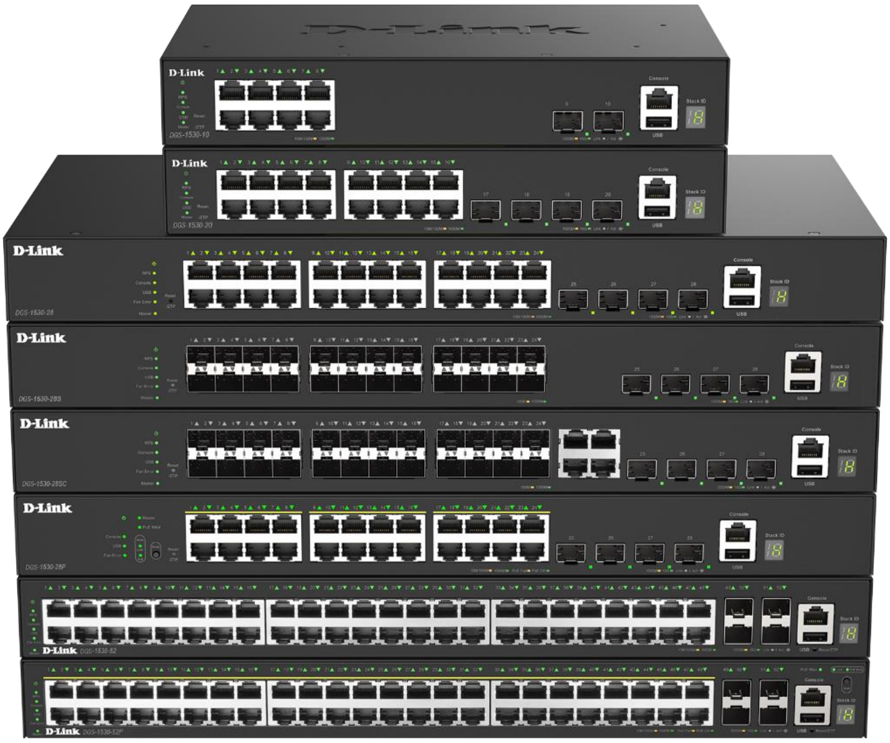
Version 1.00 | 2024/09/24



Web UI Reference Guide

Smart Managed Switch

DGS-1530 Series

FCC Compliance Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CE Mark Warning

This equipment is compliant with Class A of CISPR 32. In a residential environment, this equipment may cause radio interference.

Avertissement Concernant la Marque CE

Cet équipement est conforme à la classe A de la norme CISPR 32. Dans un environnement résidentiel, cet équipement peut provoquer des interférences radio.

VCCI Warning

この装置は、クラスA機器です。この装置を住宅環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

BSMI Notice

警告: 為避免電磁干擾，本產品不應安裝或使用於住宅環境。

Safety Compliance

Warning: Class 1 Laser Product: When using a fiber optic media expansion module, never look at the transmit laser while it is powered on. In addition, never look directly at the fiber TX port and fiber cable ends when they are powered on.

Avertissement: Produit Laser de Classe 1: Ne regardez jamais le laser tant qu’il est sous tension. Ne regardez jamais directement le port TX (Transmission) à fibres optiques et les embouts de câbles à fibres optiques tant qu’ils sont sous tension.

Table of Contents

1. Introduction 1
Audience 1
Other Documentation 1
Typographical Conventions 1
Notes and Cautions 1
2. Web User Interface (Web UI) 2
Connecting to the Web UI 2
Logging into the Web UI 2
Smart Wizard 3
Step 1 - System IP Information 3
Step 2 - User Accounts Settings 4
Step 3 - SNMP Settings 5
Web Interface Navigation 6
3. System 7
Device Information 7
System Information Settings 7
Peripheral Settings 8
Port Configuration 9
Port Settings 9
Port Status 11
Port GBIC 11
Port Auto Negotiation 12
Error Disable Settings 13
Jumbo Frame 14
Interface Description 15
Loopback Test 15
PoE 16
PoE System 16
PoE Status 17
PoE Configuration 18
PD Alive 19
PoE Statistics 20
PoE Measurement 21
PoE LLDP Classification 22
System Log 23
System Log Settings 23
System Log Discriminator Settings 25
System Log Server Settings 26
System Log 27
System Attack Log 28
Time and SNTP 28
Clock Settings 28
Time Zone Settings 29
SNTP Settings 31
Time Range 32
PTP (Precise Time Protocol) 32
PTP Global Settings 33
PTP Port Global Settings 34
Reset Button Settings 34

Archive Settings 35

4. Management 36

Command Logging 36

User Accounts Settings 36

Password Encryption 38

Password Recovery 38

Login Method 39

Web Login Lock Settings 40

SNMP 41

SNMP Global Settings 42

SNMP Linkchange Trap Settings 43

SNMP View Table Settings 44

SNMP Community Table Settings 45

SNMP Group Table Settings 46

SNMP Engine ID Local Settings 47

SNMP User Table Settings 47

SNMP Host Table Settings 49

RMON 50

RMON Global Settings 50

RMON Statistics Settings 50

RMON History Settings 51

RMON Alarm Settings 52

RMON Event Settings 53

Telnet/Web 54

Session Timeout 54

DHCP 55

Service DHCP 55

DHCP Class Settings 56

DHCP Pool Settings 57

DHCP Server 57

DHCPv6 Server 66

DHCP Relay 72

DHCPv6 Relay 77

DHCP Auto Configuration 87

DHCP Auto Image Settings 87

DNS 88

DNS Global Settings 88

DNS Name Server Settings 89

DNS Host Settings 90

NTP 90

NTP Global Settings 90

NTP Server Settings 92

NTP Peer Settings 92

NTP Access Group Settings 93

NTP Key Settings 94

NTP Interface Settings 95

NTP Associations 96

NTP Status 97

File System 98

Stacking 100

Physical Stacking 104

Stacking Bandwidth 105

Virtual Stacking (SIM) ... 106
Single IP Settings ... 108
Topology ... 109
Firmware Upgrade ... 114
Configuration File Backup/Restore ... 114
Upload Log File ... 115
D-Link Discovery Protocol ... 115
DDP Settings ... 115
DDP Neighbors ... 116
SMTP Settings ... 117
Reboot Schedule Settings ... 119
NLB FDB Settings ... 119
PPPoE Circuit ID Insertion Settings ... 120
TCP Path MTU Discovery ... 121
TCP Selective ACK ... 122
TWAMP ... 122
TWAMP Settings ... 122
TWAMP Server Connections ... 123
TWAMP Server Sessions ... 123
5. Layer 2 Features ... 124
FDB ... 124
Static FDB ... 124
MAC Address Table Settings ... 125
MAC Address Table ... 127
MAC Notification ... 128
VLAN ... 129
VLAN Configuration Wizard ... 129
802.1Q VLAN ... 132
VLAN Interface ... 133
802.1v Protocol VLAN ... 135
GVRP ... 137
Asymmetric VLAN ... 140
MAC VLAN ... 141
L2VLAN Interface Description ... 141
Auto Surveillance VLAN ... 142
Voice VLAN ... 144
Private VLAN ... 148
VLAN Tunnel ... 149
Dot1q Tunnel ... 149
VLAN Mapping ... 150
VLAN Mapping Profile ... 152
STP ... 156
STP Global Settings ... 158
STP Port Settings ... 160
MST Configuration Identification ... 161
STP Instance ... 162
MSTP Port Information ... 163
ERPS (G.8032) ... 163
ERPS ... 163
ERPS Profile ... 168
Loopback Detection ... 169
Link Aggregation ... 171

Flex Links 174
L2 Protocol Tunnel 174
L2 Multicast Control 176
IGMP Snooping 176
MLD Snooping 186
Multicast VLAN 196
Multicast Filtering Mode 200
LLDP 201
LLDP Global Settings 201
LLDP Port Settings 203
LLDP Management Address List 204
LLDP Basic TLVs Settings 204
LLDP Dot1 TLVs Settings 205
LLDP Dot3 TLVs Settings 206
LLDP-MED Port Settings 207
LLDP Statistics Information 208
LLDP Local Port Information 209
LLDP Neighbor Port Information 210

6. Layer 3 Features 213
ARP 213
ARP Aging Time 213
Static ARP 213
Proxy ARP 214
ARP Table 215
Gratuitous ARP 215
IPv6 Neighbor 217
Interface 217
IPv4 Interface 217
IPv6 Interface 220
Loopback Interface 224
Null Interface 225
UDP Helper 226
IP Forward Protocol 226
IP Helper Address 226
IPv4 Static/Default Route 227
IPv4 Route Table 228
IPv6 Static/Default Route 229
IPv6 Route Table 230
IPv6 General Prefix 231
IP Multicast Routing Protocol 231
IPMC 231
IPv6MC 234

7. Quality of Service (QoS) 235
Basic Settings 235
Port Default CoS 235
Scheduler Method 236
Queue Settings 237
CoS to Queue Mapping 238
Port Rate Limiting 238
Queue Rate Limiting 239
Advanced Settings 240
DSCP Mutation Map 240

Port Trust State 241
DSCP CoS Mapping 242
CoS Color Mapping 242
DSCP Color Mapping 243
Class Map 243
Aggregate Policer 245
Policy Map 248
Policy Binding 251
8. Access Control List (ACL) 253
ACL Configuration Wizard 253
Step 1 - Create/Update 253
Step 2 - Select Packet Type 254
Step 3 - Add Rule 255
Step 4 - Apply Port 266
ACL Access List 267
Standard IP ACL 269
Extended IP ACL 270
Standard IPv6 ACL 272
Extended IPv6 ACL 273
Extended MAC ACL 275
Extended Expert ACL 277
Extended UDF ACL 280
ACL Interface Access Group 281
ACL VLAN Access Map 282
ACL VLAN Filter 284
CPU ACL 284
9. Security 288
Port Security 288
Port Security Global Settings 288
Port Security Port Settings 289
Port Security Address Entries 290
802.1X 291
802.1X Global Settings 295
802.1X Port Settings 296
Authentication Sessions Information 297
Authenticator Statistics 297
Authenticator Session Statistics 298
Authenticator Diagnostics 299
AAA 300
AAA Global Settings 300
Application Authentication Settings 301
Application Accounting Settings 302
Authentication Settings 303
Accounting Settings 306
Server RADIUS Dynamic Author Settings 308
RADIUS 309
RADIUS Global Settings 309
RADIUS Server Settings 310
RADIUS Group Server Settings 311
RADIUS Statistic 312
TACACS+ 313
TACACS+ Server Settings 313

TACACS+ Group Server Settings....314
TACACS+ Statistic....315
IMPB....315
IPv4....315
IPv6....330
DHCP Server Screening....338
DHCP Server Screening Global Settings....338
DHCP Server Screening Port Settings....340
ARP Spoofing Prevention....340
BPDU Attack Protection....341
NetBIOS Filtering....343
MAC Authentication....343
Web-based Access Control....345
Web Authentication....347
WAC Port Settings....348
WAC Customize Page....349
Network Access Authentication....350
Guest VLAN....350
Network Access Authentication Global Settings....351
Network Access Authentication Port Settings....353
Network Access Authentication Sessions Information....354
Safeguard Engine....355
Safeguard Engine Settings....356
CPU Protect Counters....357
CPU Protect Sub-Interface....357
CPU Protect Type....358
Trusted Host....359
Traffic Segmentation Settings....359
Storm Control Settings....360
DoS Attack Prevention Settings....362
SSH....364
SSH Global Settings....364
SSH Algorithm Settings....365
Host Key....366
SSH Server Connection....367
SSH User Settings....367
SSH Client Settings....368
SSL....368
SSL Global Settings....369
Crypto PKI Trustpoint....370
SSL Service Policy....371
Network Protocol Port Protection Settings....372
10. OAM....373
CFM....373
CFM Settings....373
CFM Port Settings....380
CFM Loopback Test....381
CFM Linktrace Settings....382
CFM Packet Counter....383
CFM Counter CCM....384
CFM MIP CCM Table....384
CFM MEP Fault Table....385

Cable Diagnostics ... 385
Ethernet OAM ... 386
Ethernet OAM Settings ... 386
Ethernet OAM Configuration Settings ... 388
Ethernet OAM Event Log Table ... 390
Ethernet OAM Statistics Table ... 391
Ethernet OAM DULD Settings ... 391
DDM ... 393
DDM Settings ... 393
DDM Temperature Threshold Settings ... 394
DDM Voltage Threshold Settings ... 395
DDM Bias Current Threshold Settings ... 395
DDM TX Power Threshold Settings ... 396
DDM RX Power Threshold Settings ... 397
DDM Status Table ... 398
11. Monitoring ... 399
VLAN Counter ... 399
Utilization ... 400
Port Utilization ... 400
History Utilization ... 401
Statistics ... 402
Port ... 402
CPU Port ... 404
Interface Counters ... 405
Interface History Counters ... 407
Counters ... 408
Mirror Settings ... 409
sFlow ... 412
sFlow Agent Information ... 412
sFlow Receiver Settings ... 412
sFlow Sampler Settings ... 413
sFlow Poller Settings ... 414
Device Environment ... 415
12. Green ... 416
Power Saving ... 416
EEE ... 417
13. Toolbar ... 419
Save ... 419
Save Configuration ... 419
Tools ... 419
Firmware Upgrade & Backup ... 419
Configuration Restore & Backup ... 426
Certificate & Key Restore & Backup ... 434
Log Backup ... 441
Ping ... 444
Trace Route ... 446
Language Management ... 448
Reset ... 448
Reboot System ... 449
Language ... 449
Logout ... 449

Appendix A - Password Recovery Procedure..450

Appendix B - System Log Entries 451

Appendix C - Trap Entries 484

Appendix D - RADIUS Attributes Assignment 497

Appendix E - IETF RADIUS Attributes Support 502

1. Introduction

Audience

The *Web UI Reference Guide* 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 switches in the DGS-1530 Series, which will be generally be referred to simply as the '*Switch*' within this manual. This manual is written in a way that assumes readers already have the experience and knowledge of Ethernet and modern networking principles for Local Area Networks (LANs).

Other Documentation

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

- *DGS-1530 Series Hardware Installation Guide*
- *DGS-1530 Series CLI Reference Guide*

Typographical Conventions

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**. 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	Used to represent an example of a screen console display including example entries of CLI command input with the corresponding output.

Notes and Cautions

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

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

ATTENTION : Une précaution indique un risque de dommage matériel, de blessure corporelle ou de mort.

2. Web User Interface (Web UI)

The Web UI, which offers a more graphical interface, grants access to the majority of the software features present on the Switch. These features can be enabled, configured, disabled, or monitored through any standard web browser, such as Microsoft's Internet Explorer, Mozilla Firefox, Google Chrome, or Safari. The LAN ports provide an in-band connection to the Web UI using HTTP or HTTPS (SSL).

The Web UI examples in this guide was capture using the **Microsoft Edge** browser.

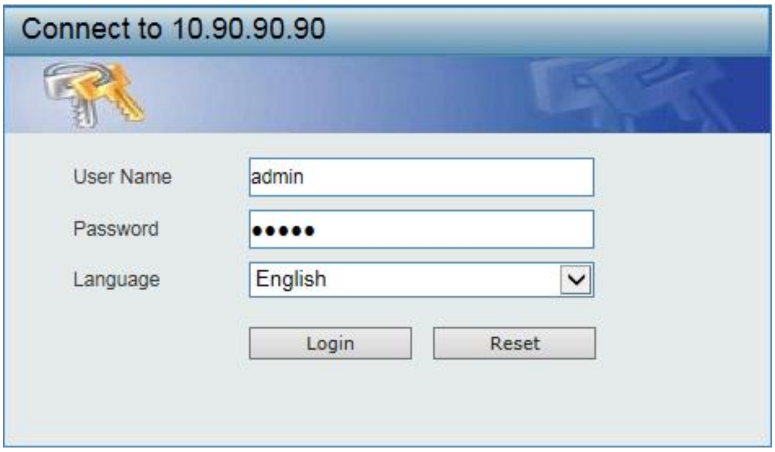
Connecting to the Web UI

By default, **Secure HTTP (https)** access is available to the Switch. To access the Web UI, open a standard web browser and enter **https://** followed by the IP address of the Switch into the address bar of the browser. Press the **Enter** key. For example, **https://10.90.90.90**.

NOTE: The default IP address of the Switch is ***10.90.90.90*** (subnet mask *255.0.0.0*).
The default username and password is ***admin***.

Logging into the Web UI

Enter the **User Name** and **Password** and click the **Login** button.



Connect to 10.90.90.90

User Name: admin

Password: ●●●●●

Language: English

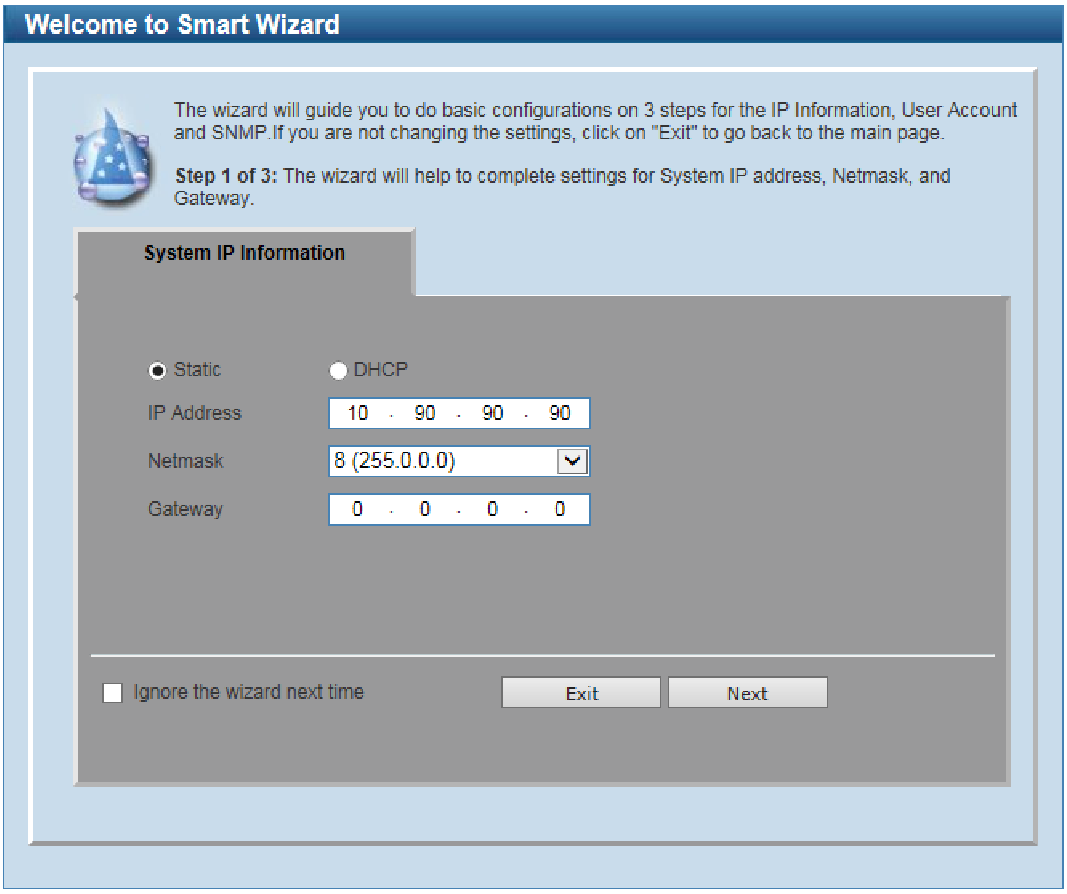
Figure 2-1 Web UI Login Window

Smart Wizard

After successfully logging into the web UI, the Smart Wizard embedded Web Utility will be launched.

Step 1 - System IP Information

In this step, we can configure System IP Information.



Welcome to Smart Wizard

The wizard will guide you to do basic configurations on 3 steps for the IP Information, User Account and SNMP.If you are not changing the settings, click on "Exit" to go back to the main page.

Step 1 of 3: The wizard will help to complete settings for System IP address, Netmask, and Gateway.

System IP Information

● Static ○ DHCP

IP Address: 10 . 90 . 90 . 90

Netmask: 8 (255.0.0.0)

Gateway: 0 . 0 . 0 . 0

□ Ignore the wizard next time

Figure 2-2 System IP Information Window

The fields that can be configured are described below:

Parameter	Description
Static	Select this option to manually assign and configure the IP address settings for the Switch. After selecting this option, the following parameters can be configured: • **IP Address** - Enter the IP address of the Switch here. • **Netmask** - Select the Netmask option here. • **Gateway** - Enter the IP address of the default gateway here.
DHCP	Select this option to obtain IP address settings automatically from a DHCP server for the Switch.

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

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

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

Step 2 - User Accounts Settings

In this step, we can configure the user account settings. This step can only be modified by a user account with the privilege level of 15.

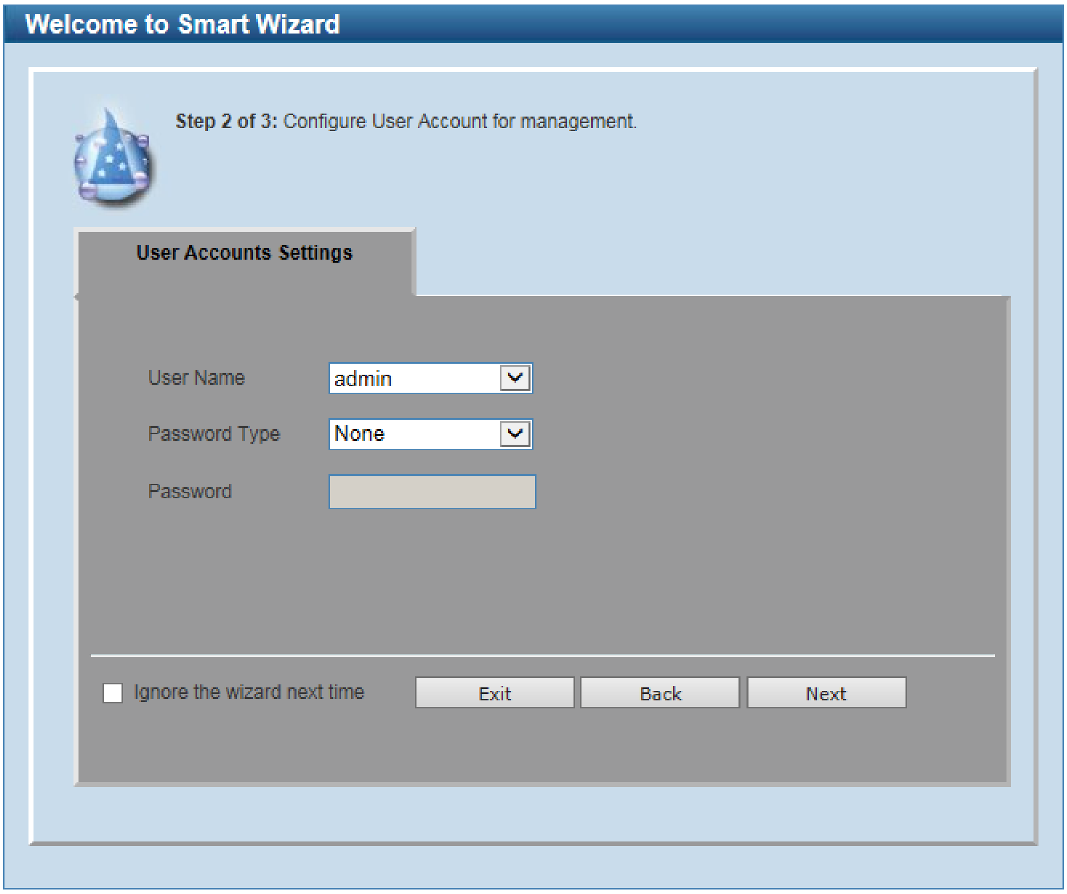


Figure 2-3 User Accounts Settings Window

The fields that can be configured are described below:

Parameter	Description
User Name	Select the user name here. This is normally an administrator-level account with the privilege level of 15.
Password Type	Select the password type here. Options to choose from are: • **None** - The password for the user account remains the same. • **Plain Text** - The password for the user account is in the plain text form. • **Encrypted-SHA1** - The password for the user account is in the encrypted form using the SHA1 encryption method. • **Encrypted-MD5** - The password for the user account is in the encrypted form using the MD5 encryption method.
Password	Enter the password for the user account either in the plain text format or the encrypted format here based on the previous selection made. In the encrypted format, the password will not be encrypted from plain text to the encrypted format. Instead, the encrypted password must be entered.

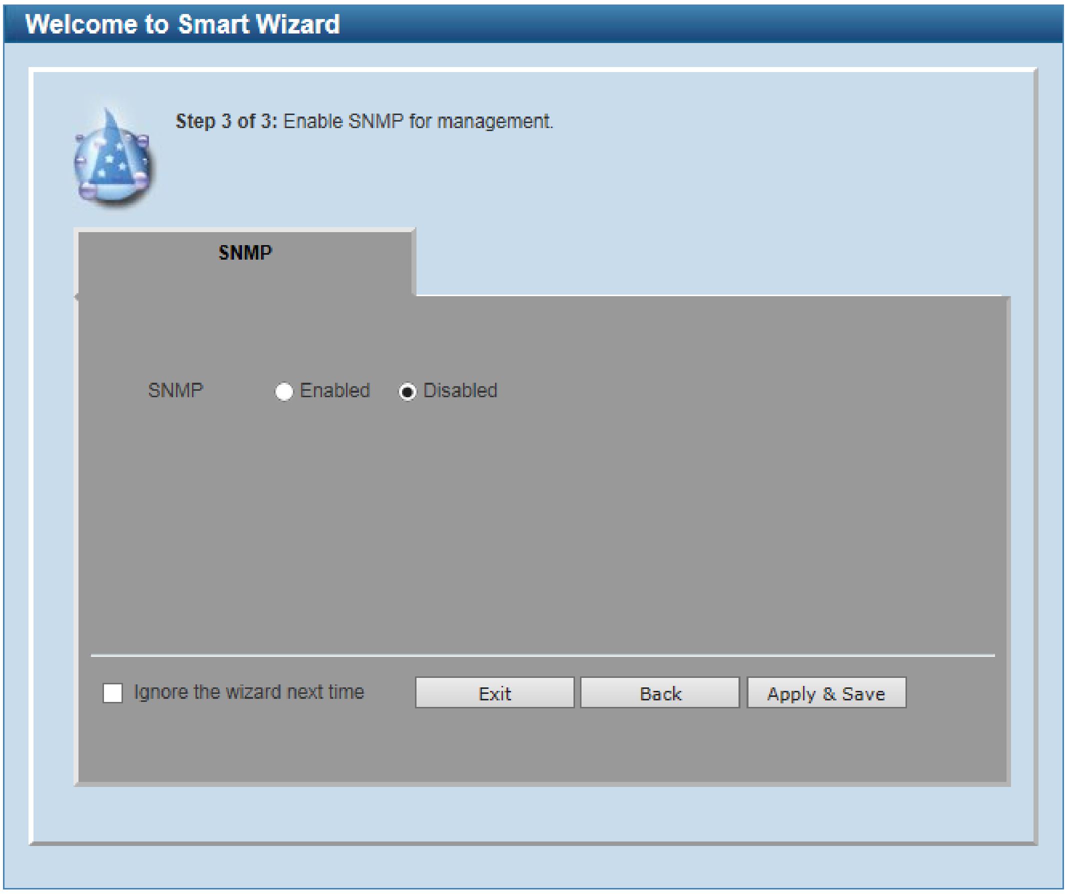
Tick the **Ignore the wizard next time** option to skip the Smart Wizard on the next login.

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

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

Step 3 - SNMP Settings

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



Step 3 of 3: Enable SNMP for management.

SNMP ○ Enabled ● Disabled

□ Ignore the wizard next time

Figure 2-4 SNMP Window

The fields that can be configured are described below:

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

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

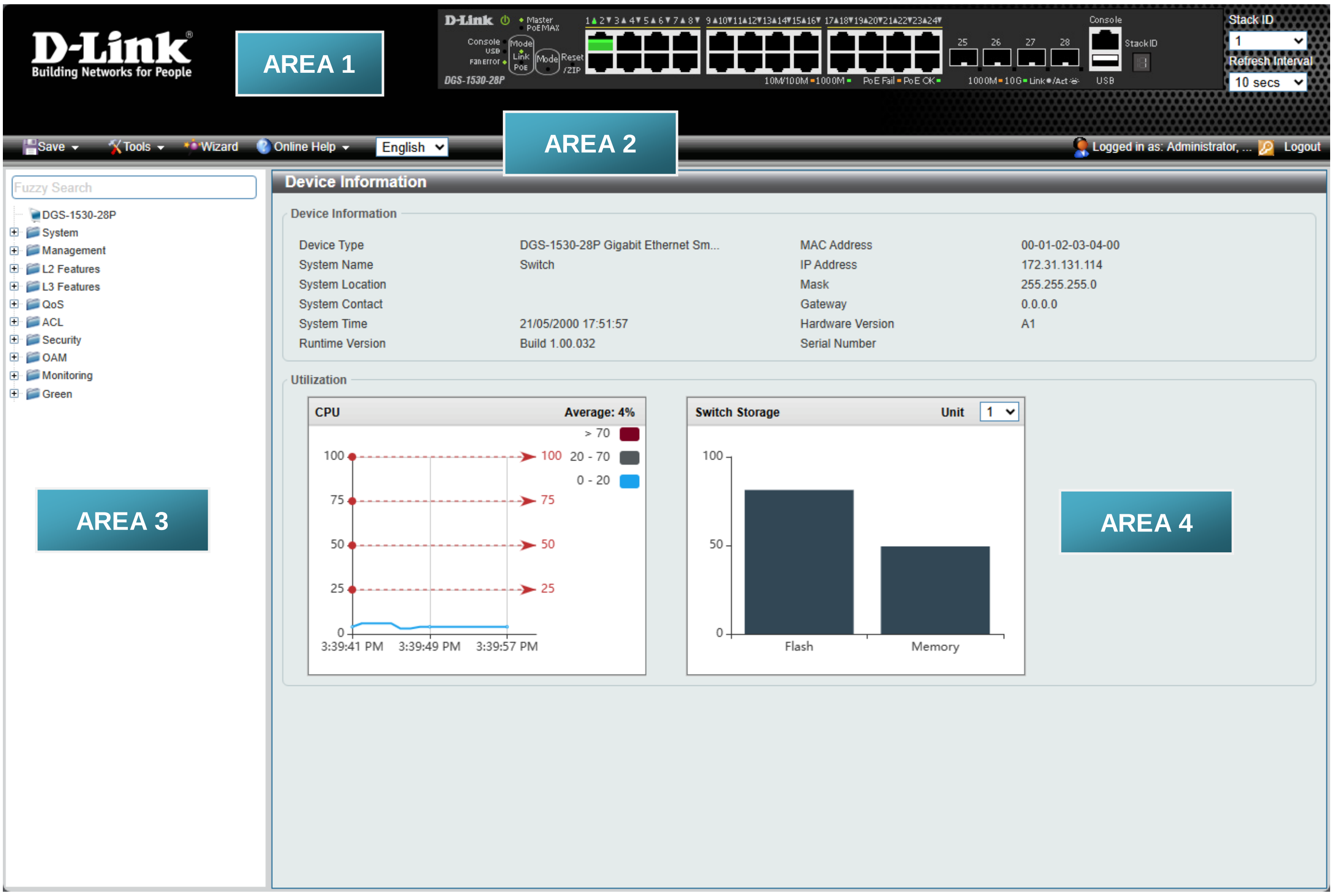
Click the **Exit** button to discard the changes made, exit the Smart Wizard, and continue to the Web UI.

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

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

Web Interface Navigation

After accessing the Web UI, the following will be displayed:



Device Information

Device Information

Device Type	DGS-1530-28P Gigabit Ethernet Sm...	MAC Address	00-01-02-03-04-00
System Name	Switch	IP Address	172.31.131.114
System Location		Mask	255.255.255.0
System Contact		Gateway	0.0.0.0
System Time	21/05/2000 17:51:57	Hardware Version	A1
Runtime Version	Build 1.00.032	Serial Number	

Utilization

Figure 2-5 Web User Interface Areas

Area Number	Description
AREA 1	In this area, a graphical near real-time image of the front panel of the Switch is displayed with ports and expansion modules. Some management functions like port monitoring are also accessible here. Click the D-Link logo to go to the D-Link website.
AREA 2	In this area, a toolbar is used to access functions like **Save**, **Tools**, **Wizard**, customized **Language** preference, and a **Logout** option. The user account and IP address, currently accessing the Web UI, is displayed on the right in this toolbar.
AREA 3	In this area, the software features available in the Web UI are grouped into folders containing hyperlinks that will open window frames in Area 4. There is also a search option in this area that can be used to search for specific feature keywords in the Web UI to easily find the link to the set of features.
AREA 4	In this area, configuration and monitoring window frames are available based on the selections made in Area 3.

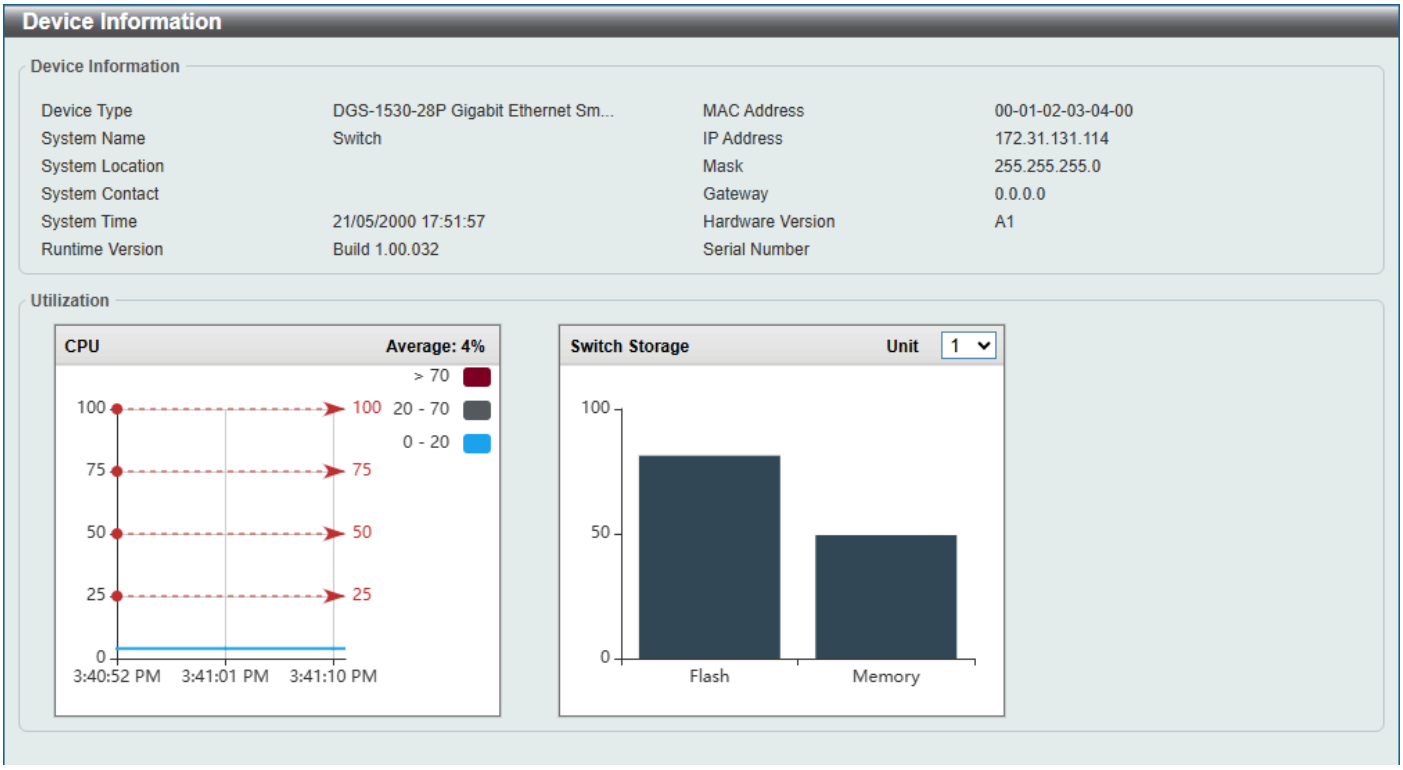
NOTE: The best screen resolution for viewing the Web UI is 1280 x 1024 pixels.

3. System

Device Information

In the Device Information section, the user can view a list of basic information regarding the Switch. It appears automatically when you log on to the Switch.

To return to the Device Information window after viewing other windows, click the **DGS-1530-28P** link.



Device Information

Device Information

Device Type	DGS-1530-28P Gigabit Ethernet Sm...	MAC Address	00-01-02-03-04-00
System Name	Switch	IP Address	172.31.131.114
System Location		Mask	255.255.255.0
System Contact		Gateway	0.0.0.0
System Time	21/05/2000 17:51:57	Hardware Version	A1
Runtime Version	Build 1.00.032	Serial Number	

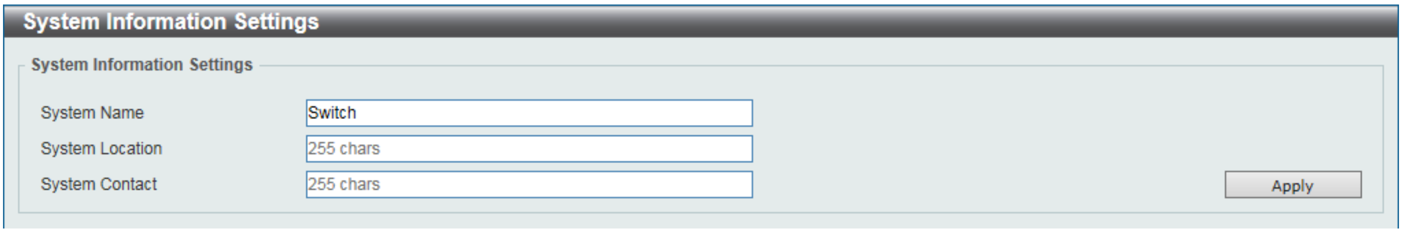
Utilization

Figure 3-1 Device Information Window

System Information Settings

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

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



System Information Settings

System Information Settings

System Name	Switch
System Location	255 chars
System Contact	255 chars

Figure 3-2 System Information Settings Window

The fields that can be configured 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.

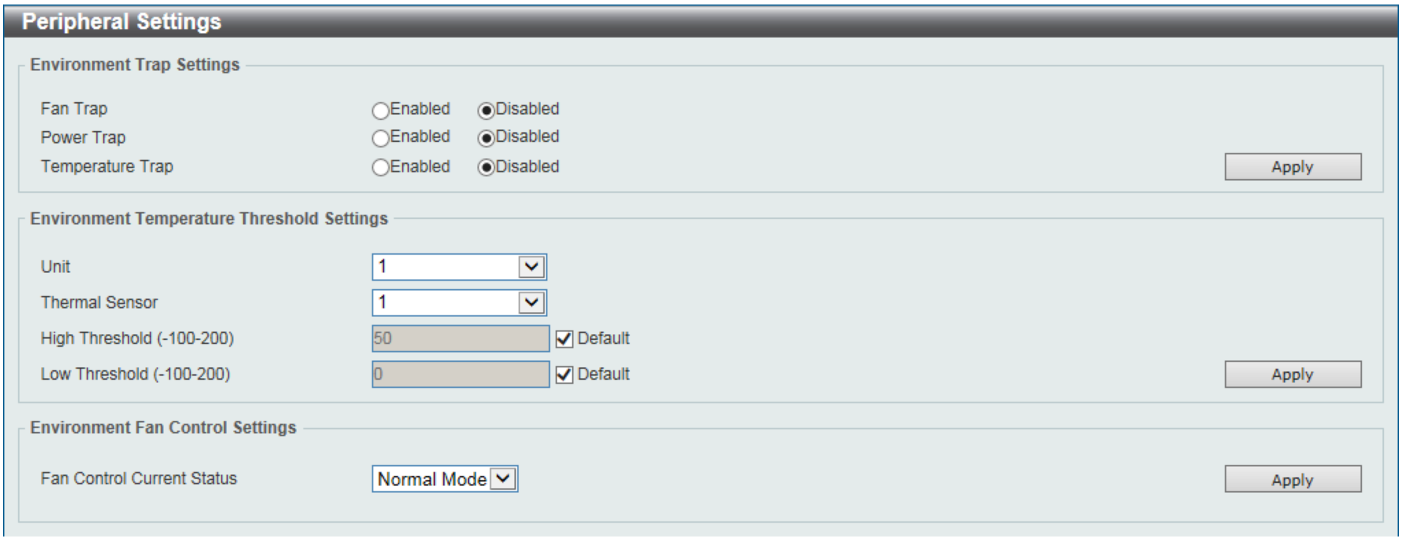
Parameter	Description
System Contact	Enter a contact name for the Switch, if so desired.

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

Peripheral Settings

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

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



Peripheral Settings

Environment Trap Settings

Fan Trap ○Enabled ●Disabled

Power Trap ○Enabled ●Disabled

Temperature Trap ○Enabled ●Disabled

Apply

Environment Temperature Threshold Settings

Unit 1

Thermal Sensor 1

High Threshold (-100-200) 50 ☑ Default

Low Threshold (-100-200) 0 ☑ Default

Apply

Environment Fan Control Settings

Fan Control Current Status Normal Mode

Apply

Figure 3-3 Peripheral Settings Window

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

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

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

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

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
Thermal	Select the thermal sensor ID.
High Threshold	Enter the high threshold value of the warning temperature setting. The range is from -100 to 200 degrees Celsius. Select the **Default** option to use the default value.
Low Threshold	Enter the low threshold value of the warning temperature setting. The range is from -100 to 200 degrees Celsius. Select the **Default** option to use the default value.

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

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

Parameter	Description
Fan Control Current State	Select the state for the fan. Options to choose from are **Normal Mode** and **Quiet Mode**.

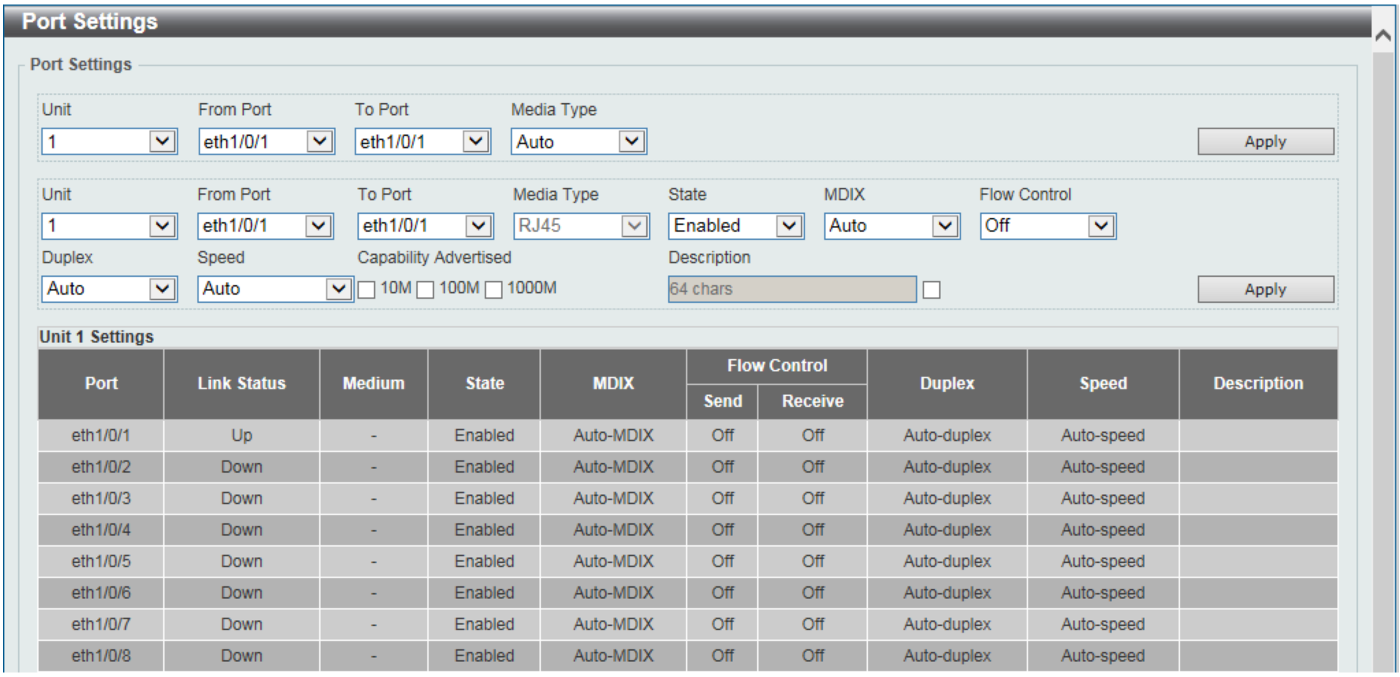
Click the **Apply** button to accept the changes made.

Port Configuration

Port Settings

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

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



Port Settings

Port Settings

Unit	From Port	To Port	Media Type	
1	eth1/0/1	eth1/0/1	Auto	Apply

Unit	From Port	To Port	Media Type	State	MDIX	Flow Control
1	eth1/0/1	eth1/0/1	RJ45	Enabled	Auto	Off

Duplex	Speed	Capability Advertised	Description	
Auto	Auto	□ 10M □ 100M □ 1000M	64 chars □	Apply

Unit 1 Settings

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

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.
From Port - To Port	Select the appropriate port range used for the configuration here.
Media Type	Select the port media type of combo ports here. Options to choose from are **Auto**, **RJ45**, and **SFP**.
Unit	Select the stacking unit ID of the Switch that will be configured here.
From Port - To Port	Select the appropriate port range used for the configuration here.
Media Type	Select the port media type here. Options to choose from are **RJ45** and **SFP**.
State	Select to enable or disable the physical port state here.
MDIX	Select the Medium Dependent Interface Crossover (MDIX) option here. Options to choose from are: • **Auto -** Select this option for auto-sensing of the optimal type of cabling.

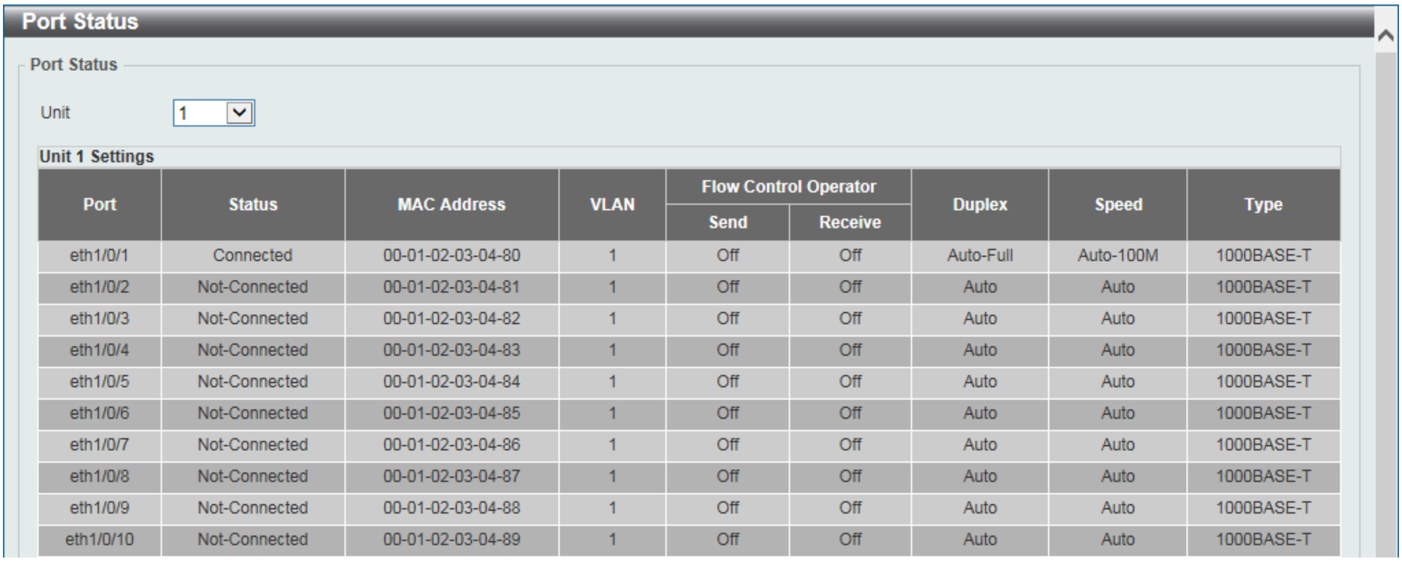
Parameter	Description
	• **Normal -** Select this option for normal cabling. If this option is selected, the port is in the MDIX mode and can be connected to a PC NIC using a straight-through cable or a port (in the MDI mode) on another Switch through a crossover cable. • **Cross -** Select this option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

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

Port Status

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

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



Port Status

Port Status

Unit: 1

Unit 1 Settings

Port	Status	MAC Address	VLAN	Flow Control Operator		Duplex	Speed	Type
				Send	Receive			
eth1/0/1	Connected	00-01-02-03-04-80	1	Off	Off	Auto-Full	Auto-100M	1000BASE-T
eth1/0/2	Not-Connected	00-01-02-03-04-81	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/3	Not-Connected	00-01-02-03-04-82	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/4	Not-Connected	00-01-02-03-04-83	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/5	Not-Connected	00-01-02-03-04-84	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/6	Not-Connected	00-01-02-03-04-85	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/7	Not-Connected	00-01-02-03-04-86	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/8	Not-Connected	00-01-02-03-04-87	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/9	Not-Connected	00-01-02-03-04-88	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/10	Not-Connected	00-01-02-03-04-89	1	Off	Off	Auto	Auto	1000BASE-T

Figure 3-5 Port Status Window

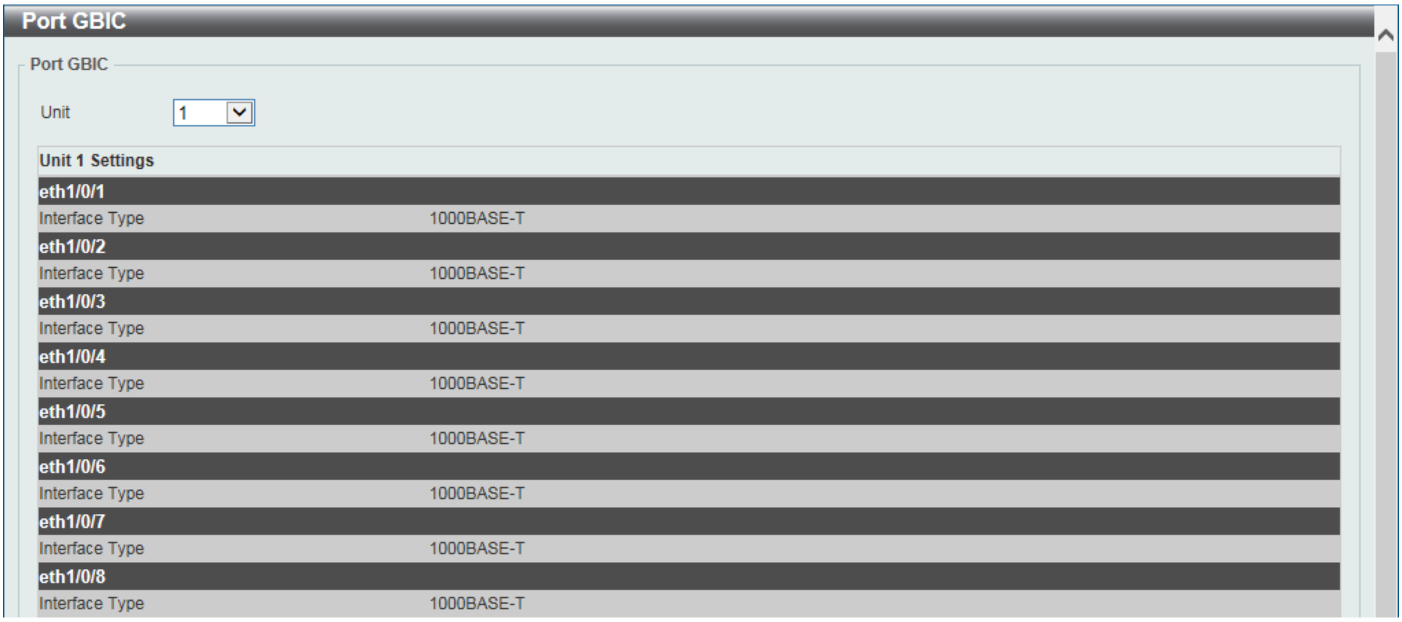
The fields that can be configured are described below:

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

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:



Port GBIC

Port GBIC

Unit: 1

Unit 1 Settings

eth1/0/1

Interface Type: 1000BASE-T

eth1/0/2

Interface Type: 1000BASE-T

eth1/0/3

Interface Type: 1000BASE-T

eth1/0/4

Interface Type: 1000BASE-T

eth1/0/5

Interface Type: 1000BASE-T

eth1/0/6

Interface Type: 1000BASE-T

eth1/0/7

Interface Type: 1000BASE-T

eth1/0/8

Interface Type: 1000BASE-T

Figure 3-6 Port GBIC Window

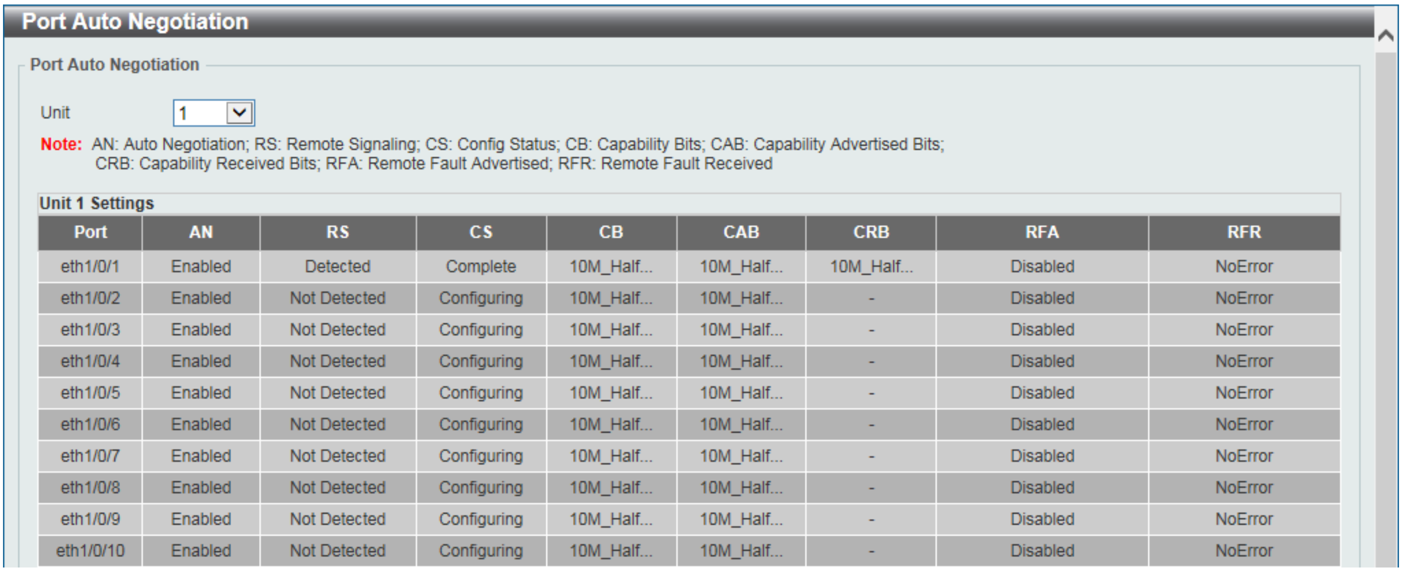
The fields that can be configured are described below:

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.

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



Unit: 1

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

Unit 1 Settings

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

Figure 3-7 Port Auto Negotiation Window

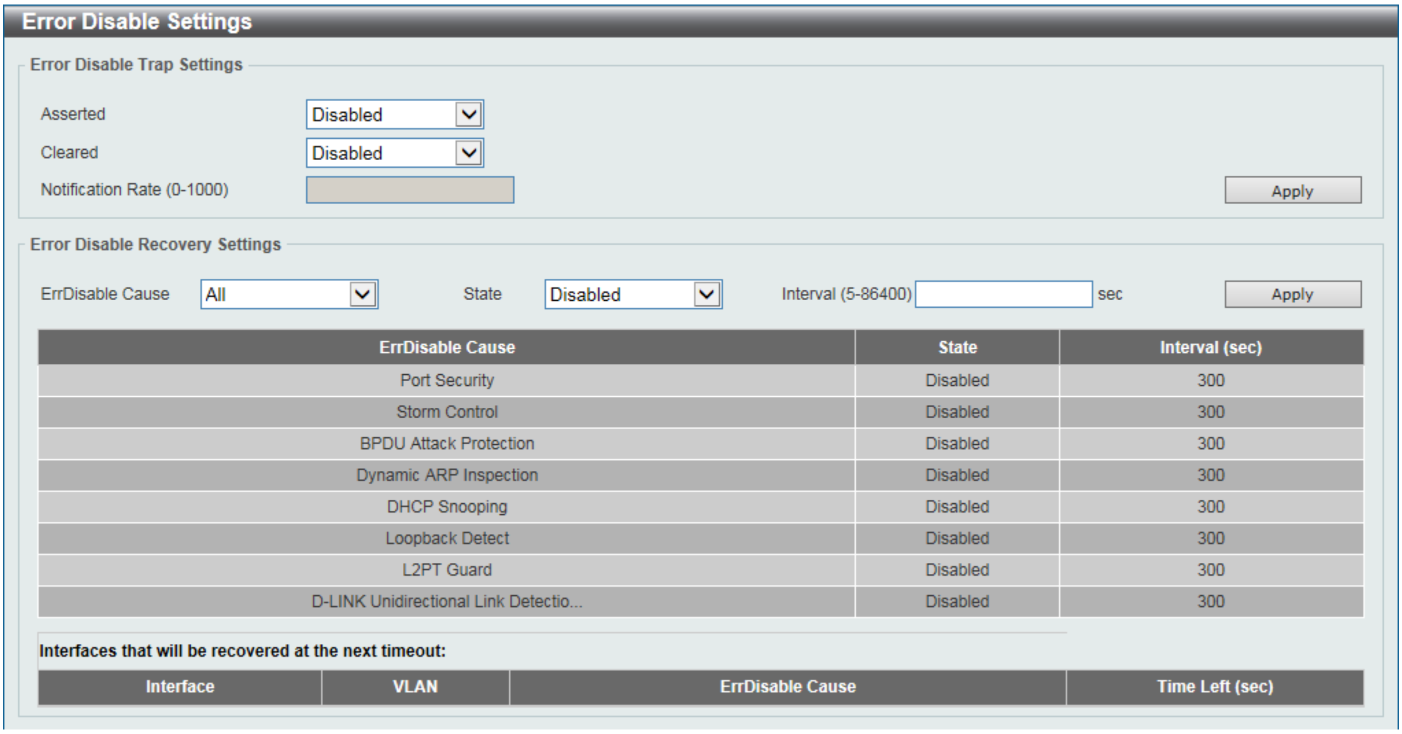
The fields that can be configured are described below:

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

Error Disable Settings

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

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



Error Disable Settings

Error Disable Trap Settings

Asserted: Disabled

Cleared: Disabled

Notification Range (0-1000):

Error Disable Recovery Settings

ErrDisable Cause: All

State: Disabled

Interval (5-86400) sec

ErrDisable Cause	State	Interval (sec)
Port Security	Disabled	300
Storm Control	Disabled	300
BPDU Attack Protection	Disabled	300
Dynamic ARP Inspection	Disabled	300
DHCP Snooping	Disabled	300
Loopback Detect	Disabled	300
L2PT Guard	Disabled	300
D-LINK Unidirectional Link Detectio...	Disabled	300

Interfaces that will be recovered at the next timeout:

Interface	VLAN	ErrDisable Cause	Time Left (sec)

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:

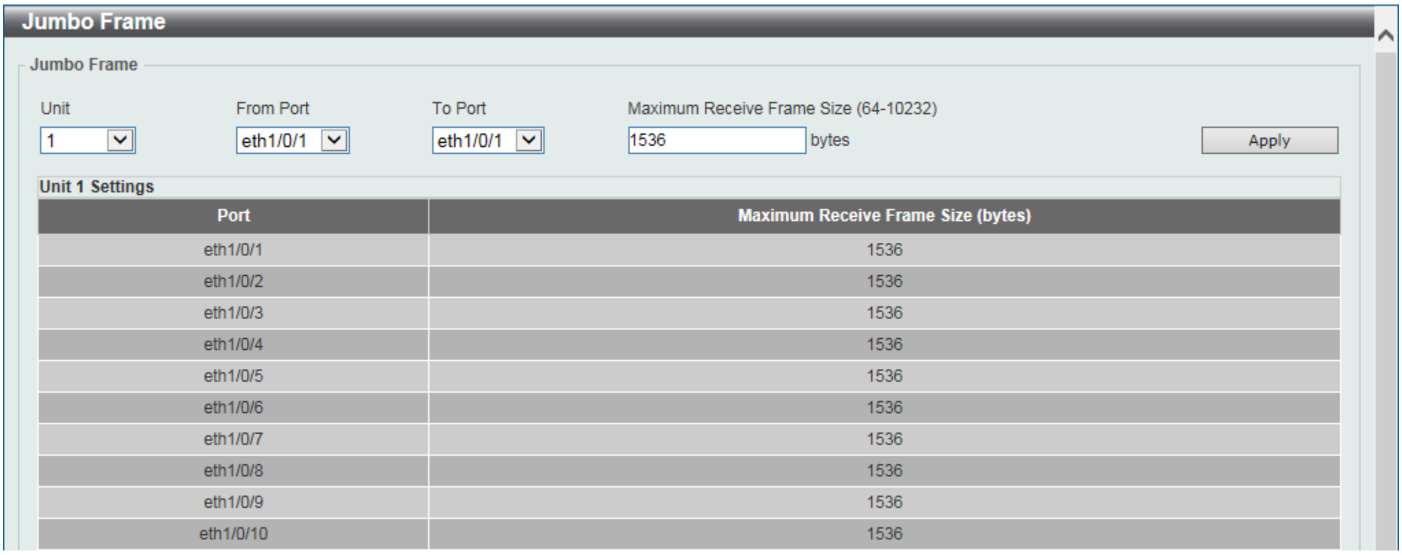
Parameter	Description
ErrDisable Cause	Select the error disabled cause here. Options to choose from are **Port Security**, **Storm Control**, **BPDU Attack Protection**, **Dynamic ARP Inspection**, **DHCP Snooping**, **Loopback Detect**, **L2PT Guard**, and **DULD**.
State	Select to enable or disable 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 seconds. By default, this value is 300 seconds.

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 1518 bytes of payload. The Switch supports jumbo frames with a maximum frame size of up to 9216 bytes.

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



Jumbo Frame

Jumbo Frame

Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1
Maximum Receive Frame Size (64-10232): 1536 bytes

Unit 1 Settings

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

Figure 3-9 Jumbo Frame Window

The fields that can be configured for **Jumbo Frame** are described below:

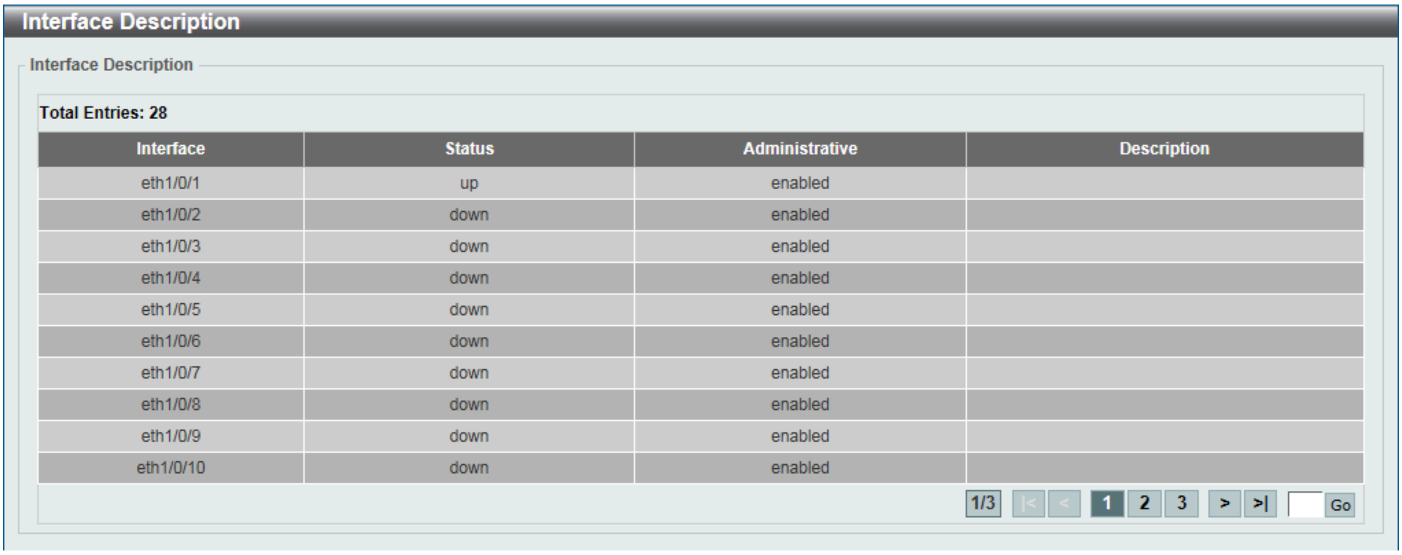
Parameter	Description
Unit	Select the stacking unit ID of the Switch that will be configured here.
From Port - To Port	Select the appropriate port range used for the configuration here.
Maximum Receive Frame Size	Enter the maximum receive frame size value here. The range is from 64 to 10232 bytes. By default, this value is 1536 bytes.

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

Interface Description

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

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



Interface Description

Interface Description

Total Entries: 28

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

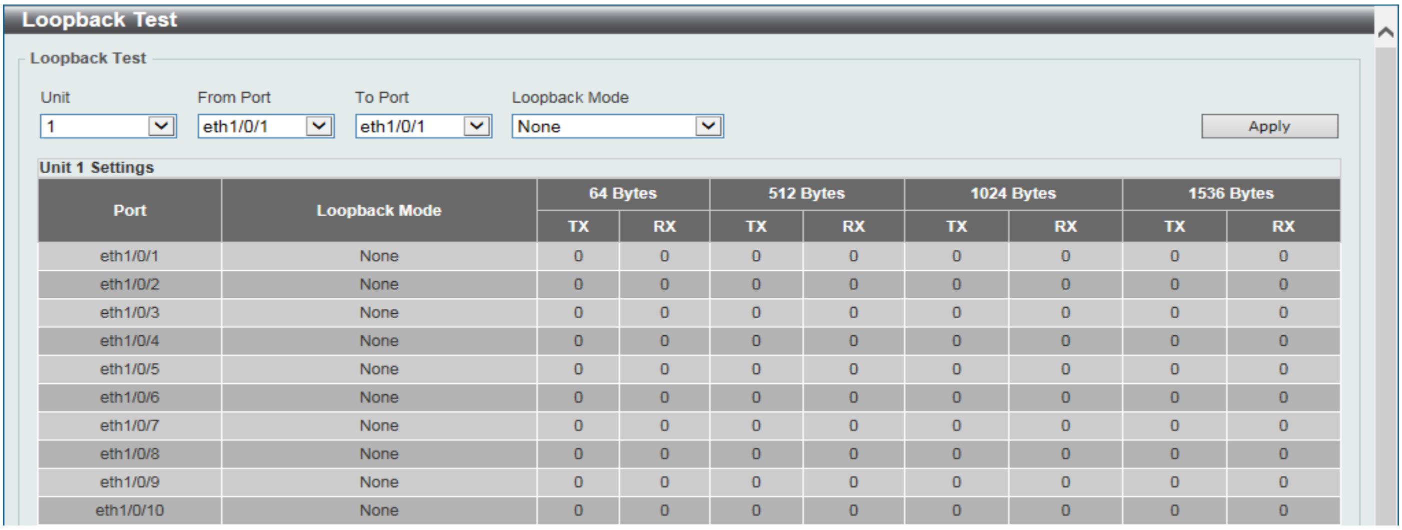
Figure 3-10 Interface Description Window

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

Loopback Test

This window is used to display and configure the loopback settings of the physical port interfaces and to perform loopback tests.

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



Loopback Test

Loopback Test

Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1
Loopback Mode: None

Unit 1 Settings

Port	Loopback Mode	64 Bytes		512 Bytes		1024 Bytes		1536 Bytes	
		TX	RX	TX	RX	TX	RX	TX	RX
eth1/0/1	None	0	0	0	0	0	0	0	0
eth1/0/2	None	0	0	0	0	0	0	0	0
eth1/0/3	None	0	0	0	0	0	0	0	0
eth1/0/4	None	0	0	0	0	0	0	0	0
eth1/0/5	None	0	0	0	0	0	0	0	0
eth1/0/6	None	0	0	0	0	0	0	0	0
eth1/0/7	None	0	0	0	0	0	0	0	0
eth1/0/8	None	0	0	0	0	0	0	0	0
eth1/0/9	None	0	0	0	0	0	0	0	0
eth1/0/10	None	0	0	0	0	0	0	0	0

Figure 3-11 Loopback 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.

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Loopback Mode	Select the loopback mode here. Options to choose from are: • **None -** Specifies not to enable the loopback mode. • **Internal MAC -** Specifies the internal loopback mode at the MAC layer. • **Internal PHY Default -** Specifies the internal loopback mode at the PHY layer to test the default medium. • **Internal PHY Copper -** Specifies the internal loopback mode at the PHY layer to test the copper medium. • **Internal PHY Fiber -** Specifies the internal loopback mode at the PHY layer to test the fiber medium. • **External MAC -** Specifies the external loopback mode at the MAC layer. • **External PHY Default -** Specifies the external loopback mode at the PHY layer to test the default medium. • **External PHY Copper -** Specifies the external loopback mode at the PHY layer to test the copper medium. • **External PHY Fiber -** Specifies the external loopback mode at the PHY layer to test the fiber medium.

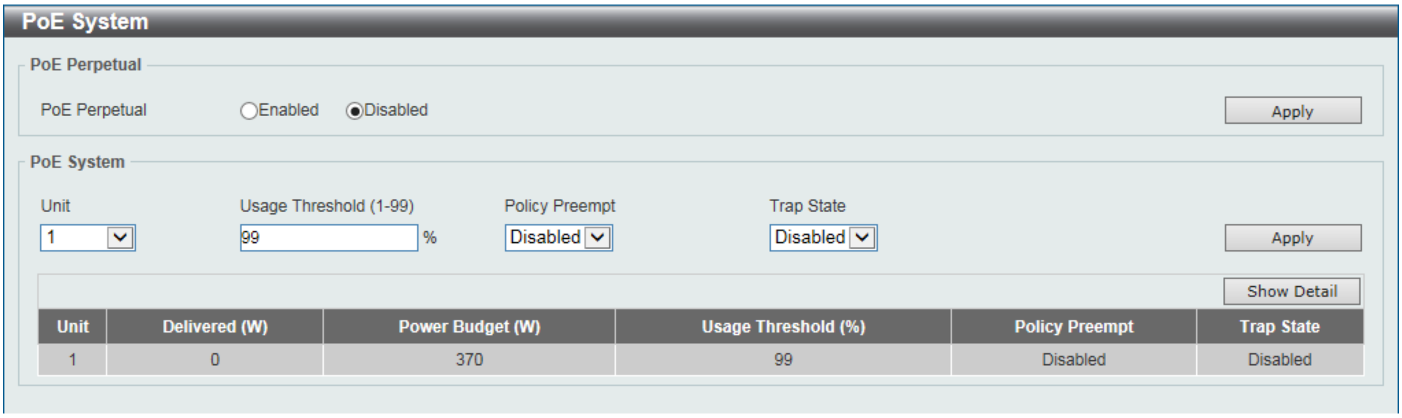
Click the **Apply** button to accept the changes made.

PoE

PoE System

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

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



PoE System

PoE Perpetual

PoE Perpetual ○Enabled ●Disabled

PoE System

Unit: 1
Usage Threshold (1-99): 99 %
Policy Preempt: Disabled
Trap State: Disabled

Unit	Delivered (W)	Power Budget (W)	Usage Threshold (%)	Policy Preempt	Trap State
1	0	370	99	Disabled	Disabled

Figure 3-12 PoE System Window

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

Parameter	Description
PoE Perpetual	Select this option to enable or disable the PoE perpetual feature.

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

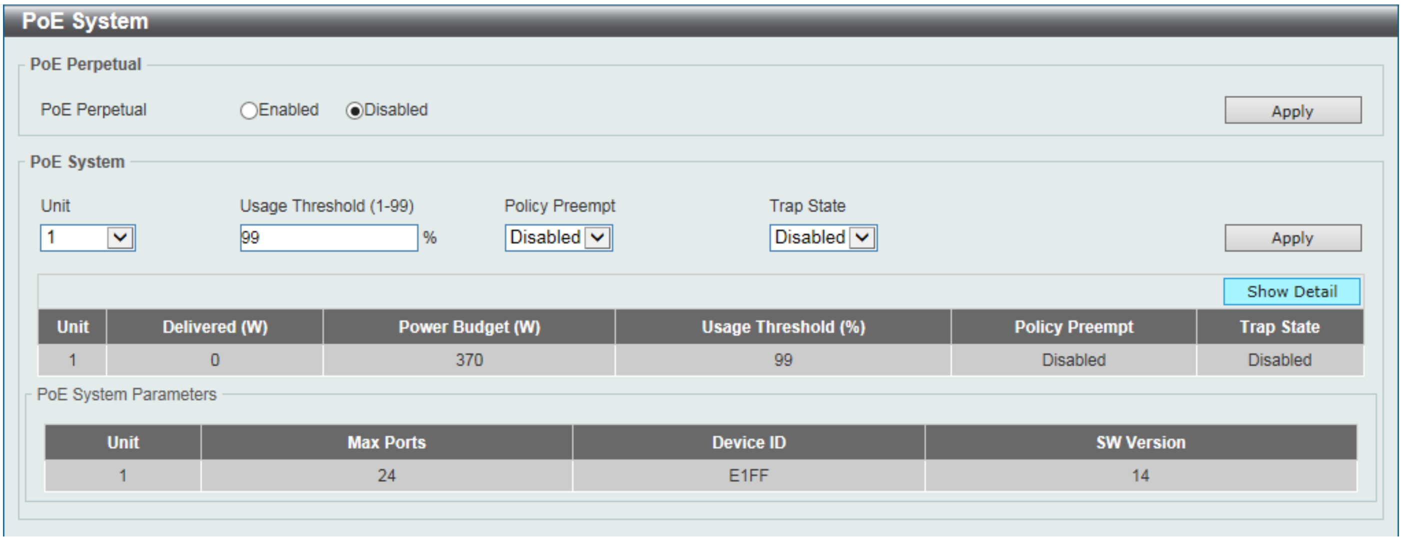
The fields that can be configured for **PoE System** are described below:

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

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

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

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



PoE Perpetual

PoE Perpetual ○Enabled ●Disabled

PoE System

Unit: 1
Usage Threshold (1-99): 99 %
Policy Preempt: Disabled
Trap State: Disabled

Unit	Delivered (W)	Power Budget (W)	Usage Threshold (%)	Policy Preempt	Trap State
1	0	370	99	Disabled	Disabled

PoE System Parameters

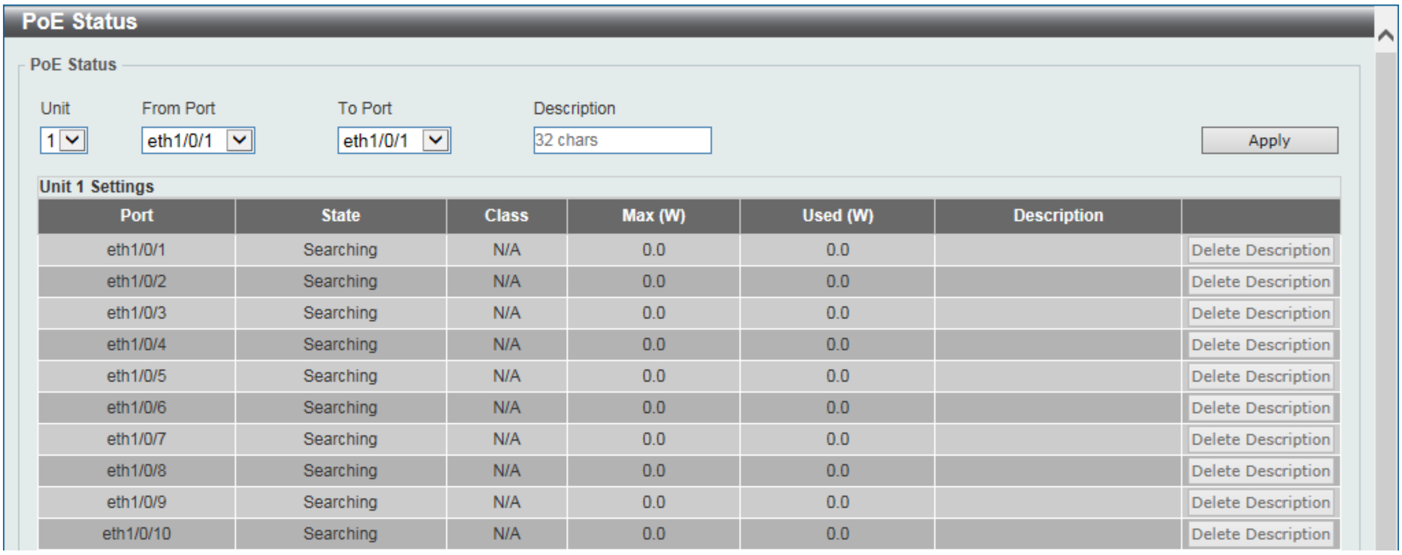
Unit	Max Ports	Device ID	SW Version
1	24	E1FF	14

Figure 3-13 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:



PoE Status

PoE Status

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

Unit 1 Settings

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

Figure 3-14 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.
From Port - To Port	Select the appropriate port range used for the configuration here.
Description	Enter the text that describes the PD connected to a PoE interface. The maximum length is 32 characters.

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

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

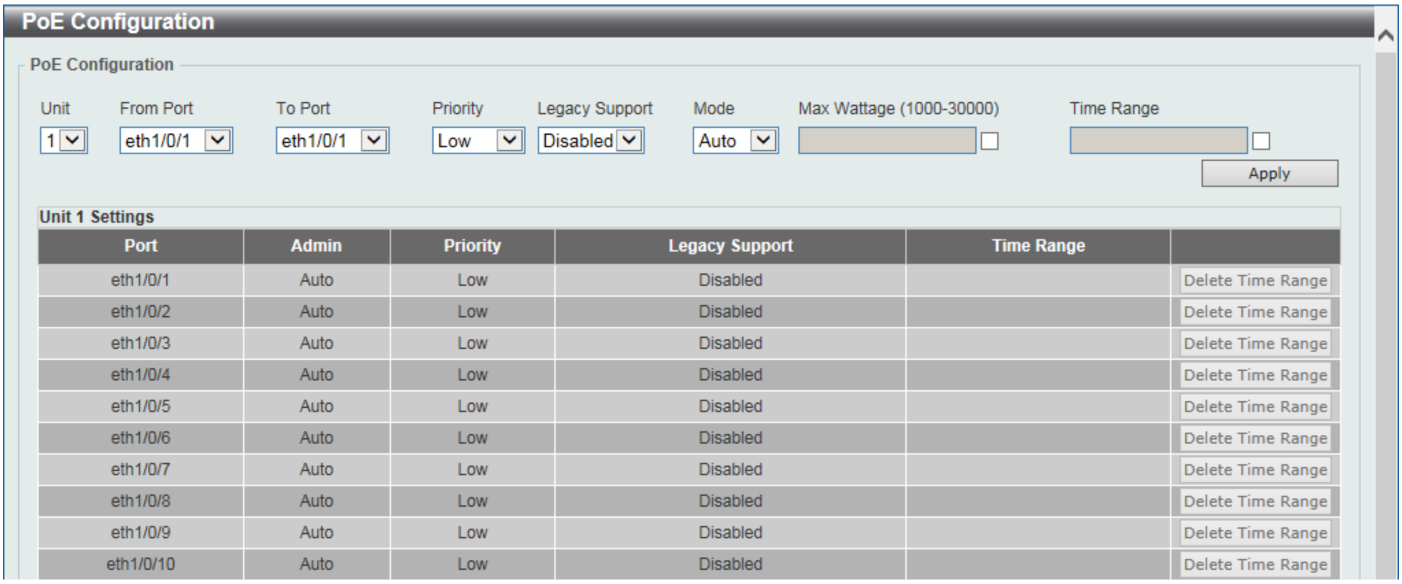
PoE Configuration

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

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

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

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



PoE Configuration

PoE Configuration

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

Unit 1 Settings

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

Figure 3-15 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.
From Port - To Port	Select the appropriate port range used for the configuration here.
Priority	Select the priority for provisioning power to the port. Options to choose from are **Critical**, **High**, and **Low**.
Legacy Support	Select this option to enable or disable the support of legacy PD.
Mode	Select the power management mode for the PoE ports. Options to choose from are **Auto** and **Never**.
Max Wattage	When selecting **Auto** in the **Mode** drop-down list, this option appears. Select 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 30000 mW.
Time Range	When selecting **Auto** in the **Mode** drop-down list, this option appears. Select the check box and enter the name of the time range to determine the activation period.

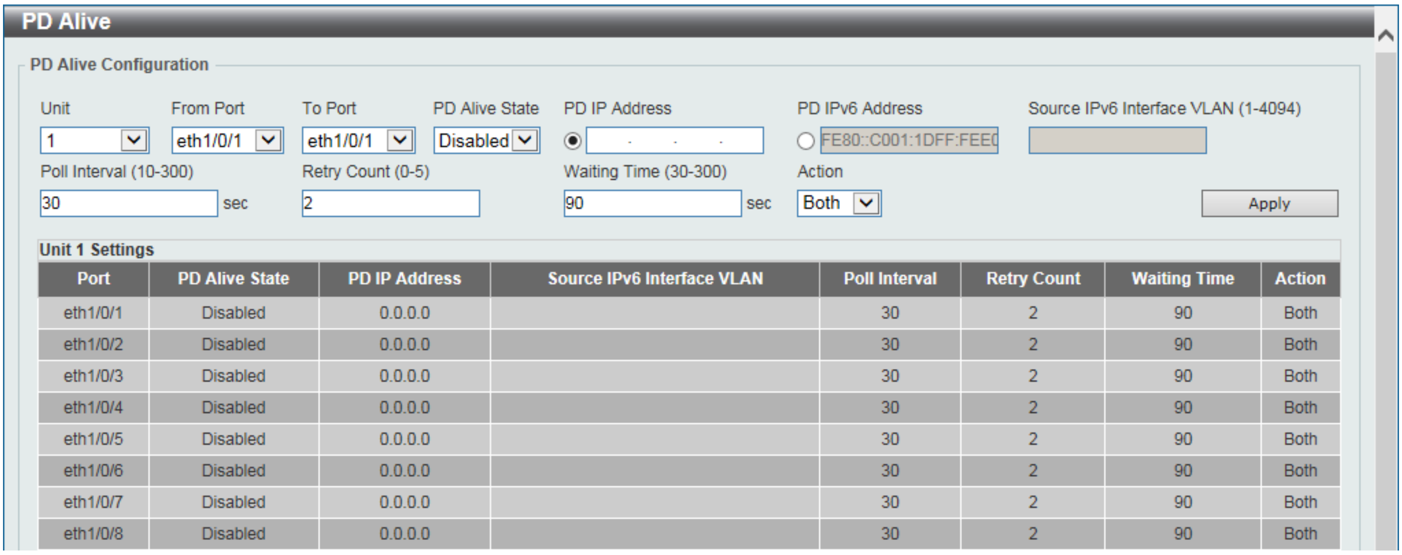
Click the **Apply** button to accept the changes made.

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

PD Alive

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

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



PD Alive

PD Alive Configuration

Unit	From Port	To Port	PD Alive State	PD IP Address	PD IPv6 Address	Source IPv6 Interface VLAN (1-4094)
1	eth1/0/1	eth1/0/1	Disabled	● . . .	○ FE80::C001:1DFF:FEE0	
Poll Interval (10-300)		Retry Count (0-5)		Waiting Time (30-300)	Action	
30 sec		2		90 sec	Both	Apply

Unit 1 Settings

Port	PD Alive State	PD IP Address	Source IPv6 Interface VLAN	Poll Interval	Retry Count	Waiting Time	Action
eth1/0/1	Disabled	0.0.0.0		30	2	90	Both
eth1/0/2	Disabled	0.0.0.0		30	2	90	Both
eth1/0/3	Disabled	0.0.0.0		30	2	90	Both
eth1/0/4	Disabled	0.0.0.0		30	2	90	Both
eth1/0/5	Disabled	0.0.0.0		30	2	90	Both
eth1/0/6	Disabled	0.0.0.0		30	2	90	Both
eth1/0/7	Disabled	0.0.0.0		30	2	90	Both
eth1/0/8	Disabled	0.0.0.0		30	2	90	Both

Figure 3-16 PD Alive Window

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

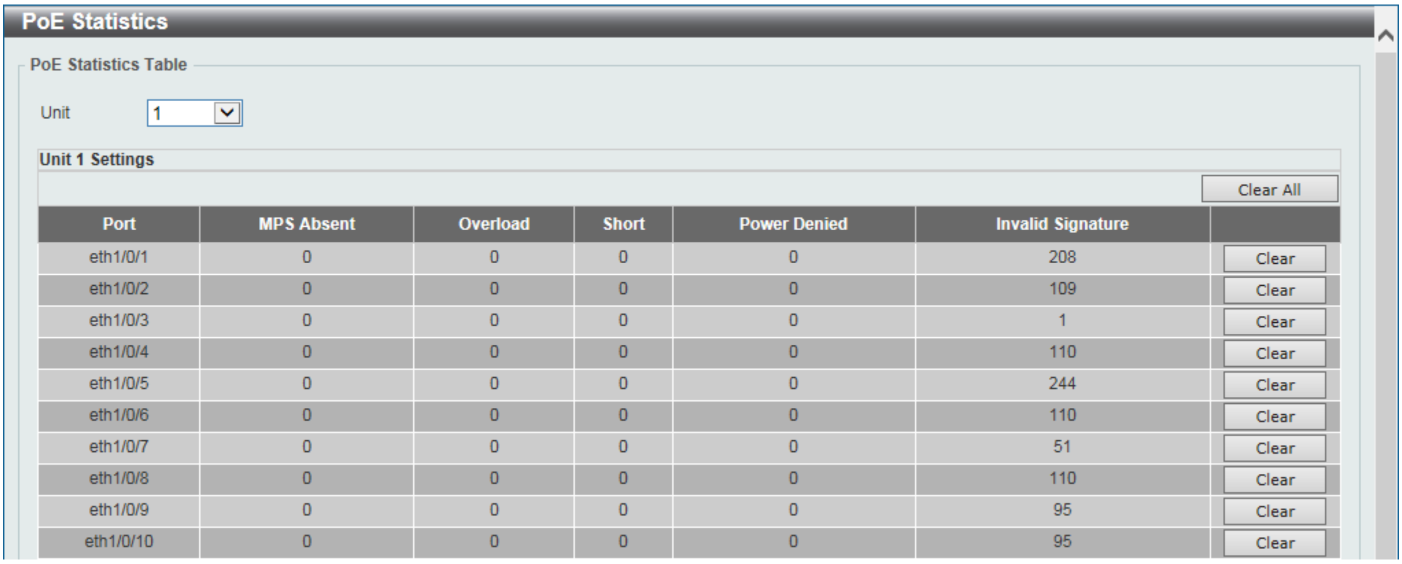
Parameter	Description
Unit	Select the stacking unit ID of the Switch that will be configured here.
From Port - To Port	Select the appropriate port range used for the configuration here.
PD Alive State	Select to enable or disable the state of the PoE alive function on the specified port(s) here.
PD IP Address	Enter the IPv4 address of the target PD here.
PD IPv6 Address	Enter the IPv6 address of the target PD here.
Source IPv6 Interface VLAN	Enter the source IPv6 interface VLAN used for the ping packet.
Poll Interval	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 amount of times that the ping request will be resend if the target PD does not respond.
Waiting Time	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.

PoE Statistics

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

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



PoE Statistics

PoE Statistics Table

Unit: 1

Unit 1 Settings

Port	MPS Absent	Overload	Short	Power Denied	Invalid Signature	
eth1/0/1	0	0	0	0	208	Clear
eth1/0/2	0	0	0	0	109	Clear
eth1/0/3	0	0	0	0	1	Clear
eth1/0/4	0	0	0	0	110	Clear
eth1/0/5	0	0	0	0	244	Clear
eth1/0/6	0	0	0	0	110	Clear
eth1/0/7	0	0	0	0	51	Clear
eth1/0/8	0	0	0	0	110	Clear
eth1/0/9	0	0	0	0	95	Clear
eth1/0/10	0	0	0	0	95	Clear

Figure 3-17 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.

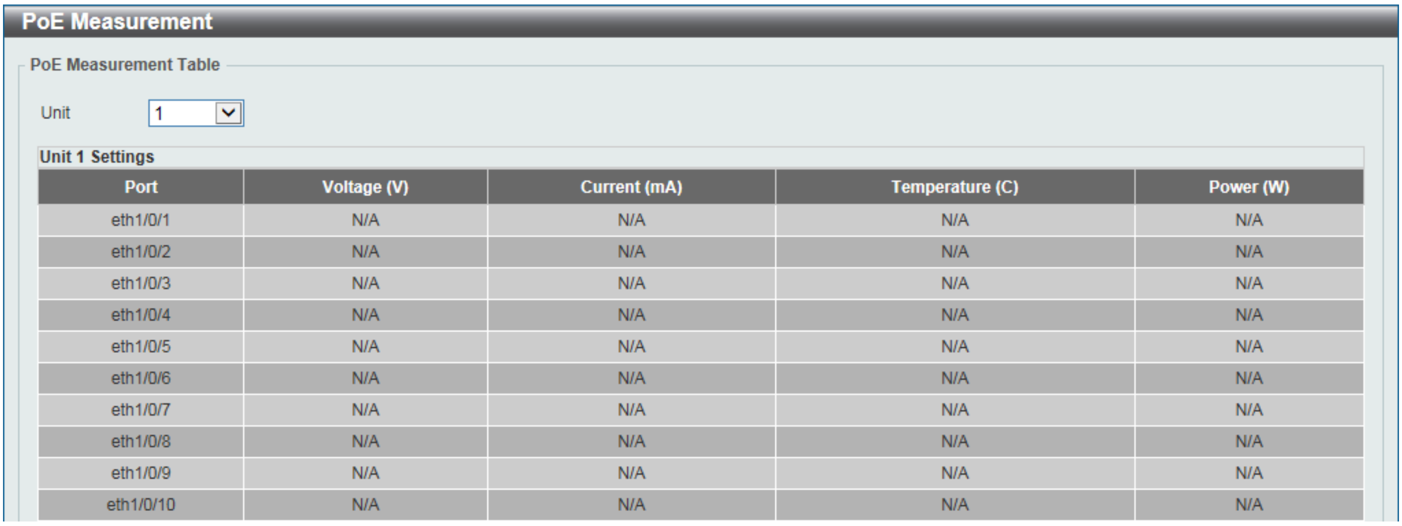
Click the **Clear All** button to clear PoE statistics for all ports.

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

PoE Measurement

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

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



PoE Measurement

PoE Measurement Table

Unit: 1

Unit 1 Settings

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

Figure 3-18 PoE Measurement Window

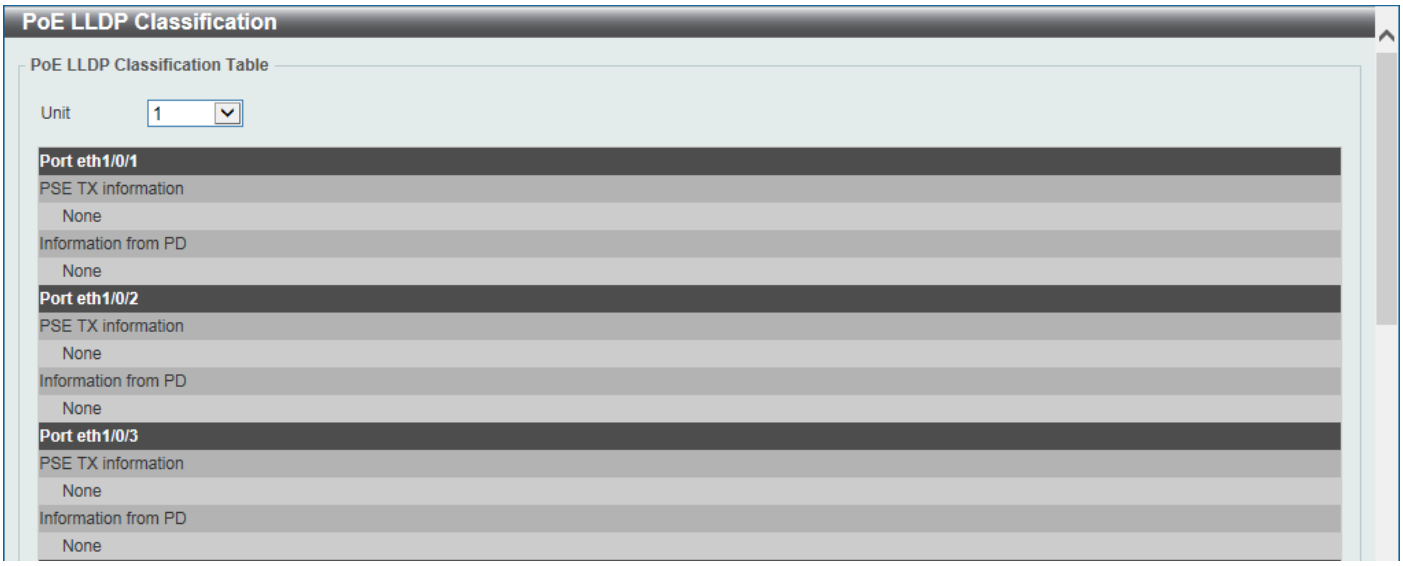
The fields that can be configured for **PoE Measurement Table** are described below:

Parameter	Description
Unit	Select the stacking unit ID of the Switch that will be used here.

PoE LLDP Classification

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

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



PoE LLDP Classification

PoE LLDP Classification Table

Unit: 1

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

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

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

Figure 3-19 PoE LLDP Classification Window

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

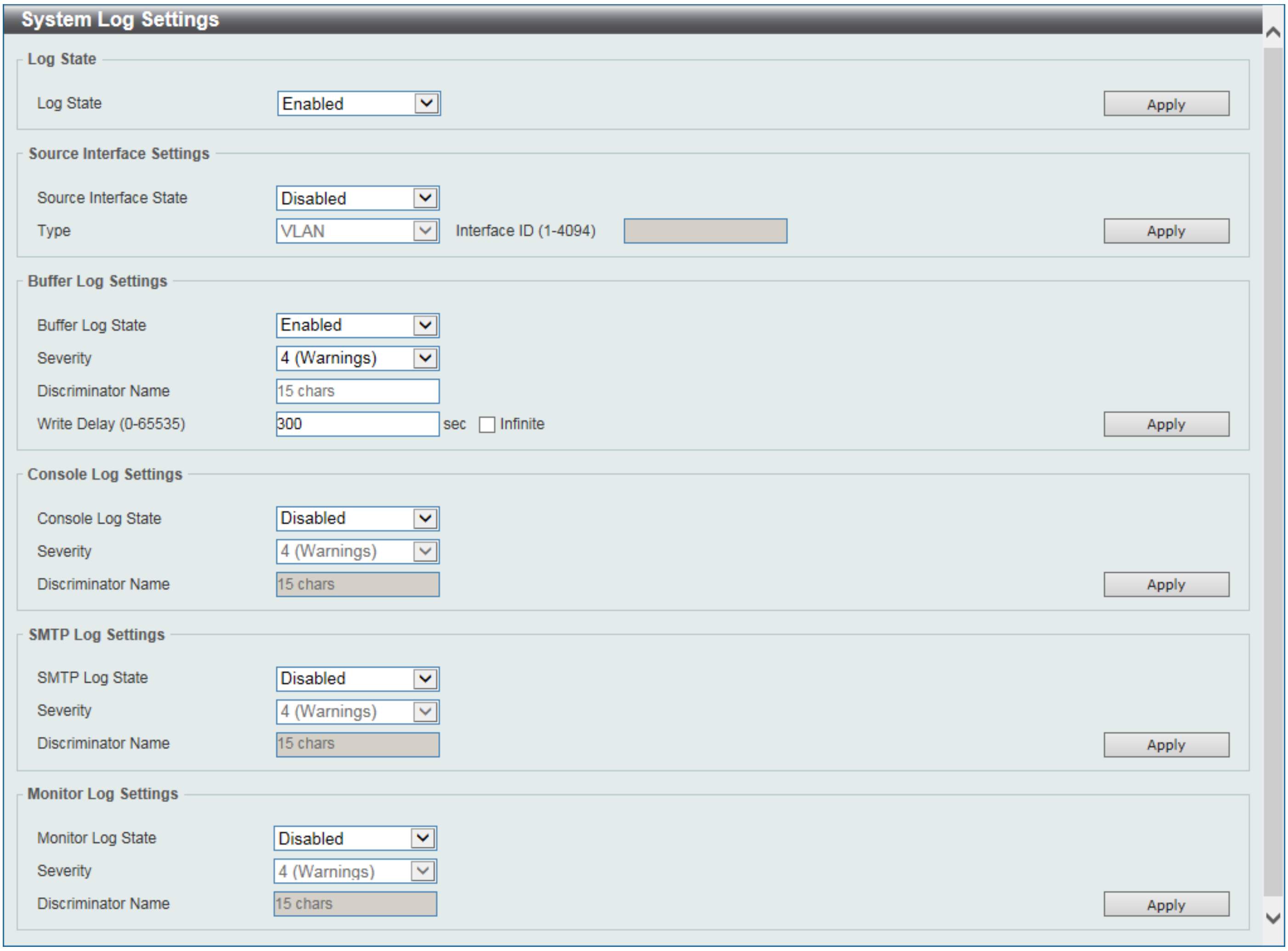
Parameter	Description
Unit	Select the stacking unit ID of the Switch that will be used here.

System Log

System Log Settings

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

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



System Log Settings

Log State

Log State: Enabled

Source Interface Settings

Source Interface State: Disabled

Type: VLAN

Interface ID (1-4094):

Buffer Log Settings

Buffer Log State: Enabled

Severity: 4 (Warnings)

Discriminator Name: 15 chars

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

Console Log Settings

Console Log State: Disabled

Severity: 4 (Warnings)

Discriminator Name: 15 chars

SMTP Log Settings

SMTP Log State: Disabled

Severity: 4 (Warnings)

Discriminator Name: 15 chars

Monitor Log Settings

Monitor Log State: Disabled

Severity: 4 (Warnings)

Discriminator Name: 15 chars

Figure 3-20 System Log Settings Window

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

Parameter	Description
Log State	Select to 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. Options to choose from are **Loopback** and **VLAN**.
Interface ID	Enter the VLAN ID here. For **loopback**, the range is from 1 to 8. For **VLAN**, the range 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	Select to globally enable or disable the buffer log state here. Options to choose from are **Enable**, **Disabled**, and **Default**. When selecting the **Default** option, the global buffer log state will follow the default behavior.
Severity	Select the severity value of the type of information that will be logged. Options to choose from are **0 (Emergencies)**, **1 (Alerts)**, **2 (Critical)**, **3 (Errors)**, **4 (Warnings)**, **5 (Notifications)**, **6 (Informational)**, and **7 (Debugging)**.
Discriminator Name	Enter the discriminator name used here. This name can be up to 15 characters long. This specifies the name of the discriminator profile that will be used to filter buffer log messages based on the filtering criteria specified within that profile.
Write Delay	Enter the log write delay value here. The range is from 0 to 65535 seconds. By default, this value is 300 seconds. Select the **Infinite** option, to disable the write delay feature.

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

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

Parameter	Description
Console Log State	Select to globally enable or disable the console log state here.
Severity	Select the severity value of the type of information that will be logged. Options to choose from are **0 (Emergencies)**, **1 (Alerts)**, **2 (Critical)**, **3 (Errors)**, **4 (Warnings)**, **5 (Notifications)**, **6 (Informational)**, and **7 (Debugging)**.
Discriminator Name	Enter the discriminator name used here. This name can be up to 15 characters long. This specifies the name of the discriminator profile that will be used to filter console log messages based on the filtering criteria specified within that profile.

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

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

Parameter	Description
SMTP Log State	Select to globally enable or disable the SMTP log state here.
Severity	Select the severity value of the type of information that will be logged. Options to choose from are **0 (Emergencies)**, **1 (Alerts)**, **2 (Critical)**, **3 (Errors)**, **4 (Warnings)**, **5 (Notifications)**, **6 (Informational)**, and **7 (Debugging)**.
Discriminator Name	Enter the discriminator name used here. This name can be up to 15 characters long. This specifies the name of the discriminator profile that will be used to filter SMTP log messages based on the filtering criteria specified within that profile.

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

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

Parameter	Description
Monitor Log State	Select to globally enable or disable the monitor 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)**.

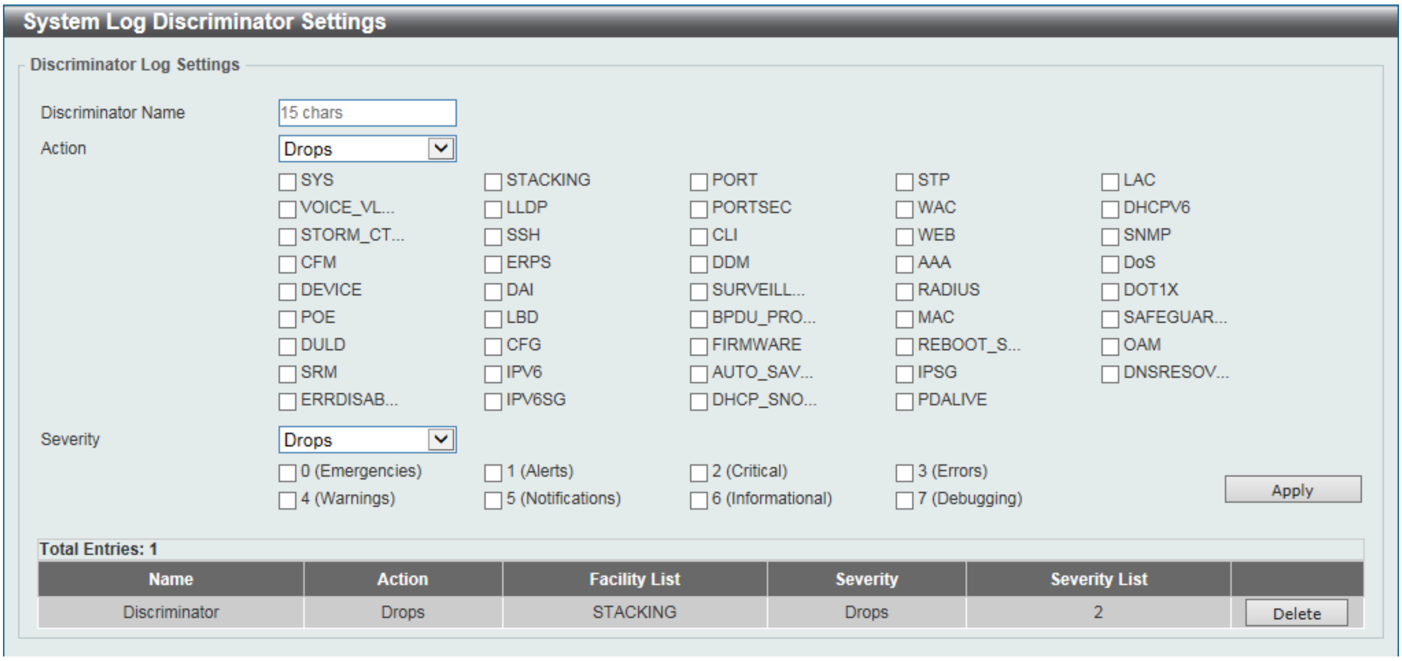
Parameter	Description
Discriminator Name	Enter the discriminator name used here. This name can be up to 15 characters long. This specifies the name of the discriminator profile that will be used to filter monitor log messages based on the filtering criteria specified within that profile.

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

System Log Discriminator Settings

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

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



System Log Discriminator Settings

Discriminator Log Settings

Discriminator Name: 15 chars

Action: Drops

□ SYS
□ VOICE_VL...
□ STORM_CT...
□ CFM
□ DEVICE
□ POE
□ DULD
□ SRM
□ ERRDISAB...
□ STACKING
□ LLDP
□ SSH
□ ERPS
□ DAI
□ LBD
□ CFG
□ IPV6
□ IPV6SG
□ PORT
□ PORTSEC
□ CLI
□ DDM
□ SURVEILL...
□ BPDU_PRO...
□ FIRMWARE
□ AUTO_SAV...
□ DHCP_SNO...
□ STP
□ WAC
□ WEB
□ AAA
□ RADIUS
□ MAC
□ REBOOT_S...
□ IPSG
□ PDALIVE
□ LAC
□ DHCPV6
□ SNMP
□ DoS
□ DOT1X
□ SAFEGUAR...
□ OAM
□ DNSRESOV...

Severity: Drops

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

Total Entries: 1

Name	Action	Facility List	Severity	Severity List	
Discriminator	Drops	STACKING	Drops	2	Delete

Figure 3-21 System Log Discriminator Settings Window

The fields that can be configured are described below:

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

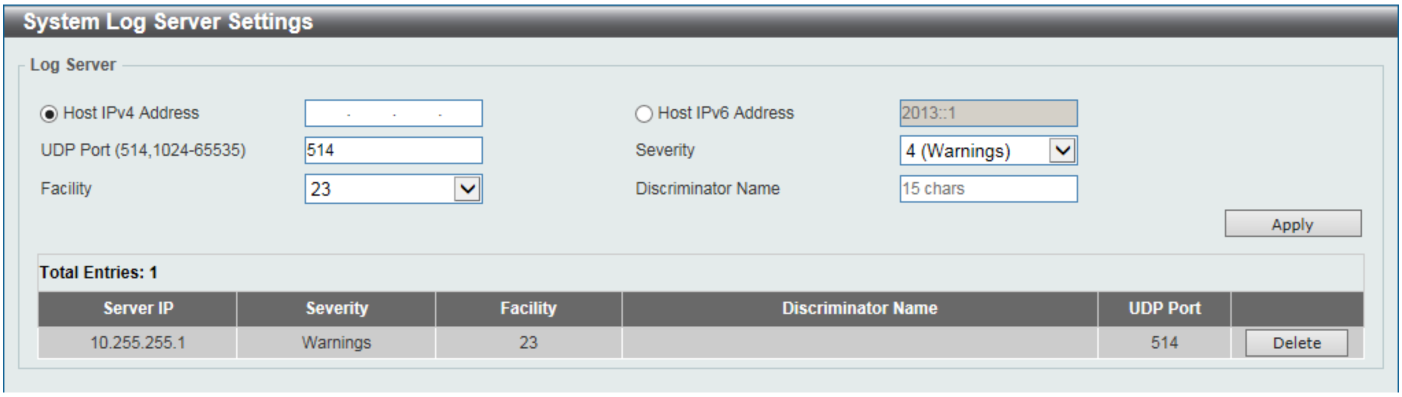
Click the **Apply** button to accept the changes made.

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

System Log Server Settings

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

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



System Log Server Settings

Log Server

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

Total Entries: 1

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

Figure 3-22 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 from 1024 to 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:

Number	Name	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.		

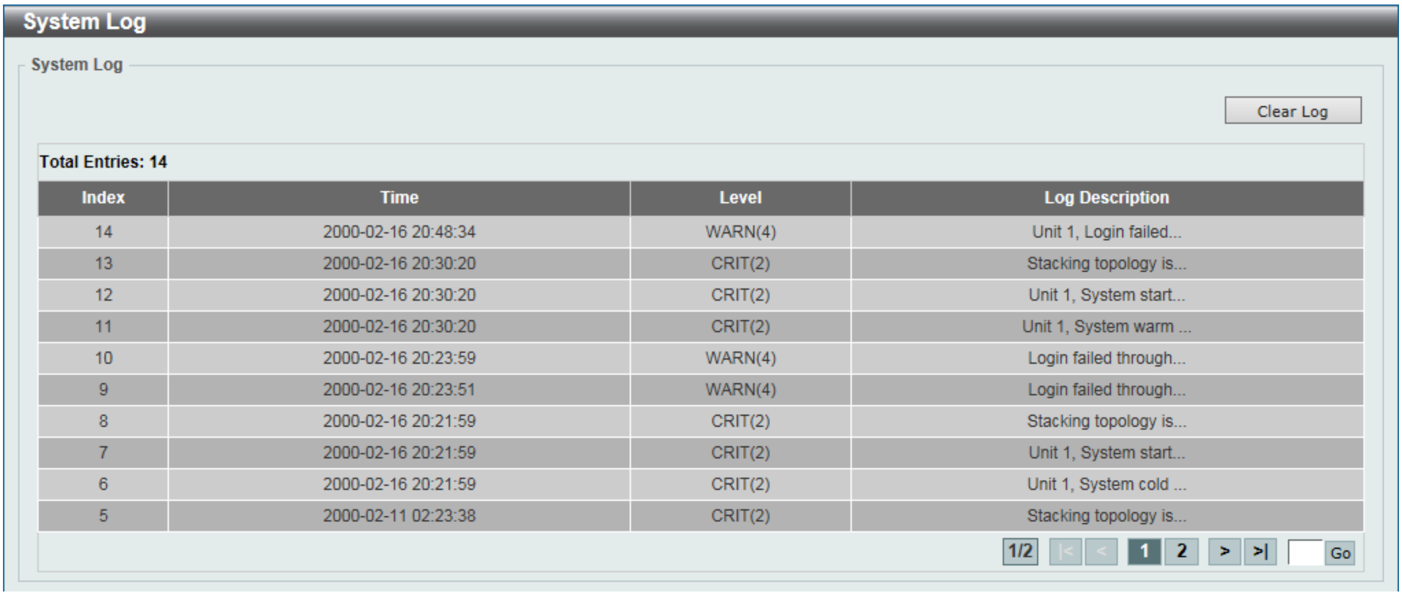
Click the **Apply** button to accept the changes made.

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:



System Log

System Log

Total Entries: 14

Index	Time	Level	Log Description
14	2000-02-16 20:48:34	WARN(4)	Unit 1, Login failed...
13	2000-02-16 20:30:20	CRIT(2)	Stacking topology is...
12	2000-02-16 20:30:20	CRIT(2)	Unit 1, System start...
11	2000-02-16 20:30:20	CRIT(2)	Unit 1, System warm ...
10	2000-02-16 20:23:59	WARN(4)	Login failed through...
9	2000-02-16 20:23:51	WARN(4)	Login failed through...
8	2000-02-16 20:21:59	CRIT(2)	Stacking topology is...
7	2000-02-16 20:21:59	CRIT(2)	Unit 1, System start...
6	2000-02-16 20:21:59	CRIT(2)	Unit 1, System cold ...
5	2000-02-11 02:23:38	CRIT(2)	Stacking topology is...

Figure 3-23 System Log Window

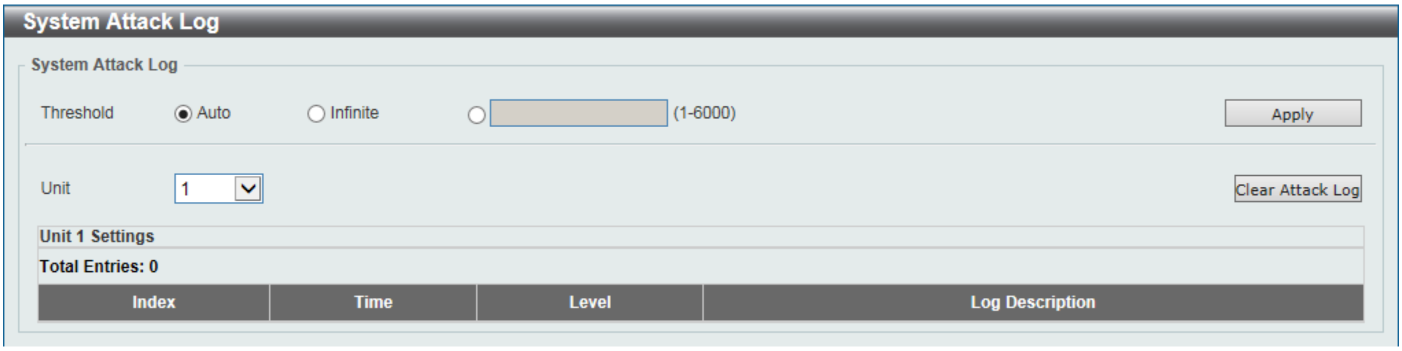
Click the **Clear Log** button to clear the system log entries displayed in the table.

