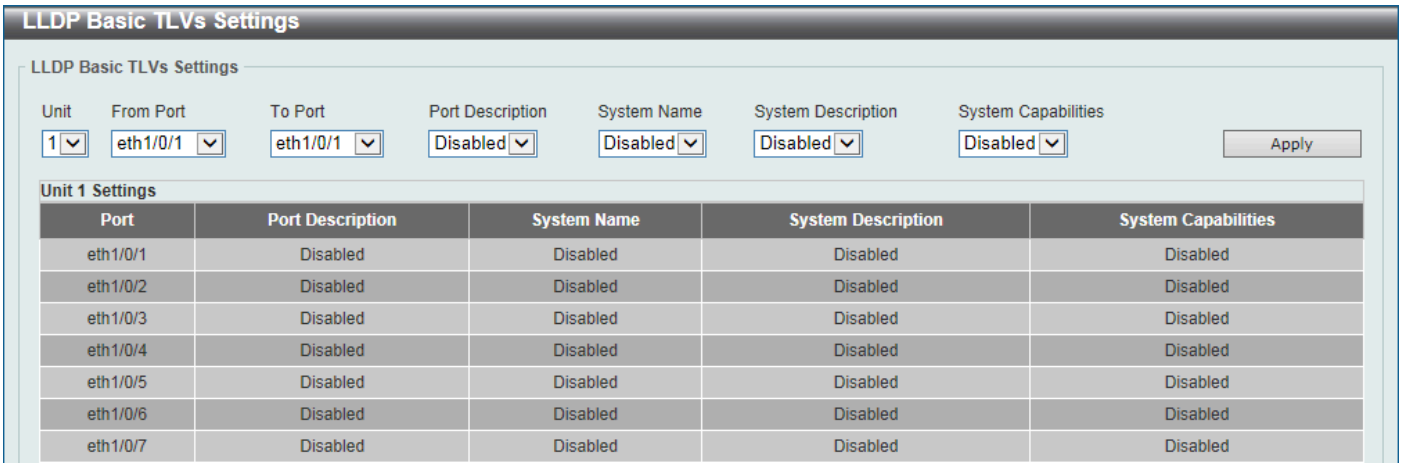


Figure 5-88 LLDP Basic TLVs Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
Port Description	Select this option to enable or disable the Port Description option.
System Name	Select this option to enable or disable the System Name option.
System Description	Select this option to enable or disable the System Description option.
System Capabilities	Select this option to enable or disable the System Capabilities option.

Click the **Apply** button to accept the changes made.

LLDP Dot1 TLVs Settings

The LLDP Dot1 TLVs Settings page is used to enable or disable outbound LLDP advertisements for IEEE 802.1 organizationally unique port VLAN ID TLVs.

To view the following window, click **L2 Features > LLDP > LLDP Dot1 TLVs Settings**, as shown below:

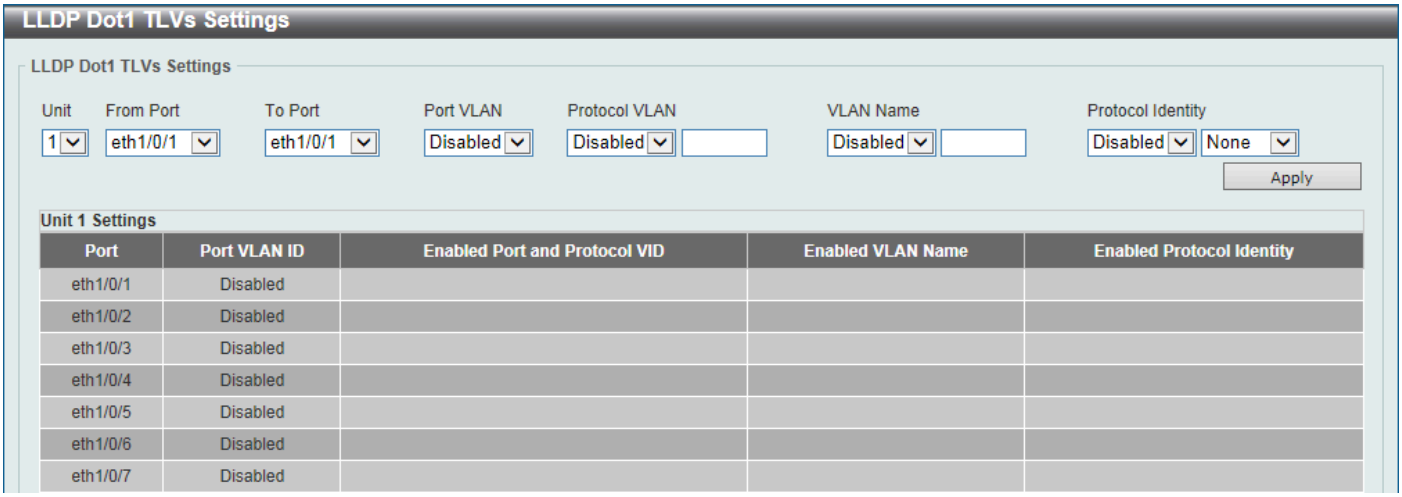


Figure 5-89 LLDP Dot1 TLVs Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.This option is only available when stacking is enbled.
From Port - To Port	Select the appropriate port range used for the configuration here.
Port VLAN	Select this option to enable or disable sending the port VLAN ID TLV. The Port VLAN ID TLV is an optional fixed length TLV that allows a VLAN bridge port to advertise the port VLAN ID (PVID) that will be associated with untagged or priority tagged frames.
Protocol VLAN	Select this option to enable or disable sending the Port and Protocol VLAN ID (PPVID) TLV. Enter the VLAN ID in PPVID TLV.
VLAN Name	Select this option to enable or disable sending the VLAN name TLV. Enter the ID of the VLAN in the VLAN name TLV.
Protocol Identity	Select this option to enable or disable sending the Protocol Identity TLV and the protocol name. Options for protocol name to choose from are **None, EAPOL, LACP, GVRP, STP**, and **All**.

Click the **Apply** button to accept the changes made.

LLDP Dot3 TLVs Settings

The LLDP Dot3 TLVs Settings page is used to enable or disable outbound LLDP advertisements for IEEE 802.3 organizationally unique TLVs.

To view the following window, click **L2 Features > LLDP > LLDP Dot3 TLVs Settings**, as shown below:

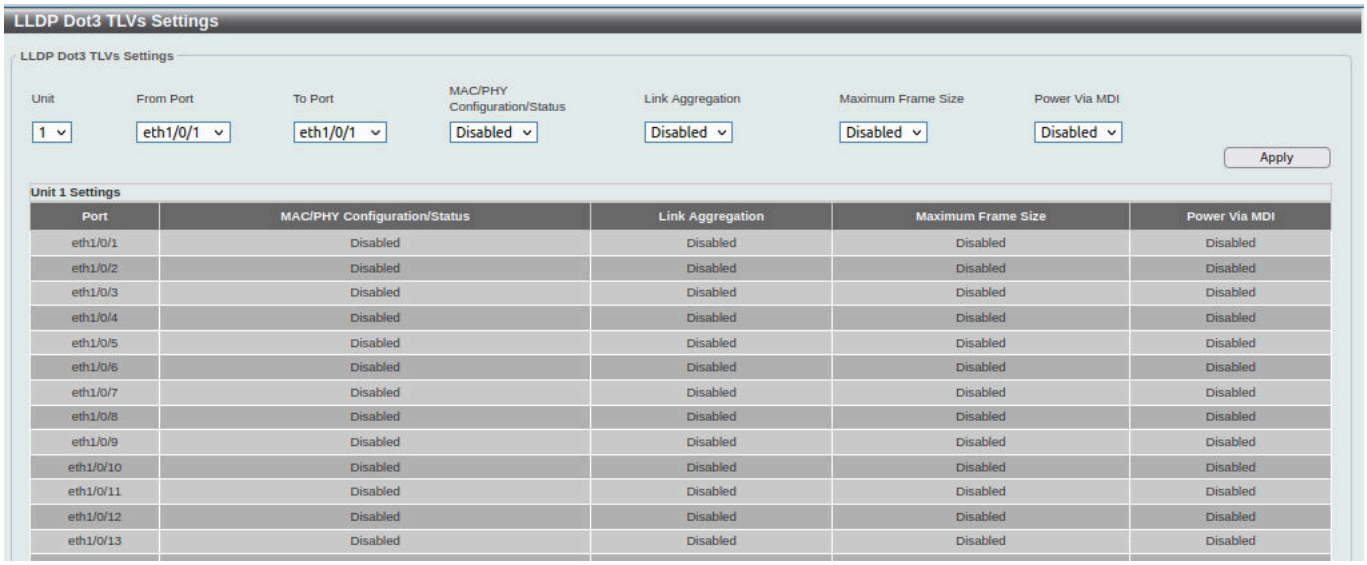


Figure 5-90 LLDP Dot3 TLVs Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
MAC/PHY Configuration/Status	Select this option to enable or disable the MAC/PHY Configuration/Status TLV to send. The MAC/PHY Configuration/Status TLV is an optional TLV that identifies (1) the duplex and bit-rate capability of the sending IEEE 802.3 LAN node, and (2) the current duplex and bit-rate settings of the sending IEEE 802.3 LAN node.
Link Aggregation	Select this option to enable or disable the Link Aggregation TLV to send. The Link Aggregation TLV indicates contains the following information. Whether the link is capable of being aggregated, whether the link is currently in an aggregation, and the aggregated port channel ID of the port. If the port is not aggregated, then the ID is 0.
Maximum Frame Size	Select this option to enable or disable the Maximum Frame Size TLV to send. The Maximum Frame Size TLV indicates the maximum frame size capability of the implemented MAC and PHY.
Power Via MDI	Enable or disable power management between network devices and connected media endpoints through LLDP power with media dependent interface (MDI).

Click the **Apply** button to accept the changes made.

LLDP-MED Port Settings

The LLDP-MED Port Settings page is used to enable or disable outbound LLDP advertisements for LLDP-MED TLVs.

To view the following window, click **L2 Features > LLDP > LLDP-MED Port Settings**, as shown below:

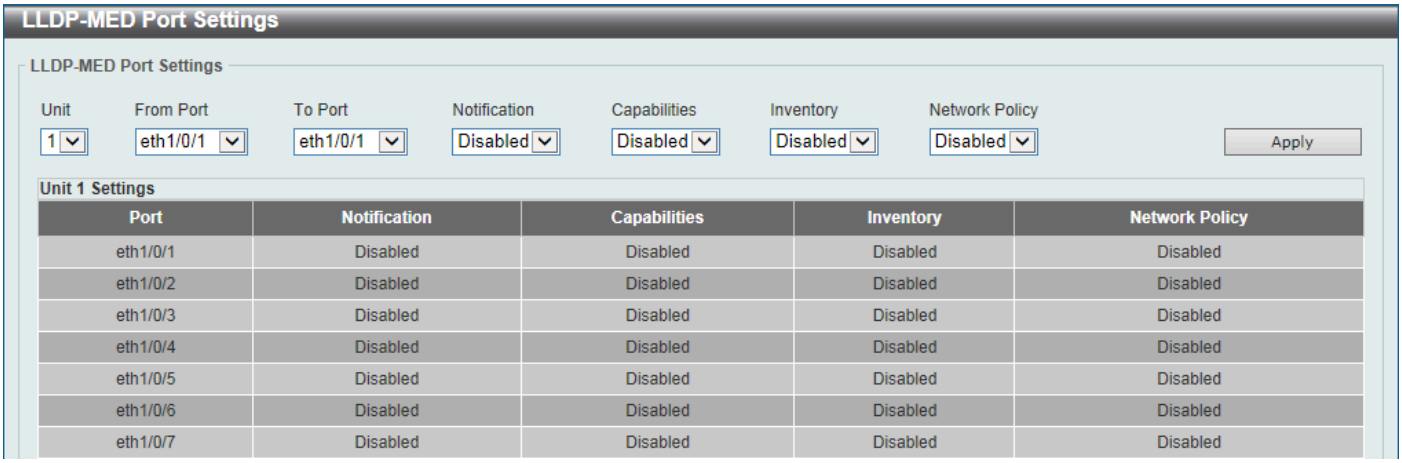


Figure 5-91 LLDP-MED Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
Notification	Select this option to enable or disable transmitting the LLDP-MED notification TLV.
Capabilities	Select this option to enable or disable transmitting the LLDP-MED capabilities TLV.
Inventory	Select this option to enable or disable transmitting the LLDP-MED inventory management TLV.
Network Policy	Select this option to enable or disable transmitting the LLDP-MED network policy TLV.

Click the **Apply** button to accept the changes made.

LLDP Statistics Information

This window is used to view the neighbor detection activity, LLDP Statistics and the settings for individual ports on the Switch.

To view the following window, click **L2 Features > LLDP > LLDP Statistics Information**, as shown below:

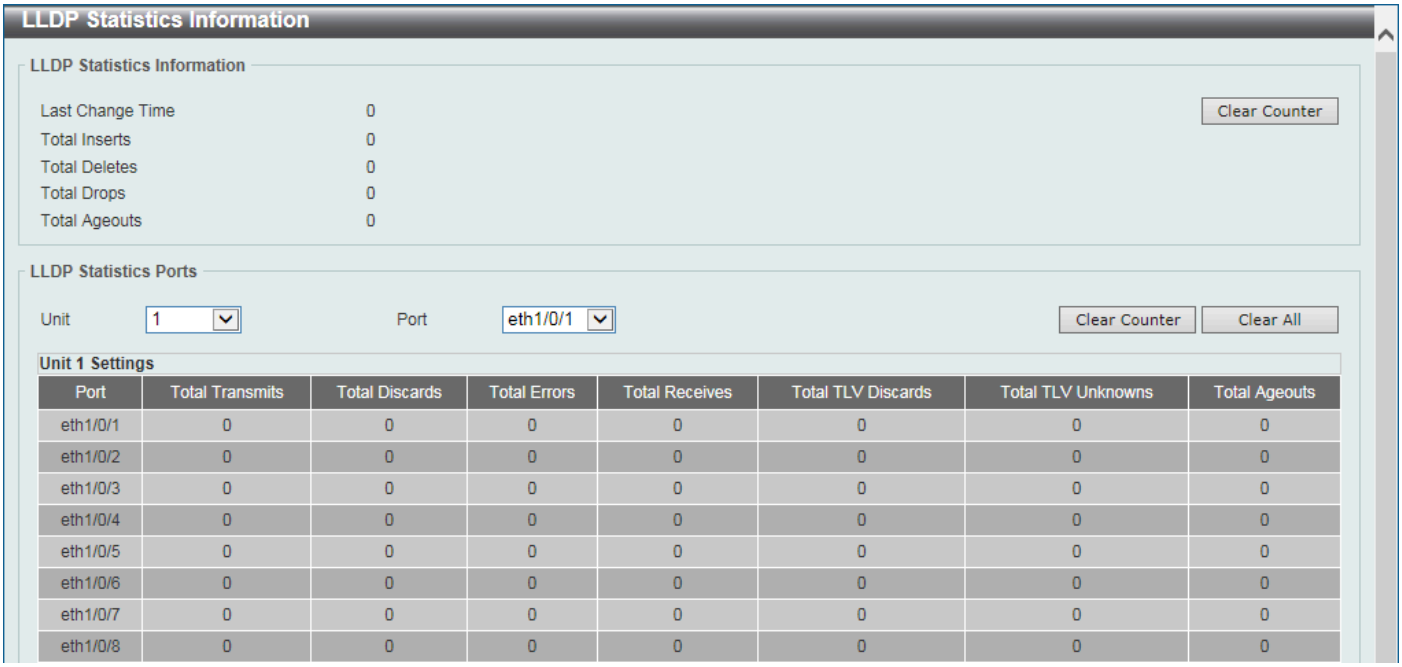


Figure 5-92 LLDP Statistics Information Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used here. This option is only available when stacking is enabled.
Port	Select the port number that will be used here.

Click the **Clear Counter** button to clear the counter information for the statistics displayed.

Click the **Clear All** button to clear all the counter information displayed.

LLDP Local Port Information

This window is used to display the information currently available for populating outbound LLDP advertisements.

To view the following window, click **L2 Features > LLDP > LLDP Local Port Information**, as shown below:

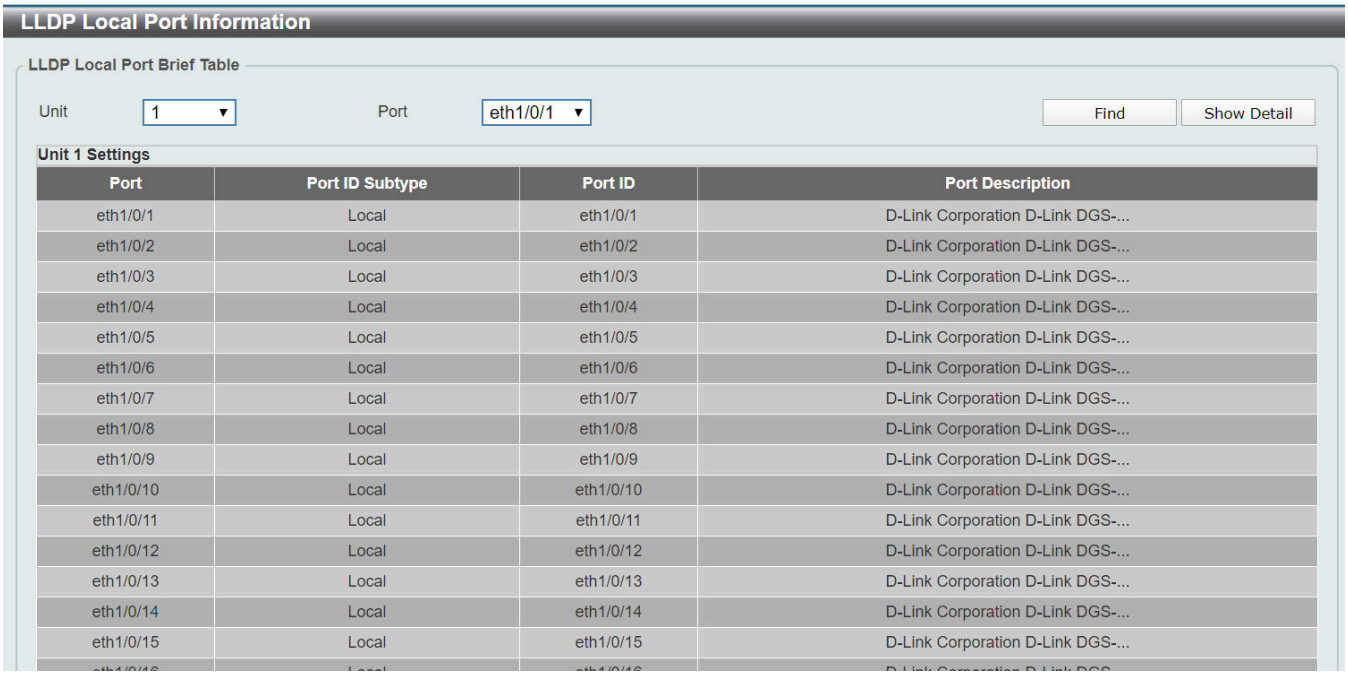


Figure 5-93 LLDP Local Port Information Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be displayed.This option is only available when stacking is enabled.
Port	Select the port number that will be displayed.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show Detail** button to view detailed information of the specific port.

After clicking the **Show Detail** button, the following window will appear.

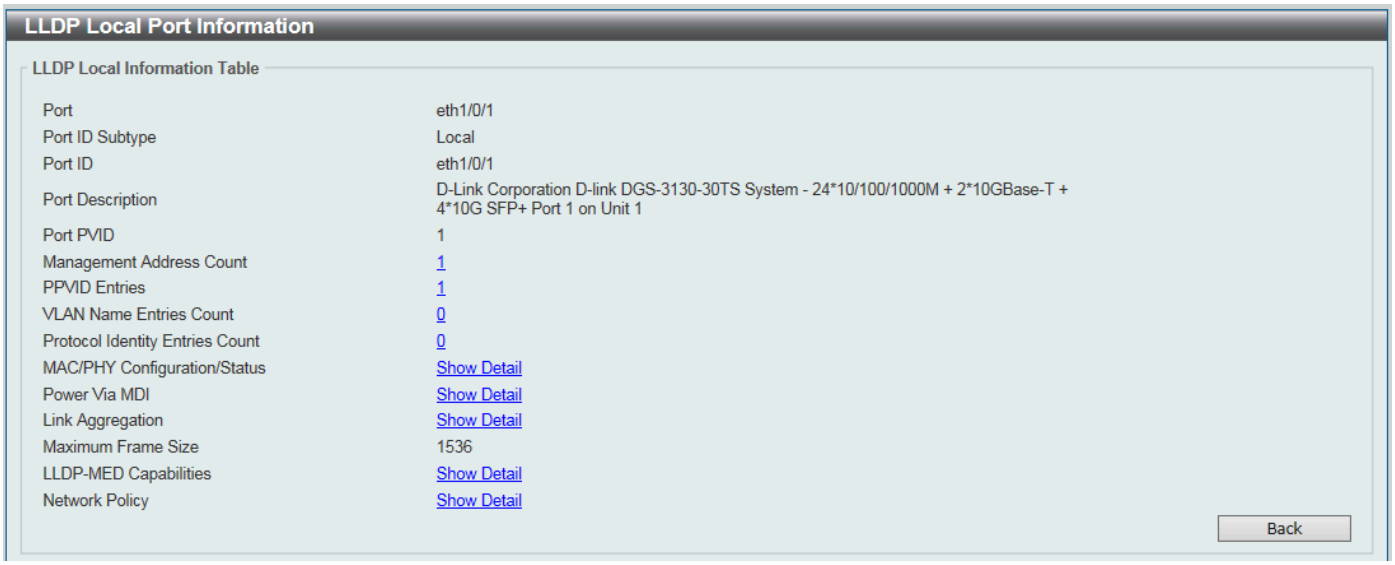


Figure 5-94 LLDP Local Port Information (Show Detail) Window

To view more details about, for example, the **MAC/PHY Configuration/Status**, click the Show Detail hyperlink.

Click the **Back** button to return to the previous window.

After clicking the Show Detail hyperlink, a new section will appear at the bottom of the window.



Figure 5-95 LLDP Local Port Information (Show Detail) Window

Click the **Back** button to return to the previous window.

LLDP Neighbor Port Information

This window is used to display the LLDP information learned from neighboring switches. The Switch receives packets from a remote station but is able to store the information locally.

To view the following window, click **L2 Features > LLDP > LLDP Neighbor Port Information**, as shown below:

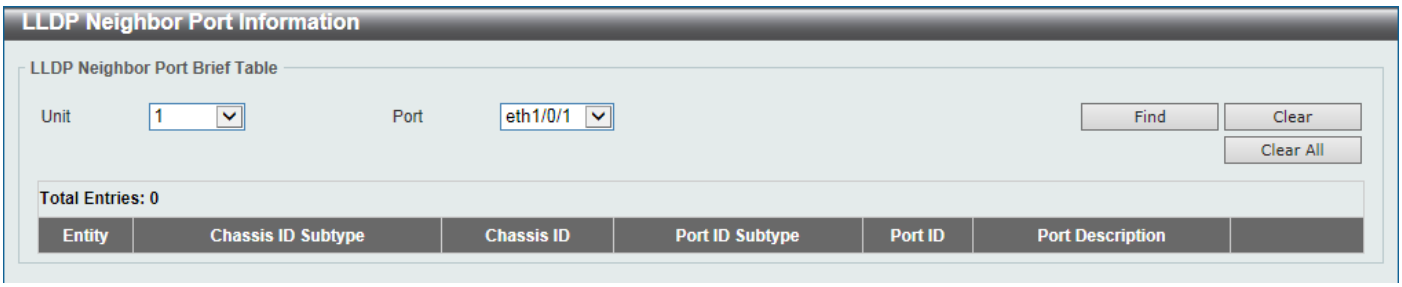


Figure 5-96 LLDP Neighbor Port Information Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be displayed.
Port	Select the port number that will be displayed.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear** button to clear the specific port information.

Click the **Clear All** button to clear all the port information displayed.

6. Layer 3 Features

ARP
Gratuitous ARP
IPv6 Neighbor
Interface
UDP Helper
IPv4 Static/Default Route
IPv4 Route Table
IPv6 Static/Default Route
IPv6 Route Table
Route Preference
ECMP Settings
RIP
RIPng
OSPF
IP Multicast Routing Protocol
IP Route Filter
Policy Route
VRRP Settings
VRRPv3 Settings

ARP

ARP Elevation

This window is used to display and configure the Address Resolution Protocol (ARP) elevation state. This is used to allow all ARP traffic to the Switch where the destination is the Switch itself. This traffic will take a higher priority than other ARP packets.

To view the following window, click **L3 Features > ARP > ARP Elevation**, as shown below:

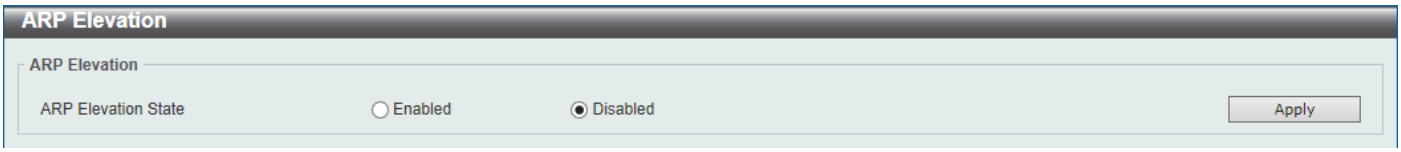


Figure 6-1 ARP Elevation Window

The fields that can be configured are described below:

Parameter	Description
ARP Elevation State	Select to enable or disable the ARP elevation feature here.

Click the **Apply** button to accept the changes made.

ARP Aging Time

This window is used to display and configure the ARP aging time settings.

To view the following window, click **L3 Features > ARP > ARP Aging Time**, as shown below:



Figure 6-2 ARP Aging Time Window

The fields that can be configured are described below:

Parameter	Description
Timeout	After click the **Edit** button, enter the ARP aging timeout value here (0~65535).

Click the **Edit** button to re-configure the specific entry.

Click the **Apply** button to accept the changes made.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Static ARP

This window is used to display and configure the static ARP settings.

To view the following window, click **L3 Features > ARP > Static ARP**, as shown below:



Figure 6-3 Static ARP Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the IP address that will be associated with the MAC address here.
Hardware Address	Enter the MAC address that will be associated with the IP address here.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Proxy ARP

This window is used to display and configure the Proxy ARP settings. The Proxy ARP feature will allow the Switch to reply to ARP requests destined for another device by faking its identity (IP and MAC Address) as the original ARP

responder. Therefore, the Switch can then route packets to the intended destination without configuring static routing or a default gateway. The host, usually a Layer 3 Switch, will respond to packets destined for another device.

To view the following window, click **L3 Features > ARP > Proxy ARP**, as shown below:

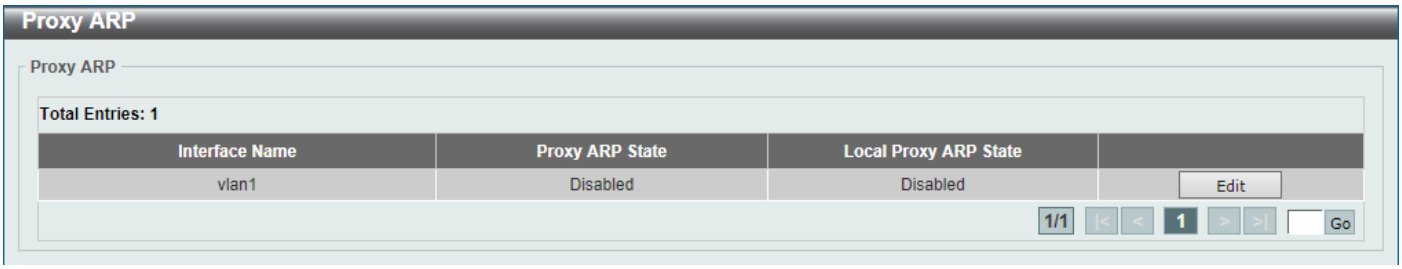


Figure 6-4 Proxy ARP Window

The fields that can be configured are described below:

Parameter	Description
Proxy ARP State	Select to enable or disable the Proxy ARP state here.
Local Proxy ARP State	Select to enable or disable the local Proxy ARP state here. This local Proxy ARP function allows the Switch to respond to the Proxy ARP, if the source IP and destination IP are in the same interface.

Click the **Edit** button to re-configure the specific entry.

Click the **Apply** button to accept the changes made.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

ARP Table

This window is used to display and configure the ARP table settings.

To view the following window, click **L3 Features > ARP > ARP Table**, as shown below:

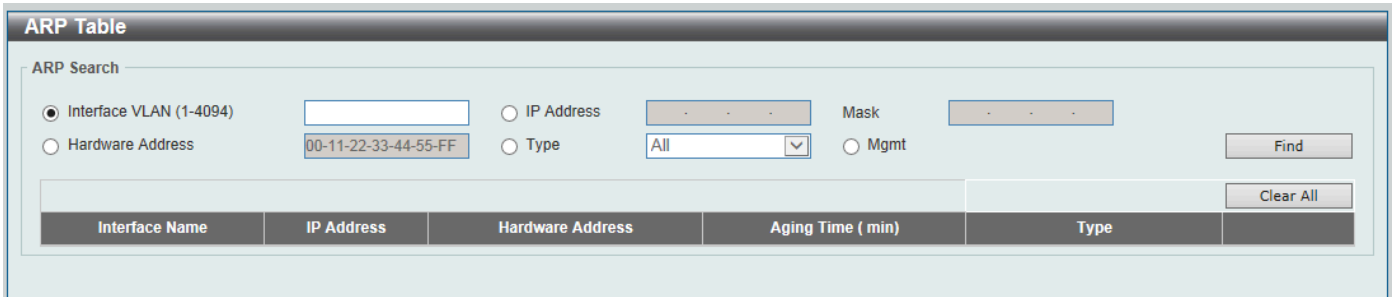


Figure 6-5 ARP Table Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the interface VLAN ID used here. This value must be between **1** and **4094**.
IP Address	Select and enter the IP address to display here.
Mask	After the **IP Address** option was selected, enter the mask address for the IP address here.
Hardware Address	Select and enter the MAC address to display here.

Parameter	Description
Type	Select the Type option here. Options to choose from are **All** and **Dynamic**.
Mgmt	Select this option to display the Management port information.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear All** button to clear all dynamic ARP cache.

Click the **Clear** button to clear the dynamic ARP cache associated with the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Gratuitous ARP

This window is used to display and configure 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.

Generally, a device uses the 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.

To view the following window, click **L3 Features > Gratuitous ARP**, as shown below:

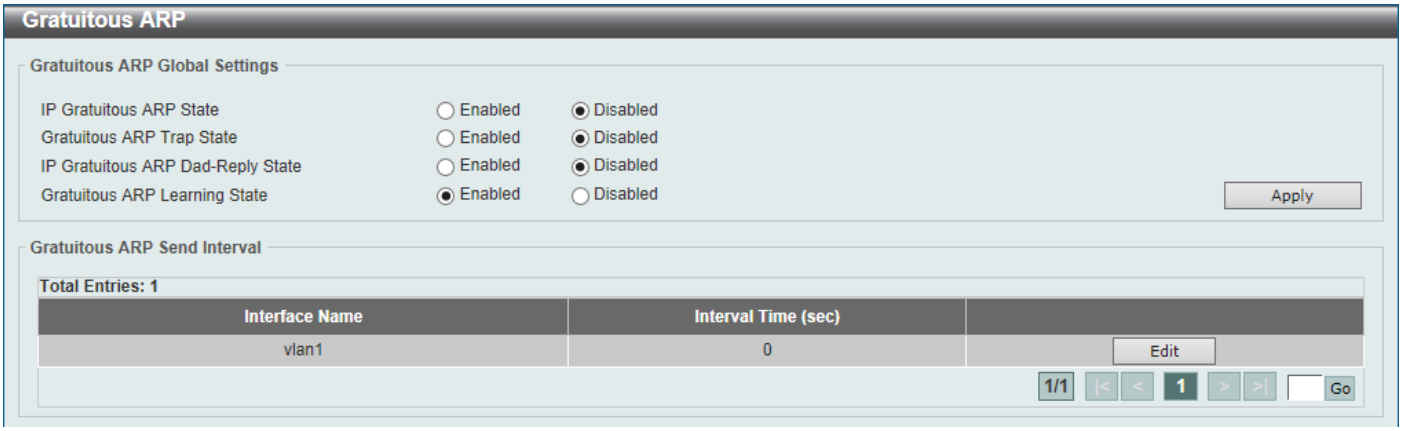


Figure 6-6 Gratuitous ARP Window

The fields that can be configured are described below:

Parameter	Description
IP Gratuitous ARP State	Select to enable or disable the learning of gratuitous ARP packets in the ARP cache table.
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 is 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.

Click the **Edit** button to re-configure the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Edit** button, the field that can be configured for **Gratuitous ARP Send Interval** is described below:

Parameter	Description
Interval Time	Enter the gratuitous ARP sending interval time, in seconds (0~3600), here.

Click the **Apply** button to accept the changes made.

IPv6 Neighbor

This window is used to display and configure the IPv6 neighbor settings.

To view the following window, click **L3 Features > IPv6 Neighbor**, as shown below:

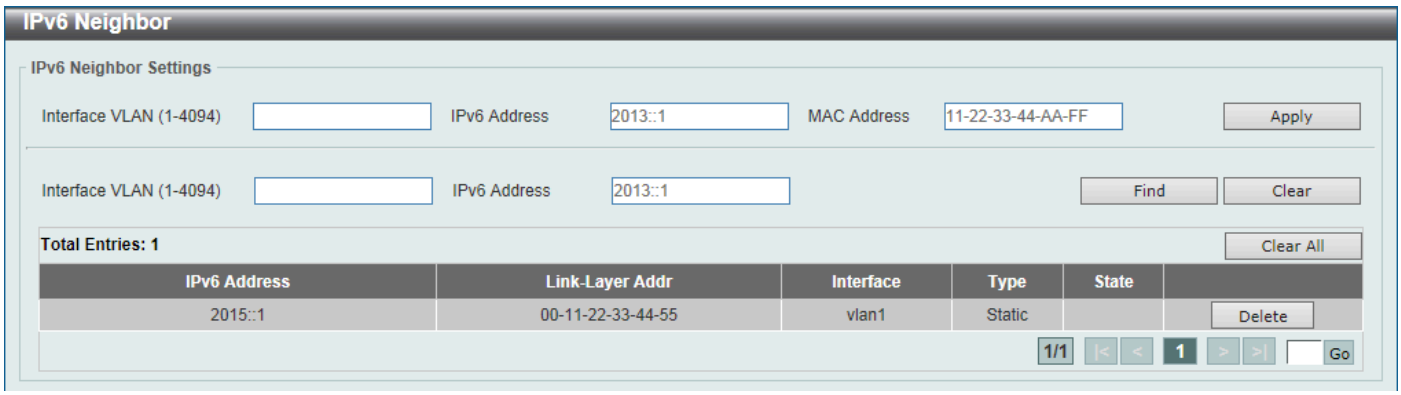


Figure 6-7 IPv6 Neighbor Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID here (1~4094).
IPv6 Address	Enter the IPv6 address.
MAC Address	Enter the MAC address.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear** button to clear all the information for the specific interface.

Click the **Clear All** button to clear all the dynamic IPv6 neighbor information in this table.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Interface

IPv4 Interface

This window is used to display and configure the IPv4 interface settings.

To view the following window, click **L3 Features > Interface > IPv4 Interface**, as shown below:

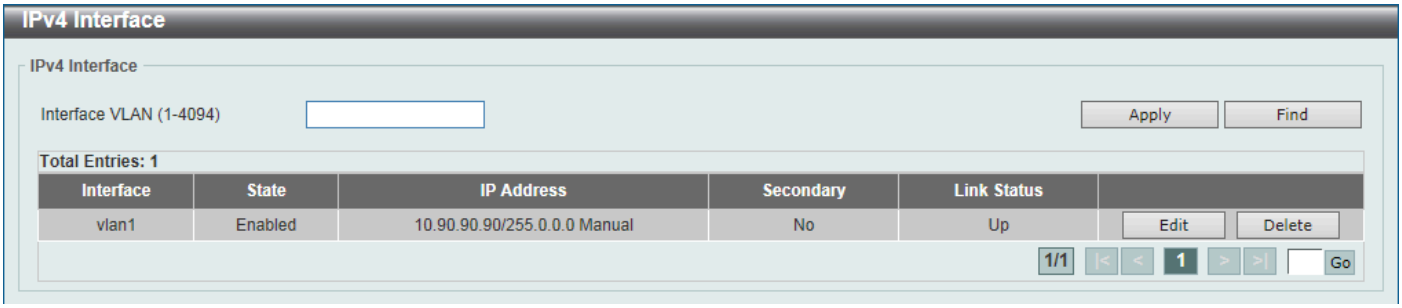


Figure 6-8 IPv4 Interface Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the interface VLAN ID here. This value must be between 1 and 4094.

The VLAN1 is the default VLAN and all switch ports belong to vlan1. It is created for management purposes.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Edit** button, the following page will be available.

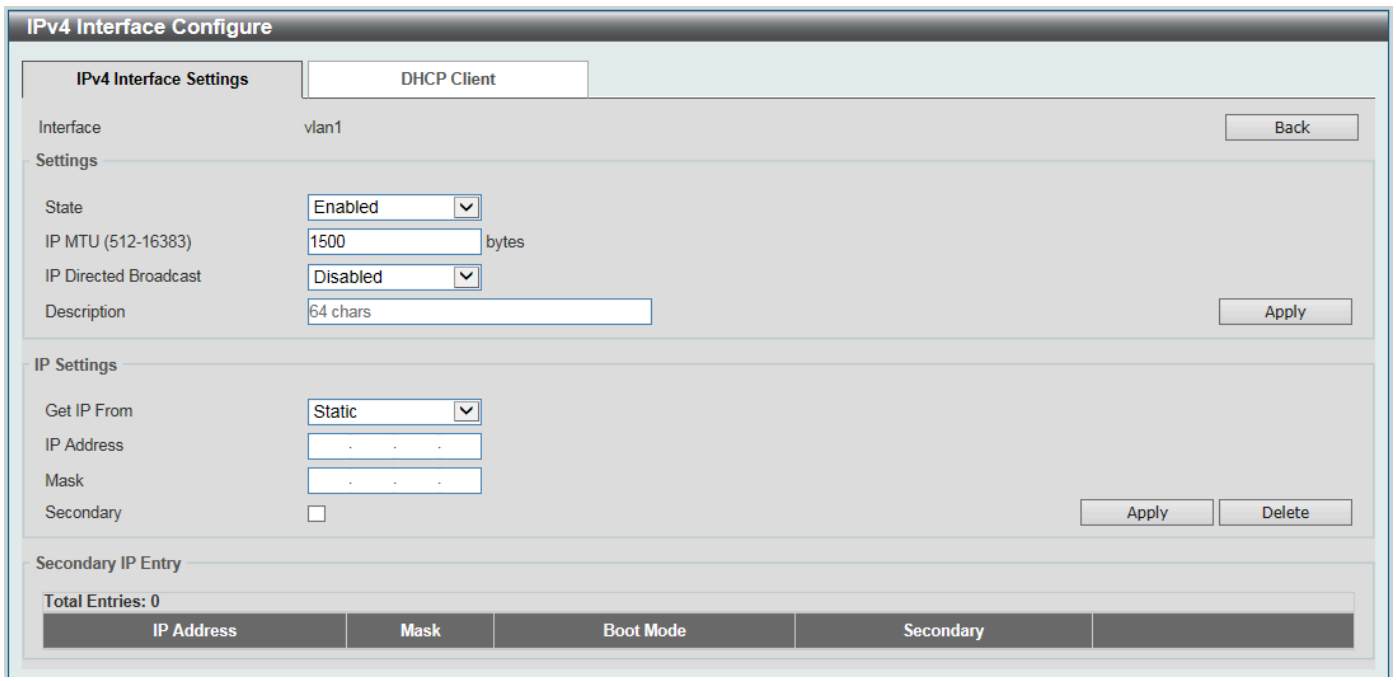


Figure 6-9 IPv4 Interface (Edit) Window

The fields that can be configured are described below:

Parameter	Description
State	Select to enable or disable the IPv4 interface global state.

Parameter	Description
IP MTU	Enter the 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.
Description	Enter the description for this entry here. This string can be up to 64 characters long.
Get IP From	Select the get IP from option here. Options to choose from are **Static** and **DHCP**. • When the **Static** option is selected, users can enter the IPv4 address of this interface manually in the fields provided. • When the **DHCP** option is selected, this interface will obtain IPv4 information automatically from the DHCP server located on the local network.
IP Address	Enter the IPv4 address for this interface here.
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 **Back** button to return to the previous window.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After selecting the **DHCP Client** tab, the following page will appear.

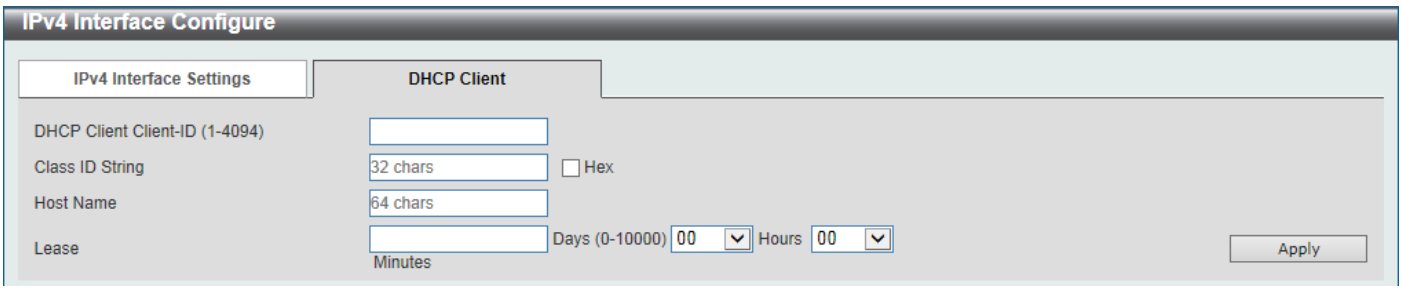


Figure 6-10 IPv4 Interface (Edit, DHCP Client) Window

The fields that can be configured are described below:

Parameter	Description
DHCP Client Client-ID	Enter the DHCP Client ID here. The range is from 1 to 4094. This parameter is used to specify the VLAN interface whose hexadecimal MAC address will be used as the client ID sent with the discover message.
Class ID String	Enter the class ID string here. This string can be up to 32 characters long. Select the **Hex** option to enter the Class ID string in the hexadecimal format. This string can be up to 64 characters long. This parameter is used to specify the vendor class identifier used as the value of Option 60 in the DHCP discover message.

Parameter	Description
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 text box the lease time, in days, can be entered. The range is from 0 to 10000 days. **Hours** and **Minutes** can also be selected optionally.

Click the **Apply** button to accept the changes made.

IPv6 Interface

This window is used to display and configure the IPv6 interface settings.

To view the following window, click **L3 Features > Interface > IPv6 Interface**, as shown below:



Figure 6-11 IPv6 Interface Window

The fields that can be configured in **IPv6 Interface** are described below:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID (1~4094) that will be associated with the IPv6 entry.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show Detail** button to view and configure more detailed settings for the IPv6 interface entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Show Detail** button, the following page will be available.

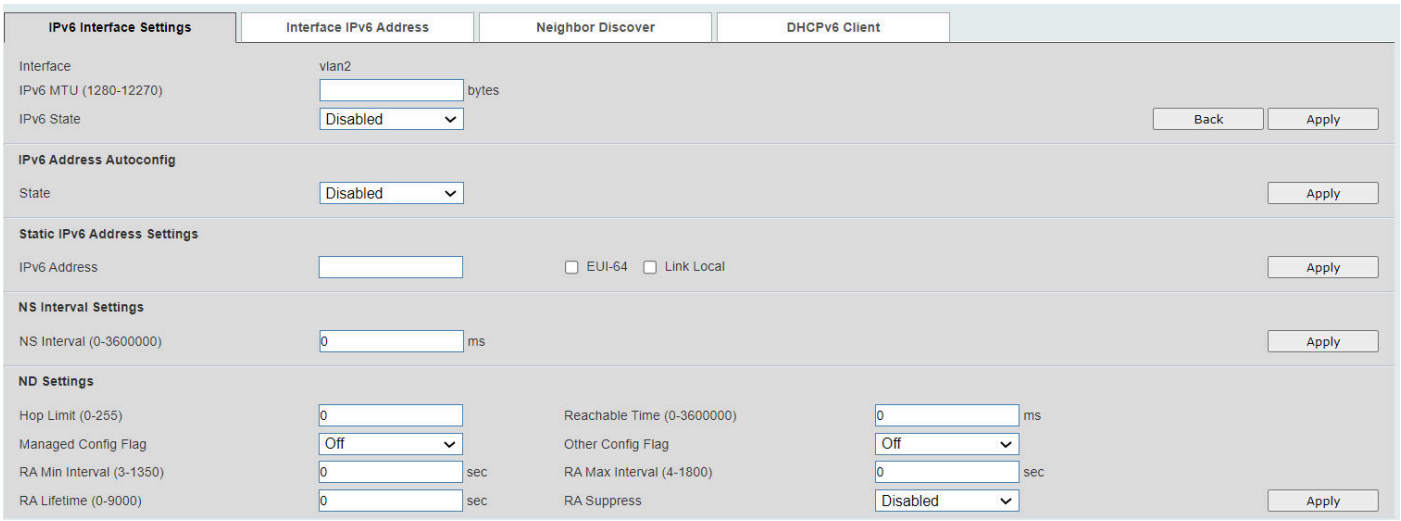


Figure 6-12 IPv6 Interface (Detail, IPv6 Interface Settings) Window

The fields that can be configured are described below:

Parameter	Description
IPv6 MTU	Enter the IPv6 MTU value here. The range is from 1280 to 12270 bytes.This parameter is used to configure the MTU to be advertised in RA messages.
IPv6 State	Select to enable or disable the IPv6 interface global state here.

Click the **Back** button to discard the changes made and return to the previous page.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **IPv6 Address Autoconfig** are described below:

Parameter	Description
State	Select to enable or disable the automatic configuration of the IPv6 address for this interface.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Static IPv6 Address Settings** are described below:

Parameter	Description
IPv6 Address	Enter the IPv6 address with prefix length (e.g. 2003:DD8:ABCD:12::1/64) for this IPv6 interface here. Select the **EUI-64** option to configure an IPv6 address on the interface using the EUI-64 interface ID. Select the **Link Local** option to configure a link-local address for the IPv6 interface.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **NS Interval Settings** are described below:

Parameter	Description
NS Interval	Enter the Neighbor Solicitation (NS) interval value here. The range is from 0 to 3600000 milliseconds, in multiples of 1000. If the specified time is 0, the router will use 1 second on the interface and advertise 0 (unspecified) in the Router Advertisement (RA) message.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **ND Settings** are described below:

Parameter	Description
Hop Limit	Enter the hop limit value here. The range is from 0 to 255. The IPv6 packet originated by the system will also use this value as the initial hop limit.
Reachable Time	Enter the Reachable Time here. The range is from 0 to 3600000 milliseconds. If the specified time is 0, the router will use 1200 seconds on the interface and advertise 1200 (unspecified) in the RA message. The Reachable Time is used by the IPv6 node in determining the reachability of the neighbor nodes.
Managed Config Flag	Turn the Managed Config Flag option **On** or **Off** here. When the neighbor host receives the RA which has flag turned on, the host should use a stateful configuration protocol to obtain IPv6 addresses.
Other Config Flag	Turn the Other Config Flag option **On** or **Off** here. By setting the other configuration flag on, the router instructs the connected hosts to use a stateful configuration protocol to obtain auto-configuration information other than the IPv6 address.
RA Min Interval	Enter the minimum RA interval time value here. The range is from 3 to 1350 seconds. This value must be smaller than 0.75 times the maximum value.
RA Max Interval	Enter the maximum RA interval time value here. The range is from 4 to 1800 seconds.
RA Lifetime	Enter the RA lifetime value here. The range is from 0 to 9000 seconds. The lifetime value in RA instructs the received host the lifetime value for taking the router as the default router.
RA Suppress	Select to enable or disable the RA suppress feature here.

Click the **Apply** button to accept the changes made.

After selecting the **Interface IPv6 Address** tab option, at the top of the page, the following page will be available.

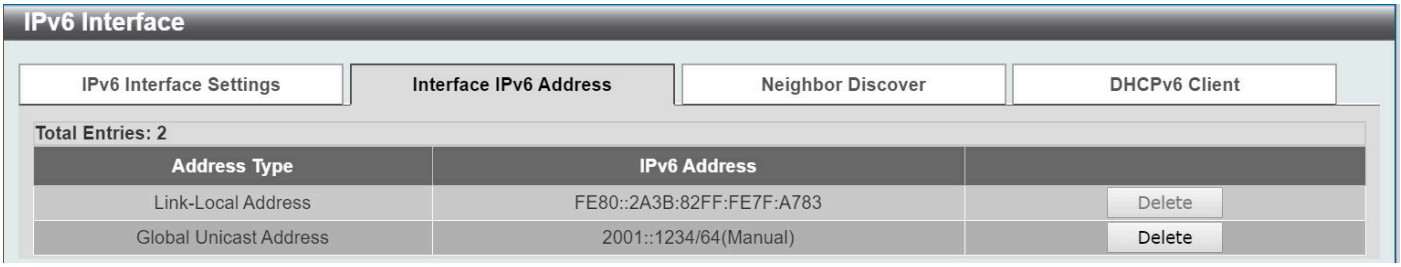


Figure 6-13 IPv6 Interface (Detail, Interface IPv6 Address) Window

Click the **Delete** button to delete the specified entry.

After selecting the **Neighbor Discover** tab option, at the top of the page, the following page will be available.

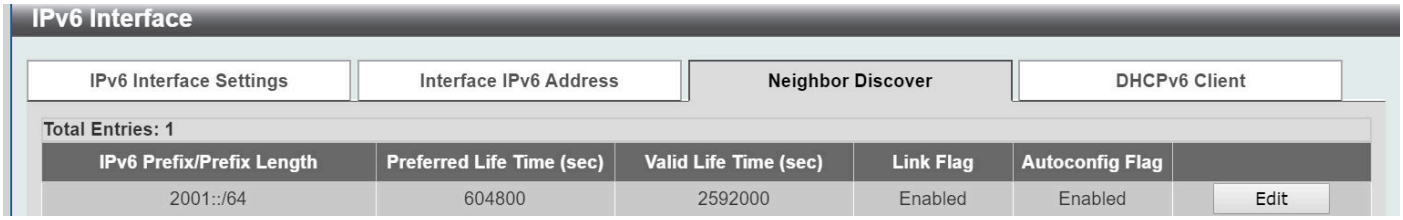


Figure 6-14 IPv6 Interface (Detail, Neighbor Discover) Window

After selecting the **DHCPv6 Client** tab option, at the top of the page, the following page will be available.

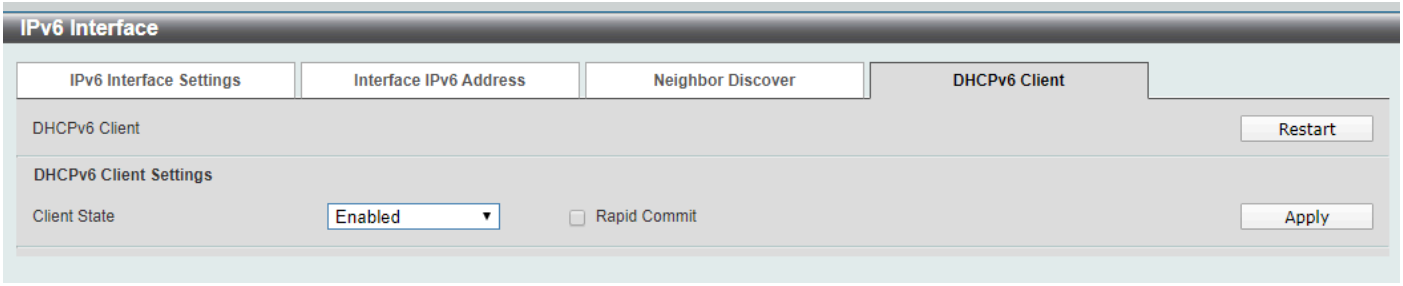


Figure 6-15 IPv6 Interface (Detail, DHCPv6 Client) Window

Click the **Restart** button to restart the DHCPv6 client service.

The fields that can be configured for **DHCPv6 Client Settings** are described below:

Parameter	Description
Client State	Select to enable or disable the DHCPv6 client service here. Select the **Rapid Commit** option to proceed with two-message exchange for address delegation. The rapid-commit option will be included in the Solicit message to request a two-message handshake.

Click the **Apply** button to accept the changes made.

Loopback Interface

This window is used to display and configure the loopback interface settings. A loopback interface is a software only interface which always stays in the up status.

To view the following window, click **L3 Features > Interface > Loopback Interface**, as shown below:

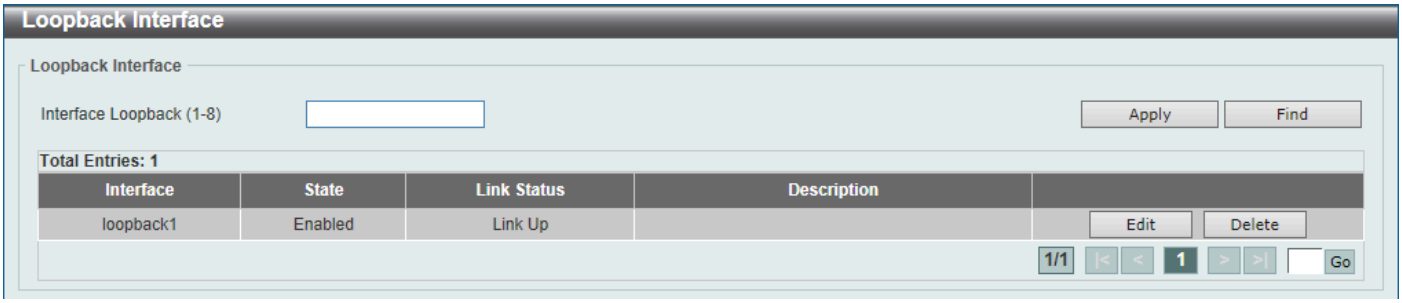


Figure 6-16 Loopback Interface Window

The fields that can be configured are described below:

Parameter	Description
Interface Loopback	Enter the loopback interface ID here. The range is from 1 to 8.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Edit** button to modify 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.

After clicking the **Edit** button, the following page will appear.

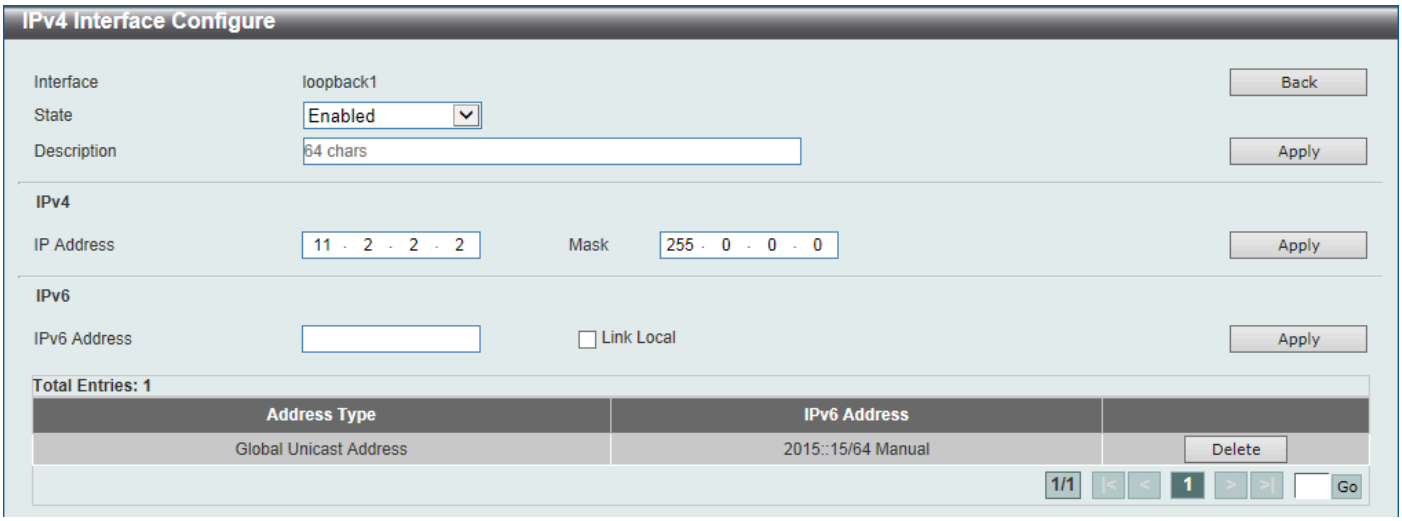


Figure 6-17 Loopback Interface (Edit) Window

The fields that can be configured are described below:

Parameter	Description
State	Select to enable or disable the loopback interface here.
Description	Enter the description for the loopback interface here. This string can be up to 64 characters long.
IP Address	Enter the IPv4 address associated with this loopback interface here.
Mask	Enter the IPv4 subnet mask associated with this loopback interface here.
IPv6 Address	Enter the IPv6 address associated with this loopback interface here.
Link Local	Select this option to specify that the IPv6 address entered is a link-local IPv6 address.

Click the **Back** button to return to the previous window.

Click the **Apply** button to accept the changes made.

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.

Null Interface

This window is used to display and configure the Null interface settings. The null0 interface is a virtual interface and it is used to drop unwanted packets or prevent routing loops.

To view the following window, click **L3 Features > Interface > Null Interface**, as shown below:

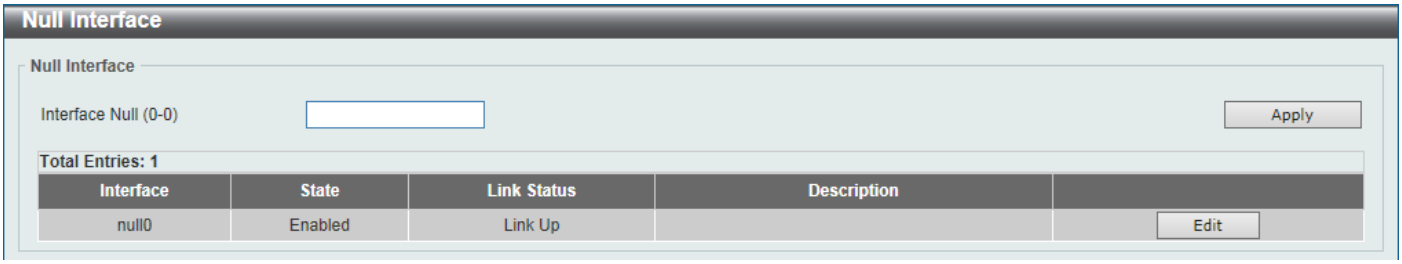


Figure 6-18 Null Interface Window

The fields that can be configured are described below:

Parameter	Description
Interface Null	Enter the Null interface ID here. This value can only be 0.
Description	After clicking the **Edit** button, enter the description for the Null interface here. This string can be up to 64 characters long.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to modify the description for the Null interface.

UDP Helper

IP Forward Protocol

This window is used to display and configure the IP forward protocol settings. This feature is used to enable the forwarding of a specific UDP service type of packets.

To view the following window, click **L3 Features > UDP Helper > IP Forward Protocol**, as shown below:

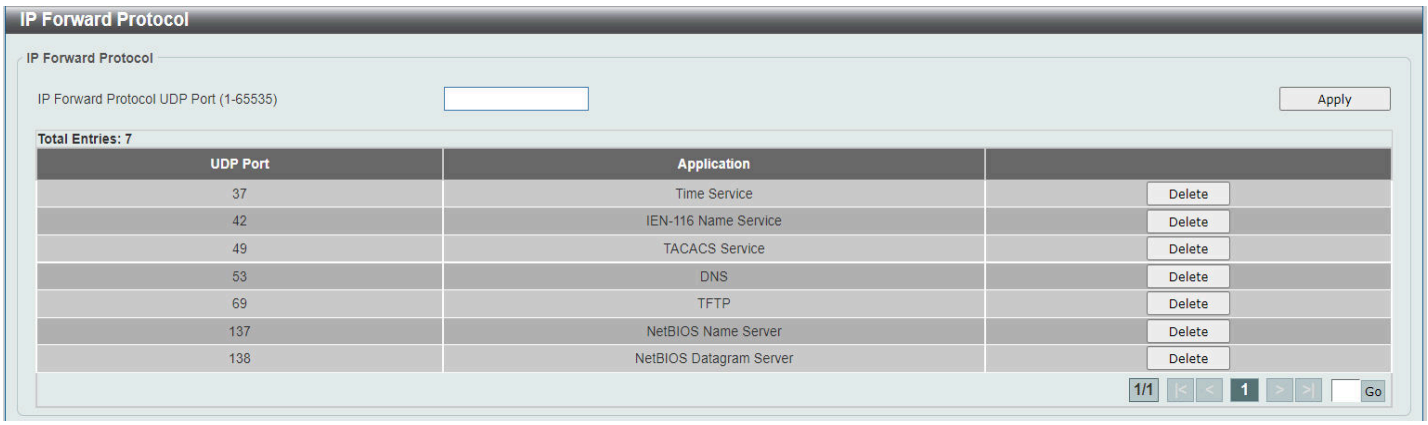


Figure 6-19 IP Forward Protocol Window

The fields that can be configured are described below:

Parameter	Description
IP Forward Protocol UDP Port	Enter the destination port of the UDP service to be forwarded here. The range is from 1 to 65535.

Click the **Apply** button to accept the changes made.

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.

IP Helper Address

This window is used to add or remove a target address for the forwarding of UDP broadcast packets. This feature takes effect only when the received interface has an IP address assigned.

The system only forwards packets that satisfy the following restrictions:

- The destination MAC address must be a broadcast address.
- The destination IP address must be an all-one broadcast.
- The packets are IPv4 UDP packets.
- The IP TTL value must be greater than or equal to 2.

To view the following window, click **L3 Features > UDP Helper > IP Helper Address**, as shown below:



Figure 6-20 IP Helper Address Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID used here. The range is from 1 to 4094.
Helper Address	Enter the target IPv4 address for the forwarding of the UDP broadcast packet here.

Click the **Apply** button to accept the changes made.

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.

IPv4 Static/Default Route

This window is used to display and configure the IPv4 static and default route settings. The Switch supports static routing for IPv4 and IPv6 formatted addressing. Users can create up to a total of 1024 static route entries for IPv4 and IPv6. For IPv4 static routes, once a static route has been set, the Switch will send an ARP request packet to the next

hop router that has been set by the user. Once an ARP response has been retrieved by the Switch from that next hop, the route becomes enabled. However, if the ARP entry already exists, an ARP request will not be sent.

The Switch also supports a floating static route, which means that the user may create an alternative static route with a different next hop. This secondary next hop device route is considered as a backup static route when the primary static route is down. If the primary route is lost, the backup route will become active and begin forwarding traffic.

Entries into the Switch's forwarding table can be made using an IP address, subnet mask and gateway.

To view the following window, click **L3 Features > IPv4 Static/Default Route**, as shown below:

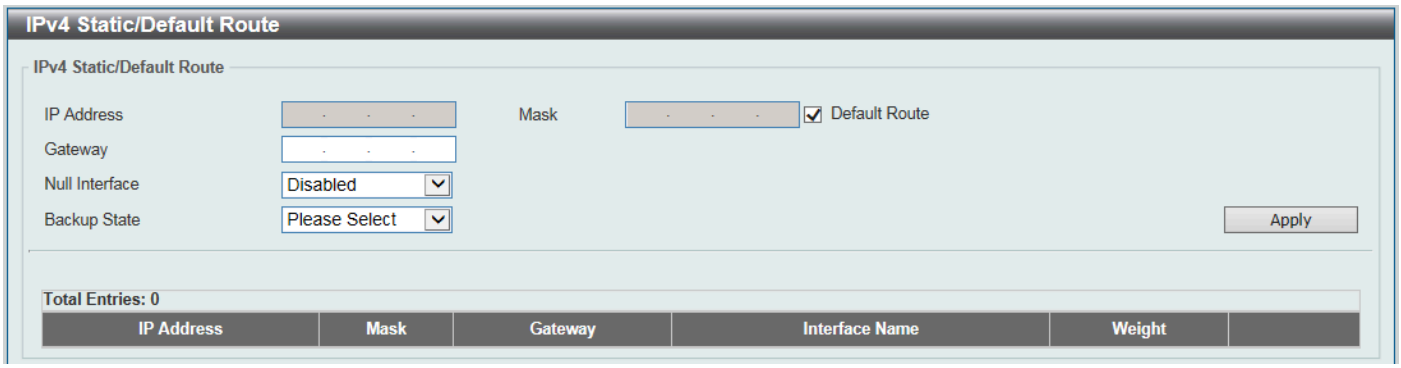


Figure 6-21 IPv4 Static/Default Route Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the IPv4 address for this route here. Tick the **Default Route** option to use the default route as the IPv4 address.
Mask	Enter the IPv4 network mask for this route here.
Gateway	Enter the gateway address for this route here.
Null Interface	Select to enable or disable the NULL interface here.
Backup State	Select the backup state option here. • **Weight** - Specifies a weight number greater than zero, but less than the maximum paths number. This number is used to replicate identical route paths (multiple copies) in the routing table, so the paths get more chance of being hit for traffic routing. If the weight number is not specified for the static route, the default for the path exists in the hashing table. Enter the weight value in the space provided. The range is from 1 to 15.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IPv4 Route Table

This window is used to display and configure the IPv4 route table settings.

To view the following window, click **L3 Features > IPv4 Route Table**, as shown below:

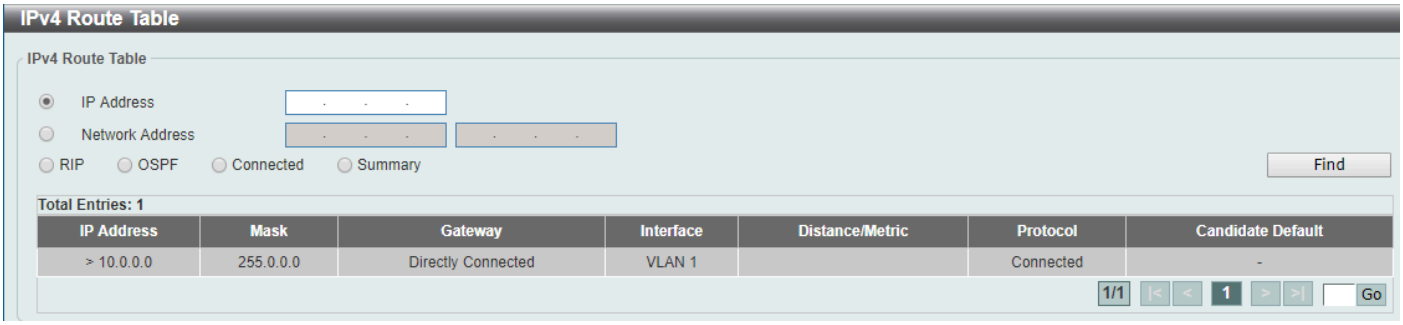


Figure 6-22 IPv4 Route Table Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Select and enter the single IPv4 address here.
Network Address	Select and enter the IPv4 network address here. In the first space enter the subnet address and in the second space enter the network mask.
RIP	Select this option to display only RIP routes.
OSPF	Select this option to display only OSPF routes.
Connected	Select this option to display only connected routes.
Summary	Select this option to display a summary and count of the route sources configured on this Switch.

Click the **Find** button to locate a specific entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IPv6 Static/Default Route

This window is used to display and configure the IPv6 static or default routes.

To view the following window, click **L3 Features > IPv6 Static/Default Route**, as shown below:

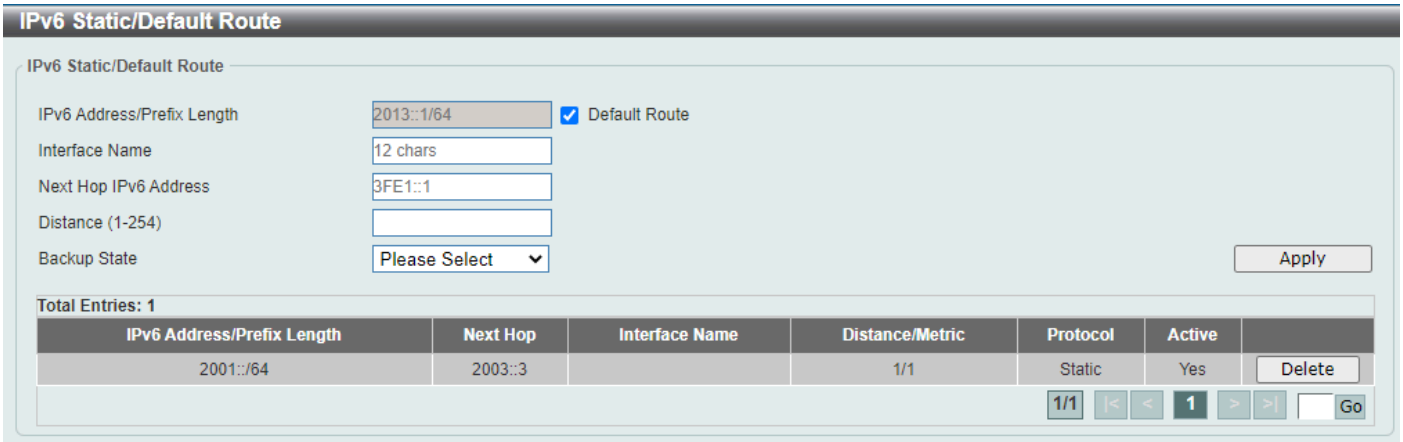


Figure 6-23 IPv6 Static/Default Route Window

The fields that can be configured are described below:

Parameter	Description
IPv6 Address/Prefix Length	Enter the IPv6 address and prefix length for this route here. Tick the **Default Route** option to use this route as the default route.
Interface Name	Enter the name of the interface that will be associated with this route here.
Next Hop IPv6 Address	Enter the next hop IPv6 address here.
Distance	Enter the administrative distance of the static route here. This value must be between **1** and **254**. A lower value represents a better route. If not specified, the default administrative distance for a static route is **1**.
Backup State	Select the backup state option here. Options to choose from are: • **Primary** - Specifies the route as the primary route to the destination. • **Backup** - Specifies the route as the backup route to the destination. • **Weight** - Specifies the route as the ECMP route. The weight number is always 1.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IPv6 Route Table

This window is used to display and configure the IPv6 route table.

To view the following window, click **L3 Features > IPv6 Route Table**, as shown below:

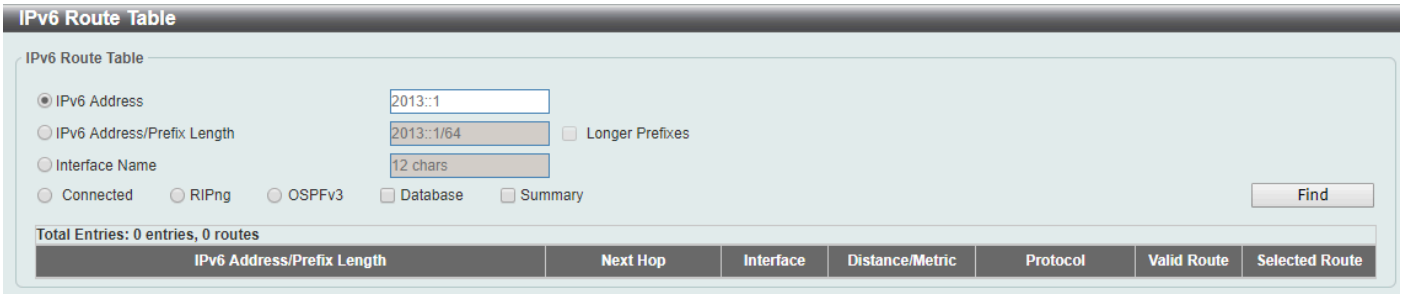


Figure 6-24 IPv6 Route Table Window

The fields that can be configured are described below:

Parameter	Description
IPv6 Address	Select and enter the IPv6 address to display here.
IPv6 Address/Prefix Length	Select and enter the IPv6 address and prefix length to display here. Select the **Longer Prefixes** option to display IPv6 routes with prefixes greater than and equal to the prefix length.
Interface Name	Select and enter the name of the interface to display here.
Connected	Select this option to display only connected routes.
RIPng	Select this option to display only RIPng routes.
OSPFv3	Select this option to display only OSPFv3 routes.
Database	Select this option to display all the related entries in the routing database instead of just the best route.

Parameter	Description
Summary	Select this option to display a summary and count of the route sources configured on this Switch.

Click the **Find** button to locate a specific entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Route Preference

This window is used to display and configure the route preference settings. Use this window to configure the distance, which represents the route's trust rating. The route with a lower distance value is preferred over the route with a higher distance value. A route with the distance 255 will not be installed for routing of packets since it indicates that the route is not trusted.

To view the following window, click **L3 Features > Route Preference**, as shown below:

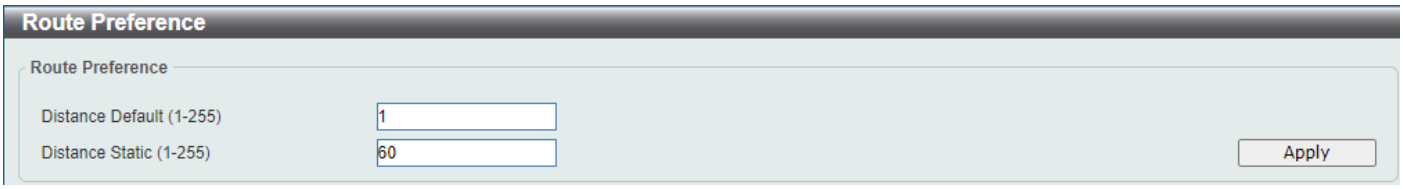


Figure 6-25 Route Preference Window

The fields that can be configured are described below:

Parameter	Description
Distance Default	Enter the administrative distance of default routes here. The range is from 1 to 255. By default, this value is 1.
Distance Static	Enter the administrative distance of static default routes here. The range is from 1 to 255. By default, this value is 60.

Click the **Apply** button to accept the changes made.

ECMP Settings

This window is used to display and configure the Equal-Cost Multi-Path (ECMP) routing settings. This is used to configure the load balancing hash algorithm and used to determine the next hop entry for multiple paths destined for the same destination.

To view the following window, click **L3 Features > ECMP Settings**, as shown below:

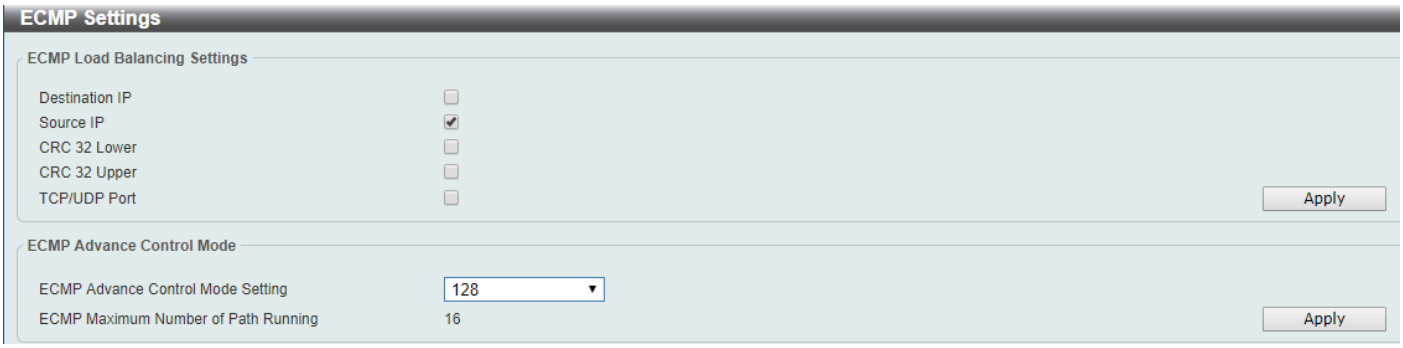


Figure 6-26 ECMP Settings Window

The fields that can be configured in **ECMP Load Balancing Settings** are described below:

Parameter	Description
Destination IP	Select this option to use the destination IP address as the ECMP hash key.
Source IP	Select this option to use the least significant bits of the source IP address as the ECMP hashing algorithm.
CRC 32 Lower	Select this option to use the lower bits of CRC-32 as the ECMP hashing algorithm.
CRC 32 Upper	Select this option to use the upper bits of CRC-32 as the ECMP hashing algorithm.
TCP/UDP Port	Select this option to use TCP/UDP port number as ECMP hash key.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **ECMP Advance Control Mode** are described below:

Parameter	Description
ECMP Advance Control Mode Setting	Select the ECMP advance control mode settings here. This specifies the number of ECMP or multipath routes and the number of next-hops of each ECMP or multipath route that will be changed according to the specified value. Options to choose from are **64**, **128**, **256**, and **512**.

Click the **Apply** button to accept the changes made.

RIP

RIP Settings

This window is used to display and configure Routing Information Protocol (RIP) settings.

To view the following window, click **L3 Features > RIP > RIP Settings**, as shown below:

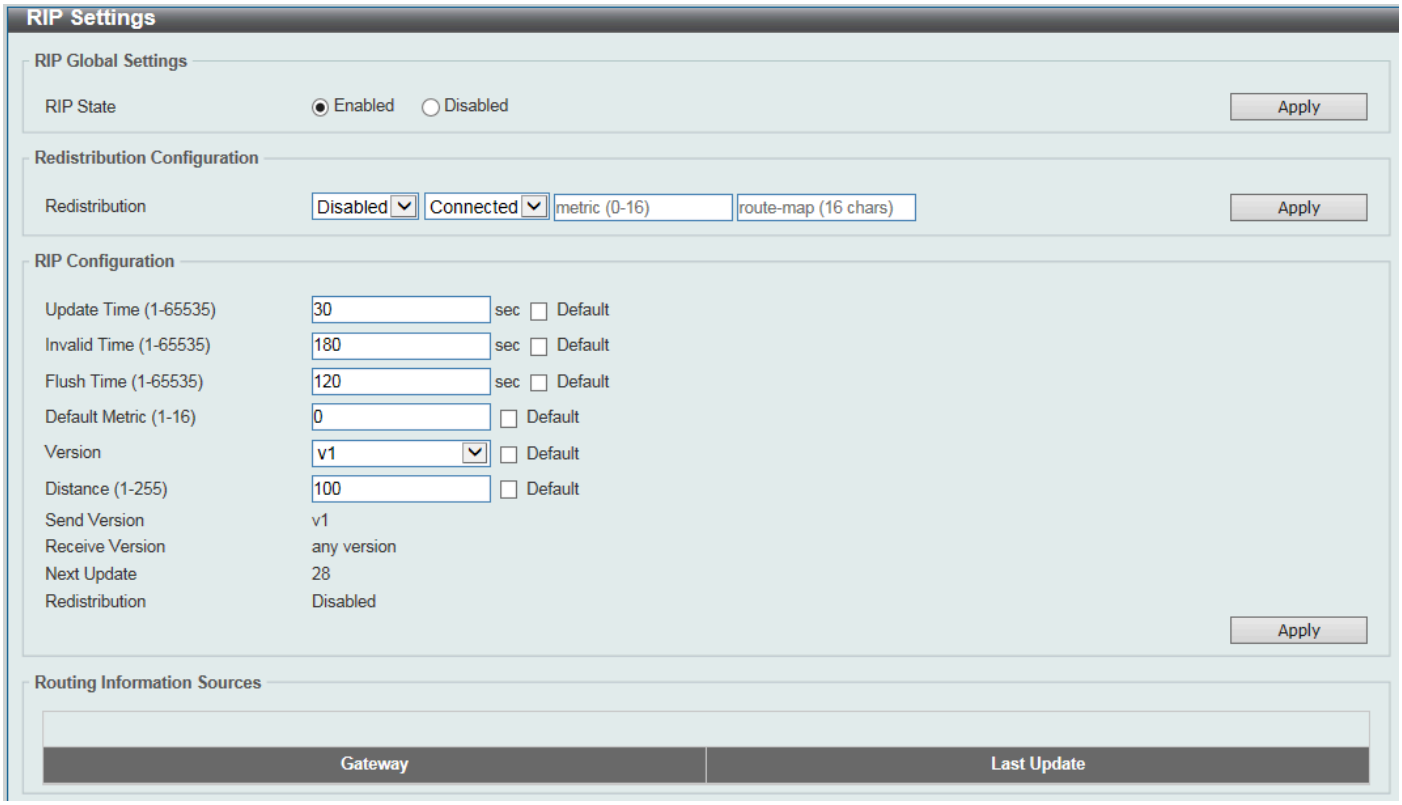


Figure 6-27 RIP Settings Window

The fields that can be configured in **RIP Global Settings** are described below:

Parameter	Description
RIP State	Select to globally enable or disable the Routing Information Protocol (RIP) feature here.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Redistribution Configuration** are described below:

Parameter	Description
Redistribution	• First, select to enable or disable the RIP redistribution feature here. • Second, select the routing protocol (domain) that will be redistributed into RIP. Options to choose from are **Connected**, **OSPF** and **Static**. The **Static** option means redistribute IP static routes. The **Connected** option refers to routes that are established automatically through configuring an IP address on an interface. • Third, enter the value to be used as the metric for the redistributed route here. The range is from 0 to 16. • Fourth, enter the Route Map name that is used in the filtering of the routes to be redistributed to the current routing protocol. If not specified, all routes are redistributed.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **RIP Configuration** are described below:

Parameter	Description
Update Time	Enter the update interval in seconds at which the update message is sent. The range is from 1 to 65535 seconds. Select the **Default** option to use the default value here which is 30 seconds.
Invalid Time	Enter the invalid time value in seconds here. The range is from 1 to 65535 seconds. Select the **Default** option to use the default value here which is 180 seconds.
Flush Time	Enter the flush time value in seconds here. The range is from 1 to 65535 seconds. Select the **Default** option to use the default value here which is 120 seconds.
Default Metric	Enter the default metric value here. The range is from 0 to 16. The default metric is used in redistributing routes from other routing protocols. The routes being redistributed are learned by other protocols and may have an incompatible metric to RIP. The specifying of the metric allows the metric to be synced. Select the **Default** option to use the default metric value, which is 0.
Version	Select the global RIP version that will be used as the default version for all interfaces here. Options to choose from are v1 (RIPv1) and v2 (RIPv2). Select the **Default** option to specify that this feature should use the default configuration. By default, RIPv1 and RIPv2 packets are received, but only RIPv1 packets are sent.
Distance	Enter the Administrative Distance for RIP here. The range is from 1 to 255. A lower value represents a better route. Select the **Default** option to use the default Administrative Distance for RIP, which is 100.

Click the **Apply** button to accept the changes made.

RIP Distribute List

This window is used to display and configure the RIP distribution list settings.

To view the following window, click **L3 Features > RIP > RIP Distribute List**, as shown below:

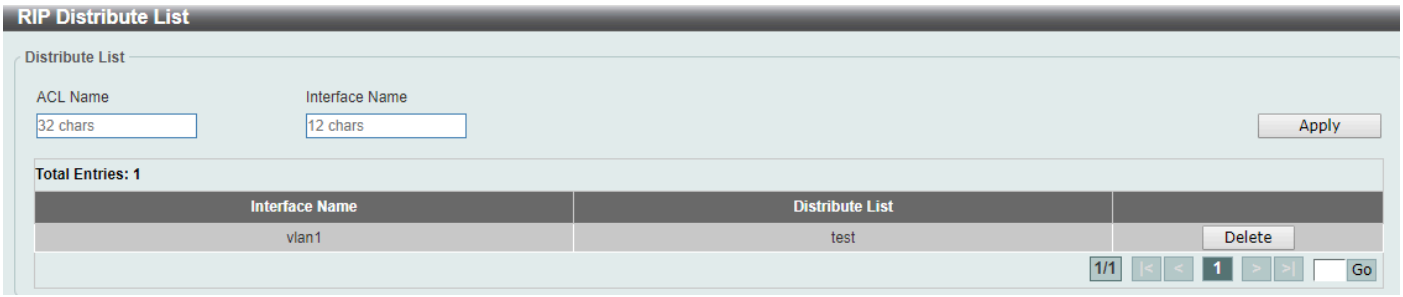


Figure 6-28 RIP Distribute List Window

The fields that can be configured are described below:

Parameter	Description
ACL Name	Enter the access list name that will be used here. This name can be up to 32 characters long. Note that RIP needs to be enabled to enter an ACL name here. Refer to **RIP > RIP Settings**.

Parameter	Description
Interface Name	Enter the interface name that will be used here. This name can be up to 12 characters long. Note that RIP needs to be enabled to enter an ACL name here. Refer to **RIP > RIP Settings** and **L3 Features > Interface**.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

RIP Interface Settings

This window is used to display and configure the RIP interface settings.

To view the following window, click **L3 Features > RIP > RIP Interface Settings**, as shown below:

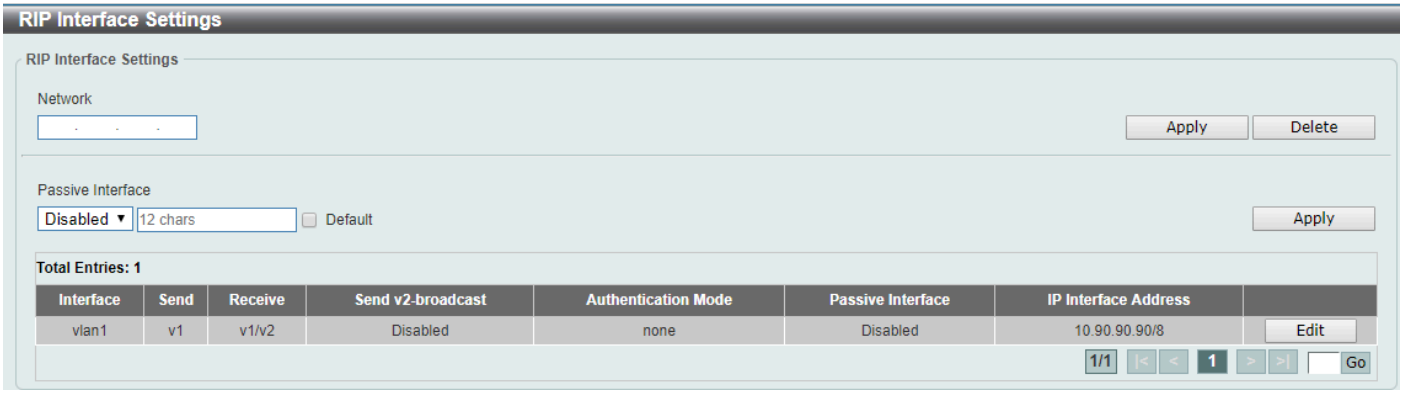


Figure 6-29 RIP Interface Settings Window

The fields that can be configured are described below:

Parameter	Description
Network	Enter the IPv4 network address used by RIP here. Interfaces that have a subnet belonging to the network specified here will be activated for RIP.
Passive Interface	Select to enable or disable the passive interface feature here. This feature is used to disable the sending and receiving of routing updates on an interface. However, RIP packets from other routers received on this interface will continue to be processed. Enter the name of the passive interface in the space provided. This name can be up to 12 characters long. Select the **Default** option to use this as the default for all interfaces.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete an entry based on the information entered.

Click the **Edit** button to configure the specific entry.

After clicking the **Edit** button, the following page will appear.



Figure 6-30 RIP interface (Edit) Window

The **fields** that can be configured in **Configure RIP interface** are described below:

Parameter	Description
Send Version	Select a RIP version to send on the interface. Options to choose from are v1(RIPv1) and v2(RIPv2).
Receive Version	Select a RIP version or both to receive on the interface. Options to choose from are v1(RIPv1), v2(RIPv2) and v1/v2(Both).
Send v2-broadcast	Select to enable or disable the sending of version 2 RIP update packets as broadcast packets instead of multicast packets.
Authentication Mode	Select to disable or enable text authentication mode.
Authentication Text Password	Enter the authentication text password. It will be used if authentication mode is enabled. The password can be up to 16 characters long.

Click the **Apply** button to accept the changes made.

Click the **Back** button to return to the previous window.

RIP Database

This window is used to display the Routing Information Protocol (RIP) routing database. Summary address entries will appear in the database only if relevant child routes exist and are being summarized. When the last child route for a summary address becomes invalid, the summary address is also removed from the routing table.

To view the following window, click **L3 Features > RIP > RIP Database**, as shown below:

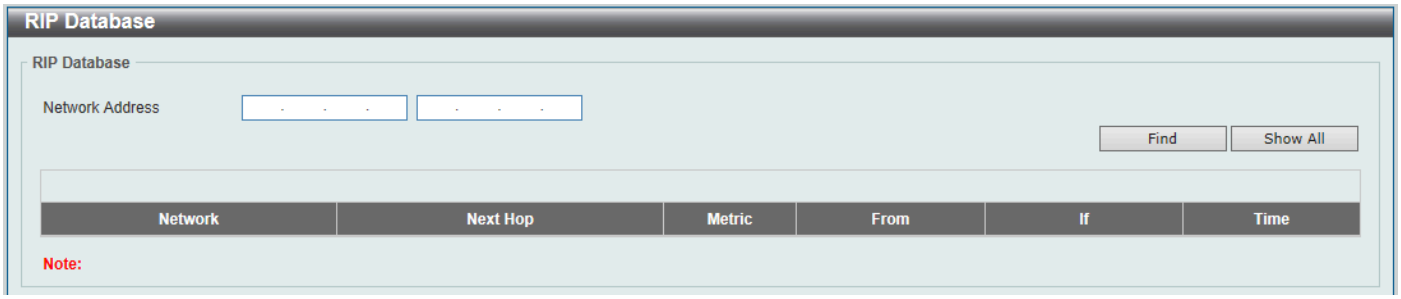


Figure 6-31 RIP Database Window

The fields that can be configured are described below:

Parameter	Description
Network Address	Enter the network and the network mask of the network(s) to be displayed here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to display all the entries.

RIPng

RIPng Settings

This window is used to display and configure the Routing Information Protocol Next Generation (RIPng) settings, also known as IPv6 RIP.

To view the following window, click **L3 Features > RIPng > RIPng Settings**, as shown below:

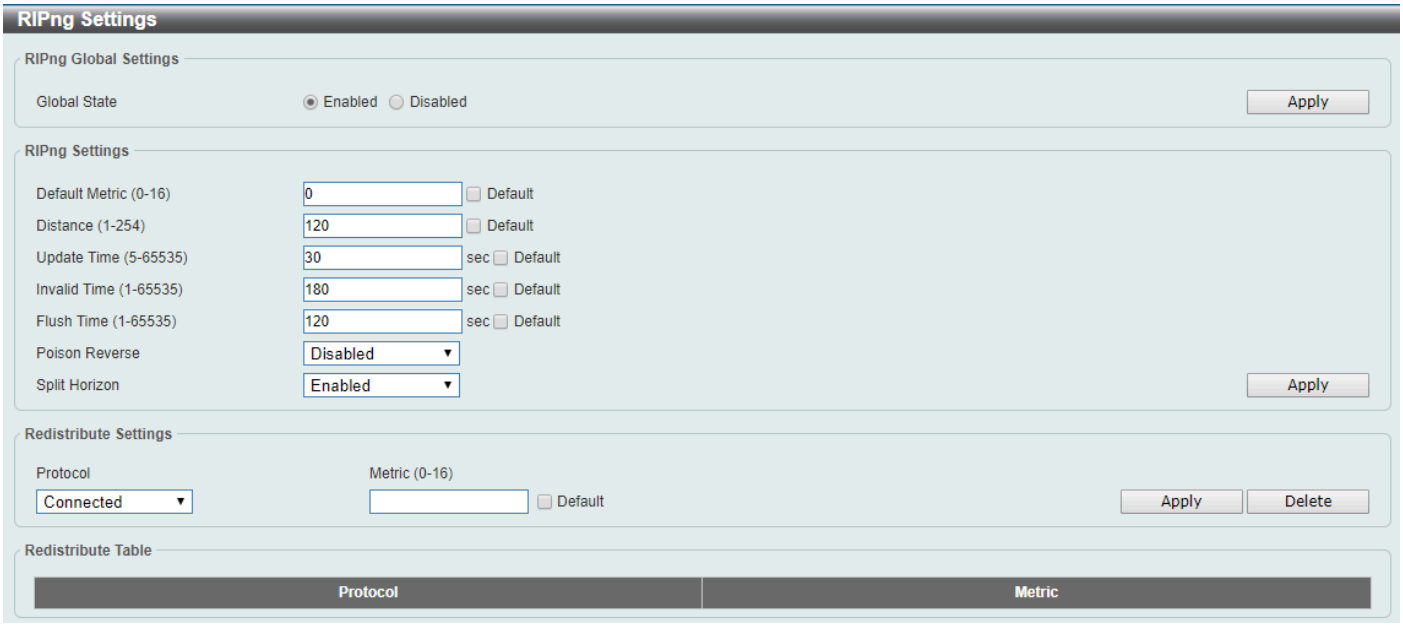


Figure 6-32 RIPng Settings Window

The fields that can be configured in **RIPng Global Settings** are described below:

Parameter	Description
Global State	Select to globally enable or disable the RIPng feature here.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **RIPng Settings** are described below:

Parameter	Description
Default Metric	Enter the default metric value here. The range is from 0 to 16. This value is used to specify the default metric for routes redistributed from other routing protocols. If the routes being redistributed are learned from other protocols, then they have an incompatible metric with IPv6 RIP. Re-specifying of metric allows the metric to be synced. Select the **Default** option to use the default metric value, which is 0.
Distance	Enter the administrative distance for RIPng here. The range is from 1 to 254. The distance value represents the trust rating of the route. The route with a lower distance value is preferred over the route with the higher distance value.

Parameter	Description
	Select the **Default** option to use the default administrative distance for RIPng, which is 120.
Update Time	Enter the update interval value at which the update message is sent here. The range is from 5 to 65535 seconds. Select the **Default** option to use the default value here which is 30 seconds.
Invalid Time	Enter the invalidate timer value in seconds here. The range is from 1 to 65535 seconds. Select the **Default** option to use the default value here which is 180 seconds.
Flush Time	Enter the flush timer value in seconds here. The range is from 1 to 65535 seconds. Select the **Default** option to use the default value here which is 120 seconds.
Poison Reverse	Select to enable or disable the Poison Reverse feature here. When Poison Reverse is enabled, the routes learned from an interface will be advertised out to the same interface with an unreachable metric.
Split Horizon	Select to enable or disable the Split Horizon feature here. When Split Horizon is enabled, the routes learned from an interface will be not advertised out to the same interface.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Redistribute Settings** are described below:

Parameter	Description
Protocol	Select the protocol whose routes are to be redistributed here. Options to choose from are **Connected, OSPF** and **Static**. The **Static** option means to redistribute IPv6 static routes. The **Connected** option refers to routes that are established automatically by virtue of configuring IPv6 address on an interface.
Metric	Enter the value to be used as the metric for the redistributed routes here. The range is from 0 to 16. Select the **Default** option to use the default metric value.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete an entry based on the information entered.

RIPng Interface Settings

This window is used to display and configure the RIPng interface settings.

To view the following window, click **L3 Features > RIPng > RIPng Interface Settings**, as shown below:

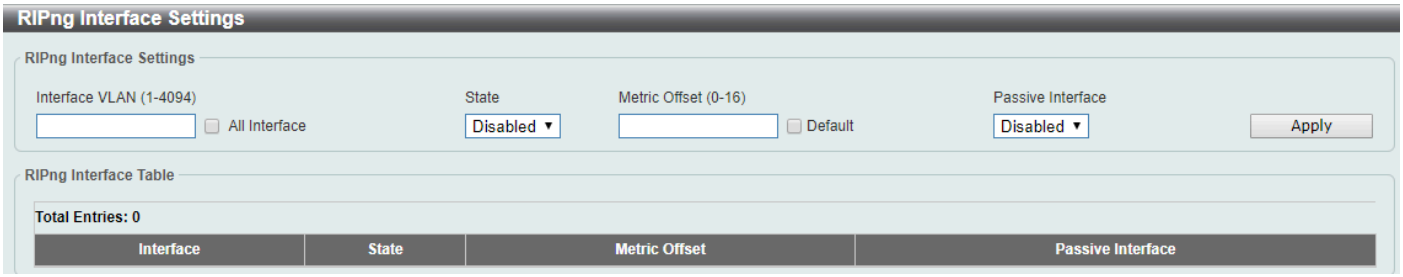


Figure 6-33 RIPng Interface Settings Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID here. The range is from 1 to 4094. Select the **All Interface** option to use all available interfaces in this configuration.
State	Select to enable or disable the IPv6 RIP feature on the VLAN interface specified.
Metric Offset	Enter the value to be added to the metric of an IPv6 RIP route received on the configured interface here. The range is from 0 to 16. The metric refers to the hop count. By default, w-hen receiving an IPv6 RIP route, a metric value of 1 is added to the route before it is inserted into the routing table. Use this option to influence the metric of routes received on different interfaces and influence the preference of the route. Select the **Default** option to use the default metric offset value, which is 0.
Passive Interface	Select to enable or disable the passive interface feature here. If this option is disabled, the router will not send RIPng packets out through the interface. However, RIPng packets from other routers received on the interface will continue to be processed.

Click the **Apply** button to accept the changes made.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

RIPng Database

This window is used to display the RIPng routing database.

To view the following window, click **L3 Features > RIPng > RIPng Database**, as shown below:



Figure 6-34 RIPng Database Window

The fields that can be configured are described below:

Parameter	Description
IPv6 Address/Prefix Length	Enter the IPv6 address with prefix length for the desired network.

Click the **Find** button to locate a specific entry based on the information entered.

OSPF

OSPFv2

OSPFv2 Process Settings

This window is used to display and configure the OSPFv2 process settings.

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPFv2 Process Settings**, as shown below:

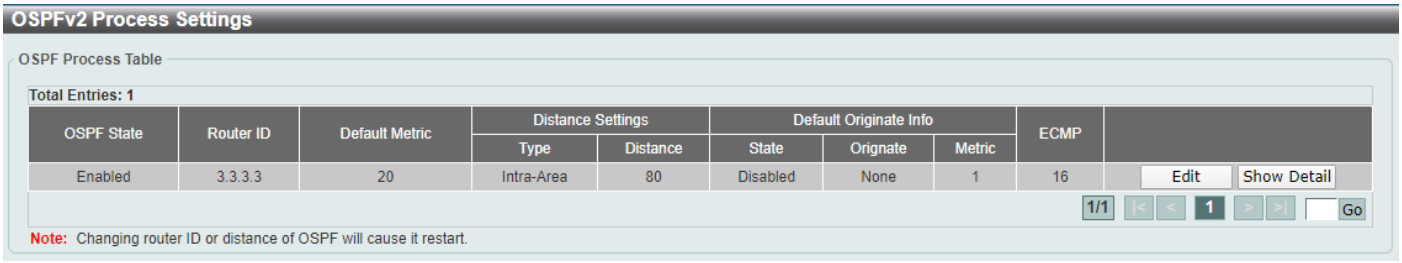


Figure 6-35 OSPFv2 Process Settings Window

Click the **Edit** button to modify the specified entry.

Click the **Show Detail** button to view more detailed information associated with the entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Edit** button, the following page will appear.

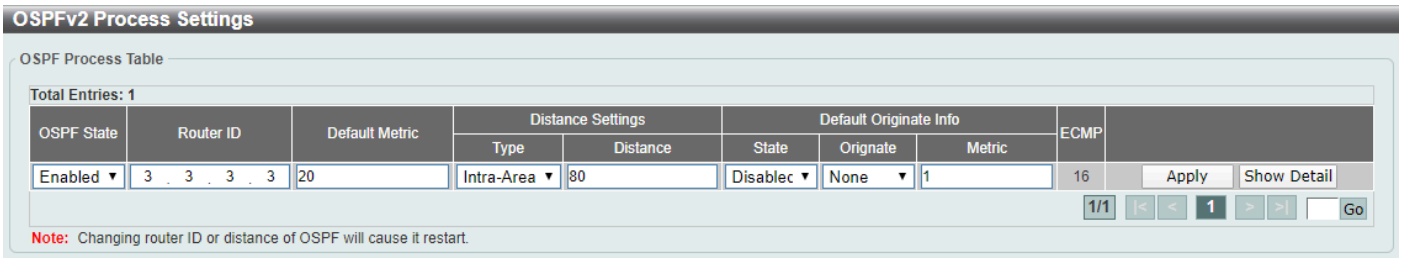


Figure 6-36 OSPFv2 Process Settings (Edit) Window

The fields that can be configured are described below:

Parameter	Description
OSPF State	Select to enable or disable the OSPFv2 state.
Router ID	Enter the router ID in the IPv4 address format here. The router ID is a 32-bit number assigned to each router running the OSPF protocol. This number uniquely identifies the router within an AS. Each router has a unique router ID.
Default Metric	Enter the default metric value used here. The range is from 1 to 16777214.
Type	Select the distance setting type here. Options to choose from are **Intra-Area**, **Inter-Area**, **External-1**, and **External-2**. • **Inter-Area** - Specifies the distance for OSPF inter-area routes. • **Intra-Area** - Specifies the distance for OSPF intra-area routes. • **External-1** - Specifies the distance for OSPF external type-5 and type-7 routes with a type-1 metric. • **External-2** - Specifies the distance for OSPF external type-5 and type-7 routes with a type-2 metric.
Distance	Enter the administrative distance value here. The range is from 1 to 255.
State	Select to enable or disable the Default Originate Information state here. This feature is used to generate a default external route (type-5 LSA) network 0.0.0.0 to the AS.
Originate	Select the Originate option here. Options to choose from are **Always** and **None**. Selecting the **Always** option specifies to always generate the default route regardless of existence of a default route in the routing table.

Parameter	Description
Metric	Enter the cost value associated with the generated default route here. If not specified, the default metric cost is 1. The range is from 1 to 65535.

Click the **Apply** buttonAfter clicking the **Show Detail** button, the following page will appear.

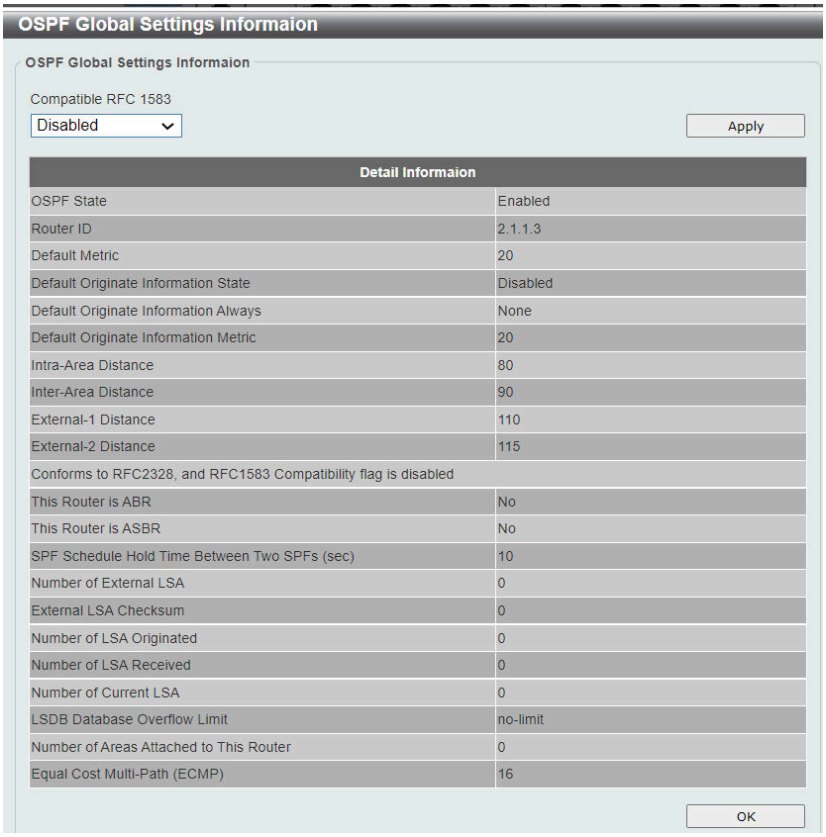


Figure 6-37 OSPFv2 Process Settings (Show Detail) Window

The fields that can be configured are described below:

Parameter	Description
Compatible RFC1583	Select to enable or disable the selection of the optimal route to a destination as specified in RFC 1583 here.

Click the **Apply** button to accept the changes made.

Click the **OK** button to accept the changes made.

OSPFv2 Distribute List

This window is used the view and configure the OSPFv2 Distribute List settings.

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPFv2 Distribute List**, as shown below:

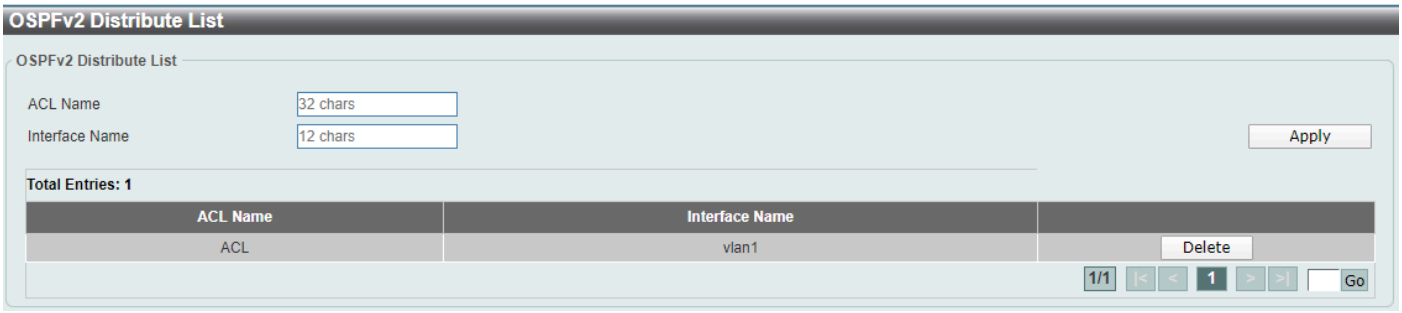


Figure 6-38 OSPFv2 Distribute List Window

The fields that can be configured are described below:

Parameter	Description
ACL Name	Enter the access list name that will be used here. This name can be up to 32 characters long. Refer to **ACL > ACL Access List**.
Interface Name	Enter the interface name that will be used here. This name can be up to 12 characters long. Refer to **L3 Features > Interface**.

Click the **Apply** button to accept the changes made.

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.

OSPFv2 GR Helper Settings

This window is used to display and configure the OSPFv2 graceful restart helper settings.

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPFv2 GR Helper Settings**, as shown below:



Figure 6-39 OSPFv2 GR Helper Settings Window

The fields that can be configured are described below:

Parameter	Description
Graceful Restart Helper	Select the graceful restart helper mode here. Options to choose from are: • **Unspec** - The OSPF graceful restart helper mode is unspecified. • **Never** - Specifies to not to allow the OSPF graceful restart helper mode. • **Only Reload** - Specifies to allow the OSPF graceful restart helper mode only for reload.

Parameter	Description
Max Grace Period	Enter the maximum grace period value here. The range is from 1 to 1800 seconds.

Click the **Apply** button to accept the changes made.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

OSPFv2 Passive Interface Settings

This window is used to display and configure the OSPFv2 passive interface settings.

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPFv2 Passive Interface Settings**, as shown below:

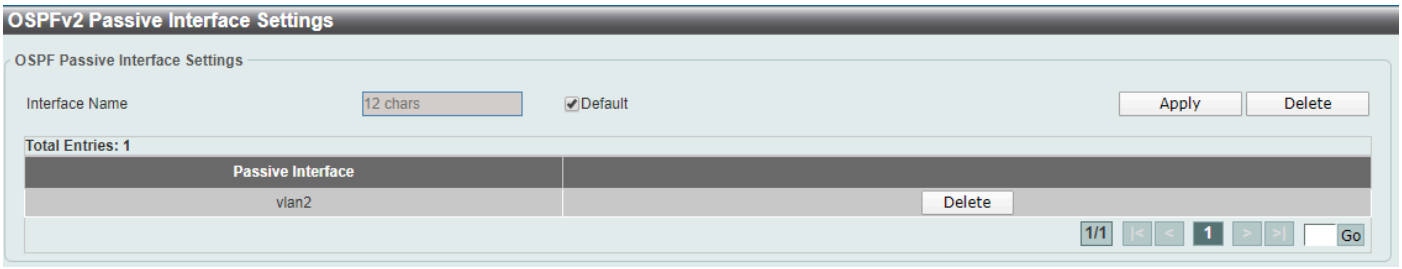


Figure 6-40 OSPFv2 Passive Interface Settings Window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the interface name that will be used here. This name can be up to 12 characters long. Refer to **L3 Features > Interface**. Select the **Default** option to use all available interfaces here.

Click the **Apply** button to accept the changes made.

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.

OSPFv2 Area Settings

This window is used to display and configure the OSPFv2 area settings.

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPFv2 Area Settings**, as shown below:

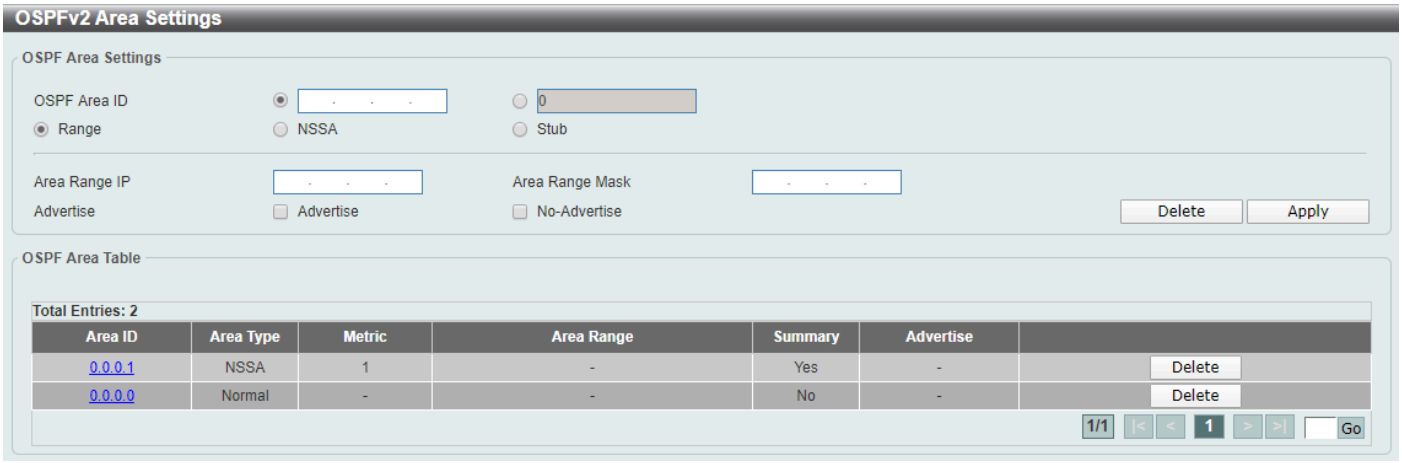


Figure 6-41 OSPFv2 Area Settings Window

The fields that can be configured in **OSPF Area Settings** are described below:

Parameter	Description
Area ID	Select and enter the OSPFv2 area ID here. This can be specified in the IP address format or in the decimal value format. The decimal range is from 0 to 4294967295. The area will be created on an interface if the subnet configured on the interface falls within the network range specified here.
Range	Select this option to summarize OSPF routes at an Area Border Router (ABR).
NSSA	Select this option to assign the OSPF area as a Not-So-Stubby Area (NSSA) area.
Stub	Select this option to specify an OSPF area as a Stub Area.
Area Range IP	This parameter is available when **Range** is selected. Enter the OSPF area range IP address here.
Area Range Mask	This parameter is available when **Range** is selected. Enter the OSPF area range subnet mask here.
Advertise	This parameter is available when **Range** is selected. Select the advertise option here. Options to choose from are **Advertise** and **No-Advertise**. • **Advertise** - Specifies to advertise a Type-3 summary Link-State Advertisement (LSA) for the specified range of addresses. • **No-Advertise** - Specifies to suppress the advertising of Type-3 summary LSAs. Component routes are still hidden behind it.
Metric	This parameter is available when **NSSA** or **Stub** is selected. Enter the metric value (0~65535) here. This is the cost associated with the Type-3 default route that will be injected into the stub area and not-so-stubby area. The range is from 0 to 65535. • **Default** - Select this option to use the default metric value. • **No-Summary** - Select this option not to inject summary routes into this area.

Click the **Delete** button to delete an entry based on the information entered.

Click the **Apply** button to accept the changes made.

Click the **Area ID** link (0.0.0.0) to view more detailed settings about the entry.

After clicking the **Area ID** link (0.0.0.0), the following page will appear.



Figure 6-42 OSPFv2 Area Settings (Area ID) Window

Click the **OK** button to close the window.

OSPFv2 Interface Settings

This window is used to display and configure the OSPFv2 interface settings.

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPFv2 Interface Settings**, as shown below:

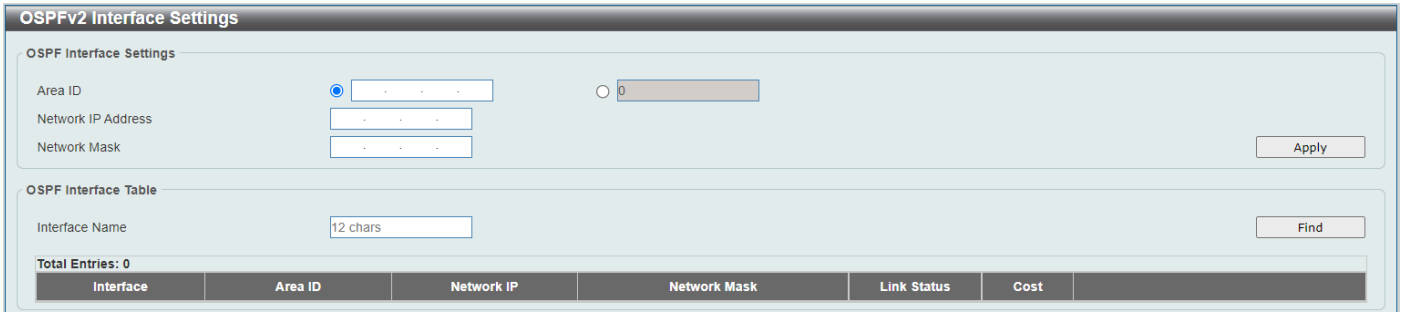


Figure 6-43 OSPFv2 Interface Settings Window

The fields that can be configured in **OSPF Interface Settings** are described below:

Parameter	Description
Area ID	Select and enter the OSPFv2 area ID here. This can be specified in the IP address format or in the decimal value format. The decimal range is from 0 to 4294967295.
Network IP Address	Enter the network IPv4 address here.
Network Mask	Enter the network IPv4 subnet mask here.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **OSPF Interface Table** are described below:

Parameter	Description
Interface Name	Enter the name of the interface to be displayed here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show Detail** button to view more detailed information about the 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.