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:



System Attack Log

System Attack Log

Threshold ● Auto ○ Infinite ○ (1-6000)

Unit 1

Unit 1 Settings

Total Entries: 0

Index	Time	Level	Log Description

Figure 3-24 System Attack Log Window

The fields that can be configured are described below:

Parameter	Description
Threshold	Select to configure the logging threshold per minute. Options to choose from are: • **Auto -** Select to use the default value for each type. • **Infinite -** Select to have unlimited logs. • **1-6000 -** Select and enter the number of logs per minute.
Unit	Select the stacking unit ID of the Switch that will be displayed here.

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

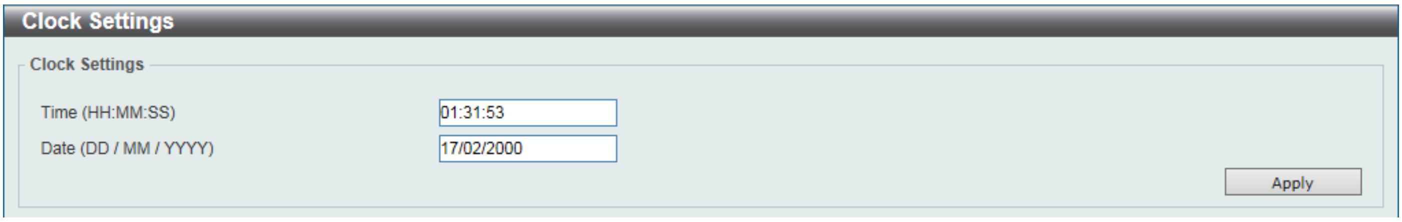
Click the **Clear Attack Log** button to clear the system attack log entries displayed in the table.

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:



Clock Settings

Clock Settings

Time (HH:MM:SS) 01:31:53

Date (DD / MM / YYYY) 17/02/2000

Figure 3-25 Clock Settings Window

The fields that can be configured are described below:

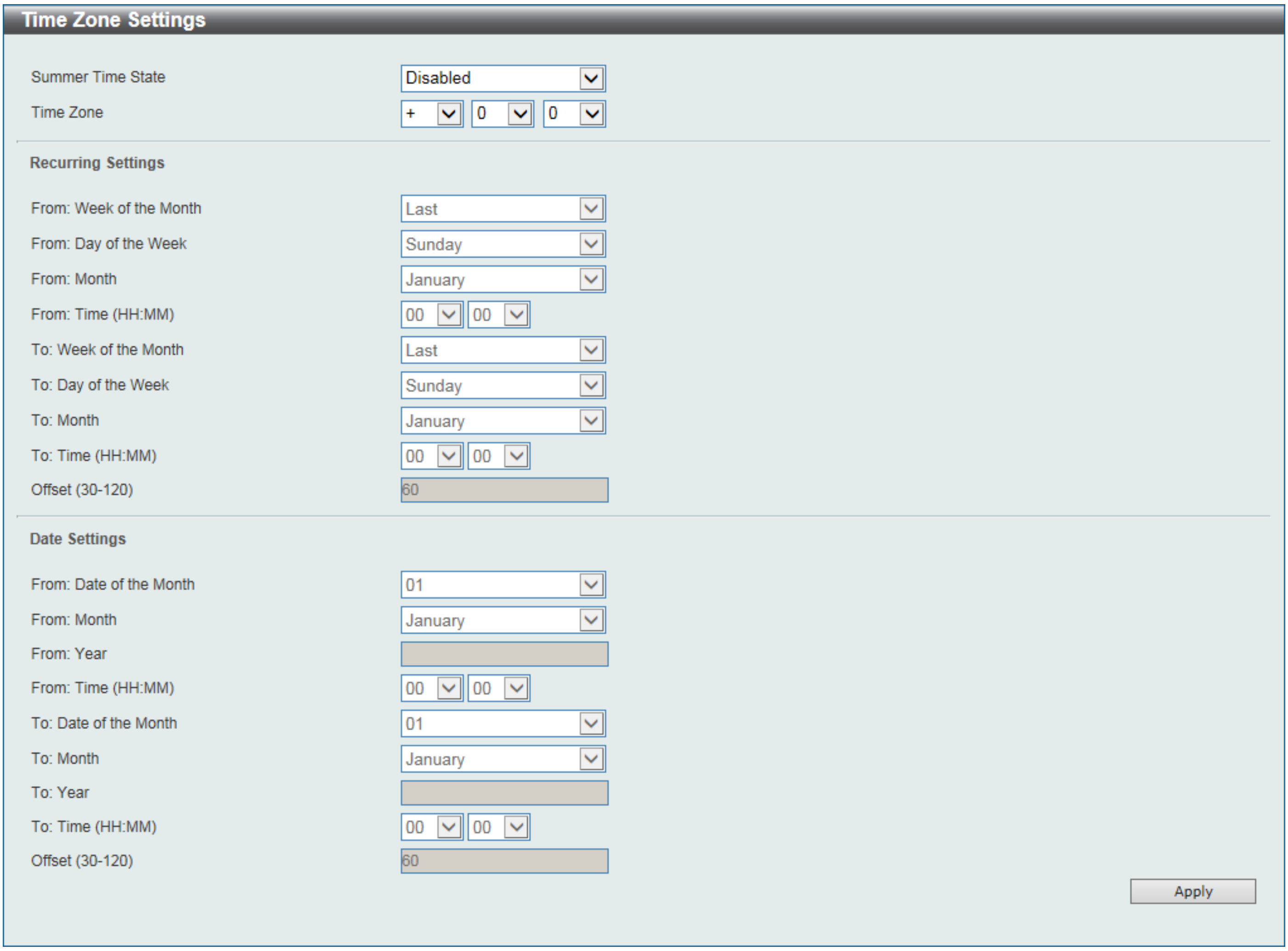
Parameter	Description
Time	Enter the current time in hours (HH), minutes (MM), and seconds (SS) here. For example, 18:30:30.
Date	Enter the current day (DD), month (MM), and year (YYYY) here. For example, 30/04/2015.

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 SNTP.

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



Time Zone Settings

Summer Time State: Disabled

Time Zone: + 0 0

Recurring Settings

From: Week of the Month: Last

From: Day of the Week: Sunday

From: Month: January

From: Time (HH:MM): 00 00

To: Week of the Month: Last

To: Day of the Week: Sunday

To: Month: January

To: Time (HH:MM): 00 00

Offset (30-120): 60

Date Settings

From: Date of the Month: 01

From: Month: January

From: Year:

From: Time (HH:MM): 00 00

To: Date of the Month: 01

To: Month: January

To: Year:

To: Time (HH:MM): 00 00

Offset (30-120): 60

Figure 3-26 Time Zone Settings Window

The fields that can be configured are described below:

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

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

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

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

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

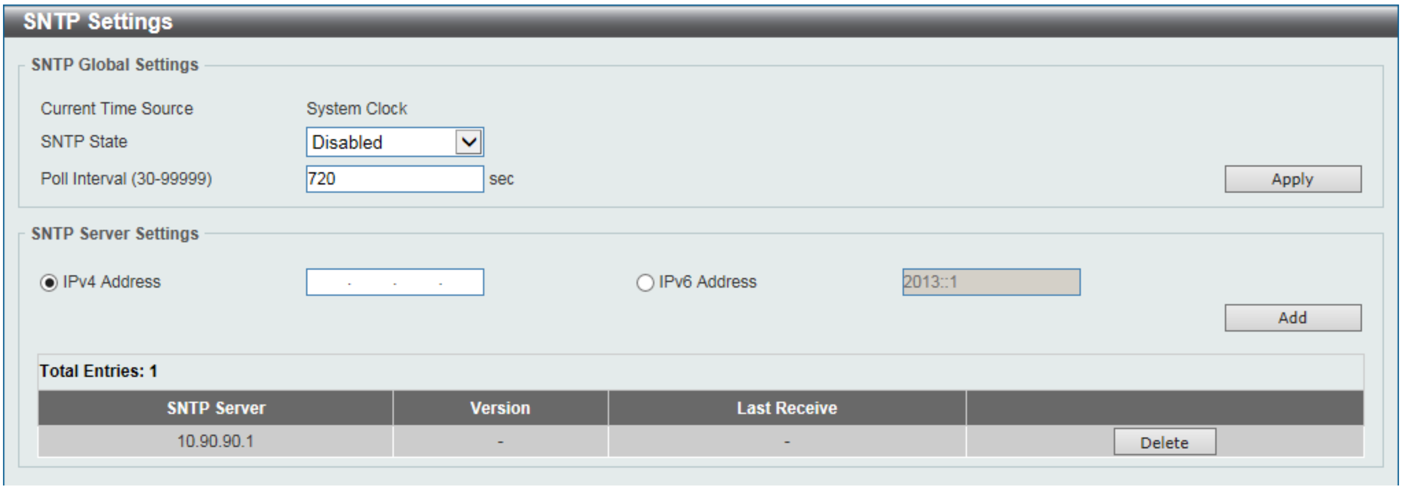
Click the **Apply** button to accept the changes made.

SNTP Settings

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

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

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



SNTP Settings

SNTP Global Settings

Current Time Source: System Clock

SNTP State: Disabled

Poll Interval (30-99999): 720 sec

SNTP Server Settings

● IPv4 Address: . . .   ○ IPv6 Address: 2013::1

Total Entries: 1

SNTP Server	Version	Last Receive	
10.90.90.1	-	-	Delete

Figure 3-27 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. By default, this value 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.

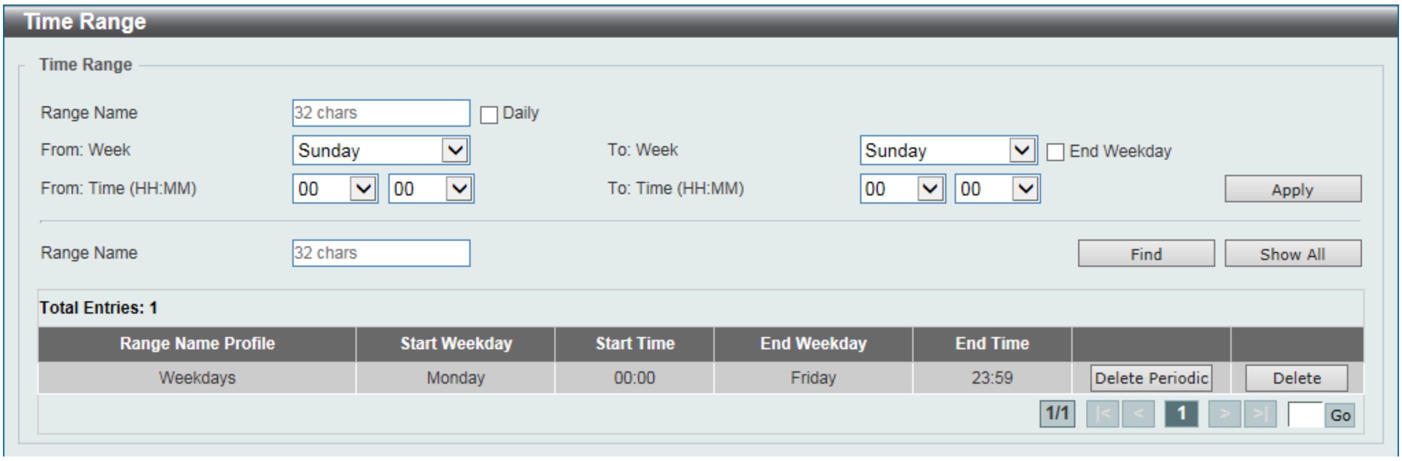
Click the **Add** button to add the SNTP server.

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:



Time Range

Time Range

Range Name: 32 chars □ Daily

From: Week: Sunday | To: Week: Sunday □ End Weekday

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

Range Name: 32 chars

Total Entries: 1

Range Name Profile	Start Weekday	Start Time	End Weekday	End Time		
Weekdays	Monday	00:00	Friday	23:59	Delete Periodic	Delete

Figure 3-28 Time Range Window

The fields that can be configured are described below:

Parameter	Description
Range Name	Enter the name of the time range profile here. This can be up to 32 characters long.
From Week - To Week	Select the starting and ending days of the week that will be used for this time range profile. Select the **Daily** option to use this time range profile every day. Select the **End Week Day** option to use this time range profile for a week.
From Time - To Time	Select the starting and ending time of the day that will be used for this time range 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 **Show All** button to display all entries in the table.

Click the **Delete Periodic** button to delete the periodic entry.

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

PTP (Precise Time Protocol)

The Precision Time Protocol (PTP) system is able to synchronize the distributed clocks with an accuracy of less than 1 microsecond via Ethernet networks.

PTP is a technology that enables precise synchronization of clocks in network systems. PTP is applicable to systems communicating by Local Area Networks supporting multicast messaging including Ethernet and UDP. PTP enables heterogeneous systems that include clocks of various inherent precision, resolution and stability to synchronize to a grandmaster clock.

The synchronization is divided into two processes. The Best Master Clock (BMC) algorithm determines the PTP status (master/slave) of all local ports. The synchronization algorithm computes the clock offset between the master and slave clock. There are two mechanisms, Delay Request-response Mechanism and Peer Delay Mechanism, for measuring the propagation time of an event message.

The PTP system has three types of PTP devices, boundary clock, end-to-end transparent clock, and peer-to-peer transparent clock. Only the boundary clock can participate in the selection of the best master clock.

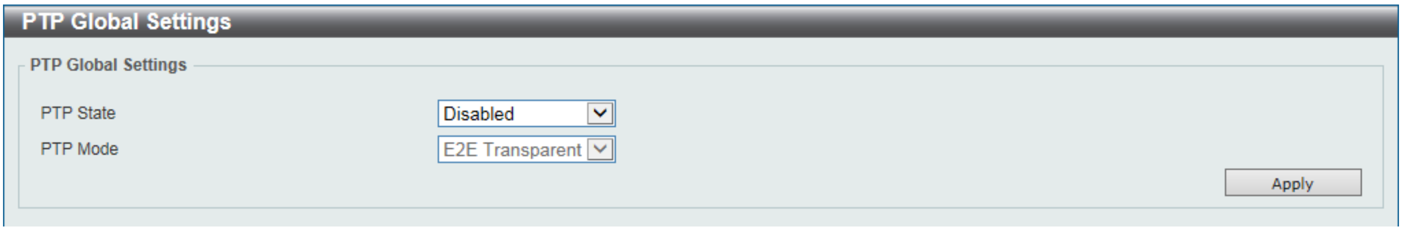
When the stacking mode is enabled and the member ports of a trunk group exists in different stack units, the PTP function will:

- Execute normally when the sending and receiving of PTP messages are to member ports that are on the same stack unit.
- Execute abnormally, when the sending and receiving of PTP messages are to member ports that are on different stack units.

PTP Global Settings

This window is used to display and configure the global Precise Time Protocol (PTP) settings.

To view the following window, click **System > PTP (Precise Time Protocol) > PTP Global Settings**, as shown below:



PTP Global Settings

PTP Global Settings

PTP State: Disabled

PTP Mode: E2E Transparent

Figure 3-29 PTP Global Settings Window

The fields that can be configured are described below:

Parameter	Description
PTP State	Select to enable or disable the PTP feature here. When the PTP function is enabled, the Switch port will add residence time to correct the field. When the PTP function is disabled, all Switch ports will forward the PTP packets according to the multicast filtering configuration.

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

When the stacking mode is enabled and the member ports of the trunk group exist in different stack units, the PTP function may not function properly.

For example:

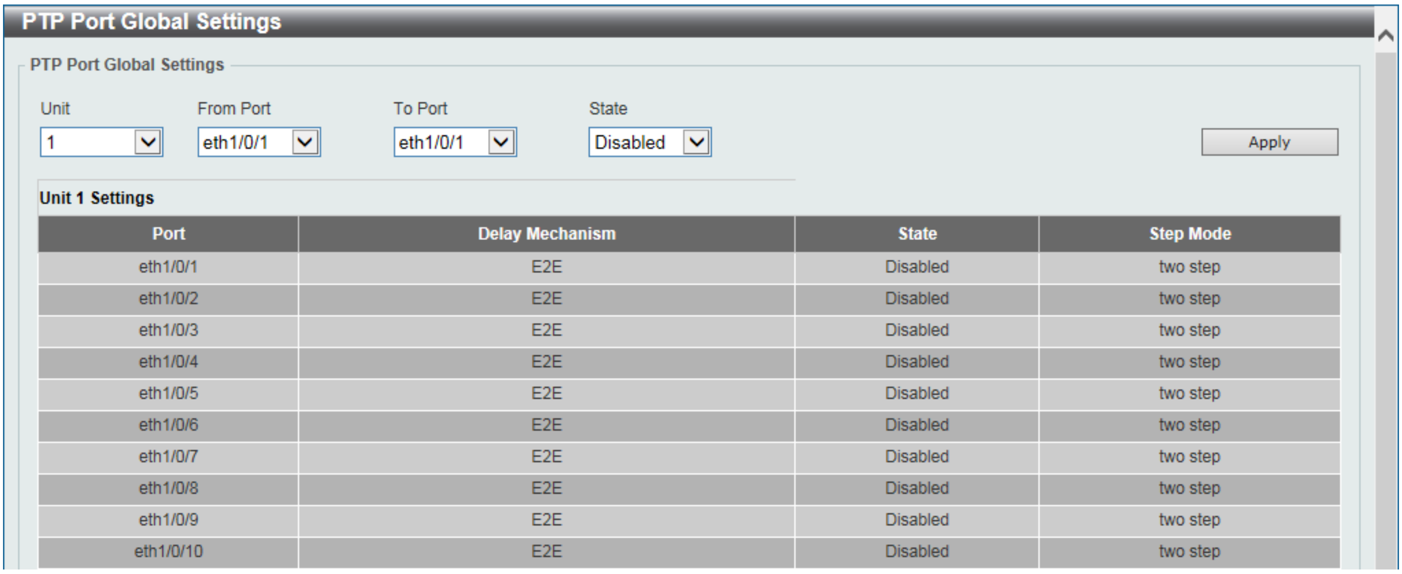
- The PTP feature will function properly when the member ports receive and send PTP messages on the same stacked unit.
- The PTP feature will not function properly when the member ports receive and send PTP messages on different stacked units.

Therefore, it is recommended not to enable the PTP feature on a trunk group that exists in different stack units.

PTP Port Global Settings

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

To view the following window, click **System > PTP (Precise Time Protocol) > PTP Port Global Settings**, as shown below:



PTP Port Global Settings

PTP Port Global Settings

Unit: 1

From Port: eth1/0/1

To Port: eth1/0/1

State: Disabled

Unit 1 Settings

Port	Delay Mechanism	State	Step Mode
eth1/0/1	E2E	Disabled	two step
eth1/0/2	E2E	Disabled	two step
eth1/0/3	E2E	Disabled	two step
eth1/0/4	E2E	Disabled	two step
eth1/0/5	E2E	Disabled	two step
eth1/0/6	E2E	Disabled	two step
eth1/0/7	E2E	Disabled	two step
eth1/0/8	E2E	Disabled	two step
eth1/0/9	E2E	Disabled	two step
eth1/0/10	E2E	Disabled	two step

Figure 3-30 PTP Port Global Settings Window

The fields that can be configured are described below:

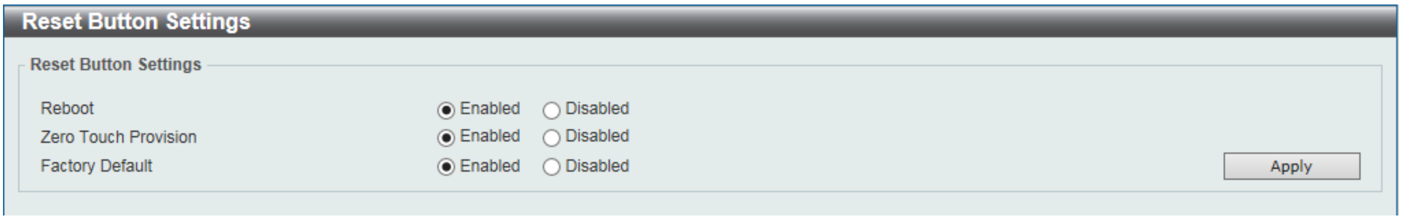
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
State	Select to enable or disable the PTP feature on the port(s) specified here.

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

Reset Button Settings

This window is used to configure the actions when pressing the reset button on the Switch.

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



Reset Button Settings

Reset Button Settings

Reboot ● Enabled ○ Disabled

Zero Touch Provision ● Enabled ○ Disabled

Factory Default ● Enabled ○ Disabled

Figure 3-31 Reset Button Settings Window

The fields that can be configured are described below:

Parameter	Description
Reboot	Select to enable or disable the rebooting action. When enabled and the reset button on the Switch is pressed and held less than 5 seconds, the DUT will reboot.

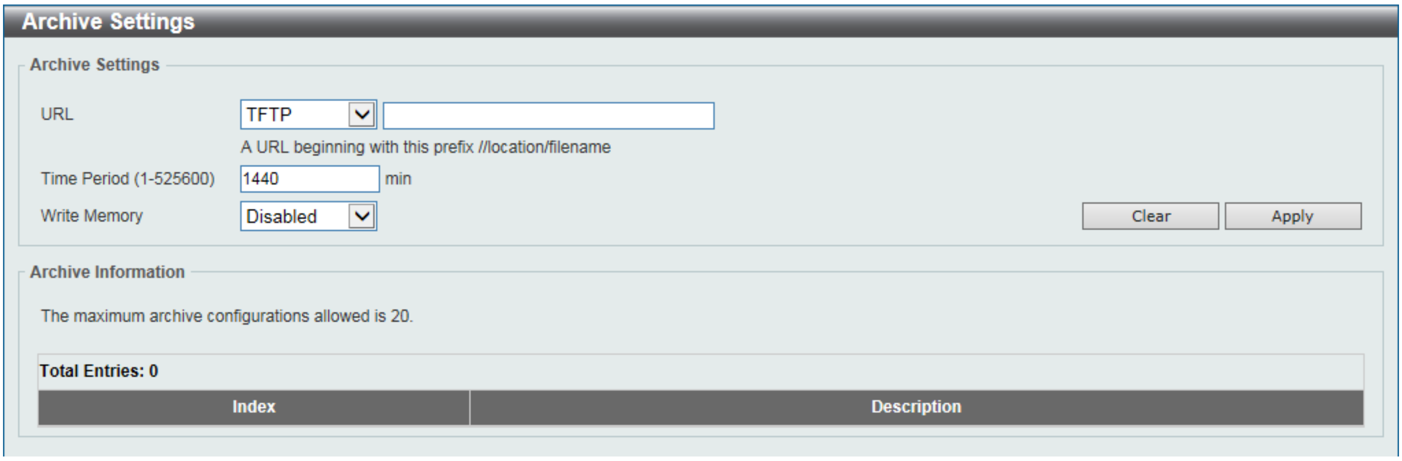
Parameter	Description
Zero Touch Provision	Select to enable or disable the ZTP action. When enabled and the reset button on the Switch is pressed and held between 5 and 10 seconds, the DUT will start the ZTP function.
Factory Default	Select to enable or disable the factory reset action. When enabled and the reset button on the Switch is pressed and held more than 10 seconds, the Switch will reboot and reset the system to its factory defaults.

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

Archive Settings

This window is used to configure the archive settings.

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



Archive Settings

Archive Settings

URL: TFTP

A URL beginning with this prefix //location/filename

Time Period (1-525600): 1440 min

Write Memory: Disabled

Archive Information

The maximum archive configurations allowed is 20.

Total Entries: 0

Index	Description

Figure 3-32 Archive Settings Window

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

Parameter	Description
URL	Select the server type and enter the IPv4/IPv6 address of the server. Available server types are **TFTP**, **FTP**, and **RCP**.
Time Period	Enter the time in minutes to archive the running configuration. The range is from 1 to 525600. By default, this value is 1440.
Write Memory	Select to enable or disable the automatic backup for the archive file.

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

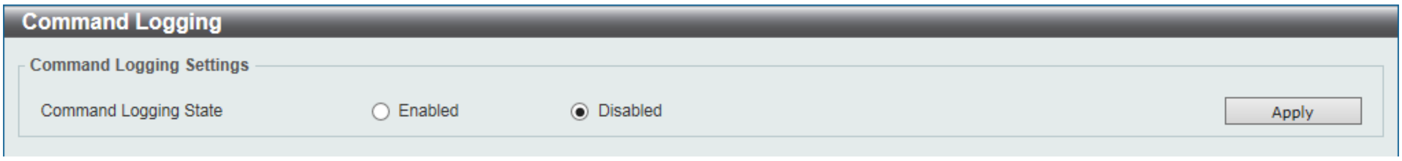
Click the **Apply** button to accept the changes made.

4. 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:



Command Logging

Command Logging Settings

Command Logging State ○ Enabled ● Disabled

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.

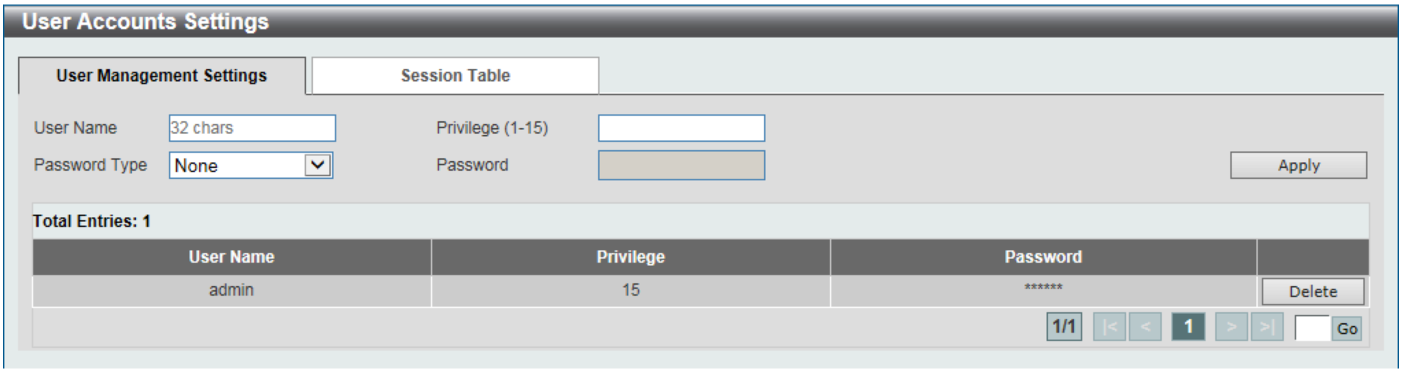
Click the **Apply** button to accept the changes made.

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**.

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

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



User Accounts Settings

User Name: 32 chars

Privilege (1-15):

Password Type: None

Password:

Total Entries: 1

User Name	Privilege	Password	
admin	15	******	Delete

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.
Privilege	Enter the privilege level for this account here. The range is from 1 to 15.
Password Type	Select the password type for this user account here. Options to choose from are **None**, **Plain Text**, **Encrypted-SHA1**, and **Encrypted-MD5**.

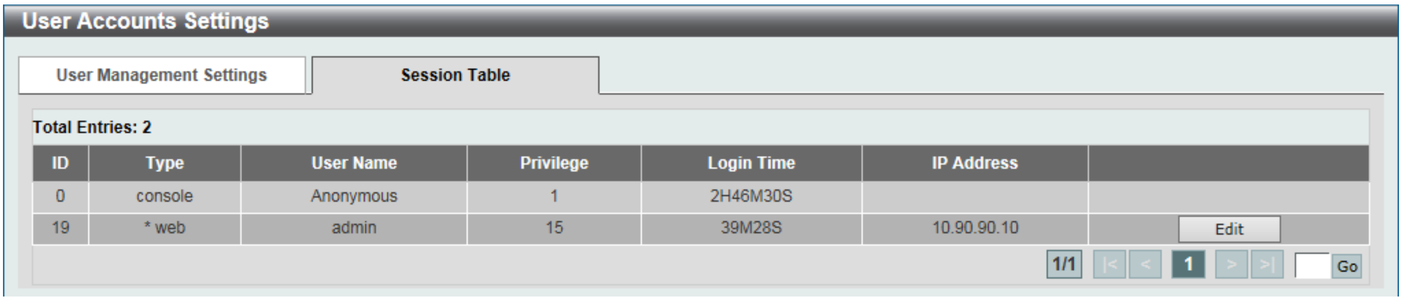
Parameter	Description
Password	After selecting **Plain Text**, **Encrypted-SHA1**, or **Encrypted-MD5** as the password type, enter the password for this user account here.

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

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

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

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



Total Entries: 2

ID	Type	User Name	Privilege	Login Time	IP Address	
0	console	Anonymous	1	2H46M30S		
19	* web	admin	15	39M28S	10.90.90.10	Edit

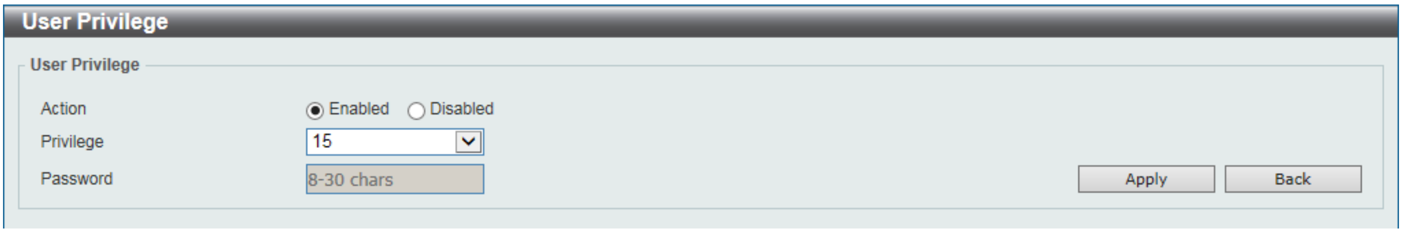
Figure 4-3 Session Table Window

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

Click the **Edit** button to access and configure the User Privilege settings.

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

After selecting the **Edit** button, the following page will appear.



Action ● Enabled ○ Disabled

Privilege 15

Password 8-30 chars

Figure 4-4 User Privilege Window

The fields that can be configured are described below:

Parameter	Description
Action	Select to enable or disable user level security.
Privilege	Select the privilege level here. The range is from 1 to 15.
Password	Enter the password here. The minimum strength of the password: • Must contain 8 to 30 UTF-8 characters (Unicode hex range 0x0021–0x007e) • Must include at least one uppercase and one lowercase alphabetical letter • Must have at least one numerical digit • Must include at least one special symbol • Must consist of non-consecutive characters • Must not be the same as the username • Must not include the default login account and default IP address

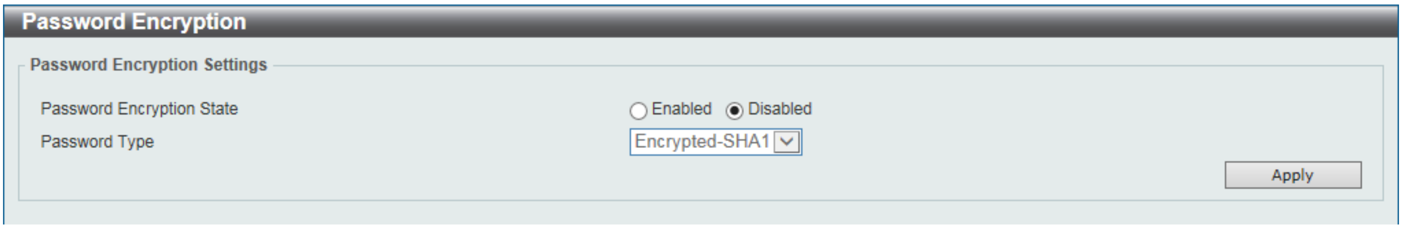
Click the **Apply** button to accept the changes made.

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

Password Encryption

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

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


Password Encryption

Password Encryption Settings

Password Encryption State ○ Enabled ● Disabled

Password Type: Encrypted-SHA1

Figure 4-5 Password Encryption Window

The fields that can be configured are described below:

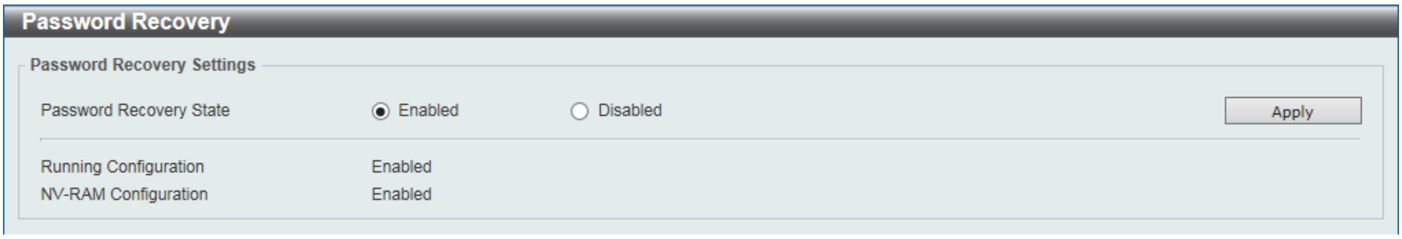
Parameter	Description
Password Encryption State	Select this option to enable or disable the encryption of the password before being stored in the configuration file.
Password Type	When the state is enabled, select the password encryption type here. Options to choose from are: • **Encrypted-SHA1 -** Specifies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


Password Recovery

Password Recovery Settings

Password Recovery State ● Enabled ○ Disabled

Running Configuration Enabled

NV-RAM Configuration Enabled

Figure 4-6 Password Recovery Window

The fields that can be configured are described below:

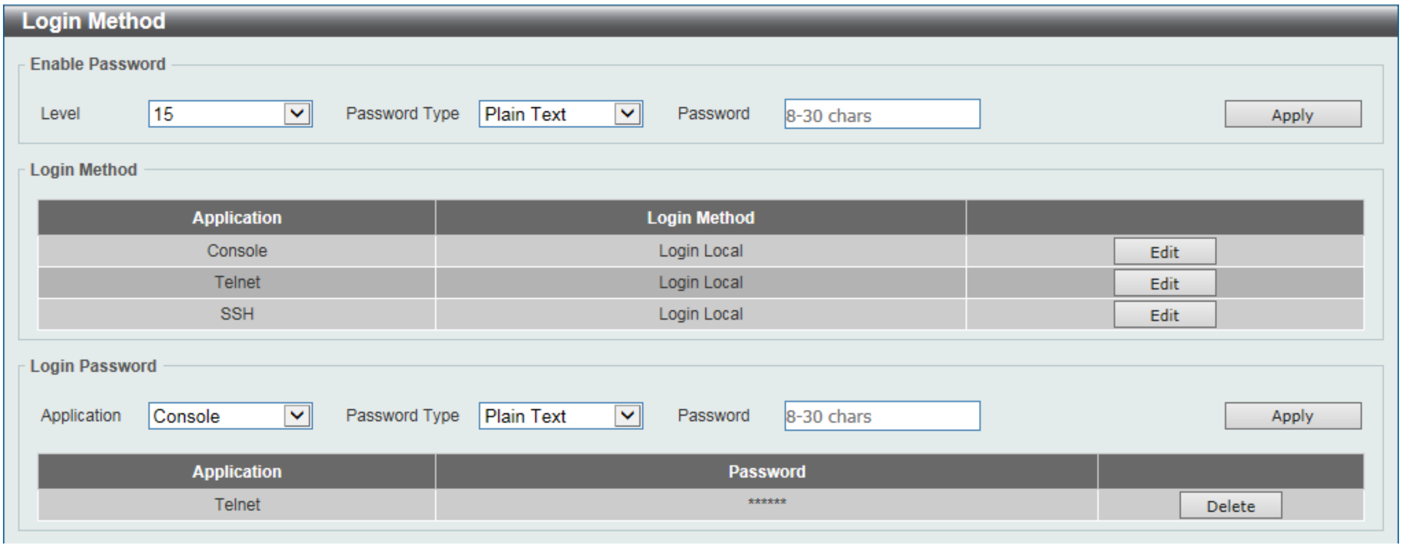
Parameter	Description
Password Recovery State	Select to enable or disable the password recovery feature here. Enabling this feature allows access to the reset configuration mode in the CLI. From the reset configuration mode, user accounts can be updated, the enable password feature can be updated for 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:



Login Method

Enable Password

Level: 15 — Password Type: Plain Text — Password: 8-30 chars — Apply

Login Method

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

Login Password

Application: Console — Password Type: Plain Text — Password: 8-30 chars — Apply

Application	Password	
Telnet	******	Delete

Figure 4-7 Login Method Window

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

Parameter	Description
Level	Select the privilege level for the user here. The range is from 1 to 15.
Password Type	Select the password type for the user here. Options to choose from are: • **Plain Text** - Specifies that the password will be in plain text. • **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. By default, the **Plain Text** option is used.
Password	Enter the password for the user account here. In the plain-text form, the minimum strength of the password: • Must contain 8 to 30 UTF-8 characters (Unicode hex range 0x0021–0x007e) • Must include at least one uppercase and one lowercase alphabetical letter • Must have at least one numerical digit • Must include at least one special symbol • Must consist of non-consecutive characters • Must not be the same as the username • Must not include the default login account and default IP address In the encrypted form, the password must be 35 bytes long and is case-sensitive. In the encrypted MD5 form, the password must be 31 bytes long and is case-sensitive.

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

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

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

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

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

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

Parameter	Description
Application	Select the application that will be configured here. Options to choose from are **Console**, **Telnet** and **SSH**.
Password Type	Select the password encryption type that will be used here. Options to choose from are **Plain Text**, **Encrypted-SHA1**, 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 minimum strength of the password: • Must contain 8 to 30 UTF-8 characters (Unicode hex range 0x0021–0x007e) • Must include at least one uppercase and one lowercase alphabetical letter • Must have at least one numerical digit • Must include at least one special symbol • Must consist of non-consecutive characters • Must not be the same as the username • Must not include the default login account and default IP address In the encrypted form, the password must be 35 bytes long and is case-sensitive. In the encrypted MD5 form, the password must be 31 bytes long and is case-sensitive.

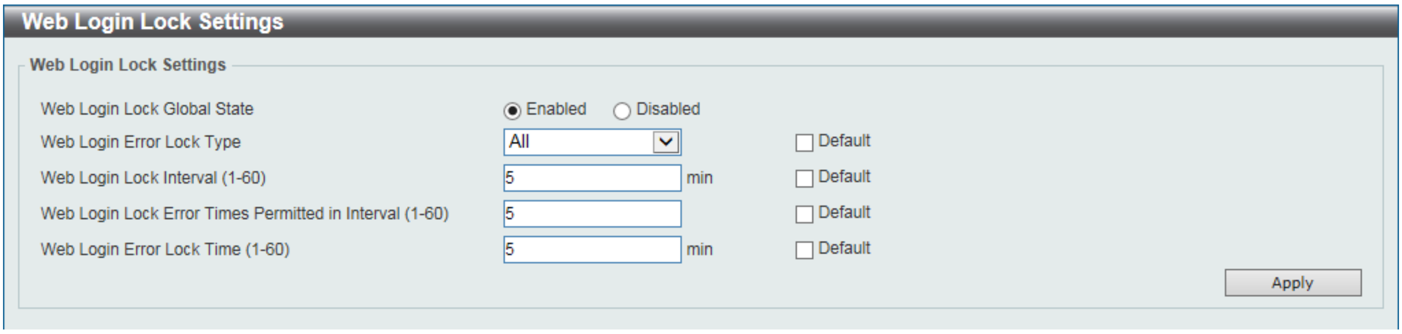
Click the **Apply** button to accept the changes made.

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

Web Login Lock Settings

This window is used to configure web login lock settings.

To view the following window, click **Management > Web Login Lock Settings**, as shown below:



Web Login Lock Settings

Web Login Lock Settings

Web Login Lock Global State	● Enabled ○ Disabled	
Web Login Error Lock Type	All	□ Default
Web Login Lock Interval (1-60)	5 min	□ Default
Web Login Lock Error Times Permitted in Interval (1-60)	5	□ Default
Web Login Error Lock Time (1-60)	5 min	□ Default

Figure 4-8 Web Login Lock Settings Window

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

Parameter	Description
Web Login Lock Global State	Select to enable or disable the web login lock function here.
Web Login Error Lock Type	Select the lock type here. Options to choose from are: • **All** - Specifies that the web login is locked by IPv4 and IPv6 addresses. • **IP** - Specifies that the web login is locked by IPv4 address. • **IPv6** - Specifies that the web login is locked by IPv6 address. • **Web Session ID** - Specifies that the web login is locked by web session ID. By default, the lock type is **All**.
Web Login Lock Interval	Enter the interval for checking the web login errors. The range is from 1 to 60 minutes. By default, this value is 5 minutes.
Web Login Lock Error Times Permitted in Interval	Enter the number of the web login errors within the interval. The range is from 1 to 60. By default, this value is 5.
Web Login Error Lock Time	Enter the lock time after the login errors are detected. The range is from 1 to 60 minutes. By default, this value is 5 minutes.

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

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.

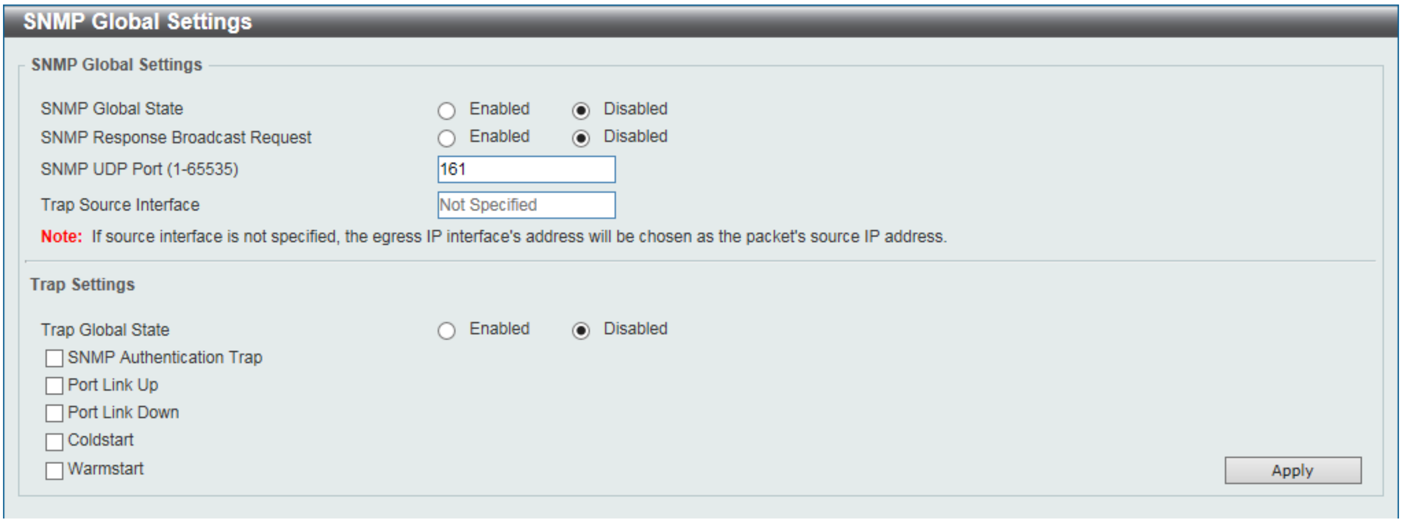
Traps

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:



SNMP Global Settings

SNMP Global Settings

SNMP Global State ○ Enabled ● Disabled

SNMP Response Broadcast Request ○ Enabled ● Disabled

SNMP UDP Port (1-65535) 161

Trap Source Interface Not Specified

Note: If source interface is not specified, the egress IP interface's address will be chosen as the packet's source IP address.

Trap Settings

Trap Global State ○ Enabled ● Disabled

□ SNMP Authentication Trap

□ Port Link Up

□ Port Link Down

□ Coldstart

□ Warmstart

Figure 4-9 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.

Parameter	Description
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:

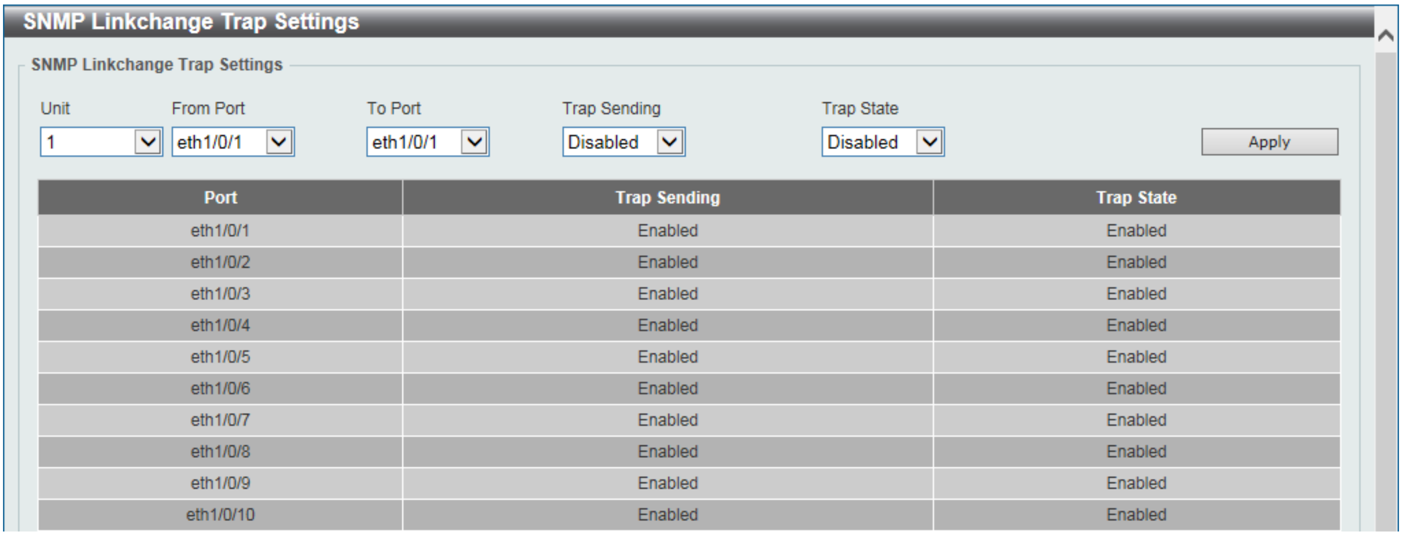
Parameter	Description
Trap Global State	Select this option to enable or disable the sending of all or specific SNMP notifications.
SNMP Authentication Trap	Tick this option to control the sending of SNMP authentication failure notifications. An *authenticationFailuretrap* trap is generated when the device 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.
Port Link Up	Tick this option to control the sending of port link up notifications. A *linkUp* trap is generated when the device recognizes that one of the communication links has come up.
Port Link Down	Tick this option to control the sending of port link down notifications. A *linkDown* trap is generated when the device recognizes that a one of the communication links is down.
Coldstart	Tick this option to control the sending of SNMP *coldStart* notifications.
Warmstart	Tick this option to control the sending of SNMP *warmStart* notifications.

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

SNMP Linkchange Trap Settings

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

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



SNMP Linkchange Trap Settings

SNMP Linkchange Trap Settings

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

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

Figure 4-10 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.
From Port - To Port	Select the appropriate port range used for the configuration here.

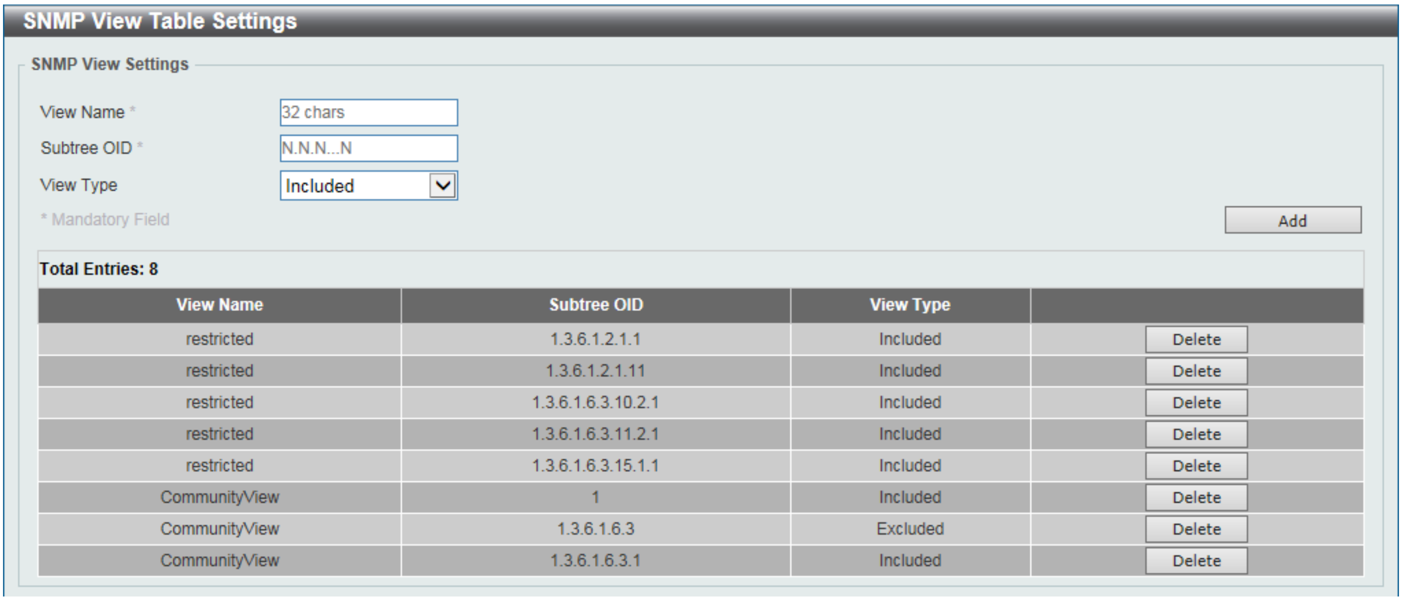
Parameter	Description
Trap Sending	Select this option to enable or disable the sending of the SNMP notification traps that are generated by the system.
Trap State	Select this option to enable or disable the SNMP *linkChange* trap.

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

SNMP View Table Settings

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

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



SNMP View Table Settings

SNMP View Settings

View Name * 32 chars

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

View Type Included

* Mandatory Field

Total Entries: 8

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

Figure 4-11 SNMP View Table Settings Window

The fields that can be configured are described below:

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

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

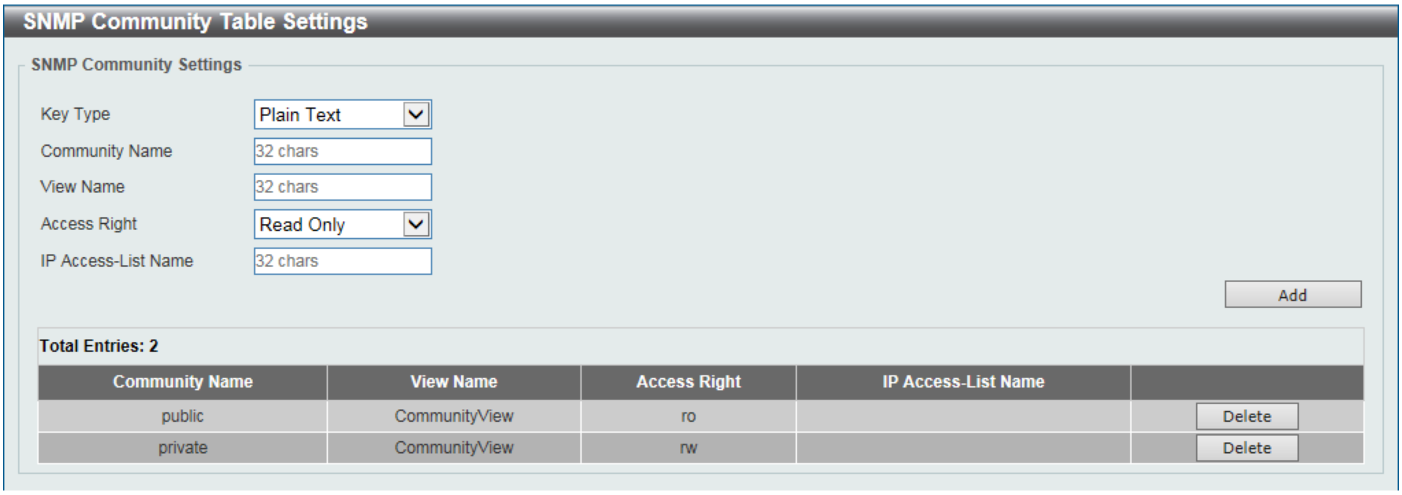
Click the **Delete** button to remove the specified entry.

SNMP Community Table Settings

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

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

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



SNMP Community Table Settings

SNMP Community Settings

Key Type: Plain Text

Community Name: 32 chars

View Name: 32 chars

Access Right: Read Only

IP Access-List Name: 32 chars

Total Entries: 2

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

Figure 4-12 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** - SNMP community members using the community string created can only read the contents of the MIBs on the Switch. • **Read Write** - SNMP community members using the community string created can read from, and write to the contents of the MIBs on the Switch.
IP Access-List Name	Enter the name of the standard access list to restrict the users that can use this community string to access to the SNMP agent.

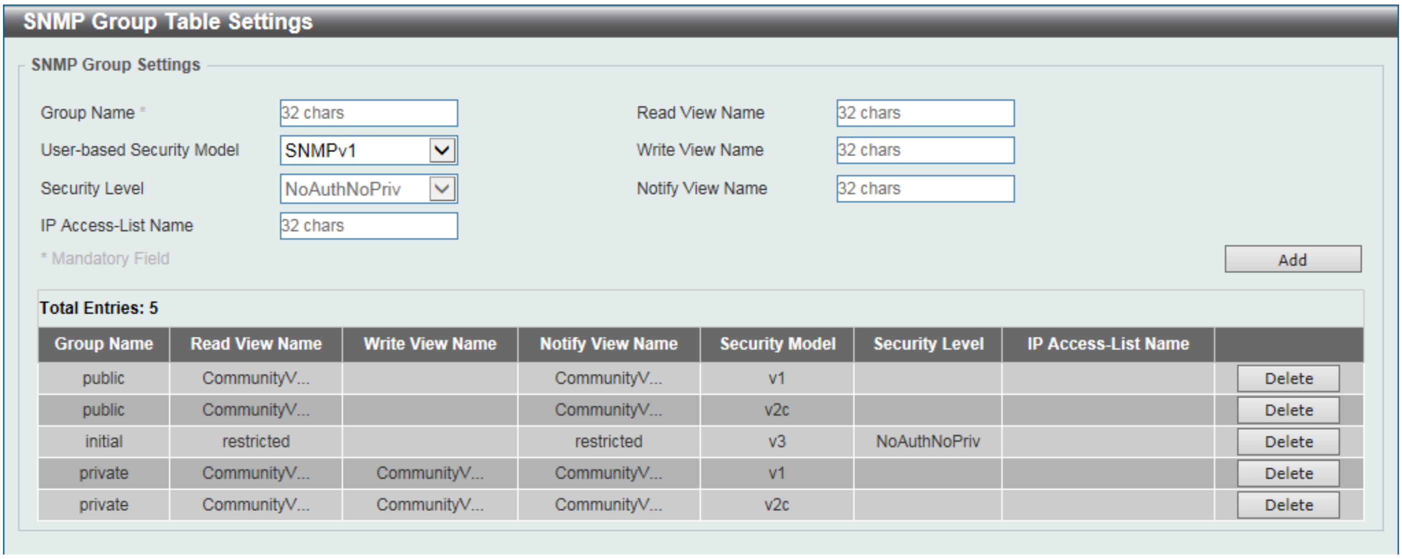
Click the **Add** button to add a new entry based on the information entered.

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

SNMP Group Table Settings

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

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



SNMP Group Table Settings

SNMP Group Settings

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

* Mandatory Field

Total Entries: 5

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

Figure 4-13 SNMP Group Table Settings Window

The fields that can be configured are described below:

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

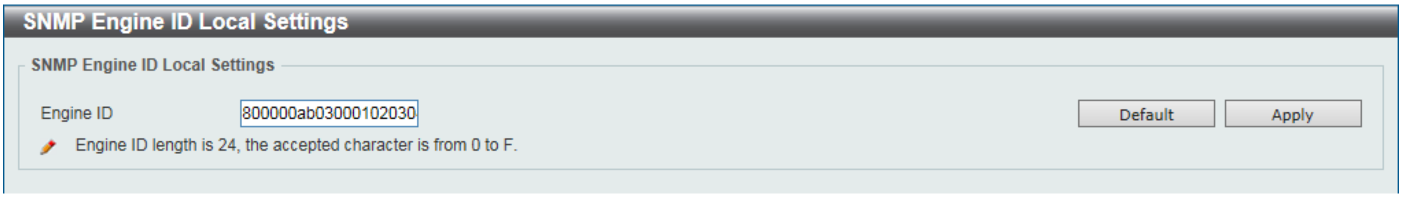
Click the **Add** button to add a new entry based on the information entered.

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

SNMP Engine ID Local Settings

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

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



SNMP Engine ID Local Settings

SNMP Engine ID Local Settings

Engine ID: 800000ab03000102030

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

Figure 4-14 SNMP Engine ID Local Settings Window

The fields that can be configured are described below:

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

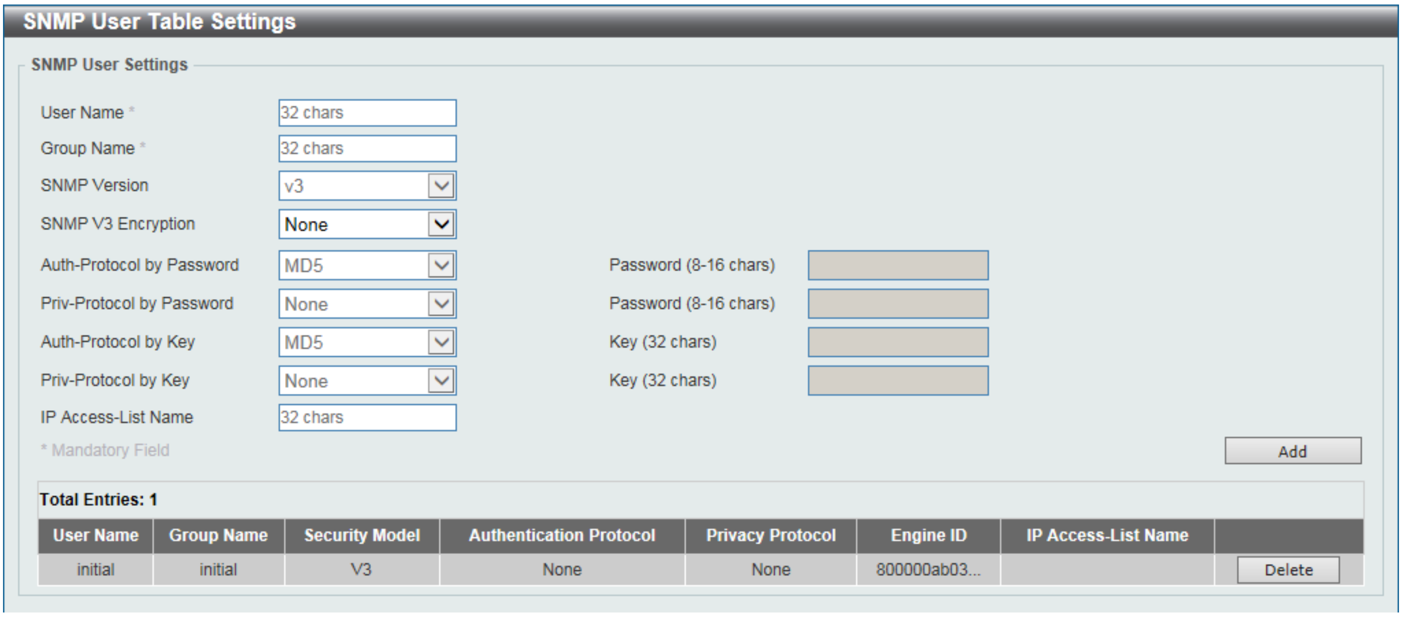
Click the **Default** button to revert the engine ID to the default.

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

SNMP User Table Settings

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

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



SNMP User Table Settings

SNMP User Settings

User Name *: 32 chars

Group Name *: 32 chars

SNMP Version: v3

SNMP V3 Encryption: None

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

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

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

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

IP Access-List Name: 32 chars

* Mandatory Field

Total Entries: 1

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

Figure 4-15 SNMP User Table Settings Window

The fields that can be configured are described below:

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

Parameter	Description
SNMP Version	Specifies that SNMP version 3 (SNMPv3) is used.
SNMP V3 Encryption	Select the SNMPv3 encryption type here. Options to choose from are **None**, **Password**, and **Key**.
Auth-Protocol by Password	After selecting the **Password** encryption type, select the authentication protocol here. Options to choose from are: • **MD5** - Specifies to use the HMAC-MD5-96 authentication protocol. Enter the password in the **Password** textbox. The password can be from 8 to 16 characters long. • **SHA** - Specifies to use the HMAC-SHA authentication protocol. Enter the password in the **Password** textbox. The password can be from 8 to 20 characters long.
Priv-Protocol by Password	After selecting the **Password** encryption type, select the private protocol here. Options to choose from are: • **None** - Specifies to use no authorization protocol. • **DES56** - Specifies to use DES 56-bit encryption based on the CBC-DES (DES-56) standard. Enter the password in the **Password** textbox. The password can be from 8 to 16 characters long. • **AES** - Specifies to use Advanced Encryption Standard (AES) encryption. Enter the password in the **Password** textbox. The password can be from 8 to 16 characters long.
Auth-Protocol by Key	After selecting the **Key** encryption type, select the authentication protocol here. Options to choose from are: • **MD5** - Specifies to use the HMAC-MD5-96 authentication protocol. Enter the key in the **Key** textbox. The key must be 32 characters long. • **SHA** - Specifies to use the HMAC-SHA authentication protocol. Enter the key in the **Key** textbox. The key must be 40 characters long.
Priv-Protocol by Key	After selecting the **Key** encryption type, select the private protocol here. Options to choose from are: • **None** - Specifies to use no authorization protocol. • **DES56** - Specifies to use DES 56-bit encryption, based on the CBC-DES (DES-56) standard. Enter the key in the **Key** textbox. The key must be 32 characters long. • **AES** - Specifies to use AES encryption. Enter the key in the **Key** textbox. The key must be 32 characters long.
IP Access-List Name	Enter the standard IP access control list to associate with the user.

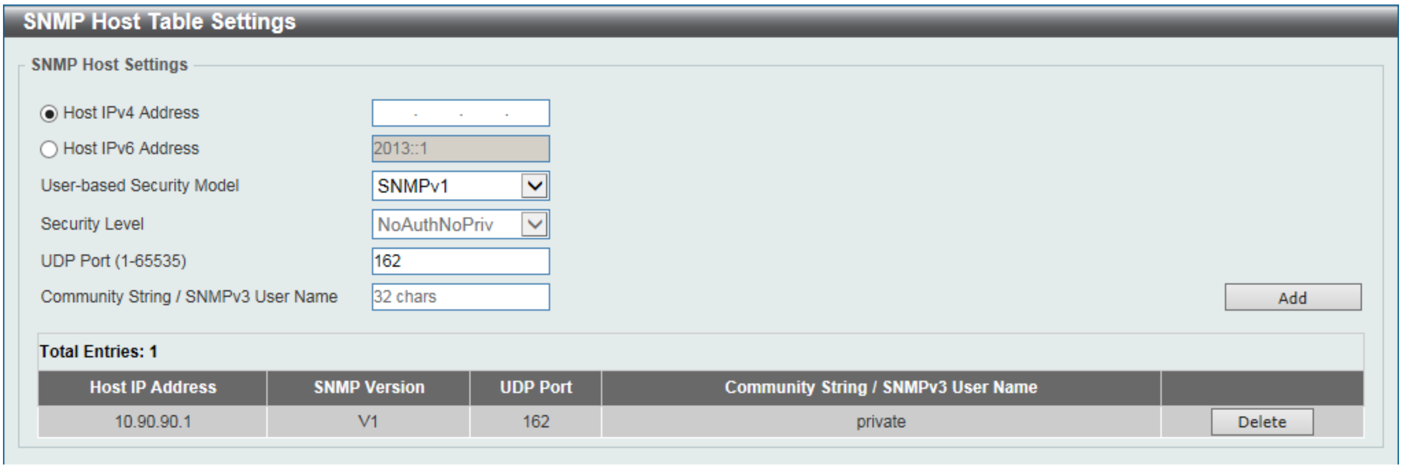
Click the **Add** button to add a new entry based on the information entered.

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

SNMP Host Table Settings

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

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



SNMP Host Table Settings

SNMP Host Settings

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

Total Entries: 1

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

Figure 4-16 SNMP Host Table Settings Window

The fields that can be configured are described below:

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

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

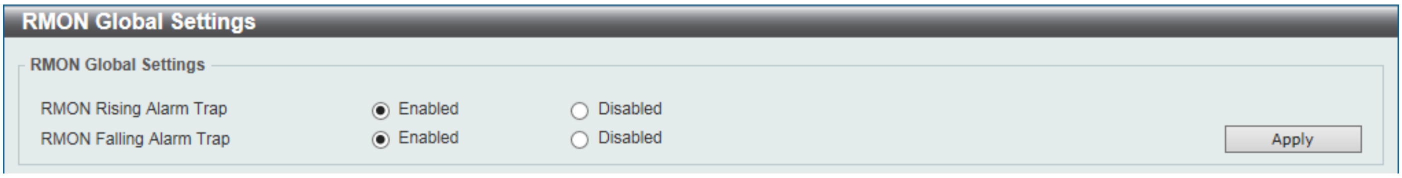
Click the **Delete** button to remove the specified entry.

RMON

RMON Global Settings

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

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



RMON Global Settings

RMON Global Settings

RMON Rising Alarm Trap ● Enabled ○ Disabled

RMON Falling Alarm Trap ● Enabled ○ Disabled

Figure 4-17 RMON Global Settings Window

The fields that can be configured are described below:

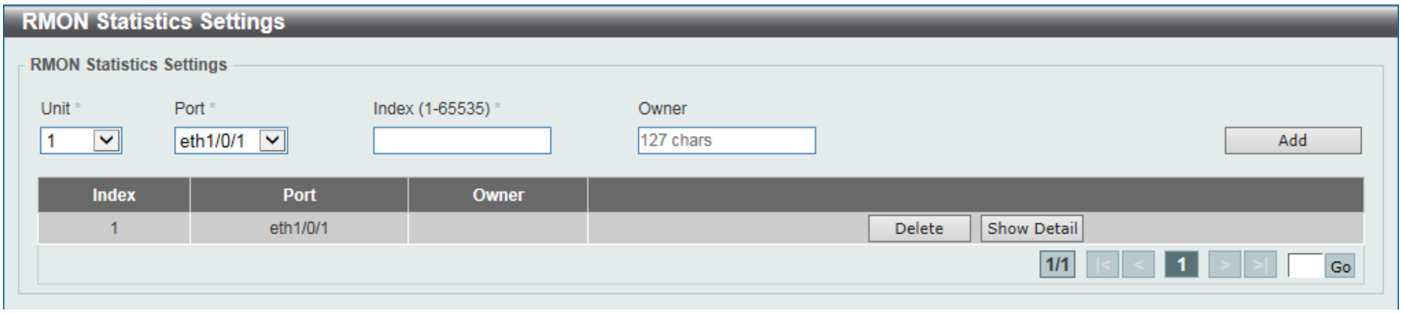
Parameter	Description
RMON Rising Alarm Trap	Select this option to enable or disable the RMON Rising Alarm Trap Feature.
RMON Falling Alarm Trap	Select this option to enable or disable the RMON Falling Alarm Trap Feature.

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

RMON Statistics Settings

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

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



RMON Statistics Settings

RMON Statistics Settings

Unit * : 1

Port * : eth1/0/1

Index (1-65535) * :

Owner : 127 chars

Index	Port	Owner	
1	eth1/0/1		Delete Show Detail

Figure 4-18 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.
Port	Select to choose the port.
Index	Enter the RMON table index. The value is from 1 to 65535.
Owner	Enter the owner string. The string can be up to 127 characters.

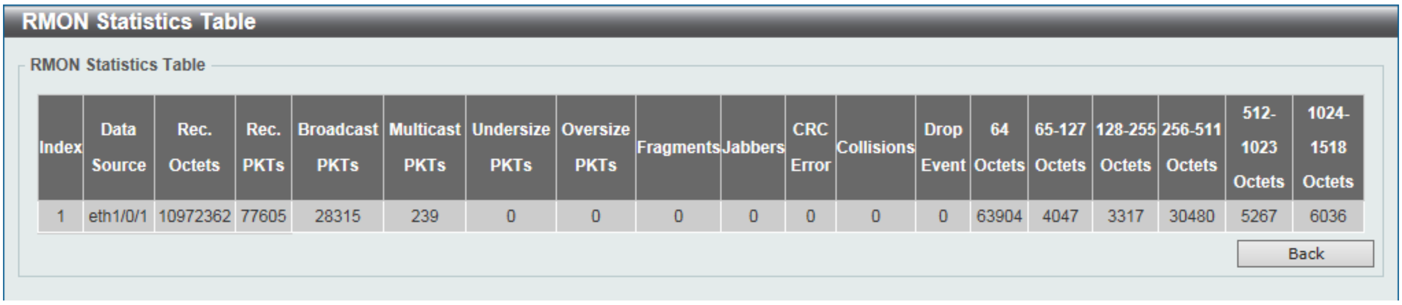
Click the **Add** button to add a new entry based on the information entered.

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

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

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

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



RMON Statistics Table

RMON Statistics Table

Index	Data Source	Rec. Octets	Rec. PKTs	Broadcast PKTs	Multicast PKTs	Undersize PKTs	Oversize PKTs	Fragments	Jabbers	CRC Error	Collisions	Drop Event	64 Octets	65-127 Octets	128-255 Octets	256-511 Octets	512-1023 Octets	1024-1518 Octets
1	eth1/0/1	10972362	77605	28315	239	0	0	0	0	0	0	0	63904	4047	3317	30480	5267	6036

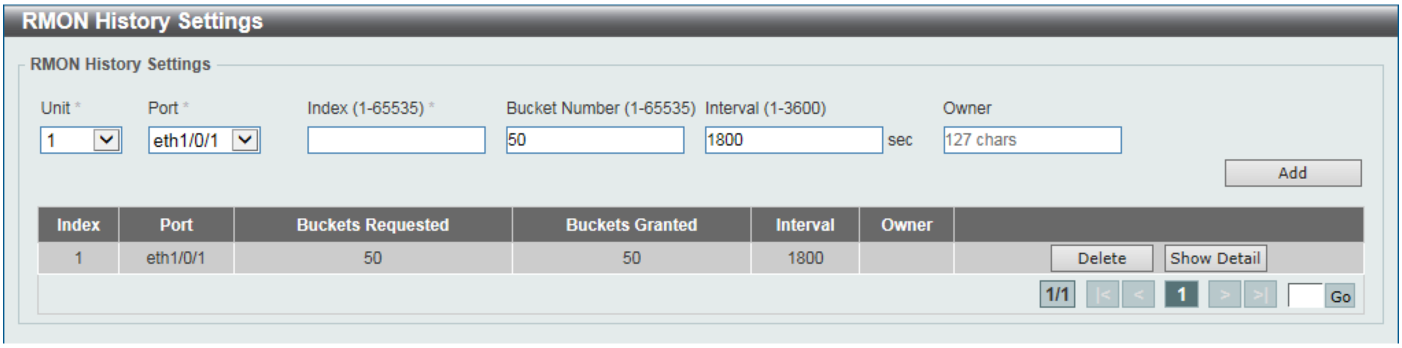
Figure 4-19 RMON Statistics Settings (Show Detail) Window

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

RMON History Settings

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

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



RMON History Settings

RMON History Settings

Unit *: 1
Port *: eth1/0/1
Index (1-65535) *:
Bucket Number (1-65535): 50
Interval (1-3600): 1800 sec
Owner: 127 chars

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

Figure 4-20 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.
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. By default, this value is 50.
Interval	Enter the time in seconds in each polling cycle. The range is from 1 to 3600.
Owner	Enter the owner string. The string can be up to 127 characters.

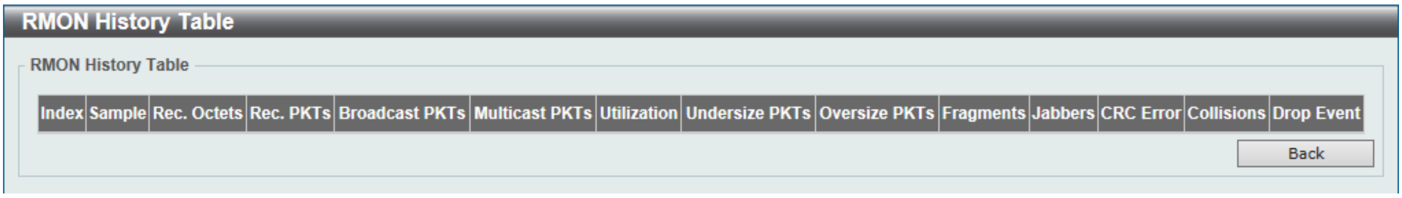
Click the **Add** button to add a new entry based on the information entered.

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

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

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

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



RMON History Table

RMON History Table

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

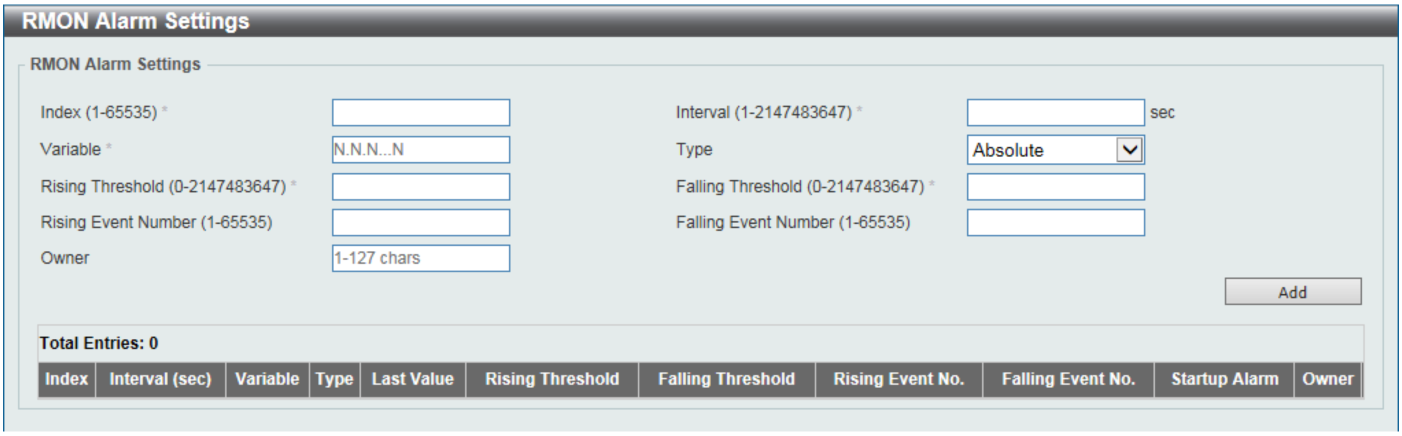
Figure 4-21 RMON History Settings (Show Detail) Window

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

RMON Alarm Settings

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

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



RMON Alarm Settings

RMON Alarm Settings

Index (1-65535) *

Interval (1-2147483647) * sec

Variable * N.N.N...N

Type Absolute

Rising Threshold (0-2147483647) *

Falling Threshold (0-2147483647) *

Rising Event Number (1-65535)

Falling Event Number (1-65535)

Owner 1-127 chars

Total Entries: 0

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

Figure 4-22 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 range is from 1 to 2147483647 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 here. The range is from 0 to 2147483647.
Falling Threshold	Enter the falling threshold value here. The range is from 0 to 2147483647.
Rising Event Number	Enter the index of the event entry that is used to notify the rising threshold-crossing event. The 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 range is from 1 to 65535. If not specified, no action is taken while crossing the falling threshold.
Owner	Enter the owner string up to 127 characters.

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

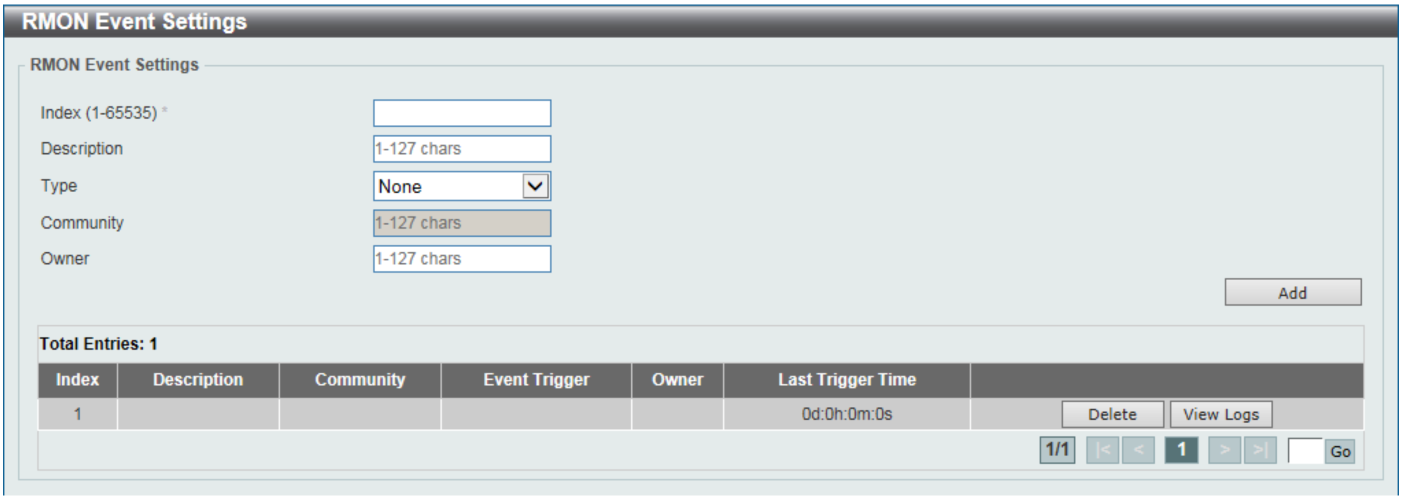
Click the **Delete** button to remove the specified entry.

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

RMON Event Settings

This window is used to display and configure event entries.

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



RMON Event Settings

RMON Event Settings

Index (1-65535) *

Description: 1-127 chars

Type: None

Community: 1-127 chars

Owner: 1-127 chars

Total Entries: 1

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

Figure 4-23 RMON Event Settings Window

The fields that can be configured are described below:

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

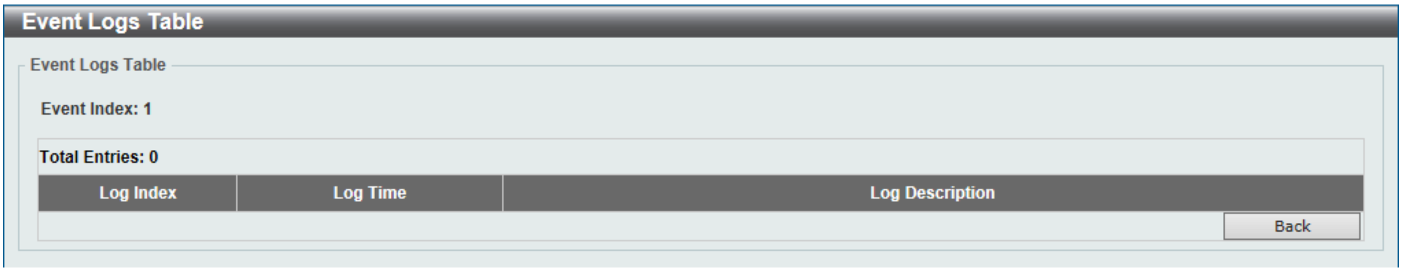
Click the **Add** button to add a new entry based on the information entered.

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

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

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

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



Event Logs Table

Event Logs Table

Event Index: 1

Total Entries: 0

Log Index	Log Time	Log Description

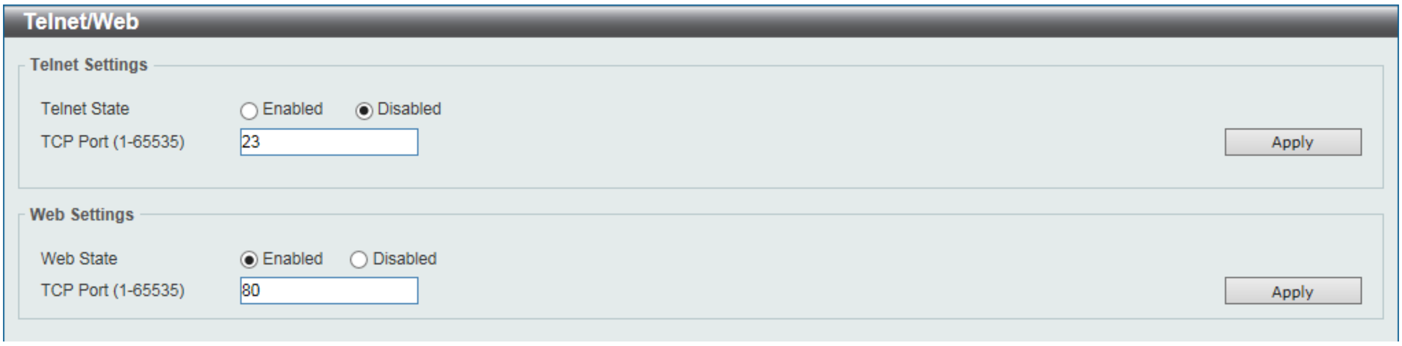
Figure 4-24 RMON Event Settings (View Logs) Window

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

Telnet/Web

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

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



Telnet/Web

Telnet Settings

Telnet State ○ Enabled ● Disabled

TCP Port (1-65535) 23

Web Settings

Web State ● Enabled ○ Disabled

TCP Port (1-65535) 80

Figure 4-25 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 **Web Settings** are described below:

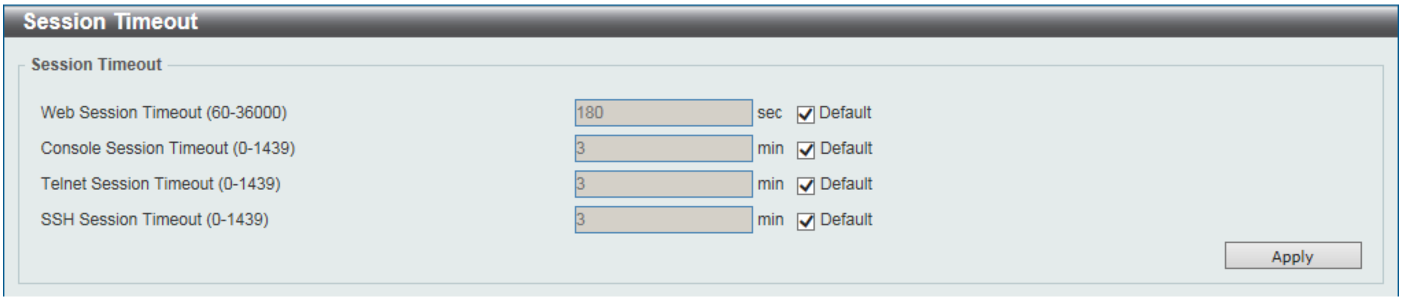
Parameter	Description
Web State	Select this option to enable or disable the configuration through the web.
Port	Enter the TCP port number used for Web management of the Switch. The well-known TCP port for the Web protocol is 80.

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

Session Timeout

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

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



Session Timeout

Session Timeout

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

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

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

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

Figure 4-26 Session Timeout Window

The fields that can be configured are described below:

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

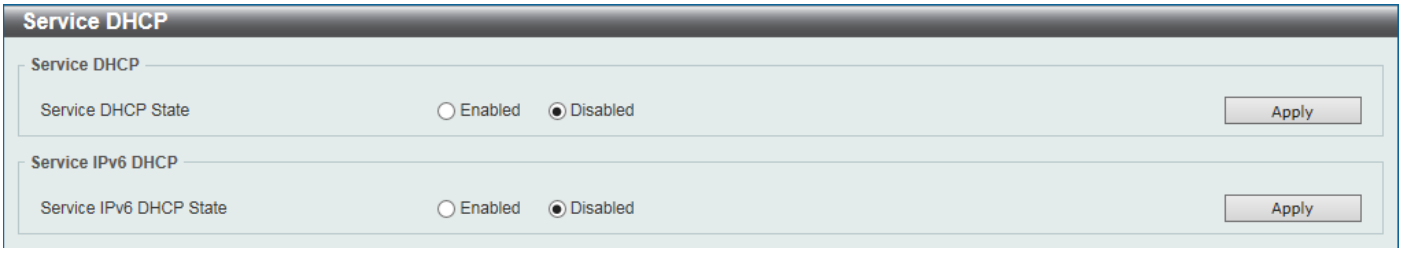
Click the **Apply** button to accept the changes made.

DHCP

Service DHCP

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

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



Service DHCP

Service DHCP

Service DHCP State ○ Enabled ● Disabled

Service IPv6 DHCP

Service IPv6 DHCP State ○ Enabled ● Disabled

Figure 4-27 Service DHCP Window

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

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

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

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

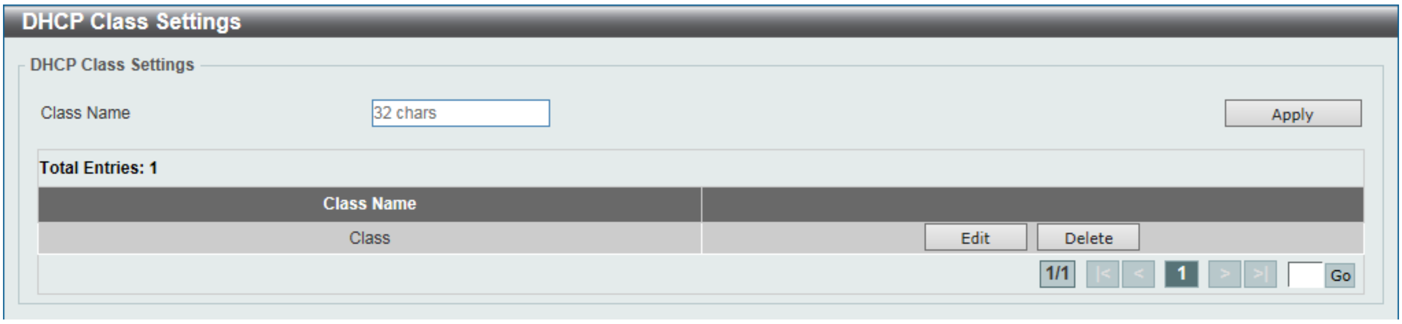
Parameter	Description
Service IPv6 DHCP State	Select this option to enable or disable the IPv6 DHCP service.

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

DHCP Class Settings

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

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



DHCP Class Settings

DHCP Class Settings

Class Name: 32 chars

Total Entries: 1

Class Name	
Class	Edit Delete

Figure 4-28 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.

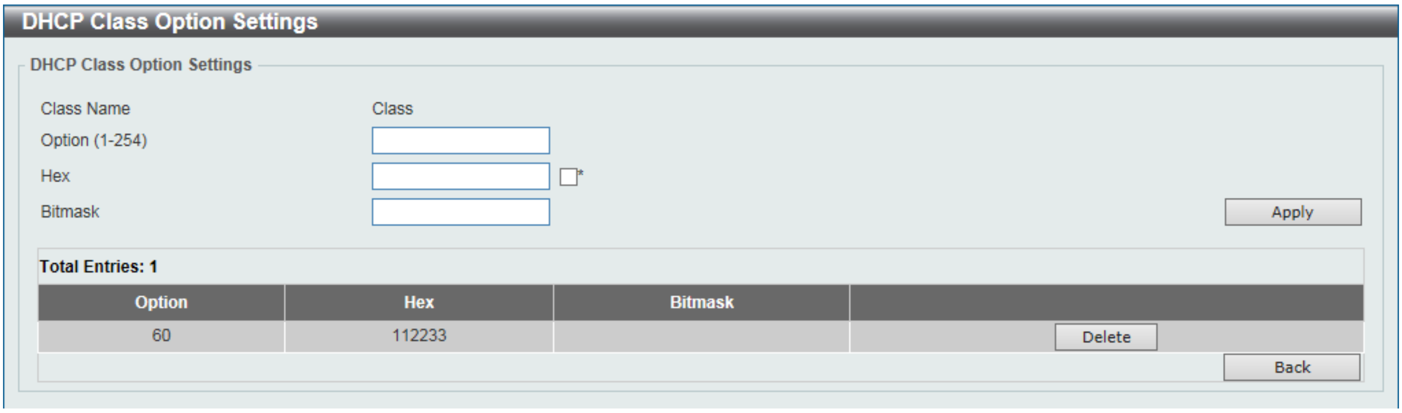
Click the **Apply** button to accept the changes made.

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.



DHCP Class Option Settings

DHCP Class Option Settings

Class Name: Class

Option (1-254)

Hex □*

Bitmask

Total Entries: 1

Option	Hex	Bitmask	
60	112233		Delete

Figure 4-29 DHCP Class Option Settings 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. Select 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.

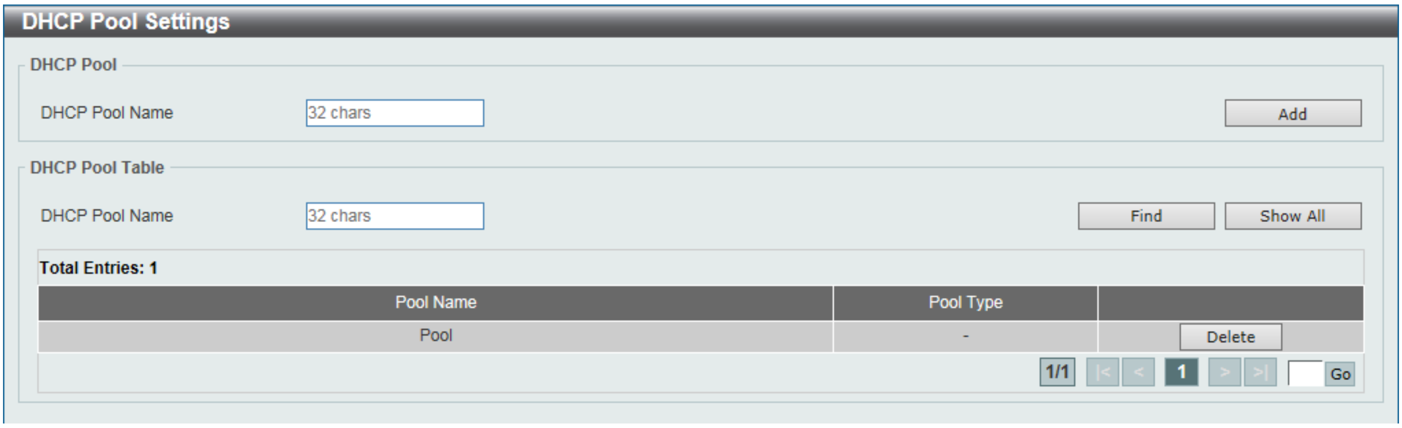
Click the **Delete** button to remove the specified entry.

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

DHCP Pool Settings

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

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



Total Entries: 1

Pool Name	Pool Type	
Pool	-	Delete

Figure 4-30 DHCP Pool Settings Window

The fields that can be configured are described below:

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

Click the **Add** button to add a new DHCP pool.

Click the **Find** button to find and display the DHCP pool in the table.

Click the **Show All** button to display all the DHCP pools in the table.

Click the **Delete** button to delete the specified DHCP pool.

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

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.

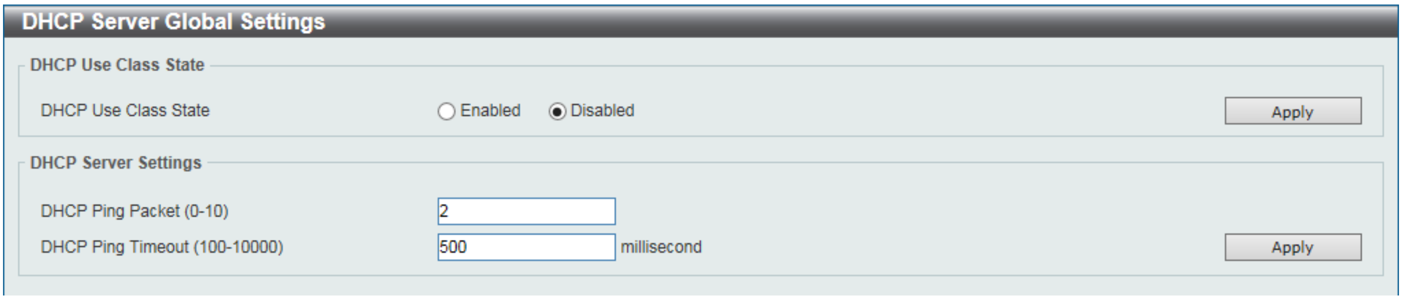
The user can configure many DHCP related parameters that it will utilize on its locally attached network, to control and limit the IP settings of clients desiring an automatic IP configuration, such as the lease time of the allocated IP address, the range of IP addresses that will be allowed in its DHCP 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:



DHCP Server Global Settings

DHCP Use Class State

DHCP Use Class State ○ Enabled ● Disabled

DHCP Server Settings

DHCP Ping Packet (0-10): 2

DHCP Ping Timeout (100-10000): 500 millisecond

Figure 4-31 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:

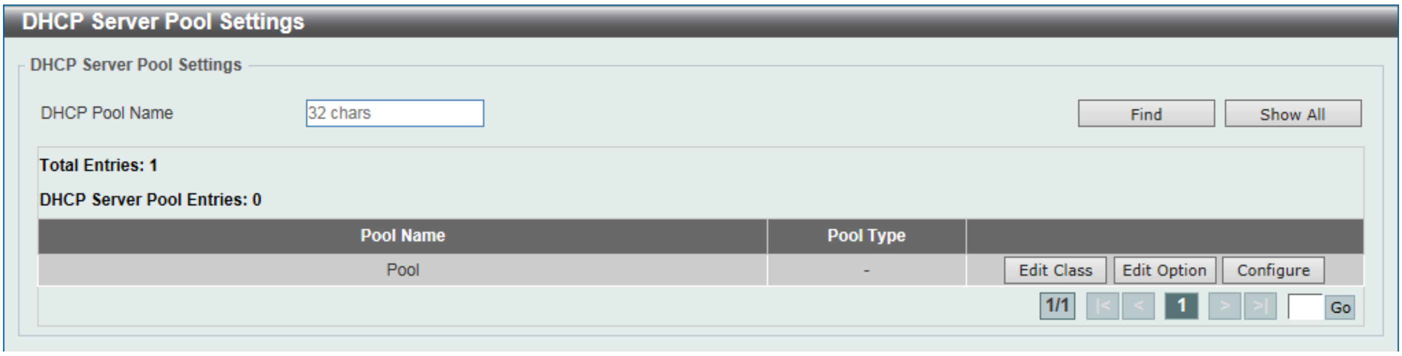
Parameter	Description
DHCP Ping Packet	Enter the number of ping packets that the Switch will send out on the network containing the IP address to be allotted. If the ping request is not returned, the IP address is considered unique to the local network and then allotted to the requesting client. A value of 0 means there is no ping test. The range is from 0 to 10. By default, this 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. By default, this 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:



DHCP Server Pool Settings

DHCP Pool Name: 32 chars

Total Entries: 1

DHCP Server Pool Entries: 0

Pool Name	Pool Type	
Pool	-	Edit Class Edit Option Configure

Figure 4-32 DHCP Server Pool Settings Window

The fields that can be configured are described below:

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

Click the **Find** button to find and display the DHCP pool in the table.

Click the **Show All** button to display all the DHCP pools in the table.

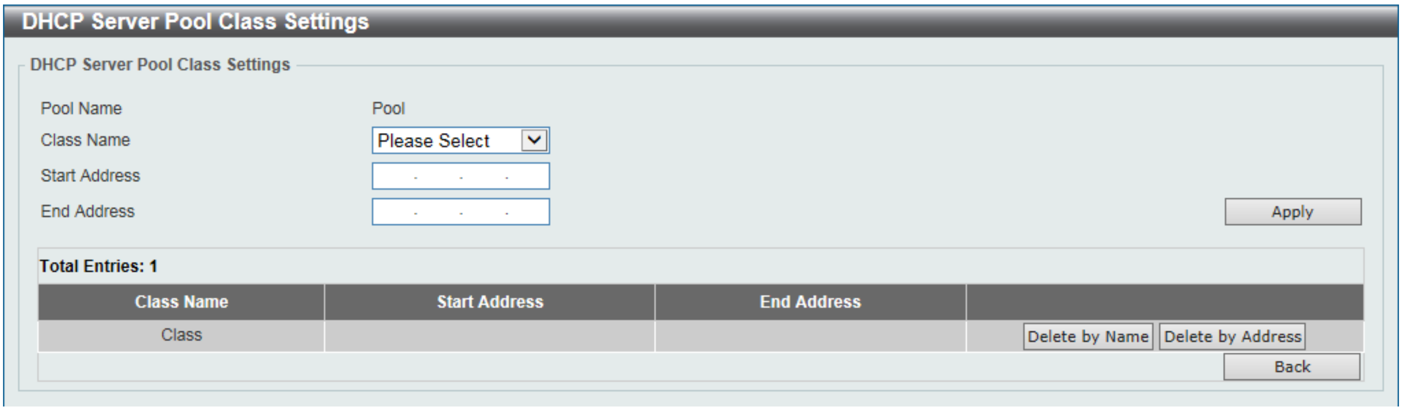
Click the **Edit Class** button to configure the DHCP class.

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

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

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.



DHCP Server Pool Class Settings

Pool Name: Pool

Class Name: Please Select

Start Address: . . .

End Address: . . .

Total Entries: 1

Class Name	Start Address	End Address	
Class			Delete by Name Delete by Address

Figure 4-33 DHCP Server Pool Class Settings 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.
Start Address	Enter the starting IPv4 address that will be associated with the DHCP class in the DHCP pool here.

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

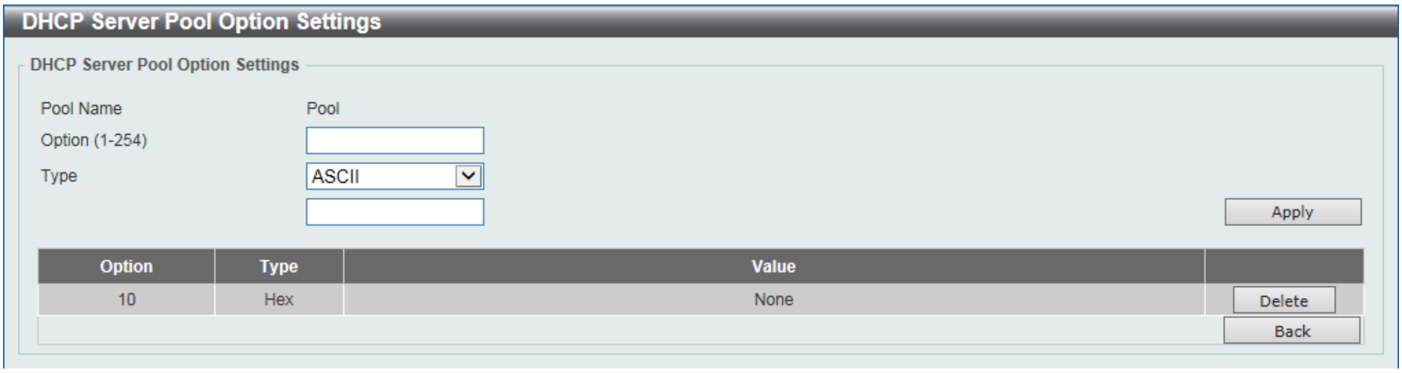
Click the **Apply** button to accept the changes made.

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.


DHCP Server Pool Option Settings
DHCP Server Pool Option Settings
Apply
Delete
Back

Pool Name: Pool

Option (1-254):

Type: ASCII

Option	Type	Value	
10	Hex	None	Delete

Figure 4-34 DHCP Server Pool Option Settings Window

The fields that can be configured are described below:

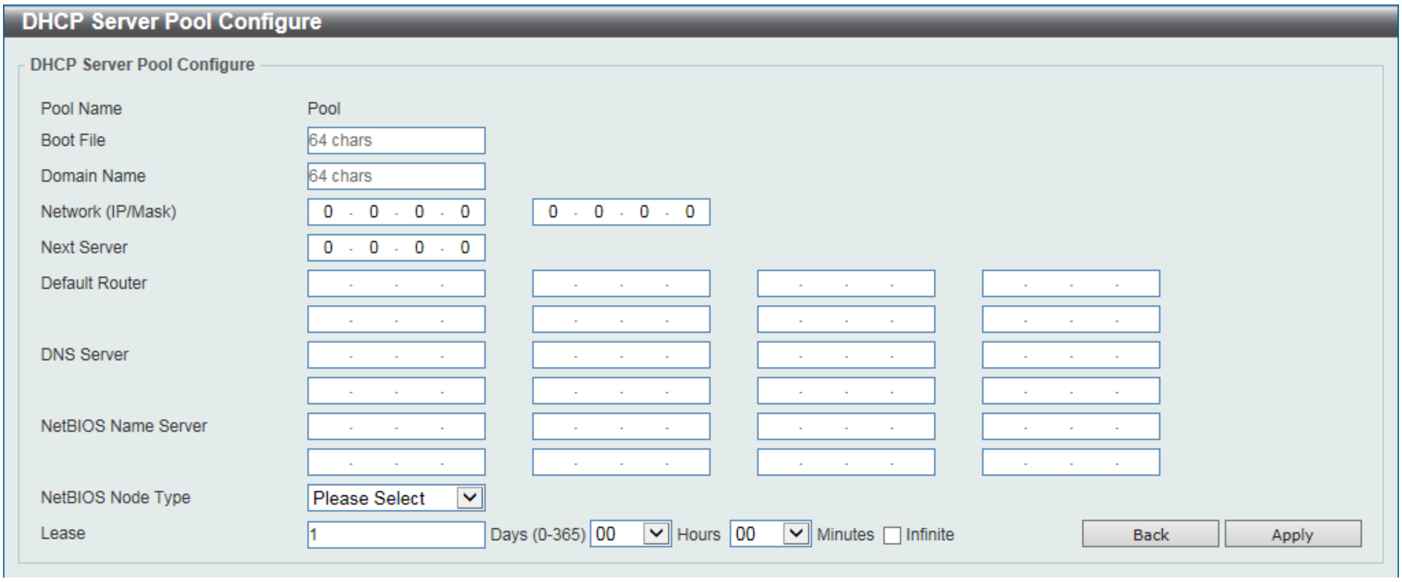
Parameter	Description
Option	Enter the DHCP option number here. The range is from 1 to 254.
Type	Select the DHCP option type here. Options to choose from are: • **ASCII** - Enter the **ASCII** string in the space provided. This string can be up to 255 characters long. • **Hex** - Enter the hexadecimal 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. • **IP** - Enter the IPv4 address in the space provided. Up to 8 IPv4 addresses 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.



DHCP Server Pool Configure

Pool Name	Pool			
Boot File	64 chars			
Domain Name	64 chars			
Network (IP/Mask)	0 . 0 . 0 . 0	0 . 0 . 0 . 0		
Next Server	0 . 0 . 0 . 0			
Default Router	. . .	. . .	. . .	. . .
	. . .	. . .	. . .	. . .
DNS Server	. . .	. . .	. . .	. . .
	. . .	. . .	. . .	. . .
NetBIOS Name Server	. . .	. . .	. . .	. . .
	. . .	. . .	. . .	. . .
NetBIOS Node Type	Please Select			
Lease	1 Days (0-365) 00 Hours 00 Minutes □ Infinite			

Figure 4-35 DHCP Server Pool 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** - This system uses broadcasts. • **Peer-to-Peer** - This system (p-node) uses only point-to-point name queries to a name server (WINS). • **Mixed** - This system (m-node) broadcasts first, and then queries the name server. • **Hybrid** - This system (h-node) queries the name server first, and then broadcasts. This is the recommended type.
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**

Parameter	Description
	and **Minutes** from the drop-down menus. Alternatively, the **Infinite** option can be selected to specify that the lease time is unlimited.

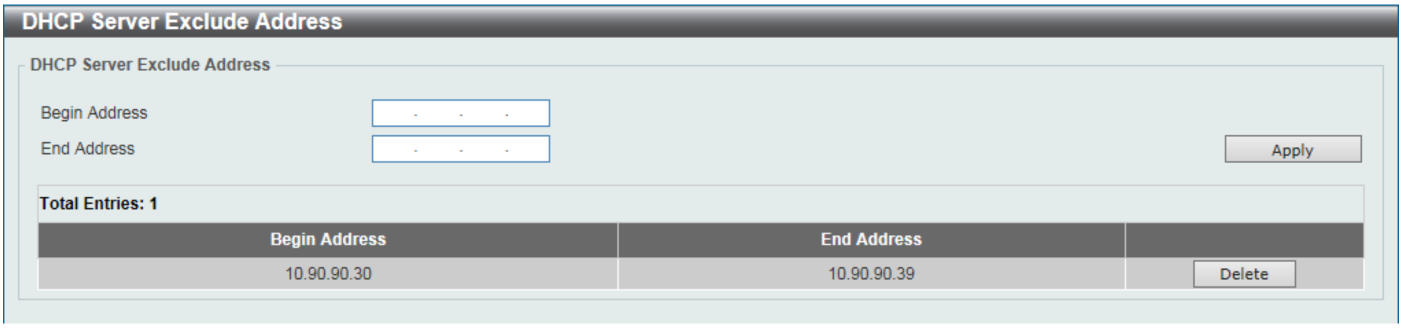
Click the **Apply** button to accept the changes made.

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:



Total Entries: 1

Begin Address	End Address	
10.90.90.30	10.90.90.39	Delete

Figure 4-36 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.

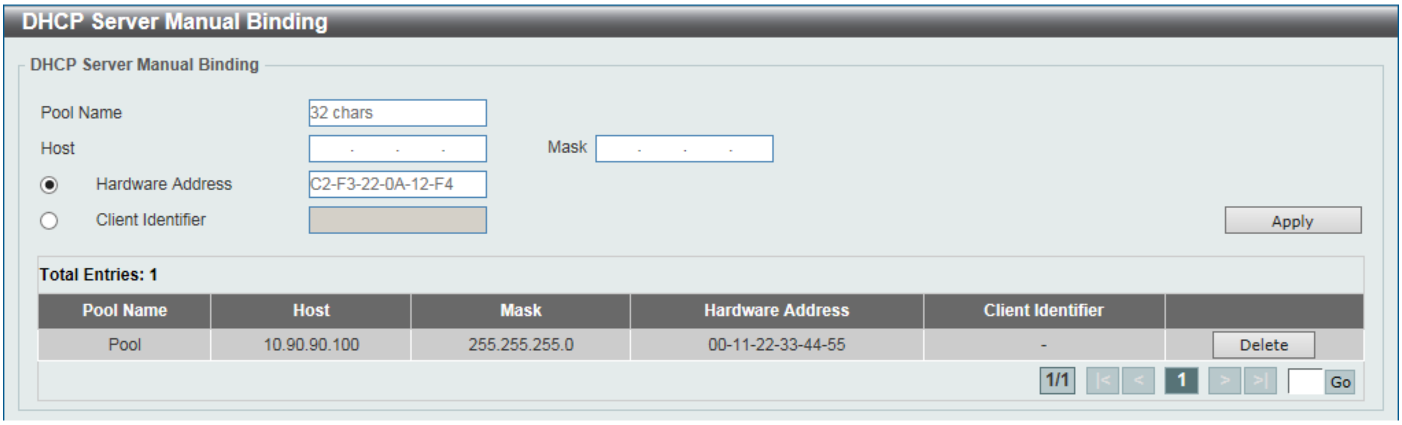
Click the **Apply** button to accept the changes made.

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

DHCP Server Manual Binding

This window is used to display and configure the extended DHCP server manual binding settings. With a manual binding entry, the IP address can 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:



DHCP Server Manual Binding

DHCP Server Manual Binding

Pool Name: 32 chars

Host: . . .   Mask: . . .

● Hardware Address: C2-F3-22-0A-12-F4

○ Client Identifier

Total Entries: 1

Pool Name	Host	Mask	Hardware Address	Client Identifier	
Pool	10.90.90.100	255.255.255.0	00-11-22-33-44-55	-	Delete

Figure 4-37 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.

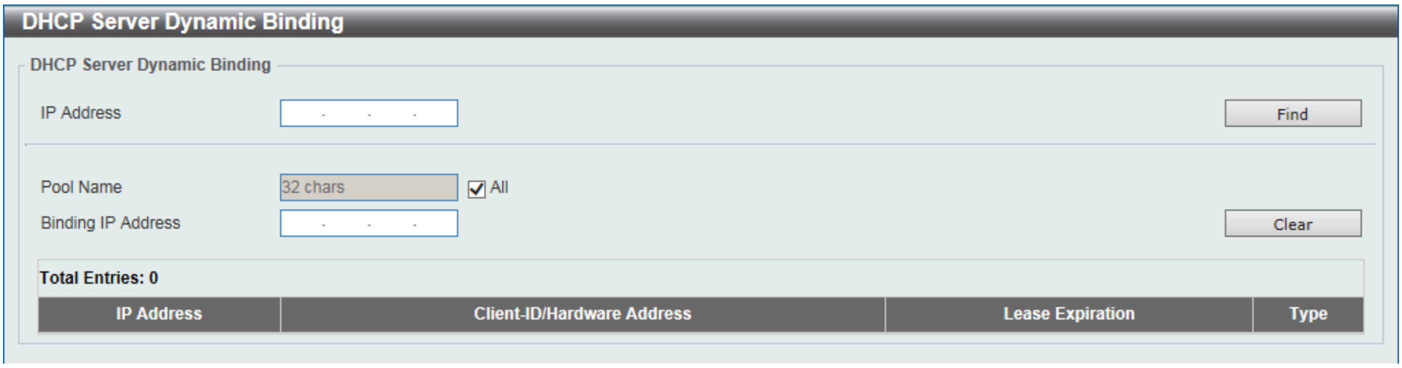
Click the **Delete** button to remove the specified entry.

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

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:



Total Entries: 0

IP Address	Client-ID/Hardware Address	Lease Expiration	Type

Figure 4-38 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.
Binding IP Address	Enter the binding IP address here.

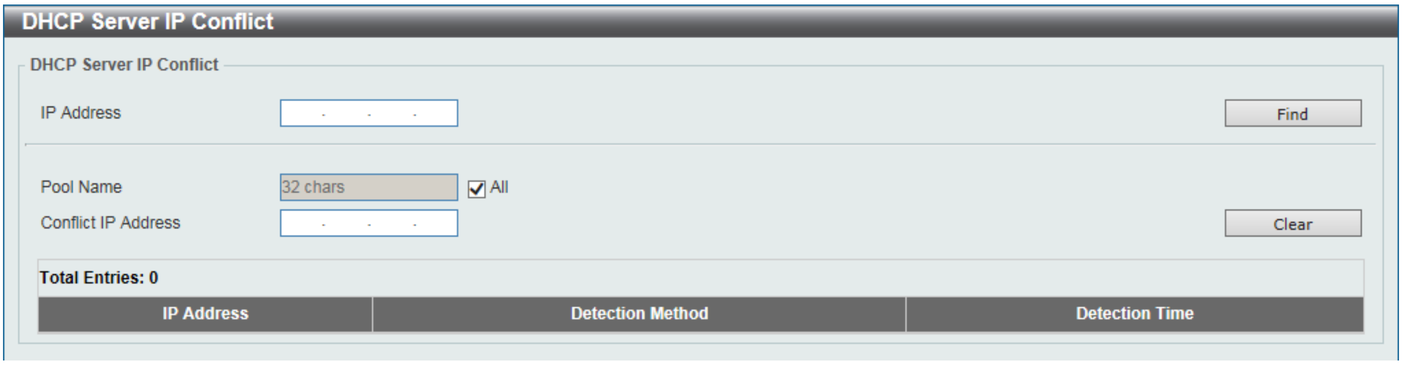
Click the **Find** button to locate a specific entry based on the information entered.

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:



Total Entries: 0

IP Address	Detection Method	Detection Time

Figure 4-39 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.

Parameter	Description
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.
Conflict IP Address	Enter the conflict IP address here.

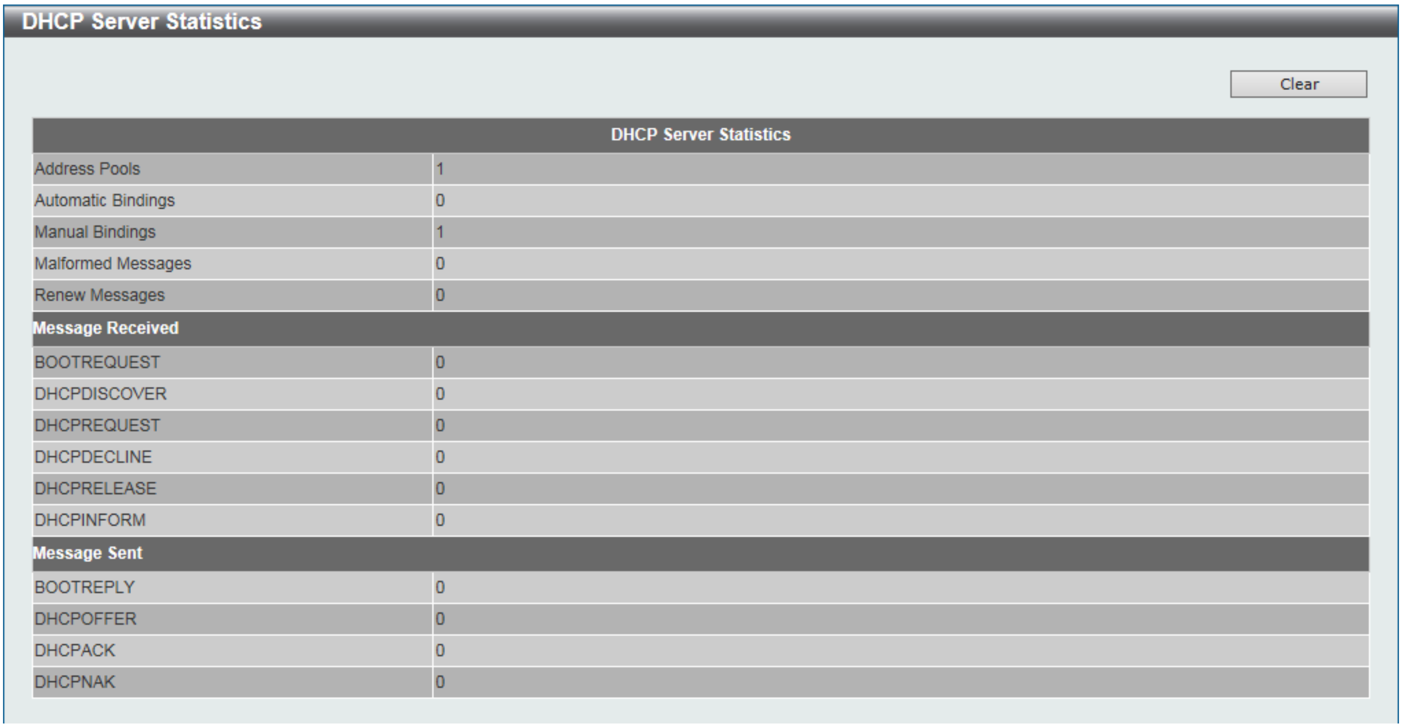
Click the **Find** button to locate a specific entry based on the information entered.

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

DHCP Server Statistic

This window is used to display DHCP server statistics.

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



DHCP Server Statistics

DHCP Server Statistics	
Address Pools	1
Automatic Bindings	0
Manual Bindings	1
Malformed Messages	0
Renew Messages	0
Message Received	
BOOTREQUEST	0
DHCPDISCOVER	0
DHCPREQUEST	0
DHCPDECLINE	0
DHCPRELEASE	0
DHCPINFORM	0
Message Sent	
BOOTREPLY	0
DHCPOFFER	0
DHCPACK	0
DHCPNAK	0

Figure 4-40 DHCP Server Statistic Window

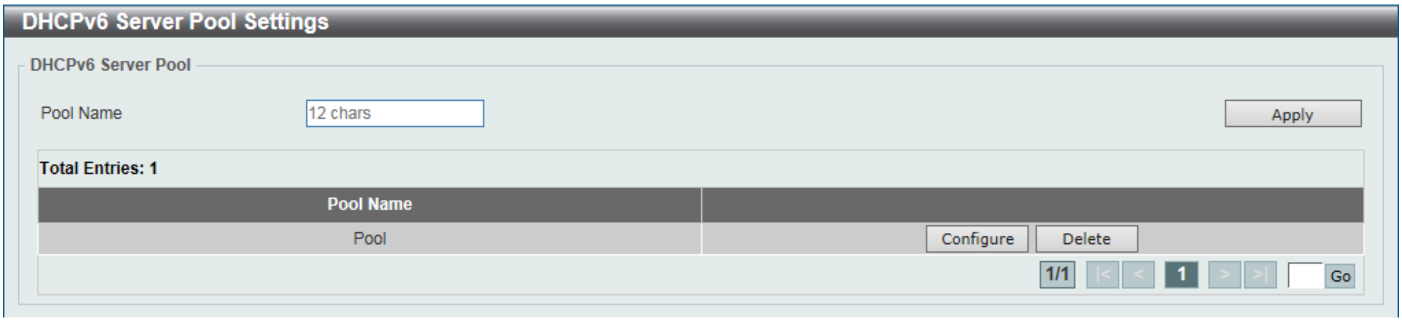
Click the **Clear** button to clear the statistics information displayed here.

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:



DHCPv6 Server Pool Settings

DHCPv6 Server Pool

Pool Name: 12 chars

Total Entries: 1

Pool Name	
Pool	Configure Delete

Figure 4-41 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.

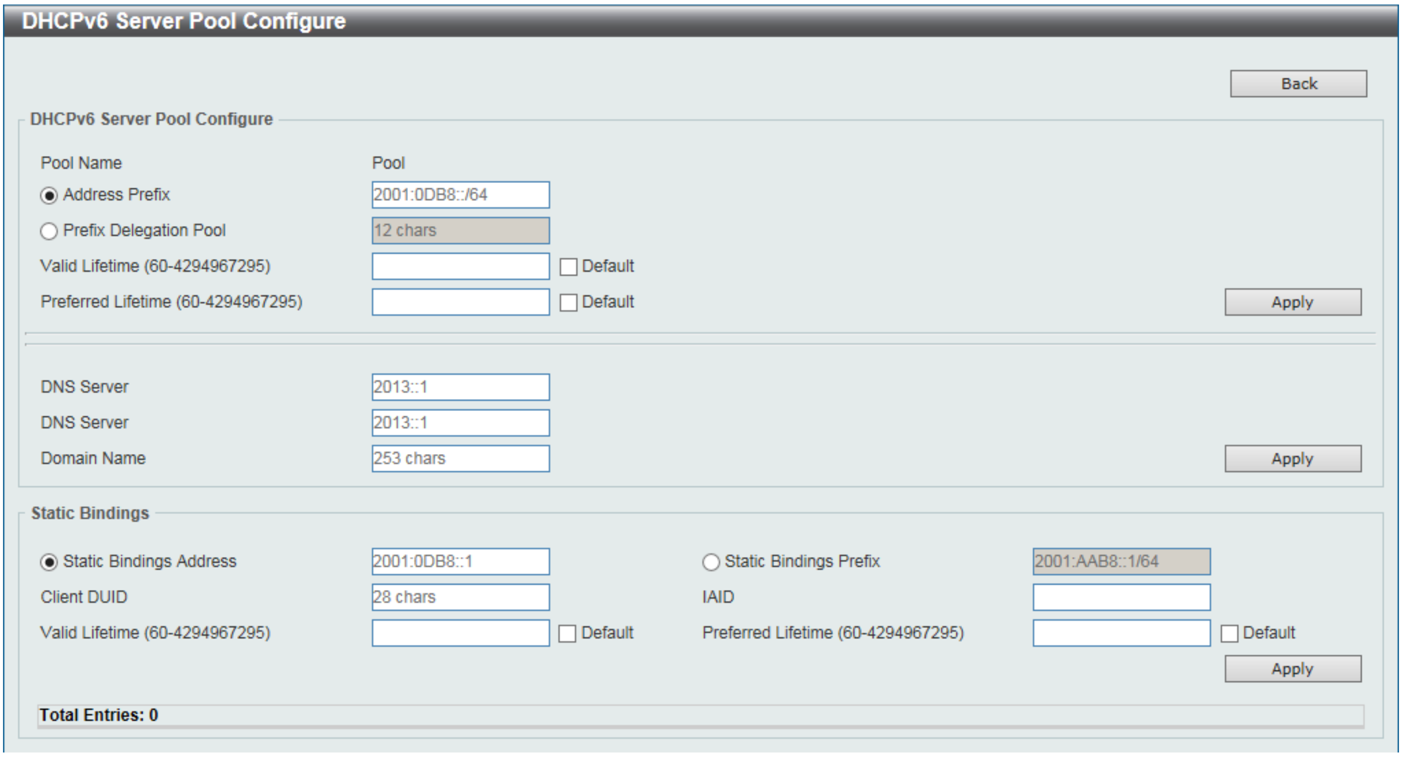
Click the **Apply** button to accept the changes made.

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.



DHCPv6 Server Pool Configure

DHCPv6 Server Pool Configure

Pool Name: Pool

● Address Prefix: 2001:0DB8::/64

○ Prefix Delegation Pool: 12 chars

Valid Lifetime (60-4294967295): □ Default

Preferred Lifetime (60-4294967295): □ Default

DNS Server: 2013::1

DNS Server: 2013::1

Domain Name: 253 chars

Static Bindings

● Static Bindings Address: 2001:0DB8::1

○ Static Bindings Prefix: 2001:AAB8::1/64

Client DUID: 28 chars

IAID:

Valid Lifetime (60-4294967295): □ Default

Preferred Lifetime (60-4294967295): □ Default

Total Entries: 0

Figure 4-42 DHCPv6 Server Pool 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.
Prefix Delegation Pool	Select and enter the DHCPv6 server pool prefix delegation name here. This name can be up to 12 characters long.
Valid Lifetime	Enter the valid lifetime value here. The valid lifetime should be greater than preferred lifetime. The range is from 60 to 4294967295 seconds. By default, this value is 2592000 seconds (30 days). Select **Default** to use the default value.
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). Select **Default** to use the default value.

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 **Configure DNS/Domain Name** are described below:

Parameter	Description
DNS Server	Enter the DNS server IPv6 address to be assigned to requesting DHCPv6 clients here. Up to two DNS server can be configured.
Domain Name	Enter the domain name to be assigned to requesting DHCPv6 clients here.

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

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.
Static Bindings Prefix	Enter the static binding IPv6 network address and prefix length 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). Select **Default** to use the default value.
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). Select **Default** to use the default value.

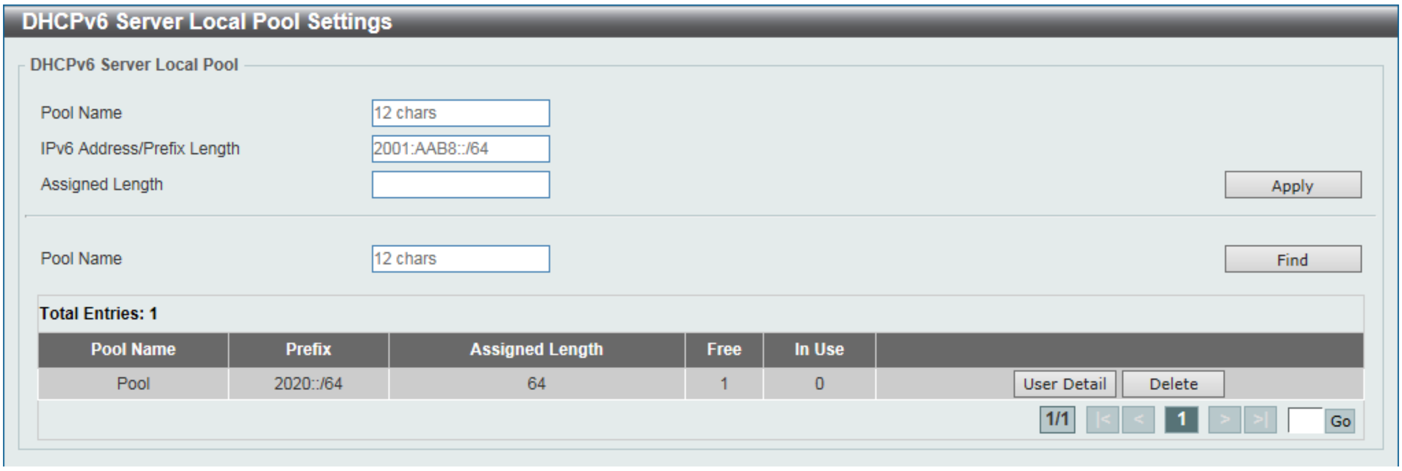
Click the **Apply** button to accept the changes made.

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

DHCPv6 Server Local Pool Settings

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

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



DHCPv6 Server Local Pool Settings

DHCPv6 Server Local Pool

Pool Name: 12 chars

IPv6 Address/Prefix Length: 2001:AAB8::/64

Assigned Length:

Pool Name: 12 chars

Total Entries: 1

Pool Name	Prefix	Assigned Length	Free	In Use	
Pool	2020::/64	64	1	0	User Detail Delete

Figure 4-43 DHCPv6 Server Local Pool Settings Window

The fields that can be configured are described below:

Parameter	Description
Pool Name	Enter the DHCPv6 local pool name here. This name can be up to 12 characters long.
IPv6 Address / Prefix Length	Enter the IPv6 prefix address and prefix length of the local pool here.
Assigned Length	Enter the prefix length to be delegated to the user from the pool here. The value of the assigned length cannot be less than the value of the prefix length.

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

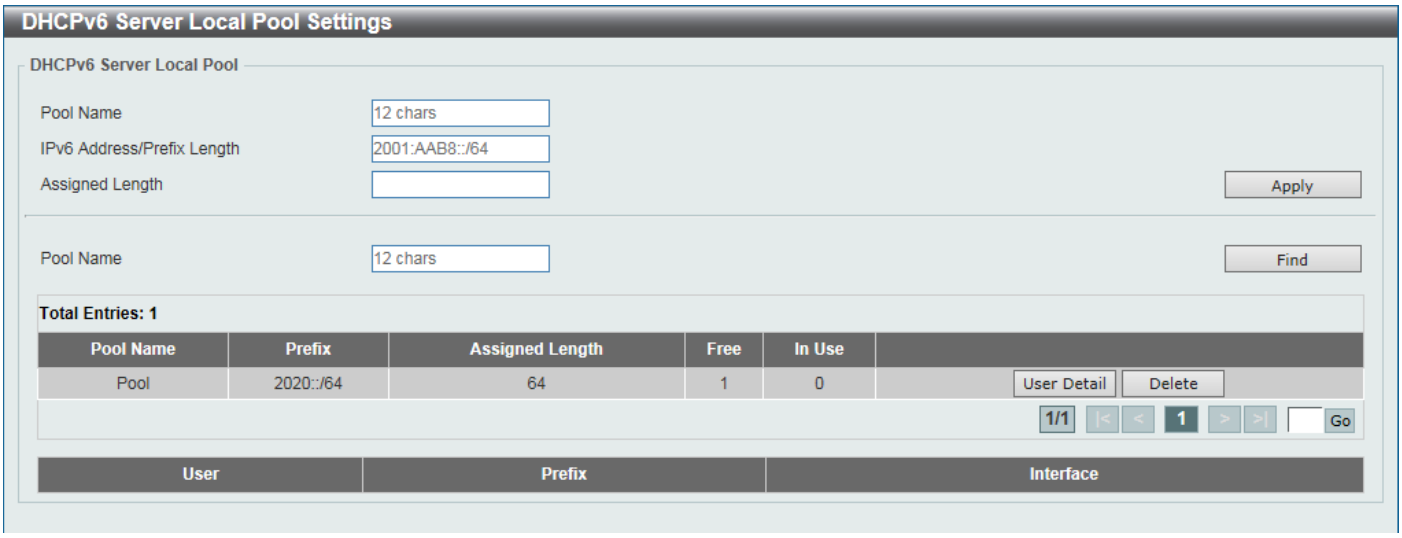
Click the **Find** button to locate a specific entry based on the information entered.

Click the **User Detail** button to view the user information displayed in the lower table.

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 **User Detail** button, the following window is displayed:



DHCPv6 Server Local Pool Settings

DHCPv6 Server Local Pool

Pool Name	12 chars
IPv6 Address/Prefix Length	2001:AAB8::/64
Assigned Length	

Pool Name: 12 chars

Total Entries: 1

Pool Name	Prefix	Assigned Length	Free	In Use	
Pool	2020::/64	64	1	0	User Detail Delete

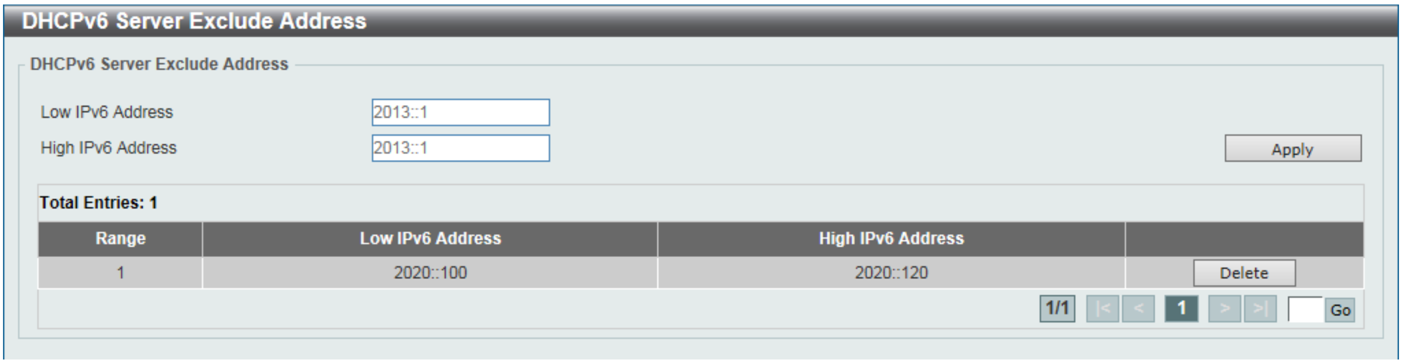
User	Prefix	Interface

Figure 4-44 DHCPv6 Server Local Pool Settings (User Detail) Window

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:



DHCPv6 Server Exclude Address

DHCPv6 Server Exclude Address

Low IPv6 Address	2013::1
High IPv6 Address	2013::1

Total Entries: 1

Range	Low IPv6 Address	High IPv6 Address	
1	2020::100	2020::120	Delete

Figure 4-45 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.

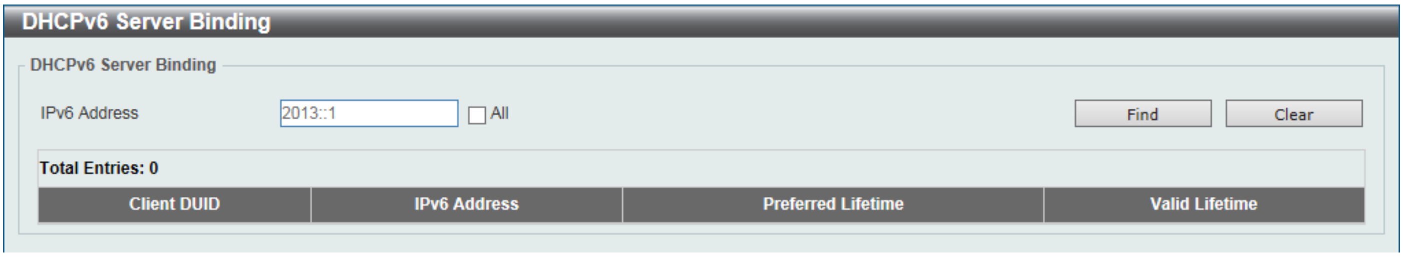
Click the **Delete** button to remove the specified entry.

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

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:



DHCPv6 Server Binding

DHCPv6 Server Binding

IPv6 Address: 2013::1 □ All

Find | Clear

Total Entries: 0

Client DUID	IPv6 Address	Preferred Lifetime	Valid Lifetime

Figure 4-46 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 **All** to display or clear all DHCPv6 client prefix bindings in or from the binding table.

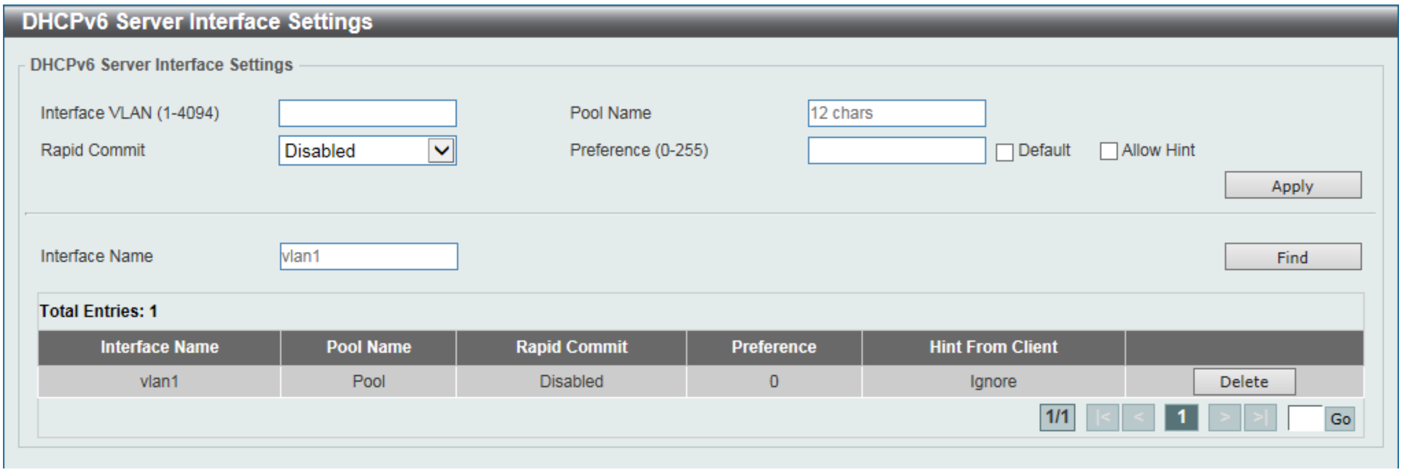
Click the **Find** button to locate a specific entry based on the information entered.

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:



DHCPv6 Server Interface Settings

DHCPv6 Server Interface Settings

Interface VLAN (1-4094):

Pool Name: 12 chars

Rapid Commit: Disabled

Preference (0-255): □ Default □ Allow Hint

Apply

Interface Name: vlan1

Find

Total Entries: 1

Interface Name	Pool Name	Rapid Commit	Preference	Hint From Client	
vlan1	Pool	Disabled	0	Ignore	Delete

Figure 4-47 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.

Parameter	Description
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. The range is from 0 to 255. Select the **Allow Hint** option to allow hints. Select **Default** to use the default value.
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.

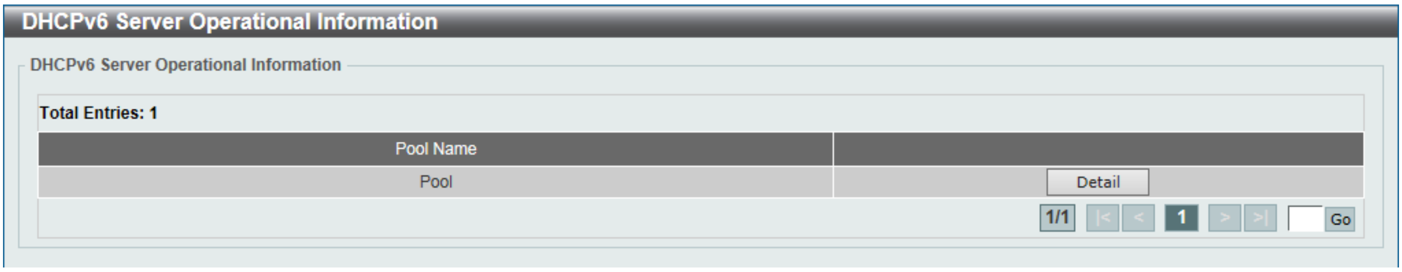
Click the **Delete** button to remove the specified entry.

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 operational information.

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



DHCPv6 Server Operational Information

DHCPv6 Server Operational Information

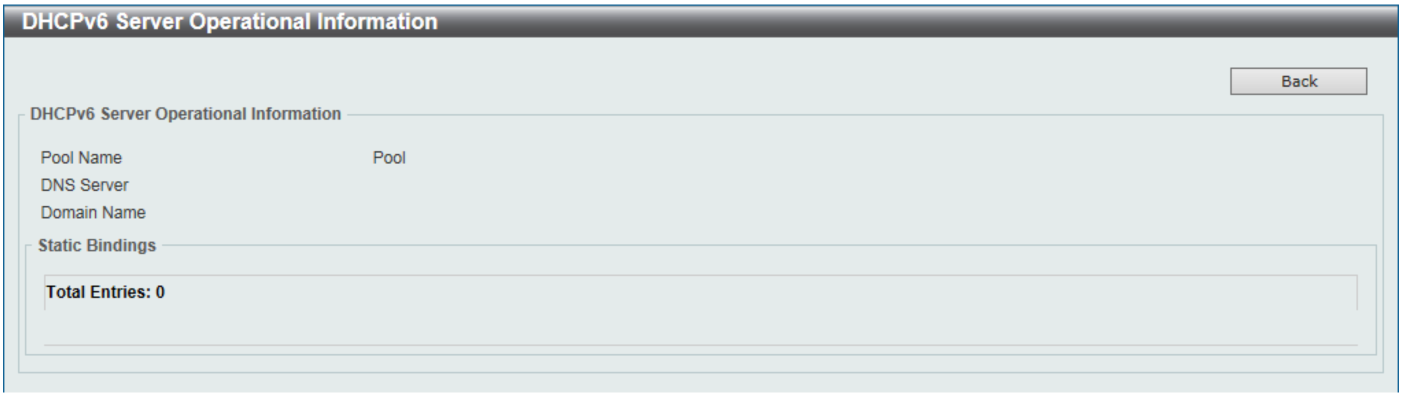
Total Entries: 1

Pool Name	
Pool	Detail

Figure 4-48 DHCPv6 Server Operational Information Window

Click the **Detail** button to view detailed DHCPv6 operational information.

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



DHCPv6 Server Operational Information

DHCPv6 Server Operational Information

Pool Name Pool
DNS Server
Domain Name

Static Bindings

Total Entries: 0

Figure 4-49 DHCPv6 Server Operational Information (Detail) Window

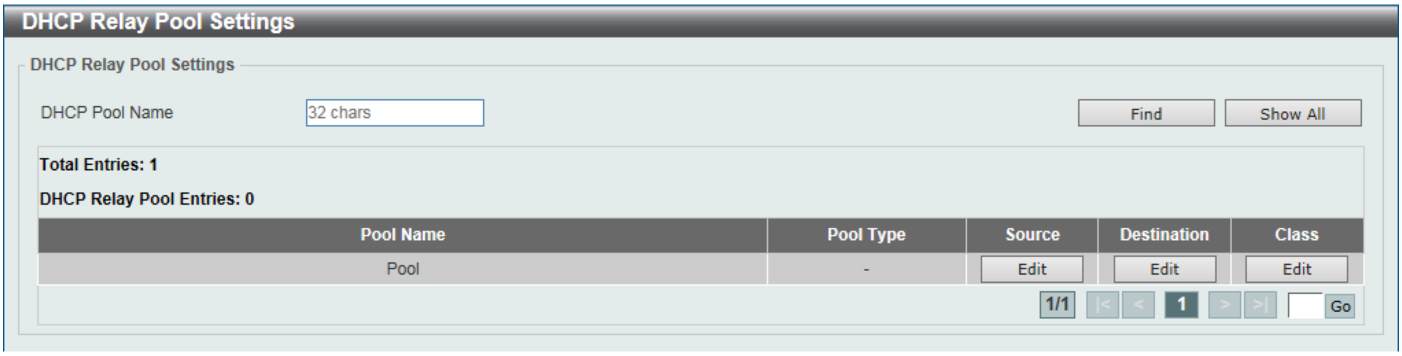
Click the **Back** button to return to the previous window.

DHCP Relay

DHCP Relay Pool Settings

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

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



DHCP Relay Pool Settings

DHCP Pool Name: 32 chars

Total Entries: 1

DHCP Relay Pool Entries: 0

Pool Name	Pool Type	Source	Destination	Class
Pool	-	Edit	Edit	Edit

Figure 4-50 DHCP Relay Pool Settings Window

The fields that can be configured are described below:

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

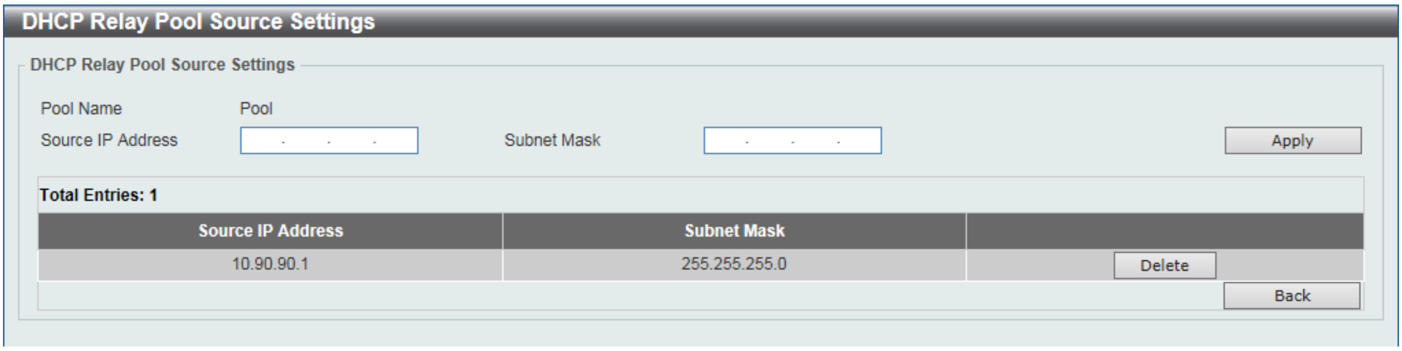
Click the **Find** button to find and display the DHCP pool in the table.

Click the **Show All** button to display all the DHCP pools in the table.

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

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

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



DHCP Relay Pool Source Settings

Pool Name: Pool

Source IP Address: . . .

Subnet Mask: . . .

Total Entries: 1

Source IP Address	Subnet Mask	
10.90.90.1	255.255.255.0	Delete

Figure 4-51 DHCP Relay Pool Source Settings Window

The fields that can be configured are described below:

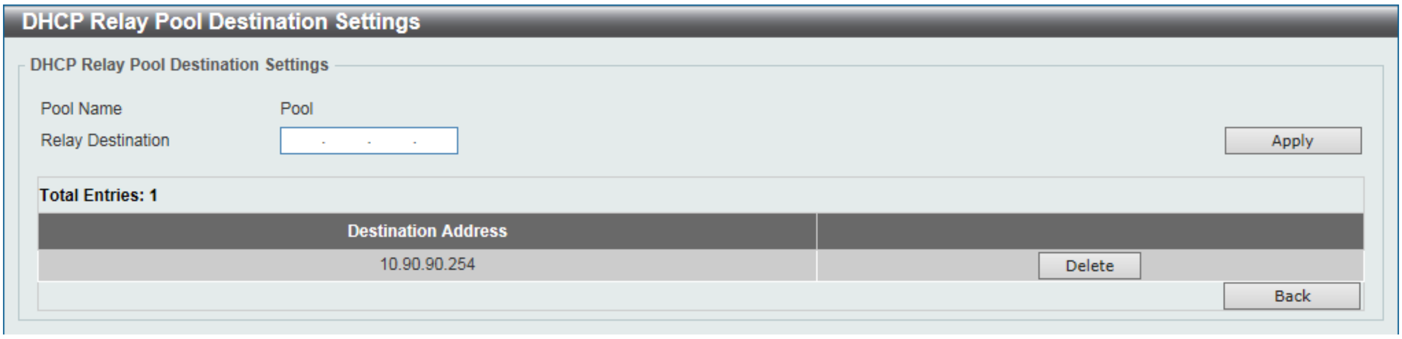
Parameter	Description
Source IP Address	Enter the source subnet of client packets.
Subnet Mask	Enter the network mask of the source subnet.

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

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

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

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



DHCP Relay Pool Destination Settings

DHCP Relay Pool Destination Settings

Pool Name Pool

Relay Destination . . .

Total Entries: 1

Destination Address	
10.90.90.254	Delete

Figure 4-52 DHCP Relay Pool Destination Settings Window

The fields that can be configured are described below:

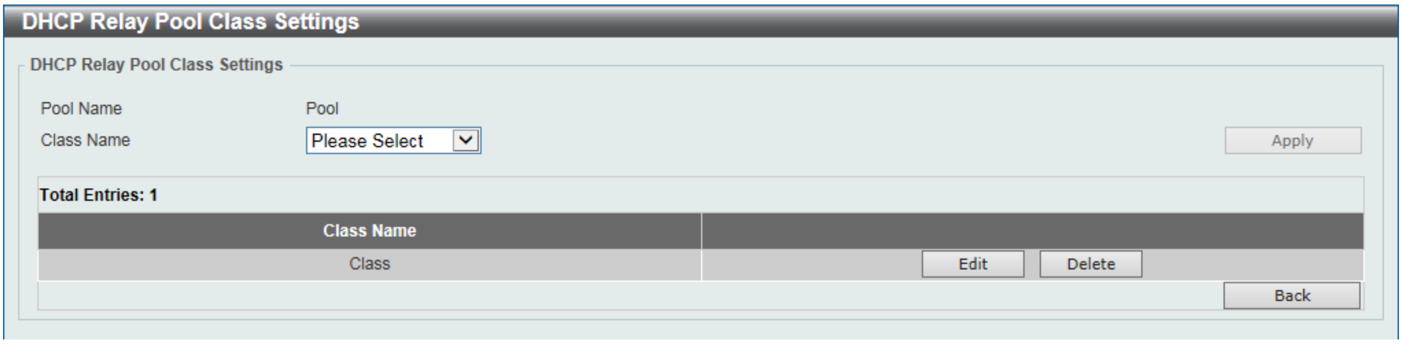
Parameter	Description
Relay Destination	Enter the relay destination DHCP server IP address.

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

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

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

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



DHCP Relay Pool Class Settings

DHCP Relay Pool Class Settings

Pool Name Pool

Class Name Please Select

Total Entries: 1

Class Name	
Class	Edit Delete

Figure 4-53 DHCP Relay Pool Class Settings Window

The fields that can be configured are described below:

Parameter	Description
Class Name	Select the DHCP class name.

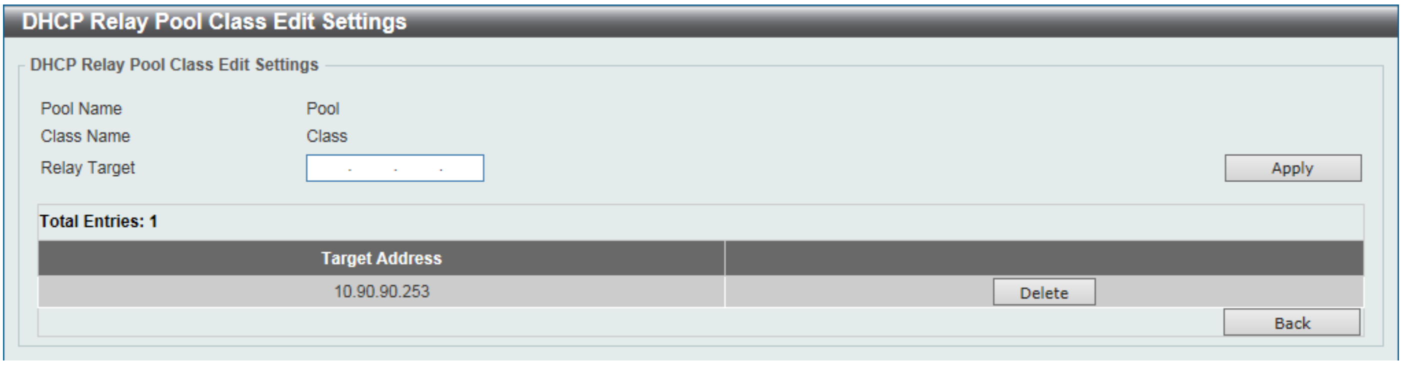
Click the **Apply** button to accept the changes made.

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

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

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

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



DHCP Relay Pool Class Edit Settings

DHCP Relay Pool Class Edit Settings

Pool Name: Pool

Class Name: Class

Relay Target: . . .

Total Entries: 1

Target Address	
10.90.90.253	Delete

Figure 4-54 DHCP Relay Pool Class Edit Settings Window

The fields that can be configured are described below:

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

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

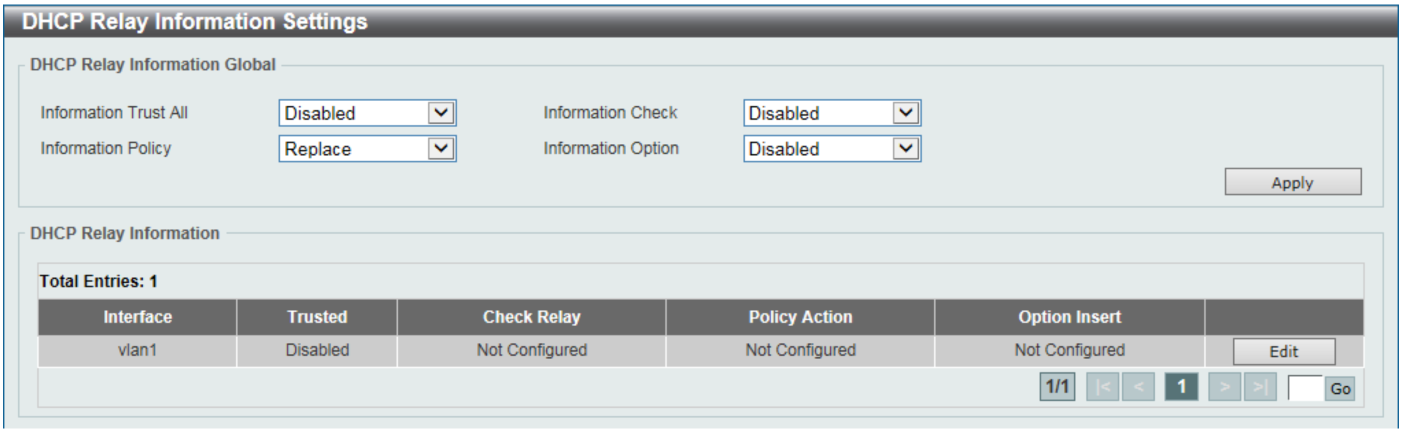
Click the **Delete** button to remove the specified entry.

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

DHCP Relay Information Settings

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

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



DHCP Relay Information Settings

DHCP Relay Information Global

Information Trust All: Disabled

Information Check: Disabled

Information Policy: Replace

Information Option: Disabled

DHCP Relay Information

Total Entries: 1

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

Figure 4-55 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:

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

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

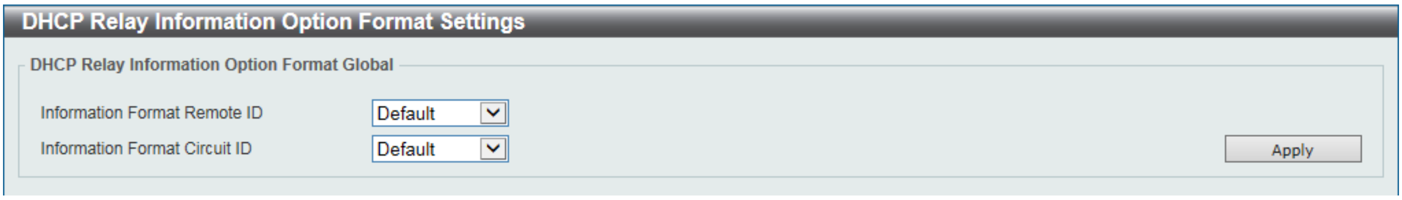
Click the **Edit** button to modify the corresponding interface.

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

DHCP Relay Information Option Format Settings

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

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



DHCP Relay Information Option Format Settings

DHCP Relay Information Option Format Global

Information Format Remote ID: Default

Information Format Circuit ID: Default

Figure 4-56 DHCP Relay Information Option Format Settings Window

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

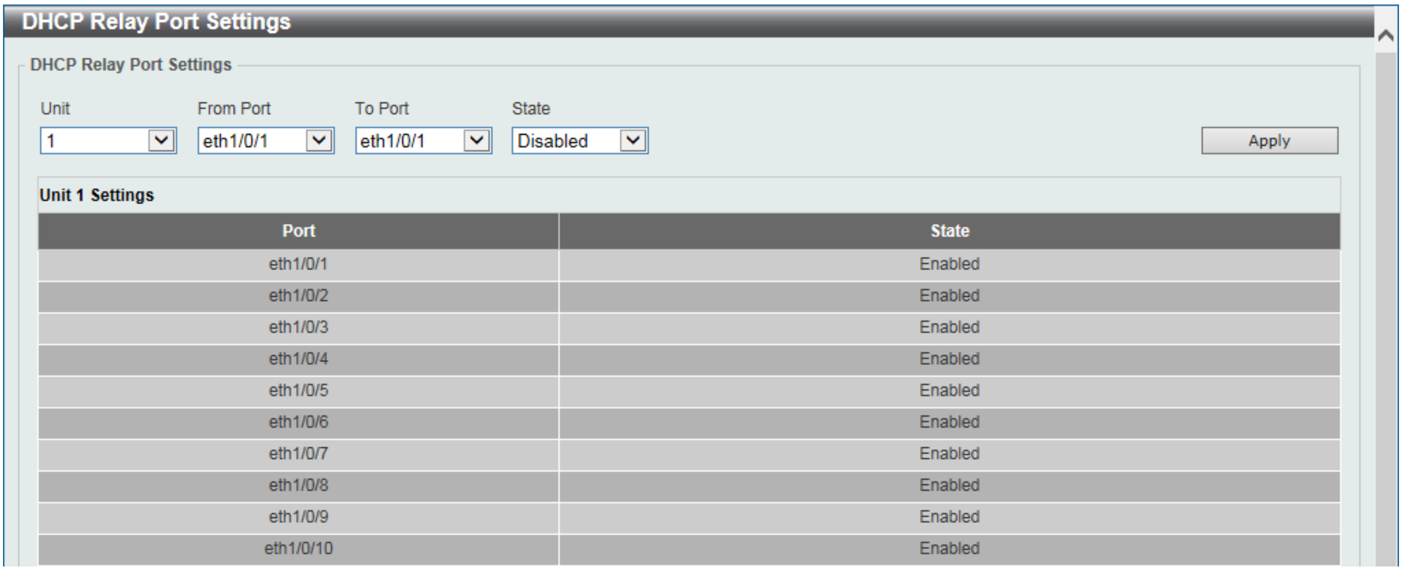
Parameter	Description
Information Format Remote ID	Select the DHCP information remote ID sub-option. Options to choose from are: • **Default** - Select to use the Switch's system MAC address as the remote ID. • **User Define** - Select to use a user-defined remote ID. ○ Enter the user-defined string in the text box. This can be up to 32 characters long. • **Vendor 2** - Select to use vendor 2 as the remote ID.
Information Format Circuit ID	Select the DHCP information circuit ID sub-option. Options to choose from are: • **Default** - Select to use the default circuit ID sub-option. • **User Define** - Select to use a user-defined circuit ID. ○ Enter the user-defined string in the text box. This can be up to 32 characters long. • **Vendor 1** - Select to use vendor 1 as the circuit ID.

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:



DHCP Relay Port Settings

DHCP Relay Port Settings

Unit: 1 | From Port: eth1/0/1 | To Port: eth1/0/1 | State: Disabled | Apply

Unit 1 Settings

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

Figure 4-57 DHCP Relay Port Settings Window

The fields that can be configured are described below:

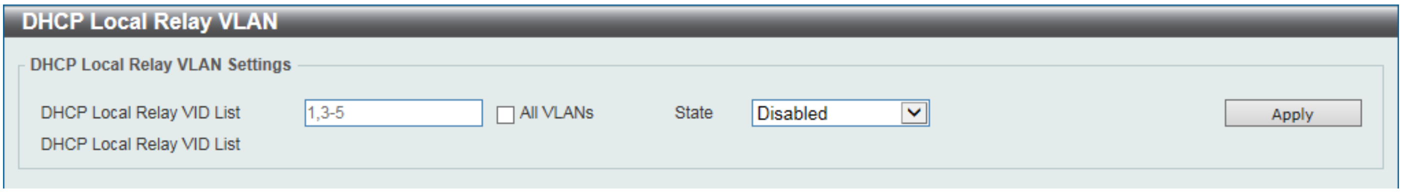
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
State	Select to enable or disable the DHCP Relay feature.

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:



DHCP Local Relay VLAN

DHCP Local Relay VLAN Settings

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

DHCP Local Relay VID List

Figure 4-58 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. Select the **All VLANs** check box to select all VLANs.

Parameter	Description
State	Select this option to enable or disable the DHCP local relay on the specific VLAN(s).

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

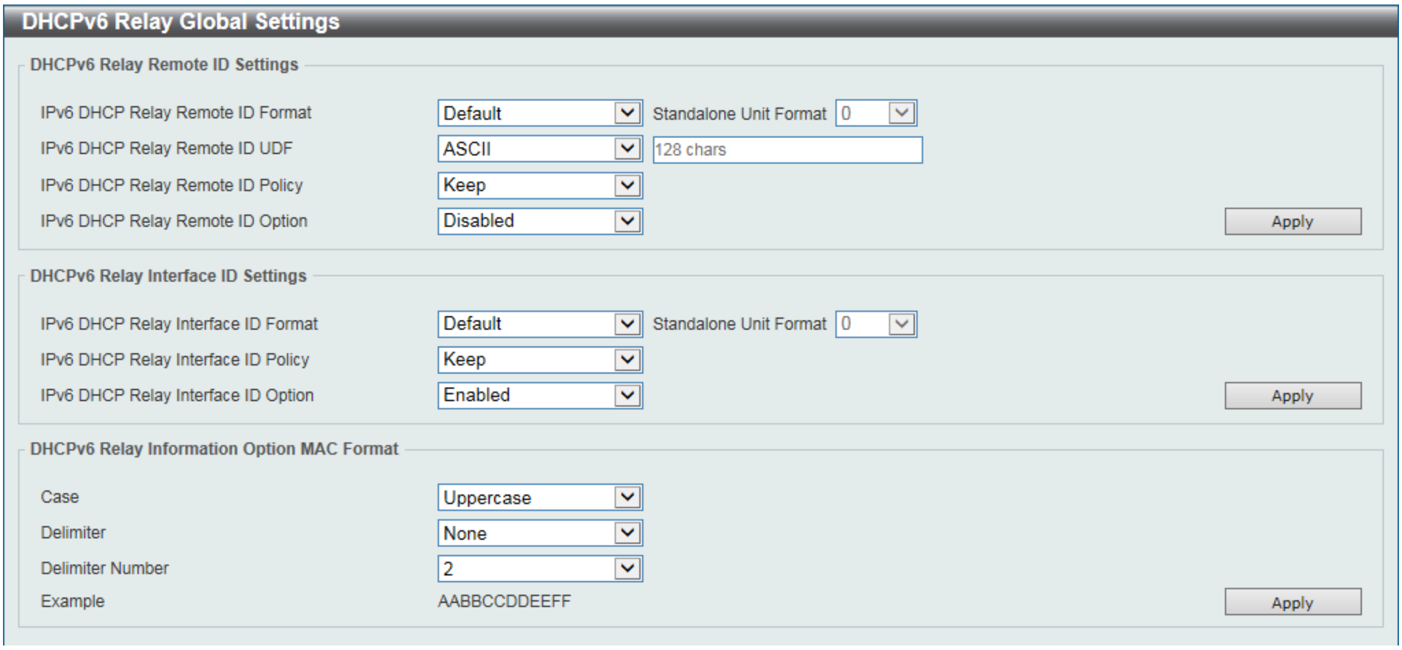
NOTE: When the state of the DHCP relay port is disabled, the port will not relay or locally relay received DHCP packets.

DHCPv6 Relay

DHCPv6 Relay Global Settings

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

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



DHCPv6 Relay Global Settings

DHCPv6 Relay Remote ID Settings

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

DHCPv6 Relay Interface ID Settings

IPv6 DHCP Relay Interface ID Format	Default	Standalone Unit Format	0
IPv6 DHCP Relay Interface ID Policy	Keep		
IPv6 DHCP Relay Interface ID Option	Enabled		Apply

DHCPv6 Relay Information Option MAC Format

Case	Uppercase	
Delimiter	None	
Delimiter Number	2	
Example	AABBCCDDEEFF	Apply

Figure 4-59 DHCPv6 Relay Global Settings Window

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

Parameter	Description
IPv6 DHCP Relay Remote ID Format	Select the IPv6 DHCP Relay remote ID format that will be used here. Options to choose from are **Default**, **CID with User Define**, **User Define**, and **Expert UDF**.
Standalone Unit Format	After selecting the **Expert UDF** option, select the standalone unit format here. Options to choose from are **0** and **1**.
IPv6 DHCP Relay Remote ID UDF	Select to choose the User Define Field (UDF) for the remote ID. Options to choose from are: • **None -** Specifies to keep the UDF empty for the remote ID. • **ASCII -** Select to enter the ASCII string with a maximum of 128 characters in the text box. • **HEX -** Select to enter the hexadecimal string with a maximum of 256 characters in the text box.

Parameter	Description
IPv6 DHCP Relay Remote ID Policy	Select to choose Option 37 forwarding policy for the DHCPv6 relay agent. Options to choose from are: • **Keep** - Select that the DHCPv6 request packet that already has the relay agent Remote-ID option is left unchanged and directly relayed to the DHCPv6 server. • **Drop** - Select to discard the packet that already has the relay agent Remote-ID Option 37.
IPv6 DHCP Relay Remote ID Option	Select this option to enable or disable the insertion of the relay agent remote ID Option 37 during the relay of DHCP for IPv6 request packets.

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

The fields that can be configured in **DHCPv6 Relay 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**, **Vendor1**, and **Expert UDF**.
Standalone Unit Format	After selecting the **Expert UDF** option, select the standalone unit format here. Options to choose from are **0** and **1**.
IPv6 DHCP Relay 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:

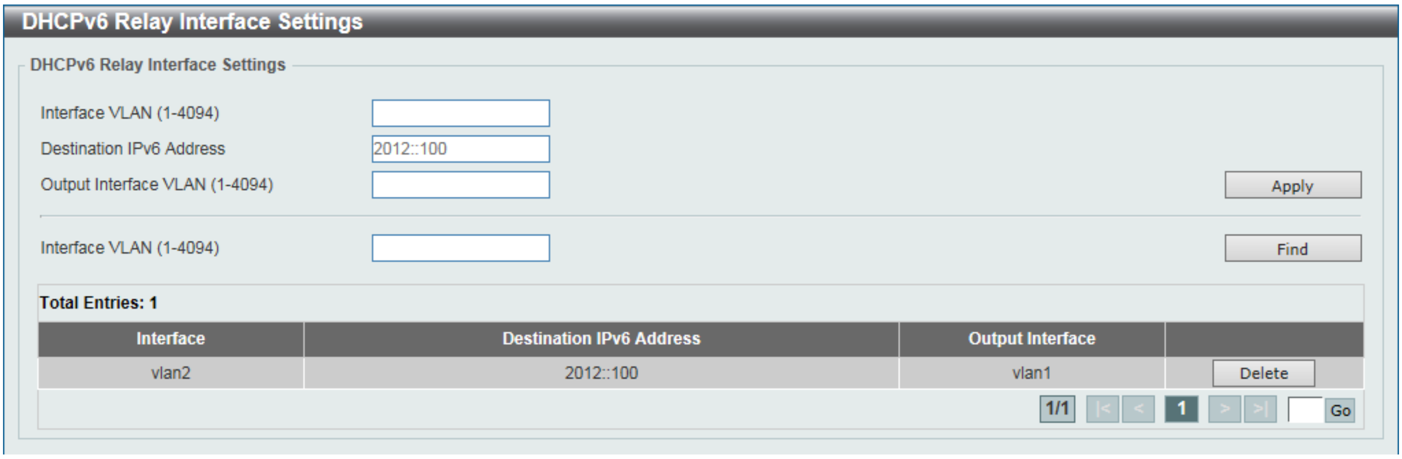
Parameter	Description
Case	Select the case that will be used here. Options to choose from are: • **Lowercase** - Specifies that the MAC format will be lowercase. For example: aa-bb-cc-dd-ee-ff. • **Uppercase** - Specifies that the MAC format will be uppercase. For example: AA-BB-CC-DD-EE-FF.
Delimiter	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: • **1** - Specifies to use a single delimiter. For example: AABBCC.DDEEFF. • **2** - Specifies to use two delimiters. For example: AABB.CCDD.EEFF • **5** - Specifies to use multiple delimiters. For example: AA.BB.CC.DD.EE.FF

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

DHCPv6 Relay Interface Settings

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

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


DHCPv6 Relay Interface Settings
DHCPv6 Relay Interface Settings
Apply
Find
Delete
1/1
1
Go

Interface VLAN (1-4094)
Destination IPv6 Address: 2012::100
Output Interface VLAN (1-4094)

Interface VLAN (1-4094)

Total Entries: 1

Interface	Destination IPv6 Address	Output Interface	
vlan2	2012::100	vlan1	Delete

Figure 4-60 DHCPv6 Relay Interface Settings Window

The fields that can be configured are described below:

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

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

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

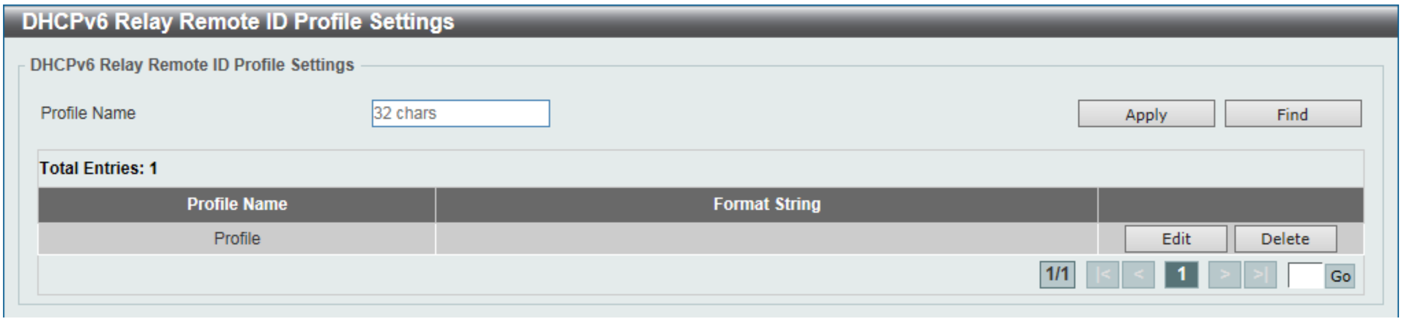
Click the **Delete** button to remove the specified entry.

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

DHCPv6 Relay Remote ID Profile Settings

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

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


DHCPv6 Relay Remote ID Profile Settings
DHCPv6 Relay Remote ID Profile Settings
Apply
Find
Edit
Delete
1/1
Go

Profile Name: 32 chars

Total Entries: 1

Profile Name	Format String	
Profile		Edit Delete

Figure 4-61 DHCPv6 Relay Remote ID Profile Settings Window

The fields that can be configured are described below:

Parameter	Description
Profile Name	Enter the profile name here. This string can be up to 32 characters long.
Format String	After clicking the **Edit** button, enter the Option 82 format string here. This string can be up to 251 characters long. The following rules need to be considered: • This string can be a hexadecimal value, an ASCII string, or any combination of hexadecimal values and ASCII characters. An ASCII string needs to be enclosed with quotation marks (“”) like “Ethernet”. Any ASCII characters outside of the quotation marks will be interpreted as hexadecimal values. • A formatted key string is a string that should be translated before being encapsulated in the packet. A formatted key string can be contained both ASCII strings and hexadecimal values. For example, **“%” +“$”+“1~32”+ “keyword”+“:”:** o **%** - Indicates that the string that follows this character is a formatted key string. o **“$”** or **“0”** - (Optional) Indicates a fill indicator. This option specifies how to fill the formatted key string to meet the length option. This option can be either “$” or “0”, and cannot be specified as both at the same time. ➢ **“$”** - Indicates to fill the leading space (0x20). ➢ **“0”** - Indicates to fill the leading 0. The fill the leading 0 (0) is the default setting. o **1**~**32** - (Optional) Indicates a length option. This specifies how many characters or bytes the translated key string should occupy. If the actual length of the translated key string is less than the length specified by this option, a fill indicator will be used to fill it. Otherwise, this length option and fill indicator will be ignored and the actual string will be used directly. o **keyword** - Indicates that the keyword will be translated based on the actual value of the system. The following keyword definitions specifies that a command will be refused if an unknown or unsupported keyword is detected: ➢ **devtype** - The model name of the device. Only an ASCII string is allowed. ➢ **sysname** - Indicates the System name of the Switch. Only an ASCII string is allowed. ➢ **ifdescr** - Derived from *ifDescr* (IF-MIB). Only an ASCII string is allowed. ➢ **portmac** - Indicates the MAC address of a port. This can be either an ASCII string or a hexadecimal value. When in the format of an ASCII string, the MAC address format can

Parameter	Description
	be customized using special CLI commands. When in the format of a hexadecimal value, the MAC address will be encapsulated in order in hexadecimal. ➢ **sysmac** - Indicates the system MAC address. This can be either an ASCII string or a hexadecimal value. In the ASCII string format, the MAC address format can be customized using special CLI commands. In the hexadecimal format, the MAC address will be encapsulated in order in hexadecimal. ➢ **unit** - Indicates the unit ID. This can be either an ASCII string or a hexadecimal value. For a standalone device, the unit ID is 0. ➢ **module** - Indicates the module ID number. This can be either an ASCII string or a hexadecimal value. ➢ **port** - Indicates the local port number. This can be either an ASCII string or a hexadecimal value. ➢ **svlan** - Indicates the outer VLAN ID. This can be either an ASCII string or a hexadecimal value. ➢ **cvlan** - Indicates the inner VLAN ID. This can be either an ASCII string or a hexadecimal value. o **: -** Indicates the end of the formatted key sting. If a formatted key string is the last parameter of the command, its ending character (":") can be ignored. The space (0x20) between "%" and ":" will be ignored. Other spaces will be encapsulated. • ASCII strings can be any combination of formatted key strings and 0~9, a~z, A~Z, !@#$%^&*()_+|-=\[]{};:'"/?.,<>`, and space characters. "\" is the escape character. The special character after "\" is the character itself, for example, "\%" is "%" itself, not the start indicator of a formatted key string. Spaces not in the formatted key string will also be encapsulated. • Hexadecimal values can be any combination of formatted key strings and 0~9, A~F, a~f, and space characters. The formatted key strings only support keywords that support hexadecimal values. Spaces not in the formatted key string will be ignored.

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

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

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

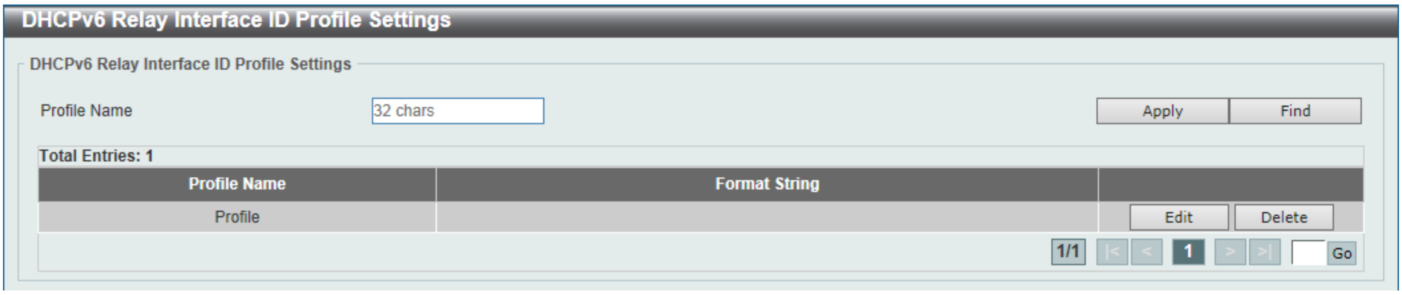
Click the **Delete** button to remove the specific entry.

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

DHCPv6 Relay Interface ID Profile Settings

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

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



DHCPv6 Relay Interface ID Profile Settings

DHCPv6 Relay Interface ID Profile Settings

Profile Name: 32 chars

Total Entries: 1

Profile Name	Format String	
Profile		Edit Delete

Figure 4-62 DHCPv6 Relay Interface ID Profile Settings Window

The fields that can be configured are described below:

Parameter	Description
Profile Name	Enter the profile name here. This string can be up to 32 characters long.
Format String	After clicking the **Edit** button, enter the Option 82 format string here. This string can be up to 251 characters long. The following rules need to be considered: • This string can be a hexadecimal value, an ASCII string, or any combination of hexadecimal values and ASCII characters. An ASCII string needs to be enclosed with quotation marks (“”) like “Ethernet”. Any ASCII characters outside of the quotation marks will be interpreted as hexadecimal values. • A formatted key string is a string that should be translated before being encapsulated in the packet. A formatted key string can be contained both ASCII strings and hexadecimal values. For example, **“%” +“$”+“1~32”+ “keyword”+“:”:** ○ **%** - Indicates that the string that follows this character is a formatted key string. ○ **“$”** or **“0”** - (Optional) Indicates a fill indicator. This option specifies how to fill the formatted key string to meet the length option. This option can be either “$” or “0”, and cannot be specified as both at the same time. ➢ **“$”** - Indicates to fill the leading space (0x20). ➢ **“0”** - Indicates to fill the leading 0. The fill the leading 0 (0) is the default setting. ○ **1**~**32** - (Optional) Indicates a length option. This specifies how many characters or bytes the translated key string should occupy. If the actual length of the translated key string is less than the length specified by this option, a fill indicator will be used to fill it. Otherwise, this length option and fill indicator will be ignored and the actual string will be used directly. ○ **keyword** - Indicates that the keyword will be translated based on the actual value of the system. The following keyword definitions specifies that a command will be refused if an unknown or unsupported keyword is detected: ➢ **devtype** - The model name of the device. Only an ASCII string is allowed. ➢ **sysname** - Indicates the System name of the Switch. Only an ASCII string is allowed. ➢ **ifdescr** - Derived from *ifDescr* (IF-MIB). Only an ASCII string is allowed. ➢ **portmac** - Indicates the MAC address of a port. This can be either an ASCII string or a hexadecimal value. When in the format of an ASCII string, the MAC address format can

Parameter	Description
	be customized using special CLI commands. When in the format of a hexadecimal value, the MAC address will be encapsulated in order in hexadecimal. ➢ **sysmac** - Indicates the system MAC address. This can be either an ASCII string or a hexadecimal value. In the ASCII string format, the MAC address format can be customized using special CLI commands. In the hexadecimal format, the MAC address will be encapsulated in order in hexadecimal. ➢ **unit** - Indicates the unit ID. This can be either an ASCII string or a hexadecimal value. For a standalone device, the unit ID is 0. ➢ **module** - Indicates the module ID number. This can be either an ASCII string or a hexadecimal value. ➢ **port** - Indicates the local port number. This can be either an ASCII string or a hexadecimal value. ➢ **svlan** - Indicates the outer VLAN ID. This can be either an ASCII string or a hexadecimal value. ➢ **cvlan** - Indicates the inner VLAN ID. This can be either an ASCII string or a hexadecimal value. o **: -** Indicates the end of the formatted key sting. If a formatted key string is the last parameter of the command, its ending character (“:”) can be ignored. The space (0x20) between “%” and “:” will be ignored. Other spaces will be encapsulated. • ASCII strings can be any combination of formatted key strings and 0~9, a~z, A~Z, !@#$%^&*()_+|-=\[]{};:'"/?.,<>`, and space characters. “\” is the escape character. The special character after “\” is the character itself, for example, “\%” is “%” itself, not the start indicator of a formatted key string. Spaces not in the formatted key string will also be encapsulated. • Hexadecimal values can be any combination of formatted key strings and 0~9, A~F, a~f, and space characters. The formatted key strings only support keywords that support hexadecimal values. Spaces not in the formatted key string will be ignored.

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

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

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

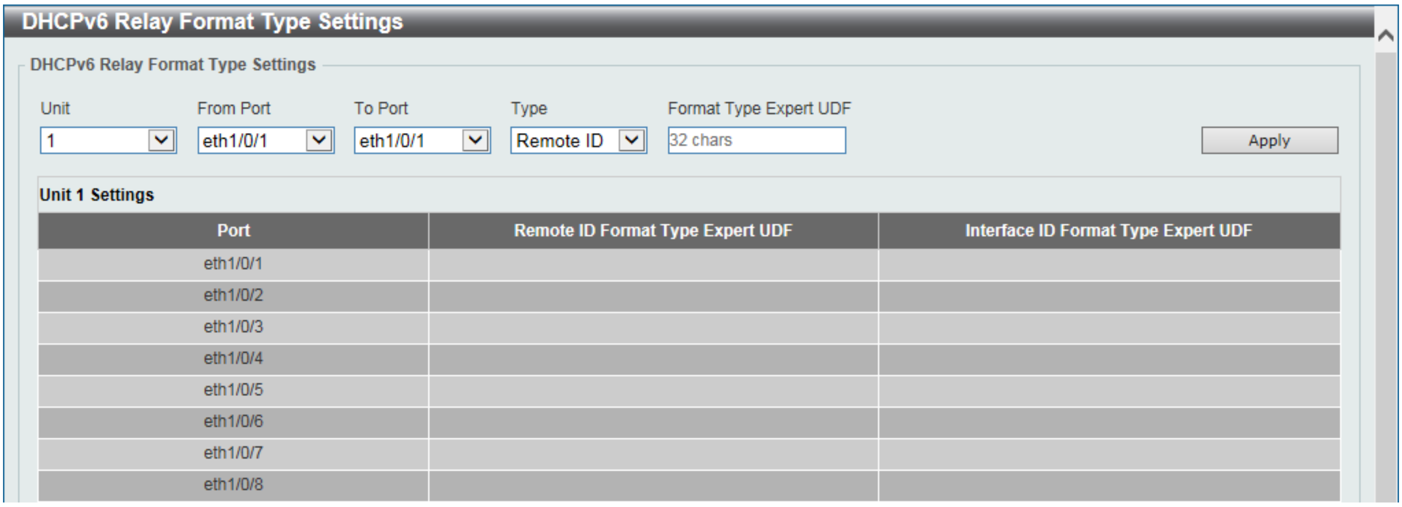
Click the **Delete** button to remove the specific entry.

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

DHCPv6 Relay Format Type Settings

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

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



DHCPv6 Relay Format Type Settings

DHCPv6 Relay Format Type Settings

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

Unit 1 Settings

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

Figure 4-63 DHCPv6 Relay Format Type Settings Window

The fields that can be configured are described below:

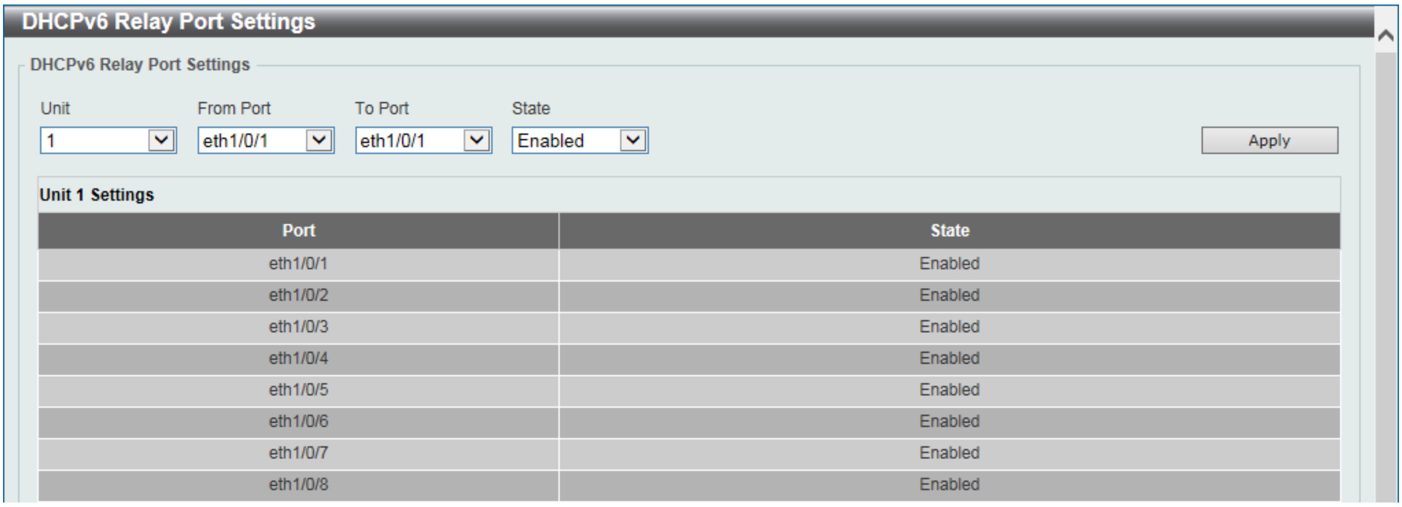
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Type	Select the type here. Options to choose from are: • **Remote ID** - Specifies to configure the Expert UDF 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:



DHCPv6 Relay Port Settings

DHCPv6 Relay Port Settings

Unit: 1 | From Port: eth1/0/1 | To Port: eth1/0/1 | State: Enabled

Unit 1 Settings

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

Figure 4-64 DHCPv6 Relay Port Settings Window

The fields that can be configured are described below:

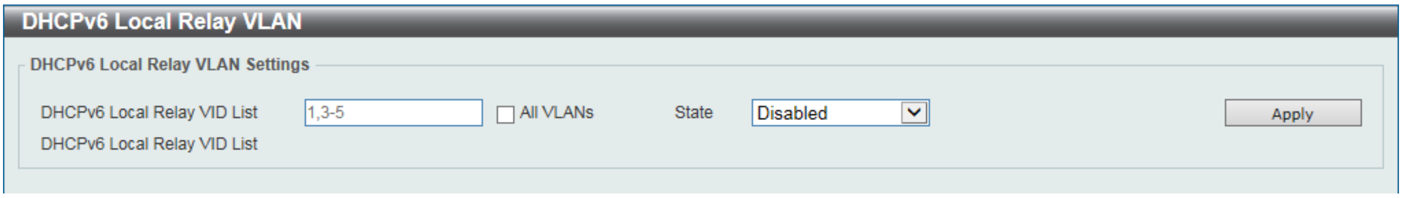
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
State	Select to enable or disable the DHCPv6 relay port feature.

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:



DHCPv6 Local Relay VLAN

DHCPv6 Local Relay VLAN Settings

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

DHCPv6 Local Relay VID List

Figure 4-65 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.

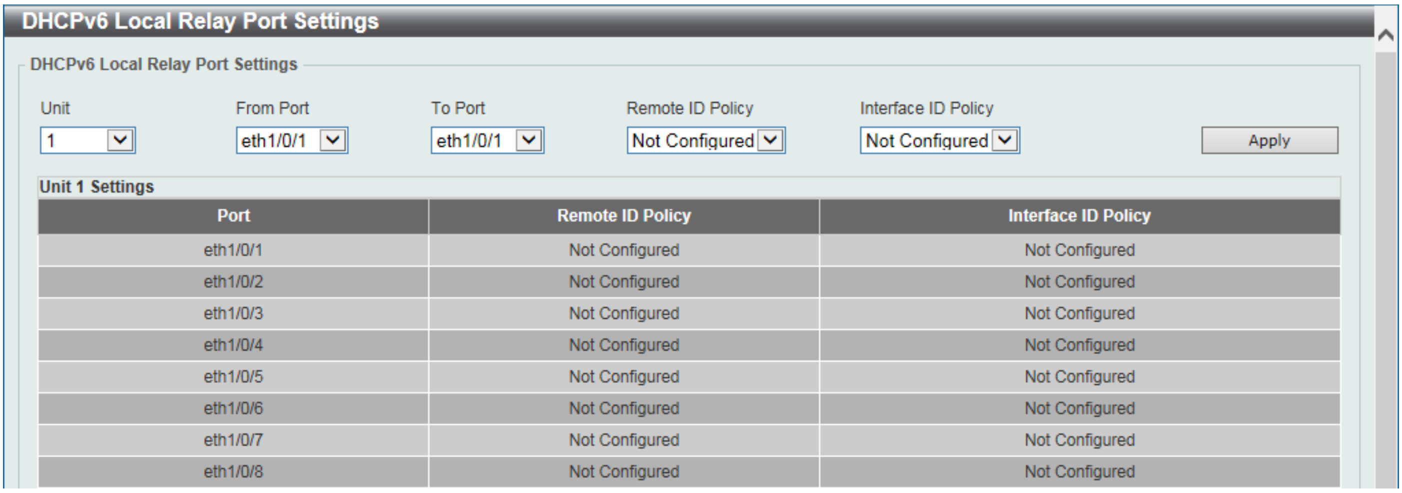
Click the **Apply** button to accept the changes made.

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

DHCPv6 Local Relay Port Settings

This window is used to display and configure the re-forwarding policy for DHCPv6 local relay port.

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



DHCPv6 Local Relay Port Settings

DHCPv6 Local Relay Port Settings

Unit	From Port	To Port	Remote ID Policy	Interface ID Policy	
1	eth1/0/1	eth1/0/1	Not Configured	Not Configured	Apply

Unit 1 Settings

Port	Remote ID Policy	Interface ID Policy
eth1/0/1	Not Configured	Not Configured
eth1/0/2	Not Configured	Not Configured
eth1/0/3	Not Configured	Not Configured
eth1/0/4	Not Configured	Not Configured
eth1/0/5	Not Configured	Not Configured
eth1/0/6	Not Configured	Not Configured
eth1/0/7	Not Configured	Not Configured
eth1/0/8	Not Configured	Not Configured

Figure 4-66 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.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Remote ID Policy	Select to choose Option 37 re-forwarding policy for the DHCPv6 relay. Options to choose from are: • **Keep** - Select to retain the existing Option 37 field in the DHCPv6 packet. • **Drop** - Select to discard the packet that already has the Option 37 field. • **Replace** - Select to replace the existing Option 37 field in the DHCPv6 packet.
Interface ID Policy	Select to choose Option 18 re-forwarding policy for the DHCPv6 relay. Options to choose from are: • **Keep** - Select to retain the existing Option 18 field in the DHCPv6 packet. • **Drop** - Select to discard the packet that already has the Option 18 field.

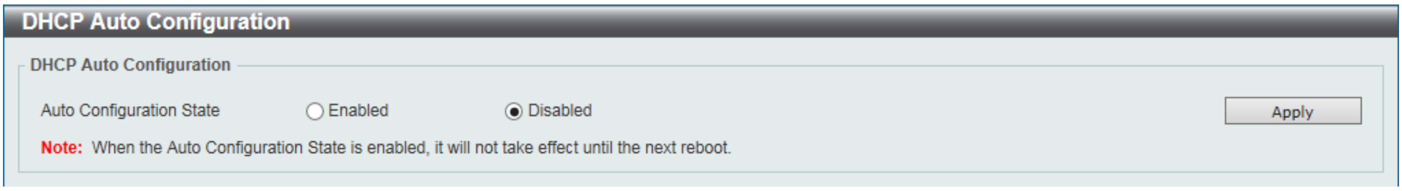
Parameter	Description
	• **Replace -** Select to replace the existing Option 18 field in the DHCPv6 packet.

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

DHCP Auto Configuration

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

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



DHCP Auto Configuration

DHCP Auto Configuration

Auto Configuration State ○ Enabled ● Disabled

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

Figure 4-67 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.

DHCP Auto Image Settings

This window is used to display and configure the DHCP auto-image settings. During the start-up time of a Switch, this function provides the capability of obtaining the image file form an external TFTP server whose IP address and file name is carried in the *DHCP OFFER* message received from the DHCP server. The system then uses this image file as the boot-up image. When the system boots up and the auto-image function is enabled, the Switch becomes a DHCP client automatically.

The DHCP client will be activated to get the network settings from the DHCP server and the DHCP server includes the TFTP server IP address and image filename with the message. The Switch then receives this information and triggers the TFTP downloading function from the specified TFTP server. At this stage, the system will display the download configuration parameters on the console. The layout is the same as using the **download firmware** command. After the firmware download was completed, the Switch will then reboot immediately.

If both the auto-configuration and auto-image features are enabled at the same time, system will download the image file first and then download the configuration. After this, the Switch will then save the configuration and reboot.

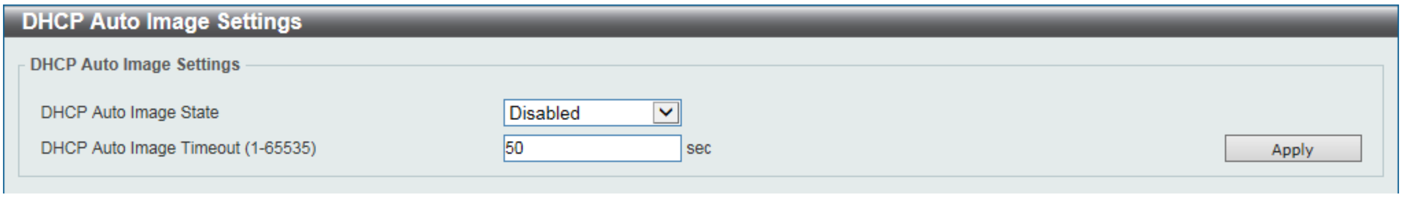
The Switch will always check the downloaded firmware. If the version is the same as the current running firmware, the Switch will terminate the auto-image process. The downloaded configuration, however, will still be executed if the auto-configuration feature is also enabled.

This function is similar to the auto-configuration function. Both the image file and the configuration file must be placed on the same TFTP server, as the DHCP option fields are not only used in the auto-image feature, but also in the auto-configuration feature. The TFTP server IP address is still placed in the DHCP *siaddr* fields Option 66 or Option 150. If Option 66, Option 150 and the *siaddr* fields exist in the DHCP response message at the same time, the Option 150 will be resolved first. If the system fails to connect to the TFTP server, then the system will resolve the Option 66, and if the system still fails to connect the TFTP server, the *siaddr* field is the last choice.

When the Switch uses Option 66 to get the TFTP server name, it resolves Option 6 first to get the DNS server IP address. If the Switch fails to connect to the DNS server or Option 6 does not exist in the response message, the Switch will try to connect the DNS server already configured in the system manually.

Option 67 is used to identify the boot file when the 'file' field in the DHCP header has been used for DHCP options. This can only be used in the DHCP auto-configuration mode and not the DHCP auto-image mode. For more information, refer to RFC 2132. When specifying the image file name, the DHCP Option 125 (RFC 3925) must be used. The Switch needs to check the *enterprise-number1* field. If the value is not the D-Link vendor ID (171), the Switch will stop the process. If the Option contains more than one field, only the first entry *enterprise-number1* will be used.

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



DHCP Auto Image Settings

DHCP Auto Image Settings

DHCP Auto Image State: Disabled

DHCP Auto Image Timeout (1-65535): 50 sec

Figure 4-68 DHCP Auto Image Settings Window

The fields that can be configured are described below:

Parameter	Description
DHCP Auto Image State	Select to enable or disable the DHCP auto-image feature here.
DHCP Auto Image Timeout	Enter the timeout value of the DHCP auto-image feature here. The range is from 1 to 65535 seconds.

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

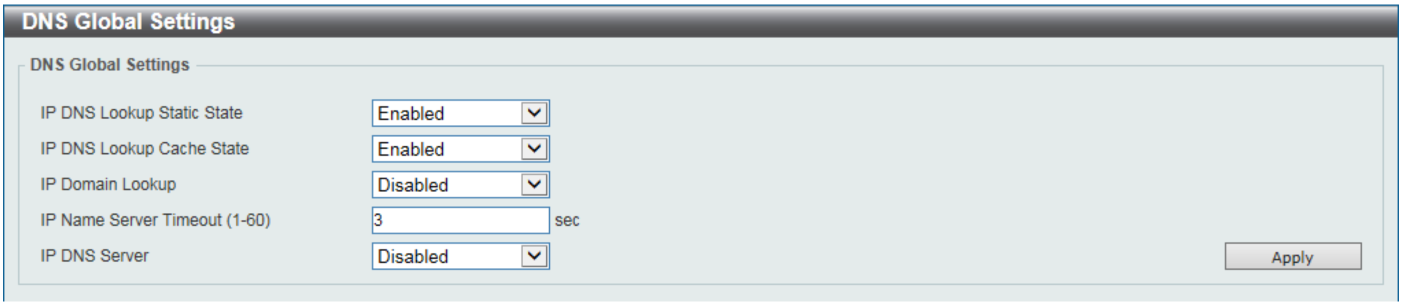
DNS

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

DNS Global Settings

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

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



DNS Global Settings

DNS Global Settings

IP DNS Lookup Static State: Enabled

IP DNS Lookup Cache State: Enabled

IP Domain Lookup: Disabled

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

IP DNS Server: Disabled

Figure 4-69 DNS Global Settings Window

The fields that can be configured are described below:

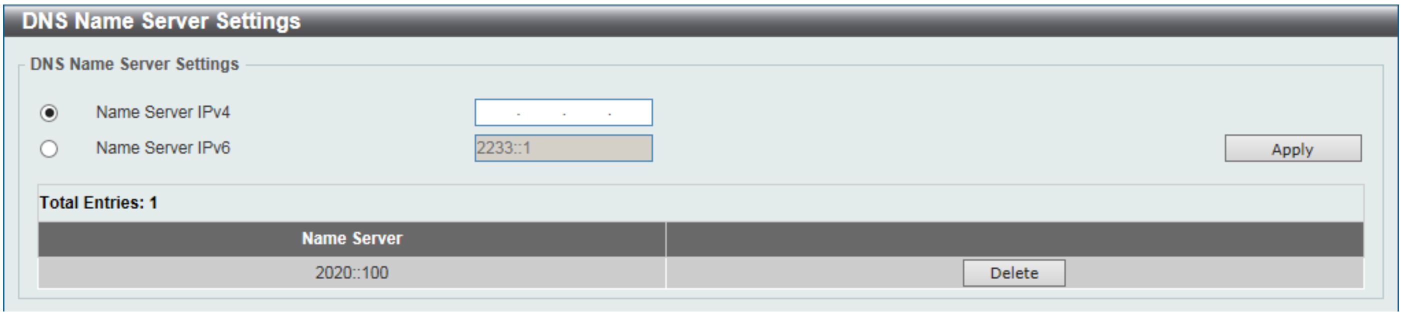
Parameter	Description
IP DNS Lookup Static State	Select to enable or disable the IP DNS lookup static state here.
IP DNS Lookup Cache State	Select to enable or disable the IP DNS lookup cache state here.
IP Domain Lookup	Select to enable or disable the IP domain lookup state here.
IP Name Server Timeout	Enter the maximum time to wait for a response from a specified name server. The range is from 1 to 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.

DNS Name Server Settings

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

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



DNS Name Server Settings

DNS Name Server Settings

● Name Server IPv4 . . .

○ Name Server IPv6 2233::1

Apply

Total Entries: 1

Name Server	
2020::100	Delete

Figure 4-70 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.

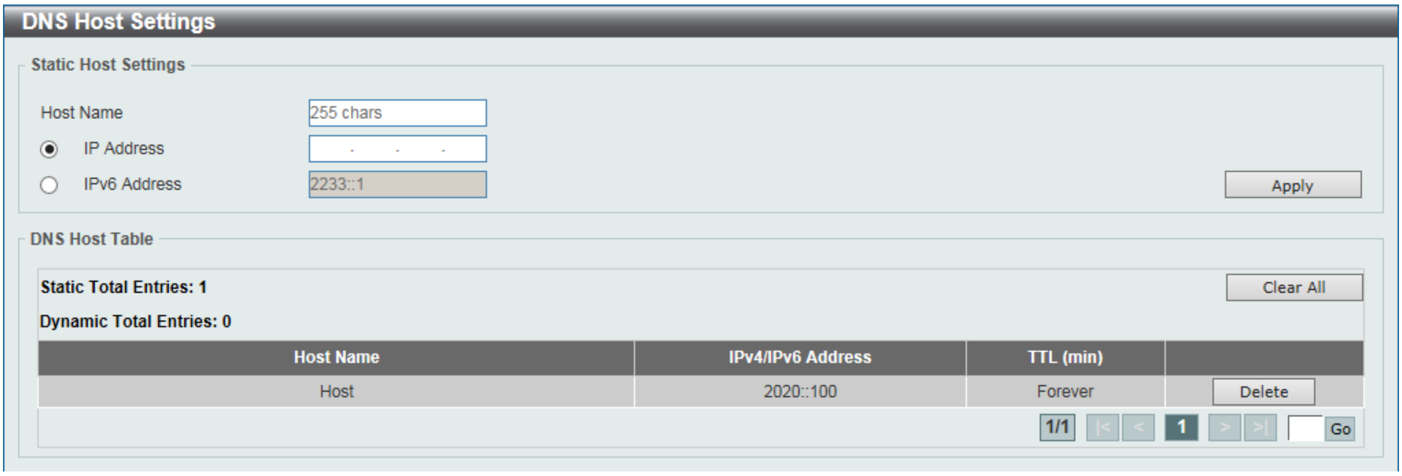
Click the **Apply** button to accept the changes made.

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:



Static Total Entries: 1

Dynamic Total Entries: 0

Host Name	IPv4/IPv6 Address	TTL (min)	
Host	2020::100	Forever	Delete

Figure 4-71 DNS Host Settings Window

The fields that can be configured are described below:

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

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

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

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

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

NTP

NTP Global Settings

This window is used to display and configure the global Network Time Protocol (NTP) settings.

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

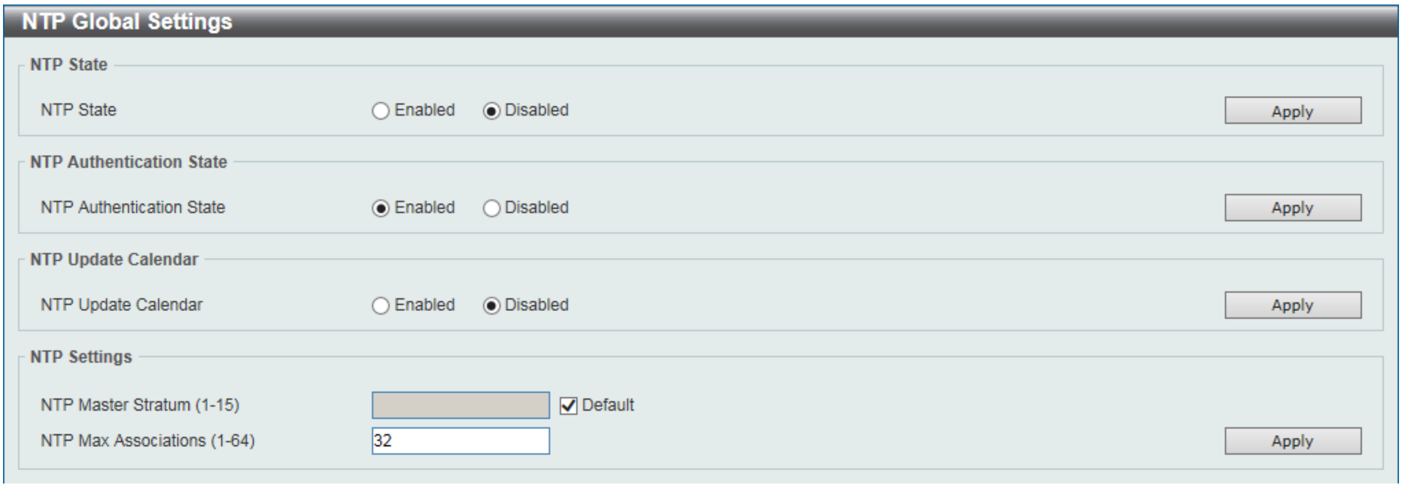

NTP Global Settings
NTP State
NTP State ○ Enabled ● Disabled
Apply
NTP Authentication State
NTP Authentication State ● Enabled ○ Disabled
Apply
NTP Update Calendar
NTP Update Calendar ○ Enabled ● Disabled
Apply
NTP Settings
NTP Master Stratum (1-15) ☑ Default
NTP Max Associations (1-64) 32
Apply

Figure 4-72 NTP Global Settings Window

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

Parameter	Description
NTP State	Select to globally enable or disable the NTP feature here.

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

The fields that can be configured in **NTP Authentication State** are described below:

Parameter	Description
NTP Authentication State	Select to enable or disable the NTP authentication state here. When this feature is enabled, networking nodes will not synchronize with the Switch unless it carries one of the authentication keys.

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

The fields that can be configured in **NTP Update Calendar** are described below:

Parameter	Description
NTP Update Calendar	Select to enable or disable the NTP update calendar feature here. This is used to periodically update the hardware clock from an NTP source.

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

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

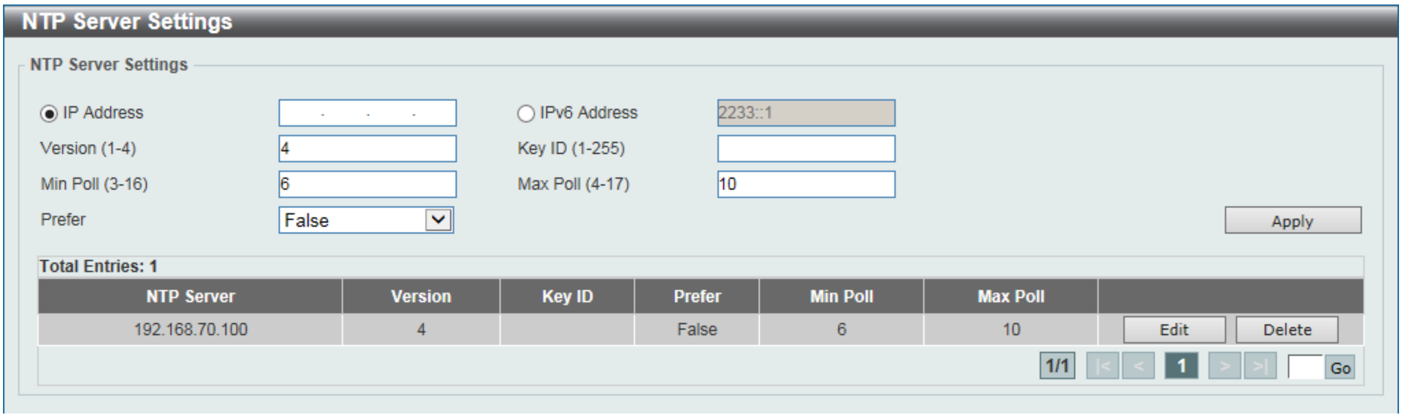
Parameter	Description
NTP Master Stratum	Enter the NTP master stratum value here. This is used to configure the Real-Time Clock (RTC) as an NTP master clock when an external NTP is not available. The range is from 1 to 15. Select the **Default** option to use the default value.
NTP Max Associations	Enter the NTP maximum association value here. This is used to configure the maximum number of NTP peers and clients on the Switch. The range is from 1 to 64.

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

NTP Server Settings

This window is used to display and configure the NTP server settings. This is used to enable the Switch to synchronize time with an NTP server.

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



NTP Server Settings

NTP Server Settings

● IP Address	. . .	○ IPv6 Address	2233::1
Version (1-4)	4	Key ID (1-255)	
Min Poll (3-16)	6	Max Poll (4-17)	10
Prefer	False		

Total Entries: 1

NTP Server	Version	Key ID	Prefer	Min Poll	Max Poll	
192.168.70.100	4		False	6	10	Edit Delete

Figure 4-73 NTP Server Settings Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Select and enter the IPv4 address of the NTP server here.
IPv6 Address	Select and enter the IPv6 address of the NTP server here.
Version	Enter the NTP version number here. The range is from 1 to 4.
Key ID	Enter the authentication key ID here. The range is from 1 to 255.
Min Poll	Enter the minimum poll value here. This specifies the minimum poll interval for NTP messages. This value is calculated as 2 to the power of the minimum poll interval value specified. For example, if the value specified here is 6, the minimum poll interval that will be used is 64 seconds (2^6=64). The range is from 3 to 16.
Max Poll	Enter the maximum poll value here. This specifies the maximum poll interval for NTP messages. This value is calculated as 2 to the power of the maximum poll interval value specified. For example, if the value specified here is 6, the maximum poll interval that will be used is 64 seconds (2^6=64). The range is from 4 to 17.
Prefer	Select whether or not this entry will be the preferred server for synchronization. Options to choose from are **True** and **False**.

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

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

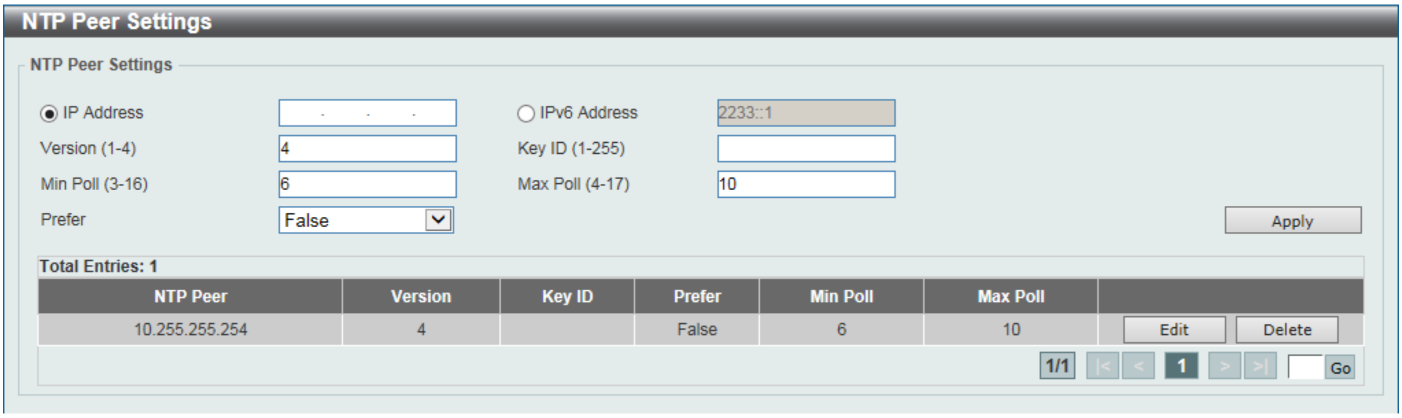
Click the **Delete** button to delete the specified entry.

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

NTP Peer Settings

This window is used to display and configure the NTP peer settings.

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



● IP Address: . . .
○ IPv6 Address: 2233::1
Version (1-4): 4
Key ID (1-255):
Min Poll (3-16): 6
Max Poll (4-17): 10
Prefer: False

Total Entries: 1

NTP Peer	Version	Key ID	Prefer	Min Poll	Max Poll	
10.255.255.254	4		False	6	10	Edit Delete

Figure 4-74 NTP Peer Settings Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Select and enter the IPv4 address of the NTP peer here.
IPv6 Address	Select and enter the IPv6 address of the NTP peer here.
Version	Enter the NTP version number here. The range is from 1 to 4.
Key ID	Enter the authentication key ID here. The range is from 1 to 255.
Min Poll	Enter the minimum poll value here. This specifies the minimum poll interval for NTP messages. This value is calculated as 2 to the power of the minimum poll interval value specified. For example, if the value specified here is 6, the minimum poll interval that will be used is 64 seconds (2^6=64). The range is from 3 to 16.
Max Poll	Enter the maximum poll value here. This specifies the maximum poll interval for NTP messages. This value is calculated as 2 to the power of the maximum poll interval value specified. For example, if the value specified here is 6, the maximum poll interval that will be used is 64 seconds (2^6=64). The range is from 4 to 17.
Prefer	Select whether or not this entry will be the preferred peer for synchronization. Options to choose from are **True** and **False**.

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

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

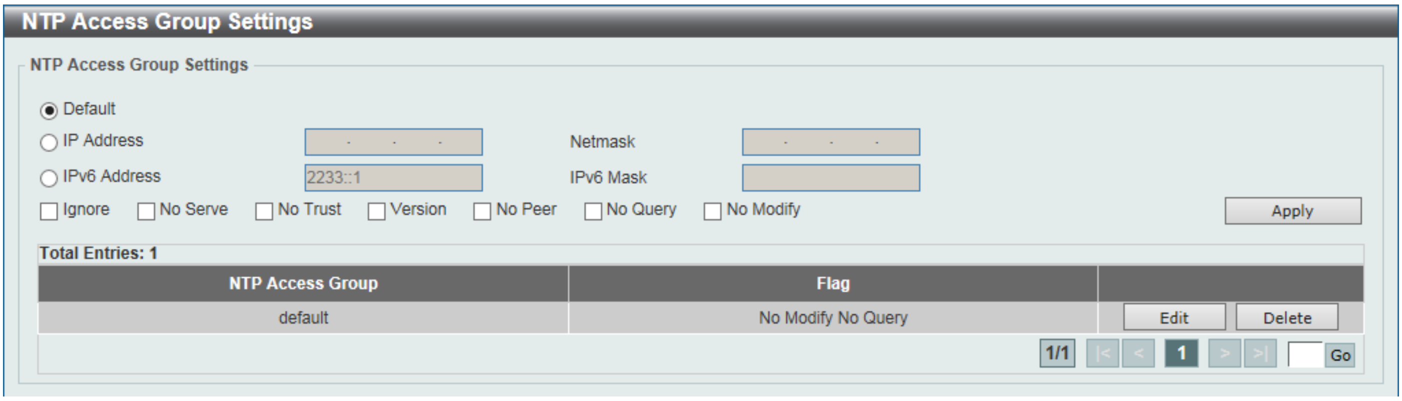
Click the **Delete** button to delete the specified entry.

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

NTP Access Group Settings

This window is used to display and configure the NTP access group settings. The NTP implements a general purpose Access Control List (ACL) containing address/match entries sorted first by increasing address values and then by increasing mask values. A match occurs when the bitwise AND of the mask and the packet source address is equal to the bitwise AND of the mask and address in the list. The list is searched in order with the last match found defining the restriction flags associated with the entry.

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



NTP Access Group Settings

NTP Access Group Settings

● Default

○ IP Address . . . Netmask . . .

○ IPv6 Address 2233::1 IPv6 Mask

□ Ignore □ No Serve □ No Trust □ Version □ No Peer □ No Query □ No Modify

Total Entries: 1

NTP Access Group	Flag	
default	No Modify No Query	Edit Delete

Figure 4-75 NTP Access Group Settings Window

The fields that can be configured are described below:

Parameter	Description
Default	Select this option to specify to use the default IPv4 (0.0.0.0/0.0.0.0) or IPv6 (::/::) address. The default IP address is always included with the lowest priority in the list.
IP Address	Select and enter the host IPv4 address here.
Netmask	Enter the IPv4 netmask of the host network here.
IPv6 Address	Select and enter the host IPv6 address here.
IPv6 Mask	Enter the IPv6 prefix length of the host network here.
Ignore	Select this option to deny all packets, including NTP control queries.
No Serve	Select this option to deny all packets except NTP control queries.
No Trust	Select this option to deny packets that are not cryptographically authenticated.
Version	Select this option to deny packets that mismatch the current NTP version.
No Peer	Select this option to deny packets that might mobilize an association unless authenticated. The packets include broadcast, symmetric-active and many cast server packets when a configured association does not exist. Note that this flag does not apply to packets that do not attempt to mobilize an association.
No Query	Select this option to deny all NTP control queries.
No Modify	Select this option to deny the NTP control queries that attempt to modify the state of the server.

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

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

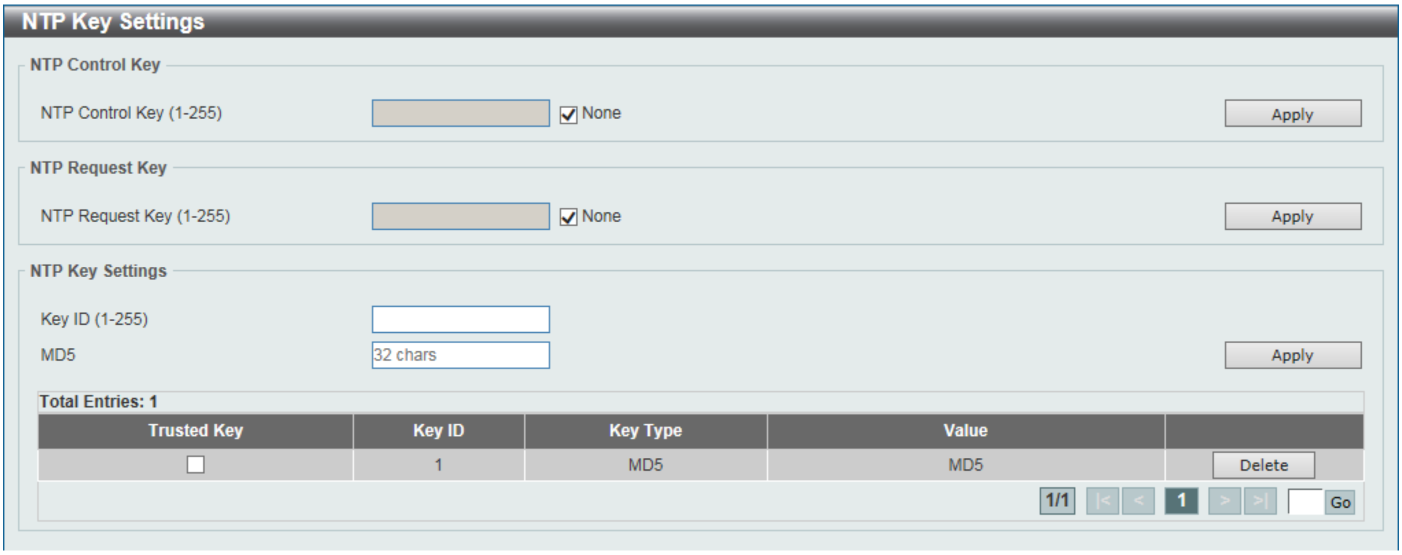
Click the **Delete** button to delete the specified entry.

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

NTP Key Settings

This window is used to display and configure the NTP key settings.

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



NTP Key Settings

NTP Control Key

NTP Control Key (1-255) ☑ None

NTP Request Key

NTP Request Key (1-255) ☑ None

NTP Key Settings

Key ID (1-255)

MD5: 32 chars

Total Entries: 1

Trusted Key	Key ID	Key Type	Value	
□	1	MD5	MD5	Delete

Figure 4-76 NTP Key Settings Window

The fields that can be configured in **NTP Control Key** are described below:

Parameter	Description
NTP Control Key	Enter the NTP control key here. This is used to define the key ID for the NTP control messages. The range is from 1 to 255. Select the **None** option to disable this feature.

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

The fields that can be configured in **NTP Request Key** are described below:

Parameter	Description
NTP Request Key	Enter the NTP request key here. This is used to define the key ID for NTP mode 7 packets, used by the *ntpdc* utility program. The range is from 1 to 255. Select the **None** option to disable this feature.

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

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

Parameter	Description
Key ID	Enter the NTP key ID here. The range is from 1 to 255.
MD5	Enter the MD5 authentication key string here. This string can be up to 32 characters long.
Trusted Key	Select this option to specify that the key for a peer NTP system is trusted for authentication.

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

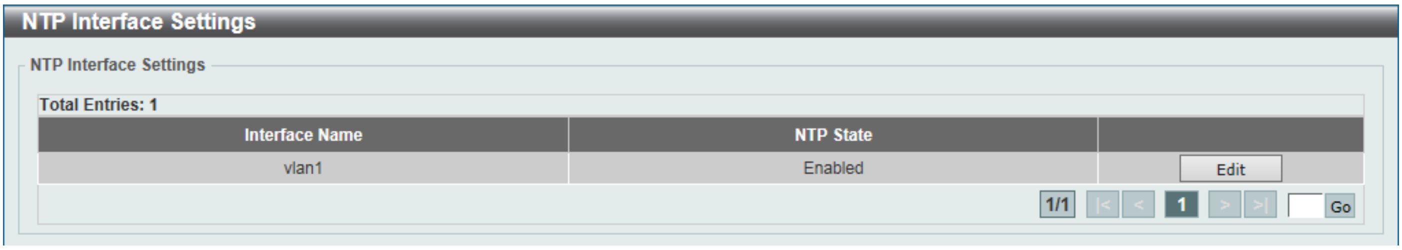
Click the **Delete** button to delete the specified entry.

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

NTP Interface Settings

This window is used to display and configure the NTP interface settings. This is used to either prevent or allow an interface from receiving NTP packets.

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



Total Entries: 1

Interface Name	NTP State	
vlan1	Enabled	Edit

Figure 4-77 NTP Interface Settings Window

The fields that can be configured are described below:

Parameter	Description
NTP State	After click the **Edit** button, select to enable or disable the NTP state for the specified VLAN interface here.

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

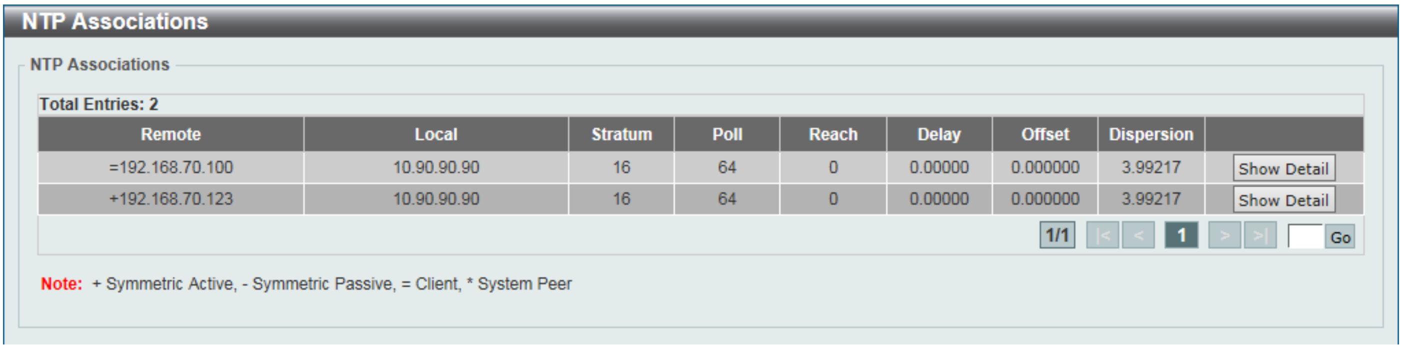
Click the **Apply** button to accept the changes made.

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

NTP Associations

This window is used to view NTP association information.

To view the following window, click **Management > NTP > NTP Associations**, as shown below:



Total Entries: 2

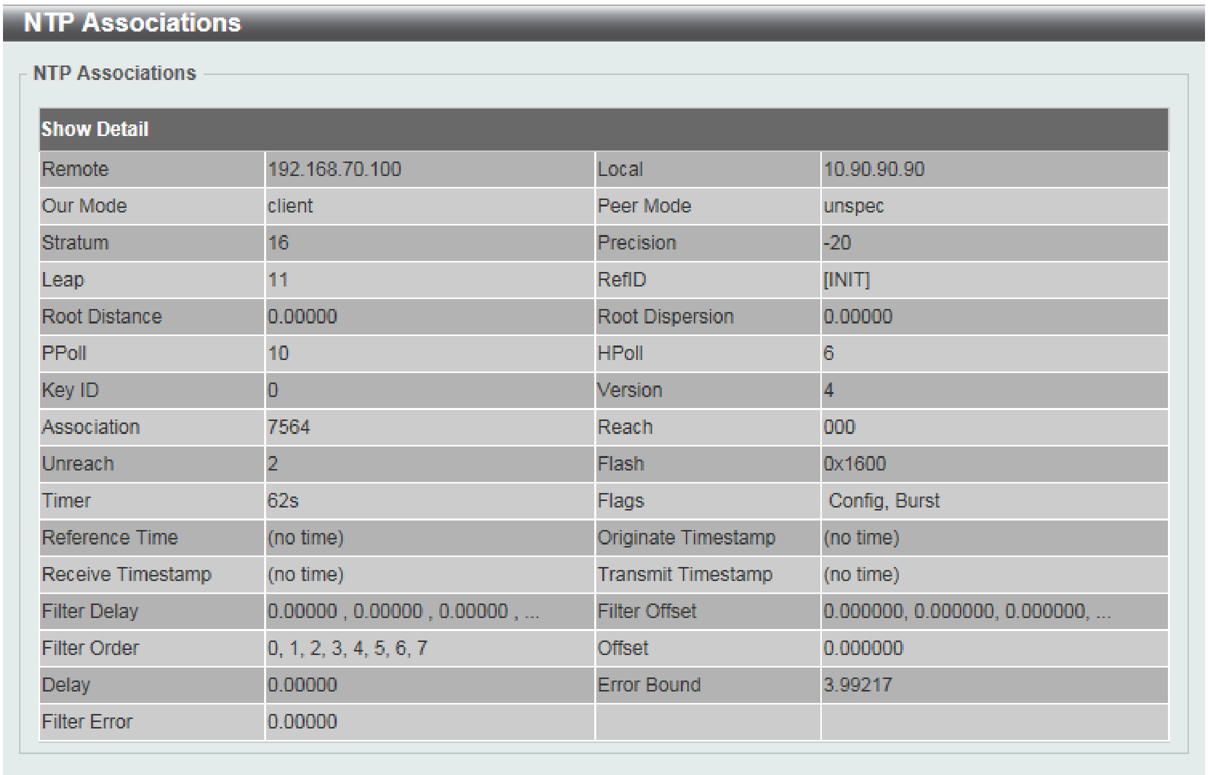
Remote	Local	Stratum	Poll	Reach	Delay	Offset	Dispersion	
=192.168.70.100	10.90.90.90	16	64	0	0.00000	0.000000	3.99217	Show Detail
+192.168.70.123	10.90.90.90	16	64	0	0.00000	0.000000	3.99217	Show Detail

Note: + Symmetric Active, - Symmetric Passive, = Client, * System Peer

Figure 4-78 NTP Associations Window

Click the **Show Detail** button to view more detailed information about the entry.

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



NTP Associations

NTP Associations

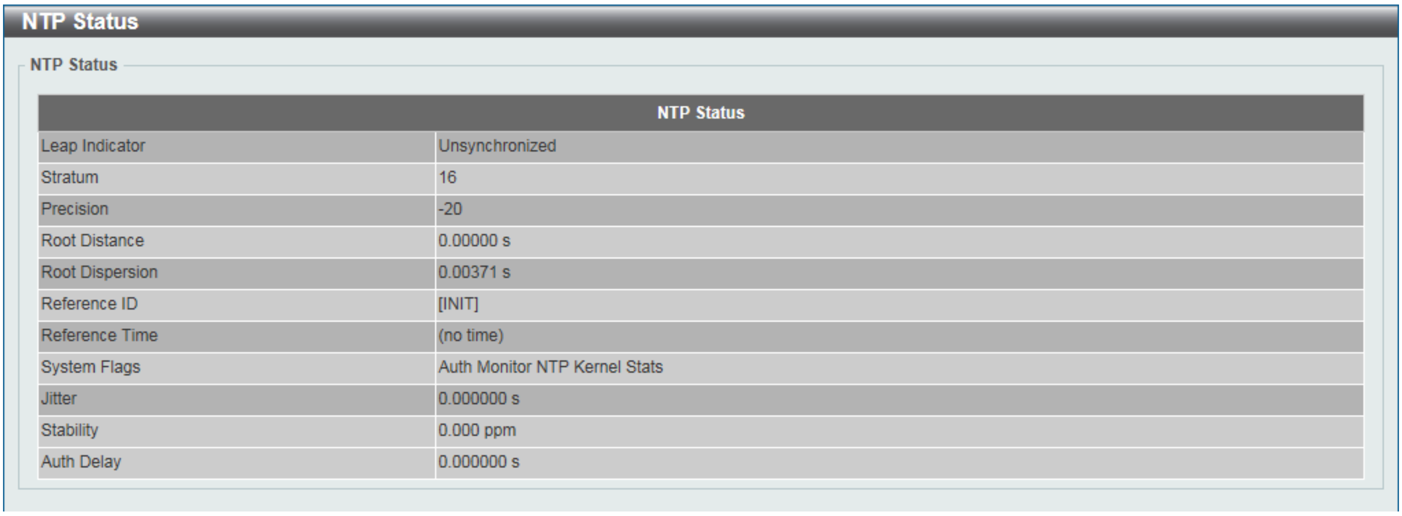
Show Detail			
Remote	192.168.70.100	Local	10.90.90.90
Our Mode	client	Peer Mode	unspec
Stratum	16	Precision	-20
Leap	11	RefID	[INIT]
Root Distance	0.00000	Root Dispersion	0.00000
PPoll	10	HPoll	6
Key ID	0	Version	4
Association	7564	Reach	000
Unreach	2	Flash	0x1600
Timer	62s	Flags	Config, Burst
Reference Time	(no time)	Originate Timestamp	(no time)
Receive Timestamp	(no time)	Transmit Timestamp	(no time)
Filter Delay	0.00000 , 0.00000 , 0.00000 , ...	Filter Offset	0.000000, 0.000000, 0.000000, ...
Filter Order	0, 1, 2, 3, 4, 5, 6, 7	Offset	0.000000
Delay	0.00000	Error Bound	3.99217
Filter Error	0.00000		

Figure 4-79 NTP Associations (Show Detail) Window

NTP Status

This window is used to view NTP status information.