After clicking the **Show Detail** button, the following page will appear.

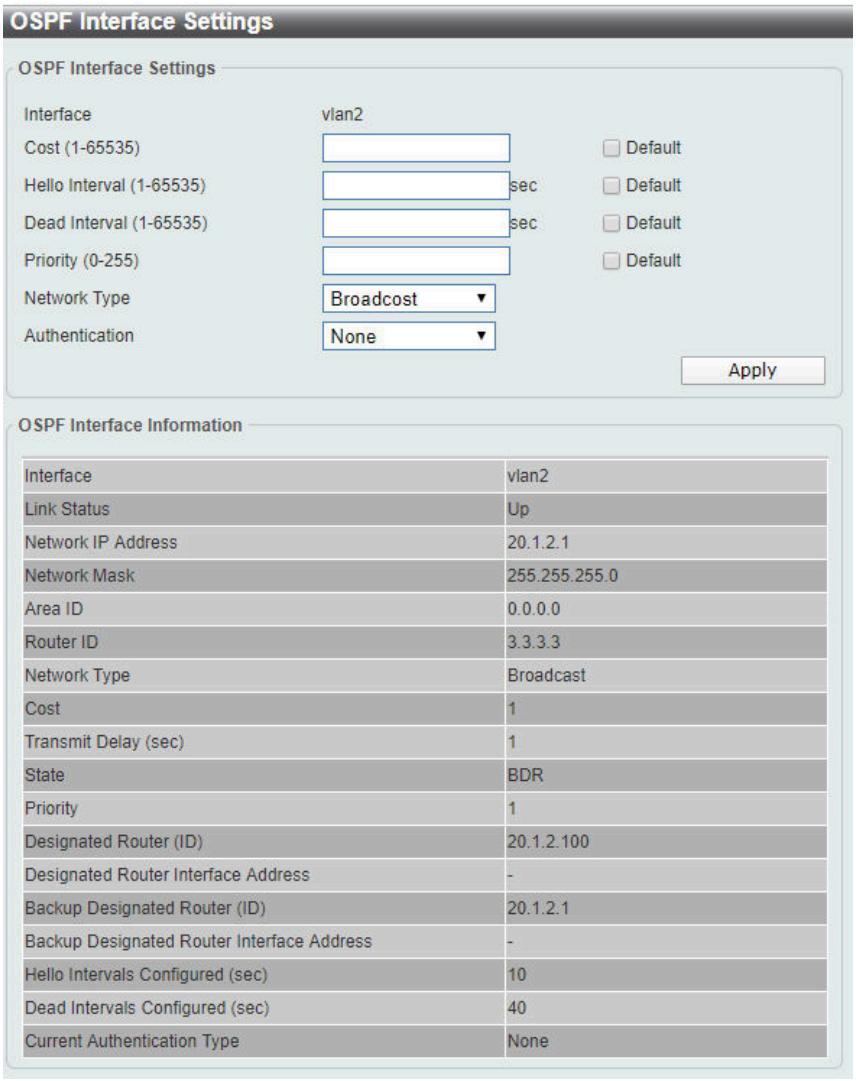


Figure 6-44 OSPFv2 Interface Settings (Show Detail) Window

The fields that can be configured are described below:

Parameter	Descriptionx
Cost	Enter the cost value here. The range is from 1 to 65535. The interface cost reflects the overhead for sending the packet across the interface. This cost is advertised as the link cost in the router link advertisement. Select the **Default** option to use the default value which is 1.

Parameter	Descriptionx
Hello Interval	Enter the Hello Interval time value here. The range is from 1 to 65535 seconds. The Hello Interval is advertised in the hello packets. Configure the same hello-interval for all routers on a specific network. A shorter Hello Interval ensures faster detection of topological changes but generates more routing traffic and might cause routing instability. Select the **Default** option to use the default value which is 10 seconds.
Dead Interval	Enter the Dead Interval time value here. The range is from 1 to 65535 seconds. The Dead Interval is the amount of time that the router waits to receive an OSPF hello packet from the neighbor before declaring the neighbor down. This value is advertised in the router's hello packets. It must be the same for all routers on a specific network. Specifying a smaller Dead Interval ensures faster detection of topology changes, but might cause routing instability. Select the **Default** option to use the default value which is 40 seconds.
Priority	Enter the priority value here. The range is from 0 to 255. The OSPF router will determine a Designated Router (DR) for the multi-access network. This sets the priority used to determine the OSPF DR for a network. If two routers attempt to become the DR, the router with the higher router priority will be elected the DR. If the routers have the same priority, the router with the higher router ID takes precedence. Only routers with non-zero router priority values are eligible to become the DR or Backup Designated Router (BDR). Select the **Default** option to use the default value which is 1.
Network Type	Select the network type here. Options to choose from are: • **Broadcast** - Specifies the network type as broadcast. • **Point-to-Point** - Specifies the network type as point-to-point. On a broadcast network, only the DR and BDR become adjacent neighbors of all other routers attached. On point-to-point networks, only two routers become adjacent if they can communicate.
Authentication	Select the authentication type that will be used here. Options to choose from are **None**, **Simple Password**, and **MD5**.
Password	After selecting the **Simple Password** option, enter the simple password here. This password can be up to 8 characters long. The syntax is general string that does not allow spaces. This creates a password (key) that is inserted into the OSPF header when the router originates routing protocol packets. Assign a separate password to each network for different interfaces. Routers on the same network must use the same password to be able to exchange OSPF routing data. Configure the routers in the same routing domain with the same password.
MD5 Key ID	Enter the MD5 key ID for the password here. The range is from 1 to 255.
MD5 Key	Enter the MD5 key here. This key can be up to 16 characters long. The syntax is an alphanumeric string that does not allow spaces. In the MD5 mode, the OSPF message sender will compute a message digest based on the message digest key for the TX message. The message digest and the key ID will be encoded in the packet. The receiver of the packet will verify the digest in the message against the digest computed based on the locally defined message digest key corresponding to the same key ID. The same key ID on the neighboring router should be defined with the same key string. All the neighboring routers on the same interface must use the same key to exchange the OSPF packet with each other. Normally, all neighboring routers on the interface use the same key. With the MD5 digest mode, the user can roll over to a new key without disrupting the current message exchange using the new key. Supposing that a router is currently using an old key to exchange OSPF packets with the

Parameter	Descriptionx
	neighbor router, as the user configures a new key, the router will start the roll over process by sending duplicated packets for both of the old and the new key. The router will stop sending duplicated packets until it finds that all routers on the network have learned the new key. After the rollover process completed, the user should delete the old key to prevent the router from communicating with the router using the old key.

Click the **Apply** button to accept the changes made.

OSPFv2 Redistribute Settings

This window is used to display and configure the OSPFv2 redistribution settings. External routes can be redistributed to normal areas as Type-5 external routes and redistributed to NSSA stub areas as Type-7 external routes by the ASBR.

If the redistributed external route is of Type-1, the metric represents the internal metric. If the redistributed external route is of Type-2, the metric represents the external metric. An internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric only considers the advertised metric to reach the destination.

If no metric value is specified by the default metric, routes redistributed from other protocols will get a metric value of 20.

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPFv2 Redistribute Settings**, as shown below:



Figure 6-45 OSPFv2 Redistribute Settings Window

The fields that can be configured are described below:

Parameter	Description
Protocol	Select the source protocol that will be redistributed here. Options to choose from are **Connected**, **Static** and **RIP**. For routing protocols like Open Shortest Path First (OSPF), these routes will be redistributed as external to the autonomous system.
Metric Type	Select the metric type here. Options to choose from are **External Type-1** and **External Type-2**. This specifies the external link type of the route being redistributed into the OSPF routing domain. By default, the Switch will adopt a Type-2 external route.
Metric	Enter the metric value for the redistributed routes here. The range is from 1 to 16777214.
Router Map Name	Enter the route map name here that filters the imported routes from this source routing protocol. If not specified, all routes are redistributed.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete the specified entry.

OSPFv2 Virtual-Link Settings

This window is used to display and configure OSPFv2 virtual-link settings. If a non-zero area is not physically connected to the zero area, it must be connected to the zero area via a virtual link. The virtual link is a point-to-point link. The router will send the OSPF message to the neighbor router as unicast IP packet.

To view the following window, click L3 Features > OSPF > OSPFv2 > OSPFv2 Virtual Link Settings, as shown below:

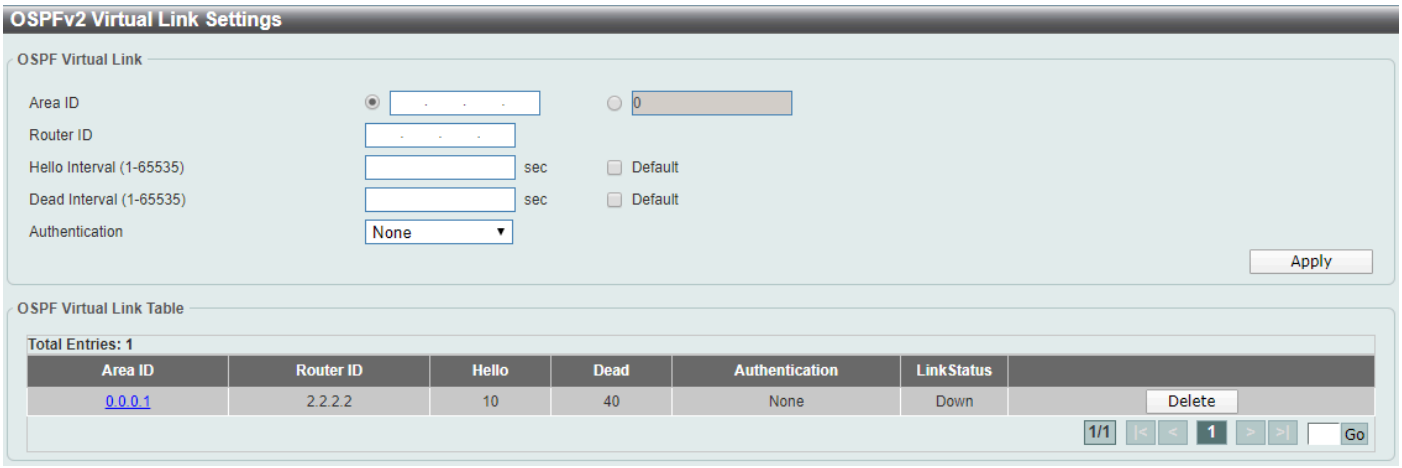


Figure 6-46 OSPFv2 Virtual Link Settings Window

The fields that can be configured in **OSPF Virtual Link** are described below:

Parameter	Description
Area ID	Select and enter the OSPFv2 area ID here. This can be specified in the IP address format or in the decimal value format. The decimal range is from 0 to 4294967295. This area will be used to establish the virtual link.
Router ID	Enter the router ID of the virtual link neighbor here.
Hello Interval	Enter the hello packet interval that the router sends on the virtual link here. The range is from 1 and 65535 seconds. Select the **Default** option to use the default value, which is 10 seconds.
Dead Interval	Enter the Dead Interval time after which a neighbor is regarded as offline if no hello packets are received within that time frame here. The range is from 1 and 65535 seconds. Select the **Default** option to use the default value, which is 40 seconds.
Authentication	Select the authentication type used here. Options to choose from are **None**, **Simple Password**, and **MD5**.
Password	After selecting the **Simple Password** authentication type, enter the password to be used here. This password can be up to 8 characters long.
MD5 Key ID	After selecting the **MD5** authentication type, enter the MD5 authentication key ID here. The range is from 1 to 255.
MD5 Key	After selecting the **MD5** authentication type, enter the MD5 authentication key here. This key can be up to 16 characters long.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete the specified entry.

Click the **Area ID** link (0.0.0.1) to view more detailed settings about the entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Area ID** link (0.0.0.1), the following page will appear.

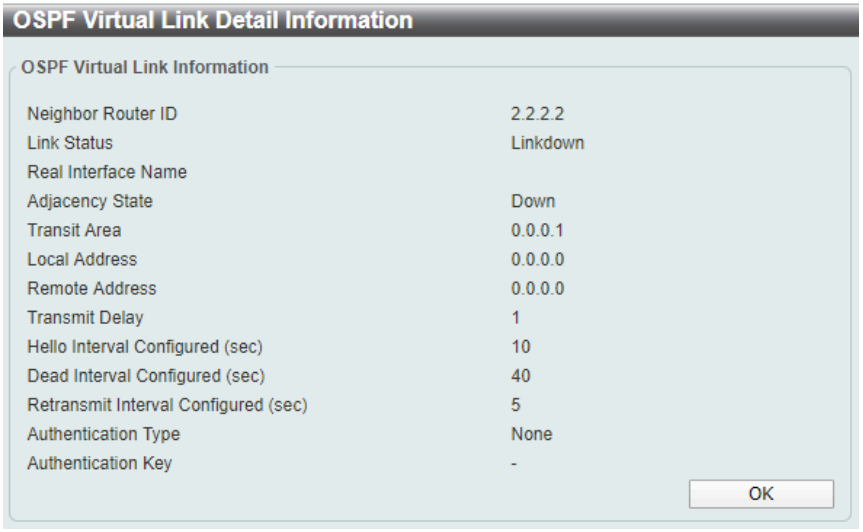


Figure 6-47 OSPFv2 Virtual Link Settings (Area ID) Window

Click the **Back** button to return to the previous window.

OSPFv2 LSDB Table

This window is used to display the OSPFv2 Link State Database (LSDB) table and information.

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPFv2 LSDB Table**, as shown below:

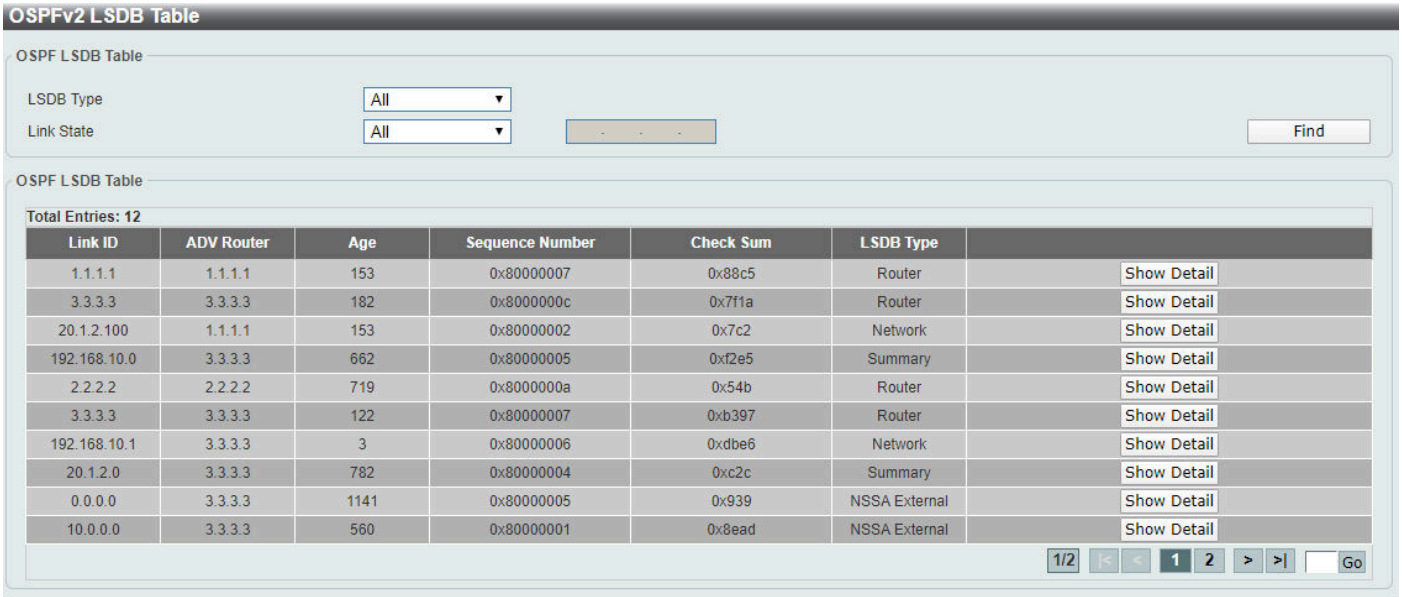


Figure 6-48 OSPFv2 LSDB Table Window

The fields that can be configured are described below:

Parameter	Description
LSDB Type	Select the LSDB type of information that will be displayed here. Options to choose from are **All**, **Router**, **Network**, **Summary**, **ASBR Summary**, **External**, **Stub**, and **NSSA External**.
Link State	Select the link-state information that will be displayed here. Options to choose from are **All**, **Link State ID**, **Self Originate**, and **Adv Router**. • **All** - Specifies to display all OSPFv2 link-state information. • **Link State ID** - Specifies to display information associated with the link-state ID. Enter the link state ID in the space provided here. • **Self Originate** - Specifies to display LSAs generated by the local router. • **Adv Router** - Specifies to display all of the LSAs generated by the advertising router. Enter the advertising router ID in the space provided here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show Detail** button to view more detailed information about the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Show Detail** button, the following page will appear.

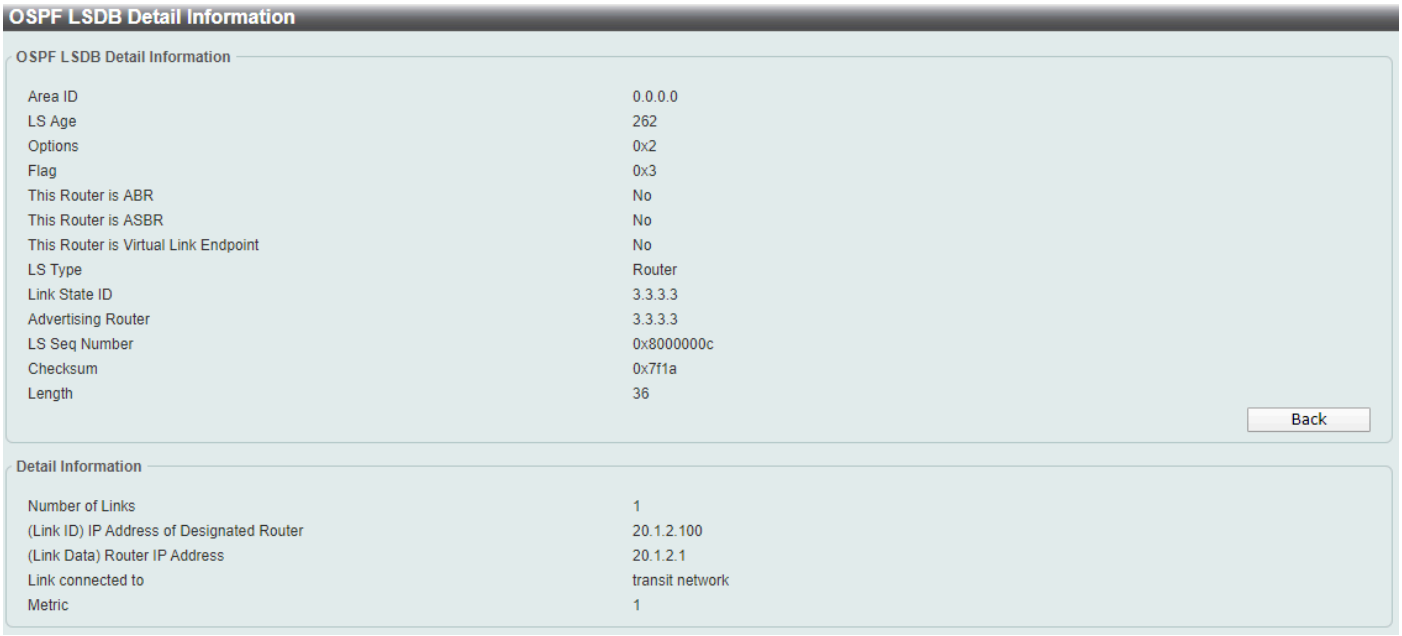


Figure 6-49 OSPFv2 LSDB Table (Show Detail) Window

Click the **Back** button to return to the previous window.

OSPFv2 Neighbor Table

This window is used to display information on OSPF neighbors.

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPFv2 Neighbor Table**, as shown below:

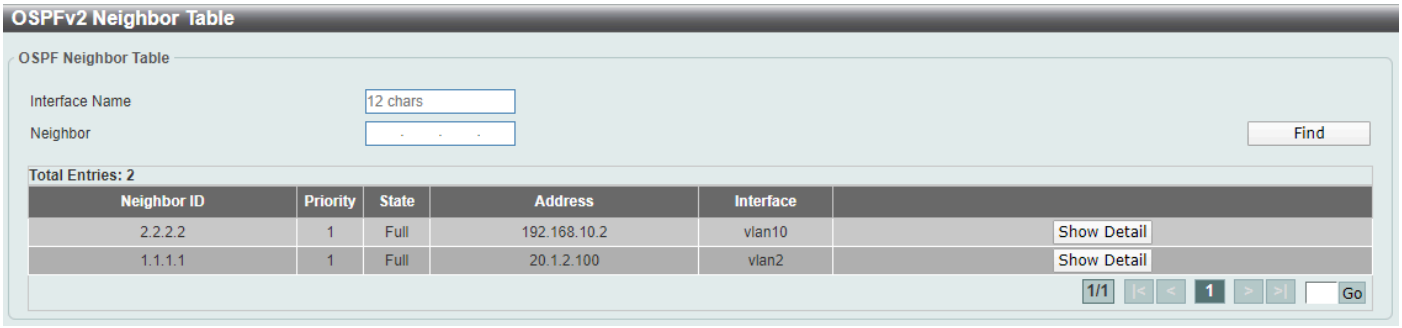


Figure 6-50 OSPFv2 Neighbor Table Window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the name of the interface that will be used in the results here.
Neighbor	Enter the neighbor ID here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show Detail** button to view more detailed information for the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Show Detail** button, the following page will appear.



Figure 6-51 OSPFv2 Neighbor Table (Show Detail) Window

Click the **Back** button to return to the previous window.

OSPFv2 Host Route Settings

This window is used to display and configure the OSPFv2 host route settings. The router will advertise specific host routes as router LSAs for a stub link.

To view the following window, click **L3 Features > OSPF > OSPFv2 > OSPFv2 Host Route Settings**, as shown below:

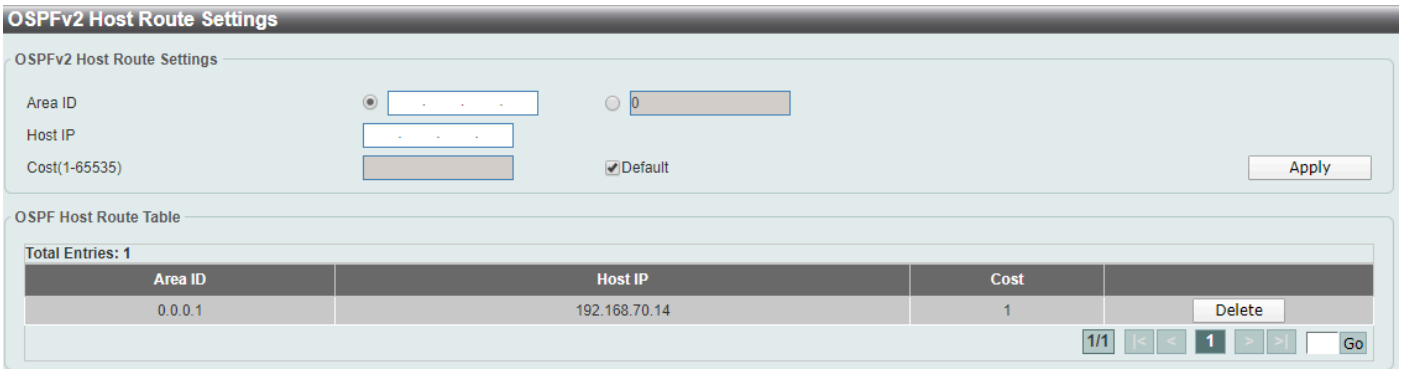


Figure 6-52 OSPFv2 Host Route Settings Window

The fields that can be configured in **OSPFv2 Host Route Settings** are described below:

Parameter	Description
Area ID	Select and enter the OSPFv2 area ID here. This can be specified in the IP address format or in the decimal value format. The decimal range is from 0 to 4294967295.
Host IP	Enter the host IPv4 address here.
Cost	Enter the cost value for the stub entry here. The range is from 1 to 65535. Select the **Default** option to use the default value, which is 1.

Click the **Apply** button to accept the changes made.

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.

OSPFv3

OSPFv3 Process Settings

This window is used to display and configure OSPFv3 process settings.

To view the following window, click **L3 Features > OSPF > OSPFv3 > OSPFv3 Process Settings**, as shown below:

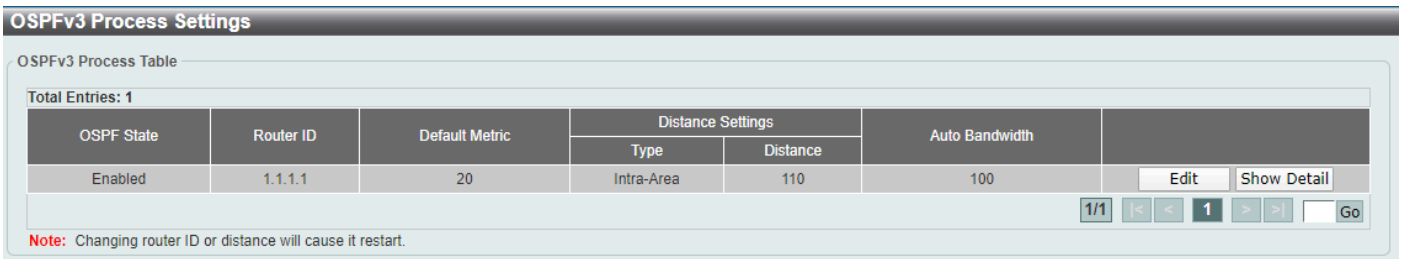


Figure 6-53 OSPFv3 Process Settings Window

Click the **Edit** button to modify the specified entry.

Click the **Show Detail** button to view more detailed information about the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Edit** button, the following page will appear.

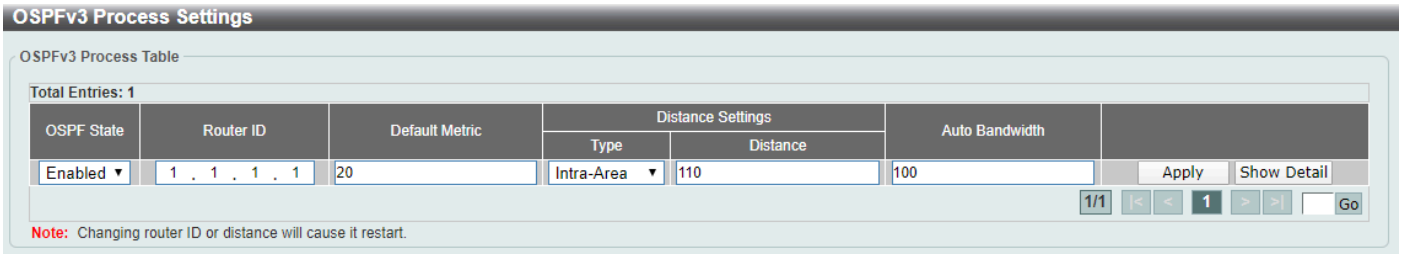


Figure 6-54 OSPFv3 Process Settings (Edit) Window

The fields that can be configured are described below:

Parameter	Description
OSPF State	Select to enable or disable the OSPFv3 state.
Router ID	Enter the router ID for the OSPF process here.
Default Metric	Enter the default metric value for the OSPF process here. The range is from 1 to 16777214. By default, this value is 20. This value is used in conjunction with the OSPFv3 redistribution feature to enable the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics. Whenever the metrics don't convert directly, using a default metric provides a reasonable substitute and enables the redistribution to proceed.
Type	Select the distance type here. Options to choose from are **Intra-Area**, **Inter-Area**, **External-1** and **External-2**. • **Intra-Area** - Specifies the distance for OSPF intra-area routes. • **Inter-Area** - Specifies the distance for OSPF inter-area routes. • **External-1** - Specifies the distance for OSPF external type-1 routes. • **External-2** - Specifies the distance for OSPF external type-2 routes.
Distance	Enter the distance value for the OSPF process here. The range is from 1 to 254. By default, this value is 110 for all OSPF routes.
Auto Bandwidth	Enter the auto-bandwidth value here. This feature is used to control the reference value IPv6 OSPF uses when calculating metrics for interfaces. The range is from 1 to 4294967.

Click the **Apply** button to accept the changes made.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Show Detail** in the table, the following page will appear.

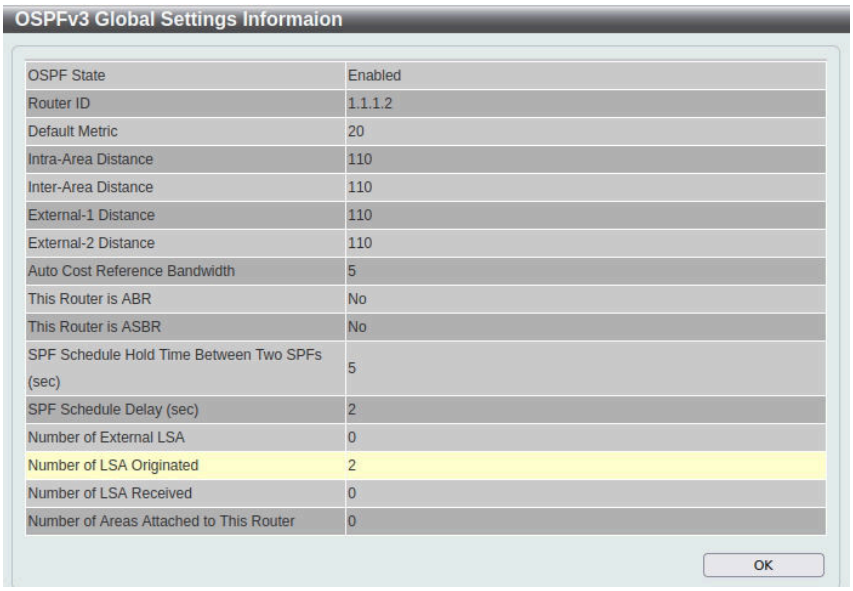


Figure 6-55 OSPFv3 Process Settings (Show Detail) Window

Click the **OK** button to close the window and return to the previous window.

OSPFv3 Passive Interface Settings

This window is used to display and configure the OSPFv3 passive interface settings. If an interface is passive, the OSPF routing update packets are not sent or received through the specified interface.

To view the following window, click **L3 Features > OSPF > OSPFv3 > OSPFv3 Passive Interface Settings**, as shown below:

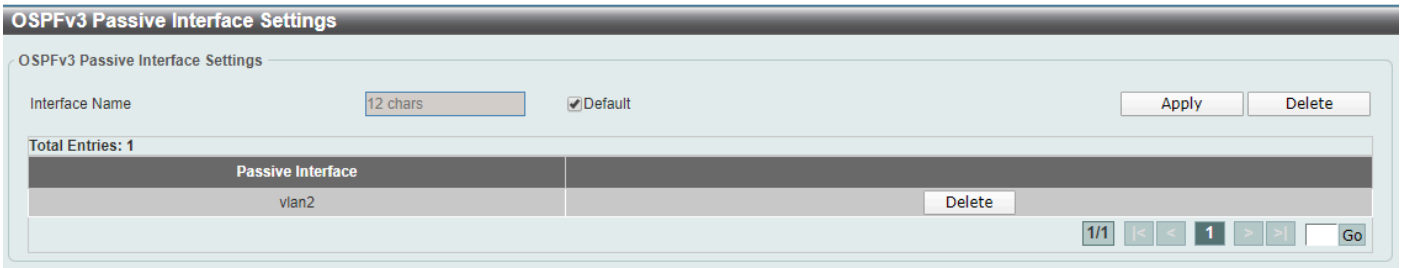


Figure 6-56 OSPFv3 Passive Interface Settings Window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the passive interface name here. This name can be up to 12 characters long. Refer to **L3 Features > Interface**. Select the **Default** option specify all the interfaces as passive interfaces.

Click the **Apply** button to accept the changes made.

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.

OSPFv3 Area Settings

This window is used to display and configure the OSPFv3 area settings.

To view the following window, click **L3 Features > OSPF > OSPFv3 > OSPFv3 Area Settings**, as shown below:

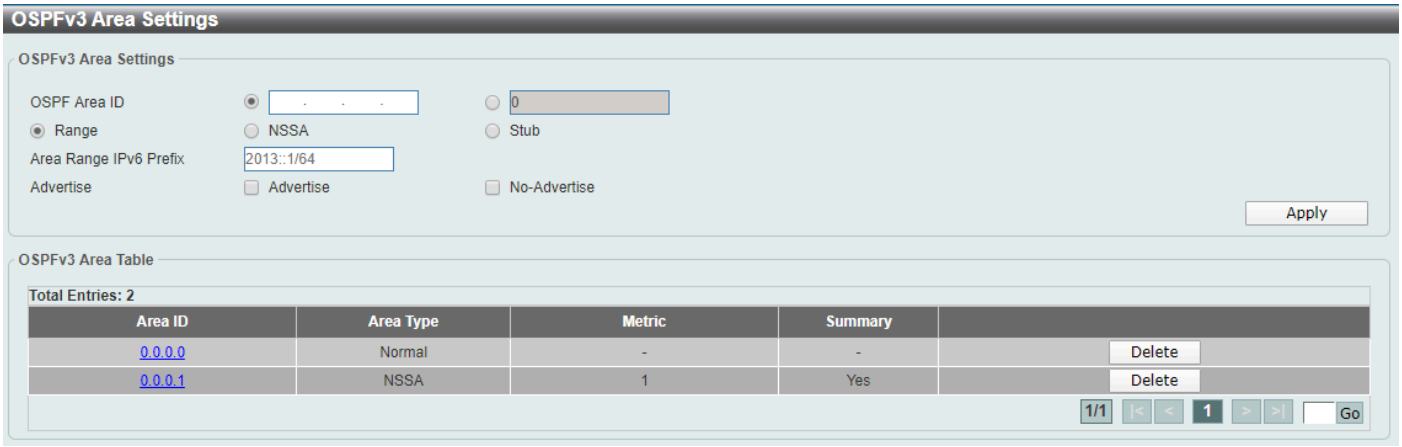


Figure 6-57 OSPFv3 Area Settings Window

The fields that can be configured in **OSPFv3 Area Settings** are described below:

Parameter	Description
OSPF Area ID	Enter the OSPF area ID used here. It can be specified as an IPv4 address or in the decimal value format. The decimal range is from 0 to 4294967295.
Range	Select this option to consolidate and summarize routes at an area boundary. This feature is used only with ABRs. It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range.
NSSA	Select this option to assign the OSPF area as a Not-So-Stubby Area (NSSA) area.
Stub	Select this option to define an area as a Stub area.
Area Range IPv6 Prefix	After selecting the **Range** option, enter the OSPF area range IPv6 prefix and prefix length here.
Advertise	After selecting the **Range** option, select the advertise option here. Options to choose from are **Advertise** and **No-Advertise**. • **Advertise** - Specifies to advertise and generate an inter-area prefix LSA for the specified address range. • **No-Advertise** - Specifies to set the status to Do-Not-Advertise for the specified address range. The inter-area prefix LSA is suppressed, and the component networks remain hidden from other networks.
Metric	After selecting the **NSSA** option or **Stub** option, enter the stub area metric value here. The range is from 0 to 65535. • **Default Metric** - Select this option use the default metric value for this area, which is 1. • **No-Summary** - Select this option to prevent an ABR from sending inter-area prefix LSAs into the stub area.

Click the **Apply** button to accept the changes made.

Click the **Area ID** link (0.0.0.1) to access the specified OSPFv3 process.

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.

After clicking a **NSSA** area the Area ID link (0.0.0.1) in the table, the following page will appear.

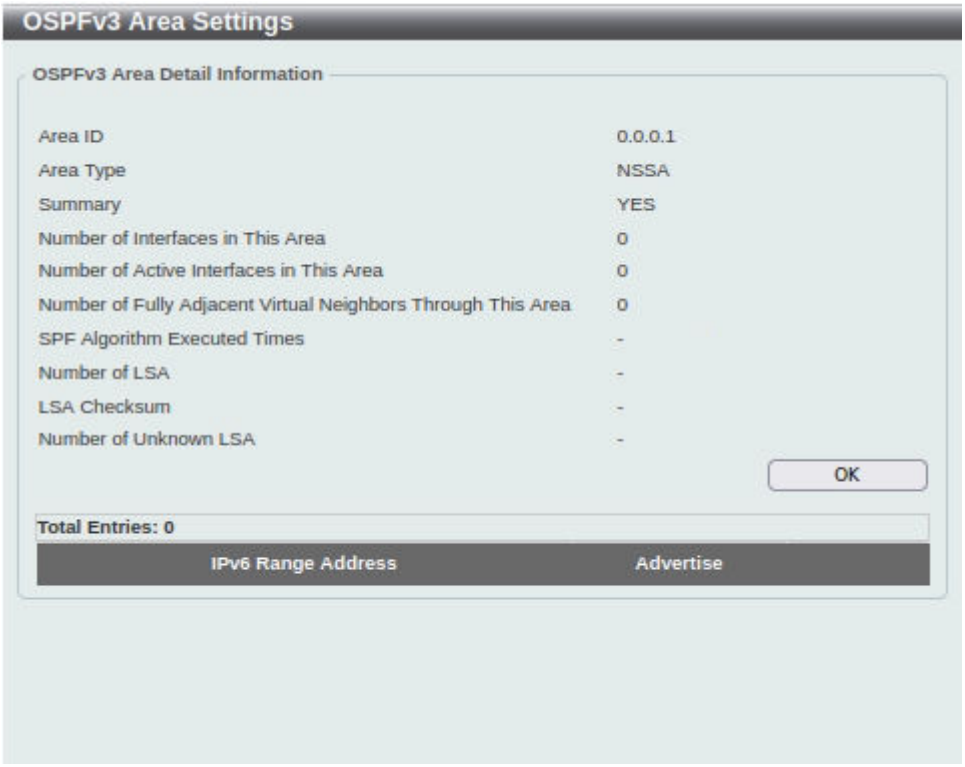


Figure 6-58 OSPFv3 Area Settings (Area ID, NSSA) Window

Click the **OK** button to close the window and return to the previous window.

After clicking a **Normal** area the Area ID link (0.0.0.0) in the table, the following page will appear.

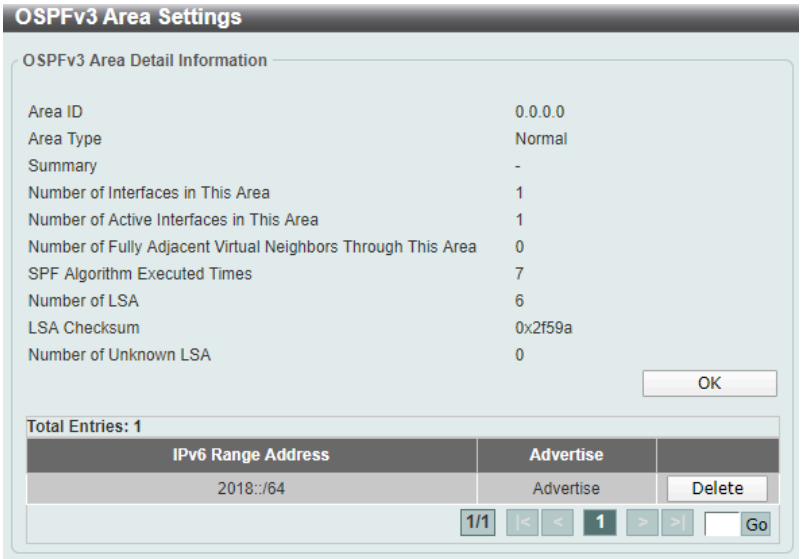


Figure 6-59 OSPFv3 Area Settings (Area ID, Normal) Window

Click the **OK** button to close the window and return to the previous window.

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.

OSPFv3 Interface Settings

This window is used to display and configure the OSPFv3 interface settings.

To view the following window, click **L3 Features > OSPF > OSPFv3 > OSPFv3 Interface Settings**, as shown below:

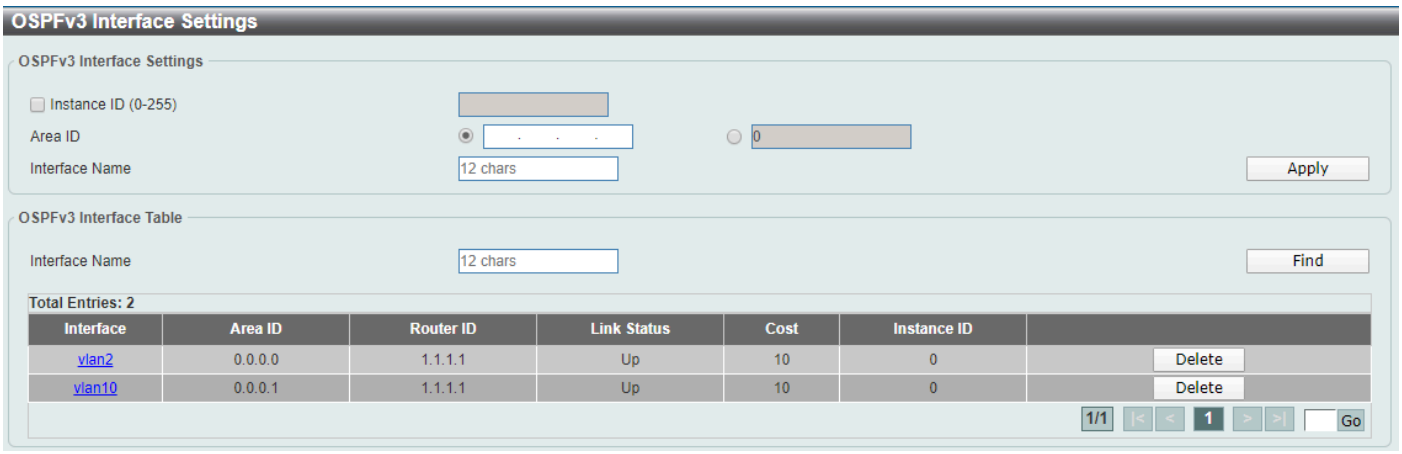


Figure 6-60 OSPFv3 Interface Settings Window

The fields that can be configured in **OSPFv3 Interface Settings** are described below:

Parameter	Description
Instance ID	Enter the instance identifier here. The range is from 0 to 255. If not specified, the default is 0.
Area ID	Enter the identifier of the area here. It can be specified as an IPv4 address or in the decimal value format. The decimal range is from 0 to 4294967295.
Interface Name	Enter the name of the VLAN interface here. This name can be up to 12 characters long. Refer to **L3 Features > Interface**.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **OSPF Interface Table** are described below:

Parameter	Description
Interface Name	Enter the name of the interface here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Interface Name** link to access and configure the specified OSPFv3 process.

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.

After clicking the **Interface Name** link button, the following page will appear.

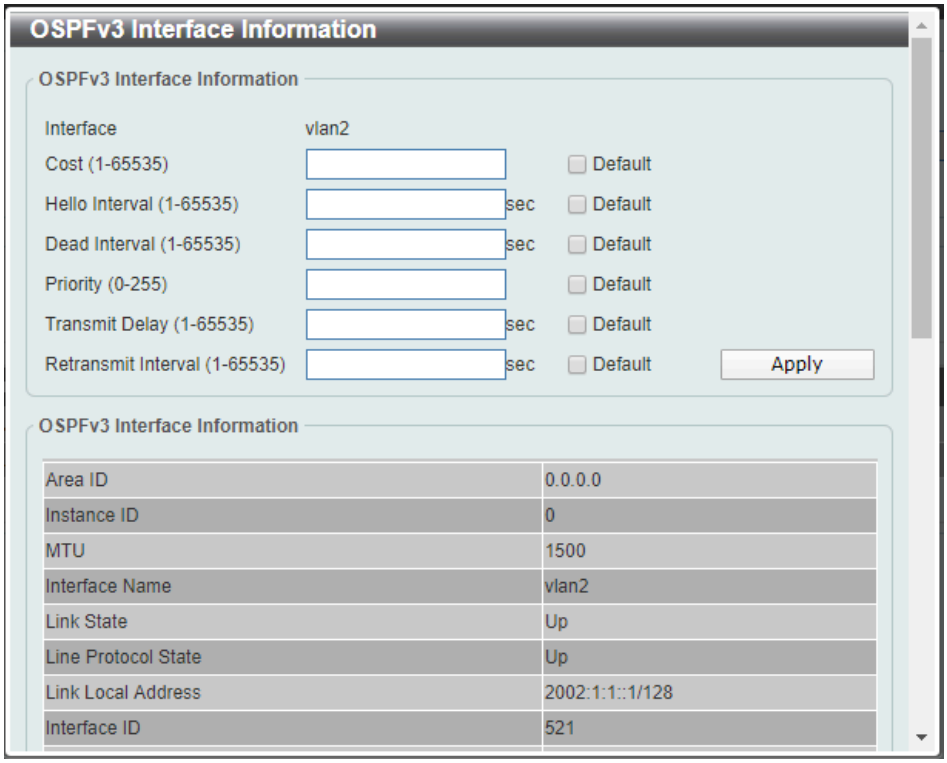


Figure 6-61 OSPFv3 Interface Settings (Interface Name) Window

The fields that can be configured are described below:

Parameter	Description
Cost	Enter cost value here. It is an integer value expressed as the link-state metric. The range is from 1 to 65535. Select the **Default** option to use the default value.
Hello Interval	Enter the Hello Interval value, between the hello packets that the router sends on an interface here. This value is advertised in the hello packets. The shorter the Hello Interval, the earlier topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network. The range is from 1 to 65535 seconds. Select the **Default** option to use the default value, which is 10 seconds.
Dead Interval	Enter the Dead Interval value here, during which no packets are received and after which a neighbor is regarded as offline. The interval is advertised in router hello packets. This value must be the same for all routers and access servers on a specific network. The range is from 1 to 65535 seconds. Select the **Default** option to use the default value, which is 40 seconds.
Priority	Enter the priority value of the router here. The range is from 0 to 255. Set the priority to help determine the OSPF Designated Router (DR) for a network. If two routers attempt to become the DR, the router with the higher router priority becomes the DR. If the router priority is the same for two routers, the router with the higher router ID takes precedence. Only routers with non-zero router priority values are eligible to become the designated or backup designated router. Configure router priority for multi-access networks (not point-to-point) only. Select the **Default** option to use the default value, which is 1.
Transmit Delay	Enter the Transmit Delay value here. The range is from 1 to 65535 seconds. Link-State Updates (LSUs) must have their ages incremented by the amount

Parameter	Description
	specified in the seconds argument before transmission. The value assigned should take into account the transmission and propagation delays for the interface. If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. This setting has more significance on very low speed links. Select the **Default** option to use the default value, which is 1 second.
Retransmit Interval	Enter the Retransmit Interval value here. The range is from 1 to 65535 seconds. After sending an LSA to a neighbor, the router keeps the LSA until it receives an acknowledgement. In case the router does not receive an acknowledgement during the set time (the Retransmit Interval value), it retransmits the LSA. Set the retransmission interval value conservatively to avoid unnecessary retransmission. The interval should be greater than the expected round-trip delay between two routers. Select the **Default** option to use the default value, which is 5 seconds.

Click the **Apply** button to accept the changes made.

OSPFv3 Redistribute Settings

This window is used to display and configure the OSPFv3 redistribution settings.

To view the following window, click **L3 Features > OSPF > OSPFv3 > OSPFv3 Redistribute Settings**, as shown below:



Figure 6-62 OSPFv3 Redistribute Settings Window

The fields that can be configured are described below:

Parameter	Description
Protocol	Select the source protocol from which routes will be redistributed here. Options to choose from are **Connected**, **Static**, and **RIPng**.
Metric Type	Select the external link type associated with the default route advertised into the IPv6 OSPF routing domain here. Options to choose from are **External Type-1** and **External Type-2**. By default, the Switch adopts a Type-2 external route.
Metric	Enter the metric value here. This value is used when redistributing other processes to an IPv6 OSPF process. The range is from 1 to 16777214. The default metric is value 20 when no metric value is specified.
Router Map Name	Enter the route map name here that filters the imported routes from this source routing protocol. If not specified, all routes are redistributed.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete the specified entry.

OSPFv3 Virtual Link Settings

This window is used to display and configure the OSPFv3 virtual link settings.

To view the following window, click **L3 Features > OSPF > OSPFv3 > OSPFv3 Virtual Link Settings**, as shown below:

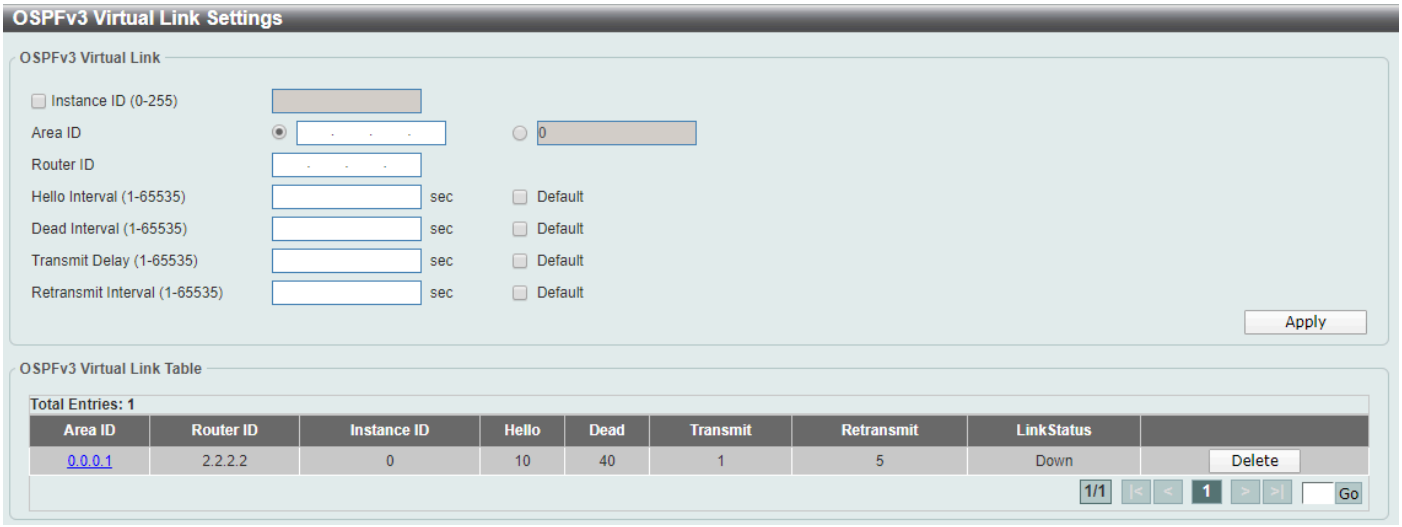


Figure 6-63 OSPFv3 Virtual Link Settings Window

The fields that can be configured in **OSPFv3 Virtual Link** are described below:

Parameter	Description
Instance ID	Select and enter the instance ID here. The range is from 0 to 255.
Area ID	Enter the OSPF area ID here. It can be specified as an IPv4 address or in the decimal value format. The decimal range is from 0 to 4294967295.
Router ID	Enter the router ID here associated with the virtual link neighbor.
Hello Interval	Enter the Hello Interval value between the hello packets that the router sends on an interface here. The range is from 1 to 65535 seconds. Select the **Default** option to use the default value, which is 10 seconds.
Dead Interval	Enter the Dead Interval value, during which no packets are received and after which a neighbor is regarded as offline, here. The range is from 1 to 65535 seconds. Select the **Default** option to use the default value, which is 40 seconds.
Transmit Delay	Enter the transmit delay value here that the router uses to wait before it transmits a packet. The range is from 1 to 65535 seconds. Select the **Default** option to use the default value, which is 1 second.
Retransmit Interval	Enter the retransmit interval value here that the router uses to wait before it retransmits a packet. The range is from 1 to 65535 seconds. Select the **Default** option to use the default value, which is 5 seconds.

Click the **Apply** button to accept the changes made.

Click the **Area ID** link (0.0.0.1) to access the specified OSPFv3 process.

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.

After clicking the **Area ID** link (0.0.0.1), the following page will appear.

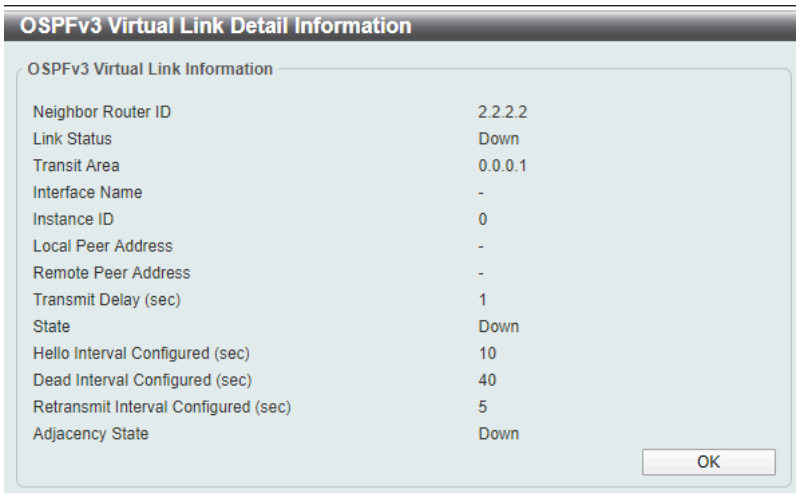


Figure 6-64 OSPFv3 Virtual Link Settings (Area ID) Window

Click the **OK** button to close the window and return to the previous window.

OSPFv3 LSDB Table

This window is used to find and display the OSPFv3 Link State Database (LSDB) information.

To view the following window, click **L3 Features > OSPF > OSPFv3 > OSPFv3 LSDB Table**, as shown below:

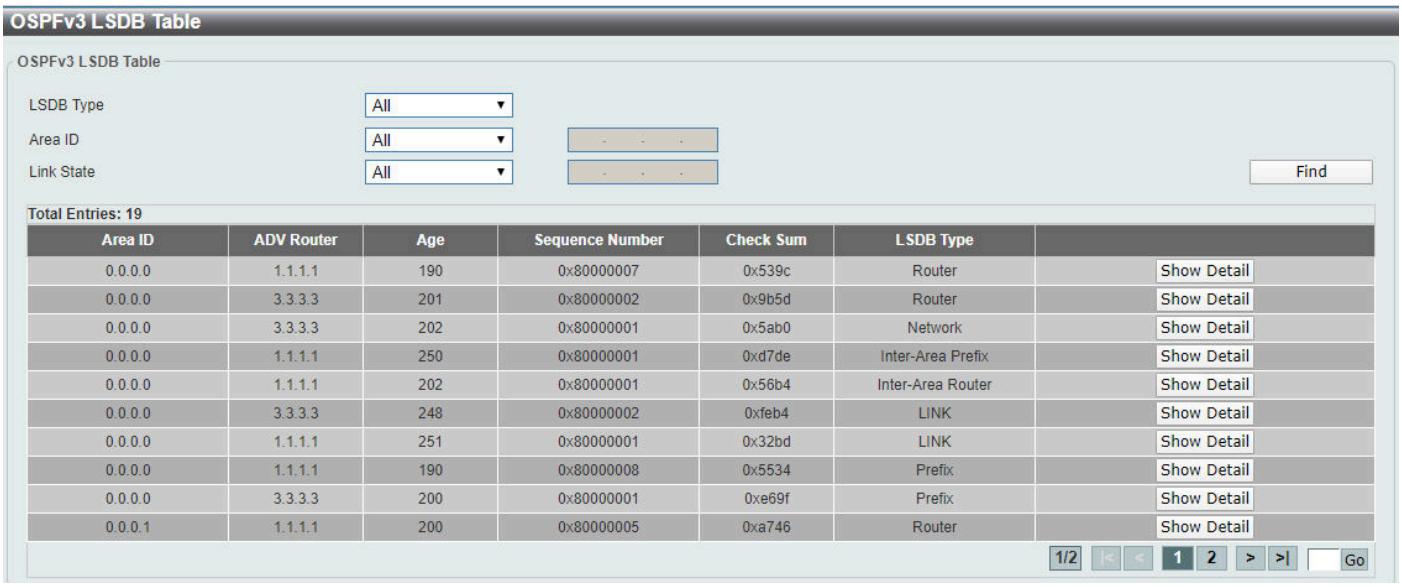


Figure 6-65 OSPFv3 LSDB Table Window

The fields that can be configured are described below:

Parameter	Description
LSDB Type	Select the LSDB display type here. Options to choose from are **All**, **Router**, **Network**, **Prefix**, **Link**, **Inter-Area Prefix**, **Inter-Area Router**, **External** and **NSSA External**.

Parameter	Description
	• **All** - Specifies to display all types of LSDB information. • **Router** - Specifies to display information only about the router LSAs. • **Network** - Specifies to display information only about the network LSAs. • **Prefix** - Specifies to display information on the intra-area-prefix LSAs. • **Link** - Specifies to display information about the link LSAs. • **Inter-Area Prefix** - Specifies to display information only about LSAs based on inter-area prefix LSAs. • **Inter-Area Router** - Specifies to display information only about LSAs based on inter-area router LSAs. • **External** - Specifies to display information only about the external LSAs. • **NSSA External** - Specifies to display information only about the NSSA external LSAs.
Area ID	Select the area ID option here. Options to choose from are **All** and **Area ID**. To display all the LSAs of the specified area, select the **Area ID** option and enter the OSPF area ID in the space provided. It can be specified as an IPv4 address.
Link State	Select the link state option here. Options to choose from are **All**, **Self Originate**, and **Adv Router**. • **All** - Specifies to display all the LSAs. • **Self Originate** - Specifies to display only self-originated LSAs (from the local router). • **Adv Router** - Specifies to display all the LSAs of the advertising router. Enter the router ID in the space provided. The router ID can be specified as an IPv4 address.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show Detail** button to view more detailed information for the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Show Detail** button, the following page will appear.



Figure 6-66 OSPFv3 LSDB Table (Show Detail) Window

Click the **Back** button to return to the previous window.

OSPFv3 Neighbor Table

This window is used to find and display the OSPFv3 neighbor information.

To view the following window, click **L3 Features > OSPF > OSPFv3 > OSPFv3 Neighbor Table**, as shown below:

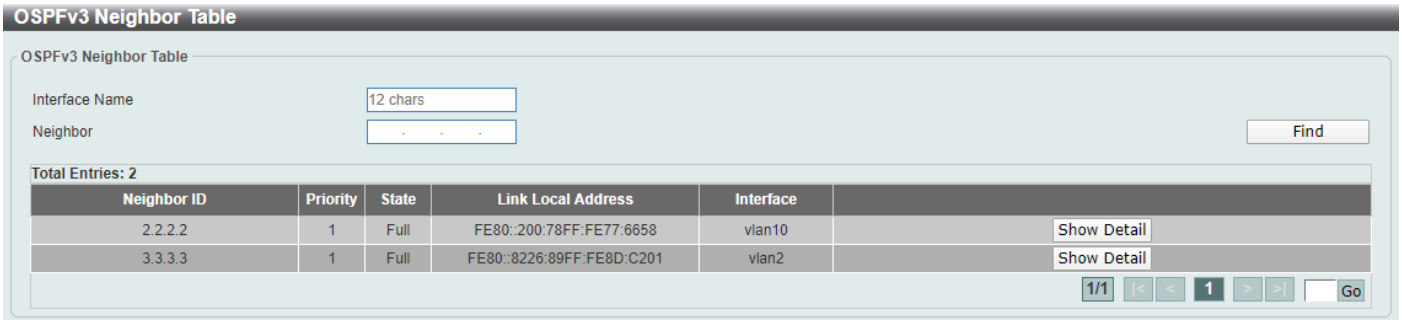


Figure 6-67 OSPFv3 Neighbor Table Window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the name of the interface here. Refer to **L3 Features > Interface**.
Neighbor	Enter the OSPF neighbor ID here. It can be specified as an IPv4 address.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show Detail** button to view more detailed information for the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Show Detail** button, the following page will appear.



Figure 6-68 OSPFv3 Neighbor Table (Show Detail) Window

Click the **Back** button to return to the previous window.

IP Multicast Routing Protocol

IGMP

IGMP Interface Settings

This window is used to display and configure the Internet Group Management Protocol (IGMP) interface settings.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > IGMP > IGMP Interface Settings**, as shown below:

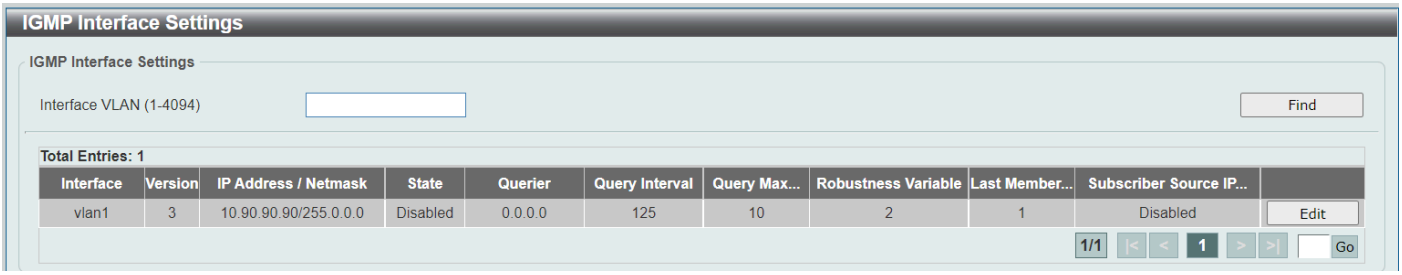


Figure 6-69 IGMP Interface Settings Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the interface VLAN ID used here. This value must be between **1** and **4094**.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Edit** button to modify the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Edit** button, the following page will appear.

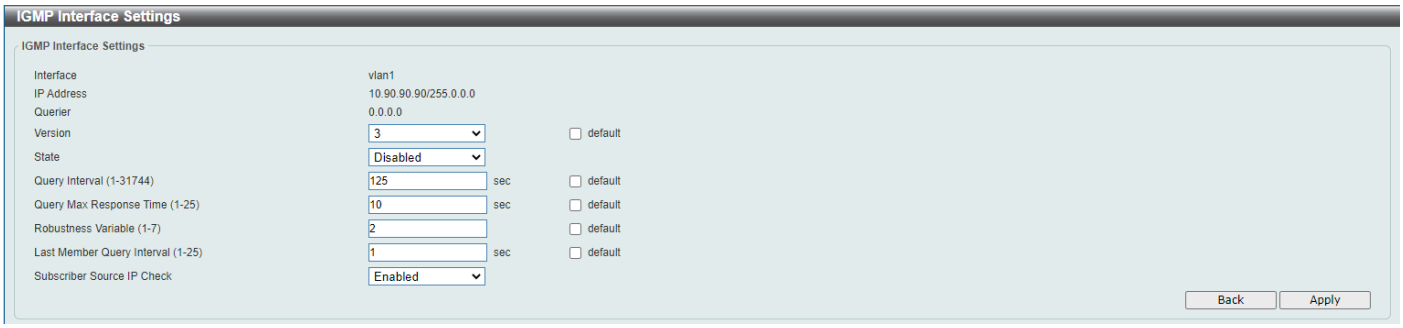


Figure 6-70 IGMP Interface Settings (Edit) Window

The fields that can be configured are described below:

Parameter	Description
Version	Select the IGMP version. Options to choose from are **1**, **2**, and **3**. The default version is 3. You can select **default** to use default value.
State	Select this option to enable or disable the IGMP protocol state. The default state is disabled. You can select **default** to use default value.

Parameter	Description
Query Interval	Enter the interval at which the router sends IGMP general query messages periodically. The range is from 1 to 31744. The default value is 125. You can select **default** to use default value.
Query Max Response Time	Enter the query maximum response time, in seconds, advertised in IGMP queries. The range is from 1 to 25. The default value is 10. You can select **default** to use default value.
Robustness Variable	Enter the robustness variable used in IGMP. The range is from 1 to 7. The default value is 2. You can select **default** to use default value.
Last Member Query Interval	Enter the interval at which the router sends IGMP group-specific or group-source-specific (channel) query messages. The range is from 1 to 25. The default value is 1. You can select **default** to use default value.
Subscriber Source IP Check	Select to enable or disable the Subscriber Source IP Check feature here. The default state is enabled. You can select **default** to use default value.

Click the **Apply** button to accept the changes made.

Click the **Back** button to return to the previous window.

IGMP Static Group Settings

This window is used to display and configure the IGMP static group settings.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > IGMP > IGMP Static Group Settings**, as shown below:

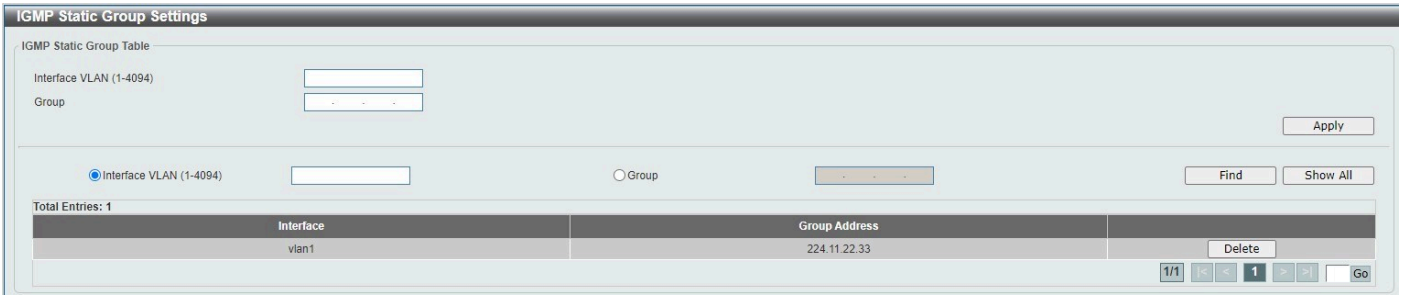


Figure 6-71 IGMP Static Group Settings Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the interface VLAN ID used here. This value must be between **1** and **4094**.
Group	Specifies the IP multicast group address. Valid address range is from 224.0.0.0 to 239.255.255.255.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to locate and display all the 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.

IGMP Dynamic Group Table

This window is used to find and display the IGMP dynamic group table.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > IGMP > IGMP Dynamic Group Table**, as shown below:

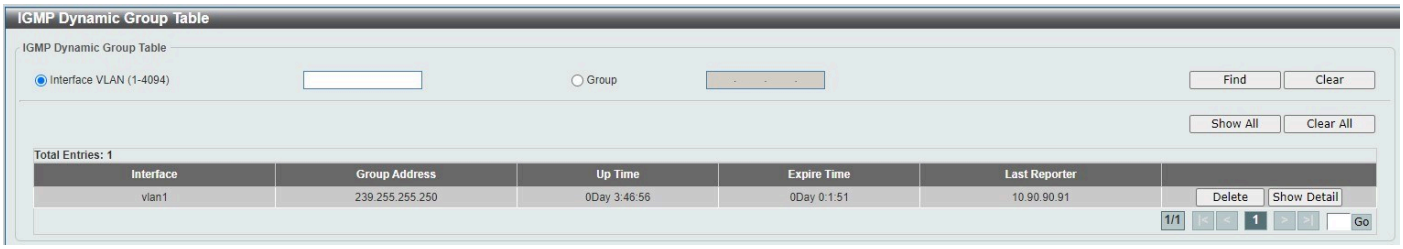


Figure 6-72 IGMP Dynamic Group Table Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the interface VLAN ID used here. This value must be between **1** and **4094**.
Group	Specifies the IP multicast group address.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to locate and display all the entries.

Click the **Clear** button to clear all the information for the specific interface.

Click the **Clear All** button to clear all the information in this table.

Click the **Delete** button to delete the specified entry.

Click the **Show Detail** button to view more detailed information for the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Show Detail** button, the following page will appear.



Figure 6-73 IGMP Dynamic Group Table (Show Detail) Window

Click the **Back** button to return to the previous window.

IGMP SSM Mapping Settings

This window is used to display and configure the IGMP Source Specific Multicast (SSM) mapping settings.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > IGMP > IGMP SSM Mapping Settings**, as shown below:

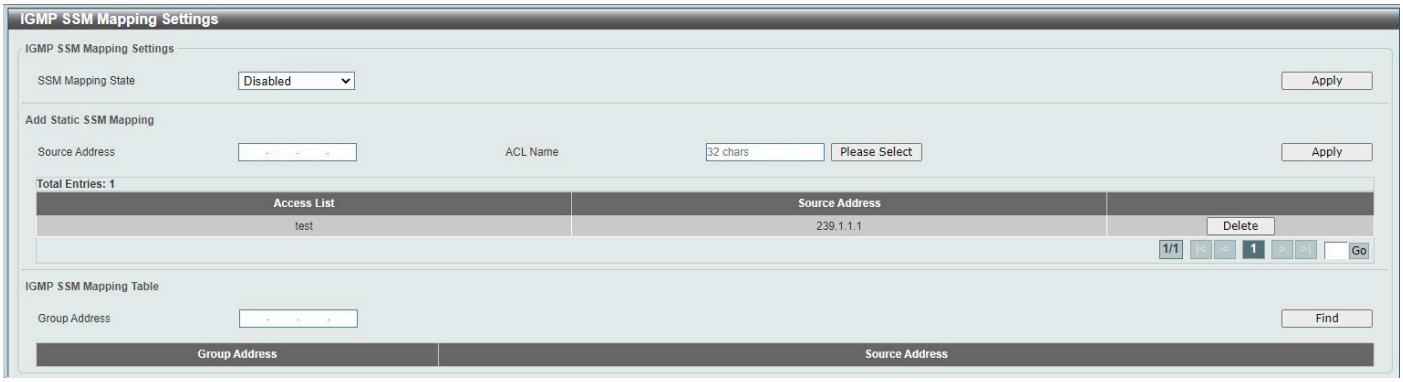


Figure 6-74 IGMP SSM Mapping Settings Window

The fields that can be configured are described below:

Parameter	Description
SSM Mapping State	Select to enable or disable the Subscriber Source IP Check feature here.
Source Address	Specify the source address to be associated with the group defined in the access list.
ACL Name	Specify a standard IP access list that contains the multicast groups to be mapped. You can also click **Please Select** to select a pre-defined Access Control List. Refer to **ACL>ACL Access List.**
Group Address	Specify the multicast group to be displayed.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete the specified entry.

Click the **Find** button to locate a specific entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Please Select** button, the following page will appear.



Figure 6-75 IGMP SSM Mapping Settings (Please Select) Window

Click the **OK** button to close the window and return to the previous window.

PIM

PIM Interface

This window is used to display and configure the PIM (Protocol Independent Multicast) interface settings.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Interface**, as shown below:

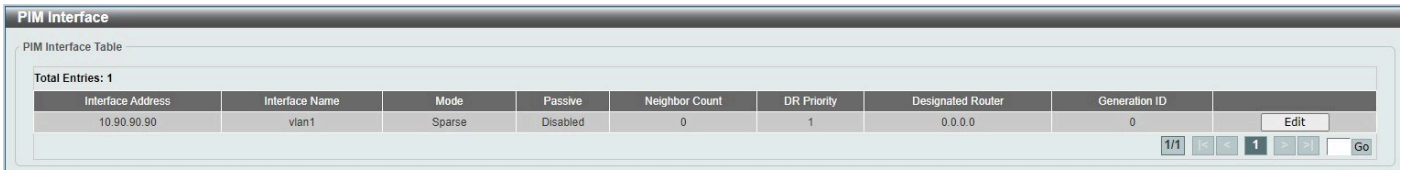


Figure 6-76 PIM Interface Window

Click the **Edit** button to modify the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Edit** button, the following page will appear.

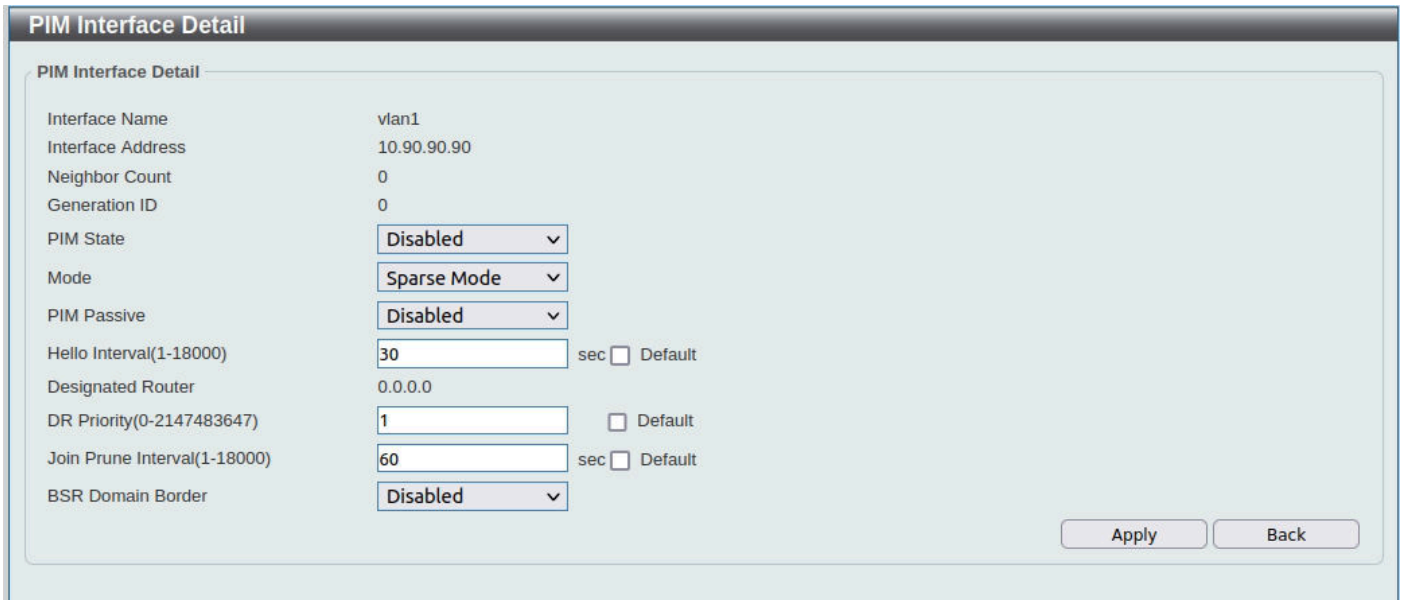


Figure 6-77 PIM Interface (Edit) Window

The fields that can be configured are described below:

Parameter	Description
PIM State	Select this option to enable or disable the PIM protocol state. The default state is disabled.
Mode	Select the mode of PIM. The only supported mode is Sparse Mode.
PIM Passive	Select to enable or disable the PIM Passive. If an interface is passive, no PIM control pacekts are sent or processed on this interface. The only supported state is disabled.
Hello Interval	Enter the interval at which the router sends PIM hello messages periodically. The range is from 1 to 18000. The default value is 30.
DR Priority	Enter the DR priority. The range is from 0 to 2147483647. The default value is 1.

Parameter	Description
Join Prune Interval	Enter the join prune interval. The range is from 1 to 18000. The default value is 60.
BSR Domain Border	Select to enable or disable the BSR Domain Border feature here. The default state is disabled.

Click the **Apply** button to accept the changes made.

Click the **Back** button to return to the previous window.

PIM BSR Candidate

This window is used to display and configure the PIM Bootstrap Router (BSR) candidate settings. A bootstrap router (BSR) is designed for communicating RP information for the RP selection process in a Protocol Independent Multicast (PIM) domain.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM BSR Candidate**, as shown below:

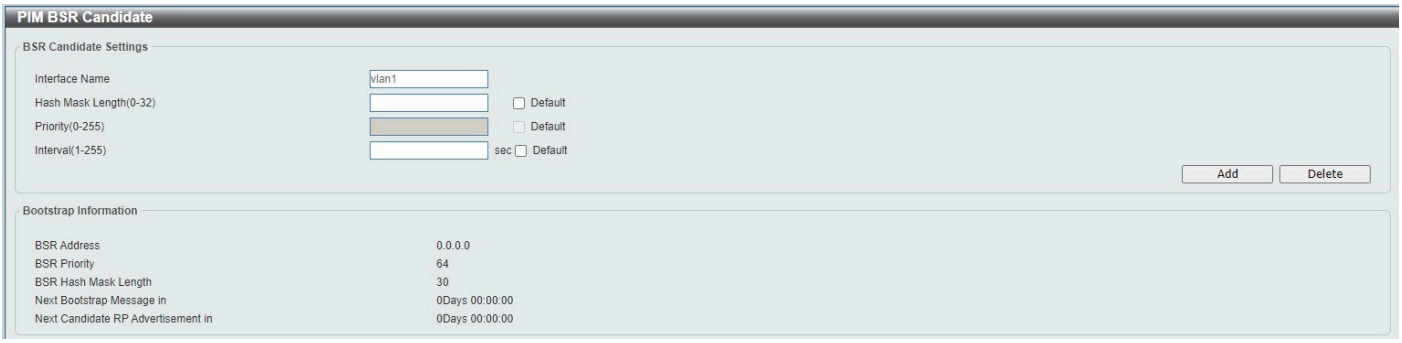


Figure 6-78 PIM BSR Candidate Window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Specify the interface name.
Hash Mask Length	Enter the hash mask length for RP selection. The range is from 0 to 32. The default value is 30. Select **Default** to use the default value.
Priority	Enter the priority for a BSR candidate. The range is from 0 to 255. The default value is 64. Select **Default** to use the default value.
Interval	Enter the interval between originating Bootstrap message. The range is from 1 to 255. The default value is 60. Select **Default** to use the default value.

Click the **Add** button to add the PIM BSR candidate.

Click the **Delete** button to remove the specified entry.

PIM RP Address

This window is used to display and configure the PIM rendezvous point (RP) address settings. An RP is designated as the meeting point for all multicast data in PIM Sparse Mode (SM).

To view the following window, click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM RP Address**, as shown below:

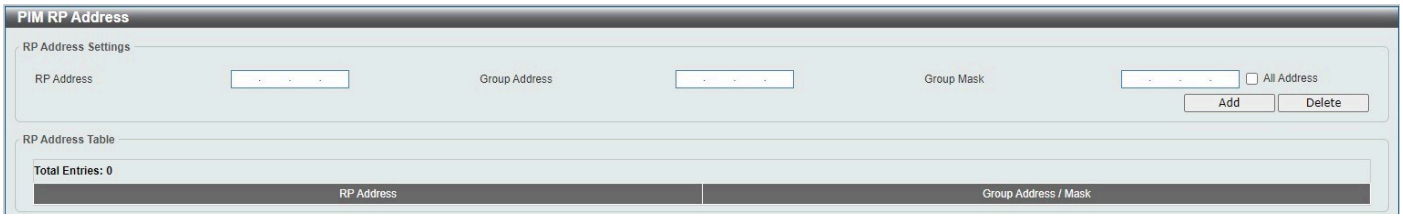


Figure 6-79 PIM RP Address Window

The fields that can be configured are described below:

Parameter	Description
RP Address	Specifies the IP address of the RP.
Group Address	Specifies the IP multicast group address. Alternatively, select **All Address**. Valid address range is from 224.0.0.0 to 239.255.255.255.
Group Mask	Specifies the IP multicast group mask. Alternatively, select **All Address**.

Click the **Add** button to add the PIM RP address.

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

PIM RP Candidate

This window is used to display and configure the PIM rendezvous point (RP) candidate settings.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM RP Candidate**, as shown below:

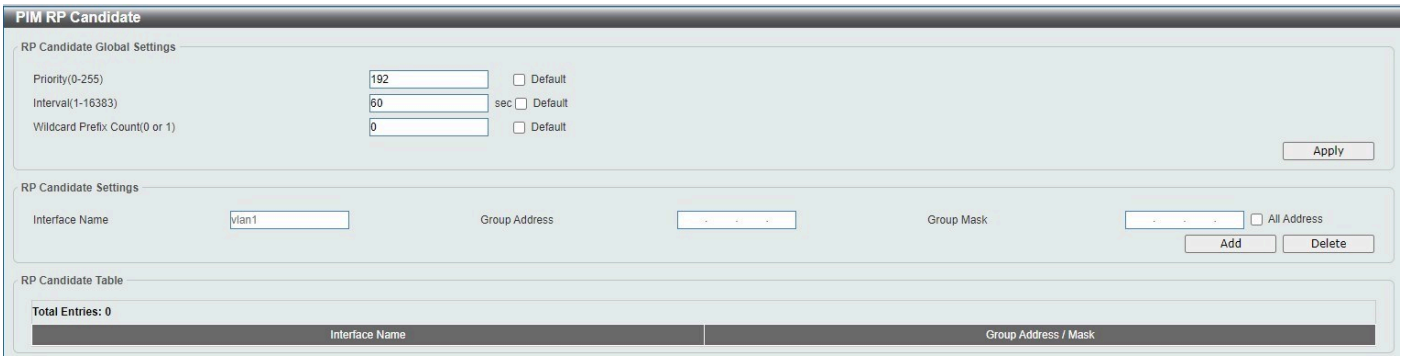


Figure 6-80 PIM RP Candidate Window

The fields that can be configured are described below:

Parameter	Description
Priority	Specifies the RP priority value. The range is from 0 to 255. The default value is 192.
Interval	Specifies the RP candidate advertisement interval. The range is from 1 to 16383 seconds. If not specified, the default value is 60 seconds.
Wildcard Prefix Count	Specifies to set the wildcard (224.0.0.0/4) prefix count 1 or 0 in C-RP message. The default value is 0.
Interface Name	Specifies the Interface name. Refer to **L3 Features > Interface**.

Parameter	Description
Group Address	Specifies the IP multicast group address. Valid address range is from 224.0.0.0 to 239.255.255.255. Alternatively, select **All Address**.
Group Mask	Specifies the IP multicast group mask. Alternatively, select **All Address**.

Click the **Apply** button to accept the changes made.

Click the **Add** button to add the PIM RP candidate.

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

PIM RP Table

This window is used to find and display the PIM RP table.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM RP Table**, as shown below:



Figure 6-81 PIM RP Table Window

The fields that can be configured are described below:

Parameter	Description
RP Hash	Enter the RP hash here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to locate and display all the entries.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

PIM Neighbor Table

This window is used to find and display the PIM neighbor table.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > PIM > PIM for IPv4 > PIM Neighbor Table**, as shown below:

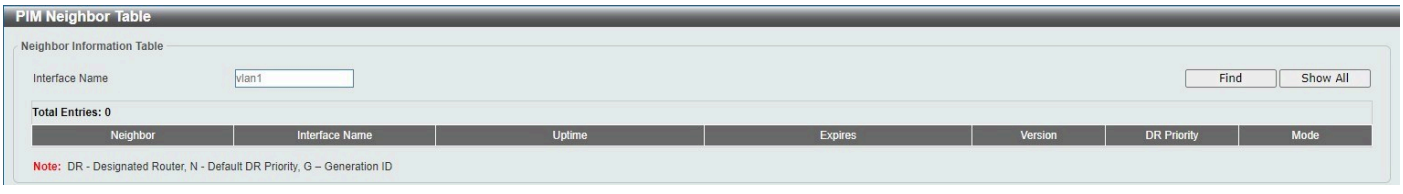


Figure 6-82 PIM Neighbor Table Window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the Interface Name here. Refer to **L3 Features > Interface**.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to locate and display all the entries.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IPMC

IP Multicast Global Settings

The fields that can be configured in **IP Multicast Routing Global State** are described below:

Parameter	Description
Global State	Enable or disable the global state of IP Multicast Routing.

Click the **Apply** button to accept the changes made.

Control Packet CPU Filtering

This window is used to display and configure the IPMC control packet CPU filtering settings.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > IPMC > Control Packet CPU Filtering**, as shown below:

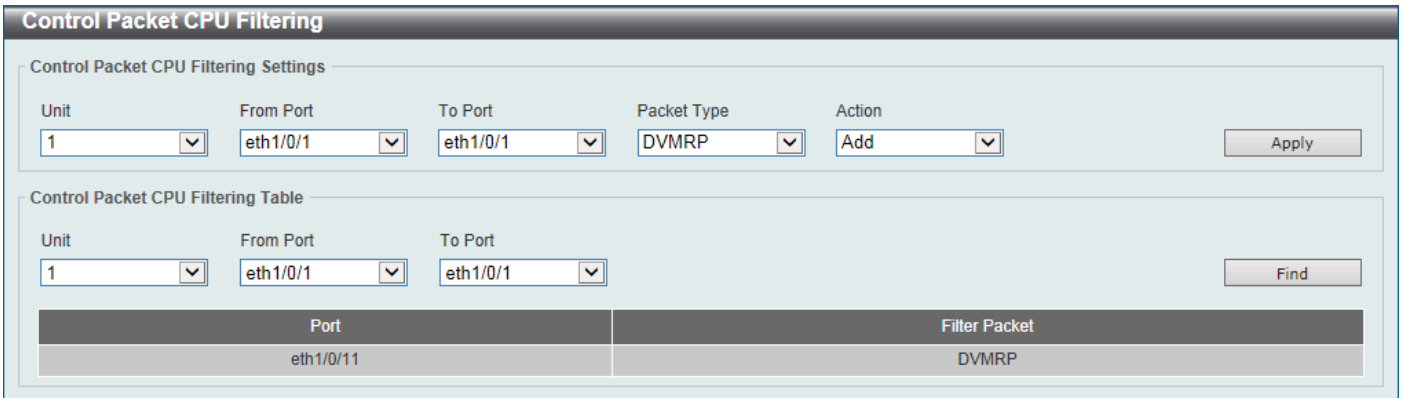


Figure 6-83 Control Packet CPU Filtering Window

The fields that can be configured in **Control Packet CPU Filtering Settings** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Packet Type	Select the packet type here. Options to choose from are: • **DVMRP** - Specifies that the CPU will discard DVMRP Layer 3 control packets sent to it. • **PIM** - Specifies that the CPU will discard PIM Layer 3 control packets sent to it. • **IGMP Query** - Specifies that the CPU will discard IGMP Query Layer 3 control packets sent to it. • **OSPF -** Specifies that the CPU will discard OSPF Layer 3 control packets sent to it.

Parameter	Description
	• **RIP -** Specifies that the CPU will discard RIP Layer 3 control packets sent to it. • **VRRP** - Specifies that the CPU will discard VRRP Layer 3 control packets sent to it.
Action	Select the action that will be taken here. Options to choose from are: • **Add** - Specifies to add a new entry based on the information entered. • **Delete** - Specifies to delete an entry based on the information entered.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Control Packet CPU Filtering Settings** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this display here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this display here.

Click the **Find** button to find and display entries based on the selections made.

IP Route Filter

Route Map

This window is used to display and configure the route map settings.

To view the following window, click **L3 Features > IP Route Filter > Route Map**, as shown below:

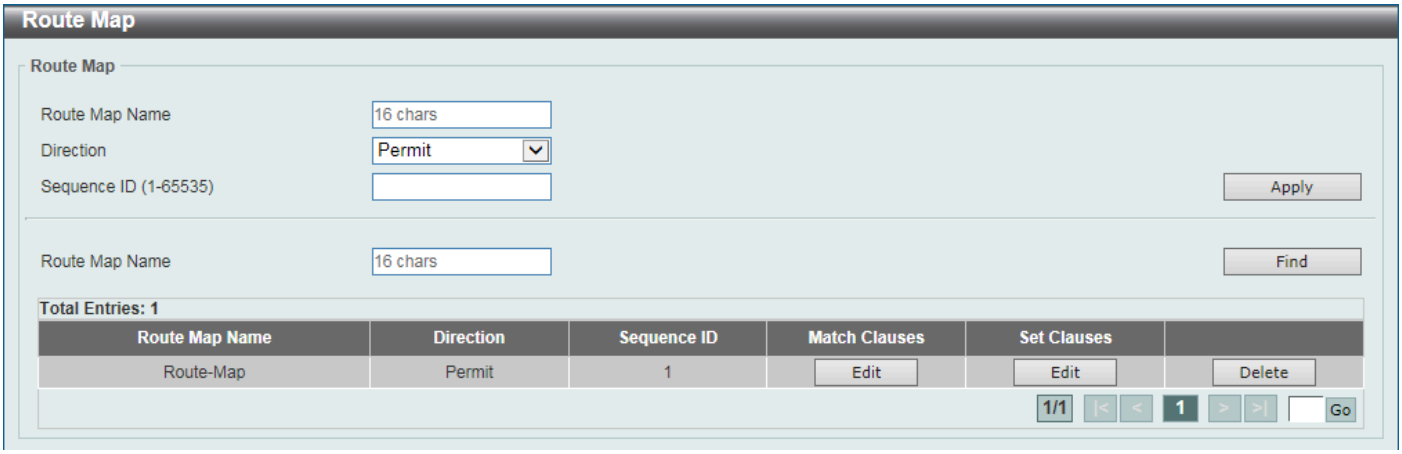


Figure 6-84 Route Map Window

The fields that can be configured are described below:

Parameter	Description
Route Map Name	Enter the route map name here. This name can be up to 16 characters long.
Direction	Select the direction for this rule here. Options to choose from are **Permit** and **Deny**.

Parameter	Description
	• **Permit** - Specifies that routes that match the rule entry are permitted. • **Deny** - Specifies that routes that match the rule entry are denied.
Sequence ID	Enter the sequence ID for this rule here. The range is from 1 to 65535.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Edit** button to modify 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.

After clicking the **Edit** button in the **Match Clauses** column, the following page will appear.

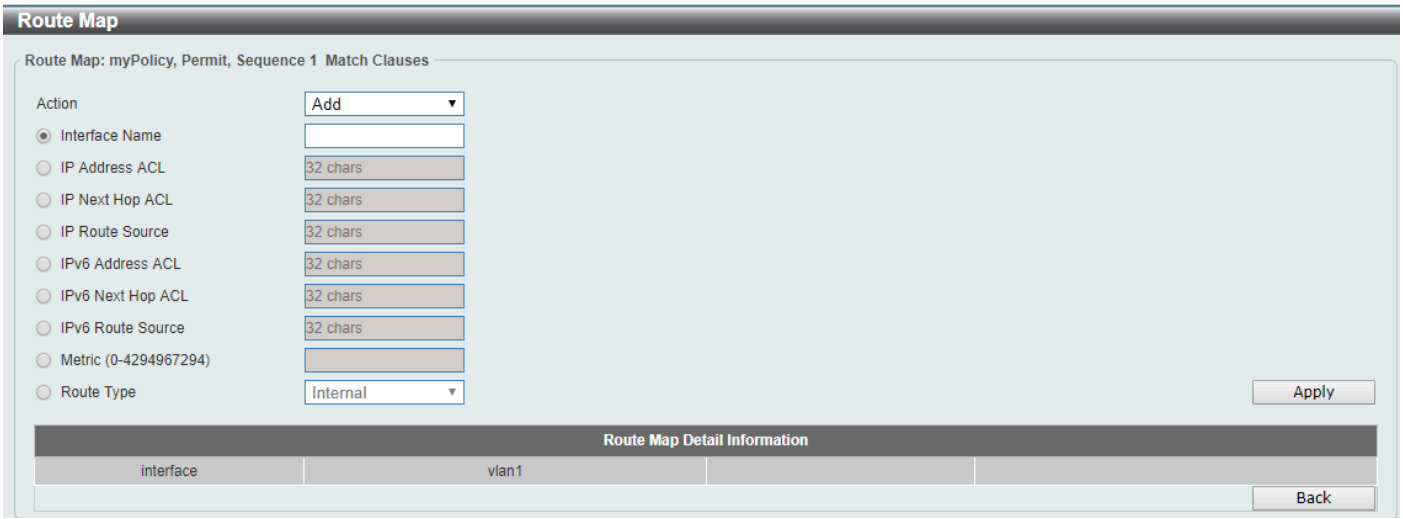


Figure 6-85 Route Map (Match Clauses, Edit) Window

The fields that can be configured are described below:

Parameter	Description
Action	Select **Add** to add a new entry based in the information entered. Select **Delete** to delete an entry based in the information entered.
Interface Name	Select and enter the interface name that will be used here. This option is used to define a clause to match the route's outgoing interface.
IP Address ACL	Select and enter the standard or extended IP access list name here. This option is used to define a clause to match the route based on the standard or extended IP access list. This string can be up to 32 characters long.
IP Next Hop ACL	Select and enter the standard IP access list name here. This option is used to define a clause to match the route's next hop based on the standard IP access list. This string can be up to 32 characters long.
IP Route Source	Select and enter the standard or extended IP access list name here. This option is used to define a clause to match the route's source based on the standard or extended IP access list. This string can be up to 32 characters long.
IPv6 Address ACL	Select and enter the standard or extended IPv6 access list name here. This option is used to define a clause to match the route based on the standard or extended IPv6 access list. This string can be up to 32 characters long.

Parameter	Description
IPv6 Next Hop ACL	Select and enter the standard IPv6 access list name here. This option is used to define a clause to match the route's next hop based on the standard IPv6 access list. This string can be up to 32 characters long.
IPv6 Route Source	Select and enter the standard or extended IPv6 access list name here. This option is used to define a clause to match the route's source based on the standard or extended IPv6 access list. This string can be up to 32 characters long.
Metric	Select and enter the metric value of the route here. The range is from 0 to 4294967294. This option is used to define a clause to match the route metric.
Route Type	Select the route type here. Options to choose from are **Internal**, **External Type-1**, **External Type-2 and Nssa-external**. • **Internal** - Specifies the intra-area and inter-area routes of Open Shortest Path First (OSPF). • **External Type-1** - Specifies the type-1 external route of OSPF. • **External Type-2** - Specifies the type-2 external route of OSPF. • **Nssa-external** - Specifies the nssa-external type-1 and type-2 route of OSPF.

Click the **Apply** button to accept the changes made.

Click the **Back** button to return to the previous window.

After clicking the **Edit** button in the **Set Clauses** column, the following page will appear.

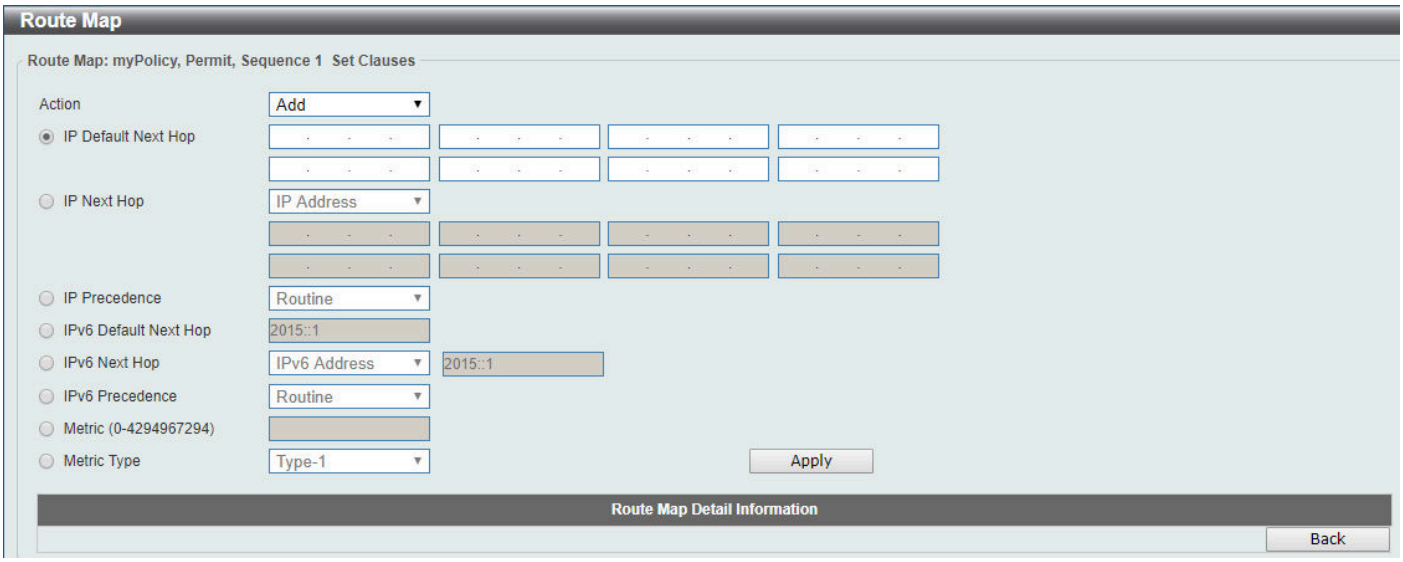


Figure 6-86 Route Map (Set Clauses, Edit) Window

The fields that can be configured are described below:

Parameter	Description
Action	Select **Add** to add a new entry based in the information entered. Select **Delete** to delete an entry based in the information entered.
IP Default Next Hop	Enter the default next-hop IP addresses in the spaces provided that will be used to route the packet. This feature can be used to specify multiple default next hop routers. If default next hops are already configured, the default next hops configured later will be added to the default next hop list. When the first default next hop router specified is down, the next default next hop router

Parameter	Description
	specified is tried in turn to route the packet. Up to 8 default next-hop IP addresses can be entered.
IP Next Hop	Select the IP next hop type here. This feature is used to configure the next-hop router to route the packet that passes the match clauses of the configured route map sequence. Options to choose from are **IP Address** and **Recursive**. • **IP Address** - Specifies the IP addresses of the next-hops to route the packet. Enter the next-hop IP addresses in the spaces provided here. Up to 8 next-hop IP addresses can be entered. • **Recursive** - Specifies the IP address of the recursive as the next-hop router. Enter the recursive next-hop IP address in the space provided here.
IP Precedence	Select the IP precedence option here. Options to choose from are **Routine**, **Priority**, **Immediate**, **Flash**, **Flash Override**, **Critical**, **Internet**, and **Network**. Use this feature to set the precedence value in the IP header. This option only takes effect when policy routing involves the IPv4 packet.
IPv6 Default Next Hop	Enter the default next-hop IPv6 address in the space provided that will be used to route the packet.
IPv6 Next Hop	Select the IPv6 next hop type here. This feature is used to configure the next-hop router to route the packet that passes the match clauses of the configured route map sequence. Options to choose from are: • **IP Address** - Specifies the IPv6 addresses of the next-hops to route the packet. Enter the next-hop IPv6 addresses in the space provided here. • **Recursive** - Specifies the IPv6 address of the recursive as the next-hop router. Enter the recursive next-hop IPv6 address in the space provided here.
IPv6 Precedence	Select the IPv6 precedence option here. Options to choose from are **Routine**, **Priority**, **Immediate**, **Flash**, **Flash Override**, **Critical**, **Internet**, and **Network**. Use this feature to set the precedence value in the IPv6 header. This option only takes effect when policy routing involves the IPv6 packet.
Metric	Select and enter the metric value here that will be used in the modification. The range is from 0 to 4294967294.
Metric Type	Select the metric type here that will be used in the modification. Options to choose from are **Type-1** and **Type-2**. • **Type-1** - Specifies to use the OSPF external type-1 metric. • **Type-2** - Specifies to use the OSPF external type-2 metric.

Click the **Apply** button to accept the changes made.

Click the **Back** button to return to the previous window.

Policy Route

This window is used to display and configure the policy route settings.

To view the following window, click **L3 Features > Policy Route**, as shown below:

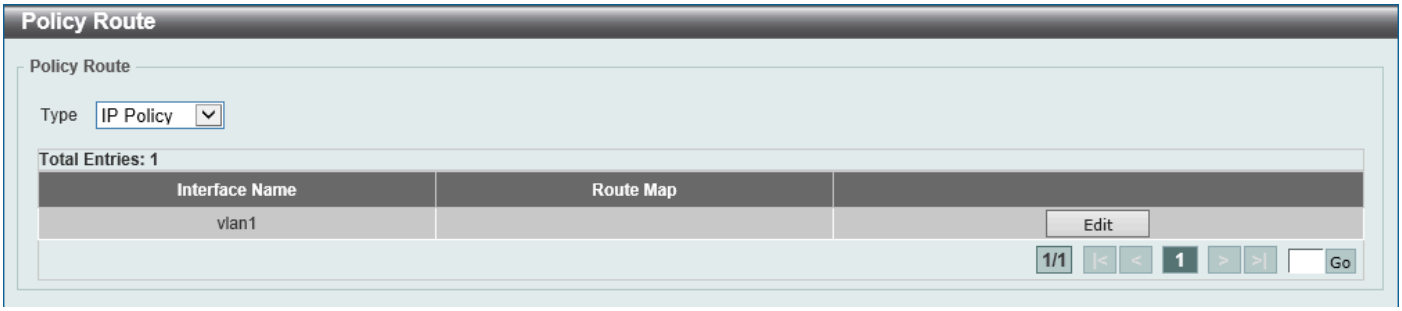


Figure 6-87 Policy Route Window

The fields that can be configured are described below:

Parameter	Description
Type	Select the policy route type here. Options to choose from are **IP Policy** and **IPv6 Policy**.

Click the **Edit** button to modify the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Edit** button, the following page will appear.

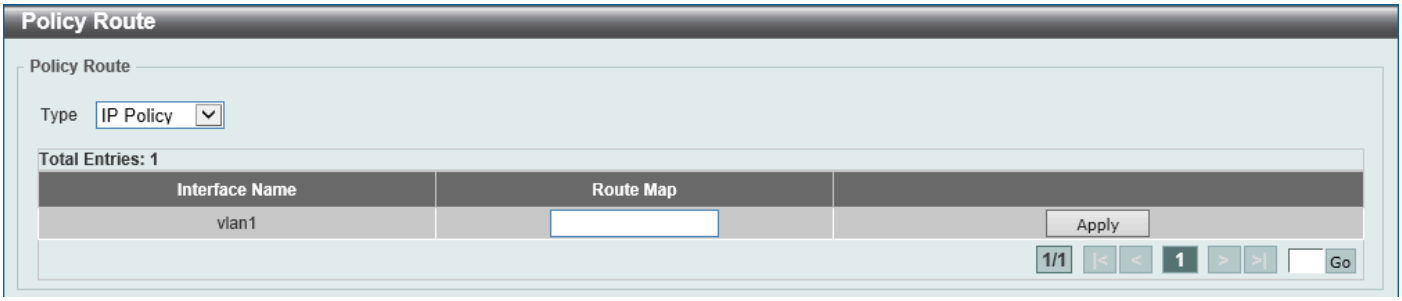


Figure 6-88 Policy Route (Edit) Window

The fields that can be configured are described below:

Parameter	Description
Route Map	Enter the route map name here that will be used in this policy route entry. Refer to **IP Route Filter > Route Map**.

Click the **Apply** button to accept the changes made.

VRRP Settings

This window is used to display and configure the Virtual Router Redundancy Protocol (VRRP) settings. All routers in the same VRRP group must be configured with the same virtual router ID and IP address.

A virtual router group is represented by a virtual router ID. The IP address of the virtual router is the default router configured on hosts. The virtual router's IP address can be a real address configured on the routers, or an unused IP address. If the virtual router address is a real IP address, the router that has this IP address is the IP address owner.

A master will be elected in a group of routers that supports the same virtual routers. Others are the backup routers. The master is responsible for forwarding the packets that are sent to the virtual router.

To view the following window, click **L3 Features > VRRP Settings**, as shown below:

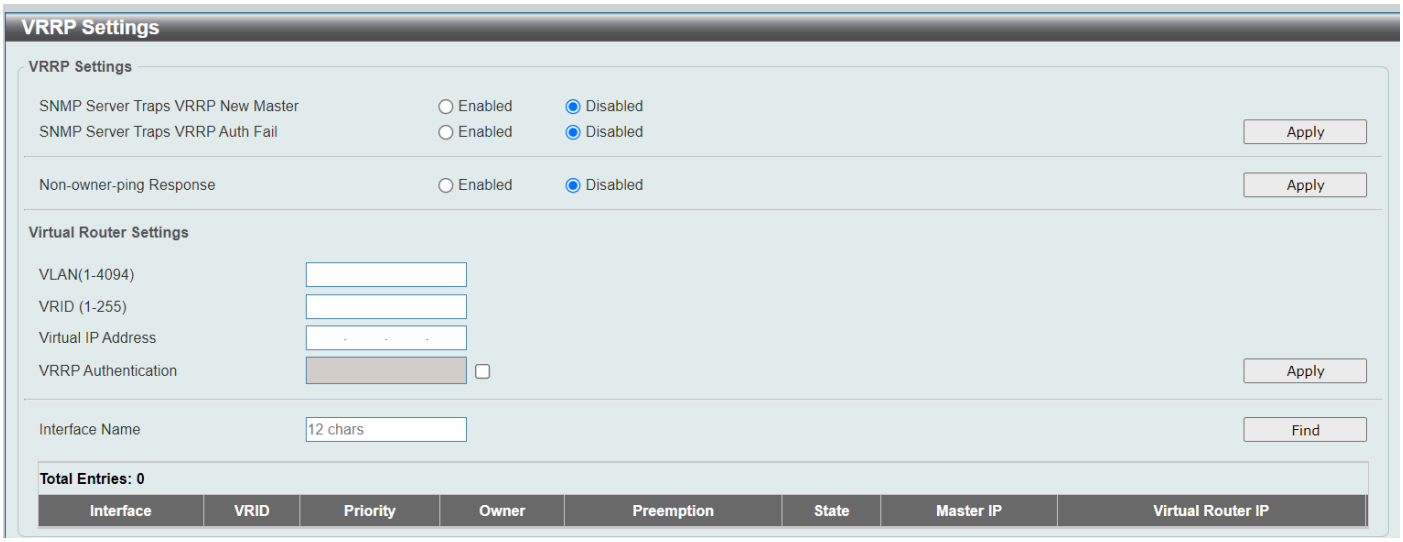


Figure 6-89 VRRP Settings Window

The fields that can be configured in **VRRP Settings** are described below:

Parameter	Description
SNMP Server Traps VRRP New Master	Select to enable or disable the SNMP server traps feature for the new VRRP master. If enabled, once the device has transitioned to the master state, a trap will be sent out.
SNMP Server Traps VRRP Auth Fail	Select to enable or disable the SNMP server traps feature for authentication failures. If enabled, if a packet has been received from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type, then a trap will be sent out.
Non-owner-ping Response	Select to enable or disable the non-owner ping response feature here. This feature is used to enable the virtual router in the master state to respond to ICMP echo requests for an IP address not owned but associated with this virtual router.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Virtual Router Settings** are described below:

Parameter	Description
VLAN	Enter the VLAN interface ID used here. The range is from 1 to 4094.
VRID	Enter the virtual router ID used here. This ID is used to identify the virtual router in the VRRP group. The range is from 1 to 255.
Virtual IP Address	Enter the IPv4 address for the created virtual router group here.
VRRP Authentication	Select to enable and then enter the plain text authentication password for VRRP authentication on the interface here. This string can be up to 8 characters long. The authentication is applied to all virtual routers on this interface. The devices in the same VRRP group must have the same authentication password.
Interface Name	Enter the interface name used here. This name can be up to 12 characters long.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Edit** button to modify 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.

After clicking the **Edit** button, the following page will appear.

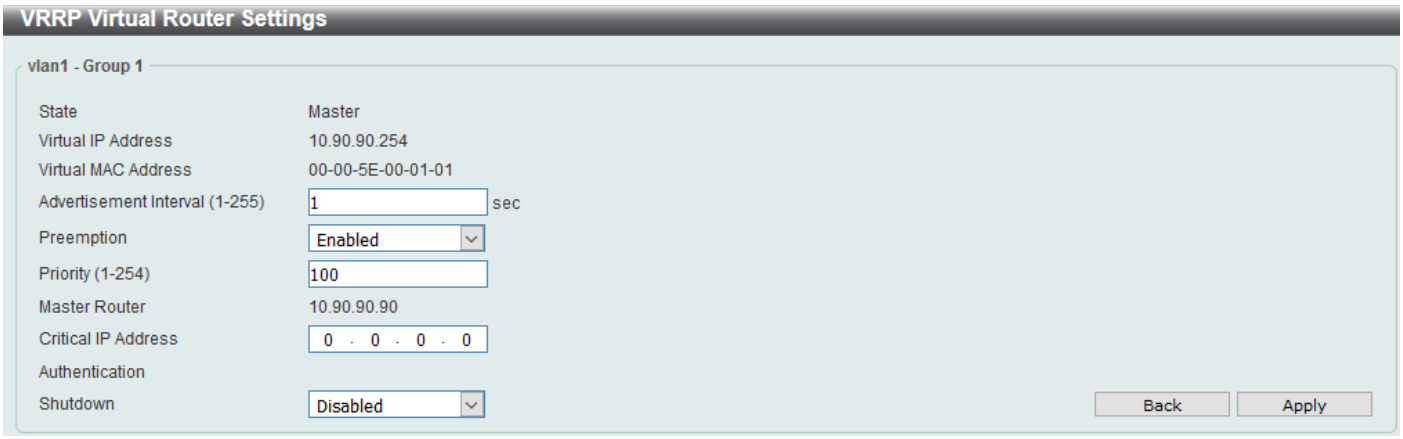


Figure 6-90 VRRP Settings (Edit) Window

The fields that can be configured are described below:

Parameter	Description
Advertisement Interval	Enter the advertisement interval value here. This is the time interval between successive VRRP advertisements by the master router. The range is from 1 to 255 seconds. By default, this value is 1 second.
Preemption	Select to enable or disable the preemption feature here. This feature is used to allow a router to take over the master role if it has a better priority than the current master.
Priority	Enter the priority value here. The range is from 1 to 254.
Critical IP Address	Enter the critical IPv4 address here. If the critical IP is configured on one virtual router, the virtual router cannot be activated when the critical IP address is unreachable. One VRRP group can only track one critical IP.
Shutdown	Select to enable or disable the shutdown feature here. This feature is used to disable a virtual router on an interface. Avoid the common mistake of shutting down the IP address owner router before shutting down other non-owner routers.

Click the **Back** button to return to the previous window.

Click the **Apply** button to accept the changes made.

VRRPv3 Settings

This window is used to display and configure the VRRP version 3 (VRRPv3) settings.

To view the following window, click **L3 Features > VRRPv3 Settings**, as shown below:

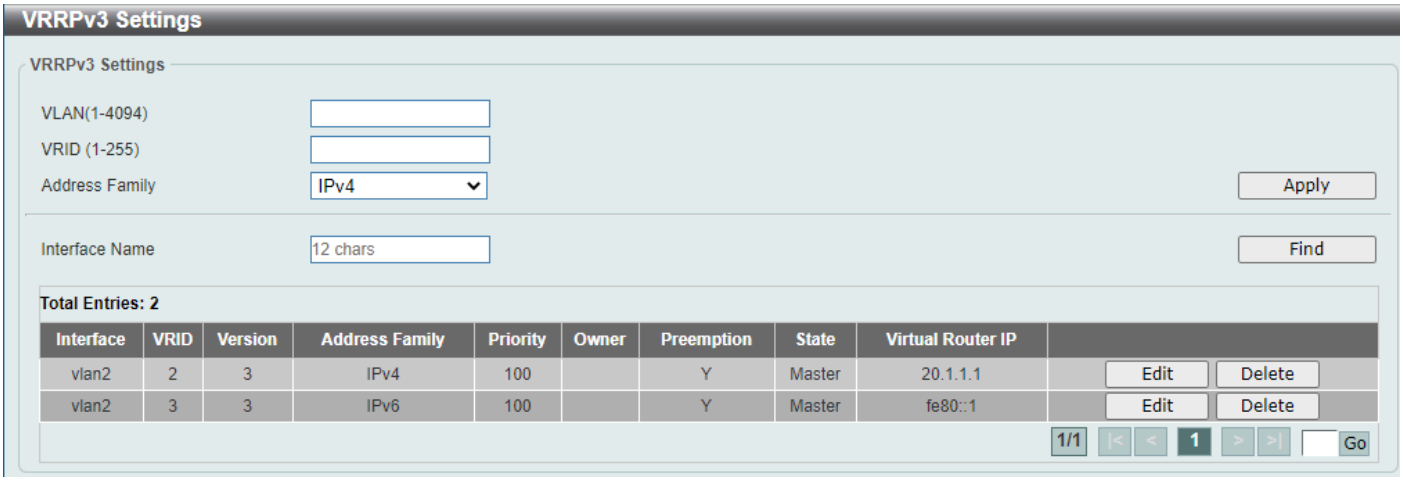


Figure 6-91 VRRPv3 Settings Window

The fields that can be configured are described below:

Parameter	Description
VLAN	Enter the ID of the VLAN interface that will be used here. The range is from 1 to 4094. Refer to **Layer 2 Features > VLAN** for vlans created on the Switch and **L3 Features > IPv6 Interface** for IPv6 interface settings. Note that an IPv6 address must be configured first on the interface.
VRID	Enter the ID of the virtual router that will be created here. The range is from 1 to 255.
Address Family	Select the address family used here. Options to choose from are: • **IPv4** - Specifies to create an IPv4 virtual router. • **IPv6** - Specifies to create an IPv6 virtual router.
Interface Name	Enter the name of the VLAN interface that will be used in the display here. This string can be up to 12 characters long.

Click the **Apply** button to accept the changes made.

Click the **Find** button to find and display an entry based on the information entered.

Click the **Edit** button to configure more detailed 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.

After clicking the **Edit** button next to the **IPv4 Address Family** entry, the following window will appear:

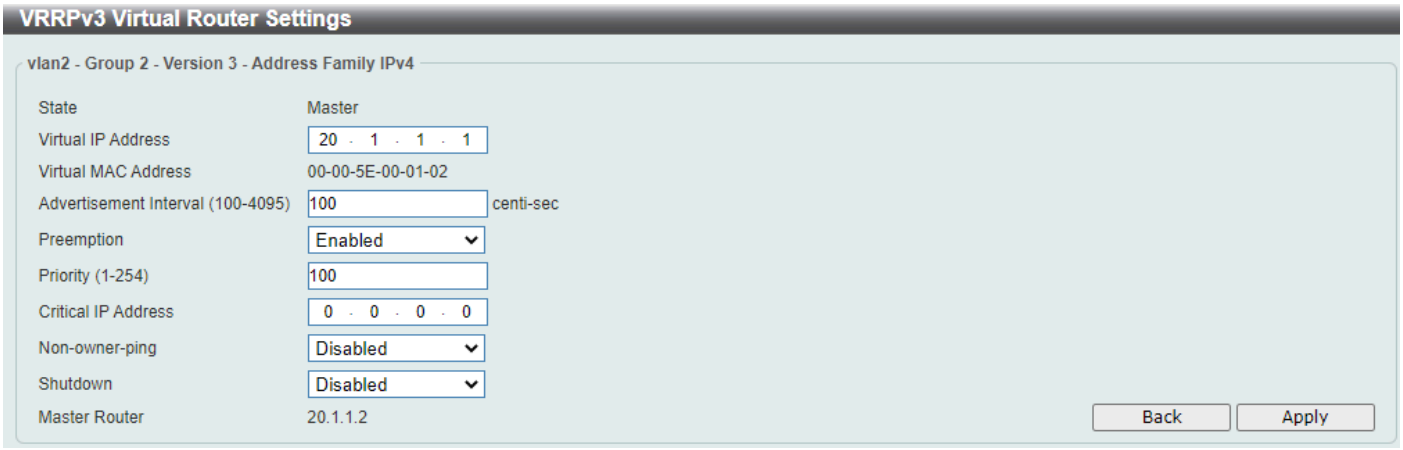


Figure 6-92 VRRPv3 Settings (Edit, IPv4) Window

The fields that can be configured are described below:

Parameter	Description
Virtual IP Address	Enter the virtual IPv4 address here. All routers in the same VRRP group must be configured with the same virtual router ID and virtual address. The IPv4 address of the virtual router can be a real address configured on the routers or an unused address. If the virtual address is equal to the real address of the interface, this virtual router is the IPv4 address owner.
Advertisement Interval	Enter the time interval value between successive advertisements by the master router here. The range is from 100 to 4095 centi-seconds. The master will constantly send VRRP advertisements. All virtual routers in a VRRP group must use the same timer values.
Preemption	Select to enable or disable the preemption feature here. This is used to allow a router to take over the master role if it has a better priority than the current master.
Priority	Enter the priority value of the virtual router here. The range is from 1 to 254. The master of a VRRP group is elected based on the priority. The virtual router with the highest priority becomes the master and others with lower priorities act as the backup for the VRRP group. If there are multiple routers with the same highest priority value, the router with the larger IPv4 address will become the Master. The router that is the IPv4 address owner of the VRRP group is always the master of the VRRP group and has the highest priority of 255.
Critical IP Address	Enter the critical IPv4 address here. If the critical IPv4 is configured on one virtual router, the virtual router cannot be activated when the critical IPv4 address is unreachable. One VRRP group can only track one critical IPv4 address.
Non-owner-ping	Select to enable or disable the non-owner ping feature here. This is used to enable a non-IPv4 address owner virtual router in the master state to respond to ICMP echo requests for IPv4 addresses.
Shutdown	Select to enable or disable the shutdown feature here. Avoid the common mistake of shutting down the IPv4 address owner routers before shutting down other non-owner routers.

Click the **Back** button to return to the previous window.

Click the **Apply** button to accept the changes made.

After clicking the **Edit** button next to the **IPv6 Address Family** entry, the following window will appear:

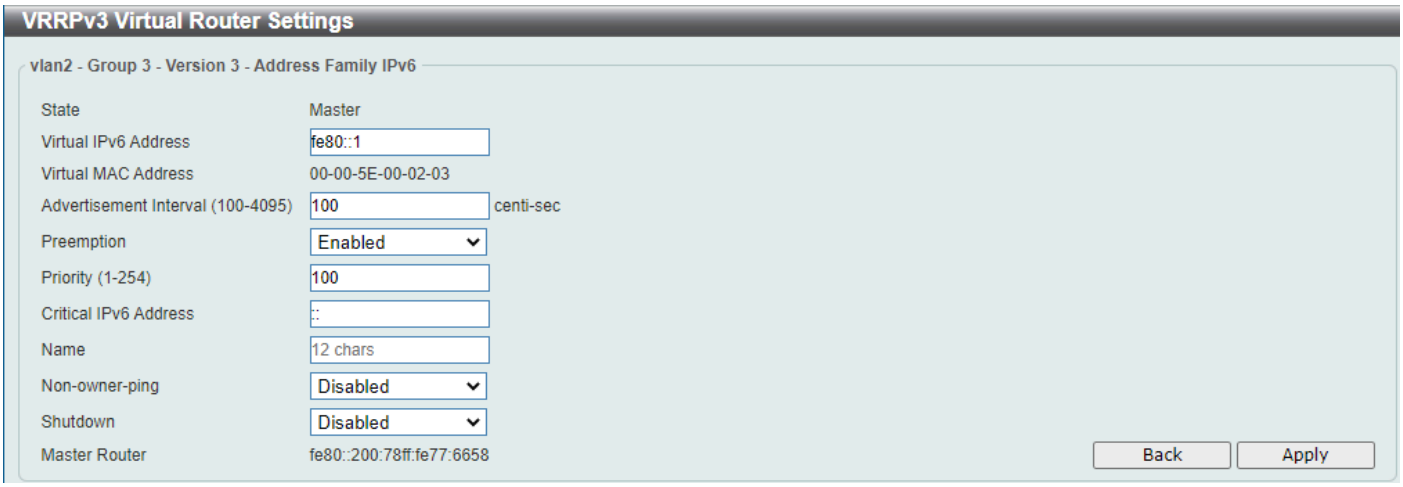


Figure 6-93 VRRPv3 Settings (Edit, IPv6) Window

Figure 6-93 VRRPv3 Settings (Edit, IPv6) WindowThe fields that can be configured are described below:

Parameter	Description
Virtual IPv6 Address	Enter the virtual IPv6 address here. All routers in the same VRRP group must be configured with the same virtual router ID and virtual address. The IPv6 address of the virtual router can be a real address configured on the routers or an unused address. If the virtual address is equal to the real address of the interface, this virtual router is the IPv6 address owner.
Advertisement Interval	Enter the time interval value between successive advertisements by the master router here. The range is from 100 to 4095 centi-seconds (0.01 seconds). The master will constantly send VRRP advertisements. All virtual routers in a VRRP group must use the same timer values.
Preemption	Select to enable or disable the preemption feature here. This is used to allow a router to take over the master role if it has a better priority than the current master.
Priority	Enter the priority value of the virtual router here. The range is from 1 to 254. The master of a VRRP group is elected based on the priority. The virtual router with the highest priority becomes the master and others with lower priorities act as the backup for the VRRP group. If there are multiple routers with the same highest priority value, the router with the larger IP address will become the Master. The router that is the IPv6 address owner of the VRRP group is always the master of the VRRP group and has the highest priority of 255.
Critical IPv6 Address	Enter the critical IPv6 address here. If the critical IPv6 is configured on one virtual router, the virtual router cannot be activated when the critical IPv6 address is unreachable. One VRRP group can only track one critical IPv6 address.
Name	Specifies the interface of critical IPv6 address which is link-local address to be used.
Non-owner-ping	Select to enable or disable the non-owner ping feature here. This is used to enable a non-IPv6 address owner virtual router in the master state to respond to ND requests for IPv6 addresses.
Shutdown	Select to enable or disable the shutdown feature here. Avoid the common mistake of shutting down the IPv6 address owner routers before shutting down other non-owner routers.

7. Quality of Service (QoS)

Basic Settings
Advanced Settings
WRED

Basic Settings

Port Default CoS

This window is used to display and configure the port default CoS settings.

To view the following window, click **QoS > Basic Settings > Port Default CoS**, as shown below:

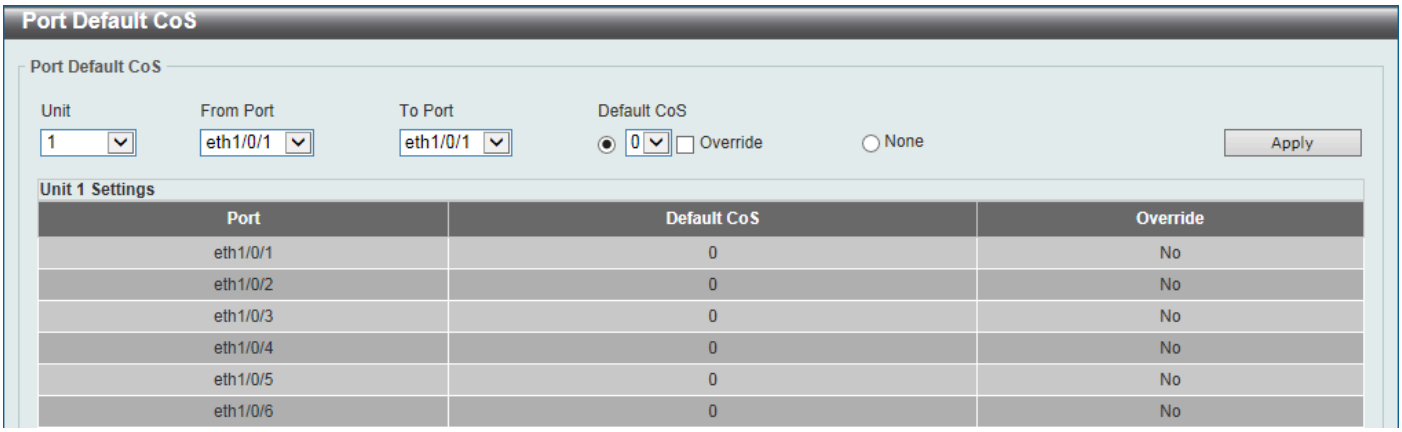


Figure 7-1 Port Default CoS Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Default CoS	Select the default CoS option for the port(s) specified here. Options to choose from are 0 to 7. Select the **Override** option to override the CoS of the packets. The default CoS will be applied to all incoming packets, tagged or untagged, received by the port. Select the **None** option to specify that the CoS of the packets will be the packet's CoS if the packets are tagged and will be the port default CoS if the packet is untagged.

Click the **Apply** button to accept the changes made.

Port Scheduler Method

This window is used to display and configure the port scheduler method settings. To view the following window, click **QoS > Basic Settings > Port Scheduler Method**, as shown below:

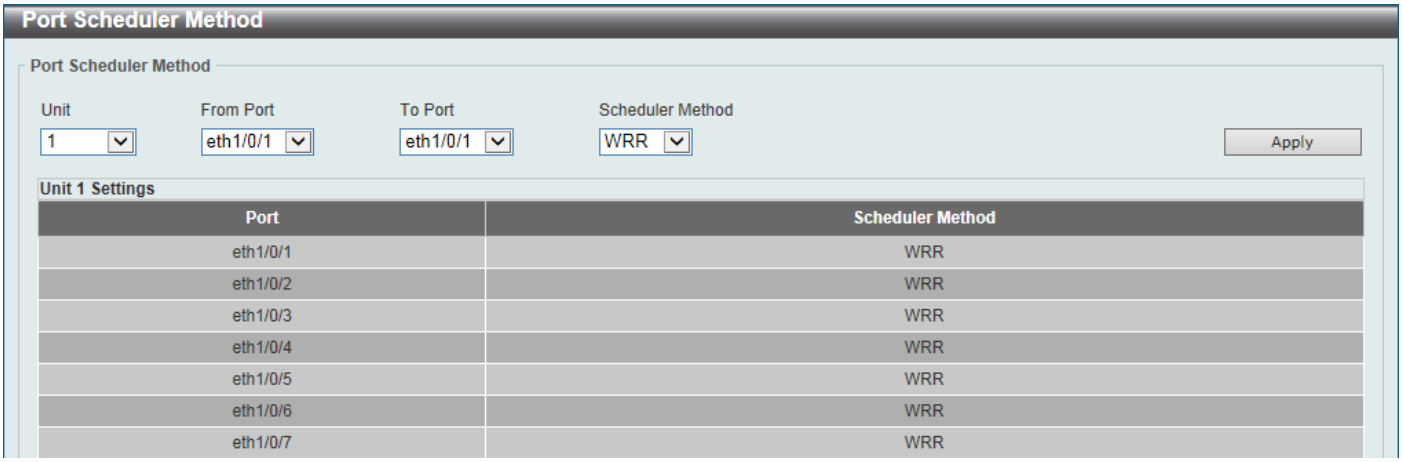


Figure 7-2 Port Scheduler Method Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Scheduler Method	Select the scheduler method that will be applied to the specified port(s). Options to choose from are Strict Priority (**SP**), Round-Robin (**RR**), Weighted Round-Robin (**WRR**), and Weighted Deficit Round-Robin (**WDRR**). By default, the output queue scheduling algorithm is **WRR**. • **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. • **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.

Parameter	Description
	To set a CoS queue in the **SP** mode, any higher priority CoS queue must also be in the strict priority mode.

Click the **Apply** button to accept the changes made.

Queue Settings

This window is used to display and configure the queue settings.

To view the following window, click **QoS > Basic Settings > Queue Settings**, as shown below:

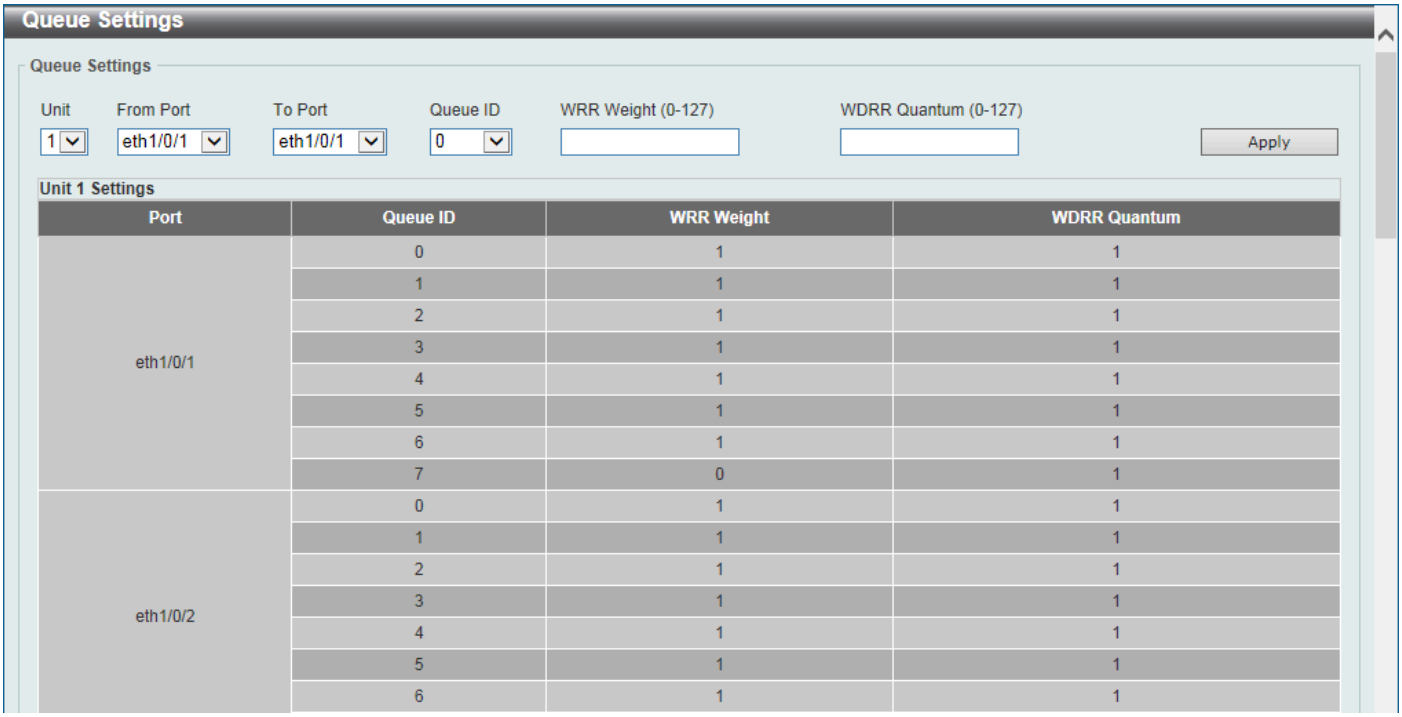


Figure 7-3 Queue Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Queue ID	Enter the queue ID value here. This value must be between 0 and 7.
WRR Weight	Enter the WRR weight value here. This value must be between 0 and 127. To satisfy the behavior requirements of Expedited Forwarding (EF), the highest queue is always selected by the Per-hop Behavior (PHB) EF and the schedule mode of this queue should be strict priority scheduling. So the weight of the last queue should be zero while the Differentiate Service is supported.
WDRR Quantum	Enter the WDRR quantum value here. This value must be between 0 and 127.

Click the **Apply** button to accept the changes made.

CoS to Queue Mapping

This window is used to display and configure the CoS-to-Queue mapping settings.

To view the following window, click **QoS > Basic Settings > CoS to Queue Mapping**, as shown below:

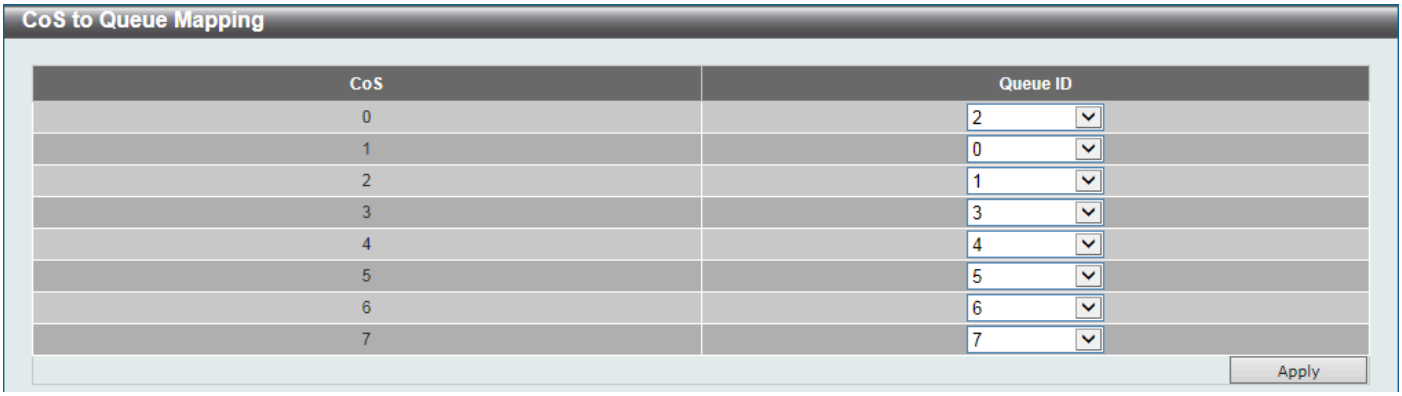


Figure 7-4 CoS to Queue Mapping Window

The fields that can be configured are described below:

Parameter	Description
Queue ID	Select the queue ID that will be mapped to the corresponding CoS value. Options to choose from are 0 to 7.

Click the **Apply** button to accept the changes made.

Port Rate Limiting

This window is used to display and configure the port rate limiting settings.

To view the following window, click **QoS > Basic Settings > Port Rate Limiting**, as shown below:

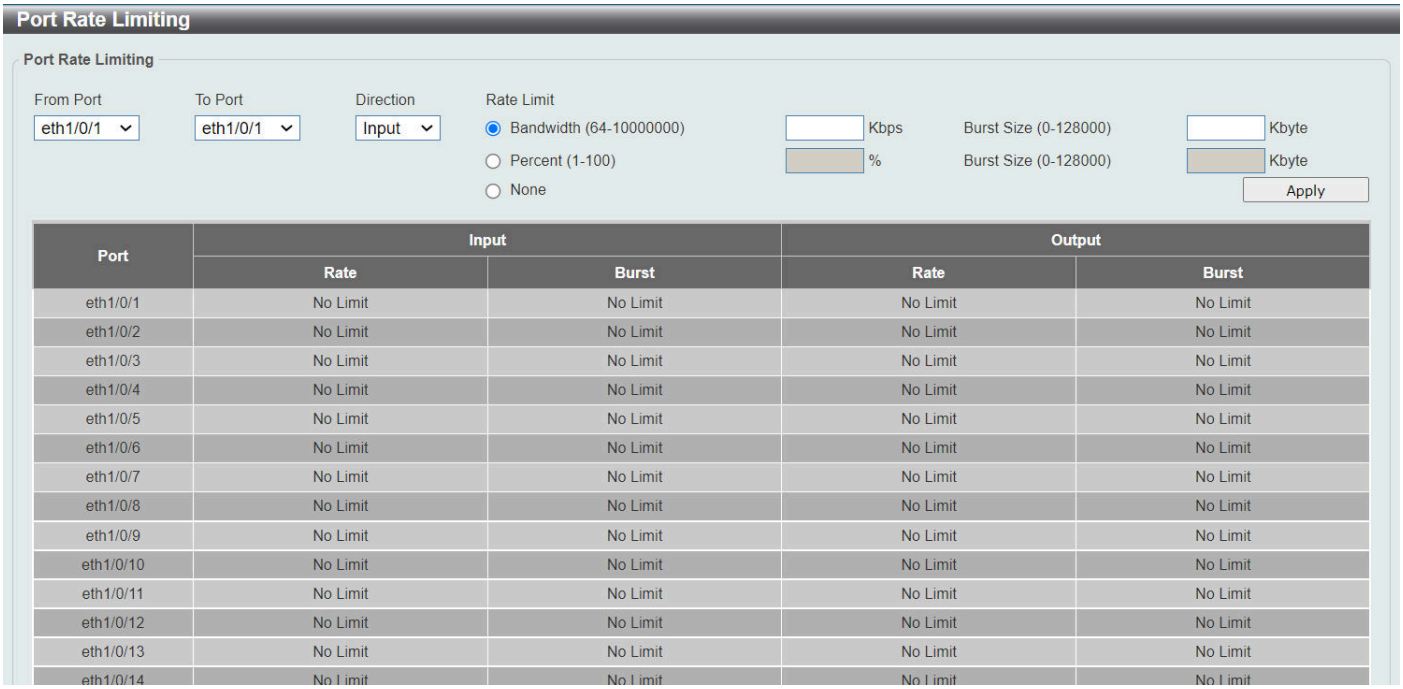


Figure 7-5 Port Rate Limiting Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Direction	Select the direction option here. Options to choose from are **Input** and **Output**. When **Input** is selected, the rate limit for ingress packets is configured. When **Output** is selected, the rate limit for egress packets is configured.
Rate Limit	Select and enter the rate limit value here. • When **Bandwidth** is selected, enter the input/output bandwidth value used in the space provided. This value must be between 64 and 10000000 kbps. Also, enter the **Burst Size** value in the space provided. This value must be between 0 and 128000 kilobytes. • When **Percent** is selected, enter the input/output bandwidth percentage value used in the space provided. This value must be between 1 and 100 percent (%). Also, enter the **Burst Size** value in the space provided. This value must be between 0 and 128000 kilobytes. • Select the **None** option to remove the rate limit on the specified port(s). The specified limitation cannot exceed the maximum speed of the specified interface. For the ingress bandwidth limitation, the ingress will send a pause frame or a flow control frame when the received traffic exceeds the limitation.

Click the **Apply** button to accept the changes made.

Queue Rate Limiting

This window is used to display and configure the queue rate limiting settings.

To view the following window, click **QoS > Basic Settings > Queue Rate Limiting**, as shown below:

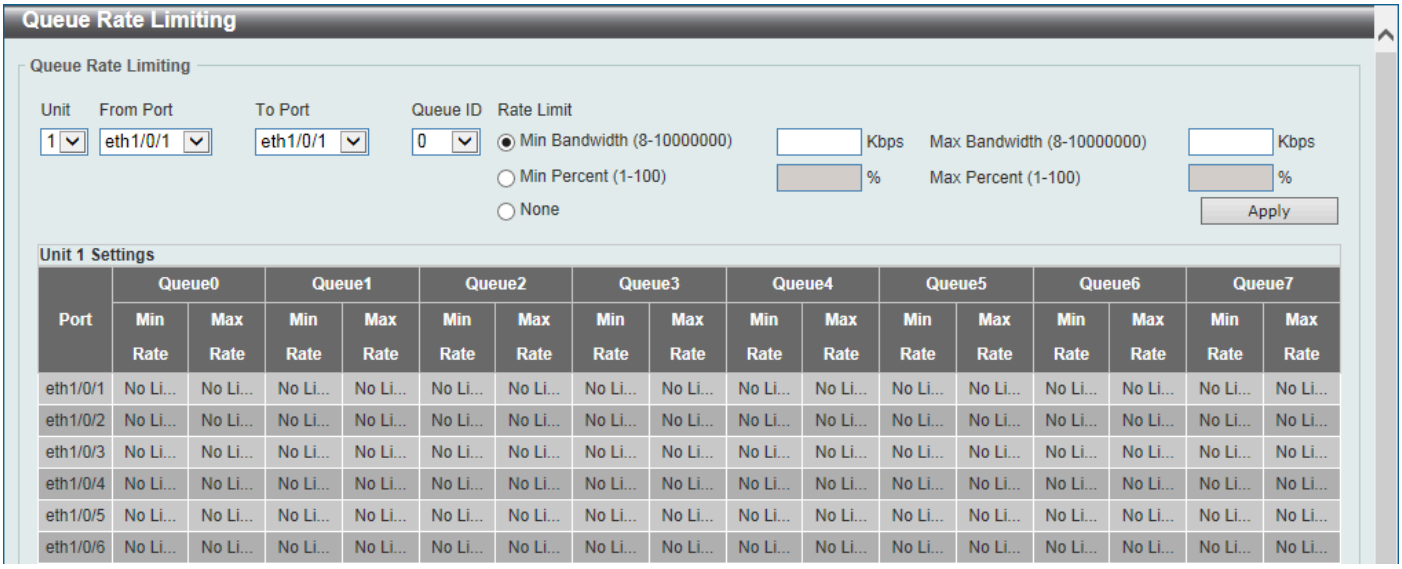


Figure 7-6 Queue Rate Limiting Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration 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 queue rate limit settings here. • When the **Min Bandwidth** option is selected, enter the minimum bandwidth rate limit value in the space provided. This value must be between 8 and 10000000 kbps. Also enter the maximum bandwidth (**Max Bandwidth**) rate limit in the space provided. This value must be between 8 and 10000000 kbps. When the minimal bandwidth is configured, the packet transmitted from the queue can be guaranteed. When the maximum bandwidth is configured, packets transmitted from the queue cannot exceed the maximum bandwidth even if the bandwidth is available. When configuring the minimal bandwidth, the aggregate of the configured minimum bandwidth must be less than 75 percent of the interface bandwidth to make sure the configured minimal bandwidth can be guaranteed. It is not necessary to set the minimum guaranteed bandwidth for the highest strict priority queue. This is because the traffic in this queue will be serviced first if the minimal bandwidth of all queues is satisfied. The configuration of this command can only be attached to a physical port but not a port-channel. That is the minimum guaranteed bandwidth of one CoS cannot be used across physical ports. • When the **Min Percent** option is selected, enter the minimum bandwidth percentage value in the space provided. This value must be between 1 and 100 percent (%). Also enter the maximum percentage value (**Max Percent**) in the space provided. This value must be between 1 and 100 percent (%).

Parameter	Description
	• Select the **None** option to remove the rate limit on the specified port(s). The specified limitation cannot exceed the maximum speed of the specified interface.

Click the **Apply** button to accept the changes made.

Advanced Settings

DSCP Mutation Map

This window is used to display and configure the Differentiated Services Code Point (DSCP) mutation map settings. When a packet is received by an interface, based on a DSCP mutation map, the incoming DSCP can be mutated to another DSCP immediately before any QoS operations. The DSCP mutation is helpful to integrate domains with different DSCP assignments. The DSCP-CoS map and DSCP-color map will still be based on the packet's original DSCP. All the subsequent operations will base on the mutated DSCP.

To view the following window, click **QoS > Advanced Settings > DSCP Mutation Map**, as shown below:

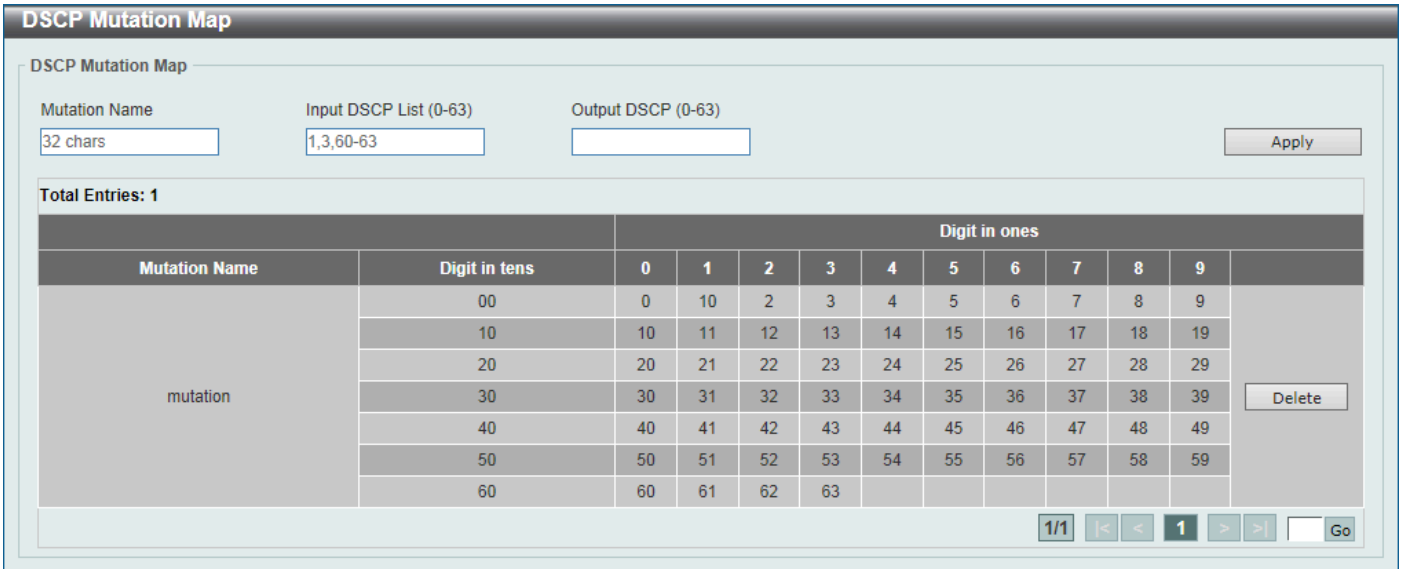


Figure 7-7 DSCP Mutation Map Window

The fields that can be configured are described below:

Parameter	Description
Mutation Name	Enter the DSCP mutation map name here. This name can be up to 32 characters long.
Input DSCP List	Enter the input DSCP list value here. This value must be between 0 and 63.
Output DSCP List	Enter the output DSCP list value here. This value must be between 0 and 63.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Port Trust State and Mutation Binding

This window is used to display and configure the port trust state and mutation binding settings.

To view the following window, click **QoS > Advanced Settings > Port Trust State and Mutation Binding**, as shown below:

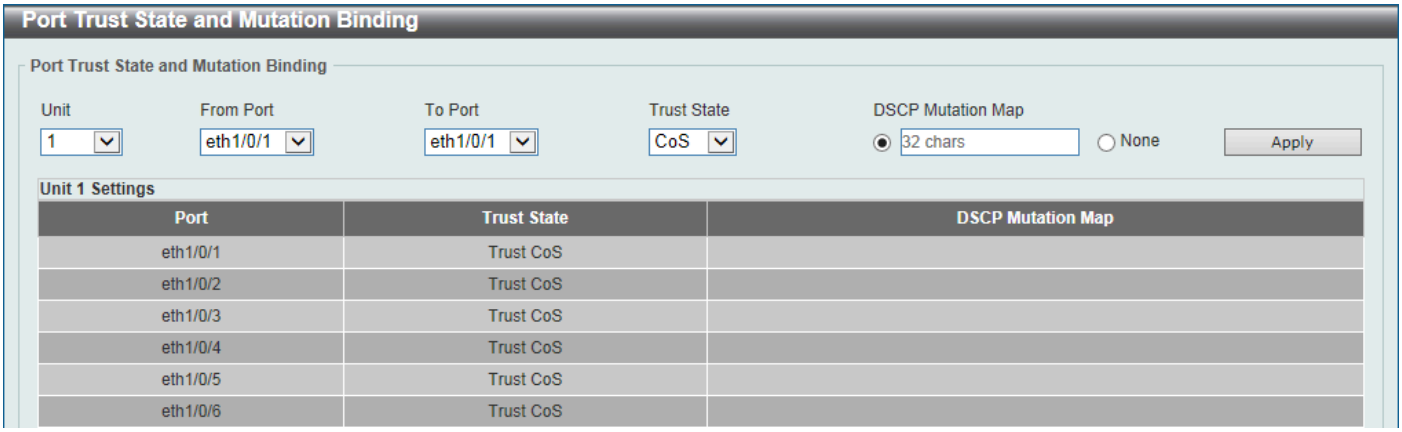


Figure 7-8 Port Trust State and Mutation Binding Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Trust State	Select the port trust state option here. Options to choose from are **CoS** and **DSCP**.
DSCP Mutation Map	Select and enter the DSCP mutation map name used here. This name can be up to 32 characters long (refer to **QoS >Advanced Settings > DSCP Mutation Map**). Select the **None** option to not allocate a DSCP mutation map to the port(s).

Click the **Apply** button to accept the changes made.

DSCP CoS Mapping

This window is used to display and configure the DSCP CoS mapping settings.

To view the following window, click **QoS > Advanced Settings > DSCP CoS Mapping**, as shown below:

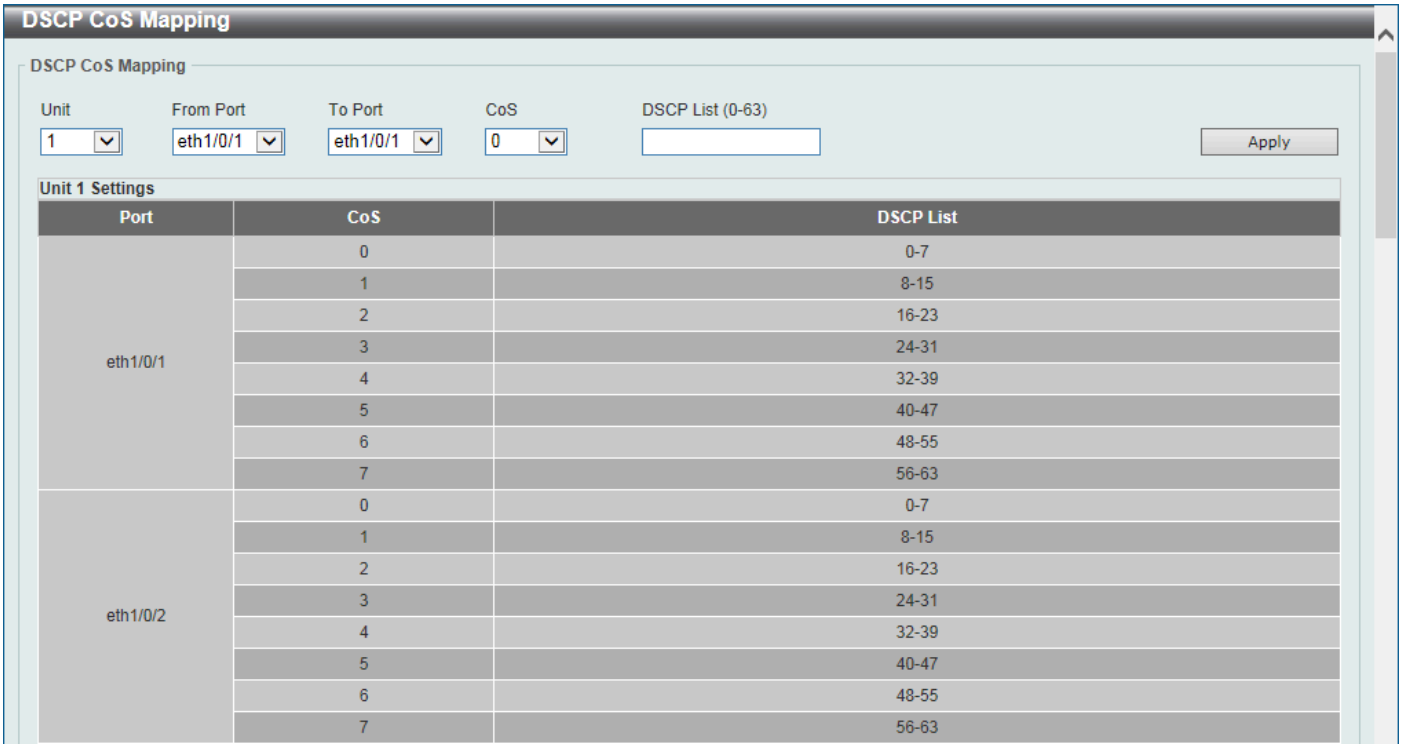


Figure 7-9 DSCP CoS Mapping Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration here.
CoS	Select the CoS value to map to the DSCP list. Options to choose from are 0 to 7.
DSCP List	Enter the DSCP list value to map to the CoS value here. This value must be between 0 and 63. Use "-" to specify the range value and "," to separate the values in the list. For example, 1-3,5,8.

Click the **Apply** button to accept the changes made.

CoS Color Mapping

This window is used to display and configure the CoS color mapping settings.

To view the following window, click **QoS > Advanced Settings > CoS Color Mapping**, as shown below:



Figure 7-10 CoS Color Mapping Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration here.
CoS List	Enter the CoS value that will be mapped to the color. This value must be between 0 and 7. Use "-" to specify the range value and "," to separate the values in the list. For example, 1-3,5,8.
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.

DSCP Color Mapping

This window is used to display and configure the DSCP color mapping settings.

To view the following window, click **QoS > Advanced Settings > DSCP Color Mapping**, as shown below:

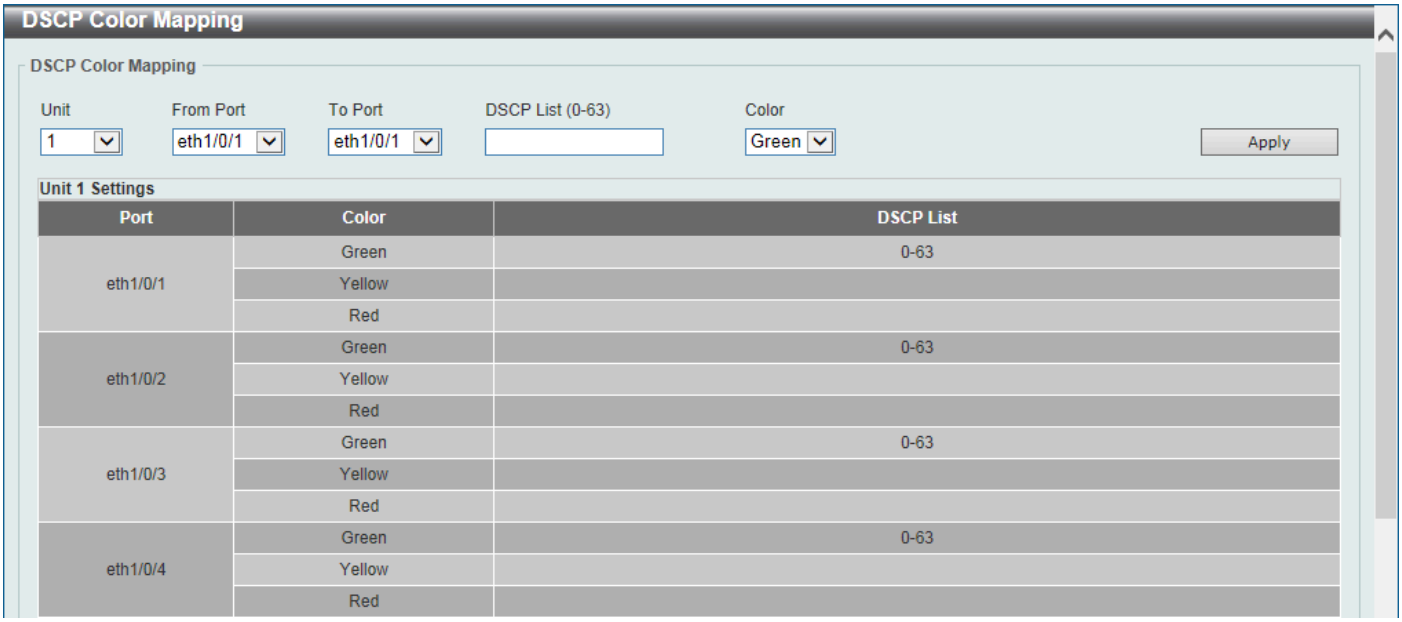


Figure 7-11 DSCP Color Mapping Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration here.
DSCP List	Enter the DSCP list value here that will be mapped to a color. This value must be between 0 and 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.

Class Map

This window is used to display and configure the class map settings.

To view the following window, click **QoS > Advanced Settings > Class Map**, as shown below:



Figure 7-12 Class Map Window

The fields that can be configured are described below:

Parameter	Description
Class Map Name	Enter the class map name here. This name can be up to 32 characters long. Do not include spaces.
Multiple Match Criteria	Select the multiple match criteria option here. Options to choose from are **Match All** and **Match Any**.

Click the **Apply** button to accept the changes made.

Click the **Match** button to configure the specific entry.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Match** button, the following page will be available.

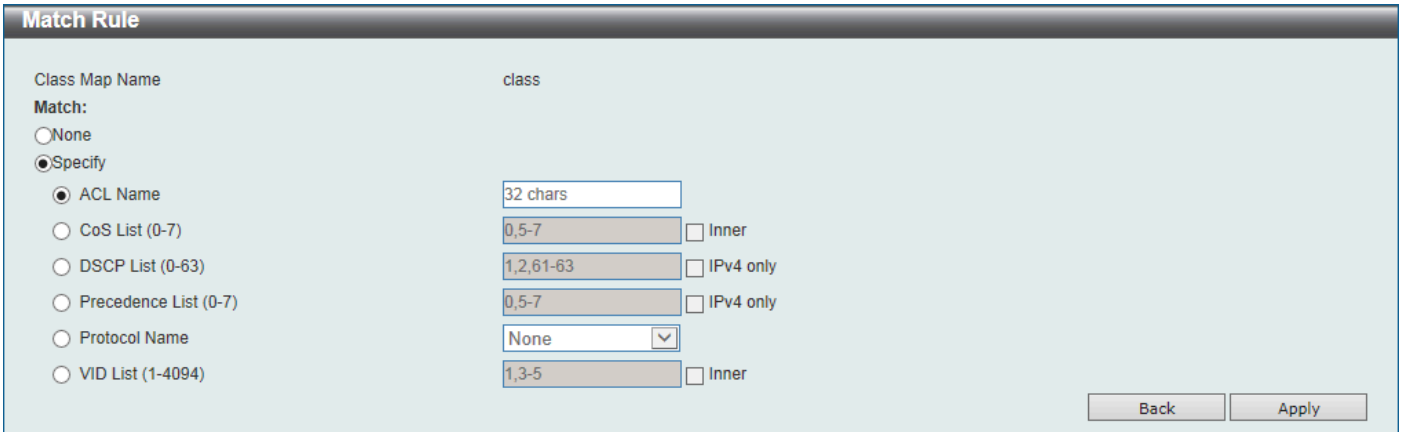


Figure 7-13 Class Map (Match) Window

The fields that can be configured are described below:

Parameter	Description
None	Select this option to match nothing to this class map.
Specify	Select the option to match something to this class map.
ACL Name	Select and enter the access list name that will be matched with this class map here. This name can be up to 32 characters long.
CoS List	Select and enter the CoS list value that will be matched with this class map here. This value must be between 0 and 7. Tick the **Inner** option to match the inner most CoS of QinQ packets on a Layer 2 class of service (CoS) marking.
DSCP List	Select and enter the DSCP list value that will be matched with this class map here. This value must be between 0 and 63. Tick the **IPv4 only** option to match IPv4 packets only. If not specified, the match is for both IPv4 and IPv6 packets.
Precedence List	Select and enter the precedence list value that will be matched with this class map here. This value must be between 0 and 7. Tick the **IPv4 only** option to match IPv4 packets only. If not specified, the match is for both IPv4 and IPv6 packets. For IPv6 packets, the precedence is most three significant bits of traffic class of IPv6 header.
Protocol Name	Select the protocol name that will be matched with the class map here. Options to choose from are **ARP**, **BGP**, **DHCP**, **DNS**, **EGP**, **FTP**, **IPv4**, **IPv6**, **NetBIOS**, **NFS**, **NTP**, **OSPF**, **PPPOE**, **RIP**, **RTSP**, **SSH**, **Telnet**, and **TFTP**.
VID List	Select and enter the VLAN list value that will be matched with the class map here. This value must be between 1 and 4094. Tick the **Inner** option to match the inner-most VLAN ID in an 802.1Q double tagged frame.

Click the **Apply** button to accept the changes made.

Click the **Back** button to discard the changes made and return to the previous page.

Aggregate Policer

This window is used to display and configure the aggregate policer settings.

To view the following window, click **QoS > Advanced Settings > Aggregate Policer**, as shown below:

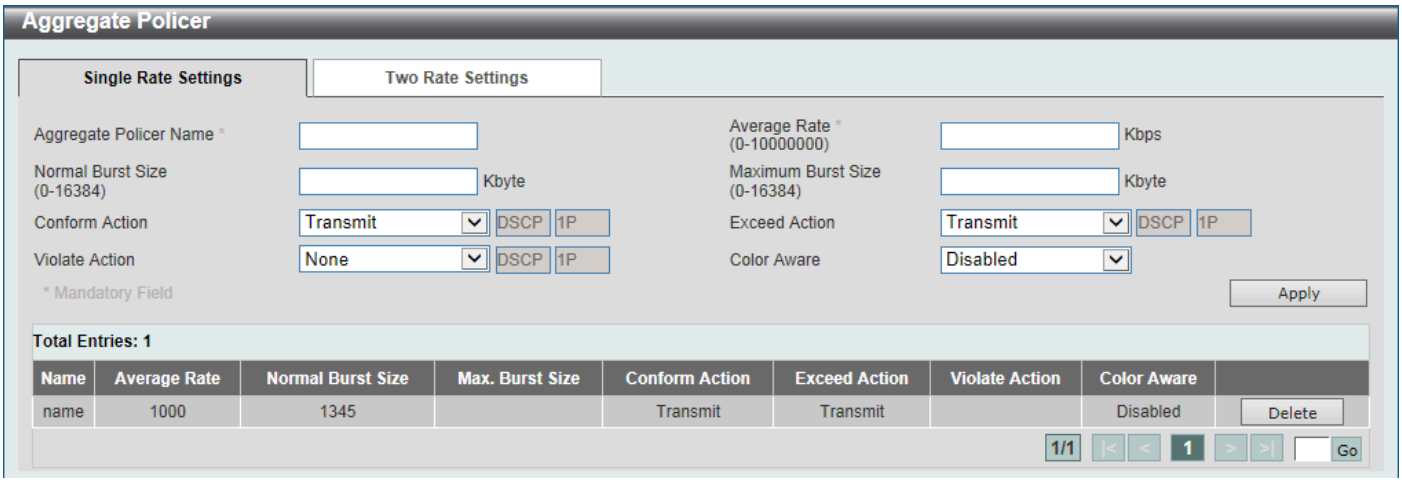


Figure 7-14 Aggregate Policer (Single Rate Setting) Window

The fields that can be configured are described below:

Parameter	Description
Aggregate Policer Name	Enter the aggregate policer name here. This name can be up to 32 characters long. Do not include spaces.
Average Rate	Enter the average rate value here. This value must be between 0 and 10000000 kbps.
Normal Burst Size	Enter the normal burst size value here. This value must be between 0 and 16384 Kbytes.
Maximum Burst Size	Enter the maximum burst size value here. This value must be between 0 and 16384 Kbytes.
Conform 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**, **Set-DSCP-Transmit**, **Set-1P-Transmit**, **Transmit**, and **Set-DSCP-1P**. • When selecting the **Drop** option, the packet will be dropped. • When selecting the **Set-DSCP-Transmit** option, enter the IP DSCP value in the space provided. This value sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value. • When selecting the **Set-1P-Transmit** option, enter the 1P transmit value in the space provided. This value sets the 802.1p value and transmits the packet with the new value. • When selecting the **Transmit** option, packets will be transmitted unaltered.

Parameter	Description
	• When selecting the **Set-DSCP-1P** option, enter the IP DSCP and 1P transmit 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**, **Set-DSCP-Transmit**, **Set-1P-Transmit**, **Transmit**, and **Set-DSCP-1P**. • When selecting the **Drop** option, the packet will be dropped. • When selecting the **Set-DSCP-Transmit** option, enter the IP DSCP value in the space provided. This value sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value. • When selecting the **Set-1P-Transmit** option, enter the 1P transmit value in the space provided. This value sets the 802.1p value and transmits the packet with the new value. • When selecting the **Transmit** option, packets will be transmitted unaltered. • When selecting the **Set-DSCP-1P** option, enter the IP DSCP and 1P transmit values in the spaces provided.
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**, **Drop**, **Set-DSCP-Transmit**, **Set-1P-Transmit**, **Transmit**, and **Set-DSCP-1P**. • When selecting the **None** option, no action will be taken. • When selecting the **Drop** option, the packet will be dropped. • When selecting the **Set-DSCP-Transmit** option, enter the IP DSCP value in the space provided. This value sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value. • When selecting the **Set-1P-Transmit** option, enter the 1P transmit value in the space provided. This value sets the 802.1p value and transmits the packet with the new value. • When selecting the **Transmit** option, packets will be transmitted unaltered. • When selecting the **Set-DSCP-1P** option, enter the IP DSCP and 1P transmit values in the spaces provided.
Color Aware	Select the color aware option here. Options to choose from are **Enabled** and **Disabled**. When color aware is disabled, the policer works in the color blind mode. When color aware is enabled, the policer works in the color aware mode.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After selecting the **Two Rate Settings** tab option, at the top of the page, the following page will be available.

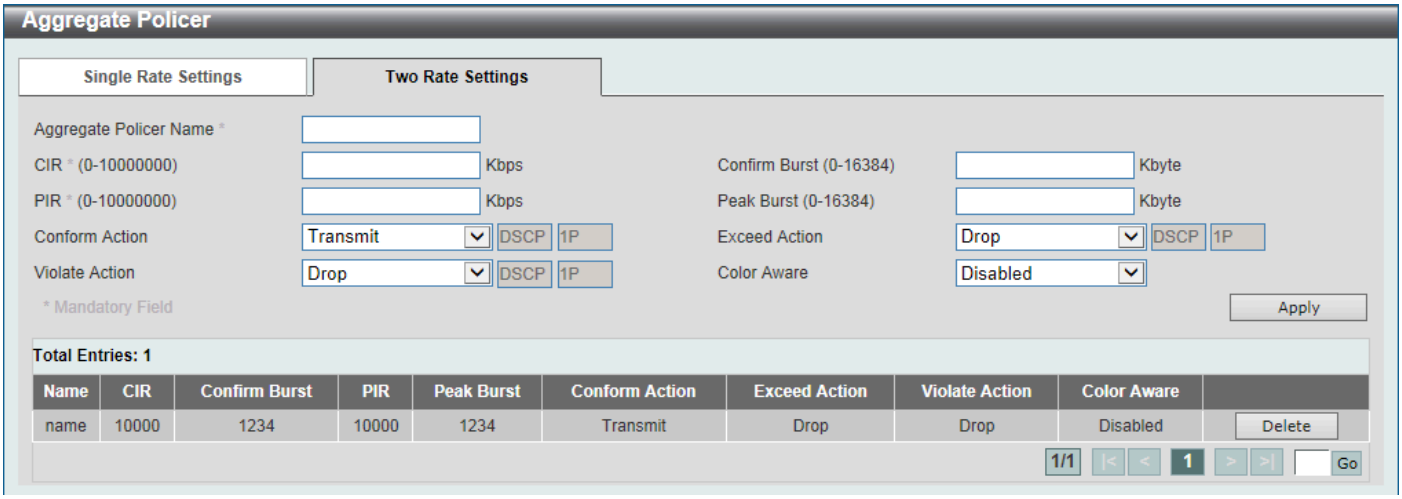


Figure 7-15 Aggregate Policer (Two Rate Settings) Window

The fields that can be configured are described below:

Parameter	Description
Aggregate Policer Name	Enter the aggregate policer name here. This name can be up to 32 characters long. Do not include spaces.
CIR	Enter the Committed Information Rate (CIR) value here. This value must be between 0 and 10000000 kbps. The committed packet rate is the first token bucket for the two-rate metering.
Confirm Burst	Enter the confirm burst value here. This value must be between 0 and 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. This value must be between 0 and 10000000 kbps. The peak information rate is the second token bucket for the two-rate metering.
Peak Burst	Enter the peak burst value here. This value must be between 0 and 16384 Kbytes. The peak burst value is the burst size for the second token bucket in kilobytes.
Conform 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**, **Set-DSCP-Transmit**, **Set-1P-Transmit**, **Transmit**, and **Set-DSCP-1P**. • When selecting the **Drop** option, the packet will be dropped. • When selecting the **Set-DSCP-Transmit** option, enter the IP DSCP value in the space provided. This value sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value. • When selecting the **Set-1P-Transmit** option, enter the 1P transmit value in the space provided. This value sets the 802.1p value and transmits the packet with the new value. • When selecting the **Transmit** option, packets will be transmitted unaltered. • When selecting the **Set-DSCP-1P** option, enter the IP DSCP and 1P transmit 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

Parameter	Description
	is not specified, the default action is **Drop**. Options to choose from are **Drop**, **Set-DSCP-Transmit**, **Set-1P-Transmit**, **Transmit**, and **Set-DSCP-1P**. • When selecting the **Drop** option, the packet will be dropped. • When selecting the **Set-DSCP-Transmit** option, enter the IP DSCP value in the space provided. This value sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value. • When selecting the **Set-1P-Transmit** option, enter the 1P transmit value in the space provided. This value sets the 802.1p value and transmits the packet with the new value. • When selecting the **Transmit** option, packets will be transmitted unaltered. • When selecting the **Set-DSCP-1P** option, enter the IP DSCP and 1P transmit values in the spaces provided.
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**, **Set-DSCP-Transmit**, **Set-1P-Transmit**, **Transmit**, and **Set-DSCP-1P**. • When selecting the **Drop** option, the packet will be dropped. • When selecting the **Set-DSCP-Transmit** option, enter the IP DSCP value in the space provided. This value sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value. • When selecting the **Set-1P-Transmit** option, enter the 1P transmit value in the space provided. This value sets the 802.1p value and transmits the packet with the new value. • When selecting the **Transmit** option, packets will be transmitted unaltered. • When selecting the **Set-DSCP-1P** option, enter the IP DSCP and 1P transmit values in the spaces provided.
Color Aware	Select the color aware option here. Options to choose from are **Disabled** and **Enabled**. When color aware is disabled, the policer works in the color-blind mode. When color aware is enabled, the policer works in the color aware mode.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Policy Map

This window is used to display and configure the policy map settings.

To view the following window, click **QoS > Advanced Settings > Policy Map**, as shown below:

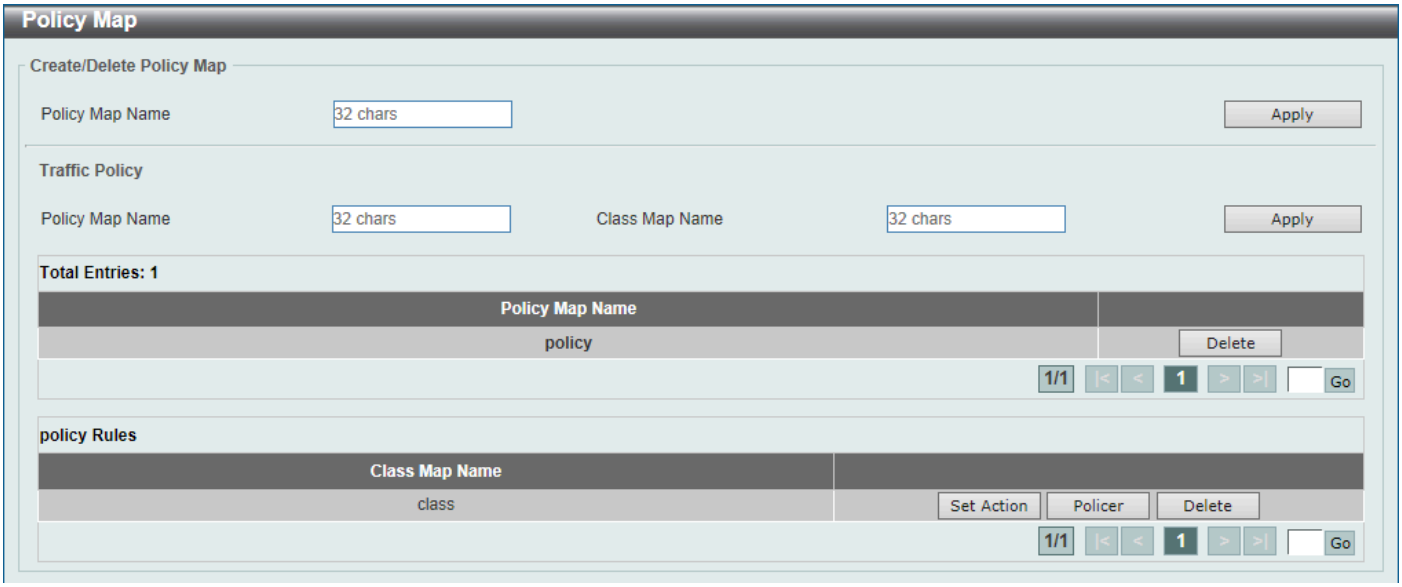


Figure 7-16 Policy Map Window

The fields that can be configured for **Create/Delete Policy Map** are described below:

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. Do not include spaces.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Traffic Policy** are described below:

Parameter	Description
Policy Map Name	Enter the policy map name here. This name can be up to 32 characters long. Do not include spaces.
Class Map Name	Enter the class map name here. This name can be up to 32 characters long. Do not include spaces. Refer to **QoS > Advanced Settings > Class Map**.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **Set Action** button to configure the set action settings for the specified entry.

Click the **Policer** button to configure the policer settings for the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Set Action** button, the following page will appear.

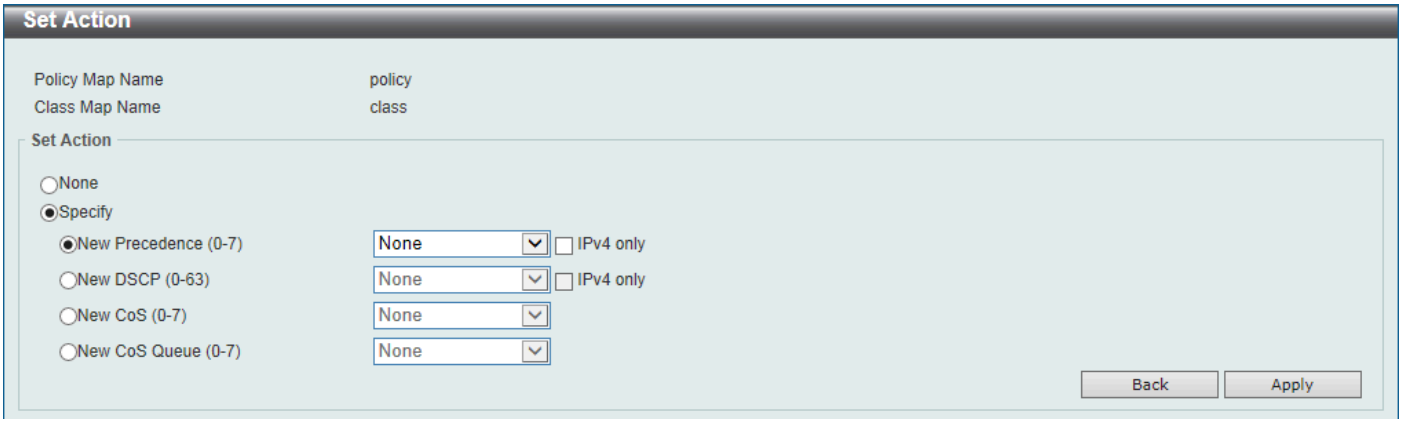


Figure 7-17 Policy Map (Set Action) Window

The fields that can be configured are described below:

Parameter	Description
None	Select this option to specify that no action will be taken.
Specify	Select this option to specify that action will be taken based on the configurations made.
New Precedence	Select the new precedence value for the packet here. The range is from 0 to 7. Select the **IPv4 only** option to specify that IPv4 precedence will be marked only. If not selected, then both IPv4 and IPv6 precedence will be marked. For IPv6 packets, the precedence is the most three significant bits of the traffic class of the IPv6 header. Setting the precedence will not affect the CoS queue selection.
New DSCP	Select the new DSCP value for the packet here. The range is from 0 to 63. Select the **IPv4 only** option to specify that the IPv4 DSCP will be marked only. If not selected, then both the IPv4 and IPv6 DSCP will be marked. Setting the DSCP will not affect the CoS queue selection.
New CoS	Select the new CoS value to the packet here. The range is from 0 to 7. Setting the CoS will not affect the CoS queue selection.
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 **Back** button to return to the previous window.

Click the **Apply** button to accept the changes made.

After clicking the **Policer** button, the following page will appear.

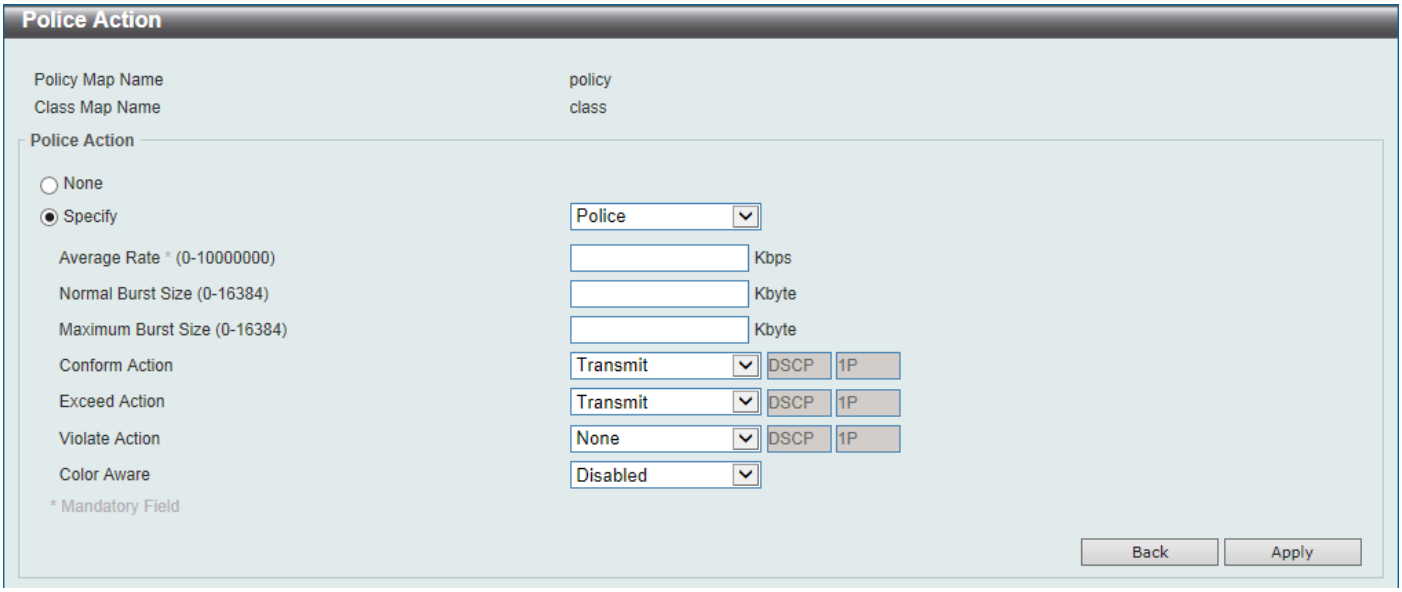


Figure 7-18 Policy Map (Policer) Window

The fields that can be configured are described below:

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 conform action is to drop the packet. **Set-DSCP-Transmit** - Specifies that the conform action is to modify the DSCP value and then to transmit the packet with the new DSCP value. Enter the new DSCP value in the space provided. **Set-1P-Transmit** - Specifies that the conform action is to modify the 802.1p value and then to transmit the packet with the new 802.1p value. Enter the new 802.1p value in the space provided. **Transmit** - Specifies that the conform action is to transmit the packet unmodified. **Set-DSCP-1P** - Specifies that the conform action is to modify the DSCP and 802.1p values and then to transmit the packet with the new DSCP and 802.1p values. Enter the new DSCP and 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 exceed action is to drop the packet. **Set-DSCP-Transmit** - Specifies that the exceed action is to modify the DSCP value and then to transmit the packet with the new DSCP value. Enter the new DSCP value in the space provided.

Parameter	Description
	Set-1P-Transmit - Specifies that the exceed action is to modify the 802.1p value and then to transmit the packet with the new 802.1p value. Enter the new 802.1p value in the space provided. **Transmit** - Specifies that the exceed action is to transmit the packet unmodified. **Set-DSCP-1P** - Specifies that the exceed action is to modify the DSCP and 802.1p values and then to transmit the packet with the new DSCP and 802.1p values. Enter the new DSCP and 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 violate action is to drop the packet. **Set-DSCP-Transmit** - Specifies that the violate action is to modify the DSCP value and then to transmit the packet with the new DSCP value. Enter the new DSCP value in the space provided. **Set-1P-Transmit** - Specifies that the violate action is to modify the 802.1p value and then to transmit the packet with the new 802.1p value. Enter the new 802.1p value in the space provided. **Transmit** - Specifies that the violate action is to transmit the packet unmodified. **Set-DSCP-1P** - Specifies that the violate action is to modify the DSCP and 802.1p values and then to transmit the packet with the new DSCP and 802.1p values. Enter the new DSCP and 802.1p values in the spaces provided.
Color Aware	Select to enable or disable the color aware feature here. When disabled, the policer works in the color blind mode. When enabled, the policer works in the color aware mode.

Click the **Back** button to return to the previous window.

Click the **Apply** button to accept the changes made.

Policy Binding

This window is used to display and configure the policy binding settings.

To view the following window, click **QoS > Advanced Settings > Policy Binding**, as shown below:

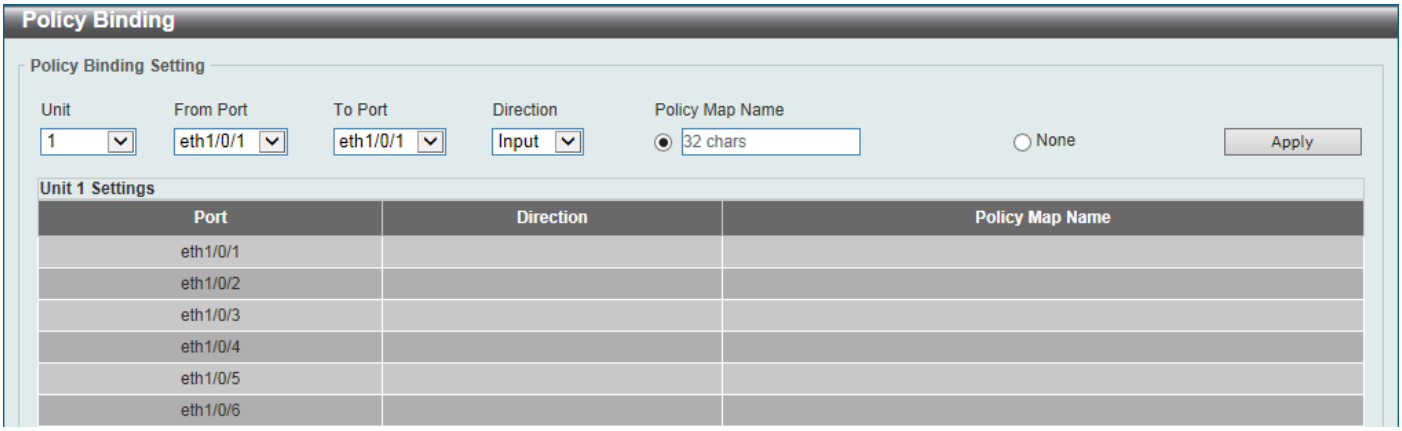


Figure 7-19 Policy Binding Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Direction	Select the direction option here. Options to choose from are **Input** 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 to not tie a policy map to this entry.

Click the **Apply** button to accept the changes made.

WRED

Weighted Random Early Detection (WRED) is another implementation for QoS that will help the overall throughput for your QoS queues. Based on the egress queue of the QoS function set on the Switch, this method will analyze these packets and their QoS queue to determine if there will be an overflow of packets entering the QoS queues and consequentially, minimize the packet flow into these queues by dropping random packets. WRED employs two methods of avoiding congestion within the QoS queue.

1. Every QoS queue has a minimum and a maximum level for acceptance of packets. Once the maximum threshold has been reached for this queue, the Switch will begin discarding all ingress packets, this minimizing the allotted bandwidth for QoS. When below the minimum threshold, the Switch will accept all ingress packets.
2. When the ingress packets are somewhere between the maximum and minimum queue, the Switch will use a slope probability function to determine a random method of dropping packets based on the maximum drop rate which specifies the drop probability when the queues reach maximum threshold. If queues are closer to the maximum threshold, the Switch will increase the discarding of random packets to even out the flow to the queues and avoid overflows to higher priority queues.

WRED Profile

This window is used to display and configure the Weighted Random Early Detection (WRED) profile settings.

To view the following window, click **QoS > WRED > WRED Profile**, as shown below:

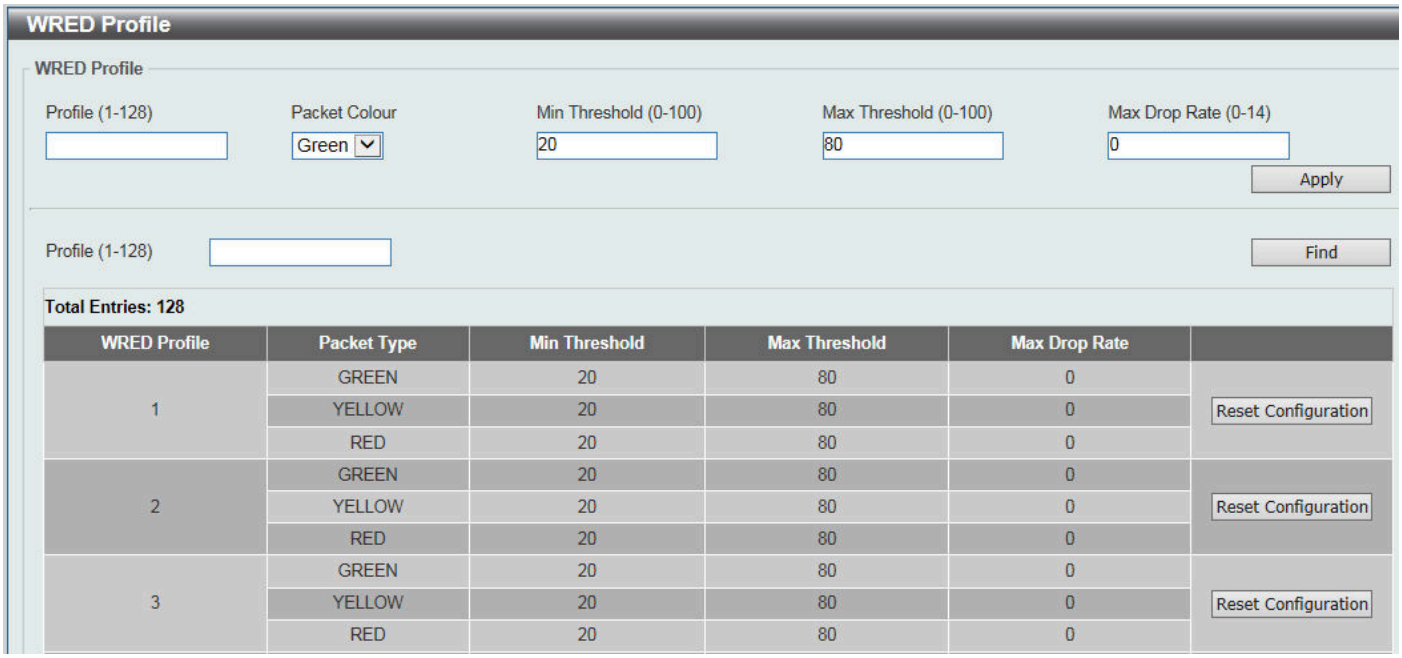


Figure 7-20 WRED Profile Window

The fields that can be configured are described below:

Parameter	Description
Profile	Enter the WRED profile ID here. The range is from 1 to 128.
Packet Colour	Select the packet color here. Options to choose from are **Green**, **Yellow**, and **Red**. **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.
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 locate a specific entry based on the information entered.

Click the **Reset Configuration** button to reset the configuration to the default values on the specified entry.

WRED Queue

This window is used to display and configure the WRED queue settings. WRED drops packets, based on the average queue size exceeding a specific threshold, to indicate congestion. Explicit Congestion Notification (ECN) is an extension to WRED in that ECN marks packets instead of dropping them when the average queue size exceeds a specific threshold value. When configuring the WRED ECN feature, routers and end hosts would use this marking as a signal that the network is congested and slow down sending packets.

To view the following window, click **QoS > WRED > WRED Queue**, as shown below:

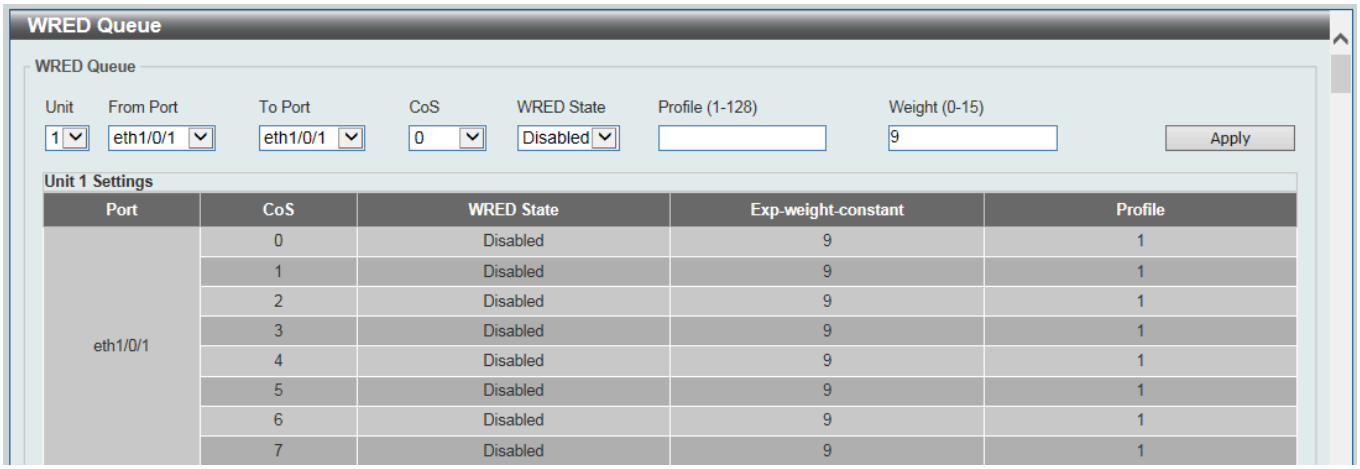


Figure 7-21 WRED Queue Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit ID that will be used here.This option is only available when stacking is enabled.
From Port - To Port	Select the Switch port range 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.

8. Access Control List (ACL)

ACL Configuration Wizard
ACL Access List
ACL Interface Access Group
ACL VLAN Access Map
ACL VLAN Filter
CPU ACL

ACL Configuration Wizard

This window is used to guide the user to create a new ACL access list or configure an existing ACL access list.

Use the following procedure to create an ACL access-list:

1. Click **ACL > ACL Configuration Wizard**. The following window displays:

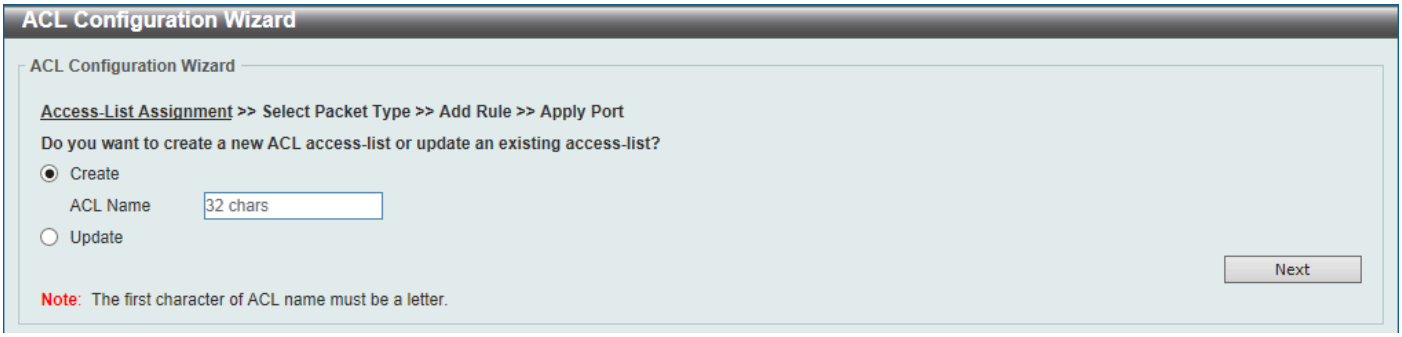


Figure 8-1 ACL Configuration Wizard (Create) Window

2. Enter the following information to create a new ACL access-list:

Parameter	Description
ACL Name	Enter the new ACL name here. This name can be up to 32 characters long.

Or click **Update** to modify an existing ACL access-list:

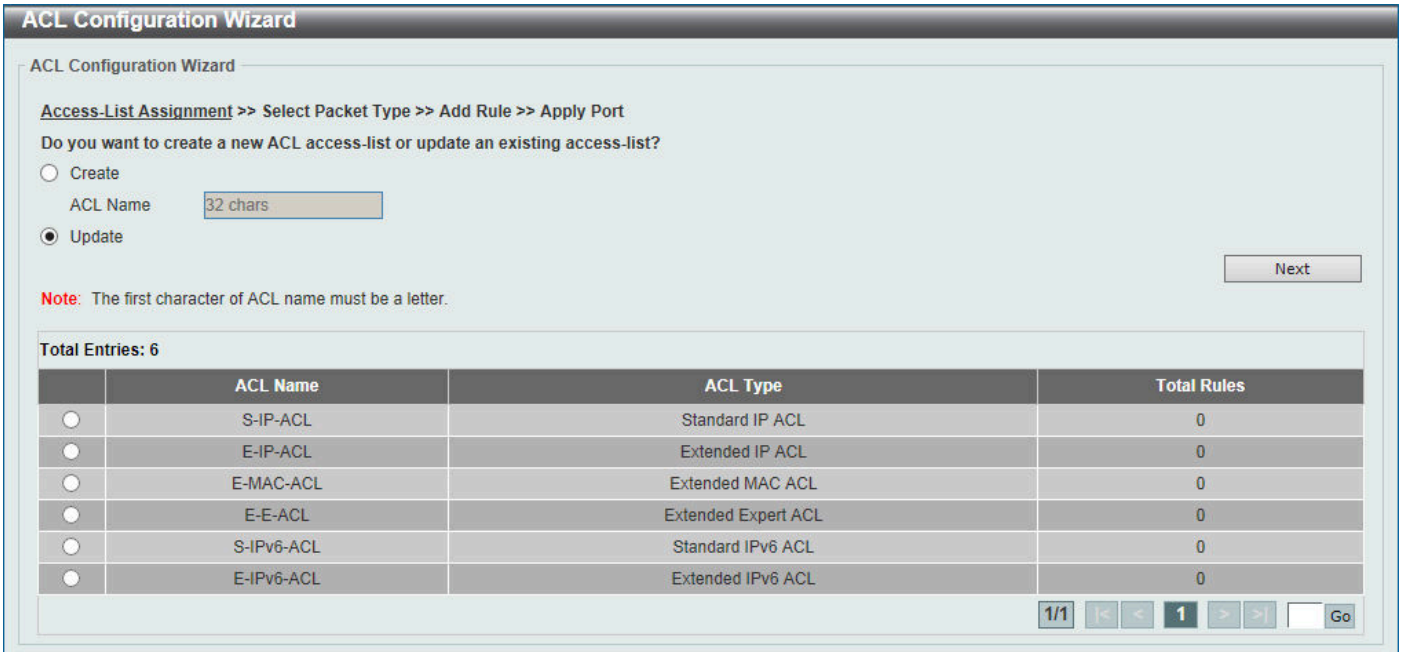


Figure 8-2 ACL Configuration Wizard (Update) Window

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **Next** button to continue to the next step.

3. Select the packet type for configuration:

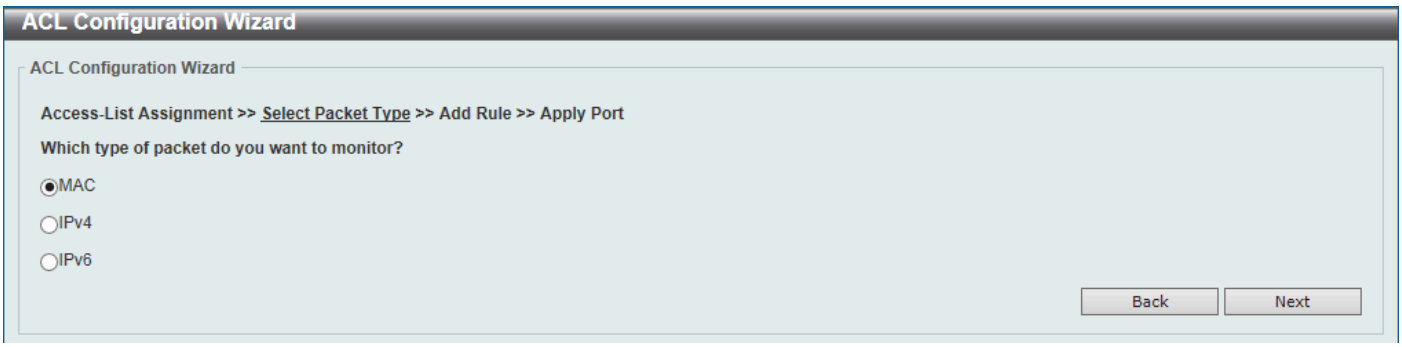


Figure 8-3 ACL Configuration Wizard (Create, Packet Type) Window

The fields that can be configured are described below:

Parameter	Description
MAC	Select to create/update a MAC ACL.
IPv4	Select to create/update an IPv4 ACL.
IPv6	Select to create/update an IPv6 ACL.

Click the **Back** button to return to the previous step.

Click the **Next** button to continue to the next step.

MAC

4. After clicking the **MAC** radio button and the **Next** button, the following window will appear. Add rule by first assigning a new sequence number first. This value must be between 1 and 65535. Or select **Auto Assign** to automatically generate an ACL rule number for this entry. For Assign Rule Criteria, refer the Extended MAC ACL configuration in the following **ACL Access List** section. For Time Range, enter the **Time Range** profile to be applied for ACL. Then select permit or deny as the **Action** that this rule will take.

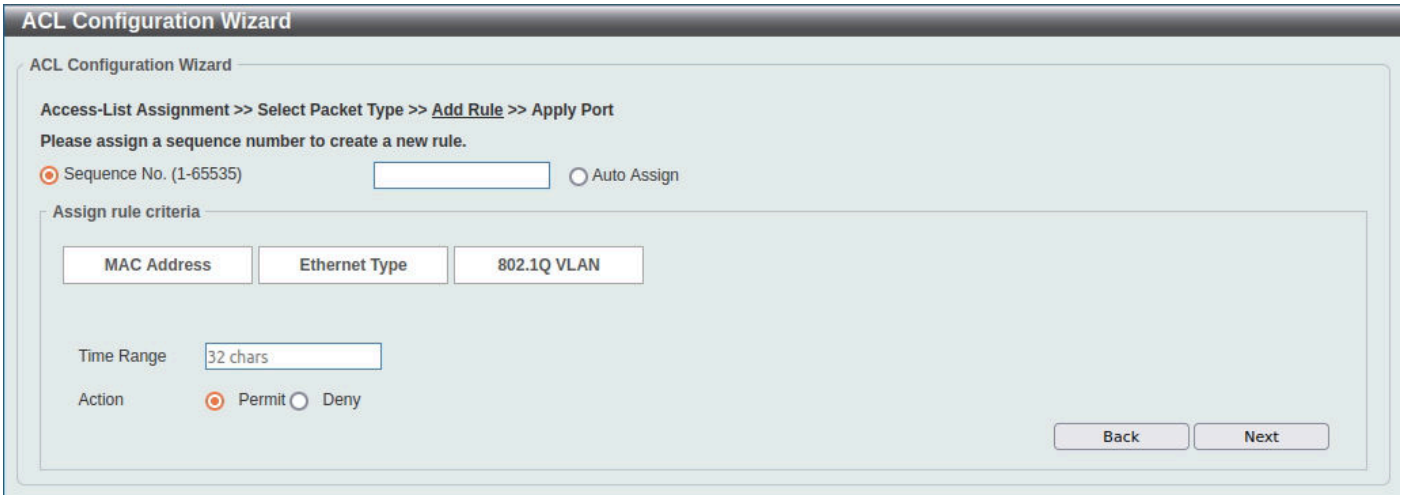


Figure 8-4 ACL Configuration Wizard (Create, Packet Type, MAC) Window

IPv4/IPv6

4. After clicking the **IPv4** or **IPv6** radio button and the **Next** button, the following window will appear.

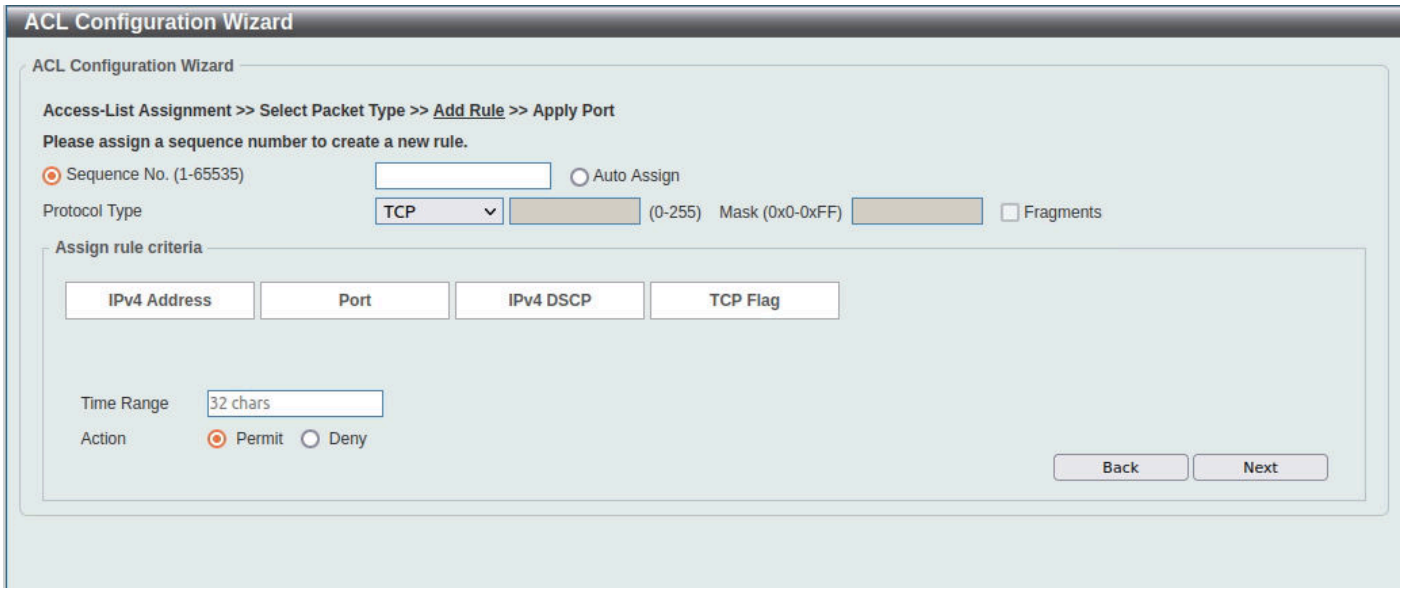


Figure 8-5 ACL Configuration Wizard (Create, Packet Type, IPv4) Window

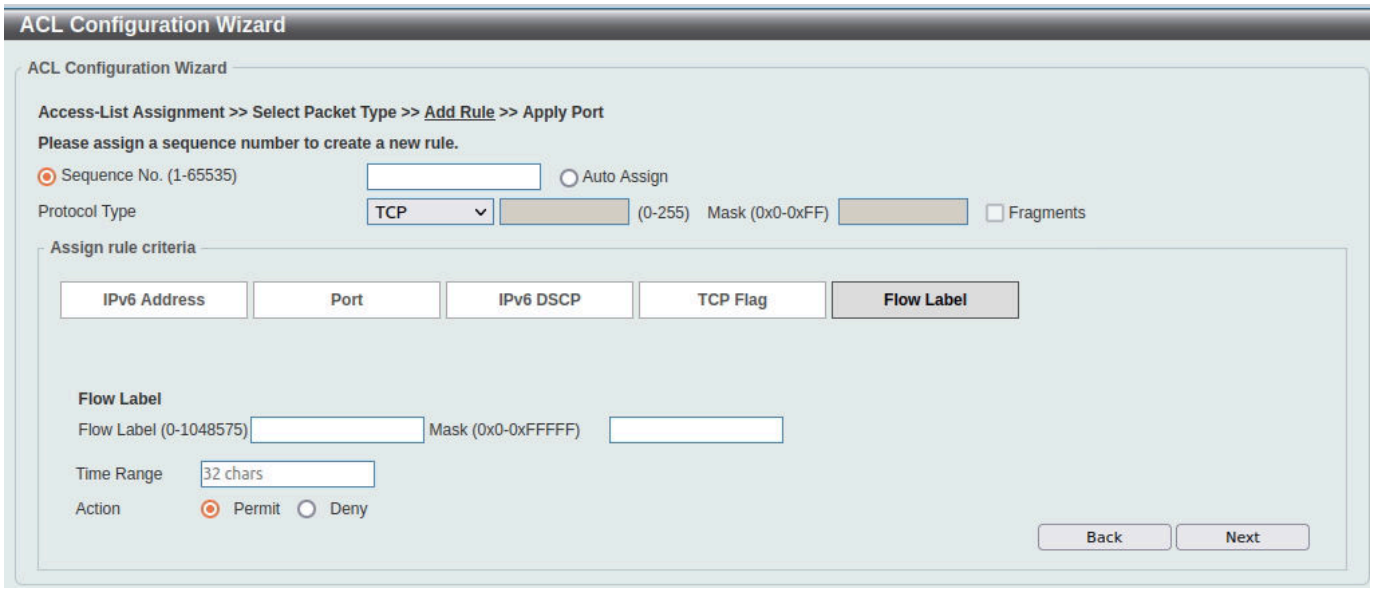


Figure 8-6 ACL Configuration Wizard (Create, Packet Type, IPv6) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. This value must be between 1 and 65535. Select **Auto Assign** to automatically generate an ACL rule number for this entry.
Protocol Type	For IPv4, select the protocol type option here: 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. • **IGMP Type** - Enter the IGMP sypte. The range is from 0 to 255 if IGMP is selected for protocol type. For IPv6, 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.
Assign Rule Criteria	For Assign Rule criteria, refer the IP/IPv6 ACL configuration in the following **ACL Access List** section.
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. Refer to **System > Time Range**.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.

Click the **Next** button to continue to the next step.

5. After clicking the **Next** button, the following window will appear.

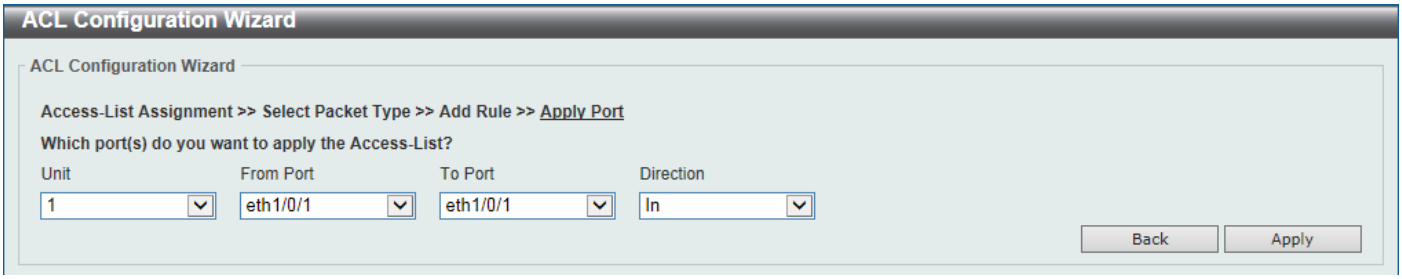


Figure 8-7 ACL Configuration Wizard (Create, Port) Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
Direction	Select the direction here. Options to choose from are **In** and **Out**.

Click the **Back** button to return to the previous step.

Click the **Apply** button to accept the changes made and return to the main ACL Wizard window.

ACL Access List

This window is used to display and configure the ACLs, ACL rules and settings.

To view the following window, click **ACL > ACL Access List**, as shown below:

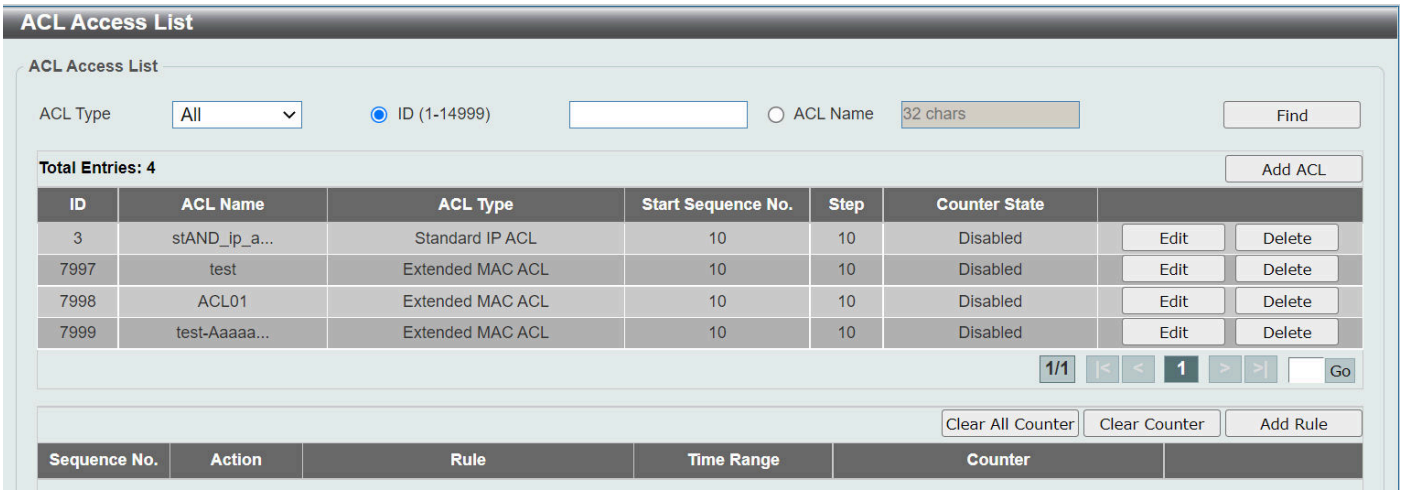


Figure 8-8 ACL Access List Window

The fields that can be configured are described below:

Parameter	Description
ACL Type	Select the ACL type to find here. Options to choose from are **All, IP ACL, IPv6 ACL, MAC ACL**, and **Expert ACL**.
ID	Select and enter the access list ID here. The range is from 1 to 14999 depending on the ACL Type selected.

Parameter	Description
ACL Name	Select and enter the access list name here. This name can be up to 32 characters long.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Add ACL** button to create a new ACL.

Click the **Edit** button to re-configure the specific ACL.

Click the **Delete** button, next to the ACL, to remove the specific ACL.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **Add Rule** button to create an ACL rule for the ACL selected (select the row of the desired ACL ID in the table of entries, then click Add Rule).

Click the **Delete** button, next to the ACL rule, to remove the specific ACL rule.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Edit** button, the following page will appear.

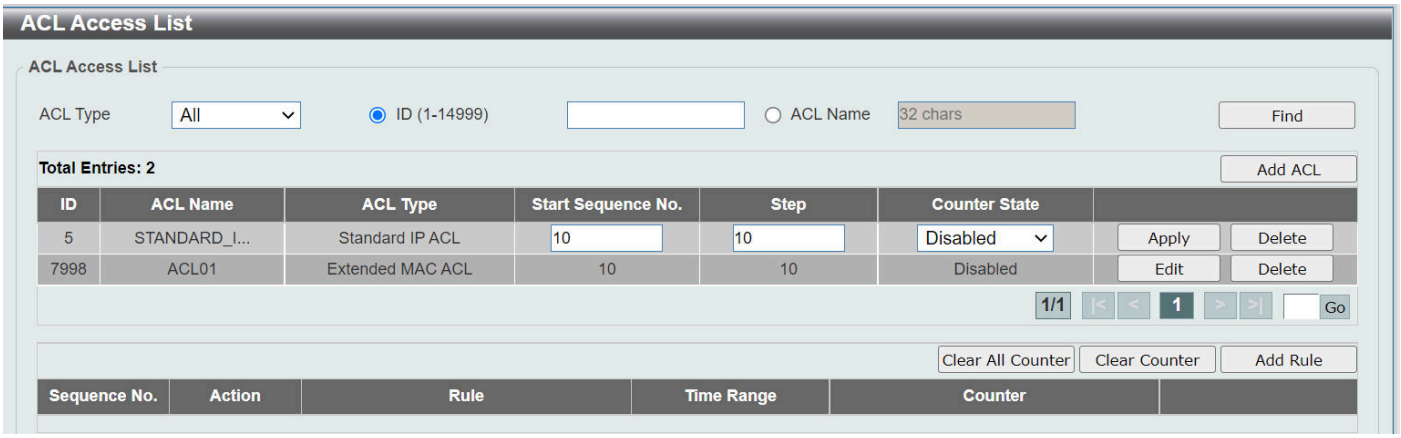


Figure 8-9 ACL Access List (Edit) Window

After clicking the **Edit** button, the fields that can be configured are described below:

Parameter	Description
Start Sequence No.	Enter the start sequence number here.
Step	Enter the sequence number step here. The step range is from 1 to 32. This specifies the number that the sequence numbers step. The default value is 10. For example, if the increment (step) value is 5 and the beginning sequence number is 20, the subsequent sequence numbers are 25, 30, 35, 40, and so on.
Counter State	Enable or disable the counting of the number of times this ACL has been matched.

Click the **Apply** button to accept the changes made.

After clicking the **Add ACL** button, the following page will appear.

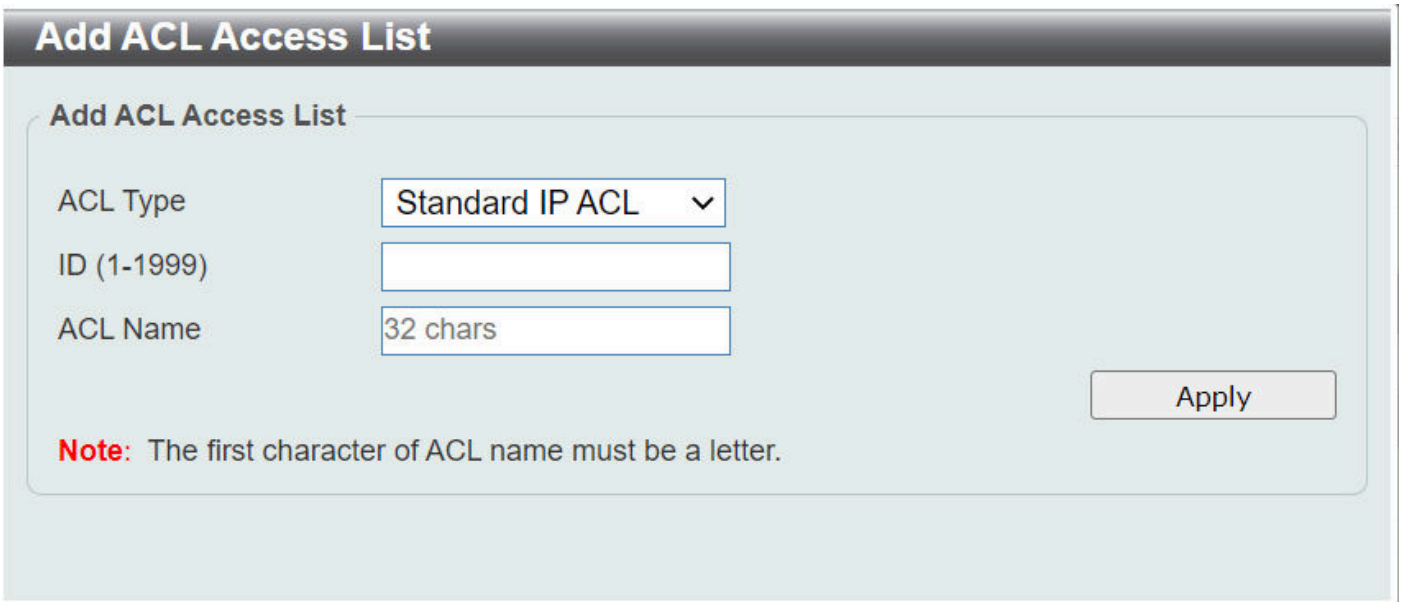


Figure 8-10 ACL Access List (Add ACL) Window

After clicking the **Add ACL** button, the fields that can be configured are described below:

Parameter	Description
ACL Type	Select the ACL type that will be created here. Options to choose from are **Standard IP ACL, Extended IP ACL, Standard IPv6 ACL, Extended IPv6 ACL, Extended MAC ACL**, and **Extended Expert ACL**.
ID	Enter the ID for the ACL here. For a **Standard IP ACL**, the range from 1 to 1999. For an **Extended IP ACL**, the range from 2000 to 3999. For a **Standard IPv6 ACL**, the range from 11000 to 12999. For an **Extended IPv6 ACL**, the range from 13000 to 14999. For an **Extended MAC ACL**, the range from 6000 to 7999. For an **Extended Expert ACL**, the range 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 accept the changes made.

Standard IP ACL

After selecting a Standard IP ACL and clicking the **Add Rule** button, the following page will appear.

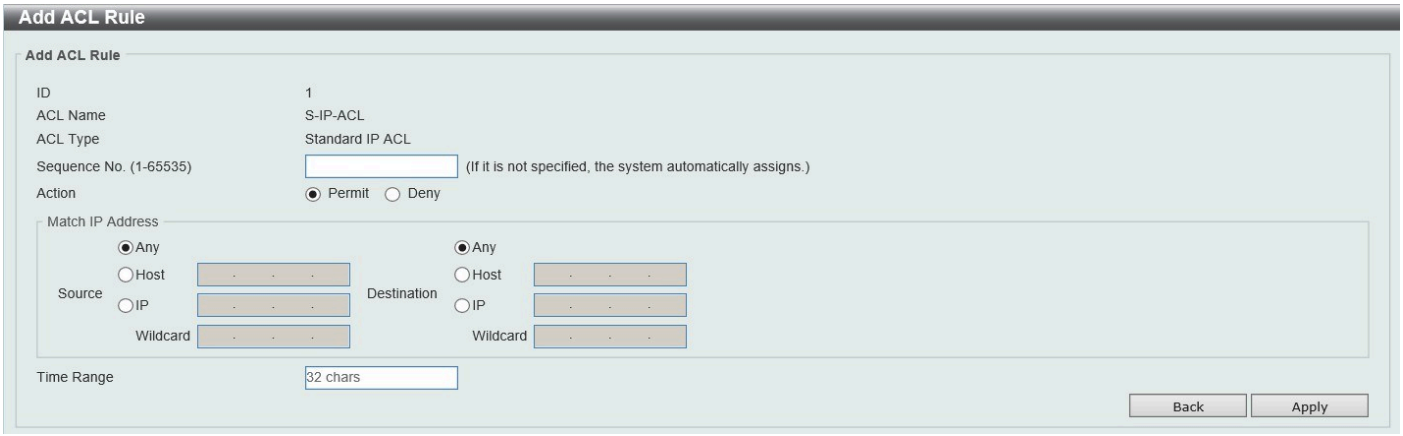


Figure 8-11 Standard IP ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the sequence number of this ACL rule here. The range is from 1 to 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are **Permit**, and **Deny**.
Source	Select and enter the source information here. Options to choose from are **Any, Host, IP**, and **Wildcard**. • When the **Any** option is selected, any source traffic will be evaluated according to the conditions of this rule. • When the **Host** option is selected, enter the source host IP address here. • When the **IP** option is selected, the **Wildcard** option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Destination	Select and enter the destination information here. Options to choose from are **Any, Host, IP**, and **Wildcard**. • When the **Any** option is selected, any destination traffic will be evaluated according to the conditions of this rule. • When the **Host** option is selected, enter the destination host IP address here. • When the **IP** option is selected, the **Wildcard** option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap (an inverted mask). 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. Refer to **System > Time** Range**.**

Click the **Apply** button to accept the changes made.

Click the **Back** button to discard the changes made and return to the previous page.

Extended IP ACL

After selecting an Extended IP ACL and clicking the **Add Rule** button, the following page will appear.

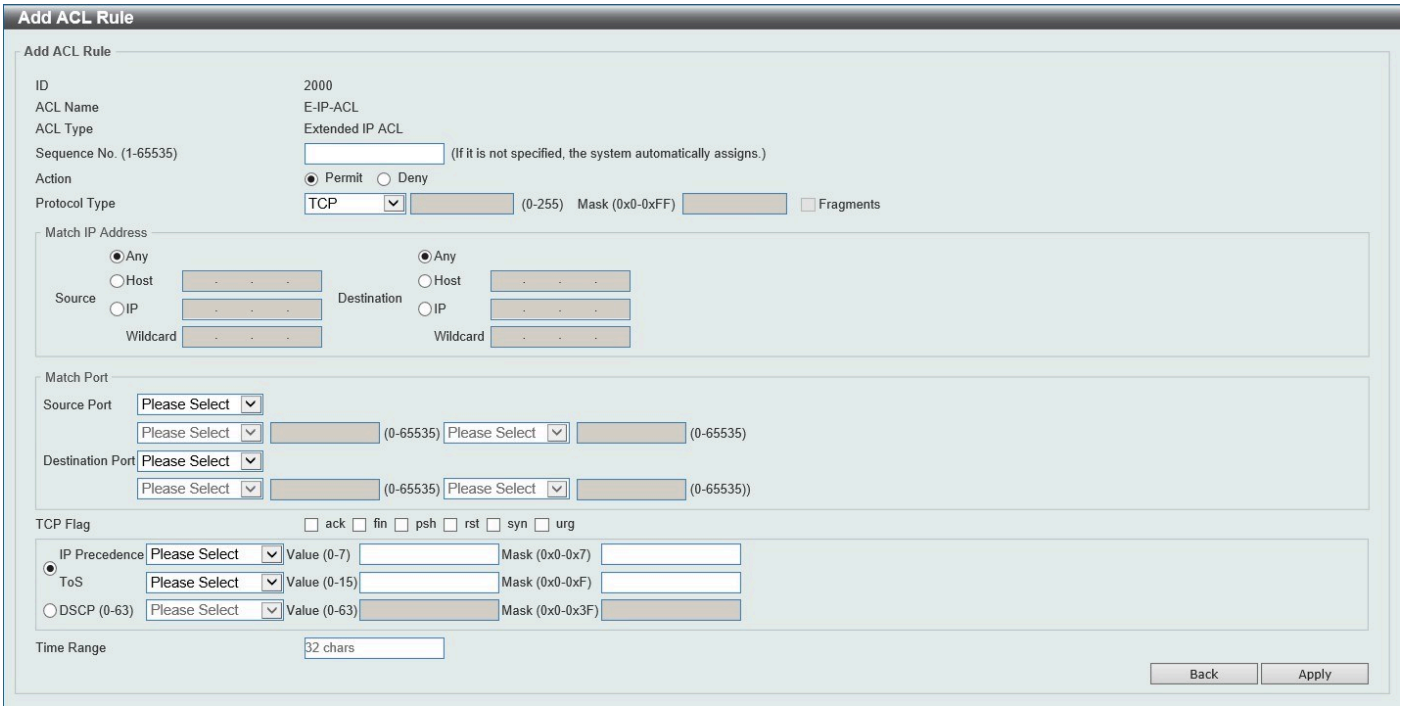


Figure 8-12 Extended IP ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the sequence number of this ACL rule here. The range is from 1 to 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are Permit, and Deny.
Protocol Type	Select the protocol type option here. Options to choose from are **TCP, UDP, ICMP, EIGRP** (88), **ESP** (50), **GRE** (47), **IGMP** (2), **OSPF** (89), **PIM** (103), **VRRP** (112), **IP-in-IP** (94), **PCP** (108), **Protocol ID**, and **None**. • **Value** - The protocol ID can also manually be entered here. The range is from 0 to 255. • **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 IP information here. Options to choose from are **Any, Host**, and **IP**. • When the **Any** option is selected, any source traffic will be evaluated according to the conditions of this rule. • When the **Host** option is selected, enter the source host IP address here. • When the **IP** option is selected, the **Wildcard** option will also be available. Enter the group of source IP addresses by using a wildcard bitmap (an inverted mask). The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.

Parameter	Description
Destination	Select and enter the destination IP information here. Options to choose from are **Any, Host,** and **IP**. • When the **Any** option is selected, any destination traffic will be evaluated according to the conditions of this rule. • When the **Host** option is selected, enter the destination host IP address here. • When the **IP** option is selected, the **Wildcard** option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap (an inverted mask). 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 if the selected protocol requires it. Options to choose from are **=, >, <, ≠, Range** and **Mask**. • When selecting the **=** option, the specific selected port number will be used. • When selecting the **>** option, all ports greater than the selected port, will be used. • When selecting the **<** option, all ports smaller than the selected port, will be used. • When selecting the **≠** option, all ports, excluding the selected port, will be used. • When selecting the **Range** option, the start port number and end port number selected for the respective service, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. • When selecting the **Mask** option, the specified source port number and mask will be used. Enter the source port mask value in the space provided. The range is from 0x0 to 0xFFFF. This parameter is only available in the protocol type **TCP** and **UDP**.
Destination Port	Select and enter the destination port value here if the selected protocol requires it. Options to choose from are **=, >, <, ≠, Range** and **Mask**. • When selecting the **=** option, the specific selected port number will be used. • When selecting the **>** option, all ports greater than the selected port, will be used. • When selecting the **<** option, all ports smaller than the selected port, will be used. • When selecting the **≠** option, all ports, excluding the selected port, will be used. • When selecting the **Range** option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. • When selecting the **Mask** option, the specified destination port number and mask will be used. Enter the destination port mask value in the space provided. The range is from 0x0 to 0xFFFF This parameter is only available in the protocol type **TCP** and **UDP**.
Specify ICMP Message Type	Select the ICMP message type used here. This parameter is only available in the protocol type **ICMP**.

Parameter	Description
ICMP Message Type	When the **ICMP Message Type** is not selected, enter the ICMP Message Type numerical value used here. The range is from 0 to 255. When the **ICMP Message Type** is selected, this numerical value will automatically be entered. This parameter is only available in the protocol type **ICMP**.
Message Code	When the **ICMP Message Type** is not selected, enter the Message Code numerical value used here. The range is from 0 to 255. When the **ICMP Message Type** is selected, this numerical value will automatically be entered. This parameter is only available in the protocol type **ICMP**.
TCP Flag	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are **ack, fin, psh, rst, syn**, and **urg**. This parameter is only available in the protocol type **TCP**.
IP Precedence	Select the IP precedence value used here. Options to choose from are **routine** (0), **priority** (1), **immediate** (2), **flash** (3), **flash-override** (4), **critical** (5), **internet** (6), and **network** (7). • **Value** - The IP precedence value can also manually be entered here. The range is from 0 to 7. • **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.
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. Refer to **System > Time** Range**.**

Click the **Apply** button to accept the changes made.

Click the **Back** button to discard the changes made and return to the previous page.

Standard IPv6 ACL

After selecting a Standard IPv6 ACL and clicking the **Add Rule** button, the following page will appear.

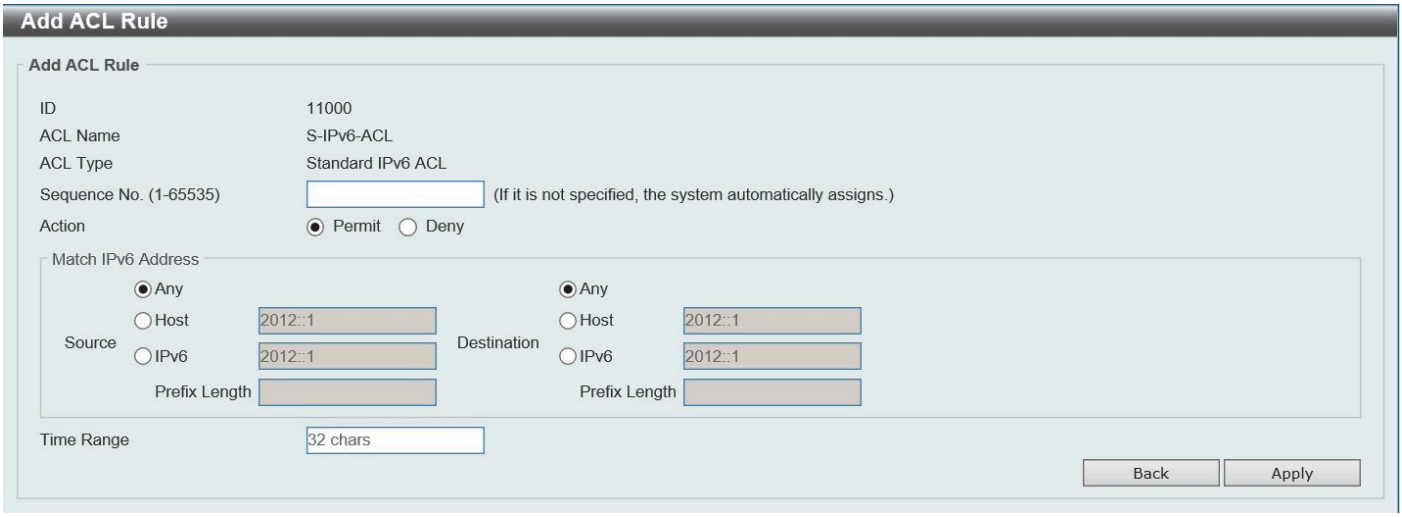


Figure 8-13 Standard IPv6 ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the sequence number of this ACL rule here. The range is from 1 to 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.
Source	Select and enter the source IPv6 information here. Options to choose from are **Any, Host, IPv6**, and **Prefix Length**. • When the **Any** option is selected, any source traffic will be evaluated according to the conditions of this rule. • When the **Host** option is selected, enter the source host IPv6 address here. • When the **IPv6** option is selected, the **Prefix Length** option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the source IPv6 information here. Options to choose from are **Any, Host, IPv6**, and **Prefix Length**. • When the **Any** option is selected, any source traffic will be evaluated according to the conditions of this rule. • When the **Host** option is selected, enter the source host IPv6 address here. • When the **IPv6** option is selected, the **Prefix Length** option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.
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. Refer to **System > Time** Range**.**

Click the **Apply** button to accept the changes made.

Click the **Back** button to discard the changes made and return to the previous page.

Extended IPv6 ACL

After selecting an Extended IPv6 ACL and clicking the **Add Rule** button, the following page will appear.