To view the following window, click **Management > NTP > NTP Status**, as shown below:



NTP Status

NTP Status

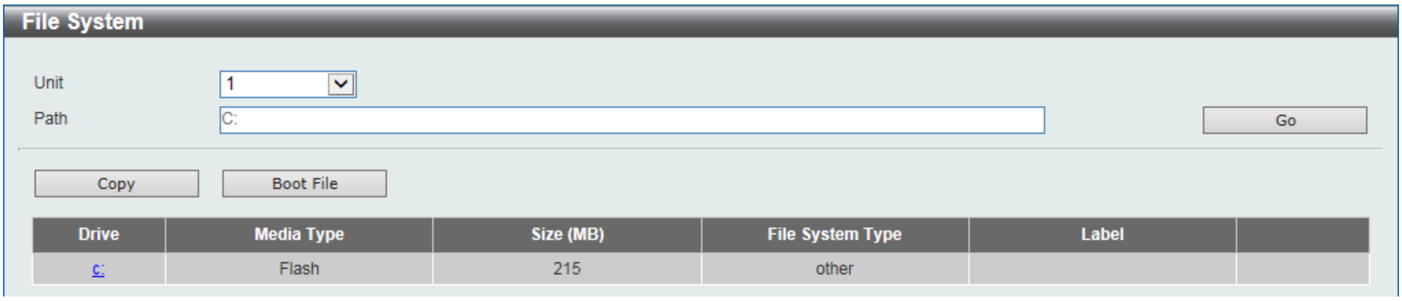
NTP Status	
Leap Indicator	Unsynchronized
Stratum	16
Precision	-20
Root Distance	0.00000 s
Root Dispersion	0.00371 s
Reference ID	[INIT]
Reference Time	(no time)
System Flags	Auth Monitor NTP Kernel Stats
Jitter	0.000000 s
Stability	0.000 ppm
Auth Delay	0.000000 s

Figure 4-80 NTP Status Window

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:



Unit: 1

Path: C:

Drive	Media Type	Size (MB)	File System Type	Label	
c:	Flash	215	other		

Figure 4-81 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.
Path	Enter the path string.

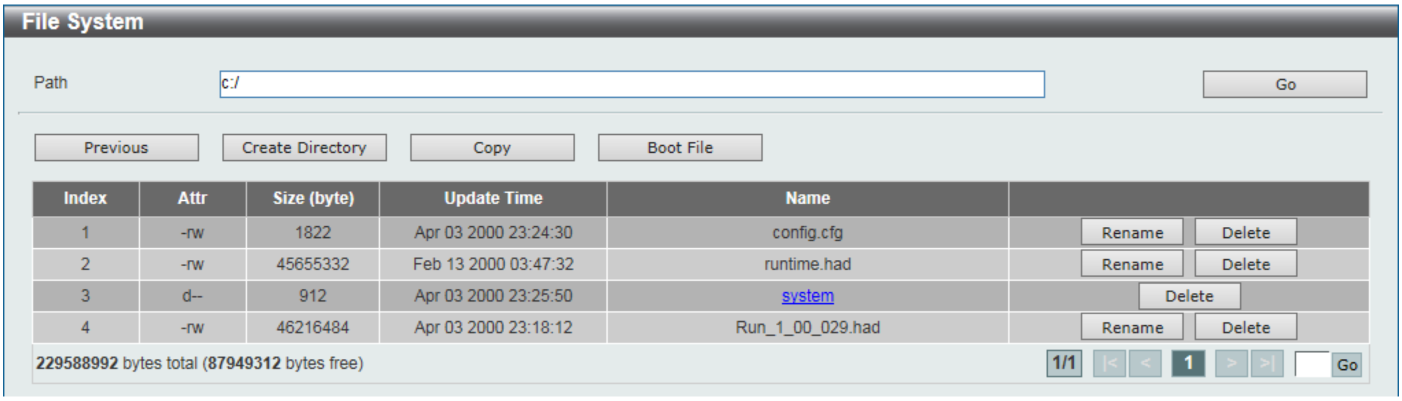
Click the **Go** button to navigate to the path entered.

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

Click the **Boot File** button to specify which boot image and configuration to use.

Click the **c:** hyperlink to navigate the C: drive

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



Path: c:/

Index	Attr	Size (byte)	Update Time	Name	
1	-rw	1822	Apr 03 2000 23:24:30	config.cfg	Rename Delete
2	-rw	45655332	Feb 13 2000 03:47:32	runtime.had	Rename Delete
3	d--	912	Apr 03 2000 23:25:50	system	Delete
4	-rw	46216484	Apr 03 2000 23:18:12	Run_1_00_029.had	Rename Delete

229588992 bytes total (**87949312** bytes free)

Figure 4-82 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.

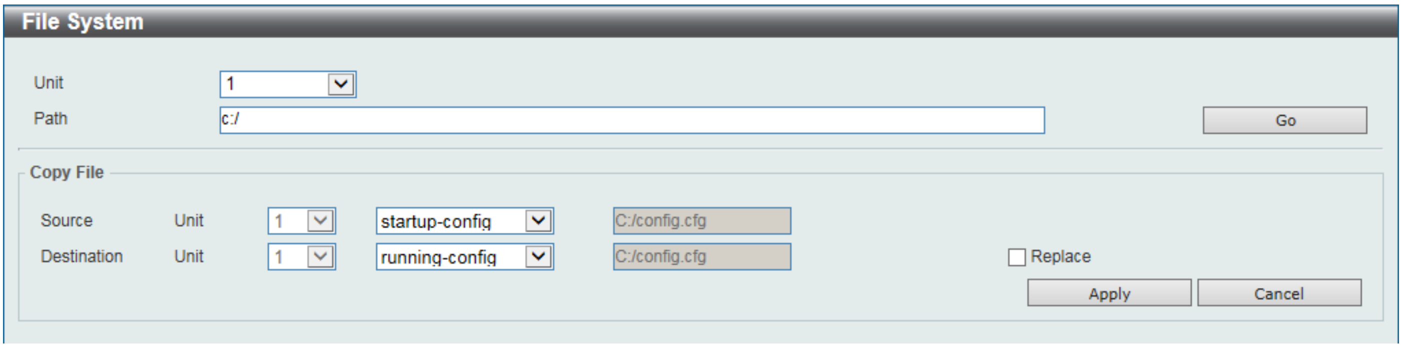
Click the **Copy** button to copy a specific file to the Switch.

Click the **Boot File** button to specify which boot image and configuration to use.

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

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

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



File System

Unit: 1

Path: c:/

Go

Copy File

Source Unit: 1, startup-config, C:/config.cfg

Destination Unit: 1, running-config, C:/config.cfg

□ Replace

Apply Cancel

Figure 4-83 File System (Copy) Window

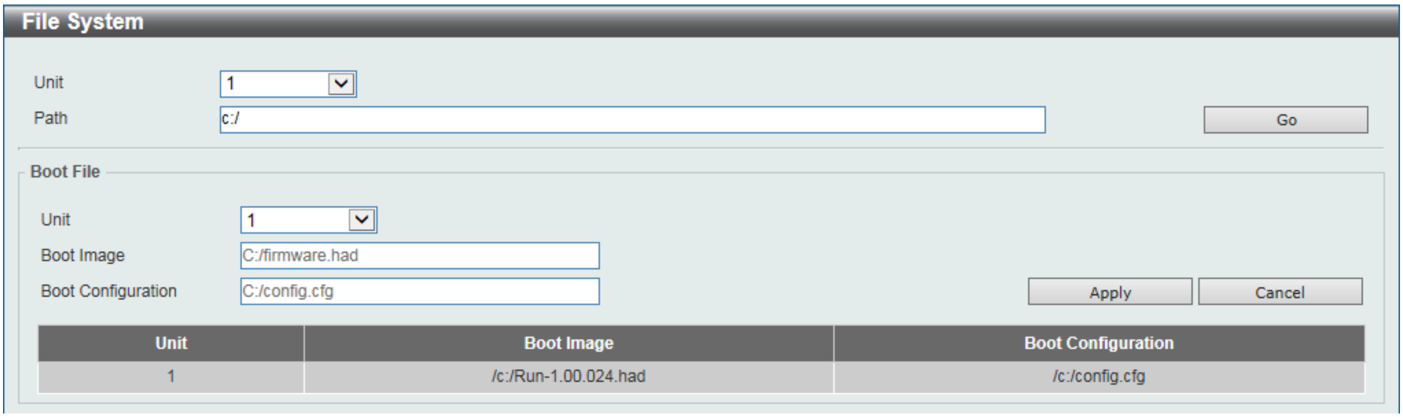
The fields that can be configured in **Copy File** are described below:

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 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 **running-config**, **startup-config**, and **Destination File**. Only after selecting the **Destination File** option can the destination file path and filename be entered in the space provided. Select the **Replace** check box to replace the current running configuration with the indicated configuration file.

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

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

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



File System

Unit: 1

Path: c:/

Go

Boot File

Unit: 1

Boot Image: C:/firmware.had

Boot Configuration: C:/config.cfg

Apply Cancel

Unit	Boot Image	Boot Configuration
1	/c:/Run-1.00.024.had	/c:/config.cfg

Figure 4-84 File System (Boot File) Window

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

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
Boot Image	Enter the path to the boot image file here.
Boot Configuration	Enter the path to the boot configuration file here.

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

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

Stacking

Switches in the series can be physically stacked by utilizing the last four ports on the front panel of the Switch. It is possible to stack up to nine Switches, which can then be managed through a single connection to any of the LAN ports using Telnet, the Web UI, and SNMP. This cost-effective Switch presents an economical solution for administrators aiming to upgrade their networks, leveraging the stacking ports for scaling and stacking purposes. This ultimately enhances overall reliability, serviceability, and availability.

The Switch supports the following stacking topologies:

- **Duplex Chain** - This topology interconnects Switches in a chain-link format, enabling data transfer in one direction only. A disruption in the chain will impact data transfer.
- **Duplex Ring** - In this topology, Switches form a ring or circle, allowing data transfer in two directions. It is highly robust, as even if the ring is broken, data can still be transmitted via the stacking cables between Switches using an alternative route.

In the following diagram, Switches are stacked in the **Duplex Chain** topology.

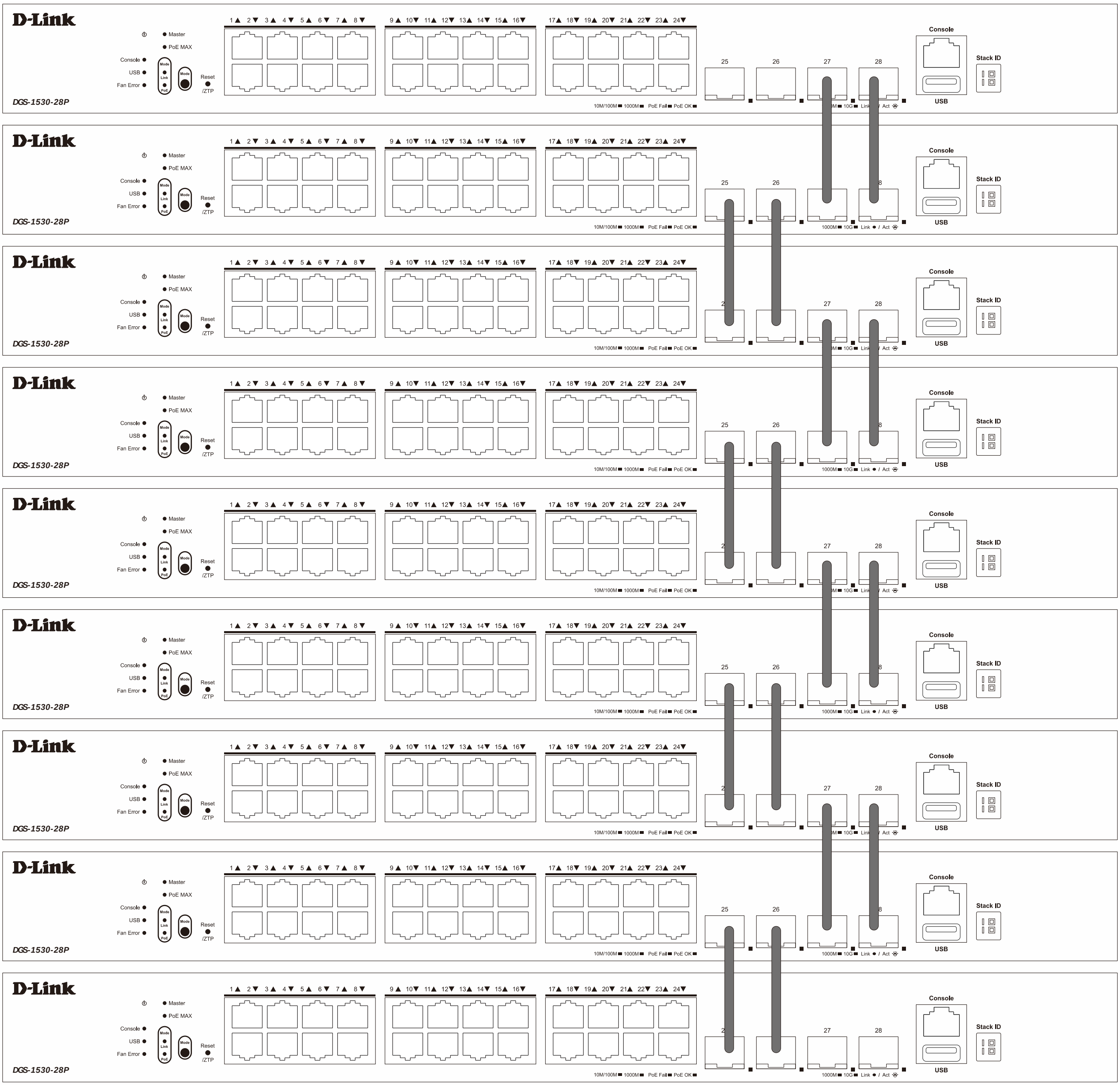


Figure 4-85 Duplex Chain Stacking Topology

In the following diagram, Switches are stacked in the **Duplex Ring** topology.

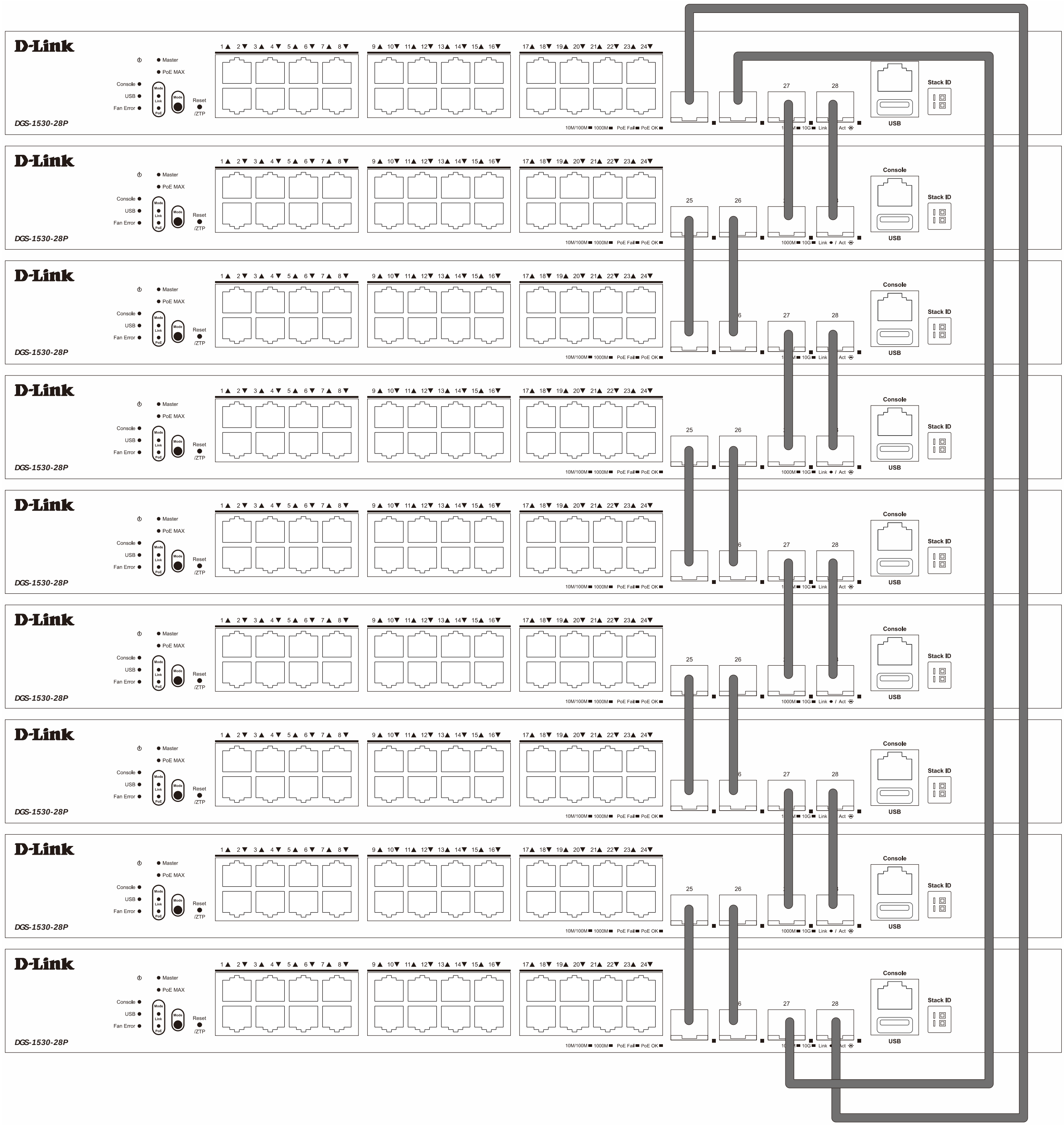


Figure 4-86 Duplex Ring Stacking Topology

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.

- **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.
- **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 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 lowest MAC address.

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.

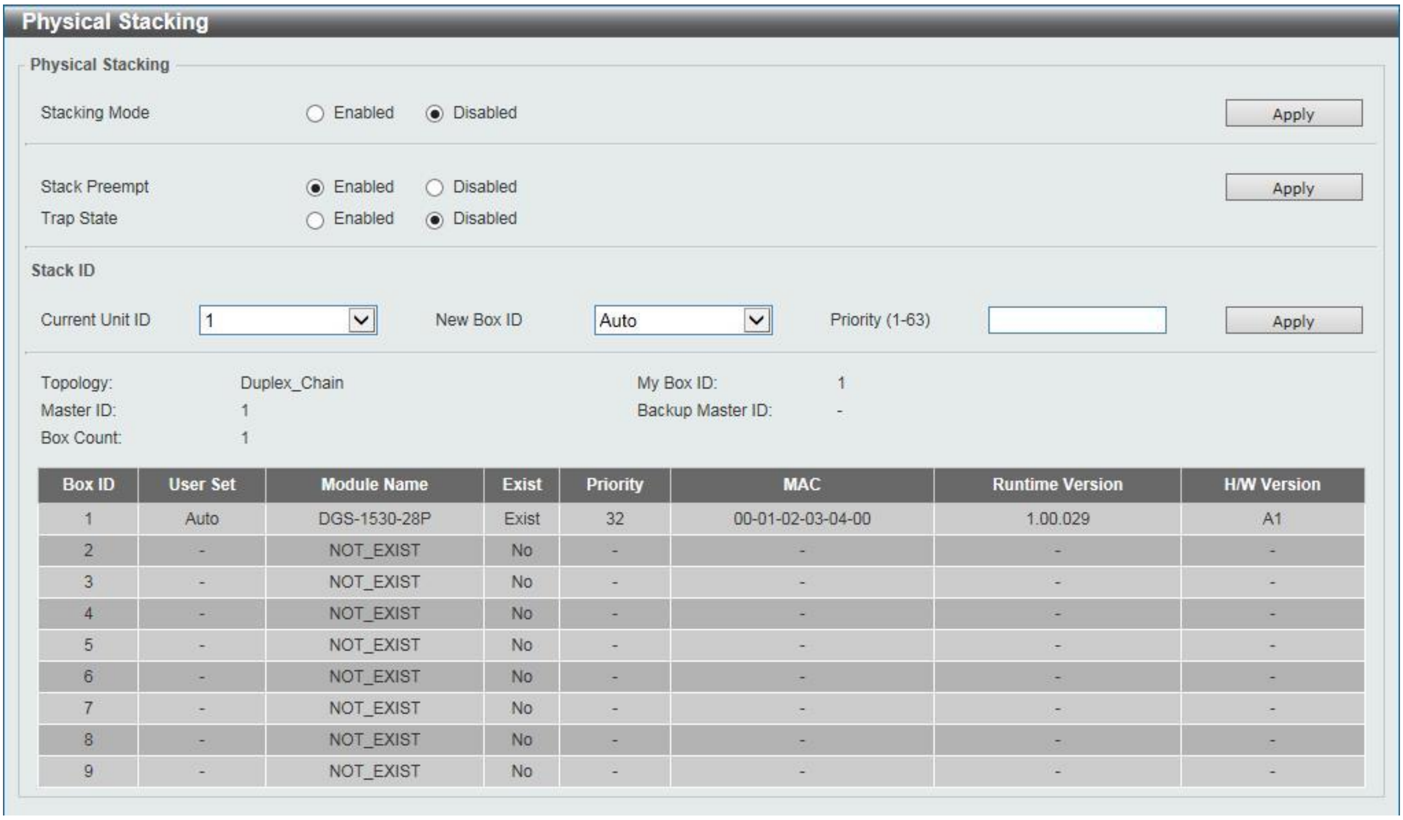
If both the Primary Master and the Backup Master are removed, the election process is immediately initiated, and a new Primary Master and Backup Master are elected. Switches in the stack will clear the configuration of the units that have been removed, and dynamically learned databases, such as ARP, 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.

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:



Physical Stacking

Physical Stacking

Stacking Mode ○ Enabled ● Disabled [Apply]

Stack Preempt ● Enabled ○ Disabled [Apply]

Trap State ○ Enabled ● Disabled

Stack ID

Current Unit ID: 1 New Box ID: Auto Priority (1-63): [Apply]

Topology: Duplex_Chain

Master ID: 1

Box Count: 1

My Box ID: 1

Backup Master ID: -

Box ID	User Set	Module Name	Exist	Priority	MAC	Runtime Version	H/W Version
1	Auto	DGS-1530-28P	Exist	32	00-01-02-03-04-00	1.00.029	A1
2	-	NOT_EXIST	No	-	-	-	-
3	-	NOT_EXIST	No	-	-	-	-
4	-	NOT_EXIST	No	-	-	-	-
5	-	NOT_EXIST	No	-	-	-	-
6	-	NOT_EXIST	No	-	-	-	-
7	-	NOT_EXIST	No	-	-	-	-
8	-	NOT_EXIST	No	-	-	-	-
9	-	NOT_EXIST	No	-	-	-	-

Figure 4-87 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.
Stack Preempt	Select this option to enable or disable preemption of the master role when a unit with a higher priority is added to the Switch.
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:

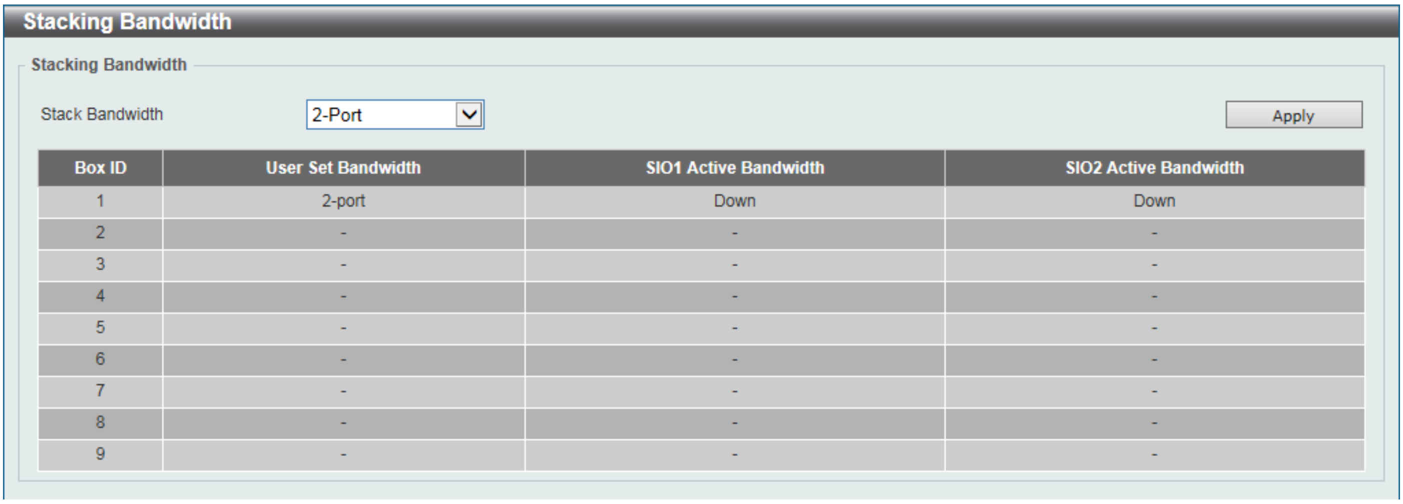
Parameter	Description
Current Unit ID	Select the unit ID of the Switch in the stack.
New Box ID	Select the new box ID for the Switch that is selected in the **Current Unit ID** field. The range is from 1 to 9. **Auto** will automatically assign a box number to the Switch in the Switch stack.
Priority	Enter the priority of the Switch stacking unit. The range is from 1 to 63.

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

Stacking Bandwidth

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

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



Stacking Bandwidth

Stacking Bandwidth

Stack Bandwidth: 2-Port

Box ID	User Set Bandwidth	SIO1 Active Bandwidth	SIO2 Active Bandwidth
1	2-port	Down	Down
2	-	-	-
3	-	-	-
4	-	-	-
5	-	-	-
6	-	-	-
7	-	-	-
8	-	-	-
9	-	-	-

Figure 4-88 Stacking Bandwidth Window

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

Parameter	Description
Stack Bandwidth	Select this option to use 2 or 4 ports 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 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:

- **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.
- **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.
- **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.

Upgrade to v1.61

To better improve SIM management, the Switches have been upgraded to SIM version 1.61. Many improvements have been made, including the Commander Switch (CS) now having the capability to automatically rediscover member switches that have left the SIM group, either through a reboot or web malfunction. This is accomplished through the use of Discover packets and Maintenance packets that previously configured SIM members will send and receive after a reboot. Once a MS has had its MAC address and password saved to the CS's database, if a reboot occurs in the MS, the CS will keep this MS information in its database and when a MS has been rediscovered, it will add the MS back into the SIM tree automatically. No configuration will be necessary to rediscover these switches.

There are some instances where pre-saved MS Switches cannot be rediscovered. For example, if the Switch is still powered down, if it has become the member of another group, or if it has been configured to be a Commander Switch, the rediscovery process cannot occur.

The topology map now includes new features for connections that are a member of a port trunking group. It will display the speed and number of Ethernet connections creating this port trunk group.

This version will support Switch upload and downloads for firmware, configuration files, and log files, as follows:

- **Firmware** - The Switch now supports MS firmware downloads from a TFTP server.
- **Configuration Files** - This Switch now supports the downloading and uploading of configuration files both to (for configuration restoration) and from (for configuration backup) MSs, using a TFTP server.
- **Log** - The Switch now supports uploading MS log files to a TFTP server.

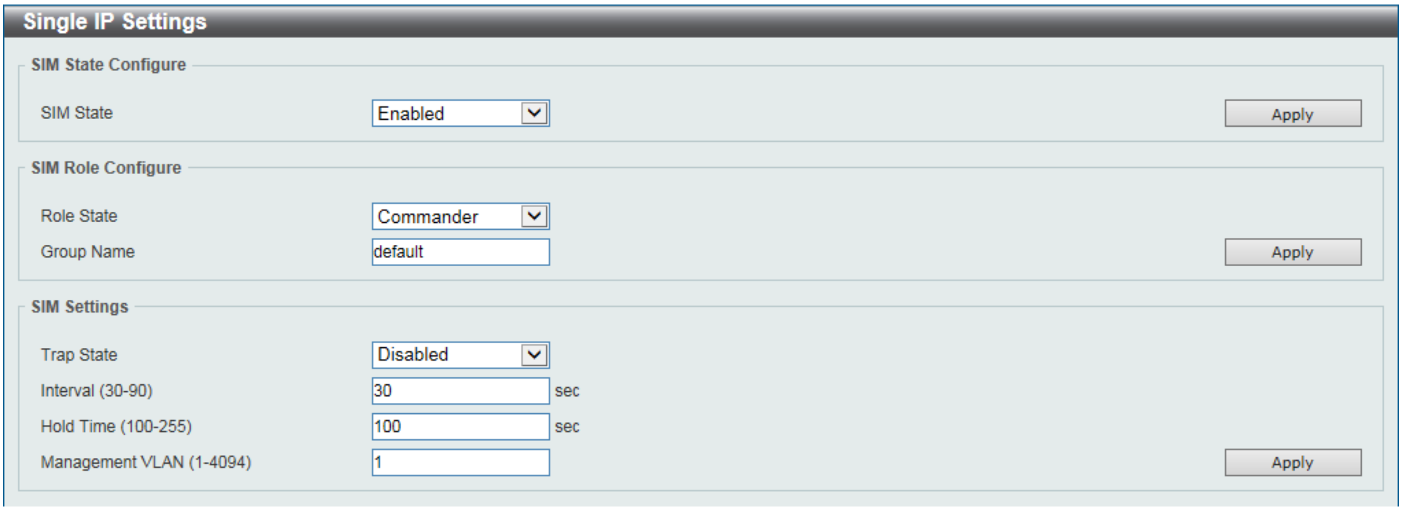
The user may zoom in and zoom out when utilizing the topology window to get a better, more defined view of the configuration.

NOTE: When the **SIM State** is enabled and the **Role State** of the Switch is **Commander**, the **Topology**, **Firmware Upgrade**, **Configuration File Backup/Restore**, and **Upload Log File** windows will be available.

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:



Single IP Settings

SIM State Configure

SIM State: Enabled

SIM Role Configure

Role State: Commander

Group Name: default

SIM Settings

Trap State: Disabled

Interval (30-90): 30 sec

Hold Time (100-255): 100 sec

Management VLAN (1-4094): 1

Figure 4-89 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** - A Candidate Switch (CaS) is not the member of a SIM group but is connected to a Commander Switch. • **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. By default, the **Candidate** option is used.
Group Name	Enter a group name. 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.

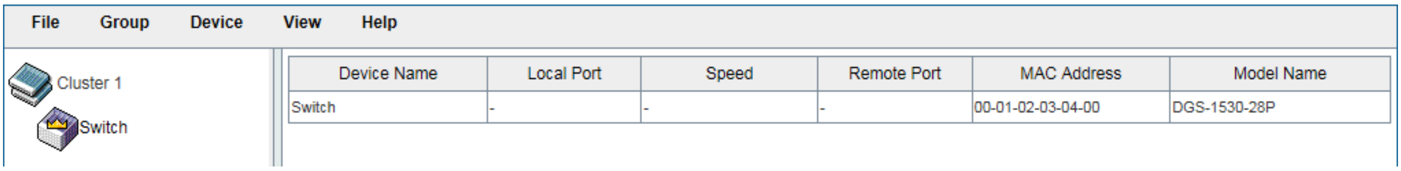
Click the **Apply** button to accept the changes made.

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 script to function properly on your computer.

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



Device Name	Local Port	Speed	Remote Port	MAC Address	Model Name
Switch	-	-	-	00-01-02-03-04-00	DGS-1530-28P

Figure 4-90 Topology Window

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

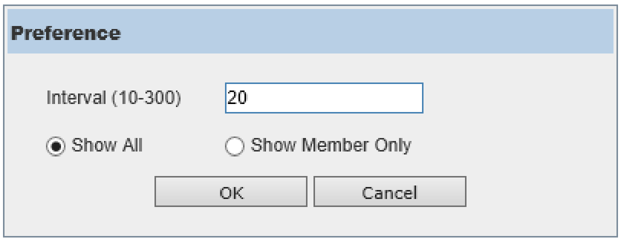
File

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.


Preference

Interval (10-300) 20

● Show All ○ Show Member Only

Figure 4-91 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.

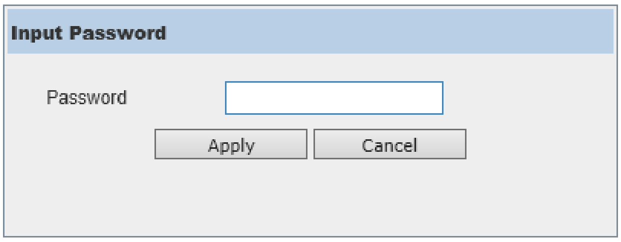
Click the **OK** button to accept the changes made.

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.



Input Password

Password

Figure 4-92 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:

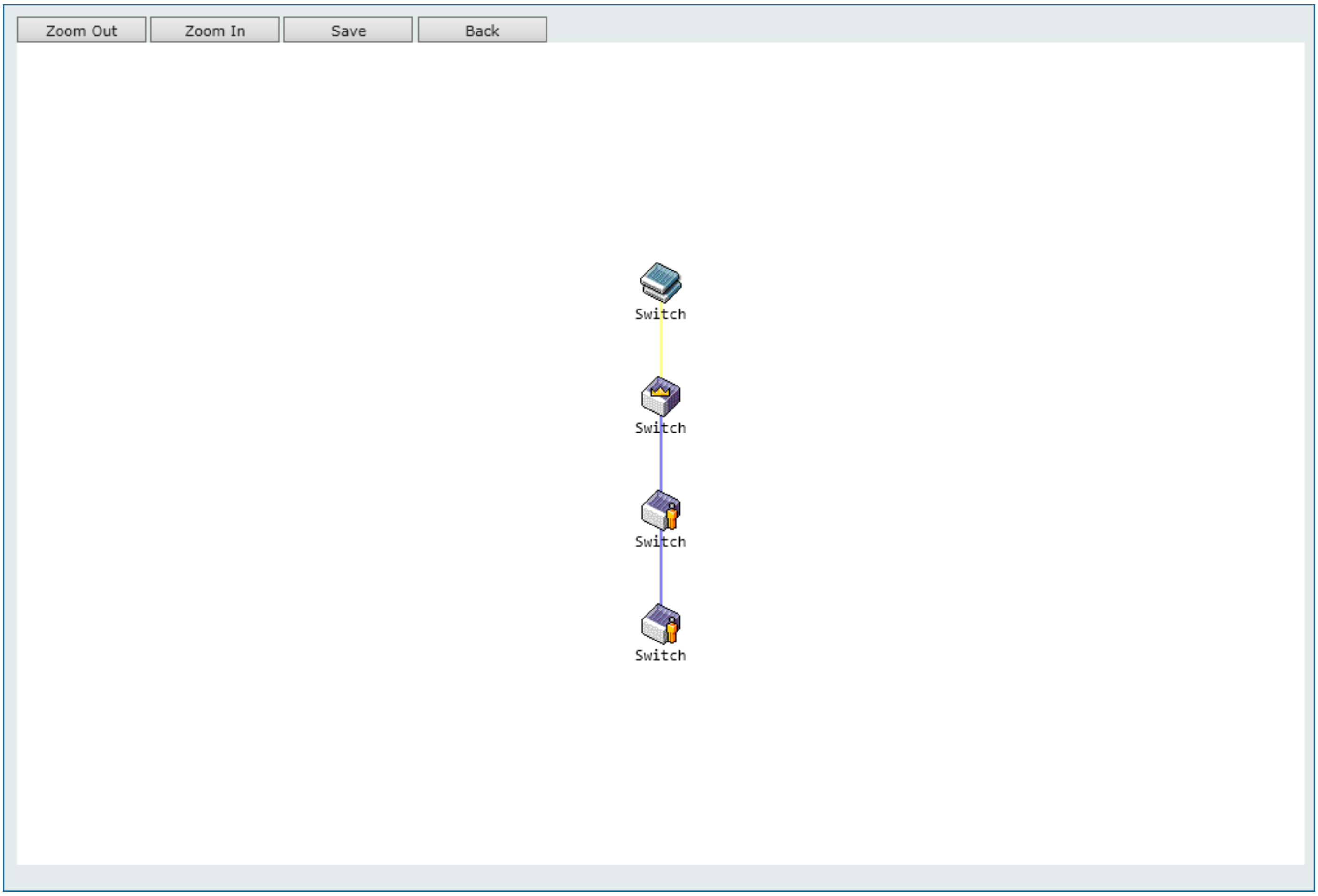


Figure 4-93 View > Topology

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.

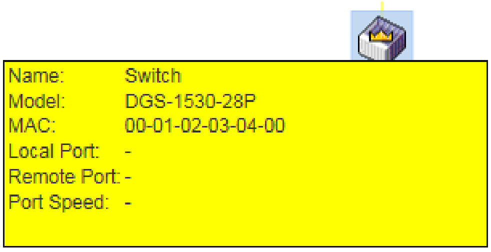
Click the **Back** button to return to the previous window.

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
	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
	Non-SIM devices		

Tool Tips

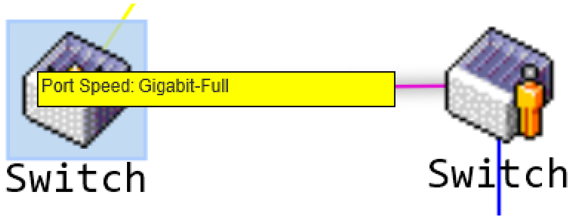
In the Topology view window, the mouse plays an important role in configuration and in viewing device information. Hover the mouse pointer over a specific device in the Topology window to display more information about the device



Name: Switch
Model: DGS-1530-28P
MAC: 00-01-02-03-04-00
Local Port: -
Remote Port: -
Port Speed: -

Figure 4-94 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.

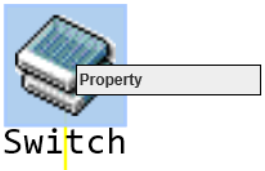
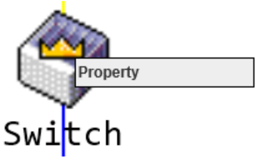
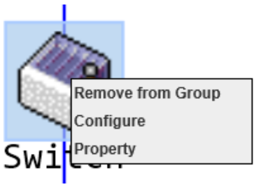
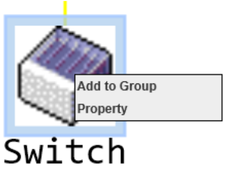


Port Speed: Gigabit-Full

Figure 4-95 Port Speed Utilizing the Tool Tip

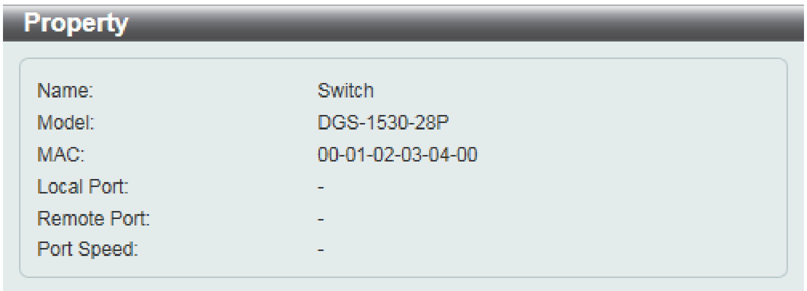
Right-Click

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.



Name:	Switch
Model:	DGS-1530-28P
MAC:	00-01-02-03-04-00
Local Port:	-
Remote Port:	-
Port Speed:	-

Figure 4-96 Property

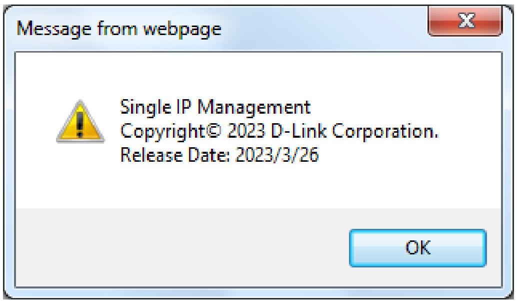
The fields displayed are described below:

Parameter	Description
Name	Displays the device name of the Switch in the SIM group.
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.



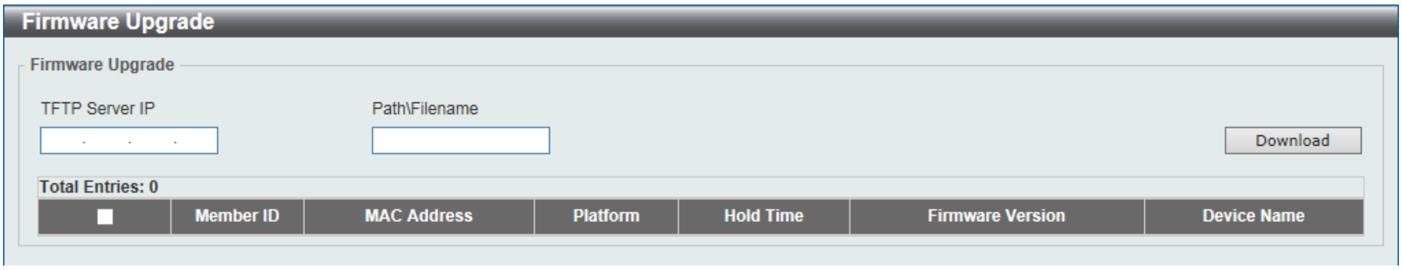
Single IP Management
Copyright© 2023 D-Link Corporation.
Release Date: 2023/3/26

Figure 4-97 About Window

Firmware Upgrade

This window is used to view and upgrade firmware from the Commander Switch to the Member Switch. Member Switches will be listed in the table.

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



Firmware Upgrade

Firmware Upgrade

TFTP Server IP: . . .

Path\Filename:

Download

Total Entries: 0

□	Member ID	MAC Address	Platform	Hold Time	Firmware Version	Device Name

Figure 4-98 Firmware Upgrade Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server IP address.
Path \ Filename	Enter the path and file name.

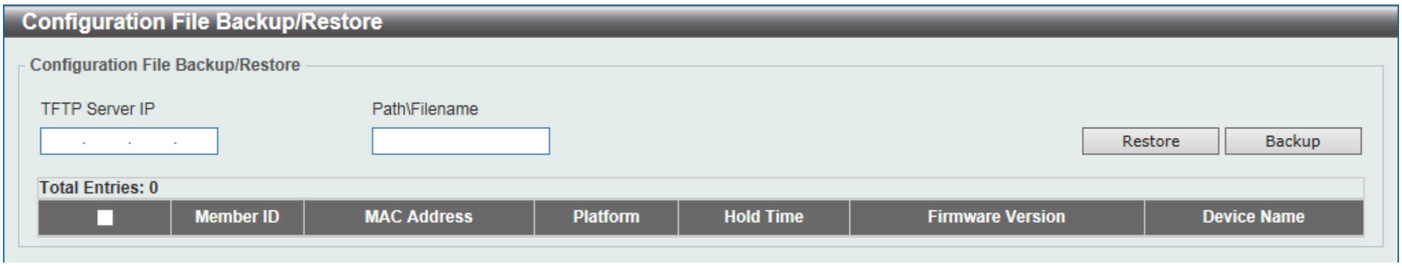
Click the **Download** button to update the firmware.

To specify a certain Switch for firmware download, tick its corresponding check box.

Configuration File Backup/Restore

This window is used to view and upgrade configuration files from the Commander Switch to the Member Switch using a TFTP server. Member Switches will be listed in the table.

To view the following window, click **Management > Virtual Stacking (SIM) > Configuration File Backup/Restore**, as shown below:



Configuration File Backup/Restore

Configuration File Backup/Restore

TFTP Server IP: . . .

Path\Filename:

Restore Backup

Total Entries: 0

□	Member ID	MAC Address	Platform	Hold Time	Firmware Version	Device Name

Figure 4-99 Configuration File Backup/Restore Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server IP address.
Path \ Filename	Enter the path and file name.

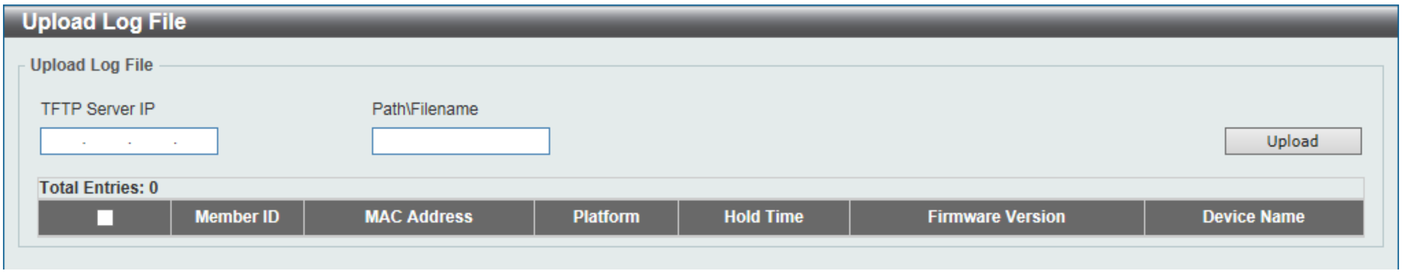
Click the **Restore** button to update the configuration from a TFTP server to the member Switch.

Click the **Backup** button to back up the configuration file to a TFTP server.

Upload Log File

This window is used to view and upload log files from SIM member Switches to a specified PC.

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



Upload Log File

Upload Log File

TFTP Server IP: . . .

Path\Filename:

Total Entries: 0

□	Member ID	MAC Address	Platform	Hold Time	Firmware Version	Device Name

Figure 4-100 Upload Log File Window

The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server IP address.
Path \ Filename	Enter the path and file name.

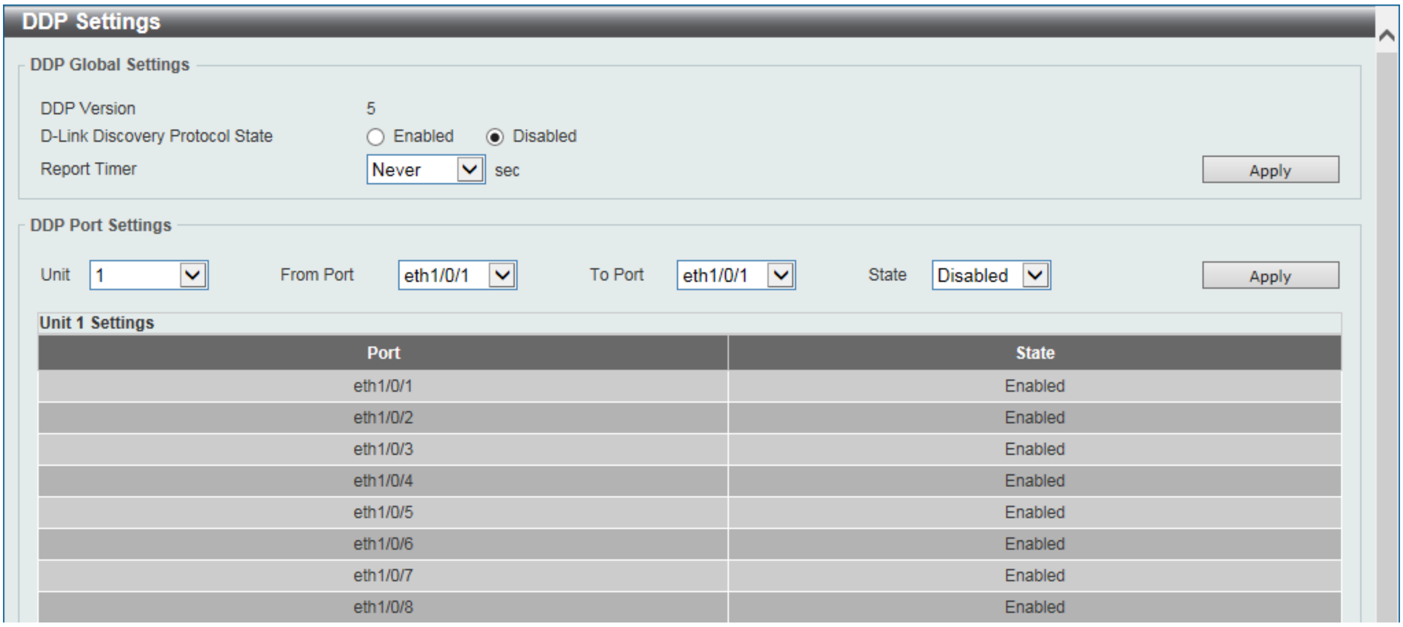
Click the **Upload** button to initiate the file transfer.

D-Link Discovery Protocol

DDP Settings

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 > DDP Settings**, as shown below:



DDP Settings

DDP Global Settings

DDP Version: 5

D-Link Discovery Protocol State: ○ Enabled ● Disabled

Report Timer: Never sec

DDP Port Settings

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

Unit 1 Settings

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

Figure 4-101 DDP Settings Window

The fields that can be configured in **DDP Global Settings** 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:

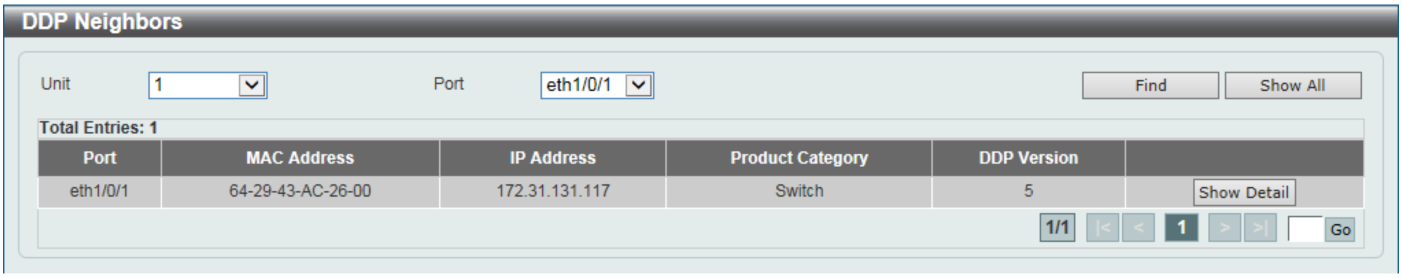
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
State	Select to enable or disable the DDP feature.

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

DDP Neighbors

This window is used to display the DDP neighbors.

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



DDP Neighbors

Unit: 1 Port: eth1/0/1

Total Entries: 1

Port	MAC Address	IP Address	Product Category	DDP Version	
eth1/0/1	64-29-43-AC-26-00	172.31.131.117	Switch	5	Show Detail

Figure 4-102 DDP Neighbors Window

The fields that can be configured are described below:

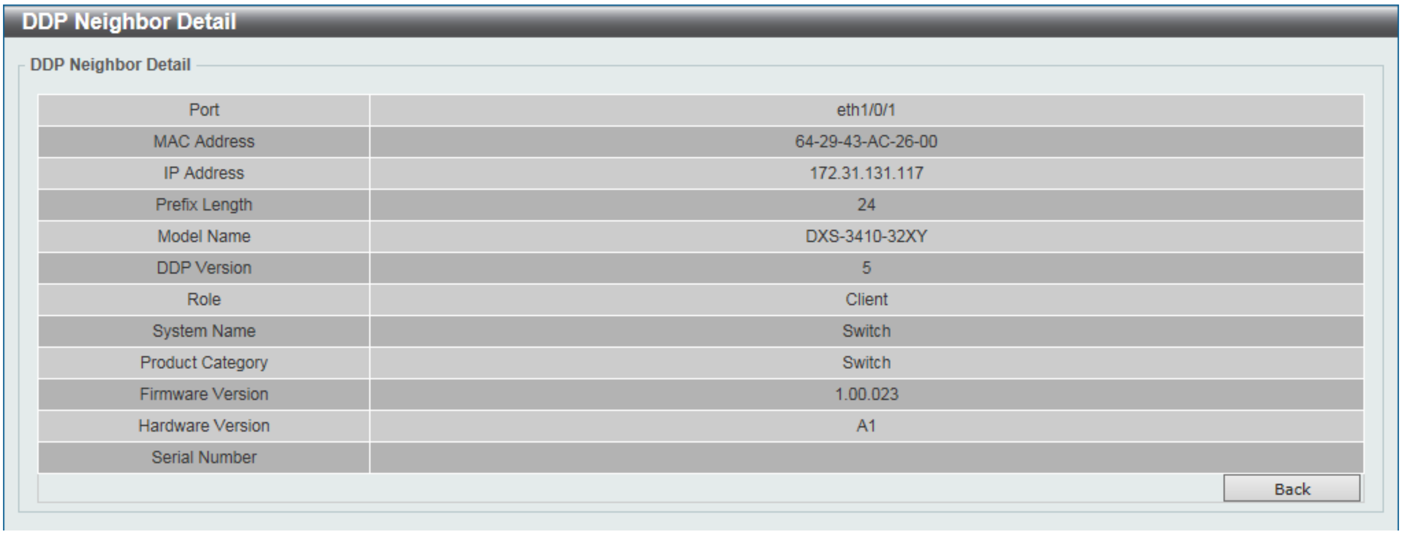
Parameter	Description
Unit	Select the Switch unit that will be used here.
Port	Select the port that will be used here.

Click the **Find** button to display the DDP neighbors connecting through the specified port.

Click the **Show All** button to display all DDP neighbors connecting to and through the Switch.

Click the **Show Detail** button to view detailed information associated with the entry.

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



DDP Neighbor Detail

DDP Neighbor Detail

Port	eth1/0/1
MAC Address	64-29-43-AC-26-00
IP Address	172.31.131.117
Prefix Length	24
Model Name	DXS-3410-32XY
DDP Version	5
Role	Client
System Name	Switch
Product Category	Switch
Firmware Version	1.00.023
Hardware Version	A1
Serial Number	

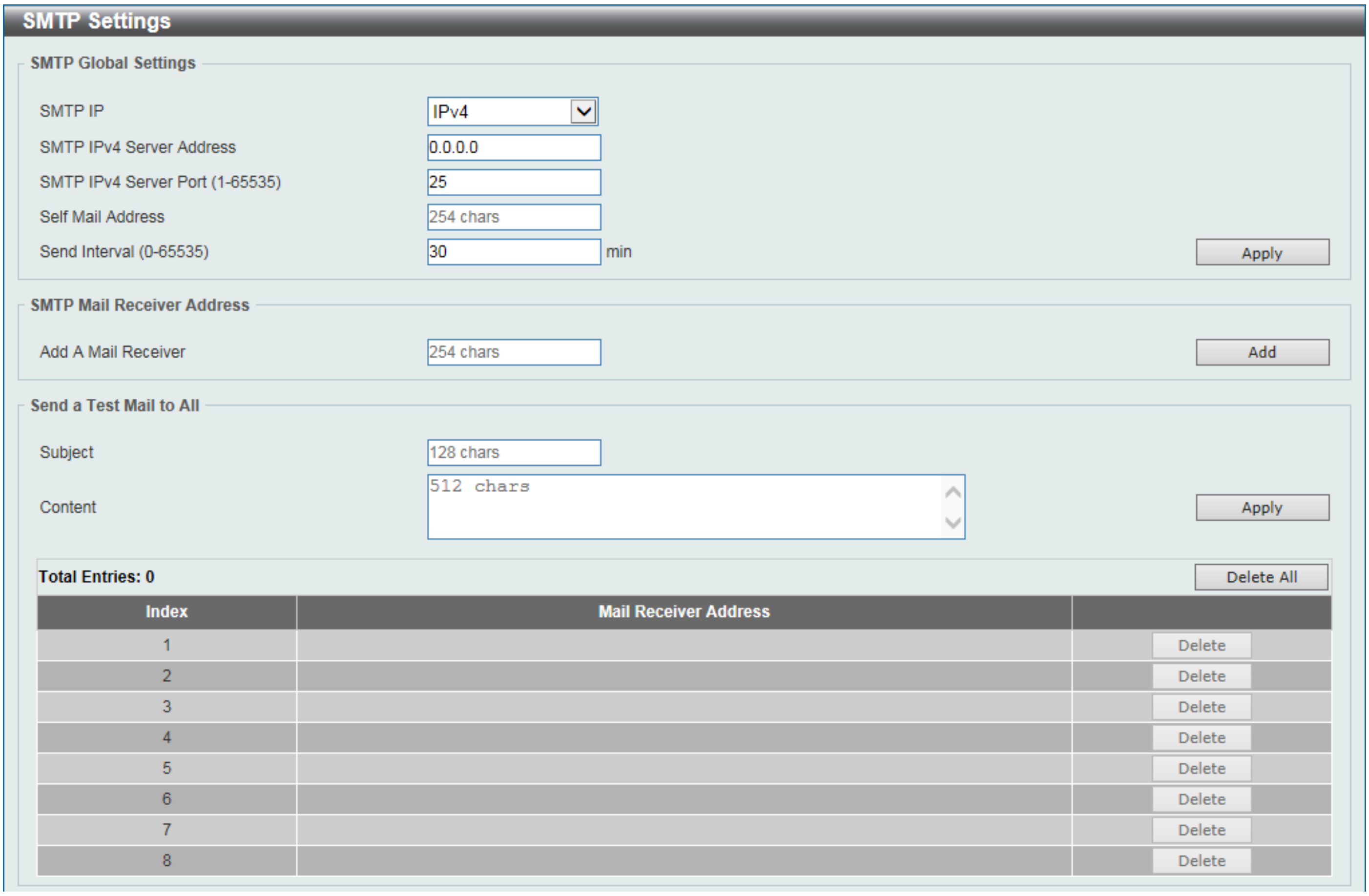
Figure 4-103 DDP Neighbors Detail Window

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

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:



SMTP Settings

SMTP Global Settings

SMTP IP: IPv4

SMTP IPv4 Server Address: 0.0.0.0

SMTP IPv4 Server Port (1-65535): 25

Self Mail Address: 254 chars

Send Interval (0-65535): 30 min

SMTP Mail Receiver Address

Add A Mail Receiver: 254 chars

Send a Test Mail to All

Subject: 128 chars

Content: 512 chars

Total Entries: 0

Index	Mail Receiver Address	
1		Delete
2		Delete
3		Delete
4		Delete
5		Delete
6		Delete
7		Delete
8		Delete

Figure 4-104 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.
SMTP IPv6 Server Address	After selecting **IPv6** as the SMTP IP type, enter the SMTP server IPv6 address here.
SMTP IPv4 Server Port	After selecting **IPv4** as the SMTP IP type, enter the SMTP server port number here. The range is from 1 to 65535. By default, this value is 25.
SMTP IPv6 Server Port	After selecting **IPv6** as the SMTP IP type, enter the SMTP server port number here. The range is from 1 to 65535. By default, this value is 25.
Self Mail Address	Enter the email address that represents the Switch here. This string can be up to 254 characters long.
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.

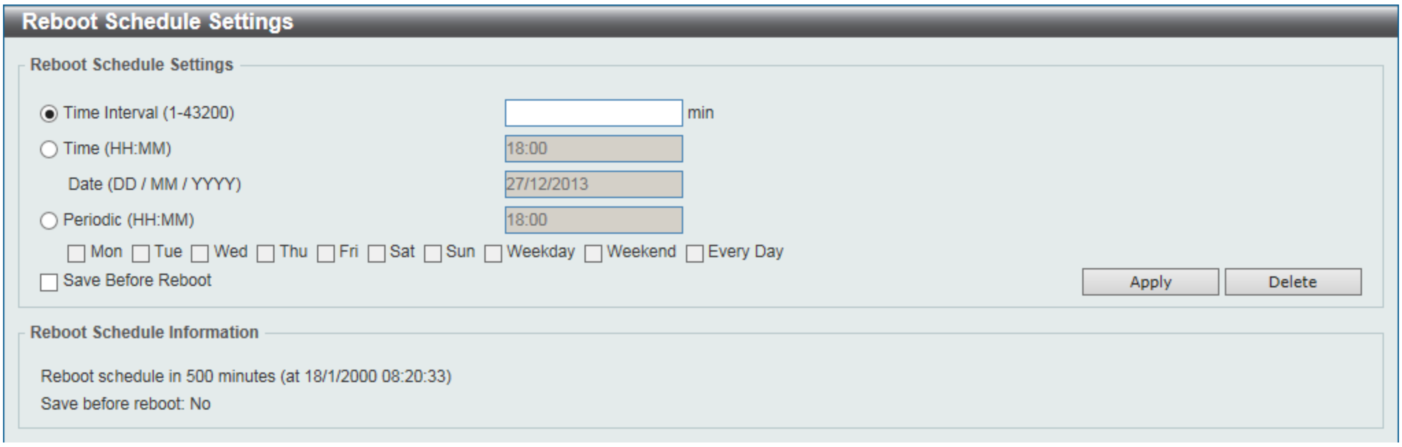
Click the **Delete All** button to delete all the entries found in the display table.

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

Reboot Schedule Settings

This window is used to display and configure the reboot schedule settings.

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



Reboot Schedule Settings

Reboot Schedule Settings

● Time Interval (1-43200) ____ min

○ Time (HH:MM) 18:00

Date (DD / MM / YYYY) 27/12/2013

○ Periodic (HH:MM) 18:00

□ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun □ Weekday □ Weekend □ Every Day

□ Save Before Reboot

Reboot Schedule Information

Reboot schedule in 500 minutes (at 18/1/2000 08:20:33)

Save before reboot: No

Figure 4-105 Reboot Schedule Settings Window

The fields that can be configured are described below:

Parameter	Description
Time Interval	Select and enter the time in minutes to initiate a reboot after the specified time period. The range is from 1 to 43200 minutes.
Time	Select and enter the time (HH:MM) at which the Switch should initiate the reboot. • **Date -** Enter the date (DD/MM/YYYY) at which the Switch should initiate the reboot. When the date is not specified, the Switch will initiate the reboot at the specified time on the current day if the specified time is later than the current time, or on the next day if the specified time is earlier than the current time.
Periodic	Select and enter the time (HH:MM) to reboot the Switch periodically. Select the days for the reboot to repeat.
Save Before Reboot	Select to save all configurations before the reboot.

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

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

NLB FDB Settings

This window is used to display and configure the Network Load Balancing (NLB) FDB settings. The NLB function is used to support the Microsoft server load balancing application where multiple servers can share the same IP address and MAC address. The requests from clients will be forwarded to all the servers, but will only be processed by one of them. The server can work in two different modes:

- **Unicast mode:** The client uses a unicast MAC address as the destination MAC address to reach the server.
- **Multicast mode:** The client uses a multicast MAC address as the destination MAC address to reach the server.

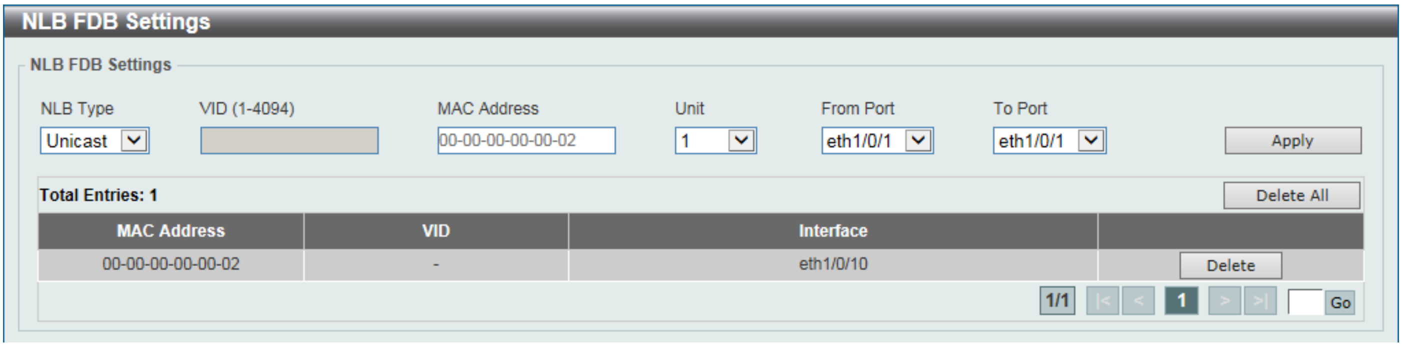
This destination MAC address is called the shared MAC address. However, the server uses its own MAC address (rather than the shared MAC address) as the source MAC address in the reply packet. In other words, a NLB unicast address is usually not the source MAC address of a packet.

When the received packet contains a destination MAC address that matches the configured unicast MAC address, it will be forwarded to those configured ports, regardless of the VLAN membership configuration.

Administrators cannot configure a static address of the MAC address table as a NLB address. However, if a MAC address is created as a NLB MAC address entry, the same MAC address can be still dynamically learnt in the Layer 2 MAC address table. In this situation, the NLB has higher priority; the dynamically learnt FDB entry won't take effect.

NOTE: Link Aggregation cannot be configured across multiple Switch units in the stack when the NLB feature is enabled.

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



NLB FDB Settings

NLB FDB Settings

NLB Type: Unicast
VID (1-4094):
MAC Address: 00-00-00-00-00-02
Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1

Total Entries: 1

MAC Address	VID	Interface	
00-00-00-00-00-02	-	eth1/0/10	Delete

Figure 4-106 NLB FDB Settings Window

The fields that can be configured are described below:

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

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

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

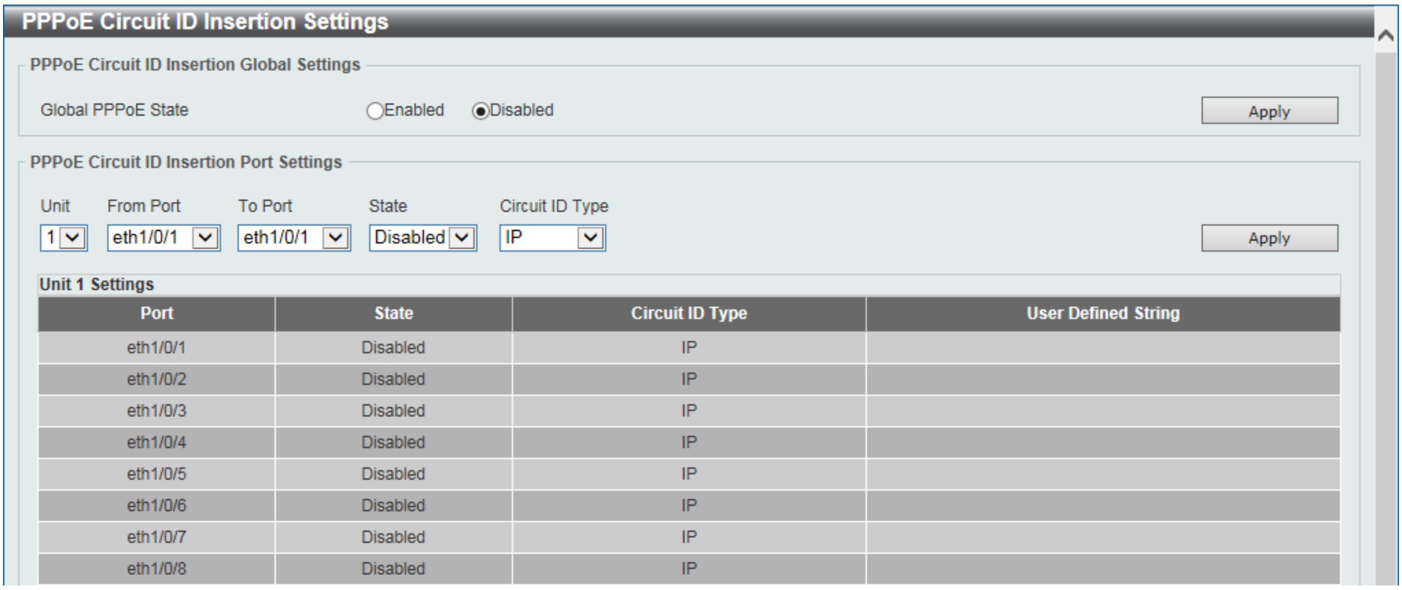
Click the **Delete** button to delete the specified entry.

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

PPPoE Circuit ID Insertion Settings

This window is used to configure the PPPoE circuit ID insertion function.

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



PPPoE Circuit ID Insertion Settings

PPPoE Circuit ID Insertion Global Settings

Global PPPoE State ○Enabled ●Disabled

PPPoE Circuit ID Insertion Port Settings

Unit	From Port	To Port	State	Circuit ID Type
1	eth1/0/1	eth1/0/1	Disabled	IP

Unit 1 Settings

Port	State	Circuit ID Type	User Defined String
eth1/0/1	Disabled	IP	
eth1/0/2	Disabled	IP	
eth1/0/3	Disabled	IP	
eth1/0/4	Disabled	IP	
eth1/0/5	Disabled	IP	
eth1/0/6	Disabled	IP	
eth1/0/7	Disabled	IP	
eth1/0/8	Disabled	IP	

Figure 4-107 PPPoE Circuit ID Insertion Settings Window

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

Parameter	Description
Global PPPoE State	Click to enable or disable the 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 Ports Settings** are described below:

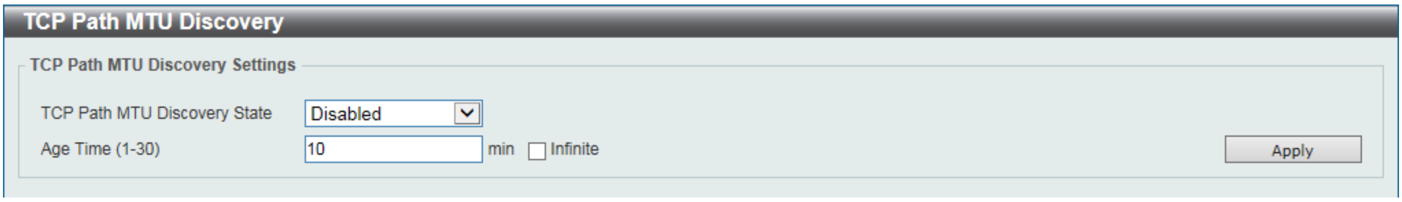
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
State	Select to enable or disable the PPPoE circuit ID insertion on the specified port(s).
Circuit ID Type	Select the device ID part for encoding of the circuit ID option. Options to choose from are **IP**, **MAC**, **UDF**, and **Vendor5**.

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

TCP Path MTU Discovery

This window is used to configure the conversion of IP TCP path Maximum Transmission Unit (MTU).

To view this window, click **Management > TCP Path MTU Discovery** as shown below:



TCP Path MTU Discovery

TCP Path MTU Discovery Settings

TCP Path MTU Discovery State: Disabled

Age Time (1-30): 10 min □ Infinite

Figure 4-108 TCP Path MTU Discovery Window

The fields that can be configured are described below:

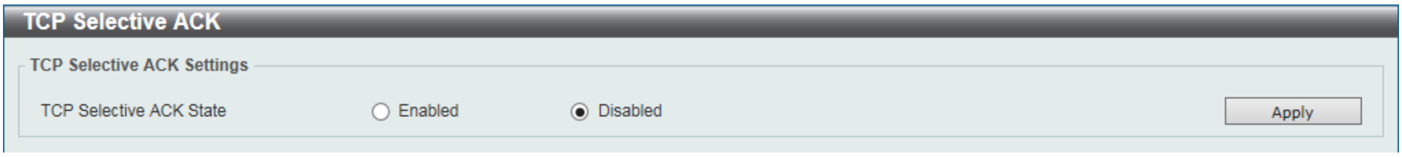
Parameter	Description
TCP Path MTU Discovery State	Click to enable or disable the conversion of TCP path MTU.
Age Time	Enter the age time in minutes here. The range is from 1 to 30. By default, this value is 10. Select the **Infinite** option to disable this feature.

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

TCP Selective ACK

This window is used to configure the TCP selective ACK state.

To view this window, click **Management > TCP Selective ACK** as shown below:



TCP Selective ACK

TCP Selective ACK Settings

TCP Selective ACK State ○ Enabled ● Disabled

Figure 4-109 TCP Selective ACK Window

The fields that can be configured are described below:

Parameter	Description
TCP Selective ACK State	Click to enable or disable the TCP selective ACK.

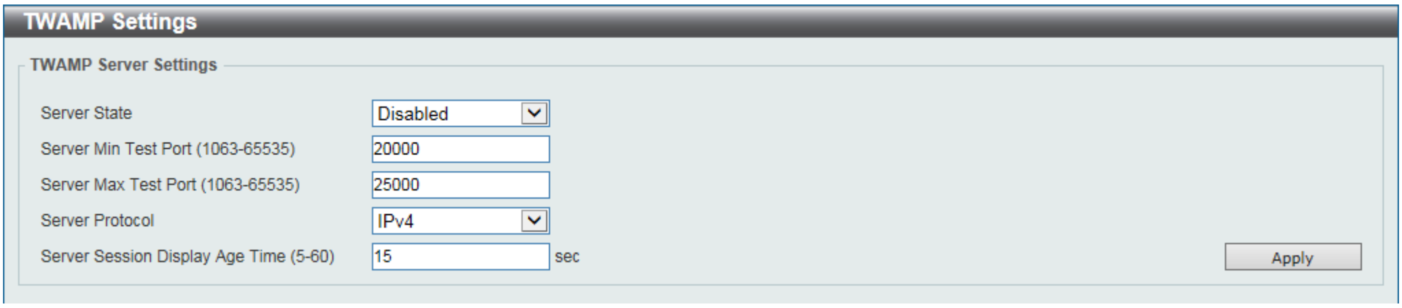
Click the **Apply** button to accept the changes made.

TWAMP

TWAMP Settings

This window is used to display and configure the Two-Way Active Measurement Protocol (TWAMP) settings.

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



TWAMP Settings

TWAMP Server Settings

Server State: Disabled

Server Min Test Port (1063-65535): 20000

Server Max Test Port (1063-65535): 25000

Server Protocol: IPv4

Server Session Display Age Time (5-60): 15 sec

Figure 4-110 TWAMP Settings Window

The fields that can be configured are described below:

Parameter	Description
Server State	Select to enable or disable the TWAMP server here.

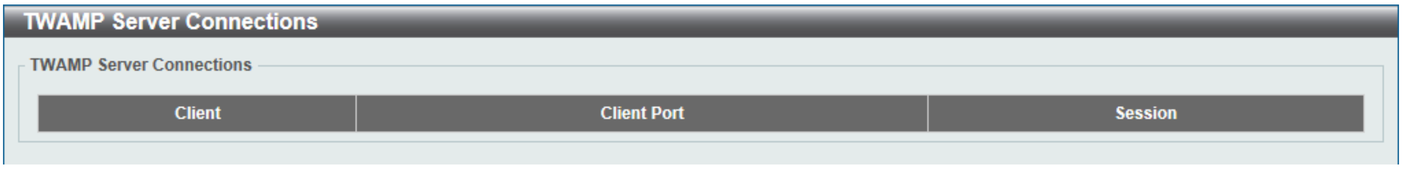
Parameter	Description
Server Min Test Port	Enter the minimum test port number. The range is from 1063 to 65535. The default value is 20000.
Server Max Test Port	Enter the maximum test port number. The range is from 1063 to 65535. The default value is 25000.
Server Protocol	Select the TWAMP server protocol type. Options to choose from are **IPv4** and **IPv6**.
Server Session Display Age Time	Enter the TWAMP client session display age time. The range is from 5 to 60 seconds. The default value is 15 seconds.

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

TWAMP Server Connections

This window is used to display the TWAMP server connections.

To view the following window, click **Management > TWAMP > TWAMP Server Connections**, as shown below:



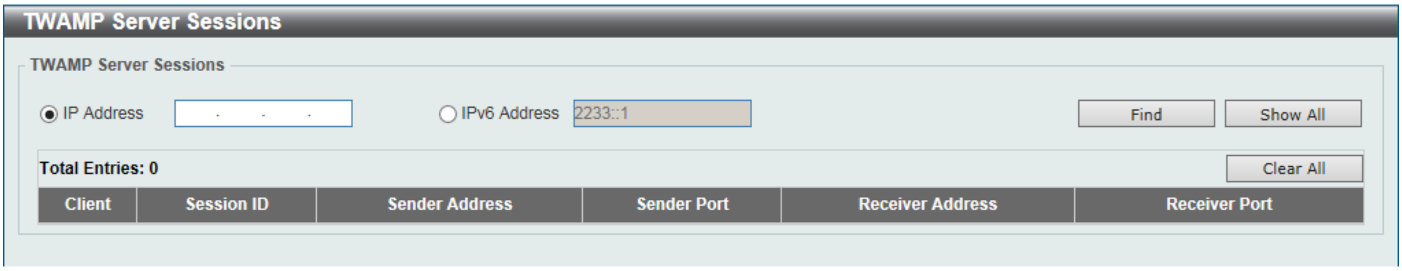
Client	Client Port	Session

Figure 4-111 TWAMP Server Connections Window

TWAMP Server Sessions

This window is used to display the TWAMP server sessions.

To view the following window, click **Management > TWAMP > TWAMP Server Sessions**, as shown below:



IPv6 Address: 2233::1

Total Entries: 0

Client	Session ID	Sender Address	Sender Port	Receiver Address	Receiver Port

Figure 4-112 TWAMP Server Sessions Window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the IPv4 address of the destination host here.
IPv6 Address	Enter the IPv6 address of the destination host here.

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 **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.

5. Layer 2 Features

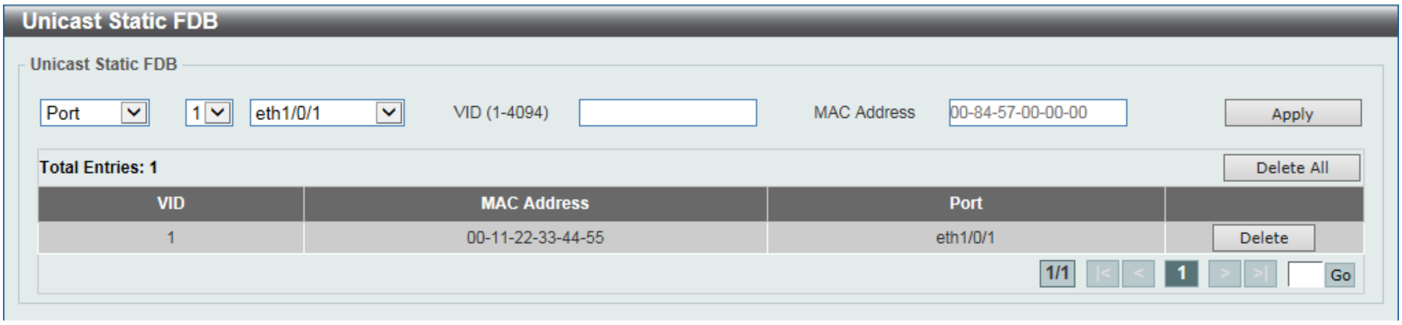
FDB

Static FDB

Unicast Static FDB

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

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



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

Total Entries: 1

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

Figure 5-1 Unicast Static FDB Window

The fields that can be configured are described below:

Parameter	Description
Port/Drop	Allows the selection of the port number on which the MAC address entered resides. This option could also drop the MAC address from the unicast static FDB. Select the port number when selecting the **Port**.
Unit	Select the stacking unit ID of the Switch that will be configured here.
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.

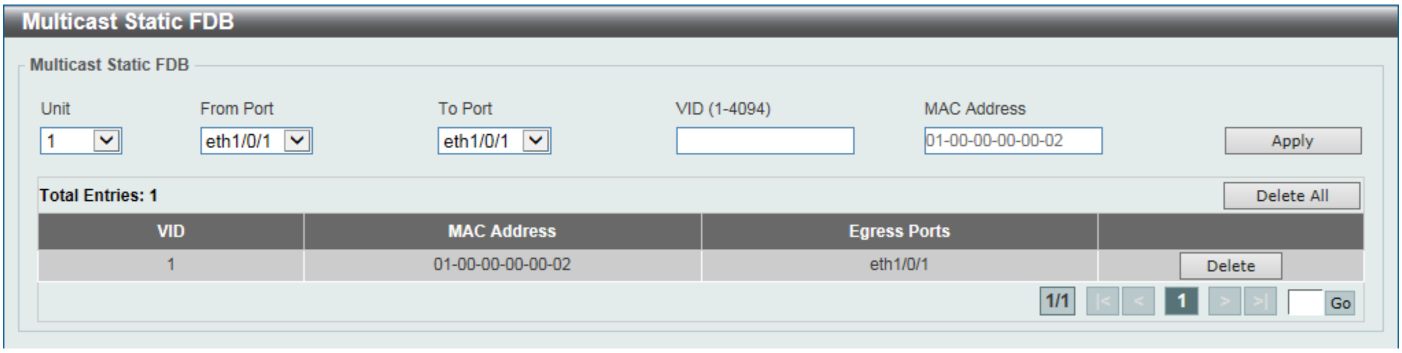
Click the **Delete** button to delete the specified entry.

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:



Multicast Static FDB

Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1
VID (1-4094):
MAC Address: 01-00-00-00-00-02

Total Entries: 1

VID	MAC Address	Egress Ports	
1	01-00-00-00-00-02	eth1/0/1	Delete

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.
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.

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

Click the **Delete All** button to remove all the entries.

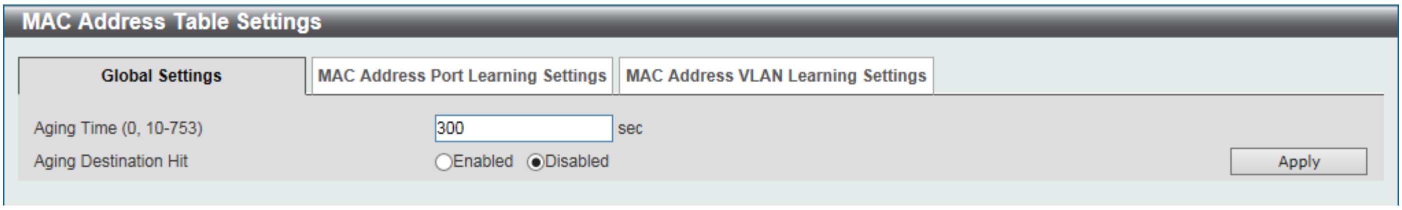
Click the **Delete** button to remove the specific entry.

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:



MAC Address Table Settings

Aging Time (0, 10-753): 300 sec
Aging Destination Hit: ○Enabled ●Disabled

Global Settings
MAC Address Port Learning Settings
MAC Address VLAN Learning Settings
Apply

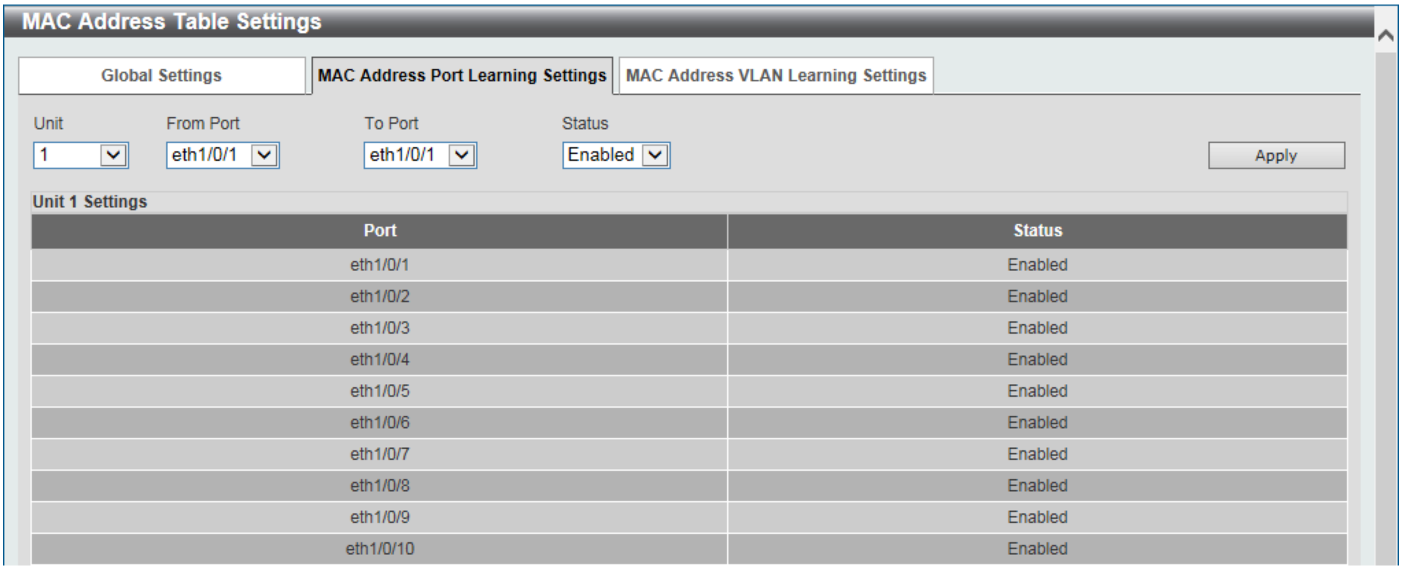
Figure 5-3 MAC Address Table Settings (Global Settings) Window

The fields that can be configured are described below:

Parameter	Description
Aging Time	Enter the MAC address table aging time here. The value is 0, and from 10 to 753 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.


MAC Address Table Settings
Global Settings
MAC Address Port Learning Settings
MAC Address VLAN Learning Settings
Apply

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

Unit 1 Settings

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

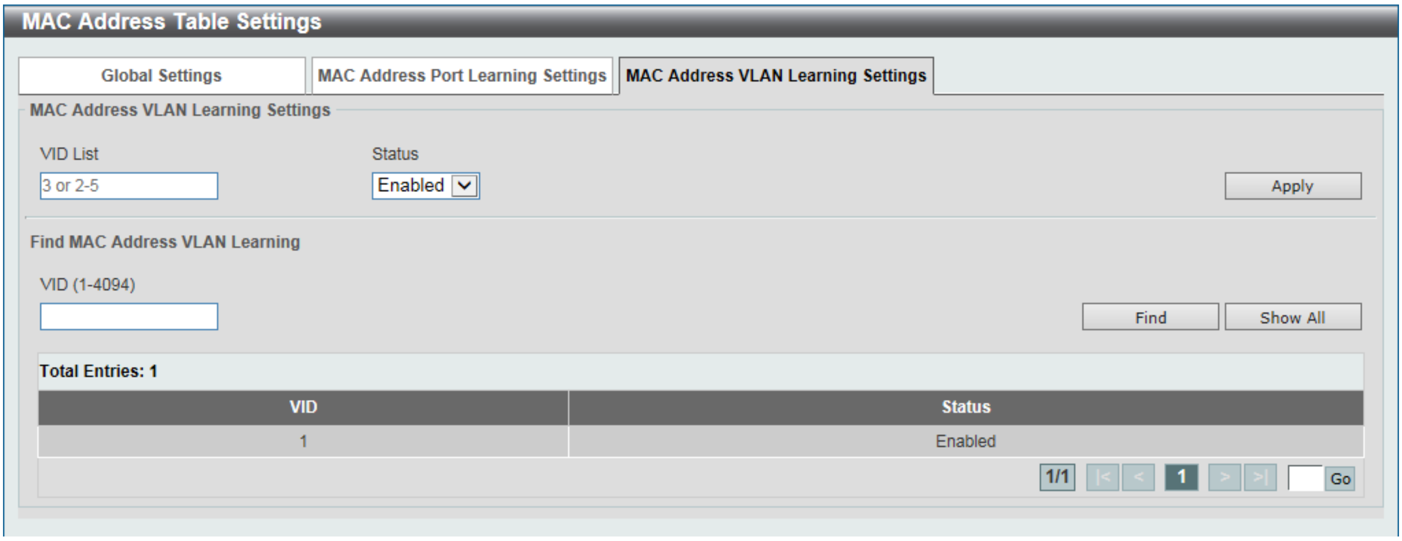
Figure 5-4 MAC Address Table Settings (MAC Address Port Learning Settings) Window

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.
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.


MAC Address Table Settings
Global Settings
MAC Address Port Learning Settings
MAC Address VLAN Learning Settings
Apply
Find
Show All
1/1
1
Go

MAC Address VLAN Learning Settings

VID List: 3 or 2-5
Status: Enabled

Find MAC Address VLAN Learning

VID (1-4094):

Total Entries: 1

VID	Status
1	Enabled

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 separated by commas or a range of VLAN IDs can be entered 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 entered.

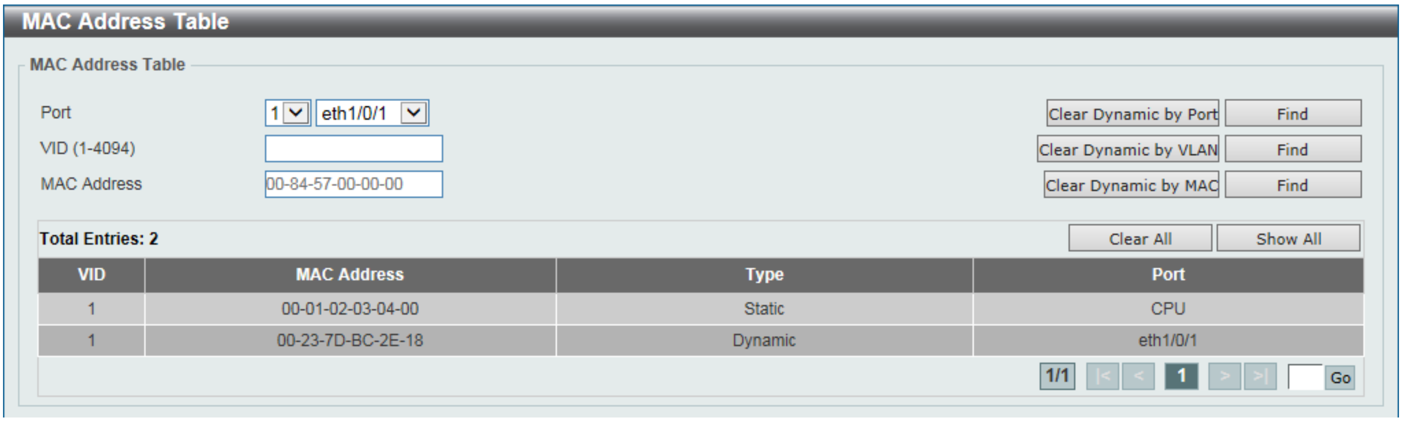
Click the **Show All** button to display all the available entries.

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:



MAC Address Table

MAC Address Table

Port: 1, eth1/0/1

VID (1-4094):

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

Total Entries: 2

VID	MAC Address	Type	Port
1	00-01-02-03-04-00	Static	CPU
1	00-23-7D-BC-2E-18	Dynamic	eth1/0/1

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.
VID	Enter the VLAN ID that will be used for this configuration here.
MAC Address	Enter the MAC address that will be used for this configuration here.

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

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

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

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

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

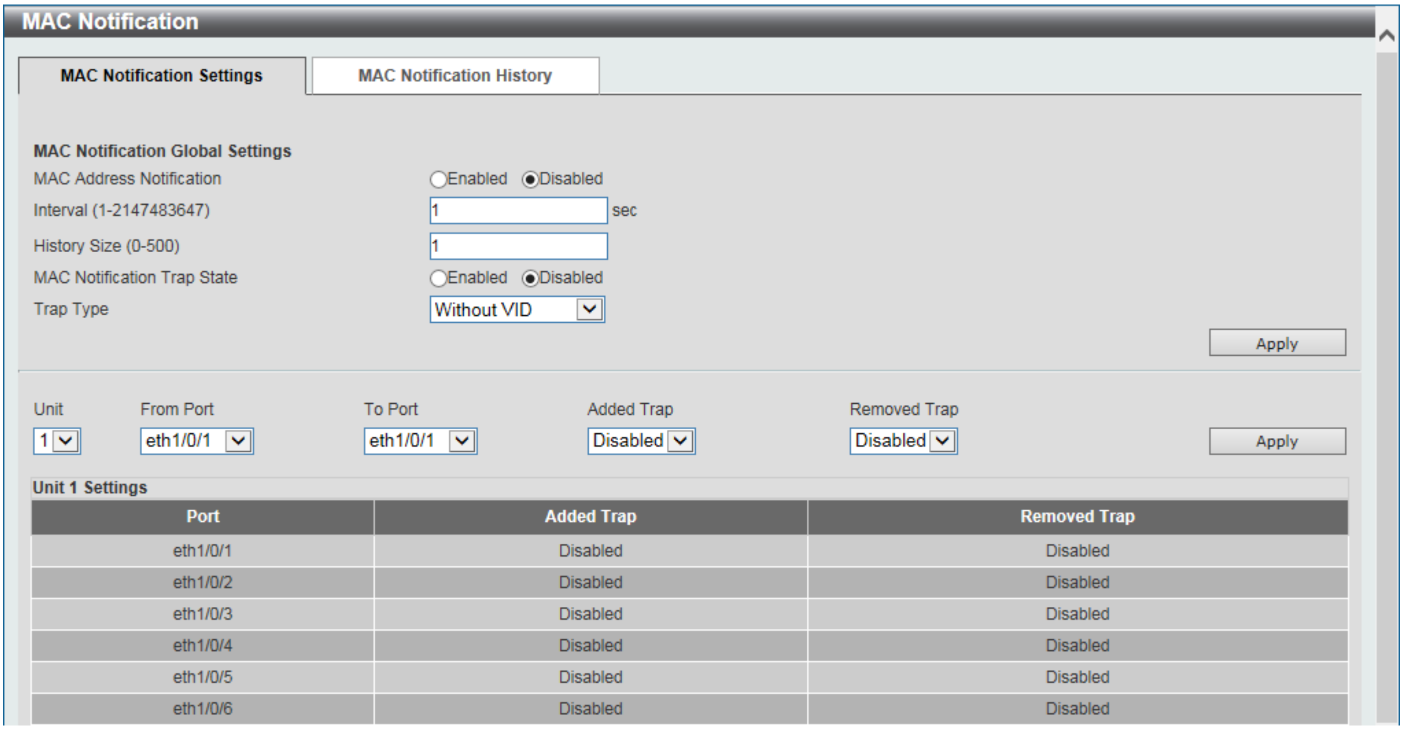
Click the **Show All** button to display all the MAC addresses recorded in the MAC address table.

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

MAC Notification

This window is used to display and configure MAC notification.

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



MAC Notification Global Settings

MAC Address Notification ○Enabled ●Disabled

Interval (1-2147483647) 1 sec

History Size (0-500) 1

MAC Notification Trap State ○Enabled ●Disabled

Trap Type Without VID

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

Unit 1 Settings

Port	Added Trap	Removed Trap
eth1/0/1	Disabled	Disabled
eth1/0/2	Disabled	Disabled
eth1/0/3	Disabled	Disabled
eth1/0/4	Disabled	Disabled
eth1/0/5	Disabled	Disabled
eth1/0/6	Disabled	Disabled

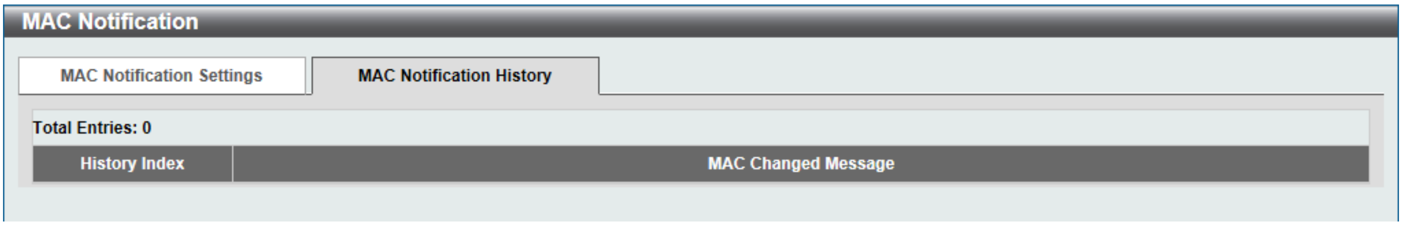
Figure 5-7 MAC Notification (MAC Notification Settings) Window

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. The range is from 1 to 2147483647 seconds. By default, this value is 1 second.
History Size	Enter the maximum number of entries listed in the history log used for notification. The range is from 0 to 500. By default, this value is 1.
MAC Notification Trap State	Select to enable or disable the MAC notification trap state.
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.
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.
Removed Trap	Select to enable or disable the removed trap.

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

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


MAC Notification

MAC Notification Settings | MAC Notification History

Total Entries: 0

History Index	MAC Changed Message

Figure 5-8 MAC Notification (MAC Notification History) Window

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

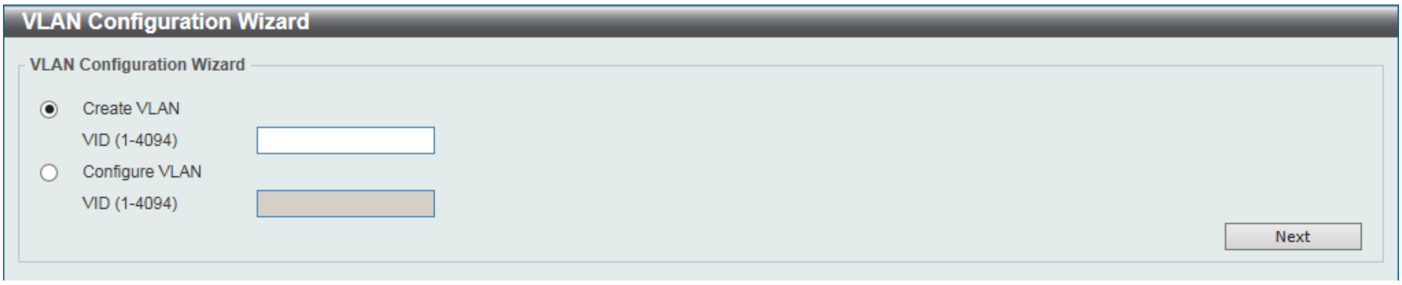
VLAN

VLAN Configuration Wizard

This window is used to start the VLAN configuration wizard.

Create/Configure VLAN

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


VLAN Configuration Wizard

VLAN Configuration Wizard

● Create VLAN

VID (1-4094)

○ Configure VLAN

VID (1-4094)

Figure 5-9 VLAN Configuration Wizard (Step 1) Window

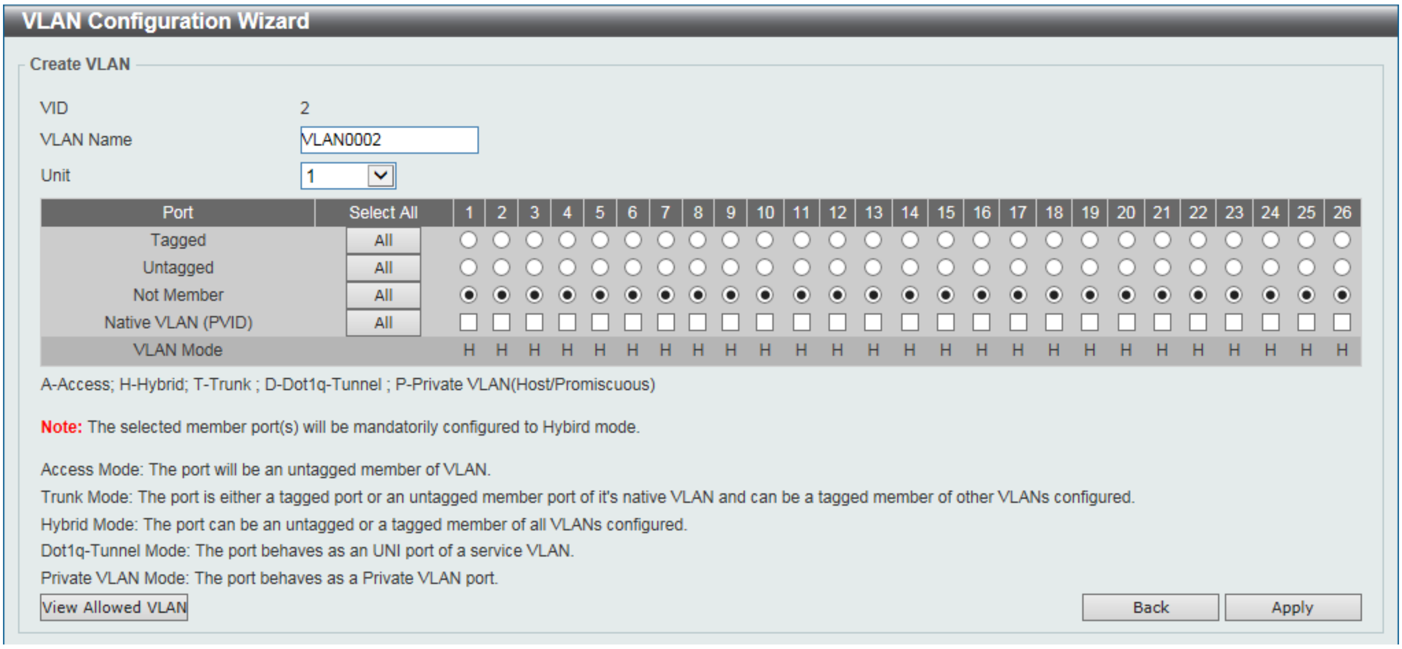
The fields that can be configured are described below:

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

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

Create VLAN

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



VID 2

VLAN Name VLAN0002

Unit 1

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

A-Access; H-Hybrid; T-Trunk ; D-Dot1q-Tunnel ; P-Private VLAN(Host/Promiscuous)

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

Access Mode: The port will be an untagged member of VLAN.
Trunk Mode: The port is either a tagged port or an untagged member port of it's native VLAN and can be a tagged member of other VLANs configured.
Hybrid Mode: The port can be an untagged or a tagged member of all VLANs configured.
Dot1q-Tunnel Mode: The port behaves as an UNI port of a service VLAN.
Private VLAN Mode: The port behaves as a Private VLAN port.

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

The fields that can be configured are described below:

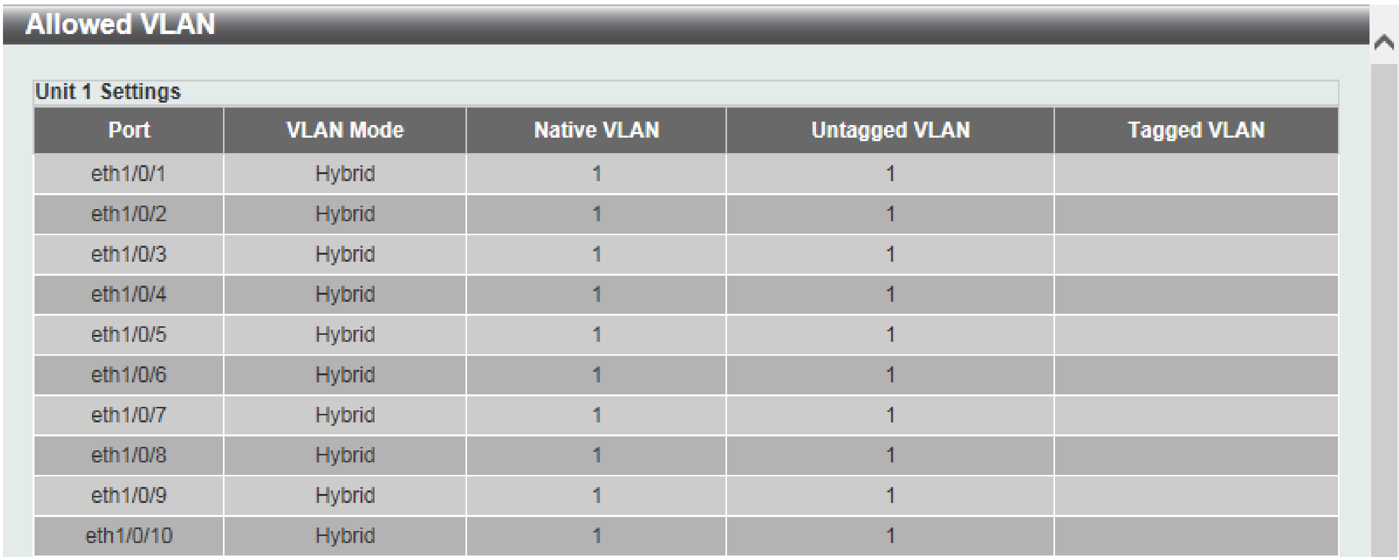
Parameter	Description
VLAN Name	Enter the name for the VLAN here.
Unit	Select the Switch unit that will be used for this configuration here.
Tagged	Select the switch ports that are tagged members of this VLAN here.
Untagged	Select the switch ports that are untagged members of this VLAN here.
Not Member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

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

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

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

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



Allowed VLAN

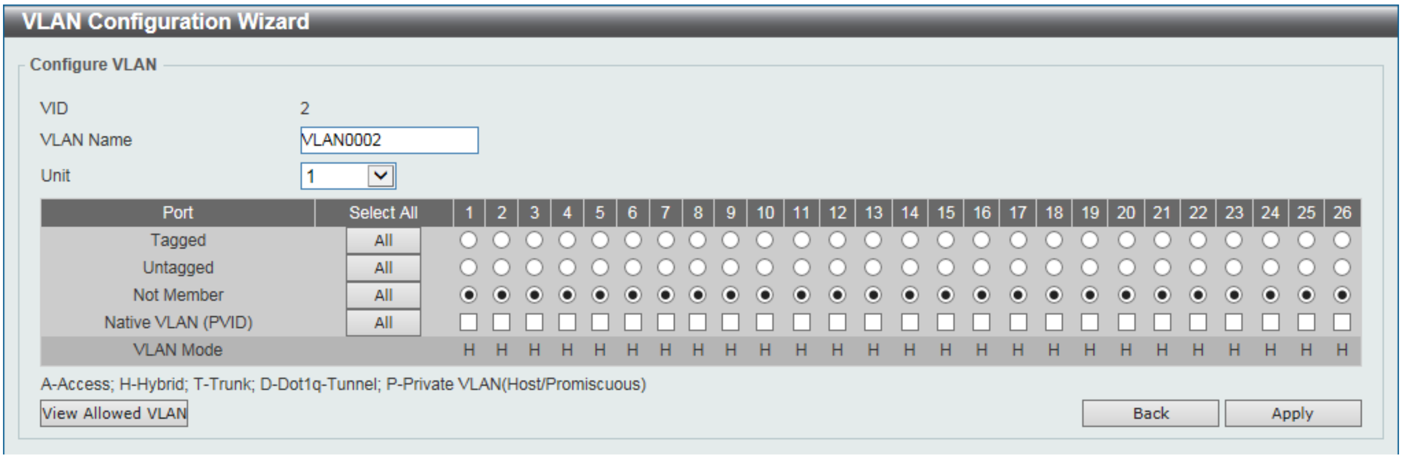
Unit 1 Settings

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

Figure 5-11 Allowed VLAN Window

Configure VLAN

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



VLAN Configuration Wizard

Configure VLAN

VID: 2

VLAN Name: VLAN0002

Unit: 1

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

A-Access; H-Hybrid; T-Trunk; D-Dot1q-Tunnel; P-Private VLAN(Host/Promiscuous)

Figure 5-12 VLAN Configuration Wizard (Configure VLAN) Window

The fields that can be configured are described below:

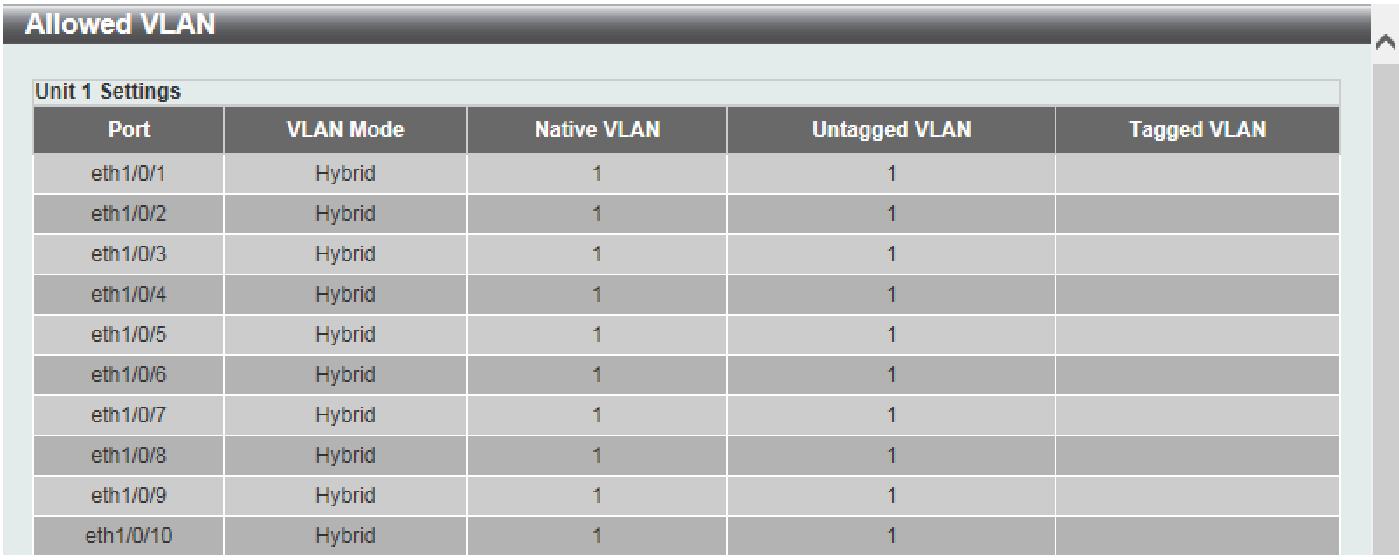
Parameter	Description
VLAN Name	Enter the name for the VLAN here.
Unit	Select the Switch unit that will be used for this configuration here.
Tagged	Select the switch ports that are tagged members of this VLAN here.
Untagged	Select the switch ports that are untagged members of this VLAN here.
Not Member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

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

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

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

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



Allowed VLAN

Unit 1 Settings

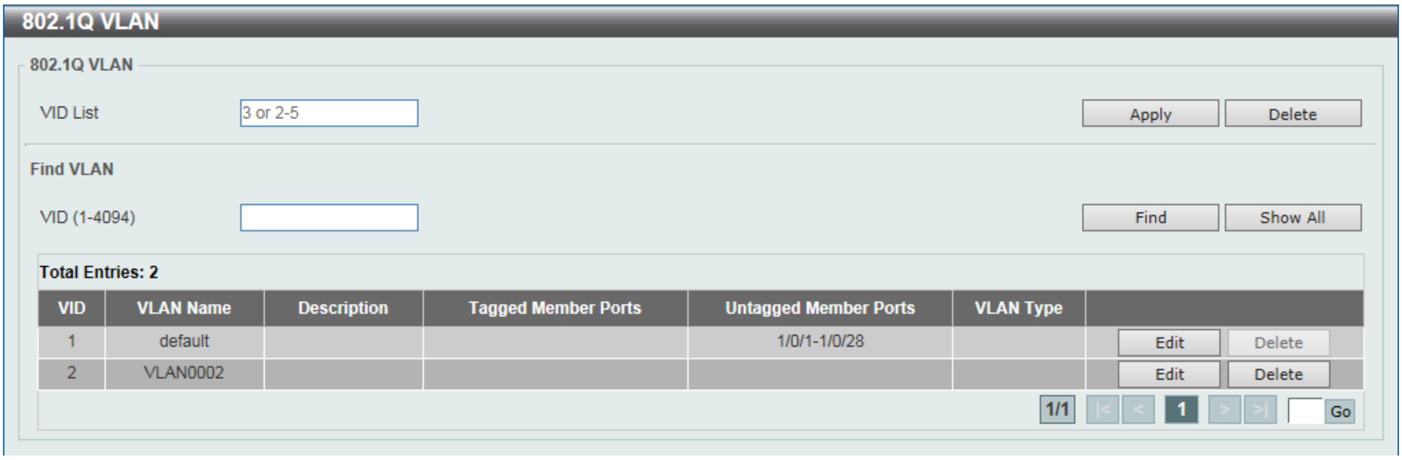
Port	VLAN Mode	Native VLAN	Untagged VLAN	Tagged VLAN
eth1/0/1	Hybrid	1	1	
eth1/0/2	Hybrid	1	1	
eth1/0/3	Hybrid	1	1	
eth1/0/4	Hybrid	1	1	
eth1/0/5	Hybrid	1	1	
eth1/0/6	Hybrid	1	1	
eth1/0/7	Hybrid	1	1	
eth1/0/8	Hybrid	1	1	
eth1/0/9	Hybrid	1	1	
eth1/0/10	Hybrid	1	1	

Figure 5-13 Allowed VLAN Window

802.1Q VLAN

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

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



802.1Q VLAN

802.1Q VLAN

VID List: 3 or 2-5

Find VLAN

VID (1-4094):

Total Entries: 2

VID	VLAN Name	Description	Tagged Member Ports	Untagged Member Ports	VLAN Type	
1	default			1/0/1-1/0/28		Edit Delete
2	VLAN0002					Edit Delete

Figure 5-14 802.1Q VLAN Window

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

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

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

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

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

Parameter	Description
VID	Enter the VLAN ID that will be displayed here.
VLAN Name	After clicking the **Edit** button, enter the name of the VLAN here.