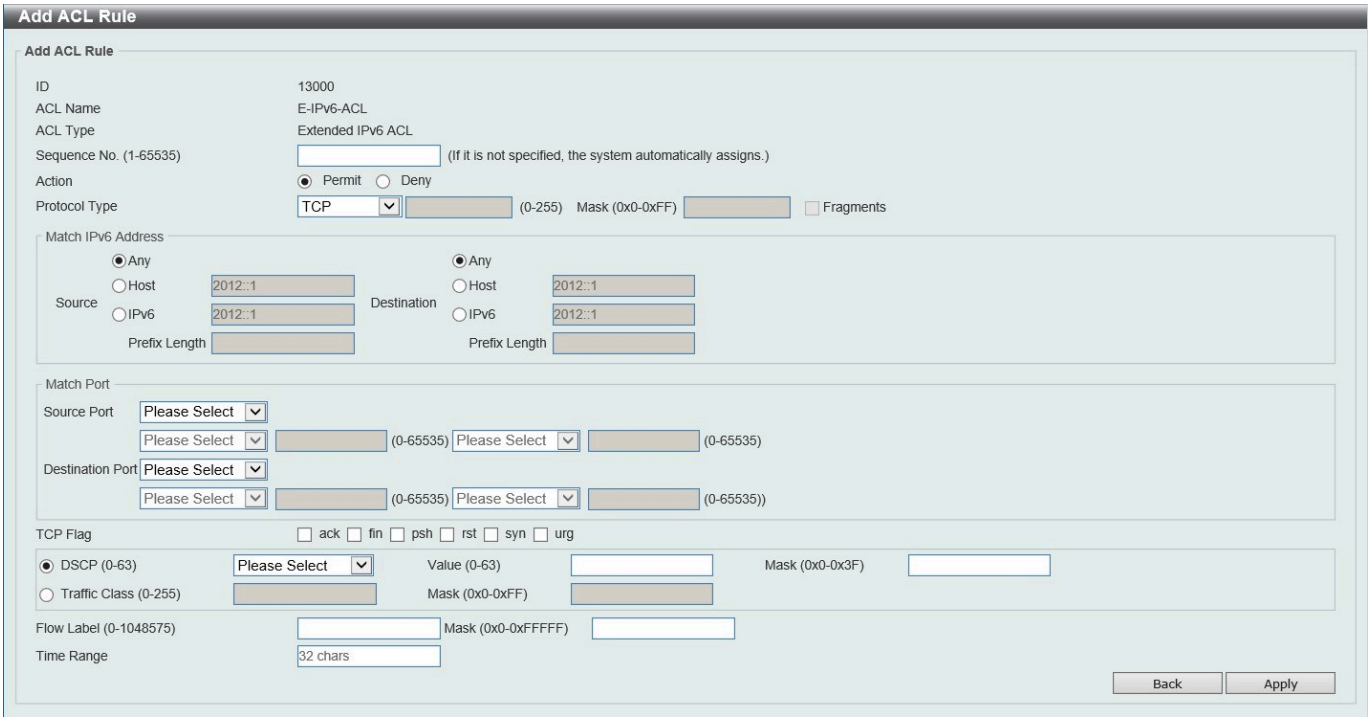


Figure 8-14 Extended IPv6 ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the sequence number of this ACL rule here. The range is from 1 to 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are **Permit**, and **Deny**.
Protocol Type	Select the protocol type option here. Options to choose from are **TCP, UDP, ICMP, Protocol ID, ESP** (50), **PCP** (108), **SCTP** (132), and **None**. • **Value** - The protocol ID can also manually be entered here. The range is from 0 to 255. • **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 IPv6 information here. Options to choose from are **Any, Host**, and **IPv6**. • When the **Any** option is selected, any source traffic will be evaluated according to the conditions of this rule. • When the **Host** option is selected, enter the source host IPv6 address here. • When the **IPv6** option is selected, the **Prefix Length** option will also be available. Enter the source IPv6 address and prefix length value in the spaces provided.

Parameter	Description
Destination	Select and enter the destination IPv6 information here. Options to choose from are **Any, Host,** and **IPv6**. • When the **Any** option is selected, any destination traffic will be evaluated according to the conditions of this rule. • When the **Host** option is selected, enter the destination host IPv6 address here. • When the **IPv6** option is selected, the **Prefix Length** option will also be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Source Port	Select and enter the source port value here. Options to choose from are **=, >, <, ≠, Range**, and **Mask**. • When selecting the **=** option, the specific selected port number will be used. • When selecting the **>** option, all ports greater than the selected port, will be used. • When selecting the **<** option, all ports smaller than the selected port, will be used. • When selecting the **≠** option, all ports, excluding the selected port, will be used. • When selecting the **Range** option, the start port number and end port number selected with respect to the selected service, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. • When selecting the **Mask** option, the specified source port number and mask will be used. Enter the source port mask value in the space provided. The range is from 0x0 to 0xFFFF. This parameter is only available in the protocol type **TCP** and **UDP**.
Destination Port	Select and enter the source port value here. Options to choose from are **=, >, <, ≠, Range**, and **Mask**. • When selecting the **=** option, the specific selected port number will be used. • When selecting the **>** option, all ports greater than the selected port, will be used. • When selecting the **<** option, all ports smaller than the selected port, will be used. • When selecting the **≠** option, all ports, excluding the selected port, will be used. • When selecting the **Range** option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. • When selecting the **Mask** option, the specified source port number and mask will be used. Enter the source port mask value in the space provided. The range is from 0x0 to 0xFFFF. This parameter is only available in the protocol type **TCP** and **UDP**.
TCP Flag	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are **ack, fin, psh, rst, syn**, and **urg**.

Parameter	Description
	This parameter is only available in the protocol type **TCP**.
Specify ICMP Message Type	Select the ICMP message type used here. This parameter is only available in the protocol type **ICMP**.
ICMP Message Type	When the **ICMP Message Type** is not selected, enter the ICMP Message Type numerical value used here. When the **ICMP Message Type** is selected, this numerical value will automatically be entered. This parameter is only available in the protocol type **ICMP**.
Message Code	When the **ICMP Message Type** is not selected, enter the ICMP Message Type numerical value used here. When the **ICMP Message Type** is selected, this numerical value will automatically be entered. This parameter is only available in the protocol type **ICMP**.
DSCP	Select the DSCP value that will be used here. Options to choose from are **default** (0), **af11** (10), **af12** (12), **af13** (14), **af21** (18), **af22** (20), **af23** (22), **af31** (26), **af32** (28), **af33** (30), **af41** (34), **af42** (36), **af43** (38), **cs1** (8), **cs2** (16), **cs3** (24), **cs4** (32), **cs5** (40), **cs6** (48), **cs7** (56), and **ef** (46). • **Value** - The DSCP value can also manually be entered here. The range is from 0 to 63. • **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. This value must be between 0 and 1048575. • **Mask** - Enter the flow label mask value 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. Refer to **System > Time** Range**.**

Click the **Apply** button to accept the changes made.

Click the **Back** button to discard the changes made and return to the previous page.

Extended MAC ACL

After selecting an Extended MAC ACL and clicking the **Add Rule** button, the following page will appear.

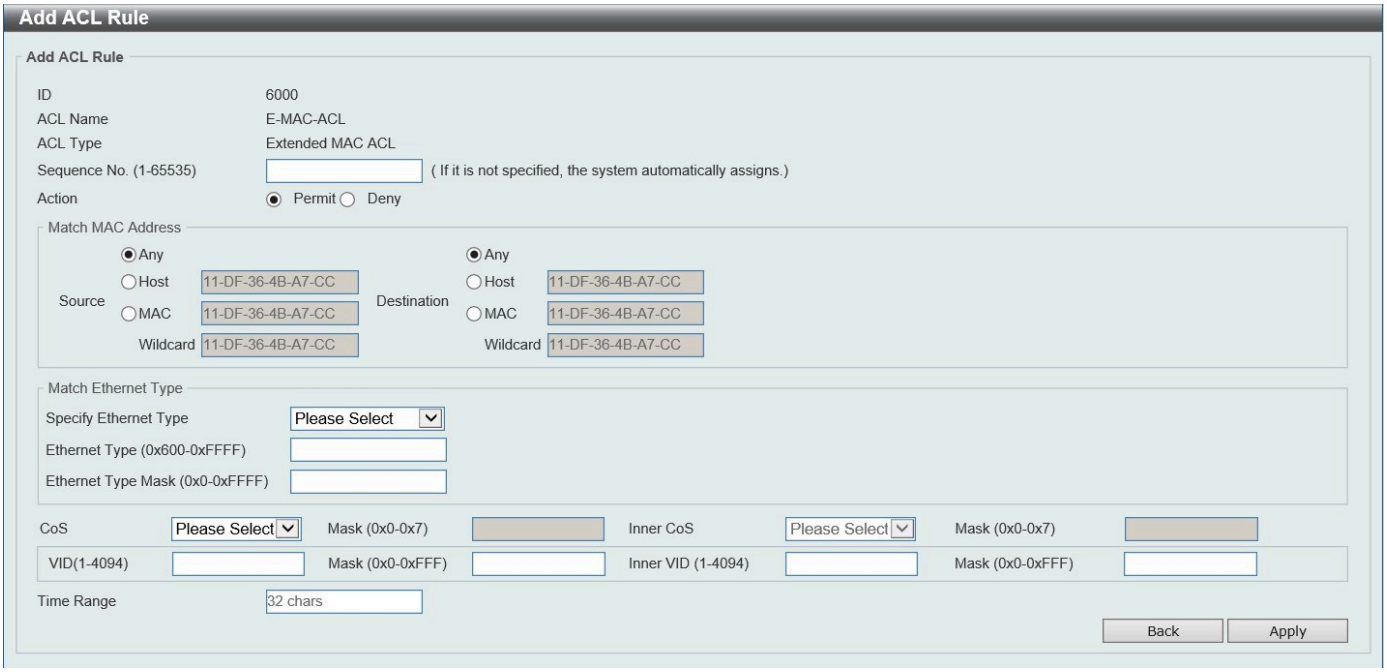


Figure 8-15 Extended MAC ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the sequence number of this ACL rule here. The range is from 1 to 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.
Source	Select and enter the source MAC address information here. Options to choose from are **Any, Host, MAC**, and **Wildcard**. When the **Any** option is selected, any source traffic will be evaluated according to the conditions of this rule. When the **Host** option is selected, enter the source host MAC address here. When the **MAC** option is selected, the **Wildcard** option will also be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination	Select and enter the destination MAC address information here. Options to choose from are **Any, Host, MAC**, and **Wildcard**. When the **Any** option is selected, any destination traffic will be evaluated according to the conditions of this rule. When the **Host** option is selected, enter the destination host MAC address here. When the **MAC** option is selected, the **Wildcard** option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
Specify Ethernet Type	Select the Ethernet type option here. Options to choose from are **aarp, appletalk, decent-iv, etype-6000, etype-8042, lat, lavc-sca, mop-console, mop-dump, vines-echo, vines-ip, xns-idp**, and **arp**.
Ethernet Type	Enter the Ethernet type hexadecimal value here. This value must be between 0x600 and 0xFFFF. When the Ethernet type profile is selected, above, the appropriate hexadecimal value will automatically be entered.

Parameter	Description
Ethernet Type Mask	Enter the Ethernet type mask hexadecimal value here. This value must be between 0x0 and 0xFFFF. When the Ethernet type profile is selected, above, the appropriate hexadecimal value will automatically be entered.
CoS	Select the CoS value that will be used here. The range is from 0 to 7. • **Mask** - Enter the CoS mask value here. The range is from 0x0 to 0x7.
Inner CoS	After selecting the CoS value, select the inner CoS value that will be used here. The range is from **0** to **7**. • **Mask** - Enter the inner CoS mask value here. The range is from 0x0 to 0x7.
VID	Enter the VLAN ID that will be associated with this ACL rule here. The range is from 1 to 4094. • **Mask** - Enter the VLAN ID mask value here. The range is from 0x0 to 0xFFF.
Inner VID	Enter the inner VLAN ID that will be associated with this ACL rule here. The range is from 1 to 4094. • **Mask** - Enter the inner 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. Refer to **System > Time** Range**.**

Click the **Apply** button to accept the changes made.

Click the **Back** button to discard the changes made and return to the previous page.

Extended Expert ACL

After selecting an Extended Expert ACL and clicking the **Add Rule** button, the following page will appear.

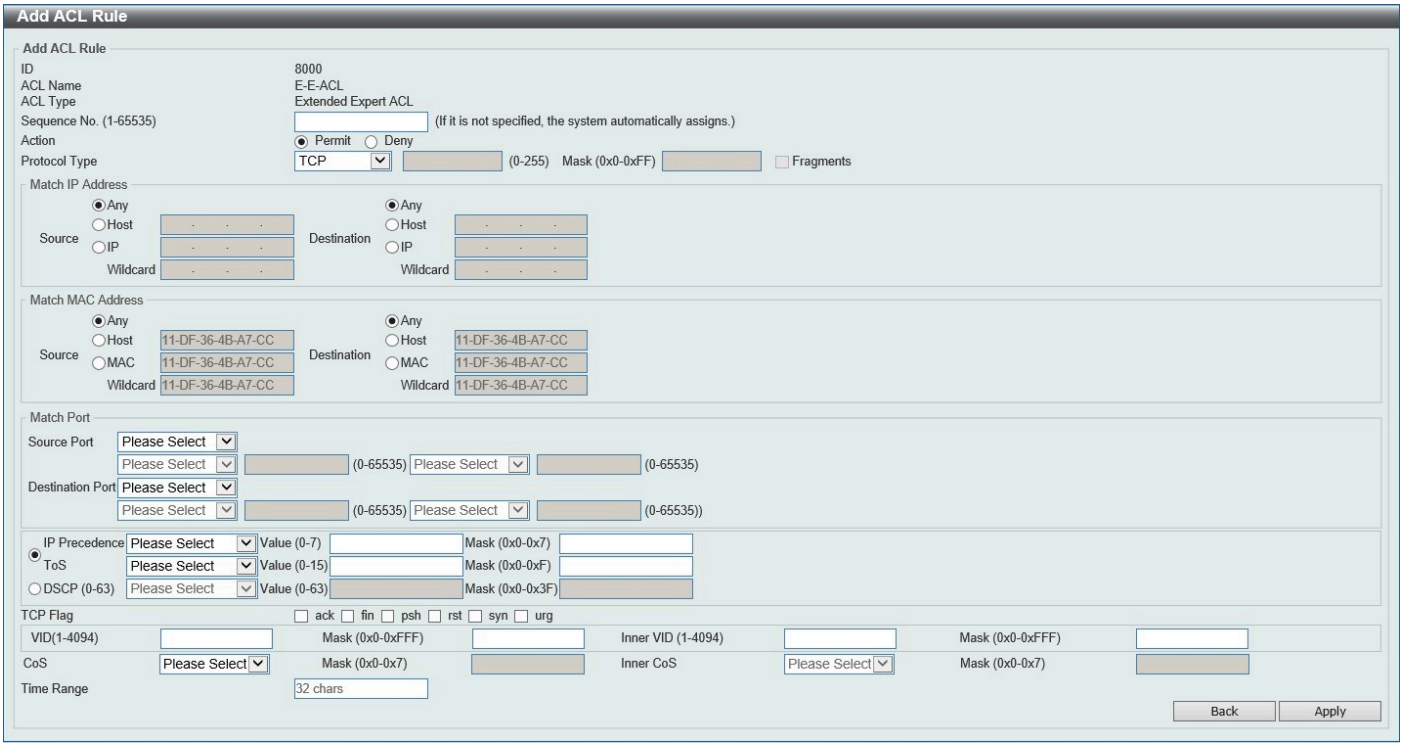


Figure 8-16 Extended Expert ACL (Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the sequence number of this ACL rule here. The range is from 1 to 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.
Protocol Type	Select the protocol type option here. Options to choose from are **TCP, UDP, ICMP, EIGRP** (88), **ESP** (50), **GRE** (47), **IGMP** (2), **OSPF** (89), **PIM** (103), **VRRP** (112), **IP-in-IP** (94), **PCP** (108), **Protocol ID**, and **None**. • **Value** - The protocol ID can also manually be entered here. The range is from 0 to 255. • **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 IP information here. Options to choose from are **Any, Host**, and **IP**. • When the **Any** option is selected, any source traffic will be evaluated according to the conditions of this rule. • When the **Host** option is selected, enter the source host IP address here. • When the **IP** option is selected, the **Wildcard** option will also be available. Enter the group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.

Parameter	Description
Destination	Select and enter the destination IP information here. Options to choose from are **Any, Host**, and **IP**. • When the **Any** option is selected, any destination traffic will be evaluated according to the conditions of this rule. • When the **Host** option is selected, enter the destination host IP address here. • When the **IP** option is selected, the **Wildcard** option will also be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source	Select and enter the source MAC address information here. Options to choose from are **Any, Host, MAC**, and **Wildcard**. • When the **Any** option is selected, any source traffic will be evaluated according to the conditions of this rule. • When the **Host** option is selected, enter the source host MAC address here. • When the **MAC** option is selected, the **Wildcard** option will also be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination	Select and enter the destination MAC address information here. Options to choose from are **Any, Host, MAC**, and **Wildcard**. • When the **Any** option is selected, any destination traffic will be evaluated according to the conditions of this rule. • When the **Host** option is selected, enter the destination host MAC address here. • When the **MAC** option is selected, the **Wildcard** option will also be available. Enter the destination MAC address and wildcard value in the spaces provided.
Source Port	Select and enter the source port value here. Options to choose from are **=, >, <, ≠, Range**, and **Mask**. • When selecting the **=** option, the specific selected port number will be used. • When selecting the **>** option, all ports greater than the selected port, will be used. • When selecting the **<** option, all ports smaller than the selected port, will be used. • When selecting the **≠** option, all ports, excluding the selected port, will be used. • When selecting the **Range** option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. • When selecting the **Mask** option, the specified source port number and mask will be used. Enter the source port mask value in the space provided. The range is from 0x0 to 0xFFFF. This parameter is only available in the protocol type **TCP** and **UDP**.
Destination Port	Select and enter the destination port value here. Options to choose from are **=, >, <, ≠, Range**, and **Mask**. • When selecting the **=** option, the specific selected port number will be used. • When selecting the **>** option, all ports greater than the selected port, will be used.

Parameter	Description
	• When selecting the **<** option, all ports smaller than the selected port, will be used. • When selecting the **≠** option, all ports, excluding the selected port, will be used. • When selecting the **Range** option, the start port number and end port number selected, of the range, will be used. Alternatively, the port number(s) can manually be entered in the space(s) provided, if the port number(s) is/are not available in the drop-down list. • When selecting the **Mask** option, the specified destination port number and mask will be used. Enter the destination port mask value in the space provided. The range is from 0x0 to 0xFFFF. This parameter is only available in the protocol type **TCP** and **UDP**.
Specify ICMP Message Type	Select the ICMP message type used here. This parameter is only available in the protocol type **ICMP**.
ICMP Message Type	When the **ICMP Message Type** is not selected, enter the ICMP Message Type numerical value used here. The range is from 0 to 255. When the **ICMP Message Type** is selected, this numerical value will automatically be entered. This parameter is only available in the protocol type **ICMP**.
Message Code	When the **ICMP Message Type** is not selected, enter the Message Code numerical value used here. The range is from 0 to 255. When the **ICMP Message Type** is selected, this numerical value will automatically be entered. This parameter is only available in the protocol type **ICMP**.
IP Precedence	Select the IP precedence value used here. Options to choose from are **routine** (0), **priority** (1), **immediate** (2), **flash** (3), **flash-soverride** (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	Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are **ack**, **fin**, **psh**, **rst**, **syn**, and **urg**. This parameter is only available in the protocol type **TCP**.
VID	Enter the VLAN ID that will be associated with this ACL rule 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
Inner VID	Enter the inner VLAN ID that will be associated with this ACL rule here. The range is from 1 to 4094. • **Mask** - Enter the inner VLAN ID mask value here. The range is from 0x0 to 0xFFF.
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.
Inner CoS	After selecting the CoS value, select the inner CoS value that will be used here. The range is from **0** to **7**. • **Mask** - Enter the inner 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. Refer to **System > Time** Range**.**

Click the **Apply** button to accept the changes made.

Click the **Back** button to discard the changes made and return to the previous page.

ACL Interface Access Group

This window is used to display and configure the ACL interface access group settings.

To view the following window, click **ACL > ACL Interface Access Group**, as shown below:

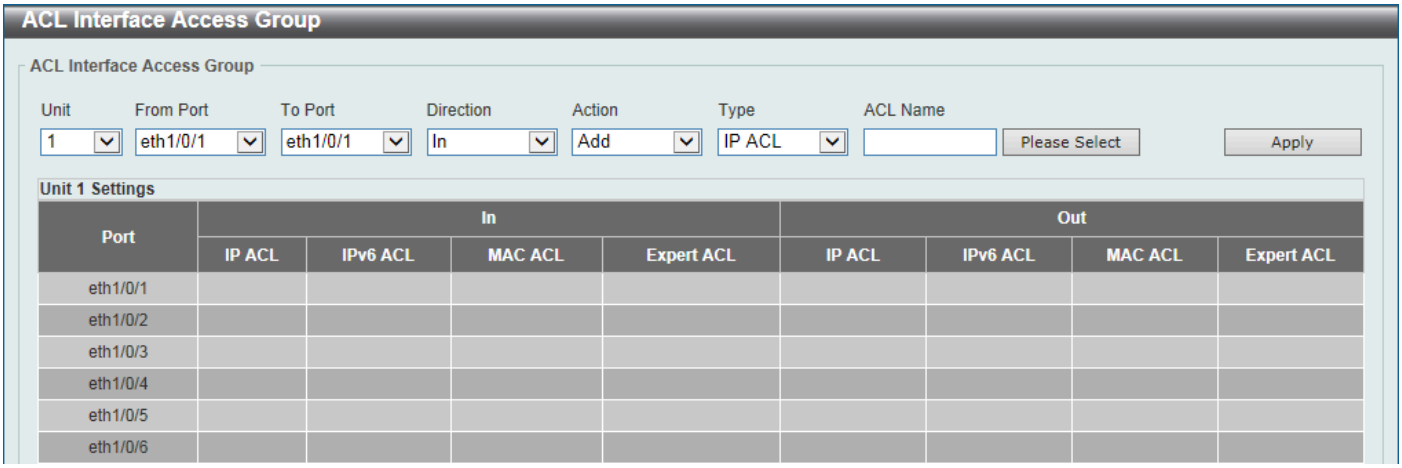


Figure 8-17 ACL Interface Access Group Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available if stacking is disabled.
From Port - To Port	Select the range of ports that will be used for this configuration 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**.

Parameter	Description
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.

After clicking the **Please Select** button, the following window will appear:

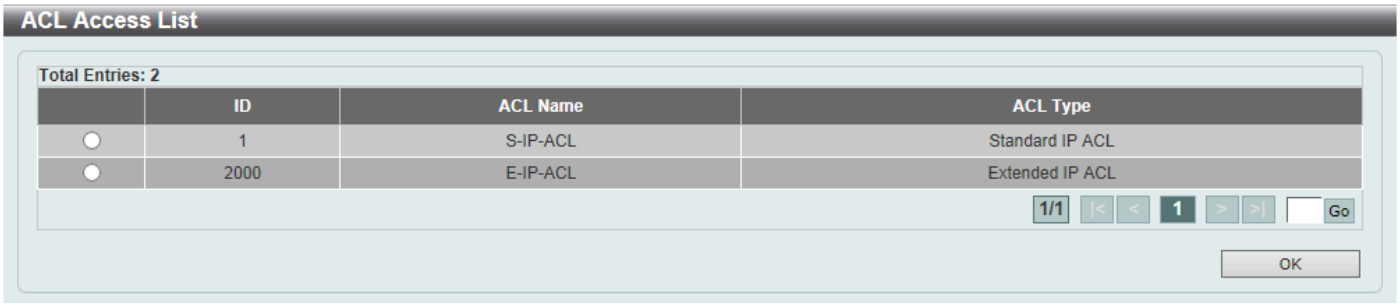


Figure 8-18 ACL Interface Access Group (Please Select) Window

Select the radio button next to the entry to use that ACL in the configuration.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **OK** button to accept the selection made.

ACL VLAN Access Map

This window is used to display and configure the ACL VLAN access map settings.

To view the following window, click **ACL > ACL VLAN Access Map**, as shown below:

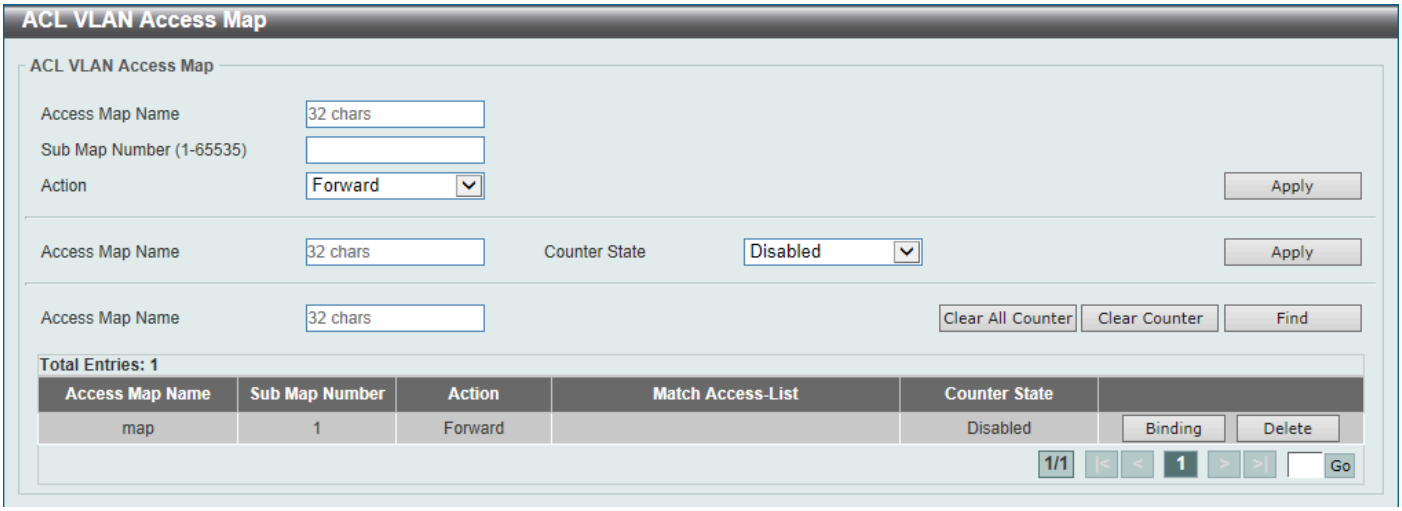


Figure 8-19 ACL VLAN Access Map Window

The fields that can be configured are described below:

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. This value must be between 1 and 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 counting of the number of times the access map has been matched.

Click the **Apply** button to accept the changes made.

Click the **Clear All Counter** button to clear the counter information for all the access maps.

Click the **Clear Counter** button to the clear the counter information for the specified access map.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Binding** button to match an access list to the ACL VLAN access map.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Binding** button, the following window will appear:

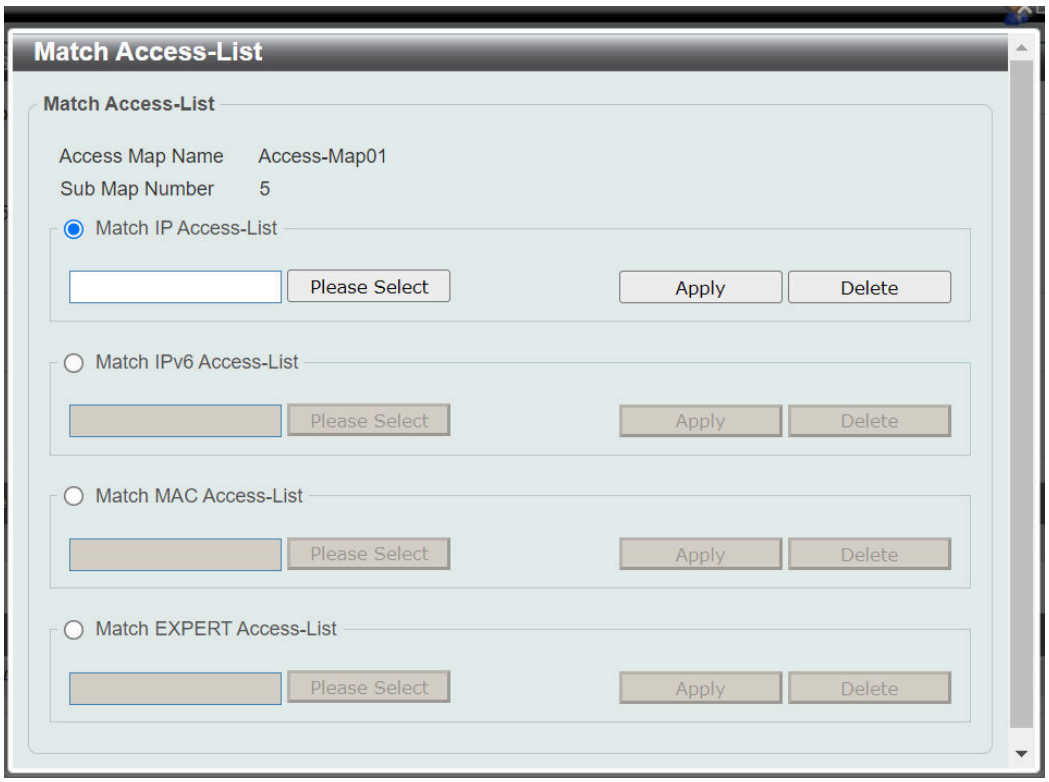


Figure 8-20 ACL VLAN Access Map (Binding) Window

The fields that can be configured are described below:

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.
Match EXPERT Access-List	Here the EXPERT access list that will be matched will be displayed.

Click the **Please Select** button navigate to a list of access lists that can be selected to be used in this configuration.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

After clicking the **Please Select** button, the following window will appear:

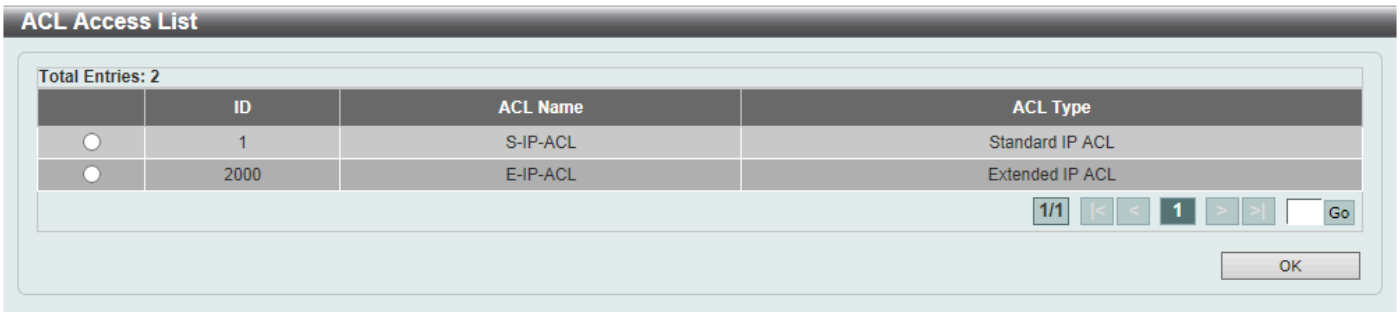


Figure 8-21 ACL VLAN Access Map (Binding, Selection) Window

Select the radio button next to the entry to use that access list in the configuration.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **OK** button to accept the selection made.

ACL VLAN Filter

This window is used to display and configure the ACL VLAN filter settings. It allows you to apply access list to a VLAN.

To view the following window, click **ACL > ACL VLAN Filter**, as shown below:



Figure 8-22 ACL VLAN Filter Window

The fields that can be configured are described below:

Parameter	Description
Access Map Name	Enter the access map name here. This name can be up to 32 characters long. Refer to **Access Control List > ACL VLAN Access Map**.
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**.
VID List	Enter the VLAN ID list that will be used here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

CPU ACL

This window is used to display and configure the CPU ACL settings.

To view the following window, click **ACL > CPU ACL**, as shown below:

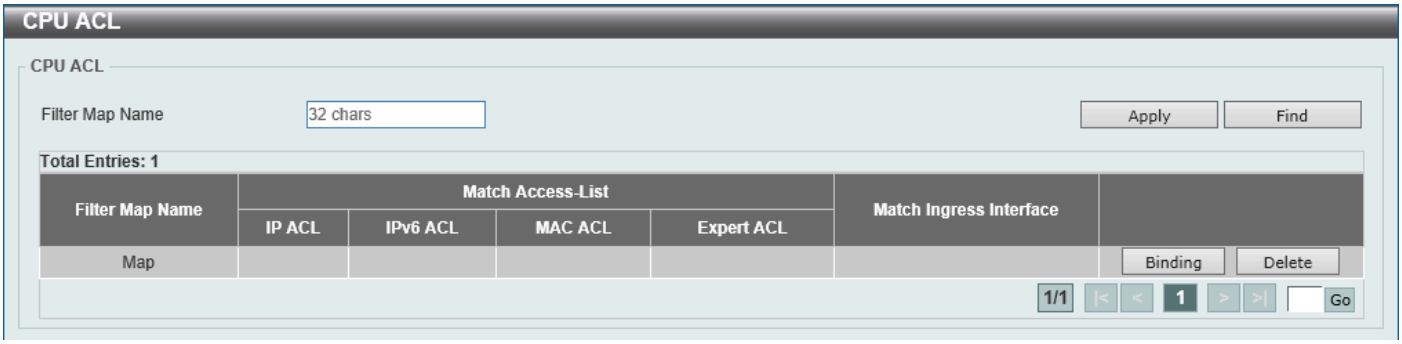


Figure 8-23 CPU ACL Window

The fields that can be configured are described below:

Parameter	Description
Filter Map Name	Enter the CPU ACL filter map name here. This name can be up to 32 characters long. Refer to **Access Control List > ACL VLAN Access Map**.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **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.

After clicking the **Binding** button, the following page will appear.

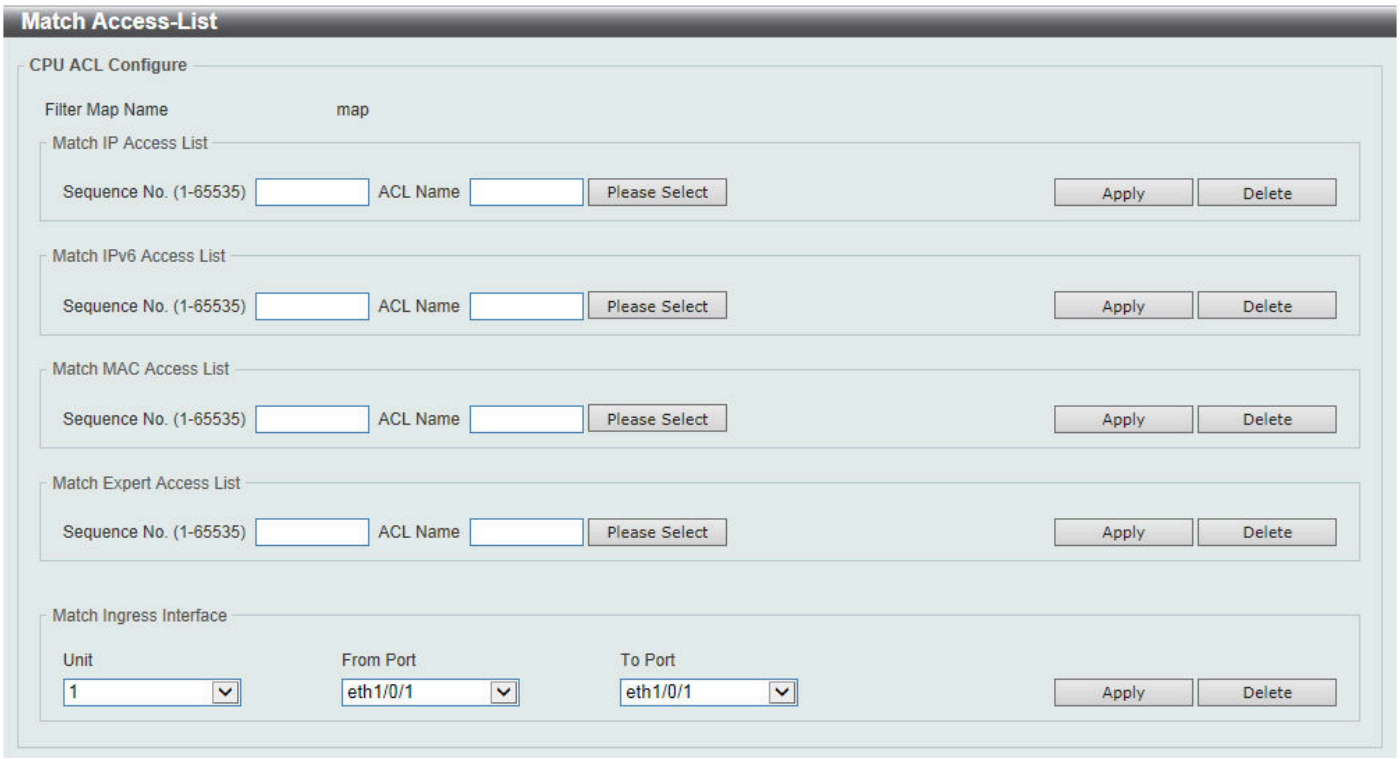


Figure 8-24 CPU ACL (Binding) Window

The fields that can be configured in **Match IP Access List** are described below:

Parameter	Description
Sequence No.	Enter the sequence number of the associated match entry here. The range is from 1 to 65535. The lower the number is, the higher the priority of the access list.
ACL Name	Enter the standard or extended IP access list name to be matched here. This name can be up to 32 characters long. Alternatively, click the **Please Select** button to select an existing ACL from the list.

After clicking the **Please Select** button, the following window will appear:

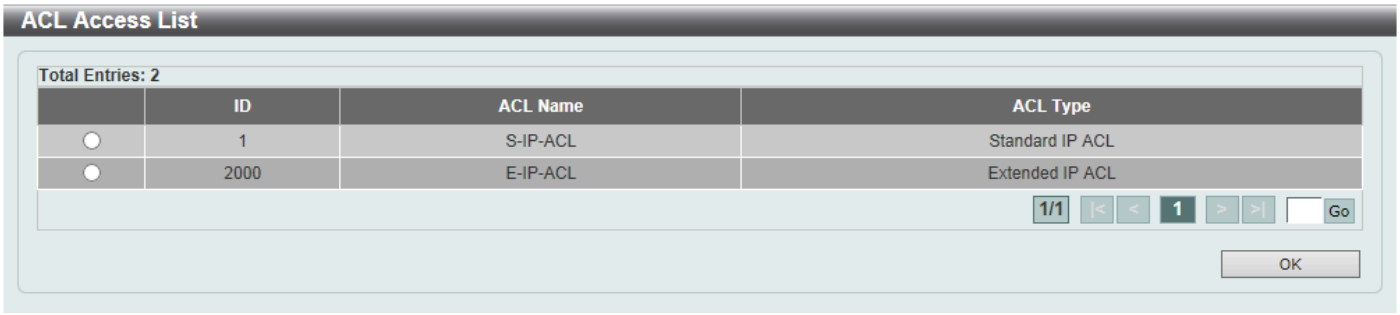


Figure 8-25 CPU ACL (Binding, Please Select) Window

The fields that can be configured are described below:

Parameter	Description
ACL List	Select the radio button next to the access list entry to use that access list in the configuration.

Select the ACL and click the **OK** button to accept the selection made.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete the specified entry.

The fields that can be configured in **Match IPv6 Access List** are described below:

Parameter	Description
Sequence No.	Enter the sequence number of the associated match entry here. The range is from 1 to 65535. The lower the number is, the higher the priority of the access list.
ACL Name	Enter the standard or extended IPv6 access list name to be matched here. This name can be up to 32 characters long. Alternatively, click the **Please Select** button to select an existing ACL from the list.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete the specified entry.

The fields that can be configured in **Match MAC Access List** are described below:

Parameter	Description
Sequence No.	Enter the sequence number of the associated match entry here. The range is from 1 to 65535. The lower the number is, the higher the priority of the access list.
ACL Name	Enter the extended MAC access list name to be matched here. This name can be up to 32 characters long. Alternatively, click the **Please Select** button to select an existing ACL from the list.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete the specified entry.

The fields that can be configured in **Match Expert Access List** are described below:

Parameter	Description
Sequence No.	Enter the sequence number of the associated match entry here. The range is from 1 to 65535. The lower the number is, the higher the priority of the access list.
ACL Name	Enter the extended expert access list name to be matched here. This name can be up to 32 characters long. Alternatively, click the **Please Select** button to select an existing ACL from the list.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete the specified entry.

The fields that can be configured in **Match Ingress Interface** are described below:

Parameter	Description
Unit	Select the Switch unit ID that will be used here.
From Port - To Port	Select the Switch port range that will be used here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete the specified entry.

9. Security

Port Security
802.1X
AAA
RADIUS
TACACS
IMPB
DHCP Server Screening
ARP Spoofing Prevention
BPDU Attack Protection
MAC Authentication
Web-based Access Control
Network Access Authentication
Safeguard Engine
Trusted Host
Traffic Segmentation Settings
Storm Control
DoS Attack Prevention Settings
SSH
SSL
SFTP Server Settings
Network Protocol Port Protect

Port Security

Port security prevents authorized access to the network by restricting connections to a port.

Port Security Global Settings

This window is used to display and configure the global port security settings. Port Security is a security feature that prevents unauthorized computers (with source MAC addresses) unknown to the Switch prior to locking the port (or ports) from connecting to the Switch's locked ports and gaining access to the network.

To view the following window, click **Security > Port Security > Port Security Global Settings**, as shown below:

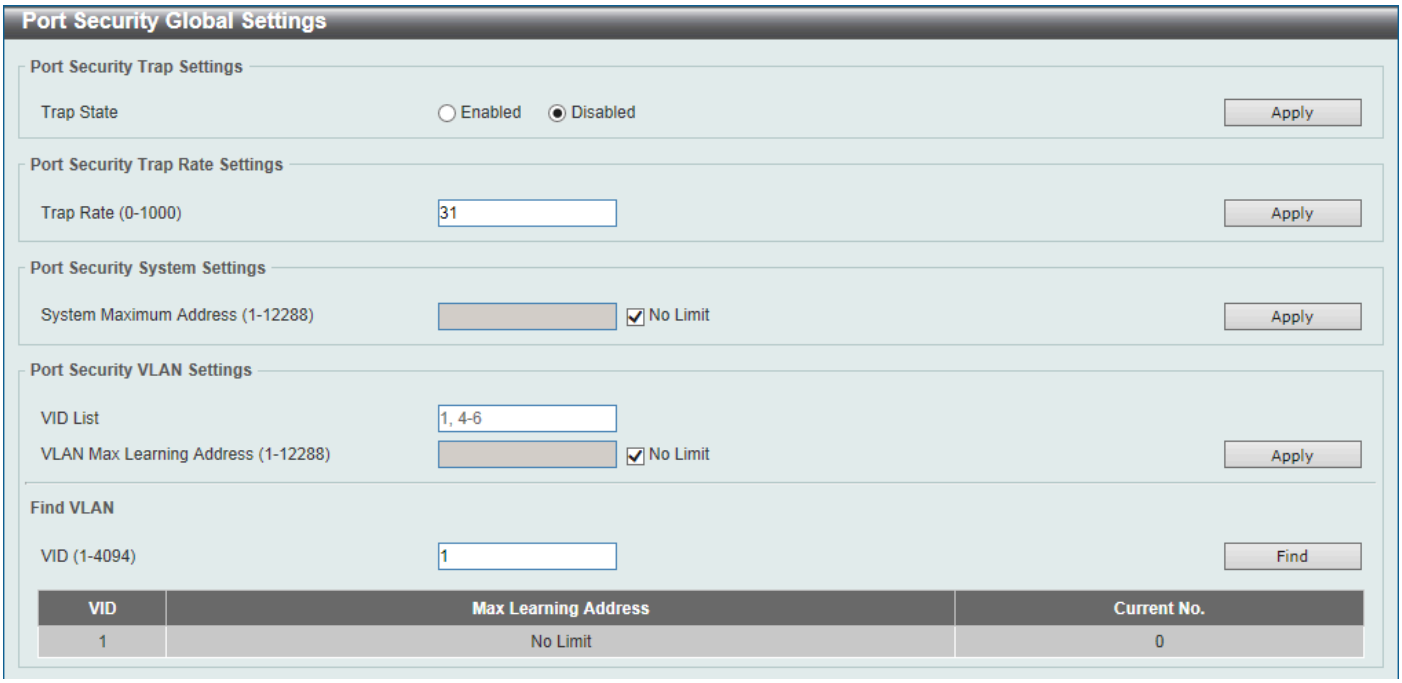


Figure 9-1 Port Security Global Settings Window

The fields that can be configured in **Port Security Trap Settings** are described below:

Parameter	Description
Trap State	Select to enable or disable port security traps on the Switch.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Port Security Trap Rate Settings** are described below:

Parameter	Description
Trap Rate	Enter the number of traps per second. The range is from 0 to 1000. The default value 31 indicates an SNMP trap to be generated for every security violation.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Port Security System Settings** are described below:

Parameter	Description
System Maximum Address	Enter the maximum number of secure MAC addresses allowed. If not specified, the default value is No Limit. The valid range is from 1 to 12288. Tick the **No Limit** checkbox to allow the maximum number of secure MAC address.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Port Security VLAN Settings** are described below:

Parameter	Description
VID List	Enter the VLAN ID(s) here. Use "-" to specify a range of ports and "," to separate multiple ports.
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 12288. Tick the **No Limit** checkbox to allow the maximum number of secure MAC address.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Find VLAN** are described below:

Parameter	Description
VID	Enter the VLAN ID that will be located here.

Click the **Find** button to locate a specific entry based on the information entered.

Port Security Port Settings

This window is used to display and configure the port security port settings.

To view the following window, click **Security > Port Security > Port Security Port Settings**, as shown below:

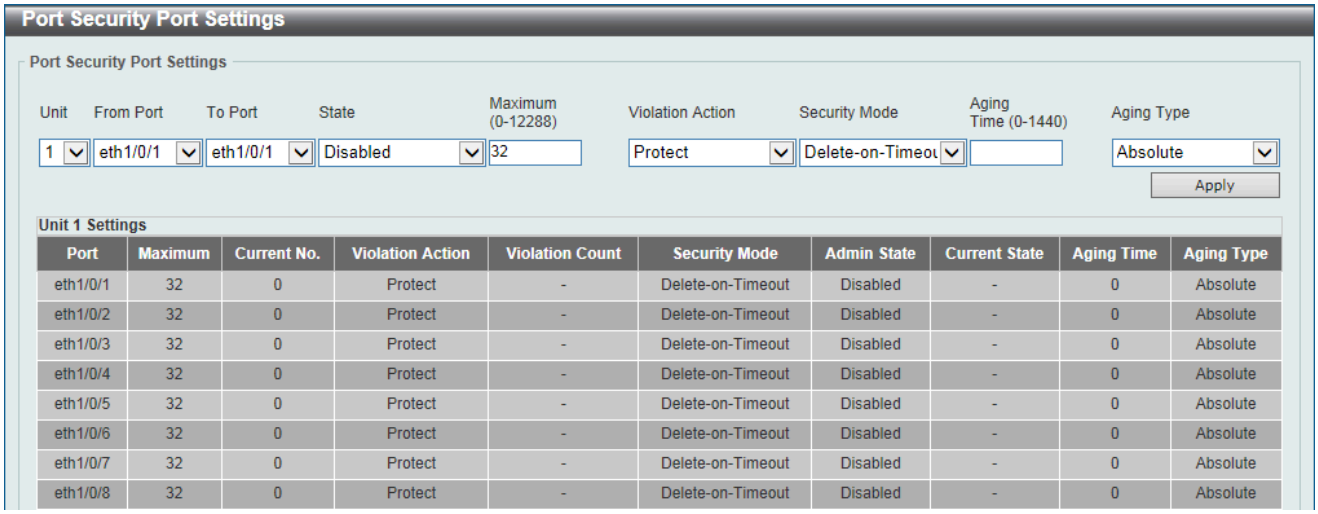


Figure 9-2 Port Security Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the port security feature on the port(s) specified.
Maximum	Enter the maximum number of secure MAC addresses that will be allowed on the port(s) specified. This value must be between 0 and 64. By default, this value is 32.
Violation Action	Select the violation action that will be taken here. Options to choose from are **Protect**, **Restrict**, and **Shutdown**. • Selecting **Protect** specifies to drop all packets from the insecure hosts at the port-security process level but does not increment the security-violation count. • Selecting **Restrict** specifies to drop all packets from the insecure hosts at the port-security process level and increment the security-violation count and record the system log. • Selecting **Shutdown** specifies to shut down the port if there is a security violation and record the system log.
Security Mode	Select the security mode option here. Options to choose from are **Permanent** and **Delete-on-Timeout**. • Selecting **Permanent** specifies that under this mode, all learned MAC addresses will not be purged out unless the user manually deletes those entries. • Selecting **Delete-on-Timeout** specifies that under this mode, 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. This value must be between 0 and 1440 minutes.
Aging Type	Select the aging type here. Options to choose from are **Absolute** and **Inactivity**. • Selecting **Absolute** specifies that all the secure addresses on this port age out exactly after the time specified and is removed from the secure address list. This is the default type. • Selecting **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 time period.

Parameter	Description
NOTE: You can configure errdisable trap and recovery settings in **System > Port Configuration > Error Disable Settings**.	

Click the **Apply** button to accept the changes made.

Port Security Address Entries

This window is used to view, clear and configure the port security address entries.

To view the following window, click **Security > Port Security > Port Security Address Entries**, as shown below:

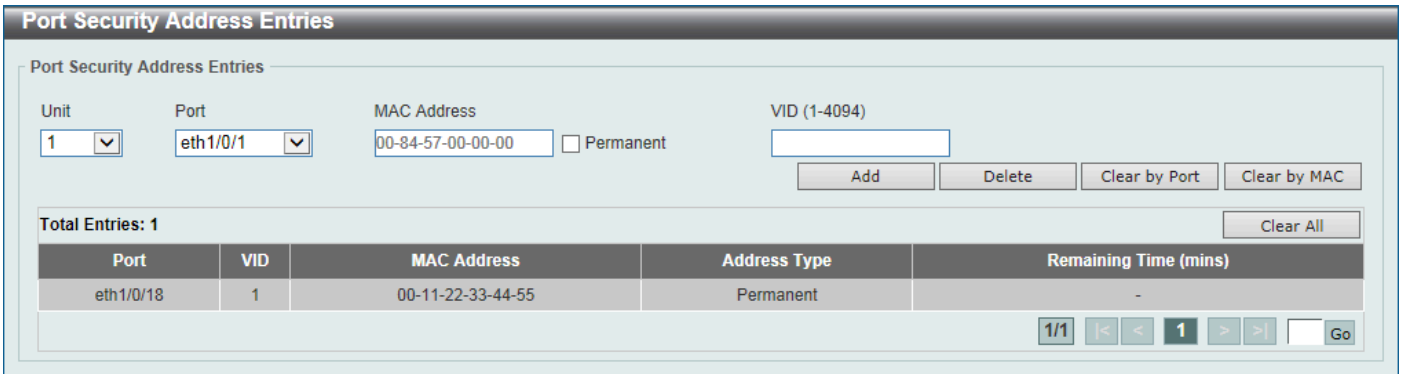


Figure 9-3 Port Security Address Entries Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available if stacking is enabled.
Port	Select the appropriate port range used for the configuration here.
MAC Address	Enter the MAC address here. Select the **Permanent** option to specify that all learned MAC addresses will not be purged out unless the user manually deletes those entries.
VID	Enter the VLAN ID here. This value must be between 1 and 4094.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove a new entry based on the information entered.

Click the **Clear by Port** button to clear the information based on the port selected.

Click the **Clear by MAC** button to clear the information based on the MAC address entered.

Click the **Clear All** button to clear all the information in this table.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

802.1X

802.1X (Port-based and Host-based Access Control)

The IEEE 802.1X standard is a security measure for authorizing and authenticating users to gain access to various wired or wireless devices on a specified Local Area Network by using a Client and Server based access control model. This is accomplished by using a RADIUS server to authenticate users trying to access a network by relaying Extensible Authentication Protocol over LAN (EAPOL) packets between the Client and the Server.

The following figure represents a basic EAPOL packet:

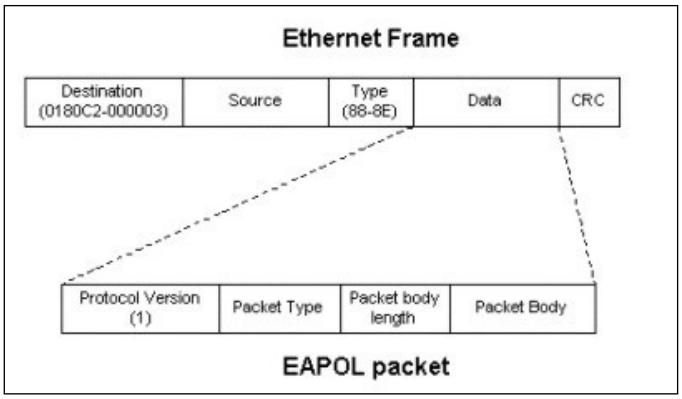


Figure 9-4 The EAPOL Packet

Utilizing this method, unauthorized devices are restricted from connecting to a LAN through a port to which the user is connected. EAPOL packets are the only traffic that can be transmitted through the specific port until authorization is granted. The 802.1X access control method has three roles, each of which are vital to creating and up keeping a stable and working Access Control security method.

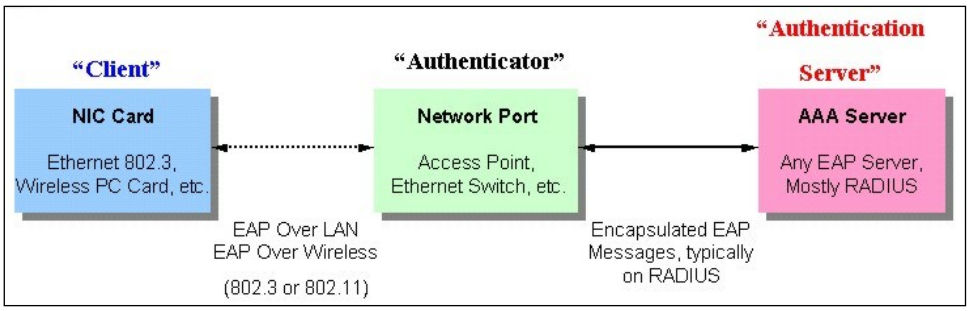


Figure 9-5 The three roles of 802.1X

The following section will explain the three roles of Client, Authenticator and Authentication Server in greater detail.

Authentication Server

The Authentication Server is a remote device that is connected to the same network as the Client and Authenticator, must be running a RADIUS Server program and must be configured properly on the Authenticator (Switch). Clients connected to a port on the Switch must be authenticated by the Authentication Server (RADIUS) before attaining any services offered by the Switch on the LAN. The role of the Authentication Server is to certify the identity of the Client attempting to access the network by exchanging secure information between the RADIUS server and the Client through EAPOL packets and, in turn, informs the Switch whether or not the Client is granted access to the LAN and/or Switches services.

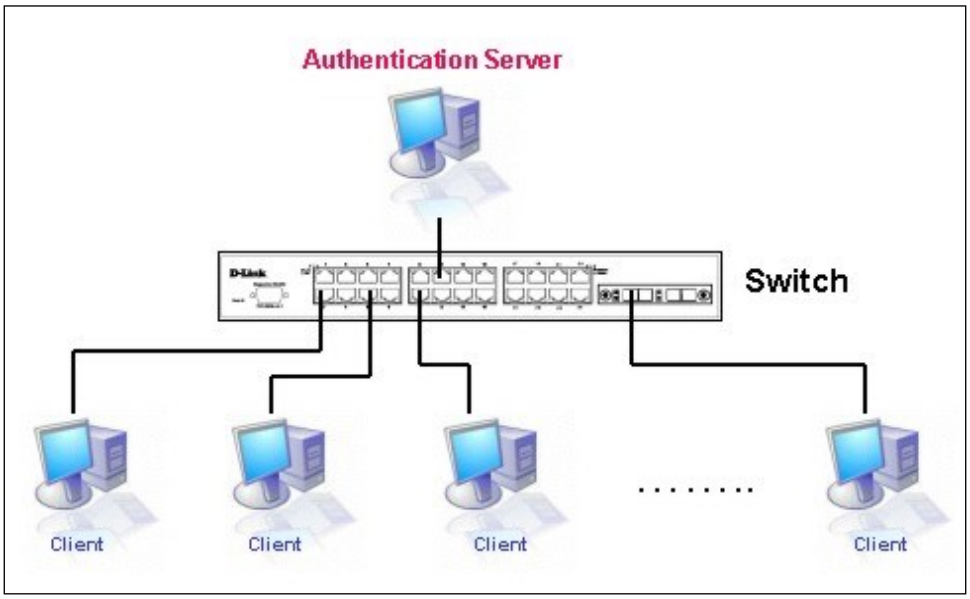


Figure 9-6 The Authentication Server

Authenticator

The Authenticator (the Switch) is an intermediary between the Authentication Server and the Client. The Authenticator serves two purposes when utilizing the 802.1X function. The first purpose is to request certification information from the Client through EAPOL packets, which is the only information allowed to pass through the Authenticator before access is granted to the Client. The second purpose of the Authenticator is to verify the information gathered from the Client with the Authentication Server, and to then relay that information back to the Client.

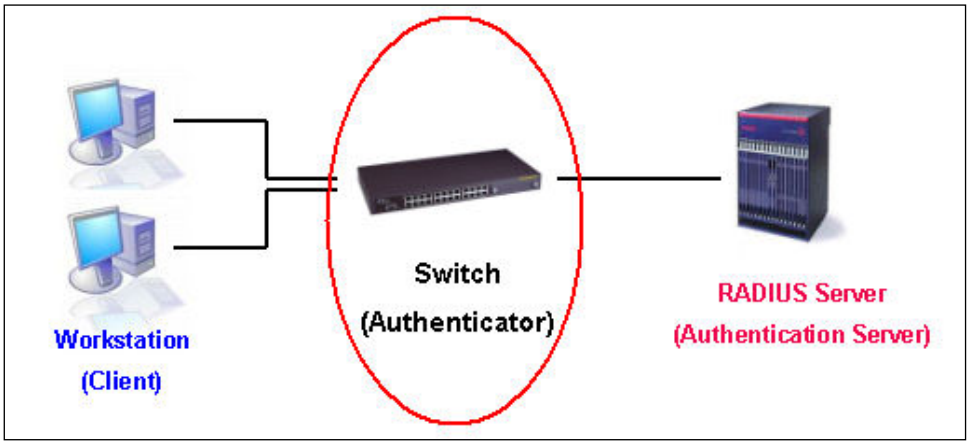


Figure 9-7 The Authenticator

Three steps must be implemented on the Switch to properly configure the Authenticator.

- The 802.1X State must be Enabled. (**Security > 802.1X > 802.1X Global Settings**)
- The 802.1X settings must be implemented by port (**Security > 802.1X > 802.1X Port Settings**)
- A RADIUS server must be configured on the Switch. (**Security > RADIUS > RADIUS Server Settings**)

Client

The Client is simply the end station that wishes to gain access to the LAN or Switch services. All end stations must be running software that is compliant with the 802.1X protocol. For users running Windows 7 and later, that software is included within the operating system. All other users are required to attain 802.1X client software from an outside

source. The Client will request access to the LAN and or Switch through EAPOL packets and, in turn will respond to requests from the Switch.

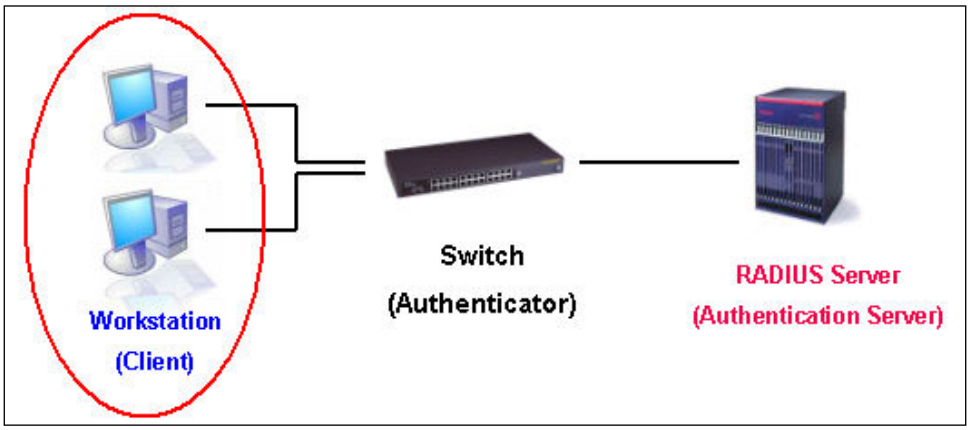


Figure 9-8 The Client

Authentication Process

Utilizing the three roles stated above, the 802.1X protocol provides a stable and secure way of authorizing and authenticating users attempting to access the network. Only EAPOL traffic is allowed to pass through the specified port before a successful authentication is made. This port is “locked” until the point when a Client with the correct username and password (and MAC address if 802.1X is enabled by MAC address) is granted access and therefore successfully “unlocks” the port. Once the port is unlocked, normal traffic is allowed to pass through the port. The following figure displays a more detailed explanation of how the authentication process is completed between the three roles stated above.

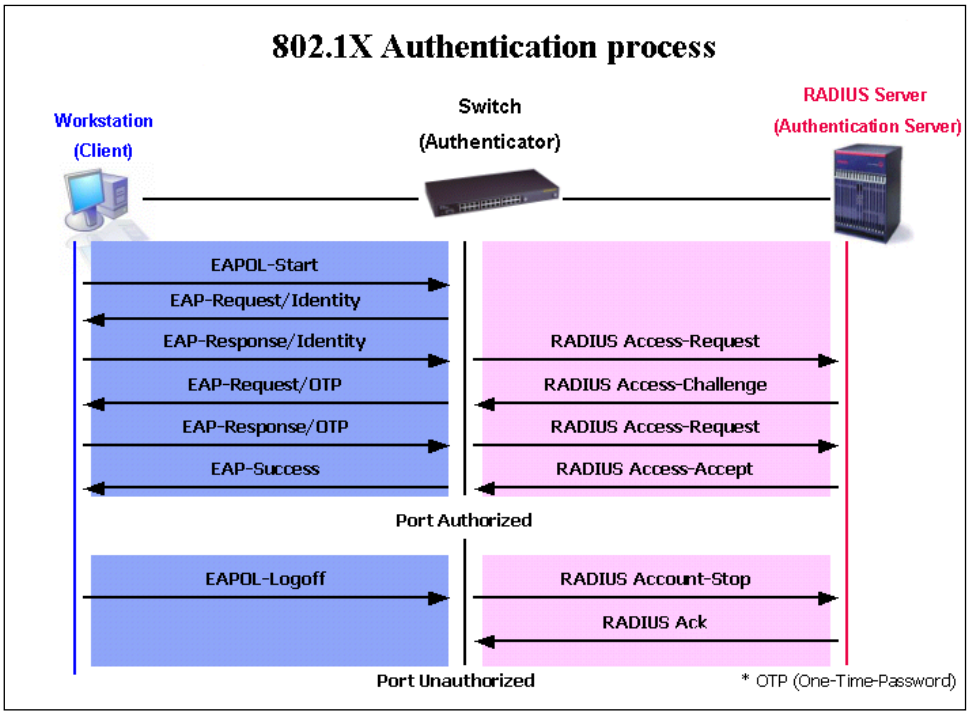


Figure 9-9 The 802.1X Authentication Process

The D-Link implementation of 802.1X allows network administrators to choose between two types of Access Control used on the Switch, which are:

- **Port-based Access Control** - This method requires only one user to be authenticated per port by a remote RADIUS server to allow the remaining users on the same port access to the network.
- **Host-based Access Control** - Using this method, the Switch will automatically learn up to a maximum of 1000 MAC addresses by port and set them in a list. Each MAC address must be authenticated by the Switch using a remote RADIUS server before being allowed access to the Network.

Understanding 802.1X Port-based and Host-based Network Access Control

The original intent behind the development of 802.1X was to leverage the characteristics of point-to-point in LANs. As any single LAN segment in such infrastructures has no more than two devices attached to it, one of which is a Bridge Port. The Bridge Port detects events that indicate the attachment of an active device at the remote end of the link, or an active device becoming inactive. These events can be used to control the authorization state of the Port and initiate the process of authenticating the attached device if the Port is unauthorized. This is the Port-based Network Access Control.

Port-based Network Access Control

Once the connected device has successfully been authenticated, the Port then becomes Authorized, and all subsequent traffic on the Port is not subject to access control restriction until an event occurs that causes the Port to become Unauthorized. Hence, if the Port is actually connected to a shared media LAN segment with more than one attached device, successfully authenticating one of the attached devices effectively provides access to the LAN for all devices on the shared segment. Clearly, the security offered in this situation is open to attack.

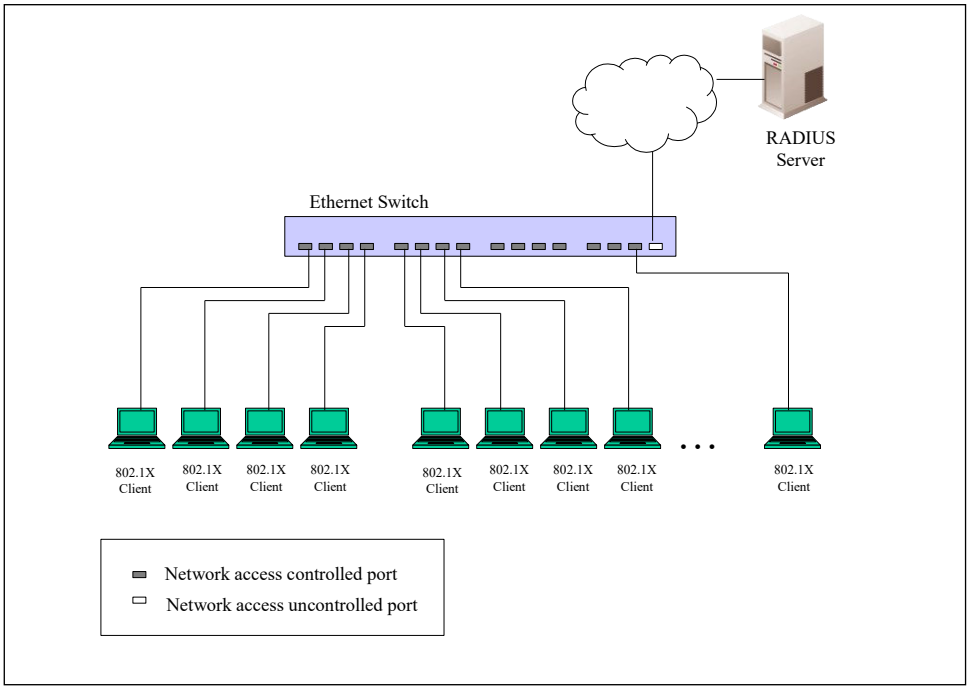


Figure 9-10 Example of Typical Port-based Configuration

Host-based Network Access Control

In order to successfully make use of 802.1X in a shared media LAN segment, it would be necessary to create “logical” Ports, one for each attached device that required access to the LAN. The Switch would regard the single physical Port connecting it to the shared media segment as consisting of a number of distinct logical Ports, each logical Port being independently controlled from the point of view of EAPOL exchanges and authorization state. The Switch learns each attached devices’ individual MAC addresses, and effectively creates a logical Port that the attached device can then use to communicate with the LAN via the Switch.

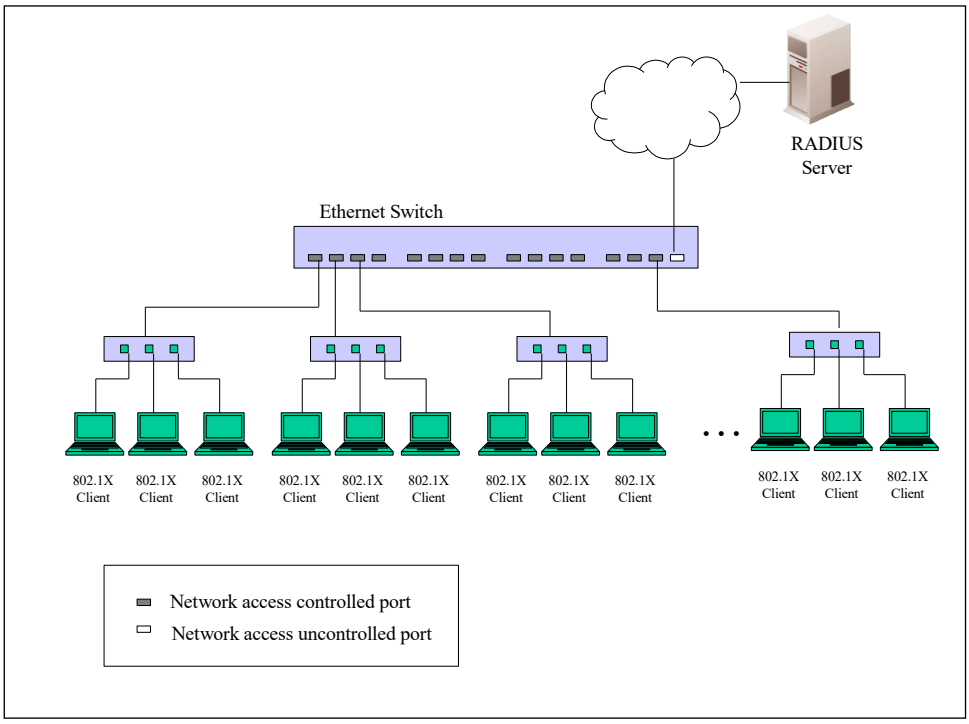


Figure 9-11 Example of Typical Host-based Configuration

802.1X Global Settings

This window is used to display and configure the global 802.1X settings.

To view the following window, click **Security > 802.1X > 802.1X Global Settings**, as shown below:

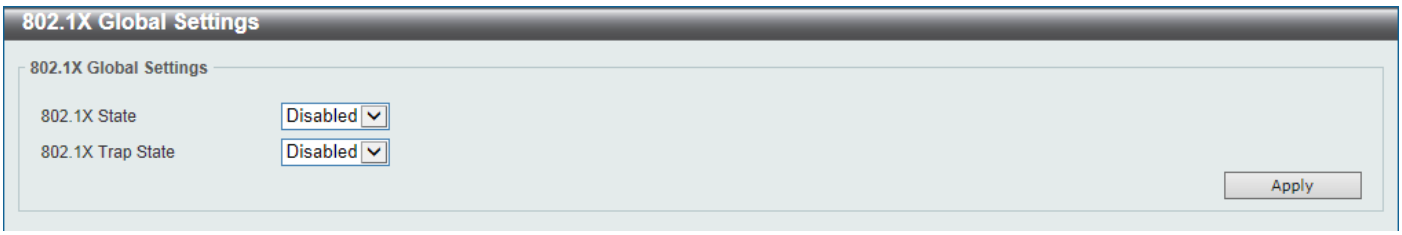


Figure 9-12 802.1X Global Settings Window

The fields that can be configured are described below:

Parameter	Description
802.1X State	Select to enable or disable the global 802.1X state here.
802.1X Trap State	Select to enable or disable the 802.1X trap state here.

Click the **Apply** button to accept the changes made.

802.1X Port Settings

This window is used to display and configure the 802.1X port settings.

To view the following window, click **Security > 802.1X > 802.1X Port Settings**, as shown below:

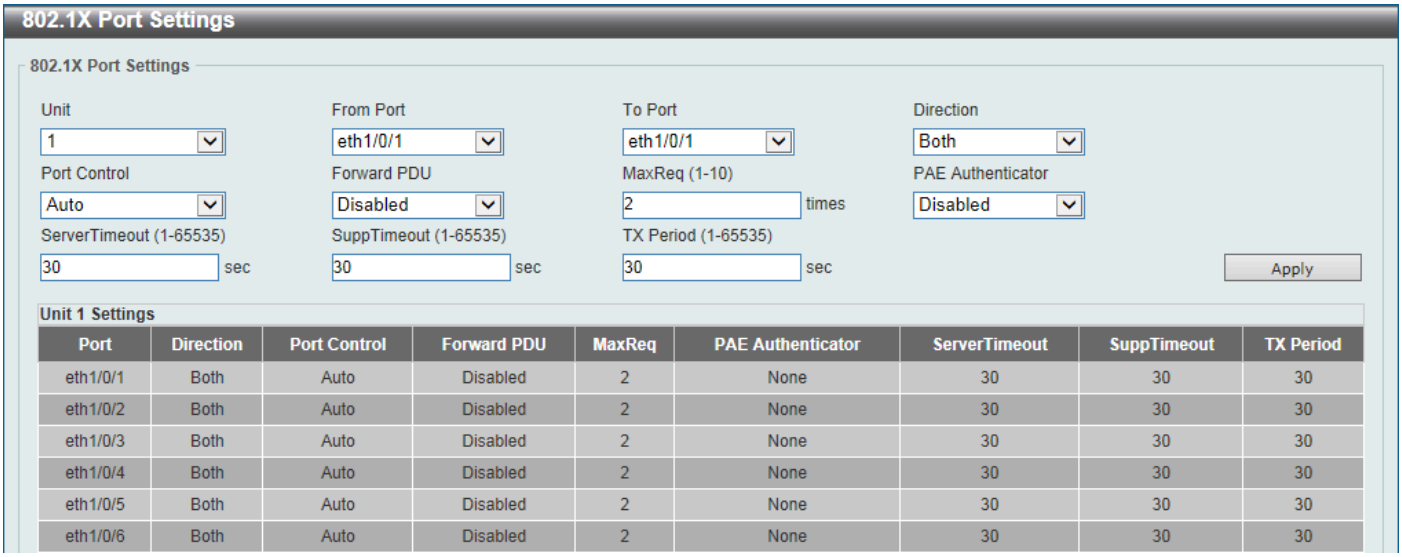


Figure 9-13 802.1X Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
Direction	Select the direction here. Options to choose from are **Both** and **In**. This option configures the direction of the traffic on a controlled port as unidirectional (**In**) or bidirectional (**Both**).
Port Control	Select the port control option here. Options to choose from are **ForceAuthorized**, **Auto**, and **ForceUnauthorized**. If the port control is set to force-authorized, then the port is not controlled in both directions. If the port control is set to automatic, then the access to the port for the controlled direction needs to be authenticated. If the port control is set to force-unauthorized, then the access to the port for the controlled direction is blocked.
Forward PDU	Select to enable or disable the forward PDU option here.
MaxReq	Enter the maximum required times value here. This value must be between 1 and 10. By default, this option is 2. This option configures the maximum number of times that the backend authentication state machine will retransmit an Extensible Authentication Protocol (EAP) request frame to the supplicant before restarting the authentication process.
PAE Authenticator	Select to enable or disable the PAE authenticator option here. This option configures a specific port as an IEEE 802.1X port access entity (PAE) authenticator.
Server Timeout	Enter the server timeout value here. This value must be between 1 and 65535 seconds. By default, this value is 30 seconds.
SuppTimeout	Enter the supplicant timeout value here. This value must be between 1 and 65535 seconds. By default, this value is 30 seconds.
TX Period	Enter the transmission period value here. This value must be between 1 and 65535 seconds. By default, this value is 30 seconds.

Click the **Apply** button to accept the changes made.

Authentication Sessions Information

This window is used to display and configure the authentication session information.

To view the following window, click **Security > 802.1X > Authentication Sessions Information**, as shown below:

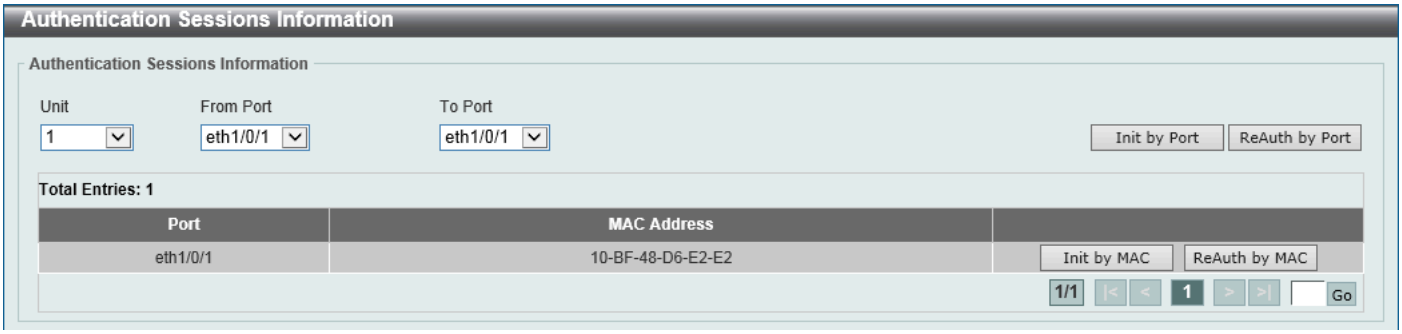


Figure 9-14 Authentication Sessions Information Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.

Click the **Init by Port** button to initiate the session information based on the port selections made.

Click the **ReAuth by Port** button to re-authenticate the session information based on the port selections made.

Click the **Init by MAC** button to initiate the session information based on the MAC address.

Click the **ReAuth by MAC** button to re-authenticate the session information based on the MAC address.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Authenticator Statistics

This window is used to view and clear the authenticator statistics.

To view the following window, click **Security > 802.1X > Authenticator Statistics**, as shown below:

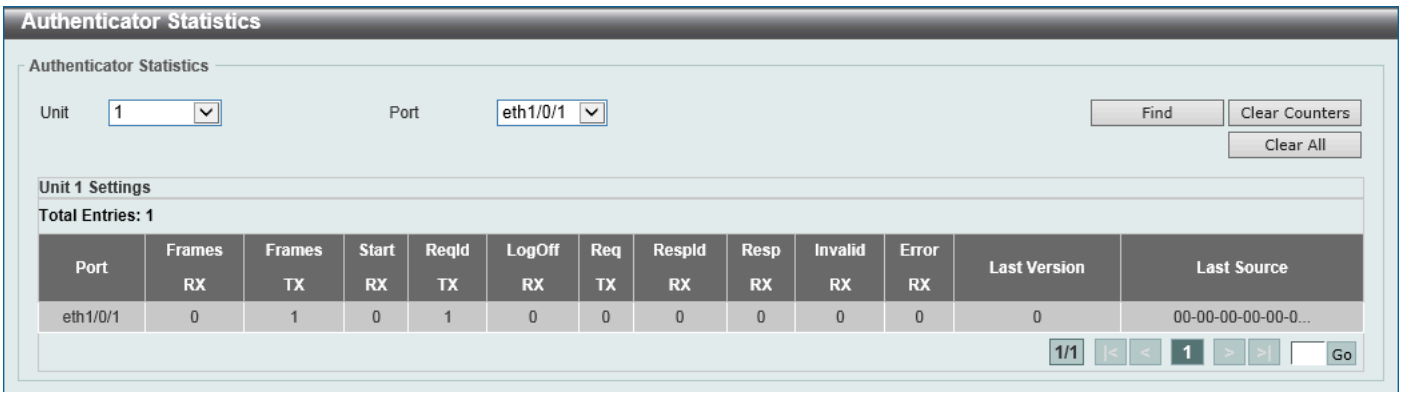


Figure 9-15 Authenticator Statistics Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this query here. This option is only available when stacking is enabled.
Port	Select the appropriate port used for the query here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear Counters** button to clear the counter information based on the selections made.

Click the **Clear All** button to clear all the information in this table.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Authenticator Session Statistics

This window is used to view and clear the authenticator session statistics.

To view the following window, click **Security > 802.1X > Authenticator Session Statistics**, as shown below:



Figure 9-16 Authenticator Session Statistics Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this query here.This option is only available when stacking is enabled.
Port	Select the appropriate port used for the query here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear Counters** button to clear the counter information based on the selections made.

Click the **Clear All** button to clear all the information in this table.

Authenticator Diagnostics

This window is used to view and clear the authenticator diagnostics information.

To view the following window, click **Security > 802.1X > Authenticator Diagnostics**, as shown below:

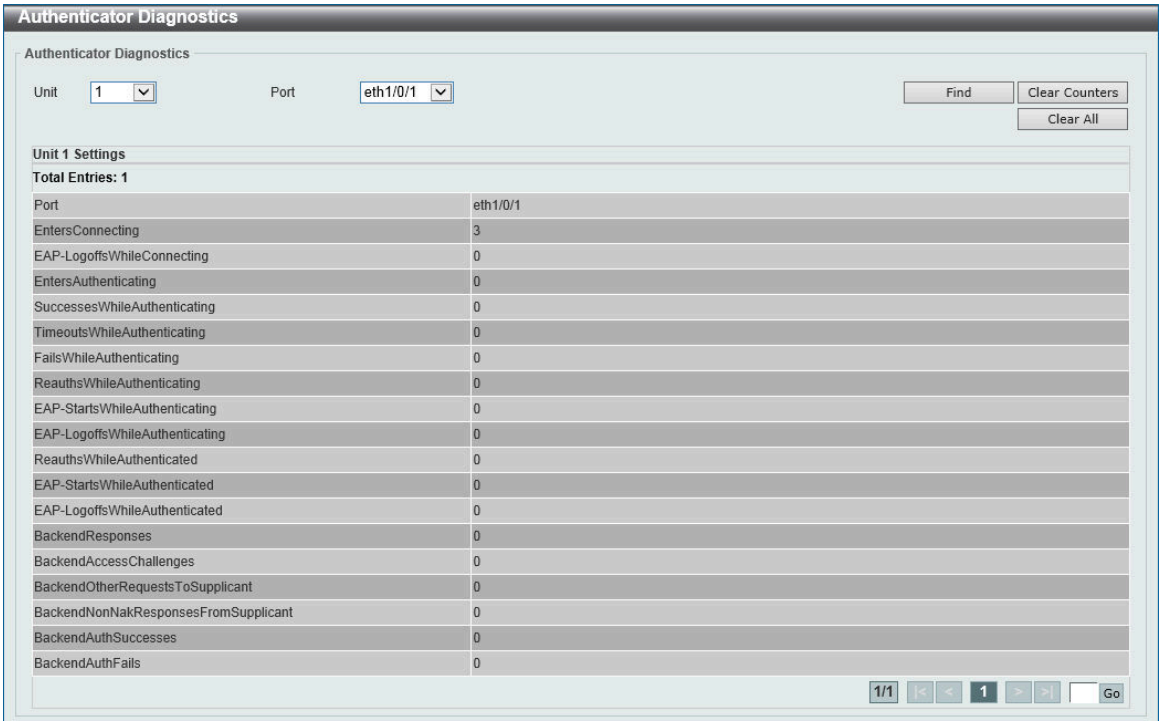


Figure 9-17 Authenticator Diagnostics Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this query here. This option is only available when stacking is enabled.
Port	Select the appropriate port used for the query here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear Counters** button to clear the counter information based on the selections made.

Click the **Clear All** button to clear all the information in this table.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

AAA

AAA stands for Authentication, Authorization, and Accounting. Its helps network administrators manage and control network service and obtain the usage statistics using their desired method.

AAA Global Settings

This window is used to enable or disable the global Authentication, Authorization, and Accounting (AAA) state.

To view the following window, click **Security > AAA > AAA Global Settings**, as shown below:

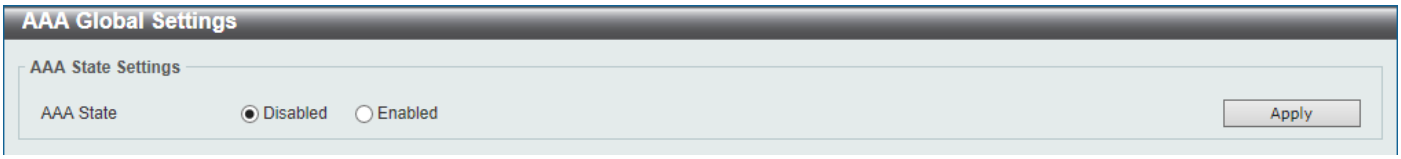


Figure 9-18 AAA Global Settings Window

The fields that can be configured are described below:

Parameter	Description
AAA State	Select to enable or disable the global Authentication, Authorization, and Accounting (AAA) state.

Click the **Apply** button to accept the changes made.

Application Authentication Settings

This window is used to display and configure the application authentication settings.

To view the following window, click **Security > AAA > Application Authentication Settings**, as shown below:

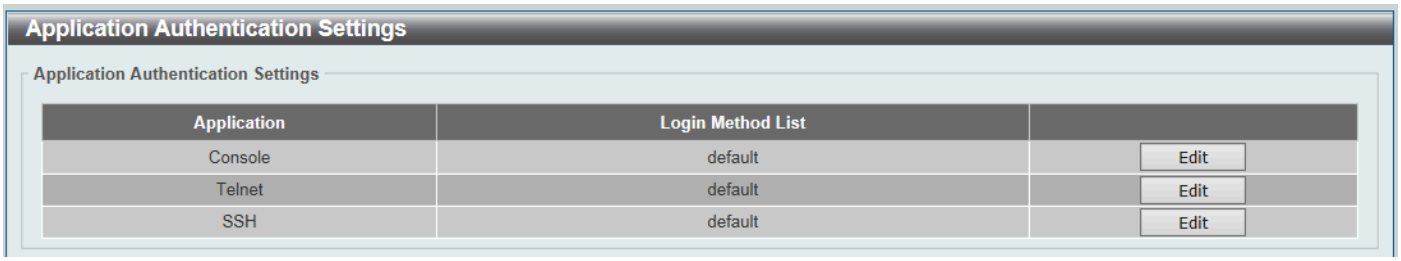


Figure 9-19 Application Authentication Settings Window

Click the **Edit** button to re-configure the specific entry.

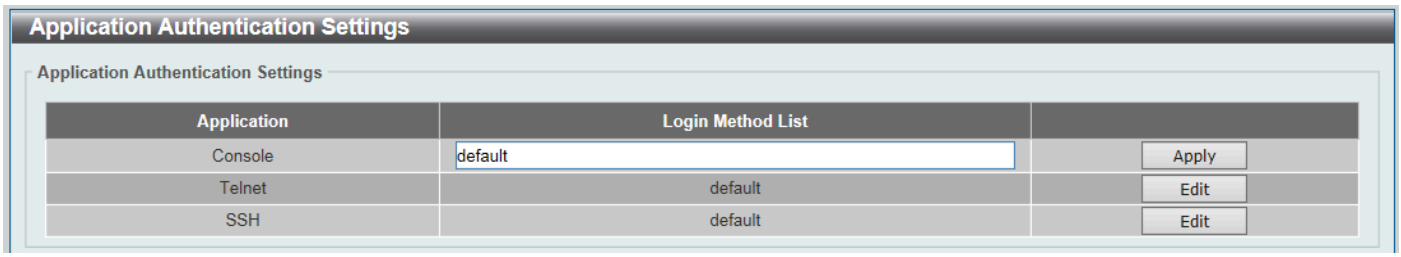


Figure 9-20 Application Authentication Settings (Edit) Window

The fields that can be configured are described below:

Parameter	Description
Login Method List	After clicking the **Edit** button for the specific entry, enter the login method list name used here.

Click the **Edit** button to re-configure the specific entry.

Click the **Apply** button to accept the changes made.

Application Accounting Settings

This window is used to display and configure the application accounting settings.

To view the following window, click **Security > AAA > Application Accounting Settings**, as shown below:

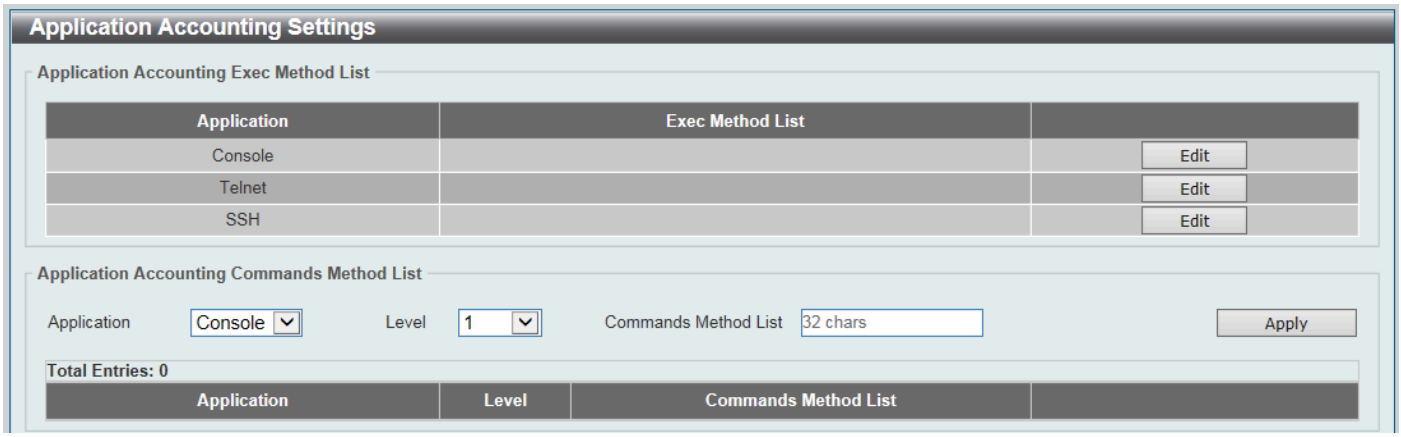


Figure 9-21 Application Accounting Settings Window

Click the **Edit** button to re-configure the specific entry.

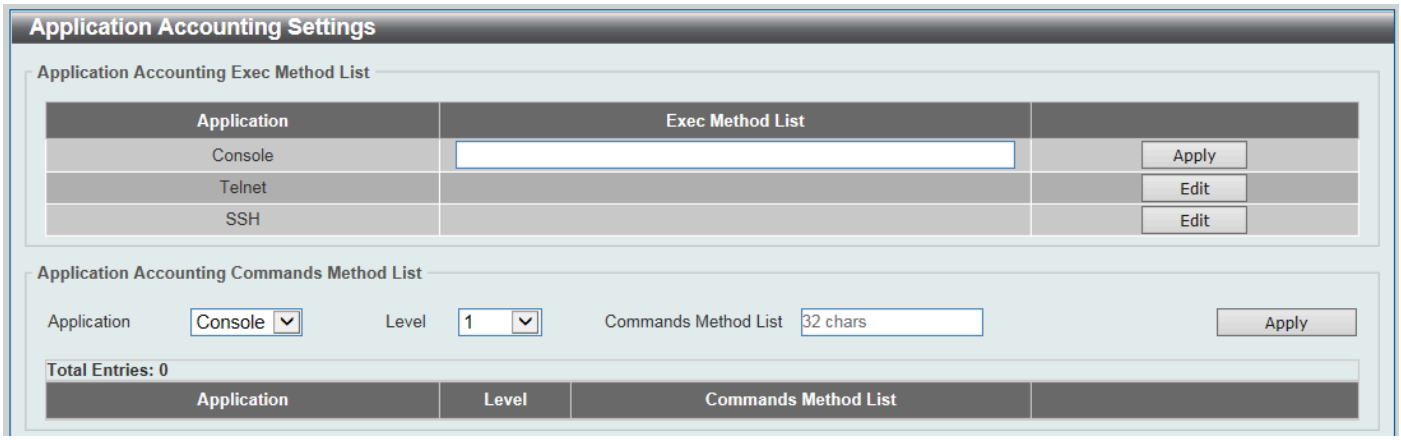


Figure 9-22 Application Accounting Settings (Edit) Window

The fields that can be configured in **Application Accounting Exec Method list** are described below:

Parameter	Description
Exec Method List	After clicking the **Edit** button for the specific entry, enter the EXEC method list name used here.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Application Accounting Commands Method List** are described below:

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 **Edit** button to re-configure the specific entry.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Authentication Settings

This window is used to display and configure the AAA network and EXEC authentication settings.

To view the following window, click **Security > AAA > Authentication Settings**, as shown below:

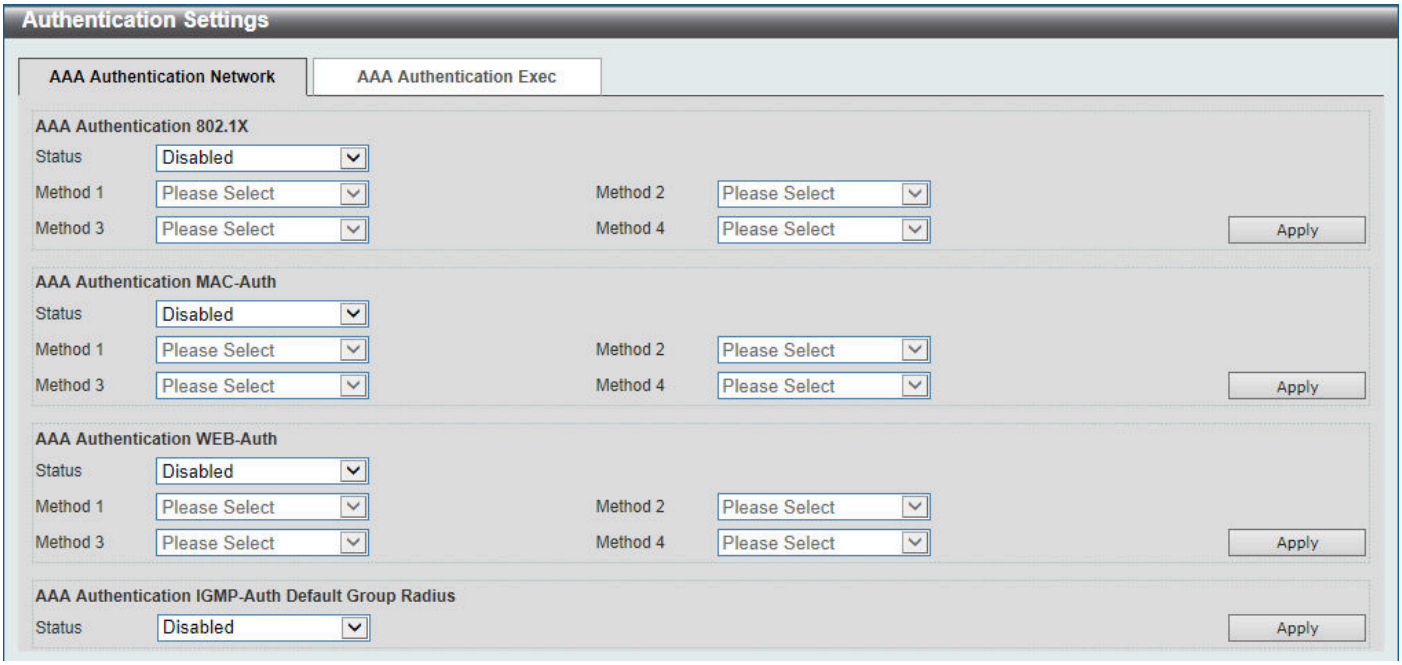


Figure 9-23 Authentication Settings Window

The fields that can be configured in **AAA Authentication 802.1X** are described below:

Parameter	Description
Status	Select to enable or disable the AAA 802.1X authentication state here.
Method 1 ~ Method 4	Select the method lists that will be used for this configuration here. Options to choose from are: • **none** - Normally, the method is listed as the last method. The user will pass authentication if it is not denied by previous method authentication. • **local** - Specifies to use the local database for authentication. • **group** - Specifies to use the server groups defined by the AAA group server. Enter the AAA group server name in the space provided. This string can be up to 32 characters long. • **radius** - Specifies to use the servers defined by the RADIUS server host command.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **AAA Authentication MAC-Auth** are described below:

Parameter	Description
Status	Select to enable or disable the AAA MAC authentication state here.
Method 1 ~ Method 4	Select the method lists that will be used for this configuration here. Options to choose from are: • **none** - Normally, the method is listed as the last method. The user will pass authentication if it is not denied by previous method authentication. • **local** - Specifies to use the local database for authentication.

Parameter	Description
	• **group** - Specifies to use the server groups defined by the AAA group server. Enter the AAA group server name in the space provided. This string can be up to 32 characters long. • **radius** - Specifies to use the servers defined by the RADIUS server host command.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **AAA Authentication WEB-Auth** are described below:

Parameter	Description
Status	Select to enable or disable the AAA Web authentication state here.
Method 1 ~ Method 4	Select the method lists that will be used for this configuration here. Options to choose from are: • **none** - Normally, the method is listed as the last method. The user will pass authentication if it is not denied by previous method authentication. • **local** - Specifies to use the local database for authentication. • **group** - Specifies to use the server groups defined by the AAA group server. Enter the AAA group server name in the space provided. This string can be up to 32 characters long. • **radius** - Specifies to use the servers defined by the RADIUS server host command.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **AAA Authentication IGMP-Auth Default Group RADIUS** are described below:

Parameter	Description
Status	Select to enable or disable the AAA authentication IGMP authentication default group RADIUS feature here.

Click the **Apply** button to accept the changes made.

After clicking the **AAA Authentication Exec** tab, the following page will appear.

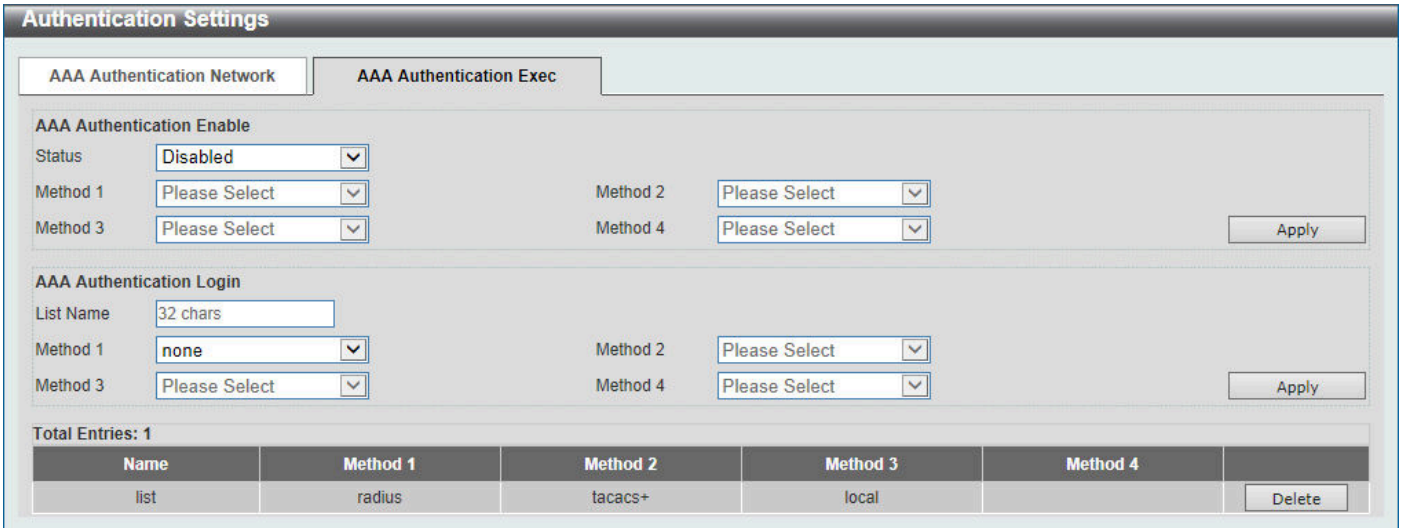


Figure 9-24 Authentication Settings (AAA Authentication EXEC) Window

The fields that can be configured in **AAA Authentication Enable** are described below:

Parameter	Description
Status	Select to enable or disable the AAA authentication enable state here.
Method 1 ~ Method 4	Select the method lists that will be used for this configuration here. Options to choose from are: • **none** - Normally, the method is listed as the last method. The user will pass the authentication if it is not denied by previous method authentication. • **enable** - Specifies to use the local enable password for authentication. • **group** - Specifies to use the server groups defined by the AAA group server command. Enter the AAA group server name in the space provided. This string can be up to 32 characters long. • **radius** - Specifies to use the servers defined by the RADIUS server host command. • **tacacs+** - Specifies to use the servers defined by the TACACS+ server host command.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **AAA Authentication Login** are described below:

Parameter	Description
List Name	Enter the method list name that will be used with the AAA authentication login option here.
Method 1 ~ Method 4	Select the method lists that will be used for this configuration here. Options to choose from are: • **none** - Normally, the method is listed as the last method. The user will pass authentication if it is not denied by previous method's authentication. • **local** - Specifies to use the local database for authentication. • **group** - Specifies to use the server groups defined by the AAA group server command. Enter the AAA group server name in the space provided. This string can be up to 32 characters long. • **radius** - Specifies to use the servers defined by the RADIUS server host command. • **tacacs+** - Specifies to use the servers defined by the TACACS+ server host command.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Accounting Settings

This window is used to display and configure the AAA accounting settings.

To view the following window, click **Security > AAA > Accounting Settings**, as shown below:

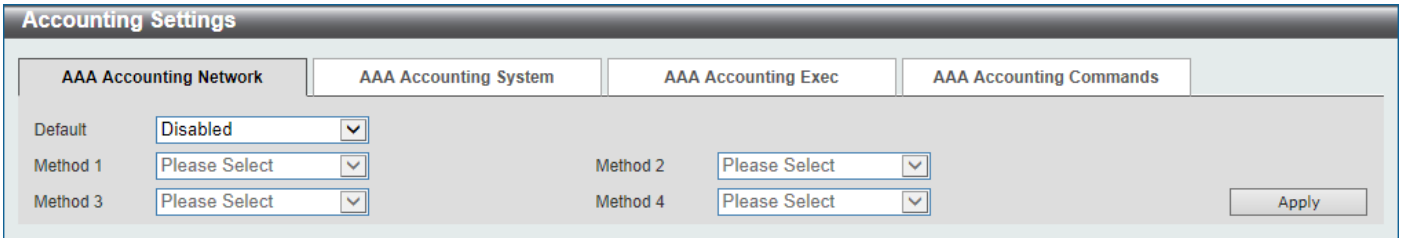


Figure 9-25 Accounting Settings Window

The fields that can be configured in **AAA Accounting Network** are described below:

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.

After clicking the **AAA Accounting System** tab, the following page will appear.

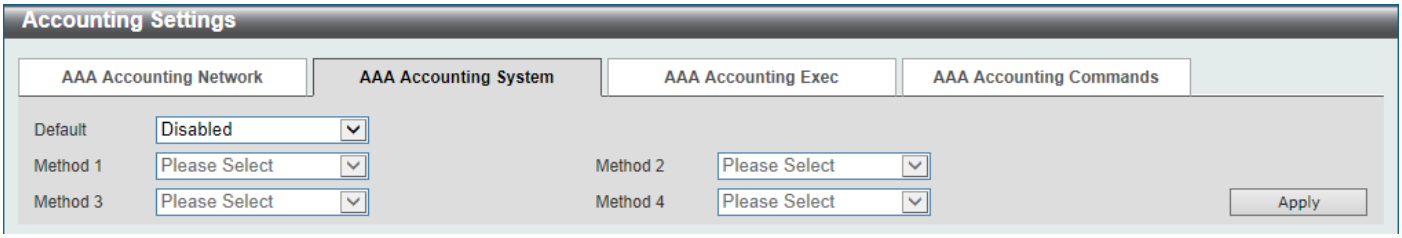


Figure 9-26 Accounting Settings (AAA Accounting System) Window

The fields that can be configured in **AAA Accounting System** are described below:

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.

After clicking the **AAA Accounting Exec** tab, the following page will appear.

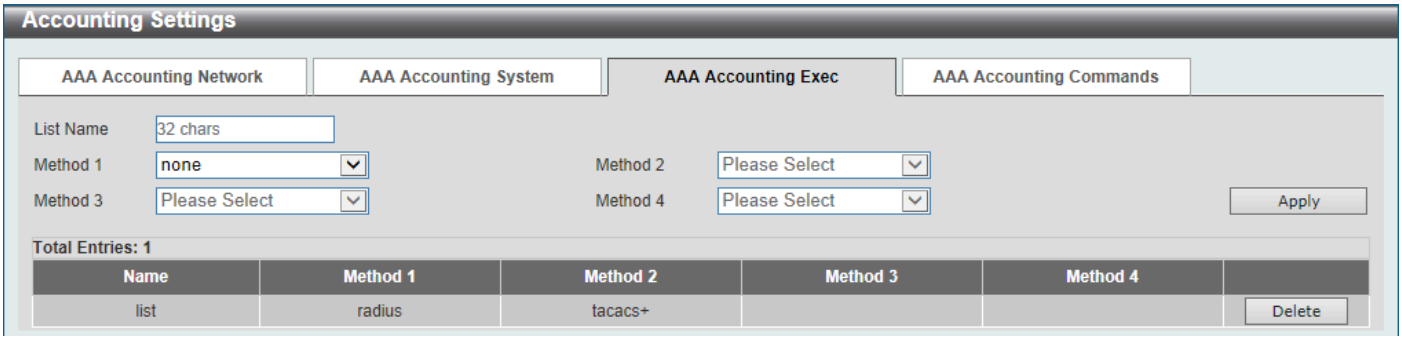


Figure 9-27 Accounting Settings (AAA Accounting Exec) Window

The fields that can be configured in **AAA Accounting Exec** are described below:

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 accept the changes made.

Click the **Delete** button to remove the specified entry.

After clicking the **AAA Accounting Commands** tab, the following page will appear.

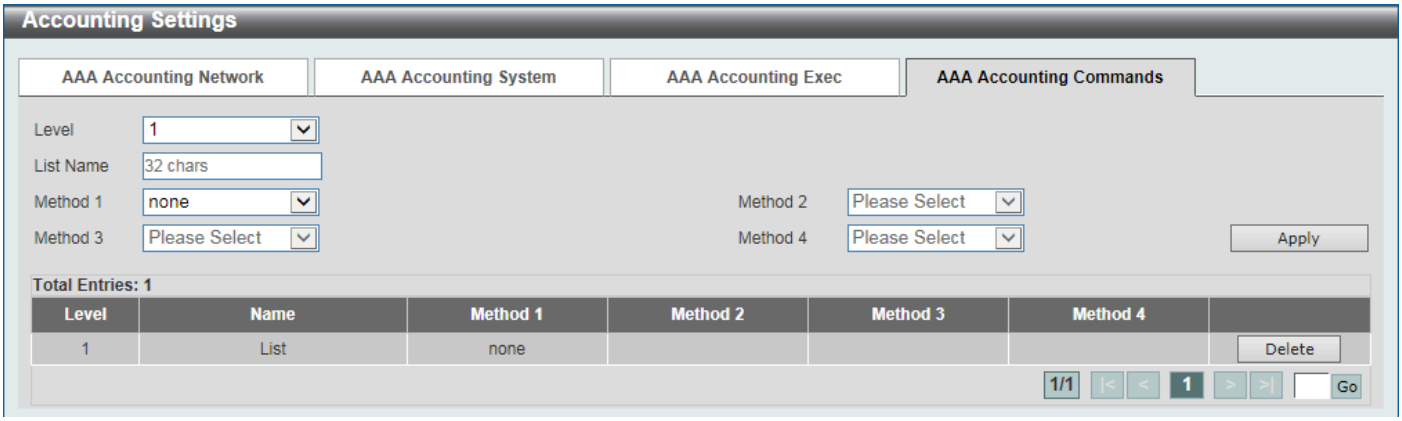


Figure 9-28 Accounting Settings (AAA Accounting Commands) Window

The fields that can be configured are described below:

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 accept the changes made.

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Server RADIUS Dynamic-Author Settings

This window is used to display and configure the dynamic authorization service. It facilitates changes of the attributes of an AAA session after it is established.

To view the following window, click **Security > AAA > Server RADIUS Dynamic-Author Settings**, as shown below:

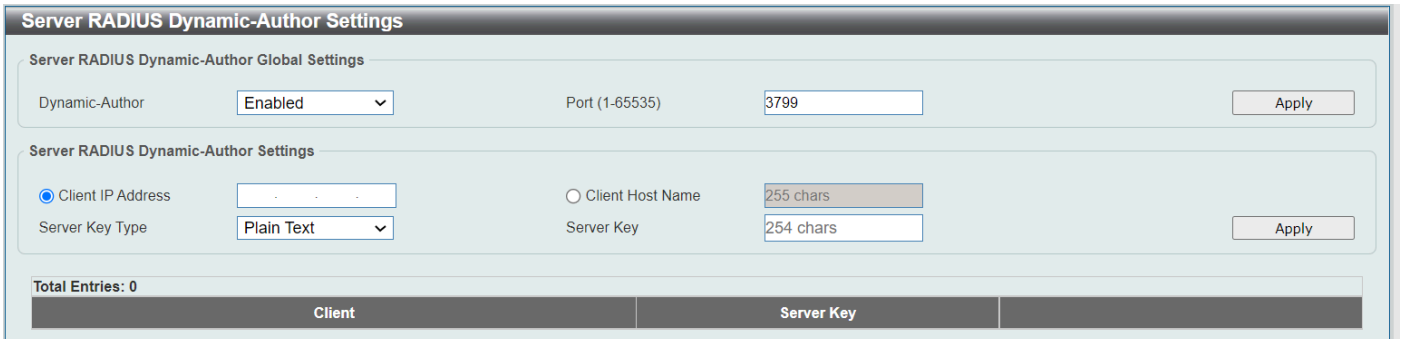


Figure 9-29 Accounting Settings (AAA Dynamic-Author Settings) Window

The fields that can be configured in **Server RADIUS Dynamic-Author Global Settings** are described below:

Parameter	Description
Dynamic-Author	Enable or disable the dynamic authorization service.
Port	Configure the port number for service requests.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Server RADIUS Dynamic-Author Settings** are described below:

Parameter	Description
Client IP Address	Configures the IP address of a RADIUS client that will accept change of authorization (CoA) requests.
Client Host Name	Alternatively, configure the host name of a RADIUS client that will accept change of authorization authorization (CoA) requests.
Server Key Type	Select whether the key will be plain text or encrypted: **Plain Text** or **Encrypted**.
Server Key	Enter the key which can be up to 254 characters if using plain text and must be 344 characters if using the encrypted option.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

RADIUS

Remote Authentication Dial-In User Service (RADIUS) helps implement centralized AAA service for a NAS (Network Access Server).

RADIUS Global Settings

This window is used to display and configure the global RADIUS settings.

To view the following window, click **Security > RADIUS > RADIUS Global Settings**, as shown below:

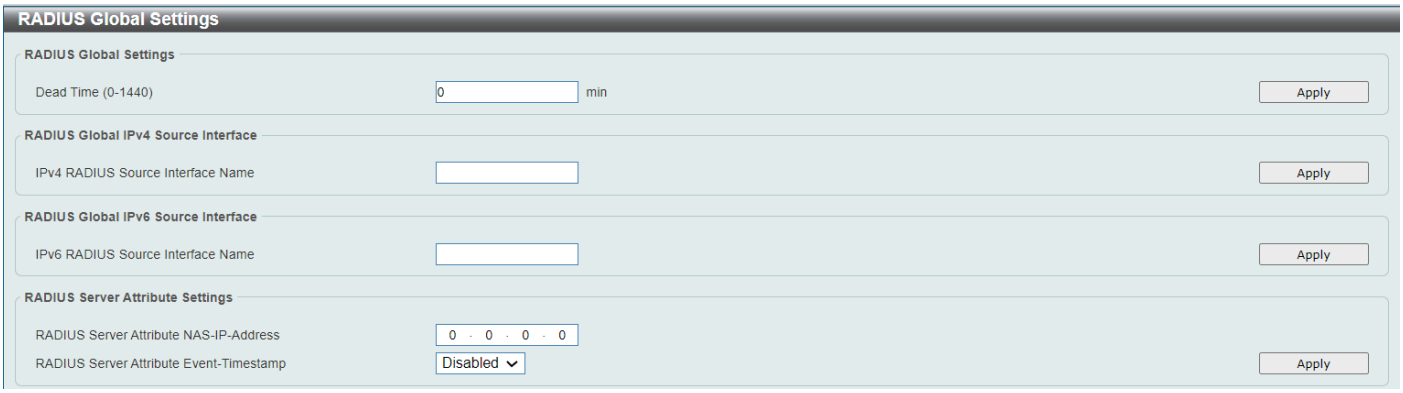


Figure 9-30 RADIUS Global Settings Window

The fields that can be configured in **RADIUS Global Settings** are described below:

Parameter	Description
Dead Time	Enter the dead time value here. This value must be between 1 and 1440 minutes. By default, this value is 0 minutes. When this option is 0, the unresponsive server will not be marked as dead. This setting can be used to improve the authentication processing time by setting the dead time to skip the unresponsive server host entries. When the system performs authentication with the authentication server, it attempts one server at a time. If the attempted server does not respond, the system will attempt the next server. When the system finds a server does not respond, it will mark the server as down, start a dead time timer, and skip them in authentication of the following requests until expiration of the dead time.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **RADIUS Global IPv4 Source Interface** are described below:

Parameter	Description
IPv4 RADIUS Source Interface Name	Enter the name of the IPv4 RADIUS source interface here. Refer to **L3 Features > Interface**.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **RADIUS Global IPv6 Source Interface** are described below:

Parameter	Description
IPv6 RADIUS Source Interface Name	Enter the name of the IPv6 RADIUS source interface here. Refer to **L3 Features > Interface**.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **RADIUS Server Attribute Settings** are described below:

Parameter	Description
RADIUS Server Attribute NAS-IP-Address	Enter the IP address of a Network Access Server (NAS) for the RADIUS Server Attribute.
RADIUS Server Attribute Event-Timestamp	Enable or disable the event timestamp for the RADIUS Server Attribute.

Click the **Apply** button to accept the changes made.

RADIUS Server Settings

This window is used to display and configure the RADIUS server settings.

To view the following window, click **Security > RADIUS > RADIUS Server Settings**, as shown below:

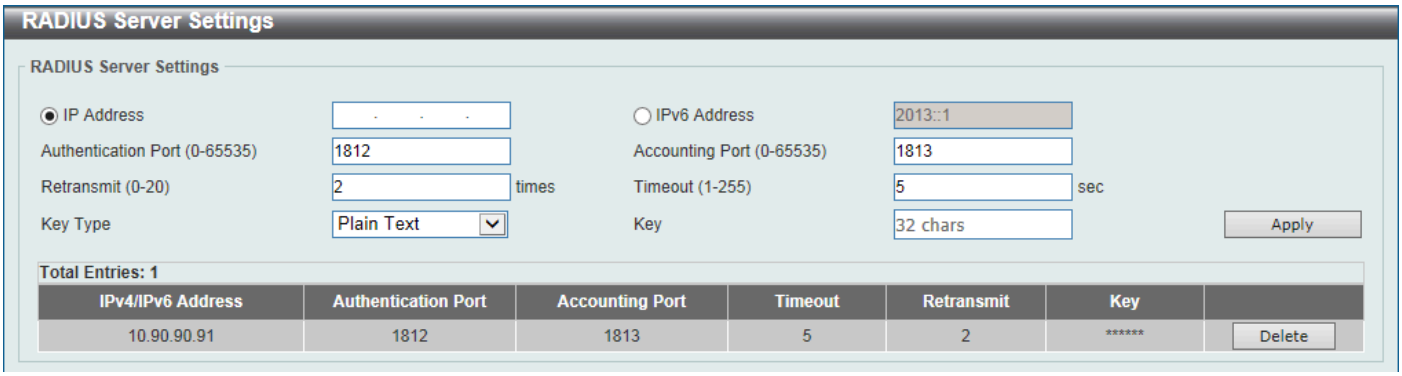


Figure 9-31 RADIUS Server Settings Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the RADIUS server IPv4 address here.
IPv6 Address	Enter the RADIUS server IPv6 address here.
Authentication Port	Enter the authentication port number used here. This value must be between 0 and 65535. By default, this value is 1812. If no authentication is used, use the value 0.
Accounting Port	Enter the accounting port number used here. This value must be between 0 and 65535. By default, this value is 1813. If no accounting is used, use the value 0.
Retransmit	Enter the retransmit value used here. This value must be between 0 and 20. By default, this value is 2. To disable this option, enter the value 0.
Timeout	Enter the timeout value used here. This value must be between 1 and 255 seconds. By default, this value is 5 seconds.
Key Type	Select the key type that will be used here. Options to choose from are **Plain Text** and **Encrypted**.
Key	Enter the key, used to communicate with the RADIUS server, here. This key can be up to 32 characters for plain text and must be 44 characters for encrypted.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

RADIUS Group Server Settings

This window is used to display and configure the RADIUS group server settings.