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

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

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

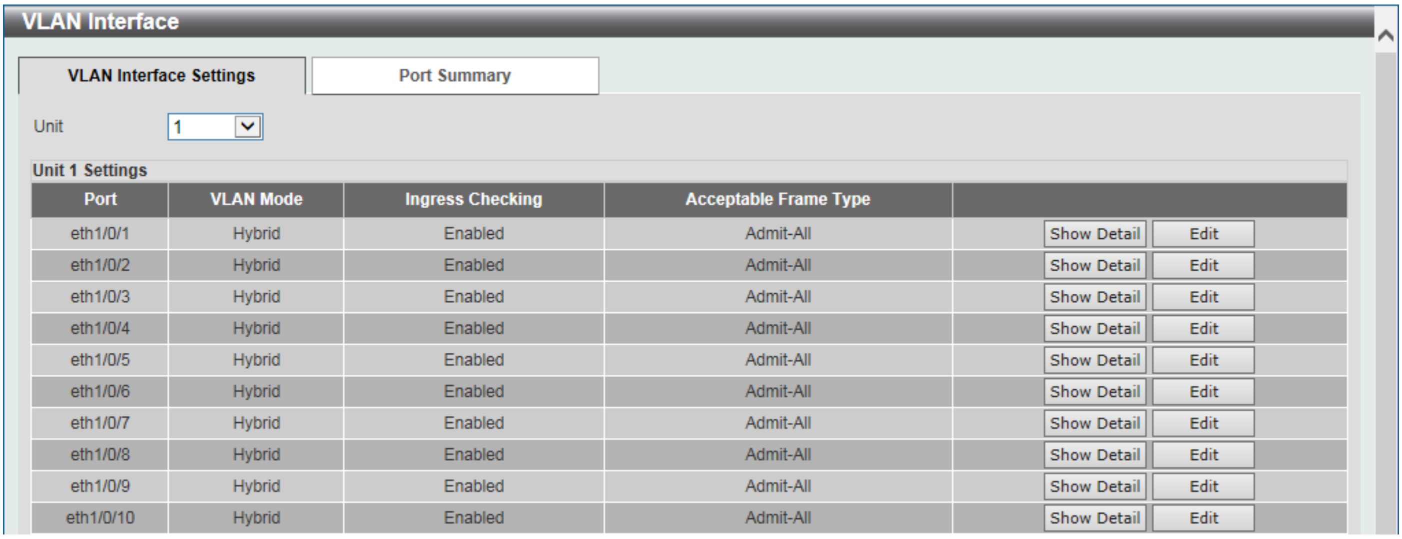
Click the **Delete** button to remove the specific entry.

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

VLAN Interface

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

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



VLAN Interface

VLAN Interface Settings | Port Summary

Unit: 1

Unit 1 Settings

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

Figure 5-15 VLAN Interface Settings Window

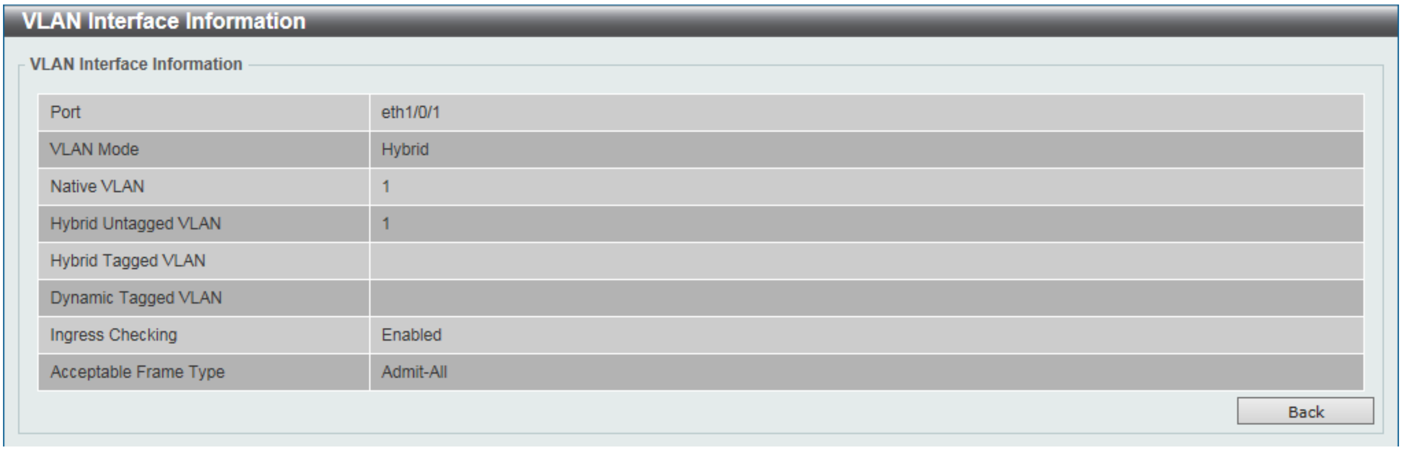
The fields that can be configured are described below:

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

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

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

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



VLAN Interface Information

VLAN Interface Information

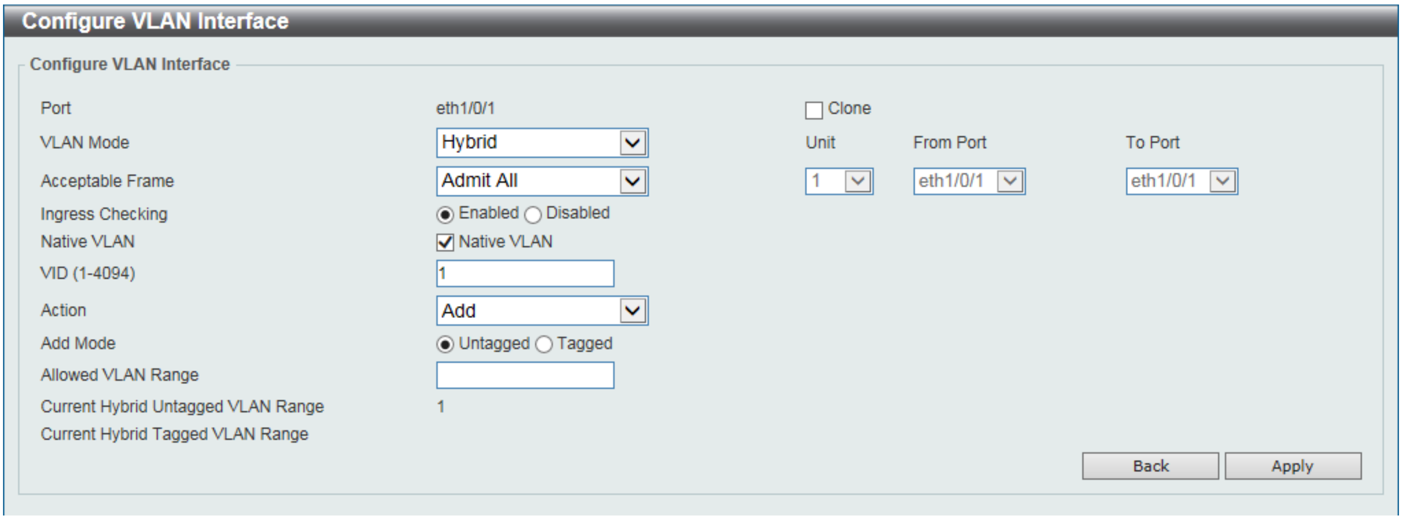
Port	eth1/0/1
VLAN Mode	Hybrid
Native VLAN	1
Hybrid Untagged VLAN	1
Hybrid Tagged VLAN	
Dynamic Tagged VLAN	
Ingress Checking	Enabled
Acceptable Frame Type	Admit-All

Figure 5-16 VLAN Interface (VLAN Detail) Window

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

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

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



Configure VLAN Interface

Configure VLAN Interface

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

Figure 5-17 VLAN Interface Window

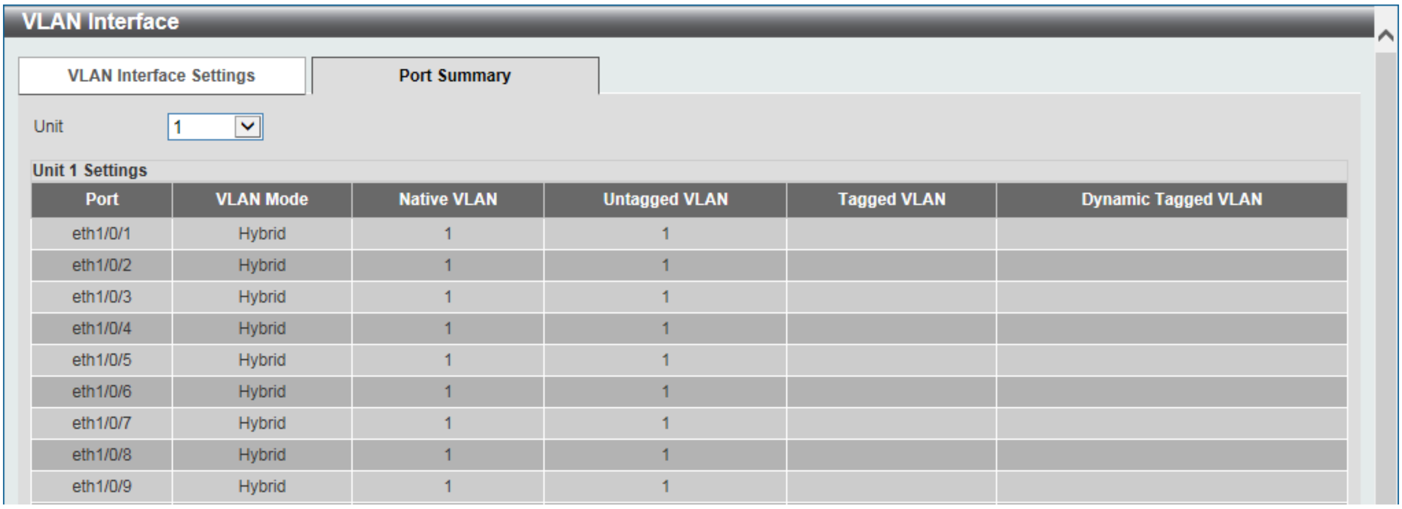
The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are **Access**, **Hybrid**, **Trunk**, **Dot1q-Tunnel**, **Promiscuous**, and **Host**.
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are **Tagged Only**, **Untagged Only**, and **Admit All**.
Ingress Checking	Select to enable or disable the ingress checking function.
Native VLAN	After selecting **Hybrid** or **Trunk** under **VLAN Mode**, select this option to enable the native VLAN function.
VID	After selecting **Access**, **Hybrid**, **Trunk**, or **Dot1q-Tunnel** under **VLAN Mode** and selecting the **Native VLAN** option, enter the VLAN ID here. The range is from 1 to 4094.
Action	After selecting **Hybrid**, **Trunk**, or **Dot1q-Tunnel** under **VLAN Mode**, select the action that will be taken here. Options to choose from are **Add**, **Remove**, **Tagged**, and **Untagged**.
Add Mode	After selecting **Hybrid** or **Dot1q-Tunnel** under **VLAN Mode**, select **Untagged** or **Tagged** here.
Allowed VLAN Range	After selecting **Hybrid**, **Trunk**, or **Dot1q-Tunnel** under **VLAN Mode**, enter the allowed VLAN range here.
Clone	Select this option to enable the clone feature.
Unit	Select the unit ID of the Switch in the stack here.
From Port - To Port	Select the range of ports that will be used in the clone feature here.

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

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

To view the following window, select the **Port Summary** tab, as shown below:



Unit: 1

Unit 1 Settings

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

Figure 5-18 Port Summary Window

The fields that can be configured are described below:

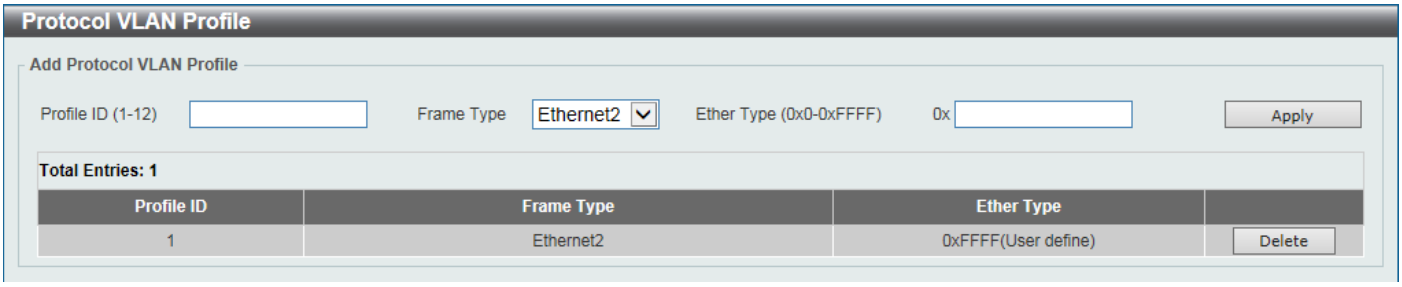
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.

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:



Profile ID (1-12):
Frame Type: Ethernet2
Ether Type (0x0-0xFFFF): 0x

Total Entries: 1

Profile ID	Frame Type	Ether Type	
1	Ethernet2	0xFFFF(User define)	Delete

Figure 5-19 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. The range is from 1 to 12.
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**.

Parameter	Description
Ether Type	Enter the Ethernet type value for the group here. The protocol value is used to identify a protocol of the frame type specified. The range is from 0x0 to 0xFFFF. Depending on the frame type, the octet string will have one of the following values: • For **Ethernet2**, 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.

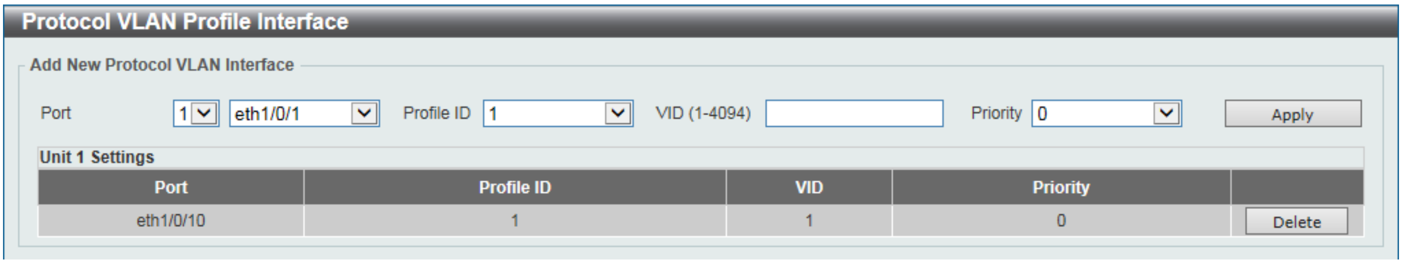
Click the **Apply** button to accept the changes made.

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:



Protocol VLAN Profile Interface

Add New Protocol VLAN Interface

Port: 1, eth1/0/1 — Profile ID: 1 — VID (1-4094): — Priority: 0 — Apply

Unit 1 Settings

Port	Profile ID	VID	Priority	
eth1/0/10	1	1	0	Delete

Figure 5-20 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.
Profile ID	Select the 802.1v protocol VLAN profile ID here.
VID	Enter the VLAN ID used here.
Priority	Select the priority value used here. The range is from 0 to 7. This parameter is specified to rewrite 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.

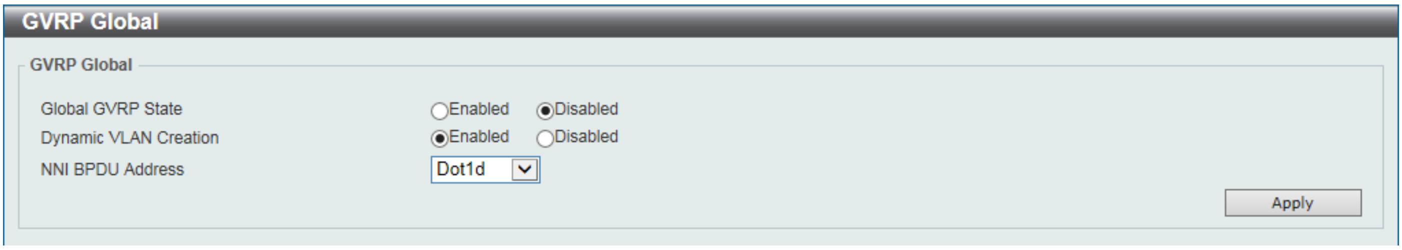
Click the **Delete** button to remove the specific entry.

GVRP

GVRP Global

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

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



GVRP Global

GVRP Global

Global GVRP State	○Enabled	●Disabled
Dynamic VLAN Creation	●Enabled	○Disabled
NNI BPDU Address	Dot1d	

Figure 5-21 GVRP Global Window

The fields that can be configured are described below:

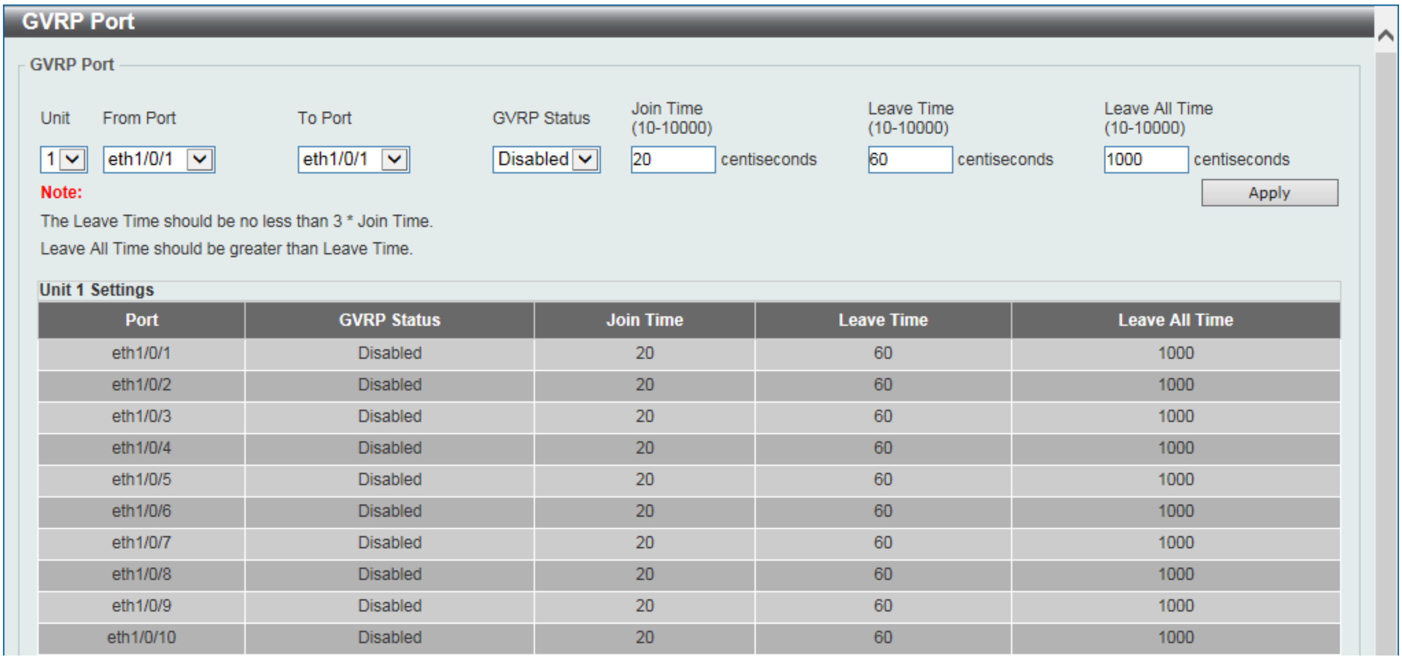
Parameter	Description
Global GVRP State	Select to enable or disable the global GVRP state here.
Dynamic VLAN Creation	Select to enable or disable the dynamic VLAN creation function here.
NNI BPDU Address	Select the NNI BPDU address option here. This option is used to determine the BPDU protocol address 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:



GVRP Port

GVRP Port

Unit	From Port	To Port	GVRP Status	Join Time (10-10000)	Leave Time (10-10000)	Leave All Time (10-10000)
1	eth1/0/1	eth1/0/1	Disabled	20 centiseconds	60 centiseconds	1000 centiseconds

Note:
The Leave Time should be no less than 3 * Join Time.
Leave All Time should be greater than Leave Time.

Unit 1 Settings

Port	GVRP Status	Join Time	Leave Time	Leave All Time
eth1/0/1	Disabled	20	60	1000
eth1/0/2	Disabled	20	60	1000
eth1/0/3	Disabled	20	60	1000
eth1/0/4	Disabled	20	60	1000
eth1/0/5	Disabled	20	60	1000
eth1/0/6	Disabled	20	60	1000
eth1/0/7	Disabled	20	60	1000
eth1/0/8	Disabled	20	60	1000
eth1/0/9	Disabled	20	60	1000
eth1/0/10	Disabled	20	60	1000

Figure 5-22 GVRP Port Window

The fields that can be configured are described below:

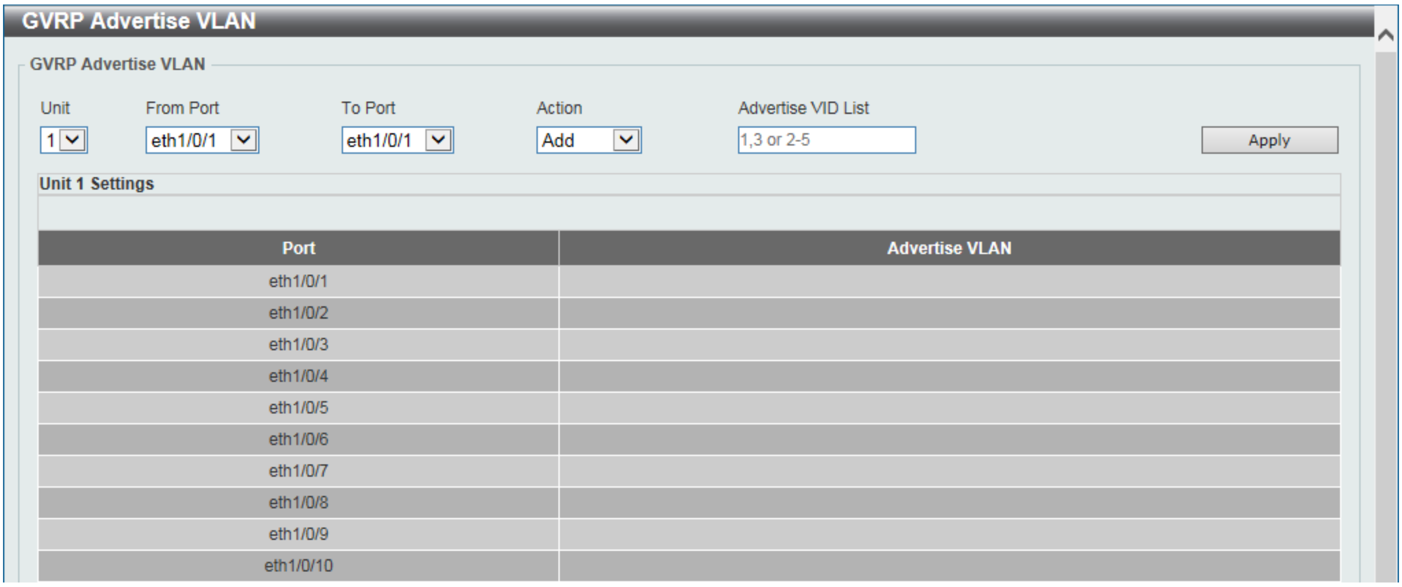
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
GVRP Status	Select the enable or disable the GVRP port status. This enables the port to dynamically become a member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



GVRP Advertise VLAN

GVRP Advertise VLAN

Unit: 1

From Port: eth1/0/1

To Port: eth1/0/1

Action: Add

Advertise VID List: 1,3 or 2-5

Unit 1 Settings

Port	Advertise VLAN
eth1/0/1	
eth1/0/2	
eth1/0/3	
eth1/0/4	
eth1/0/5	
eth1/0/6	
eth1/0/7	
eth1/0/8	
eth1/0/9	
eth1/0/10	

Figure 5-23 GVRP Advertise VLAN Window

The fields that can be configured are described below:

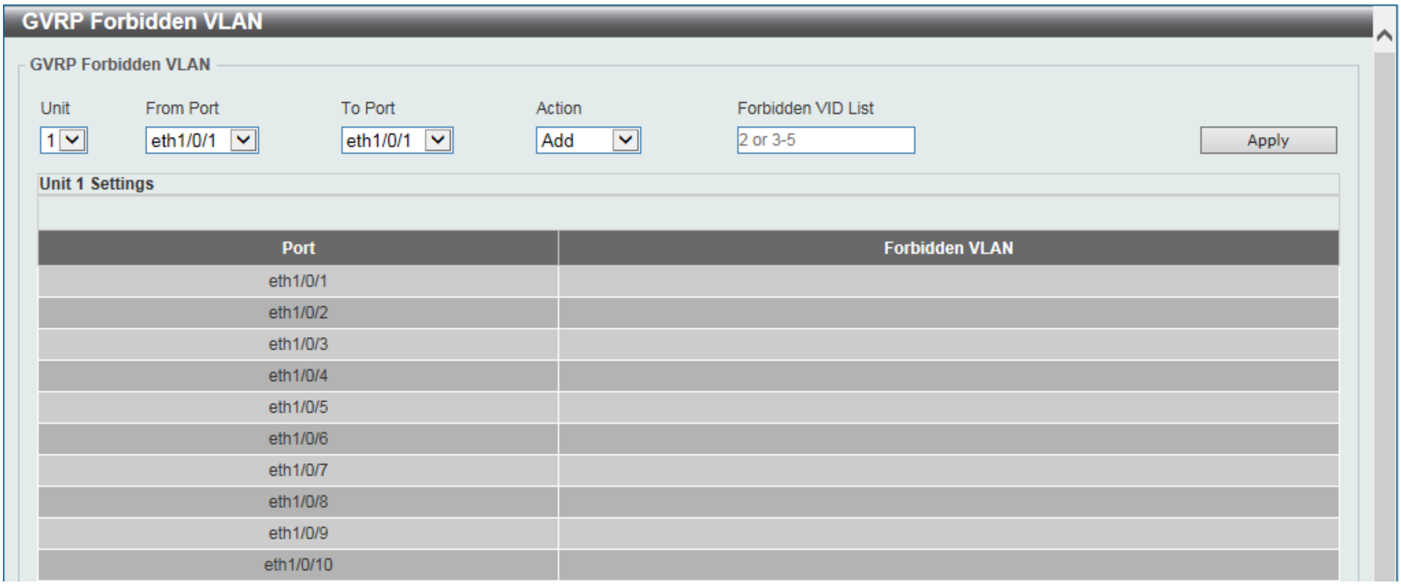
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Action	Select the advertised VLAN to port mapping action here. Options to choose from are **All**, **Add**, **Remove**, 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:



GVRP Forbidden VLAN

GVRP Forbidden VLAN

Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1
Action: Add
Forbidden VID List: 2 or 3-5

Unit 1 Settings

Port	Forbidden VLAN
eth1/0/1	
eth1/0/2	
eth1/0/3	
eth1/0/4	
eth1/0/5	
eth1/0/6	
eth1/0/7	
eth1/0/8	
eth1/0/9	
eth1/0/10	

Figure 5-24 GVRP Forbidden VLAN Window

The fields that can be configured are described below:

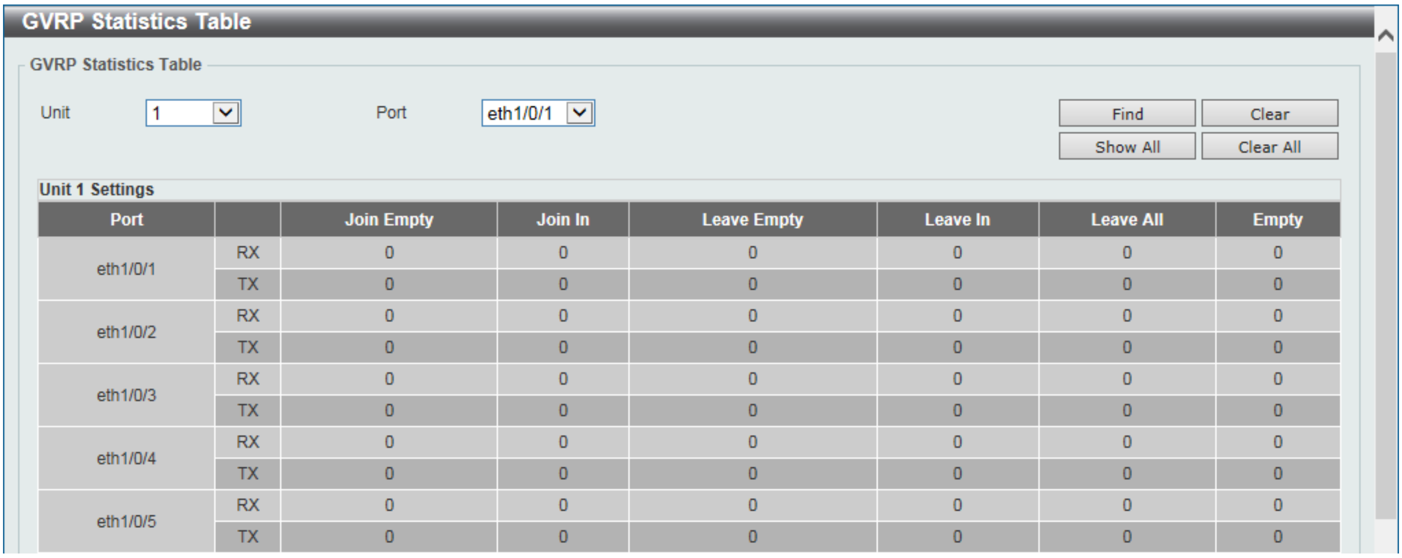
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Action	Select the forbidden VLAN to port mapping action that will be taken here. Options to choose from are **All**, **Add**, **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:



Unit: 1

Port: eth1/0/1

Unit 1 Settings

Port		Join Empty	Join In	Leave Empty	Leave In	Leave All	Empty
eth1/0/1	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0
eth1/0/2	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0
eth1/0/3	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0
eth1/0/4	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0
eth1/0/5	RX	0	0	0	0	0	0
	TX	0	0	0	0	0	0

Figure 5-25 GVRP Statistics Table Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit to be displayed here.
Port	Select the port number to display GVRP statistic information for here.

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.

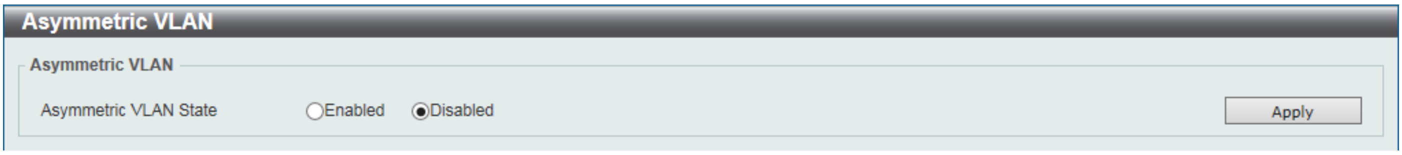
Click the **Show All** button to view all GVRP statistic information.

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:



Asymmetric VLAN State ○Enabled ●Disabled

Figure 5-26 Asymmetric VLAN Window

The fields that can be configured are described below:

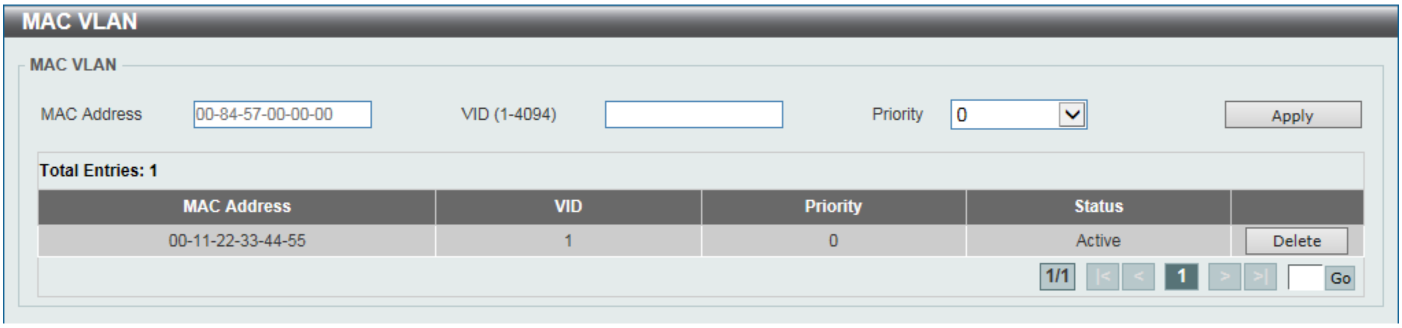
Parameter	Description
Asymmetric VLAN State	Select to enable or disable the asymmetric VLAN feature here.

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:



MAC VLAN

MAC VLAN

MAC Address: 00-84-57-00-00-00 VID (1-4094): Priority: 0

Total Entries: 1

MAC Address	VID	Priority	Status	
00-11-22-33-44-55	1	0	Active	Delete

Figure 5-27 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. The range is from 0 to 7.

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

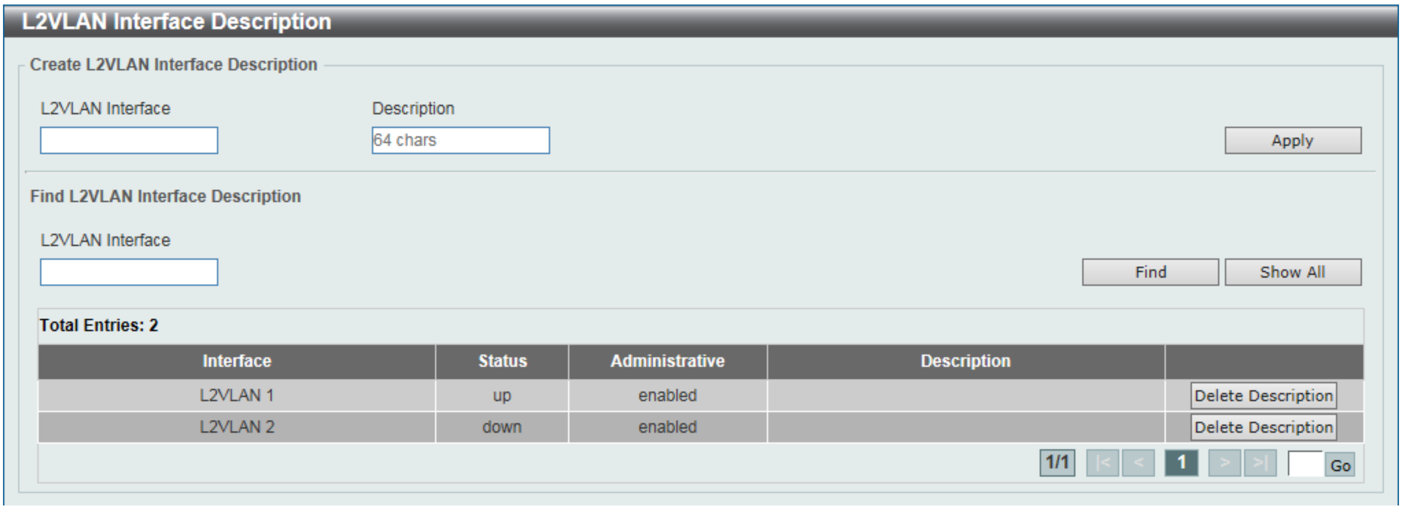
Click the **Delete** button to remove the specific entry.

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

L2VLAN Interface Description

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

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



L2VLAN Interface Description

Create L2VLAN Interface Description

L2VLAN Interface: Description: 64 chars

Find L2VLAN Interface Description

L2VLAN Interface:

Total Entries: 2

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

Figure 5-28 L2VLAN Interface Description Window

The fields that can be configured are described below:

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

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

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

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

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

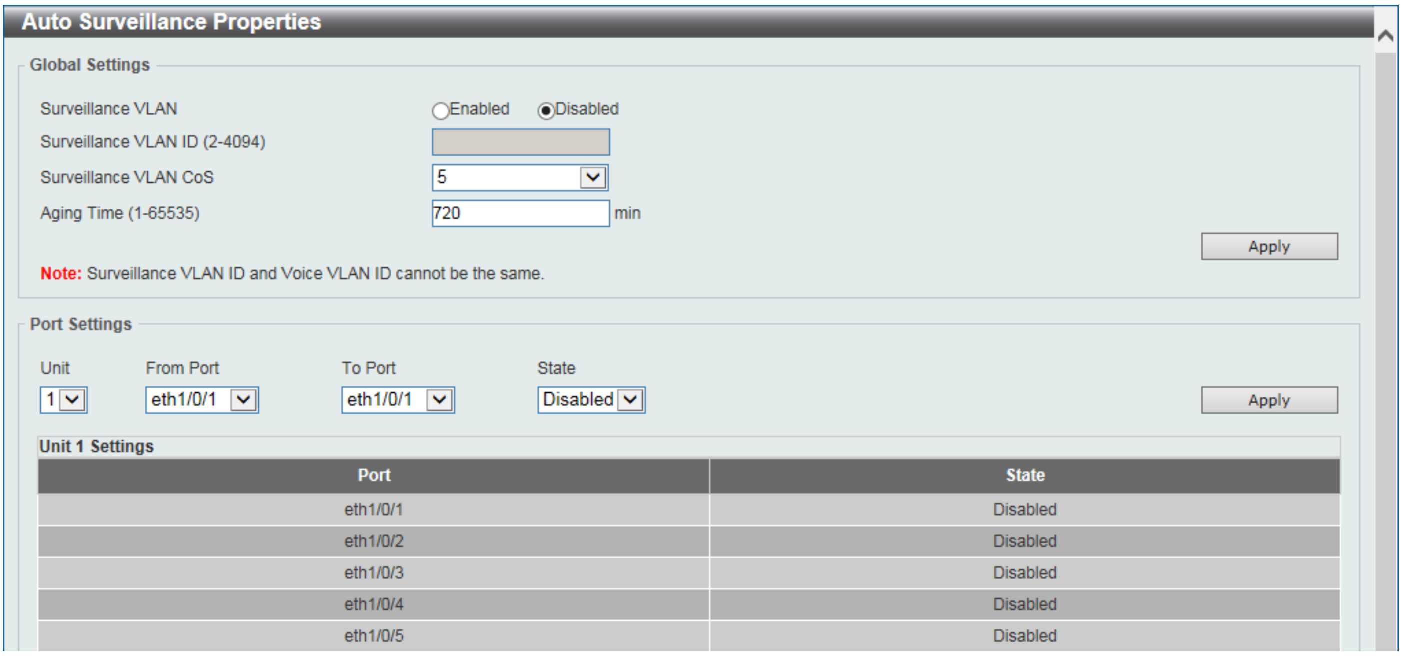
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Auto Surveillance VLAN

Auto Surveillance Properties

This window is used to 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:



Auto Surveillance Properties

Global Settings

Surveillance VLAN ○Enabled ●Disabled

Surveillance VLAN ID (2-4094)

Surveillance VLAN CoS: 5

Aging Time (1-65535): 720 min

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

Port Settings

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

Unit 1 Settings

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

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.

Parameter	Description
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:

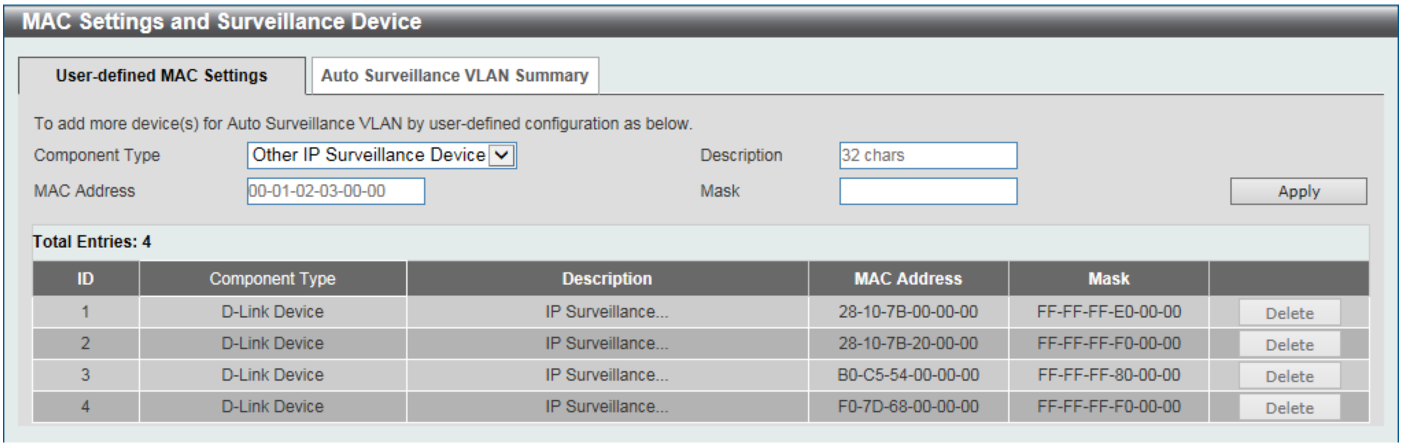
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
State	Select to enable or disable the surveillance VLAN feature. When surveillance VLAN is enabled for a port, 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** and select the **User-defined MAC Settings** tab, as shown below:



MAC Settings and Surveillance Device

User-defined MAC Settings | Auto Surveillance VLAN Summary

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

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

Total Entries: 4

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

Figure 5-30 MAC Settings and Surveillance Device Window

The fields that can be configured are described below:

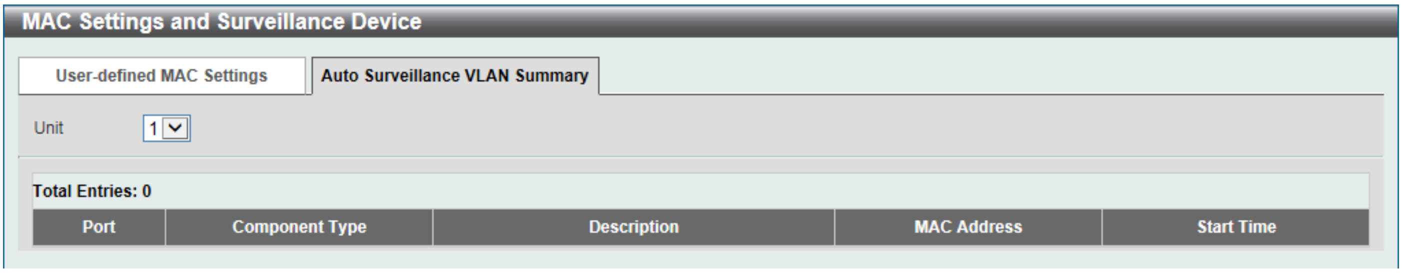
Parameter	Description
Component Type	Select the component type here. Option to choose from are: • **Video Management Server -** Specifies the surveillance device type as Video Management Server (VMS). • **VMS Client/Remote Viewer -** Specifies the surveillance device type as VMS client.

Parameter	Description
	- **Video Encoder** - Specifies the surveillance device type as Video Encoder. - **Network Storage** - Specifies the surveillance device type as Network Storage. - **Other IP Surveillance Device** - Specifies the surveillance device type as other IP Surveillance Devices.
Description	Enter the description for the user-defined OUI here. This string can be up to 32 characters long.
MAC Address	Enter the OUI MAC address here. If the source MAC addresses of the received packet matches any of the OUI pattern, the received packet is determined as a surveillance packet.
Mask	Enter the matching bitmask for the OUI MAC address here.

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

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

To view the following window, select the **Auto Surveillance VLAN Summary** tab, as shown below:


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

Unit: 1

Total Entries: 0

Port	Component Type	Description	MAC Address	Start Time

Figure 5-31 MAC Settings and Surveillance Device (Auto Surveillance VLAN Summary) Window

The fields that can be configured are described below:

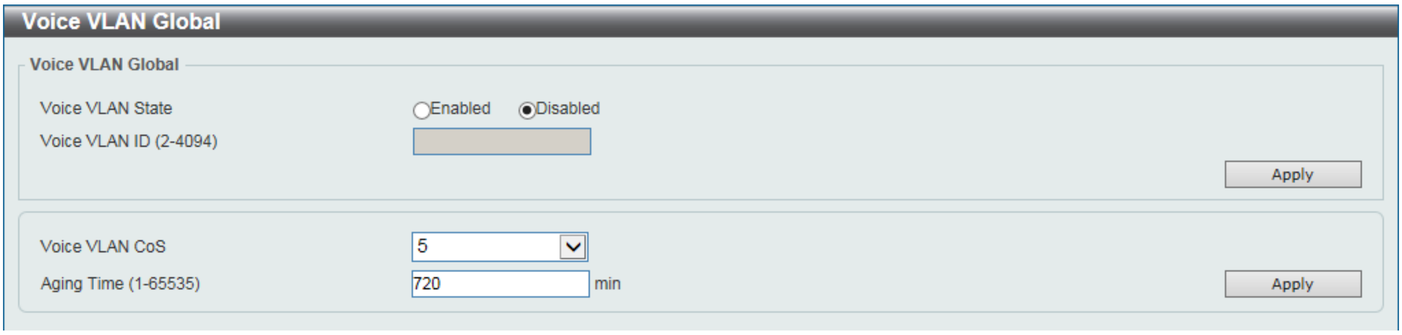
Parameter	Description
Unit	Select the stacking unit ID of the Switch that will be used in this display here.

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:



Voice VLAN State ○Enabled ●Disabled

Voice VLAN ID (2-4094)

Voice VLAN CoS: 5

Aging Time (1-65535): 720 min

Figure 5-32 Voice VLAN Global Window

The fields that can be configured are described below:

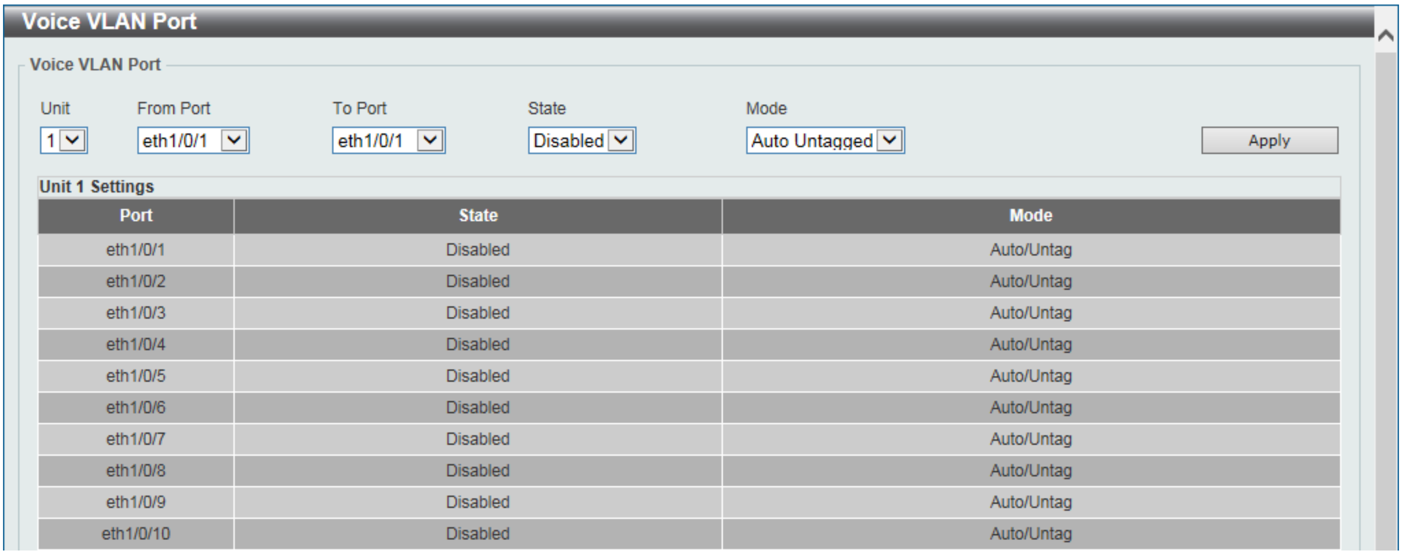
Parameter	Description
Voice VLAN State	Select to globally enable or disable the voice VLAN feature here.
Voice VLAN ID	Enter the VLAN ID of the voice VLAN here. The VLAN to be specified as the voice VLAN needs to pre-exist before configuration. The range is from 2 to 4094.
Voice VLAN CoS	Select the CoS 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:



Voice VLAN Port

Voice VLAN Port

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

Unit 1 Settings

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

Figure 5-33 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.
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. 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 comply with the OUI addresses.
Mode	Select the mode here. Options to choose from are: • **Auto Untagged -** Specifies that voice VLAN untagged membership will be automatically learned.

Parameter	Description
	• **Auto Tagged** - Specifies that voice VLAN tagged membership will be automatically learned. • **Manual** - Specifies that voice VLAN membership will be manually configured. If auto-learning is enabled, the port will automatically be learned as a voice VLAN member. This membership will automatically be aged out. When the port is working in the auto-tagged mode and the port captures a voice device through the device's OUI, it will join the voice VLAN as a tagged member automatically. When the voice device sends tagged packets, the Switch will change its priority. When the voice device sends untagged packets, it will forward them in the Port VLAN ID (PVID). When the port is working in auto-untagged mode, and the port captures a voice device through the device's OUI, it will join the voice VLAN as an untagged member automatically. When the voice device sends tagged packets, the Switch will change its priority. When the voice device sends untagged packets, it will forward them in the voice VLAN. When the Switch receives LLDP-MED packets, it checks the VLAN ID, tagged flag, and priority flag. The Switch should follow the tagged flag and priority setting.

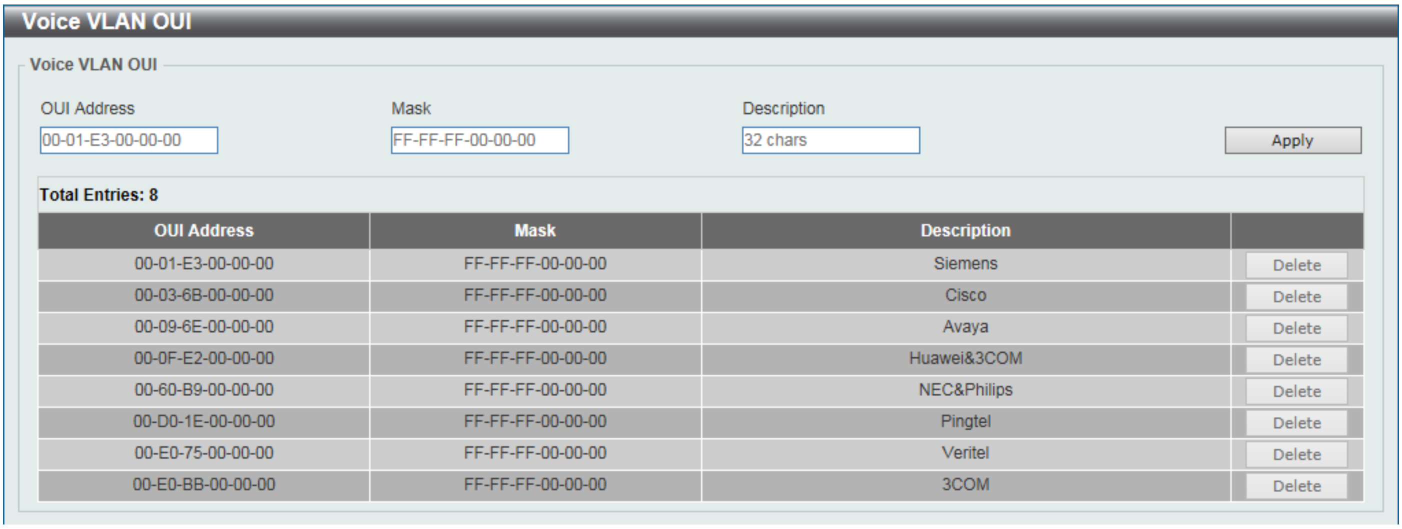
Click the **Apply** button to accept the changes made.

Voice VLAN OUI

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

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

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



OUI Address: 00-01-E3-00-00-00
Mask: FF-FF-FF-00-00-00
Description: 32 chars

Total Entries: 8

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

Figure 5-34 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.

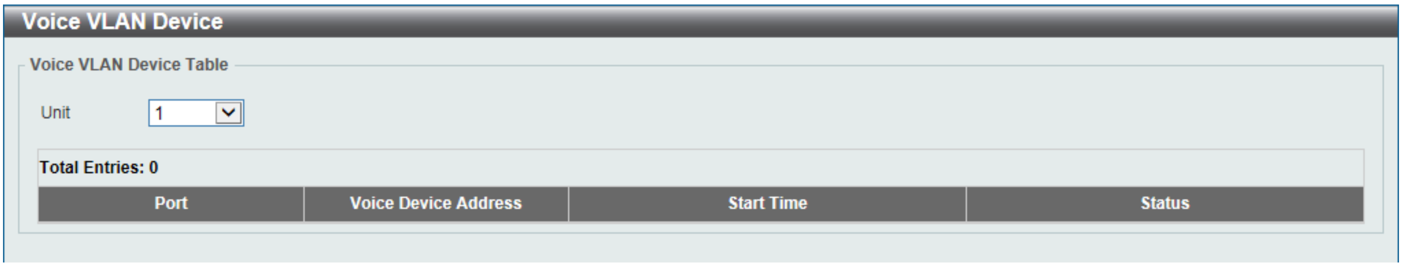
Click the **Apply** button to accept the changes made.

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:



Voice VLAN Device

Voice VLAN Device Table

Unit: 1

Total Entries: 0

Port	Voice Device Address	Start Time	Status

Figure 5-35 Voice VLAN Device Window

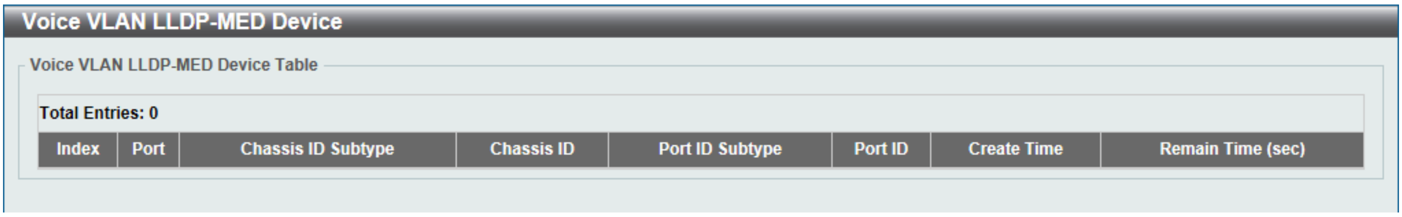
The fields that can be configured are described below:

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

Voice VLAN LLDP-MED Device

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

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



Voice VLAN LLDP-MED Device

Voice VLAN LLDP-MED Device Table

Total Entries: 0

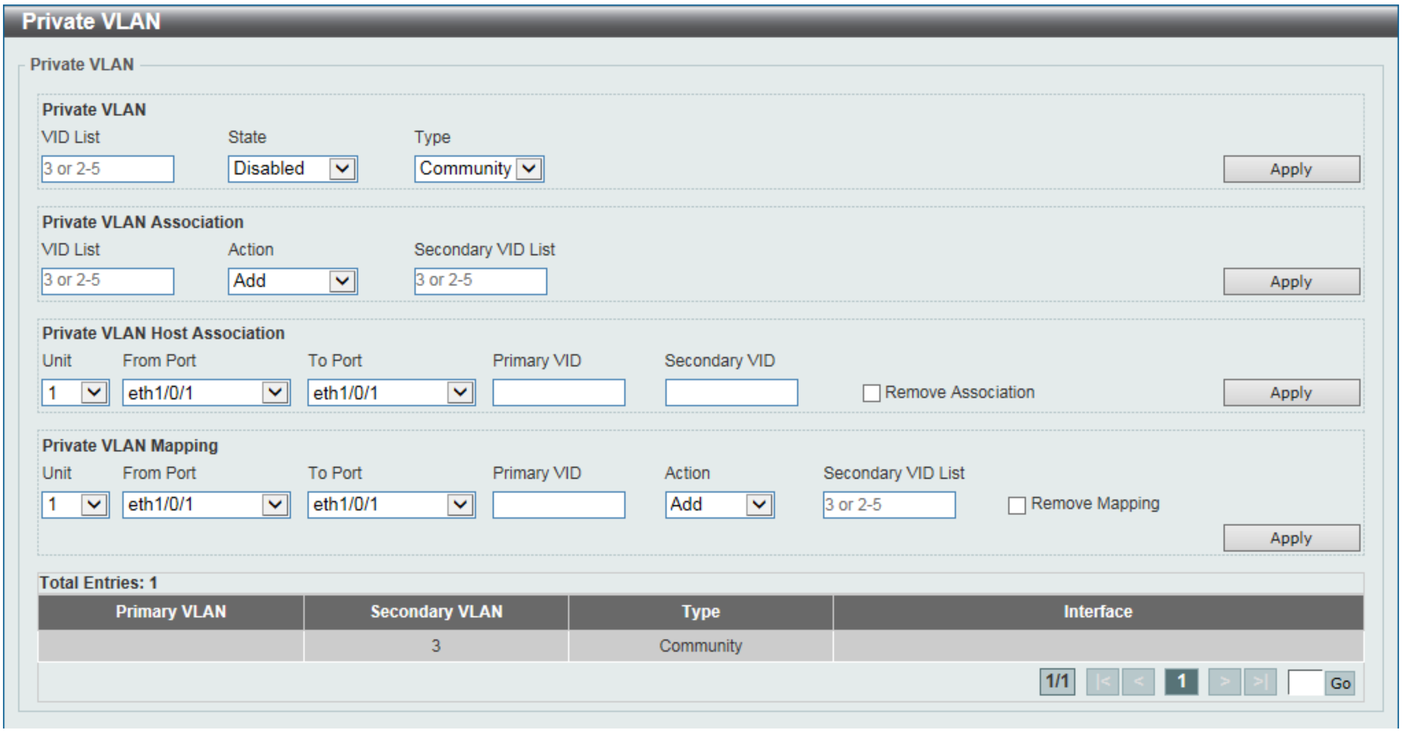
Index	Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	Create Time	Remain Time (sec)

Figure 5-36 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:



Private VLAN

Private VLAN

Private VLAN

VID List: 3 or 2-5 State: Disabled Type: Community

Private VLAN Association

VID List: 3 or 2-5 Action: Add Secondary VID List: 3 or 2-5

Private VLAN Host Association

Unit: 1 From Port: eth1/0/1 To Port: eth1/0/1 Primary VID: Secondary VID: □ Remove Association

Private VLAN Mapping

Unit: 1 From Port: eth1/0/1 To Port: eth1/0/1 Primary VID: Action: Add Secondary VID List: 3 or 2-5 □ Remove Mapping

Total Entries: 1

Primary VLAN	Secondary VLAN	Type	Interface
	3	Community	

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.
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**, **Remove**, and **Disabled**.
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.
From Port - To Port	Select the range of ports that will be used for this configuration here.

Parameter	Description
Primary VID	Enter the primary private VLAN ID here.
Secondary VID	Enter the secondary private VLAN ID here. When ticking the **Remove Association** option, 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.
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

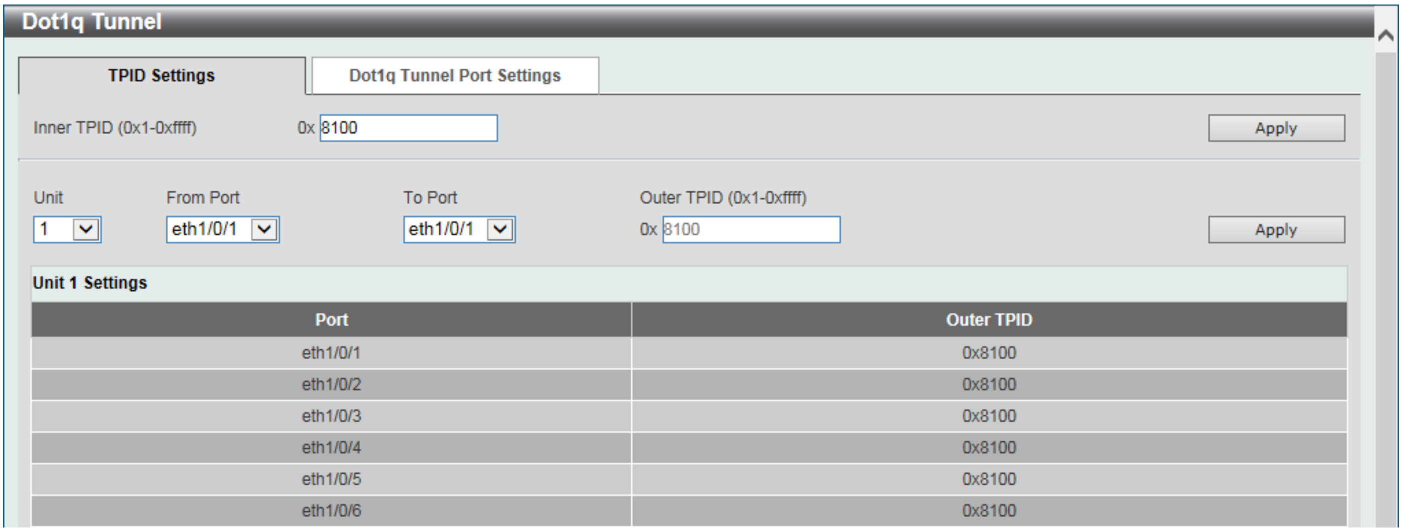
Dot1q Tunnel

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** and select the **TPID Settings** tab, as shown below:



Inner TPID (0x1-0xffff) 0x 8100

Unit 1 | From Port eth1/0/1 | To Port eth1/0/1 | Outer TPID (0x1-0xffff) 0x 8100

Unit 1 Settings

Port	Outer TPID
eth1/0/1	0x8100
eth1/0/2	0x8100
eth1/0/3	0x8100
eth1/0/4	0x8100
eth1/0/5	0x8100
eth1/0/6	0x8100

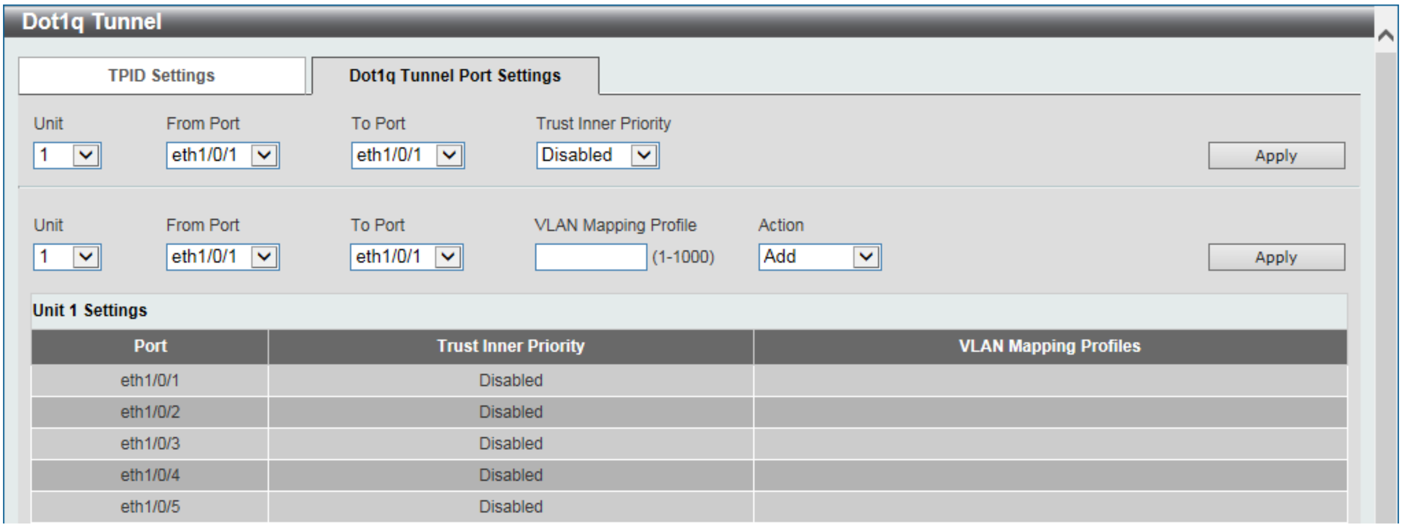
Figure 5-38 Dot1q Tunnel Window

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.
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.

To view the following window, select the **Dot1q Tunnel Port Settings** tab, as shown below:



Unit: 1 | From Port: eth1/0/1 | To Port: eth1/0/1 | Trust Inner Priority: Disabled

Unit: 1 | From Port: eth1/0/1 | To Port: eth1/0/1 | VLAN Mapping Profile: (1-1000) | Action: Add

Unit 1 Settings

Port	Trust Inner Priority	VLAN Mapping Profiles
eth1/0/1	Disabled	
eth1/0/2	Disabled	
eth1/0/3	Disabled	
eth1/0/4	Disabled	
eth1/0/5	Disabled	

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.
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.
VLAN Mapping Profile	Enter the ID of the VLAN mapping profile here. In each Profile type, a lower ID value has higher priority. The 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.

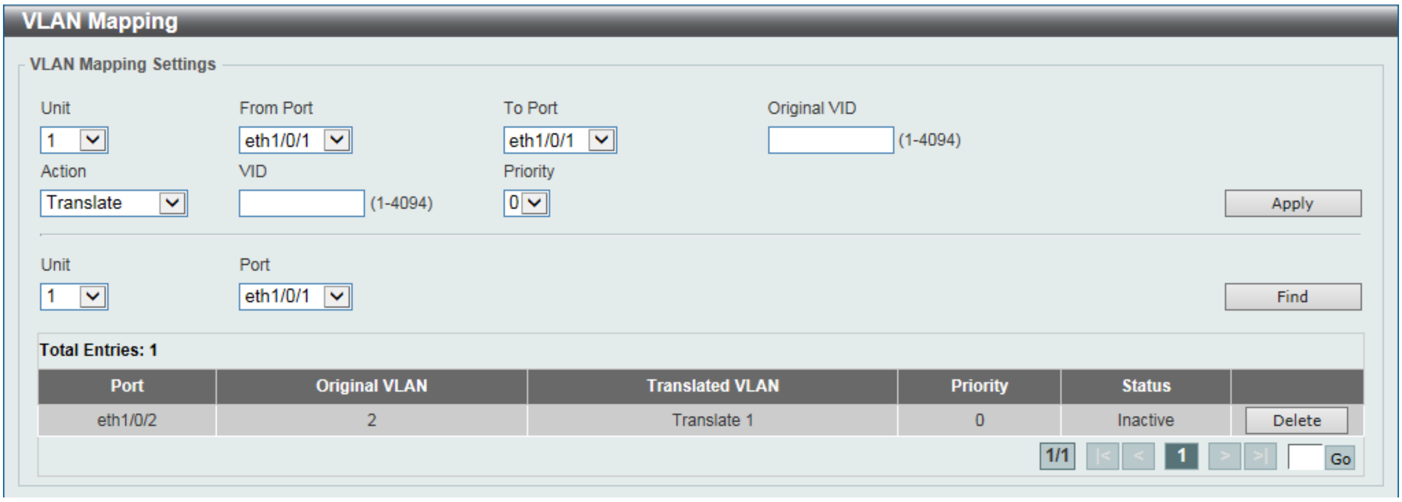
Click the **Apply** button to accept the changes made.

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 sequence number of the rule in the profile and stops when matched first. 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:



VLAN Mapping

VLAN Mapping Settings

Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1
Original VID: (1-4094)
Action: Translate
VID: (1-4094)
Priority: 0

Unit: 1
Port: eth1/0/1

Total Entries: 1

Port	Original VLAN	Translated VLAN	Priority	Status	
eth1/0/2	2	Translate 1	0	Inactive	Delete

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.
From Port - To Port	Select the port range that will be used here.
Original VID	Enter the original 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** - Specifies that the outer-VID will replace the outer-VID of the matched packets. • **Dot1q-tunnel** - Specifies that the outer-VID will be added for matched packets.
VID	Enter the VLAN ID 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.
Port	Select the port that will be used for the search here.

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

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

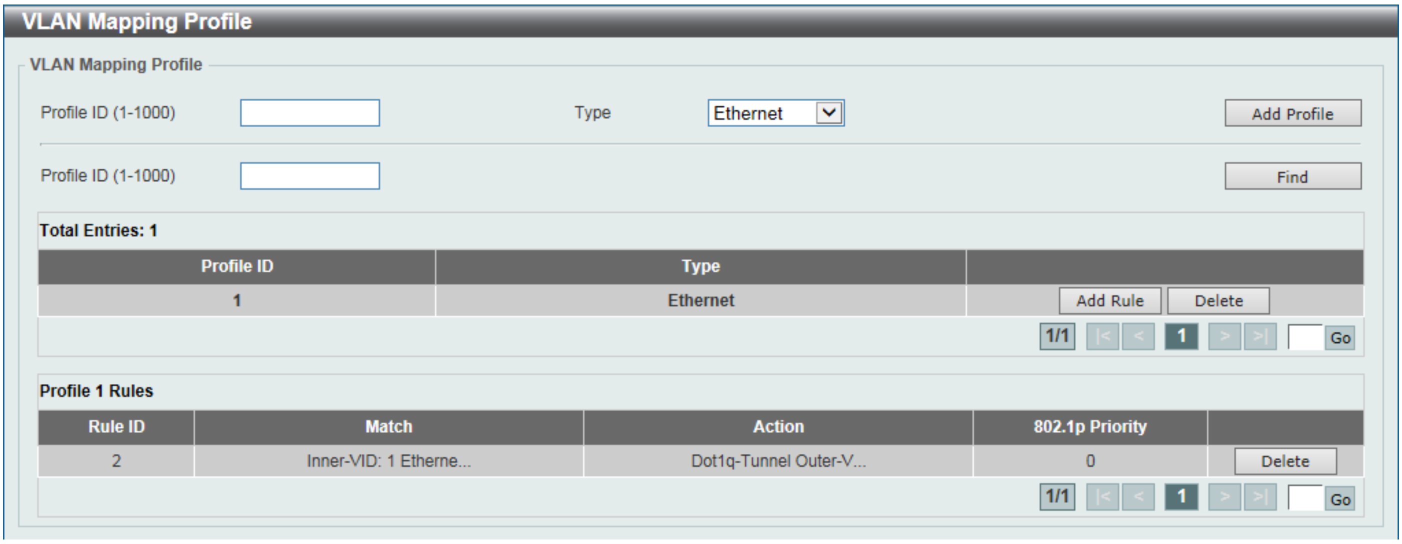
Click the **Delete** button to delete the specified entry.

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**, as shown below:



VLAN Mapping Profile

VLAN Mapping Profile

Profile ID (1-1000)

Type: Ethernet

Profile ID (1-1000)

Total Entries: 1

Profile ID	Type	
1	Ethernet	Add Rule Delete

Profile 1 Rules

Rule ID	Match	Action	802.1p Priority	
2	Inner-VID: 1 Etherne...	Dot1q-Tunnel Outer-V...	0	Delete

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. In each Profile type, a lower ID value has 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** - 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.

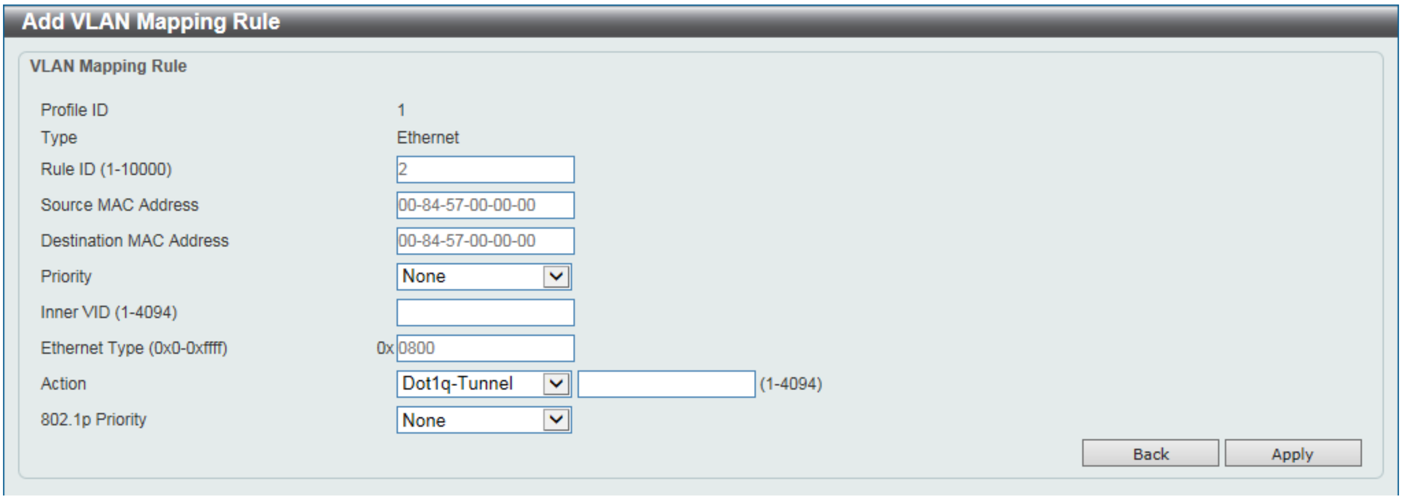
Click the **Find** button to locate a specific entry based on the information entered.

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.



Add VLAN Mapping Rule

VLAN Mapping Rule

Profile ID	1
Type	Ethernet
Rule ID (1-10000)	2
Source MAC Address	00-84-57-00-00-00
Destination MAC Address	00-84-57-00-00-00
Priority	None
Inner VID (1-4094)	
Ethernet Type (0x0-0xffff)	0x 0800
Action	Dot1q-Tunnel (1-4094)
802.1p Priority	None

Figure 5-42 VLAN Mapping Profile (Ethernet, Add Rule) Window

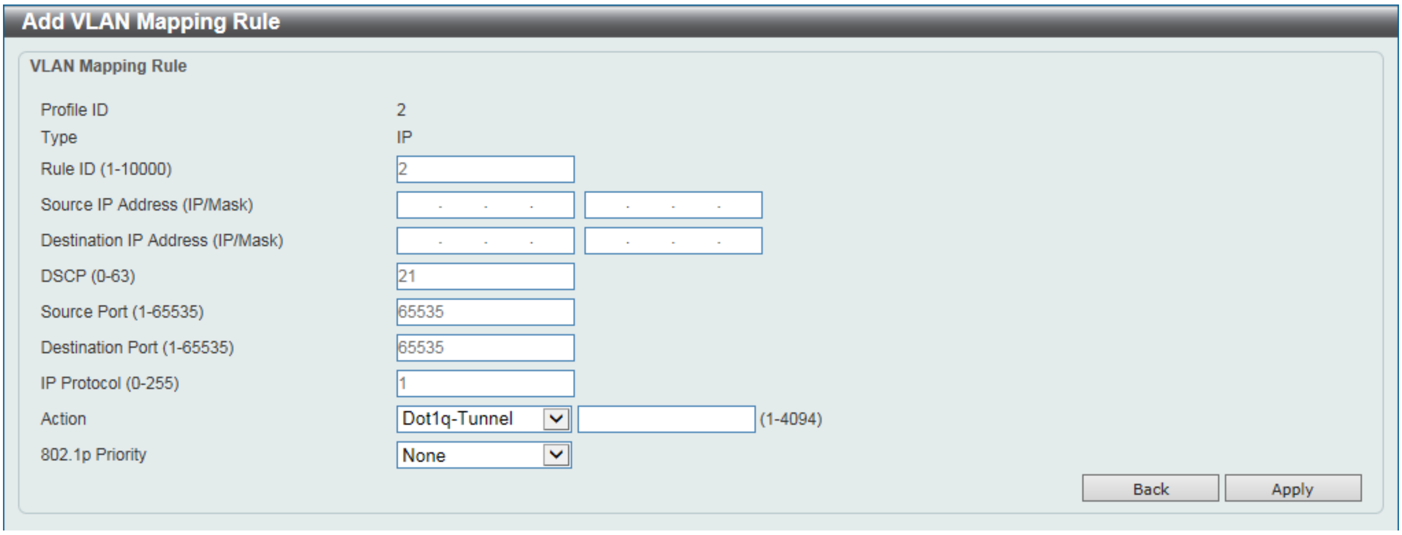
The fields that can be configured are described below:

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.
Source MAC Address	Enter the source MAC address here.
Destination 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** - Specifies that the outer-VID will be added for matched packets.
802.1p Priority	Select the 802.1p priority value here. The range is from 0 to 7. A higher value has a higher priority.

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.



Add VLAN Mapping Rule

VLAN Mapping Rule

Profile ID	2	
Type	IP	
Rule ID (1-10000)	2	
Source IP Address (IP/Mask)	. . .	. . .
Destination IP Address (IP/Mask)	. . .	. . .
DSCP (0-63)	21	
Source Port (1-65535)	65535	
Destination Port (1-65535)	65535	
IP Protocol (0-255)	1	
Action	Dot1q-Tunnel	(1-4094)
802.1p Priority	None	

Figure 5-43 VLAN Mapping Profile (IP, Add Rule) Window

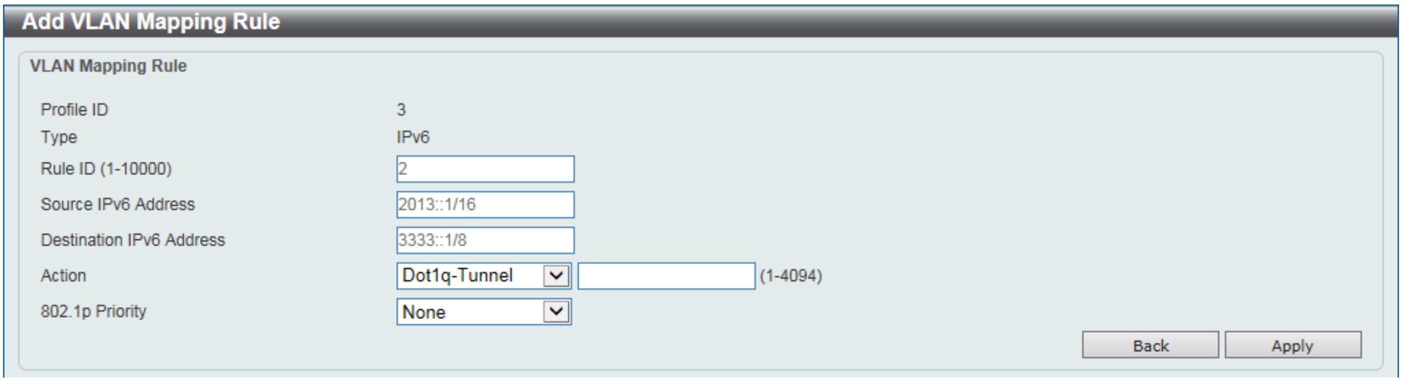
The fields that can be configured are described below:

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
Source IP Address (IP/Mask)	Enter the source IPv4 address and subnet mask here.
Destination IP Address (IP/Mask)	Enter the destination IPv4 address and subnet mask here.
DSCP	Enter the 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** - Specifies that the outer-VID will be added for matched packets.
802.1p Priority	Select the 802.1p priority value here. The range is from 0 to 7. A higher value has a higher priority.

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.



Add VLAN Mapping Rule

VLAN Mapping Rule

Profile ID	3	
Type	IPv6	
Rule ID (1-10000)	2	
Source IPv6 Address	2013::1/16	
Destination IPv6 Address	3333::1/8	
Action	Dot1q-Tunnel	(1-4094)
802.1p Priority	None	

Figure 5-44 VLAN Mapping Profile (IPv6, Add Rule) Window

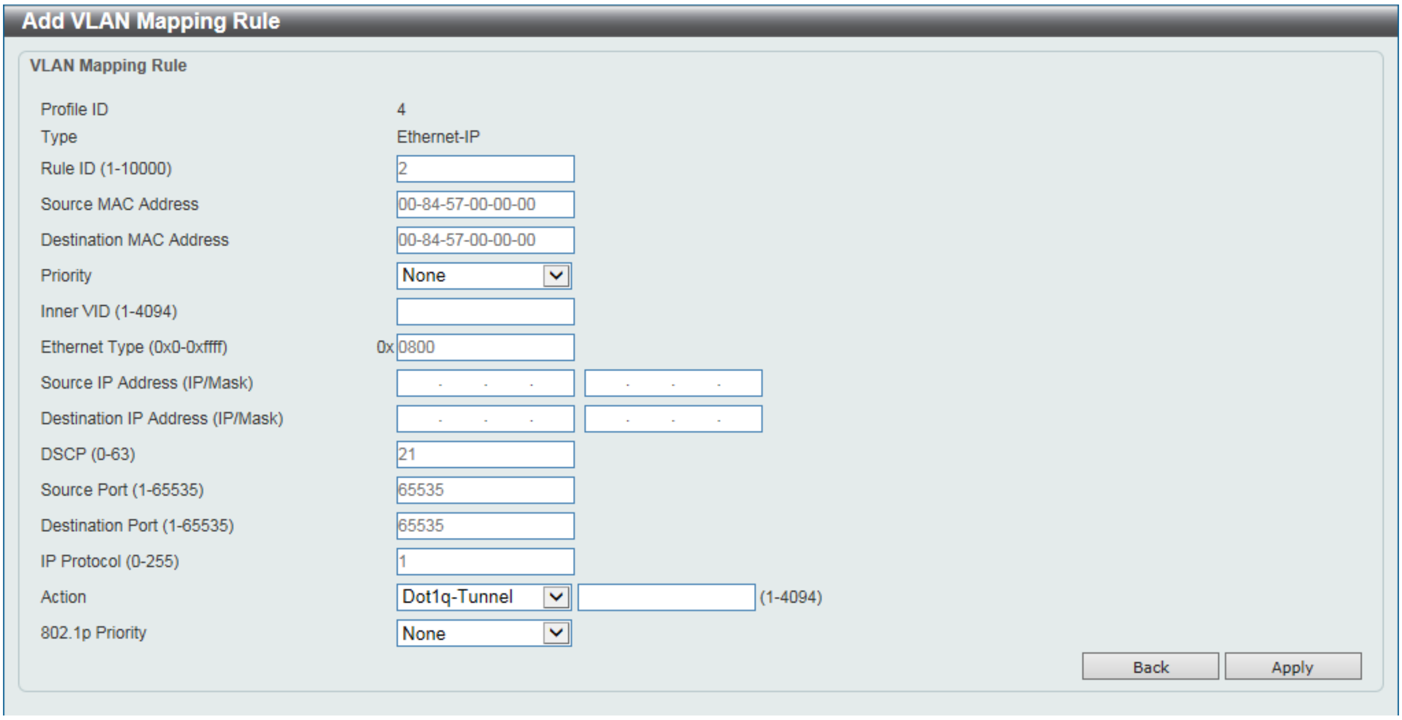
The fields that can be configured are described below:

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
Source IPv6 Address	Enter the source IPv6 address and prefix length here.
Destination 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** - Specifies that the outer-VID will be added for matched packets.
802.1p Priority	Select the 802.1p priority value here. The range is from 0 to 7. A higher value has a higher priority.

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.



Add VLAN Mapping Rule

VLAN Mapping Rule

Profile ID	4
Type	Ethernet-IP
Rule ID (1-10000)	2
Source MAC Address	00-84-57-00-00-00
Destination MAC Address	00-84-57-00-00-00
Priority	None
Inner VID (1-4094)	
Ethernet Type (0x0-0xffff)	0x 0800
Source IP Address (IP/Mask)	. . . / . . .
Destination IP Address (IP/Mask)	. . . / . . .
DSCP (0-63)	21
Source Port (1-65535)	65535
Destination Port (1-65535)	65535
IP Protocol (0-255)	1
Action	Dot1q-Tunnel (1-4094)
802.1p Priority	None

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.
Source MAC Address	Enter the source MAC address here.
Destination 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.
Source IP Address	Enter the source IPv4 address and subnet mask here.

Parameter	Description
Destination IP Address	Enter the destination IPv4 address and subnet mask here.
DSCP	Enter the 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** - Specifies that the outer-VID will be added for matched packets.
802.1p Priority	Select the IEEE 802.1p priority value here. The range is from 0 to 7. A higher value has a higher priority.

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 create 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. The table below compares how the three protocols differ regarding the port state transition.

All three protocols calculate a stable topology in the same way. Every segment will have a single path to the root bridge. All bridges listen for BPDU packets. However, BPDU packets are sent more frequently, with every Hello packet. BPDU packets are sent even if a BPDU packet was not received. Therefore, each link between bridges is sensitive to the status of the link. Ultimately, this difference results in faster detection of failed links, and therefore faster topology adjustment. A drawback of IEEE 802.1D-1998 is this absence of immediate feedback from adjacent bridges.

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

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

Edge Port

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

P2P Port

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

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

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

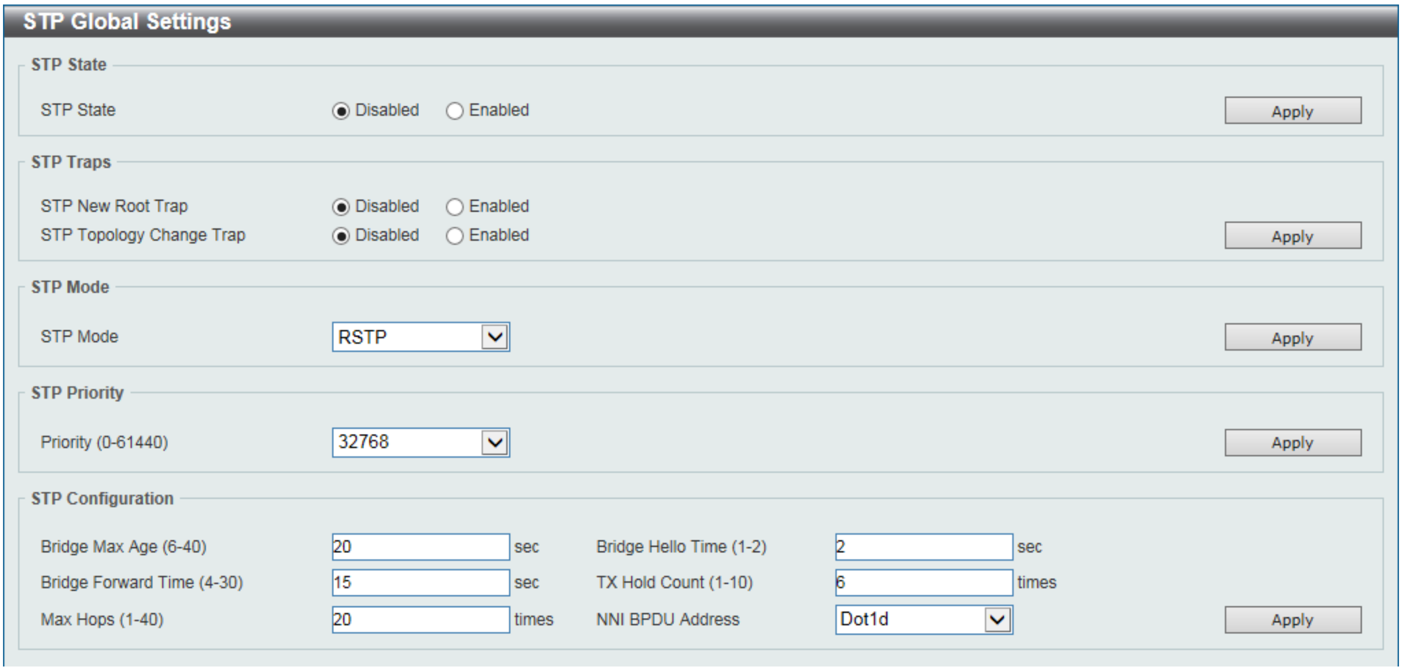
The Spanning Tree Protocol (STP) operates on two levels:

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

STP Global Settings

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

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



STP Global Settings

STP State

STP State ● Disabled ○ Enabled Apply

STP Traps

STP New Root Trap ● Disabled ○ Enabled

STP Topology Change Trap ● Disabled ○ Enabled Apply

STP Mode

STP Mode: RSTP Apply

STP Priority

Priority (0-61440): 32768 Apply

STP Configuration

Bridge Max Age (6-40): 20 sec

Bridge Hello Time (1-2): 2 sec

Bridge Forward Time (4-30): 15 sec

TX Hold Count (1-10): 6 times

Max Hops (1-40): 20 times

NNI BPDU Address: Dot1d Apply

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. The range is from 0 to 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:

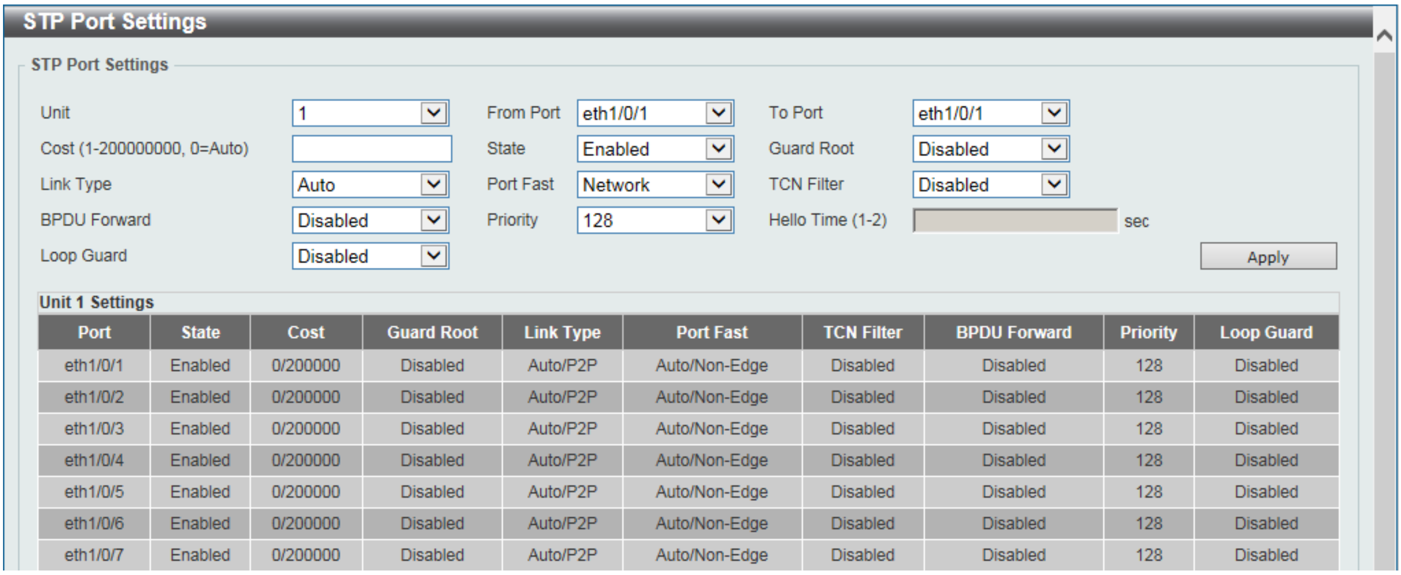
Parameter	Description
Bridge Max Age	Enter the bridge Maximum Age value here. The range is from 6 to 40 seconds. By default, this value is 20 seconds. The Maximum Age value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN.
Bridge Hello Time	After selecting **RSTP/STP** as the **Spanning Tree Mode**, this parameter will be available. Enter the bridge Hello Time value here. The range is from 1 to 2 seconds. By default, this value is 2 seconds. This is the interval between two transmissions of 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. The range is from 4 to 30 seconds. By default, this value is 15 seconds. Every port on the Switch spends this time in the Listening state while moving from the Blocking state to the Forwarding state.
TX Hold Count	Enter the Transmit Hold Count value here. The range is from 1 to 10 times. By default, this value is 6 times. This value is used to set the maximum number of Hello packets transmitted per interval.
Max Hops	Enter the maximum number of hops that are allowed. The range is from 1 to 40 hops. By default, this value is 20 hops. This value is used to set the number of hops between devices in a spanning tree region before the Bridge Protocol Data Unit (BPDU) packet sent by the Switch will be discarded. Each Switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BDPU packet and the information held for the port will age out.
NNI BPDU Address	Select the NNI BPDU Address option here. Options to choose from are **Dot1d** and **Dot1ad**. 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. By default, the **Dot1d** option is used.

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

STP Port Settings

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

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



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

Unit 1 Settings

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

Figure 5-47 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.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Cost	Enter the cost value here. The range is from 1 to 200000000. This value defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. By default, this 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. By default, port cost for 10 Mbps is 2000000, 100 Mbps is 200000, 1Gbps is 20000, 2.5Gbps is 8000, and 10Gbps is 2000. The lower the number, the greater the probability the port will be chosen to forward packets.
State	Select to enable or disable the STP port state.
Guard Root	Select to enable or disable the Guard Root function.
Link Type	Select the link type here. Options to choose from are **Auto**, **P2P**, and **Shared**. A full-duplex port is considered to have a Point-to-Point (**P2P**) connection. The port cannot transit into the forwarding state rapidly by setting the link type to **Shared**. By default, the **Auto** option is used.
Port Fast	Select the Port Fast option here. Options to choose from are: • **Network** - The port will remain in the non-port-fast state for three seconds. The port will change to the port-fast state if no BPDU is received and changes to the forwarding state. If the port received the BPDU later, it will change to the non-port-fast state. • **Disable** - The port will always be in the non-port-fast state. It will always wait for the forward-time delay to change to the forwarding state. • **Edge** - The port will directly change to the spanning-tree forwarding state when a link-up occurs without waiting for the forward-time delay. If the interface receives a BPDU later, its operation state changes to the non-port-fast state.

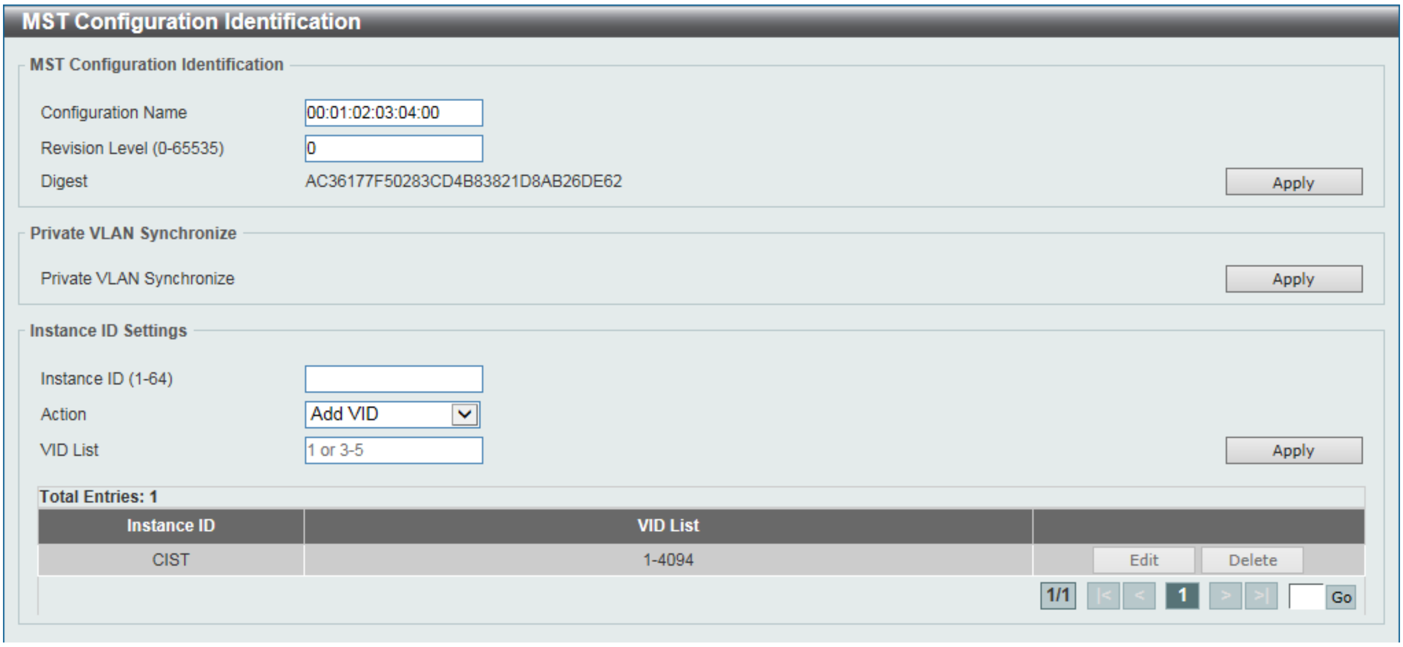
Parameter	Description
TCN Filter	Select to enable or disable the TCN Filter option. When a port is set to the TCN filter mode, the TC event received by the port will be ignored. By default, this option is disabled.
BPDU Forward	Select to enable or disable BPDU forwarding. If enabled, the received STP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

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

MST Configuration Identification

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

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



MST Configuration Identification

MST Configuration Identification

Configuration Name: 00:01:02:03:04:00

Revision Level (0-65535): 0

Digest: AC36177F50283CD4B83821D8AB26DE62

Private VLAN Synchronize

Private VLAN Synchronize

Instance ID Settings

Instance ID (1-64):

Action: Add VID

VID List: 1 or 3-5

Total Entries: 1

Instance ID	VID List	
CIST	1-4094	Edit Delete

Figure 5-48 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. The range is from 0 to 65535. By default, this value is 0. This value, along with the Configuration Name, identifies the MSTP region configured on the Switch.

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

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. The range is from 1 to 64.
Action	Select the action that will be taken here. Options to choose from are **Add VID** and **Remove VID**.
VID List	Enter the VID list value here. This field is used to specify the VID range from configured VLANs set on the Switch.

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

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

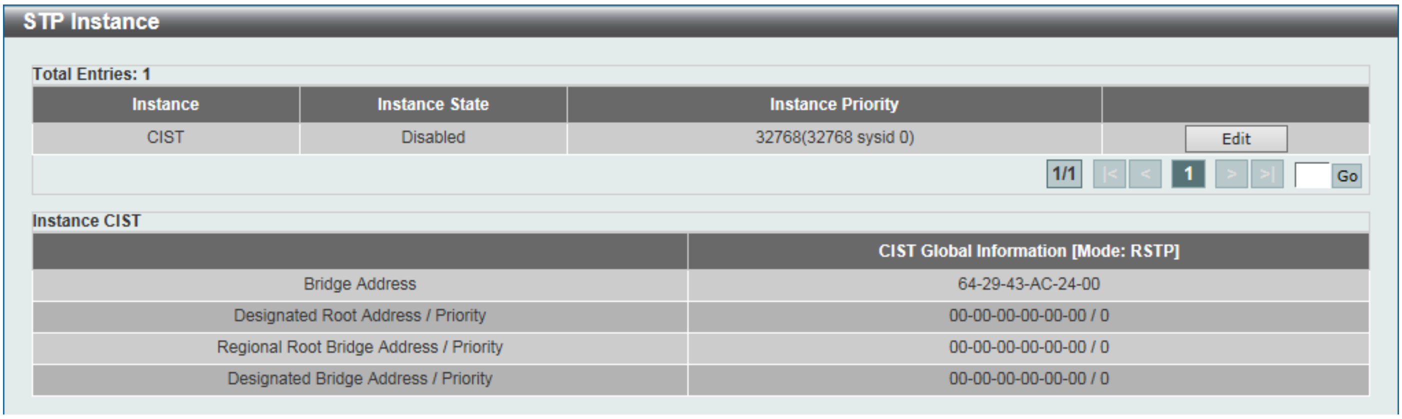
Click the **Delete** button to remove the specific entry.

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

STP Instance

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

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



STP Instance

Total Entries: 1

Instance	Instance State	Instance Priority	
CIST	Disabled	32768(32768 sysid 0)	Edit

Instance CIST

	CIST Global Information [Mode: RSTP]
Bridge Address	64-29-43-AC-24-00
Designated Root Address / Priority	00-00-00-00-00-00 / 0
Regional Root Bridge Address / Priority	00-00-00-00-00-00 / 0
Designated Bridge Address / Priority	00-00-00-00-00-00 / 0

Figure 5-49 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.

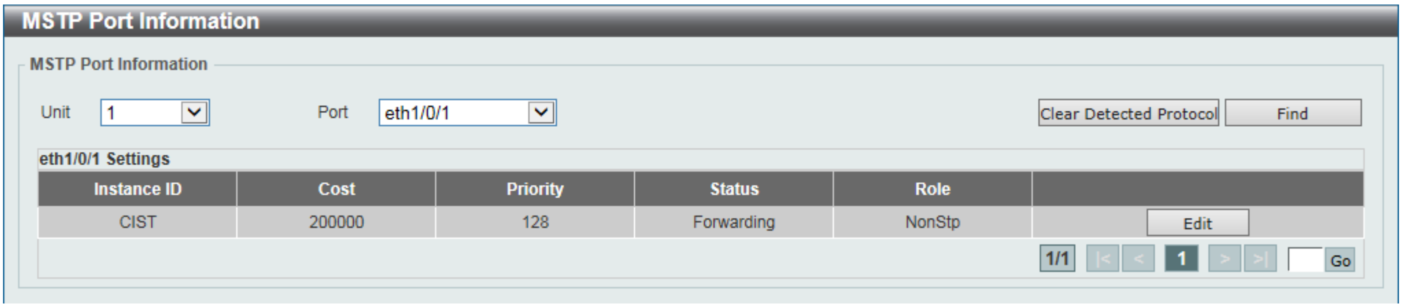
Click the **Apply** button to accept the changes made.

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:



MSTP Port Information

MSTP Port Information

Unit: 1 Port: eth1/0/1

eth1/0/1 Settings

Instance ID	Cost	Priority	Status	Role	
CIST	200000	128	Forwarding	NonStp	Edit

Figure 5-50 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.
Port	Select the port number that will be cleared here.
Cost	After clicking the **Edit** button, enter the cost value here. The range is from 1 to 200000000.
Priority	After clicking the **Edit** button, select the priority value here. Options to choose from are 0 to 240. By default, this value is 128. 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 protection for Ethernet traffic in a ring topology. It ensures that there are no loops formed at the Ethernet layer.

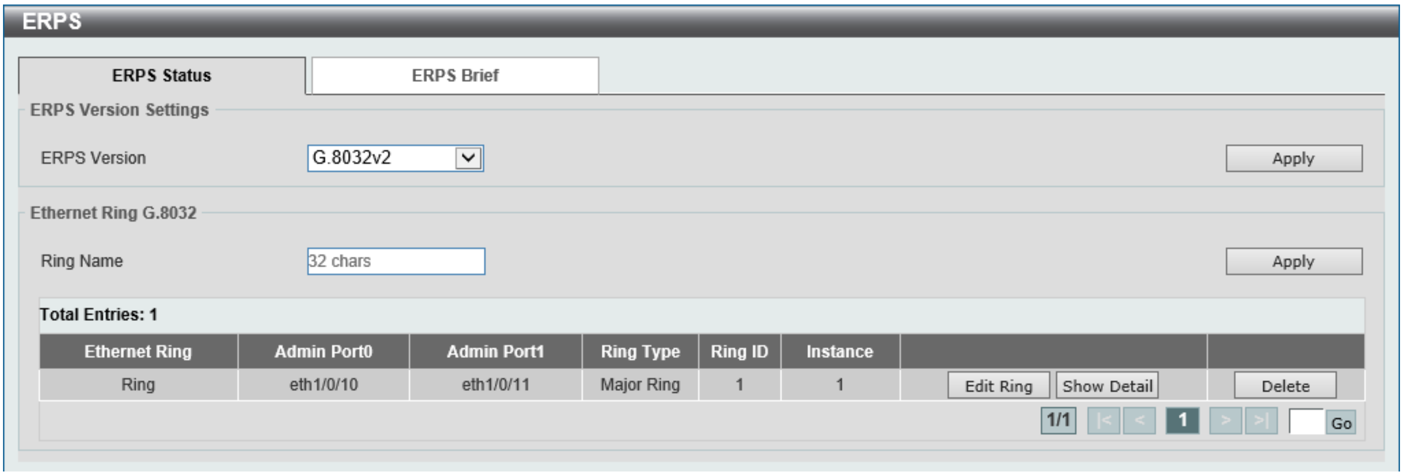
One link within a ring will be blocked to avoid a Loop (RPL, Ring Protection Link). When the failure happens, protection switching blocks the failed link and unblocks the RPL. When the failure clears, protection switching blocks the RPL again and unblocks the link on which the failure is cleared.

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** and select the **ERPS Status** tab, as shown below:



ERPS Version Settings

ERPS Version: G.8032v2

Ethernet Ring G.8032

Ring Name: 32 chars

Total Entries: 1

Ethernet Ring	Admin Port0	Admin Port1	Ring Type	Ring ID	Instance		
Ring	eth1/0/10	eth1/0/11	Major Ring	1	1	Edit Ring Show Detail	Delete

Figure 5-51 ERPS Window

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

Parameter	Description
ERPS Version	Select the ERPS version here. Options to choose from are **G.8032v1** and **G.8032v2**. 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. Before specifying G.8032v1 for a G.8032v2-running device, delete all ERPS configurations that G.8032v1 does not support. Otherwise, the version cannot be changed. Changing the ERPS version will lead to the restart of the running protocol. The following configurations will check when to change from G.8032v2 to G.8032v1: • Manual switch or force switch command will be cleared. • The major ring instance and sub-ring instance of the interconnection node must have different R-APS VLAN IDs. • In a physical ring, only one instance is supported. 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.

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.

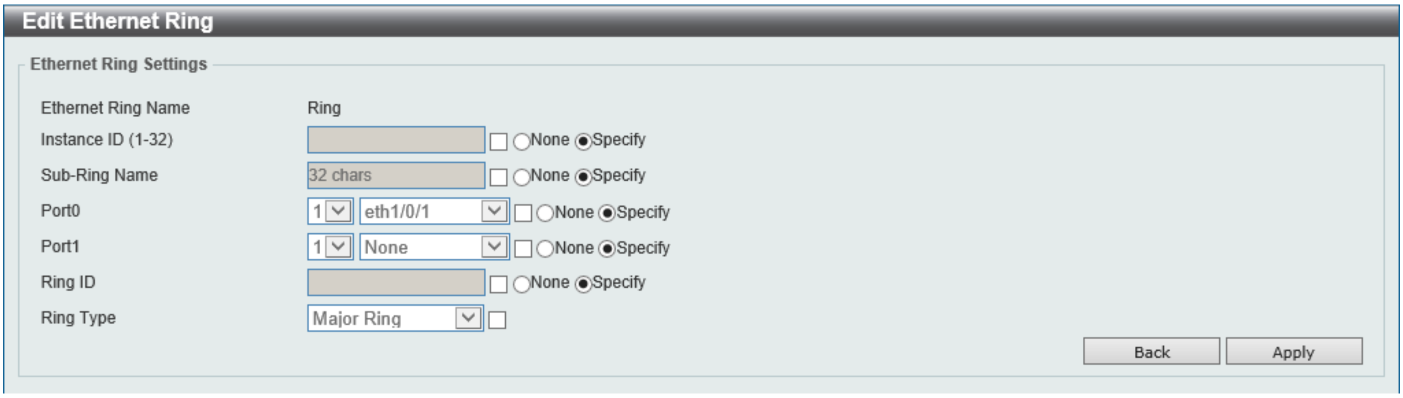
Click the **Edit Ring** button to modify an ITU-T G.8032 ERP physical ring.

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.



Edit Ethernet Ring

Ethernet Ring Settings

Ethernet Ring Name	Ring
Instance ID (1-32)	□ ○None ●Specify
Sub-Ring Name	32 chars □ ○None ●Specify
Port0	1 eth1/0/1 □ ○None ●Specify
Port1	1 None □ ○None ●Specify
Ring ID	□ ○None ●Specify
Ring Type	Major Ring □

Figure 5-52 ERPS (Edit Ring) Window

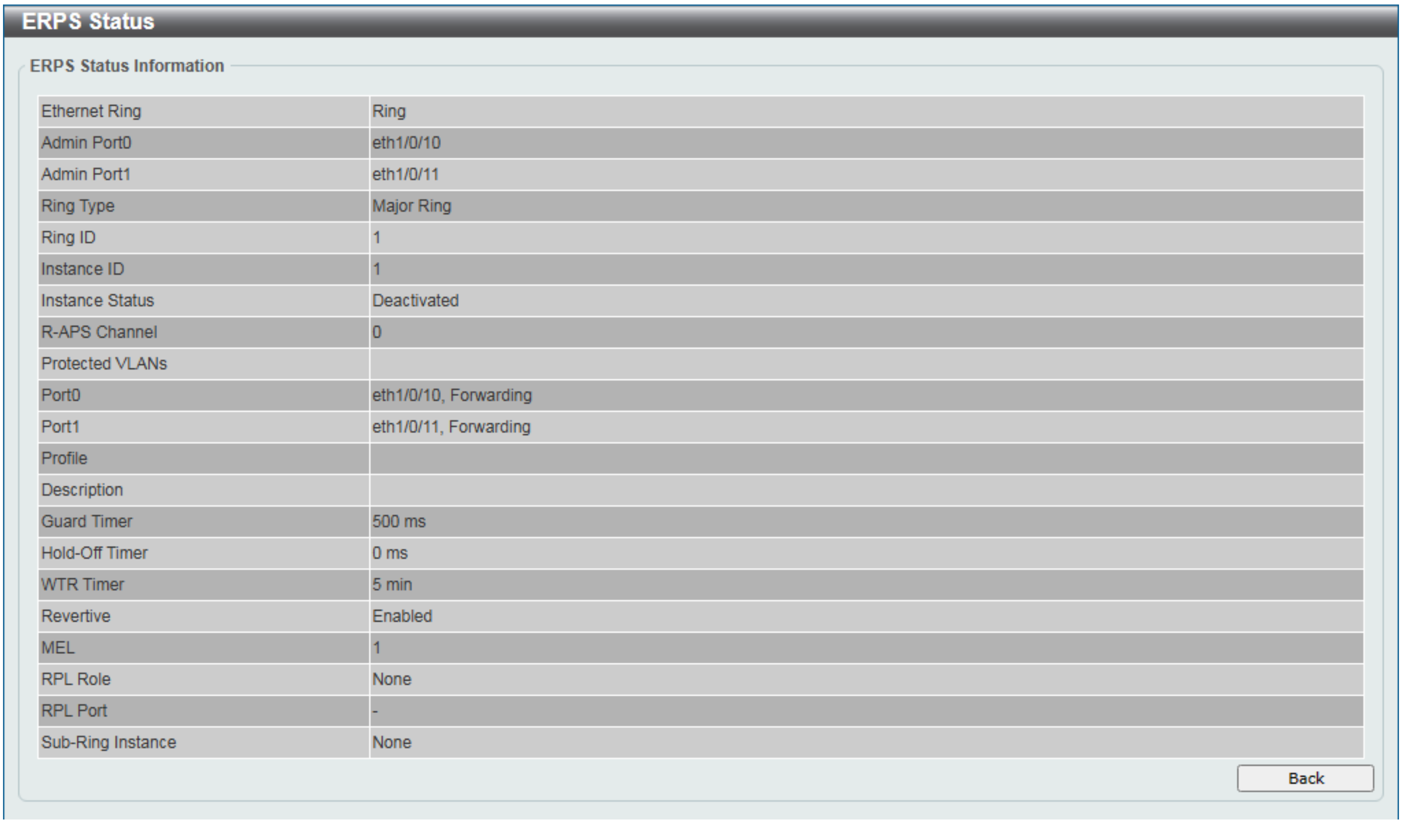
The fields that can be configured are described below:

Parameter	Description
Instance ID	Select the checkbox and enter the ERP instance number here. The range is from 1 to 32. Select the **None** radio button to revert this parameter to the default setting. Select the **Specify** radio button to configure this parameter as normal.
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 **None** radio button to revert this parameter to the default setting. Select the **Specify** radio button to configure this parameter as normal.
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 **None** radio button to revert this parameter to the default setting. Select the **Specify** radio button to configure this parameter as normal.
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 **None** radio button to revert this parameter to the default setting. Select the **Specify** radio button to configure this parameter as normal.
Ring ID	Select the checkbox and enter the ring ID here. The range is from 1 to 239. Select the **None** radio button to revert this parameter to the default setting. Select the **Specify** radio button to configure this parameter as normal.
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.