To view the following window, click **Security > RADIUS > RADIUS Group Server Settings**, as shown below:



Figure 9-32 RADIUS Group Server Settings Window

The fields that can be configured are described below:

Parameter	Description
Group Server Name	Enter the RADIUS group server name here. This name can be up to 32 characters long.
IP Address	Enter the group server IPv4 address here.
IPv6 Address	Enter the group server IPv6 address here.

Click the **Add** button to add a new entry based on the information entered.

Click the **Show Detail** button to view and configure more detailed settings for the RADIUS group server.

Click the **Delete** button to remove the specified entry.

After clicking the **Show Detail** button, the following page will be available.

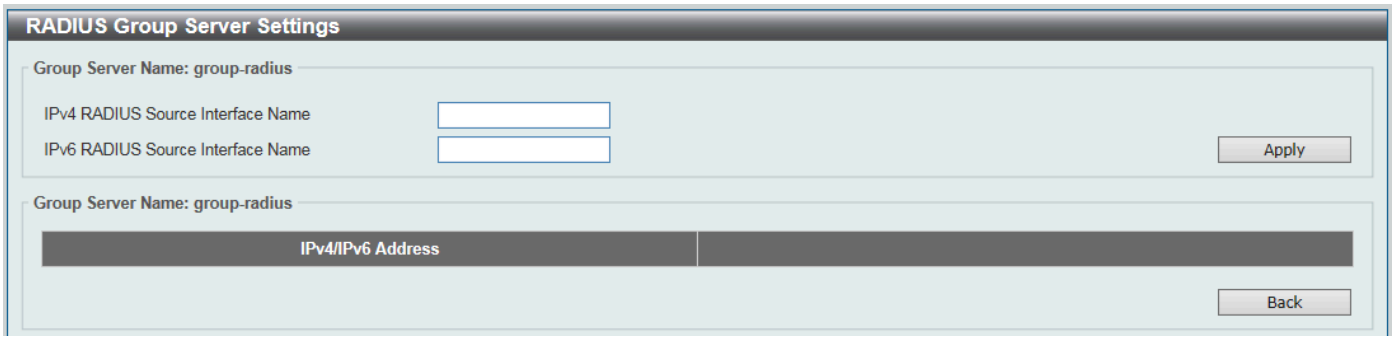


Figure 9-33 RADIUS Group Server Settings (Detail) Window

The fields that can be configured are described below:

Parameter	Description
IPv4 RADIUS Source Interface Name	Enter the name of the source IPv4 RADIUS interface here. Refer to L3 Features > Interface.
IPv6 RADIUS Source Interface Name	Enter the name of the source IPv6 RADIUS interface here. Refer to L3 Features > Interface.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Click the **Back** button to return to the previous window.

RADIUS Statistic

This window is used to view and clear the RADIUS statistics information.

To view the following window, click **Security > RADIUS > RADIUS Statistic**, as shown below:

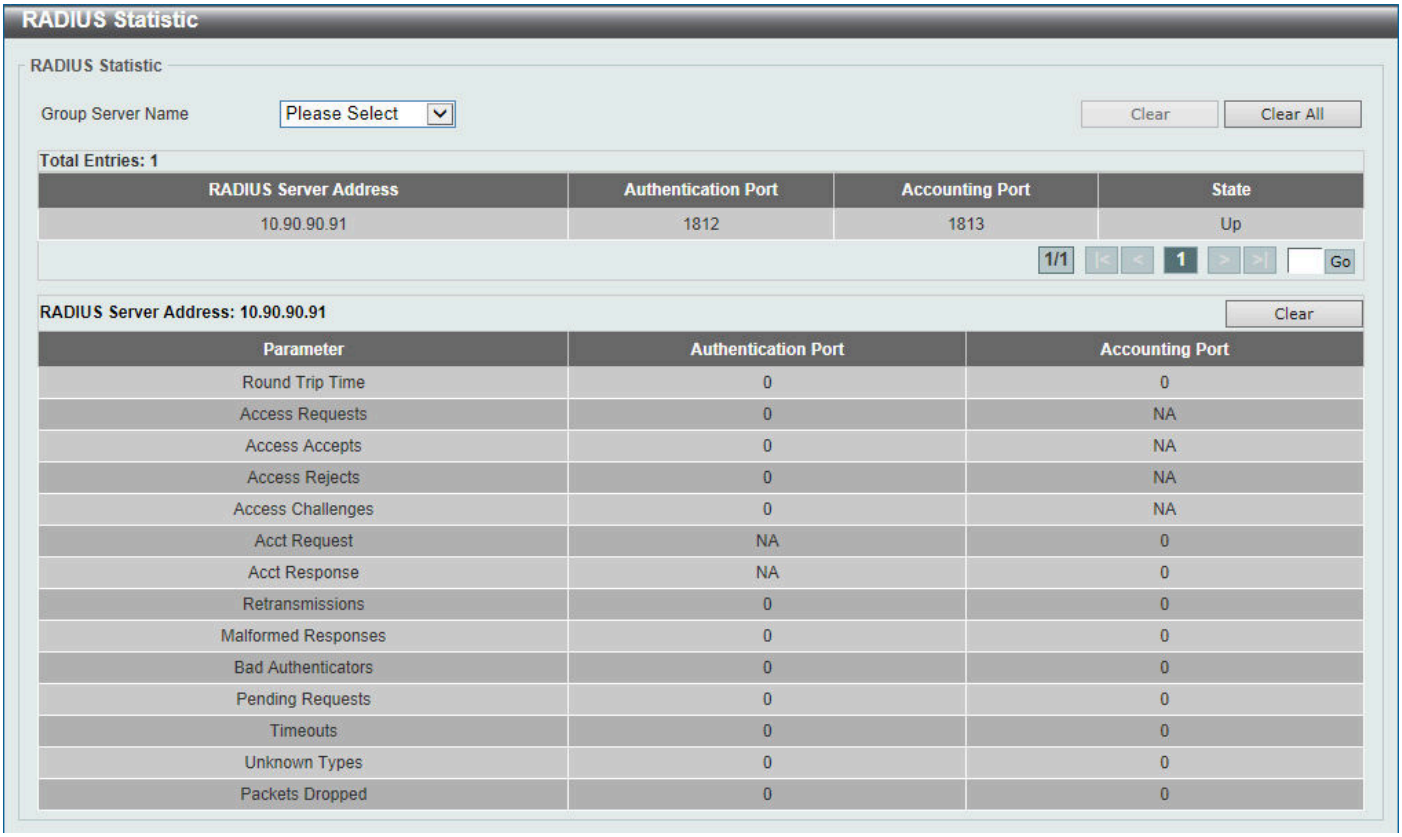


Figure 9-34 RADIUS Statistic Window

The fields that can be configured are described below:

Parameter	Description
Group Server Name	Select the RADIUS group server name from this list here.

Click the **Clear** button to clear the information based on the selections made.

Click the **Clear All** button to clear all the information in this table.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

TACACS

TACACS (Terminal Access Controller Access Control System) is another method (comparable to RAIUDS) that helps implement AAA in the network.

NOTE: In this section, settings associated with the TACACS+ feature will be configured, even though the word “TACACS” is used in the Web UI.

TACACS Global Settings

This window is used to display and configure the global TACACS+ server settings.

To view the following window, click **Security > TACACS > TACACS Global Settings**, as shown below:

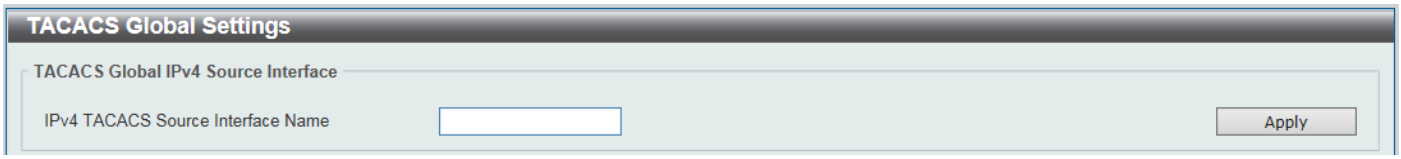


Figure 9-35 TACACS Global Settings Window

The fields that can be configured in **TACACS Global IPv4 Source Interface** are described below:

Parameter	Description
IPv4 TACACS Source Interface Name	Enter the name of the IPv4 TACACS+ source interface here. Refer to **L3 Features > Interface > IPv4 Interface**.

Click the **Apply** button to accept the changes made.

TACACS Server Settings

This window is used to display and configure the TACACS+ server settings.

To view the following window, click **Security > TACACS > TACACS Server Settings**, as shown below:

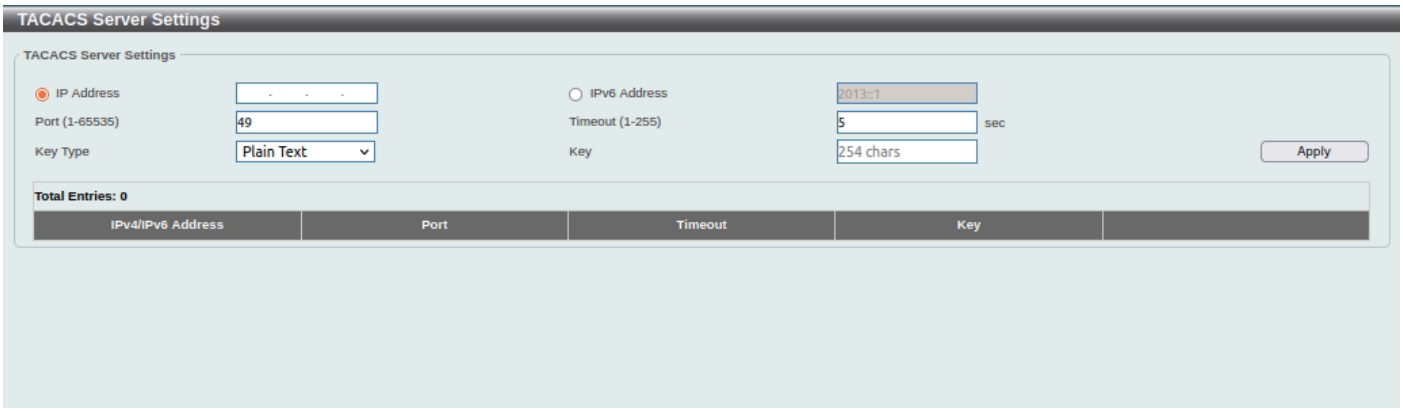


Figure 9-36 TACACS Server Settings Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the TACACS+ server IPv4 address here.
IPv6 Address	Enter the TACACS+ server IPv6 address here.
Port	Enter the port number used here. This value must be between 1 and 65535. By default, this value is 49.
Timeout	Enter the timeout value here. This value must be between 1 and 255 seconds. By default, this value is 5 seconds.
Key Type	Select the key type that will be used here. Options to choose from are **Plain Text** and **Encrypted**.

Parameter	Description
Key	Enter the key, used to communicate with the TACACS+ server, here. This key can be up to 254 characters if plain text is used and must be 344 characters if the encrypted option is used.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

TACACS Group Server Settings

This window is used to display and configure the TACACS+ group server settings.

To view the following window, click **Security > TACACS > TACACS Group Server Settings**, as shown below:



Figure 9-37 TACACS Group Server Settings Window

The fields that can be configured are described below:

Parameter	Description
Group Server Name	Enter the TACACS+ group server name here. This name can be up to 32 characters long.
IPv4 Address	Enter the group server IPv4 address here.
IPv6 Address	Enter the group server IPv6 address here.

Click the **Add** button to add a new entry based on the information entered.

Click the **Show Detail** button to view and configure more detailed settings for the TACACS+ group server.

Click the **Delete** button to remove the specified entry.

After clicking the **Show Detail** button, the following page will be available.

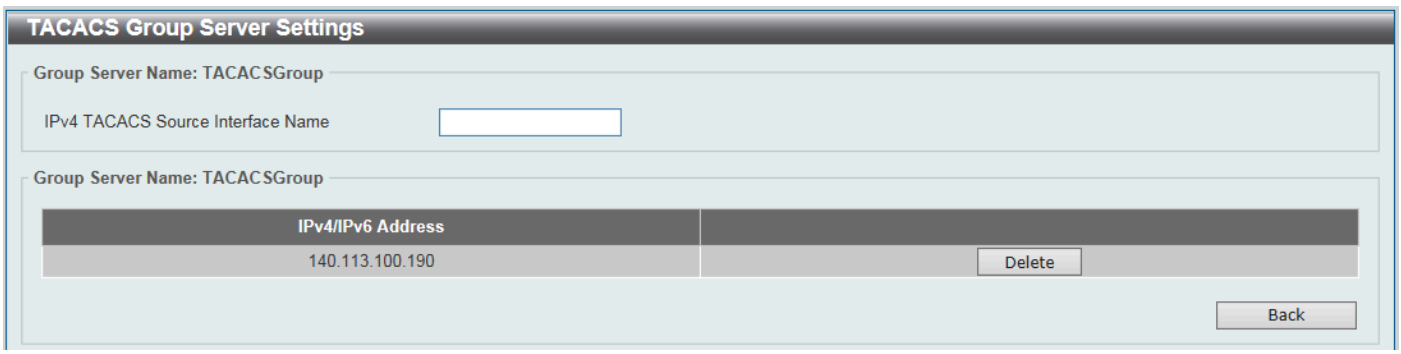


Figure 9-38 TACACS Group Server Settings (Show Detail) Window

The fields that can be configured are described below:

Parameter	Description
IPv4 TACACS Source Interface Name	Enter the name of the source IPv4 TACACS+ interface here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Click the **Back** button to return to the previous window.

TACACS Statistic

This window is used to view and clear the TACACS+ statistic information.

To view the following window, click **Security > TACACS > TACACS Statistic**, as shown below:

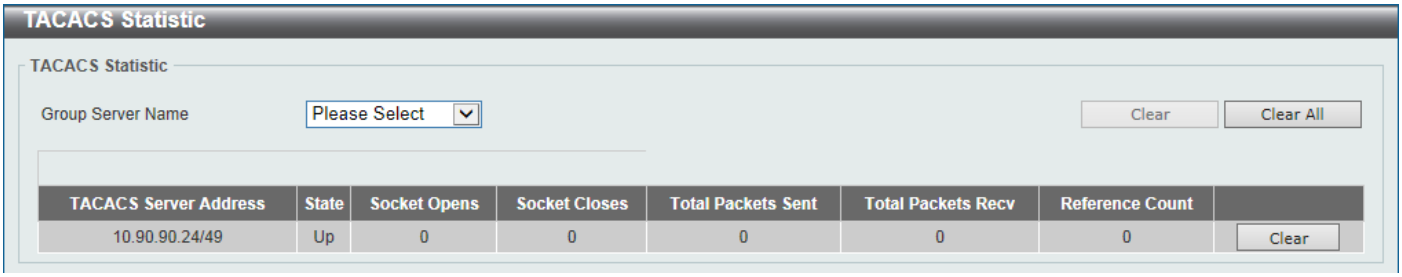


Figure 9-39 TACACS Statistic Window

The fields that can be configured are described below:

Parameter	Description
Group Server Name	Select the TACACS+ group server name from this list here.

Click the first **Clear** button to clear the information based on the group selected.

Click the **Clear All** button to clear all the information in this table.

Click the second **Clear** button to clear all the information for the specific entry.

IMPB

The IP network layer uses a four-byte address. The Ethernet link-layer uses a six-byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP-MAC-Port Binding (IMPB) is to restrict the access to a Switch to a number of authorized users. Authorized clients can access a Switch's port by either checking the pair of IP-MAC addresses with the pre-configured database or if DHCP snooping has been enabled in which case the Switch will automatically learn the IP/MAC pairs by snooping DHCP packets and saving them to the IMPB white list. If an unauthorized user tries to access an IP-MAC binding enabled port, the system will block the access by dropping its packet. Active and inactive entries use the same database. The function is port-based, meaning a user can enable or disable the function on the individual port.

IPv4

DHCPv4 Snooping

DHCP Snooping Global Settings

This window is used to display and configure the global DHCP snooping settings.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Global Settings**, as shown below:

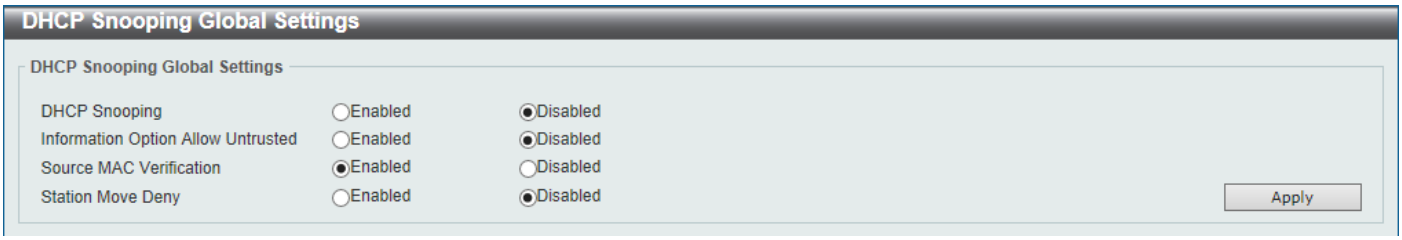


Figure 9-40 DHCP Snooping Global Settings Window

The fields that can be configured are described below:

Parameter	Description
DHCP Snooping	Select to enable or disable the global DHCP snooping status. The default is enabled.
Information Option Allow Untrusted	Select to enable or disable the option to globally allow DHCP packets with the relay Option 82 on the untrusted interface. The default is disabled.
Source MAC Verification	Select to enable or disable the verification that the source MAC address in a DHCP packet matches the client hardware address. The default is enabled.
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. The default is disabled.

Click the **Apply** button to accept the changes made.

DHCP Snooping Port Settings

This window is used to display and configure the DHCP snooping port settings.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Port Settings**, as shown below:

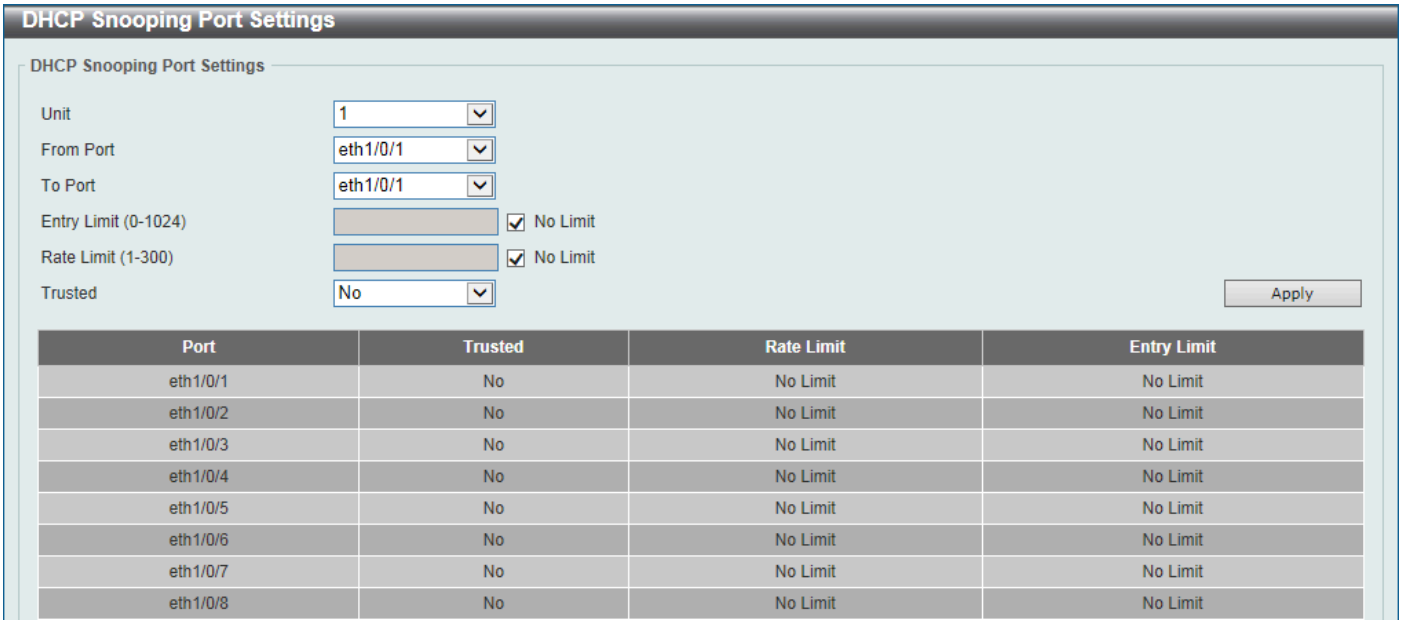


Figure 9-41 DHCP Snooping Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.This option is only available if stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
Entry Limit	Enter the entry limit value here. This value must be between 0 and 1024. Tick the **No Limit** option to disable the function.
Rate Limit	Enter the rate limit value here. This value must be between 1 and 300. Tick the **No Limit** option to disable the function.
Trusted	Select the trusted option here. Options to choose from are **No** and **Yes**. Ports connected to the DHCP server or to other Switches should be configured as trusted interfaces. The ports connected to DHCP clients should be configured as untrusted interfaces. DHCP snooping acts as a firewall between untrusted interfaces and DHCP servers.
NOTE: You can configure errdisable trap and recovery settings in **System > Port Configuration > Error Disable Settings**.	

Click the **Apply** button to accept the changes made.

DHCP Snooping VLAN Settings

This window is used to display and configure the DHCP snooping VLAN settings.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping VLAN Settings**, as shown below:

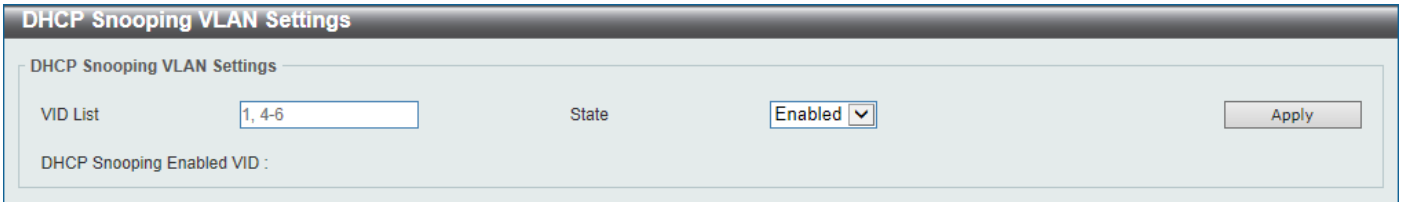


Figure 9-42 DHCP Snooping VLAN Settings Window

The fields that can be configured are described below:

Parameter	Description
VID List	Enter the VLAN ID list used here. Use "-" to specify the range value and "," to separate a list of values. For example, 1,4-6.
State	Select to enable or disable the DHCP snooping VLAN setting here.

Click the **Apply** button to accept the changes made.

DHCP Snooping Database

This window is used to display and configure the DHCP snooping database settings.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Database**, as shown below:

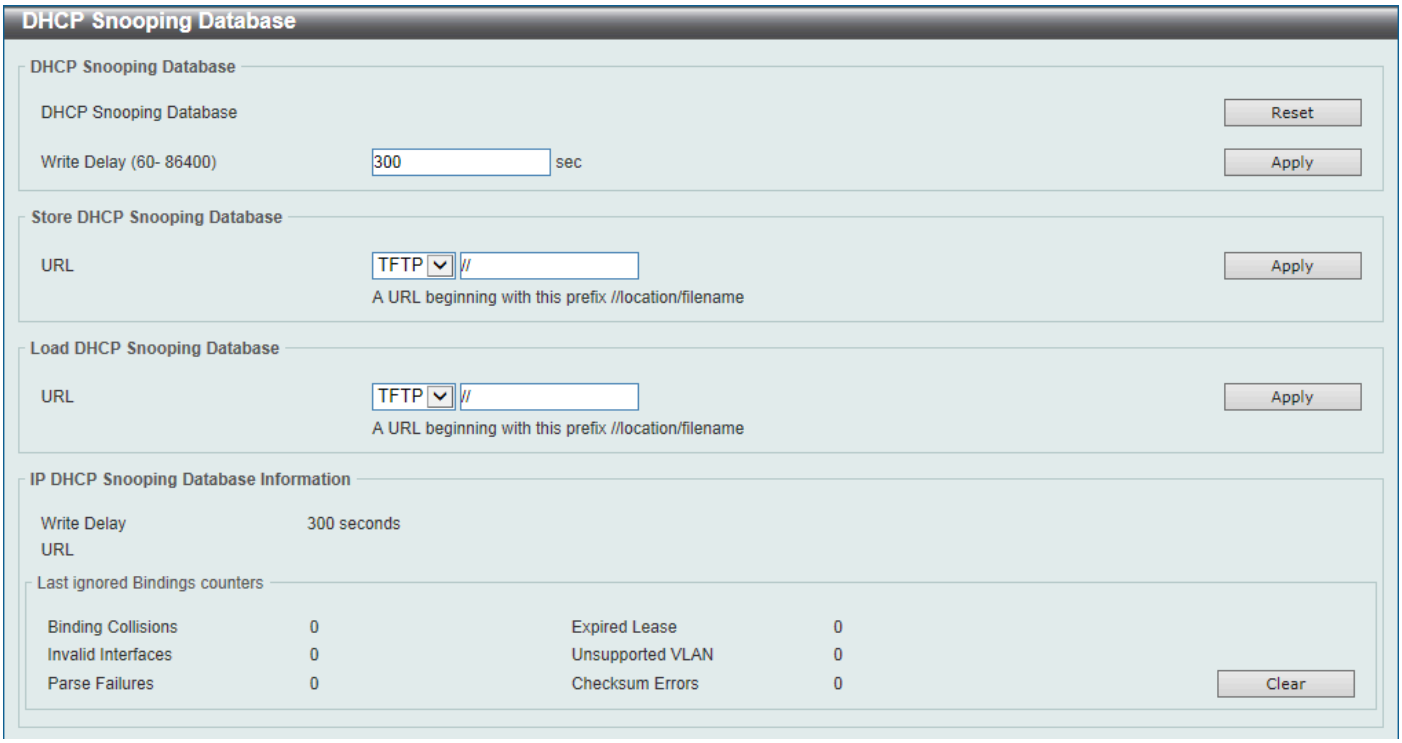


Figure 9-43 DHCP Snooping Database Window

The fields that can be configured in **DHCP Snooping Database** are described below:

Parameter	Description
Write Delay	Enter the write delay time value here. This value must be between 60 and 86400 seconds. By default, this value is 300 seconds.

Click the **Reset** button to reset the information entered.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Store DHCP Snooping Database** are described below:

Parameter	Description
URL	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 **Flash**. An example URL is given.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Load DHCP Snooping Database** are described below:

Parameter	Description
URL	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 **Flash**. An example URL is given.

Click the **Apply** button to accept the changes made.

Click the **Clear** button to clear all the counter information.

DHCP Snooping Binding Entry

This window is used to display and configure the DHCP snooping binding entries.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Binding Entry**, as shown below:

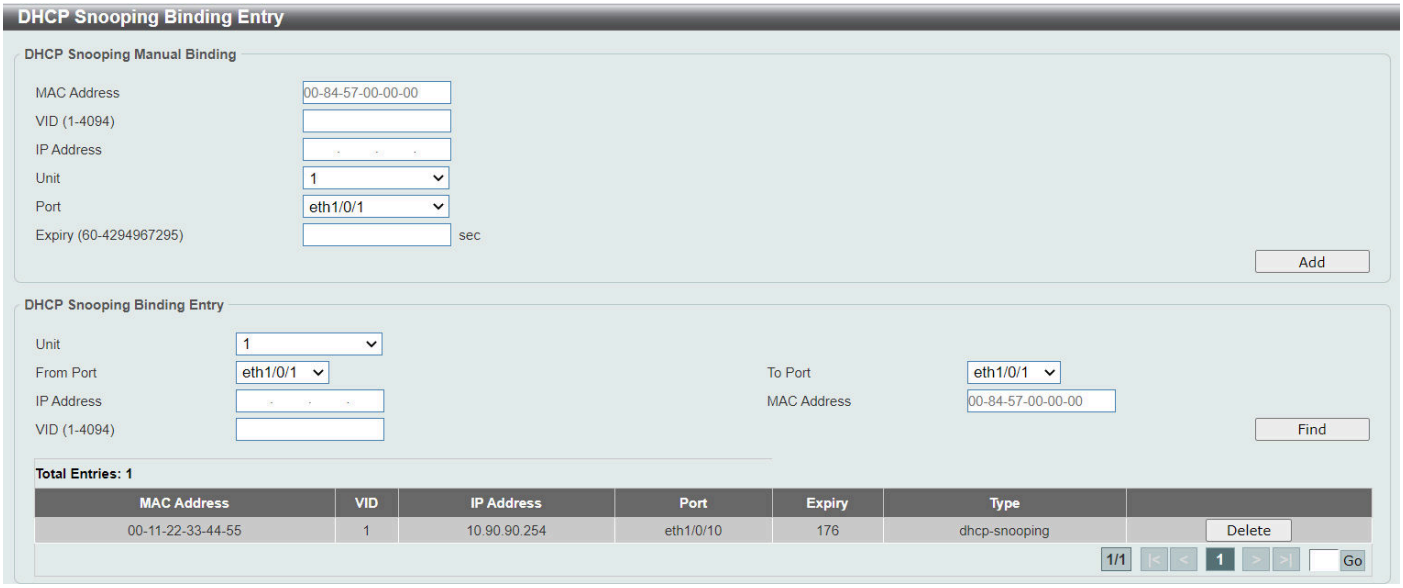


Figure 9-44 DHCP Snooping Binding Entry Window

The fields that can be configured are described below:

Parameter	Description
MAC Address	Enter the MAC address of the DHCP snooping binding entry here.
VID	Enter the VLAN ID of the DHCP snooping binding entry here. This value must be between 1 and 4094.

Parameter	Description
IP Address	Enter the IP address of the DHCP snooping binding entry here.
Unit	Select the Switch unit that will be used for this configuration here.This option is only available if stacking is enabled.
Port	Select the appropriate port used for the configuration here.
Expiry	Enter the expiry time value used here. This value must be between 60 and 4294967295 seconds.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove the specified entry.

Click the **Find** button to display the entry based on the entered information.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Dynamic ARP Inspection

ARP Access List

This window is used to display and configure the dynamic ARP inspection settings.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Access List**, as shown below:

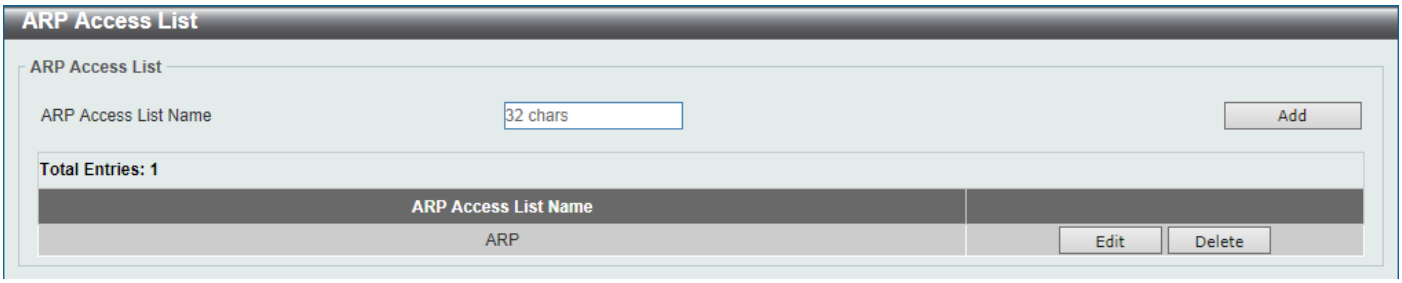


Figure 9-45 ARP Access List Window

The fields that can be configured are described below:

Parameter	Description
ARP Access List Name	Enter the ARP access list name used here. This name can be up to 32 characters long.

Click the **Add** button to add a new entry based on the information entered.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

After clicking the **Edit** button, the following window will appear.

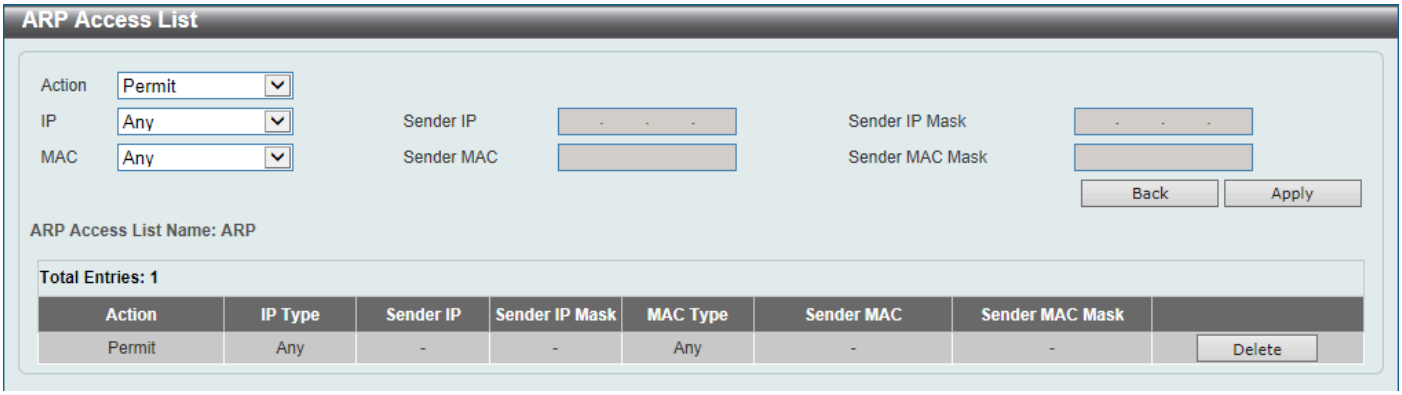


Figure 9-46 ARP Access List (Edit) Window

The fields that can be configured are described below:

Parameter	Description
Action	Select the action that will be taken here. Options to choose from are **Permit** and **Deny**.
IP	Select the type of sender IP address that will be used here. Options to choose from are **Any**, **Host**, and **IP with Mask**.
Sender IP	After selecting the **Host** or **IP with Mask** options as the type of **IP**, enter the sender IP address used here.
Sender IP Mask	After selecting the **IP with Mask** option as the type of **IP**, enter the sender IP mask used here.
MAC	Select the type of sender MAC address that will be used here. Options to choose from are **Any, Host,** and **MAC with Mask**.
Sender MAC	After selecting the **Host** or **MAC with Mask** options as the type of **MAC**, enter the sender MAC address used here.
Sender MAC Mask	After selecting the **MAC with Mask** option as the type of **MAC**, enter the sender MAC mask used here.

Click the **Back** button to return to the previous page.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

ARP Inspection Settings

This window is used to display and configure the ARP inspection settings.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Settings**, as shown below:

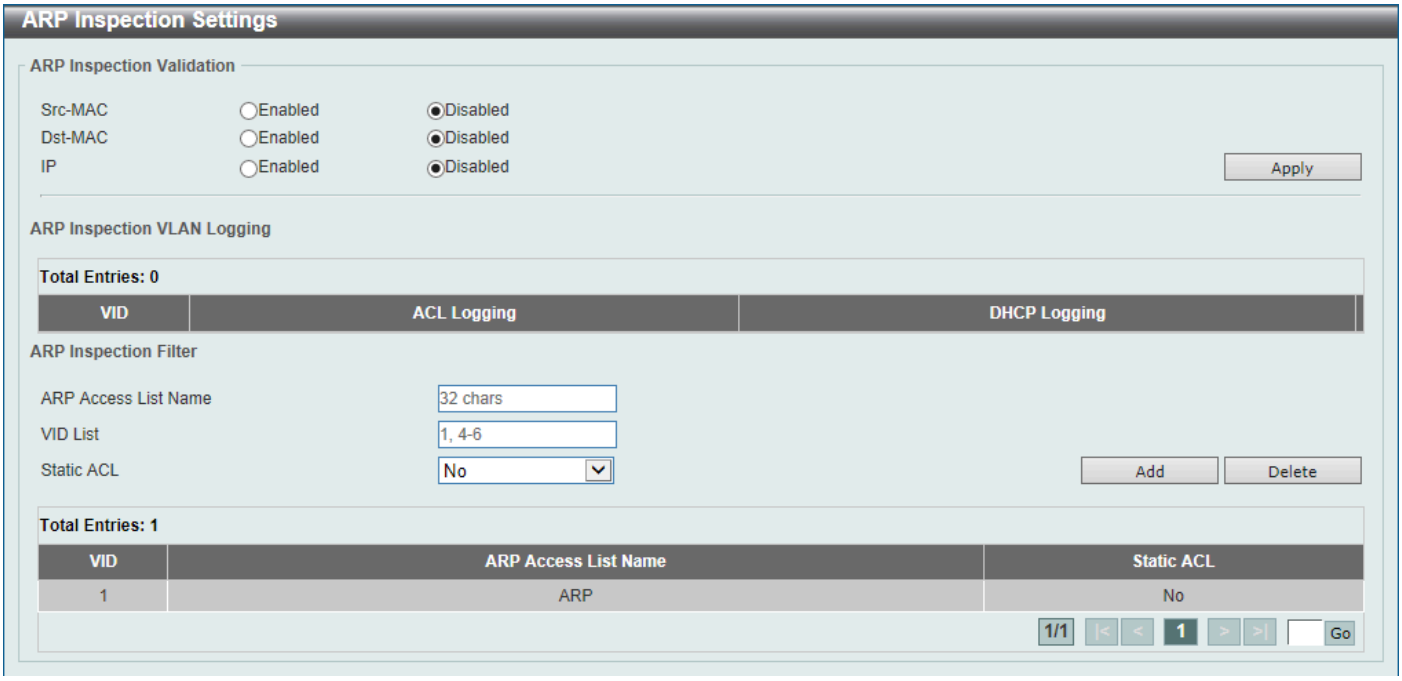


Figure 9-47 ARP Inspection Settings Window

The fields that can be configured in **ARP Inspection Validation** are described below:

Parameter	Description
Src-MAC	Select to enable or disable the source MAC option here. This option specifies to check for ARP requests and response packets and the consistency of the source MAC address in the Ethernet header against the sender MAC address in the ARP payload.
Dst-MAC	Select to enable or disable the destination MAC option here. This option specifies to check for ARP response packets and the consistency of the destination MAC address in the Ethernet header against the target MAC address in the ARP payload.
IP	Select to enable or disable the IP option here. This option specifies to check the ARP body for invalid and unexpected IP addresses. It also specifies to check the validity of IP address in the ARP payload. The sender IP in both the ARP request and response and target IP in the ARP response are validated. Packets destined for the IP addresses 0.0.0.0, 255.255.255.255, and all IP multicast addresses are dropped. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **ARP Inspection VLAN Logging** are described below:

Parameter	Description
ACL Logging	After clicking Edit, select a logging option for ACL logging: **Deny, Permit, All** and **None**. Select Deny to log denied ARP requests. Select Permit to log permitted requests. Select All to log all request. Select None to disable logging.
DHCP Logging	After clicking Edit, select a logging option for DHCP logging: **Deny, Permit, All** and **None**. Select Deny to log denied ARP requests. Select Permit to log permitted requests. Select All to log all request. Select None to disable logging.

The fields that can be configured in **ARP Inspection Filter** are described below:

Parameter	Description
ARP Access List Name	Enter the ARP access list name used here. This name can be up to 32 characters long.
VID List	Enter the VLAN ID list used here.
Static ACL	Select whether to use a static ACL or not here by either selecting **Yes** or **No**.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove an entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

ARP Inspection Port Settings

This window is used to display and configure the ARP inspection port settings.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Port Settings**, as shown below:

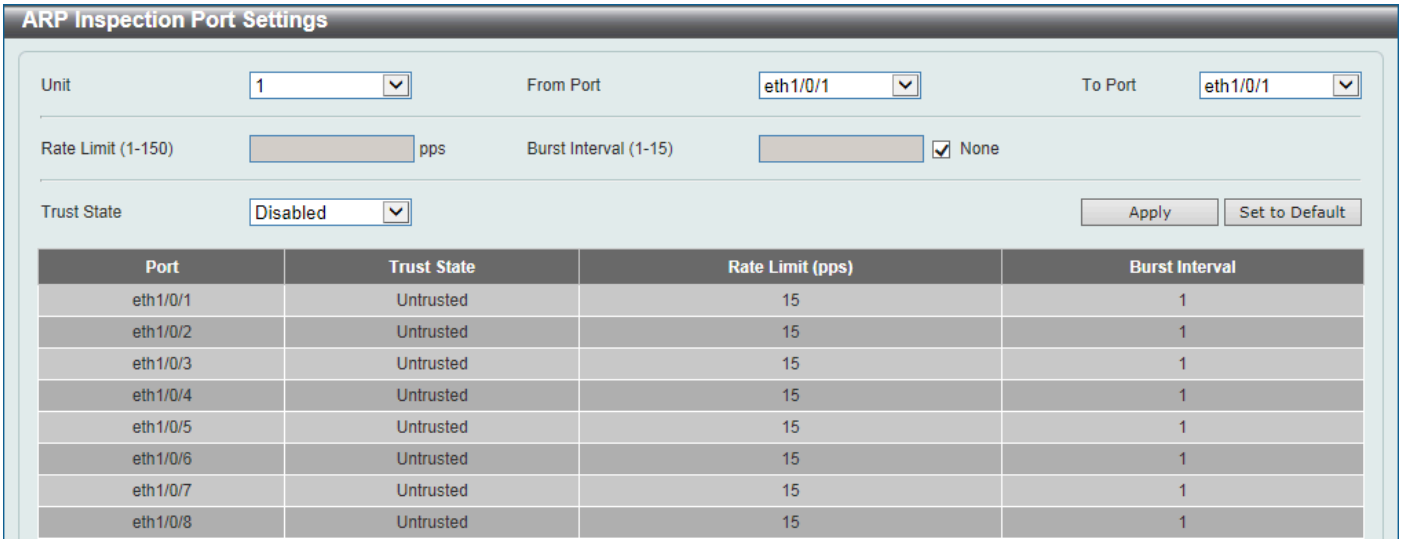


Figure 9-48 ARP Inspection Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available if stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
Rate Limit	Enter the rate limit value here. This value must be between 1 and 150 packets per seconds.
Burst Interval	Enter the burst interval value here. This value must be between 1 and 15. Tick the **None** option to disable the option.
Trust State	Select to enable or disable the trust state here.
NOTE: You can configure errdisable trap and recovery settings in **System > Port Configuration > Error Disable Settings**.	

Click the **Apply** button to accept the changes made.

Click the **Set to Default** button to change the information to the default values.

ARP Inspection VLAN

This window is used to display and configure the ARP inspection VLAN settings.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection VLAN**, as shown below:

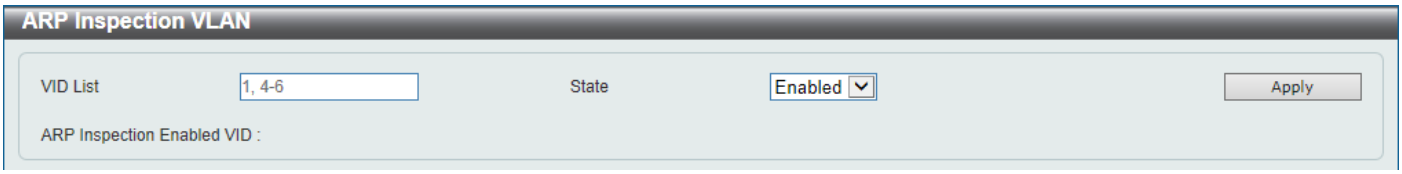


Figure 9-49 ARP Inspection VLAN Window

The fields that can be configured are described below:

Parameter	Description
VID List	Enter the VLAN ID list used here. Use "-" to specify the range value and "," to separate the list of values. For example, 1,4-6.
State	Select to enable or disable the ARP inspection option's state for the specified VLAN here.

Click the **Apply** button to accept the changes made.

ARP Inspection Statistics

This window is used to view and clear the ARP inspection statistics information.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Statistics**, as shown below:

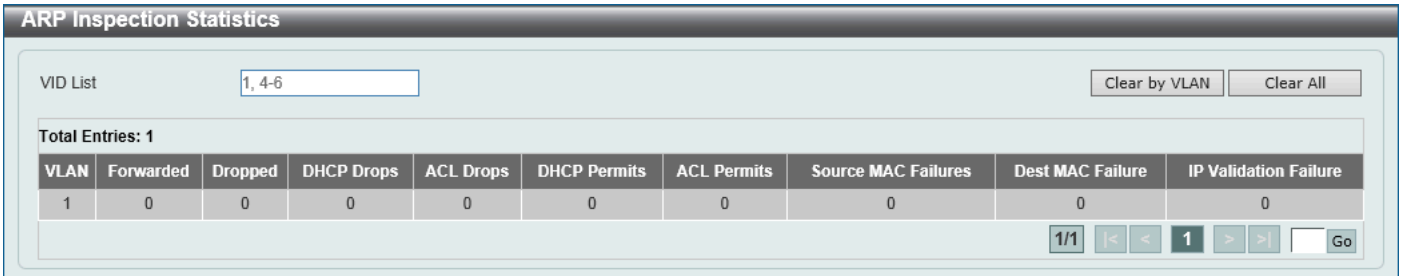


Figure 9-50 ARP Inspection Statistics Window

The fields that can be configured are described below:

Parameter	Description
VID List	Enter the VLAN ID list used here.

Click the **Clear by VLAN** button to clear the information based on the VLAN ID(s) entered.

Click the **Clear All** button to clear all the information in this table.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

ARP Inspection Log

This window is used to view, configure, and clear the ARP inspection log information.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Log**, as shown below:



Figure 9-51 ARP Inspection Log Window

The fields that can be configured are described below:

Parameter	Description
Log Buffer	Enter the log buffer value used here. This value must be between 1 and 1024. By default, this value is 32.

Click the **Apply** button to accept the changes made.

Click the **Clear Log** button to clear the log.

IP Source Guard

IP Source Guard Port Settings

This window is used to display and configure the IP source guard port settings.

To view the following window, click **Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Port Settings**, as shown below:

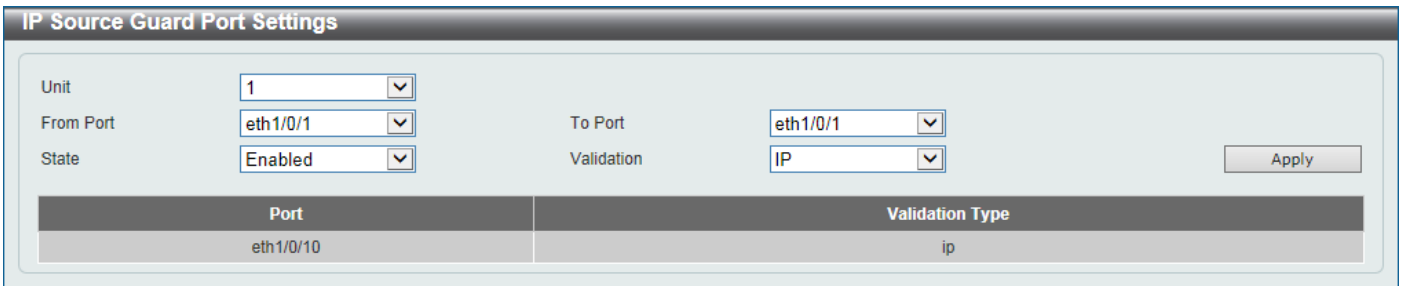


Figure 9-52 IP Source Guard Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available if stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the IP source guard's state for the specified port(s) here.

Parameter	Description
Validation	Select the validation method used here. Options to choose from are **IP** and **IP-MAC**. Selecting **IP** means that the IP address of the received packets will be checked. Selecting **IP-MAC** means that the IP address and the MAC address of the received packets will be checked.

Click the **Apply** button to accept the changes made.

IP Source Guard Binding

This window is used to display and configure the IP source guard binding settings.

To view the following window, click **Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Binding**, as shown below:

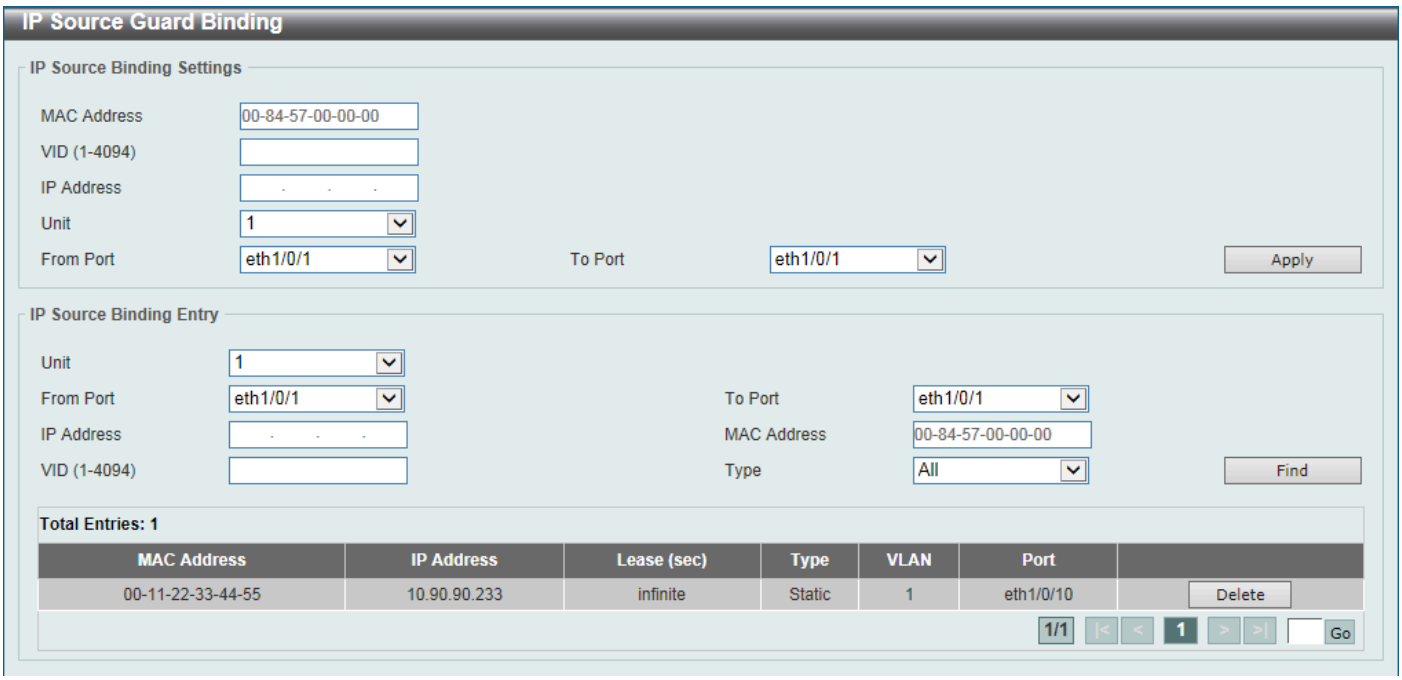


Figure 9-53 IP Source Guard Binding Window

The fields that can be configured in **IP Source Binding Settings** are described below:

Parameter	Description
MAC Address	Enter the MAC address of the binding entry here.
VID	Enter the VLAN ID of the binding entry here.
IP Address	Enter the IP address of the binding entry here.
Unit	Select the Switch unit that will be used for this configuration here. This option is only available is stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **IP Source Binding Entry** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this query here. This option is only available if stacking is enabled.
From Port - To Port	Select the appropriate port range used for the query here.
IP Address	Enter the IP address of the binding entry here.
MAC Address	Enter the MAC address of the binding entry here.
VID	Enter the VLAN ID of the binding entry here.
Type	Select the type of binding entry to find here. Options to choose from are **All**, **DHCP Snooping**, and **Static**. • Selecting **All** specifies that all the DHCP binding entries will be displayed. • Selecting **DHCP Snooping** specifies to display the IP-source guard binding entry learned by DHCP snooping. • Selecting **Static** specifies to display the IP-source guard binding entry that is manually configured.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IP Source Guard HW Entry

This window is used to view the IP source guard hardware entries.

To view the following window, click **Security > IMPB > IPv4 > IP Source Guard > IP Source Guard HW Entry**, as shown below:

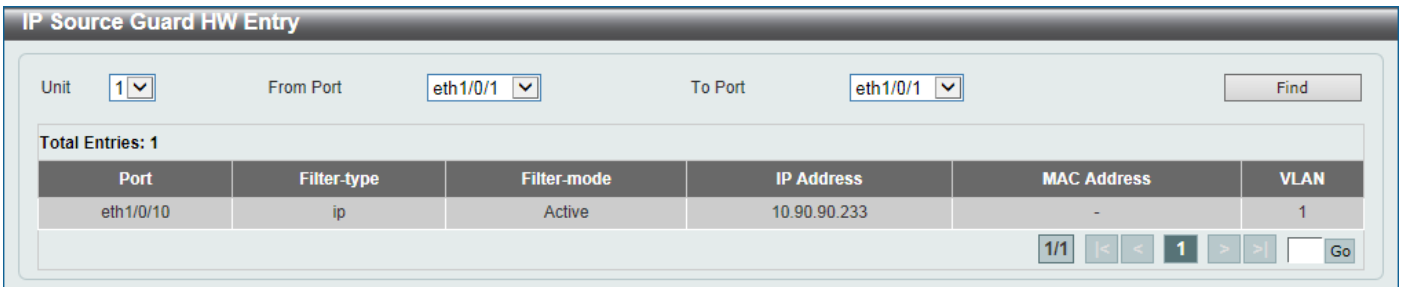


Figure 9-54 IP Source Guard HW Entry Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this query here. This option is only available is stacking is enabled.
From Port - To Port	Select the appropriate port range used for the query here.

Click the **Find** button to locate a specific entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Advanced Settings

IP-MAC-Port Binding Settings

This window is used to display and configure the IP-MAC-Port binding settings.

To view the following window, click **Security > IMPB > IPv4 > Advanced Settings > IP-MAC-Port Binding Settings**, as shown below:

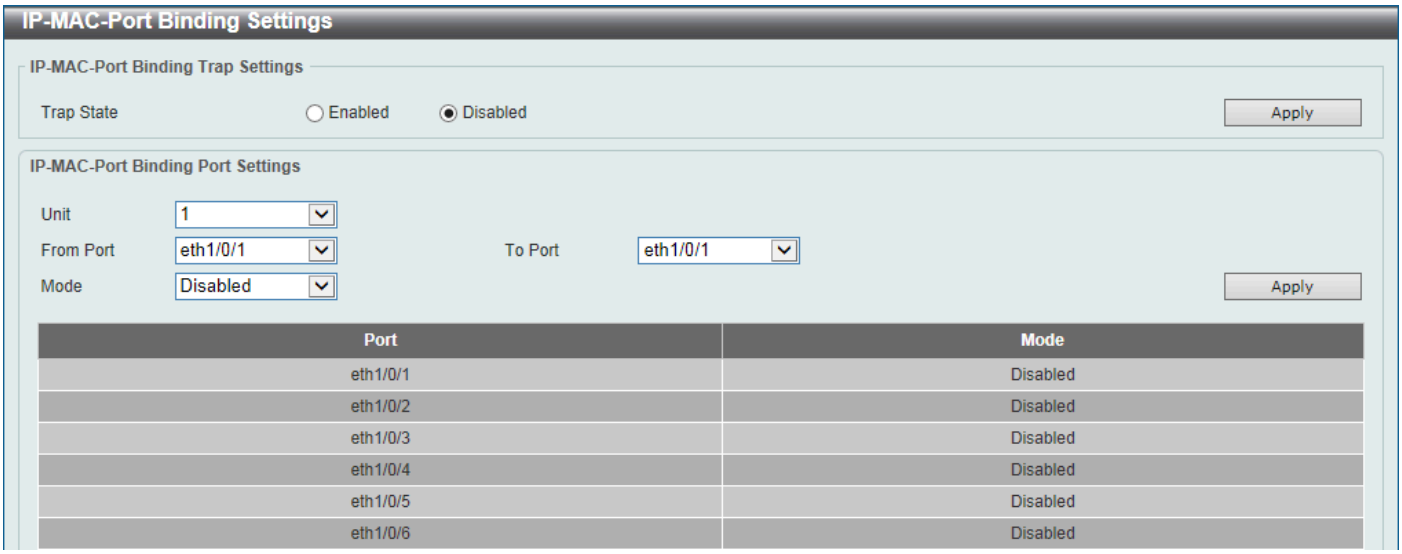


Figure 9-55 IP-MAC-Port Binding Settings Window

The fields that can be configured in **IP-MAC-Port Binding Trap Settings** are described below:

Parameter	Description
Trap State	Select the enable or disable the IP-MAC-Port binding option's trap state.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **IP-MAC-Port Binding Port Settings** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available if stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
Mode	Select the mode of access control that will be used here. Options to choose from are **Disabled**, **Strict**, and **Loose**. When a port is enabled for IMPB strict-mode access control, a host can only access the port after the host sends ARP or IP packets and the ARP packet or IP packet sent by the host passes the binding check. To pass the binding check, the source IP address, source MAC address, VLAN ID, and arrival port number must match any of the entries defined by either the IP source guard static binding entry or the DHCP snooping learned dynamic binding entry. When a port is enabled for IMPB loose-mode access control, a host will be denied to access the port after the host sends ARP or IP packets and the ARP packet or IP packet sent by the host does not pass the binding check. To pass the binding check, the source IP address, source MAC address, VLAN ID, and arrival port must match any of the entries defined by either the IP source guard static binding entry or the DHCP snooping learned dynamic binding entry.

Click the **Apply** button to accept the changes made.

IP-MAC-Port Binding Blocked Entry

This window is used to view and clear the IP-MAC-Port binding blocked entry table.

To view the following window, click **Security > IMPB > IPv4 > Advanced Settings > IP-MAC-Port Binding Blocked Entry**, as shown below:

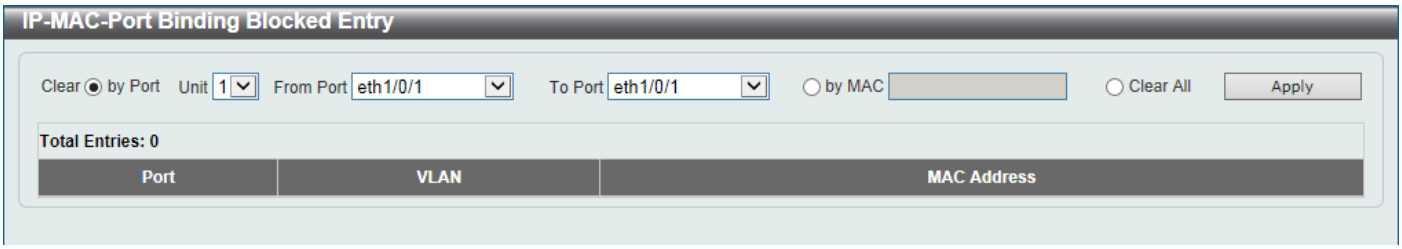


Figure 9-56 IP-MAC-Port Binding Blocked Entry Window

The fields that can be configured are described below:

Parameter	Description
Clear by Port	Select this option to clear the entry table based on the port(s) selected.
Unit	Select the Switch unit that will be clear here. This option is only available if stacking is enabled.
From Port - To Port	Select the appropriate port range that will be cleared here.
Clear by MAC	Select this option to clear the entry table based on the MAC address entered. Enter the MAC address that will be cleared in the space provided.
Clear All	Select this option to clear all entries that contain MAC addresses.

Click the **Apply** button to accept the changes made.

IPv6

IPv6 Snooping

This window is used to display and configure the IPv6 snooping settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 Snooping**, as shown below:

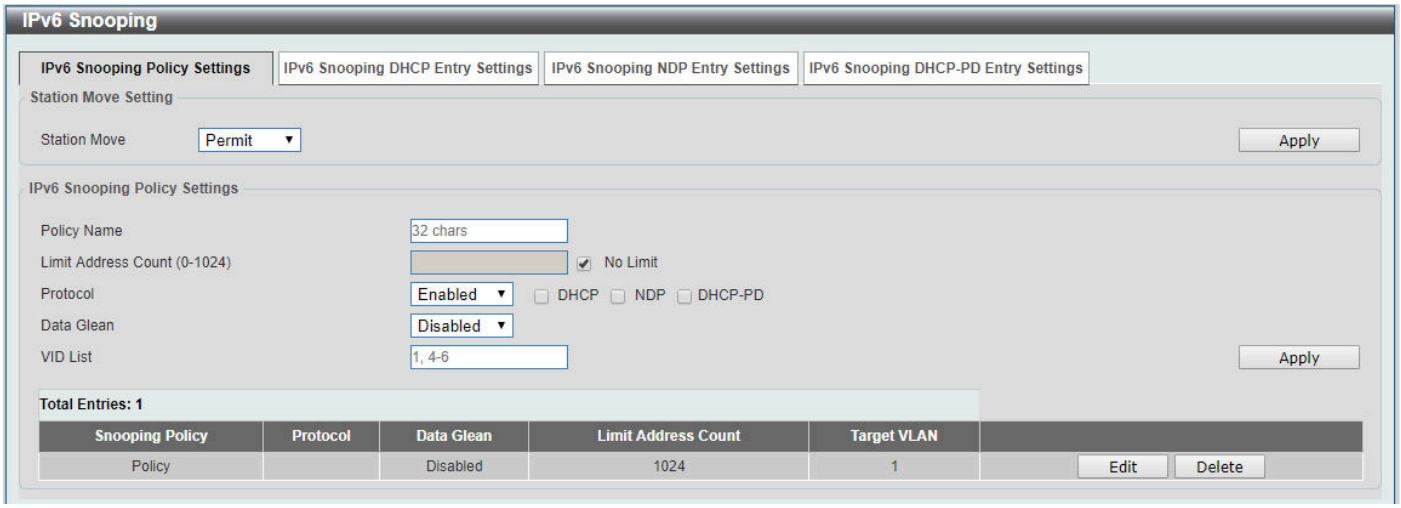


Figure 9-57 IPv6 Snooping Window

The fields that can be configured in **Station Move Setting** are described below:

Parameter	Description
Station Move	Select the station move options here. Options to choose from are **Permit** and **Deny**.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **IPv6 Snooping Policy Settings** are described below:

Parameter	Description
Policy Name	Enter the IPv6 snooping policy name used here. This name can be up to 32 characters long.
Limit Address Count	Enter the address count limit value used here. This value must be between 0 and 1024. Tick the **No Limit** option to disable this option.
Protocol	Select the protocol state here. Options to choose from are **Enabled** and **Disabled**. • Select **DHCP** to specify that addresses should be snooped in DHCPv6 packets. • Select **NDP** to specify that addresses should be snooped in NDP packets. • Select **DHCP-PD** to specify that the IPv6 prefix should be snooped in DHCPv6-PD packets. DHCPv6 snooping sniffs the DHCPv6 packets sent between the DHCPv6 client and server in the address assigning procedure. When a DHCPv6 client successfully got a valid IPv6 address, DHCPv6 snooping creates its binding database. ND Snooping is designed for a stateless auto-configuration assigned IPv6 address and manually configured IPv6 address. Before assigning an IPv6 address, the host must perform Duplicate Address Detection first. ND snooping detects DAD messages (DAD Neighbor Solicitation (NS) and DAD Neighbor Advertisement (NA)) to build its binding database. The NDP packet (NS and NA) is also used to detect whether a host is still reachable and determine whether to delete a binding or not. DHCP-PD snooping performs DHCPv6 snooping of Prefix Delegation (PD) to setup bindings between the Delegating Router (assigned with an IPv6 prefix) and the corresponding Requesting Router. The bindings can be used to validate the source prefix in the packets.

Parameter	Description
Data Glean	Select to enable or disable the data-glean function here. In some circumstances (DAD-NS packet lost or Switch reboot), a valid IPv6 address cannot be found in the binding table for some devices and as a result traffic to and from these devices are denied by the IPv6 source guard. The data-glean function provides a method for the Switch to recover the lost IPv6 addresses using IPv6 Duplicate Address Detection (DAD).
VID List	Enter the VLAN ID list used here.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

After selecting the **IPv6 Snooping DHCP Entry Settings** tab option, the following page will be available.

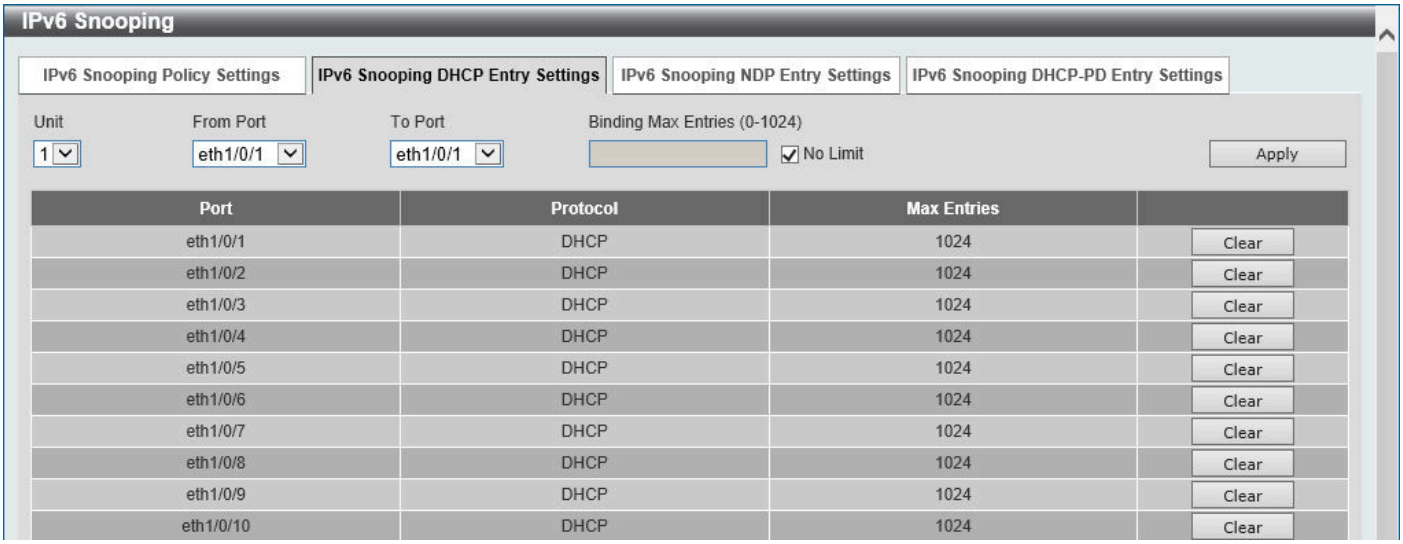


Figure 9-58 IPv6 Snooping (IPv6 Snooping DHCP Entry Settings) Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch stacking unit ID here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used here.
Binding Max Entries	Enter the maximum number of IPv6 snooping binding entries that is allowed here. The range is from 0 to 1024.

Click the **Apply** button to accept the changes made.

Click the **Clear** button to clear DHCPv6 snooping entries from the specified port.

After selecting the **IPv6 Snooping NDP Entry Settings** tab option, the following page will be available.

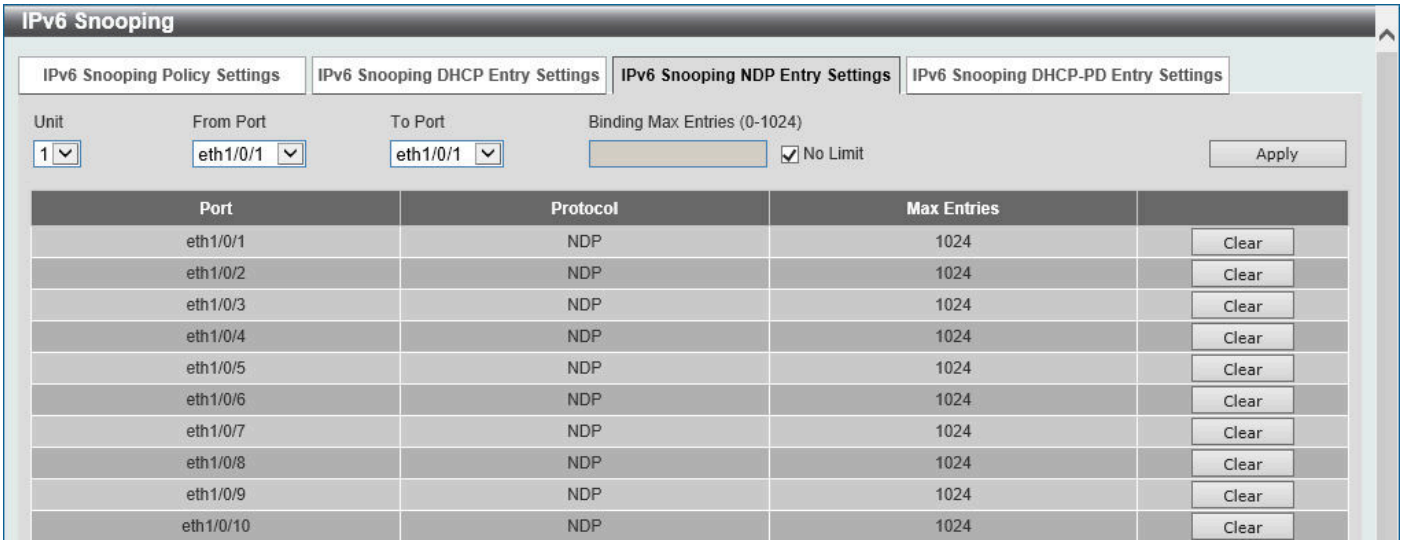


Figure 9-59 IPv6 Snooping (IPv6 Snooping NDP Entry Settings) Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch stacking unit ID here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used here.
Binding Max Entries	Enter the maximum number of IPv6 snooping binding entries that is allowed here. The range is from 0 to 1024. Or select No Limit not to restrict the number of binding entries.

Click the **Apply** button to accept the changes made.

Click the **Clear** button to clear ND snooping entries from the specified port.

After selecting the **IPv6 Snooping DHCP-PD Entry Settings** tab option, the following page will be available.

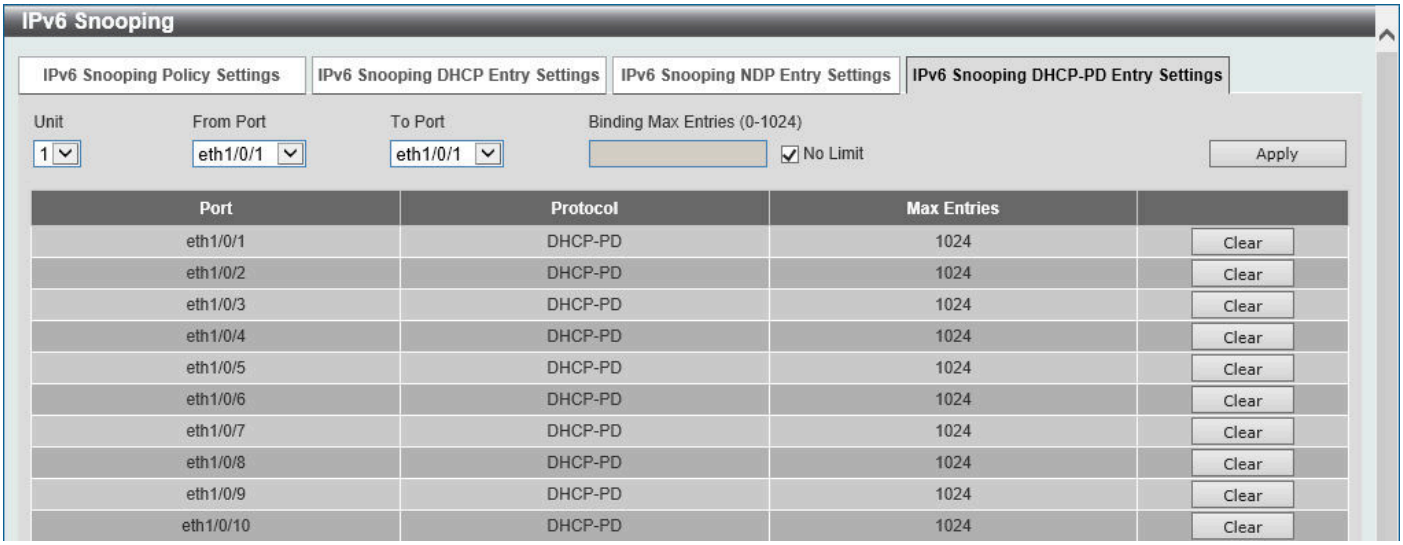


Figure 9-60 IPv6 Snooping (IPv6 Snooping DHCP-PD Entry Settings) Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch stacking unit ID here. This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used here.
Binding Max Entries	Enter the maximum number of IPv6 snooping binding entries that is allowed here. The range is from 0 to 1024. Or select No Limit not to restrict the number of binding entries.

Click the **Apply** button to accept the changes made.

Click the **Clear** button to clear DHCPv6 PD snooping entries from the specified port.

IPv6 ND Inspection

This window is used to display and configure the IPv6 ND inspection settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 ND Inspection**, as shown below:

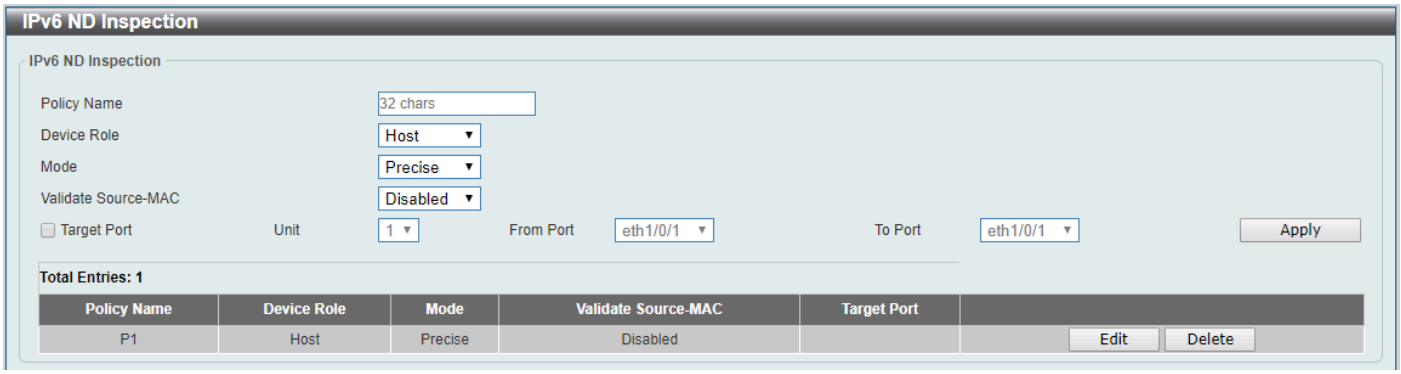


Figure 9-61 IPv6 ND Inspection Window

The fields that can be configured are described below:

Parameter	Description
Policy Name	Enter the policy name used here. This name can be up to 32 characters long.
Device Role	Select the device role here. Options to choose from are **Host** and **Router**. By default, the device's role is set as host and inspection for NS and NA messages are performed. If the device role is set as router, the NS and NA inspection is not performed. When performing NS/NA inspection, the message will be verified against the dynamic binding table learned from the ND protocol or from the DHCP.
Mode	Select the mode of ND inspection here. Options to choose from are: • **Precise** - Specifies to use the precise mode. ND inspection checks if the target address is the same as the source address in DANA/NA packets. • **Fuzzy** - Specifies to use the fuzzy mode. ND inspection checks if both the target and the source addresses exist in the binding table.
Validate Source-MAC	Select to enable or disable the validation of the source MAC address option here. When the Switch receives an ND message that contains a link-layer address, the source MAC address is checked against the link-layer address. The packet will be dropped if the link-layer address and the MAC addresses are different from each other.
Target Port	Tick this option to specify the target port and enter the following information.

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available if stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

IPv6 RA Guard

This window is used to display and configure the IPv6 Router Advertisement (RA) guard settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 RA Guard**, as shown below:

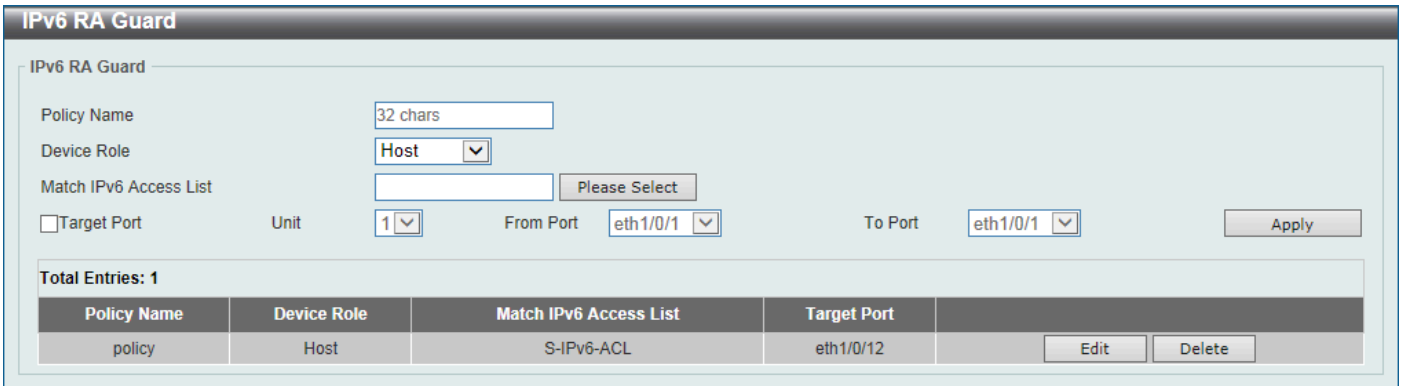


Figure 9-62 IPv6 RA Guard Window

The fields that can be configured are described below:

Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Device Role	Select the device role here. Options to choose from are **Host** and **Router**. By default, the device's role is **Host**, which will block all the RA packets. If the device's role is **Router**, RA packets will be forwarded according to the port's bound ACL.
Match IPv6 Access List	Enter or select the IPv6 access list to match here. Click the **Please Select** button to select an existing ACL from the list.
Target Port	Tick this option to specify the target port and enter the following information.
Unit	Select the Switch unit that will be used for this configuration here. This option is only available if stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

After clicking the **Please Select** button, the following window will appear:

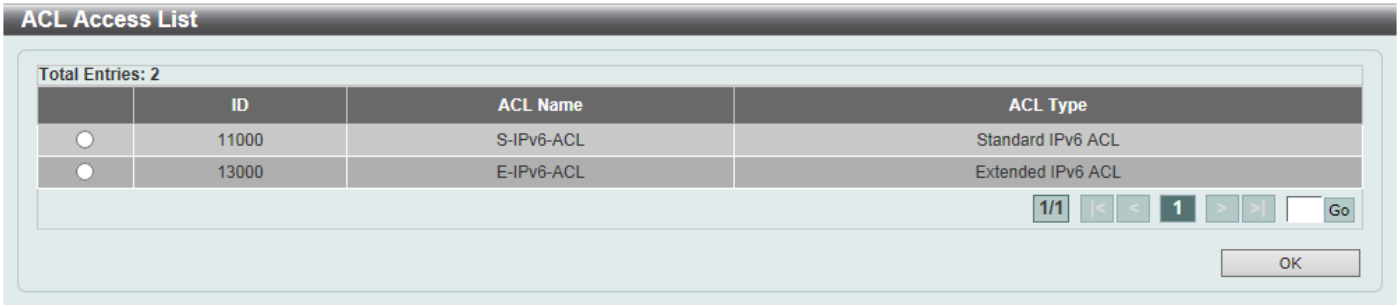


Figure 9-63 IPv6 RA Guard (Please Select) Window

Select the radio button next to the entry to use that ACL in the configuration.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **OK** button to accept the selection made.

IPv6 DHCP Guard

This window is used to display and configure the IPv6 DHCP guard settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 DHCP Guard**, as shown below:

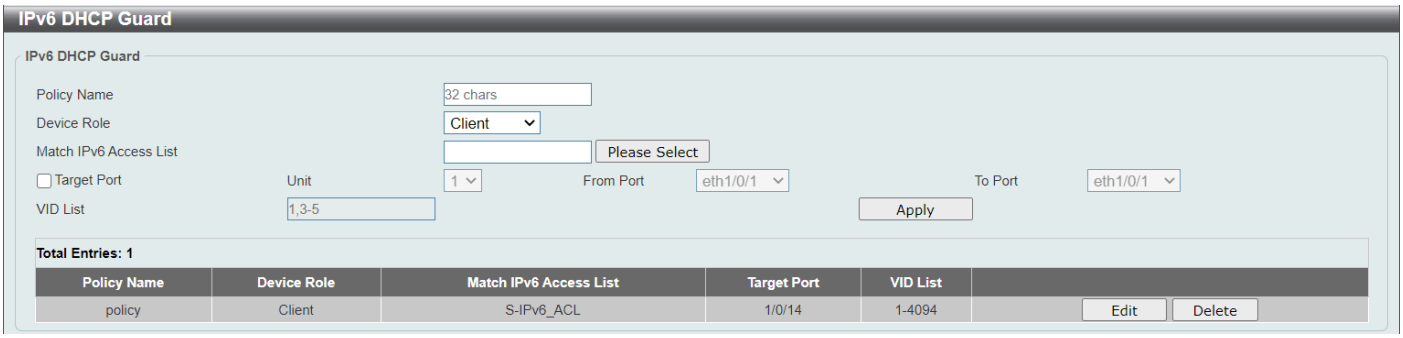


Figure 9-64 IPv6 DHCP Guard Window

The fields that can be configured are described below:

Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Device Role	Select the device role here. Options to choose from are **Client** and **Server**. By default, the device's role is set as **Client**, which will block all the DHCPv6 packets from the DHCPv6 Server. If the device's role is set as **Server**, DHCPv6 Server packets will be forwarded according to the port's bound ACL.
Match IPv6 Access List	Enter or select the IPv6 access list to match here. Click the **Please Select** button to select an existing ACL from the list.
Target Port	Tick this option to specify the target port.
Unit	Select the Switch unit that will be used for this configuration here. This option is only available if stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
VID List	Enter the VLAN ID list for configuration. Use "-" to specify the list range and "," to separate the values of the list. For example, 1,3-5.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

After clicking the **Please Select** button, the following window will appear:

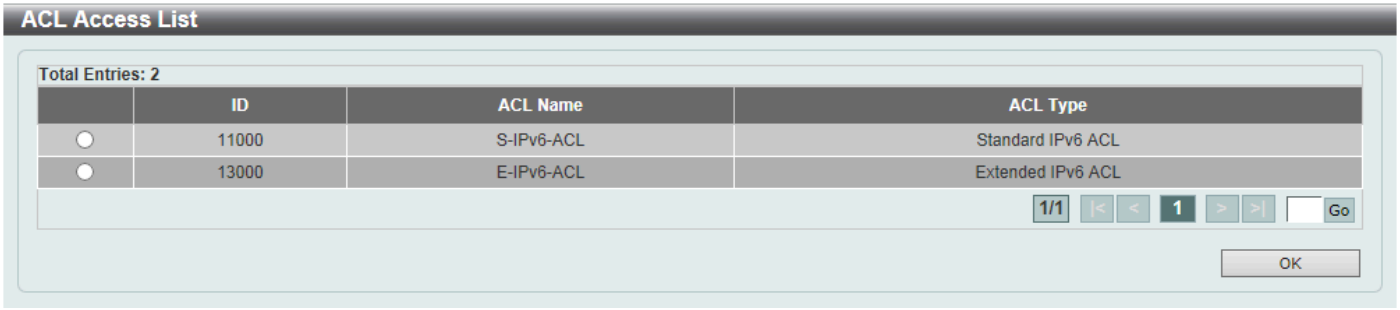


Figure 9-65 IPv6 DHCP Guard (Please Select) Window

Select the radio button next to the entry to use that ACL in the configuration.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **OK** button to accept the selection made.

IPv6 Source Guard

IPv6 Source Guard Settings

This window is used to display and configure the IPv6 source guard settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 Source Guard > IPv6 Source Guard Settings**, as shown below:

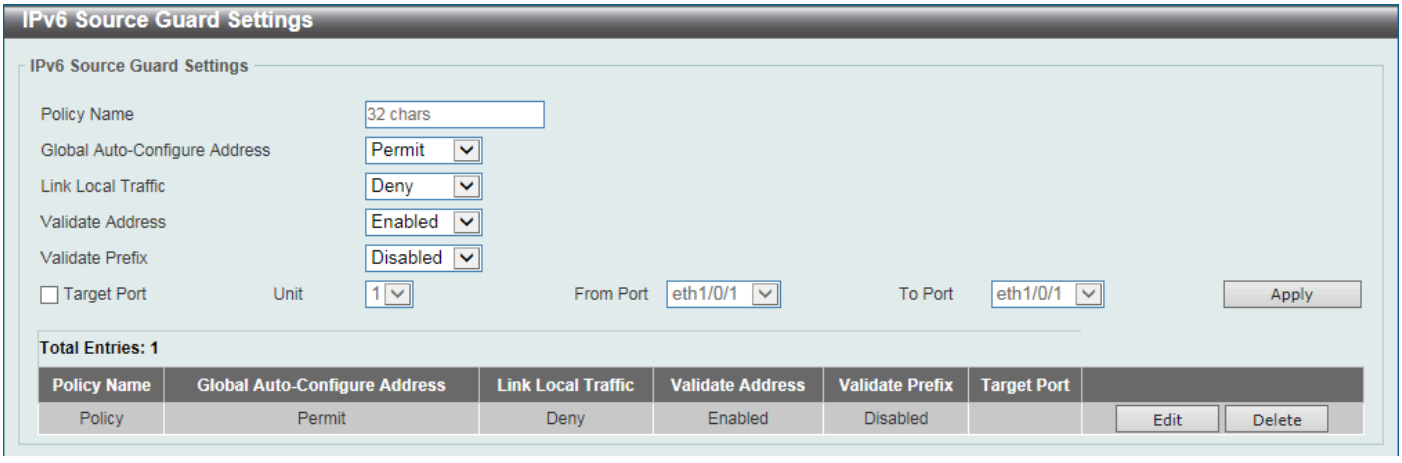


Figure 9-66 IPv6 Source Guard Settings Window

The fields that can be configured are described below:

Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Global Auto-Configure Address	Select to permit of deny data traffic from the auto-configured global address. It is useful when all global addresses on a link are assigned by DHCP and the

Parameter	Description
	administrator that wants to block hosts with self-configured addresses from sending traffic.
Link Local Traffic	Select to permit or deny hardware permitted data traffic send by the link-local address.
Validate Address	Select to enable or disable the validate address feature here. This is used to enable the IPv6 source guard to perform the validate address feature.
Validate Prefix	Select to enable or disable the validate prefix feature here. This is used to enable the IPv6 source guard to perform the IPv6 prefix-guard operation.
Target Port	Tick this option to specify the target port.
Unit	Select the Switch unit that will be used for this configuration here. This option is only available if stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

IPv6 Neighbor Binding

This window is used to display and configure the IPv6 neighbor binding settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 Source Guard > IPv6 Neighbor Binding**, as shown below:

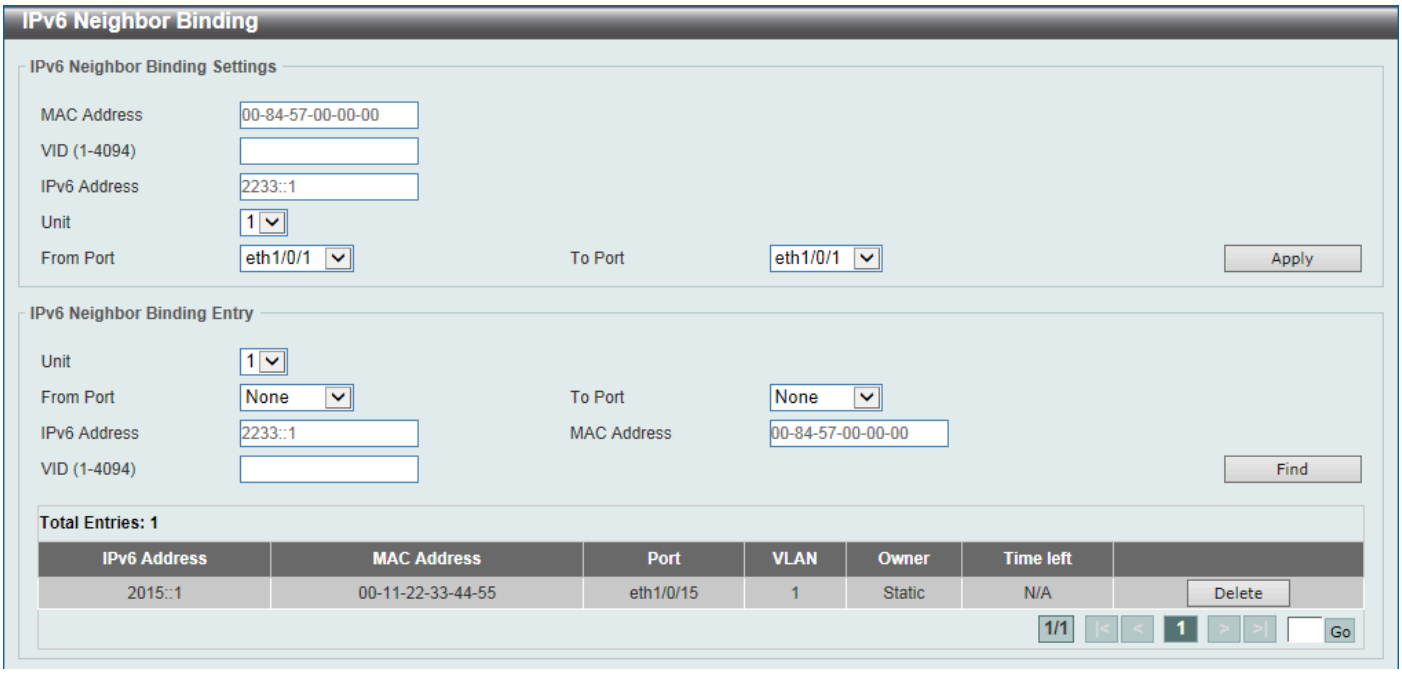


Figure 9-67 IPv6 Neighbor Binding Window

The fields that can be configured in **IPv6 Neighbor Binding Settings** are described below:

Parameter	Description
MAC Address	Enter the MAC address used here in the format:xx-xx-xx-xx-xx-xx (x is a hexadecimal digit).

Parameter	Description
VID	Enter the VLAN ID used here. This value must be between 1 and 4094.
IPv6 Address	Enter the IPv6 address in the format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (x is a hexadecimal digit).
Unit	Select the Switch unit that will be used for this configuration here.This option is only available if stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **IPv6 Neighbor Binding Entry** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this search here. This option is only available if stacking is enabled.
From Port - To Port	Select the appropriate port range used for the search here.
IPv6 Address	Enter the IPv6 address to find here.
MAC Address	Enter the MAC address to find here.
VID	Enter the VLAN ID to find here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

DHCP Server Screening

This function allows users to not only to restrict all DHCP server packets but also to receive any specified DHCP server packet by any specified DHCP client. It is useful when one or more DHCP servers are present on the network and both provide DHCP services to different groups of clients.

When the DHCP Server Screening function is enabled on a port, all DHCP server packets received on this ports will be redirected to the CPU for a software-based check. Legal DHCP server packets will be forwarded out and illegal DHCP server packets will be dropped.

When DHCP Server Screening function is enabled all DHCP Server packets will be filtered from a specific port.

DHCP Server Screening Global Settings

This window is used to display and configure the global DHCP server screening settings.

To view the following window, click **Security > DHCP Server Screening > DHCP Server Screening Global Settings**, as shown below:

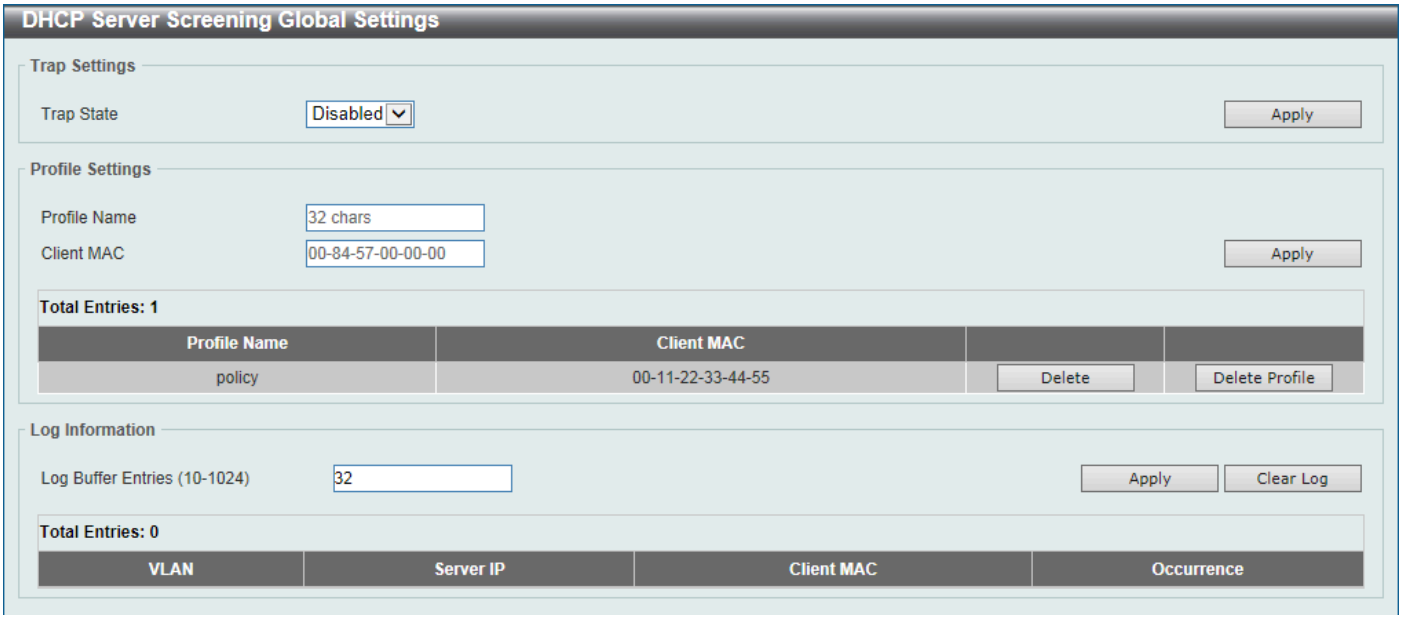


Figure 9-68 DHCP Server Screening Global Settings Window

The fields that can be configured in **Trap Settings** are described below:

Parameter	Description
Trap State	Select to enable or disable the DHCP server screening trap here.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Profile Settings** are described below:

Parameter	Description
Profile Name	Enter the DHCP server screening profile name here. This name can be up to 32 characters long.
Client MAC	Enter the MAC address used here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Click the **Delete Profile** button to remove the specified profile.

The fields that can be configured in **Log Information** are described below:

Parameter	Description
Log Buffer Entries	Enter the logged buffer entries value here. This value must be between 10 and 1024. By default, this value is 32.

Click the **Apply** button to accept the changes made.

Click the **Clear Log** button to clear the log.

DHCP Server Screening Port Settings

This window is used to display and configure the DHCP server screening port settings.

To view the following window, click **Security > DHCP Server Screening > DHCP Server Screening Port Settings**, as shown below:

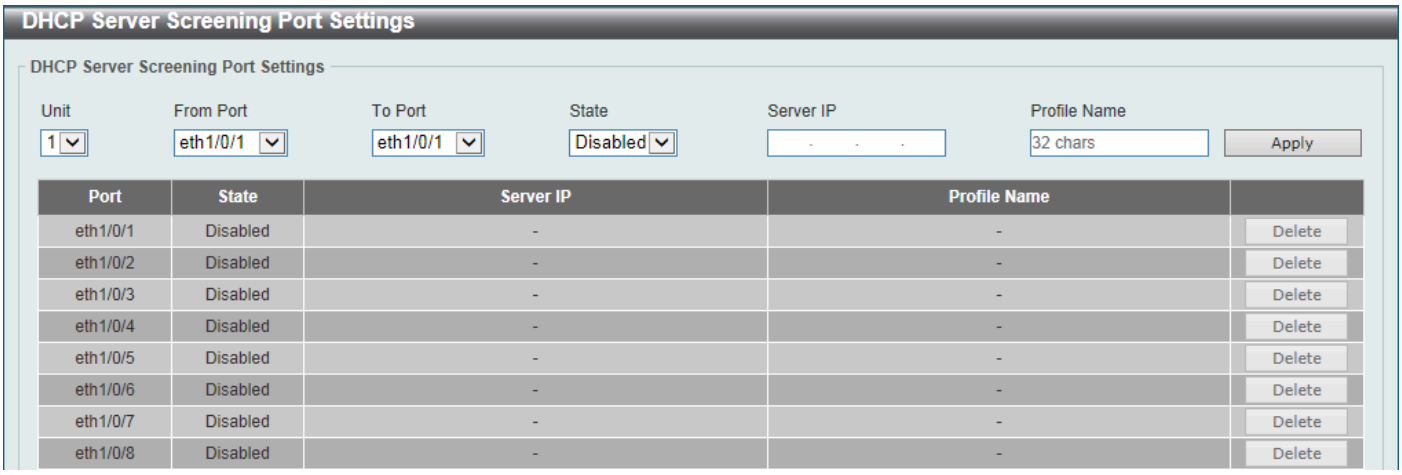


Figure 9-69 DHCP Server Screening Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available if stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the DHCP server screening function on the port(s) specified.
Server IP	Enter the DHCP server IP address here.
Profile Name	Enter the DHCP server screening profile that will be used for the port(s) specified here. Refer to **Security > DHCP Server Screening > DHCP Server Screening Port Settings**.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

ARP Spoofing Prevention

This window is used to display and configure the ARP spoofing prevention settings. When an entry is created, ARP packets whose sender IP address matches the gateway IP address, of an entry, but its sender MAC address field does not match the gateway MAC address, of the entry, will be dropped by the system. The ASP will bypass the ARP packets whose sender IP address doesn't match the configured gateway IP address.

If an ARP address matches a configured gateway's IP address, MAC address, and port list, then bypass the Dynamic ARP Inspection (DAI) check no matter if the receiving port is ARP trusted or untrusted.

To view the following window, click **Security > ARP Spoofing Prevention**, as shown below:



Figure 9-70 ARP Spoofing Prevention Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available if stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
Gateway IP	Enter the gateway IP address used here.
Gateway MAC	Enter the gateway MAC address used here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

BPDU Attack Protection

This window is used to display and configure the BPDU attack protection settings. In generally, there are two states in the BPDU attack protection function. One is normal state, and another is under attack state. The under attack state has three modes: drop, block, and shutdown. A BPDU protection enabled port will enter an under attack state when it receives one STP BPDU packet and it will take action based on the configuration.

BPDU protection has a higher priority than the (Forward BPDU) FBPDU setting configured by configure STP command in the determination of BPDU handling. That is, when FBPDU is configured to forward STP BPDU but BPDU protection is enabled, then the port will not forward STP BPDU.

BPDU protection also has a higher priority than the BPDU tunnel port setting in determination of BPDU handling. That is, when a port is configured as BPDU tunnel port for STP, it will forward STP BPDU. But if the port is BPDU protection enabled. Then the port will not forward STP BPDU.

To view the following window, click **Security > BPDU Attack Protection**, as shown below:

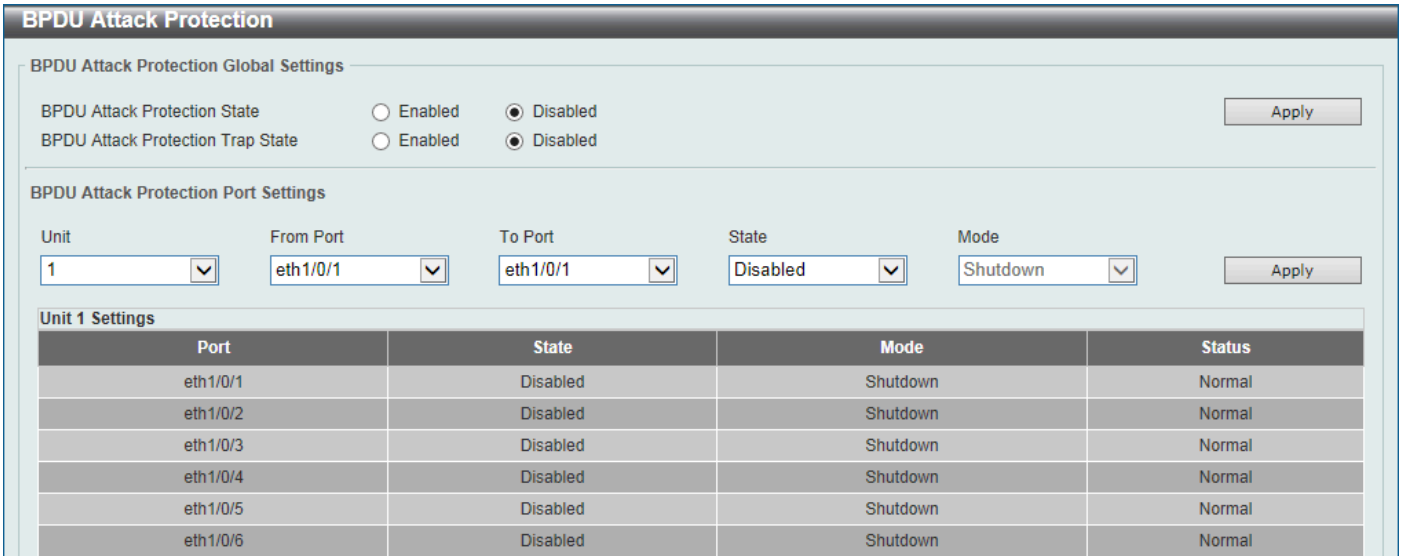


Figure 9-71 BPDU Attack Protection Window

The fields that can be configured in **BPDU Attack Protection Global Settings** are described below:

Parameter	Description
BPDU Attack Protection State	Select to enable or disable the global BPDU attack protection state here.
BPDU Attack Protection Trap State	Select to enable or disable the BPDU attack protection trap state here.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **BPDU Attack Protection Port Settings** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available if stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the BPDU attack protection state on the port(s) specified.
Mode	Select the BPDU attack protection mode that will be applied to the port(s) specified. Options to choose from are **Drop**, **Block** and **Shutdown**. • **Drop** - Drop all received BPDU packets when the port enters under attack state. • **Block** - Drop all packets (including BPDU and normal packets) when the port enters under attack state. • **Shutdown** - Shut down the port when the port enters under attack state.
You can configure errdisable trap and recovery settings in **System > Port Configuration > Error Disable Settings**.	

Click the **Apply** button to accept the changes made.

MAC Authentication

This window is used to display and configure the MAC authentication settings. MAC authentication is a feature designed to authenticate a user by MAC address when the user is trying to access the network via the Switch. The

Switch itself can perform the authentication based on a local database or be a RADIUS client and perform the authentication process via the RADIUS protocol with a remote RADIUS server.

To view the following window, click **Security > MAC Authentication**, as shown below:

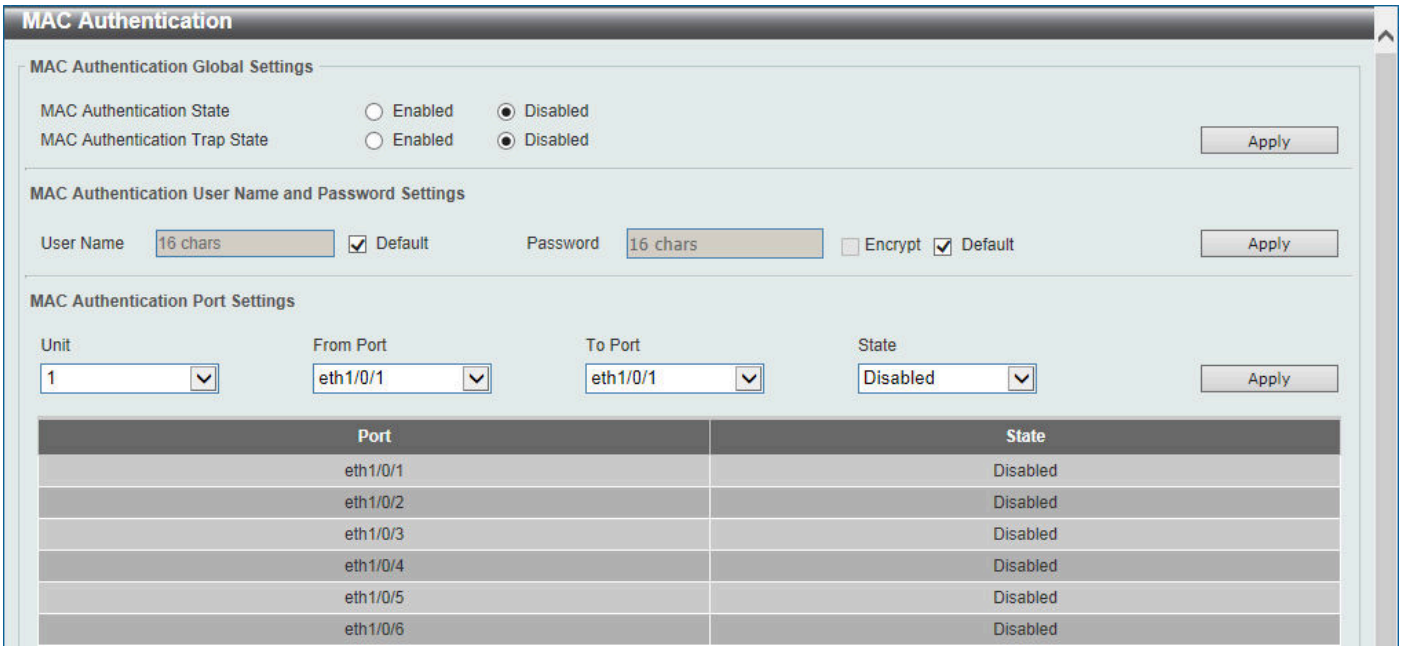


Figure 9-72 MAC Authentication Window

The fields that can be configured in **MAC Authentication Global Settings** are described below:

Parameter	Description
MAC Authentication State	Select to enable or disable the global MAC authentication state.
MAC Authentication Trap State	Select to enable or disable the MAC authentication trap state.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **MAC Authentication User Name and Password Settings** are described below:

Parameter	Description
User Name	Enter the username used for MAC authentication here. This name can be up to 16 characters long. Tick the **Default** option to restore the username to the client MAC address here.
Password	Enter the password used for MAC authentication here. Tick the **Encrypt** option to save this password in the encrypted form. Tick the **Default** option to restore the password to the client MAC address here.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **MAC Authentication Port Settings** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available if stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable MAC authentication for the port(s) specified here.

Click the **Apply** button to accept the changes made.

Web-based Access Control

Web-based Access Control (WAC) is a feature designed to authenticate a user when the user is trying to access the Internet via the Switch. The authentication process uses the HTTP or HTTPS protocol. The Switch enters the authenticating stage when users attempt to browse Web pages (e.g., http://www.dlink.com) through a Web browser. When the Switch detects HTTP or HTTPS packets and this port is unauthenticated, the Switch will redirect user to an authentication Web page. Users are not able to access the Internet until the authentication process is passed.

The Switch can be the authentication server itself and do the authentication based on a local database, or be a RADIUS client and perform the authentication process via the RADIUS protocol with a remote RADIUS server. The client user initiates the authentication process of WAC by attempting to gain Web access.

D-Link's implementation of WAC uses a virtual IP that is exclusively used by the WAC function and is not known by any other modules of the Switch. In fact, to avoid affecting a Switch's other features, WAC will only use a virtual IP address to communicate with hosts. Thus, all authentication requests must be sent to a virtual IP address but not to the IP address of the Switch's physical interface.

Virtual IP works like this, when a host PC communicates with the WAC Switch through a virtual IP, the virtual IP is transformed into the physical IPIF (IP interface) address of the Switch to make the communication possible. The host PC and other servers' IP configurations do not depend on the virtual IP of WAC. The virtual IP does not respond to any ICMP packets or ARP requests, which means it is not allowed to configure a virtual IP on the same subnet as the Switch's IPIF (IP interface) or the same subnet as the host PCs' subnet.

As all packets to a virtual IP from authenticated and authenticating hosts will be trapped to the Switch's CPU, if the virtual IP is the same as other servers or PCs, the hosts on the WAC-enabled ports cannot communicate with the server or PC which really own the IP address. If the hosts need to access the server or PC, the virtual IP cannot be the same as the one of the server or PC. If a host PC uses a proxy to access the Web, to make the authentication work properly the user of the PC should add the virtual IP to the exception of the proxy configuration. If the virtual IP is not configured, then access cannot start Web authentication.

The Switch's implementation of WAC features a user-defined port number that allows the configuration of the TCP port for either the HTTP or HTTPS protocols. This TCP port for HTTP or HTTPs is used to identify the HTTP or HTTPs packets that will be trapped to the CPU for authentication processing, or to access the login page. If not specified, the default port number for HTTP is 80 and the default port number for HTTPS is 443. If no protocol is specified, the default protocol is HTTP.

The following diagram illustrates the basic six steps all parties go through in a successful Web Authentication process:

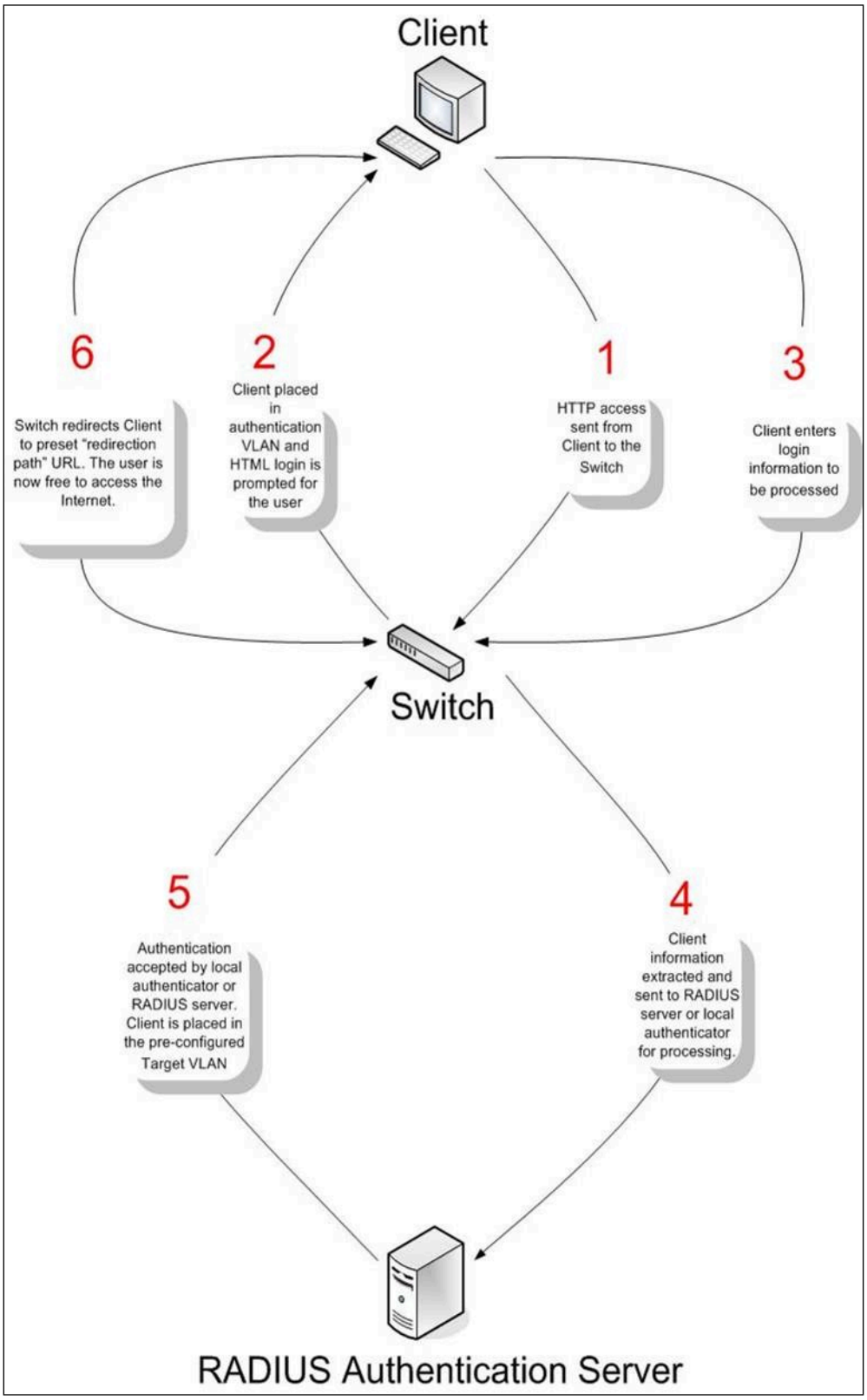


Figure 9-73 RADIUS Authentication Server

Conditions and Limitations

- If the client is utilizing DHCP to attain an IP address, the authenticating VLAN must provide a DHCP server or a DHCP relay function so that client may obtain an IP address.

- Certain functions exist on the Switch that will filter HTTP packets, such as the ACL function. The user needs to be very careful when setting filter functions for the target VLAN, so that these HTTP packets are not denied by the Switch.
- If a RADIUS server is to be used for authentication, the user must first establish a RADIUS Server with the appropriate parameters, including the target VLAN, before enabling Web Authentication on the Switch.

Web Authentication

This window is used to display and configure the Web authentication settings.

To view the following window, click **Security > Web-based Access Control > Web Authentication**, as shown below:

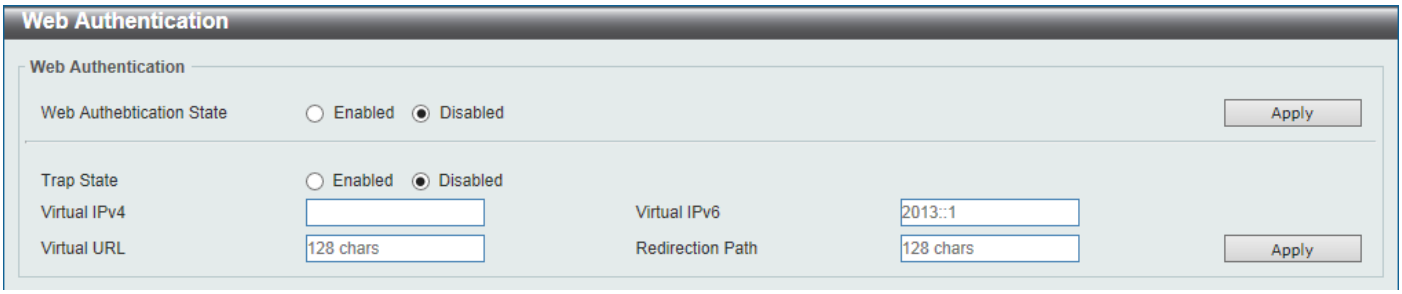


Figure 9-74 Web Authentication Window

The fields that can be configured are described below:

Parameter	Description
Web Authentication State	Select to enable or disable the global Web authentication state.
Trap State	Select to enable or disable the Web authentication trap state.
Virtual IPv4	Enter the virtual IPv4 address used here. The virtual IP of Web authentication is just the characterization of the Web authentication function on the Switch. All Web authentication processes communicate with this IP address, however, the virtual IP does not respond to any ICMP packet or ARP request. So it's not allowed to configure virtual IP in the same subnet as the Switch's IP interface or the same subnet as the host PCs' subnet, otherwise the Web authentication cannot operate correctly. The defined URL only takes effect when the virtual IP address is configured. The users get the FQDN URL stored on the DNS server to get the virtual IP address. The obtained IP address must match the virtual IP address configured by the command. If the IPv4 virtual IP is not configured, the IPv4 access cannot start a Web authentication.
Virtual IPv6	Enter the virtual IPv6 address used here. If the IPv6 virtual IP is not configured, the IPv6 access cannot start a Web authentication.
Virtual URL	Enter the FQDN URL used here. This FQDN URL can be up to 128 characters.
Redirection Path	Enter the redirection path here. This path can be up to 128 characters.

Click the **Apply** button to accept the changes made.

NOTE: The WAC virtual IP address should be configured before enabling WAC because WAC will not function correctly if the virtual IP is not configured.

WAC Port Settings

This window is used to display and configure the WAC port settings.

To view the following window, click **Security > Web-based Access Control > WAC Port Settings**, as shown below:

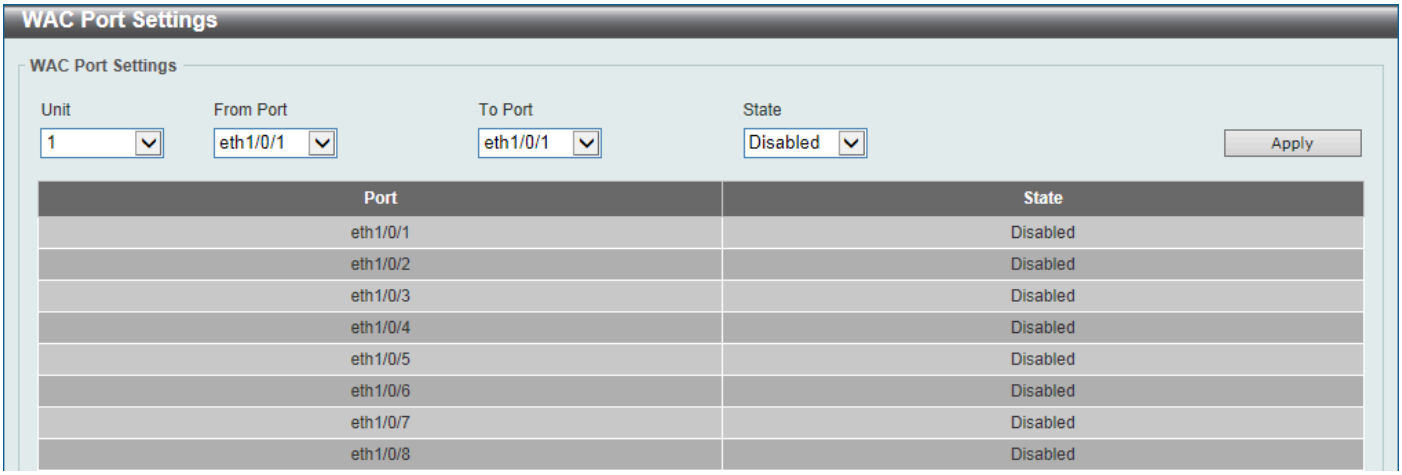


Figure 9-75 WAC Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available if stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the WAC feature on the port(s) specified.

Click the **Apply** button to accept the changes made.

WAC Customize Page

This window is used to display and configure the WAC customized login page.

To view the following window, click **Security > Web-based Access Control > WAC Customize Page**, as shown below:

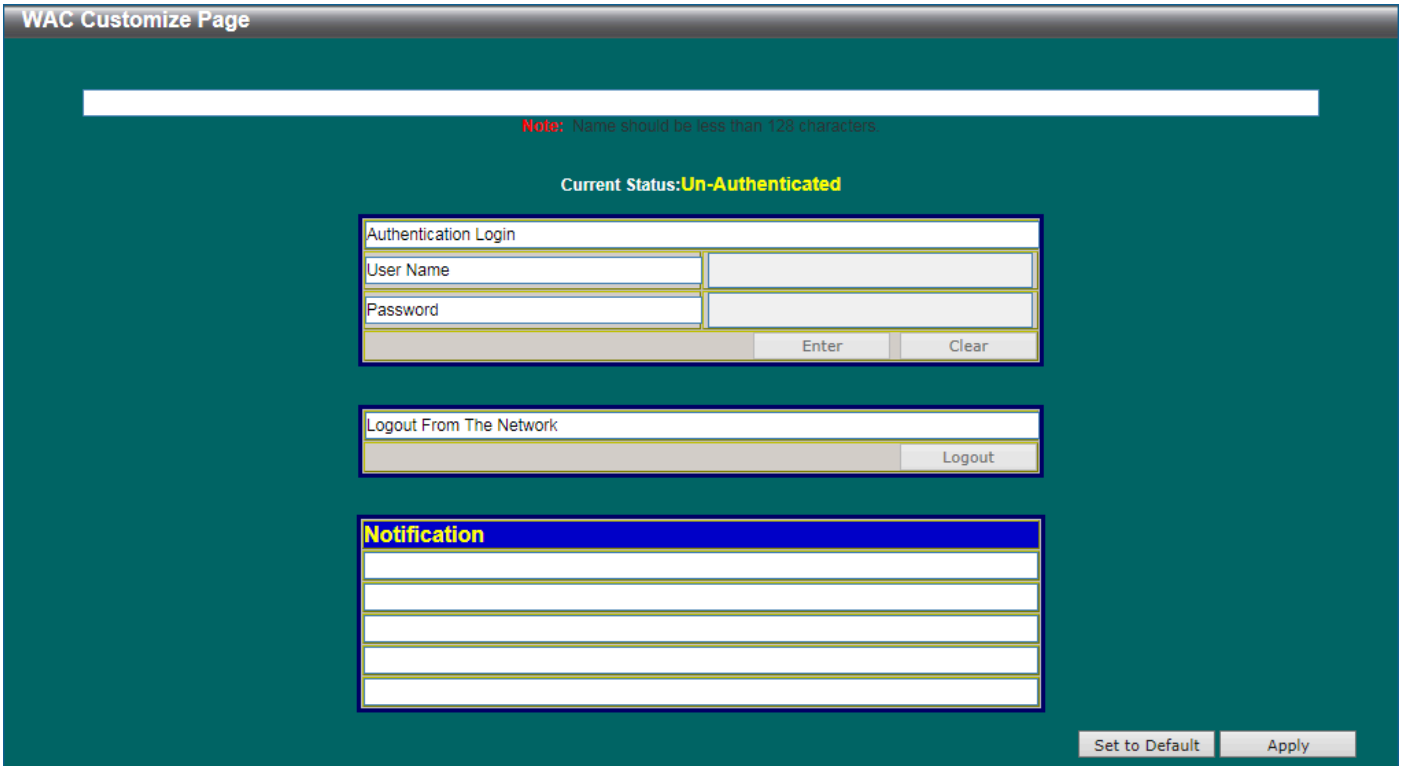


Figure 9-76 WAC Customize Page Window

The fields that can be configured are described below:

Parameter	Description
Page Title	Enter a custom page title message at the top. This message can be up to 128 characters. The default is empty.
Login Window Title	Enter a custom login window title here. This title can be up to 64 characters. The default is Authentication Login.
User Name Title	Enter a custom username title here. This title can be up to 32 characters. The default is User Name.
Password Title	Enter a custom password title here. This title can be up to 32 characters. The default is Password.
Logout Window Title	Enter a custom logout window title here. This title can be up to 64 characters. The default is Logout From The Network.
Notification	Enter additional information to display in the notification area here. This information can be up to 128 characters for each line. There are 5 lines available for additional information.

Click the **Set to Default** button to replace the information with the default information.

Click the **Apply** button to accept the changes and preview the customized page

Network Access Authentication

Guest VLAN

This window is used to display and configure the network access authentication guest VLAN settings.

To view the following window, click **Security > Network Access Authentication > Guest VLAN**, as shown below:

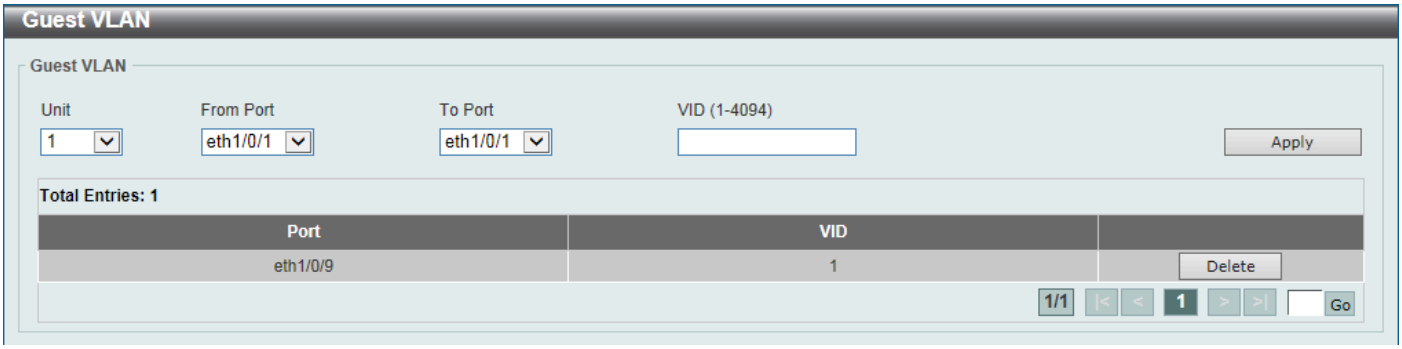


Figure 9-77 Guest VLAN Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.This option is only available if stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
VID	Enter the VLAN ID used here. This value must be between 1 and 4094.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Network Access Authentication Global Settings

This window is used to display and configure the global Network Access Authentication settings.

To view the following window, click **Security > Network Access Authentication > Network Access Authentication Global Settings**, as shown below:

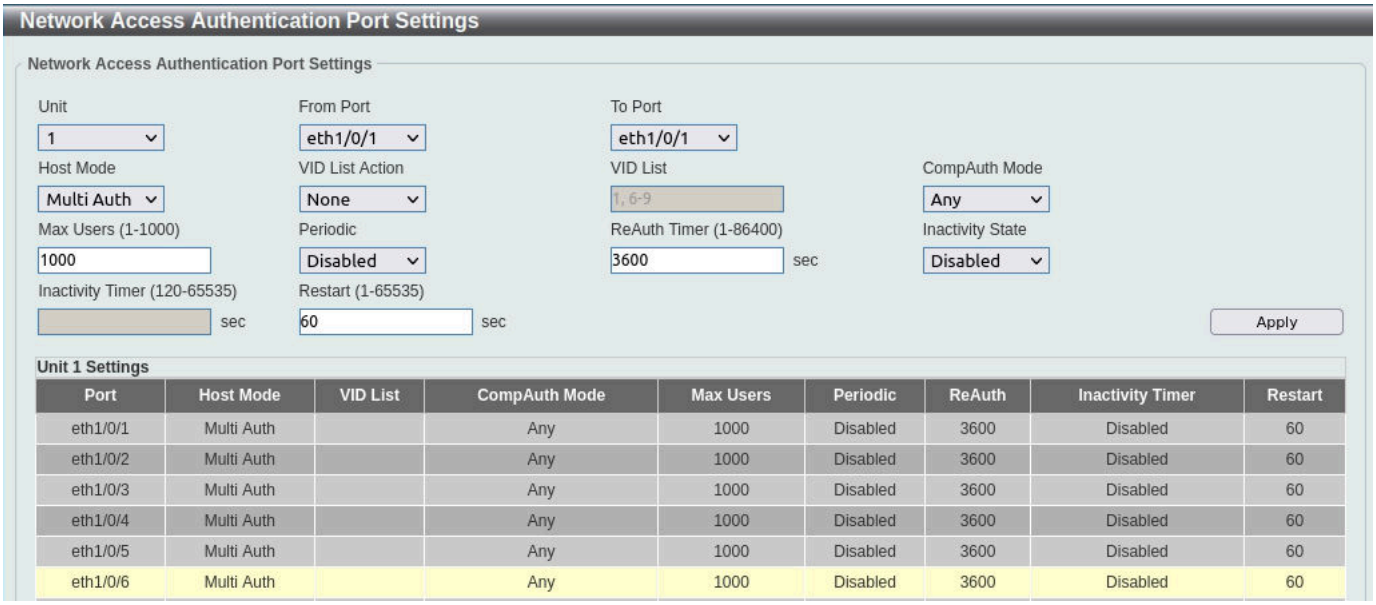


Figure 9-78 Network Access Authentication Global Settings Window

The fields that can be configured in **Network Access Authentication MAC Format Settings** are described below:

Parameter	Description
Case	Select the case format that will be used for the network access authentication MAC address here. Options to choose from are **Lowercase** and **Uppercase**.
Delimiter	Select the delimiter that will be used here. Options to choose from are: • **Hyphen** - Specifies that the format will be AA-BB-CC-DD-EE-FF. • **Colon** - Specifies that the format will be AA:BB:CC:DD:EE:FF. • **Dot** - Specifies that the format will be AA.BB.CC.DD.EE.FF. **None** - Specifies that when not using any delimiter, the format will be AABBCCDDEEFF.
Delimiter Number	Select the delimiter number here. Options to choose from are: • **1** - Single delimiter, the format is: AABBCC.DDEEFF. • **2** - Double delimiters, the format is: AABB.CCDD.EEFF. • **5** - Multiple delimiters, the format is: AA.BB.CC.DD.EE.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **General Settings** are described below:

Parameter	Description
Max Users	Enter the maximum number of users allowed here. This value must be between 1 and 1000. By default, this option is 1000.
Deny MAC-Move	Select to enable or disable the deny MAC-move feature here. This option controls whether to allow authenticated hosts to do roaming across different Switch ports and only controls whether a host, which is authenticated at a port set to the multi-authenticate mode, is allowed to move to another port. If a station is allowed to move, there are two situations. It may either need to be re-authenticated or directly moved to the new port without re-authentication based on the following rule. If the new port has the same authentication configuration as the original port, then re-authentication is not needed. The host will inherit the same authorization attributes with new port. The authenticated host can do roaming from port 1 to port 2 and inherit the authorization attributes without re-authentication. If the new port has the different authentication configuration as the original port, then re-authentication is needed. The authenticated host on port 1 can move and re-authenticated by port 2. If the new port has no authentication method enabled, then the station is directly moved to the new port. The session with the original port is removed. The authenticated host on port 1 can be moved to port 2. If this feature is disabled and an authenticated host moves to another port, then this is treated as a violation error.
Authorization State	Select to enable or disable the authorized state here. The option is used to enable or disable the acceptance of an authorized configuration. When authorization is enabled for authentication, the authorized attributes (for example VLAN, 802.1p default priority, bandwidth, and ACL) assigned by the RADIUS server will be accepted if the authorization status is enabled. Bandwidth and ACL are assigned on a per-port basis. If in the multi-authenticated mode, VLAN and 802.1p are assigned on a per-host basis. Otherwise, Bandwidth and ACL are assigned on a per-port basis.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **User Information** are described below:

Parameter	Description
User Name	Enter the user name used here. This name can be up to 32 characters long.
VID	Enter the VLAN ID used here.
Password Type	Select the password type option here. Options to choose from are **Plain Text** and **Encrypted**.
Password	Enter the password used here. For plain text, the limit is 32 characters. For encrypted, enter 44 characters.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Network Access Authentication Port Settings

This window is used to display and configure the network access authentication port settings.

To view the following window, click **Security > Network Access Authentication > Network Access Authentication Port Settings**, as shown below:

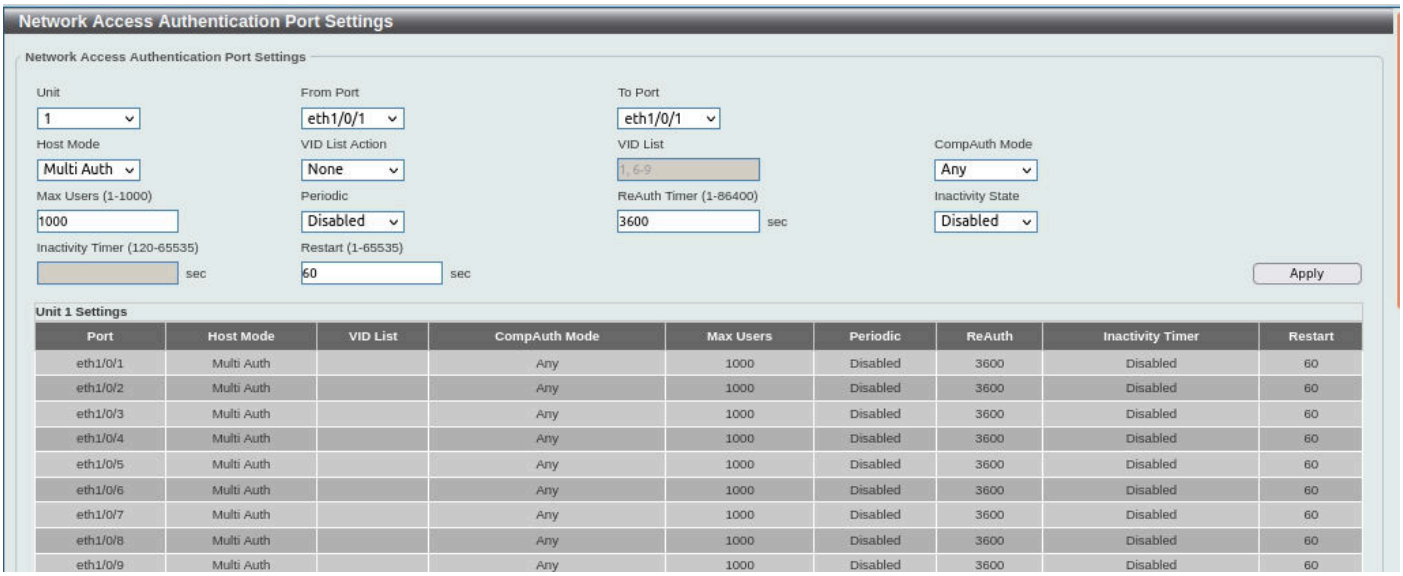


Figure 9-79 Network Access Authentication Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available if stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
Host Mode	Select the host mode option that will be associated with the selected port(s) here. Options to choose from are **Multi Host** and **Multi Auth**. If the port is operated in the multi-host mode, and if one of the hosts is authenticated, then all other hosts are allowed to access the port. According to 802.1X authentication, if the re-authentication fails or the authenticated user logs off, the port will be blocked for a quiet period. The port restores the processing of EAPOL packets after the quiet period. If the port is operated in the multi-authenticated mode, then each host needs to be authenticated individually to access the port. A host is represented by its MAC address. Only the authorized host is allowed to access.

Parameter	Description
VID List Action	After selecting the **Multi Auth** option as the **Host Mode**, this and the following parameter will be available. Select the VID list action here. Options to choose from are **None**, **Add**, and **Delete**.
VID List	Enter the VLAN ID used here. This is useful when different VLANs on the Switch have different authentication requirements. After the client is authenticated, the client will not be re-authenticated when received from other VLANs. This option is useful for trunk ports to do per-VLAN authentication control. When a port's authentication mode is changed to multi-host, the previous authentication VLAN(s) on this port will be cleared.
CompAuth Mode	Select the compound authentication mode option here. Options to choose from are **Any** and **MAC-WAC**. • Selecting **Any** specifies that if any of the authentication method (802.1X, MAC-based Access Control or WAC) to passes, then pass. • Selecting **MAC-WAC** specifies to verify MAC-based authentication first. If the client passes, WAC will be verified next. Both authentication methods need to be passed.
Max Users	Enter the maximum users value used here. This value must be between 1 and 1000.
Periodic	Select to enable or disable periodic re-authentication for the selected port here. This parameter only affects the 802.1X protocol.
ReAuth Timer	Enter the re-authentication timer value here. This value must be between 1 and 86400 seconds. By default, this value is 3600 seconds.
Inactivity State	Select to enable or disable the inactivity state here. Select the **Time** option to enable this feature.
Inactivity Timer	When the Time option is selected for **Inactivity State**, enter the inactivity timer value here. This value must be between 120 and 65535 seconds. This parameter only affects the WAC authentication protocol.
Restart	Enter the restart time value used here. This value must be between 1 and 65535 seconds.

Click the **Apply** button to accept the changes made.

Network Access Authentication Sessions Information

This window is used to view and clear the network access authentication session information.

To view the following window, click **Security > Network Access Authentication > Network Access Authentication Sessions Information**, as shown below:

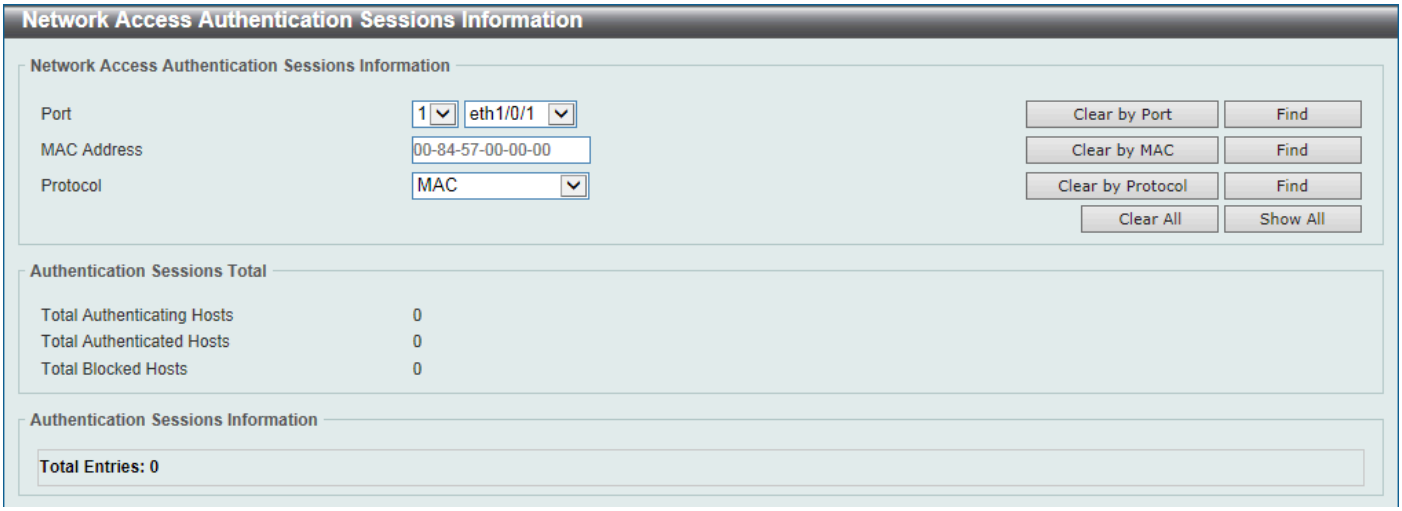


Figure 9-80 Network Access Authentication Sessions Information Window

The fields that can be configured are described below:

Parameter	Description
Port	Select the appropriate Switch unit and port used for the query here.
MAC Address	Enter the MAC address used here.
Protocol	Select the protocol option used here. Options to choose from are **MAC**, **WAC**, and **DOT1X**.

Click the **Clear by Port** button to the clear the information based on the port selected.

Click the **Clear by MAC** button to the clear the information based on the MAC address entered.

Click the **Clear by Protocol** button to the clear the information based on the protocol selected.

Click the **Clear All** button to clear all the information in this table.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to locate and display all the entries.

Safeguard Engine

Periodically, malicious hosts on the network will attack the Switch by utilizing packet flooding (ARP Storm) or other methods. These attacks may increase the Switch's CPU load beyond its capability. To alleviate this problem, the Safeguard Engine function was added to the Switch's software.

The Safeguard Engine can help the overall operability of the Switch by minimizing the workload of the Switch while the attack is ongoing, thus making it capable to forward essential packets over its network in a limited bandwidth.

If the CPU load rises above the rising threshold value, the Safeguard Engine function will be activated and the Switch will enter the exhausted mode. In the exhausted mode, the Switch will limit the bandwidth available for ARP and broadcast IP packets. If the CPU load falls below the falling threshold value, the Safeguard Engine will be deactivated and the Switch will exit the exhausted mode and enter the normal mode.

Packets that are destined to the CPU can be classified into three groups. These groups, otherwise known as sub-interfaces, are logical interfaces that the CPU will use to identify certain types of traffic. The three groups are **Protocol**, **Manage**, and **Route**. Generally, the **Protocol** group should receive the highest priority when the Switch's CPU processes received packets and the **Route** group should receive the lowest priority as the Switch's CPU usually does get involved in the processing of routing packets. In the **Protocol** group, packets are protocol control packets identified by the router. In the **Manage** group, packets are destined to any router or system network management

interface by means of interactive access protocols, like Telnet and SSH. In the **Route** group, packets are identified as traversing routing packets that is generally processed by the router CPU.

In the following table a list of supported protocols is displayed with their respective sub-interfaces (groups):

Protocol Name	Sub-interface (Group)	Description
802.1X	Protocol	Port-based Network Access Control
ARP	Protocol	Address resolution Protocol
DHCP	Protocol	Dynamic Host Configuration Protocol
DNS	Protocol	Domain Name System
GVRP	Protocol	GARP VLAN Registration Protocol
ICMPv4	Protocol	Internet Control Message Protocol
ICMPv6-Neighbor	Protocol	IPv6 Internet Control Message Protocol Neighbor Discovery Protocol (NS/NA/RS/RA)
ICMPv6-Other	Protocol	IPv6 Internet Control Message Protocol except Neighbor Discovery Protocol (NS/NA/RS/RA)
IGMP	Protocol	Internet Group Management Protocol
LACP	Protocol	Link Aggregation Control Protocol
NTP	Protocol	Network Time Protocol
OSPF	Protocol	Open Shortest Path First
PIM	Protocol	Protocol Independent Multicast
PPPoE	Protocol	Point-to-point protocol over Ethernet
RIP	Protocol	Routing Information Protocol
SNMP	Manage	Simple Network Management Protocol
SSH	Manage	Secure Shell
STP	Protocol	Spanning Tree Protocol
Telnet	Manage	Telnet
TFTP	Manage	Trivial File Transfer Protocol
VRRP	Protocol	Virtual Router Redundancy Protocol
Web	Manage	Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS)

A customized rate limit (in packets per second) can be assigned to the Safeguard Engine's sub-interfaces as a whole or to individual protocols specified by the user in the management interface. Be careful when customizing the rate limit for individual protocols, using this function, as improper rate limits can cause the Switch to process packets abnormally.



NOTE: When Safeguard Engine is enabled, the Switch will allot bandwidth to various traffic flows (ARP, IP) using the FFP (Fast Filter Processor) metering table to control the CPU utilization and limit traffic. This may limit the speed of routing traffic over the network.

Safeguard Engine Settings

This window is used to display and configure the safeguard engine settings.

To view the following window, click **Security > Safeguard Engine > Safeguard Engine Settings**, as shown below:

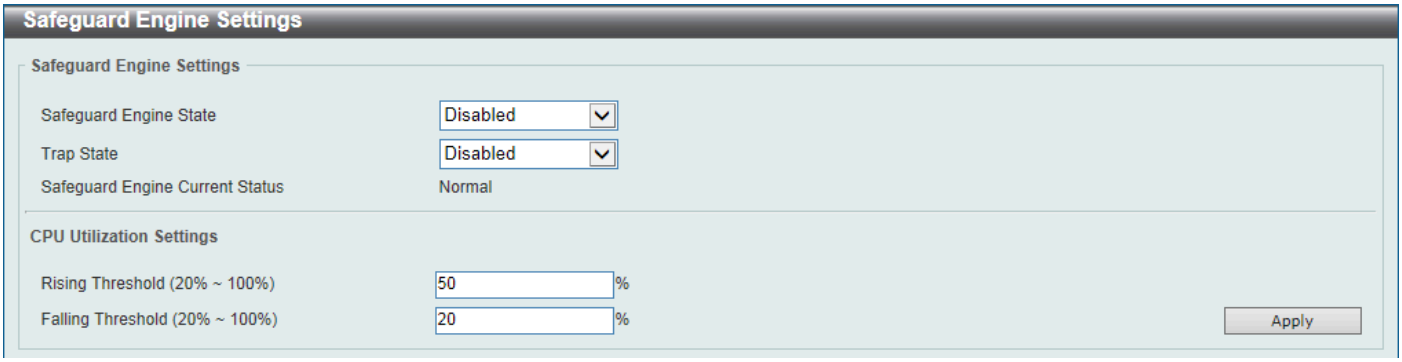


Figure 9-81 Safeguard Engine Settings Window

The fields that can be configured in **Safeguard Engine Settings** are described below:

Parameter	Description
Safeguard Engine State	Select to enable or disable the safeguard engine feature here.
Trap State	Select to enable or disable the safeguard engine trap state here.

The fields that can be configured in **CPU Utilization Settings** are described below:

Parameter	Description
Rising Threshold	Enter the rising threshold value here. This value must be between 20% and 100%. This value is used to configure the acceptable level of CPU utilization before the Safeguard Engine mechanism is enabled. Once the CPU utilization reaches this percentage level, the Switch will move into Exhausted mode, based on the parameters provided in this window. The default is 50%.
Falling Threshold	Enter the falling threshold value here. This value must be between 20% and 100%. This value is used to configure the acceptable level of CPU utilization as a percentage, where the Switch leaves the Safeguard Engine state and returns to normal mode. The default is 20%.

Click the **Apply** button to accept the changes made.

CPU Protect Counters

This window is used to view and clear the CPU protection counter information.

To view the following window, click **Security > Safeguard Engine > CPU Protect Counters**, as shown below:

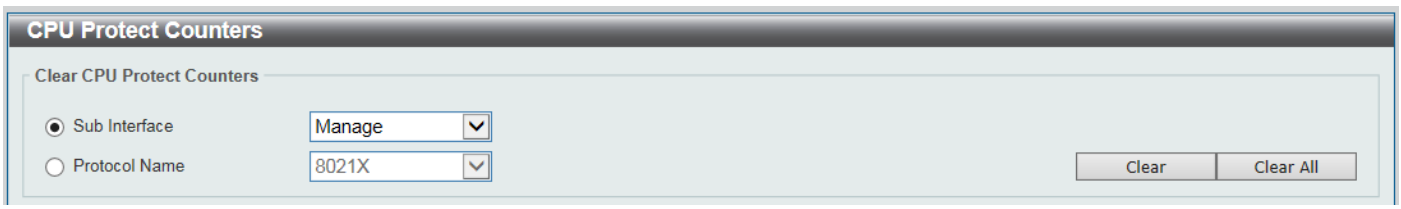


Figure 9-82 CPU Protect Counters Window

The fields that can be configured are described below:

Parameter	Description
Sub Interface	Select the sub-interface option here. Options to choose from are **Manage**, **Protocol**, **Route**, and **All**. This option specifies to clear the CPU protect related counters of sub-interfaces.
Protocol Name	Select the protocol name option here. The options are 8021X, ARP, DHCP, DNS, GVRP, ICMPv4, ICMPv6-NDP, ICMPv6-OTHER, IGMP, LACP, NTP, RIP, STP, VRRP, SNMP, SSH, Telnet, TFTP, WEB, and All.

Click the **Clear** button to clear the information based on the selections made.

Click the **Clear All** button to clear all the information in this table.

CPU Protect Sub-Interface

This window is used to display and configure the CPU protection sub-interface settings.

To view the following window, click **Security > Safeguard Engine > CPU Protect Sub-Interface**, as shown below:

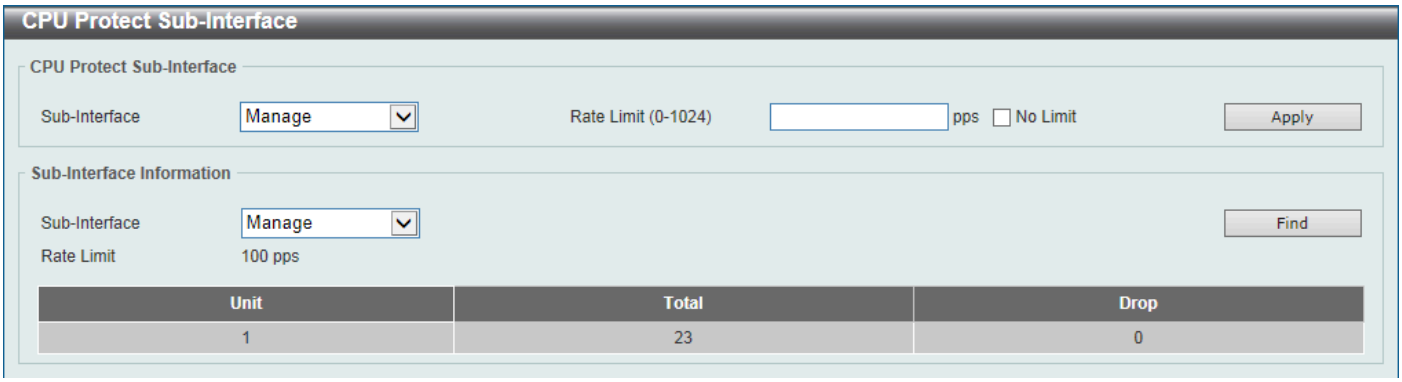


Figure 9-83 CPU Protect Sub-Interface Window

The fields that can be configured in **CPU Protect Sub-Interface** are described below:

Parameter	Description
Sub-Interface	Select the sub-interface option here. Options to choose from are **Manage**, **Protocol**, and **Route**.
Rate Limit	Enter the rate limit value used here. This value must be between 0 and 1024 packets per second. Tick the **No Limit** option to disable the rate limit.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Sub-Interface Information** are described below:

Parameter	Description
Sub-Interface	Select the sub-interface option here. Options to choose from are **Manage**, **Protocol**, and **Route**.

Click the **Find** button to locate a specific entry based on the information entered.

CPU Protect Type

This window is used to display and configure the CPU protection type settings.

To view the following window, click **Security > Safeguard Engine > CPU Protect Type**, as shown below:

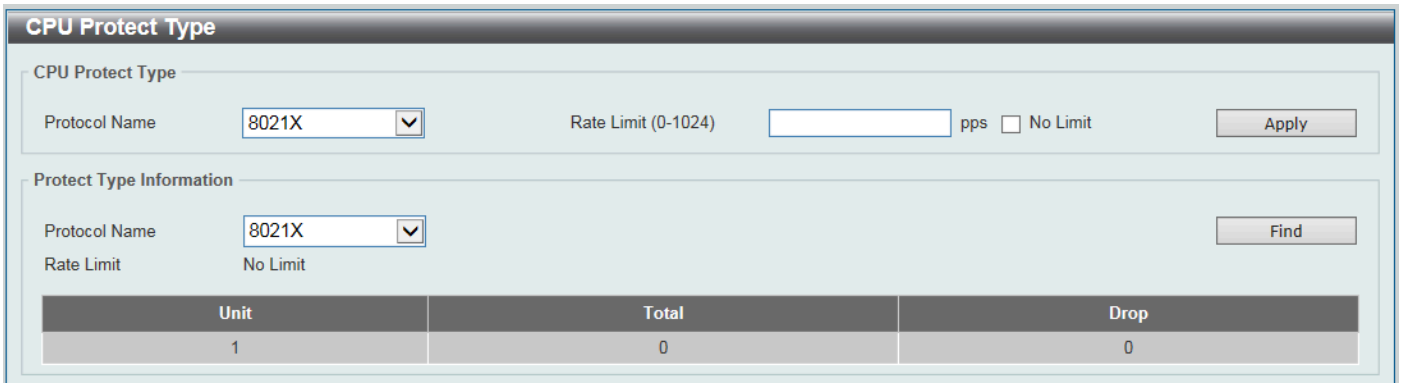


Figure 9-84 CPU Protect Type Window

The fields that can be configured in **CPU Protect Type** are described below:

Parameter	Description
Protocol Name	Select the protocol name option here. The options are 8021X, ARP, DHCP, DNS, GVRP, ICMPv4, ICMPv6-NDP, ICMPv6-OTHER, IGMP, LACP, NTP, OSPF, PIM, PPPoE, RIP, STP, VRRP, SNMP, SSH, Telnet, TFTP, and WEB.
Rate Limit	Enter the rate limit value used here. This value must be between 0 and 1024 packets per second. Tick the **No Limit** option to disable the rate limit.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Protect Type Information** are described below:

Parameter	Description
Protocol Name	Select the protocol name option here. The options are 8021X, ARP, DHCP, DNS, GVRP, ICMPv4, ICMPv6-NDP, ICMPv6-OTHER, IGMP, LACP, NTP, OSPF, PIM, PPPoE, RIP, STP, VRRP, SNMP, SSH, Telnet, TFTP, WEB, and All.

Click the **Find** button to locate a specific entry based on the information entered.

Trusted Host

This window is used to display and configure the trusted host settings.

To view the following window, click **Security > Trusted Host**, as shown below:

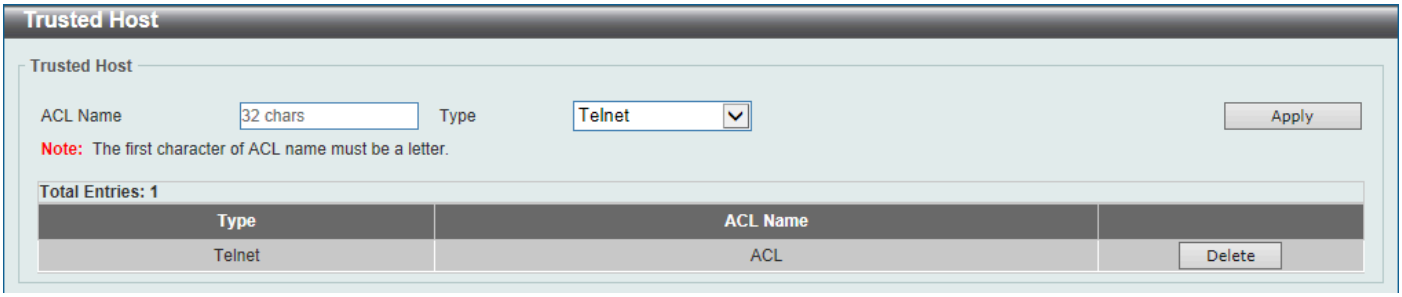


Figure 9-85 Trusted Host Window

The fields that can be configured are described below:

Parameter	Description
ACL Name	Enter the access list name here. This name can be up to 32 characters long. Refer to **ACL** > **ACL Access List**.
Type	Select the type of application for trusted host configuration here. Options to choose from are **Telnet, SSH, Ping, HTTP**, and **HTTPS**.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Traffic Segmentation Settings

This window is used to display and configure the traffic segmentation settings. When the traffic segmentation forwarding domain is specified, packets received by the port will be restricted in Layer 2 packet forwarding to interfaces within the domain. When the forwarding domain of a port is empty, Layer 2 forwarding for packets received by the port is not restricted.

The traffic segmentation member list can be comprised of different interface types, for example port and port-channel in the same forwarding domain. If the interfaces specified by the command include a port-channel, all the member ports of this port-channel will be included in the forwarding domain.

If the forwarding domain of an interface is empty, then there is no restriction on Layer 2 forwarding of packets received by the port.

To view the following window, click **Security > Traffic Segmentation Settings**, as shown below:

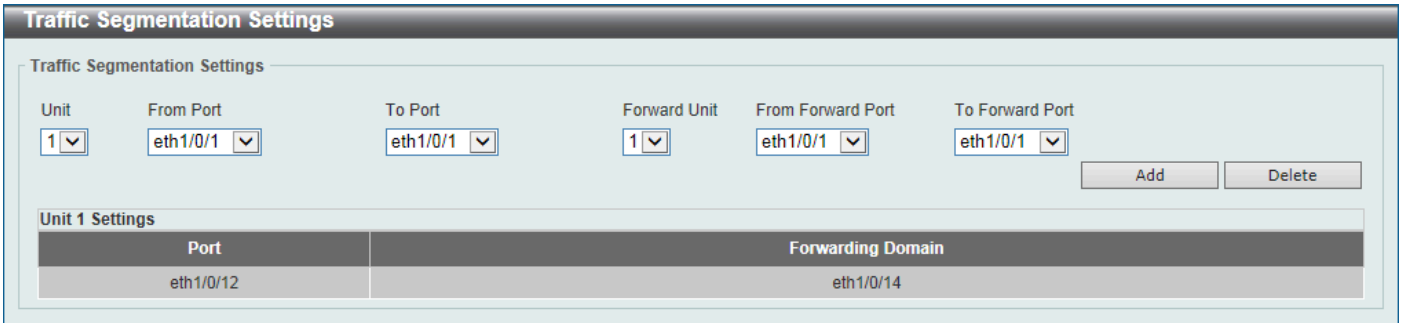


Figure 9-86 Traffic Segmentation Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the receiving Switch unit that will be used for this configuration here. This option is only available if stacking is enabled.

Parameter	Description
From Port - To Port	Select the receiving port range used for the configuration here.
Forward Unit	Select the forward Switch unit that will be used for this configuration here. This option is only available if stacking is enabled.
From Forward Port ~ To Forward Port	Select the forward port range used for the configuration here.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove an entry based on the information entered.

Storm Control

This window is used to display and configure the storm control settings.

To view the following window, click **Security > Storm Control**, as shown below:

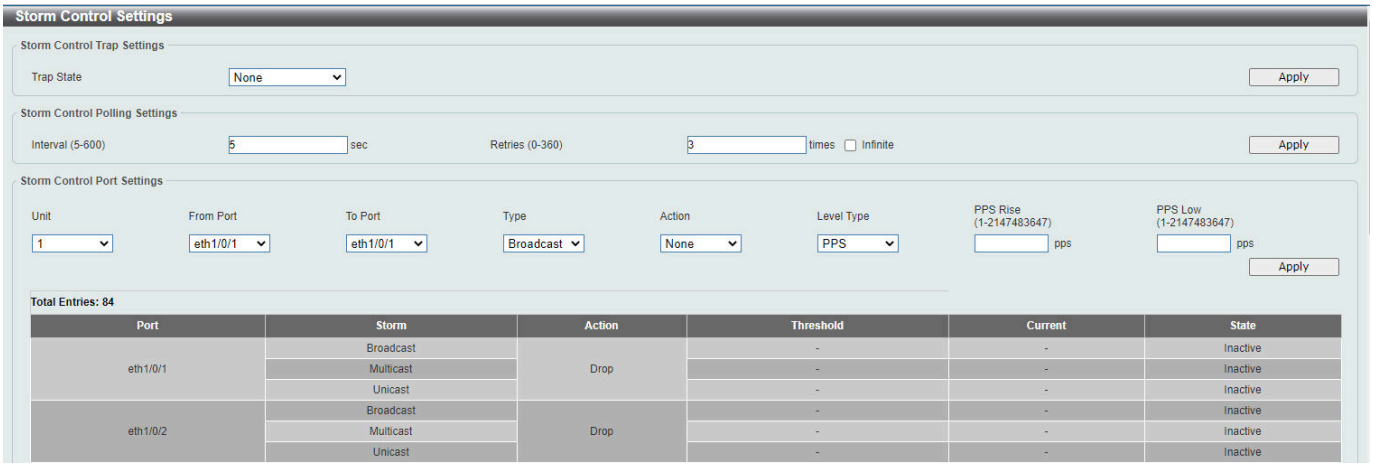


Figure 9-87 Storm Control Window

The fields that can be configured in **Storm Control Trap Settings** are described below:

Parameter	Description
Trap State	Select the storm control trap option here. Options to choose from are **None**, **Storm Occur**, **Storm Clear**, and **Both**. When **None** is selected, no traps will be sent. When **Storm Occur** is selected, a trap notification will be sent when a storm event is detected. When **Storm Clear** is selected, a trap notification will be sent when a storm event is cleared. **NOTE:** For unicast traffic (including both unknown and known unicast traffic), only the Shutdown action will trigger logs and generate traps (action specified as error-disabling the port during a storm). Refer to the **Storm Control Port Settings** below.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Storm Control Polling Settings** are described below:

Parameter	Description
Interval	Enter the interval value used here. This value must be between 5 and 600 seconds. By default, this value is 5 seconds.

Parameter	Description
Retries	Enter the retries value used here. This value must be between 0 and 360. By default, this value is 3. Tick the **Infinite** option to disable this feature.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Storm Control Port Settings** are described below:

Parameter	Description
Unit	Select the receiving Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
Type	Select the type of storm attack that will be controlled here. Options to choose from are **Broadcast**, **Multicast**, and **Unicast**. When the action is configured as the shutdown mode, the unicast refers to both known and unknown unicast traffic; that is, if the unicast packets with known and unknown destination MAC addresses hit the specified threshold, the port will be shutdown. Otherwise, unicast refers to unicast packets with unknown destination MAC addresses.
Action	Select the action that will be taken here. Options to choose from are **None**, **Shutdown**, and **Drop**. Selecting **None** specifies not to filter the storm packets. Selecting **Shutdown** specifies to shut down the port when the value specified for rise threshold is reached. Selecting **Drop** specifies to discard packets that exceed the rising threshold. You can configure traps to be generated when storms occur and/or clear (refer to **Storm Control Trap Settings** above). However, for unicast traffic, only the Shutdown action will trigger traps and event logs.
Level Type	Select the level type option here. Options to choose from are **PPS**, **Kbps**, and **Level**.
PPS Rise	Enter the rise packets per second value here. This option specifies the rise threshold value in packets count per second. This value must be between 1 and 2147483647 packets per second. If the low PPS value is not specified, the default value is 80% of the specified rising PPS.
PPS Low	Enter the low packets per second value here. This option specifies the low threshold value in packets count per second. This value must be between 1 and 2147483647 packets per second. If the low PPS value is not specified, the default value is 80% of the specified rising PPS.
NOTE: You can configure errdisable trap and recovery settings in **System > Port Configuration > Error Disable Settings**.	

Click the **Apply** button to accept the changes made.

After selecting the **Kbps** option as the **Level Type**, the following parameters are available.

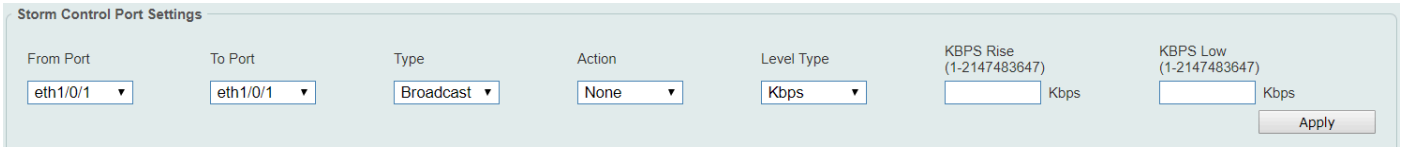


Figure 9-88 Storm Control (Level Type - Kbps) Window

The additional fields that can be configured in **Storm Control Port Settings** are described below:

Parameter	Description
KBPS Rise	Enter the rise KBPS value used here. This option specifies the rise threshold value as a rate of kilobits per second at which traffic is received on the port. This value must be between 1 and 2147483647 Kbps.

Parameter	Description
KBPS Low	Enter the low KBPS value used here. This option specifies the low threshold value as a rate of kilobits per second at which traffic is received on the port. This value must be between 1 and 2147483647 Kbps. If the low KBPS is not specified, the default value is 80% of the specified rising KBPS.

Click the **Apply** button to accept the changes made.

After selecting the **Level** option as the **Level Type**, the following parameters are available.

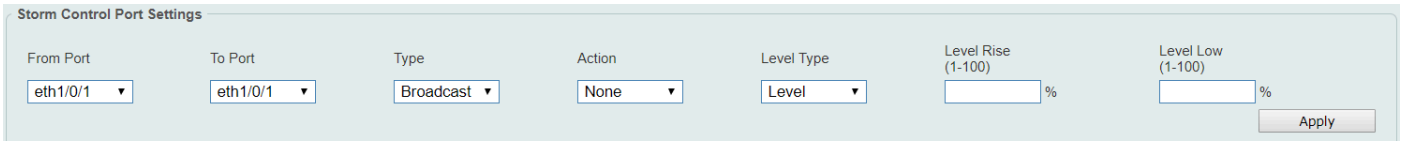


Figure 9-89 Storm Control (Level Type - Level) Window

The additional fields that can be configured in **Storm Control Port Settings** are described below:

Parameter	Description
Level Rise	Enter the rise level value used here. This option specifies the rise threshold value as a percentage of the total bandwidth per port at which traffic is received on the port. This value must be between 1% and 100%.
Level Low	Enter the low level value used here. This option specifies the low threshold value as a percentage of the total bandwidth per port at which traffic is received on the port. This value must be between 1% and 100%. If the low level is not specified, the default value is 80% of the specified rising level.

Click the **Apply** button to accept the changes made.

DoS Attack Prevention Settings

This window is used to display and configure the Denial-of-Service (DoS) attack prevention settings. The following well-known DoS types which can be detected by most Switches:

- **Land Attack:** This type of attack involves IP packets where the source and destination address are set to the address of the target device. It may cause the target device to reply to itself continuously.
- **Blat Attack**: This type of attack will send packets with the TCP/UDP source port equal to the destination port of the target device. It may cause the target device to respond to itself.
- **TCP Null:** This type of attack involves port scanning by using specific packets which contain a sequence number of 0 and no flags.
- **TCP Xmas:** This type of attack involves port scanning by using specific packets which contain a sequence number of 0 and the Urgent (URG), Push (PSH), and FIN flags.
- **TCP SYN-FIN:** This type of attack involves port scanning by using specific packets which contain SYN and FIN flags.
- **TCP SYN SrcPort Less 1024:** This type of attack involves port scanning by using specific packets which contain source port 0 to 1023 and SYN flag.
- **Ping of Death Attack:** A ping of death is a type of attack on a computer that involves sending a malformed or otherwise a malicious ping to a computer. A ping is normally 64 bytes in size (many computers cannot handle a ping larger than the maximum IP packet size which is 65535 bytes). The sending of a ping of this size can crash the target computer. Traditionally, this bug has been relatively easy to exploit. Generally, sending a 65536 byte ping packet is illegal according to networking protocol, but a packet of such a size can be sent if it is

fragmented; when the target computer reassembles the packet, a buffer overflow can occur, which often causes a system crash.

- **TCP Tiny Fragment Attack:** The Tiny TCP Fragment attacker uses IP fragmentation to create extremely small fragments and force the TCP header information into a separate packet fragment to pass through the check function of the router and issue an attack.
- **All Types:** All of the above types.

To view the following window, click **Security > DoS Attack Prevention Settings**, as shown below:

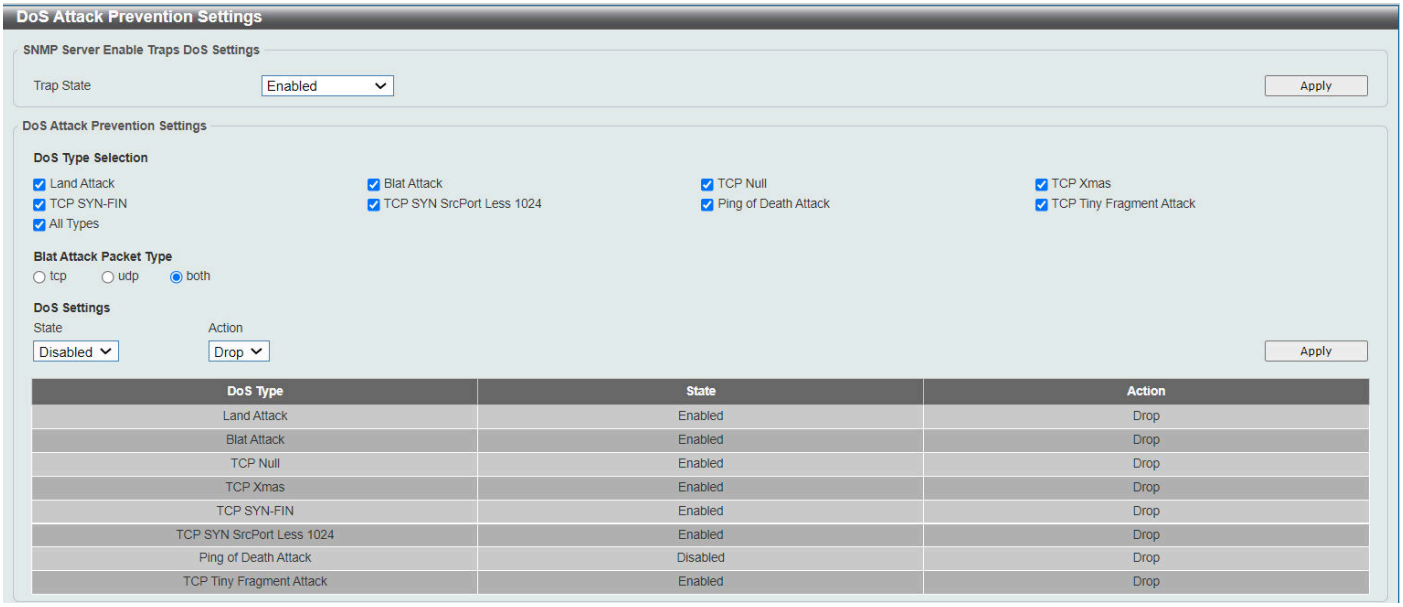


Figure 9-90 DoS Attack Prevention Settings Window

The fields that can be configured in **SNMP Server Enable Traps DoS Settings** are described below:

Parameter	Description
Trap State	Select to enable or disable the DoS attack prevention trap state here.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **DoS Attack Prevention Settings** are described below:

Parameter	Description
DoS Type Selection	Tick the DoS type option that will be prevented here.
Blat Attack Packet Type	Select the packet type for Blat attack that will be prevented here. Blat attack sends packets with the TCP/UDP source port equal to the destination port of the target device.
State	Select to enable or disable the global DoS attack prevention state here.
Action	Select the action that will be taken when the DoS attack was detected here. The only option to select here is **Drop**.

Click the **Apply** button to accept the changes made.

SSH

Secure Shell (SSH) is a program allowing secure remote login and secure network services over an insecure network. It allows a secure login to remote host computers, a safe method of executing commands on a remote end node and will provide secure encrypted and authenticated communication between two non-trusted hosts. SSH, with its array of unmatched security features is an essential tool in today's networking environment. It is a powerful guardian against numerous existing security hazards that now threaten network communications.

The steps required to use the SSH protocol for secure communication between a remote PC (the SSH client) and the Switch (the SSH server) are as follows:

- Create a user account with admin-level access using the User Accounts window. This is identical to creating any other admin-level User Account on the Switch, including specifying a password. This password is used to log on to the Switch, once a secure communication path has been established using the SSH protocol.
- Configure the User Account to use a specified authorization method to identify users that are allowed to establish SSH connections with the Switch using the SSH User Authentication Mode window. There are three choices as to the method SSH will use to authorize the user, which are Host Based, Password, and Public Key.
- Configure the encryption algorithm that SSH will use to encrypt and decrypt messages sent between the SSH client and the SSH server, using the SSH Authentication Method of SSH User Settings and Algorithm Settings window.
- Finally, enable SSH on the Switch using the SSH Configuration window.

After completing the preceding steps, a SSH Client on a remote PC can be configured to manage the Switch using a secure, in band connection.

SSH Global Settings

This window is used to display and configure the global SSH settings.

To view the following window, click **Security > SSH > SSH Global Settings**, as shown below:

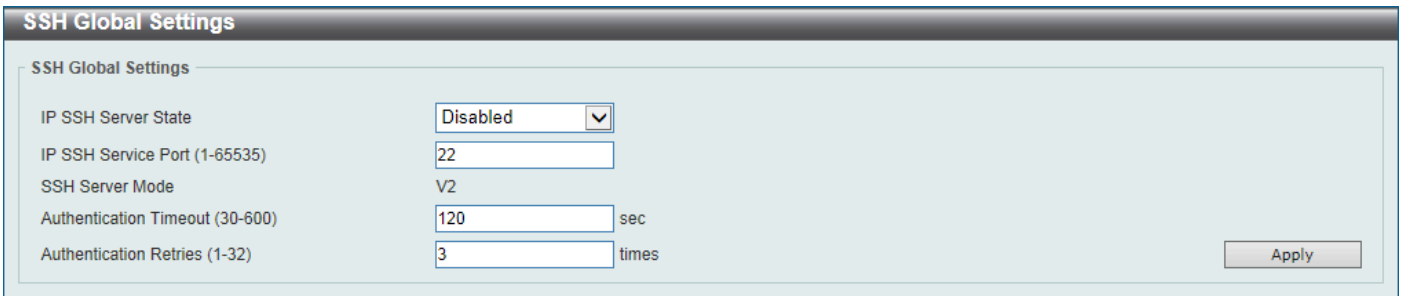


Figure 9-91 SSH Global Settings Window

The fields that can be configured are described below:

Parameter	Description
IP SSH Server State	Select to enable or disable the global SSH server.
IP SSH Service Port	Enter the SSH service port number used here. This value must be between 1 and 65535. By default, this number is 22.
Authentication Timeout	Enter the authentication timeout value here. This value must be between 30 and 600 seconds. By default, this value is 120 seconds.
Authentication Retries	Enter the authentication retries value here. This value must be between 1 and 32. By default, this value is 3.

Click the **Apply** button to accept the changes made.

SSH Algorithm Settings

This window is used to configure the algorithms to secure communication in different phases of an SSH session. Only the configured algorithms of the supported algorighms list will be negotiated with a Secure Shell (SSH) client.

To view the following window, click **Security > SSH > SSH Algorithm Settings**, as shown below:

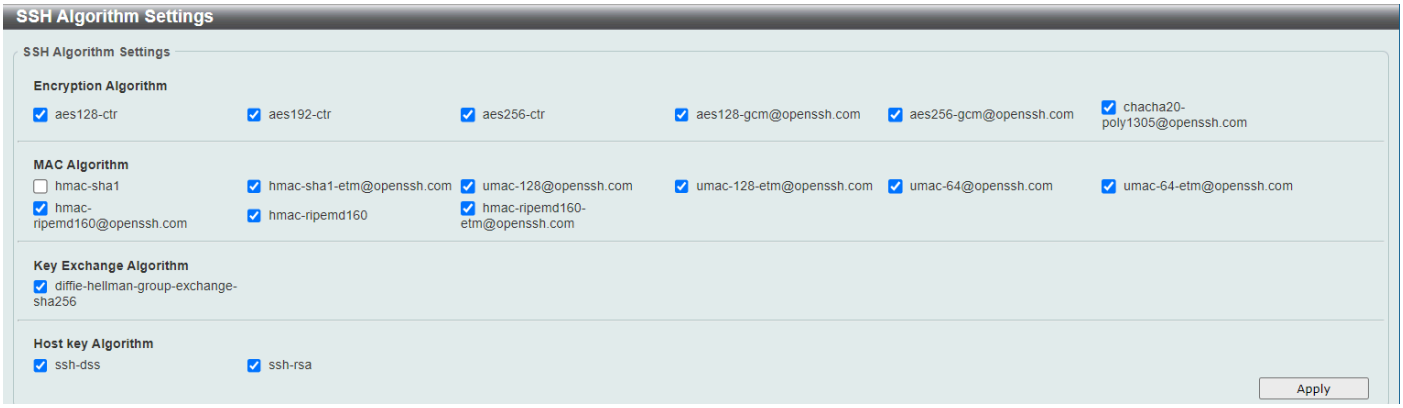


Figure 9-92 SSH Algorithm Settings Window

The fields that can be configured are described below:

Parameter	Description
Encryption Algorithm	Select the encryption algorithms to encrypt the data packets: aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com, and chacha20-poly1305@openssh.com.
MAC Algorithm	Select MAC (Message Authentication Code) algorithms to ensure the authentication of messages: hmac-sha1, hmac-sha1-etm@openssh.com, umac-128@openssh.com, umac-128-etm@openssh.com, umac-64@openssh.com, umac-64-etm@openssh.com, hmac-ripemd160@openssh.com, hmac-ripemd160, and hmac-ripemd160-etm@openssh.com.
Key Exchange Algorithm	Select the key exchange algorithm for key exchange security with a secret encryption key: diffie-hellman-group-exchange-sha256.
Host Key Algorithm	Select the host key algorithms as the encryption algorithms for computing the server's private and public key pair: ssh-dss and ssh-rsa.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Delete** button to remove the specified entry.

Host Key

This window is used to view and generate the SSH host key.

To view the following window, click **Security > SSH > Host Key**, as shown below:

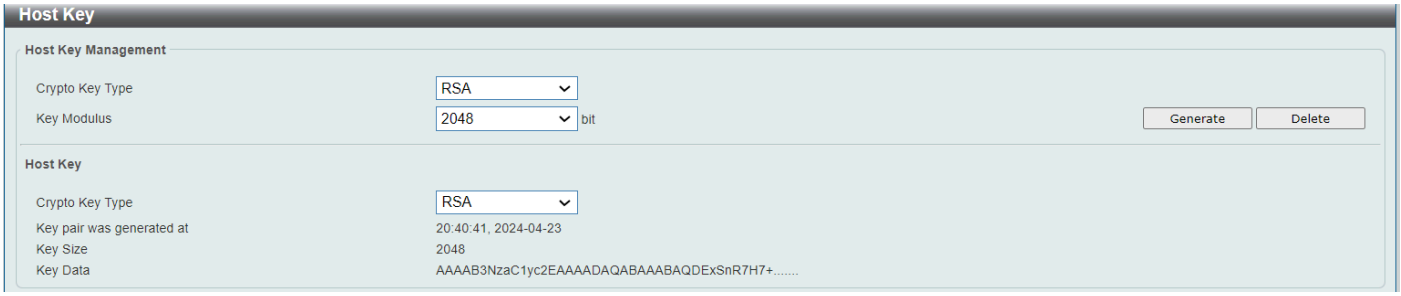


Figure 9-93 Host Key Window

The fields that can be configured in **Host Key Management** are described below:

Parameter	Description
Crypto Key Type	Select the crypto key type used here. Options to choose from are the Rivest Shamir Adleman (**RSA**) key type and the Digital Signature Algorithm (**DSA**) key type.
Key Modulus	Select the key modulus value here for the RSA type. Options to choose from are **360, 512, 768, 1024**, and **2048** bit.

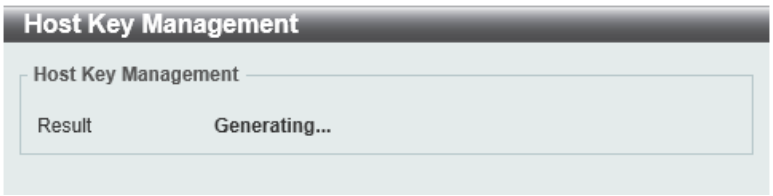
Click the **Generate** button to generate a host key based on the selections made.

Click the **Delete** button to remove a host key based on the selections made.

The fields that can be configured in **Host Key** are described below:

Parameter	Description
Crypto Key Type	Select the crypto key type used here. Options to choose from are the Rivest Shamir Adleman (**RSA**) key type and the Digital Signature Algorithm (**DSA**) key type.

After clicking the **Generate** button, the following generating and completion windows will appear:



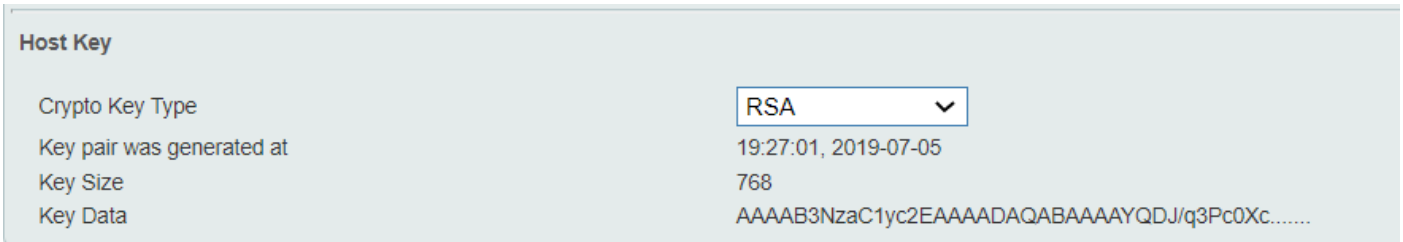


Figure 9-94 Host Key (Generating) Window

SSH Server Connection

This window is used to view the SSH server connections table.

To view the following window, click **Security > SSH > SSH Server Connection**, as shown below:



Figure 9-95 SSH Server Connection Window

SSH User Settings

This window is used to display and configure the SSH user settings.

To view the following window, click **Security > SSH > SSH User Settings**, as shown below:

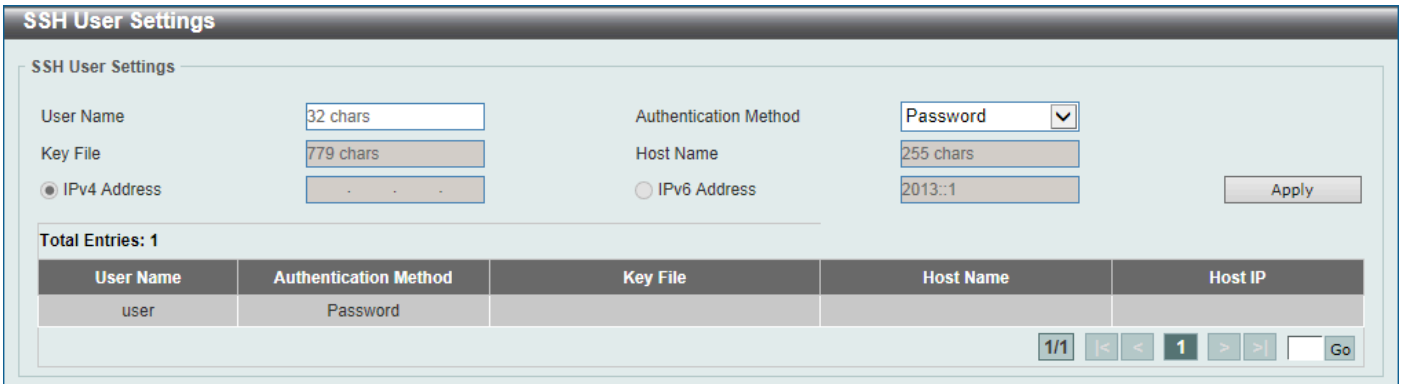


Figure 9-96 SSH User Settings Window

The fields that can be configured are described below:

Parameter	Description
User Name	Enter the SSH user's username used here. This name can be up to 32 characters long. Refer to **Management > User Accounts Settings** for users created in the system.
Authentication Method	Select the authentication methods used here. Options to choose from are **Password, Public Key**, and **Host-based**.
Key File	After selecting the **Public Key** or **Host-based** option as the **Authentication Method**, enter the public key file stored in the Switch here. The host-based option also uses the public key authentication method but does not require that a public/private key pair be created for each user.
Host Name	After selecting the **Host-based** option as the **Authentication Method**, enter the host name here and enter the corresponding IPv4 or IPv6 address below to register the allowed clients.
IPv4 Address	After selecting the **Host-based** option as the **Authentication Method**, select and enter the IPv4 address here for the above registered clients.
IPv6 Address	After selecting the **Host-based** option as the **Authentication Method**, select and enter the IPv6 address here for the above registered clients.

Click the **Apply** button to accept the changes made.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

SSL

Secure Sockets Layer (SSL) is a security feature that will provide a secure communication path between a host and client through the use of authentication, digital signatures and encryption. These security functions are implemented through the use of a cipher suite, which is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session and consists of three levels:

- **Key Exchange:** The first part of the Cipher suite string specifies the public key algorithm to be used. This Switch utilizes the Rivest Shamir Adleman (RSA) public key algorithm and the Digital Signature Algorithm (DSA), specified here as the DHE DSS Diffie-Hellman (DHE) public key algorithm. This is the first authentication process between client and host as they “exchange keys” in looking for a match and therefore authentication to be accepted to negotiate encryptions on the following level. The supported ECDHE_RSA is the advanced Ephemeral Elliptic Curve Diffie-Hellman algorithm that utilizes RSA server certificates.
- **Encryption:** The second part of the cipher suite that includes the encryption used for encrypting the messages sent between client and host. The Switch supports three types of cryptology algorithms:
  - **Stream Ciphers** - There are two types of stream ciphers on the Switch, RC4 with 40-bit keys and RC4 with 128-bit keys. These keys are used to encrypt messages and need to be consistent between client and host for optimal use.
  - **CBC Block Ciphers** - CBC refers to Cipher Block Chaining, which means that a portion of the previously encrypted block of encrypted text is used in the encryption of the current block. The Switch supports the 3DES EDE encryption code defined by the Data Encryption Standard (DES) to create the encrypted text.
  - **AES Block Ciphers** - Advanced Encryption Standard (AES) is also a block cipher and operates with different key lengths, including 128 and 256 bits. The switch supports AES_128_GCM and AES_256_GCM (Galois/Counter Mode) for higher efficiency and to incorporate advanced data authentication.
- **Hash Algorithm:** This part of the cipher suite allows the user to choose a message digest function which will determine a Message Authentication Code. This Message Authentication Code will be encrypted with a sent message to provide integrity and prevent against replay attacks. The Switch supports two hash algorithms, MD5 (Message Digest 5) and SHA (Secure Hash Algorithm).

These three parameters are uniquely assembled in four choices on the Switch to create a three-layered encryption code for secure communication between the server and the host. The user may implement any one or combination of the cipher suites available, yet different cipher suites will affect the security level and the performance of the secured connection. The information included in the cipher suites is not included with the Switch and requires downloading from a third source in a file form called a certificate. This function of the Switch cannot be executed without the presence and implementation of the certificate file and can be downloaded to the Switch by utilizing a TFTP server. The Switch supports TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. Other versions of SSL may not be compatible with this Switch and may cause problems upon authentication and transfer of messages from client to host.

When the SSL function has been enabled, the web will become disabled. To manage the Switch through the web-based management while utilizing the SSL function, the web browser must support SSL encryption and the header of the URL must begin with https://. (Ex. https://xx.xx.xx.xx) Any other method will result in an error and no access can be authorized for the web-based management.

Users can download a certificate file for the SSL function on the Switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the client must have consistent certificate files for optimal use of the SSL function. Currently, the Switch comes with a certificate pre-loaded though you may need to download more, depending on the circumstances.

SSL Global Settings

This window is used to display and configure the global SSL settings.

To view the following window, click **Security > SSL > SSL Global Settings**, as shown below:

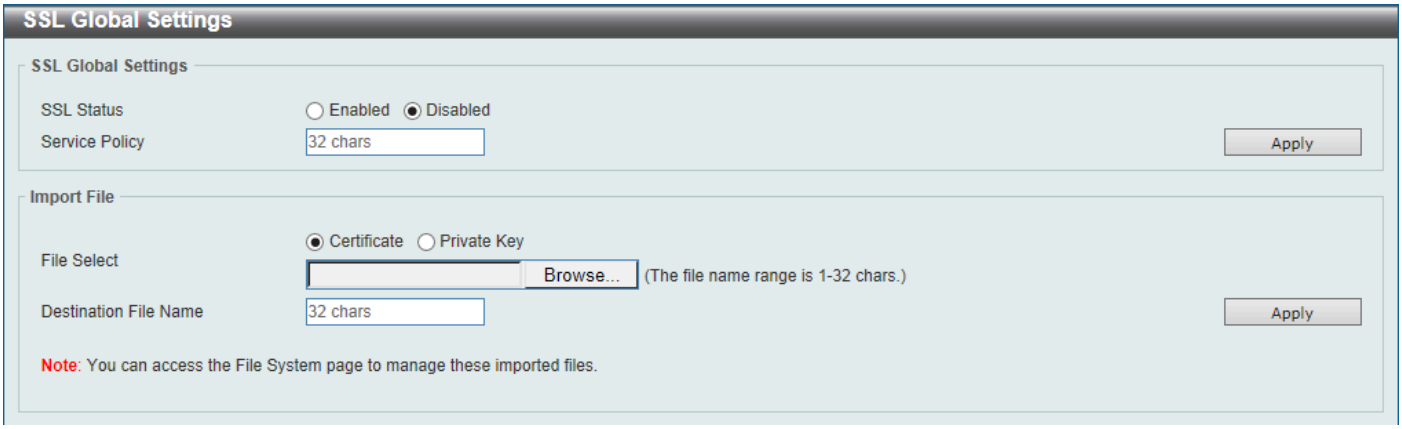


Figure 9-97 SSL Global Settings Window

The fields that can be configured in **SSL Global Settings** are described below:

Parameter	Description
SSL Status	Select to enable or disable the global SSL status here.
Service Policy	Enter the service policy name here. This name can be up to 32 characters long. Refer to below **SSL > SSL Service Policy**.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Import File** are described below:

Parameter	Description
File Select	Select the file type that will be loaded here. Options to choose from are **Certificate** and **Private Key**. After selecting the file type, browse to the appropriate file by clicking the **Choose File** button.
Destination File Name	Enter the destination file name to be stored in the Switch here. (Refer to **Management > File System**.) This name can be up to 32 characters long.

Click the **Apply** button to accept the changes made.

Crypto PKI Trustpoint

This window is used to display and configure the crypto PKI trust point settings.

To view the following window, click **Security > SSL > Crypto PKI Trustpoint**, as shown below:

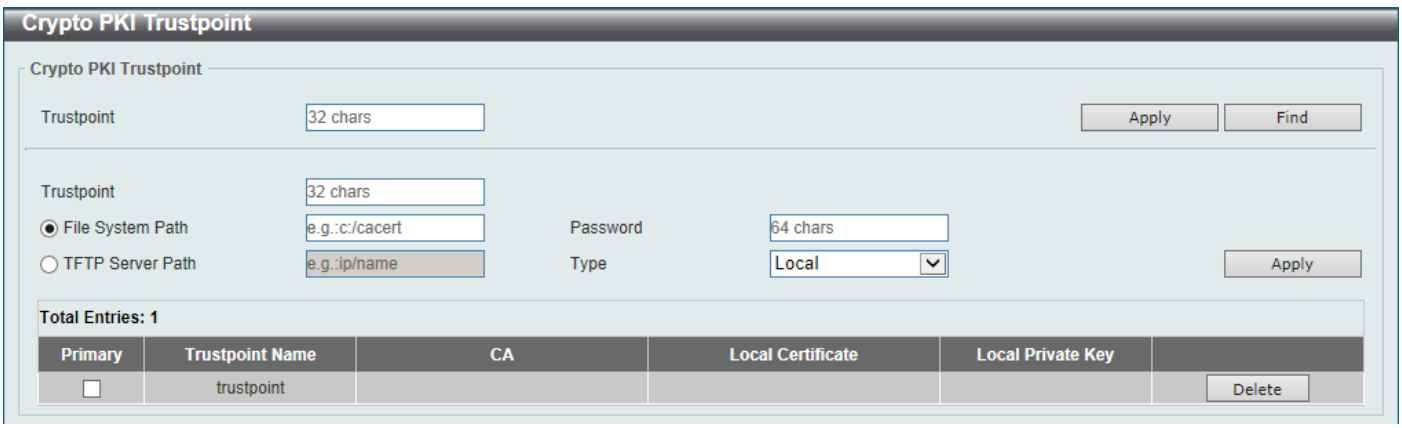


Figure 9-98 Crypto PKI Trustpoint Window

The fields that can be configured are described below:

Parameter	Description
Trustpoint	Enter the name of the trustpoint 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**, **CA**, and **Local**. • Selecting **Both** specifies to import the CA certificate, local certificate and key pairs. • Selecting **CA** specifies to import the CA certificate only. • Selecting **Local** specifies to import local certificate and key pairs only.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Delete** button to remove the specified entry.

SSL Service Policy

This window is used to display and configure the SSL service policy settings.

To view the following window, click **Security > SSL > SSL Service Policy**, as shown below:

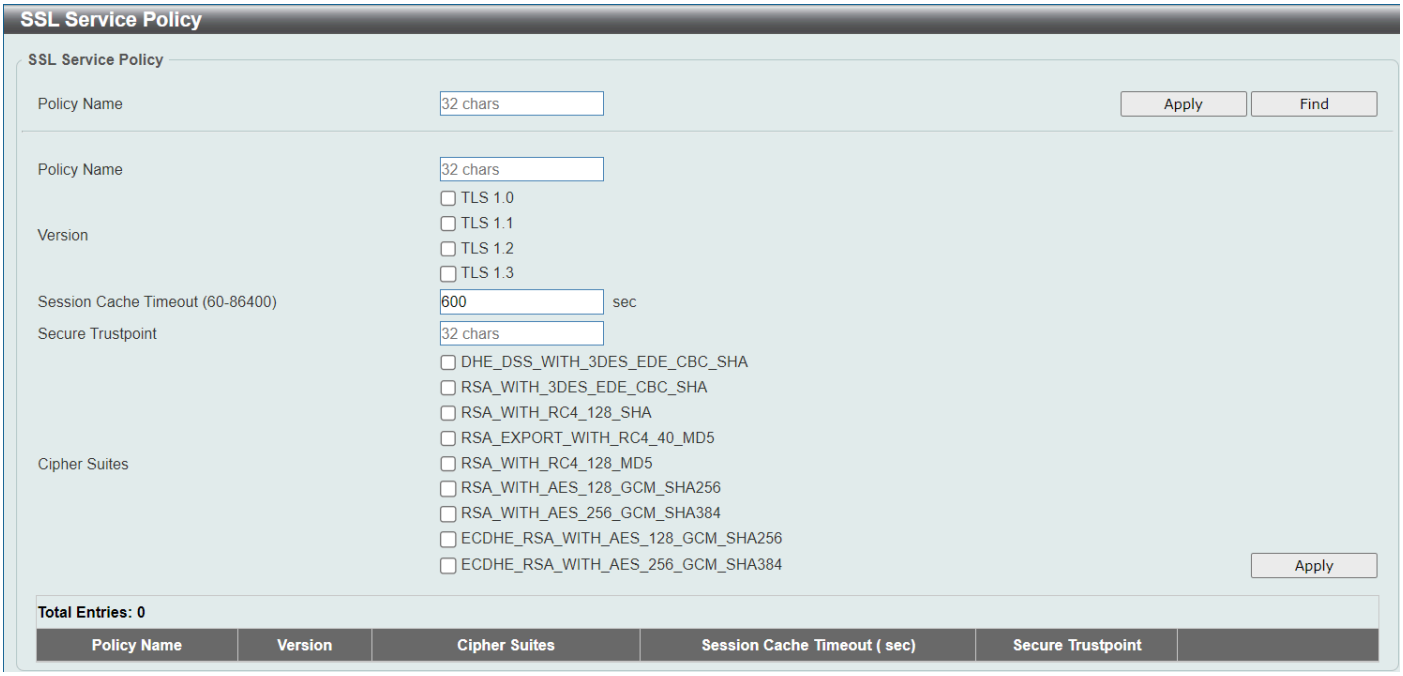


Figure 9-99 SSL Service Policy Window

The fields that can be configured are described below:

Parameter	Description
Policy Name	Enter the SSL service policy name here. This name can be up to 32 characters long.
Version	Select the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) version here. Options to choose from are **TLS 1.0**, **TLS 1.1**, **TLS 1.2,** and **TLS 1.3**.
Session Cache Timeout	Enter the session cache timeout value used here. This value must be between 60 and 86400 seconds. By default, this value is 600 seconds.
Secure Trustpoint	Enter the secure trust point name here. This name can be up to 32 characters long. Refer to **Security > SSL > Crypto PKI Trustpoint.**
Cipher Suites	Select the cipher suites that will be associated with this profile here. The available options are: DHE_DSS_WITH_3DES_EDE_CBC_SHA, RSA_WITH_3DES_EDE_CBC_SHA, RSA_WITH_RC4_128_SHA, RSA_EXPORT_WITH_RC4_40_MD5, RSA_WITH_RC4_128_MD5, RSA_WITH_AES_128_GCM_SHA256, RSA_WITH_AES_256_GCM_SHA384, ECDHE_RSA_WITH_AES_128_GCM_SHA256, ECDHE_RSA_WITH_AES_256_GCM_SHA384.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

SFTP Server Settings

This window is used to display and configure the Secure File Transfer Protocol (SFTP) server settings. SFTP is a remotely secure file transfer protocol over a reliable data stream. Because SFTP itself does not provide authentication and security, the SFTP server runs as a sub-system of the SSH server.

NOTE: Only IPv4 SFTP servers are supported.

To view the following window, click **Security > SFTP Server Settings**, as shown below:

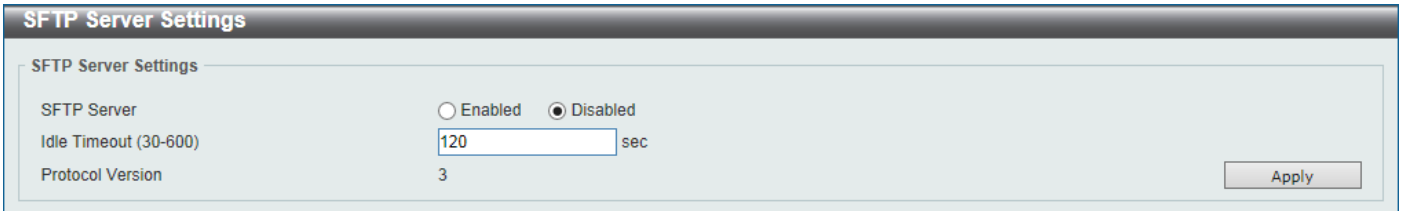


Figure 9-100 SFTP Server Settings Window

The fields that can be configured are described below:

Parameter	Description
SFTP Server	Select to globally enable or disable the SFTP server feature here.
Idle Timeout	Enter the idle timeout value here. If the SFTP server detects no operation after the duration of the idle timer for a specific SFTP session, the Switch will close this SFTP session. The range is from 30 to 600 seconds. By default, this value is 120 seconds.

Click the **Apply** button to accept the changes made.

Network Protocol Port Protect

This window is used to enable or disable the network protocol port protection settings. Disabling sending of response messages for a port not being used for connections can protect against malicious attacks proactively.

To view the following window, click **Security > Network Protocol Port Protect**, as shown below:

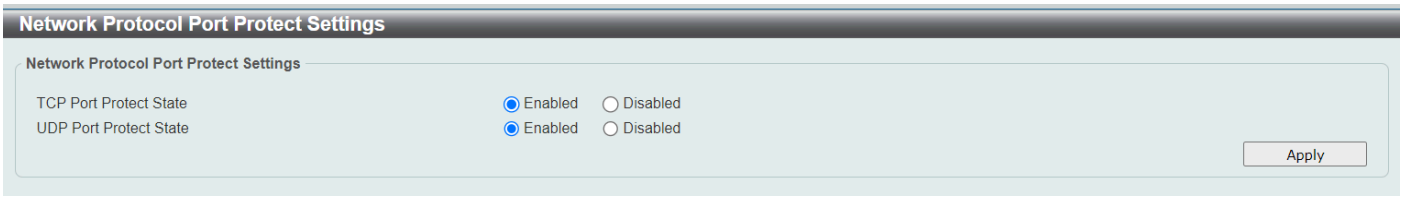


Figure 9-101 Network Protocol Port Protect Window

The fields that can be configured are described below:

Parameter	Description
TCP Port Protect State	Enable or disable sending TCP response messages to any connections of closed ports. This is enabled by default.
UDP Port Protect State	Enable or disable sending UDP response messages to any connections of closed ports. This is enabled by default.

Click the **Apply** button to accept the changes made.

10. OAM

CFM
Cable Diagnostics
Ethernet OAM
DDM

CFM

Connectivity Fault Management (CFM) works at the Ethernet for end-to-end operation, administration, and management (OAM).

CFM Settings

This window is used to display and configure the Connectivity Fault Management (CFM) settings.

To view the following window, click **OAM > CFM > CFM Settings**, as shown below:

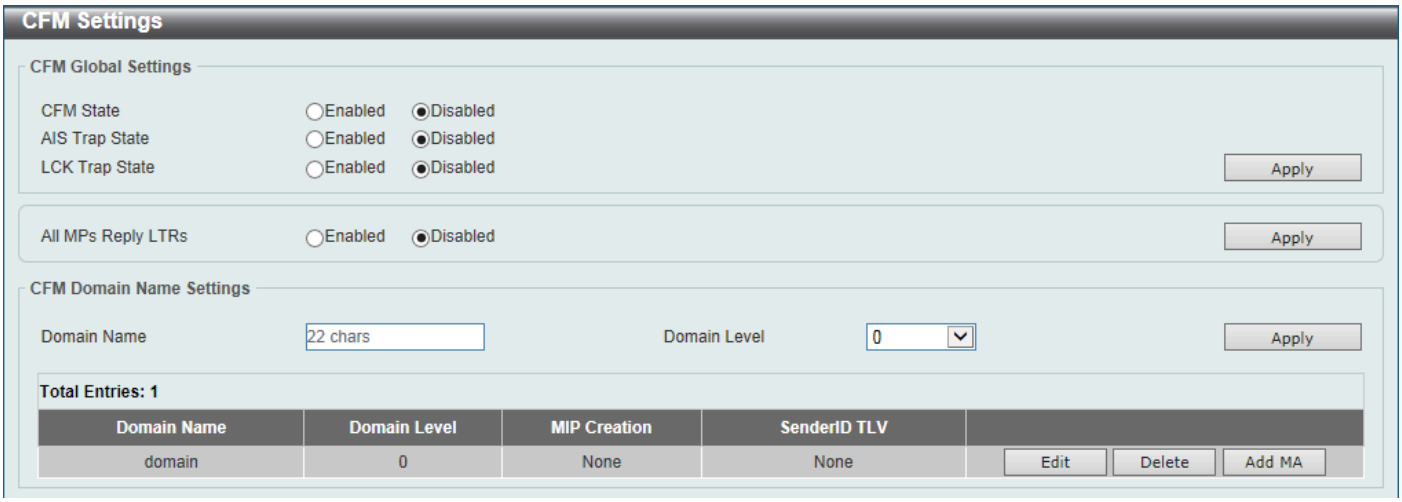


Figure 10-1 CFM Settings Window

The fields that can be configured in **CFM Global Settings** are described below:

Parameter	Description
CFM State	Select to globally enable or disable the CFM feature here.
AIS Trap State	Select to enable or disable the Alarm Indication Signal (AIS) trap feature here. If the trap status of AIS is enabled, once an ETH-AIS event occurs or an ETH-AIS event clears, a trap will be sent out.
LCK Trap State	Select to enable or disable the Locked Signal (LCK) trap feature here. If the trap status of LCK is enabled, once an ETH-LCK event occurs or an ETH-LCK event clears, a trap will be sent out.
All MPs Reply LTRs	Select to enable or disable the all MPs Link-Trace Reply (LTR) feature here. According to IEEE 802.1ag, a Bridge replies with one LTR to a Link-Trace Message (LTM). This feature can make all MPs on an LTM's forwarding path reply with LTRs, whether they are on a Bridge or not.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **CFM Domain Name Settings** are described below:

Parameter	Description
Domain Name	Enter the Maintenance Domain (MD) name here. This name can be up to 22 characters long. The name does not allow spaces. Each MD has a unique name amongst all those used or available to a service provider or operator. It facilitates easy identification of administrative responsibility for each maintenance domain.
Domain Level	Enter the Maintenance Domain (MD) level here. The range is from 0 to 7. A unique MD level is assigned to define the hierarchical relationship between domains. The larger range of domain has the higher value of level.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to modify the specified entry.

Click the **Delete** button to delete the specified entry.

Click the **Add MA** button to add a new Maintenance Association (MA) rule.

After clicking the **Edit** button, the entries in the table can be edited.

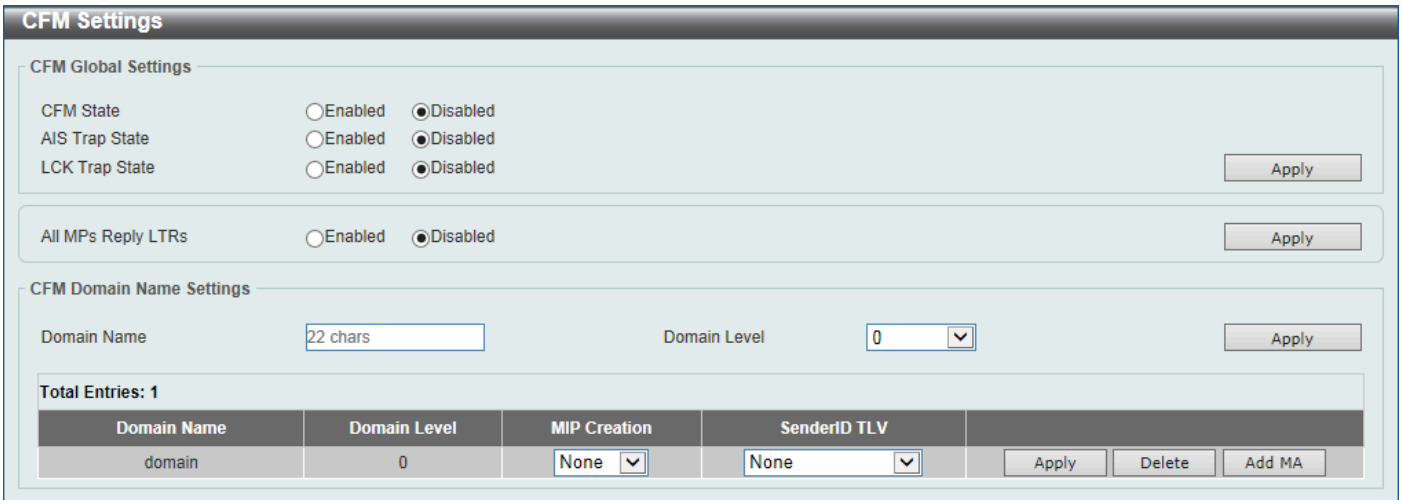


Figure 10-2 CFM Settings (Edit) Window

The fields that can be configured in the table are described below:

Parameter	Description
MIP Creation	Select the Maintenance Intermediate Point (MIP) option here. The creation of MIPs on a maintenance domain is useful for tracing the link, MIP by MIP. It also allows the user to perform a loopback from an MEP to an MIP. An enumerated value indicates whether the management entity can create MIP Half Functions (MHF) for a maintenance domain. Options to choose from are **None**, **Auto**, and **Explicit**. • **None** - Specifies not to create the MIP for a maintenance domain. • **Auto** - Specifies that MIPs will always be created on any port in this MD, when there is no MEP configured on that port for the MAs with the same VID at this MD level or any higher active MD levels, and at the same time there is an MEP configured on that port for the MA with the same VID at the next lower active MD level or there is no MA with the same VID at any lower active MD levels. For an intermediate Switch in an MA, the setting should be **Auto** in order for the MIPs to be created on this device. • **Explicit** - Specifies that MIPs will be created on any port for the MAs in this maintenance, when there is no MEP configured on that port for the

Parameter	Description
	MAs with the same VID at this MD level or any higher active MD levels, and at the same time there is an MEP configured on that port for the MA with the same VID at the next lower active MD level.
SenderID TLV	This option is used to configure the default transmission of the sender ID TLV by MPs in an MD. Select one of the following options: • **None** - Specifies not to transmit the sender ID TLV. • **Chassis** - Specifies to transmit the sender ID TLV with the chassis ID information. • **Manage** - Specifies to transmit the sender ID TLV with the managed address information. • **Chassis_Manage** - Specifies to transmit the sender ID TLV with the chassis ID information and the managed address information.

Click the **Apply** button to accept the changes made.

After clicking the **Add MA** button, the following page will appear.



Figure 10-3 CFM Settings (Add MA) Window

The fields that can be configured are described below:

Parameter	Description
MA Name	Enter the Maintenance Association (MA) entry name here. This name can be up to 22 characters long. Each MA in an MD must have a unique MA name. MAs configured in different MDs may have the same MA identifier. When the MA entry is deleted, the configuration on it is also deleted.
MA VID	Enter the Maintenance Association (MA) entry VLAN ID here. 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.

Click the **Edit** button to modify the specified entry.

Click the **Delete** button to delete the specified entry.

Click the **Add MEP** button to add a new Maintenance association End Point (MEP) entry.

After clicking the **Edit** button, the following page will appear.

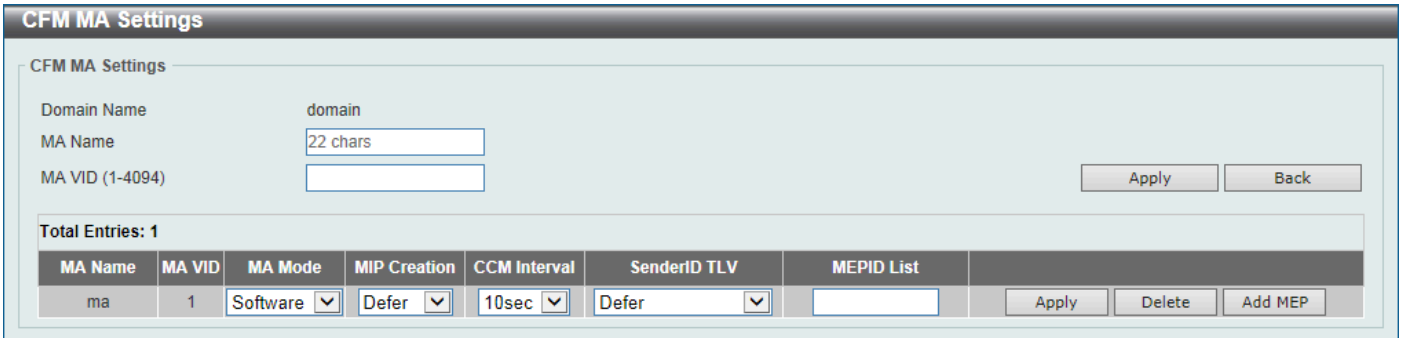


Figure 10-4 CFM Settings (Add MA, Edit) Window

The fields that can be configured in the table are described below:

Parameter	Description
MA Mode	Select the MA mode here. Options to choose from are: • **Software** - Specifies that the MA works in the CFM software mode. • **Hardware** - Specifies that the MA works in the CFM hardware mode. The CFM hardware mode is used to improve the performance of the CCM process. In the CFM hardware mode, the CCM packet is processed by hardware and in general does not need to involve the CPU. In addition, the CCM interval can be set to the lowest value of 3.3ms which is not supported in the CFM software mode due to the CPU capability constraints. The CFM hardware and software mode can be used together. The user can configure an MA as the CFM hardware mode. Then, all MEPs in the MA will be working in the CFM hardware mode. For some MAs, if the performance of the CCM process is considered, e.g. requiring 3.3ms and 10ms CCM interval, and the MEPs in the MA are down MEPs, the user can use the CFM hardware mode; For other MAs, if the performance of the CCM process is not a problem, or up MEPs and MIPs need to be set up, or full CFM function are required, the CFM software mode is a better choice.
MIP Creation	This option is used to configure the MIP creation for an MA. Select one of the following options: • **None** - Specifies not to create the MIP on ports in an MA. • **Auto** - Specifies that MIPs will be created on any port for this MA, when there is no MEP configured on that port for the MAs with the same VID at this MD level or any higher active MD levels, and at the same time there is an MEP configured on that port for the MA with the same VID at the next lower active MD level or there is no MA with the same VID at any lower active MD levels. For an intermediate Switch in an MA, the setting should be **Auto** in order for the MIPs to be created on this device. • **Explicit** - Specifies that MIPs will be created on any port for this MA, when there is no MEP configured on that port for the MAs with the same VID at this MD level or any higher active MD levels, and at the same time there is an MEP configured on that port for the MA with the same VID at the next lower active MD level. • **Defer** - Specifies to inherit the settings configured for the maintenance domain that the MA is associated with. This is the default value.
CCM Interval	Select the Continuity Check Message (CCM) interval value here. Options to choose from are **3.3ms**, **10ms**, **100ms**, **1sec**, **10sec**, **1min**, and **10min**. An MEP will transmit a CCM packet periodically across the MA. The CCM interval indicates the interval at which CCMs are sent by a MEP in a MA.

Parameter	Description
SenderID TLV	This option is used to configure the transmission of the sender ID TLV by MPs for an MA. Select one of the following options: • **None** - Specifies not to transmit the sender ID TLV. In the CFM hardware mode, the value is fixed to none. • **Chassis** - Specifies to transmit the sender ID TLV with the chassis ID information. • **Manage** - Specifies to transmit the sender ID TLV with the managed address information. • **Chassis_Manage** - Specifies to transmit the sender ID TLV with the chassis ID information and the managed address information. • **Defer** - Specifies to inherit the setting configured for the maintenance domain that the MA is associated with. This is the default value.
MEPID List	Enter the Maintenance association End Point (MEP) ID contained in the MA here. The range is from 1 to 8191.

Click the **Apply** button to accept the changes made.

After clicking the **Add MEP** button, the following page will appear.

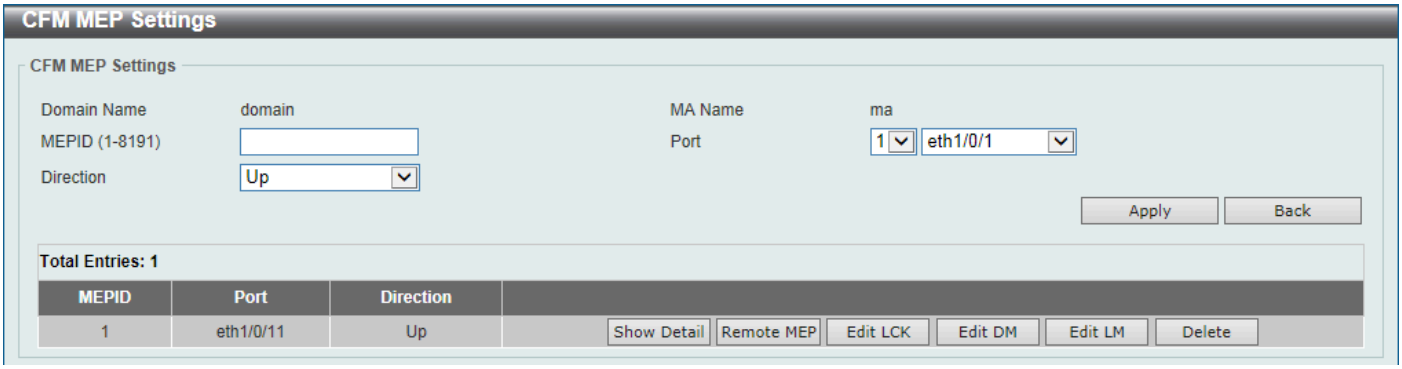


Figure 10-5 CFM Settings (Add MA, Add MEP) Window

The fields that can be configured are described below:

Parameter	Description
MEPID	Enter the MEP ID here. The range is from 1 to 8191. Each MEP configured in the same MA must have a unique MEP ID. The MEP on different MA can have the same MEPID. Before creating a MEP, its MEP ID should be configured in the MA's MEP ID list.
Port	Select the Switch unit ID and port number that will be used here.
Direction	Select the direction of the MEP here. Options to choose from are **Up** and **Down**. • **Up** - Specifies to create an inward facing (up) MEP. • **Down** - Specifies to create an outward facing (down) MEP.

Click the **Apply** button to accept the changes made.

Click the **Back** button to return to the previous window.

Click the **Show Detail** button to view more detailed information about the specified MEP.

Click the **Remote MEP** button to view the remove MEP table.

Click the **Edit LCK** button to modify the LCK settings of the specified entry.

Click the **Edit DM** button to access the CFM Delay Measurement (DM) settings.

Click the **Edit LM** button to access the CFM Loss Measurement (LM) settings.

Click the **Delete** button to delete the specified entry.

After clicking the **Show Detail** button, the following page will appear.

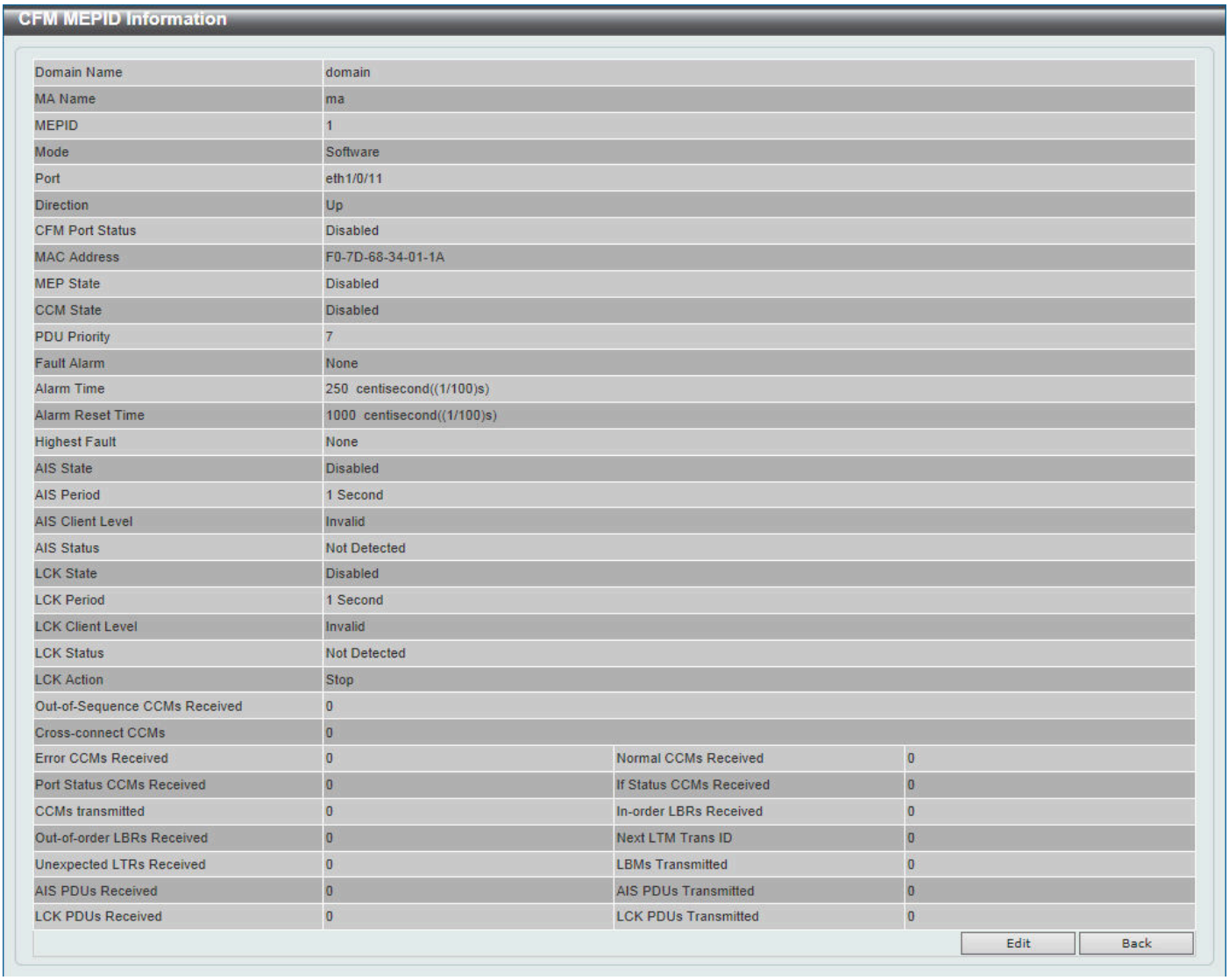


Figure 10-6 CFM Settings (Add MA, Add MEP, MEPID Detail) Window

Click the **Edit** button to modify the specified entry.

Click the **Back** button to return to the previous window.

After clicking the **Edit** button, the following page will appear.

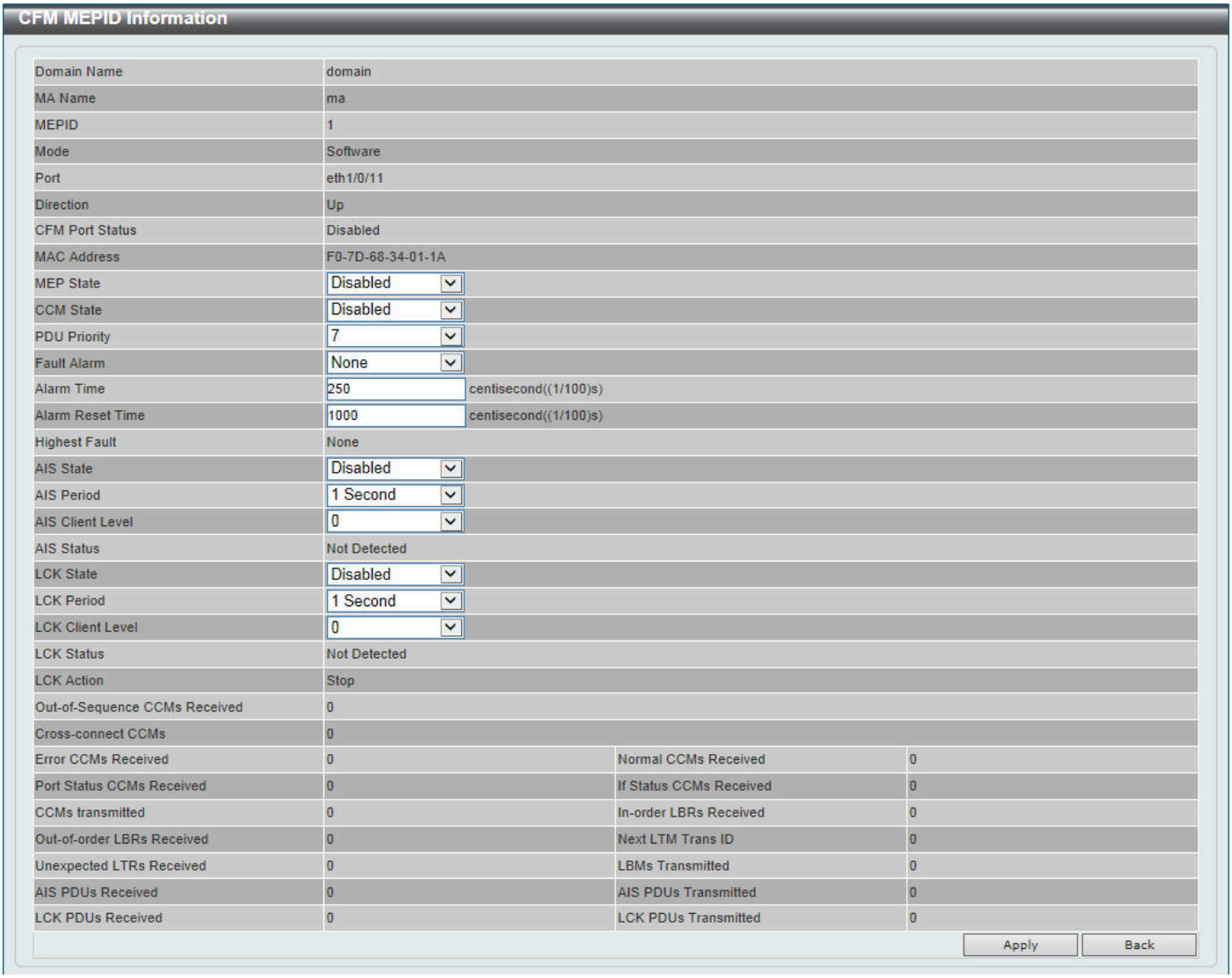


Figure 10-7 CFM Settings (Add MA, Add MEP, MEPID Detail, Edit) Window

The fields that can be configured are described below:

Parameter	Description
MEP State	Select to enable or disable the MEP state on the interface here.
CCM State	Select to enable or disable the CCM state here.
PDU Priority	Select the PDU priority value here. The range is from 0 to 7. This feature is used to define the 802.1p priority that is set in the CCM and other CFM PDUs transmitted by the MEP.
Fault Alarm	Select the type of defects whose fault alarms can be sent by this MEP. Options to choose from are **None**, **All**, **MAC-Status**, **Remote-CCM**, **Error-CCM**, and **XCON-CCM**. • **None** - Specifies that no fault alarm will be sent. • **All** - Specifies that the fault alarms can be sent for all types of defects. • **MAC-Status** - Specifies that the fault alarms can be sent for the defects whose priority is equal to or higher than *DefMACstatus*. • **Remote-CCM** - Specifies that the fault alarms can be sent for the defects whose priority is equal to or higher than *DefRemoteCCM*.

Parameter	Description
	• **Error-CCM** - Specifies that the fault alarms can be sent for the defects whose priority is equal to or higher than *DefErrorCCM*. • **XCON-CCM** - Specifies that only the fault alarm of *DefXconCCM* can be sent.
Alarm Time	Enter the time period used to define the time from when a defect is detected on the MEP to when a fault alarm will be sent. The range is from 250 to 1000 centiseconds. By default, this value is 250 centiseconds (1 centisecond equals to 0.01 seconds).
Alarm Reset Time	Enter the time period used to define the time from when all defects detected on the MEP are removed to when the fault alarm mechanism will be reset. The range is from 250 to 1000 centiseconds. By default, this value is 1000 centiseconds.
AIS State	Select the enable or disable the AIS feature on this interface here.
AIS Period	Select the transmitting interval of the AIS PDU here. Options to choose from are **1 Second** and **1 Minute**. The default period is 1 second.
AIS Client Level	Select the client level ID to which the MEP sends the AIS PDUs here. The default client MD level is that the most immediate client layer Maintenance domain Intermediate Points (MIP) and MEPs exist on. The range is from 0 to 7 and invalid.
LCK State	Select the enable or disable the LCK feature on this interface here.
LCK Period	Select the transmitting interval of the LCK PDU here. Options to choose from are **1 Second** and **1 Minute**. The default period is 1 second.
LCK Client Level	Select the client level ID to which the MEP sends the LCK PDU here. The default client MD level is the MD level that the most immediate client layer MIPs and MEPs exist on. The range is from 0 to 7 and invalid.

Click the **Apply** button to accept the changes made.

Click the **Back** button to return to the previous window.

After clicking the **Remote MEP** button, the following page will appear.

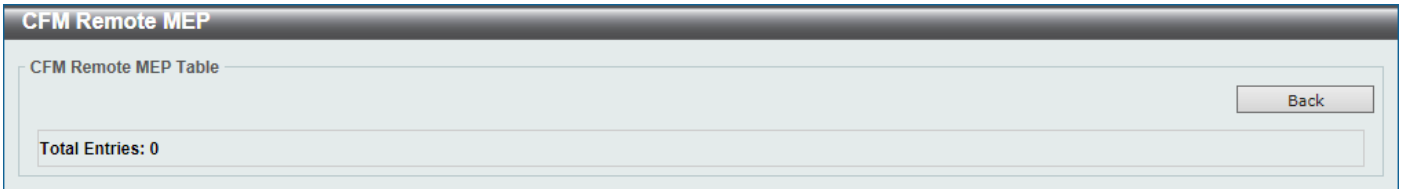


Figure 10-8 CFM Settings (Add MA, Add MEP, Remote MEP) Window

Click the **Back** button to return to the previous window.

After clicking the **Edit LCK** button, the following page will appear.

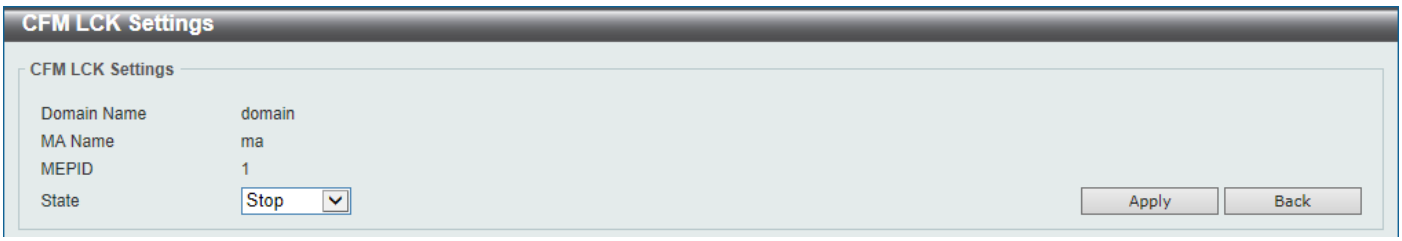


Figure 10-9 CFM Settings (Add MA, Add MEP, Edit LCK) Window

The fields that can be configured are described below:

Parameter	Description
State	Select to **Start** or **Stop** the administrative lock action here. This feature will result in the MEP to send LCK PDUs to a client level MEP.

Click the **Apply** button to accept the changes made.

Click the **Back** button to return to the previous window.

After clicking the **Edit DM** button, the following page will appear.