ERPS Status

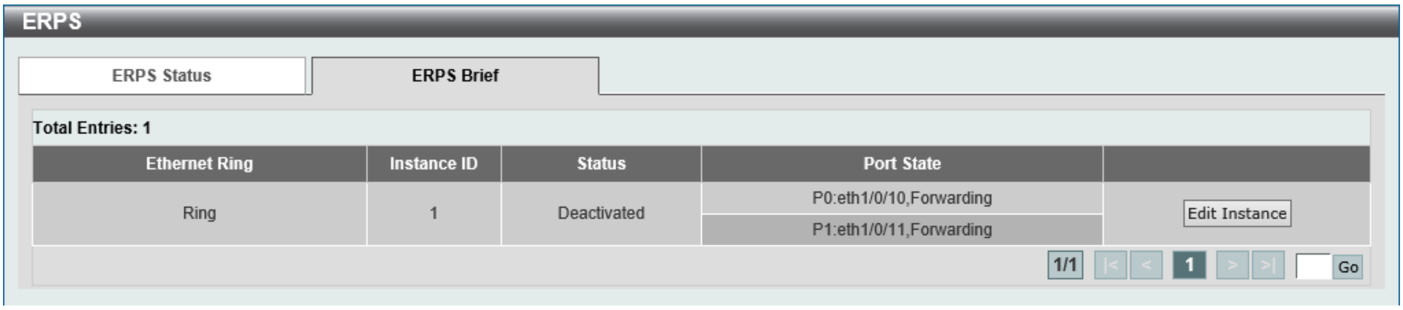
ERPS Status Information

Ethernet Ring	Ring
Admin Port0	eth1/0/10
Admin Port1	eth1/0/11
Ring Type	Major Ring
Ring ID	1
Instance ID	1
Instance Status	Deactivated
R-APS Channel	0
Protected VLANs	
Port0	eth1/0/10, Forwarding
Port1	eth1/0/11, Forwarding
Profile	
Description	
Guard Timer	500 ms
Hold-Off Timer	0 ms
WTR Timer	5 min
Revertive	Enabled
MEL	1
RPL Role	None
RPL Port	-
Sub-Ring Instance	None

Figure 5-53 ERPS (View Detail) Window

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

To view the following window, select the **ERPS Brief** tab, as shown below:



ERPS

Total Entries: 1

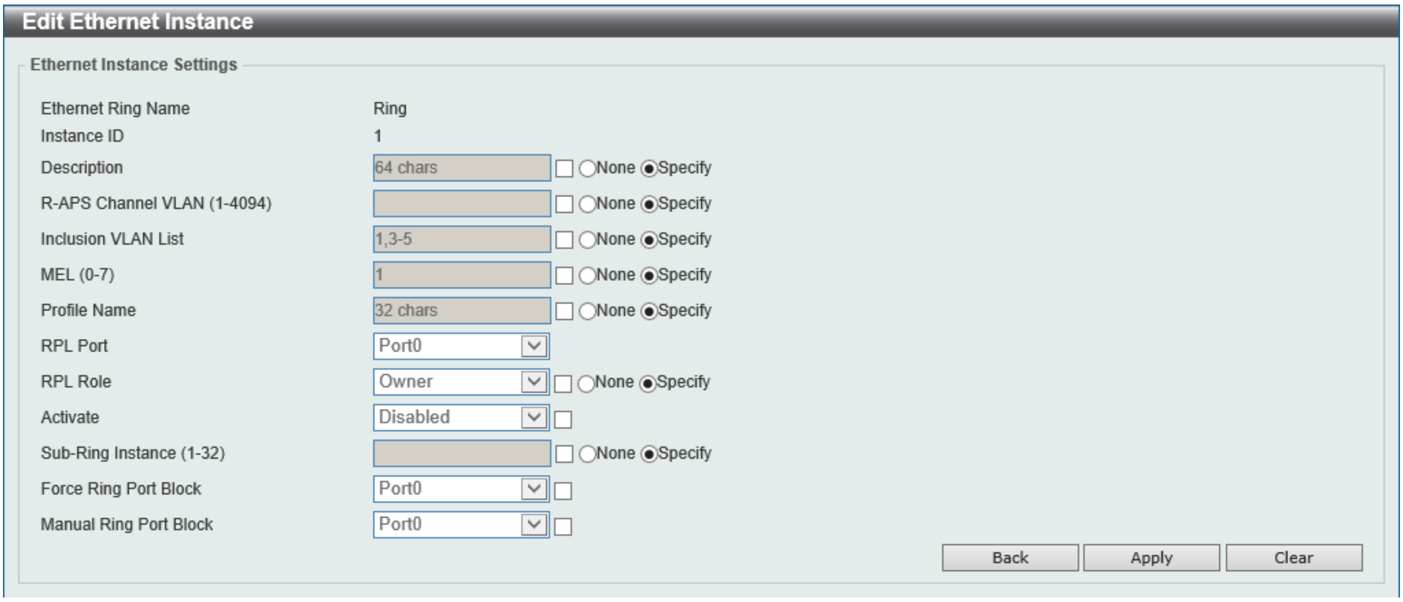
Ethernet Ring	Instance ID	Status	Port State	
Ring	1	Deactivated	P0:eth1/0/10,Forwarding P1:eth1/0/11,Forwarding	Edit Instance

Figure 5-54 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.



Edit Ethernet Instance

Ethernet Instance Settings

Ethernet Ring Name	Ring
Instance ID	1
Description	64 chars □ ○None ●Specify
R-APS Channel VLAN (1-4094)	□ ○None ●Specify
Inclusion VLAN List	1,3-5 □ ○None ●Specify
MEL (0-7)	1 □ ○None ●Specify
Profile Name	32 chars □ ○None ●Specify
RPL Port	Port0
RPL Role	Owner □ ○None ●Specify
Activate	Disabled □
Sub-Ring Instance (1-32)	□ ○None ●Specify
Force Ring Port Block	Port0 □
Manual Ring Port Block	Port0 □

Figure 5-55 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 **None** radio button to revert this parameter to the default setting. Select the **Specify** radio button to configure this parameter as normal.
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. The range is from 1 to 4094. Select the **None** radio button to revert this parameter to the default setting. Select the **Specify** radio button to configure this parameter as per normal.
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 **None** radio button to revert this parameter to the default setting. Select the **Specify** radio button to configure this parameter as normal.
MEL	Select the checkbox and enter the ring MEL value of the ERP instance here. The range is from 0 to 7. The configured MEL value of all ring nodes that participate in the same ERP instance should be identical. Select the **None** radio button to revert this parameter to the default setting. Select the **Specify** radio button to configure this parameter as normal.
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 **None** radio button to revert this parameter to the default setting. Select the **Specify** radio button to configure this parameter as normal.
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.
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 **None** radio button to revert this parameter to the default setting.

Parameter	Description
	Select the **Specify** radio button to configure this parameter as normal.
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 **None** radio button to revert this parameter to the default setting. Select the **Specify** radio button to configure this parameter as normal.
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.

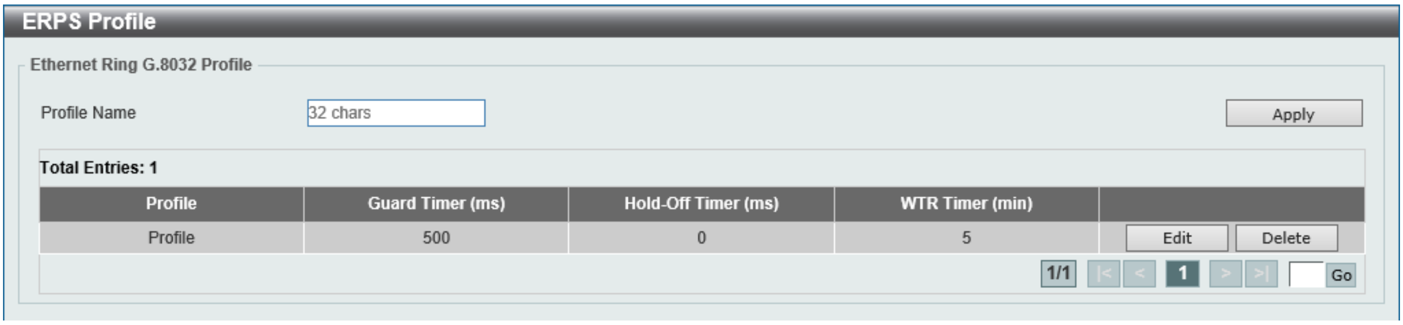
Click the **Apply** button to accept the changes made.

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:



ERPS Profile

Ethernet Ring G.8032 Profile

Profile Name: 32 chars

Total Entries: 1

Profile	Guard Timer (ms)	Hold-Off Timer (ms)	WTR Timer (min)	
Profile	500	0	5	Edit Delete

Figure 5-56 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.

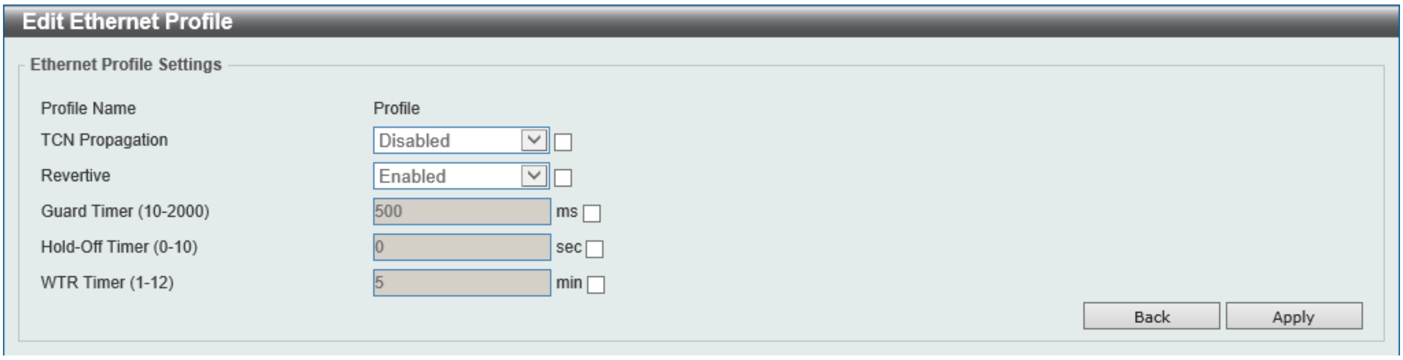
Click the **Apply** button to associate the G.8032 profile with the ERP instance created.

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.



Edit Ethernet Profile

Ethernet Profile Settings

Profile Name	Profile	
TCN Propagation	Disabled	□
Revertive	Enabled	□
Guard Timer (10-2000)	500	ms □
Hold-Off Timer (0-10)	0	sec □
WTR Timer (1-12)	5	min □

Figure 5-57 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. The range is from 10 to 2000 milliseconds. By default, this value is 500 milliseconds.
Hold-Off Timer	Select the checkbox and enter hold-off timer value here. The range is from 0 to 10 seconds. By default, this value is 0 seconds.
WTR Timer	Select the checkbox and enter the Wait To Restore (WTR) timer value here. The range is from 1 to 12 minutes. By default, this value is 5 minutes.

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

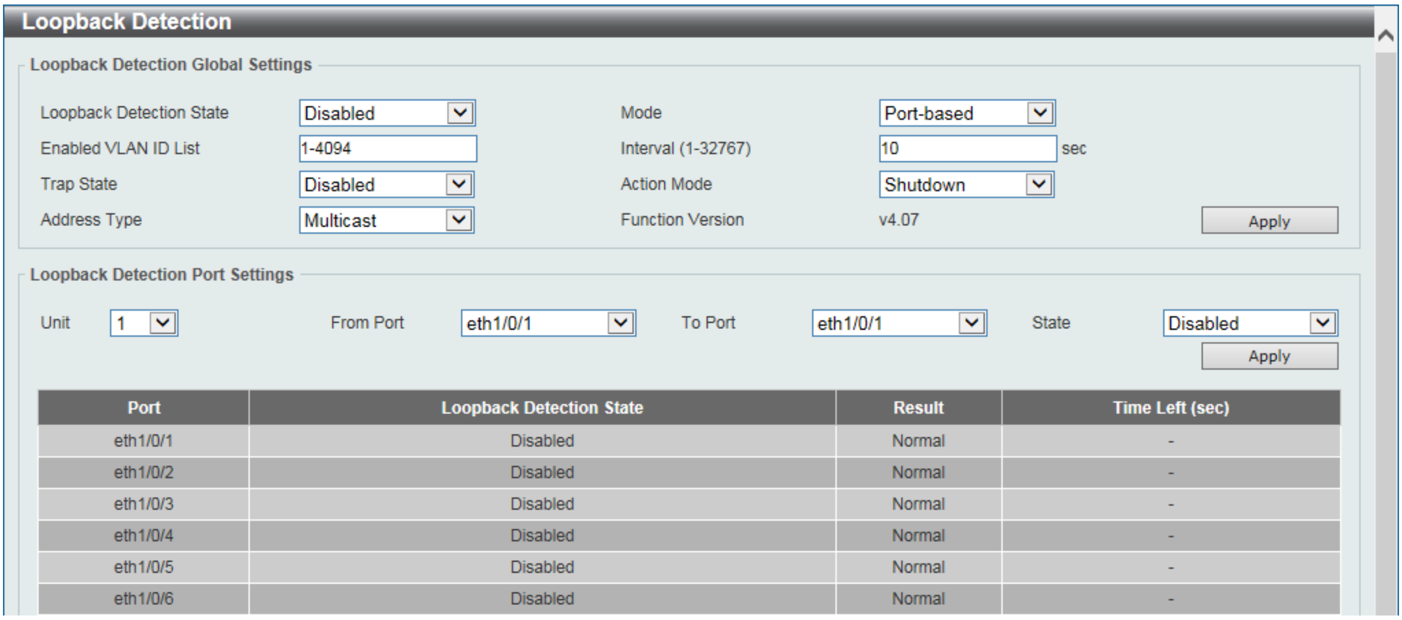
Click the **Apply** button to accept the changes made.

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:



Loopback Detection

Loopback Detection Global Settings

Loopback Detection State	Disabled	Mode	Port-based
Enabled VLAN ID List	1-4094	Interval (1-32767)	10 sec
Trap State	Disabled	Action Mode	Shutdown
Address Type	Multicast	Function Version	v4.07

Loopback Detection Port Settings

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

Port	Loopback Detection State	Result	Time Left (sec)
eth1/0/1	Disabled	Normal	-
eth1/0/2	Disabled	Normal	-
eth1/0/3	Disabled	Normal	-
eth1/0/4	Disabled	Normal	-
eth1/0/5	Disabled	Normal	-
eth1/0/6	Disabled	Normal	-

Figure 5-58 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. By default, this option is disabled.
Mode	Select the loopback detection mode. Options to choose from are **Port-based** and **VLAN-based**.
Enabled VLAN ID List	Enter the VLAN ID for loop detection. This only takes effect when **VLAN-based** is selected in the **Mode** drop-down list.
Interval	Enter the interval in seconds that the device will use to transmit Configuration Test Protocol (CTP) packets to detect a loopback event. The range is from 1 to 32767 seconds. By default, this value 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**.

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.
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.

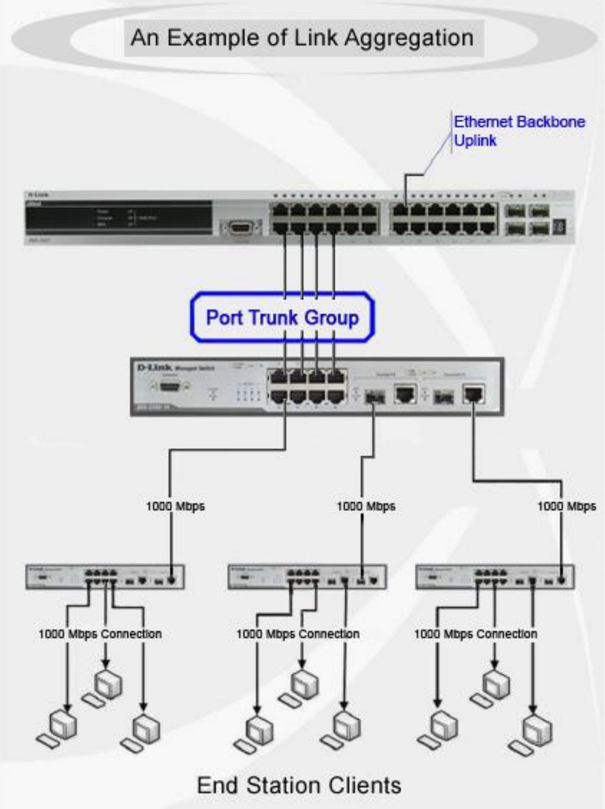


Figure 5-59 Example of Port Trunk Group

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.

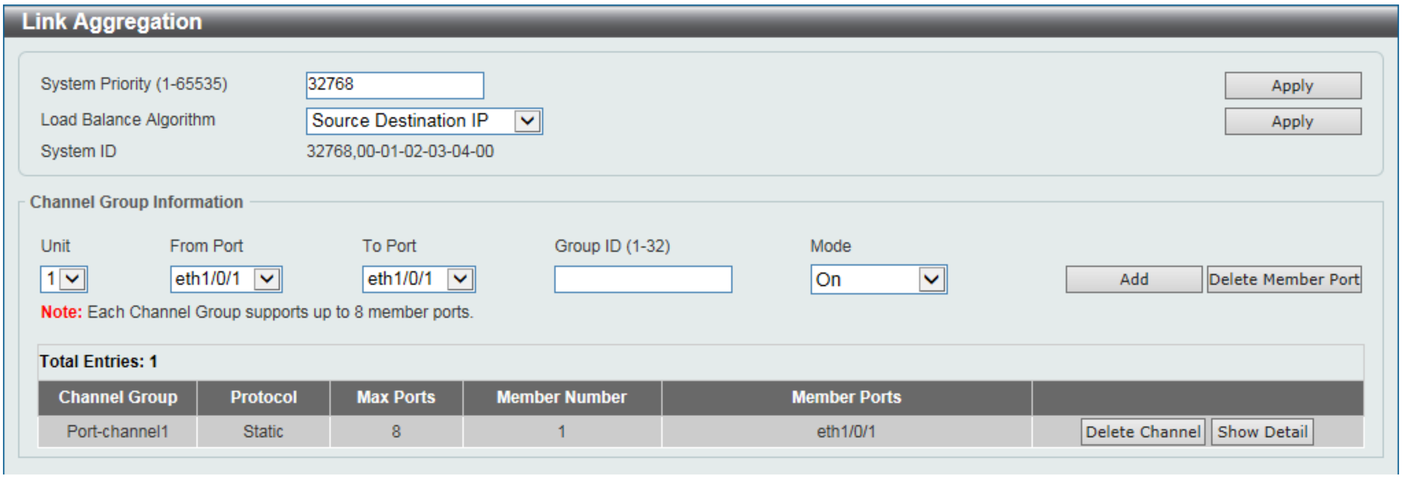
Link aggregation allows several ports to be grouped together and to act as a single link. This results in a bandwidth that is a multiple of a single link's bandwidth. Link aggregation is most commonly used to link bandwidth intensive network devices, such as servers, to the backbone of a network.

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:



Link Aggregation

System Priority (1-65535): 32768

Load Balance Algorithm: Source Destination IP

System ID: 32768,00-01-02-03-04-00

Channel Group Information

Unit: 1 | From Port: eth1/0/1 | To Port: eth1/0/1 | Group ID (1-32): | Mode: On

Note: Each Channel Group supports up to 8 member ports.

Total Entries: 1

Channel Group	Protocol	Max Ports	Member Number	Member Ports	
Port-channel1	Static	8	1	eth1/0/1	Delete Channel Show Detail

Figure 5-60 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. The range is from 1 to 65535. By default, this value is 32768. The system priority determines which ports can join a port-channel and which ports are put in the stand-alone mode. The lower value has a higher priority. If two or more ports have the same priority, the port number determines the priority.
Load Balance Algorithm	Select the load-balancing algorithm that will be used here. Options to choose from are **Source MAC**, **Destination MAC**, **Source Destination MAC**, **Source IP**, **Destination IP**, and **Source Destination IP**. By default, the **Source Destination IP** option is used.

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.
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. The range is from 1 to 32. The system will automatically create the port-channel when a physical port first joins a channel group. An interface can only join one channel-group.
Mode	Select the mode option here. Options to choose from are **On**, **Active**, and **Passive**. If the mode **On** is specified, the channel group type is static. If the mode **Active** or **Passive** is specified, the channel group type is LACP. A channel group can only consist of either static members or LACP members. Once the type of channel group has been determined, other types of interfaces cannot join the channel group.

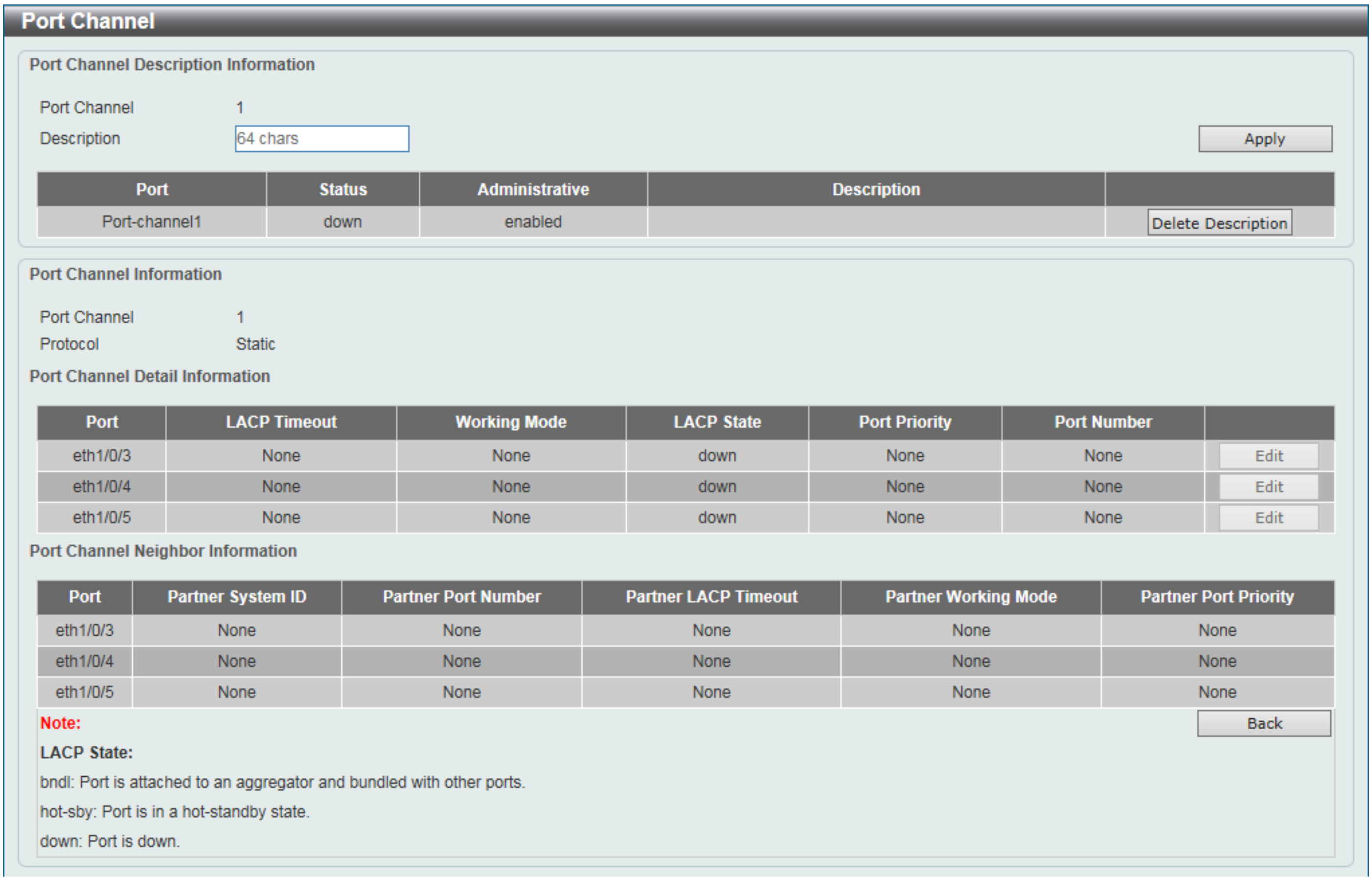
Click the **Add** button to add a new channel group.

Click the **Delete Member Port** button, to delete the member port(s) specified from the group.

Click the **Delete Channel** button to delete the specified channel group.

Click the **Show Detail** button to view detailed information about the channel.

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



Port Channel

Port Channel Description Information

Port Channel 1

Description 64 chars

Port	Status	Administrative	Description	
Port-channel1	down	enabled		Delete Description

Port Channel Information

Port Channel 1

Protocol Static

Port Channel Detail Information

Port	LACP Timeout	Working Mode	LACP State	Port Priority	Port Number	
eth1/0/3	None	None	down	None	None	Edit
eth1/0/4	None	None	down	None	None	Edit
eth1/0/5	None	None	down	None	None	Edit

Port Channel Neighbor Information

Port	Partner System ID	Partner Port Number	Partner LACP Timeout	Partner Working Mode	Partner Port Priority
eth1/0/3	None	None	None	None	None
eth1/0/4	None	None	None	None	None
eth1/0/5	None	None	None	None	None

Note:

LACP State:

bndl: Port is attached to an aggregator and bundled with other ports.

hot-sby: Port is in a hot-standby state.

down: Port is down.

Figure 5-61 Link Aggregation (Channel 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.

After clicking the **Edit** button, the fields that can be configured are described below:

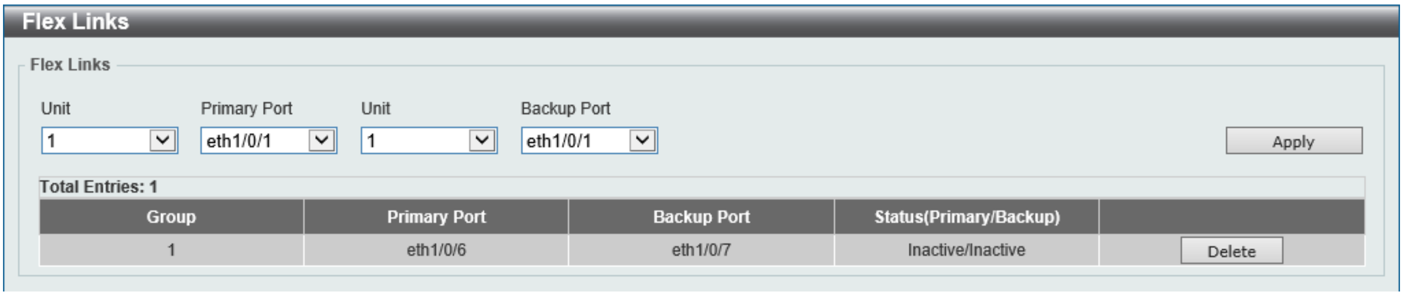
Parameter	Description
LACP Timeout	Select the LACP timeout here. Options to choose from are **Short** and **Long**.
Working Mode	Select the working mode here. Options to choose from are **Active** and **Passive**.
Port Priority	Enter the port priority value here.

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

Flex Links

This window is used to display and configure the Flex Link feature. Flex Links belong to a pair of Layer 2 interfaces where one interface is configured to act as a backup to the other. Flex Links provide link-level redundancy as an alternative to STP and LBD.

To view the following window, click **L2 Features > Flex Links**, as shown below:



Flex Links

Flex Links

Unit: 1 | Primary Port: eth1/0/1 | Unit: 1 | Backup Port: eth1/0/1

Total Entries: 1

Group	Primary Port	Backup Port	Status(Primary/Backup)	
1	eth1/0/6	eth1/0/7	Inactive/Inactive	Delete

Figure 5-62 L2 Flex Links Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit of the primary port here.
Primary Port	Select the primary port here.
Unit	Select the Switch unit of the backup port here.
Backup Port	Select the backup port here.

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

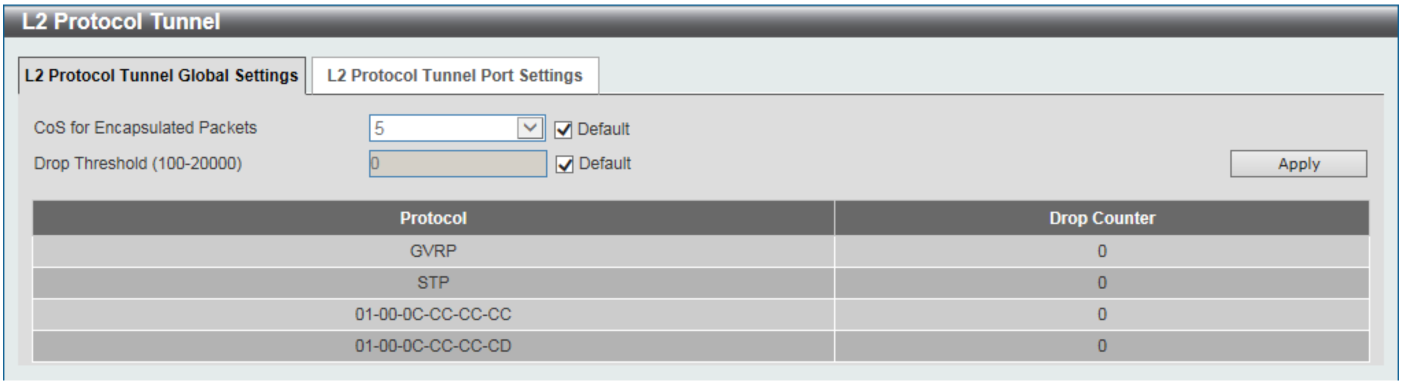
Click the **Delete** button to remove the specific entry.

NOTE: Flex Link and STP, ERPS and LBD are mutually exclusive.

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** and select the **L2 Protocol Tunnel Global Settings** tab, as shown below:



L2 Protocol Tunnel

L2 Protocol Tunnel Global Settings
L2 Protocol Tunnel Port Settings

CoS for Encapsulated Packets: 5 ☑ Default

Drop Threshold (100-20000): 0 ☑ Default

Protocol	Drop Counter
GVRP	0
STP	0
01-00-0C-CC-CC-CC	0
01-00-0C-CC-CC-CD	0

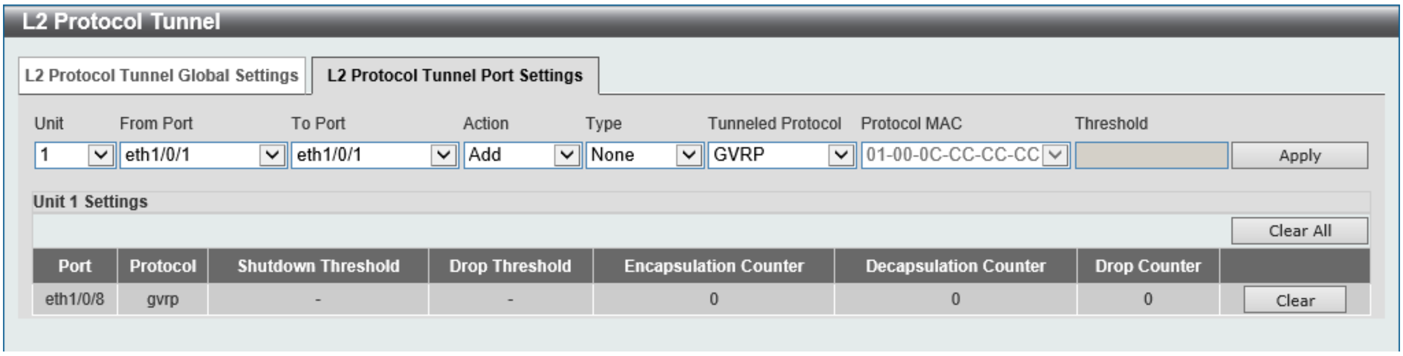
Figure 5-63 L2 Protocol Tunnel (L2 Protocol Tunnel Global Setting) Window

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.

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

To view the following window, select the **L2 Protocol Tunnel Port Setting** tab, as shown below:



L2 Protocol Tunnel

L2 Protocol Tunnel Global Settings | L2 Protocol Tunnel Port Settings

Unit: 1 | From Port: eth1/0/1 | To Port: eth1/0/1 | Action: Add | Type: None | Tunneled Protocol: GVRP | Protocol MAC: 01-00-0C-CC-CC-CC | Threshold: | Apply

Unit 1 Settings

Clear All

Port	Protocol	Shutdown Threshold	Drop Threshold	Encapsulation Counter	Decapsulation Counter	Drop Counter	
eth1/0/8	gvrp	-	-	0	0	0	Clear

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.
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, the following parameter will be available. Enter the threshold value here. The range is from 1 to 4096.

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

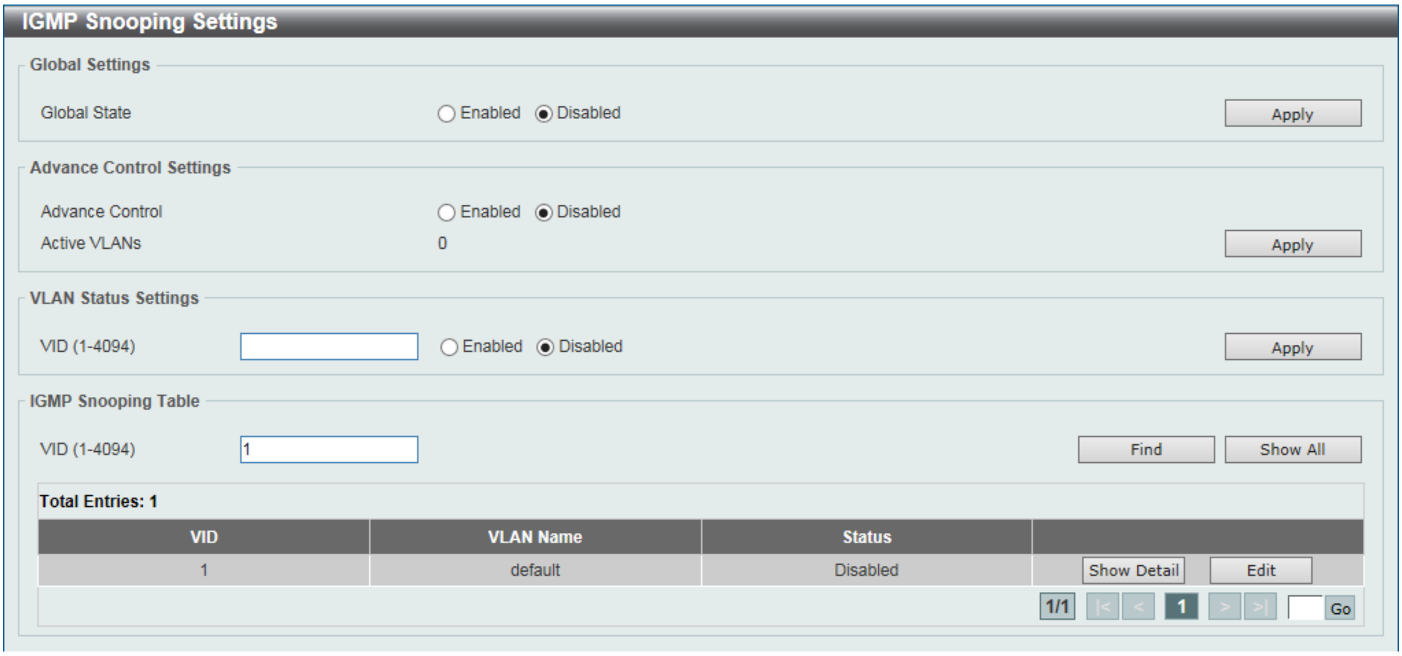
IGMP Snooping

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:



IGMP Snooping Settings

Global Settings

Global State ○ Enabled ● Disabled

Advance Control Settings

Advance Control ○ Enabled ● Disabled

Active VLANs 0

VLAN Status Settings

VID (1-4094) ○ Enabled ● Disabled

IGMP Snooping Table

VID (1-4094) 1

Total Entries: 1

VID	VLAN Name	Status	
1	default	Disabled	Show Detail Edit

1/1

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 **Advanced Control Settings** are described below:

Parameter	Description
Advance Control	Select to enable or disable the IGMP snooping advanced control function.

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 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.

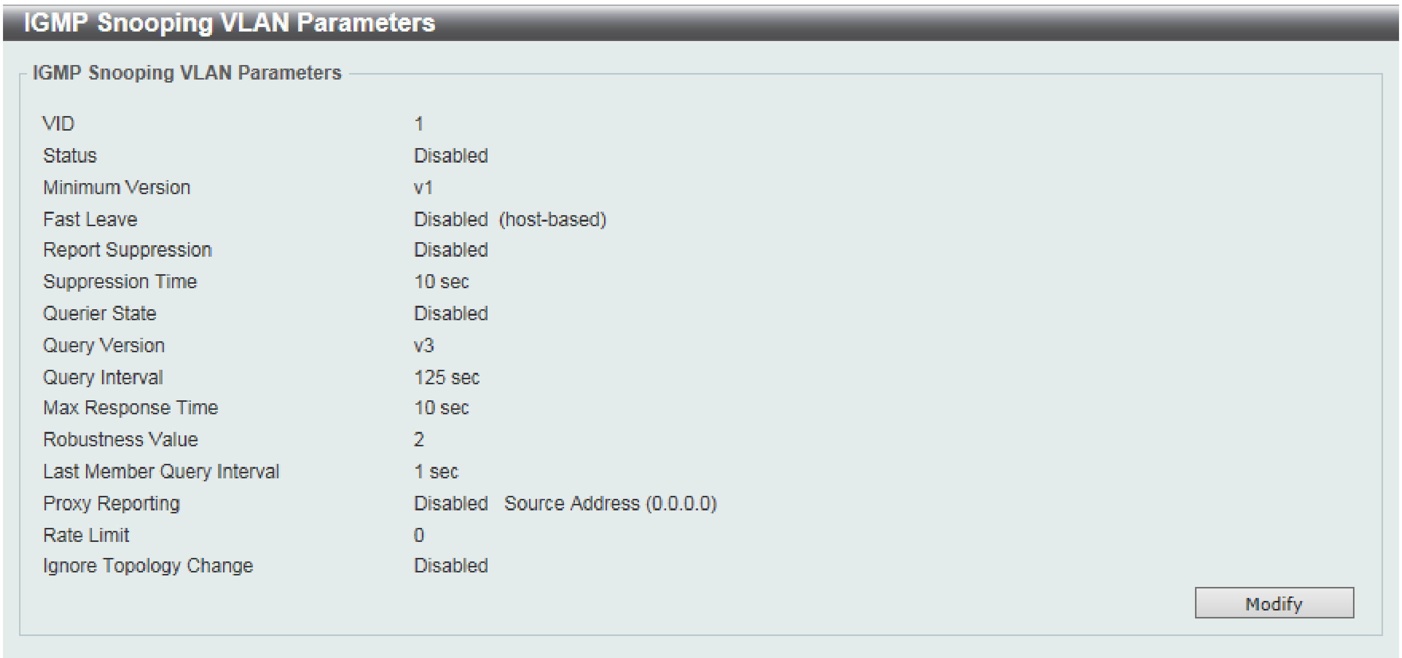
Click the **Show All** button to view all the entries.

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.



IGMP Snooping VLAN Parameters

IGMP Snooping VLAN Parameters

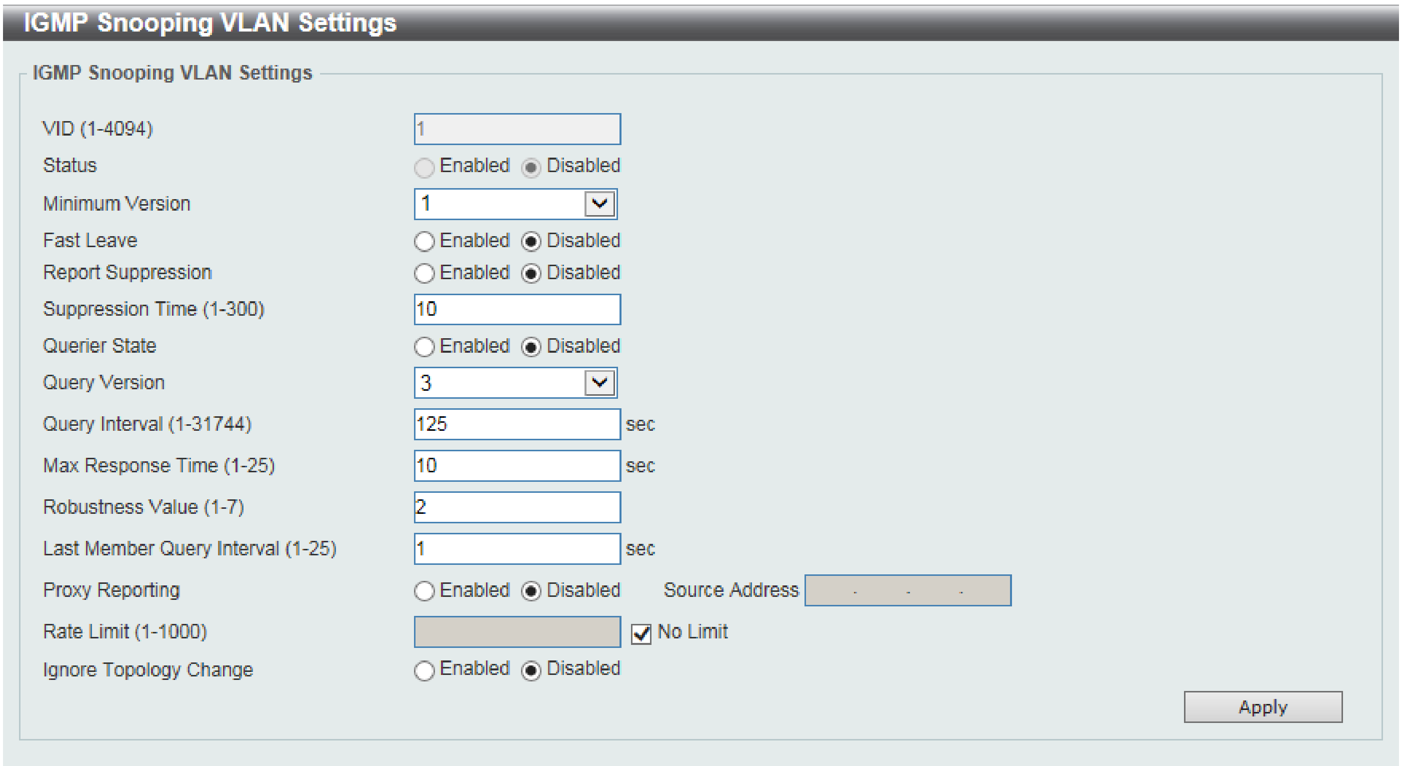
VID	1
Status	Disabled
Minimum Version	v1
Fast Leave	Disabled (host-based)
Report Suppression	Disabled
Suppression Time	10 sec
Querier State	Disabled
Query Version	v3
Query Interval	125 sec
Max Response Time	10 sec
Robustness Value	2
Last Member Query Interval	1 sec
Proxy Reporting	Disabled Source Address (0.0.0.0)
Rate Limit	0
Ignore Topology Change	Disabled

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.



IGMP Snooping VLAN Settings

IGMP Snooping VLAN Settings

VID (1-4094): 1

Status: ○ Enabled ● Disabled

Minimum Version: 1

Fast Leave: ○ Enabled ● Disabled

Report Suppression: ○ Enabled ● Disabled

Suppression Time (1-300): 10

Querier State: ○ Enabled ● Disabled

Query Version: 3

Query Interval (1-31744): 125 sec

Max Response Time (1-25): 10 sec

Robustness Value (1-7): 2

Last Member Query Interval (1-25): 1 sec

Proxy Reporting: ○ Enabled ● Disabled Source Address: . . .

Rate Limit (1-1000): ☑ No Limit

Ignore Topology Change: ○ Enabled ● Disabled

Apply

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 done message from the last member. When fast leave is enabled, the Switch will not generate specific queries. When fast leave is disabled, the Switch will generate specific queries.
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.

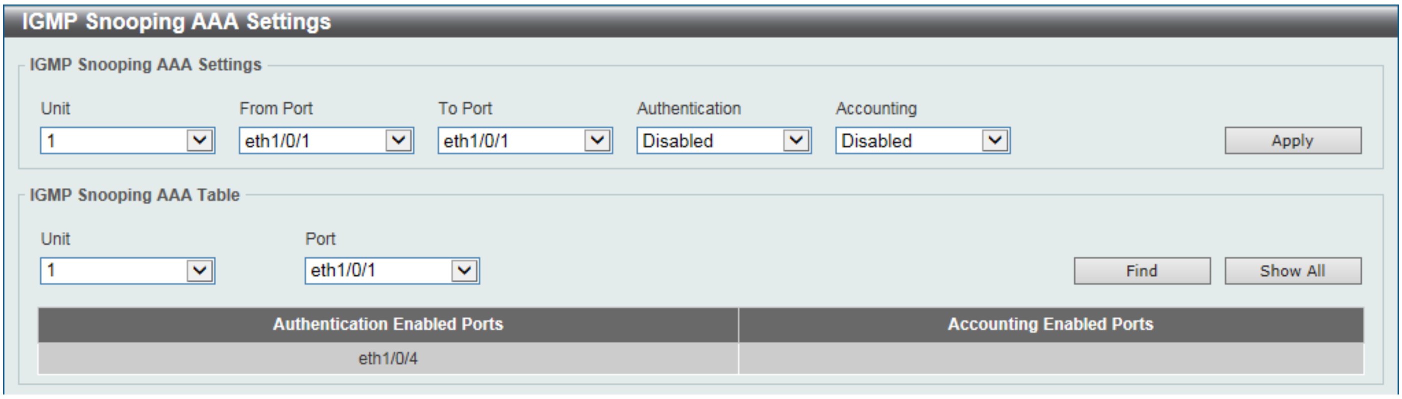
Parameter	Description
Source Address	Enter the source IP of proxy reporting. This is available when **Enabled** is selected in **Proxy Reporting**.
Rate Limit	Enter the rate limit value here. The range is from 1 to 1000. Select the **No Limit** option to apply no rate limit on this profile.
Ignore Topology 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:



IGMP Snooping AAA Settings

IGMP Snooping AAA Settings

Unit: 1; From Port: eth1/0/1; To Port: eth1/0/1; Authentication: Disabled; Accounting: Disabled

IGMP Snooping AAA Table

Unit: 1; Port: eth1/0/1

Authentication Enabled Ports	Accounting Enabled Ports
eth1/0/4	

Figure 5-68 IGMP Snooping AAA Settings Window

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.
From Port - To Port	Select the appropriate port range used for the configuration here.
Authentication	Select to enable or disable authentication function for IGMP join messages.
Accounting	Select to enable or disable accounting when a listener joining an IGMP group.

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 configuration here.
Port	Select to choose the port.

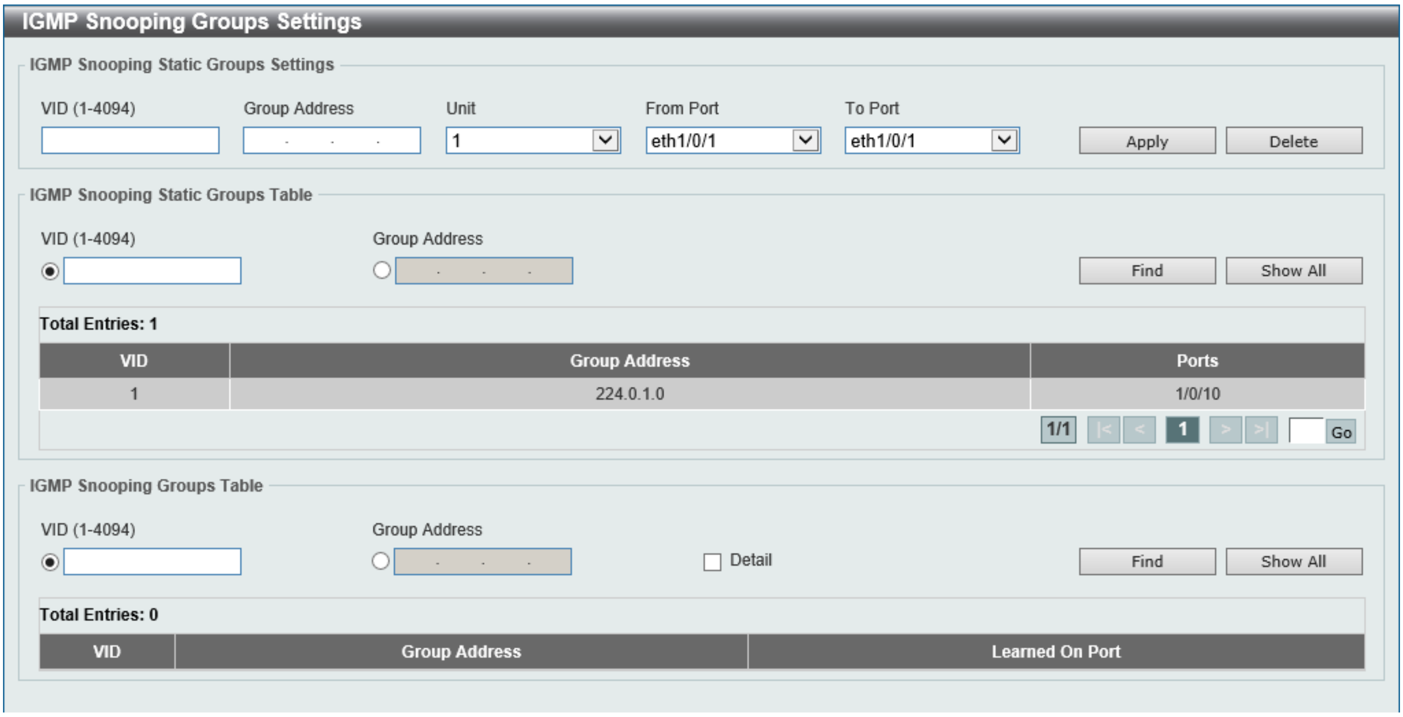
Click the **Find** button to locate a specific entry based on the information entered.

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

IGMP Snooping 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:



IGMP Snooping Groups Settings

IGMP Snooping Static Groups Settings

VID (1-4094) | Group Address | Unit: 1 | From Port: eth1/0/1 | To Port: eth1/0/1 | Apply | Delete

IGMP Snooping Static Groups Table

● VID (1-4094) ○ Group Address | Find | Show All

Total Entries: 1

VID	Group Address	Ports
1	224.0.1.0	1/0/10

1/1 |< < 1 > >| Go

IGMP Snooping Groups Table

● VID (1-4094) ○ Group Address □ Detail | Find | Show All

Total Entries: 0

VID	Group Address	Learned On Port

Figure 5-69 IGMP Snooping Groups Settings Window

The fields that can be configured in **IGMP Snooping Static Groups Settings/Table** 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.
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.
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.

Parameter	Description
Detail	Select this option to display the IGMP snooping group detail information.

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

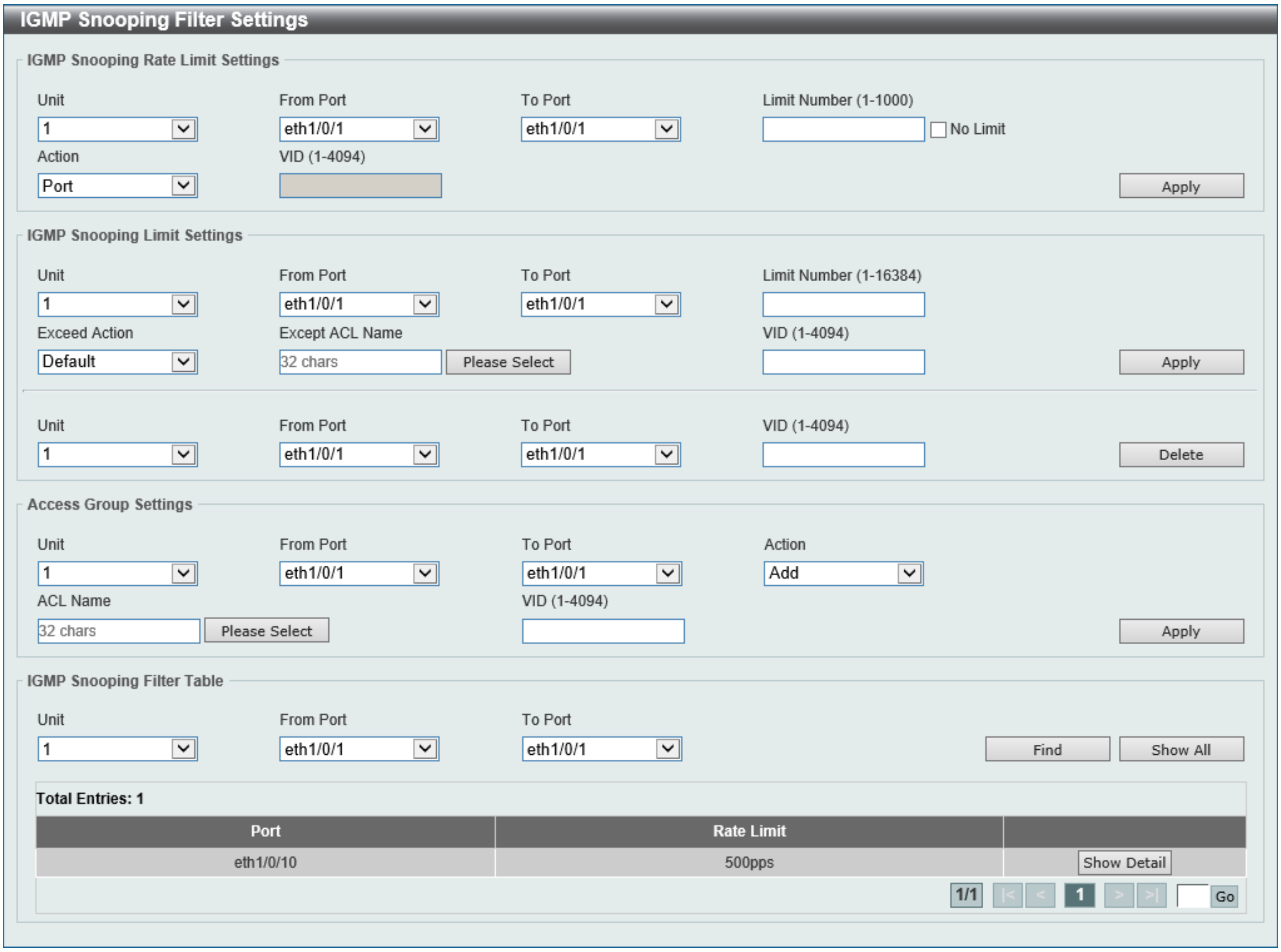
Click the **Show All** button to view all the entries.

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

IGMP Snooping Filter Settings

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

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Filter Settings**, as shown below:



IGMP Snooping Filter Settings

IGMP Snooping Rate Limit Settings

Unit: 1 | From Port: eth1/0/1 | To Port: eth1/0/1 | Limit Number (1-1000): | □ No Limit

Action: Port | VID (1-4094):

IGMP Snooping Limit Settings

Unit: 1 | From Port: eth1/0/1 | To Port: eth1/0/1 | Limit Number (1-16384):

Exceed Action: Default | Except ACL Name: 32 chars | VID (1-4094):

Unit: 1 | From Port: eth1/0/1 | To Port: eth1/0/1 | VID (1-4094):

Access Group Settings

Unit: 1 | From Port: eth1/0/1 | To Port: eth1/0/1 | Action: Add

ACL Name: 32 chars | VID (1-4094):

IGMP Snooping Filter Table

Unit: 1 | From Port: eth1/0/1 | To Port: eth1/0/1

Total Entries: 1

Port	Rate Limit	
eth1/0/10	500pps	Show Detail

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 ID that will be used here.
From Port - To Port	Select the Switch port range that will be used 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. The range is from 1 to 1000 packets per second.

Parameter	Description
	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**.
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 **IGMP Snooping Limit Settings** 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.
Limit Number	Enter the limit number here. This is used to set the limitation on the number of IGMP cache entries that can be created. The range is from 1 to 16384.
Exceed Action	Select the exceed action here. This parameter specifies the action for handling newly learned groups when the limitation is exceeded. Options to choose from are: • **Default** - Specifies that the default action will be taken. • **Drop** - Specifies that the new group will be dropped. • **Replace** - Specifies that the new group will replace the oldest group.
Except ACL Name	Enter the standard IP access list name here. The group (*,G) 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 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.
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 **IGMP Snooping Filter Table** 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.

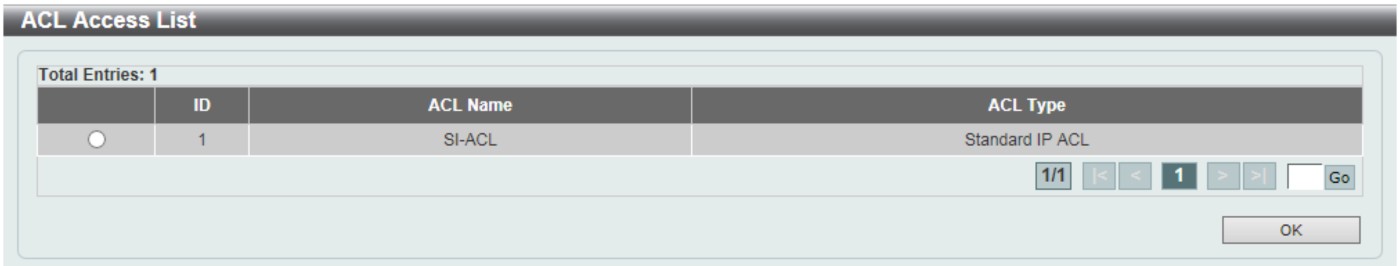
Click the **Find** button to locate a specific entry based on the information entered.

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

Click the **Show Detail** button to view 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 **Please Select** button, the following page will appear.



ACL Access List

Total Entries: 1

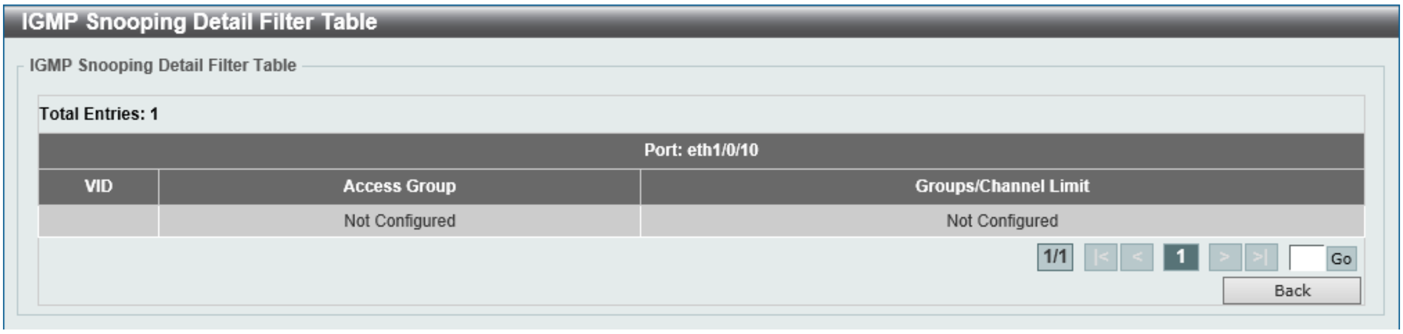
	ID	ACL Name	ACL Type
○	1	SI-ACL	Standard IP ACL

Figure 5-71 IGMP 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 page will appear.



IGMP Snooping Detail Filter Table

IGMP Snooping Detail Filter Table

Total Entries: 1

Port: eth1/0/10

VID	Access Group	Groups/Channel Limit
	Not Configured	Not Configured

Figure 5-72 IGMP Snooping Filter Settings (Show Detail) Window

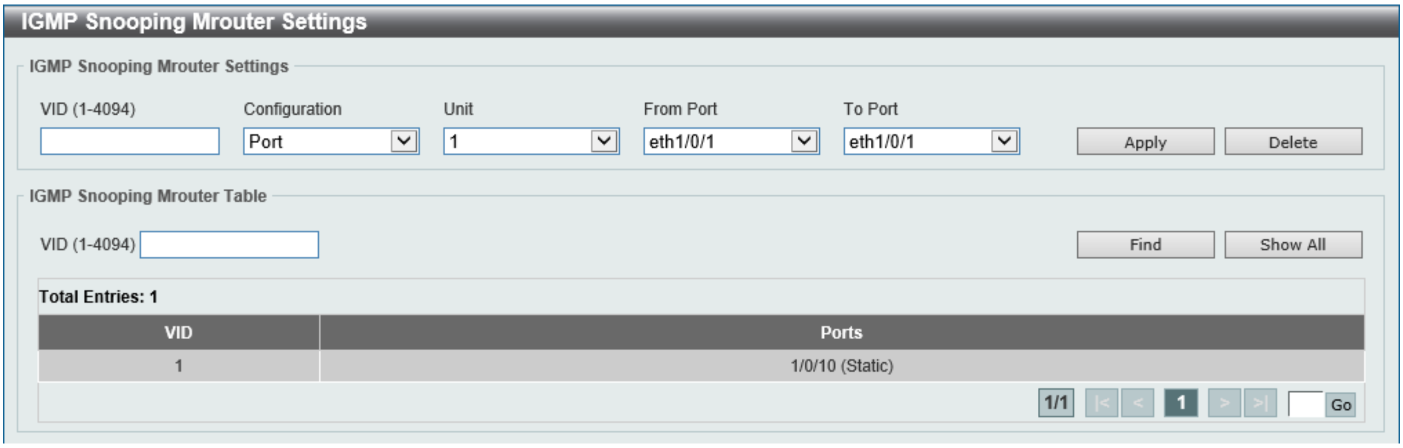
Click the **Back** button to return to the previous window.

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

IGMP Snooping Mrouter Settings

This window is used to display and configure the IGMP Snooping Multicast Router settings.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Mrouter Settings**, as shown below:



IGMP Snooping Mrouter Settings

IGMP Snooping Mrouter Settings

VID (1-4094):
Configuration: Port
Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1

IGMP Snooping Mrouter Table

VID (1-4094):

Total Entries: 1

VID	Ports
1	1/0/10 (Static)

Figure 5-73 IGMP Snooping Mrouter Settings Window

The fields that can be configured in **IGMP Snooping Mrouter Settings** are described below:

Parameter	Description
VID	Enter the VLAN ID used here. The range is from 1 to 4094.
Configuration	Select the port configuration. Options to choose from are: • **Port -** Select to have the configured ports to be static multicast router ports. • **Forbidden Port -** Select to have the configured ports not to be multicast router ports.
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.

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

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

The fields that can be configured in **IGMP Snooping Mrouter Table** are described below:

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

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

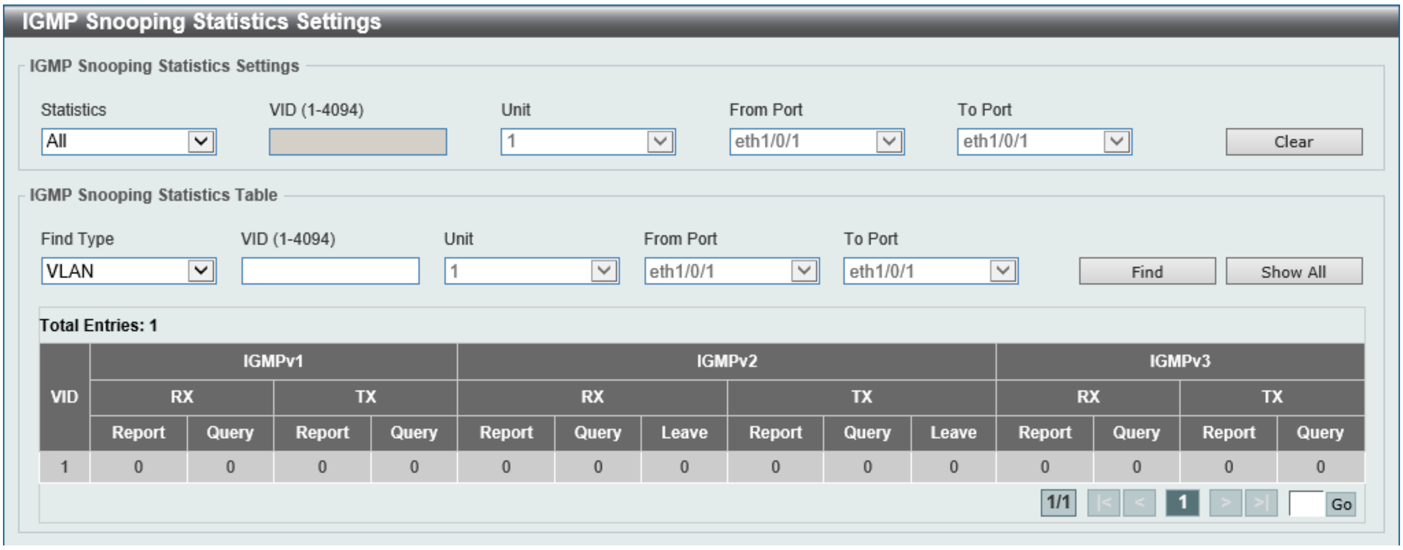
Click the **Show All** button to view all the entries.

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

IGMP Snooping Statistics Settings

This window is used to view and clear the IGMP snooping related statistics.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Statistics Settings**, as shown below:



IGMP Snooping Statistics Settings

IGMP Snooping Statistics Settings

Statistics: All
VID (1-4094):
Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1

IGMP Snooping Statistics Table

Find Type: VLAN
VID (1-4094):
Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1

Total Entries: 1

VID	IGMPv1				IGMPv2						IGMPv3			
	RX		TX		RX			TX			RX		TX	
	Report	Query	Report	Query	Report	Query	Leave	Report	Query	Leave	Report	Query	Report	Query
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 5-74 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.
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 an 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

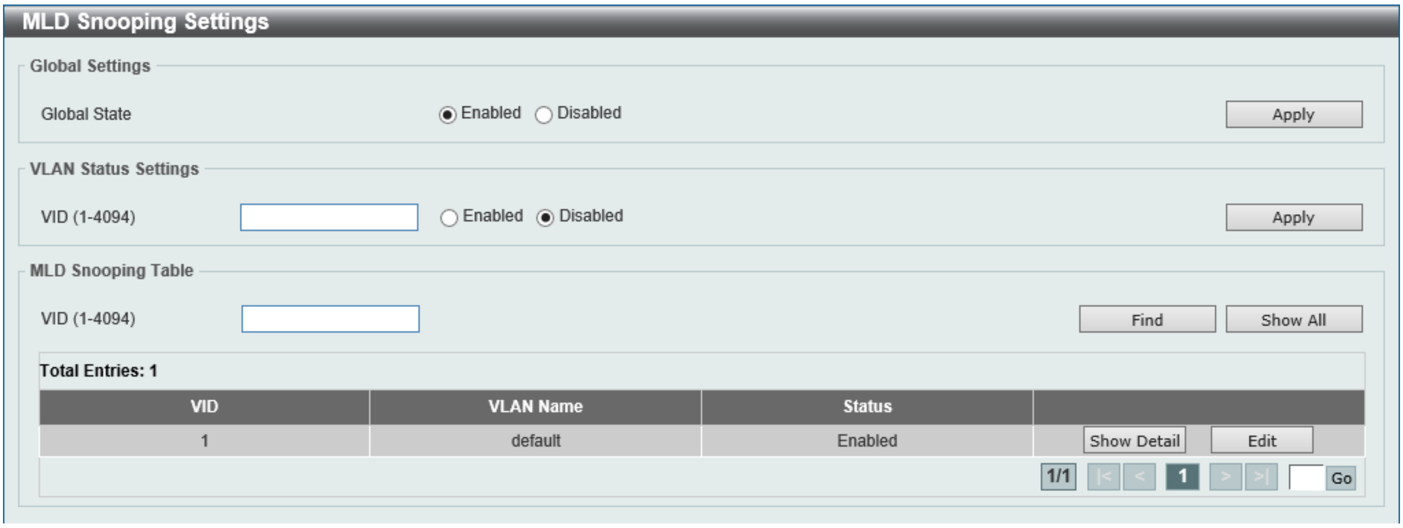
These types of messages are transferred between devices using MLD snooping. These messages are all defined by four ICMPv6 packet headers, labeled 130, 131, 132, and 143.

- **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:



MLD Snooping Settings

Global Settings

Global State ● Enabled ○ Disabled

VLAN Status Settings

VID (1-4094) ○ Enabled ● Disabled

MLD Snooping Table

VID (1-4094)

Total Entries: 1

VID	VLAN Name	Status	
1	default	Enabled	Show Detail Edit

Figure 5-75 MLD Snooping Settings Window

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

Parameter	Description
Global State	Select this option to enable or disable the global MLD snooping state.

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

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

Parameter	Description
VID	Enter a VLAN ID from 1 to 4094, and select to enable or disable MLD snooping on the VLAN.

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

The fields that can be configured in **MLD Snooping Table** are described below:

Parameter	Description
VID	Enter a VLAN ID from 1 to 4094.

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

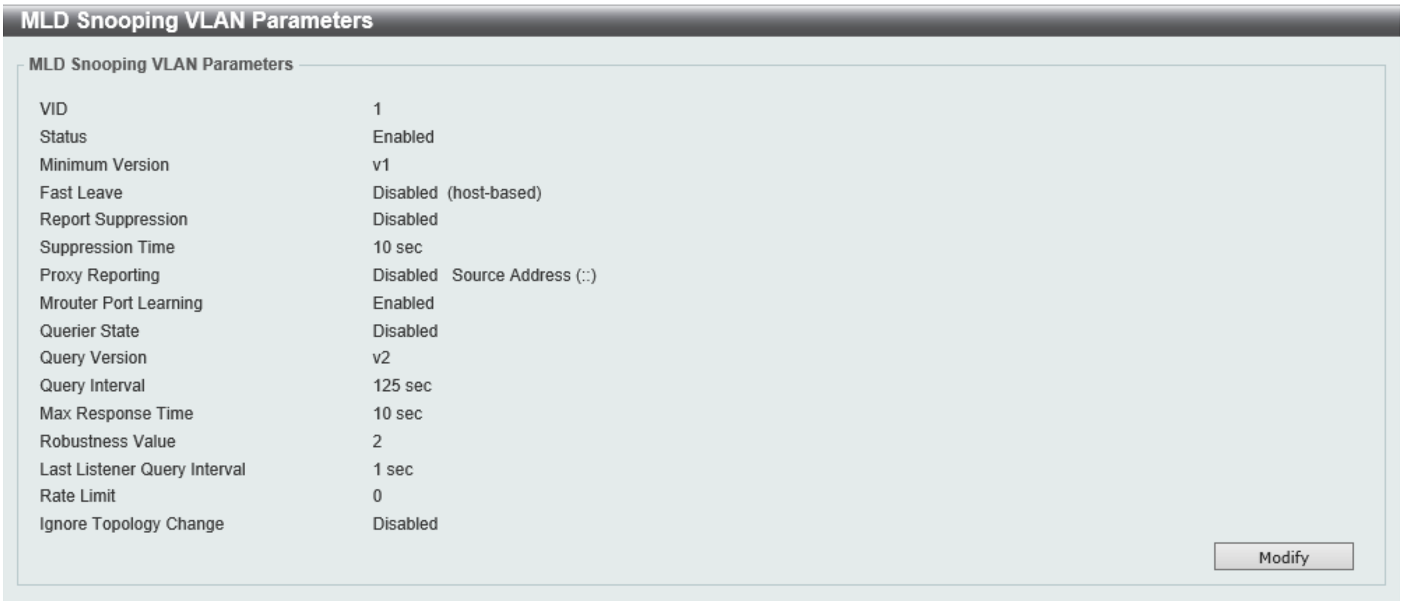
Click the **Show All** button to view all the entries.

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

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

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

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



MLD Snooping VLAN Parameters

MLD Snooping VLAN Parameters

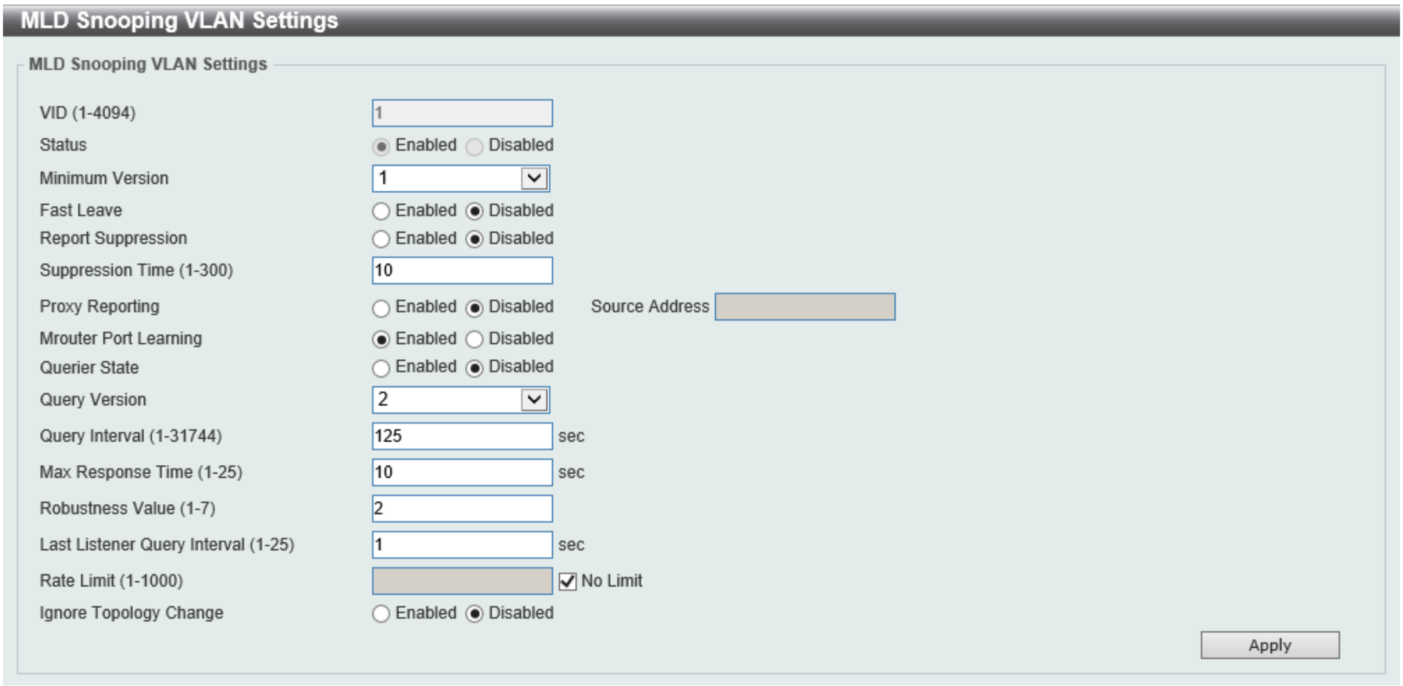
VID	1
Status	Enabled
Minimum Version	v1
Fast Leave	Disabled (host-based)
Report Suppression	Disabled
Suppression Time	10 sec
Proxy Reporting	Disabled Source Address (::)
Mrouter Port Learning	Enabled
Querier State	Disabled
Query Version	v2
Query Interval	125 sec
Max Response Time	10 sec
Robustness Value	2
Last Listener Query Interval	1 sec
Rate Limit	0
Ignore Topology Change	Disabled

Figure 5-76 MLD Snooping Settings (Show Detail) Window

The window displays the detail information about MLD snooping VLAN.

Click the **Modify** button to edit the information in the following window.

After clicking the **Modify** or **Edit** button in MLD Snooping Settings window, the following window will appear.



MLD Snooping VLAN Settings

MLD Snooping VLAN Settings

VID (1-4094)	1
Status	● Enabled ○ Disabled
Minimum Version	1
Fast Leave	○ Enabled ● Disabled
Report Suppression	○ Enabled ● Disabled
Suppression Time (1-300)	10
Proxy Reporting	○ Enabled ● Disabled Source Address
Mrouter Port Learning	● Enabled ○ Disabled
Querier State	○ Enabled ● Disabled
Query Version	2
Query Interval (1-31744)	125 sec
Max Response Time (1-25)	10 sec
Robustness Value (1-7)	2
Last Listener Query Interval (1-25)	1 sec
Rate Limit (1-1000)	☑ No Limit
Ignore Topology Change	○ Enabled ● Disabled

Figure 5-77 MLD Snooping Settings (Modify, Edit) Window

The fields that can be configured are described below:

Parameter	Description
Minimum Version	Select the minimum version of MLD hosts that is allowed on the VLAN. Options to choose from are **1** and **2**.
Fast Leave	Select this option to enable or disable the MLD snooping Fast Leave function. If enabled, the membership is immediately removed when the system receives the MLD done message from the last member.

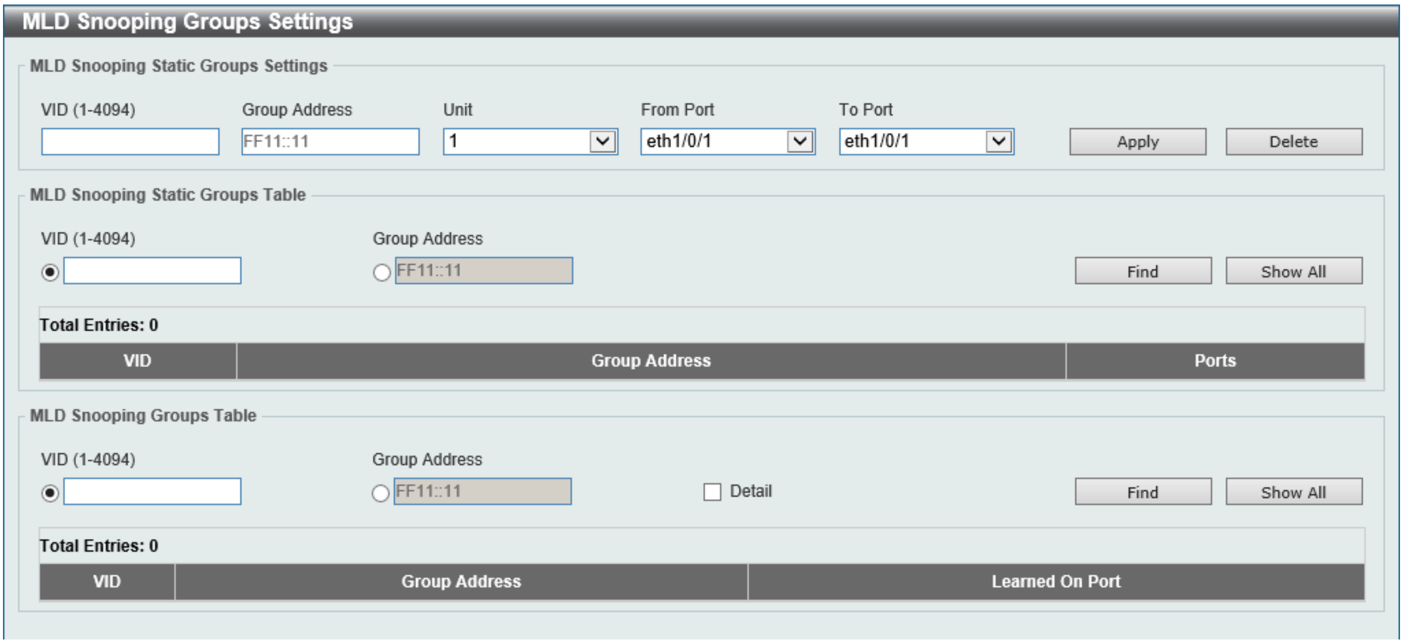
Parameter	Description
Report Suppression	Select this option to enable or disable the report suppression.
Suppression Time	Enter the interval of suppressing duplicate MLD reports or leaves. The range is from 1 to 300.
Proxy Reporting	Select this option to enable or disable the proxy-reporting function.
Mrouter Port Learning	Select to enable or disable the Mrouter port learning function here.
Source Address	Enter the source IPv6 address 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. Select 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:



MLD Snooping Groups Settings

MLD Snooping Static Groups Settings

VID (1-4094)	Group Address	Unit	From Port	To Port
	FF11::11	1	eth1/0/1	eth1/0/1

MLD Snooping Static Groups Table

● VID (1-4094) ○ Group Address FF11::11

Total Entries: 0

VID	Group Address	Ports

MLD Snooping Groups Table

● VID (1-4094) ○ Group Address FF11::11 □ Detail

Total Entries: 0

VID	Group Address	Learned On Port

Figure 5-78 MLD Snooping Groups Settings Window

The fields that can be configured in **MLD Snooping Static Groups Settings/Table** 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.
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.
VID	Click the radio button and enter a VLAN ID of the multicast group. The range is from 1 to 4094.
Group Address	Click the radio button and enter an IPv6 multicast group address.

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

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

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

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

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

The fields that can be configured 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 IPv6 multicast group address.
Detail	Select this option to display the MLD snooping group detail information.

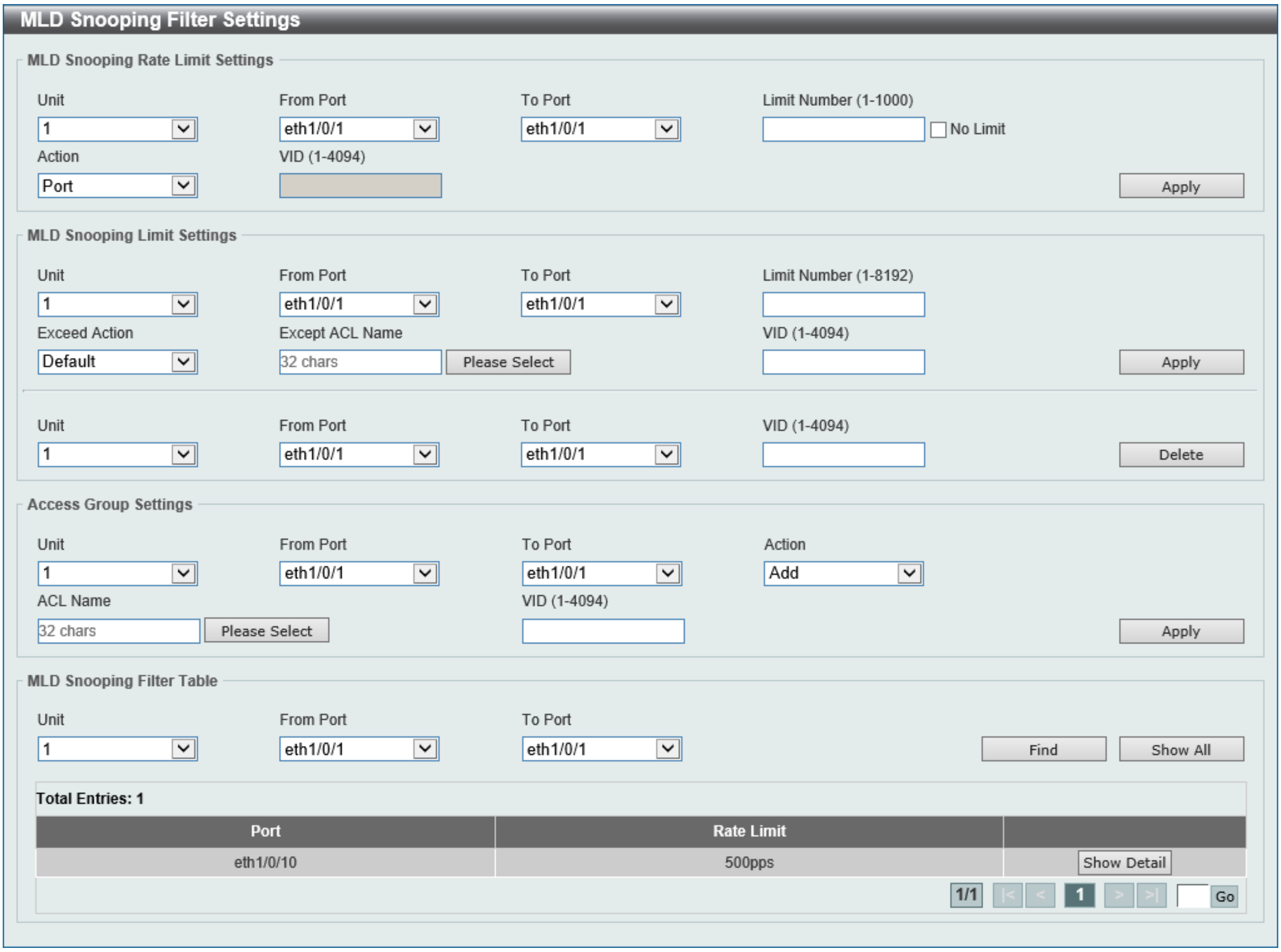
Click the **Find** button to locate a specific entry based on the information entered.

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 filter settings.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Filter Settings**, as shown below:



MLD Snooping Filter Settings

MLD Snooping Rate Limit Settings

Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1
Limit Number (1-1000): □ No Limit
Action: Port
VID (1-4094):

MLD Snooping Limit Settings

Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1
Limit Number (1-8192):
Exceed Action: Default
Except ACL Name: 32 chars
VID (1-4094):

Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1
VID (1-4094):

Access Group Settings

Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1
Action: Add
ACL Name: 32 chars
VID (1-4094):

MLD Snooping Filter Table

Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1

Total Entries: 1

Port	Rate Limit	
eth1/0/10	500pps	Show Detail

Figure 5-79 MLD Snooping Filter Settings Window

The fields that can be configured in **MLD Snooping Rate Limit Settings** are described below:

Parameter	Description
Unit	When **Port** is selected as the **Action**, select the Switch unit ID that will be used here.
From Port - To Port	When **Port** is selected as the **Action**, select the Switch port range that will be used here.
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 here. Options to choose from are **Port** and **VLAN**.
VID	When **VLAN** is selected as the **Action**, enter the VLAN ID 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 Limit Settings** 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.
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 8192.
Exceed Action	Select the exceed action here. This parameter specifies the action for handling newly learned groups when the limitation is exceeded. Options to choose from are: • **Default** - Specifies that the default action will be taken. • **Drop** - Specifies that the new group will be dropped. • **Replace** - Specifies that the new group will replace the oldest group.
Except ACL Name	Enter the standard IP access list name here. The group (*,G) 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 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.
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.
From Port - To Port	Select the Switch port range that will be used here.

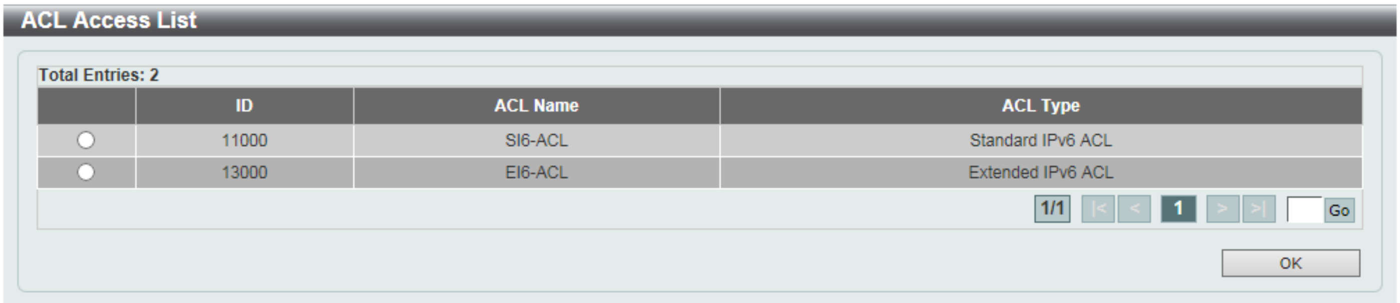
Click the **Find** button to locate a specific entry based on the information entered.

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

Click the **Show Detail** button to view 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.



ACL Access List

Total Entries: 2

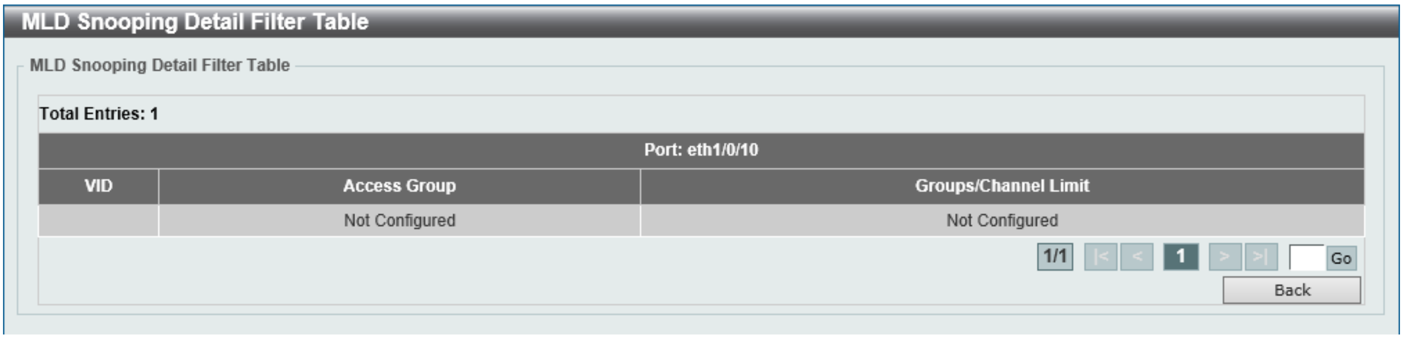
	ID	ACL Name	ACL Type
○	11000	SI6-ACL	Standard IPv6 ACL
○	13000	EI6-ACL	Extended IPv6 ACL

Figure 5-80 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.



MLD Snooping Detail Filter Table

MLD Snooping Detail Filter Table

Total Entries: 1

Port: eth1/0/10

VID	Access Group	Groups/Channel Limit
	Not Configured	Not Configured

Figure 5-81 MLD Snooping Filter Settings (Show Detail) Window

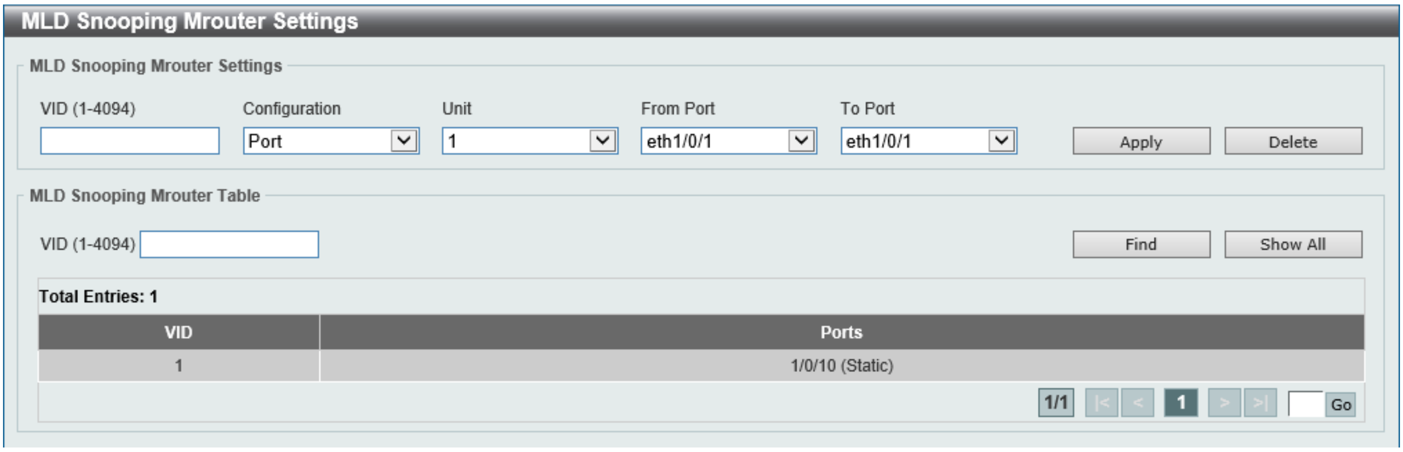
Click the **Back** button to return to the previous window.

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 MLD Snooping Multicast Router settings.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Mrouter Settings**, as shown below:



MLD Snooping Mrouter Settings

MLD Snooping Mrouter Settings

VID (1-4094)	Configuration	Unit	From Port	To Port
	Port	1	eth1/0/1	eth1/0/1

MLD Snooping Mrouter Table

VID (1-4094)

Total Entries: 1

VID	Ports
1	1/0/10 (Static)

Figure 5-82 MLD Snooping Mrouter Settings Window

The fields that can be configured in **MLD Snooping Mrouter Settings** are described below:

Parameter	Description
VID	Enter a VLAN ID between 1 and 4094.
Configuration	Select the port configuration. Options to choose from are: • **Port** - Select to have the configured ports as being connected to multicast-enabled routers. • **Forbidden Port** - Select to have the configured ports as being not connected to multicast-enabled routers. • **Learn pimv6** - Select to enable dynamic learning of multicast router port.
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.

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

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

The fields that can be configured in **MLD Snooping Mrouter Table** are described below:

Parameter	Description
VID	Enter a VLAN ID between 1 and 4094.

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

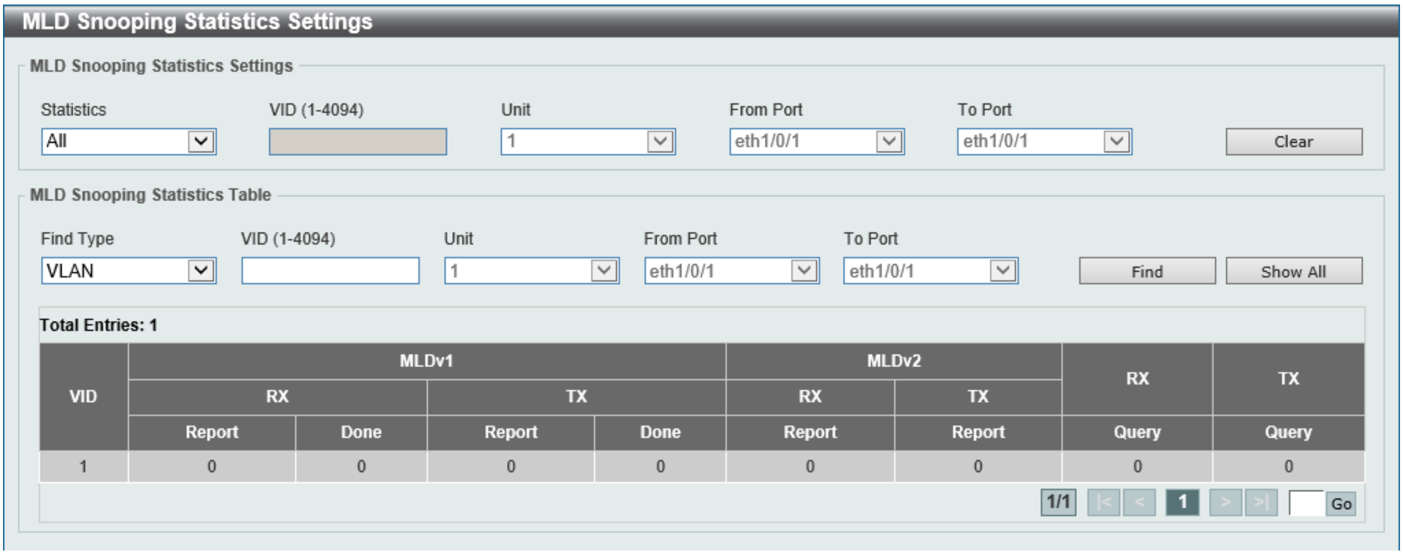
Click the **Show All** button to view all the entries.

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

MLD Snooping Statistics Settings

This window is used to view and clear the MLD snooping related statistics.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Statistics Settings**, as shown below:



MLD Snooping Statistics Settings

MLD Snooping Statistics Settings

Statistics: All; VID (1-4094): ; Unit: 1; From Port: eth1/0/1; To Port: eth1/0/1

MLD Snooping Statistics Table

Find Type: VLAN; VID (1-4094): ; Unit: 1; From Port: eth1/0/1; To Port: eth1/0/1

Total Entries: 1

VID	MLDv1				MLDv2		RX	TX
	RX		TX		RX	TX		
	Report	Done	Report	Done	Report	Report	Query	Query
1	0	0	0	0	0	0	0	0

Figure 5-83 MLD Snooping Statistics Settings Window

The fields that can be configured in **MLD Snooping Statistics Settings** are described below:

Parameter	Description
Statistics	Select the interface here. Options to choose from are **All**, **VLAN**, and **Port**.

Parameter	Description
VID	Enter a VLAN ID between 1 and 4094. This is available when **VLAN** is selected in the **Statistics** drop-down list.
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.
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 **Find Type** drop-down list.
From Port - To Port	Select the appropriate port range used for the configuration here. This is available when **Port** is selected in the **Find Type** drop-down list.

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

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

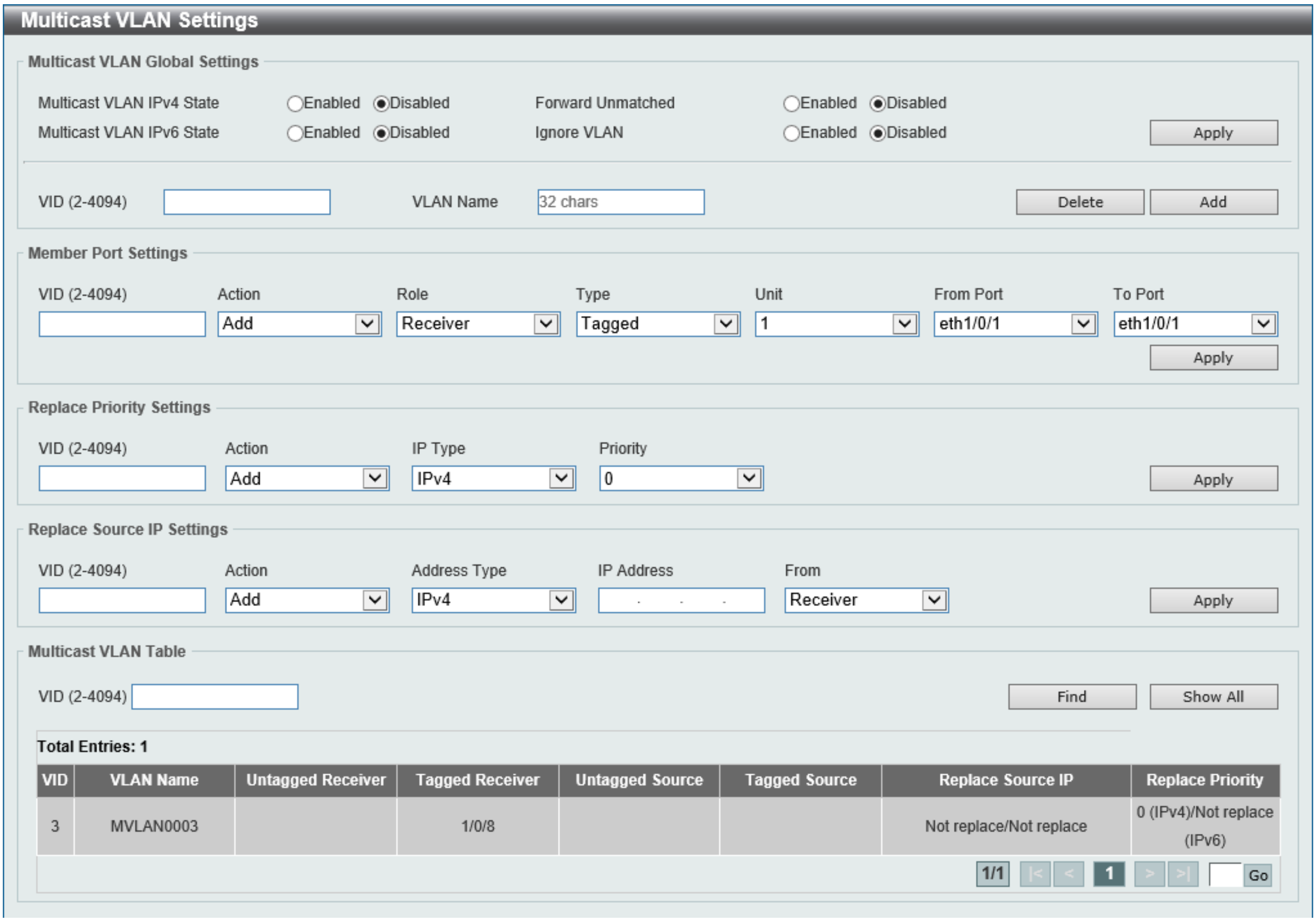
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Multicast 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:



Multicast VLAN Settings

Multicast VLAN Global Settings

Multicast VLAN IPv4 State ○Enabled ●Disabled   Forward Unmatched ○Enabled ●Disabled

Multicast VLAN IPv6 State ○Enabled ●Disabled   Ignore VLAN ○Enabled ●Disabled   Apply

VID (2-4094)   VLAN Name: 32 chars   Delete   Add

Member Port Settings

VID (2-4094)	Action	Role	Type	Unit	From Port	To Port
	Add	Receiver	Tagged	1	eth1/0/1	eth1/0/1

Apply

Replace Priority Settings

VID (2-4094)	Action	IP Type	Priority
	Add	IPv4	0

Apply

Replace Source IP Settings

VID (2-4094)	Action	Address Type	IP Address	From
	Add	IPv4	. . .	Receiver

Apply

Multicast VLAN Table

VID (2-4094)   Find   Show All

Total Entries: 1

VID	VLAN Name	Untagged Receiver	Tagged Receiver	Untagged Source	Tagged Source	Replace Source IP	Replace Priority
3	MVLAN0003		1/0/8			Not replace/Not replace	0 (IPv4)/Not replace (IPv6)

Figure 5-84 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.

Parameter	Description
VID	Enter the VLAN ID of the multicast VLAN here. The range is 2 to 4094.
VLAN Name	Enter the VLAN name of the multicast VLAN 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 -** 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 -** 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.
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 Priority 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.
IP Type	Select the IP type here. Options to choose from are: • **IPv4 -** Specifies to the remap priority for IPv4 multicast packets forwarded on the multicast VLAN. • **IPv6 -** Specifies to the remap priority for IPv6 multicast packets forwarded on the multicast VLAN.
Priority	Select the priority value here. The range is from 0 to 7.

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:

Parameter	Description
	• **IPv4** - Specifies to enter the source IPv4 address for IGMP control packet reporting up to routers. • **IPv6** - Specifies to enter the source IPv6 address for MLD control packet reporting up to routers.
IP Address	Enter the IPv4/IPv6 address here.
From	Select the "from" option here. Options to choose from are: • **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.

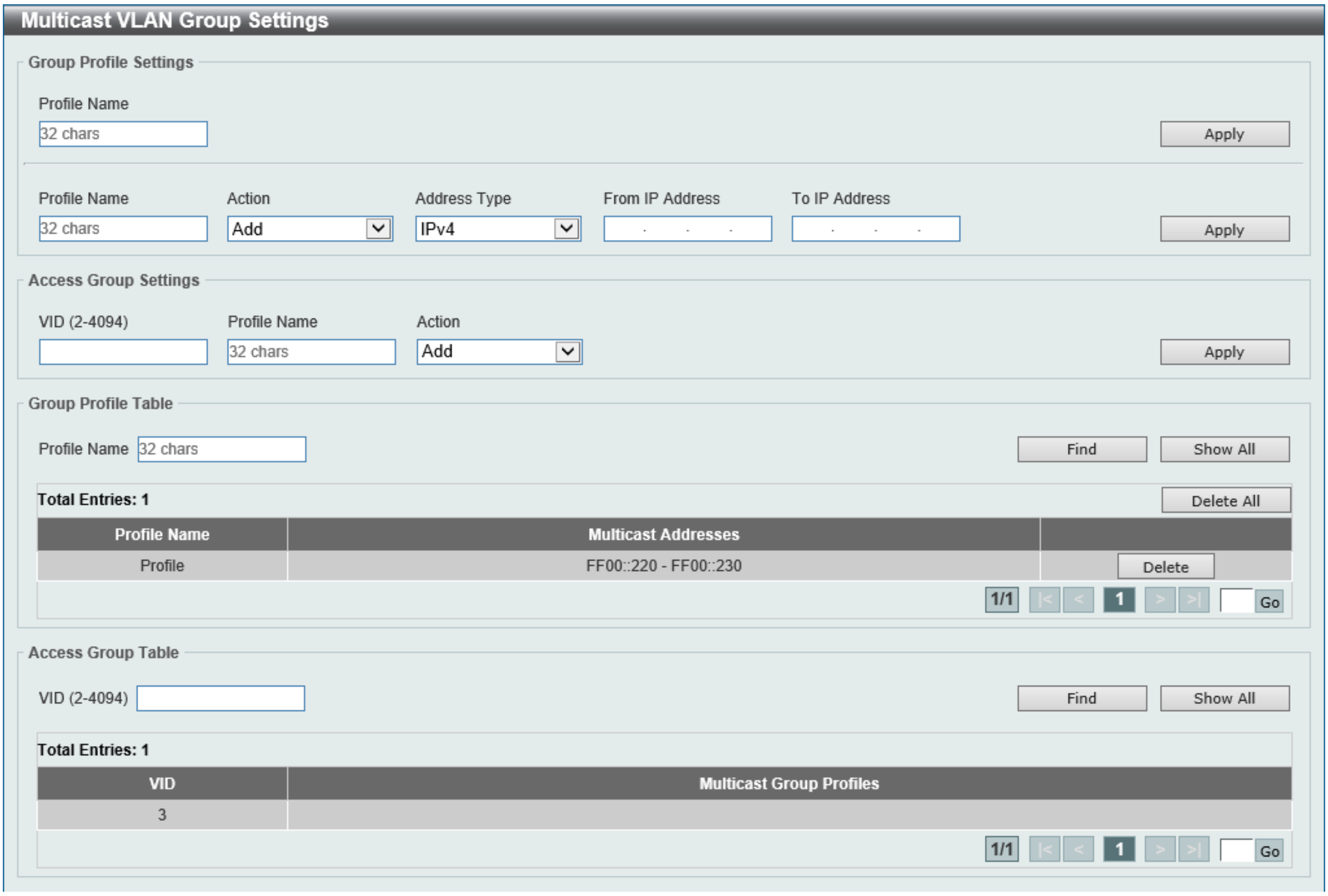
Click the **Show All** button to view all the entries.

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

Multicast VLAN Group Settings

This window 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:



Group Profile Settings

Profile Name: 32 chars

Profile Name: 32 chars; Action: Add; Address Type: IPv4; From IP Address: . . . ; To IP Address: . . .

Access Group Settings

VID (2-4094): ; Profile Name: 32 chars; Action: Add

Group Profile Table

Profile Name: 32 chars

Total Entries: 1

Profile Name	Multicast Addresses	
Profile	FF00::220 - FF00::230	Delete

Access Group Table

VID (2-4094):

Total Entries: 1

VID	Multicast Group Profiles
3	

Figure 5-85 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.
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** - Specifies to use IPv4 multicast addresses in the range. • **IPv6** - Specifies to use IPv6 multicast addresses in the range.
From IP Address	Enter the start IPv4/IPv6 address here.
To IP Address	Enter the end 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.

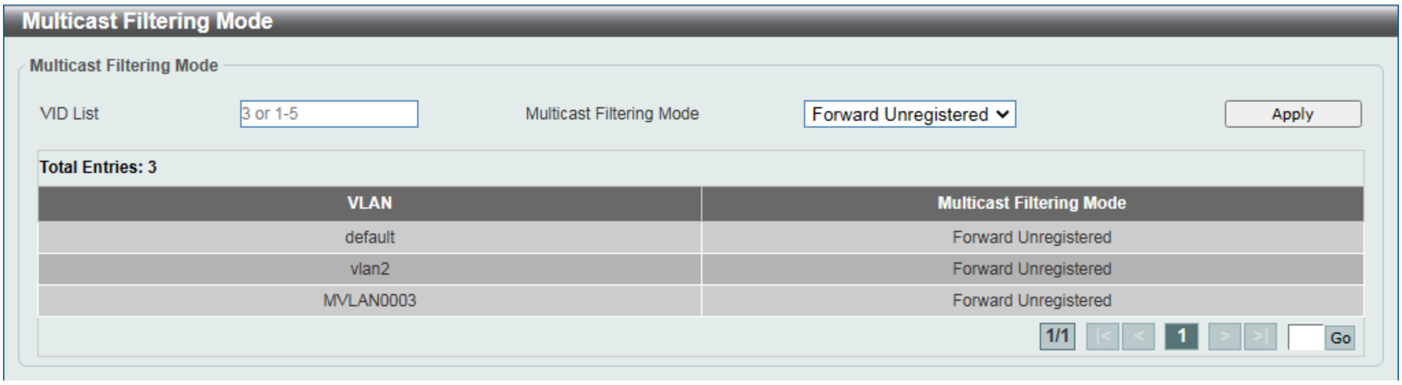
Click the **Show All** button to display all the entries.

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

Multicast Filtering Mode

This window is used to display and configure the Layer 2 multicast filtering settings.

To view the following window, click **L2 Features > L2 Multicast Control > Multicast Filtering Mode**, as shown below:



Multicast Filtering Mode

Multicast Filtering Mode

VID List: 3 or 1-5

Multicast Filtering Mode: Forward Unregistered

Total Entries: 3

VLAN	Multicast Filtering Mode
default	Forward Unregistered
vlan2	Forward Unregistered
MVLAN0003	Forward Unregistered

Figure 5-86 Multicast Filtering Mode Window

The fields that can be configured are described below:

Parameter	Description
VID List	Enter the VLAN ID list that will be used for this configuration here.
Multicast Filtering Mode	Select the multicast filtering mode here. Options to choose from are: • **Forward Unregistered** - Registered multicast packets will be forwarded based on the forwarding table and all unregistered multicast packets will be flooded based on the VLAN domain. • **Filter Unregistered** - Registered packets will be forwarded based on the forwarding table and all unregistered multicast packets will be filtered.

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

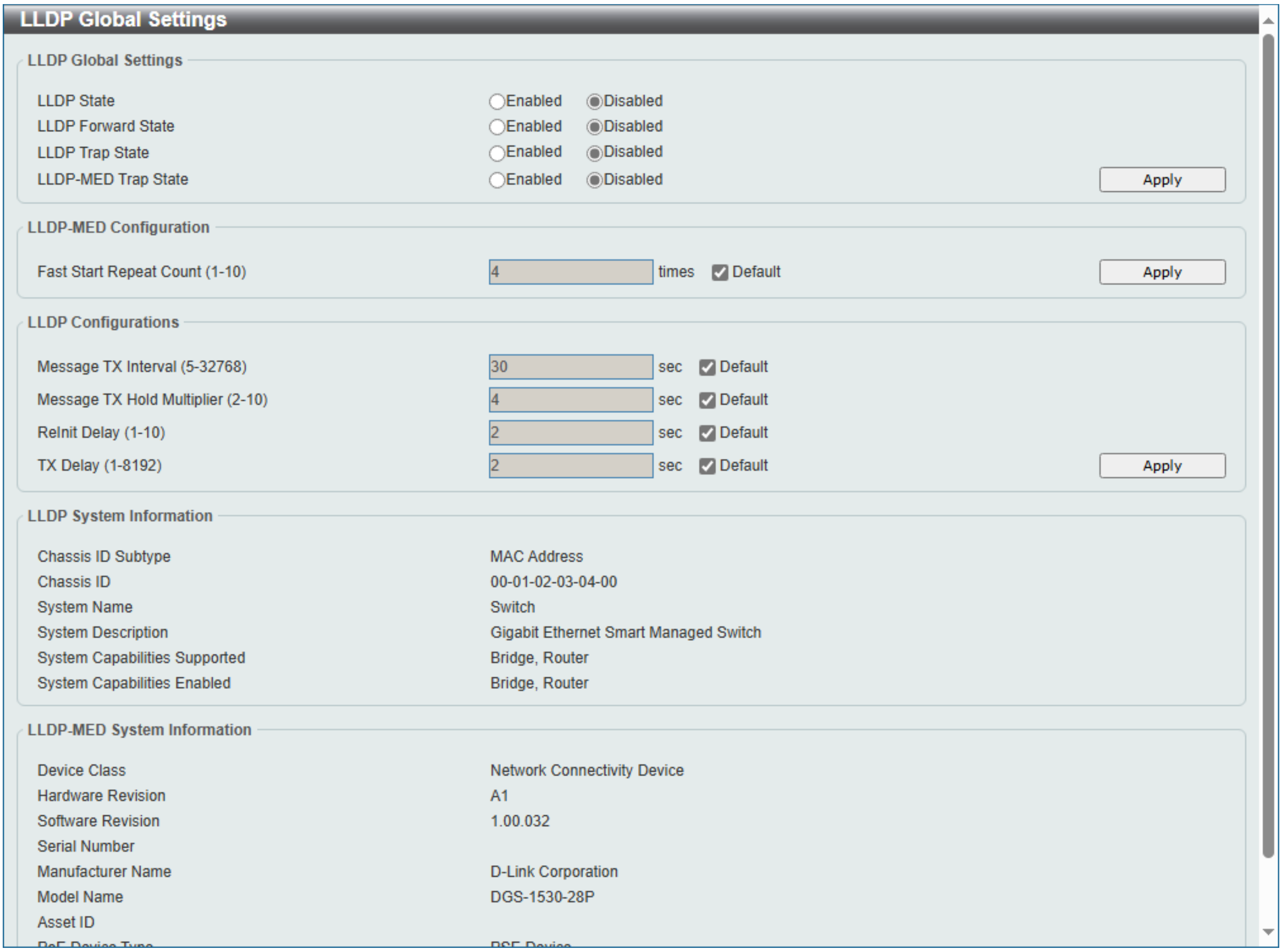
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

LLDP

LLDP Global Settings

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

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



LLDP Global Settings

LLDP Global Settings

LLDP State	○Enabled ●Disabled
LLDP Forward State	○Enabled ●Disabled
LLDP Trap State	○Enabled ●Disabled
LLDP-MED Trap State	○Enabled ●Disabled

LLDP-MED Configuration

Fast Start Repeat Count (1-10): 4 times ☑ Default

LLDP Configurations

Message TX Interval (5-32768)	30 sec ☑ Default
Message TX Hold Multiplier (2-10)	4 sec ☑ Default
ReInit Delay (1-10)	2 sec ☑ Default
TX Delay (1-8192)	2 sec ☑ Default

LLDP System Information

Chassis ID Subtype	MAC Address
Chassis ID	00-01-02-03-04-00
System Name	Switch
System Description	Gigabit Ethernet Smart Managed Switch
System Capabilities Supported	Bridge, Router
System Capabilities Enabled	Bridge, Router

LLDP-MED System Information

Device Class	Network Connectivity Device
Hardware Revision	A1
Software Revision	1.00.032
Serial Number	
Manufacturer Name	D-Link Corporation
Model Name	DGS-1530-28P
Asset ID	
PoE Device Type	PSE Device

Figure 5-87 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 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. The range is from 1 to 10.