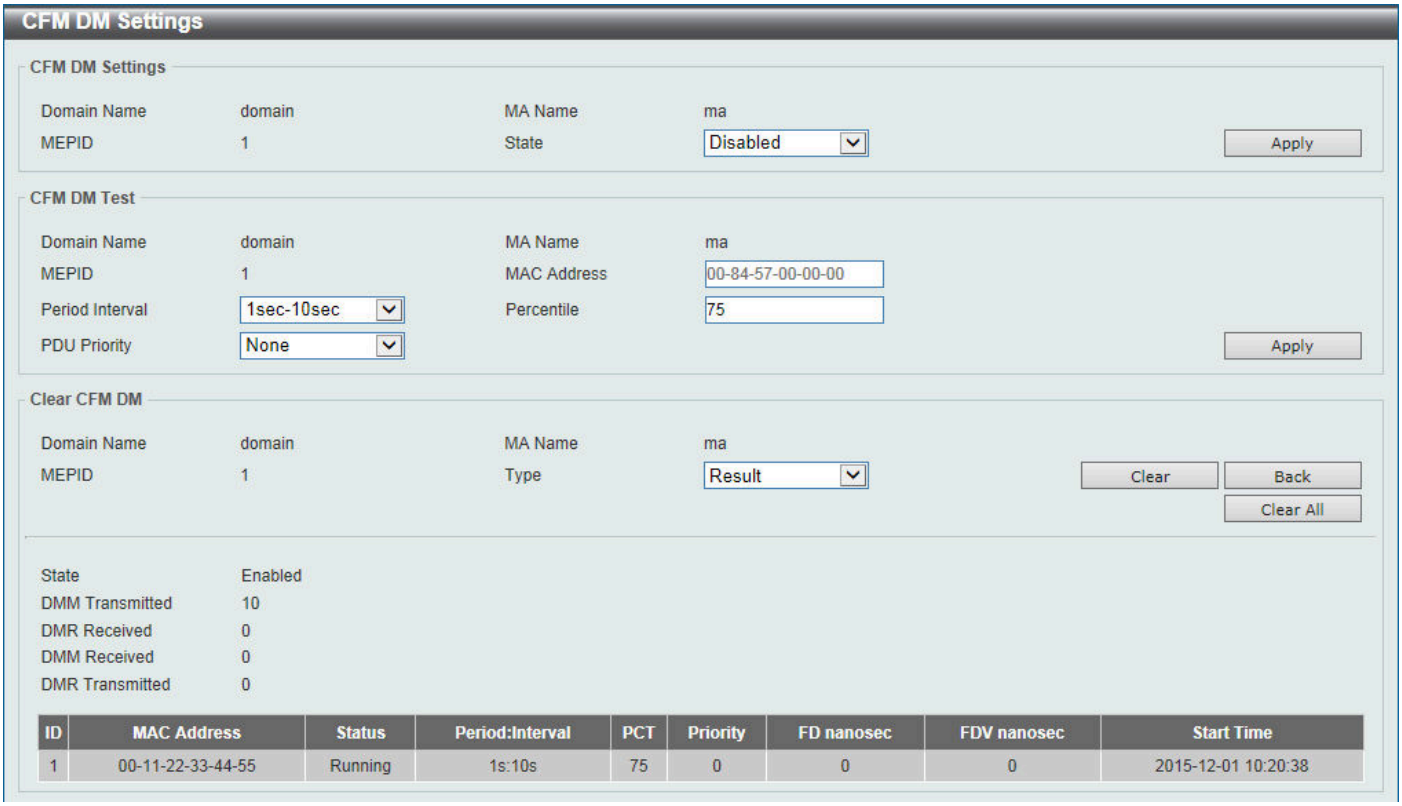


Figure 10-10 CFM Settings (Add MA, Add MEP, Edit DM) Window

The fields that can be configured in **CFM DM Settings** are described below:

Parameter	Description
State	Select to enable or disable the ITU Y.1731 frame Delay Measurement (DM) feature here. When the administrative state of frame delay measurement function is enabled on an MEP, the MEP will be enabled to generate timestamp information, and can reply DMR messages when receiving DMM messages.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **CFM DM Test** are described below:

Parameter	Description
MAC Address	Enter the MAC address for the DM test here.
Period Interval	Select the period interval time here. This specifies the transmitting period of the DDM message and diagnostic interval. Options to choose from are:

Parameter	Description
	• **100ms-1sec** - The transmission period is 100 milliseconds and the diagnostic interval is 1 second. • **1sec-10sec** - The transmission period is 1 second and the diagnostic interval is 10 seconds. This is the default value. • **10sec-1min** - The transmission period is 10 seconds and the diagnostic interval is 1 minute.
Percentile	Enter the percentile value here. This specifies the percentile of Frame Delay (FD) and Frame Delay Variation (FDV) measurement. The range is from 0 to 100. The default value is 75.
PDU Priority	Select the PDU priority value here. The range is from 0 to 7and none. This specifies the 802.1p priority to be set in the DMM messages transmitted by the MEP. The default value is the PDU priority of the MEP.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Clear CFM DM** are described below:

Parameter	Description
Type	Select the type of information to clear here. Options to choose from are: • **Result** - Specifies to clear the stored DM results. • **Statistics** - Specifies to clear the stored statistics of ETH-DM frames (DMM and DMR).

Click the **Clear** button to clear the CFM DM statistics information based on the selection made.

Click the **Clear All** button to clear all the CFM DM statistics information.

Click the **Back** button to return to the previous window.

After clicking the **Edit LM** button, the following page will appear.

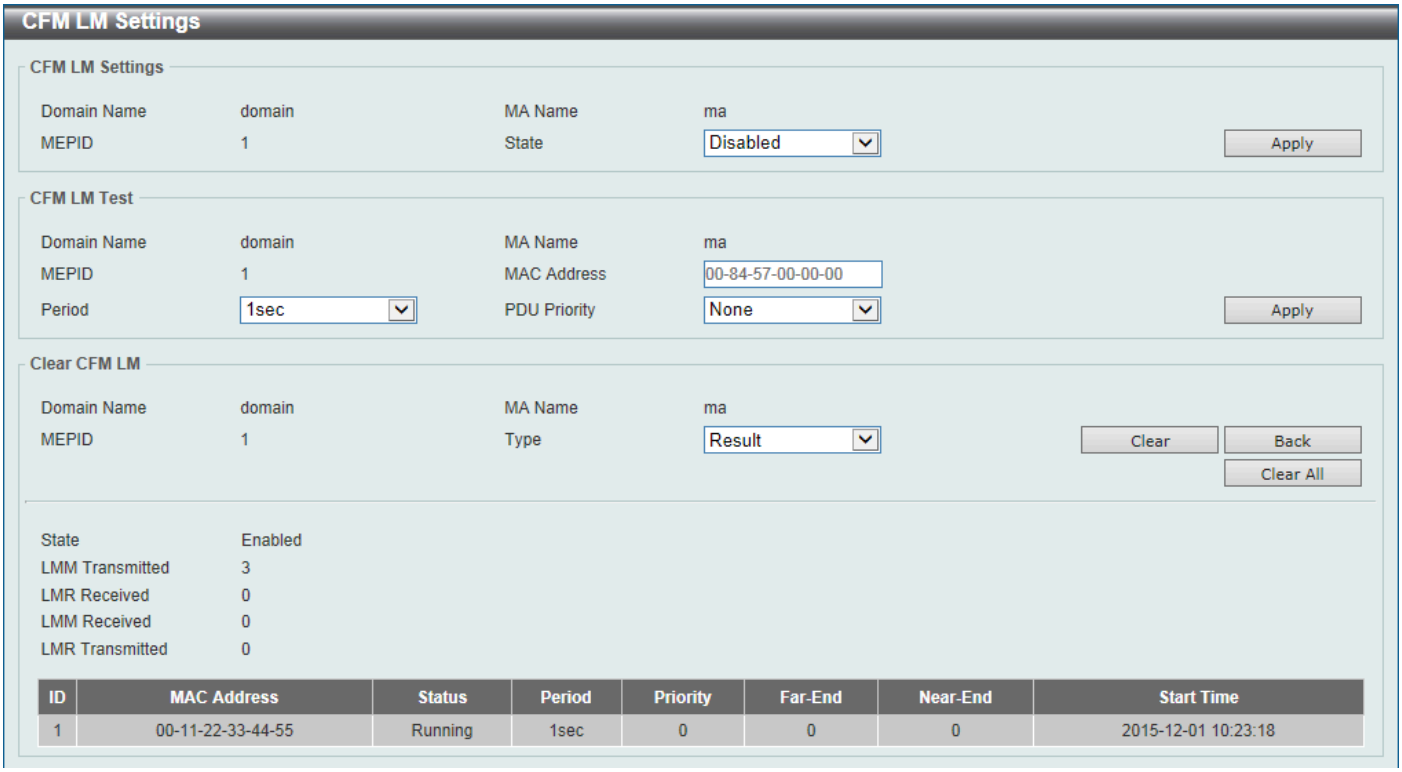


Figure 10-11 CFM Settings (Add MA, Add MEP, Edit LM) Window

The fields that can be configured in **CFM LM Settings** are described below:

Parameter	Description
State	Select to enable or disable the ITU Y.1731 Loss Measurement (LM) feature here. When the administrative state of frame loss measurement function is enabled on an MEP, the MEP will maintain the counters of frame loss measurement function and can reply LMR messages when receiving LMM messages.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **CFM LM Test** are described below:

Parameter	Description
MAC Address	Enter the MAC address for the LM test here.
Period	Select the time period here. This specifies the transmitting interval of the LM PDU. Options to choose from are **100ms**, **1sec**, and **10sec**.
PDU Priority	Select the PDU priority value here. The range is from 0 to 7 and none. This specifies the 802.1p priority to be set in the LMM messages transmitted by the MEP. The default value is the PDU priority of the MEP.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Clear CFM LM** are described below:

Parameter	Description
Type	Select the type of information to clear here. Options to choose from are: • **Result** - Specifies to clear the stored LM results. • **Statistics** - Specifies to clear the stored statistics of ETH-LM frames (LMM and LMR).

Click the **Clear** button to clear the CFM LM statistics information based on the selection made.

Click the **Clear All** button to clear all the CFM LM statistics information.

Click the **Back** button to return to the previous window.

CFM Port Settings

This window is used to display and configure the CFM port settings.

To view the following window, click **OAM > CFM > CFM Port Settings**, as shown below:

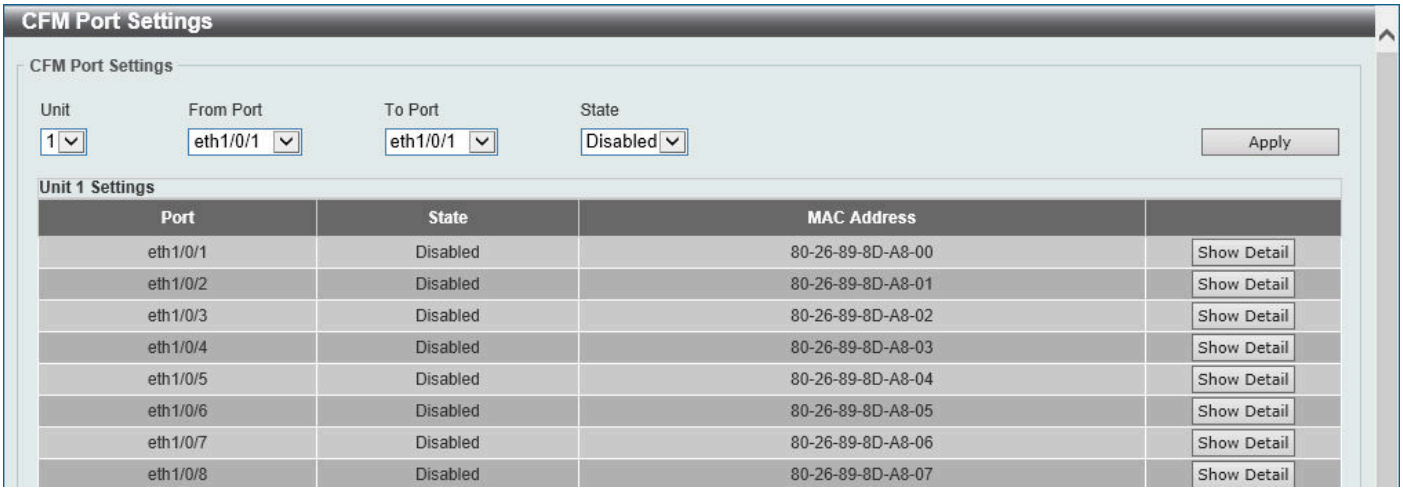


Figure 10-12 CFM Port Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit ID that will be used here. This option is only available if stacking is enabled.
From Port - To Port	Select the Switch port range that will be used here.
State	Select the enable or disable the CFM feature on the specified port(s) here.

Click the **Apply** button to accept the changes made.

Click the **Show Detail** button to more detailed information about the CFM settings on the specified port.

After clicking the **Show Detail** button, the following page will appear.



Figure 10-13 CFM Port Settings (View Detail) Window

Click the **Back** button to return to the previous window.

CFM Loopback Test

This window is used to display and configure the CFM loopback test settings.

To view the following window, click **OAM > CFM > CFM Loopback Test**, as shown below:

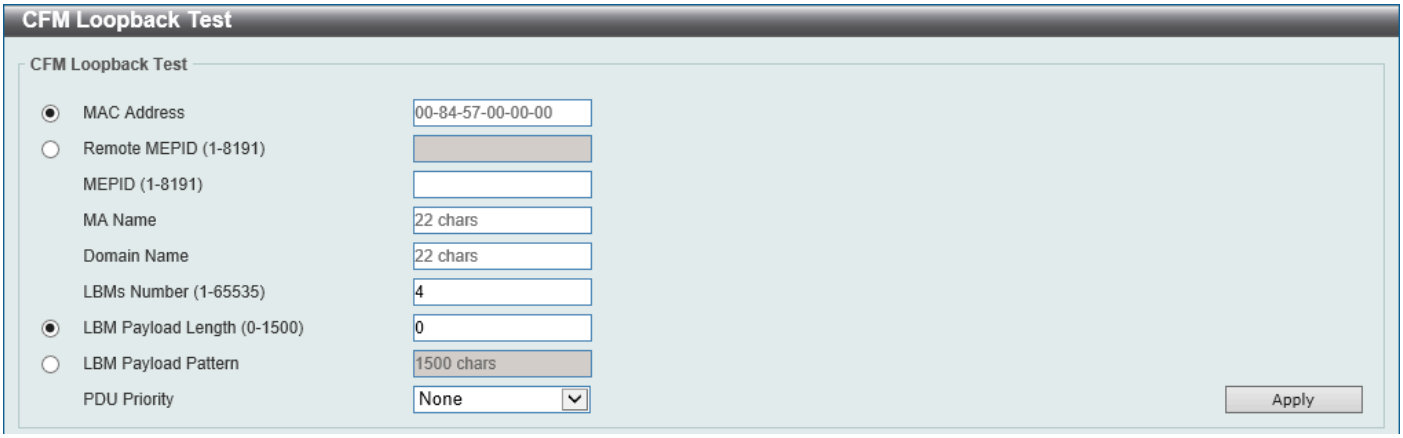


Figure 10-14 CFM Loopback Test Window

The fields that can be configured are described below:

Parameter	Description
MAC Address	Select and enter the destination MAC address here.
Remote MEPID	Select and enter the remote MEP ID here. The range is from 1 to 8191.
MEPID	Enter the MEP ID that will initiate the loopback test here. The range is from 1 to 8191.
MA Name	Enter the MA name here. This name can be up to 22 characters long.
Domain Name	Enter the MD name here. This name can be up to 22 characters long.
LBMs Number	Enter the number of LBMs to be sent here. The range is from 1 to 65535. By default, this value is 4.
LBM Payload Length	Select and enter the payload length of the LBM to be sent here. The range is from 0 to1500. By default, this value is 0.
LBM Payload Pattern	Select and enter the LBM payload pattern here. This specifies an arbitrary amount of data to be included in a Data TLV, along with an indication whether the Data TLV is to be included. This string can be up to 1500 characters long. spaces are not allowed.
PDU Priority	Select the 802.1p priority to be set in the transmitted LBMs here. If not specified, it uses the same priority as the CCMs sent by the MA. The range is from 0 to 7 and none. Select the **None** option to use the default setting.

Click the **Apply** button to accept the changes made. The CFM Loopback Test Result screen will be displayed.

CFM Linktrace Settings

This window is used to display and configure the CFM linktrace settings.

To view the following window, click **OAM > CFM > CFM Linktrace Settings**, as shown below:

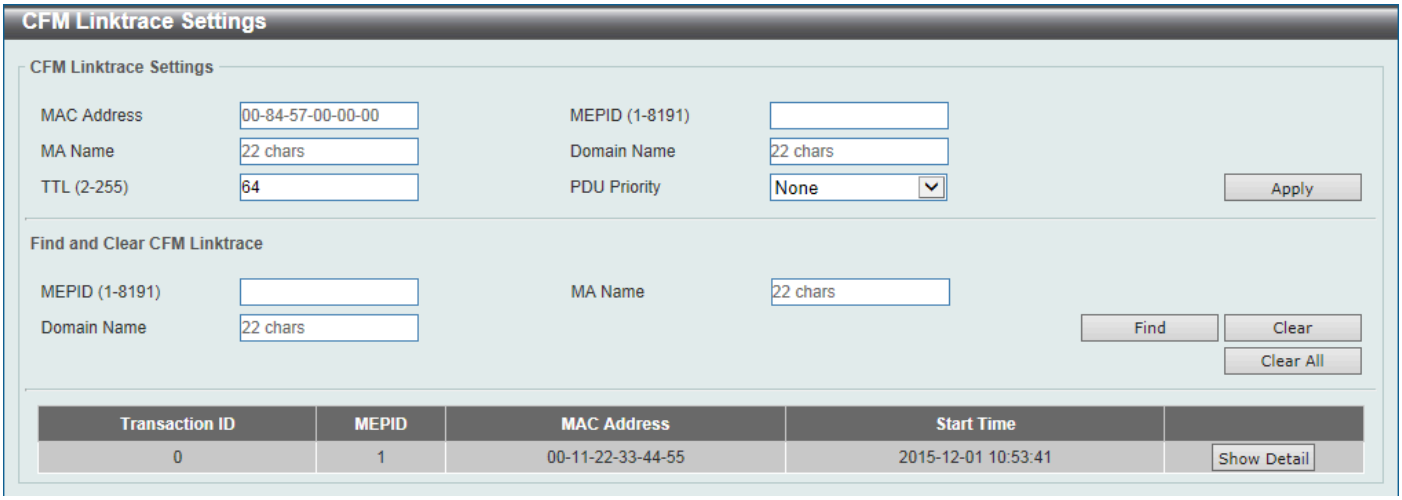


Figure 10-15 CFM Linktrace Settings Window

The fields that can be configured in **CFM Linktrace Settings** are described below:

Parameter	Description
MAC Address	Enter the destination MAC address here.
MEPID	Enter the MEP ID here used to initiate the link-trace feature. The range is from 1 to 8191.
MA Name	Enter the MA name here. The name can be up to 22 characters long.
Domain Name	Enter the MD name here. The name can be up to 22 characters long.
TTL	Enter the link-trace message's TTL value here. The range is from 2 to 255. The default value is 64.
PDU Priority	Select the 802.1p priority to be set in the transmitted LBMs here. If not specified, it uses the same priority as the CCMs sent by the MA. The range is from 0 to 7 and none. Select the **None** option to use the default setting.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Find and Clear CFM Linktrace** are described below:

Parameter	Description
MEPID	Enter the MEP ID here. The range is from 1 to 8191.
MA Name	Enter the MA name here. The name can be up to 22 characters long.
Domain Name	Enter the MD name here. The name can be up to 22 characters long.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear** button to clear the entries based on the information specified.

Click the **Clear All** button to clear the information associated with all entries.

Click the **Show Detail** button to view more detailed information about the link-trace entry.

After clicking the **Show Detail** button, the following page will appear.



Figure 10-16 CFM Linktrace Settings (Show Detail) Window

Click the **Back** button to return to the previous window.

CFM Packet Counter

This window is used to find and display the CFM packet counter information.

To view the following window, click **OAM > CFM > CFM Packet Counter**, as shown below:

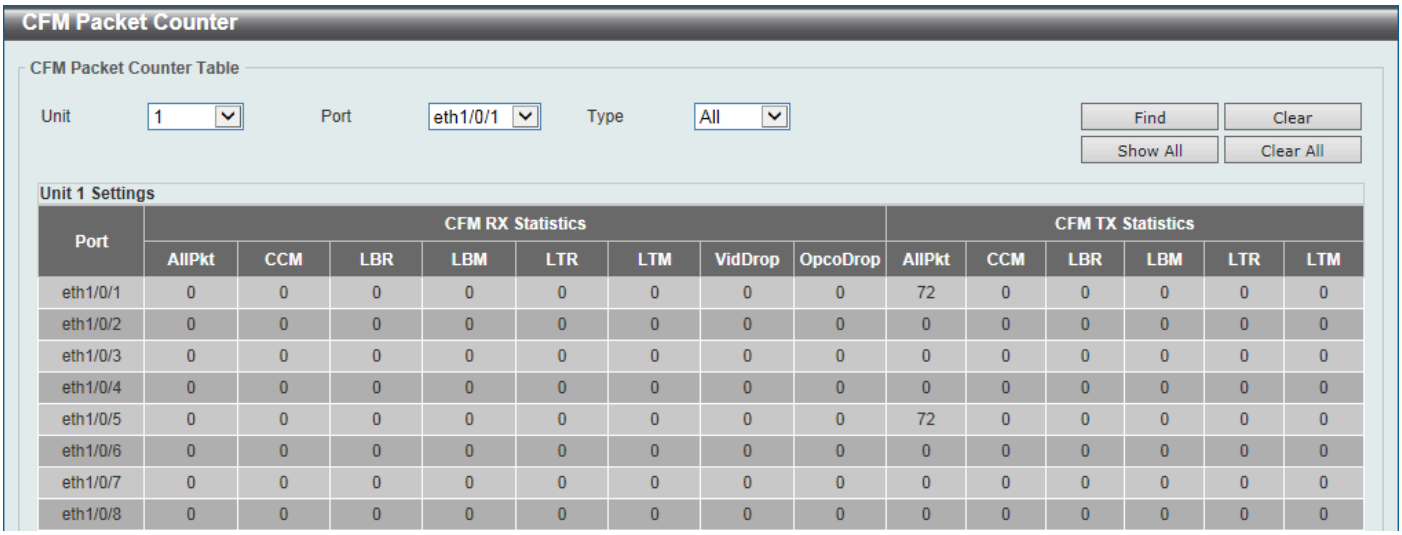


Figure 10-17 CFM Packet Counter Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit ID that will be used here. This option is only available if stacking is enabled.
Port	Select the Switch port that will be used here.
Type	Select the type of counter information that will be cleared or displayed here. Options to choose from are **All**, **TX**, and **RX**.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear** button to clear the counter information based on the information specified.

Click the **Show All** button to display all the entries.

Click the **Clear All** button to clear the counter information associated with all entries.

CFM Counter CCM

This window is used to view and clear the CFM CCM counter information.

To view the following window, click **OAM > CFM > CFM Counter CCM**, as shown below:

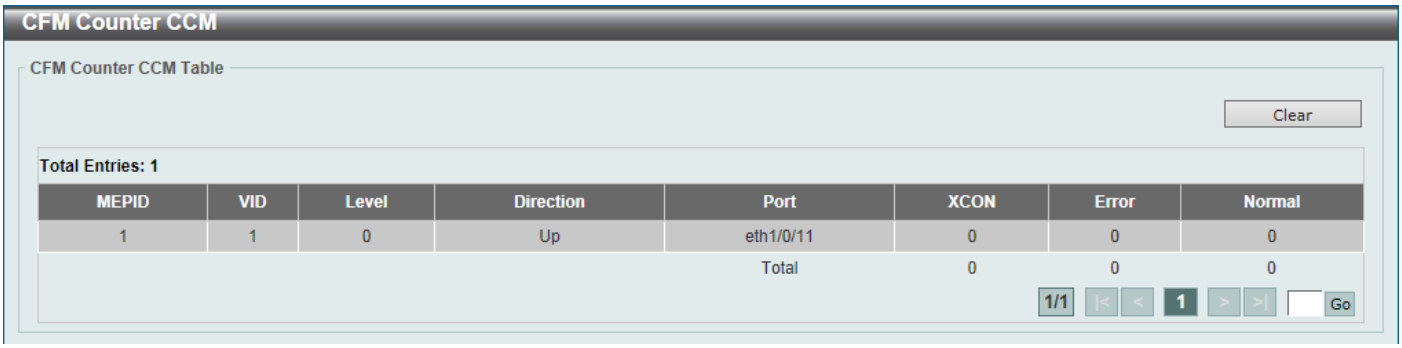


Figure 10-18 CFM Counter CCM Window

Click the **Clear** button to clear the counter information associated with all entries.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

CFM MIP CCM Table

This window is used to display the MIP CCM database entries.

To view the following window, click **OAM > CFM > CFM MIP CCM Table**, as shown below:



Figure 10-19 CFM MIP CCM Table Window

CFM MEP Fault Table

This window is used to display the MEPs that have faults.

To view the following window, click **OAM > CFM > CFM MEP Fault Table**, as shown below:

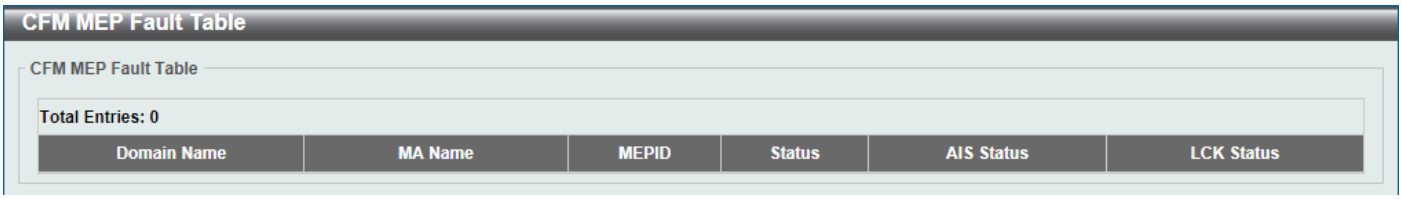


Figure 10-20 CFM MEP Fault Table Window

Cable Diagnostics

The cable diagnostics feature is designed primarily for administrators or customer service representatives to verify and test copper cables; it can rapidly determine the quality of the cables and the types of error.

To view the following window, click **OAM > Cable Diagnostics**, as shown below:

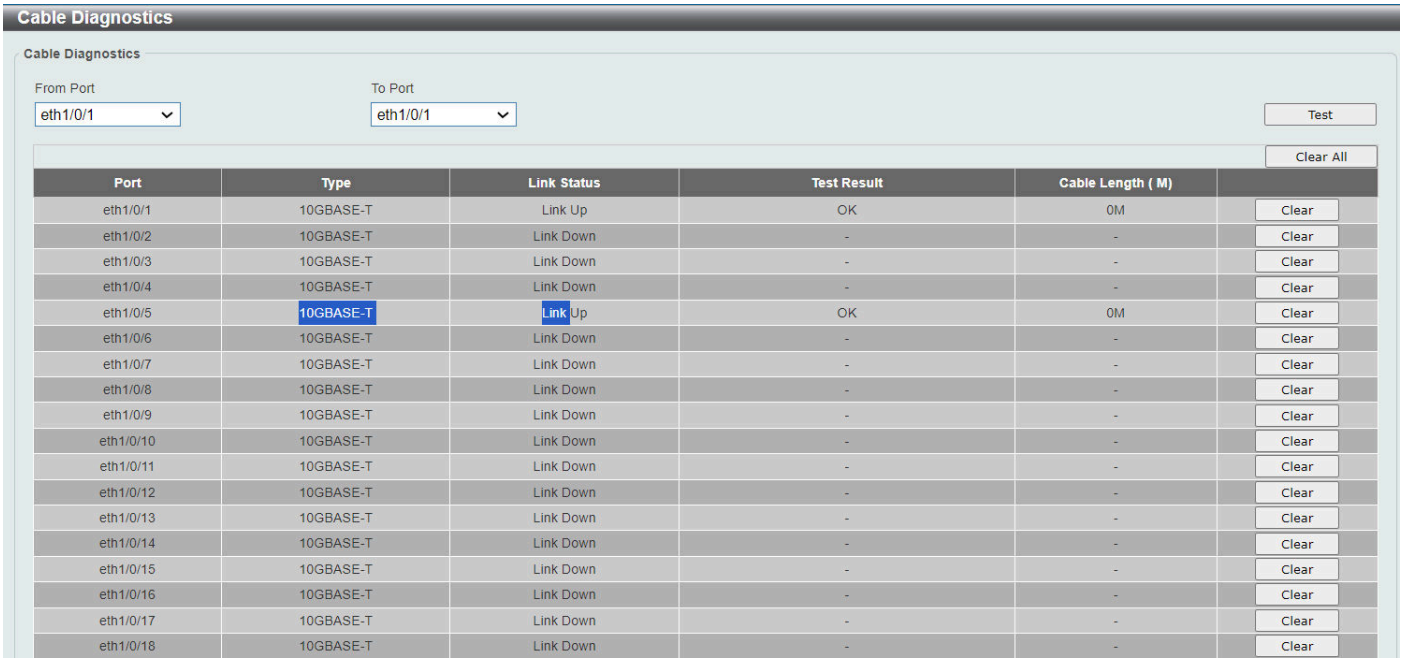


Figure 10-21 Cable Diagnostics Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available if stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.

Click the **Test** button to test the specific port.

Click the **Clear** button to clear all the information for the specific port.

Click the **Clear All** button to clear all the information in this table.

NOTE: Cable diagnostic function limitations. Cable length detection is only supported on physical port interface.

NOTE: The maximum cable diagnosis length is 120 meters.

NOTE: The deviation of cable length detection is about 10 meters for GE ports.

Fault messages:

- **Unknown** - The diagnosis result contains open, short or cross talk status. Any one of the status be detected, switch will display unknow error message.
- **NA** - No cable was found, maybe it's because cable is out of diagnosis specification or the quality is too bad.

Ethernet OAM

Ethernet OAM Settings

This window is used to display and configure the Ethernet Operations, Administration, and Maintenance (OAM) settings.

To view the following window, click **OAM > Ethernet OAM > Ethernet OAM Settings**, as shown below:

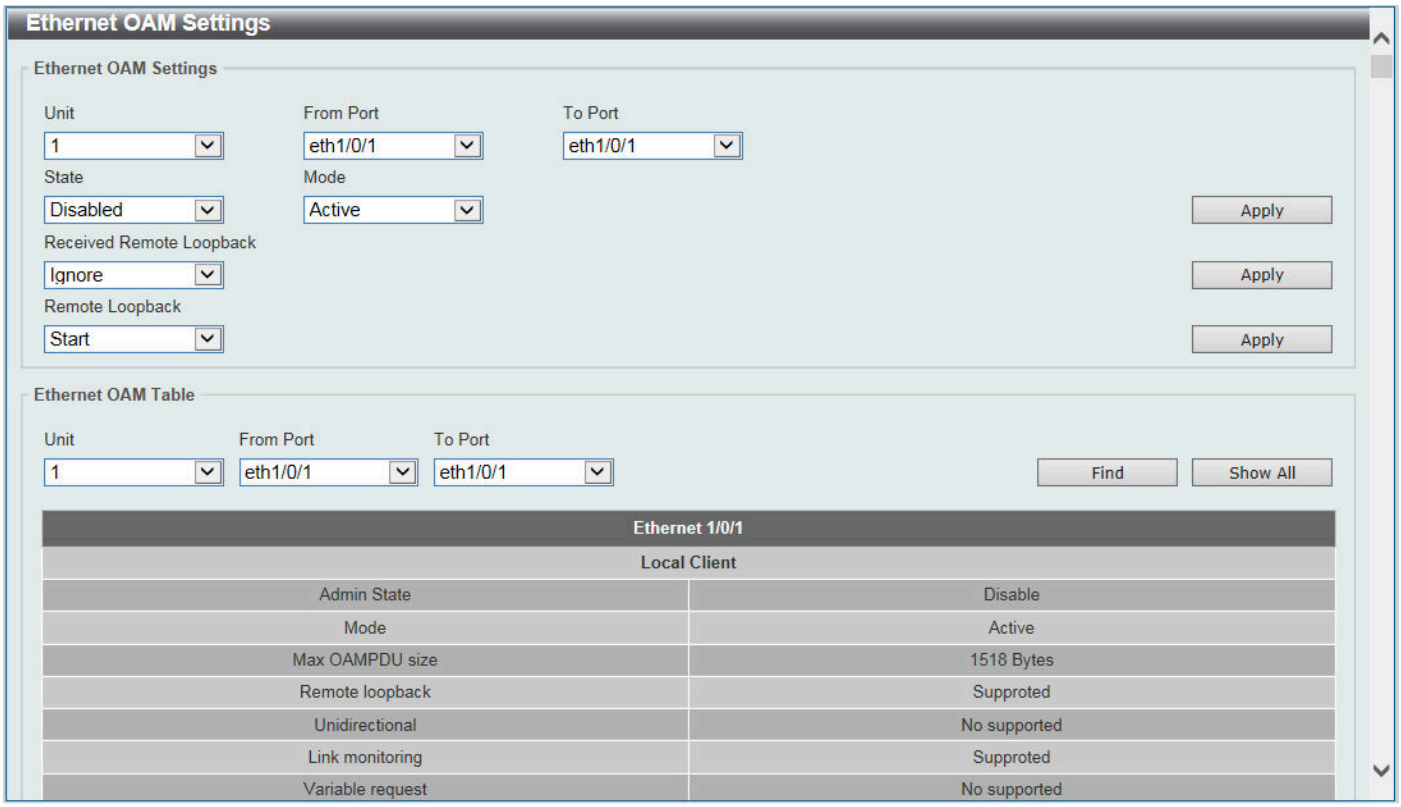


Figure 10-22 Ethernet OAM Settings Window

The fields that can be configured in **Ethernet OAM Settings** are described below:

Parameter	Description
Unit	Select the Switch unit ID that will be used here. This option is only available if stacking is enabled.
From Port - To Port	Select the Switch port range that will be used here.

Parameter	Description
State	Select to enable or disable the Ethernet OAM feature on the specified port(s) here. After enabling this function on the interface, the interface will start OAM discovery. If the OAM mode of this interface is active, it initiates the discovery. Otherwise, it reacts to the discovery received from the peer.
Mode	Select the Ethernet OAM mode here. Options to choose from are **Active** and **Passive**. The following two actions are allowed by ports in the active mode but disallowed by ports in the passive mode. (1) Initiate OAM discovery. (2) Start or stop remote loopback.
Received Remote Loopback	Select to configure the behavior of the received remote loopback requirement from the peer on the specified port(s) here. Options to choose from are **Ignore** and **Process**. • **Ignore** - Specifies not to react to remote loopback requirements from a peer. • **Process** - Specifies to react to remote loopback requirements from a peer. The feature is used to configure the client to process or to ignore the received Ethernet OAM remote loopback feature. In the remote loopback mode, all user traffic will not be processed. Ignoring the received remote loopback feature will prevent the port from entering the remote loopback mode.
Remote Loopback	Select the remote loopback action here. Options to choose from are **Start** and **Stop**. • **Start** - Specifies to request the peer to change to the remote loopback mode. • **Stop** - Specifies to request the peer to change to the normal operation mode. If the remote peer is configured to ignore the remote loopback request, then the remote peer will not enter or exit the remote loopback mode upon receiving the request. To start the remote peer to enter the remote loopback mode, administrators must ensure that the local client is in the active mode and the OAM connection is established. If the local client is already in the remote loopback mode, then this feature cannot be applied.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Ethernet OAM Table** are described below:

Parameter	Description
Unit	Select the Switch unit ID that will be used here. This option is only available if stacking is enabled.
From Port - To Port	Select the Switch port range that will be used here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to display all the entries.

Ethernet OAM Configuration Settings

This window is used to display and configure the Ethernet OAM configuration settings.

To view the following window, click **OAM > Ethernet OAM > Ethernet OAM Configuration Settings**, as shown below:

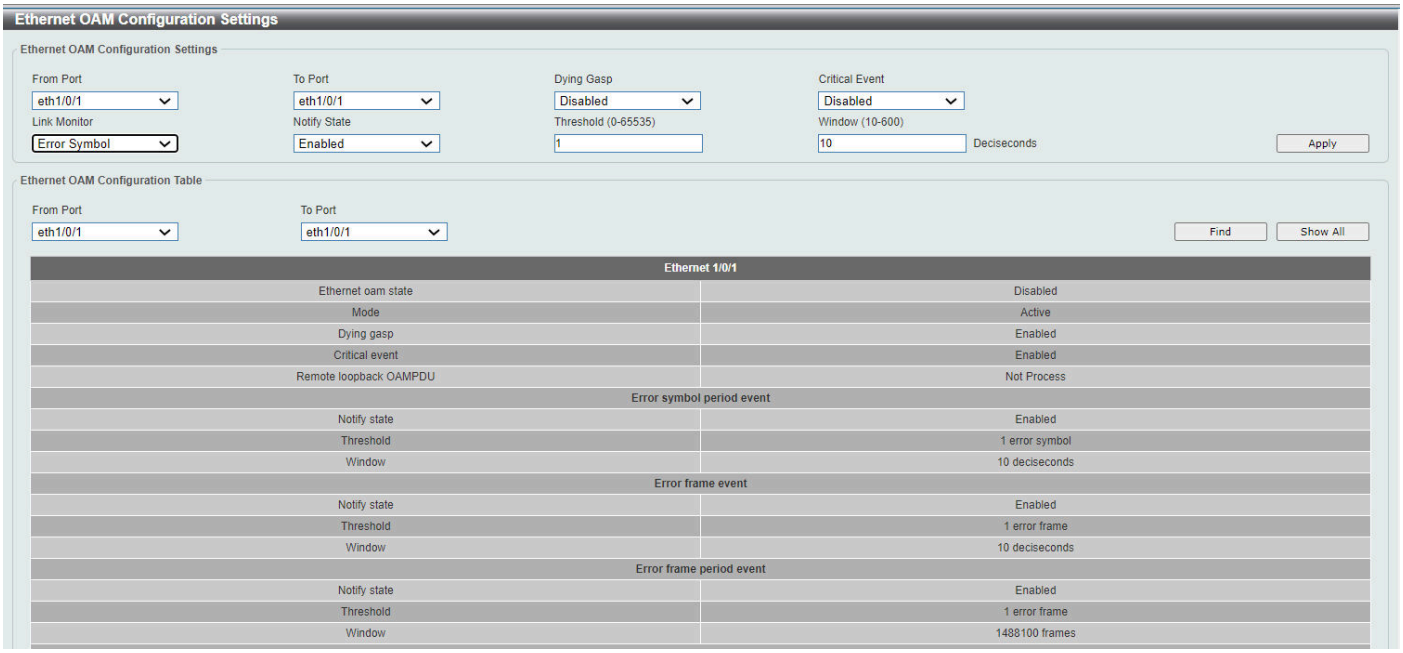


Figure 10-23 Ethernet OAM Configuration Settings Window

The fields that can be configured in **Ethernet OAM Configuration Settings** are described below:

Parameter	Description
Unit	Select the Switch unit ID that will be used here. This option is only available if stacking is enabled.
From Port - To Port	Select the Switch port range that will be used here.
Dying Gasp	Select to enable or disable the dying gasp feature here. This feature is used to configure the capability of the dying gasp event. If the capability for the dying gasp event is disabled, the port will never send out OAM PDUs with the dying gasp event bit set when an unrecoverable local failure condition has occurred.
Critical Event	Select to enable or disable the critical event feature here. This feature is used to configure the capability of the critical event. If the capability for a critical event is disabled, the port will never send out OAM PDUs with critical event bit set when an unspecified critical event has occurred.
Link Monitor	Select the link monitor feature here. Options to choose from are **Error Symbol**, **Error Frame**, **Error Frame Seconds**, and **Error Frame Period**. • **Error Symbol** - This feature is used to enable notifying the Ethernet OAM error symbol event and configure the monitor threshold rangeand window on the specified port. • **Error Frame** - This feature is used to enable notifying the Ethernet OAM error frame event and configure the monitor threshold and window on the specified port. • **Error Frame Seconds** - This feature is used to enable notifying the Ethernet OAM error frame second event and configure the monitor threshold and window on the specified port. • **Error Frame Period** - This feature is used to enable notifying the Ethernet OAM error frame period event and configure the monitor threshold and window on the specified port.
Notify State	Select to enable or disable the notify state here.
Threshold	Enter the threshold value here. • When **Error Symbol** is selected as the link monitor, enter the number of symbol errors here. If symbol errors occur in the specified window and it

Parameter	Description
	exceeds the threshold value, then the event is generated. The range is from 0 to 65535 and default is 1. • When **Error Frame** is selected as the link monitor, enter the number of frame errors here. If the error frames occur in the specified window and exceeds the threshold value, then an error frame event is triggered. The range is from 0 to 65535 and default is 1. • When **Error Frame Seconds** is selected as the link monitor, enter the number of error frames in seconds here. If the number of the error frames occurred in the specified window and exceeds the threshold value, then the frame event is triggered. The range is from 1 to 900 seconds and default is 1. • When **Error Frame Period** is selected as the link monitor, enter the number of frame errors that must occur for this event to be triggered here. The range is from 0 to 65535 and default is 1.
Window	Enter the window value here. • When **Error Symbol** is selected as the link monitor, enter the amount of time over which the threshold is defined here. If threshold symbol errors occur within the period, an event notification OAM PDU should be generated with an error symbol period event TLV, indicating that the threshold has been crossed in this window. The range is from 10 to 600 deciseconds and default is 10 deciseconds (1 decisecond = 0.1 second) . • When **Error Frame** is selected as the link monitor, enter the amount of time over which the threshold is defined here. If the threshold frame errors occur within the period, an event notification OAM PDU will be generated with an error frame event TLV, indicating that the threshold has been crossed in this window. The range is from 10 to 600 deciseconds and default is 10 deciseconds. • When **Error Frame Seconds** is selected as the link monitor, enter the amount of time over which the threshold is defined here. If threshold frame errors occur within the period, an event notification OAM PDU will be generated with an error frame seconds summary event TLV indicating that the threshold has been crossed in this window. The range is from 100 to 9000 deciseconds and default is 600 deciseconds (1 decisecond = 0.1 second). • When **Error Frame Period** is selected as the link monitor, enter the number of frames over which the threshold is defined here. If threshold frame errors occur within the period, an event notification OAM PDU should be generated with an error frame period event TLV indicating that the threshold has been crossed in this window. The lower bound is the number of minimum frame-size frames that can be received in 100ms on the underlying physical layer. The upper bound is the number of minimum frame-size frames that can be received in one minute on the underlying physical layer. The range is from 148810 to 892860000 and default is 148810 deciseconds (1 decisecond = 0.1 second).

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Ethernet OAM Configuration Table** are described below:

Parameter	Description
Unit	Select the Switch unit ID that will be used here.This option is only available when stacking is enabled.
From Port - To Port	Select the Switch port range that will be used here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to display all the entries.

Ethernet OAM Event Log Table

This window is used to view and clear the Ethernet OAM event log table.

To view the following window, click **OAM > Ethernet OAM > Ethernet OAM Event Log Table**, as shown below:

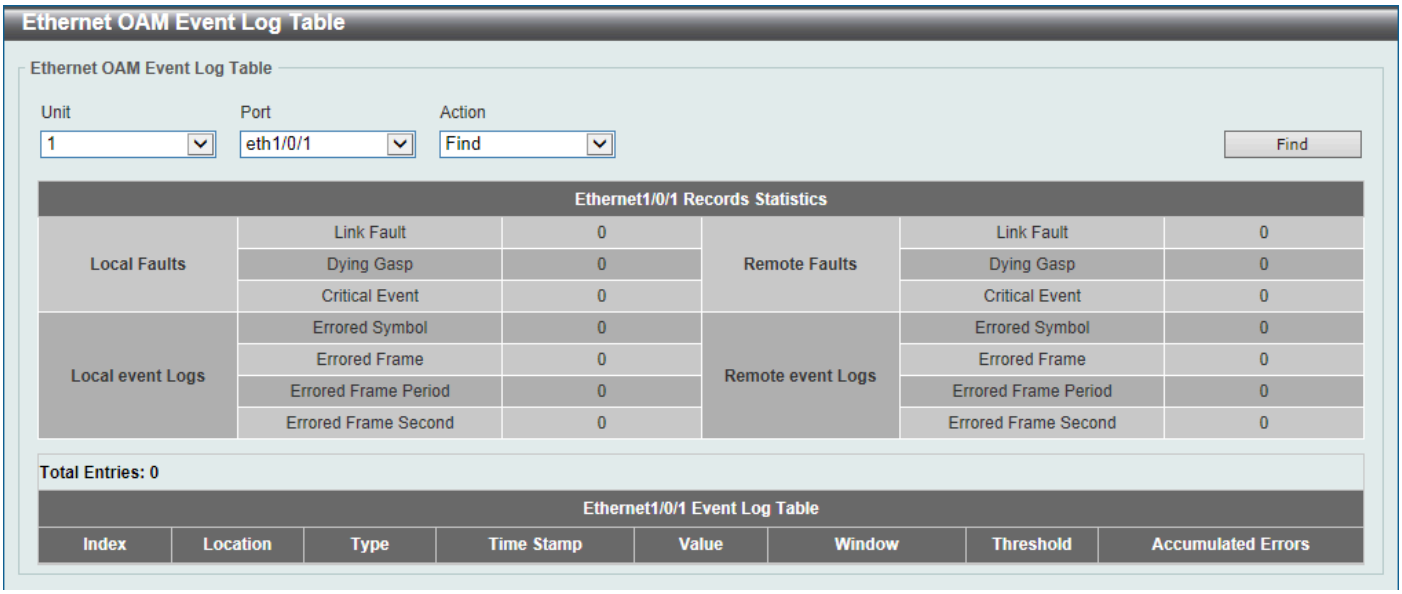


Figure 10-24 Ethernet OAM Event Log Table Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit ID that will be used here. This option is only available if stacking is enabled.
Port	Select the Switch port that will be used here.
Action	Select the **Find** option to find and display the log entries associated with the specified port. Select the **Clear** option to clear the log entries associated with the specified port.

Click the **Find** button to find and display the log entries associated with the specified port.

Ethernet OAM Statistics Table

This window is used to view and clear the Ethernet OAM statistics table.

To view the following window, click **OAM > Ethernet OAM > Ethernet OAM Statistics Table**, as shown below:

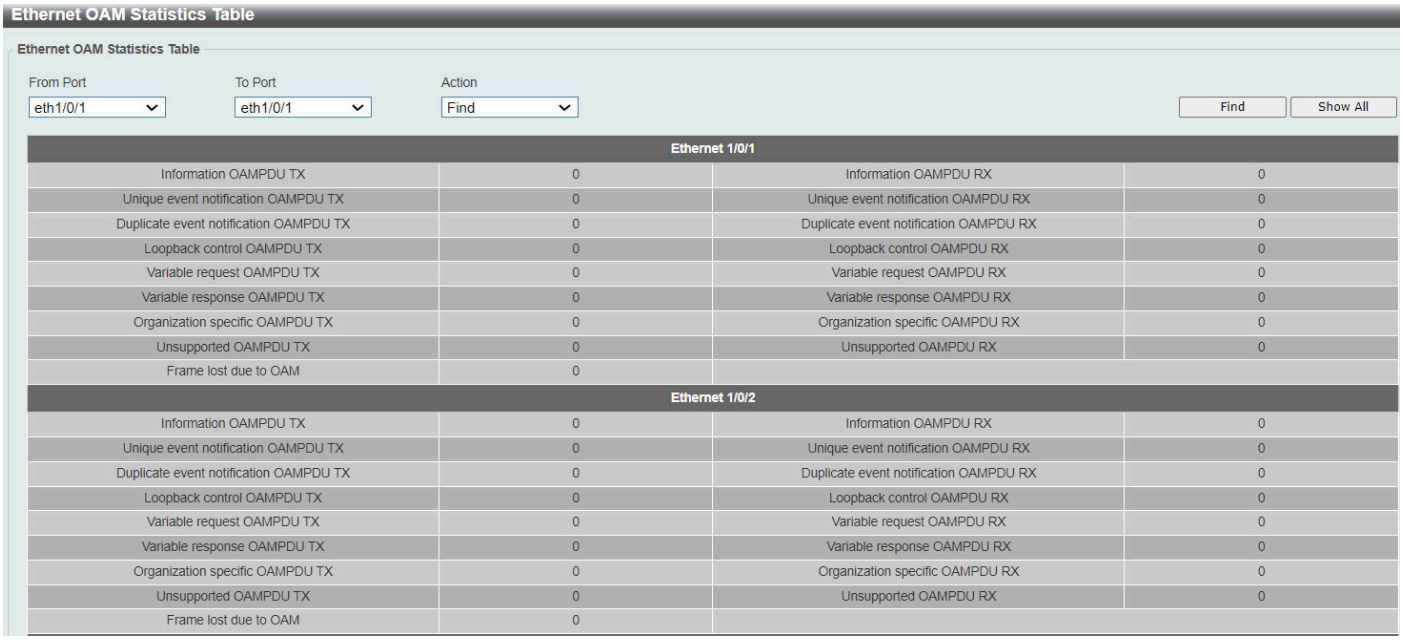


Figure 10-25 Ethernet OAM Statistics Table Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit ID that will be used here. This option is only available if stacking is enabled.
From Port - To Port	Select the Switch port range that will be used here.
Action	Select the **Find** option to find and display the statistics information associated with the specified port. Select the **Clear** option to clear the statistics information associated with the specified port(s).

Click the **Find** button to find and display the statistics information associated with the specified port(s).

Click the **Show All** button to display all the statistics information.

Ethernet OAM DULD Settings

This window is used to display and configure the Ethernet OAM D-Link Unidirectional Link Detection (DULD) settings. DULD is an extension of 802.3ah Ethernet OAM. It provides a mechanism to detect a unidirectional point-to-point Ethernet link without PHY support. OAM vendor specific messages are used in the detection. The detection process is started after OAM discovery was started but does not complete the negotiation in the configured discovery time.

To view the following window, click **OAM > Ethernet OAM > Ethernet OAM DULD Settings**, as shown below:

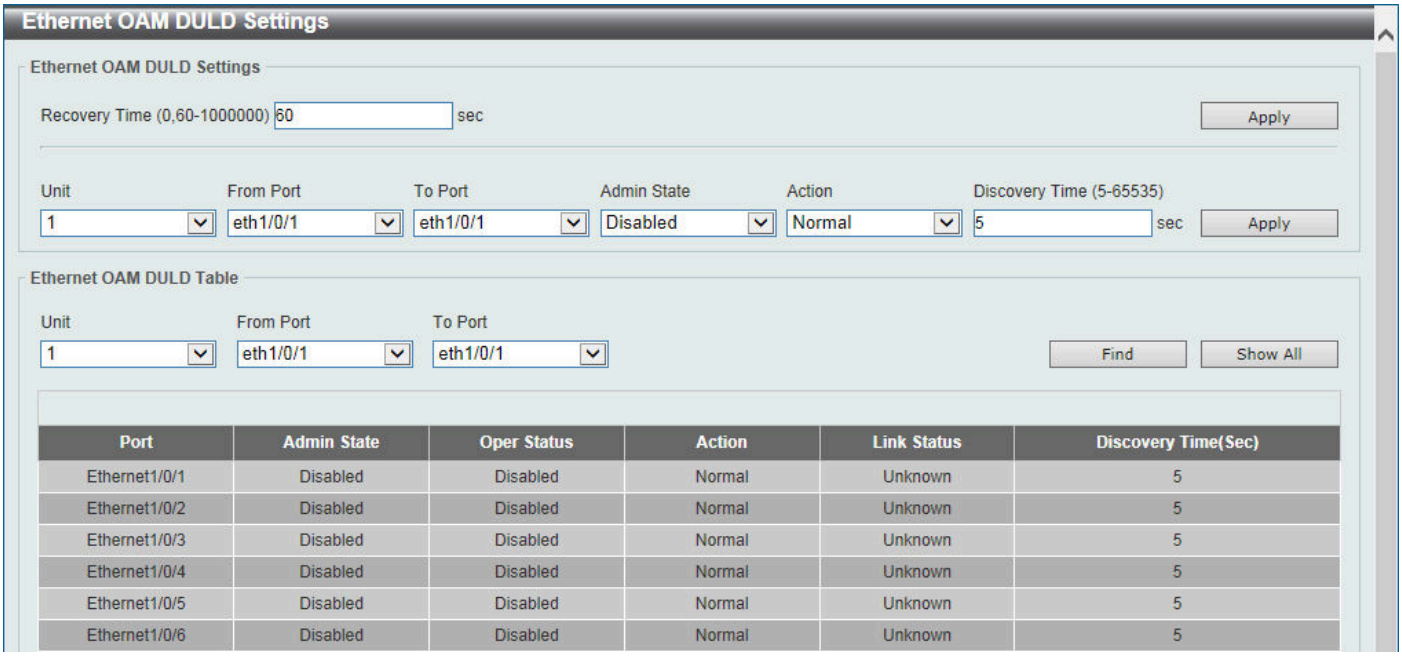


Figure 10-26 Ethernet OAM DULD Settings Window

The fields that can be configured in **Ethernet OAM DULD Settings** are described below:

Parameter	Description
Recovery Time	Enter the time interval value used by DULD to decide how long to recover the disabled port here. When the timer has expired, the disabled port by DULD will be recovered automatically. 0 represents that this function is disabled. This value is either 0 seconds or in the range from 60 to 1000000 seconds.
Unit	Select the Switch unit ID that will be used here. This option is only available if stacking is enabled.
From Port - To Port	Select the Switch port range that will be used here.
Admin State	Select to enable or disable the admin state here. This feature is used to enable Ethernet OAM unidirectional link detection on the specified port(s). The default is disabled.
Action	Select the action that will be taken here. Options to choose from are **Normal** and **Shutdown**.
Discovery Time	Enter the discovery time value here. The range is from 5 to 65535 seconds. By default, this value is 5 seconds. If the OAM discovery does not successfully negotiate before discovery time expired, OAM unidirectional link detection will start.
NOTE: You can configure errdisable trap and recovery settings in **System > Port Configuration > Error Disable Settings**.	

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Ethernet OAM DULD Table** are described below:

Parameter	Description
Unit	Select the Switch unit ID that will be used here. This option is only available if stacking is enabled.
From Port - To Port	Select the Switch port range that will be used here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to display all the entries.

DDM

This folder contains windows that perform Digital Diagnostic Monitoring (DDM) functions on the Switch. There are windows that allow the user to view the digital diagnostic monitoring status of SFP28/SFP+ modules inserting to the Switch and to configure alarm settings, warning settings, temperature threshold settings, voltage threshold settings, bias current threshold settings, Tx power threshold settings, and Rx power threshold settings.

DDM Settings

The window is used to view and configure the action that will occur for specific ports when an exceeding alarm threshold or warning threshold event is encountered.

To view the following window, click **OAM > DDM > DDM Settings**, as shown below:

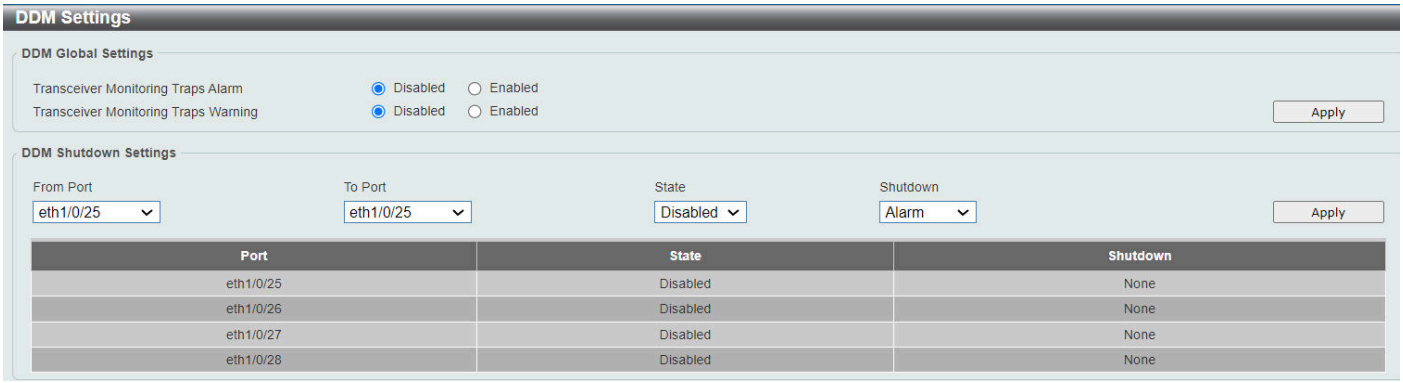


Figure 10-27 DDM Settings Window

The fields that can be configured in **DDM Global Settings** are described below:

Parameter	Description
Transceiver Monitoring Traps Alarm	Select to enable or disable the transceiver monitoring traps alarm feature here. This is disabled by default.
Transceiver Monitoring Traps Warning	Select to enable or disable the transceiver monitoring traps warning feature here. This is disabled by default.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **DDM Shutdown Settings** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. The option is only available when stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here. **NOTE:** Port number specific to fiber optical transceivers will not be available if stacking is enabled (refer to **Management > Stacking**).
State	Use the drop-down menu to enable or disable the DDM state.

Parameter	Description
Shutdown	Specify whether to shut down the port, when the operating parameter exceeds the Alarm or Warning threshold. • **Alarm** - Shutdown the port when the configured alarm threshold range is exceeded. • **Warning** - Shutdown the port when the configured warning threshold range is exceeded. • **None** - The port will never shut down whether the threshold ranges are exceeded or not. This is the default.

Click the **Apply** button to accept the changes made.

DDM Temperature Threshold Settings

This window is used to display and configure the DDM Temperature Threshold Settings for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM Temperature Threshold Settings**, as shown below:

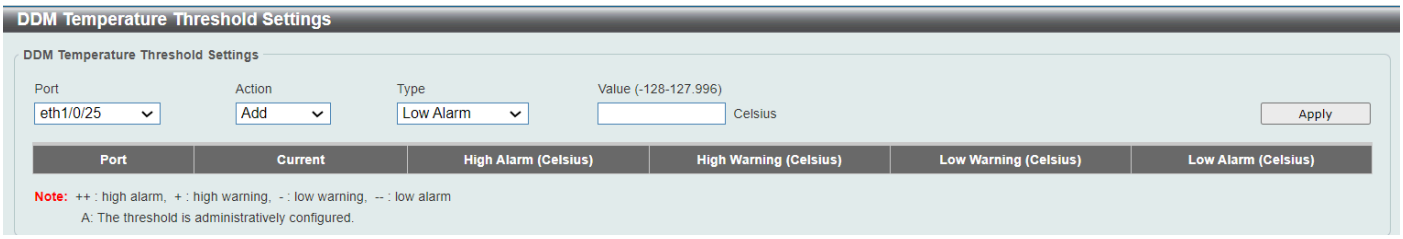


Figure 10-28 DDM Temperature Threshold Settings Window

The fields that can be configured are described below:

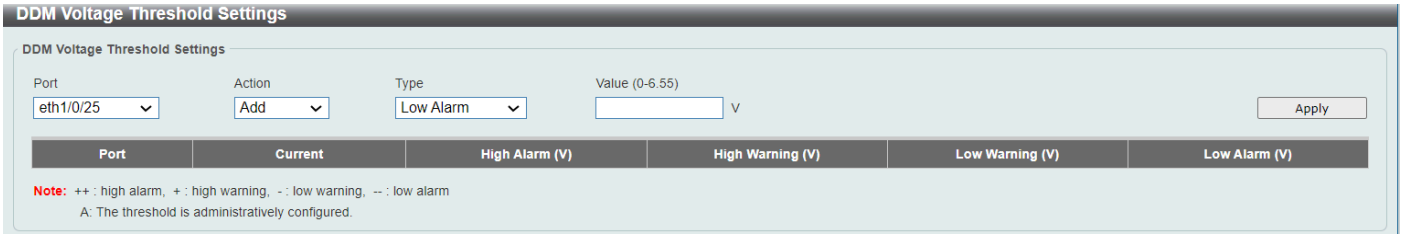
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. The option is only available when stacking is enabled.
Port	Select the port used for the configuration here. **NOTE:** Port number specific to fiber optical transceivers will not be available if stacking is enabled (refer to **Management > Stacking**).
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**.
Type	Select the type of temperature threshold. Options to choose from are **Low Alarm, Low Warning, High Alarm**, and **High Warning**.
Value	Enter the threshold value. This value must be between -128 and 127.996 °C.

Click the **Apply** button to accept the changes made.

DDM Voltage Threshold Settings

This window is used to display and configure the DDM Voltage Threshold Settings for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM Voltage Threshold Settings**, as shown below:



gure 10-29 DDM Voltage Threshold Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
Port	Select the port used for the configuration here. **NOTE:** Port number specific to fiber optical transceivers will not be available if stacking is enabled (refer to **Management > Stacking**).
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**.
Type	Select the type of voltage threshold. Options to choose from are **Low Alarm, Low Warning, High Alarm**, and **High Warning**.
Value	Enter the threshold value. This value must be between 0 and 6.55 Volt.

Click the **Apply** button to accept the changes made.

DDM Bias Current Threshold Settings

This window is used to display and configure the threshold of the bias current for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM Bias Current Threshold Settings**, as shown below:

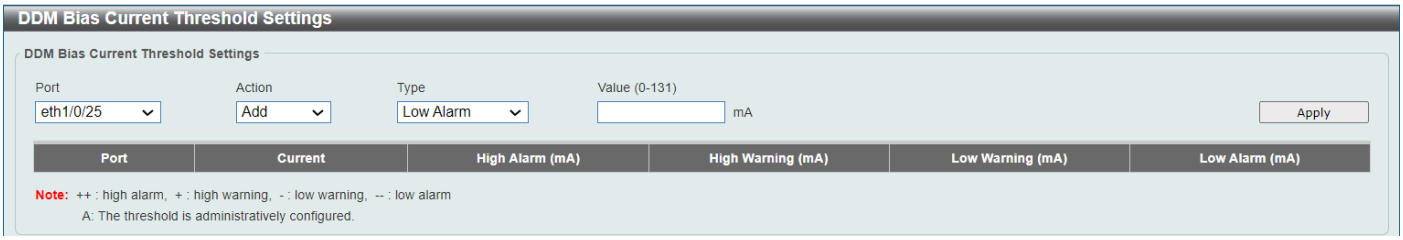


Figure 10-30 DDM Bias Current Threshold Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
Port	Select the port used for the configuration here. **NOTE:** Port number specific to fiber optical transceivers will not be available if stacking is enabled (refer to **Management > Stacking**).
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**.

Parameter	Description
Value	Enter the threshold value. This value must be between 0 and 131 mA.

Click the **Apply** button to accept the changes made.

DDM TX Power Threshold Settings

This window is used to display and configure the threshold of TX power for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM TX Power Threshold Settings**, as shown below:

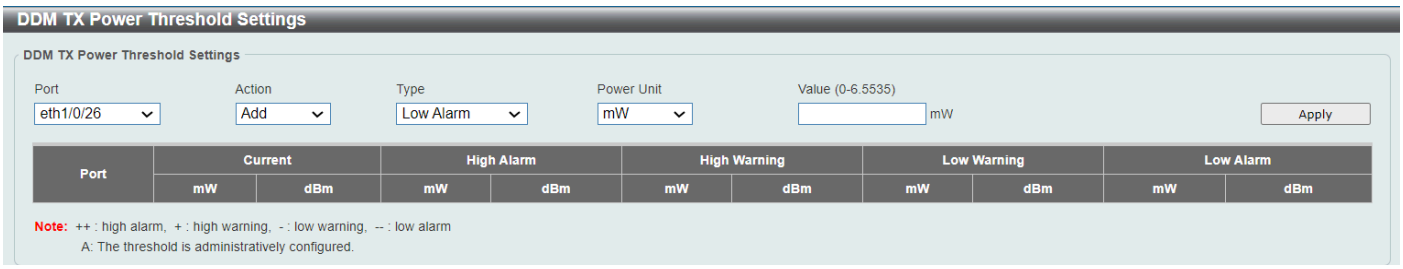


Figure 10-31 DDM TX Power Threshold Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
Port	Select the port used for the configuration here. **NOTE:** Port number specific to fiber optical transceivers will not be available if stacking is enabled (refer to **Management > Stacking**).
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**.
Type	Select the type of TX power threshold. Options to choose from are **Low Alarm, Low Warning, High Alarm**, and **High Warning**.
Power Unit	Select the power unit here. Options to choose from are **mW** and **dBm**.
Value	Enter the threshold value either in **mW** or **dBm** here. • When selecting **mW** in the **Power Unit** drop-down list, this value must be between 0 and 6.5535. • When selecting **dBm** in the **Power Unit** drop-down list, this value must be between -40 and 8.1647.

Click the **Apply** button to accept the changes made.

DDM RX Power Threshold Settings

This window is used to display and configure the threshold of RX power for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM RX Power Threshold Settings**, as shown below:

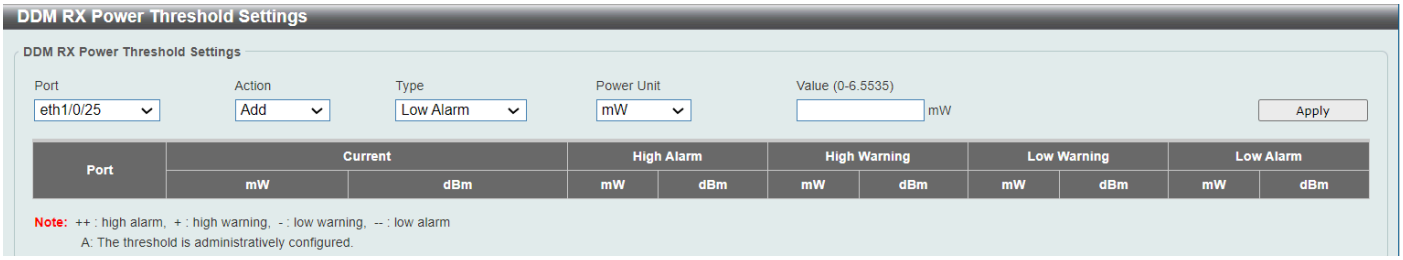


Figure 10-32 DDM RX Power Threshold Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
Port	Select the port used for the configuration here. **NOTE:** Port number specific to fiber optical transceivers will not be available if stacking is enabled (refer to **Management > Stacking**).
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**.
Type	Select the type of RX power threshold. Options to choose from are **Low Alarm, Low Warning, High Alarm**, and **High Warning**.
Power Unit	Select the power unit here. Options to choose from are **mW** and **dBm**.
Value	Enter the threshold value either in **mW** or **dBm** here. • When selecting **mW** in the **Power Unit** drop-down list, this value must be between 0 and 6.5535. • When selecting **dBm** in the **Power Unit** drop-down list, this value must be between -40 and 8.1647.

Click the **Apply** button to accept the changes made.

DDM Status Table

This window is used to display the current operating digital diagnostic monitoring parameters and their values on the SFP28/SFP+ module for specified ports.

To view the following window, click **OAM > DDM > DDM Status Table**, as shown below:

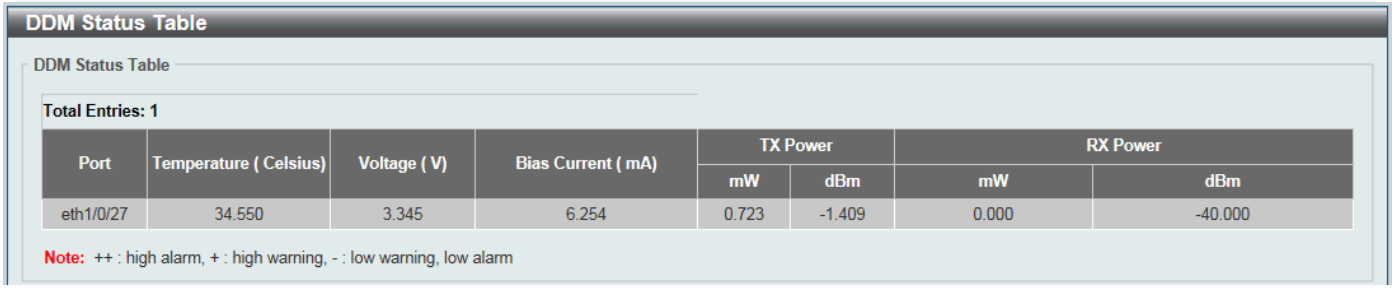


Figure 10-33 DDM Status Table Window

11. Monitoring

VLAN Counter
Utilization
Statistics
Mirror Settings
sFlow
Device Environment

VLAN Counter

This window is used to display and configure the VLAN counter settings. This is used to create a control entry for traffic statistics on specified Layer 2 VLAN interface(s).

To view the following window, click **Monitoring > VLAN Counter**, as shown below:

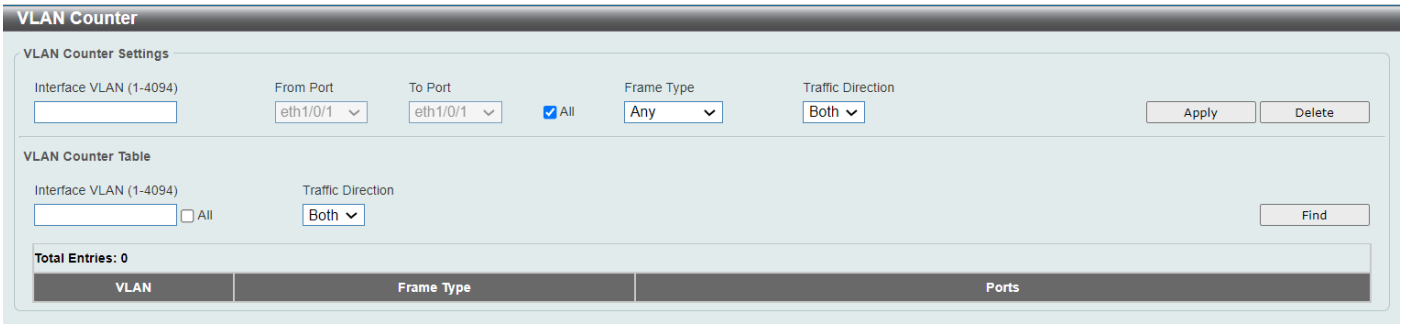


Figure 11-1 VLAN Counter Window

The fields that can be configured for **VLAN Counter Settings** are described below:

Parameter	Description
Interface VLAN	Enter the VLAN ID that will be used here. The range is from 1 to 4094.
Unit	Select the Switch unit that will be used for this configuration here. This option is only available if stacking is enabled.
From Port - To Port	Select the range of ports that will be used for this configuration here. Select the **All** option to use all the ports in this configuration.
Frame Type	Select the frame type here. Options to choose from are: • **Broadcast** - Specifies to count only broadcast frames. • **Multicast** - Specifies to count only multicast frames. • **Unicast** - Specifies to count only unicast frames. • **Any** - Specifies to count all frames regardless of the frame type. • **All** - Specifies to count all frames regardless of the frame type.
Traffic Direction	Select the traffic direction here. Options to choose from are: • **RX** - Specifies to count ingress traffic. • **TX** - Specifies to count egress traffic. • **Both** - Specifies to count ingress and egress traffic.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to delete the specified entry based on the information entered/selected.

The fields that can be configured for **VLAN Counter Table** are described below:

Parameter	Description
Interface VLAN	Enter the VLAN ID that will be used here. The range is from 1 to 4094. Select the **All** option to display counter information associated with all VLAN interfaces.
Traffic Direction	Select the traffic direction here. Options to choose from are: • **RX** - Specifies to count ingress traffic. • **TX** - Specifies to count egress traffic. • **Both** - Specifies to count ingress and egress traffic.

Click the **Find** button to display entries in the table based on the information entered/selected.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Utilization

Port Utilization

This window is used to view the port utilization table.

To view the following window, click **Monitoring > Utilization > Port Utilization**, as shown below:

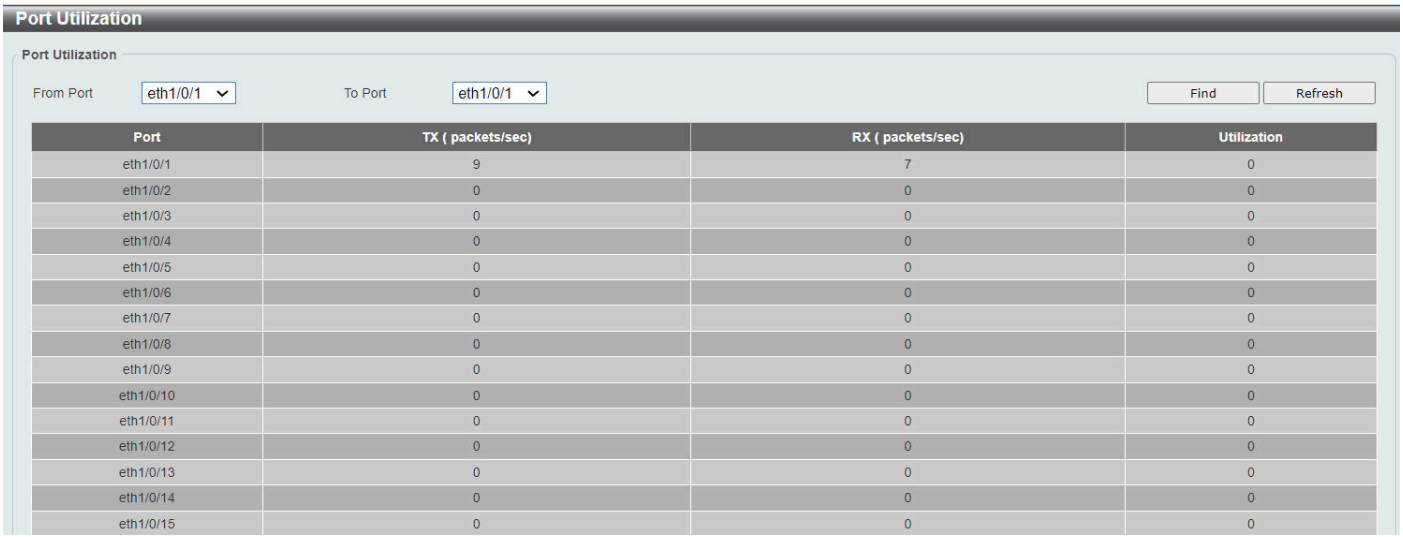


Figure 11-2 Port Utilization Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used here.This option is only available when stacking is enabled.
From Port - To Port	Select the range of ports that will be used here.

Click the **Find** button to display entries in the table based on the information entered/selected.

Click the **Refresh** button to refresh the information displayed in the table.

History Utilization

This window is used to view the memory, CPU and port history utilization.

To view the following window, click **Monitoring > Utilization > History Utilization**, as shown below:

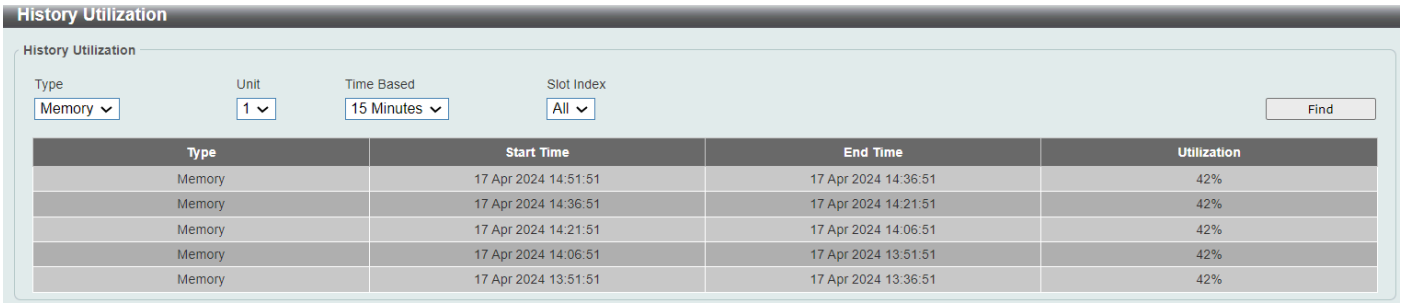


Figure 11-3 History Utilization (Memory) Window

After selecting **CPU** as the **Type**, the following window will appear:

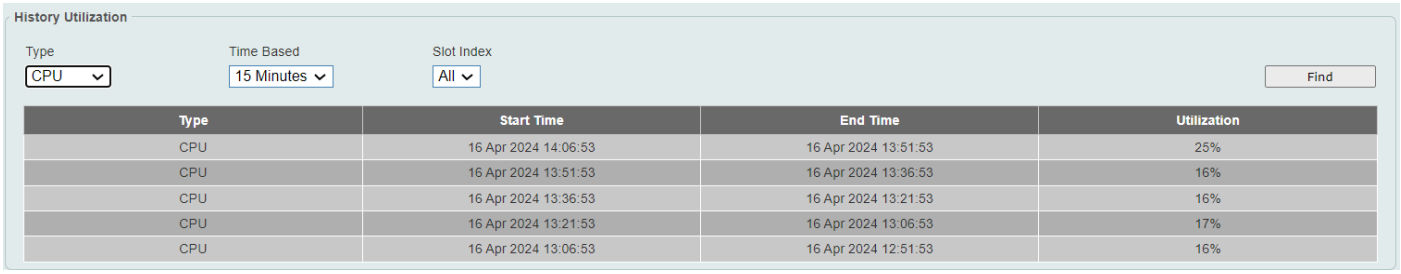


Figure 11-4 History Utilization (CPU) Window

After selecting **Port** as the **Type**, the following window will appear:

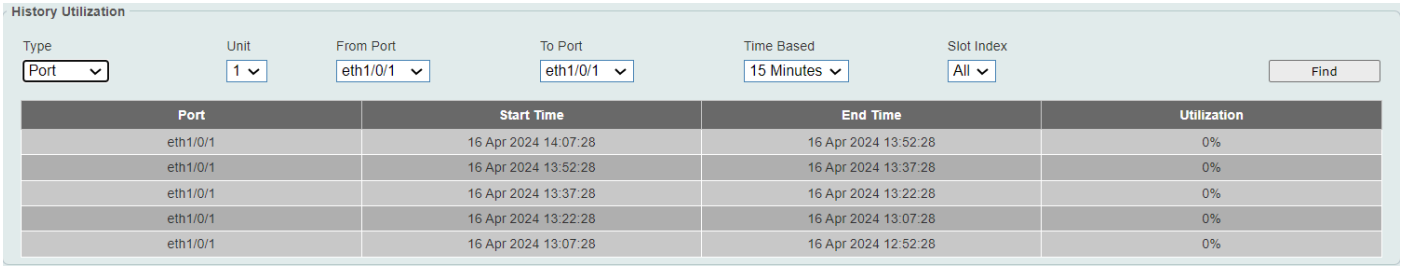


Figure 11-5 History Utilization (Port) Window

The fields that can be configured are described below:

Parameter	Description
Type	Select the history utilization type to display here. Options to choose from are: • **Memory** - Specifies to display the historical memory utilization information. • **Port -** Specifies to display the historical port utilization information. • **CPU -** Specifies to display the historical CPU utilization information.
Unit	Select the Switch unit that will be used here. This option is only available if stacking is enabled.
From Port - To Port	Select the range of ports that will be used here.
Time Based	Select the time-based statistical count value here. Options to choose from are: • **15 Minutes** - Specifies to display 15-minute based statistics count. • **1 Day** - Specifies to display daily based statistics count. For 15-minute based statistics, slot 1 represents the time from 15 minutes ago until now, slot 2 represents the time from 30 minutes ago until 15 minutes ago and so on. For 1-day based statistics, slot 1 represents the time from 24 hours ago until now and slot 2 represents the time from 48 hours ago until 24 hours ago.
Slot Index	Select the slot index here. Options to choose from are **All**, and **1** to **5**. Select the slot index here. Options to choose from are **1** to **5** for the above **15-minute** time base and **1** to **2** for the above **1-day** time base.

Click the **Find** button to display entries in the table based on the information selected.

Statistics

Port

This window is used to view the port statistics information.

To view the following window, click **Monitoring > Statistics > Port**, as shown below:

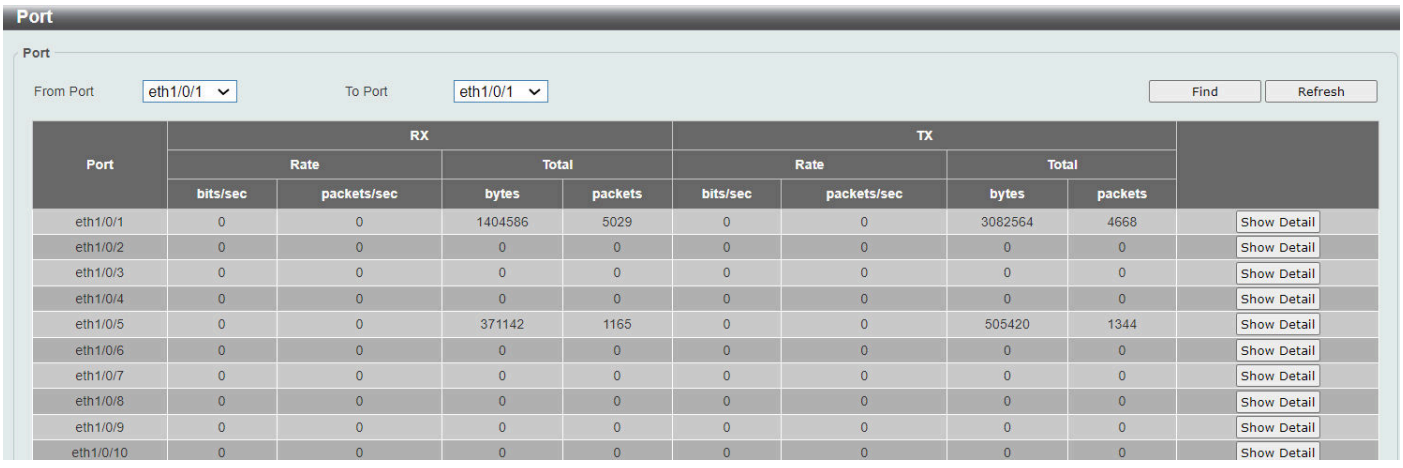


Figure 11-6 Port Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used in this display here. This option is only available if stacking is enabled.
From Port - To Port	Select the range of ports that will be used in this display here.

Click the **Find** button to display entries in the table based on the information selected.

Click the **Refresh** button to refresh the information displayed in the table.

Click the **Show Detail** button to view more detailed statistics information on the specified port.

After clicking the **Show Detail** button, the following window will appear:

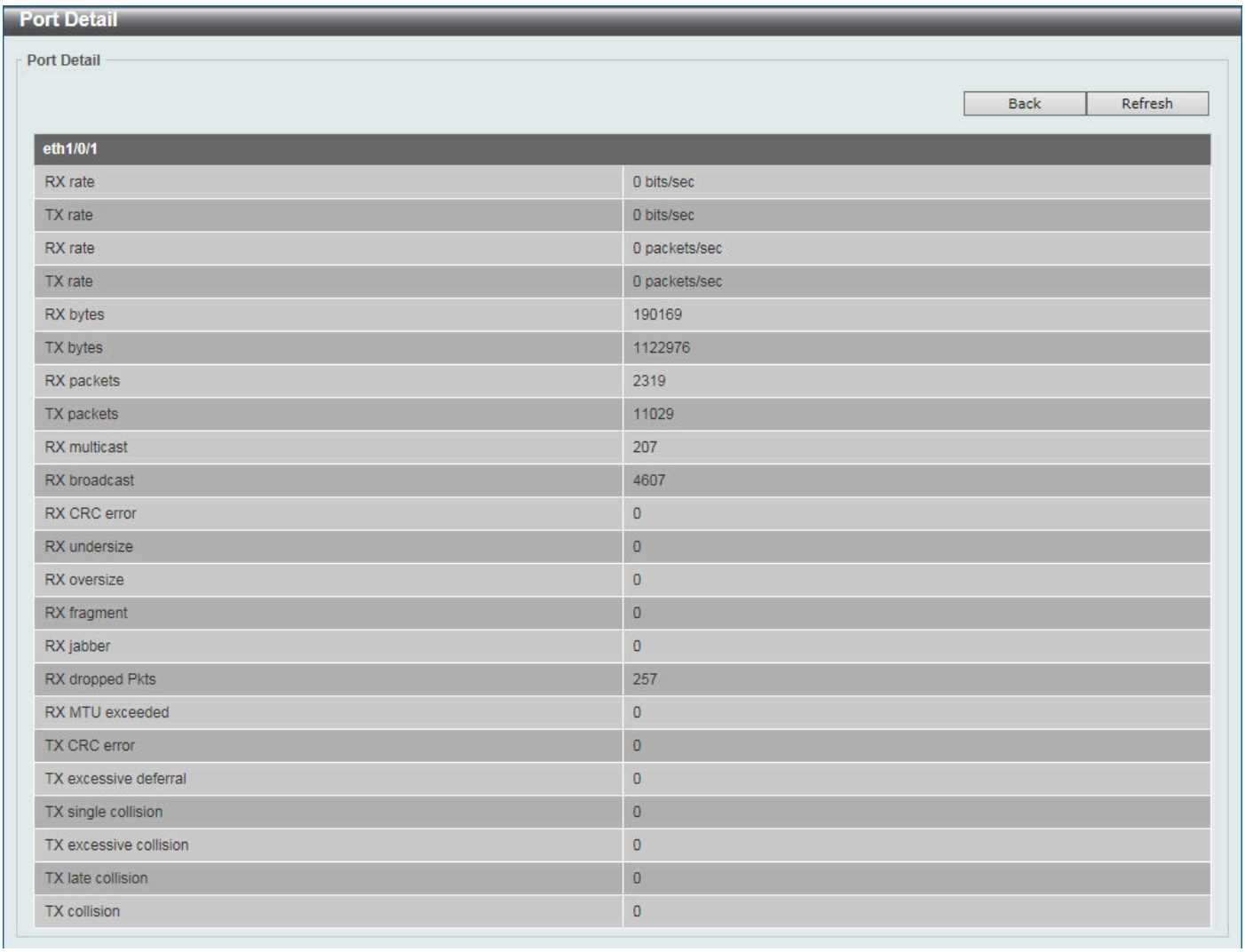


Figure 11-7 Port (Show Detail) Window

Click the **Back** button to return to the previous window.

Click the **Refresh** button to refresh the information displayed in the table.

CPU Port

This window is used to view the CPU statistics information.

To view the following window, click **Monitoring > Statistics > CPU Port**, as shown below:

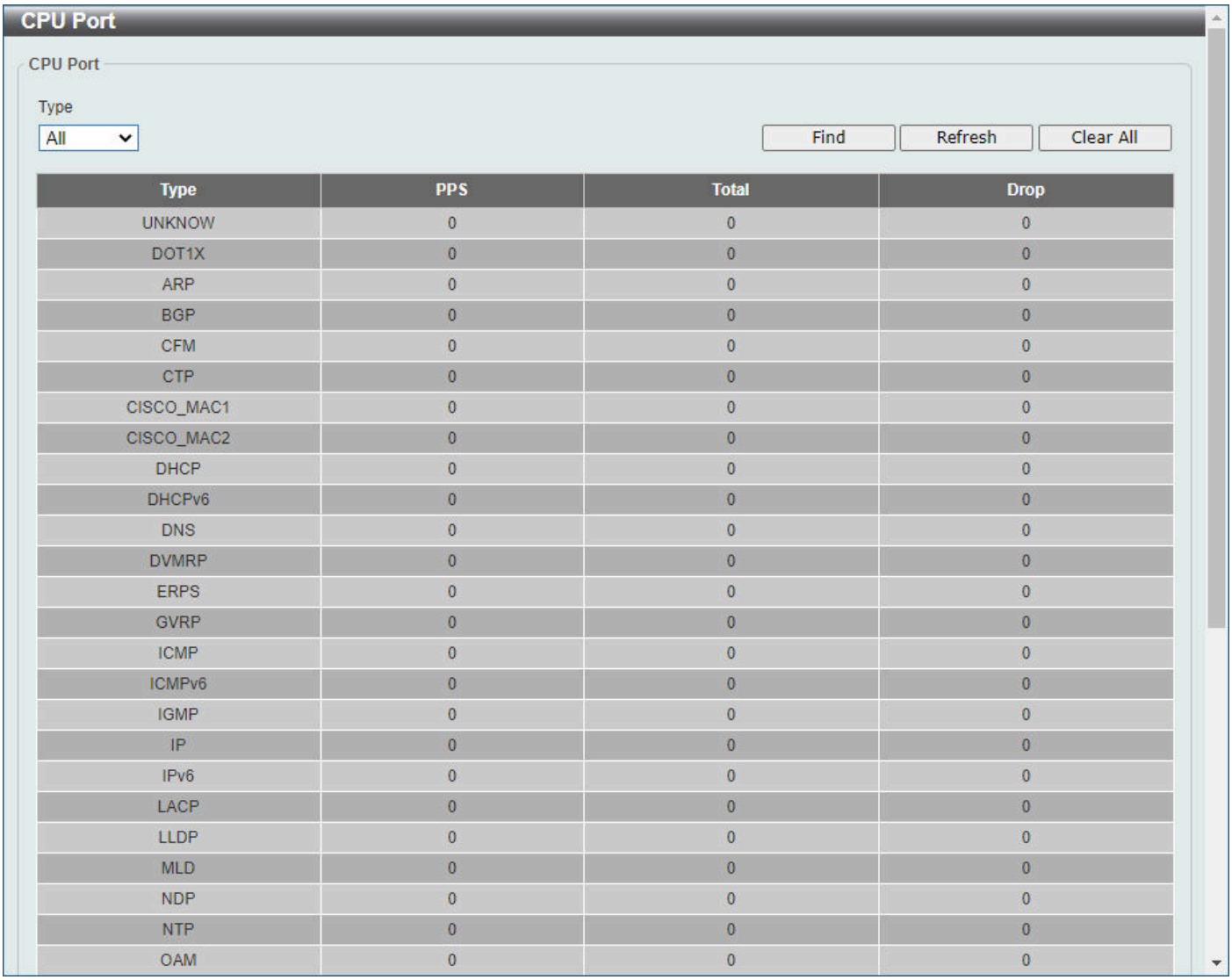


Figure 11-8 CPU Port Window

The fields that can be configured are described below:

Parameter	Description
Type	Select the type of information to display here. Options to choose from are **All**, Layer 2 (**L2**), Layer 3 (**L3**), and **Protocol**.
Routing	Select the type of packet if L3 is selected above: All, Unicast or Multicast. Enter the protocol name if Protocol is selected above.

Click the **Find** button to display entries in the table based on the information selected.

Click the **Refresh** button to refresh the information displayed in the table.

Click the **Clear All** button to clear all the statistics information displayed in the table.

Interface Counters

This window is used to view the interface counter information.

To view the following window, click **Monitoring > Statistics > Interface Counters**, as shown below:

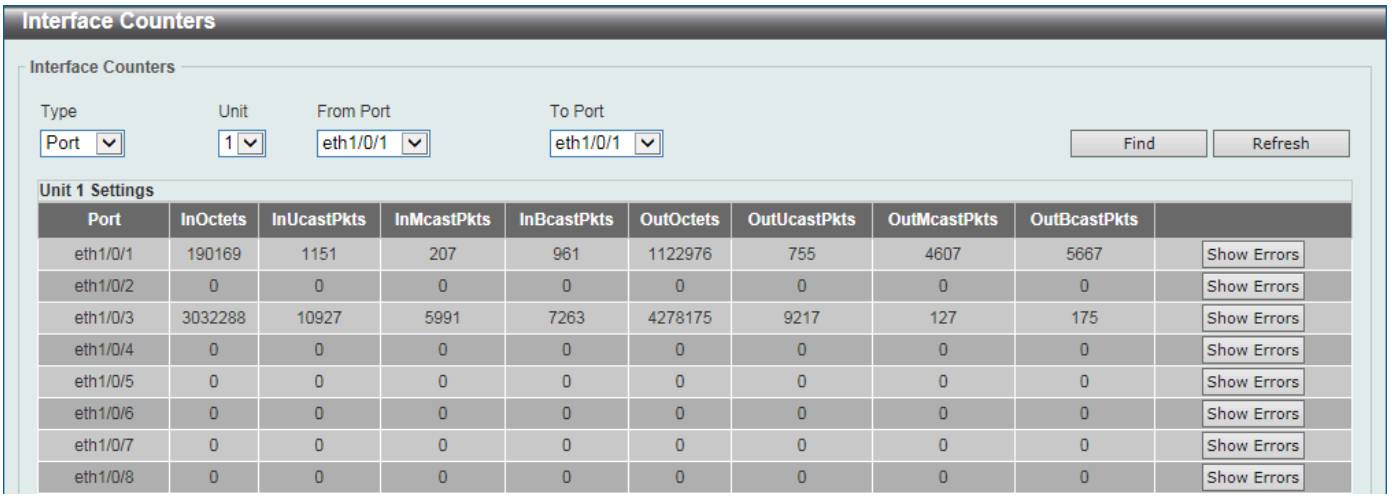


Figure 11-9 Interface Counters (Port) Window

The fields that can be configured are described below:

Parameter	Description
Type	Select the type of information to display here. Options include **Port** and **VLAN**.
Interface VLAN	Enter the VLAN ID (1-4094) if VLAN is selected for type.
Unit	Select the Switc/h unit that will be used in this display here. This option is only available if stacking is enabled.
From Port - To Port	Select the range of ports that will be used in this display here. Enter the port range here is Port is selected for type.

Click the **Find** button to display entries in the table based on the information selected.

Click the **Refresh** button to refresh the information displayed in the table.

Click the **Show Errors** button to view more detailed error information on the specified port.

After clicking the **Show Errors** button, the following window will appear:

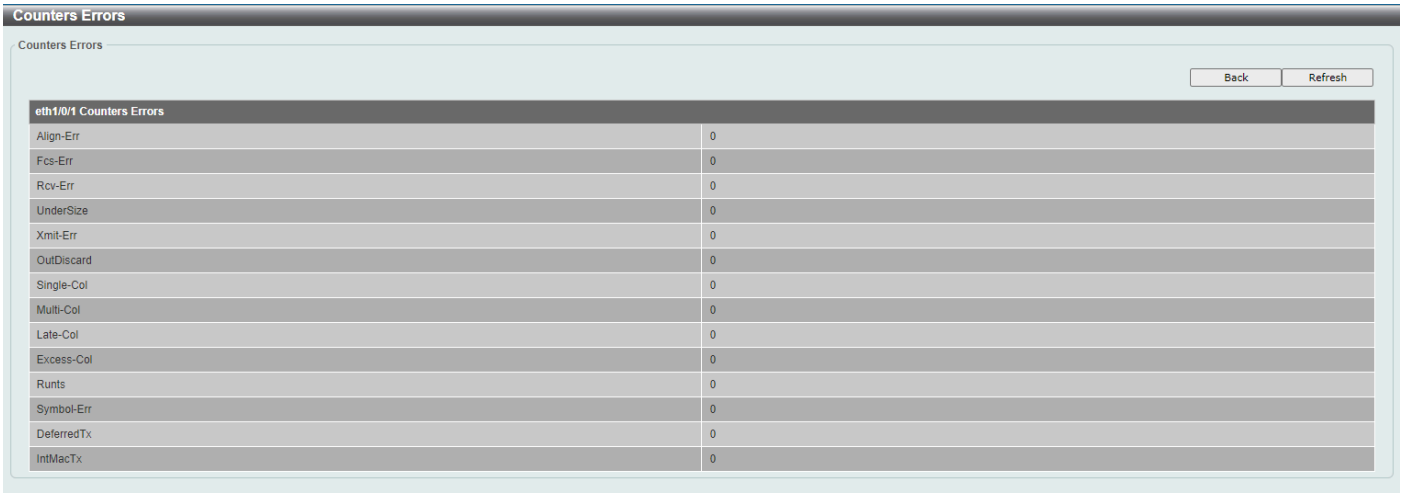


Figure 11-10 Interface Counters (Show Errors) Window

Click the **Back** button to return to the previous window.

Click the **Refresh** button to refresh the information displayed in the table.

After selecting **VLAN** as the **Type**, the following window will appear:

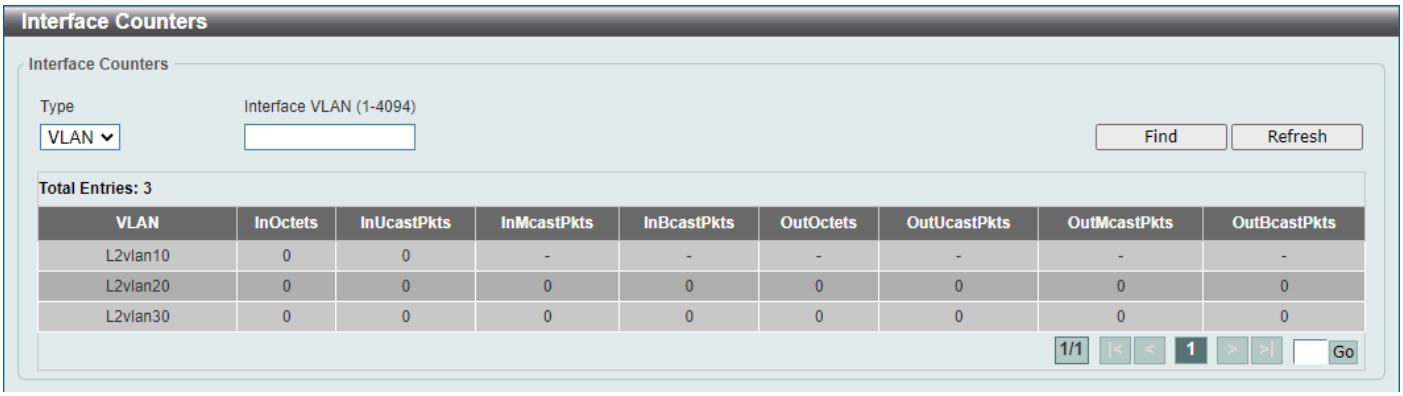


Figure 11-11 Interface Counters (VLAN) Window

Click the **Refresh** button to refresh the counter information displayed in the table.

Interface History Counters

This window is used to view the history counter information per interface.

To view the following window, click **Monitoring > Statistics > Interface History Counters**, as shown below:

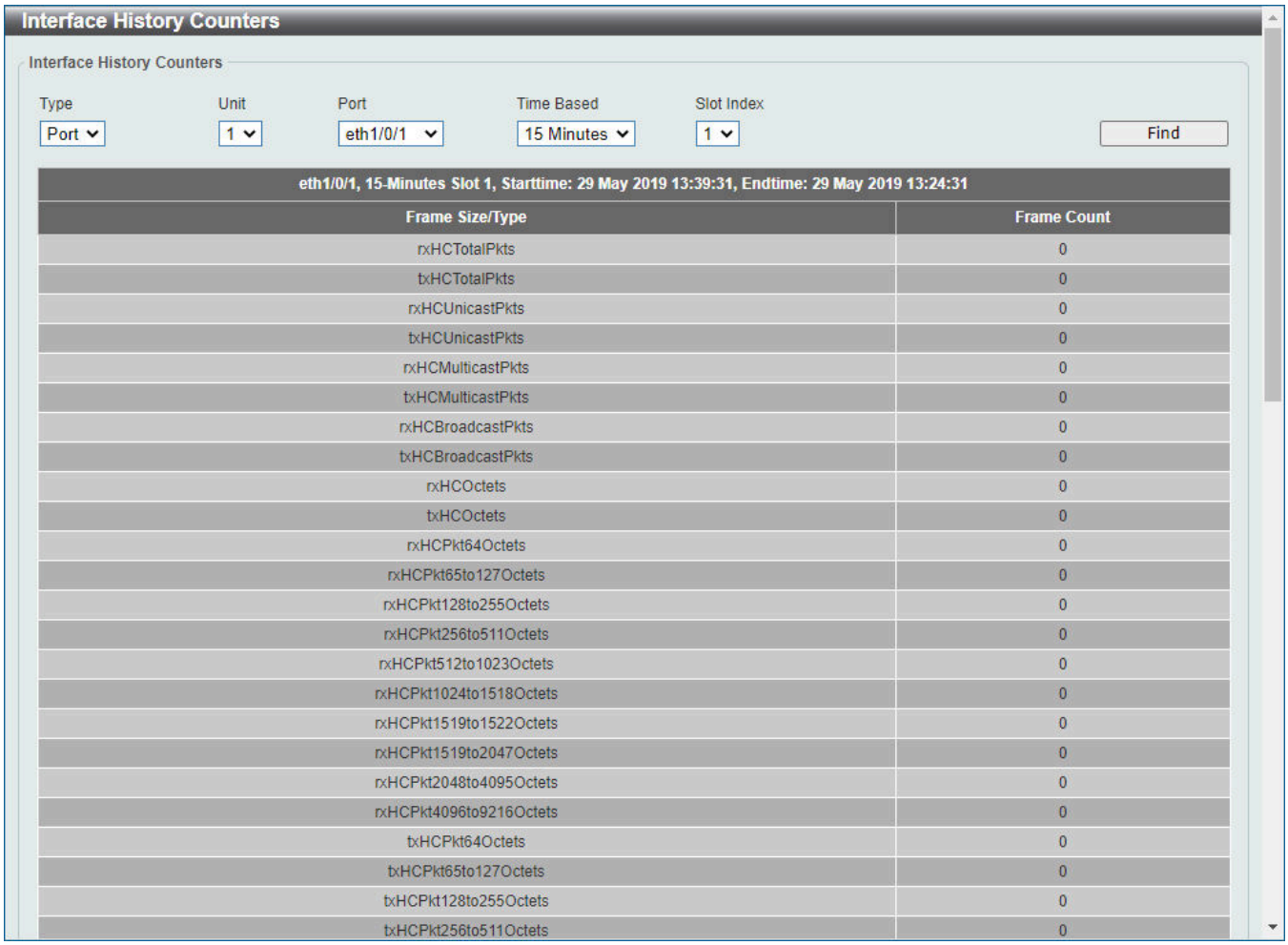


Figure 11-12 Interface History Counters (Port) Window

The fields that can be configured are described below:

Parameter	Description
Type	Select the type of information to display here.
Unit	Select the Switch unit that will be used in this display here. This option is only available when stacking is enabled.
Port	Select the port that will be used in this display here.
Time Based	Select the time-based statistical count value here. Options to choose from are: • **15 Minutes** - Specifies to display 15-minute based statistics count. • **1 Day** - Specifies to display daily based statistics count. For 15-minute based statistics, slot 1 represents the time from 15 minutes ago until now, slot 2 represents the time from 30 minutes ago until 15 minutes ago and so on. For 1-day based statistics, slot 1 represents the time from 24 hours

Parameter	Description
	ago until now and slot 2 represents the time from 48 hours ago until 24 hours ago.
Slot index	Select the slot index here. Options to choose from are **1** to **5** for the above **15-minute** time base and **1** to **2** for the above **1-day** time base.

Click the **Find** button to display entries in the table based on the information selected/entered

Counters

This window is used to view and clear counter information.

To view the following window, click **Monitoring > Statistics > Counters**, as shown below:



Figure 11-13 Counters (Port) Window

The fields that can be configured are described below:

Parameter	Description
Type	Select the type of information to display here. Options supports **Port** and **VLAN**.
Interface VLAN	Enter the VLAN ID (1-4094) if VLAN is selected for type.
Unit	Select the Switch unit that will be used in this display here. This option is only available if stacking is enabled.
From Port - To Port	Select the range of ports that will be used in this display here if Port is selected for type.

Click the **Find** button to display entries in the table based on the information selected.

Click the **Refresh** button to refresh the counter information displayed in the table.

Click the **Clear** button to clear the counter information displayed in the table based on the information selected.

Click the **Clear All** button to clear all the counter information displayed in the table.

Click the **Show Detail** button to view more detailed counter information on the specified port.

After clicking the **Show Detail** button, the following window will appear:

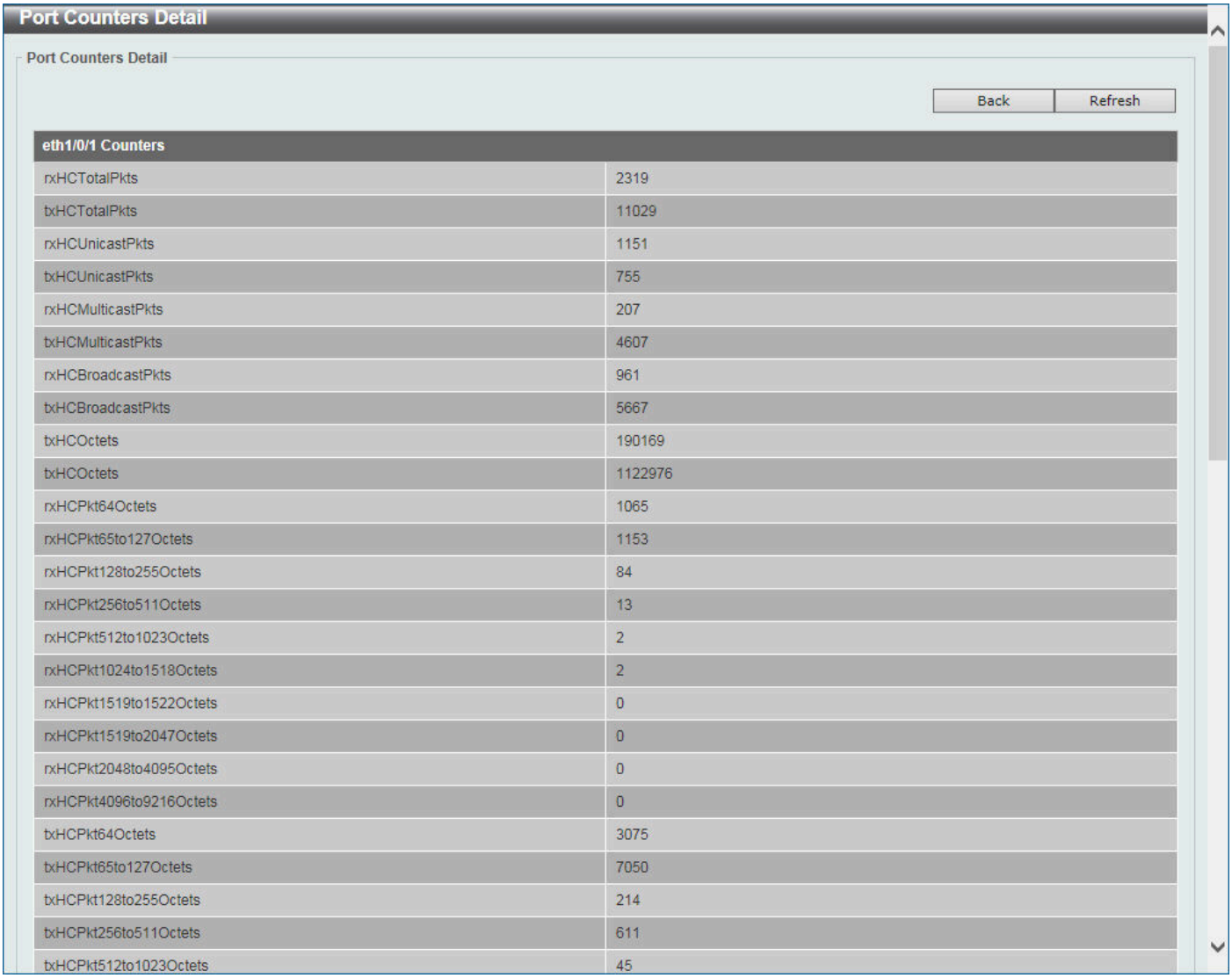


Figure 11-14 Counters (Show Detail) Window

After selecting **VLAN** as the **Type**, the following window will appear:

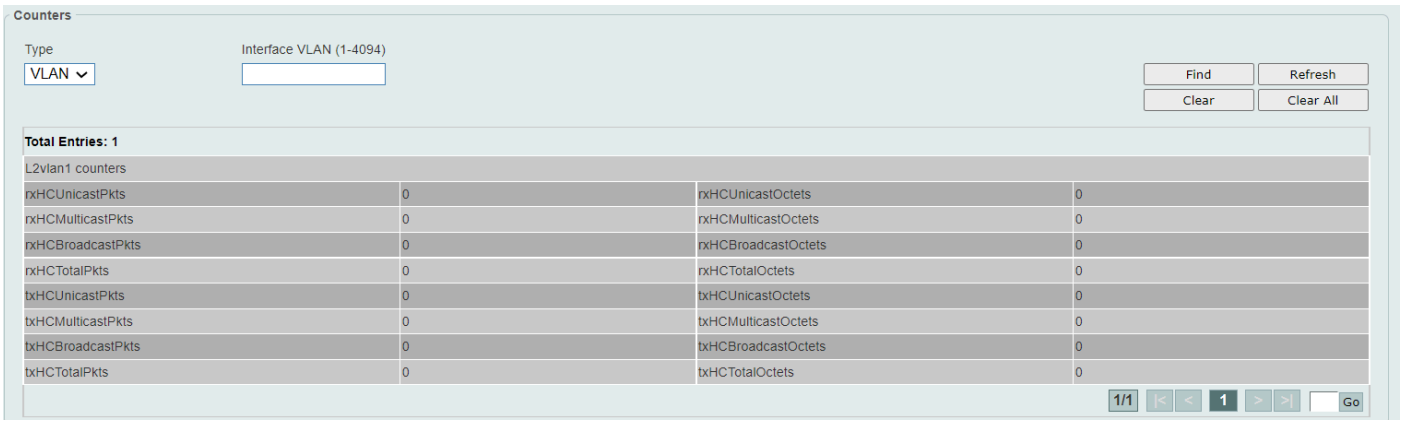


Figure 11-15 Interface Counters (VLAN) Window

Click the **Find** button to display entries in the table based on the information selected.

Click the **Refresh** button to refresh the counter information displayed in the table.

Click the **Clear** button to clear the counter information displayed in the table based on the information selected.

Click the **Clear All** button to clear all the counter information displayed in the table.

Mirror Settings

This window is used to display and configure the mirror feature's settings. The Switch allows users to copy frames transmitted and received on a port and redirect the copies to another port. Attach a monitoring device to the mirroring port, such as a sniffer or an RMON probe, to view details about the packets passing through the first port. This is useful for network monitoring and troubleshooting purposes.

To view the following window, click **Monitoring > Mirror Settings**, as shown below:

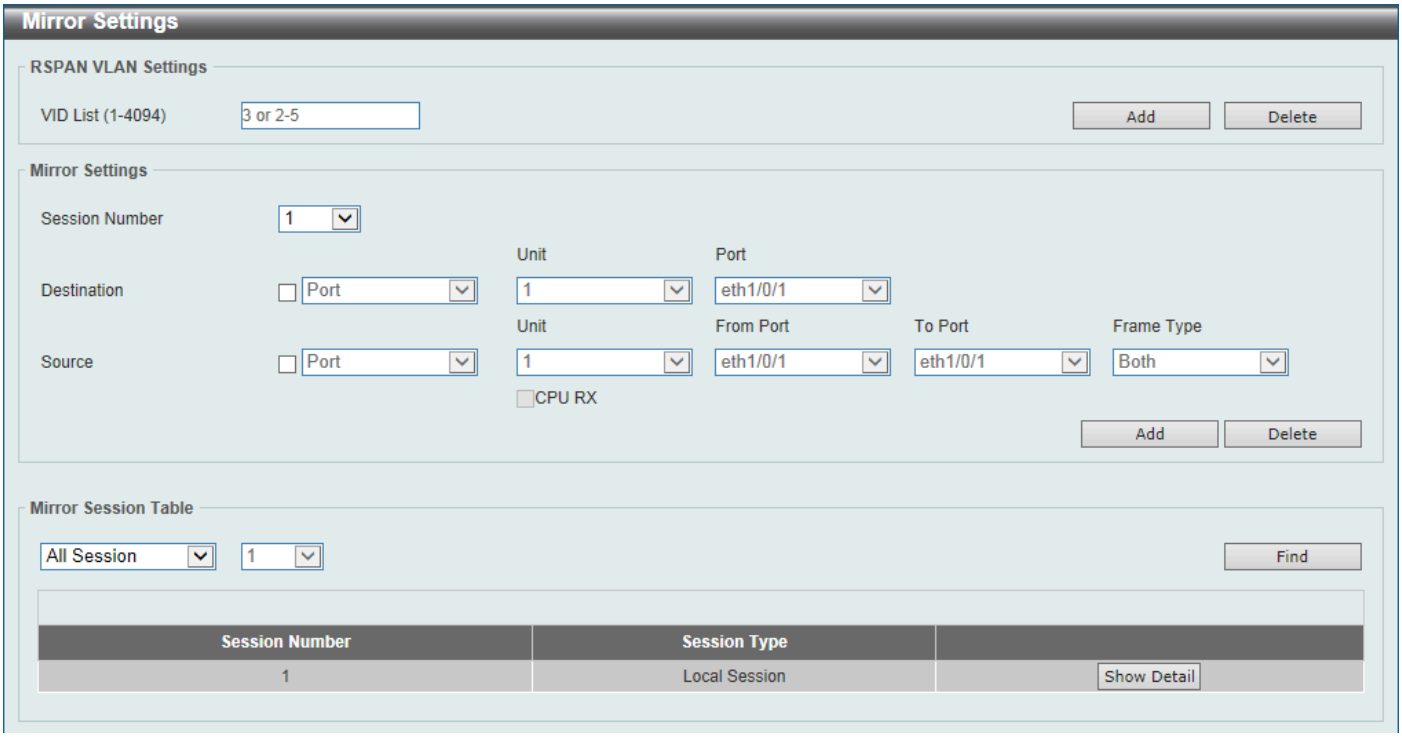


Figure 11-16 Mirror Settings Window

The fields that can be configured for **RSPAN VLAN Settings** are described below:

Parameter	Description
VID List	Enter the VLAN list ID(s) that will be associated with this configuration here.

Click the **Add** button to add the VLAN(s) to the configuration.

Click the **Delete** button to delete the VLAN(s) from the configuration.

The fields that can be configured for **Mirror Settings** are described below:

Parameter	Description
Session Number	Select the mirror session number for this entry here. This number is between 1 and 4.
Destination	Tick the checkbox, next to the **Destination** option, to configure the destination for this port mirror entry. In the first drop-down menu select the destination type option. Options to choose from are **Port**, **Remote VLAN**, and **Replace**. • **Port** - After selecting this option, select the Switch **Unit** ID and destination **Port** number from the drop-down menus.

Parameter	Description
	• **Remote VLAN** - After selecting this option, select the Switch **Unit** ID and destination **Port** number from the drop-down menus and enter the **VID** in the space provided. The VID must be between 2 and 4094. • **Replace** - After selecting this option, enter the **ACL Access List** name and **VID** (VLAN ID) in the spaces provided.
Source	Tick the checkbox, next to the **Source** option, to configure the source for this port mirror entry. In the first drop-down menu select the source type option. Options to choose from are **Port**, **ACL**, **VLAN**, and **Remote VLAN**. • **Port** - After selecting this option, select the Switch **Unit** ID, **From Port** and **To Port** numbers from the drop-down menus. Lastly select the **Frame Type** option from the last drop-down menu. Options to choose from are **Both**, **RX**, **TX**, and **TX Forwarding**. When selecting **Both**, traffic in both the incoming and outgoing directions will be mirrored. When selecting **RX**, traffic in only the incoming direction will be mirrored. When selecting **TX**, traffic in only the outgoing direction will be mirrored. Select the **CPU RX** option to also monitor CPU RX traffic. • **ACL** - After selecting this option, enter the **ACL Name** in the space provided. • **VLAN** - After selecting this option, enter the **VID List** in the space provided and select the **Frame Type** from the drop-down menu. • **Remote VLAN** - After selecting this option, enter the **VID** in the space provided. The VID must be between 2 and 4094.

Click the **Add** button to add the newly configured mirror entry based on the information entered.

Click the **Delete** button to delete an existing mirror entry based on the information entered.

The fields that can be configured for **Mirror Session Table** are described below:

Parameter	Description
Mirror Session Type	Select the mirror session type of information that will be displayed from the drop-down menu. 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 second drop-down menu. This number is from 1 to 4.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show Detail** button to view more detailed information about the mirror session.