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

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

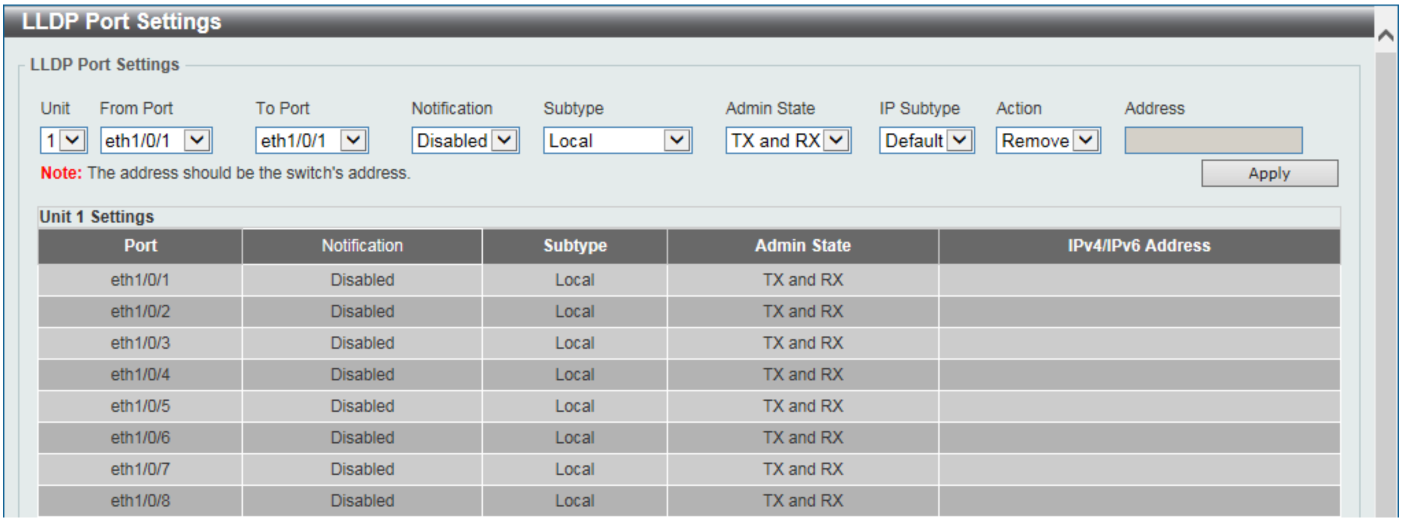
Parameter	Description
Message TX Interval	Enter the interval between consecutive transmissions of LLDP advertisements on each physical interface. The range is from 5 to 32768 seconds.
Message TX Hold Multiplier	Enter the multiplier on the LLDPDUs transmission interval that used to calculate the TTL value of an LLDPDU. This value must be between 2 and 10.
ReInit Delay	Enter the delay value for LLDP initialization on an interface. The range is from 1 to 10 seconds.
TX Delay	Enter the delay value for sending successive LLDPDUs on an interface. The valid values are from 1 to 8192 seconds and should not be greater than one-fourth of the transmission interval timer.

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

LLDP Port Settings

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

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



LLDP Port Settings

LLDP Port Settings

Unit	From Port	To Port	Notification	Subtype	Admin State	IP Subtype	Action	Address
1	eth1/0/1	eth1/0/1	Disabled	Local	TX and RX	Default	Remove	

Note: The address should be the switch's address.

Unit 1 Settings

Port	Notification	Subtype	Admin State	IPv4/IPv6 Address
eth1/0/1	Disabled	Local	TX and RX	
eth1/0/2	Disabled	Local	TX and RX	
eth1/0/3	Disabled	Local	TX and RX	
eth1/0/4	Disabled	Local	TX and RX	
eth1/0/5	Disabled	Local	TX and RX	
eth1/0/6	Disabled	Local	TX and RX	
eth1/0/7	Disabled	Local	TX and RX	
eth1/0/8	Disabled	Local	TX and RX	

Figure 5-88 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.
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** - The local LLDP agent can only transmit LLDP frames. • **RX** - The local LLDP agent can only receive LLDP frames. • **TX and RX** - The local LLDP agent can both transmit and receive LLDP frames. • **Disabled** - The local LLDP agent can neither transmit nor receive LLDP frames. By default, the **TX and RX** option is used.
IP Subtype	Select the type of the IP address information to be sent. Options to choose from are **Default**, **IPv4**, and **IPv6**.
Action	Select the action that will be taken here. Options to choose from are **Remove** and **Add**.
Address	Enter the IP address that will be sent.

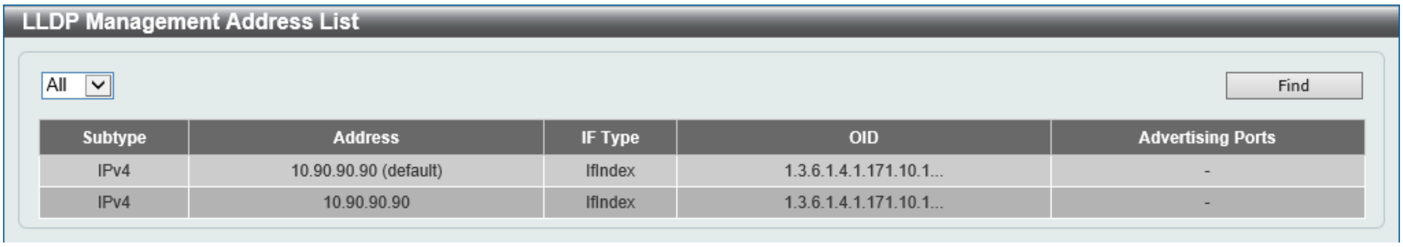
Click the **Apply** button to accept the changes made.

NOTE: The IPv4 or IPv6 address entered here should be an existing LLDP management IP address.

LLDP Management Address List

This window is used to view the LLDP management address list.

To view the following window, click **L2 Features > LLDP > LLDP Management Address List**, as shown below:



LLDP Management Address List

All ▾ Find

Subtype	Address	IF Type	OID	Advertising Ports
IPv4	10.90.90.90 (default)	IfIndex	1.3.6.1.4.1.171.10.1...	-
IPv4	10.90.90.90	IfIndex	1.3.6.1.4.1.171.10.1...	-

Figure 5-89 LLDP Management Address List Window

The fields that can be configured are described below:

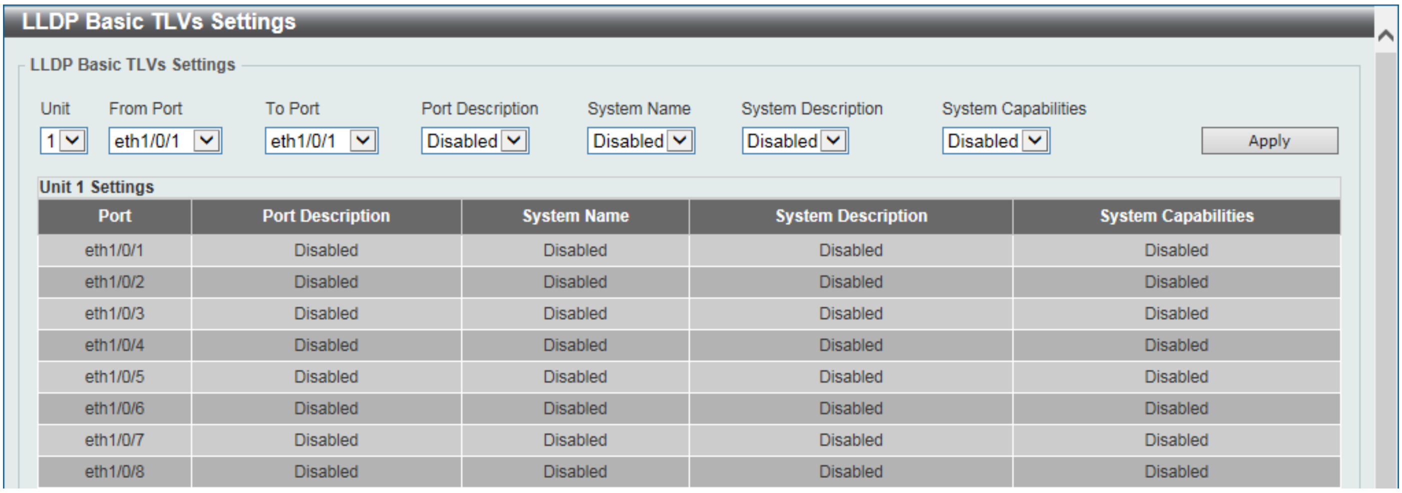
Parameter	Description
Subtype	Select the subtype. Options to choose from are: • **All** - Specifies to display all entries. • **IPv4** - Enter the IPv4 address in the space provided. • **IPv6** - Enter the IPv6 address in the space provided.

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:



LLDP Basic TLVs Settings

LLDP Basic TLVs Settings

Unit	From Port	To Port	Port Description	System Name	System Description	System Capabilities	
1	eth1/0/1	eth1/0/1	Disabled	Disabled	Disabled	Disabled	Apply

Unit 1 Settings

Port	Port Description	System Name	System Description	System Capabilities
eth1/0/1	Disabled	Disabled	Disabled	Disabled
eth1/0/2	Disabled	Disabled	Disabled	Disabled
eth1/0/3	Disabled	Disabled	Disabled	Disabled
eth1/0/4	Disabled	Disabled	Disabled	Disabled
eth1/0/5	Disabled	Disabled	Disabled	Disabled
eth1/0/6	Disabled	Disabled	Disabled	Disabled
eth1/0/7	Disabled	Disabled	Disabled	Disabled
eth1/0/8	Disabled	Disabled	Disabled	Disabled

Figure 5-90 LLDP Basic TLVs Settings Window

The fields that can be configured are described below:

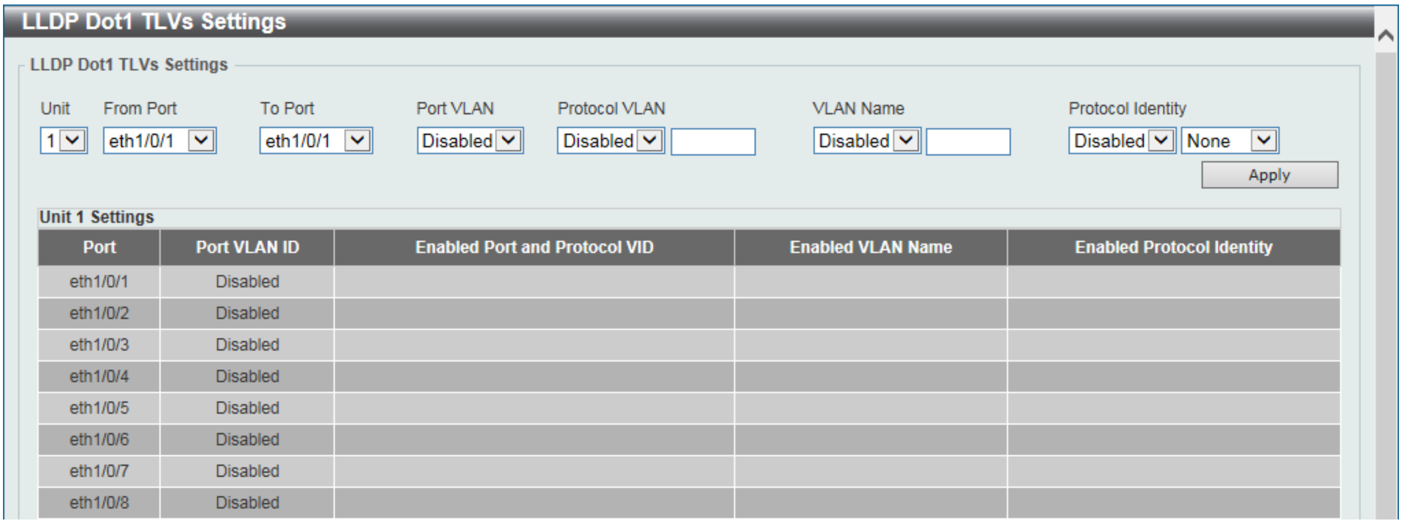
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
Port Description	Select this option to enable or disable the Port Description option.
System Name	Select this option to enable or disable the System Name option.
System Description	Select this option to enable or disable the System Description option.
System Capabilities	Select this option to enable or disable the System Capabilities option.

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

LLDP Dot1 TLVs Settings

The LLDP Dot1 TLVs Settings page is used to enable or disable outbound LLDP advertisements for IEEE 802.1 organizationally unique port VLAN ID TLVs.

To view the following window, click **L2 Features > LLDP > LLDP Dot1 TLVs Settings**, as shown below:



LLDP Dot1 TLVs Settings

LLDP Dot1 TLVs Settings

Unit	From Port	To Port	Port VLAN	Protocol VLAN		VLAN Name		Protocol Identity	
1	eth1/0/1	eth1/0/1	Disabled	Disabled		Disabled		Disabled	None

Unit 1 Settings

Port	Port VLAN ID	Enabled Port and Protocol VID	Enabled VLAN Name	Enabled Protocol Identity
eth1/0/1	Disabled			
eth1/0/2	Disabled			
eth1/0/3	Disabled			
eth1/0/4	Disabled			
eth1/0/5	Disabled			
eth1/0/6	Disabled			
eth1/0/7	Disabled			
eth1/0/8	Disabled			

Figure 5-91 LLDP Dot1 TLVs Settings Window

The fields that can be configured are described below:

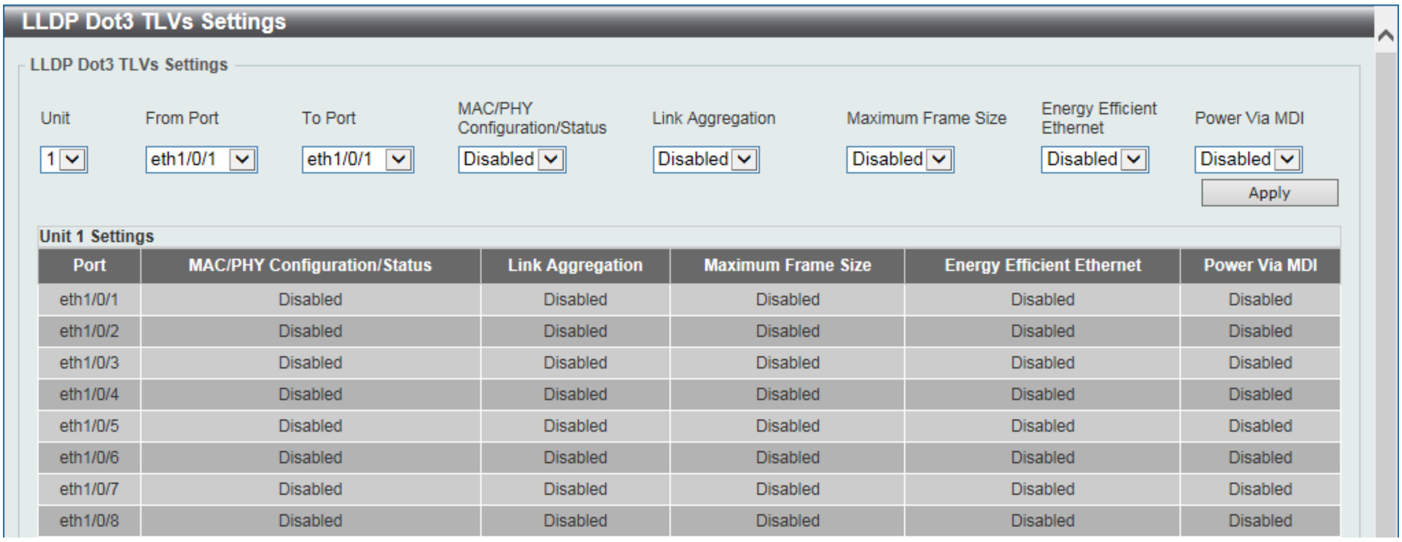
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
Port VLAN	Select this option to enable or disable sending the port VLAN ID TLV. The Port VLAN ID TLV is an optional fixed 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:



LLDP Dot3 TLVs Settings

LLDP Dot3 TLVs Settings

Unit	From Port	To Port	MAC/PHY Configuration/Status	Link Aggregation	Maximum Frame Size	Energy Efficient Ethernet	Power Via MDI
1	eth1/0/1	eth1/0/1	Disabled	Disabled	Disabled	Disabled	Disabled

Unit 1 Settings

Port	MAC/PHY Configuration/Status	Link Aggregation	Maximum Frame Size	Energy Efficient Ethernet	Power Via MDI
eth1/0/1	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/2	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/3	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/4	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/5	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/6	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/7	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/8	Disabled	Disabled	Disabled	Disabled	Disabled

Figure 5-92 LLDP Dot3 TLVs Settings Window

The fields that can be configured are described below:

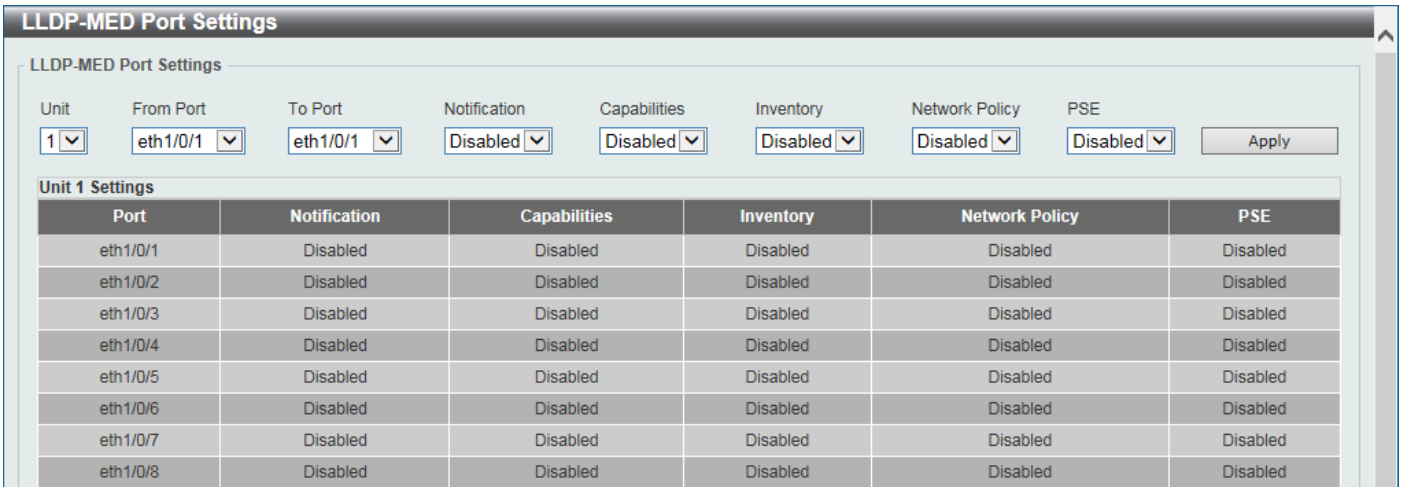
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
MAC/PHY Configuration/Status	Select this option to enable or disable the MAC/PHY Configuration/Status TLV to send. The 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.
Energy Efficient Ethernet	Select this option to enable or disable the Energy Efficient Ethernet (EEE) function.
Power Via MDI	Select this option to enable or disable the power via MDI function.

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:



LLDP-MED Port Settings

LLDP-MED Port Settings

Unit: 1 | From Port: eth1/0/1 | To Port: eth1/0/1 | Notification: Disabled | Capabilities: Disabled | Inventory: Disabled | Network Policy: Disabled | PSE: Disabled

Unit 1 Settings

Port	Notification	Capabilities	Inventory	Network Policy	PSE
eth1/0/1	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/2	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/3	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/4	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/5	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/6	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/7	Disabled	Disabled	Disabled	Disabled	Disabled
eth1/0/8	Disabled	Disabled	Disabled	Disabled	Disabled

Figure 5-93 LLDP-MED Port Settings Window

The fields that can be configured are described below:

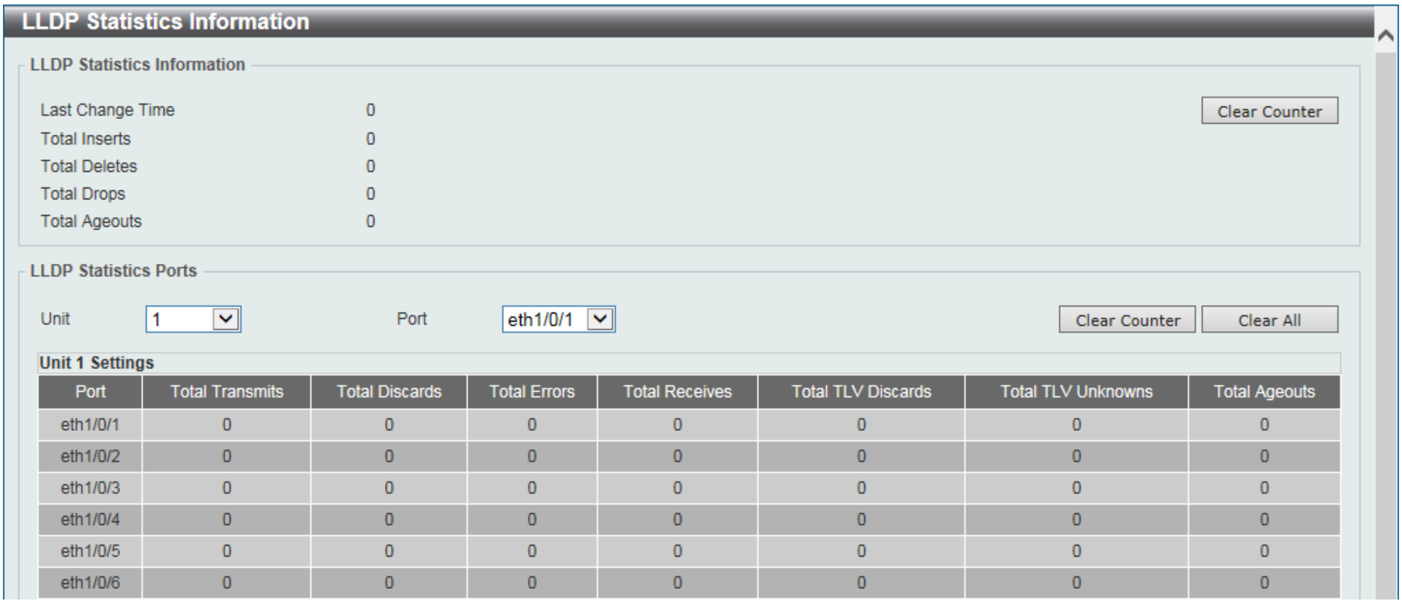
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
Notification	Select this option to enable or disable transmitting the LLDP-MED notification TLV.
Capabilities	Select this option to enable or disable transmitting the LLDP-MED capabilities TLV.
Inventory	Select this option to enable or disable transmitting the LLDP-MED inventory management TLV.
Network Policy	Select this option to enable or disable transmitting the LLDP-MED network policy TLV.
PSE	Select this option to enable or disable transmitting the LLDP-MED Extended Power-via MDI TLV if the local device is a PSE device or PD device. This is only available for switches that support PoE.

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:



Last Change Time	0
Total Inserts	0
Total Deletes	0
Total Drops	0
Total Ageouts	0

Unit 1 Port eth1/0/1

Unit 1 Settings

Port	Total Transmits	Total Discards	Total Errors	Total Receives	Total TLV Discards	Total TLV Unknowns	Total Ageouts
eth1/0/1	0	0	0	0	0	0	0
eth1/0/2	0	0	0	0	0	0	0
eth1/0/3	0	0	0	0	0	0	0
eth1/0/4	0	0	0	0	0	0	0
eth1/0/5	0	0	0	0	0	0	0
eth1/0/6	0	0	0	0	0	0	0

Figure 5-94 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.
Port	Select the port number that will be used here.

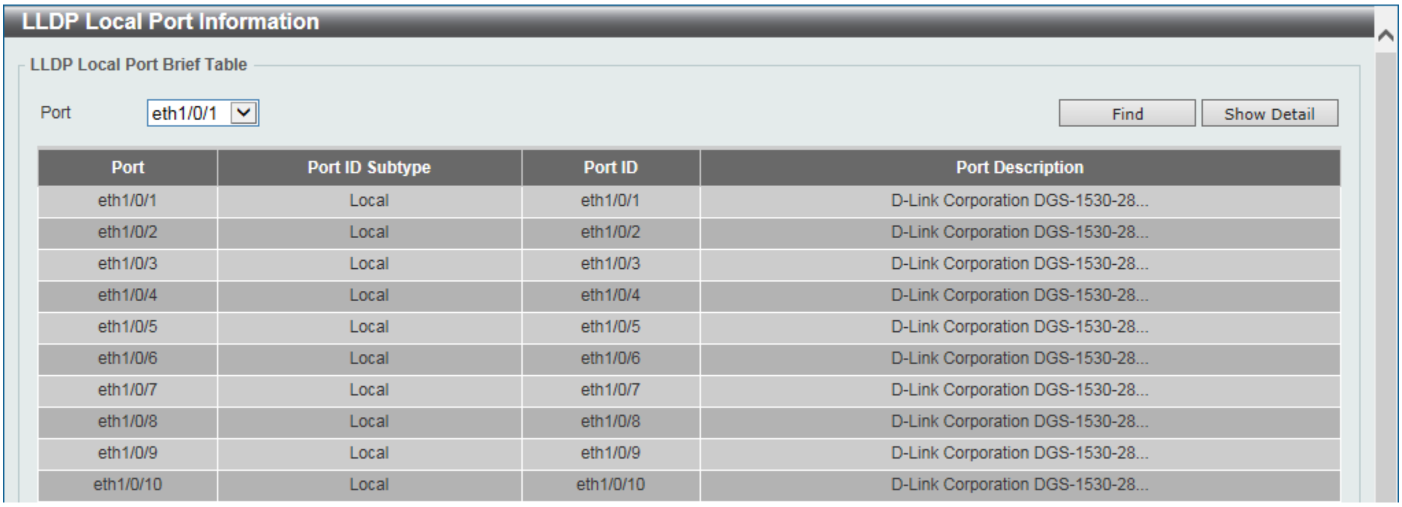
Click the **Clear Counter** button to clear the counter information for the statistics displayed.

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

LLDP Local Port Information

This window is used to display the information currently available for populating outbound LLDP advertisements.

To view the following window, click **L2 Features > LLDP > LLDP Local Port Information**, as shown below:



LLDP Local Port Information

LLDP Local Port Brief Table

Port: eth1/0/1

Port	Port ID Subtype	Port ID	Port Description
eth1/0/1	Local	eth1/0/1	D-Link Corporation DGS-1530-28...
eth1/0/2	Local	eth1/0/2	D-Link Corporation DGS-1530-28...
eth1/0/3	Local	eth1/0/3	D-Link Corporation DGS-1530-28...
eth1/0/4	Local	eth1/0/4	D-Link Corporation DGS-1530-28...
eth1/0/5	Local	eth1/0/5	D-Link Corporation DGS-1530-28...
eth1/0/6	Local	eth1/0/6	D-Link Corporation DGS-1530-28...
eth1/0/7	Local	eth1/0/7	D-Link Corporation DGS-1530-28...
eth1/0/8	Local	eth1/0/8	D-Link Corporation DGS-1530-28...
eth1/0/9	Local	eth1/0/9	D-Link Corporation DGS-1530-28...
eth1/0/10	Local	eth1/0/10	D-Link Corporation DGS-1530-28...

Figure 5-95 LLDP Local Port Information Window

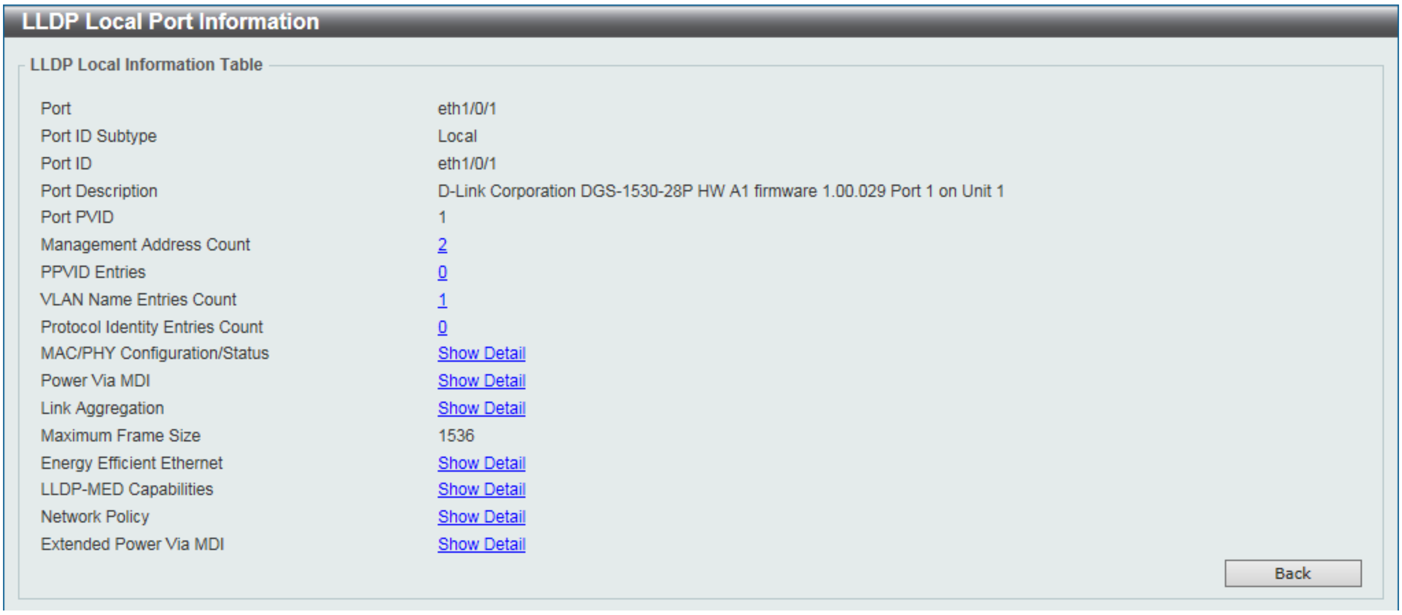
The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be displayed.
Port	Select the port number that will be displayed.

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

Click the **Show Detail** button to view detailed information of the specific port.

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



LLDP Local Port Information

LLDP Local Information Table

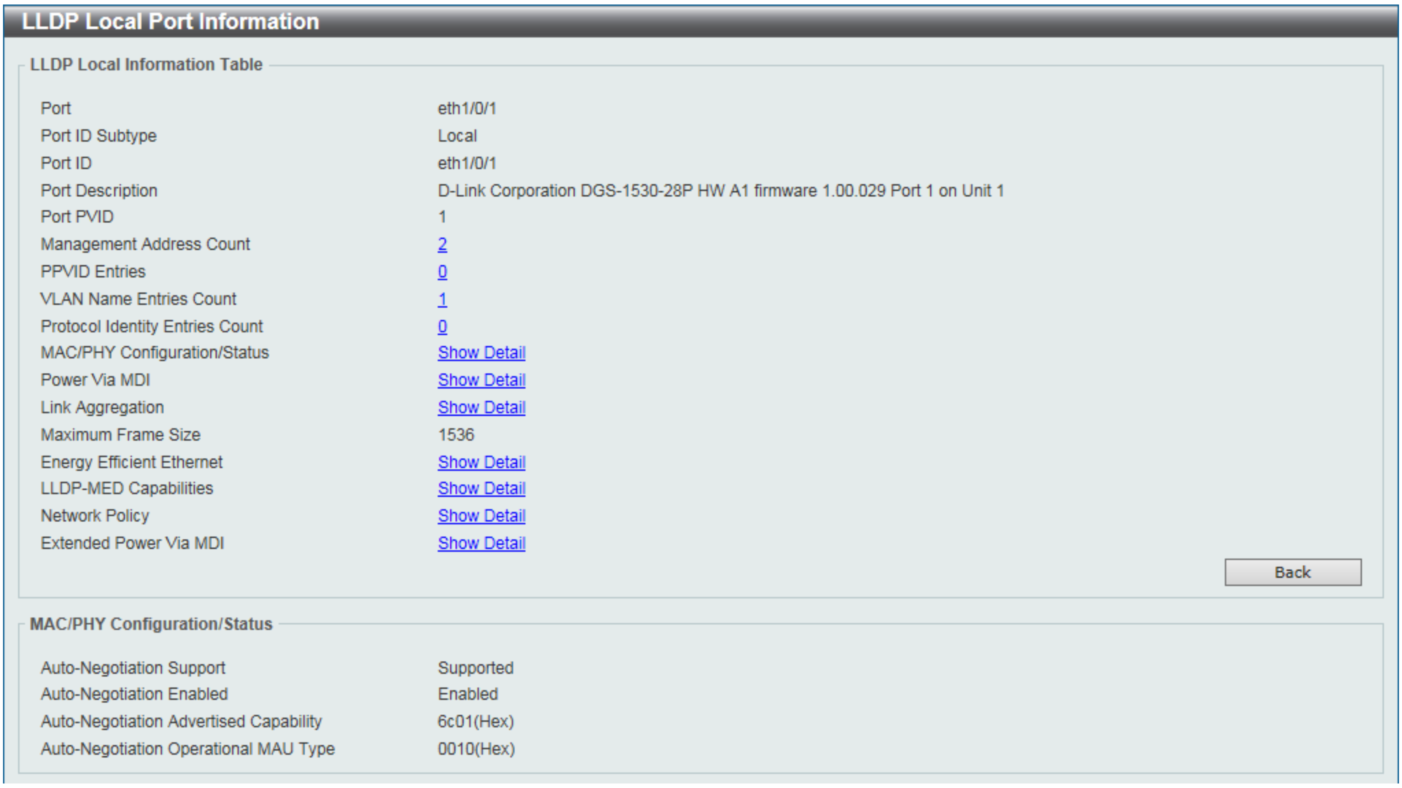
Port	eth1/0/1
Port ID Subtype	Local
Port ID	eth1/0/1
Port Description	D-Link Corporation DGS-1530-28P HW A1 firmware 1.00.029 Port 1 on Unit 1
Port PVID	1
Management Address Count	2
PPVID Entries	0
VLAN Name Entries Count	1
Protocol Identity Entries Count	0
MAC/PHY Configuration/Status	Show Detail
Power Via MDI	Show Detail
Link Aggregation	Show Detail
Maximum Frame Size	1536
Energy Efficient Ethernet	Show Detail
LLDP-MED Capabilities	Show Detail
Network Policy	Show Detail
Extended Power Via MDI	Show Detail

Figure 5-96 LLDP Local Port Information (Show Detail) Window

To view more details about, for example, the **MAC/PHY Configuration/Status**, click the Show Detail hyperlink.

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

After clicking the Show Detail hyperlink, a new section will appear at the bottom of the window.



LLDP Local Port Information

LLDP Local Information Table

Port	eth1/0/1
Port ID Subtype	Local
Port ID	eth1/0/1
Port Description	D-Link Corporation DGS-1530-28P HW A1 firmware 1.00.029 Port 1 on Unit 1
Port PVID	1
Management Address Count	2
PPVID Entries	0
VLAN Name Entries Count	1
Protocol Identity Entries Count	0
MAC/PHY Configuration/Status	Show Detail
Power Via MDI	Show Detail
Link Aggregation	Show Detail
Maximum Frame Size	1536
Energy Efficient Ethernet	Show Detail
LLDP-MED Capabilities	Show Detail
Network Policy	Show Detail
Extended Power Via MDI	Show Detail

MAC/PHY Configuration/Status

Auto-Negotiation Support	Supported
Auto-Negotiation Enabled	Enabled
Auto-Negotiation Advertised Capability	6c01(Hex)
Auto-Negotiation Operational MAU Type	0010(Hex)

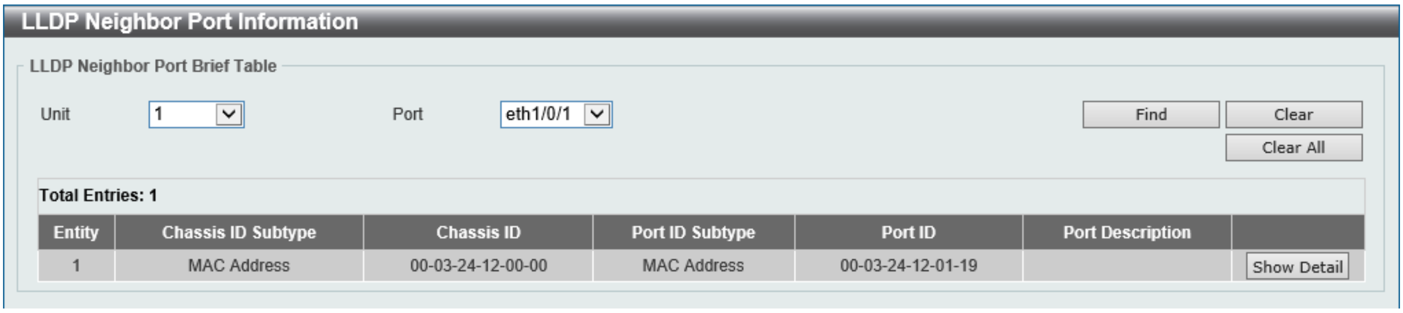
Figure 5-97 LLDP Local Port Information (Show Detail) Window

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

LLDP Neighbor Port Information

This window is used to display the LLDP information learned from neighboring switches. The Switch receives packets from a remote station but is able to store the information locally.

To view the following window, click **L2 Features > LLDP > LLDP Neighbor Port Information**, as shown below:



LLDP Neighbor Port Information

LLDP Neighbor Port Brief Table

Unit: 1 Port: eth1/0/1

Total Entries: 1

Entity	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	Port Description	
1	MAC Address	00-03-24-12-00-00	MAC Address	00-03-24-12-01-19		Show Detail

Figure 5-98 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.

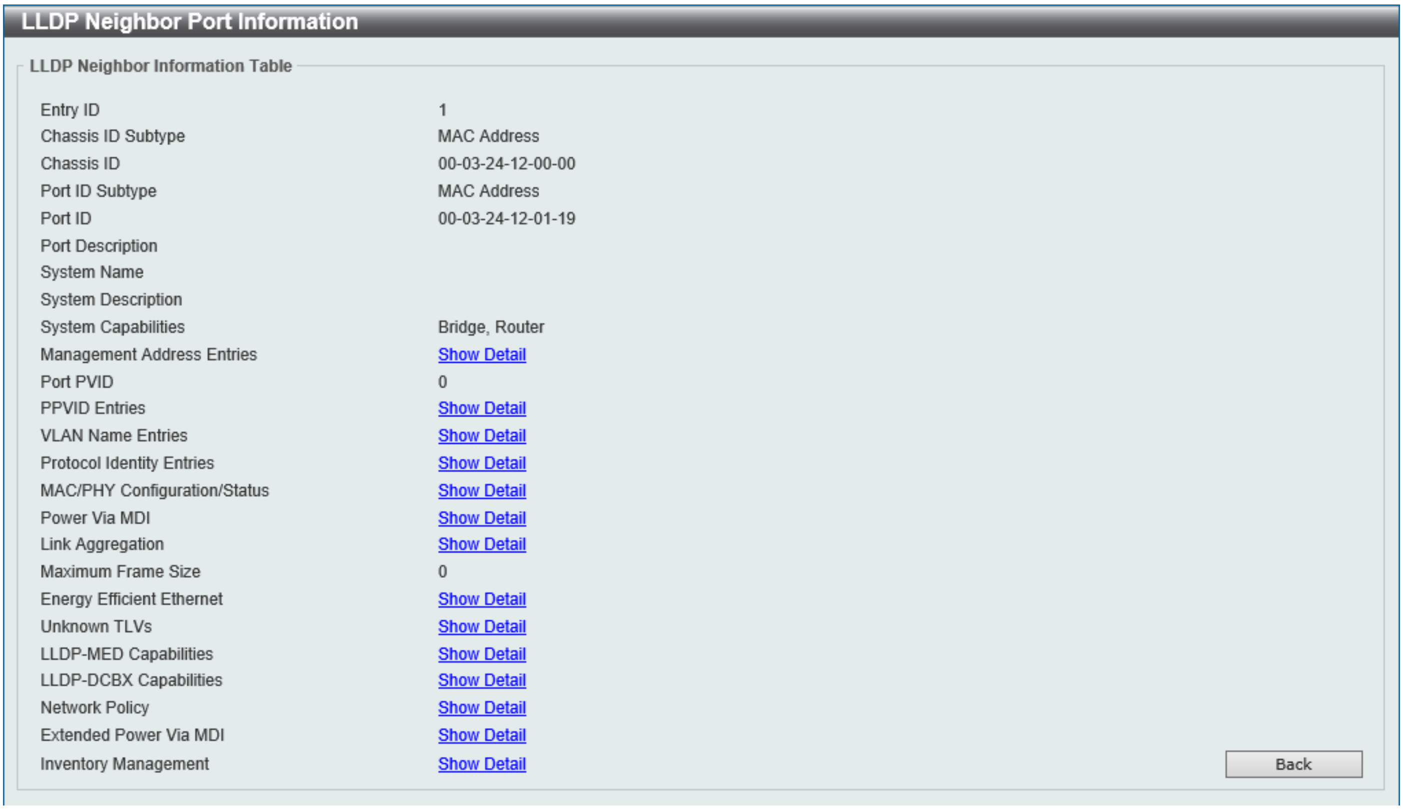
Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear** button to clear the specific port information.

Click the **Clear All** button to clear all the port information displayed.

Click the **Show Detail** button to view detailed information of the specific port.

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



LLDP Neighbor Port Information

LLDP Neighbor Information Table

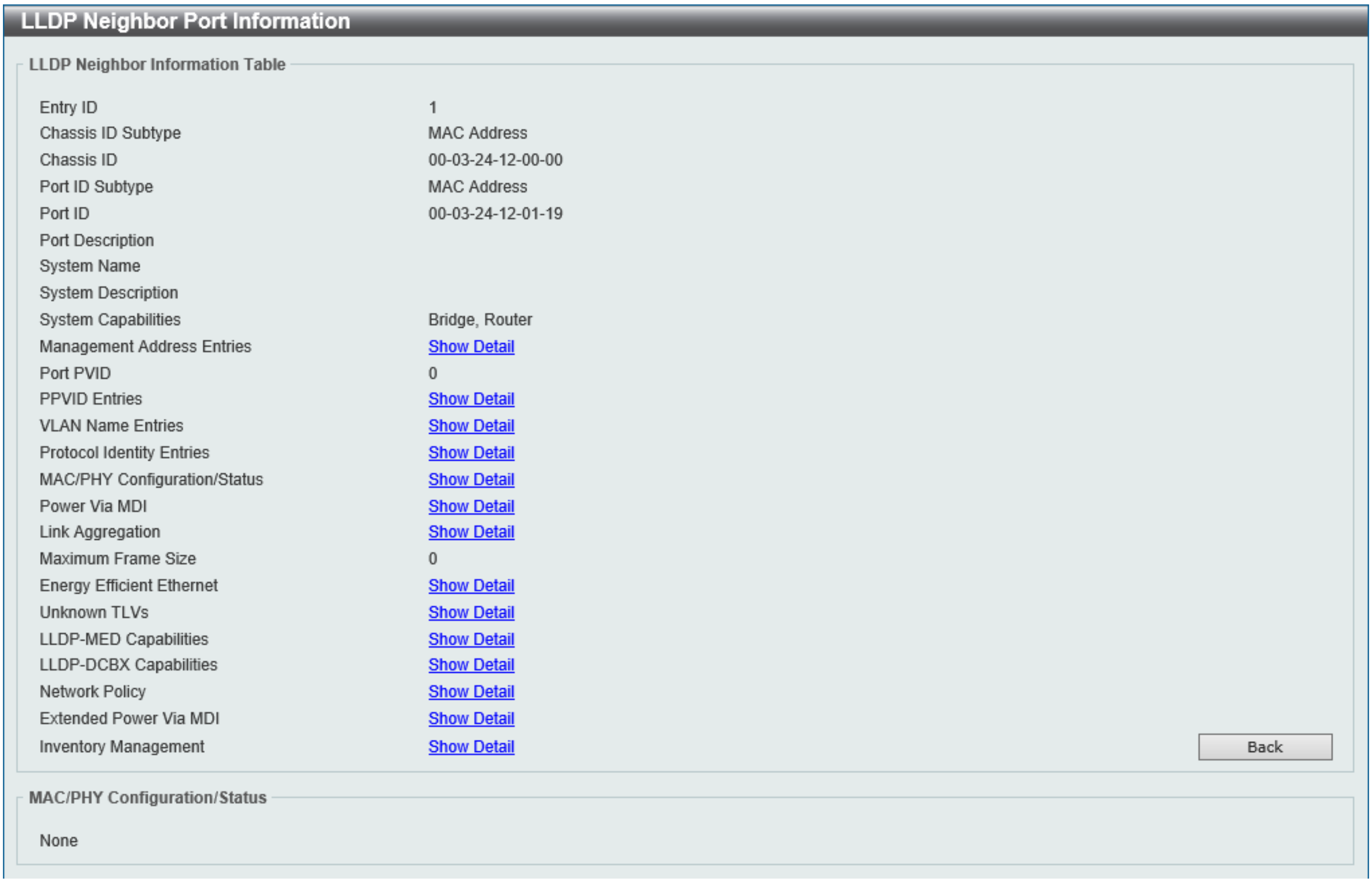
Entry ID	1
Chassis ID Subtype	MAC Address
Chassis ID	00-03-24-12-00-00
Port ID Subtype	MAC Address
Port ID	00-03-24-12-01-19
Port Description	
System Name	
System Description	
System Capabilities	Bridge, Router
Management Address Entries	Show Detail
Port PVID	0
PPVID Entries	Show Detail
VLAN Name Entries	Show Detail
Protocol Identity Entries	Show Detail
MAC/PHY Configuration/Status	Show Detail
Power Via MDI	Show Detail
Link Aggregation	Show Detail
Maximum Frame Size	0
Energy Efficient Ethernet	Show Detail
Unknown TLVs	Show Detail
LLDP-MED Capabilities	Show Detail
LLDP-DCBX Capabilities	Show Detail
Network Policy	Show Detail
Extended Power Via MDI	Show Detail
Inventory Management	Show Detail

Figure 5-99 LLDP Neighbor Port Information (Show Detail) Window

To view more details about, for example, the **MAC/PHY Configuration/Status**, click the Show Detail hyperlink.

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

After clicking the Show Detail hyperlink, a new section will appear at the bottom of the window.



LLDP Neighbor Port Information

LLDP Neighbor Information Table

Entry ID	1
Chassis ID Subtype	MAC Address
Chassis ID	00-03-24-12-00-00
Port ID Subtype	MAC Address
Port ID	00-03-24-12-01-19
Port Description	
System Name	
System Description	
System Capabilities	Bridge, Router
Management Address Entries	Show Detail
Port PVID	0
PPVID Entries	Show Detail
VLAN Name Entries	Show Detail
Protocol Identity Entries	Show Detail
MAC/PHY Configuration/Status	Show Detail
Power Via MDI	Show Detail
Link Aggregation	Show Detail
Maximum Frame Size	0
Energy Efficient Ethernet	Show Detail
Unknown TLVs	Show Detail
LLDP-MED Capabilities	Show Detail
LLDP-DCBX Capabilities	Show Detail
Network Policy	Show Detail
Extended Power Via MDI	Show Detail
Inventory Management	Show Detail

MAC/PHY Configuration/Status

None

Figure 5-100 LLDP Neighbor Port Information (Show Detail) Window

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

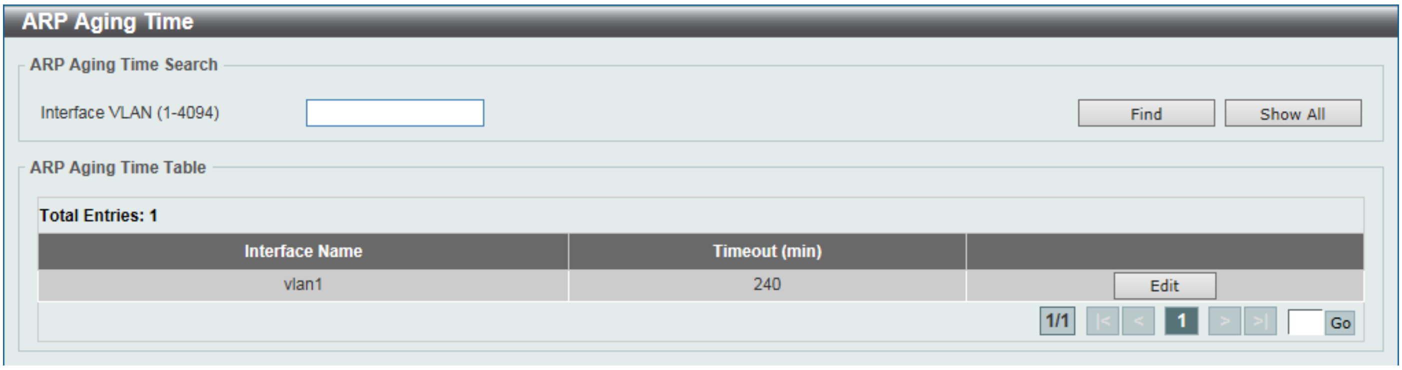
6. Layer 3 Features

ARP

ARP Aging Time

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

To view the following window, click **L3 Features > ARP > ARP Aging Time**, as shown below:



ARP Aging Time

ARP Aging Time Search

Interface VLAN (1-4094)

ARP Aging Time Table

Total Entries: 1

Interface Name	Timeout (min)	
vlan1	240	Edit

Figure 6-1 ARP Aging Time Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the interface VLAN ID here. The range is from 1 to 4094.
Timeout	After click the **Edit** button, enter the ARP aging timeout value here.

Click the **Find** button to find and display the entries, based on the information entered, in the **ARP Aging Time Table**.

Click the **Show All** button to display all the ARP aging time entries in the **ARP Aging Time Table**.

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

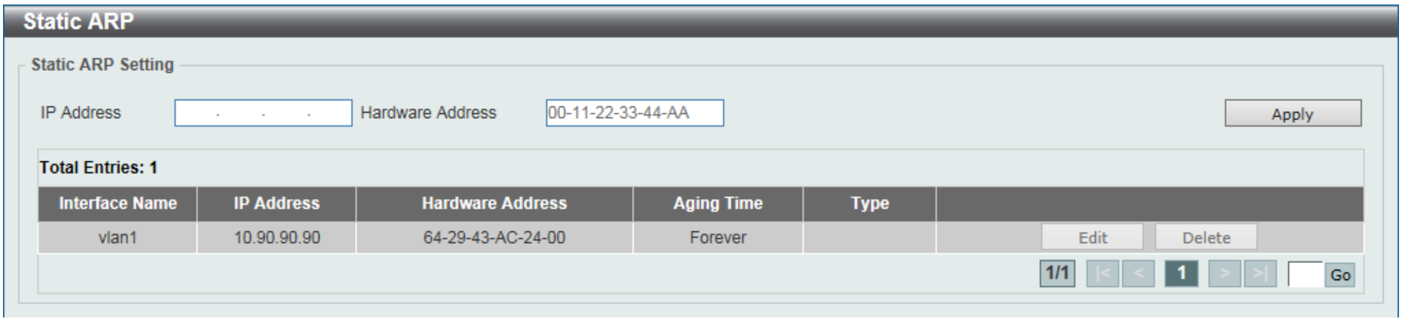
Click the **Apply** button to accept the changes made.

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:



Static ARP

Static ARP Setting

IP Address . . . Hardware Address 00-11-22-33-44-AA

Total Entries: 1

Interface Name	IP Address	Hardware Address	Aging Time	Type	
vlan1	10.90.90.90	64-29-43-AC-24-00	Forever		Edit Delete

Figure 6-2 Static ARP Window

The fields that can be configured in the **Static ARP Setting** section 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.

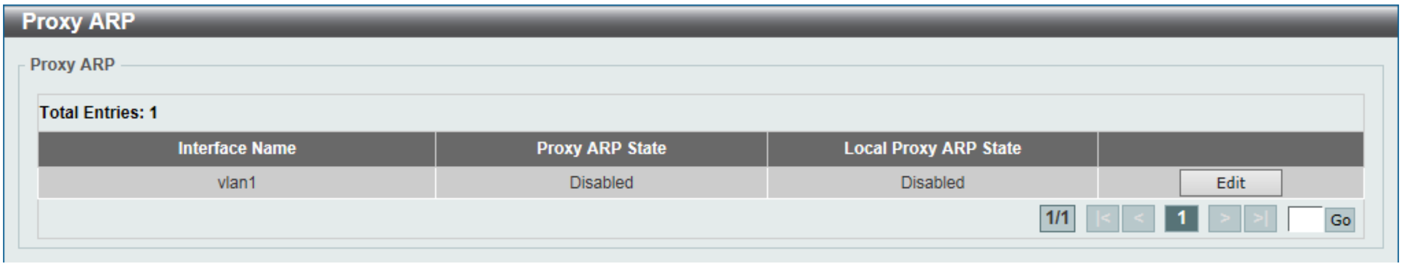
Click the **Delete** button to remove the specific entry.

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:



Proxy ARP

Proxy ARP

Total Entries: 1

Interface Name	Proxy ARP State	Local Proxy ARP State	
vlan1	Disabled	Disabled	Edit

Figure 6-3 Proxy ARP Window

After clicking the **Edit** button, 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.

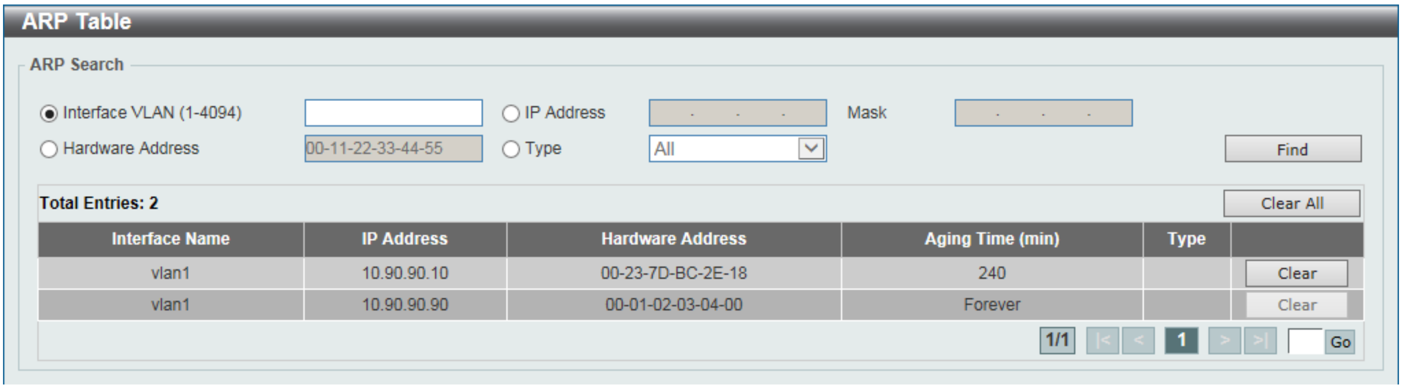
Click the **Apply** button to accept the changes made.

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:



ARP Table

ARP Search

● Interface VLAN (1-4094) ○ IP Address Mask

○ Hardware Address 00-11-22-33-44-55 ○ Type All

Total Entries: 2

Interface Name	IP Address	Hardware Address	Aging Time (min)	Type	
vlan1	10.90.90.10	00-23-7D-BC-2E-18	240		Clear
vlan1	10.90.90.90	00-01-02-03-04-00	Forever		Clear

Figure 6-4 ARP Table Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the interface VLAN ID used here. The range is from 1 to 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.
Type	Select the Type option here. Options to choose from are **All** and **Dynamic**.

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

Click the **Clear All** button to clear all dynamic ARP cache.

Click the **Clear** button to clear the dynamic ARP cache associated with the specific entry.

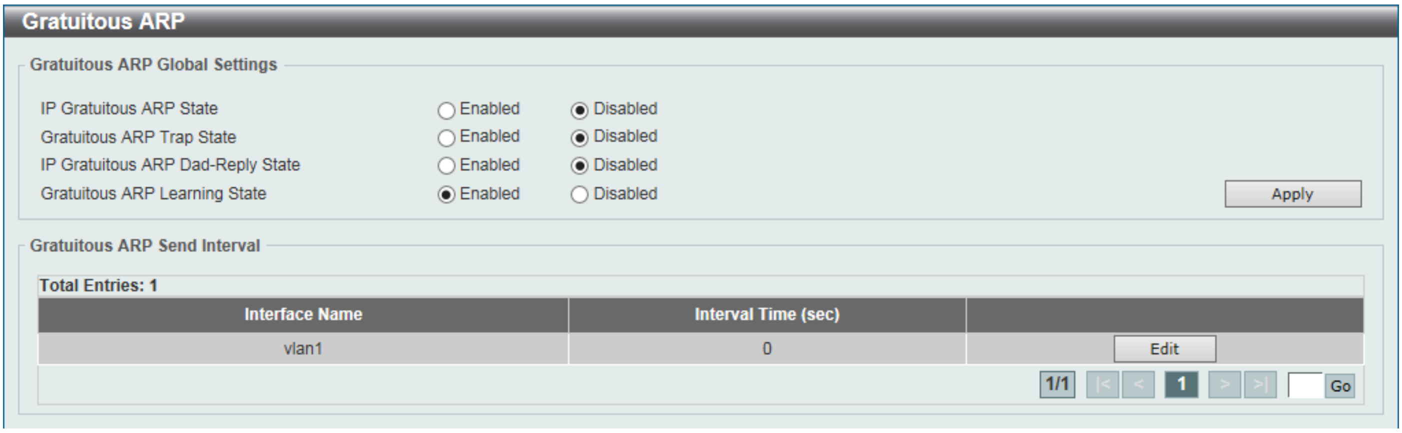
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Gratuitous ARP

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:



Gratuitous ARP

Gratuitous ARP Global Settings

IP Gratuitous ARP State	○ Enabled	● Disabled
Gratuitous ARP Trap State	○ Enabled	● Disabled
IP Gratuitous ARP Dad-Reply State	○ Enabled	● Disabled
Gratuitous ARP Learning State	● Enabled	○ Disabled

Gratuitous ARP Send Interval

Total Entries: 1

Interface Name	Interval Time (sec)	
vlan1	0	Edit

Figure 6-5 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 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:

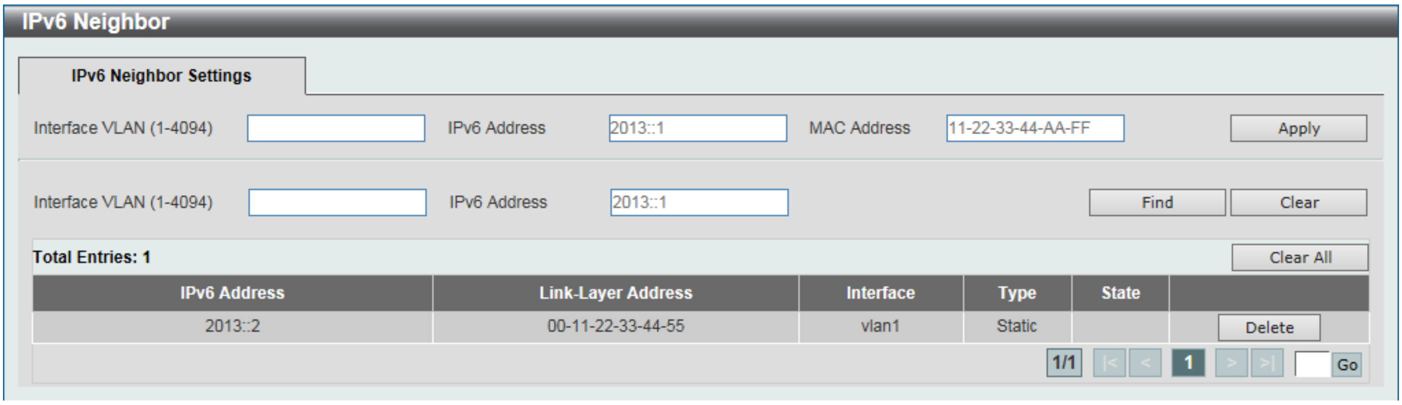
Parameter	Description
Interval Time	Enter the gratuitous ARP sending interval time, in seconds, here.

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:



IPv6 Neighbor

IPv6 Neighbor Settings

Interface VLAN (1-4094):
IPv6 Address: 2013::1
MAC Address: 11-22-33-44-AA-FF

Interface VLAN (1-4094):
IPv6 Address: 2013::1

Total Entries: 1

IPv6 Address	Link-Layer Address	Interface	Type	State	
2013::2	00-11-22-33-44-55	vlan1	Static		Delete

Figure 6-6 IPv6 Neighbor Window

The fields that can be configured are described below:

Parameter	Description
Interface VLAN	Enter the VLAN interface ID here.
IPv6 Address	Enter the IPv6 address.
MAC Address	Enter the MAC address.

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

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

Click the **Clear** button to clear all the dynamic information for the specific interface.

Click the **Clear All** button to clear all the dynamic IPv6 neighbor information in this table.

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

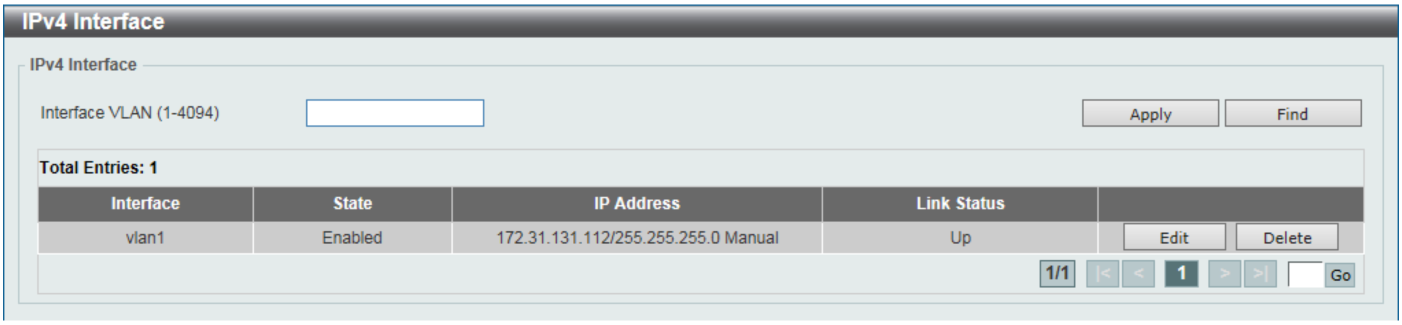
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Interface

IPv4 Interface

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

To view the following window, click **L3 Features > Interface > IPv4 Interface**, as shown below:



IPv4 Interface

IPv4 Interface

Interface VLAN (1-4094):

Total Entries: 1

Interface	State	IP Address	Link Status	
vlan1	Enabled	172.31.131.112/255.255.255.0 Manual	Up	Edit Delete

Figure 6-7 IPv4 Interface 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.

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

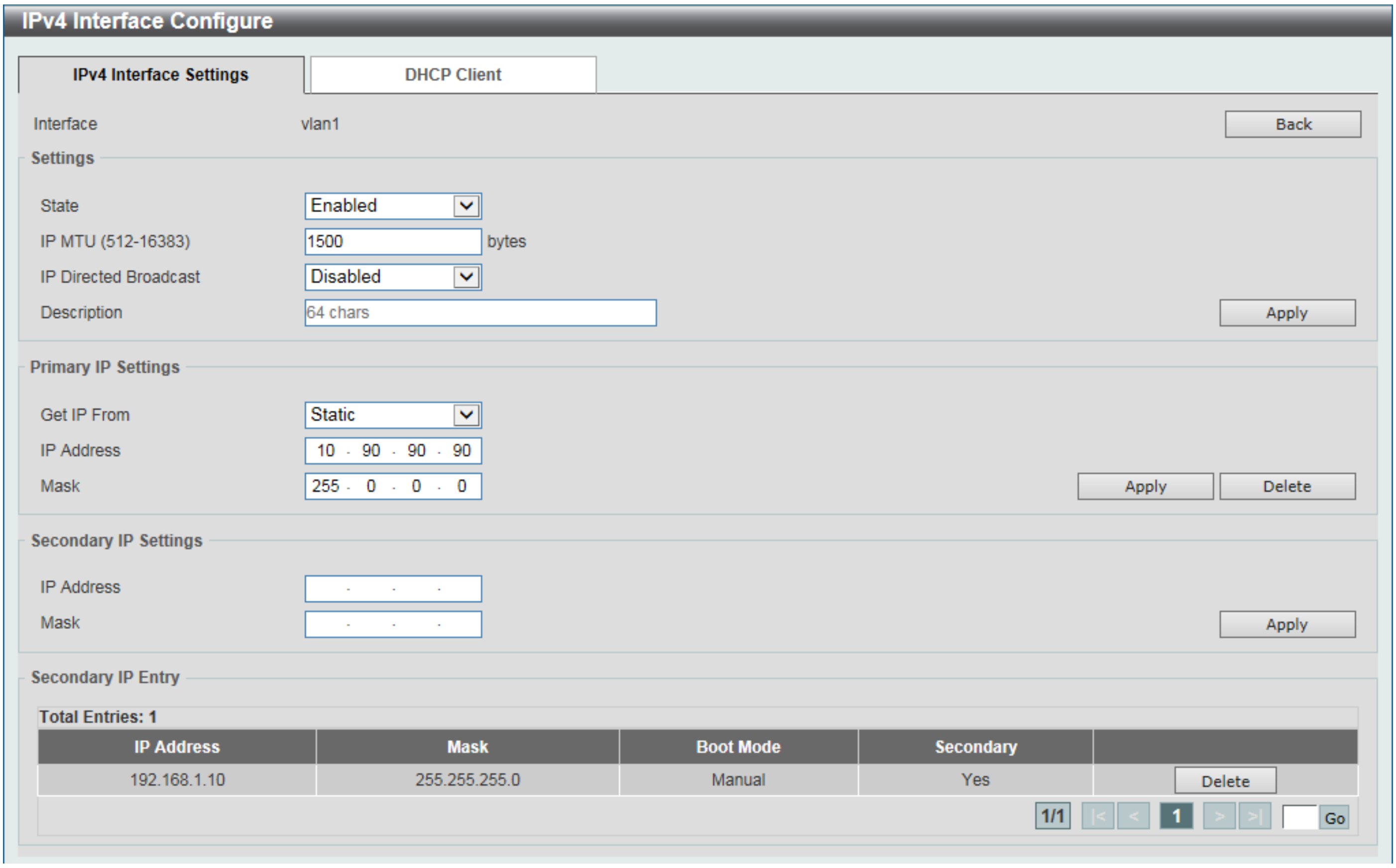
Click the **Find** button to locate a specific entry based on the information entered.

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.



IPv4 Interface Configure

Interface: vlan1

Settings

State: Enabled

IP MTU (512-16383): 1500 bytes

IP Directed Broadcast: Disabled

Description: 64 chars

Primary IP Settings

Get IP From: Static

IP Address: 10 . 90 . 90 . 90

Mask: 255 . 0 . 0 . 0

Secondary IP Settings

IP Address: . . .

Mask: . . .

Secondary IP Entry

Total Entries: 1

IP Address	Mask	Boot Mode	Secondary	
192.168.1.10	255.255.255.0	Manual	Yes	Delete

Figure 6-8 IPv4 Interface (Edit) Window

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

Parameter	Description
State	Select to enable or disable the IPv4 interface global state.
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 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.

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

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

The fields that can be configured in the **Primary IP Settings** section are described below:

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

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

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

The fields that can be configured in the **Secondary IP Settings** section are described below:

Parameter	Description
IP Address	Enter the secondary IPv4 address for this interface here.
Mask	Enter the secondary IPv4 subnet mask for this interface here.

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

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

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.

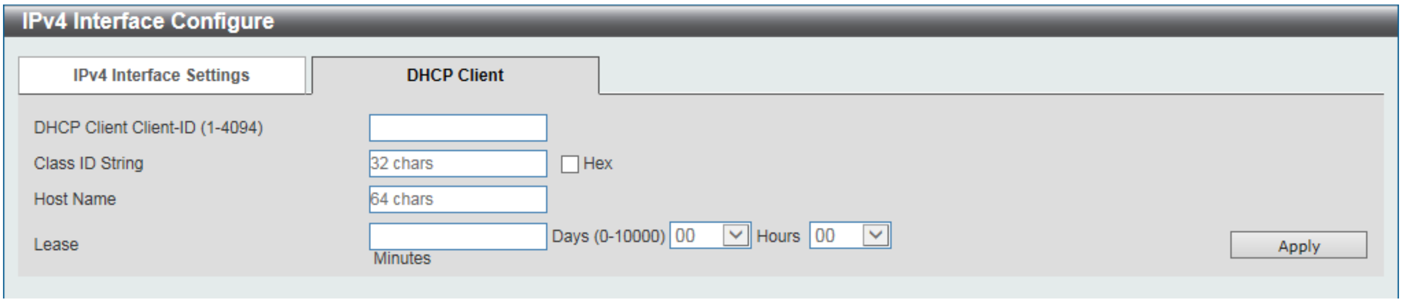


Figure 6-9 IPv4 Interface (Edit, DHCP Client) Window

The fields that can be configured are described below:

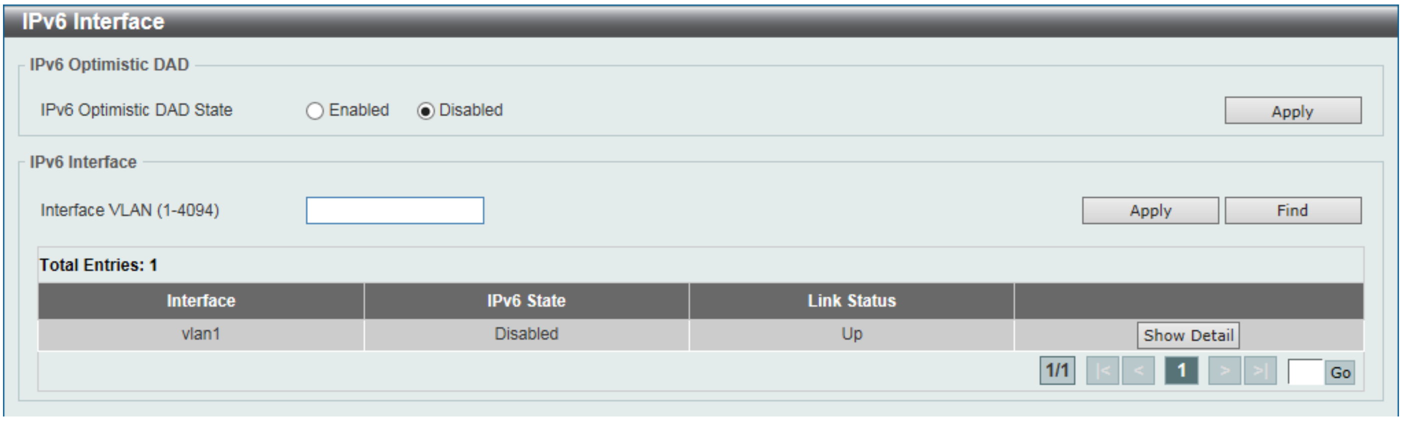
Parameter	Description
DHCP Client Client-ID	Enter the DHCP Client ID here. The range is from 1 to 4094. This parameter is used to specify the VLAN interface whose hexadecimal MAC address will be used as the client ID sent with the discover message.
Class ID String	Enter the class ID string here. This 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.
Host Name	Enter the host name here. This string can be up to 64 characters long. This parameter is used to specify the value of the host name option to be sent with the DHCP discover message.
Lease	Enter and optionally select the DHCP client lease time here. In the textbox, the lease time, in days, can be entered. The range is from 0 to 10000 days. **Hours** and **Minutes** can also be selected optionally.

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

IPv6 Interface

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

To view the following window, click **L3 Features > Interface > IPv6 Interface**, as shown below:



IPv6 Interface

IPv6 Optimistic DAD

IPv6 Optimistic DAD State ○ Enabled ● Disabled [Apply]

IPv6 Interface

Interface VLAN (1-4094) [Apply] [Find]

Total Entries: 1

Interface	IPv6 State	Link Status	
vlan1	Disabled	Up	Show Detail

Figure 6-10 IPv6 Interface Window

The fields that can be configured in **IPv6 Optimistic DAD** are described below:

Parameter	Description
IPv6 Optimistic DAD State	Select to enable or disable the IPv6 Optimistic Duplicate Address Detection (DAD) state here.

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

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

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

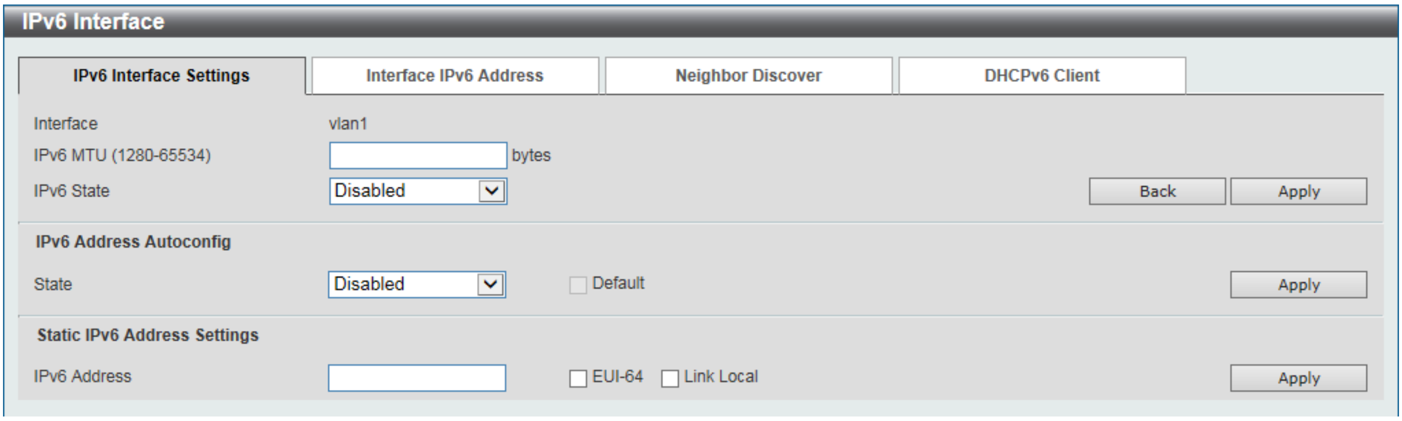
Click the **Apply** button to accept the changes made.

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

Click the **Show Detail** button to view and configure detailed settings for the IPv6 interface entry.

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

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



IPv6 Interface

Interface vlan1

IPv6 MTU (1280-65534) bytes

IPv6 State Disabled [Back] [Apply]

IPv6 Address Autoconfig

State Disabled □ Default [Apply]

Static IPv6 Address Settings

IPv6 Address □ EUI-64 □ Link Local [Apply]

Figure 6-11 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. This is used to configure the MTU to be advertised in RA messages. The range is from 1280 to 65534 bytes. By default, this value is 1500 bytes.
IPv6 State	Select to enable or disable the IPv6 interface global state here.

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

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

The fields that can be configured for **IPv6 Address Autoconfig** are described below:

Parameter	Description
State	Select to enable or disable the automatic configuration of the IPv6 address using stateless auto-configuration here. Select the **Default** option to specify that if the default router is selected on this interface, a default route will be installed using that default router. This option can only be specified on one interface.

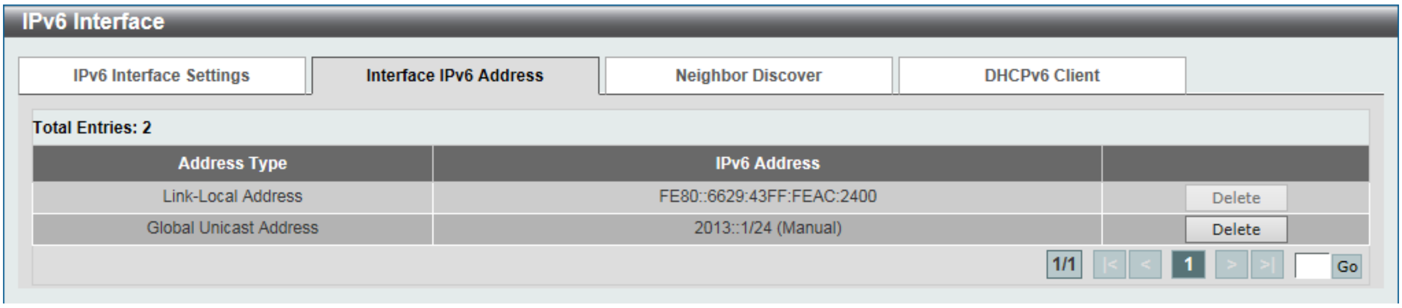
Click the **Apply** button to accept the changes made.

The fields that can be configured for **Static IPv6 Address Settings** are described below:

Parameter	Description
IPv6 Address	Enter the IPv6 address 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.

After selecting the **Interface IPv6 Address** tab option, at the top of the page, the following page will be available.



Total Entries: 2

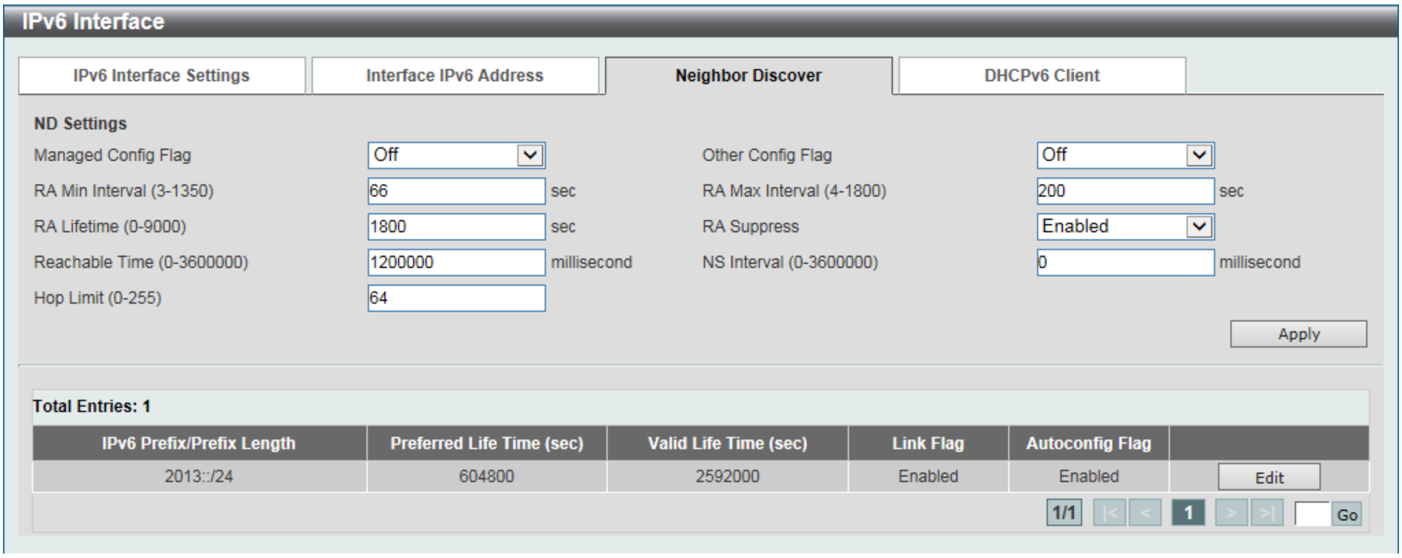
Address Type	IPv6 Address	
Link-Local Address	FE80::6629:43FF:FEAC:2400	Delete
Global Unicast Address	2013::1/24 (Manual)	Delete

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

After selecting the **Neighbor Discover** tab option, at the top of the page, the following page will be available.



ND Settings

Managed Config Flag	Off		Other Config Flag	Off	
RA Min Interval (3-1350)	66	sec	RA Max Interval (4-1800)	200	sec
RA Lifetime (0-9000)	1800	sec	RA Suppress	Enabled	
Reachable Time (0-3600000)	1200000	millisecond	NS Interval (0-3600000)	0	millisecond
Hop Limit (0-255)	64				

Total Entries: 1

IPv6 Prefix/Prefix Length	Preferred Life Time (sec)	Valid Life Time (sec)	Link Flag	Autoconfig Flag	
2013::/24	604800	2592000	Enabled	Enabled	Edit

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

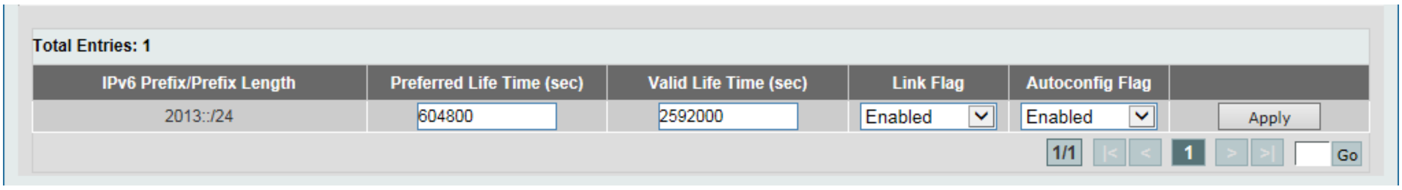
The fields that can be configured for **ND Settings** are described below:

Parameter	Description
Managed Config Flag	Turn the Managed Config Flag option **On** or **Off** here. When the neighbor host receives the RA which has flag turned on, the host should use a stateful configuration protocol to obtain IPv6 addresses.
Other Config Flag	Turn the Other Config Flag option **On** or **Off** here. By setting the other configuration flag on, the router instructs the connected hosts to use a stateful configuration protocol to obtain auto-configuration information other than the IPv6 address.
RA Min Interval	Enter the minimum RA interval time value here. The range is from 3 to 1350 seconds. This value must be smaller than 0.75 times the maximum value.
RA Max Interval	Enter the maximum RA interval time value here. The range is from 4 to 1800 seconds.
RA Lifetime	Enter the RA lifetime value here. The range is from 0 to 9000 seconds. The lifetime value in RA instructs the received host the lifetime value for taking the router as the default router.
RA Suppress	Select to enable or disable the RA suppress feature here.
Reachable Time	Enter the Reachable Time here. The range is from 0 to 3600000 milliseconds. If the specified time is 0, the router will use 1200 seconds on the interface and advertise 0 (unspecified) in the RA message. The Reachable Time is used by the IPv6 node in determining the reachability of the neighbor nodes.
NS Interval	Enter the Neighbor Solicitation (NS) interval value here. The range is from 0 to 3600000 milliseconds, in multiples of 1000. If the specified time is 0, the router will use 1 second on the interface and advertise 0 (unspecified) in the Router Advertisement (RA) message.
Hop Limit	Enter the hop limit value here. The range is from 0 to 255. The IPv6 packet originated by the system will also use this value as the initial hop limit.

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

Click the **Edit** button to modify the settings in the specified entry.

After clicking the **Edit** button, the fields that can be configured in the table are described below:



Total Entries: 1

IPv6 Prefix/Prefix Length	Preferred Life Time (sec)	Valid Life Time (sec)	Link Flag	Autoconfig Flag	
2013::/24	604800	2592000	Enabled	Enabled	Apply

Figure 6-14 IPv6 Interface (Detail, Neighbor Discover, Edit) Window

After clicking the **Edit** button the following can be configured:

Parameter	Description
Preferred Life Time	Enter the preferred lifetime value here. The range is from 0 to 4294967295 seconds.
Valid Life Time	Enter the valid lifetime value here. The range is from 0 to 4294967295 seconds.
Link Flag	Select to enable or disable the link flag function here.
Autoconfig Flag	Select to enable or disable the auto-configure flag function here.

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

After selecting the **DHCPv6 Client** tab option, at the top of the page, the following page will be available.

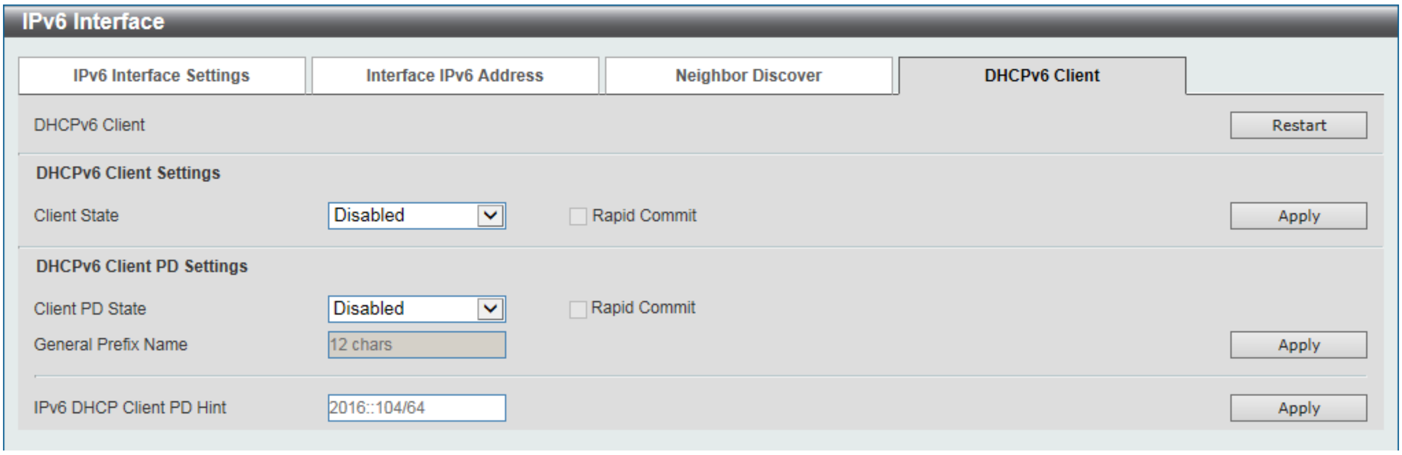


Figure 6-15 IPv6 Interface (Detail, DHCPv6 Client) Window

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.

The fields that can be configured for **DHCPv6 Client PD Settings** are described below:

Parameter	Description
Client PD State	Select to enable or disable the DHCPv6 client process that requests a Prefix Delegation (PD) through a specified interface.

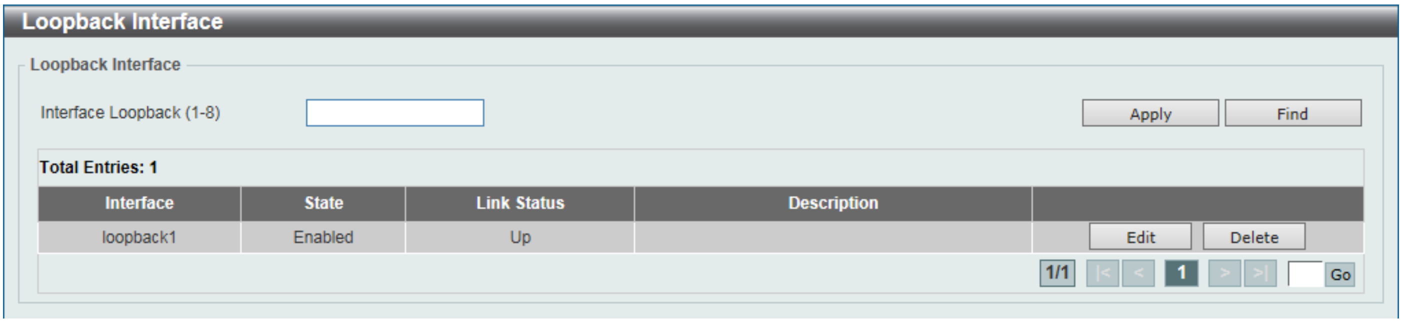
Parameter	Description
	Select the **Rapid Commit** option to proceed with two-message exchange for prefix delegation. The rapid-commit option will be included in the Solicit message to request a two-message handshake.
General Prefix Name	Enter the IPv6 general prefix name here. This name can be up to 12 characters long.
IPv6 DHCP Client PD Hint	Enter the IPv6 prefix to be sent in the message as a hint here.

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

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:



Loopback Interface

Loopback Interface

Interface Loopback (1-8)

Total Entries: 1

Interface	State	Link Status	Description	
loopback1	Enabled	Up		Edit Delete

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.

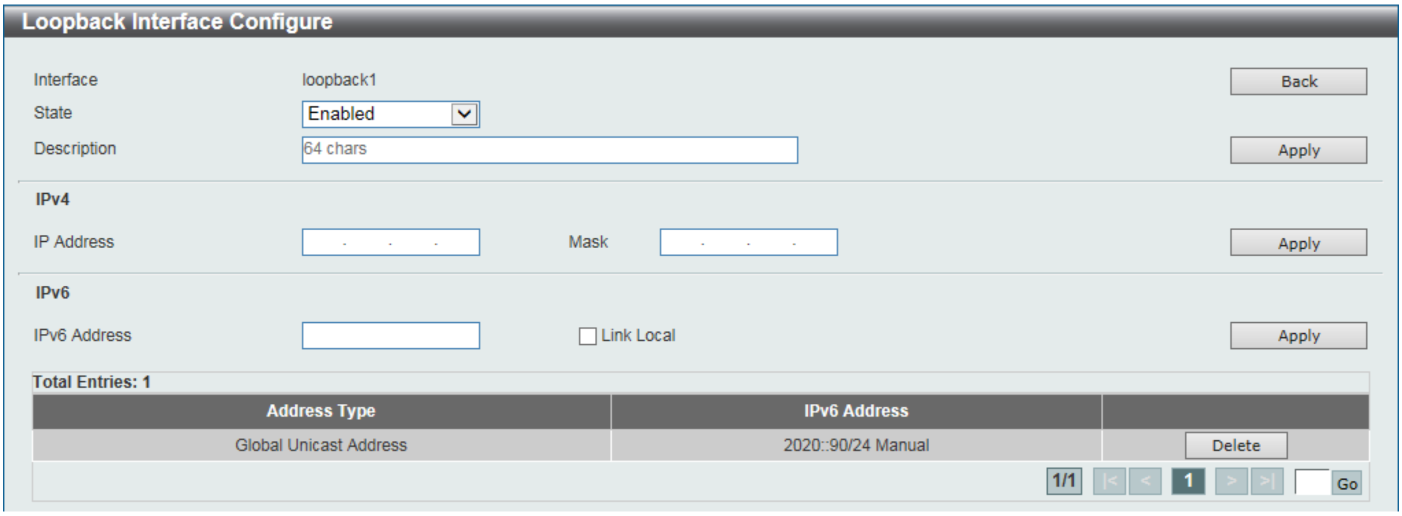
Click the **Find** button to locate a specific entry based on the information entered.

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.



Loopback Interface Configure

Interface: loopback1

State: Enabled

Description: 64 chars

IPv4

IP Address: . . . — Mask: . . .

IPv6

IPv6 Address: — □ Link Local

Total Entries: 1

Address Type	IPv6 Address	
Global Unicast Address	2020::90/24 Manual	Delete

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 the link-local IPv6 address.

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

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

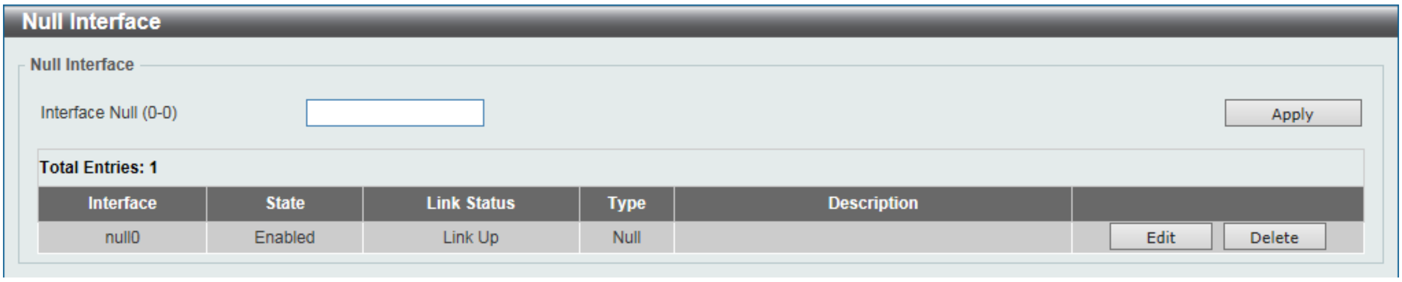
Click the **Delete** button to delete the specified entry.

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.

To view the following window, click **L3 Features > Interface > Null Interface**, as shown below:



Null Interface

Null Interface

Interface Null (0-0):

Total Entries: 1

Interface	State	Link Status	Type	Description	
null0	Enabled	Link Up	Null		Edit Delete

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.

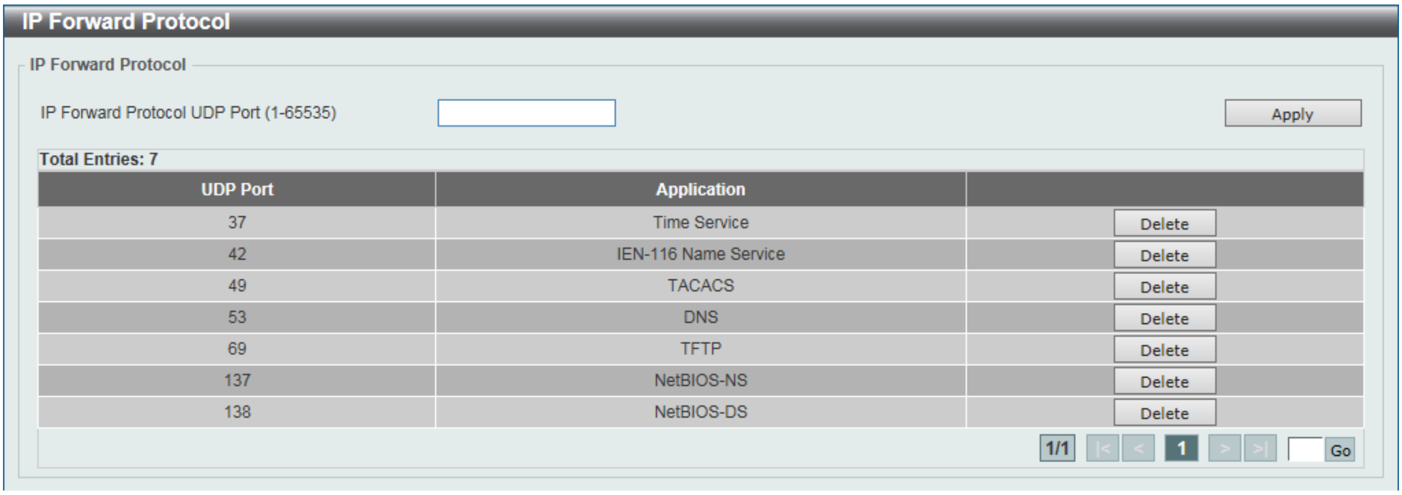
Click the **Delete** button to delete the specified entry.

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:



UDP Port	Application	
37	Time Service	Delete
42	IEN-116 Name Service	Delete
49	TACACS	Delete
53	DNS	Delete
69	TFTP	Delete
137	NetBIOS-NS	Delete
138	NetBIOS-DS	Delete

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.

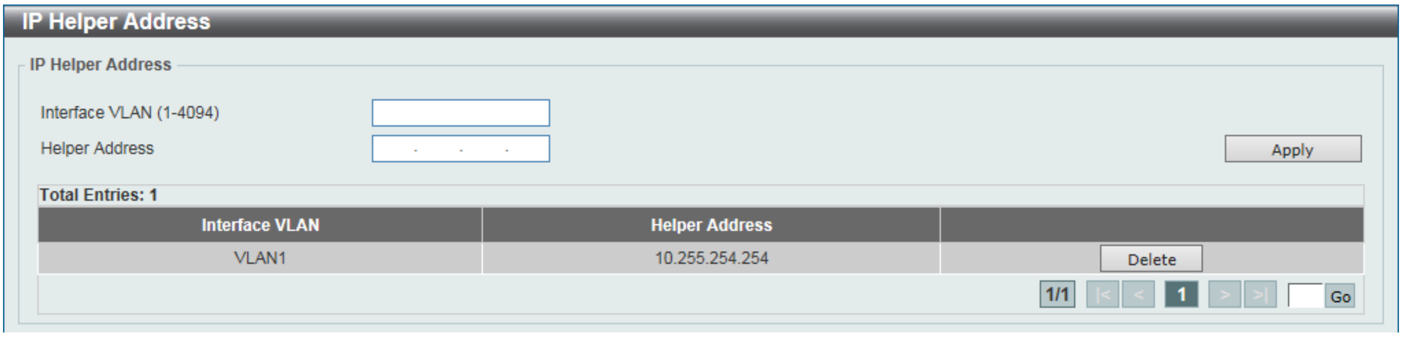
IP Helper Address

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:



IP Helper Address

IP Helper Address

Interface VLAN (1-4094)

Helper Address

Total Entries: 1

Interface VLAN	Helper Address	
VLAN1	10.255.254.254	Delete

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.

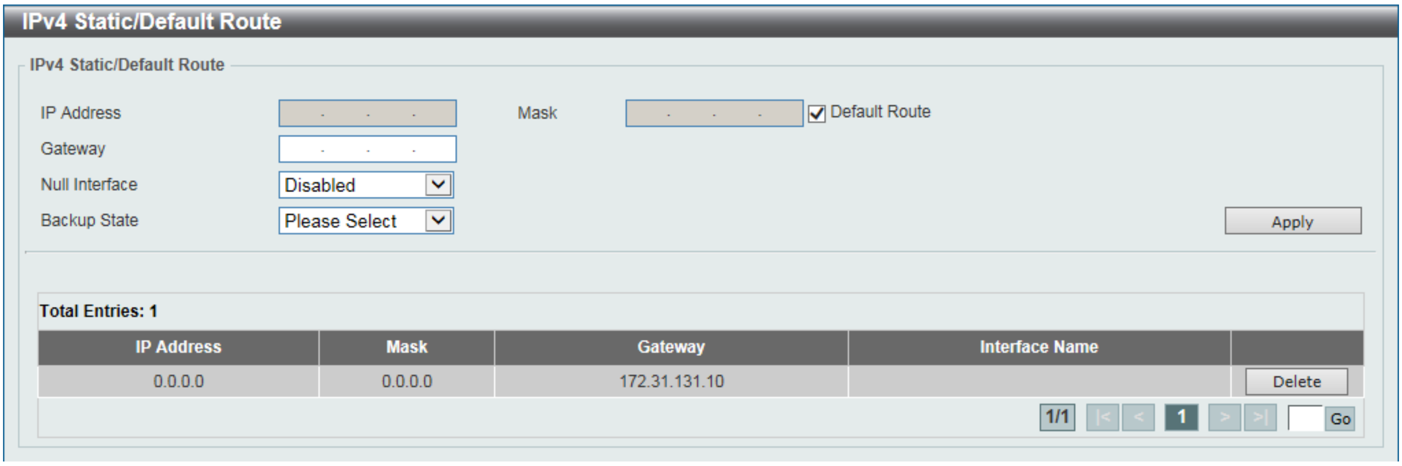
IPv4 Static/Default Route

This window is used to display and configure the IPv4 static and default route settings. The Switch supports static routing for IPv4 formatted addressing. When an IPv4 static route is defined, the Switch will send an ARP request packet to the next hop router. When the ARP response is retrieved by the Switch from that next hop, the route becomes enabled. However, if the ARP entry already exists, an ARP request will not be sent.

The Switch also supports a floating static route, which means that the user may create an alternative static route with a different next hop. This secondary next hop device route is considered as a backup static route when the primary static route is down. If the primary route is lost, the backup route will become active and begin forwarding traffic.

Entries into the Switch's forwarding table can be made using an IP address, subnet mask, and gateway.

To view the following window, click **L3 Features > IPv4 Static/Default Route**, as shown below:



IPv4 Static/Default Route

IPv4 Static/Default Route

IP Address: . . . Mask: . . . ☑ Default Route

Gateway: . . .

Null Interface: Disabled

Backup State: Please Select

Total Entries: 1

IP Address	Mask	Gateway	Interface Name	
0.0.0.0	0.0.0.0	172.31.131.10		Delete

Figure 6-21 IPv4 Static/Default Route Window

The fields that can be configured are described below:

Parameter	Description
IP Address	When **Default Route** is not selected, enter the IPv4 address for this route here.
Mask	When **Default Route** is not selected, enter the IPv4 network mask for this route here.
Default Route	Select this option to use the default route as the IPv4 address.
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. Options to choose from are: • **Primary** - Specifies the route as the primary route to the destination. • **Backup** - Specifies the route as the backup route to the destination.

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

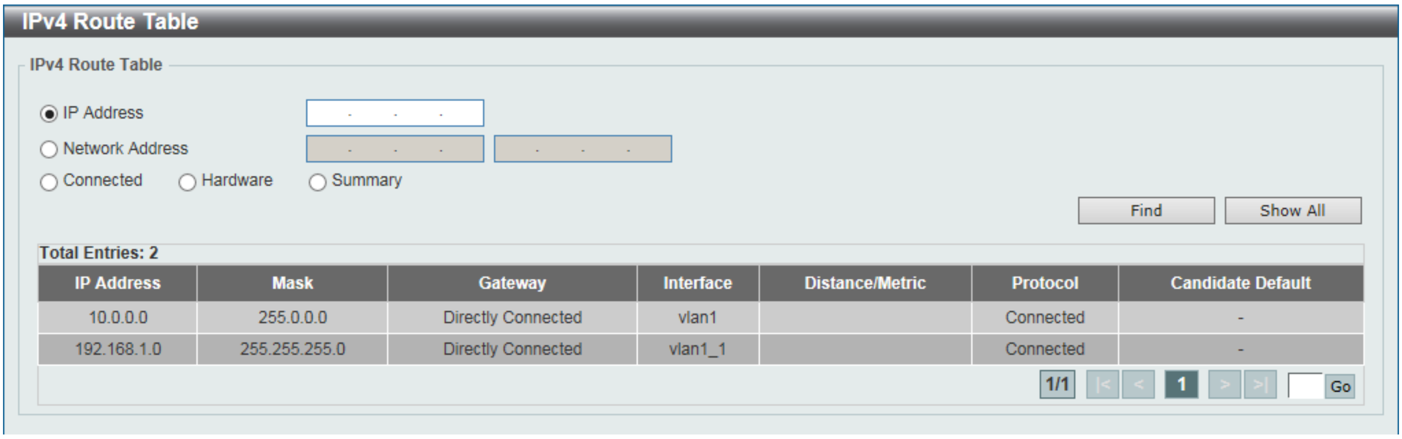
Click the **Delete** button to remove the specific entry.

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

IPv4 Route Table

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

To view the following window, click **L3 Features > IPv4 Route Table**, as shown below:



IPv4 Route Table

IPv4 Route Table

● IP Address: . . .

○ Network Address: . . . | . . .

○ Connected ○ Hardware ○ Summary

Total Entries: 2

IP Address	Mask	Gateway	Interface	Distance/Metric	Protocol	Candidate Default
10.0.0.0	255.0.0.0	Directly Connected	vlan1		Connected	-
192.168.1.0	255.255.255.0	Directly Connected	vlan1_1		Connected	-

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 network prefix and in the second space enter the network mask.
Connected	Select this option to display only connected routes.
Hardware	Select this option to display only hardware routes. Hardware routes are routes that have been written into the hardware chip.
Summary	Select this option to display a summary and count of the route sources configured on this Switch.

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

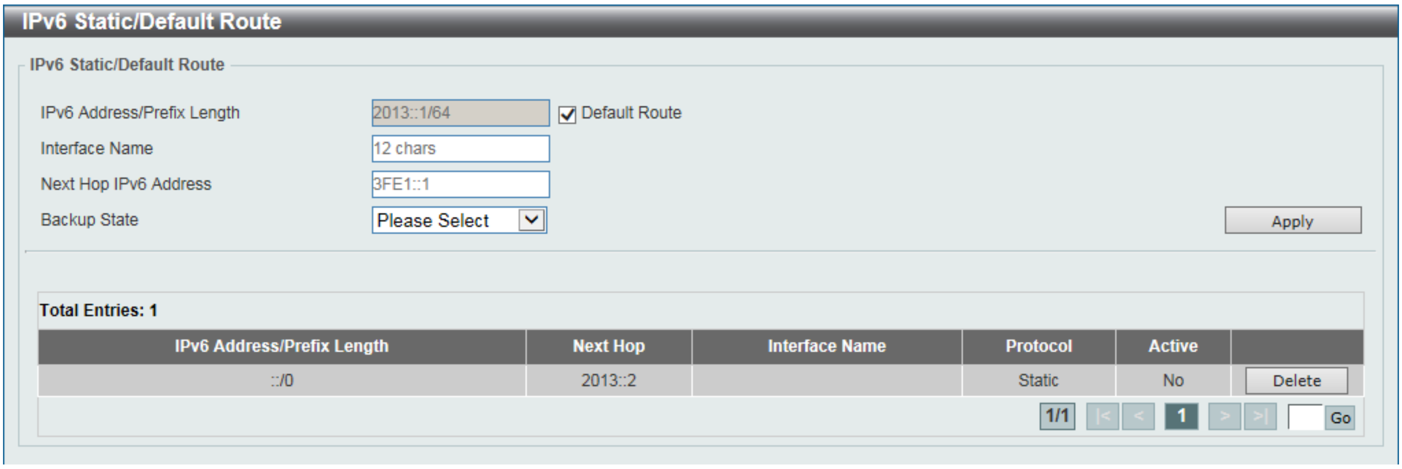
Click the **Show All** button to display all the entries in the table.

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

IPv6 Static/Default Route

This window is used to display and configure the IPv6 static or default routes.

To view the following window, click **L3 Features > IPv6 Static/Default Route**, as shown below:



IPv6 Static/Default Route

IPv6 Static/Default Route

IPv6 Address/Prefix Length: 2013::1/64 ☑ Default Route

Interface Name: 12 chars

Next Hop IPv6 Address: 3FE1::1

Backup State: Please Select

Total Entries: 1

IPv6 Address/Prefix Length	Next Hop	Interface Name	Protocol	Active	
::/0	2013::2		Static	No	Delete

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. Select **Default Route** to use this route as the default route.
Interface Name	Enter the name of the interface that will be associated with this route here.
Next Hop IPv6 Address	Enter the next hop IPv6 address here.
Backup State	Select the backup state option here. Options to choose from are: • **Primary** - The route is specified as the primary route to the destination. • **Backup** - The route is specified as the backup route to the destination.

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

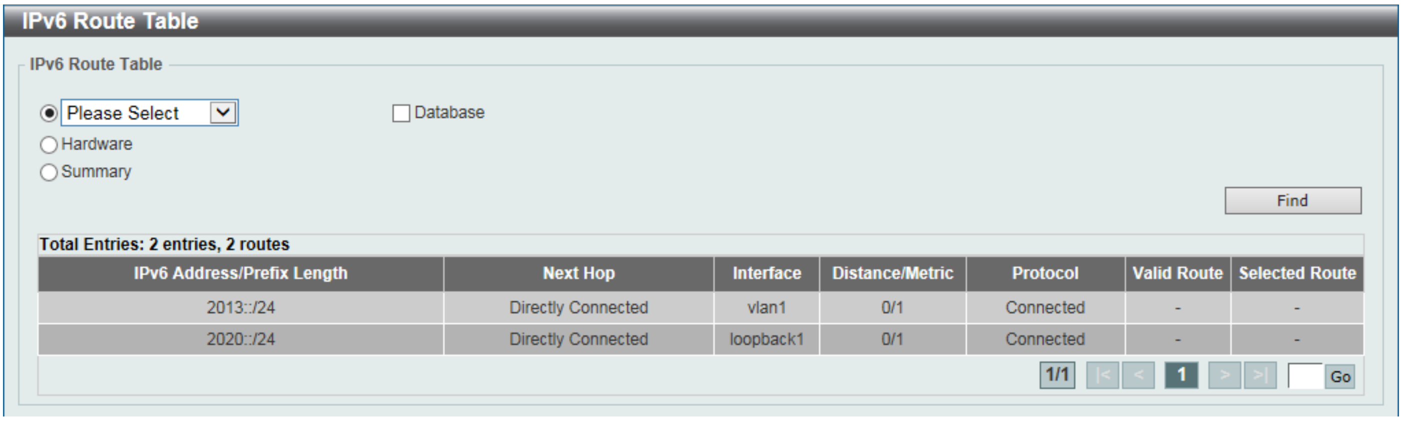
Click the **Delete** button to remove the specific entry.

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

IPv6 Route Table

This window is used to display and configure the IPv6 route table.

To view the following window, click **L3 Features > IPv6 Route Table**, as shown below:



● Please Select
□ Database
○ Hardware
○ Summary

Total Entries: 2 entries, 2 routes

IPv6 Address/Prefix Length	Next Hop	Interface	Distance/Metric	Protocol	Valid Route	Selected Route
2013::/24	Directly Connected	vlan1	0/1	Connected	-	-
2020::/24	Directly Connected	loopback1	0/1	Connected	-	-

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.
Database	Select this option to display all the related entries in the routing database instead of just the best route.
Hardware	Select this option to display only hardware routes. Hardware routes are routes that have been written into the hardware chip.
Summary	Select this option to display a summary and count of the route sources configured on this Switch.

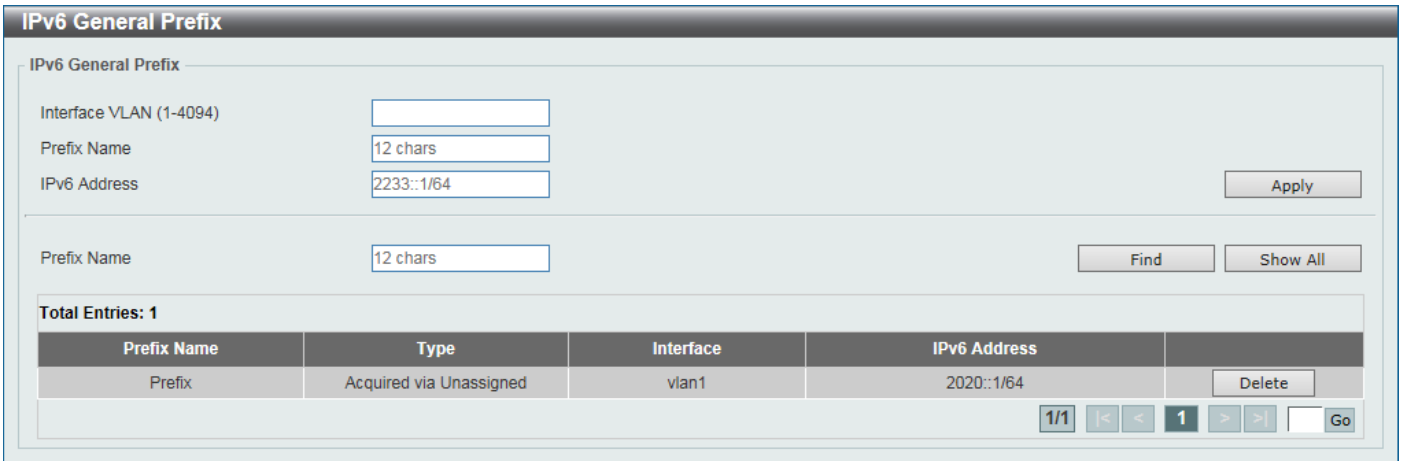
Click the **Find** button to locate a specific entry based on the information entered.