After clicking the **Show Detail** button, the following window will appear:

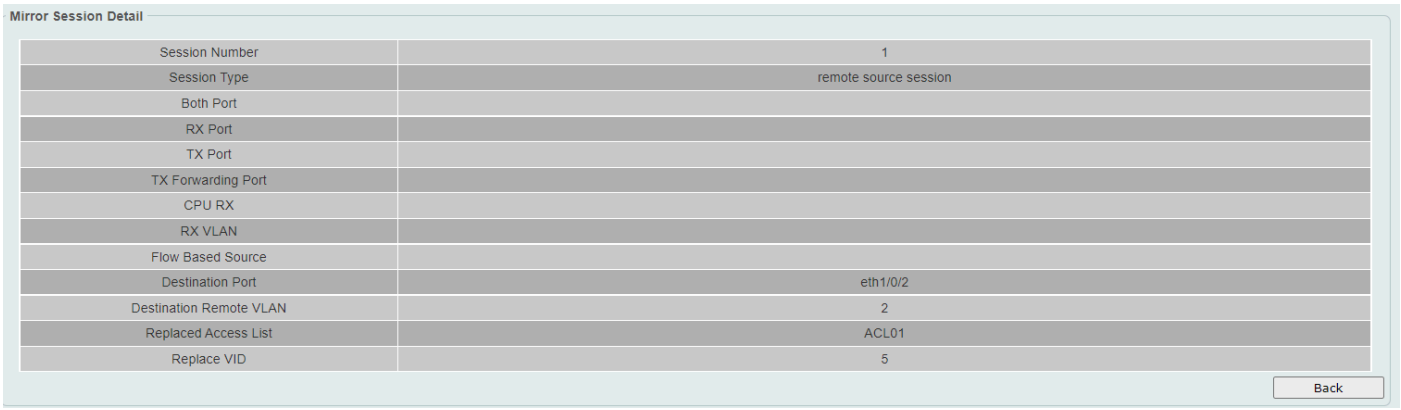


Figure 11-17 Mirror Settings (Show Detail) Window

Click the **Back** button to return to the previous page.

sFlow

sFlow Agent Info-rmation

This window is used to configure and view the sFlow agent (sampled flow agent) information for advanced network monitoring based on collected statistic samples.

To view the following window, click **Monitoring > sFlow > sFlow Agent Information**, as shown below:

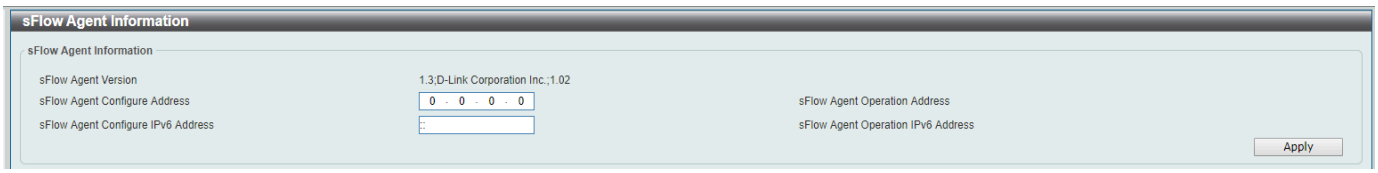


Figure 11-18 sFlow Agent Information Window

The fields that can be configured are described below:

Parameter	Description
sFlow Agent Configure Address	Enter the sFlow agent IPv4 address.
sFlow Agent Configure IPv6 Address	Enter the sFlow agent IPv6 address

sFlow Receiver Settings

This window is used to display and configure receivers for the sFlow agents. Receivers cannot be added to or removed from the sFlow agent.

To view the following window, click **Monitoring > sFlow > sFlow Receiver Settings**, as shown below:

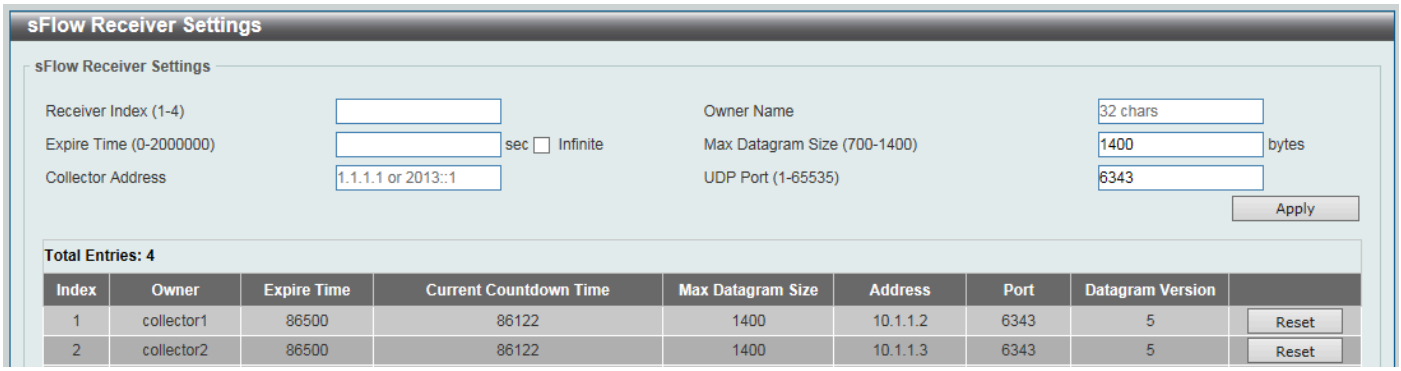


Figure 11-19 sFlow Receiver Settings Window

The fields that can be configured are described below:

Parameter	Description
Receiver Index	Enter the index number of the receiver here. This number must be between 1 and 4.
Owner Name	Enter the owner name of the receiver here. This name can be up to 32 characters long.
Expire Time	Enter the expiration time for the entry here. The parameters of the entry will reset when the timer expired. The range is from 1 to 2000000 seconds. Selecting **Infinite** specifies that the entry will not expire.
Max Datagram Size	Enter the maximum number of data bytes of a single sFlow datagram here. The range is from 700 to 1400 bytes. By default, this value is 1400 bytes.
Collector Address	Enter the remote sFlow collector's IPv4 or IPv6 address here.
UDP Port	Enter the remote sFlow collector's UDP port number here. This number must be between 1 and 65535. By default, this value is 6343.

Click the **Apply** button to accept the changes made.

Click the **Reset** button to reset the specified entry's settings to the default settings.

sFlow Sampler Settings

This window is used to display and configure the sFlow sampler settings.

To view the following window, click **Monitoring > sFlow > sFlow Sampler Settings**, as shown below:

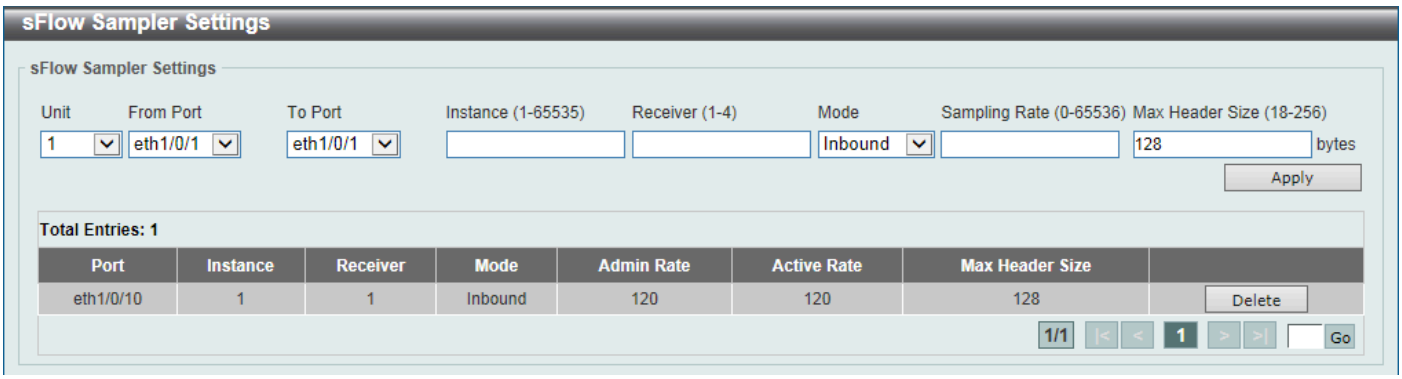


Figure 11-20 sFlow Sampler Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
Instance	Enter the instance index number if multiple samplers are associated with one interface. The valid range is from 1 to 65535.
Receiver	Enter the receiver index for this sampler. If not specified, the value is 0. This value must be between 1 and 4.
Mode	Select the mode here. Options to choose from are **Inbound** and **Outbound**. • Selecting **Inbound** specifies to sample ingress packets. This is the default direction of a sampler. • Selecting **Outbound** specifies to sample egress packets.
Sampling Rate	Enter packet sampling rate for packets. This value must be between 0 and 65536. Entering 0 will disable this function. If not specified, the default value is 0.
Max Header Size	Enter the maximum number of bytes that should be copied from sampled packets. This value must be between 18 and 256 bytes. By default, this value is 128 bytes.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

sFlow Poller Settings

This window is used to display and configure the sFlow poller settings.

To view the following window, click **Monitoring > sFlow > sFlow Poller Settings**, as shown below:



Figure 11-21 sFlow Poller Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
Instance	Enter the instance index number if multiple samplers are associated with one interface. The valid range is from 1 to 65535.

Parameter	Description
Receiver	Enter the receiver index value for this poller here. This value must be between 1 and 4.
Interval	Enter the maximum number of seconds between successive polling samples. This value must be between 0 and 120 seconds. Entering 0 will disable this feature.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Device Environment

The device environment feature displays the Switch internal temperature status and the operation of fan and power modules.

To view the following window, click **Monitoring > Device Environment**, as shown below:

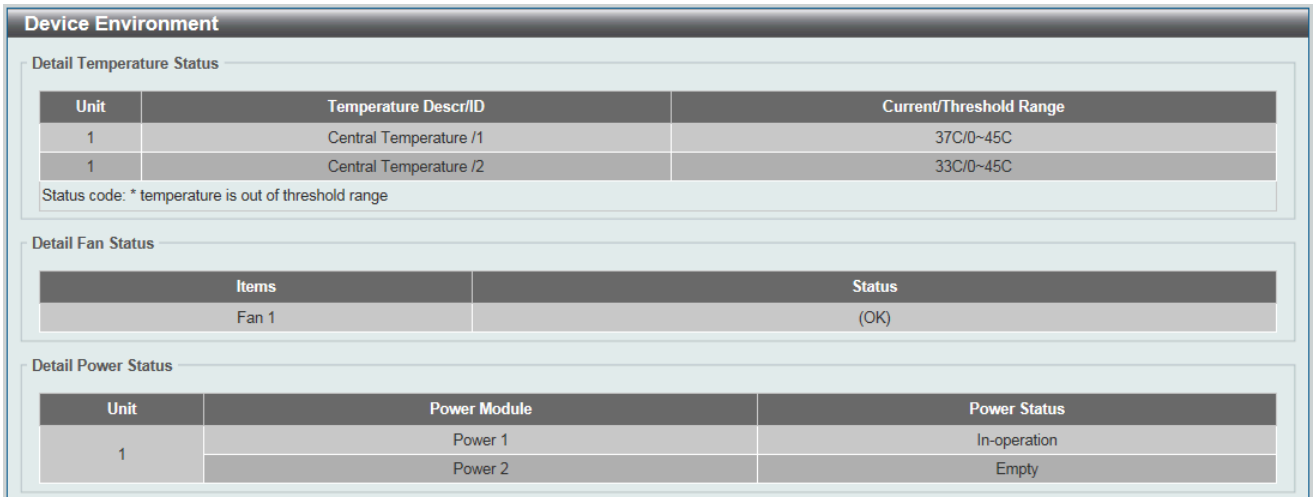


Figure 11-22 Device Environment Window

12. Green

Power Saving
EEE

Power Saving

This window is used to display and configure the power saving settings of the Switch.

To view the following window, click **Green > Power Saving**, as shown below:

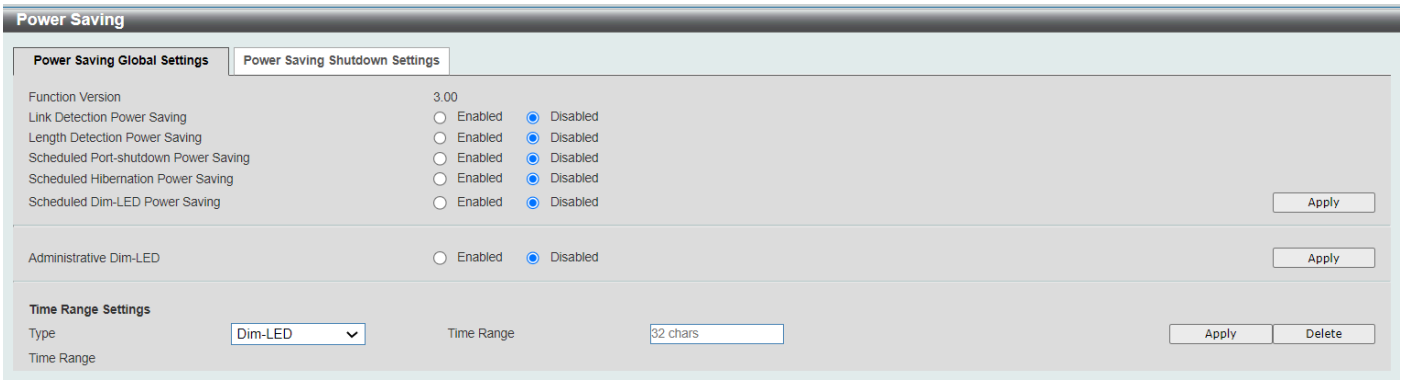


Figure 12-1 Power Saving Global Settings Window

The fields that can be configured in **Power Saving Global Settings** are described below:

Parameter	Description
Link Detection Power Saving	Select this option to enable or disable the link detection state. When enabled, a port which has a link down status will be turned off to save power to the Switch. This will not affect the port's capabilities when the port status is link up. The default is disabled.
Length Detection Power Saving	Select this option to enable or disable the cable length detection power saving feature. This feature will allow the Switch to automatically detect the cable length connected to the port and increase or reduce the required power to this port accordingly to save power. The default is disabled.
Scheduled Port-shutdown Power Saving	Select this option to enable or disable applying the power saving by scheduled port shutdown. Refer to below **Power Saving Shutdown Settings.** The default is disabled.
Scheduled Hibernation Power Saving	Select this option to enable or disable applying the power saving by scheduled hibernation. Refer to below **Time Range Settings**. The default is disabled.
Scheduled Dim-LED Power Saving	Select this option to enable or disable applying the power saving by scheduled dimming LEDs. Refer to below **Time Range Settings**. The default is disabled.
Administrative Dim-LED	Select this option to enable or disable the port LED function. The default is disabled.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Time Range Settings** are described below:

Parameter	Description
Type	Select the power saving type

Parameter	Description
	: Dim-LED or Hibernation.
Time Range	Enter the name of the time range for the power saving type configuration. Refer to **System > Time** Range.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Delete** button to remove the specified entry.

NOTE: The hibernation feature can only be configured when physical stacking is disabled on the Switch.

After clicking the **Power Saving Shutdown Settings** tab, the following page will appear.

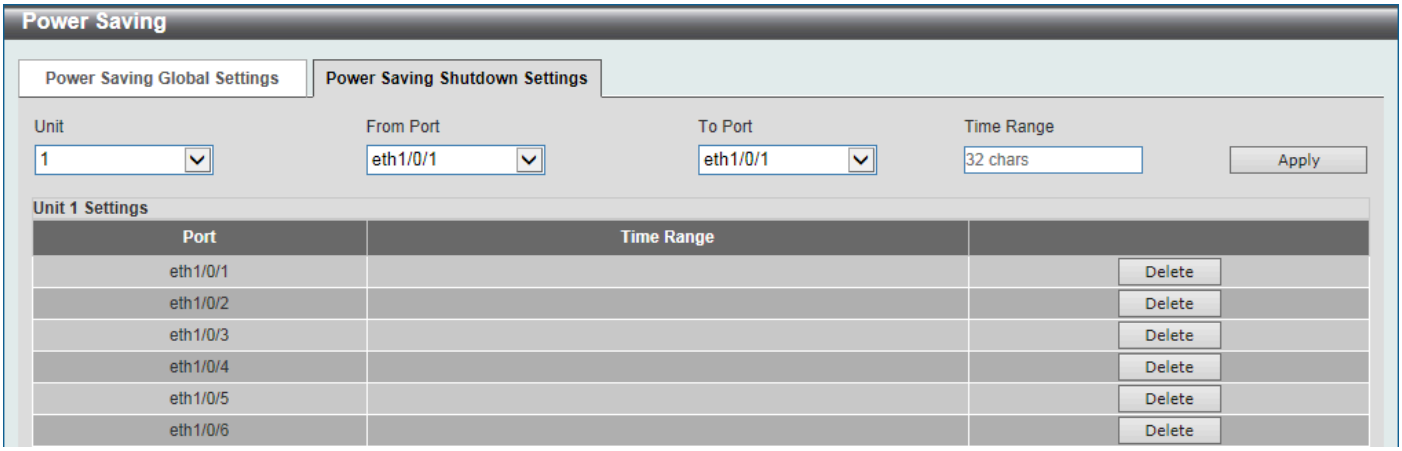


Figure 12-2 Power Saving Shutdown Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available if stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
Time Range	Enter the name of the time range for configuartion. Refer to **System > Time** Range.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

EEE

Energy Efficient Ethernet (EEE) is defined in IEEE 802.3az. It is designed to reduce the energy consumption of a link when no packets are being sent.

To view the following window, click **Green > EEE**, as shown below:

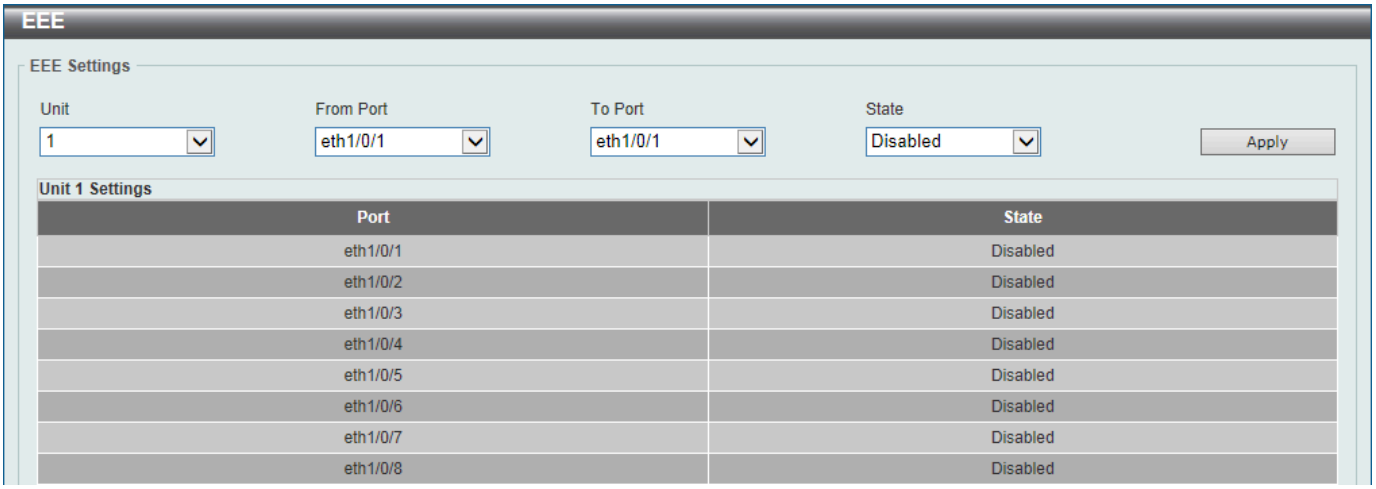


Figure 12-3 EEE Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available if stacking is enabled.
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select this option to enable or disable the state of the EEE feature here.

Click the **Apply** button to accept the changes made.

13. Save and Tools

Save Configuration
Firmware Upgrade & Backup
Configuration Restore & Backup
Log Backup
Ping
Trace Route
Reset
Reboot System

Save Configuration

This window is used to save the running configuration to the start-up configuration. This is to prevent the loss of configuration in the event of a power failure.

To view the following window, click **Save > Save Configuration**, as shown below:

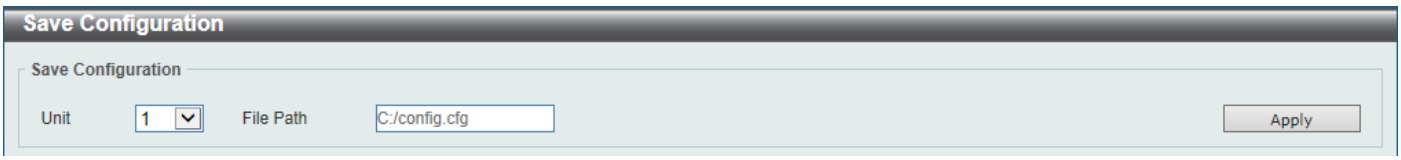


Figure 13-1 Save Configuration Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
File Path	Enter the filename and path in the space provided. If path is not specified, it will be saved in c:/ in the file system.

Click the **Apply** button to save the configuration.

Firmware Upgrade & Backup

Firmware Upgrade from HTTP

This window is used to initiate a firmware upgrade from a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP**, as shown below:

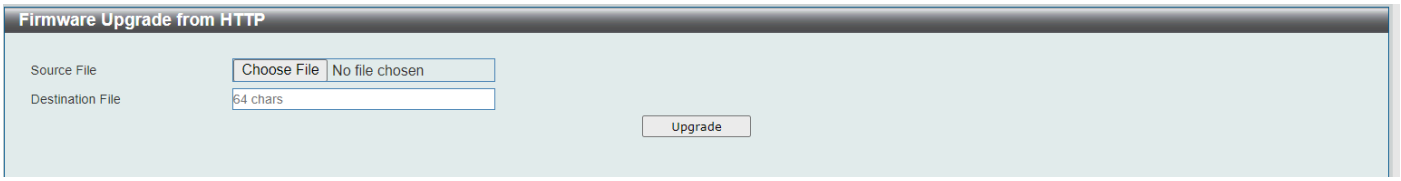


Figure 13-2 Firmware Upgrade from HTTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
Source File	In this field the source firmware file's filename and path will be displayed after selection. To navigate to the location of the firmware file located on the local PC, either double click in the text box or click the **Choose File** button.
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. You can obtain the current directory structure on the Switch in **Management > File System**.

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Upgrade from TFTP

This window is used to initiate a firmware upgrade from a TFTP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from TFTP**, as shown below:

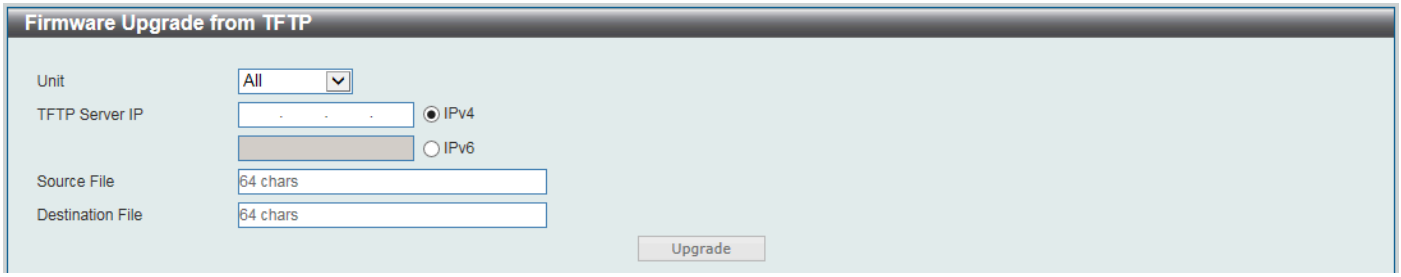


Figure 13-3 Firmware Upgrade from TFTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
TFTP Server IP	Enter the TFTP server IP address here. When select the **IPv4** option, enter the IPv4 address of the TFTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 address of the TFTP server in the space provided.
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. You can obtain the current directory structure on the Switch in **Management > File System**.

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Backup to HTTP

This window is used to initiate a firmware backup to a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to HTTP**, as shown below:

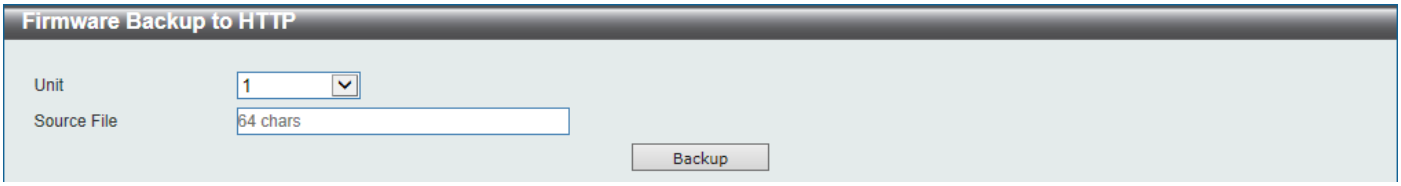


Figure 13-4 Firmware Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
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. For a complete list of firmware files stored on the Switch, go to **Management > File System.**

Click the **Backup** button to initiate the firmware backup.

Firmware Backup to TFTP

This window is used to initiate a firmware backup to a TFTP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to TFTP**, as shown below:

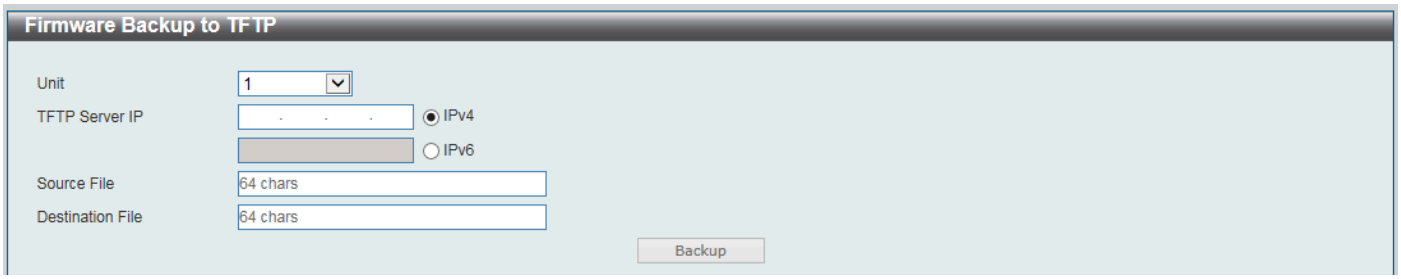


Figure 13-5 Firmware Backup to TFTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here. This option is only available when stacking is enabled.
TFTP Server IP	Enter the TFTP server IP address here. When select the **IPv4** option, enter the IPv4 address of the TFTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 address of the TFTP server in the space provided.
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. For a complete list of firmware files stored on the Switch, go to **Management > File System.**
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 initiate the firmware backup.

Configuration Restore & Backup

Configuration Restore from HTTP

This window is used to initiate a configuration restore from a local PC using HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from HTTP**, as shown below:



Figure 13-6 Configuration Restore from HTTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
Source File	In this field the source configuration file's filename and path will be displayed after selection. To navigate to the location of the configuration file located on the local PC, either double click in the text box or click the **Browse** button.
Destination File	Enter the destination path and location where the configuration file should be stored on the Switch. (You can obtain the current directory structure on the Switch in Management > File System.) This field can be up to 64 characters long. Or select the **running-config** option to restore and overwrite the running configuration file on the Switch or 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 initiate the configuration restore.

Configuration Restore from TFTP

This window is used to initiate a configuration restore from a TFTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from TFTP**, as shown below:

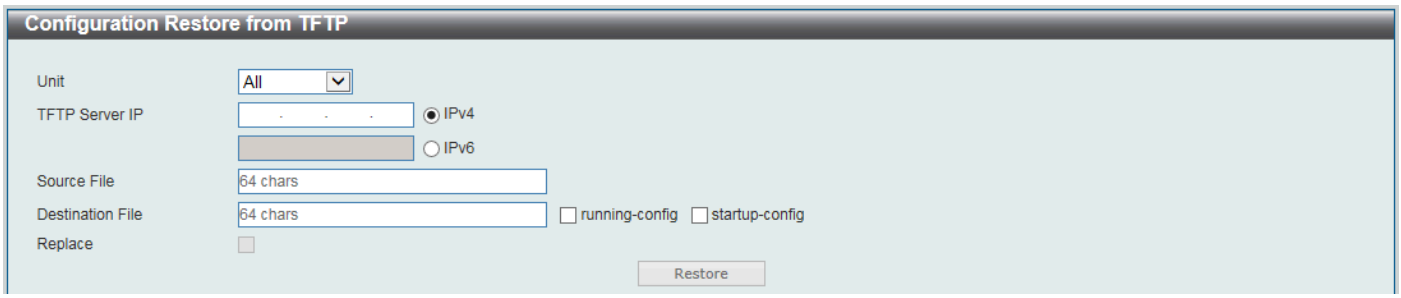


Figure 13-7 Configuration Restore from TFTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
TFTP Server IP	Enter the TFTP server IP address here. When select the **IPv4** option, enter the IPv4 address of the TFTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 address of the TFTP server in the space provided.
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. (You can obtain the current directory structure on the Switch in Management > File System.) This field can be up to 64 characters long. Or select the **running-config** option to restore and overwrite the running configuration file on the Switch or 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 initiate the configuration restore.

Configuration Backup to HTTP

This window is used to initiate a configuration file backup to a local PC using HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to HTTP**, as shown below:

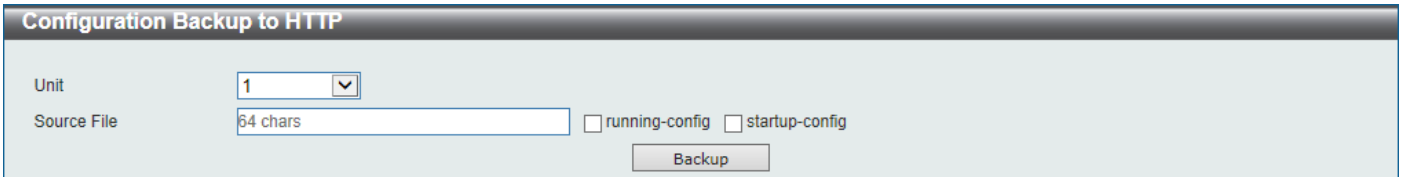


Figure 13-8 Configuration Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
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 or select the **startup-config** option to back up the start-up configuration file from the Switch. For a complete list of firmware files stored on the Switch, go to **Management > File System.**

Click the **Backup** button to initiate the configuration file backup. The file will be downloaded to your browser's default download directory.

Configuration Backup to TFTP

This window is used to initiate a configuration file backup to a TFTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to TFTP**, as shown below:

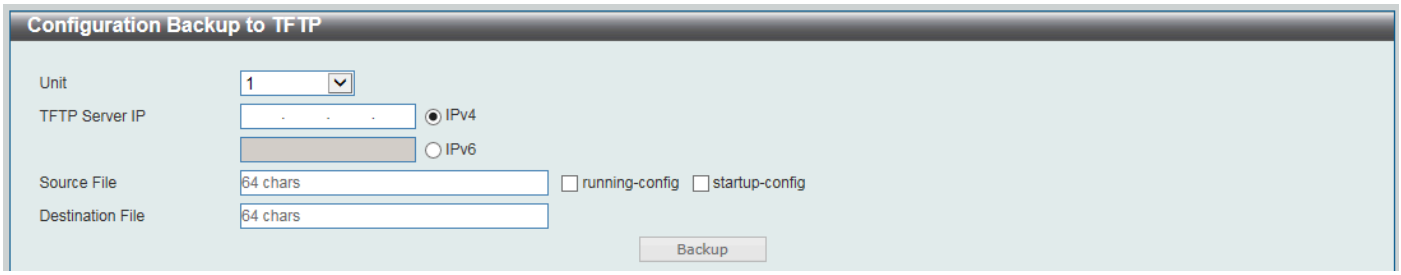


Figure 13-9 Configuration Backup to TFTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
TFTP Server IP	Enter the TFTP server IP address here. When select the **IPv4** option, enter the IPv4 address of the TFTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 address of the TFTP server in the space provided.
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 or select the **startup-config** option to back up the start-up configuration file from the Switch. For a complete list of firmware files stored on the Switch, go to **Management > File System.**
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 initiate the configuration file backup.

Log Backup

Log Backup to HTTP

This window is used to initiate a system log backup to a local PC using HTTP.

To view the following window, click **Tools > Log Backup > Log Backup to HTTP**, as shown below:

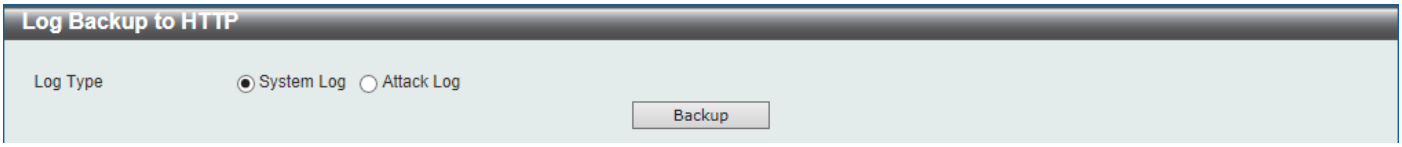


Figure 13-10 Log Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Log Type	Select the log type that will be backed up to the local PC using HTTP. • When the **System Log** option is selected, the system log will be backed up. • When the **Attack Log** is selected, the attack log will be backed up.

Click the **Backup** button to initiate the system log backup. The log file (.log) will be downloaded to your browser's default download directory.

Log Backup to TFTP

This window is used to initiate a system log backup to a TFTP server.

To view the following window, click **Tools > Log Backup > Log Backup to TFTP**, as shown below:

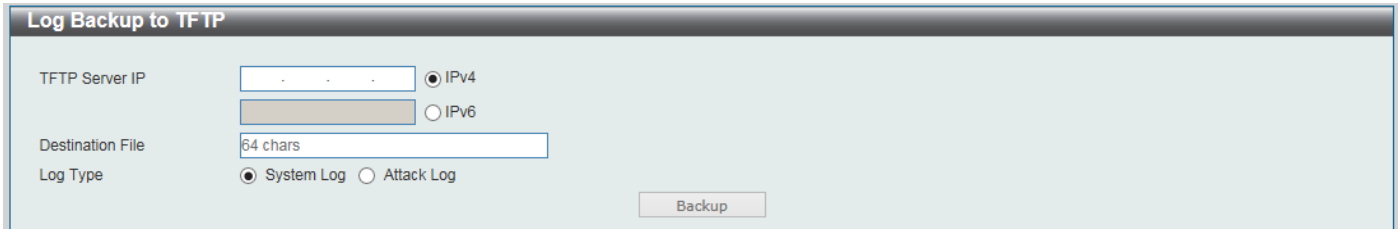


Figure 13-11 Log Backup to TFTP Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server IP address here. When select the **IPv4** option, enter the IPv4 address of the TFTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 address of the TFTP server in the space provided.
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. • When the **System Log** option is selected, the system log will be backed up. • When the **Attack Log** is selected, the attack log will be backed up.

Click the **Backup** button to initiate the system log backup.

Ping

Ping is a small program that sends ICMP Echo packets to the IP address you specify. The destination node then responds to or “echoes” the packets sent from the Switch. This is very useful to verify connectivity between the Switch and other nodes on the network.

To view the following window, click **Tools > Ping**, as shown below:

-

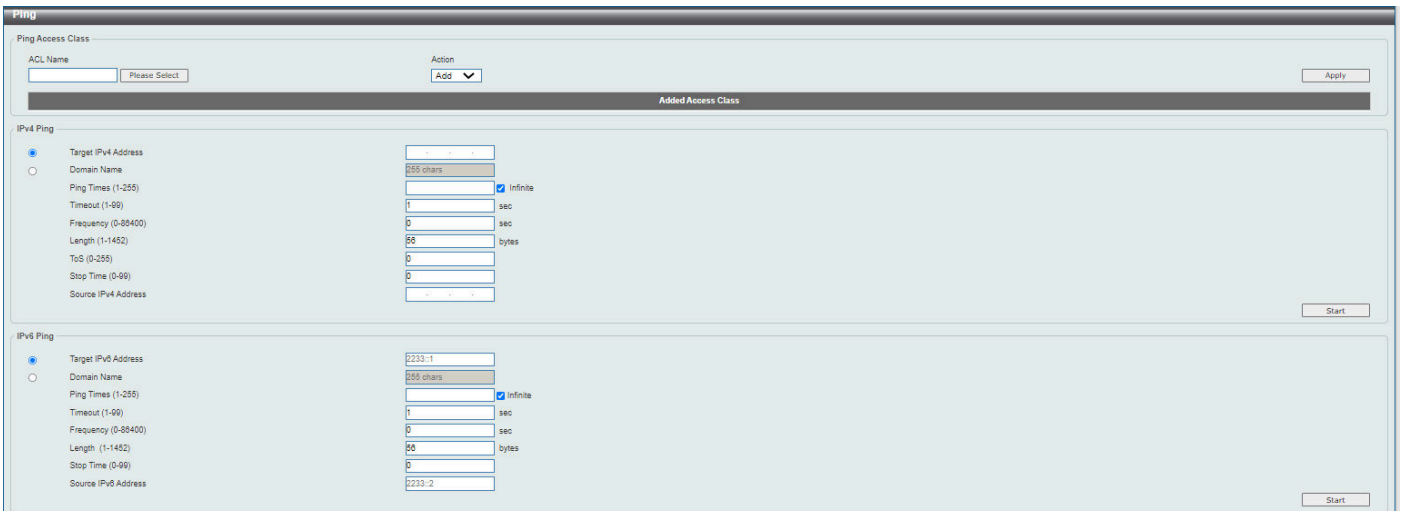


Figure 13-12 Ping Window

The fields that can be configured in **Ping Access Class** are described below:

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 accept the changes made.

The fields that can be configured in **IPv4 Ping** are described below:

Parameter	Description
Target IPv4 Address	Select and enter an IP address to be pinged.
Domain Name	Select and enter the domain name of the system to discover.
Ping Times	Enter the number of times desired to attempt to Ping the IPv4 address configured in this window. Enter number of times between 1 and 255. Tick the Infinite check box to keep sending ICMP Echo packets to the specified IP address until the program is stopped.
Timeout	Select a timeout period between 1 and 99 seconds for this Ping message to reach its destination. If the packet fails to find the IP address in this specified time, the Ping packet will be dropped.
Frequency	Enter the time interval between each Internet Control Message Protocol (ICMP) request. The range is from 0 to 86400 and the default is 0.
Length	Enter the length value here. This specifies the number of data bytes to send. The default value is 56, which translates into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data. It does not include any VLAN or IEEE 802.1Q tag length. The range is from 1 to 1452 bytes.
ToS	Enter the ToS value here. This is used to configure the QoS on ICMP datagrams. The range is from 0 to 255.
Stop Time	Enter the stop time value here. This specifies to stop the ping after the number of times entered here. If this value is configured as 0, then the ping can only be stopped by clicking the **Stop** button manually. The range is from 0 to 99.

Parameter	Description
Source IPv4 Address	Enter the source IPv4 address. If the current Switch has more than one IP address, you can enter one of them to this field. When entered, this IPv4 address will be used as the packets' source IP address sent to the remote host, or as primary IP address.

Click the **Start** button to initiate the Ping Test for each individual section.

The fields that can be configured in **IPv6 Ping** are described below:

Parameter	Description
Target IPv6 Address	Enter an IPv6 address to be pinged.
Domain Name	Select and enter the domain name of the system to discover.
Ping Times	Enter the number of times desired to attempt to Ping the IPv6 address configured in this window. Enter number of times between 1 and 255. Tick the **Infinite** check box to keep sending ICMP Echo packets to the specified IPv6 address until the program is stopped.
Timeout	Select a timeout period between 1 and 99 seconds for this Ping message to reach its destination. If the packet fails to find the IP address in this specified time, the Ping packet will be dropped.
Frequency	Enter the time interval between each Internet Control Message Protocol (ICMP) request. The range is from 0 to 86400 and the default is 0.
Length	Enter the length value here. This specifies the number of data bytes to send. The default value is 56, which translates into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data. It does not include any VLAN or IEEE 802.1Q tag length. The range is from 1 to 1452 bytes.
Stop Time	Enter the stop time value here. This specifies to stop the ping after the number of times entered here. If this value is configured as 0, then the ping can only be stopped by clicking the **Stop** button manually. The range is from 0 to 99.
Source IPv6 Address	Enter the source IPv6 address. If the current Switch has more than one IPv6 address, you can enter one of them to this field. When entered, this IPv6 address will be used as the packets' source IP address sent to the remote host, or as primary IP address.

Click the **Start** button to initiate the Ping Test for each individual section.

After clicking the **Please Select** button, the following window will appear:

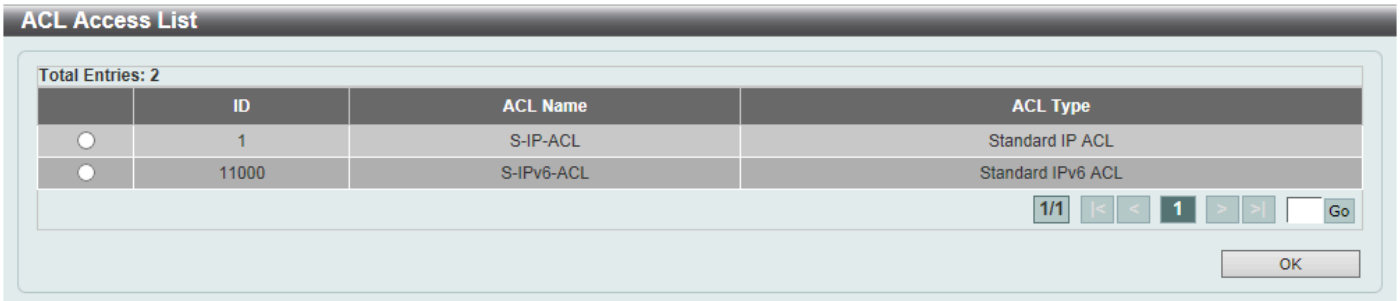


Figure 13-13 Ping (Please Select) Window

Select the radio button next to the entry to use that ACL in the configuration.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **OK** button to accept the selection made.

After clicking the **Start** button in **IPv4 Ping** section, the following **IPv4 Ping Result** section will appear:

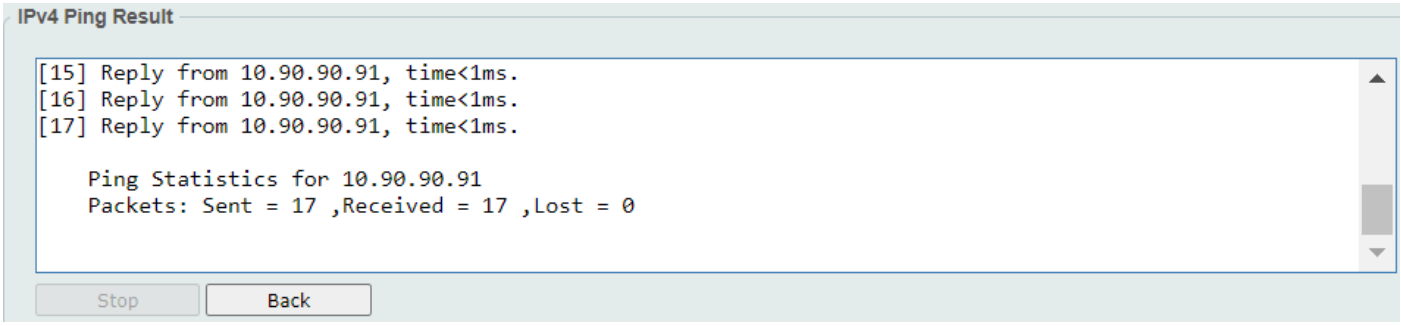


Figure 13-14 Ping (Start) Window

Click the **Stop** button to halt the Ping Test.

Click the **Back** button to return to the IPv4 Ping section.

Trace Route

The trace route page allows the user to trace a route between the Switch and a given host on the network.

To view the following window, click **Tools > Trace Route**, as shown below:

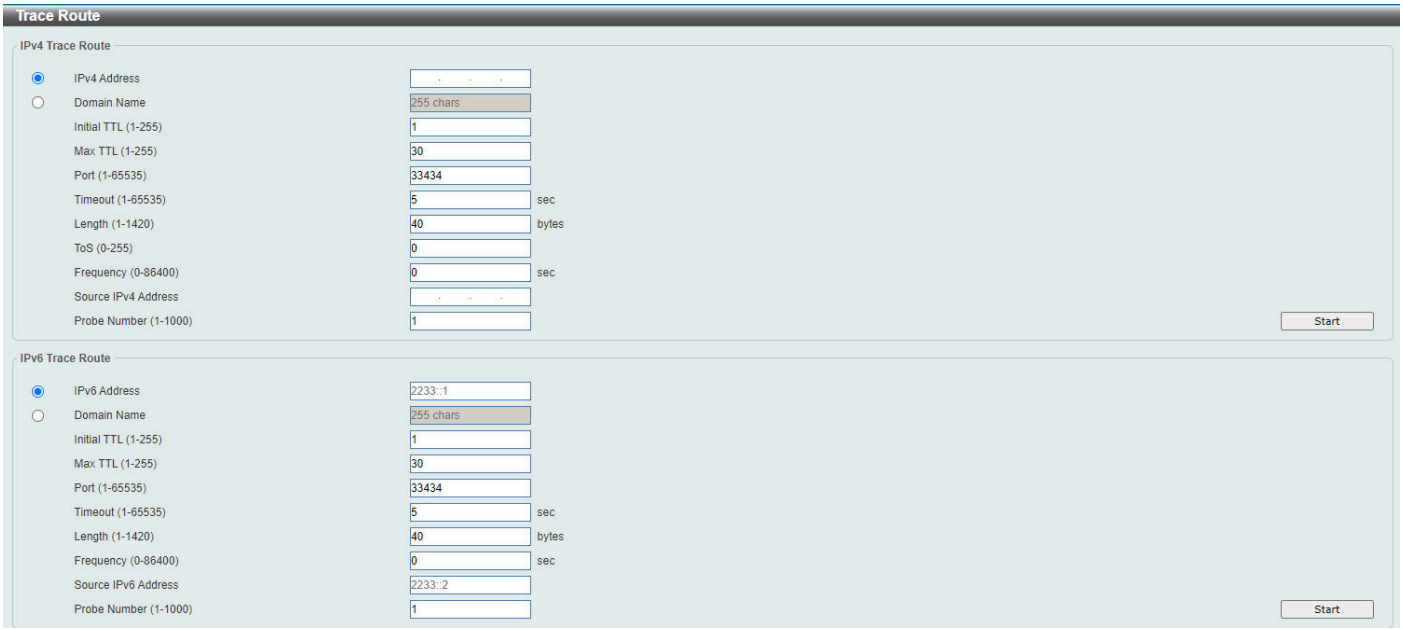


Figure 13-15 Trace Route Window

The fields that can be configured in **IPv4 Trace Route** are described below:

Parameter	Description
IPv4 Address	Select and enter the IPv4 address of the destination here.
Domain Name	Select and enter the domain name of the destination here.
Initial TTL	Enter the initial Time-To-Live (TTL) value here. The range is from 1 to 255.

Parameter	Description
Max TTL	Enter the 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 for the TTL is 1 to 255 hops.
Port	Enter the port number here. The value range is from 1 to 65535.
Timeout	Enter the timeout period while waiting for a response from the remote device here. A value of 1 to 65535 seconds can be specified. The default is 5 seconds.
Length	Enter the length value here. This specifies the number of bytes of the outgoing datagram. The range is from 1 to 1420 bytes.
ToS	Enter the ToS value here. This specifies the ToS to be set in the IP header of the outgoing datagram. The range is from 0 to 255.
Frequency	Enter the time interval between each probe packet. The range is from 0 to 86400 and the default is 0.
Source IPv4 Address	Enter the source IPv4 address here. The specified IPv4 address must one of the IPv4 addresses configured for the Switch.
Probe Number	Enter the probe time number here. The range is from 1 to 1000. If unspecified, the default value is 1.

Click the **Start** button to initiate the route trace for each individual section.

The fields that can be configured in **IPv6 Trace Route** are described below:

Parameter	Description
IPv6 Address	Select and enter the IPv6 address of the destination here.
Domain Name	Select and enter the domain name of the destination here.
Initial TTL	Enter the initial Time-To-Live (TTL) value here. The range is from 1 to 255.
Max TTL	Enter the 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 for the TTL is 1 to 255 hops.
Port	Enter the port number here. The value range is from 1 to 65535.
Timeout	Enter the timeout period while waiting for a response from the remote device here. A value of 1 to 65535 seconds can be specified. The default is 5 seconds.
Length	Enter the length value here. This specifies the number of bytes of the outgoing datagram. The range is from 1 to 1420 bytes.
Frequency	Enter the time interval between each probe packet. The range is from 0 to 86400 and the default is 0.
Source IPv6 Address	Enter the source IPv6 address here. The specified IPv6 address must one of the IPv6 addresses configured for the Switch.
Probe Number	Enter the probe time number here. The range is from 1 to 1000. If unspecified, the default value is 1.

Click the **Start** button to initiate the route trace for each individual section.

After clicking the **Start** button in **IPv4 Trace Route** section, the following **IPv4 Trace Route Result** section will appear:

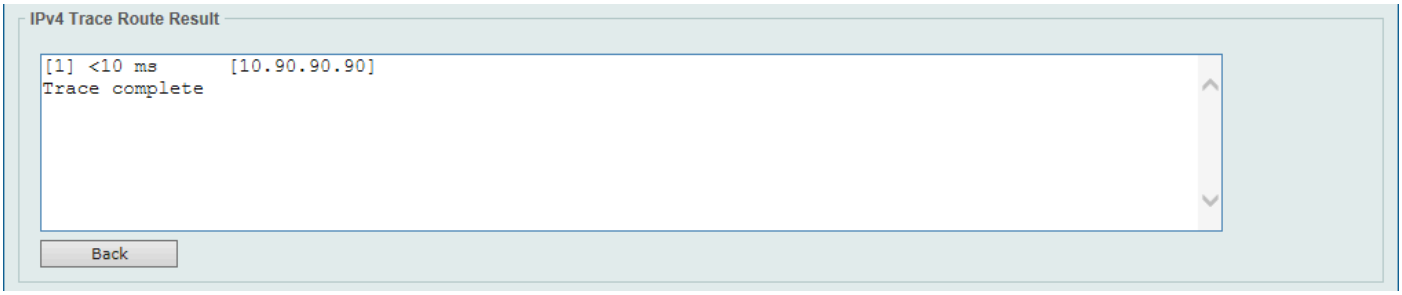


Figure 13-16 Trace Route (Start) Window

Click the **Back** button to stop the trace route and return to the IPv4 Trace Route section.

Reset

This window is used to reset the Switch's configuration to the factory default settings.

To view the following window, click **Tools > Reset**, as shown below:

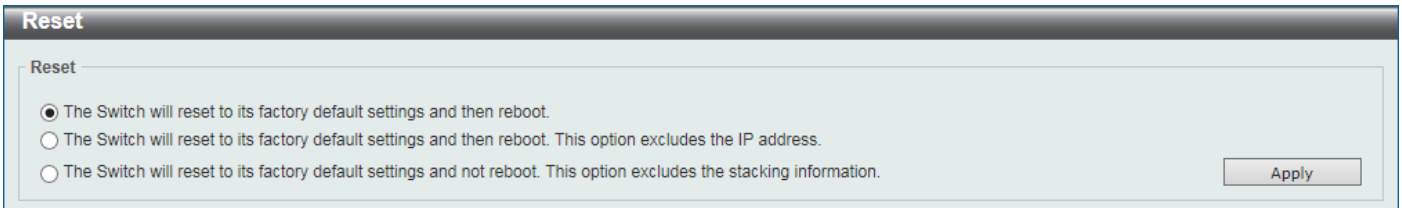


Figure 13-17 Reset Window

Select one of the following 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. This option excludes the stacking information.

Click the **Apply** button to initiate the reset.

Reboot System

This window is used to reboot the Switch and alternatively save the configuration before doing so.

To view the following window, click **Tools > Reboot System**, as shown below:

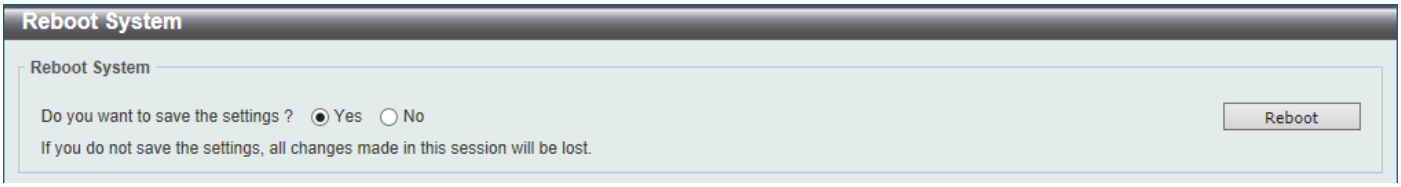


Figure 13-18 Reboot System Window

When rebooting the Switch, any configuration changes that was made during this session will be lost unless the **Yes** option is selected when asked to save the settings.

Click the **Reboot** button to alternatively save the settings and reboot the Switch.

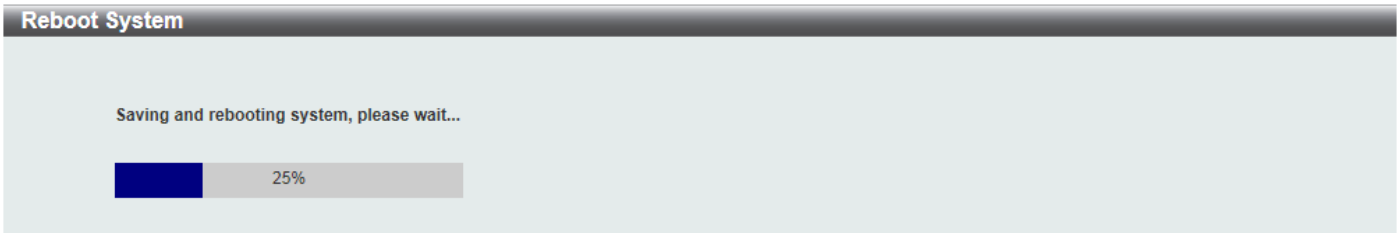


Figure 13-19 Reboot System (Rebooting) Window

Appendix A - Password Recovery Procedure

This section describes the procedure for resetting passwords on the D-Link DXS-3130 Series Switch.

Authenticating any user who tries to access networks is necessary and important. The basic authentication method used to accept qualified users is through a local login, utilizing a Username and Password. Sometimes, passwords will be forgotten or destroyed, so network administrators need to reset these passwords. This section will explain how the **Password Recovery** feature can help network administrators reach this goal.

The following steps explain how to use the Password Recovery feature on this Switch to easily recover passwords. Complete these steps to reset the password:

- For security reasons, the Password Recovery feature requires the user to physically access the device. Therefore, this feature is only applicable when there is a direct connection to the console port of the device. It is necessary for the user needs to attach a terminal or PC with terminal emulation to the console port of the Switch.
- Power on the Switch. After the **UART init** is loaded to 100%, the Switch will allow 2 seconds for the user to press the hotkey [**^**] (**Shift+6**) to enter the "Password Recovery Mode." Once the Switch enters the "Password Recovery Mode," all ports on the Switch will be disabled.

```
  Boot Procedure                                          V1.00.003
-------------------------------------------------------------------------------

  Power On Self Test ....................................  100 %

  MAC Address    : F0-7D-68-36-30-00
  H/W Version    : A1

  Please Wait, Loading 1.01.006 Runtime Image ..............  100 %
  UART init .................................................  100 %
```

```
Password Recovery Mode
Switch(reset-config)#
```

In the "Password Recovery Mode" only the following commands can be used.

Command	Description
`no enable password`	This command is used to delete all account level passwords.
`no login password`	This command is used to clear the local login methods.
`no username`	This command is used to delete all local user accounts.
`password-recovery`	This command is used to initiate the password recovery procedure.
`reload`	This command is used to save and reboot the Switch.
`reload clear running-config`	This command is used to reset the running configuration to the factory default settings and then reboot the Switch.
`show running-config`	This command is used to display the current running configuration.
`show username`	This command is used to display local user account information.

Appendix B - System Log Entries

The following table lists all possible entries and their corresponding meanings that will appear in the System Log of this Switch.

802.1X

Log Description	Severity
Event description: 802.1X Authentication failure. Log Message: 802.1X authentication fail [due to <reason>] from (Username: <username>, <interface-id>, MAC: <mac-address>) Parameters description: reason: The reason for the failed authentication. username: The user that is being authenticated. interface-id: The interface name. mac-address: The MAC address of the authenticated device.	Critical
Event description: 802.1X Authentication successful. Log Message: 802.1X authentication success (Username: <username>, <interface-id>, MAC: <mac-address>) Parameters description: username: The user that is being authenticated. interface-id: The interface name. mac-address: The MAC address of the authenticated device.	Informational

AAA

Log Description	Severity
Event description: AAA global state is enabled or disabled. Log Message: AAA is <status>. Parameters description: status: The status indicates the AAA enabled or disabled.	Informational
Event description: Successful login. Log Message: Successful login through <exec-type> from <client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>). Parameters description: exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL). client-ip: It indicates the client's IP address if valid through IP protocol. aaa-method: It indicates the authentication method, e.g.: none, local, server. server-ip: It indicates the AAA server IP address if authentication method is remote server. username: It indicates the username for authentication.	Informational
Event description: Login failed. Log Message: Login failed through <exec-type> from <client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>). Parameters description: exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL).	Warning

Log Description	Severity
client-ip: It indicates the client's IP address if valid through IP protocol. aaa-method: It indicates the authentication method, e.g.: none, local, server. server-ip: It indicates the AAA server IP address if authentication method is remote server. username: It indicates the username for authentication.	
Event description: Login failed due to AAA server timeout or improper configuration. Log Message: Login failed through <exec-type> from <client-ip> due to AAA server <server-ip> timeout (Username: <username>). Parameters description: exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL). client-ip: It indicates the client's IP address if valid through IP protocol. server-ip: It indicates the AAA server IP address if authentication method is remote server. username: It indicates the username for authentication.	Warning
Event description: Enable privilege successfully. Log Message: Successful enable privilege through <exec-type> from <client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>). Parameters description: exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL). client-ip: It indicates the client's IP address if valid through IP protocol. aaa-method: It indicates the authentication method, e.g.: none, local, server. server-ip: It indicates the AAA server IP address if authentication method is remote server. username: It indicates the username for authentication.	Informational
Event description: Enable privilege failure. Log Message: Enable privilege failed through <exec-type> from <client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>). Parameters description: exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL). client-ip: It indicates the client's IP address if valid through IP protocol. aaa-method: It indicates the authentication method, e.g.: none, local, server. server-ip: It indicates the AAA server IP address if authentication method is remote server. username: It indicates the username for authentication.	Warning
Event description: the remote server does not respond to the enable password authentication request. Log Message: Enable privilege failed through <exec-type> from <client-ip> due to AAA server <server-ip> timeout (Username: <username>). Parameters description: exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL). client-ip: It indicates the client's IP address if valid through IP protocol. server-ip: It indicates the AAA server IP address if authentication method is remote server. username: It indicates the username for authentication.	Warning
Event description: 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.	Informational

Log Description	Severity
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.	
Event description: 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
Event description: 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
Event description: 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

ARP

Log Description	Severity
Event description: Gratuitous ARP detected duplicate IP. Log Message: Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:]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. unitID: 1.Interger value;2.Represent the id of the device in the stacking system. 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

Auto-save

Log Description	Severity
Event description: Record the event when the configure information of DDP is saved automatically. Log Message: [Unit <unitID>,]Configuration automatically saved to flash due to configuring from DDP(Username: <username>, IP: <ipaddr>) Parameters description: Unit: Box ID username: Represent current login user. ipaddr: Represent client IP address	Informational

BPDU Protection

Log Description	Severity
Event description: Record the event when the BPDU attack happened. Log Message: <interface-id> enter STP BPDU under protection state (mode: <mode>) Parameters description: interface-id: Interface on which detected STP BPDU attack. mode: BPDU Protection mode of the interface. Mode can be drop, block, or shutdown	Informational
Event description: Record the event when the STP BPDU attack recovered. Log Message: <interface-id> recover from BPDU under protection state. Parameters description: interface-id: Interface on which detected STP BPDU attack.	Informational

CFM

Log Description	Severity
Event Description: Cross-connect is detected Log Message: CFM cross-connect. VLAN:<vlanid>, Local(MD Level:<mdlevel>, Interface:<interface-id>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>) Parameters Description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. interface-id: Represents the interface number of the MEP. mepdirection: Can be "inward" or "outward". mepid: Represents the MEPID of the MEP. The value 0 means unknown MEPID. macaddr: Represents the MAC address of the MEP. The value all zeros mean unknown MAC address. Note: In CFM hardware mode, remote MEP information (mepid and macaddr) is unknown.	Critical
Event Description: Error CFM CCM packet is detected. Log Message: CFM error CCM. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>) Parameters Description: vlanid: Represents the VLAN identifier of the MEP.	Warning

Log Description	Severity
mdlevel: Represents MD level of the MEP. interface-id: Represents the interface number of the MEP. mepdirection: Can be "inward" or "outward". mepid: Represents the MEPID of the MEP. The value 0 means unknown MEPID. macaddr: Represents the MAC address of the MEP. The value all zeros means unknown MAC address. Note: In CFM hardware mode, remote MEP information (mepid and macaddr) is unknown.	
Event Description: Cannot receive the remote MEP's CCM packet. Log Message: CFM remote down. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>) Parameters Description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. interface-id: Represents the interface number of the MEP. mepdirection: Represents the MEP direction, which can be "inward" or "outward". mepid: Represents the MEPID of the MEP. macaddr: Represents the MAC address of the MEP.	Warning
Event Description: Remote MEP's MAC reports an error status. Log Message: CFM remote MAC error. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>) Parameters Description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. interface-id: Represents the interface number of the MEP. mepdirection: Represents the MEP direction, which can be "inward" or "outward". mepid: Represents the MEPID of the MEP. macaddr: Represents the MAC address of the MEP.	Warning
Event Description: Remote MEP detects CFM defects. Log Message: CFM remote detects a defect. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>) Parameters Description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. interface-id: Represents the interface number of the MEP. mepdirection: Represents the MEP direction, which can be "inward" or "outward". mepid: Represents the MEPID of the MEP. macaddr: Represents the MAC address of the MEP.	Informational

CFM Extension

Log Description	Severity
Event Description: AIS condition detected. Log Message: AIS condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>, MEPID:<mepid>) Parameters Description: vlanid: Represents the VLAN identifier of the MEP.	Notification

Log Description	Severity
mdlevel: Represents the MD level of the MEP. interface-id: Represents the interface number of the MEP. mepdirection: Represents the direction of the MEP. This can be "inward" or "outward". mepid: Represents the MEPID of the MEP.	
Event Description: AIS condition cleared. Log Message: AIS condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>, MEPID:<mepid>) Parameters Description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. interface-id: Represents the interface number of the MEP. mepdirection: Represents the direction of the MEP. This can be "inward" or "outward". mepid: Represents the MEPID of the MEP.	Notification
Event Description: LCK condition detected. Log Message: LCK condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>, MEPID:<mepid>) Parameters Description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. interface-id: Represents the interface number of the MEP. mepdirection: Represents the direction of the MEP. This can be "inward" or "outward". mepid: Represents the MEPID of the MEP.	Notification
Event Description: LCK condition cleared. Log Message: LCK condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>, MEPID:<mepid>) Parameters Description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. interface-id: Represents the interface number of the MEP. mepdirection: Represents the direction of the MEP. This can be "inward" or "outward". mepid: Represents the MEPID of the MEP.	Notification

Configuration/Firmware

Log Description	Severity
Event description: Firmware upgraded successfully. Log Message: [Unit <unitID>,]Firmware upgraded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: The unit ID. 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

Log Description	Severity
Event description: Firmware upgraded unsuccessfully. Log Message: [Unit <unitID>,]Firmware upgraded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: The unit ID. 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
Event description: Firmware uploaded successfully. Log Message: [Unit <unitID>,]Firmware uploaded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: The unit ID. 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
Event description: Firmware uploaded unsuccessfully. Log Message: [Unit <unitID>,]Firmware uploaded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: The unit ID. 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
Event description: Configuration downloaded successfully. Log Message: [Unit <unitID>,]Configuration downloaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: The unit ID. 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

Log Description	Severity
Event description: Configuration downloaded unsuccessfully. Log Message: [Unit <unitID>,]Configuration downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: The unit ID. 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
Event description: Configuration uploaded successfully. Log Message: [Unit <unitID>] Configuration uploaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: The unit ID. 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
Event description: Configuration uploaded unsuccessfully. Log Message: [Unit <unitID>] Configuration uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: The unit ID. 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
Event description: Unknown type files downloaded unsuccessfully. Log Message: [Unit <unitID>] Downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters description: unitID: The unit ID. 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

DAD

Log Description	Severity
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
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

DDM

Log Description	Severity
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
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

Log Description	Severity
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

DHCPv6 Client

Log Description	Severity
Event description: DHCPv6 client interface administrator state changed. Log Message: DHCPv6 client on interface <ipif-name> changed state to [enabled | disabled]. Parameters description: <ipif-name>: Name of the DHCPv6 client interface.	Informational
Event description: DHCPv6 client obtains an IPv6 address from a DHCPv6 server. Log Message: DHCPv6 client obtains an IPv6 address <ipv6address> on interface <ipif-name>. Parameters description: ipv6address: IPv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
Event description: The IPv6 address obtained from a DHCPv6 server starts renewing. Log Message: The IPv6 address <ipv6address> on interface <ipif-name> starts renewing. Parameters description: ipv6address: IPv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
Event description: The IPv6 address obtained from a DHCPv6 server 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
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
Event description: The IPv6 address obtained from a DHCPv6 server rebinds success	Informational

Log Description	Severity
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.	
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
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
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
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

DHCPv6 Server

Log Description	Severity
Event description: The address of the DHCPv6 Server pool is used up Log Message: The address of the DHCPv6 Server pool <pool-name> is used up. Parameters description: <pool-name>: Name of the DHCPv6 Server pool.	Informational
Event description: The number of allocated IPv6 addresses is equal to 4096 Log Message: The number of allocated IPv6 addresses of the DHCPv6 Server pool is equal to 4096.	Informational

Dynamic ARP Inspection

Log Description	Severity
Event description: Detect illegal ARP packet	Warning

Log Description	Severity
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. ipaddr: IP address macaddr: MAC address. vlanid: VLAN ID interface-id: Interface name	

ERPS

Log Description	Severity
Event description: manual Switch is issued. Log Message: "Manual Switch is issued on node (MAC: <macaddr>, instance <InstanceID>)" Parameters description: macaddr: MAC address InstanceID: Instance ID	Warning
Event description: signal fail is detected. Log Message: "Signal fail detected on node (MAC: <macaddr>, instance <InstanceID>)" Parameters description: macaddr: MAC address InstanceID: Instance ID	Warning
Event description: Signal fail cleared. Log Message: "Signal fail cleared on node(MAC: <macaddr>, instance <InstanceID>)" Parameters description: macaddr: MAC address InstanceID: Instance ID	Warning
Event description: Force Switch is issued. Log Message: "Force Switch is issued on node (MAC: <macaddr>, instance <InstanceID>)" Parameters description: macaddr: MAC address InstanceID: Instance ID	Warning
Event description: Clear command is issued. Log Message: "Clear command is issued on node (MAC: <macaddr>, instance <InstanceID>)" Parameters description: macaddr: MAC address InstanceID: Instance ID	Warning
Event description: "RPL owner conflicted. Log Message: "RPL owner conflicted on the node (MAC: <macaddr>, instance <InstanceID>)" Parameters description: macaddr: MAC address InstanceID: Instance ID	Warning

Ethernet OAM

Log Description	Severity
Event description: Dying gasp event(remote) Log Message: OAM dying gasp event received (Port<interface-id>) Parameters description: interface-id: The interface name.	Warning
Event description: Dying gasp event(local) Log Message: Device encountered an OAM dying gasp event.	Warning
Event description: Critical event(remote) Log Message: OAM critical event received (Port<interface-id>) Parameters description: interface-id: The interface name.	Warning
Event description: Critical event(local) Log Message: Device encountered an OAM critical event (Port<interface-id>, <condition>) Parameters description: interface-id: The interface name. condition: Display string for the condition of generating critical link event. e.g. OAM disable, Port shutdown, Port link down, Packet overload.	Warning
Event description: Errored Symbol Period Event(remote) Log Message: Errored symbol period event received (Port <interface-id>) Parameters description: interface-id: The interface name.	Warning
Event description: Errored Frame Event Log Message: Errored frame event received(Port <interface-id>) Parameters description: interface-id: The interface name.	Warning
Event description: Errored Frame Period Event Log Message: Errored frame period event received(Port <interface-id>) Parameters description: interface-id: The interface name.	Warning
Event description: Errored Frame Seconds Summary Event Log Message: Errored frame seconds summary event received (Port <interface-id>) Parameters description: interface-id: The interface name.	Warning
Event description: Remote loopback start Log Message: OAM Remote loopback started (Port <interface-id>) Parameters description: interface-id: The interface name.	Warning
Event description: Remote loopback stop Log Message: OAM Remote loopback stopped (Port <interface-id>) Parameters description: interface-id: The interface name.	Warning

Interface

Log Description	Severity
Event description: Port link up. Log Message: Port <portNum> link up, <link state> Parameters description: portNum: 1.Interger value;2.Represent the logic port number of the device. link state: for ex: , 100Mbps FULL duplex	Informational
Event description: Port link down. Log Message: Port <portNum> link down Parameters description: portNum: 1.Interger value; 2.Represent the logic port number of the device.	Informational

IP Directed Broadcast

Log Description	Severity
Event description: IP Directed-broadcast rate exceed 50 packets per second on a certain subnet. Log Message: IP Directed Broadcast packet rate is high on subnet. [(IP: %s)] Parameters description: IP: the Broadcast IP destination address.	Informational
Event description: IP Directed-broadcast rate exceed 100 packets per second Log Message: IP Directed Broadcast rate is high.	Informational

LACP

Log Description	Severity
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
Event description: Link Aggregation Group link down. Log Message: Link Aggregation Group <group_id> link down. Parameters description: group_id: The group id of the link down aggregation group.	Informational
Event description: Member port attach to Link Aggregation Group. Log Message: <ifname> attach to Link Aggregation Group <group_id>. Parameters description: Ifname: The interface name of the port that attach to aggregation group. group_id: The group id of the aggregation group that port attach to.	Informational
Event description: Member port detach from Link Aggregation Group. Log Message: <ifname> detach from Link Aggregation Group <group_id>. Parameters description: Ifname: The interface name of the port that detach from aggregation group. group_id: The group id of the aggregation group that port detach from.	Informational

LBD

Log Description	Severity
Event Description: Loop back is detected under port-based mode. Log Message: IfInfo LBD loop occurred. Parameters Description: IfInfo: The interface info.	Critical
Event Description: Port recovered from LBD blocked state under port-based mode. Log Message: IfInfo LBD loop recovered. Parameters Description: IfInfo: The interface info.	Critical
Event Description: Loop back is detected under VLAN-based mode. Log Message: IfInfo VID <vlanID> LBD loop occurred. Parameters Description: IfInfo: The interface info. vlanID: The VLAN ID number.	Critical
Event Description: Port recovered from LBD blocked state under VLAN-based mode. Log Message: IfInfo VID <vlanID> LBD loop recovered. Parameters Description: IfInfo: The interface info. vlanID: The VLAN ID number.	Critical
Event Description: The number of VLANs that loop back has occurred hit the specified number. Log Message: Loop VLAN numbers overflow. Parameters Description: None	Critical

LLDP-MED

Log Description	Severity
Event description: LLDP-MED topology change detected Log Message: LLDP-MED topology change detected (on port <portNum>. chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>) Parameters description: portNum: The port number. chassisType: chassis ID subtype. Value list: 1. chassisComponent(1) 2. interfaceAlias(2)	Notice

Log Description	Severity
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.	
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
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>)	Notice

Log Description	Severity
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.	

Login/Logout

Log Description	Severity
Event description: Login through console successfully. Log Message: [Unit <unitID>,]Successful login through Console (Username: <username>) Parameters description: unitID: The unit ID. username: Represent current login user.	Informational
Event description: Login through console unsuccessfully. Log Message: [Unit <unitID>,] Login failed through Console (Username: <username>) Parameters description: unitID: The unit ID. username: Represent current login user.	Warning
Event description: Console session timed out. Log Message: [Unit <unitID>,] Console session timed out (Username: <username>) Parameters description: unitID: The unit ID. username: Represent current login user.	Informational
Event description: Logout through console. Log Message: [Unit <unitID>,] Logout through Console (Username: <username>) Parameters description:	Informational

Log Description	Severity
unitID: The unit ID. username: Represent current login user.	
Event description: Login through telnet successfully. Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event description: Login through telnet unsuccessfully. Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Warning
Event description: Telnet session timed out. Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event description: Logout through telnet. Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event description: Login through SSH successfully. Log Message: Successful login through SSH (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event description: Login through SSH unsuccessfully. Log Message: Login failed through SSH (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Critical
Event description: SSH session timed out. Log Message: SSH session timed out (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event description: Logout through SSH. Log Message: Logout through SSH (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Informational

MAC

Log Description	Severity
Event description: the host has passed MAC authentication Log Message: MAC-based Access Control host login success (MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Parameters description: mac-address: the host MAC addresses. interface-id: the interface on which the host is authenticated. vlan-id: the VLAN ID on which the host exists.	Informational
Event description: the host has aged out. Log Message: MAC-based Access Control host aged out (MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Parameters description: mac-address: the host MAC addresses. interface-id: the interface on which the host is authenticated. vlan-id: the VLAN ID on which the host exists.	Informational
Event description: the host failed to pass the authentication. Log Message: MAC-based Access Control host login fail (MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Parameters description: mac-address: the host MAC addresses. interface-id: the interface on which the host is authenticated. vlan-id: the VLAN ID on which the host exists.	Critical
Event description: the authorized user number on the whole device has reached the maximum user limit. Log Message: MAC-based Access Control enters stop learning state.	Warning
Event description: the authorized user number on the whole device is below the maximum user limit in a time interval. Log Message: MAC-based Access Control recovers from stop learning state.	Warning
Event description: the authorized user number on an interface has reached the maximum user limit. Log Message: <interface-id> enters MAC-based Access Control stop learning state Parameters description: interface-id: the interface on which the host is authenticated.	Warning
Event description: the authorized user number on an interface is below the maximum user limit in a time interval. Log Message: <interface-id> recovers from MAC-based Access Control stop learning state. Parameters description: interface-id: the interface on which the host is authenticated.	Warning

MSTP Debug Enhancement

Log Description	Severity
Event description: Topology changed. Log Message: Topology changed [([Instance:<InstanceID>] , <portNum> ,MAC: <macaddr>)] Parameters description: InstanceID: Instance ID.	Notice

Log Description	Severity
portNum: Port ID macaddr: MAC address	
Event description: Spanning Tree new Root Bridge Log Message: [CIST | CIST Regional | MSTI Regional] New Root bridge selected([Instance: <InstanceID>],MAC: <macaddr>, Priority :<value>) Parameters description: InstanceID: Instance ID. macaddr: Mac address value: priority value	Informational
Event description: Spanning Tree Protocol is enabled Log Message: Spanning Tree Protocol is enabled	Informational
Event description: Spanning Tree Protocol is disabled Log Message: Spanning Tree Protocol is disabled	Informational
Event description: New root port Log Message: New root port selected [([Instance:<InstanceID>], <portNum>)] Parameters description: InstanceID: Instance ID. portNum: Port ID	Notice
Event description: Spanning Tree port status changed Log Message: Spanning Tree port status change [([Instance:<InstanceID>], <portNum>)] <old_status> -> <new_status> Parameters description: InstanceID: Instance ID. portNum: Port ID old_status: Old status new_status: New status	Notice
Event description: Spanning Tree port role changed. Log Message: Spanning Tree port role change. [([Instance:<InstanceID>], <[portNum>)] <old_role> -> <new_role> Parameters description: InstanceID: Instance ID. portNum: Port ID/ old_role: Old role new_status: New role	Informational
Event description: Spanning Tree instance created. Log Message: Spanning Tree instance created. (Instance:<InstanceID>) Parameters description: InstanceID: Instance ID.	Informational
Event description: Spanning Tree instance deleted. Log Message: Spanning Tree instance deleted. (Instance:<InstanceID>) Parameters description: InstanceID: Instance ID.	Informational
Event description: Spanning Tree Version changed. Log Message: Spanning Tree version change.(New version:<new_version>) Parameters description: new_version: New STP version.	Informational

Log Description	Severity
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
Event description: Spanning Tree MST configuration ID VLAN mapping table deleted. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <InstanceID> delete vlan <startvlanid> [- <endvlanid>]). Parameters description: InstanceID: Instance ID. startvlanid- endvlanid: VLAN list	Informational
Event description: Spanning Tree MST configuration ID VLAN mapping table added. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <InstanceID> add vlan <startvlanid> [- <endvlanid>]). Parameters description: InstanceID: Instance ID. startvlanid- endvlanid: VLAN list	Informational
Event description: Spanning Tree port role change to alternate port due to the guard root. Log Message: Spanning Tree port role change (Instance : <InstanceID>, <portNum>) to alternate port due to the guard root. Parameters description: InstanceID: Instance ID. portNum: Port ID	Informational
Event description: Spanning Tree loop guard blocking. Log Message: Spanning Tree loop guard blocking(Instance : <InstanceID>, <portNum>) Parameters description: InstanceID: Instance ID. portNum: Port ID	Informational

Peripheral

Log Description	Severity
Event description: Temperature sensor enters alarm state. Log Message: Unit <unit-id> <thermal-sensor-descr> detects abnormal temperature <degree> Parameters description: unitID: The unit ID. thermal-sensor-descr: Description of the sensor. degree: The current temperature of the sensor.	Warning
Event description: Temperature recovers to normal. Log Message: Unit <unit-id> <thermal-sensor-descr> temperature back to normal Parameters description: unitID: The unit ID.	Informational

Log Description	Severity
thermal-sensor-descr: Description of the sensor. degree: The current temperature of the sensor.	
Event description: Power failed. Log Message: Unit <unit-id> <power-descr> failed Parameters description: Unit <id>: The unit ID. power-descr: Describe the power.	Critical
Event description: Power is recovered. Log Message: Unit <unit-id> <power-descr> back to normal Parameters description: Unit <id>: The unit ID. power-descr: Describe the power.	Critical
Event description: External Alarm state to change. Log Message: Unit <unit-id> External Alarm Channel <channelID> :<alarmMsg> Parameters description: Unit <id>: The unit ID. channelID: The channel ID. alarmMsg: The alarm Msg.	Critical

Port

Log Description	Severity
Event description: port linkup Log Message: Port <port> link up, <nway> Parameters description: port: Represents the logical port number. nway: Represents the speed and duplex of link.	Informational
Event description: port linkdown Log Message: Port <port> link down Parameters description: port: Represents the logical port number.	Informational

Port Security

Log Description	Severity
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 name.	Warning
Event description: Address full on system Log Message: Limit on system entry number has been exceeded.	Warning

Reboot Schedule

Log Description	Severity
Event description: Tips is about will to reboot Switch within the specified time. Log Message: Display “Reboot scheduled in 5 minutes” when the countdown equals 5 minutes. Display ”Reboot scheduled in 1 minute” when the countdown equals 1 minute.	Critical

Safeguard

Log Description	Severity
Event description: When the CPU utilization is over the rising threshold, the Switch enters exhausted mode, and the syslog will be recorded. Log Message: Unit <unit-id>, Safeguard Engine enters EXHAUSTED mode. Parameters description: unit-id: Unit ID.	Warning
Event description: When the CPU utilization is lower than the falling threshold, the Switch enters normal mode, and the syslog will be recorded. Log Message: Unit <unit-id>, Safeguard Engine enters NORMAL mode. Parameters description: unit-id: Unit ID.	Informational

SNMP

Log Description	Severity
Event Description: SNMP request received with invalid community string Log Message: SNMP request received from <ipaddr> with invalid community string. Parameters Description: ipaddr: The IP address.	Informational

SSH

Log Description	Severity
Event description: SSH server is enabled. Log Message: SSH server is enabled	Informational
Event description: SSH server is disabled. Log Message: SSH server is disabled	Informational

SSL

Log Description	Severity
Event description: Successful login through Web (SSL). Log Message: Successful login through Web (SSL) (Username: <username>, IP: <ipaddr>). Parameters description:	Informational

Log Description	Severity
username: The username that used to login SSL server. ipaddr: The IP address of SSL client.	
Event description: Login failed through Web (SSL). Log Message: Login failed through Web (SSL) (Username: <username>, IP: <ipaddr>). Parameters description: username: The username that used to login SSL server. ipaddr: The IP address of SSL client.	Warning
Event description: Web (SSL) session timed out. Log Message: Web (SSL) session timed out (Username: <username>, IP: <ipaddr>). Parameters description: username: The username that used to login SSL server. ipaddr: The IP address of SSL client.	Informational
Event description: Logout through Web (SSL). Log Message: Logout through Web (SSL) (Username: <username>, IP: <ipaddr>). Parameters description: username: The username that used to login SSL server. ipaddr: The IP address of SSL client.	Informational

Stacking

Log Description	Severity
Event description: Hot insertion. Log Message: Unit: <unitID>, MAC: <macaddr> Hot insertion. Parameters description: unitID: Box ID. Macaddr: MAC address.	Informational
Event description: Hot removal. Log Message: Unit: <unitID>, MAC: <macaddr> Hot removal. Parameters description: unitID: Box ID. Macaddr: MAC address.	Informational
Event description: Backup master changed to master. Log Message: Backup master changed to master. Master (Unit: <unitID>). Parameters description: unitID: Box ID.	Informational
Event description: Stacking topology change. Log Message: Stacking topology is <Stack_TP_TYPE>.Master(Unit <unitID>, MAC: <macaddr>) Parameters description: Stack_TP_TYPE: The stacking topology type is one of the following: 1. Ring 2. Chain unitID: Box ID. Macaddr: MAC address.	Critical
Event description: Slave changed to master Log Message: Slave changed to master. Master (Unit: <unitID>).	Informational

Log Description	Severity
Parameters description: unitID: Box ID.	
Event description: Stacking port link up. Log Message: Stacking port <portID> link up. Parameters description: portID: port ID.	Critical
Event description: Stacking port link down. Log Message: Stacking port <portID> link down. Parameters description: portID: port ID.	Critical

Storm Control

Log Description	Severity
Event description: Storm occurrence. Log Message: <Broadcast | Multicast | Unicast> storm is occurring on <interface-id>. Parameters description: Broadcast: Storm is resulted by broadcast packets (DA = FF:FF:FF:FF:FF:FF). Multicast: Storm is resulted by multicast packets, including unknown L2 multicast, known L2 multicast, unknown IP multicast and known IP multicast. Unicast: Storm is resulted by unicast packets, including both known and unknown unicast packets interface-id: The interface ID on which a storm is occurring.	Warning
Event description: Storm cleared. Log Message: <Broadcast | Multicast | Unicast> storm is cleared on <interface-id>. Parameters description: Broadcast: Broadcast storm is cleared. Multicast: Multicast storm is cleared. Unicast: Unicast storm (including both known and unknown unicast packets) is cleared. interface-id: The interface ID on which a storm is cleared.	Informational
Event description: Port shut down due to a packet storm Log Message: <interface-id> is currently shut down due to the <Broadcast | Multicast | Unicast> storm. Parameters description: interface-id: The interface ID on which is error-disabled by storm. Broadcast: The interface is disabled by broadcast storm. Multicast: The interface is disabled by multicast storm. Unicast: The interface is disabled by unicast storm (including both known and unknown unicast packets).	Warning
Note: Logs will be generated only if the control action is set to Shutdown for unicast traffic, including both known and unknown unicast traffic. Actions other than Shutdown such as Drop for unicast traffic will not generate logs.	

Telnet

Log Description	Severity
Event description: Successful login through Telnet. Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Informational
Event description: Login failed through Telnet. Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Warning
Event description: Logout through Telnet. Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Informational
Event description: Telnet session timed out. Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>). Parameters description: ipaddr: The IP address of telnet client. username: the user name that used to login telnet server.	Informational

WAC

Log Description	Severity
Event description: When a client host fails to authenticate. Log Message: WAC unauthenticated user (User Name: <string>, IP: <ipaddr | ipv6address>, MAC: <macaddr>, Port: <[unitID:]portNum>) Parameters description: string: User name ipaddr: IP address ipv6address: IPv6 address macaddr: MAC address unitID: The unit ID portNum : The port number	Warning
Event description: This log will be triggered when the number of authorized users reaches the maximum user limit on the whole device. Log Message: WAC enters stop learning state.	Warning
Event description: This log will be triggered when the number of authorized users is below the maximum user limit on whole device in a time interval (The interval is project dependent). Log Message: WAC recovered from stop learning state.	Warning
Event description: When a client host authenticated successful. Log Message: WAC authenticated user (Username: <string>, IP: <ipaddr | ipv6address>, MAC: <macaddr>, Port: <[unitID:] portNum>)	Informational

Log Description	Severity
Parameters description: string: User name ipaddr: IP address ipv6address: IPv6 address macaddr: MAC address unitID: The unit ID portNum : The port number	

Web

Log Description	Severity
Event description: Successful login through Web. Log Message: Successful login through Web (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational
Event description: Login failed through Web. Log Message: Login failed through Web (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Warning
Event description: Web session timed out. Log Message: Web session timed out (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational
Event description: Logout through Web. Log Message: Logout through Web (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational

Appendix C - Trap Entries

The following table lists all possible trap log entries and their corresponding meanings that will appear in the Switch.

802.1X

Trap Name	Description	OID
esDot1xExtLoggedSuccess	The trap is sent when a host has successfully logged in (passed 802.1X authentication). Binding objects: (1) ifIndex, (2) esnaSessionClientMacAddress (3) esnaSessionAuthVlan (4) esnaSessionAuthUserName	1.3.6.1.4.1.17 1.17.30.0.1
esDot1xExtLoggedFail	The trap is sent when a host failed to pass 802.1X authentication (login failed). Binding objects: (1) ifIndex, (2) esnaSessionClientMacAddress (3) esnaSessionAuthVlan (4) esnaSessionAuthUserName (5) esDot1xExtNotifyFailReason	1.3.6.1.4.1.17 1.17.30.0.2

802.3ah OAM

Trap Name	Description	OID
dot3OamThresholdEvent	This notification is sent when a local or remote threshold crossing event is detected. Binding objects: (1) dot3OamEventLogTimestamp (2) dot3OamEventLogOui (3) dot3OamEventLogType (4) dot3OamEventLogLocation (5) dot3OamEventLogWindowHi (6) dot3OamEventLogWindowLo (7) dot3OamEventLogThresholdHi (8) dot3OamEventLogThresholdLo (9) dot3OamEventLogValue (10) dot3OamEventLogRunningTotal (11) dot3OamEventLogEventTotal	1.3.6.1. 2.1.158. 0.1
dot3OamNonThresholdEvent	This notification is sent when a local or remote non-threshold crossing event is detected. Binding objects: (1) dot3OamEventLogTimestamp (2) dot3OamEventLogOui (3) dot3OamEventLogType	1.3.6.1. 2.1.158. 0.2

Trap Name	Description	OID
	(4) dot3OamEventLogLocation (5) dot3OamEventLogEventTotal	

Authentication Fail

Trap Name	Description	OID
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

BPDU Protection

Trap Name	Description	OID
esBpduProtectionAttackOccur	This trap is sent when the BPDU attack happened on an interface. Binding objects: (1) ifIndex (2) esBpduProtectionIfCfgMode	1.3.6.1.4.1.17 1.17.47.0.1
esBpduProtectionAttackRecover	This trap is sent when the BPDU attack recovered on an interface. Binding objects: (1) ifIndex	1.3.6.1.4.1.17 1.17.47.0.2

CFM

Trap Name	Description	OID
dot1agCfmFaultAlarm	The trap is initiated when a connectivity defect is detected. Binding objects: (1) dot1agCfmMdIndex (2) dot1agCfmMaIndex (3) dot1agCfmMepIdentifier	1.3.111.2.802. 1.1.8.0.1

CFM Extension

Trap Name	Description	OID
dCfmAisOccurred	This trap is initiated when local MEP enters AIS status. Binding objects: (1) dCfmEventMdIndex (2) dCfmEventMaIndex (3) dCfmEventMepIdentifier	1.3.6.1.4.1.17 1.14.86.0.1

Trap Name	Description	OID
dCfmAisCleared	This trap is initiated when local MEP exits AIS status. Binding objects: (1) dCfmEventMdIndex (2) dCfmEventMaIndex (3) dCfmEventMepIdentifier	1.3.6.1.4.1.17 1.14.86.0.2
dCfmLockOccurred	This trap is initiated when local MEP enters lock status. Binding objects: (1) dCfmEventMdIndex (2) dCfmEventMaIndex (3) dCfmEventMepIdentifier	1.3.6.1.4.1.17 1.14.86.0.3
dCfmLockCleared	This trap is initiated when local MEP exits lock status. Binding objects: (1) dCfmEventMdIndex (2) dCfmEventMaIndex (3) dCfmEventMepIdentifier	1.3.6.1.4.1.17 1.14.86.0.4

DDM

Trap Name	Description	OID
esDdmAlarmTrap	A notification is generated when an abnormal alarm situation occurs or recovers from an abnormal alarm situation to normal status. Only when the current value> low warning or current value < high warning will send recover trap. Binding objects: (1) esDdmNotifyInfoIfIndex, (2) esDdmNotifyInfoComponent (3) esDdmNotifyInfoAbnormalLevel (4) esDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.17 1.17.72.0.1
esDdmWarningTrap	A notification is generated when an abnormal warning situation occurs or recovers from an abnormal warning situation to normal status. Binding objects: (1) esDdmNotifyInfoIfIndex, (2) esDdmNotifyInfoComponent (3) esDdmNotifyInfoAbnormalLevel (4) esDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.17 1.17.72.0.2

DHCP Server Screen Prevention

Trap Name	Description	OID
esDhcpFilterAttackDetected	When DHCP Server Screen is enabled, if the Switch received the forge DHCP Server packet, the Switch will trap the event if any attacking packet is received. Binding objects: (1) esDhcpFilterLogBufServerIpAddr	1.3.6.1.4.1.17 1.17.133.0.1

Trap Name	Description	OID
	(2) esDhcpFilterLogBufClientMacAddr (3) esDhcpFilterLogBufferVlanId (4) esDhcpFilterLogBufferOccurTime	

DoS Prevention

Trap Name	Description	OID
esDosPreveAttackDetectedPacket	The trap is sent when detect DOS attack. Binding objects: (1) esDoSPrevCtrlAttackType (2) esDosPrevNotiInfoDropIpAddr (3) esDosPrevNotiInfoDropPortNumber	1.3.6.1.4.1.17 1.17.59.0.2

ERPS

Trap Name	Description	OID
esErpsFailuredetectedNotif	A esErpsFailureNotification is sent when esErpsNotificationEnabled is 'true' and a signal failure is detected.	1.3.6.1.4.1.17 1.17.78.0.1
esErpsFailureClearedNotif	A esErpsFailureClearedNotif is sent when esErpsNotificationEnabled is 'true' and a signal failure is cleared.	1.3.6.1.4.1.17 1.17.78.0.2
esErpsRPLOwnerConflictNotif	A esErpsOwnerConflictNotif is sent when esErpsNotificationEnabled is 'true' and RPL owner conflict is detected	1.3.6.1.4.1.17 1.17.78.0.3

ErrDisable

Trap Name	Description	OID
esErrDisNotifyPortDisabledAssert	The trap is sent when a port enters into error disabled state. Binding objects: (1) esErrDisNotifyInfoPortIfIndex (2) esErrDisNotifyInfoReasonID	1.3.6.1.4.1.17 1.17.45.0.1
esErrDisNotifyPortDisabledClear	The trap is sent when a port loop restarts after the interval time. Binding objects: (1) esErrDisNotifyInfoPortIfIndex (2) esErrDisNotifyInfoReasonID	1.3.6.1.4.1.17 1.17.45.0.2
esErrDisNotifyVlanDisabledAssert	The trap is sent when a vlan enters into error disabled state. Binding objects: (1) esErrDisNotifyInfoPortIfIndex (2) esErrDisNotifyInfoReasonID (3) esErrDisNotifyInfoLoopDetectedVID	1.3.6.1.4.1.17 1.17.45.0.3

Trap Name	Description	OID
esErrDisNotifyVlanDisabledClear	The trap is sent when a vlan loop restarts after the interval time. Binding objects: (1) esErrDisNotifyInfoPortIfIndex (2) esErrDisNotifyInfoReasonID (3) esErrDisNotifyInfoLoopDetectedVID	1.3.6.1.4.1.17 1.17.45.0.4

Gratuitous ARP

Trap Name	Description	OID
esIpExtGratuitousARPTrap	The trap is sent when IP address conflicted. Binding objects: (1) esIpExtGratuitousARPIpAddr (2) esIpExtGratuitousARPMacAddr (3) esIpExtGratuitousARPPortNumber (4) esIpExtIfCfgIfIndex	1.3.6.1.4.1.17 1.17.75.0.1

IP-MAC-Port Binding

Trap Name	Description	OID
dImpbViolationTrap	The address violation notification is generated when IP-MAC-Port Binding address violation is detected. Binding objects: (1) ifIndex (2) dImpbViolationIpAddrType (3) dImpbViolationIpAddress (4) dImpbViolationMacAddress (5) dImpbViolationVlan	1.3.6.1.4.1.17 1.14.22.0.1

LACP

Trap Name	Description	OID
linkUp	A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus. Binding objects: (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1 .5.4
linkDown	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the	1.3.6.1.6.3.1.1 .5.3

Trap Name	Description	OID
	down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus. Binding objects: (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	

LBD

Trap Name	Description	OID
esLbdLoopOccurred	The trap is sent when a port loop occurs. Binding objects: (1) esLbdNotifyInfoIfIndex	1.3.6.1.4.1.17 1.17.46.0.1
esLbdLoopRestart	The trap is sent when a port loop restarts after the interval time. Binding objects: (1) esLbdNotifyInfoIfIndex	1.3.6.1.4.1.17 1.17.46.0.2
esLbdVlanLoopOccurred	The trap is sent when a port loop occurs under LBD VLAN-based mode. Binding objects: (1) esLbdNotifyInfoIfIndex (2) esLbdNotifyInfoVlanId	1.3.6.1.4.1.17 1.17.46.0.3
esLbdVlanLoopRestart	The trap is sent when a port loop restarts under LBD VLAN-based mode after the interval time. Binding objects: (1) esLbdNotifyInfoIfIndex (2) esLbdNotifyInfoVlanId	1.3.6.1.4.1.17 1.17.46.0.4

LLDP-MED

Trap Name	Description	OID
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
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	1.0.8808.1.1.2 .1.5.4795.0.1

Trap Name	Description	OID
	(2) lldpRemChassisId (3) lldpXMedRemDeviceClass	

MAC-based Access Control

Trap Name	Description	OID
esMacAuthLoggedSuccess	The trap is sent when a MAC-based Access Control host is successfully logged in. Binding objects: (1) ifIndex, (2) esnaSessionClientMacAddress (3) esnaSessionAuthVlan	1.3.6.1.4.1.17 1.17.153.0.1
esMacAuthLoggedFail	The trap is sent when a MAC-based Access Control host login fails. Binding objects: (1) ifIndex, (2) esnaSessionClientMacAddress (3) esnaSessionAuthVlan	1.3.6.1.4.1.17 1.17.153.0.2
esMacAuthLoggedAgesOut	The trap is sent when a MAC-based Access Control host ages out. Binding objects: (1) ifIndex, (2) esnaSessionClientMacAddress (3) esnaSessionAuthVlan	1.3.6.1.4.1.17 1.17.153.0.3

MAC Notification

Trap Name	Description	OID
dL2FdbMacNotification	This trap indicates the MAC addresses variation in the address table. Binding objects: (1) dL2FdbMac ChangeNotifyInfo	1.3.6.1.4.1.17 1.14.3.0.1
dL2FdbMacNotificationWithVID	This trap indicates the MAC addresses variation in the address table. Binding objects: (1) dL2FdbMacChangeNotifyInfoWithVID	1.3.6.1.4.1.17 1.14.3.0.2

MSTP

Trap Name	Description	OID
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,	1.3.6.1.2.1.17. 0.1

Trap Name	Description	OID
	immediately subsequent to its election. Implementation of this trap is optional.	
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 of this trap is optional	1.3.6.1.2.1.17.0.2

Peripheral

Trap Name	Description	OID
esEntityExtFanStatusChg	The commander Switch will send this notification when a fan fails (esEntityExtEnvFanStatus is 'fault') or recovers (esEntityExtEnvFanStatus is 'ok'). Binding objects: (1) esEntityExtEnvFanUnitId (2) esEntityExtEnvFanIndex (3) esEntityExtEnvFanStatus	1.3.6.1.4.1.171.17.5.0.1
esEntityExtThermalStatusChg	The commander Switch will send this notification when a thermal alarms (esEntityExtEnvTempStatus is 'abnormal') or recover (esEntityExtEnvTempStatus is 'ok'). Binding objects: (1) esEntityExtEnvTempUnitId (2) esEntityExtEnvTempIndex (3) esEntityExtEnvTempStatus	1.3.6.1.4.1.171.17.5.0.2
esEntityExtPowerStatusChg	The commander Switch will send this notification when a power module fails, recovers or is removed. Binding objects: (1) esEntityExtEnvPowerUnitId (2) esEntityExtEnvPowerIndex (3) esEntityExtEnvPowerStatus	1.3.6.1.4.1.171.17.5.0.3

PoE

Trap Name	Description	OID
pethMainPowerUsageOnNotification	This trap indicates PSE Threshold usage indication is on, the usage power is above the threshold. At least 500 msec must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethMainPseConsumptionPower	1.3.6.1.2.1.105.0.2
pethMainPowerUsageOffNotification	This trap indicates PSE Threshold usage indication is off, The usage power is below the threshold. At least 500 msec must elapse between notifications being emitted by the same object instance. Binding objects:	1.3.6.1.2.1.105.0.3

Trap Name	Description	OID
	(1) pethMainPseConsumptionPower	
esPoeIfPowerDeniedNotification	This Notification indicates if PSE state diagram enters the state POWER_DENIED. At least 500 msec must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethPsePortPowerDeniedCounter	1.3.6.1.4.1.17 1.17.24.0.1
esPoeIfPowerOverLoadNotification	This trap indicates if PSE state diagram enters the state ERROR_DELAY_OVER. At least 500 msec must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethPsePortOverLoadCounter	1.3.6.1.4.1.17 1.17.24.0.2
esPoeIfPowerShortCircuitNotification	This trap indicates if PSE state diagram enters the state ERROR_DELAY_SHORT. At least 500 msec must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethPsePortShortCounter	1.3.6.1.4.1.17 1.17.24.0.3

Port Security

Trap Name	Description	OID
esPortSecMacAddrViolation	When the port security trap is enabled, new MAC addresses that violate the pre-defined port security configuration will trigger trap messages to be sent out. Binding objects: (1) ifIndex, (2) esPortSecIfCurrentStatus (3) esPortSecIfViolationMacAddress	1.3.6.1.4.1.17 1.17.8.0.1

Port

Trap Name	Description	OID
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
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

RMON

Trap Name	Description	OID
risingAlarm	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps. Binding objects: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmRisingThreshold	1.3.6.1.2.1.16.0.1
fallingAlarm	The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps. Binding objects: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmFallingThreshold	1.3.6.1.2.1.16.0.2

Safeguard

Trap Name	Description	OID
esSafeguardChgToExhausted	This trap indicates System change operation mode from normal to exhaust. Binding objects: (1) esSafeguardEngineCurrentMode	1.3.6.1.4.1.171.17.19.1.1.0.1
esSafeguardChgToNormal	This trap indicates system change operation mode from exhausted to normal. Binding objects: (1) esSafeguardEngineCurrentMode	1.3.6.1.4.1.171.17.19.1.1.0.2

SIM

Trap Name	Description	OID
esSingleIPMSColdStart	The commander Switch will send this notification when its member generates a cold start notification. Binding objects: (1) esSingleIPMSMacAddr	1.3.6.1.4.1.171.17.225.0.0.11
esSingleIPMSWarmStart	The commander Switch will send this notification when its member generates a warm start notification. Binding objects: (1) esSingleIPMSMacAddr	1.3.6.1.4.1.171.17.225.0.0.12

Trap Name	Description	OID
esSingleIPMSLinkDown	The commander Switch will send this notification when its member generates a link down notification. Binding objects: (1) esSingleIPMSMacAddr (2) ifIndex	1.3.6.1.4.1.171.17.225.0.0.13
esSingleIPMSLinkUp	The commander Switch will send this notification when its member generates a link up notification. Binding objects: (1) esSingleIPMSMacAddr (2) ifIndex	1.3.6.1.4.1.171.17.225.0.0.14
esSingleIPMSAuthFail	The commander Switch will send this notification when its member generates an authentication failure notification. Binding objects: (1) esSingleIPMSMacAddr	1.3.6.1.4.1.171.17.225.0.0.15
esSingleIPMSnewRoot	The commander Switch will send this notification when its member generates a new root notification. Binding objects: (1) esSingleIPMSMacAddr	1.3.6.1.4.1.171.17.225.0.0.16
esSingleIPMSTopologyChange	The commander Switch will send this notification when its member generates a topology change notification. Binding objects: (1) esSingleIPMSMacAddr	1.3.6.1.4.1.171.17.225.0.0.17
esSingleIpMSrisingAlarm	The commander switch will send this notification to the indicated host when its member generates a rising alarm notification. (1) esSingleIpMSTrapMacAddr	1.3.6.1.4.1.171.17.225.0.0.18
esSingleIpMSfallingAlarm	The commander switch will send this notification to the indicated host when its member generates a falling alarm notification. (1) esSingleIpMSTrapMacAddr	1.3.6.1.4.1.171.17.225.0.0.19
esSingleIpMSmacNotification	The commander switch will send this notification to the indicated host when its member generates a MAC address variation notification. (1) esSingleIpMSTrapMacAddr (2) esSingleIpMSTrapMessage	1.3.6.1.4.1.171.17.225.0.0.20
esSingleIpMSPortTypeChange	The commander switch will send this notification to the indicated host when its member generates a port type change notification. (1) esSingleIpMSTrapMacAddr (2) ifIndex (3) esSingleIpMSTrapMessage	1.3.6.1.4.1.171.17.225.0.0.21
esSingleIpMSPowerStatusChg-	The commander switch will send this notification to the indicated host when its member generates a power status change notification. (1) esSingleIpMSTrapMacAddr (2) esSingleIpMSTrapMessage	1.3.6.1.4.1.171.17.225.0.0.22

Trap Name	Description	OID
esSingleIpMSPowerFailure	The commander switch will send this notification to the indicated host when its member generates a power failure notification. (1) esSingleIpMSTrapMacAddr (2) esSingleIpMSTrapMessage	1.3.6.1.4.1.17 1.17.225.0.0.2 3
esSingleIpMSPowerRecover	The commander switch will send this notification to the indicated host when its member generates a power recover notification. (1) esSingleIpMSTrapMacAddr (2) esSingleIpMSTrapMessage	1.3.6.1.4.1.17 1.17.225.0.0.2 4

Stacking

Trap Name	Description	OID
esStackTPChangeNotification	The stacking topology change notification. Binding objects: (1) esStackNotifyInfoTopologyType (2) esStackNotifyInfoBoxId (3) esStackInfoMacAddr	1.3.6.1.4.1.17 1.17.9.0.4

Start

Trap Name	Description	OID
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
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

Storm Control

Trap Name	Description	OID
esStormCtrlOccurred	This trap is sent when esStormCtrlNotifyEnable is 'stormOccurred' or 'both' and a storm is detected. Binding objects: (1) ifIndex, (2) esStormCtrlNotifyTrafficType	1.3.6.1.4.1.17 1.17.25.0.1
esStormCtrlStormCleared	This trap is sent when esStormCtrlNotifyEnable is 'stormCleared' or 'both' and a storm is cleared. Binding objects: (1) ifIndex, (2) esStormCtrlNotifyTrafficType	1.3.6.1.4.1.17 1.17.25.0.2

Trap Name	Description	OID
Note: Traps will be generated only if the control action is set to Shutdown for unicast traffic, including both known and unknown unicast traffic. Actions other than Shutdown such as Drop for unicast traffic will not generate traps.		

System File

Trap Name	Description	OID
dsfUploadImage	The notification is sent when the user uploads image file successfully.	1.3.6.1.4.1.17 1.14.14.0.1
dsfDownloadImage	The notification is sent when the user downloads image file successfully.	1.3.6.1.4.1.17 1.14.14.0.2
dsfUploadCfg	The notification is sent when the user uploads configuration file successfully.	1.3.6.1.4.1.17 1.14.14.0.3
dsfDownloadCfg	The notification is sent when the user downloads configuration file successfully.	1.3.6.1.4.1.17 1.14.14.0.4
dsfSaveCfg	The notification is sent when the user saves configuration file successfully.	1.3.6.1.4.1.17 1.14.14.0.5

Upload/Download

Trap Name	Description	OID
agentFirmwareUpgrade	This trap is sent when the process of upgrading the firmware via SNMP has finished. Binding objects: (1) swMultiImageVersion	1.3.6.1.4.1.17 1.12.1.7.2.0.7
agentCfgOperCompleteTrap	The trap is sent when the configuration is completely saved, uploaded or downloaded Binding objects: (1) unitID (2) agentCfgOperate (3) agentLoginUserName	1.3.6.1.4.1.17 1.12.1.7.2.0.9

VRRP

Trap Name	Description	OID
vrrpTrapNewMaster	The newMaster trap indicates that the sending agent has transitioned to 'Master' state. Binding objects: (1) vrrpOperMasterIpAddr	1.3.6.1.2.1.68. 0.1
vrrpTrapAuthFailure	A vrrpAuthFailure trap signifies that a packet has been received from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type. Implementation of this trap is optional. Binding objects:	1.3.6.1.2.1.68. 0.2

Trap Name	Description	OID
	(1) vrrpTrapPacketSrc (2) vrrpTrapAuthErrorType	

WAC

Trap Name	Description	OID
esWebAuthLoggedSuccess	The trap is sent when a host has successfully logged in (passed Web-Authentication). Binding objects: (1) ifIndex (2) esnaSessionAuthVlan (3) esnaSessionClientMacAddress (4) esnaSessionClientAddrType (5) esnaSessionClientAddress (6) esnaSessionAuthUserName	1.3.6.1.4.1.17 1.17.154.0.1
esWebAuthLoggedFail	The trap is sent when a host has failed to pass Web-Authentication (login failed). Binding objects: (1) ifIndex (2) esnaSessionAuthVlan (3) esnaSessionClientMacAddress (4) esnaSessionClientAddrType (5) esnaSessionClientAddress (6) esnaSessionAuthUserName	1.3.6.1.4.1.17 1.17.154.0.2

Appendix D - RADIUS Attributes Assignment

The RADIUS Attributes Assignment on the Switch is used in the following modules: Console, Telnet, SSH, Web, 802.1X, MAC-based Access Control, and WAC.

The description that follows explains the following RADIUS Attributes Assignment types:

- Privilege Level
- Ingress/Egress Bandwidth
- 802.1p Default Priority
- VLAN
- ACL

To assign the **Privilege Level** by the RADIUS server, the proper parameters should be configured on the RADIUS server. The table below shows the parameters for the bandwidth.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	1	Required
Attribute-Specific Field	Used to assign the privilege level of the user to operate the Switch.	Range (1-15)	Required

If the user has configured the privilege level attribute of the RADIUS server (for example, level 15) and the Console, Telnet, SSH, and Web authentication is successful, the device will assign the privilege level (according to the RADIUS server) to this access user. However, if the user does not configure the privilege level attribute and authenticates successfully, the device will not assign any privilege level to the access user. If the privilege level is configured less than the minimum supported value or greater than the maximum supported value, the privilege level will be ignored.

To assign the **Ingress/Egress Bandwidth** by the RADIUS server, the proper parameters should be configured on the RADIUS Server. The table below shows the parameters for bandwidth.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	2 (for ingress bandwidth) 3 (for egress bandwidth)	Required
Attribute-Specific Field	Used to assign the bandwidth of a port.	Unit (Kbits)	Required

If the user has configured the bandwidth attribute of the RADIUS server (for example, ingress bandwidth 1000Kbps) and 802.1X authentication is successful, the device will assign the bandwidth (according to the RADIUS server) to the port. However, if the user does not configure the bandwidth attribute and authenticates successfully, the device will not assign any bandwidth to the port. If the bandwidth attribute is configured on the RADIUS server with a value of “0”,

the effective bandwidth will be set “no_limited”, and if the bandwidth is configured less than “0” or greater than maximum supported value, the bandwidth will be ignored.

To assign the **802.1p Default Priority** by the RADIUS server, the proper parameters should be configured on the RADIUS server. The table below shows the parameters for 802.1p default priority.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	4	Required
Attribute-Specific Field	Used to assign the 802.1p default priority of the port.	0 to 7	Required

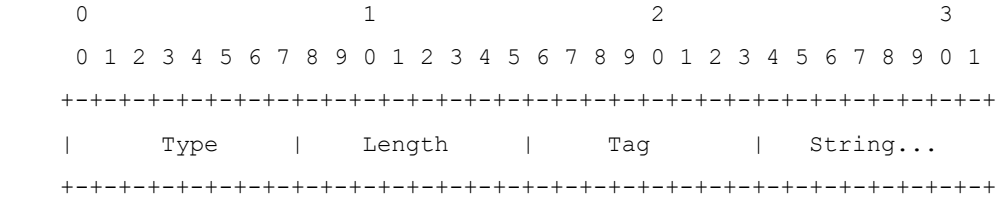
If the user has configured the 802.1p priority attribute of the RADIUS server (for example, priority 7) and the 802.1X, or MAC based authentication is successful, the device will assign the 802.1p default priority (according to the RADIUS server) to the port. However, if the user does not configure the priority attribute and authenticates successfully, the device will not assign a priority to this port. If the priority attribute is configured on the RADIUS server is a value out of range (>7), it will not be set to the device.

To assign the **VLAN** by the RADIUS server, the proper parameters should be configured on the RADIUS server. To use VLAN assignment, RFC 3580 defines the following tunnel attributes in RADIUS packets.

The table below shows the parameters for a VLAN:

RADIUS Tunnel Attribute	Description	Value	Usage
Tunnel-Type	This attribute indicates the tunneling protocol(s) to be used (in the case of a tunnel initiator) or the tunneling protocol in use (in the case of a tunnel terminator).	13 (VLAN)	Required
Tunnel-Medium-Type	This attribute indicates the transport medium being used.	6 (802)	Required
Tunnel-Private-Group-ID	This attribute indicates group ID for a particular tunneled session.	A string (VID)	Required

A summary of the Tunnel-Private-Group-ID Attribute format is shown below.



The table below shows the definition of Tag field (different with RFC 2868):

Tag field value	String field format
0x01	VLAN name (ASCII)
0x02	VLAN ID (ASCII)

Tag field value	String field format
Others (0x00, 0x03 ~ 0x1F, >0x1F)	When the Switch receives the VLAN setting string, it will think it is the VLAN ID first. In other words, the Switch will check all existing VLAN IDs and check if there is one matched. If the Switch can find one matched, it will move to that VLAN. If the Switch cannot find the matched VLAN ID, it will think the VLAN setting string as a “VLAN Name”. Then it will check that it can find out a matched VLAN Name.



NOTE: A tag field of greater than 0x1F is interpreted as the first octet of the following field.

If the user has configured the VLAN attribute of the RADIUS server (for example, VID 3) and the 802.1X, or MAC based Access Control, or WAC authentication is successful, the port will be assigned to VLAN 3. However if the user does not configure the VLAN attributes, when the port is not guest VLAN member, it will be kept in its current authentication VLAN, and when the port is guest VLAN member, it will be assigned to its original VLAN.

To assign the **ACL** by the RADIUS server, the proper parameters should be configured on the RADIUS server. The table below shows the parameters for an ACL.

The parameters of the Vendor-Specific Attribute are:

RADIUS Tunnel Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	14 (for ACL script)	Required
Attribute-Specific Field	Used to assign the ACL script. The format is based on Access Control List (ACL) Commands.	ACL Script For example: ip access-list a1;permit host 10.90.90.100;exit; mac access-list extended m1;permit host 00-00-00-01-90-10 any; exit;	Required

If the user has configured the ACL attribute of the RADIUS server (for example, ACL script: ip access-list a1;permit host 10.90.90.100;exit; mac access-list extended m1;permit host 00-00-00-01-90-10 any; exit;), and the 802.1X or MAC-based Access Control WAC is successful, the device will assign the ACL script according to the RADIUS server. The enter **Access-List Configuration Mode** and exit **Access-List Configuration Mode** must be a pair, otherwise the ACP script will be reject. For more information about the ACL module, please refer to **Access Control List (ACL) Commands** chapter.

Appendix E - IETF RADIUS Attributes Support

Remote Authentication Dial-In User Service (RADIUS) attributes carry specific authentication, authorization, information and configuration details for the request and reply. This appendix lists the RADIUS attributes currently supported by the Switch.

RADIUS attributes are supported by the IETF standard and Vendor-Specific Attribute (VSA). VSA allows the vendor to create an additionally owned RADIUS attribute. For more information about D-Link VSA, refer to the **RADIUS Attributes Assignment** Appendix.

IETF standard RADIUS attributes are defined in the RFC 2865 Remote Authentication Dial-In User Service (RADIUS), RFC 2866 RADIUS Accounting, RFC 2868 RADIUS Attributes for Tunnel Protocol Support, and RFC 2869 RADIUS Extensions.

The following table lists the IETF RADIUS attributes supported by the D-Link Switch.

RADIUS Authentication Attributes:

Number	IETF Attribute
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
7	Framed-Protocol
8	Framed-IP-Address
12	Framed-MTU
18	Reply-Message
24	State
26	Vendor-Specific
27	Session-Timeout
29	Termination-Action
30	Called-Station-ID
31	Calling-Station-ID
32	NAS-Identifier
60	CHAP-Challenge
61	NAS-Port-Type
64	Tunnel-Type
65	Tunnel-Medium-Type
77	Connect-Info
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID
85	Acct-Interim-Interval

Number	IETF Attribute
87	NAS-Port-ID
95	NAS-IPv6-Address

RADIUS Accounting Attributes:

Number	IETF Attribute
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
8	Framed-IP-Address
31	Calling-Station-ID
32	NAS-Identifier
40	Acct-Status-Type
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-ID
45	Acct-Authentic
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
49	Acct-Terminate-Cause
52	Acct-Input-Gigawords
53	Acct-Output-Gigawords
61	NAS-Port-Type
95	NAS-IPv6-Address