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

IPv6 General Prefix

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

To view the following window, click **L3 Features > IPv6 General Prefix**, as shown below:



IPv6 General Prefix

IPv6 General Prefix

Interface VLAN (1-4094):

Prefix Name: 12 chars

IPv6 Address: 2233::1/64

Prefix Name: 12 chars

Total Entries: 1

Prefix Name	Type	Interface	IPv6 Address	
Prefix	Acquired via Unassigned	vlan1	2020::1/64	Delete

Figure 6-25 IPv6 General Prefix 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.
Prefix Name	Enter the IPv6 general prefix entry name here. This name can be up to 12 characters long.
IPv6 Address	Enter the IPv6 address and prefix length here. The prefix length of the IPv6 address is also the local subnet on the VLAN interface.

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

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

Click the **Show All** button to display all the IPv6 general prefix entries in the 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.

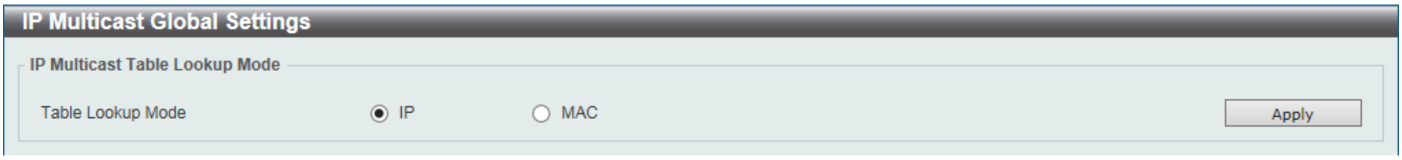
IP Multicast Routing Protocol

IPMC

IP Multicast Global Settings

This window is used to display and configure the global IP Multicast (IPMC) settings.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > IPMC > IP Multicast Global Settings**, as shown below:



IP Multicast Global Settings

IP Multicast Table Lookup Mode

Table Lookup Mode: ● IP ○ MAC

Figure 6-26 IP Multicast Global Settings Window

The fields that can be configured are described below:

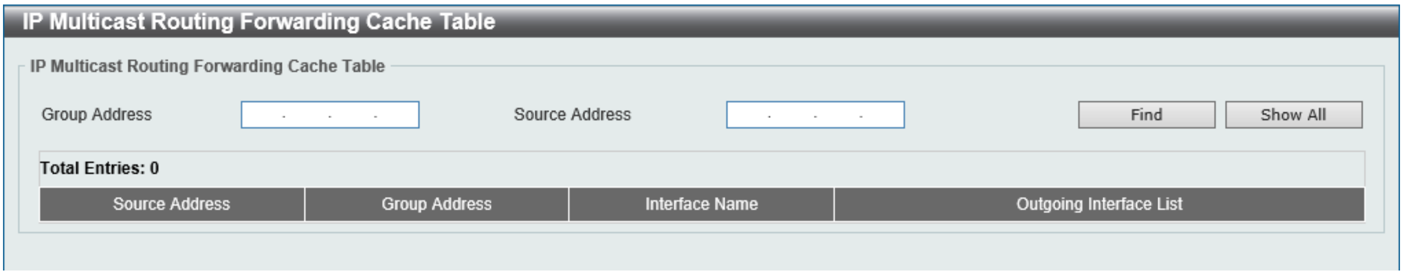
Parameter	Description
Table Lookup Mode	Select to the multicasting forwarding lookup mode. Options to choose from are: • **IP** - Specifies that multicasting forwarding lookup is based on IP address. • **MAC** - Specifies that multicasting forwarding lookup is based on MAC address.

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

IP Multicast Routing Forwarding Cache Table

This window is used to display the content of the IP multicast routing forwarding cache database.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > IPMC > IP Multicast Routing Forwarding Cache Table**, as shown below:



IP Multicast Routing Forwarding Cache Table

IP Multicast Routing Forwarding Cache Table

Group Address: . . .

Source Address: . . .

Total Entries: 0

Source Address	Group Address	Interface Name	Outgoing Interface List

Figure 6-27 IP Multicast Routing Forwarding Cache Table Window

The fields that can be configured are described below:

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

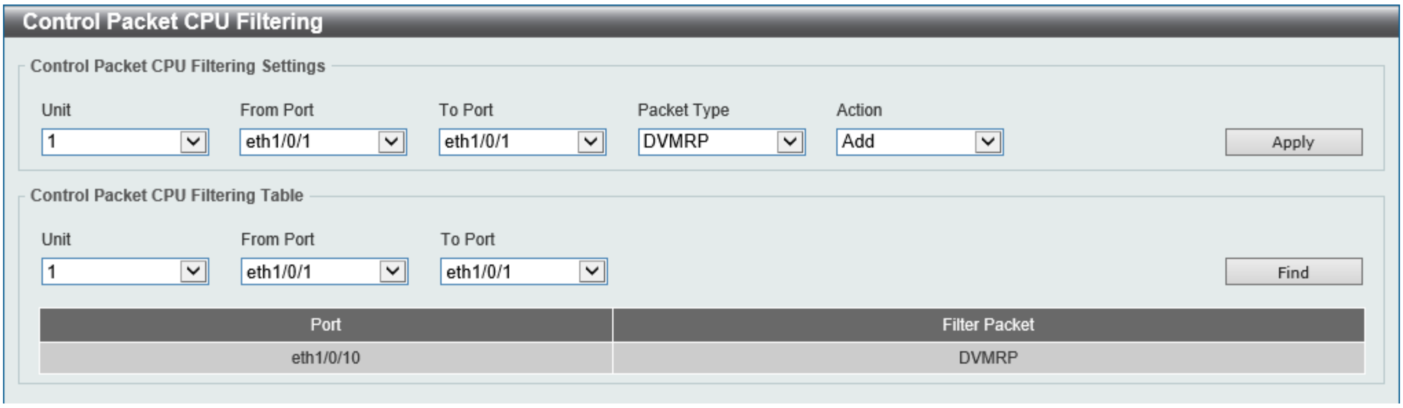
Click the **Find** button to locate a specific entry based on the information entered.

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

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:



Control Packet CPU Filtering

Control Packet CPU Filtering Settings

Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1
Packet Type: DVMRP
Action: Add

Control Packet CPU Filtering Table

Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1

Port	Filter Packet
eth1/0/10	DVMRP

Figure 6-28 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.
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. • **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 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.

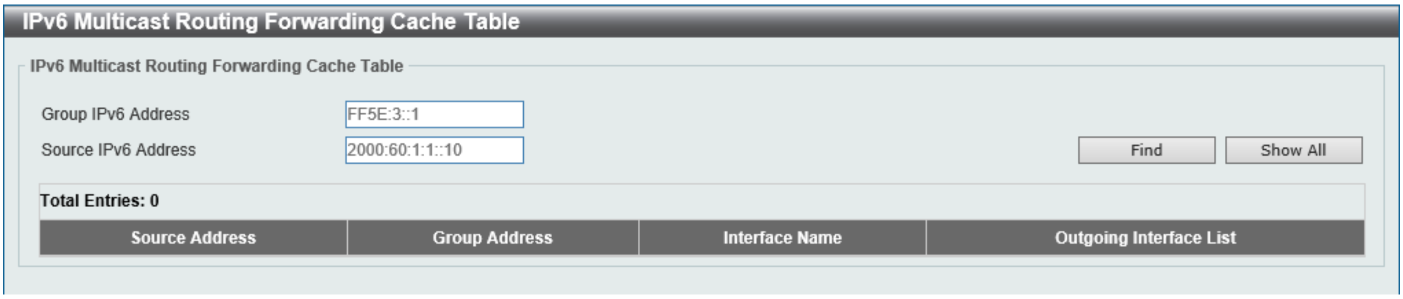
Click the **Find** button to find and display entries based on the selections made.

IPv6MC

IPv6 Multicast Routing Forwarding Cache Table

This window is used to display the contents of the IPv6 multicast routing forwarding cache database.

To view the following window, click **L3 Features > IP Multicast Routing Protocol > IPv6MC > IPv6 Multicast Routing Forwarding Cache Table**, as shown below:



IPv6 Multicast Routing Forwarding Cache Table
IPv6 Multicast Routing Forwarding Cache Table
Find
Show All

Group IPv6 Address: FF5E:3::1

Source IPv6 Address: 2000:60:1:1::10

Total Entries: 0

Source Address	Group Address	Interface Name	Outgoing Interface List

Figure 6-29 IPv6 Multicast Routing Forwarding Cache Table Window

The fields that can be configured are described below:

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

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

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

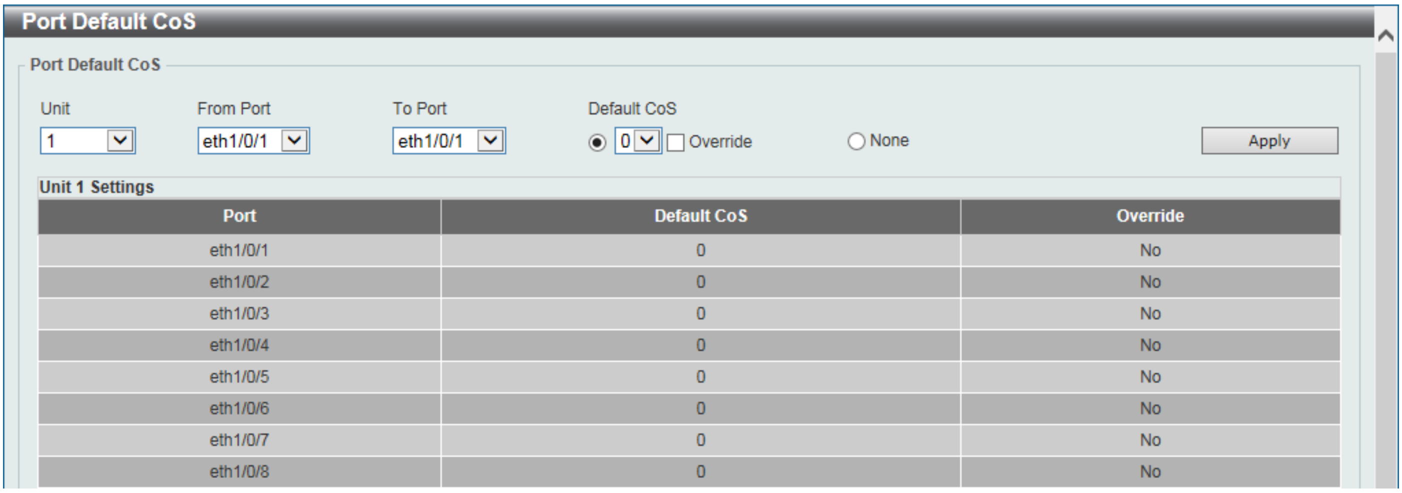
7. Quality of Service (QoS)

Basic Settings

Port Default CoS

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

To view the following window, click **QoS > Basic Settings > Port Default CoS**, as shown below:



Port Default CoS

Port Default CoS

Unit: 1 | From Port: eth1/0/1 | To Port: eth1/0/1 | Default CoS: ● 0 □ Override ○ None

Unit 1 Settings

Port	Default CoS	Override
eth1/0/1	0	No
eth1/0/2	0	No
eth1/0/3	0	No
eth1/0/4	0	No
eth1/0/5	0	No
eth1/0/6	0	No
eth1/0/7	0	No
eth1/0/8	0	No

Figure 7-1 Port Default CoS Window

The fields that can be configured are described below:

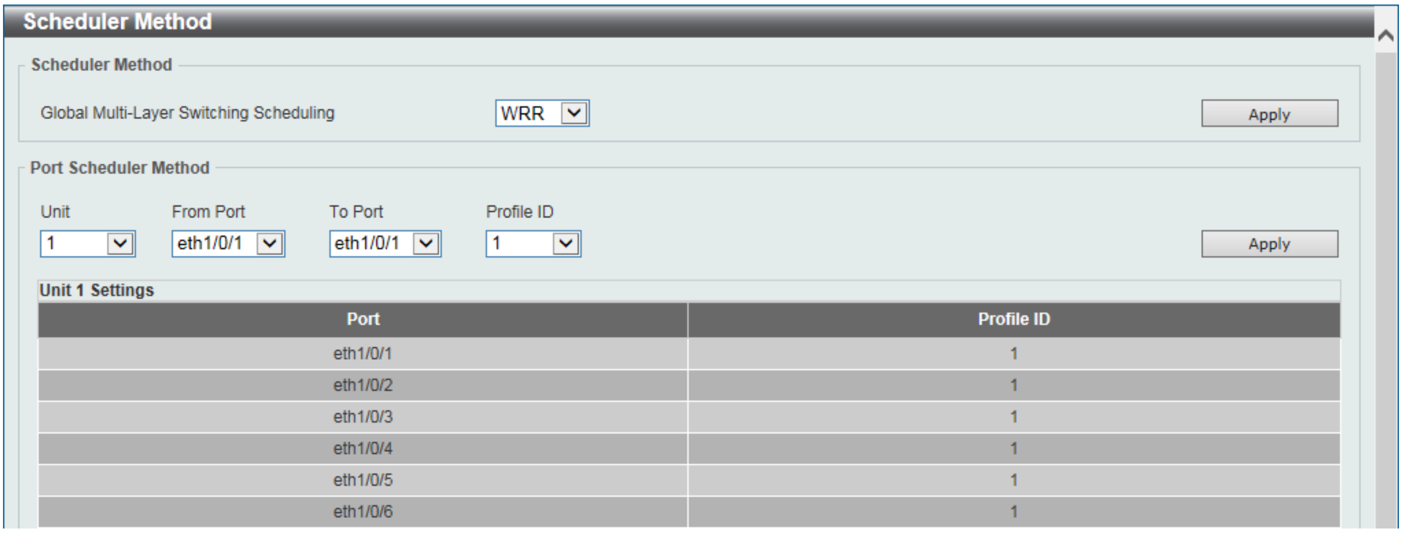
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Default CoS	Select the default CoS option for the port(s) specified here. Options to choose from are 0 to 7. Select 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.

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:



Scheduler Method

Scheduler Method

Global Multi-Layer Switching Scheduling: WRR

Port Scheduler Method

Unit: 1 | From Port: eth1/0/1 | To Port: eth1/0/1 | Profile ID: 1

Unit 1 Settings

Port	Profile ID
eth1/0/1	1
eth1/0/2	1
eth1/0/3	1
eth1/0/4	1
eth1/0/5	1
eth1/0/6	1

Figure 7-2 Port Scheduler Method Window

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

Parameter	Description
Global Multi-Layer Switching Scheduling	Select the scheduler method that will be applied to the specified port(s). Options to choose from are: • **SP** (Strict Priority) - Specifies that all queues use strict priority scheduling. It provides strict priority access to the queues from the highest CoS queue to the lowest. • **WRR** (Weighted Round-Robin) - 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. • **WDRR** (Weighted Deficit Round-Robin) - Operates by serving an accumulated set of backlogged credits in the transmit queue in a round robin order. Initially, each queue sets its credit counter to a configurable quantum value. Every time a packet from a CoS queue is sent, the size of the packet is subtracted from the corresponding credit counter and the service right is turned over to the next lower CoS queue. When the credit counter drops below 0, the queue is no longer serviced until its credits are replenished. When the credit counters of all CoS queues reaches 0, the credit counters will be replenished at that time. All packets are serviced until their credit counter is zero or negative and the last packet is transmitted completely. When this condition happens, the credits are replenished. When the credits are replenished, a quantum of credits are added to each CoS queue credit counter. The quantum for each CoS queue may be different based on the user configuration. To set a CoS queue in the **SP** mode, any higher priority CoS queue must also be in the strict priority mode. By default, the **WRR** option is used.

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

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

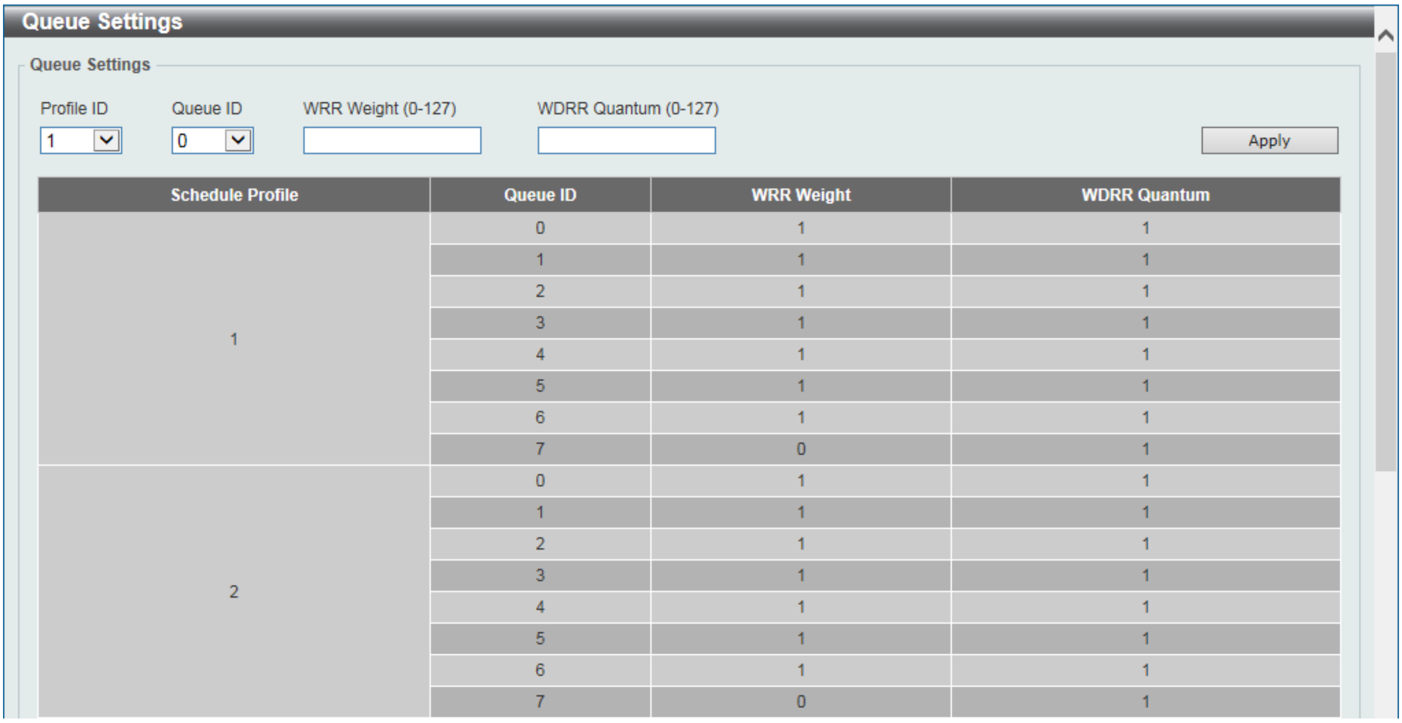
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Profile ID	Select the scheduling profile ID. The range is from 1 to 8.

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

Queue Settings

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

To view the following window, click **QoS > Basic Settings > Queue Settings**, as shown below:



Queue Settings

Queue Settings

Profile ID: 1

Queue ID: 0

WRR Weight (0-127):

WDRR Quantum (0-127):

Schedule Profile	Queue ID	WRR Weight	WDRR Quantum
1	0	1	1
	1	1	1
	2	1	1
	3	1	1
	4	1	1
	5	1	1
	6	1	1
	7	0	1
2	0	1	1
	1	1	1
	2	1	1
	3	1	1
	4	1	1
	5	1	1
	6	1	1
	7	0	1

Figure 7-3 Queue Settings Window

The fields that can be configured are described below:

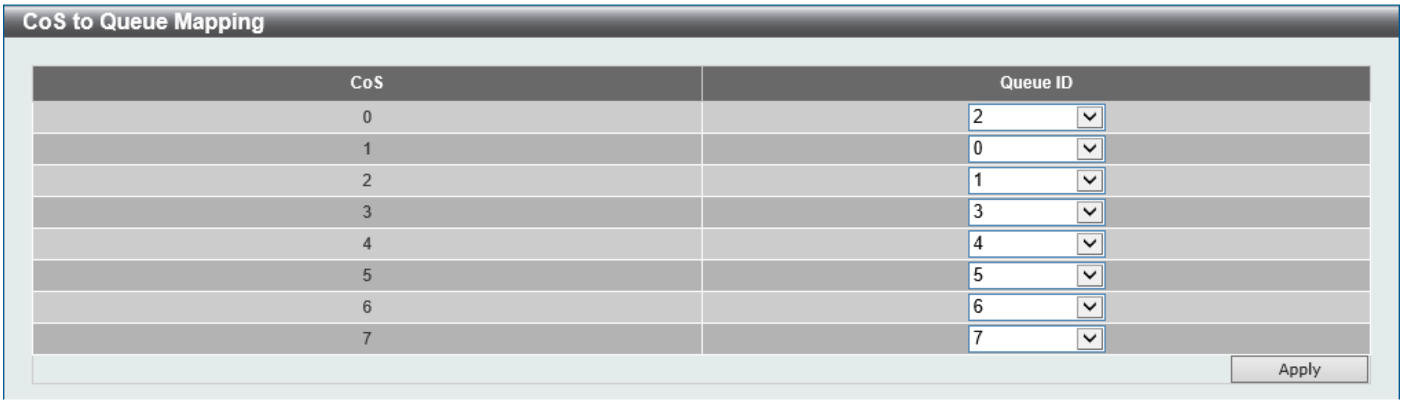
Parameter	Description
Profile ID	Select the scheduling profile ID. The range is from 1 to 8.
Queue ID	Enter the queue ID value here. The range is from 0 to 7.
WRR Weight	Enter the WRR weight value here. The range is from 0 to 127. To satisfy the behavior requirements of Expedited Forwarding (EF), the highest queue is always selected by the Per-hop Behavior (PHB) EF and the schedule mode of this queue should be strict priority scheduling. Therefore, the weight of the last queue should be zero while the Differentiate Service is supported.
WDRR Quantum	Enter the WDRR quantum value here. The range is from 0 to 127.

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

CoS to Queue Mapping

This window is used to display and configure the CoS-to-Queue mapping settings.

To view the following window, click **QoS > Basic Settings > CoS to Queue Mapping**, as shown below:



CoS to Queue Mapping

CoS	Queue ID
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

Figure 7-4 CoS to Queue Mapping Window

The fields that can be configured are described below:

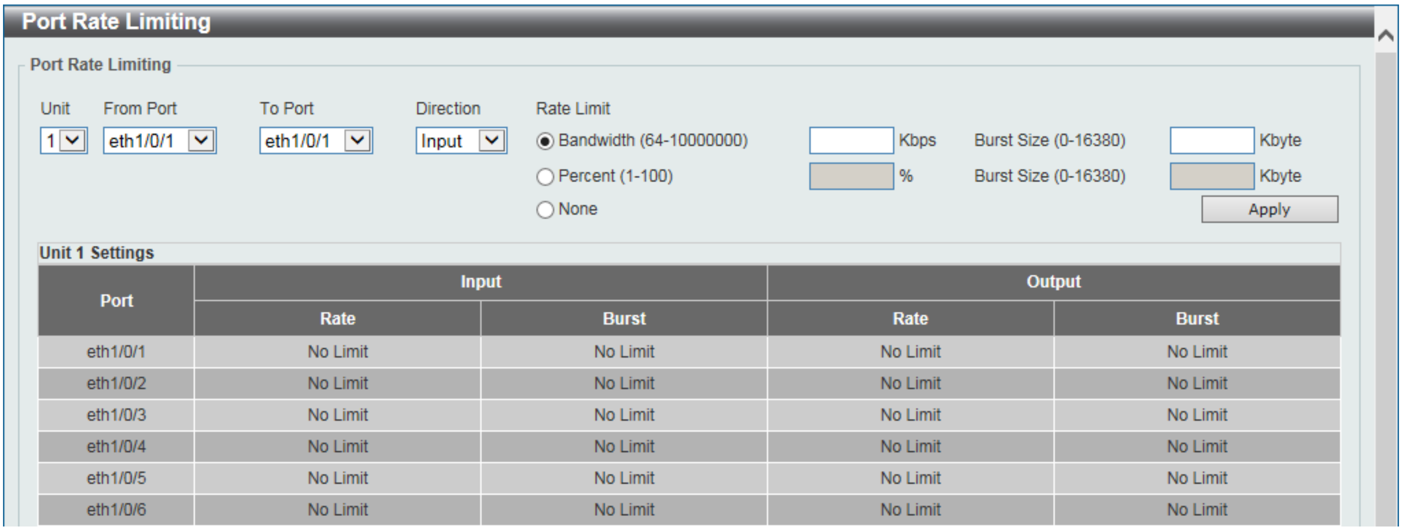
Parameter	Description
Queue ID	Select the queue ID that will be mapped to the corresponding CoS value. Options to choose from are 0 to 7.

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

Port Rate Limiting

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

To view the following window, click **QoS > Basic Settings > Port Rate Limiting**, as shown below:



Port Rate Limiting

Port Rate Limiting

Unit: 1 | From Port: eth1/0/1 | To Port: eth1/0/1 | Direction: Input

Rate Limit:
● Bandwidth (64-10000000) ___ Kbps Burst Size (0-16380) ___ Kbyte
○ Percent (1-100) ___ % Burst Size (0-16380) ___ Kbyte
○ None

Unit 1 Settings

Port	Input		Output	
	Rate	Burst	Rate	Burst
eth1/0/1	No Limit	No Limit	No Limit	No Limit
eth1/0/2	No Limit	No Limit	No Limit	No Limit
eth1/0/3	No Limit	No Limit	No Limit	No Limit
eth1/0/4	No Limit	No Limit	No Limit	No Limit
eth1/0/5	No Limit	No Limit	No Limit	No Limit
eth1/0/6	No Limit	No Limit	No Limit	No Limit

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.

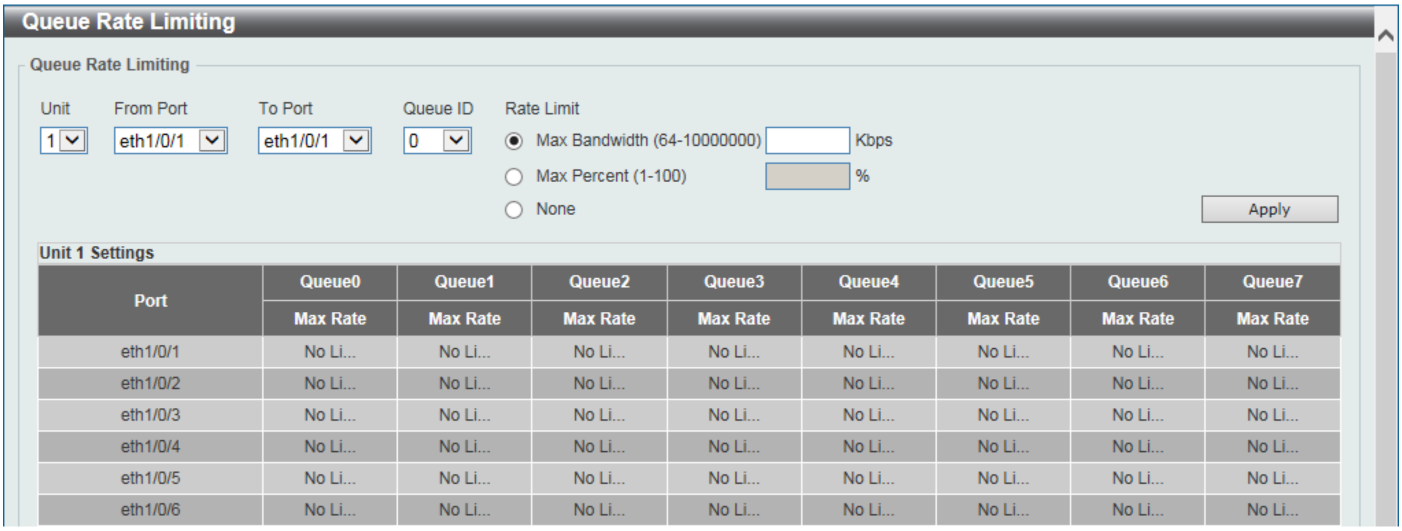
Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
Direction	Select the direction of the rate limit. Options to choose from are: **Input** and **Output**. Input specified ingress traffic and output specifies egress traffic.
Rate Limit	Select and enter the rate limit value here. 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. Options to choose from are: • **Bandwidth** - Select and enter the rate limit bandwidth value here. The range is from 64 to 10000000 Kbps. ○ **Burst Size** - Enter the burst size here. The range is from 0 to 16380 Kilobytes. When this value is 0, the rate limit function is disabled (no limit) on the interface. • **Percent** - Select and enter the rate limit bandwidth percentage here. The range is from 1 to 100 percent (%). ○ **Burst Size** - Enter the burst size here. The range is from 0 to 16380 Kilobytes. • **None** - Select this option to remove the rate limit on the specified port(s). By default, this option is used for Input and Output through all the ports.

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

Queue Rate Limiting

This window is used to display and configure the queue rate limiting settings.

To view the following window, click **QoS > Basic Settings > Queue Rate Limiting**, as shown below:



Queue Rate Limiting

Queue Rate Limiting

Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1
Queue ID: 0
Rate Limit:
● Max Bandwidth (64-10000000) Kbps
○ Max Percent (1-100) %
○ None

Unit 1 Settings

Port	Queue0	Queue1	Queue2	Queue3	Queue4	Queue5	Queue6	Queue7
	Max Rate	Max Rate	Max Rate	Max Rate	Max Rate	Max Rate	Max Rate	Max Rate
eth1/0/1	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/2	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/3	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/4	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/5	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
eth1/0/6	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...

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.
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. Options to choose from are:

Parameter	Description
	• **Max Bandwidth -** Enter the maximum rate limit bandwidth value here. The range is from 64 to 10000000 Kbps. • **Max Percent** - Enter the maximum rate limit percentage here. The range is from 1 to 100 percent (%). • **None** - Select this option to remove the rate limit on the specified port(s). By default, this option is used for through all the queues on all the ports. When the maximum bandwidth is configured, packets transmitted from the queue cannot exceed the maximum bandwidth even if the bandwidth is available. The configuration of this command can only be attached to a physical port but not a port-channel.

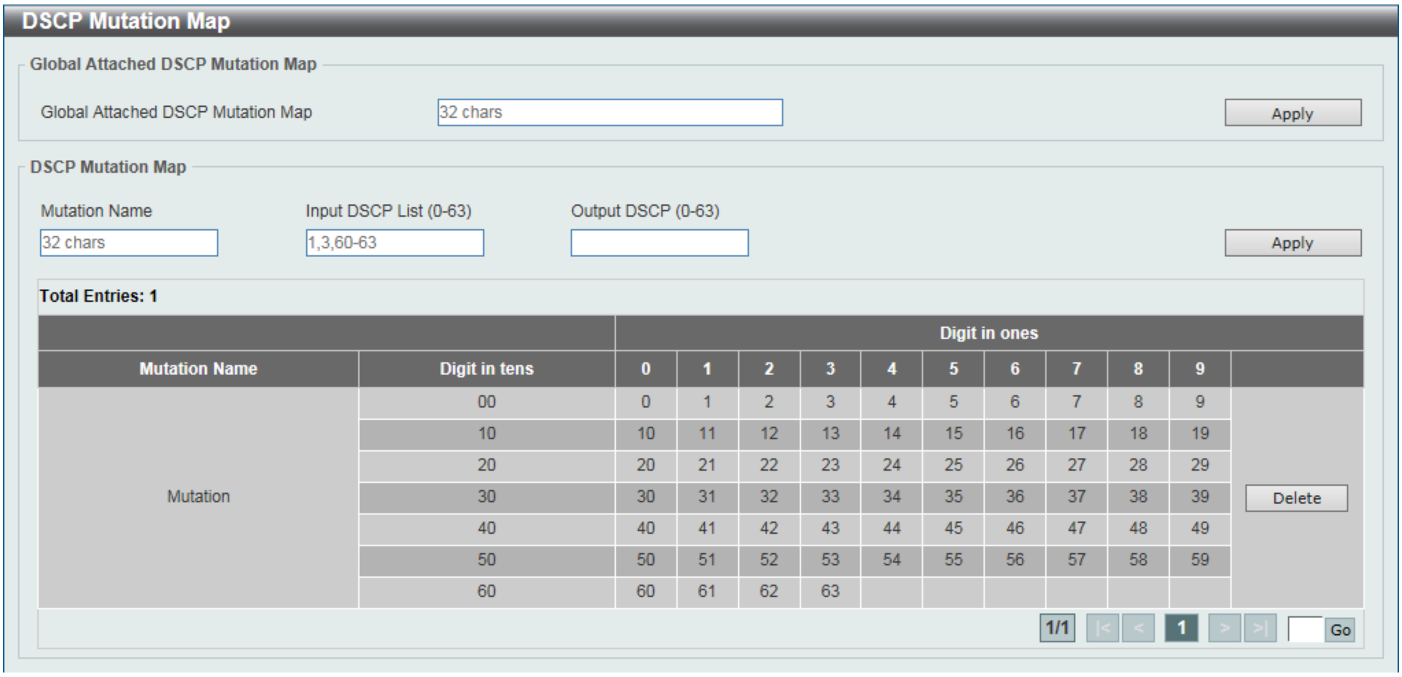
Click the **Apply** button to accept the changes made.

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. All the subsequent operations will base on the mutated DSCP.

To view the following window, click **QoS > Advanced Settings > DSCP Mutation Map**, as shown below:



DSCP Mutation Map

Global Attached DSCP Mutation Map

Global Attached DSCP Mutation Map: 32 chars

DSCP Mutation Map

Mutation Name: 32 chars

Input DSCP List (0-63): 1,3,60-63

Output DSCP (0-63):

Total Entries: 1

		Digit in ones										
Mutation Name	Digit in tens	0	1	2	3	4	5	6	7	8	9	
Mutation	00	0	1	2	3	4	5	6	7	8	9	Delete
	10	10	11	12	13	14	15	16	17	18	19	
	20	20	21	22	23	24	25	26	27	28	29	
	30	30	31	32	33	34	35	36	37	38	39	
	40	40	41	42	43	44	45	46	47	48	49	
	50	50	51	52	53	54	55	56	57	58	59	
	60	60	61	62	63							

Figure 7-7 DSCP Mutation Map Window

The fields that can be configured in **Global Attached DSCP Mutation Map** are described below:

Parameter	Description
Global Attached DSCP Mutation Map	Enter the name of the global DSCP mutation map. This name can be up to 32 characters long.

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

The fields that can be configured in **DSCP Mutation Map** 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. The range is from 0 to 63.
Output DSCP List	Enter the output DSCP list value here. The range is from 0 to 63.

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

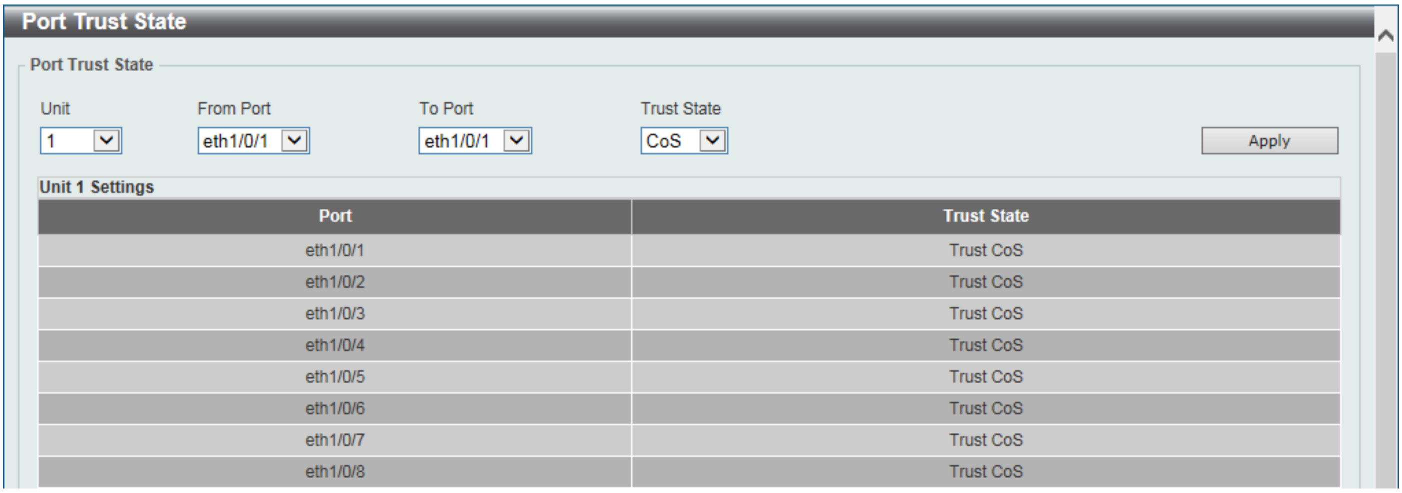
Click the **Delete** button to remove the specific entry.

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

Port Trust State

This window is used to display and configure the port trust state and mutation binding settings.

To view the following window, click **QoS > Advanced Settings > Port Trust State and Mutation Binding**, as shown below:



Port Trust State

Port Trust State

Unit: 1 | From Port: eth1/0/1 | To Port: eth1/0/1 | Trust State: CoS

Unit 1 Settings

Port	Trust State
eth1/0/1	Trust CoS
eth1/0/2	Trust CoS
eth1/0/3	Trust CoS
eth1/0/4	Trust CoS
eth1/0/5	Trust CoS
eth1/0/6	Trust CoS
eth1/0/7	Trust CoS
eth1/0/8	Trust CoS

Figure 7-8 Port Trust State and Mutation Binding Window

The fields that can be configured are described below:

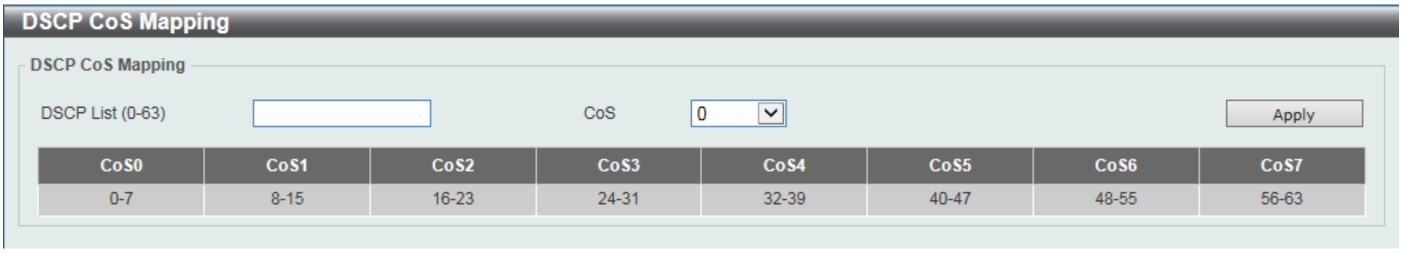
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Trust State	Select the port trust state option here. Options to choose from are **CoS** and **DSCP**.

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

DSCP CoS Mapping

This window is used to display and configure the DSCP CoS mapping settings.

To view the following window, click **QoS > Advanced Settings > DSCP CoS Mapping**, as shown below:



DSCP List (0-63)

CoS 0

CoS0	CoS1	CoS2	CoS3	CoS4	CoS5	CoS6	CoS7
0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63

Figure 7-9 DSCP CoS Mapping Window

The fields that can be configured are described below:

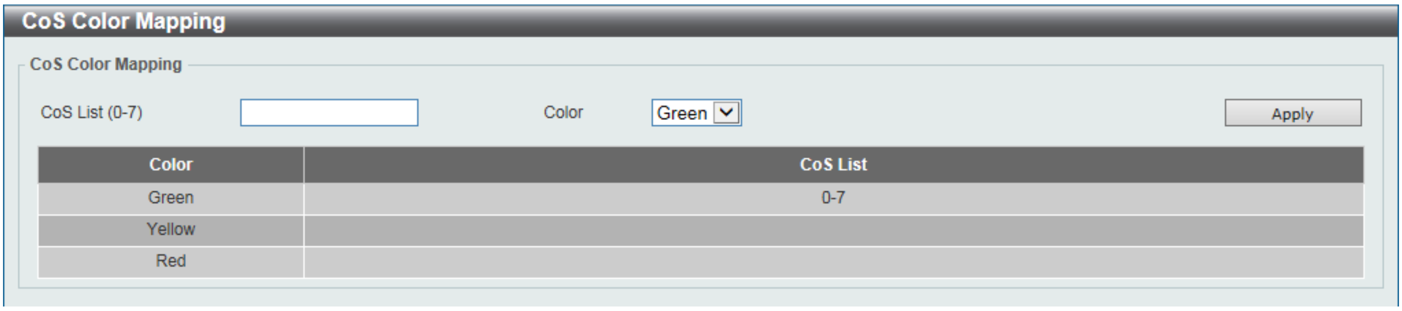
Parameter	Description
DSCP List	Enter the DSCP list value to map to the CoS value here. The range is from 0 to 63.
CoS	Select the CoS value to map to the DSCP list. Options to choose from are 0 to 7.

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:



CoS List (0-7)

Color Green

Color	CoS List
Green	0-7
Yellow	
Red	

Figure 7-10 CoS Color Mapping Window

The fields that can be configured are described below:

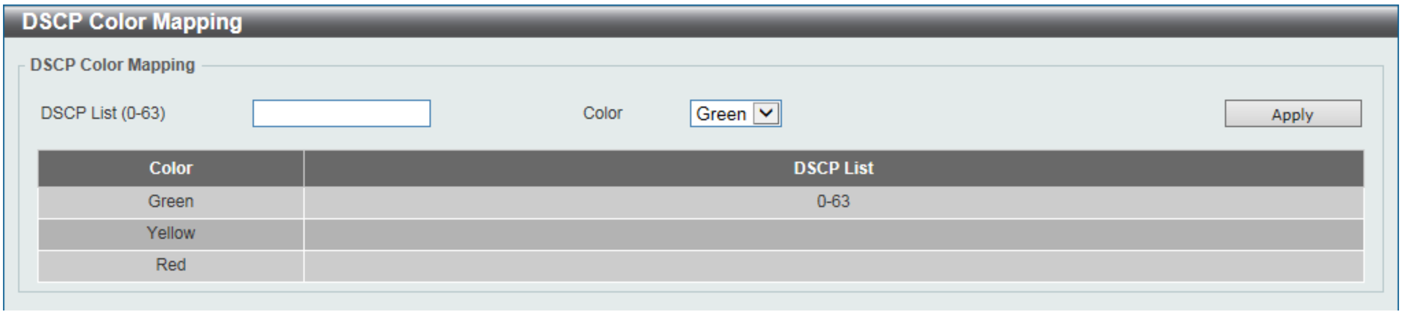
Parameter	Description
CoS List	Enter the CoS value that will be mapped to the color. The range is from 0 to 7.
Color	Select the color option that will be mapped to the CoS value. Options to choose from are **Green**, **Yellow**, and **Red**.

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

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:



DSCP Color Mapping

DSCP Color Mapping

DSCP List (0-63): (empty) Color: Green Apply

Color	DSCP List
Green	0-63
Yellow	
Red	

Figure 7-11 DSCP Color Mapping Window

The fields that can be configured are described below:

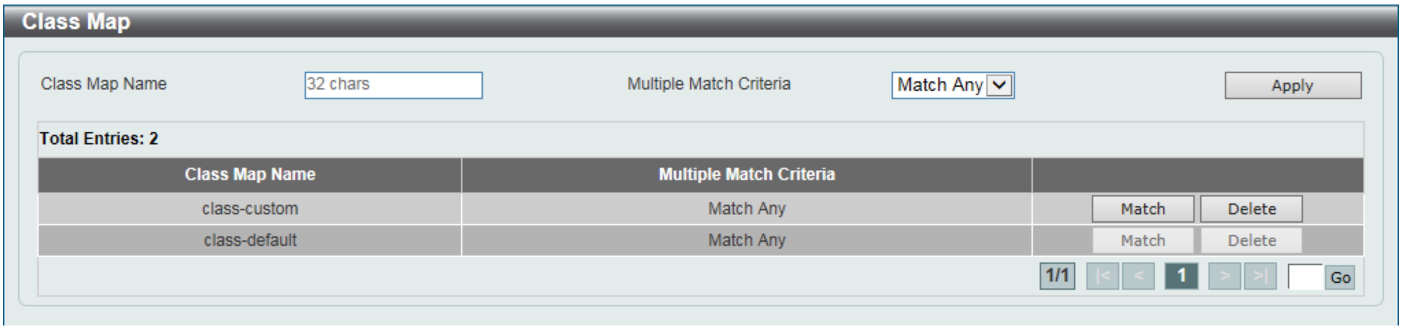
Parameter	Description
DSCP List	Enter the DSCP list value here that will be mapped to a color. The range is from 0 to 63.
Color	Select the color option that will be mapped to the DSCP value. Options to choose from are **Green**, **Yellow**, and **Red**.

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

Class Map

This window is used to display and configure the class map settings.

To view the following window, click **QoS > Advanced Settings > Class Map**, as shown below:



Class Map

Class Map Name: 32 chars Multiple Match Criteria: Match Any Apply

Total Entries: 2

Class Map Name	Multiple Match Criteria	
class-custom	Match Any	Match Delete
class-default	Match Any	Match Delete

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.
Multiple Match Criteria	Select the multiple match criteria option here. Options to choose from are **Match All** and **Match Any**.

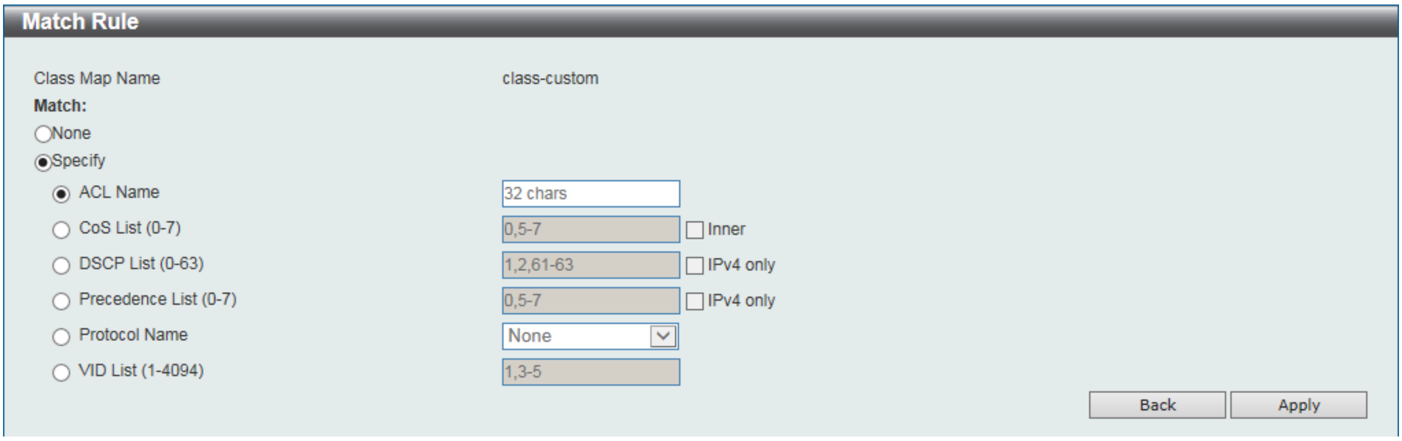
Click the **Apply** button to accept the changes made.

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

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Match** button, the following page will be available.



Match Rule

Class Map Name class-custom

Match:

○ None

● Specify

● ACL Name 32 chars

○ CoS List (0-7) 0,5-7 □ Inner

○ DSCP List (0-63) 1,2,61-63 □ IPv4 only

○ Precedence List (0-7) 0,5-7 □ IPv4 only

○ Protocol Name None

○ VID List (1-4094) 1,3-5

Figure 7-13 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. The range is from 0 to 7. Select the **Inner** option to match the inner most CoS of the QinQ packets on a Layer 2 CoS marking.
DSCP List	Select and enter the DSCP list value that will be matched with this class map here. The range is from 0 to 63. Select the **IPv4 only** option to match IPv4 packets only. If not specified, the match is for both IPv4 and IPv6 packets.
Precedence List	Select and enter the precedence list value that will be matched with this class map here. The range is from 0 to 7. Select 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. The range is from 1 to 4094.

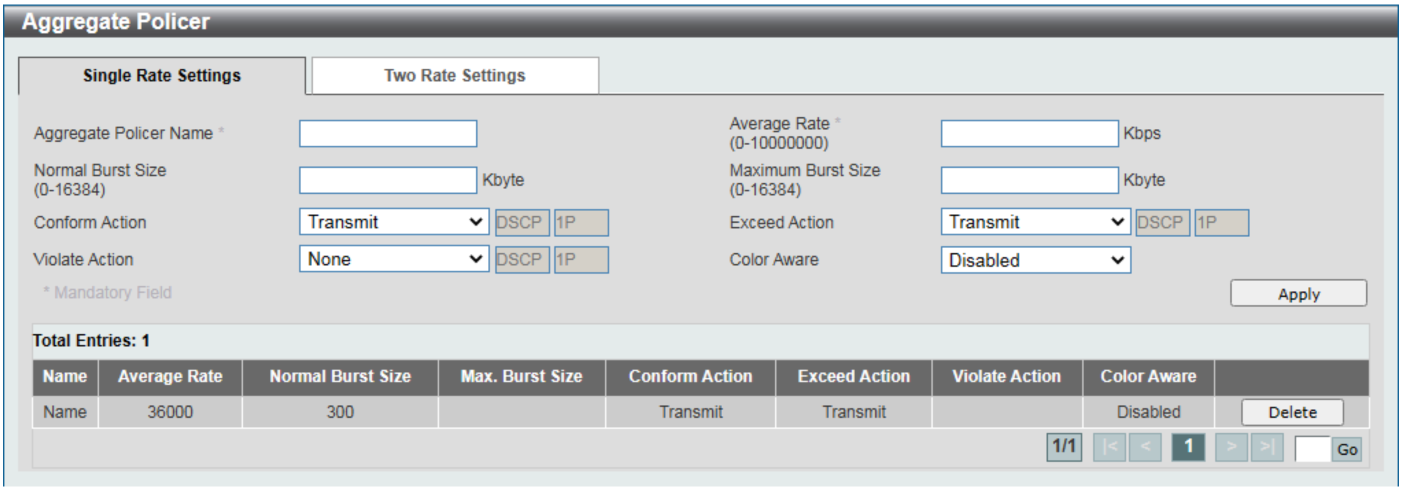
Click the **Apply** button to accept the changes made.

Click the **Back** button to discard the changes made and return to the previous page.

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** and select the **Single Rate Settings** tab, as shown below:



Aggregate Policer

Single Rate Settings | Two Rate Settings

Aggregate Policer Name *		Average Rate * (0-10000000)	Kbps
Normal Burst Size (0-16384)	Kbyte	Maximum Burst Size (0-16384)	Kbyte
Conform Action	Transmit, DSCP, 1P	Exceed Action	Transmit, DSCP, 1P
Violate Action	None, DSCP, 1P	Color Aware	Disabled

* Mandatory Field

Total Entries: 1

Name	Average Rate	Normal Burst Size	Max. Burst Size	Conform Action	Exceed Action	Violate Action	Color Aware	
Name	36000	300		Transmit	Transmit		Disabled	Delete

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.
Average Rate	Enter the average rate value here. The range is from 0 to 10000000 kbps.
Normal Burst Size	Enter the normal burst size value here. The range is from 0 to 16384 Kbytes.
Maximum Burst Size	Enter the maximum burst size value here. The range is from 0 to 16384 Kbytes.
Confirm Action	Select the confirm action here. The confirm action specifies the action to take on green color packets. Options to choose from are: • **Drop** - Specifies that the packet will be dropped. • **Set-DSCP-Transmit** - Specifies to 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. • **Set-1P-Transmit** - Specifies to enter the 1P transmit value in the space provided. This value sets the 802.1p value and transmits the packet with the new value. • **Transmit** - Specifies that packets will be transmitted unaltered. • **Set-DSCP-1P** - Specifies to enter the IP DSCP and 1P transmit values in the spaces provided. By default, the **Transmit** option is used. Packets are transmitted unaltered.
Exceed Action	Select the exceed action here. The exceed action specifies the action to take on packets that exceed the rate limit. Options to choose from are: • **Drop** - Specifies that the packet will be dropped. • **Set-DSCP-Transmit** - Specifies to 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. • **Set-1P-Transmit** - Specifies to enter the 1P transmit value in the space provided. This value sets the 802.1p value and transmits the packet with the new value. • **Transmit** - Specifies that packets will be transmitted unaltered. • **Set-DSCP-1P** - Specifies to enter the IP DSCP and 1P transmit values in the spaces provided.

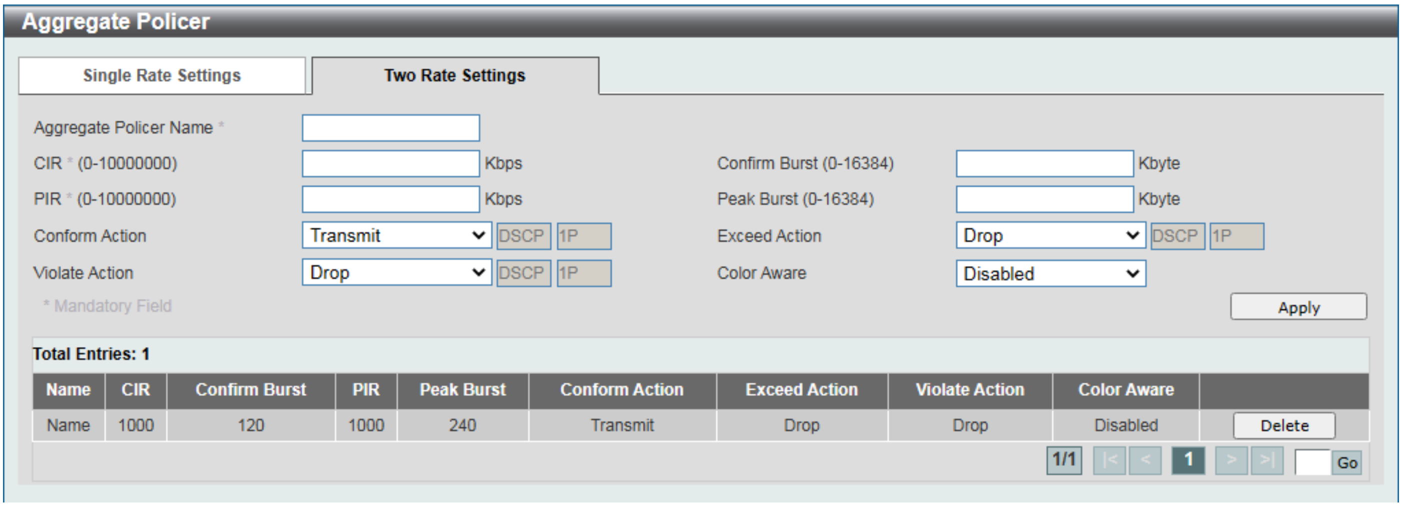
Parameter	Description
	By default, the **Drop** option is used. Packets are dropped.
Violate Action	Select the violate action here. The violate action specifies the action to take on packets that violate the normal and maximum burst sizes for singe rate policing. It specifies the action to take for those packets that did not conform to both CIR and PIR. Options to choose from are: • **None** - Specifies that no action will be taken. • **Drop** - Specifies that the packet will be dropped. • **Set-DSCP-Transmit** - Specifies to 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. • **Set-1P-Transmit** - Specifies to enter the 1P transmit value in the space provided. This value sets the 802.1p value and transmits the packet with the new value. • **Transmit** - Specifies that packets will be transmitted unaltered. • **Set-DSCP-1P** - Specifies to enter the IP DSCP and 1P transmit values in the spaces provided. By default, for a single rate policer, a single-rate two-color policer is created. By default, for a two-rate policer, the **Drop** option is used. Packets are dropped.
Color Aware	Select the color aware option here. Options to choose from are: • **Enabled** - Specifies that the policer work in the color-aware mode. • **Disabled** - Specifies that the policer work in the colorblind 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.

To view the following window, select the **Two Rate Settings** tab, as shown below:



Aggregate Policer

Single Rate Settings | Two Rate Settings

Aggregate Policer Name *

CIR * (0-10000000) Kbps

PIR * (0-10000000) Kbps

Confirm Burst (0-16384) Kbyte

Peak Burst (0-16384) Kbyte

Conform Action: Transmit DSCP 1P

Violate Action: Drop DSCP 1P

Exceed Action: Drop DSCP 1P

Color Aware: Disabled

* Mandatory Field

Apply

Total Entries: 1

Name	CIR	Confirm Burst	PIR	Peak Burst	Conform Action	Exceed Action	Violate Action	Color Aware	
Name	1000	120	1000	240	Transmit	Drop	Drop	Disabled	Delete

1/1 |< < 1 > >| Go

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.
CIR	Enter the Committed Information Rate (CIR) value here. The range is from 0 to 10000000 kbps. The committed packet rate is the first token bucket for the two-rate metering.
Confirm Burst	Enter the confirm burst value here. The range is from 0 to 16384 Kbytes. The confirm burst value specifies the burst size for the first token bucket in kbps.

Parameter	Description
PIR	Enter the Peak Information Rate (PIR) value here. The range is from 0 to 10000000 kbps. The peak information rate is the second token bucket for the two-rate metering.
Peak Burst	Enter the peak burst value here. The range is from 0 to 16384 Kbytes. The peak burst value is the burst size for the second token bucket in kilobytes.
Confirm Action	Select the confirm action here. The confirm action specifies the action to take on green color packets. Options to choose from are: • **Drop** - Specifies that the packet will be dropped. • **Set-DSCP-Transmit** - Specifies to 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. • **Set-1P-Transmit** - Specifies to enter the 1P transmit value in the space provided. This value sets the 802.1p value and transmits the packet with the new value. • **Transmit** - Specifies that packets will be transmitted unaltered. • **Set-DSCP-1P** - Specifies to enter the IP DSCP and 1P transmit values in the spaces provided. By default, the **Transmit** option is used. Packets are transmitted unaltered.
Exceed Action	Select the exceed action here. The exceed action specifies the action to take on packets that exceed the rate limit. Options to choose from are: • **Drop** - Specifies that the packet will be dropped. • **Set-DSCP-Transmit** - Specifies to 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. • **Set-1P-Transmit** - Specifies to enter the 1P transmit value in the space provided. This value sets the 802.1p value and transmits the packet with the new value. • **Transmit** - Specifies that packets will be transmitted unaltered. • **Set-DSCP-1P** - Specifies to enter the IP DSCP and 1P transmit values in the spaces provided. By default, for a two rate policer, the **Drop** option is used. Packets are dropped.
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. Options to choose from are: • **Drop** - Specifies that the packet will be dropped. • **Set-DSCP-Transmit** - Specifies to 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. • **Set-1P-Transmit** - Specifies to enter the 1P transmit value in the space provided. This value sets the 802.1p value and transmits the packet with the new value. • **Transmit** - Specifies that packets will be transmitted unaltered. • **Set-DSCP-1P** - Specifies to enter the IP DSCP and 1P transmit values in the spaces provided. By default, for a single rate policer, a single-rate two-color policer is created. By default, for a two-rate policer, the **Drop** option is used. Packets are dropped.
Color Aware	Select the color aware option here. Options to choose from are: • **Enabled** - Specifies that the policer work in the color-aware mode. • **Disabled** - Specifies that the policer work in the colorblind 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:

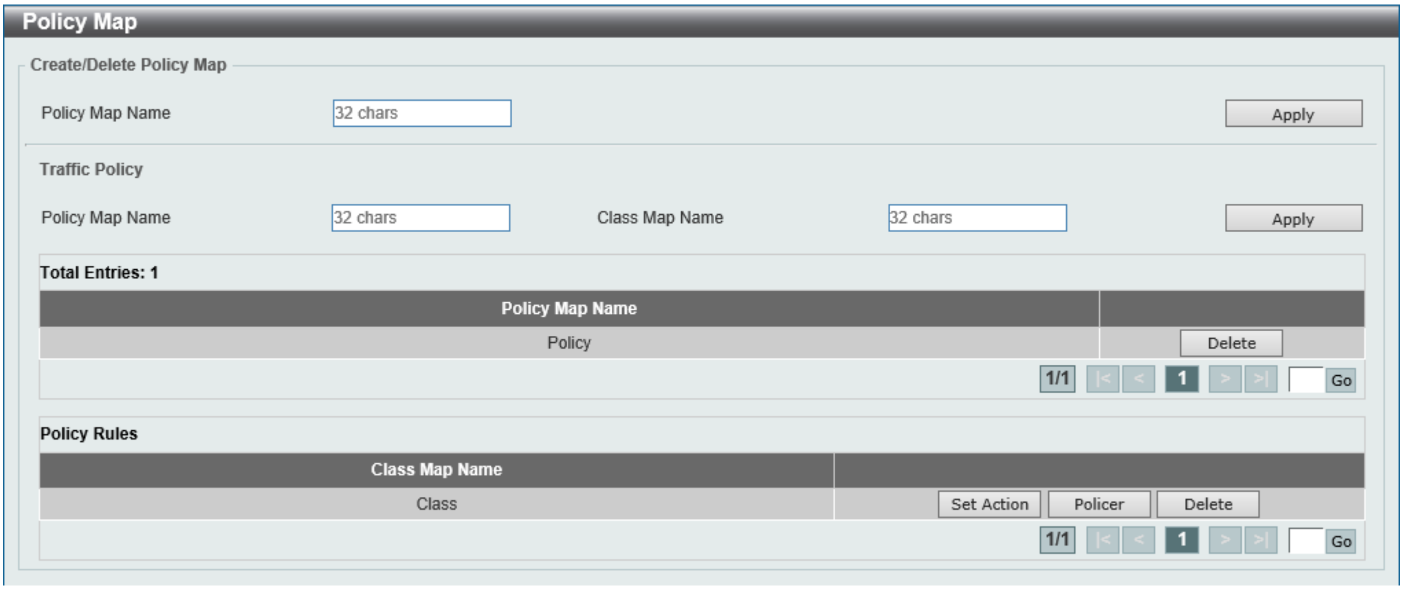


Figure 7-16 Policy Map Window

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.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Traffic Policy** are described below:

Parameter	Description
Policy Map Name	Enter the policy map name here. This name can be up to 32 characters long.
Class Map Name	Enter the class map name here. This name can be up to 32 characters long.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

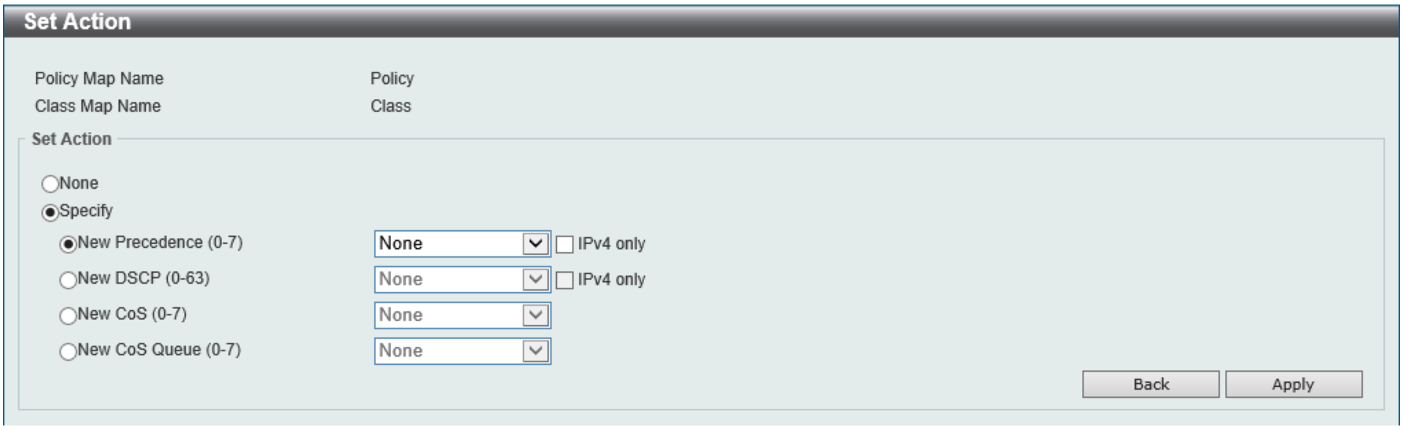
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

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.



Set Action

Policy Map Name: Policy

Class Map Name: Class

Set Action

○ None

● Specify

● New Precedence (0-7): None □ IPv4 only

○ New DSCP (0-63): None □ IPv4 only

○ New CoS (0-7): None

○ New CoS Queue (0-7): None

Figure 7-17 Policy Map (Set Action) Window

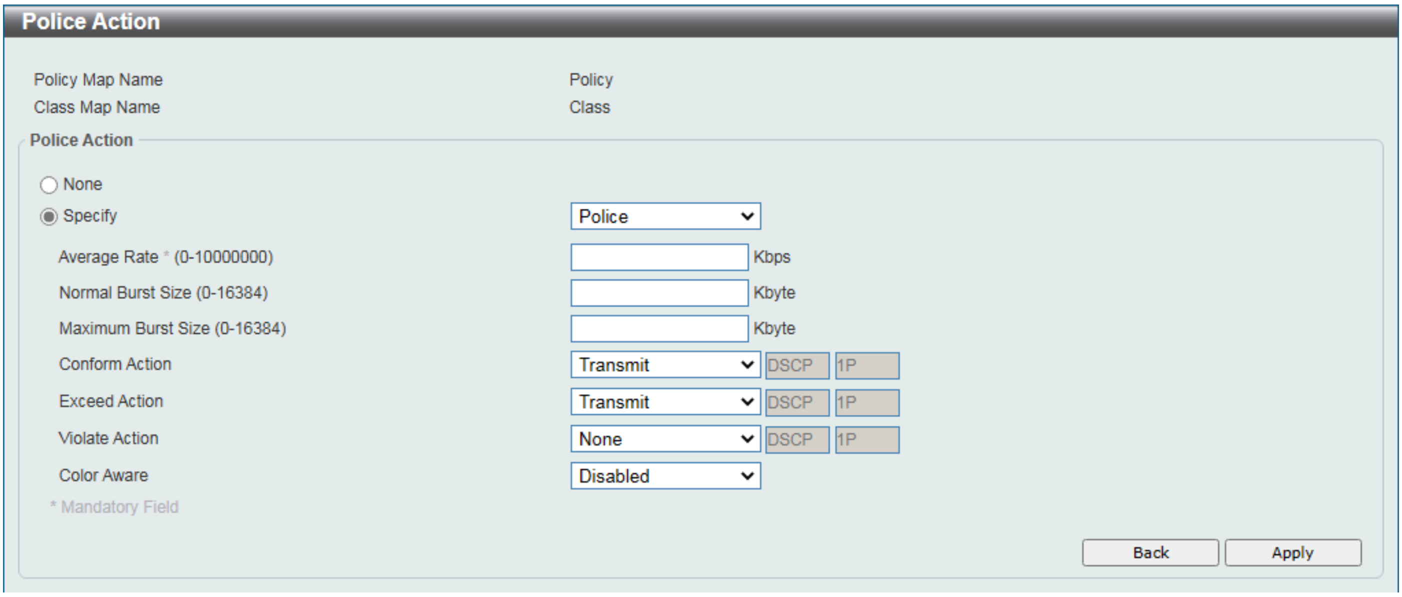
The fields that can be configured are described below:

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 affect the CoS queue selection while the policy map is applied on the ingress interface.
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.



Police Action

Policy Map Name: Policy

Class Map Name: Class

Police Action

○ None

● Specify: Police

Average Rate * (0-10000000): Kbps

Normal Burst Size (0-16384): Kbyte

Maximum Burst Size (0-16384): Kbyte

Conform Action: Transmit, DSCP, 1P

Exceed Action: Transmit, DSCP, 1P

Violate Action: None, DSCP, 1P

Color Aware: Disabled

* Mandatory Field

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. • **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.

Parameter	Description
	• **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 colorblind mode. When enabled, the policer works in the color-aware mode.

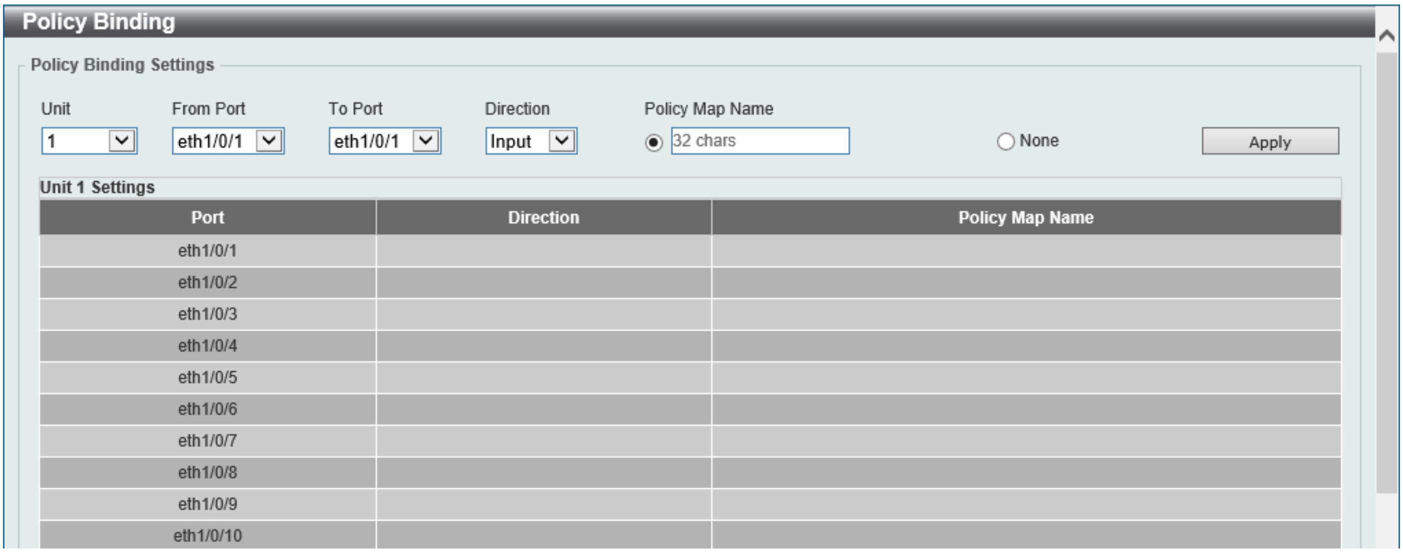
Click the **Back** button to return to the previous window.

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:



Policy Binding

Policy Binding Settings

Unit: 1

From Port: eth1/0/1

To Port: eth1/0/1

Direction: Input

Policy Map Name: ● 32 chars ○ None

Unit 1 Settings

Port	Direction	Policy Map Name
eth1/0/1		
eth1/0/2		
eth1/0/3		
eth1/0/4		
eth1/0/5		
eth1/0/6		
eth1/0/7		
eth1/0/8		
eth1/0/9		
eth1/0/10		

Figure 7-19 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.
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.

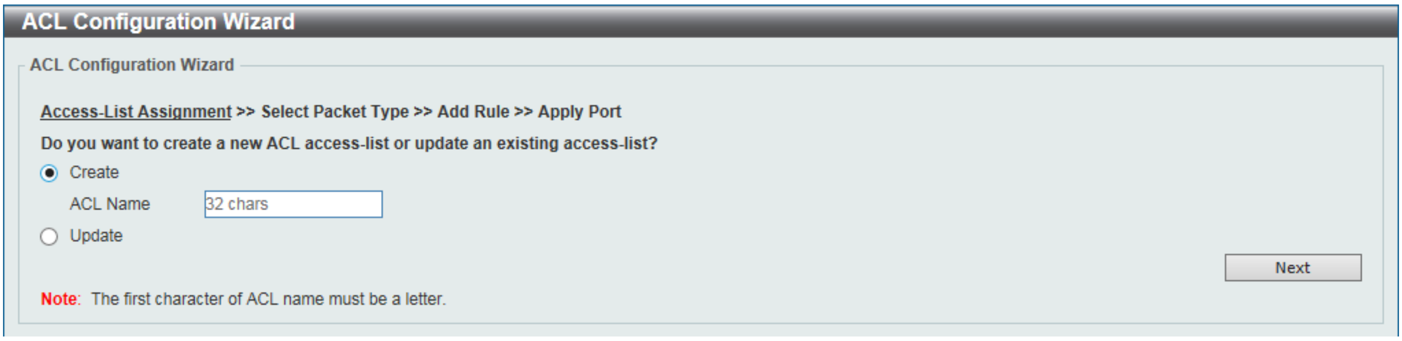
8. Access Control List (ACL)

ACL Configuration Wizard

This window is used to guide the user to create a new ACL access list or configure an existing ACL access list.

Step 1 - Create/Update

To view the following window, click **ACL > ACL Configuration Wizard**, as shown below:



ACL Configuration Wizard

ACL Configuration Wizard

Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port

Do you want to create a new ACL access-list or update an existing access-list?

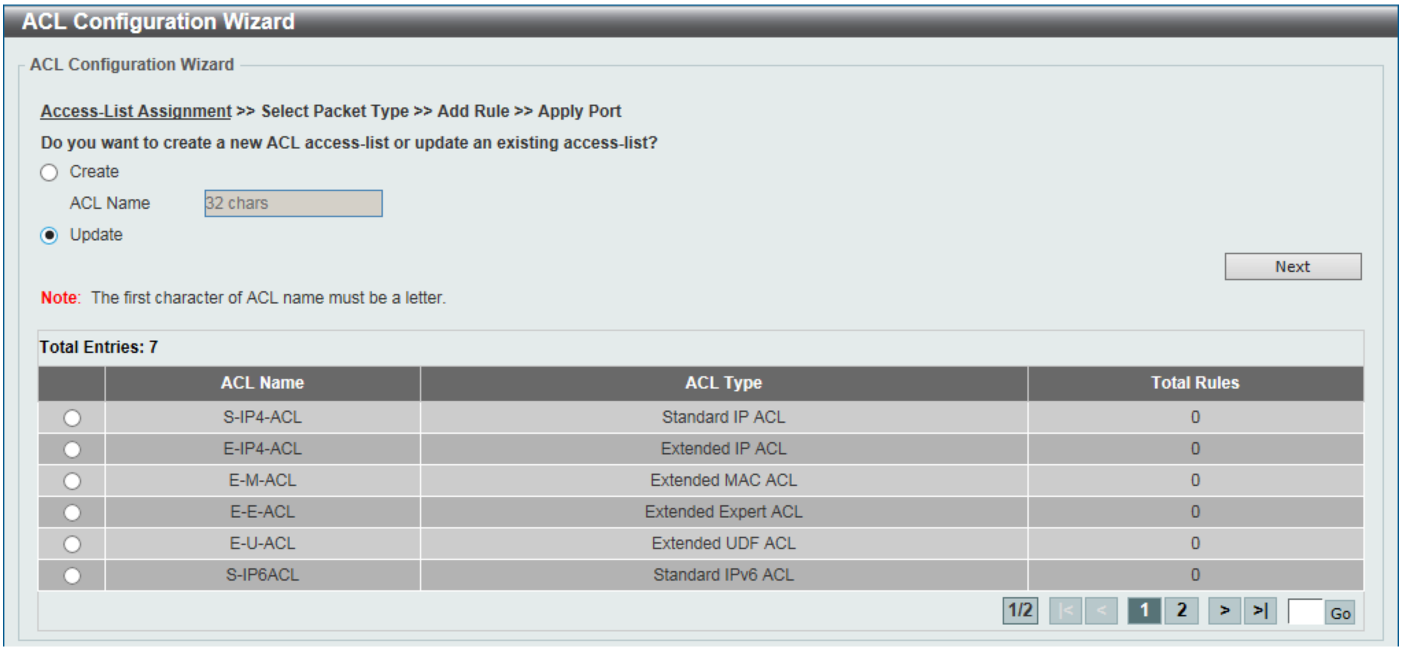
● Create

ACL Name: 32 chars

○ Update

Note: The first character of ACL name must be a letter.

Figure 8-1 ACL Configuration Wizard (Create) Window



ACL Configuration Wizard

ACL Configuration Wizard

Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port

Do you want to create a new ACL access-list or update an existing access-list?

○ Create

ACL Name: 32 chars

● Update

Note: The first character of ACL name must be a letter.

Total Entries: 7

	ACL Name	ACL Type	Total Rules
○	S-IP4-ACL	Standard IP ACL	0
○	E-IP4-ACL	Extended IP ACL	0
○	E-M-ACL	Extended MAC ACL	0
○	E-E-ACL	Extended Expert ACL	0
○	E-U-ACL	Extended UDF ACL	0
○	S-IP6ACL	Standard IPv6 ACL	0

Figure 8-2 ACL Configuration Wizard (Update) Window

The fields that can be configured are described below:

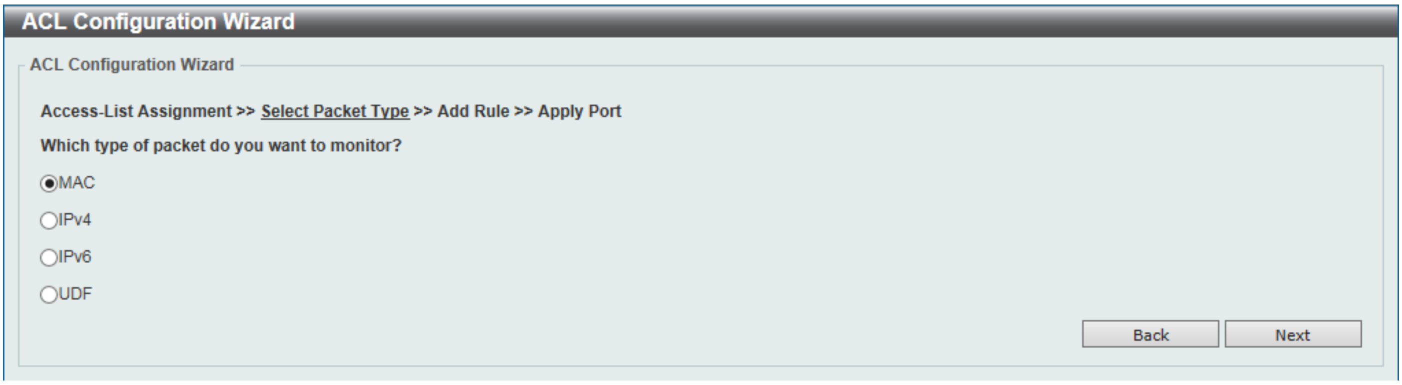
Parameter	Description
Create	Select this option to create a new ACL access list using the configuration wizard.
ACL Name	Enter the new ACL name here. This name can be up to 32 characters long.
Update	Select this option to update an existing ACL access list. Select the existing ACL in the table to process with the update.

Click the **Next** button to continue to the next step.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Step 2 - Select Packet Type

After clicking the **Next** button, the following window will appear.



ACL Configuration Wizard

ACL Configuration Wizard

Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port

Which type of packet do you want to monitor?

● MAC

○ IPv4

○ IPv6

○ UDF

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.
UDF	Select to create/update an UDF ACL.

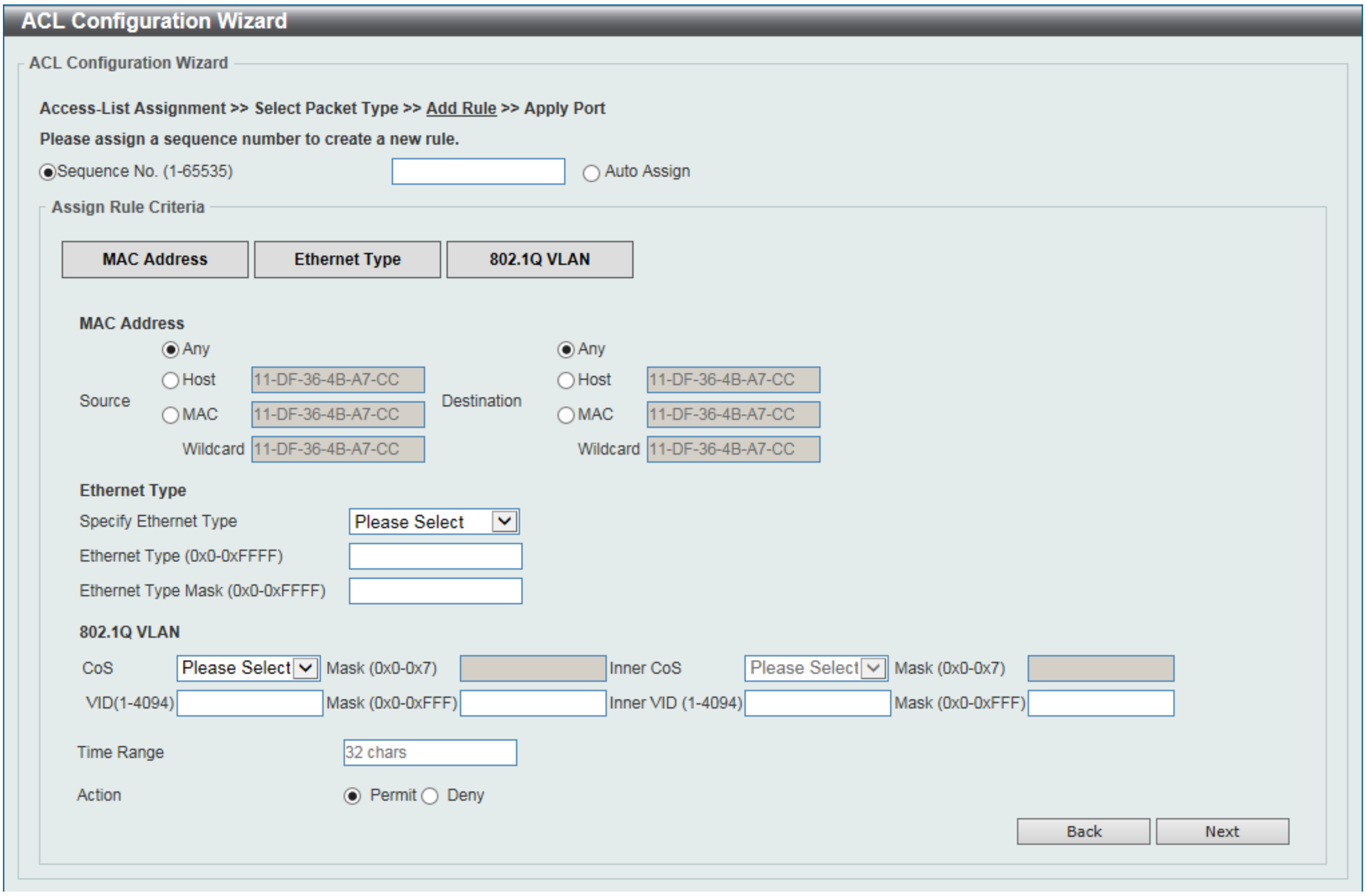
Click the **Back** button to return to the previous step.

Click the **Next** button to continue to the next step.

Step 3 - Add Rule

Extended MAC ACL

Selecting to **Create** or **Update** a **MAC** ACL and click the **Next** button to view the following window:



ACL Configuration Wizard

ACL Configuration Wizard

Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port

Please assign a sequence number to create a new rule.

● Sequence No. (1-65535) ○ Auto Assign

Assign Rule Criteria

MAC Address

Source: ● Any; ○ Host 11-DF-36-4B-A7-CC; ○ MAC 11-DF-36-4B-A7-CC; Wildcard 11-DF-36-4B-A7-CC

Destination: ● Any; ○ Host 11-DF-36-4B-A7-CC; ○ MAC 11-DF-36-4B-A7-CC; Wildcard 11-DF-36-4B-A7-CC

Ethernet Type

Specify Ethernet Type: Please Select

Ethernet Type (0x0-0xFFFF)

Ethernet Type Mask (0x0-0xFFFF)

802.1Q VLAN

CoS: Please Select; Mask (0x0-0x7); Inner CoS: Please Select; Mask (0x0-0x7)

VID(1-4094); Mask (0x0-0xFFF); Inner VID (1-4094); Mask (0x0-0xFFF)

Time Range: 32 chars

Action: ● Permit ○ Deny

Figure 8-4 ACL Configuration Wizard (Extended MAC ACL) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. The range is from 1 to 65535. Select **Auto Assign** to automatically generate an ACL rule number for this entry.
Source	Select and enter the source MAC address information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host MAC address here. • **MAC** - The **Wildcard** option will 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** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host MAC address here. • **MAC** - The **Wildcard** option will 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**.

Parameter	Description
Ethernet Type	Enter the Ethernet type hexadecimal value here. The range is from 0x0 to 0xFFFF. When any Ethernet type profile is selected in the **Specify Ethernet Type** drop-down list, the appropriate hexadecimal value will automatically be entered.
Ethernet Type Mask	Enter the Ethernet type mask hexadecimal value here. The range is from 0x0 to 0xFFFF. When any Ethernet type profile is selected in the **Specify Ethernet Type** drop-down list, the appropriate hexadecimal value will automatically be entered.
CoS	Select the CoS value that will be used here. The range is from **0** to **7**. • **Mask** - Enter the CoS mask value here. The range is from 0x0 to 0x7.
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.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.

Click the **Back** button to return to the previous step.

Click the **Next** button to continue to the next step.

Extended/Standard IPv4 ACL

Selecting to **Create** or **Update** an **IPv4** ACL and click the **Next** button to view the following window:

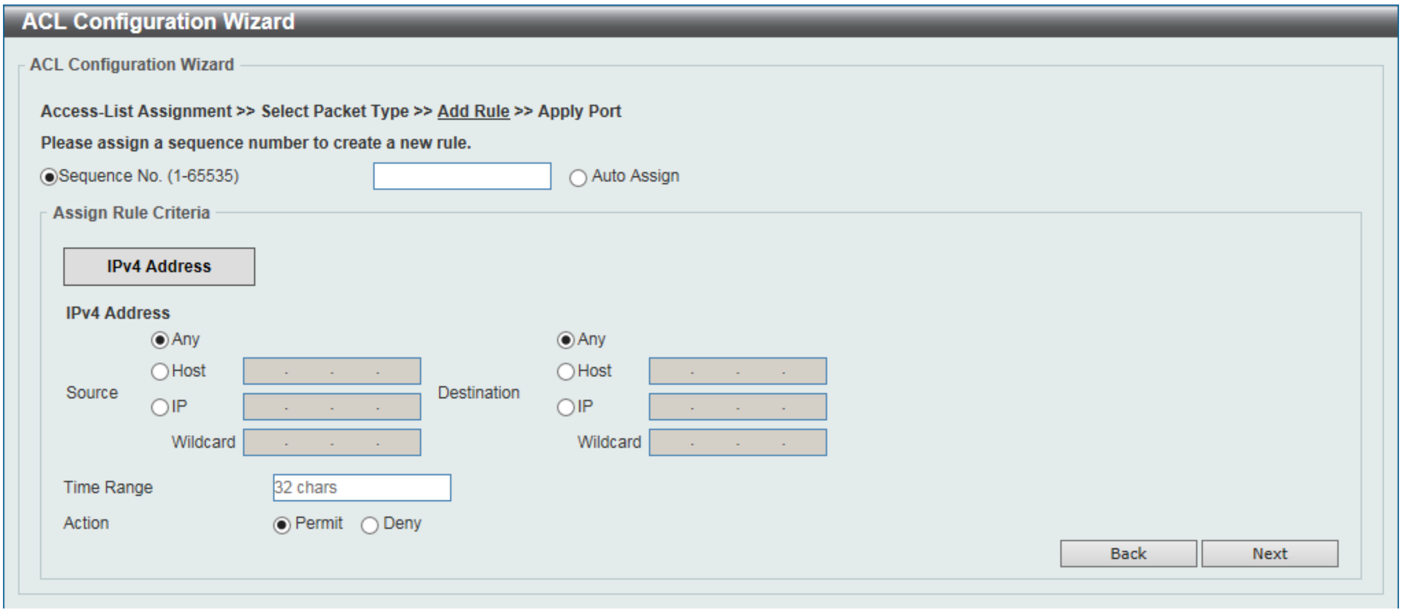
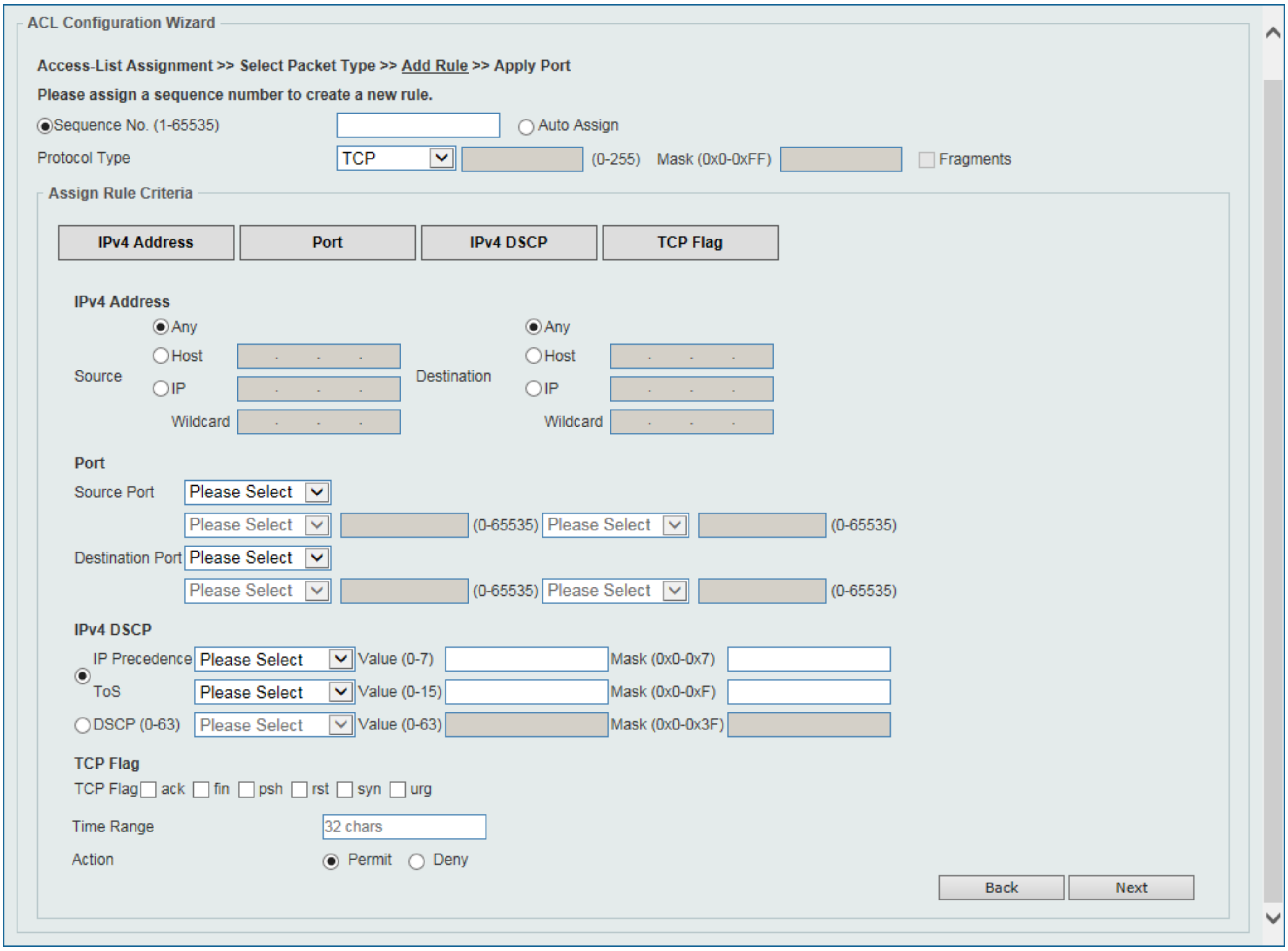


Figure 8-5 ACL Configuration Wizard (Standard IPv4 ACL) Window



ACL Configuration Wizard

Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port

Please assign a sequence number to create a new rule.

● Sequence No. (1-65535) ○ Auto Assign

Protocol Type: TCP (0-255) Mask (0x0-0xFF) □ Fragments

Assign Rule Criteria

IPv4 Address | Port | IPv4 DSCP | TCP Flag

IPv4 Address

Source: ● Any ○ Host ○ IP Wildcard

Destination: ● Any ○ Host ○ IP Wildcard

Port

Source Port: Please Select
Please Select (0-65535) Please Select (0-65535)

Destination Port: Please Select
Please Select (0-65535) Please Select (0-65535)

IPv4 DSCP

● IP Precedence: Please Select Value (0-7) Mask (0x0-0x7)
ToS: Please Select Value (0-15) Mask (0x0-0xF)

○ DSCP (0-63): Please Select Value (0-63) Mask (0x0-0x3F)

TCP Flag

TCP Flag □ ack □ fin □ psh □ rst □ syn □ urg

Time Range: 32 chars

Action: ● Permit ○ Deny

Back | Next

Figure 8-6 ACL Configuration Wizard (Extended IPv4 ACL) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. The range is from 1 to 65535. Select **Auto Assign** to automatically generate an ACL rule number for this entry.
Protocol Type	Select the protocol type option here. Options to choose from are **TCP**, **UDP**, **ICMP**, **EIGRP** (88), **ESP** (50), **GRE** (47), **IGMP** (2), **OSPF** (89), **PIM** (103), **VRRP** (112), **IP-in-IP** (94), **PCP** (108), **Protocol ID**, and **None**. • **Value** - The protocol ID can also manually be entered here. The range is from 0 to 255. • **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.

The fields that can be configured in **Assign rule criteria** are described below:

Parameter	Description
Source	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host IP address here. • **IP** - The **Wildcard** option will 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 information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host IP address here. • **IP** - The **Wildcard** option will be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source Port	Select and enter the source port value here. Options to choose from are: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Mask** - 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: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Mask** - 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-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**

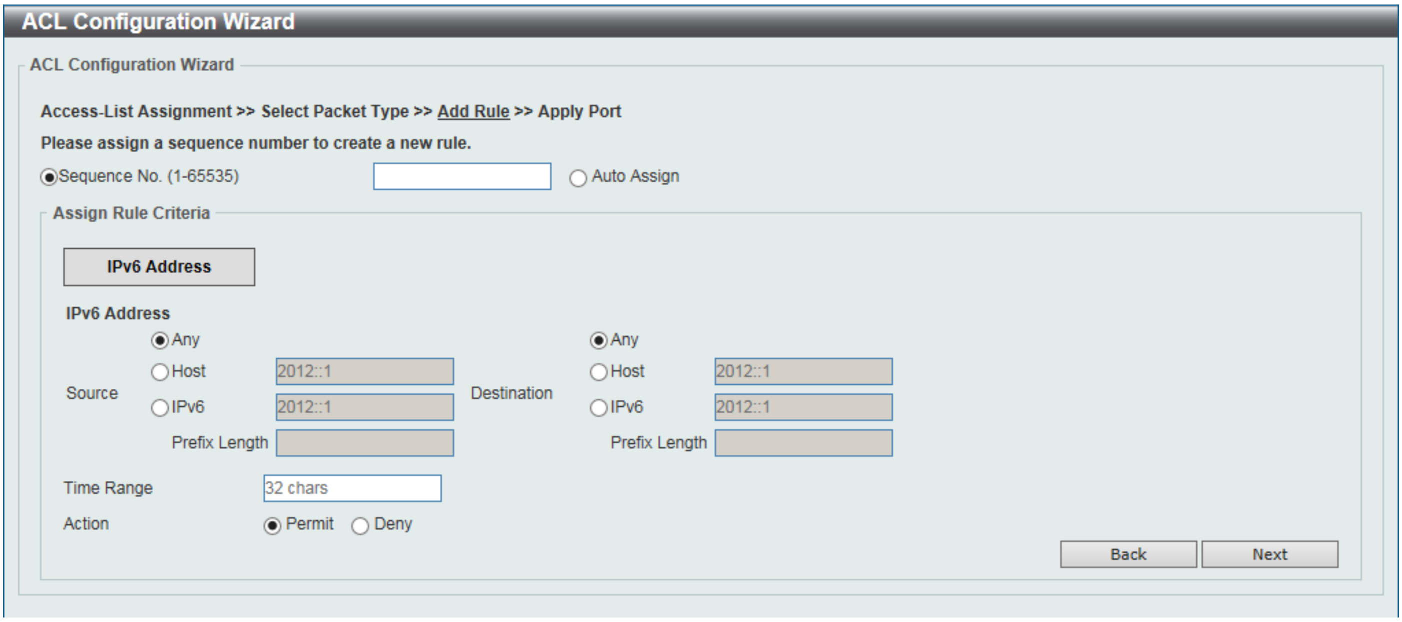
Parameter	Description
	(28), **af33** (30), **af41** (34), **af42** (36), **af43** (38), **cs1** (8), **cs2** (16), **cs3** (24), **cs4** (32), **cs5** (40), **cs6** (48), **cs7** (56), and **ef** (46). • **Value** - The DSCP value can also manually be entered here. The range is from 0 to 63. • **Mask** - Enter the DSCP mask value here. The range is from 0x0 to 0x3F.
TCP Flag	Select the appropriate TCP flag option to include the flag in this rule. Options to choose from are **ack**, **fin**, **psh**, **rst**, **syn**, and **urg**. This parameter is only available in the protocol type **TCP**.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.
Action	Select the action that this rule will take here. Options to choose from are **Permit**, and **Deny**.

Click the **Back** button to return to the previous step.

Click the **Next** button to continue to the next step.

Extended/Standard IPv6 ACL

Selecting to **Create** or **Update** an **IPv6** ACL and click the **Next** button to view the following window:



ACL Configuration Wizard

ACL Configuration Wizard

Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port

Please assign a sequence number to create a new rule.

● Sequence No. (1-65535) ○ Auto Assign

Assign Rule Criteria

IPv6 Address

IPv6 Address

Source: ● Any ○ Host 2012::1 ○ IPv6 2012::1 Prefix Length

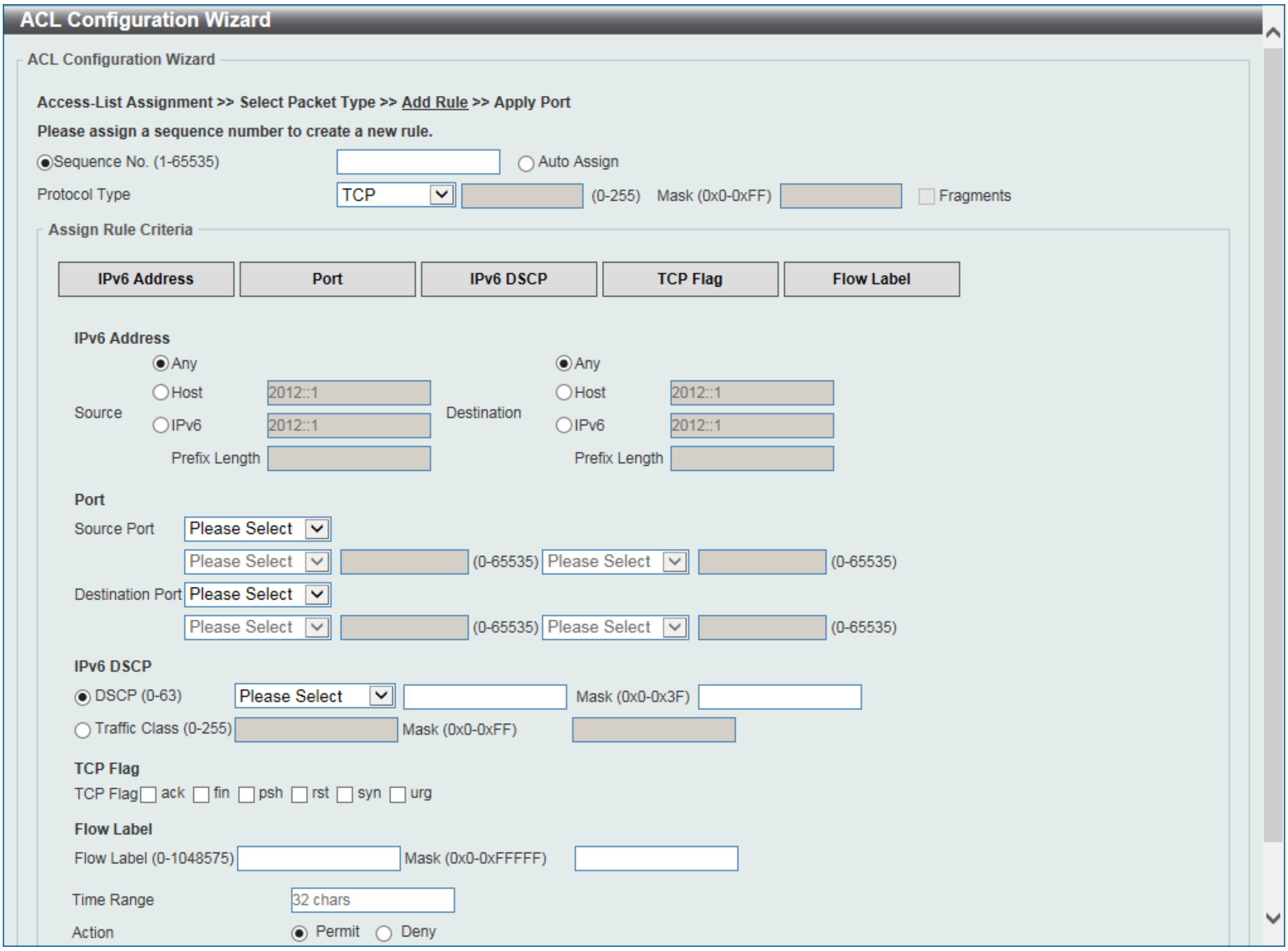
Destination: ● Any ○ Host 2012::1 ○ IPv6 2012::1 Prefix Length

Time Range 32 chars

Action ● Permit ○ Deny

Back Next

Figure 8-7 ACL Configuration Wizard (Standard IPv6 ACL) Window



ACL Configuration Wizard

ACL Configuration Wizard

Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port

Please assign a sequence number to create a new rule.

● Sequence No. (1-65535) ○ Auto Assign

Protocol Type: TCP (0-255) Mask (0x0-0xFF) □ Fragments

Assign Rule Criteria

IPv6 Address

Source: ● Any ○ Host 2012::1 ○ IPv6 2012::1 Prefix Length

Destination: ● Any ○ Host 2012::1 ○ IPv6 2012::1 Prefix Length

Port

Source Port: Please Select; Please Select (0-65535) Please Select (0-65535)

Destination Port: Please Select; Please Select (0-65535) Please Select (0-65535)

IPv6 DSCP

● DSCP (0-63) Please Select Mask (0x0-0x3F)

○ Traffic Class (0-255) Mask (0x0-0xFF)

TCP Flag

TCP Flag □ ack □ fin □ psh □ rst □ syn □ urg

Flow Label

Flow Label (0-1048575) Mask (0x0-0xFFFFF)

Time Range: 32 chars

Action: ● Permit ○ Deny

Figure 8-8 ACL Configuration Wizard (Extended IPv6 ACL) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. The range is from 1 to 65535. Select **Auto Assign** to automatically generate an ACL rule number for this entry.
Protocol Type	Select the protocol type option here. Options to choose from are **TCP**, **UDP**, **ICMP**, **Protocol ID**, **ESP** (50), **PCP** (108), **SCTP** (132), and **None**. • **Value** - The protocol ID can also manually be entered here. The range is from 0 to 255. • **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.

The fields that can be configured in **Assign rule criteria** are described below:

Parameter	Description
Source	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host IPv6 address here. • **IPv6** - The **Prefix Length** option will be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are:

Parameter	Description
	• **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host IPv6 address here. • **IPv6** - The **Prefix Length** option will 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: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Mask** - 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: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Mask** - 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. 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. 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.
TCP Flag	Select the appropriate TCP flag option to include the flag in this rule. Options to choose from are **ack**, **fin**, **psh**, **rst**, **syn**, and **urg**. This parameter is only available in the protocol type **TCP**.
Flow Label	Enter the flow label value here. The range is from 0 to 1048575. • **Mask** - Enter the flow label mask value here. The range is from 0x0 to 0xFFFFF.

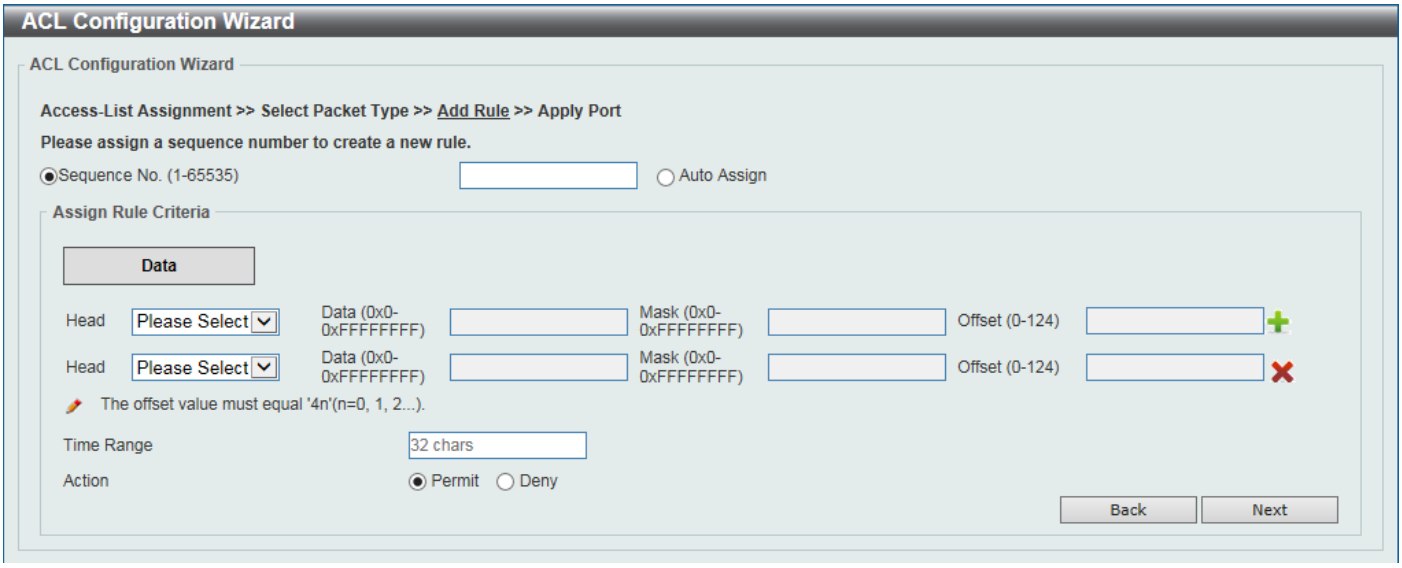
Parameter	Description
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.

Click the **Back** button to return to the previous step.

Click the **Next** button to continue to the next step.

Extended UDF ACL

Selecting to **Create** or **Update** an **UDF** ACL and click the **Next** button to view the following window:



Please assign a sequence number to create a new rule.

● Sequence No. (1-65535) ○ Auto Assign

Head: Please Select | Data (0x0-0xFFFFFFFF) | Mask (0x0-0xFFFFFFFF) | Offset (0-124)

Head: Please Select | Data (0x0-0xFFFFFFFF) | Mask (0x0-0xFFFFFFFF) | Offset (0-124)

The offset value must equal '4n'(n=0, 1, 2...).

Time Range: 32 chars

Action: ● Permit ○ Deny

Figure 8-9 ACL Configuration Wizard (Extended UDF ACL) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. The range is from 1 to 65535. Select **Auto Assign** to automatically generate an ACL rule number for this entry.

The fields that can be configured in **Assign rule criteria** are described below:

Parameter	Description
Head	Select the offset value specified by the header. Options to choose from are **L2**, **L3**, and **L4**.
Data	Enter the UDF fields per rule to match the content of the packet. • **Mask -** Enter the data mask value here. The bit corresponding to bit value 0 will be ignored, and the bit corresponding to bit value 1 will be checked. The range is from **0x0** to **0xFFFFFFFF**.
Offset	Specifies the offset value specified by the header. The offset reference can be one of the following: • **L2** - Specifies the offset starts from the L2 header. • **L3** - Specifies the offset starts from the L3 header minus 2 bytes. • **L4** - Specifies the offset starts from the L4 header.
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.

Parameter	Description
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.

Click the ✚ button to add more data entries.

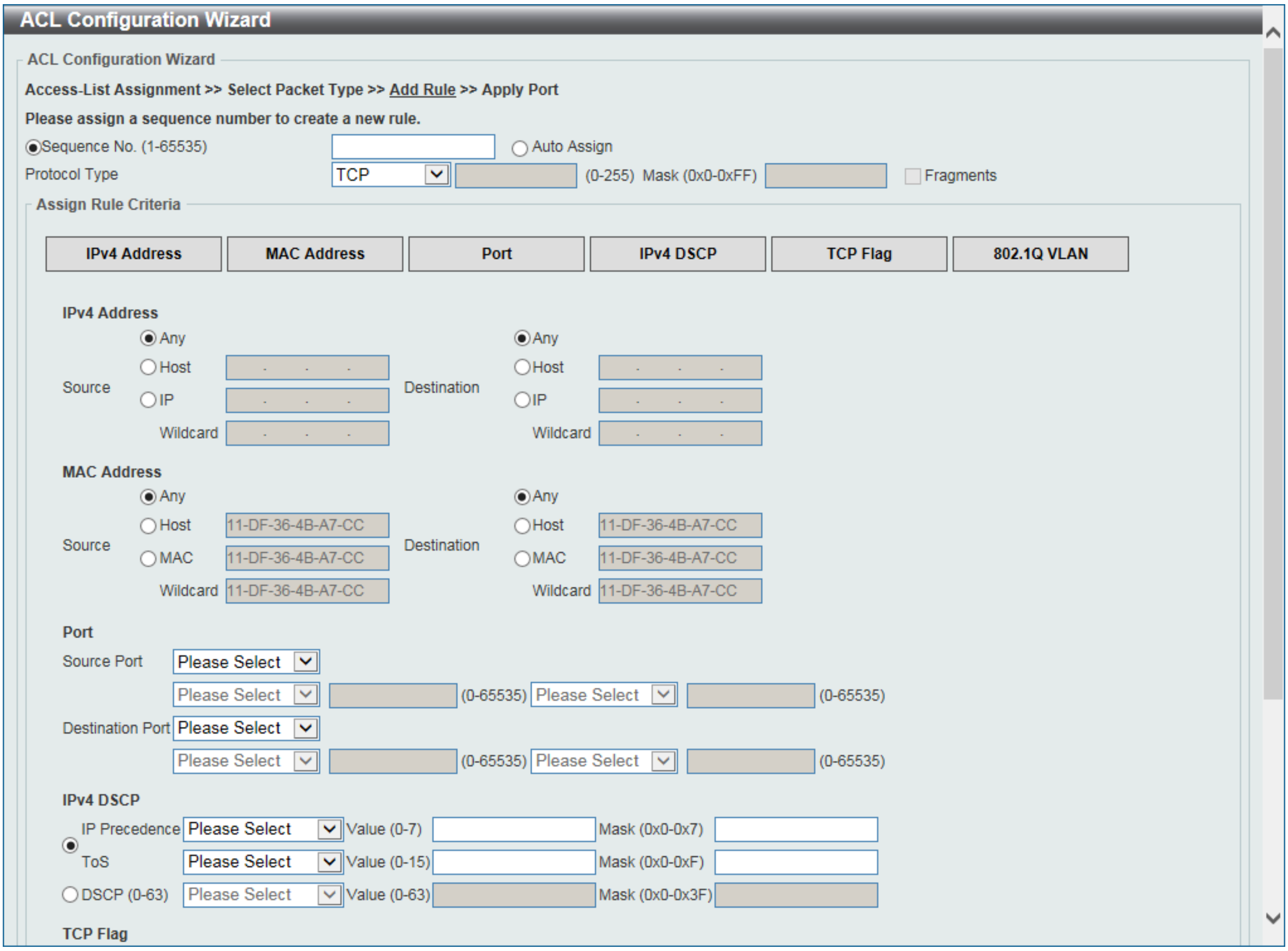
Click the ✖ button to remove the specific entry.

Click the **Back** button to return to the previous step.

Click the **Next** button to continue to the next step.

Extended Expert ACL

Selecting to **Update** an extended expert ACL and click the **Next** button to view the following window:



ACL Configuration Wizard

ACL Configuration Wizard

Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port

Please assign a sequence number to create a new rule.

● Sequence No. (1-65535) ○ Auto Assign

Protocol Type: TCP (0-255) Mask (0x0-0xFF) □ Fragments

Assign Rule Criteria

IPv4 Address

Source: ● Any ○ Host ○ IP Wildcard

Destination: ● Any ○ Host ○ IP Wildcard

MAC Address

Source: ● Any ○ Host 11-DF-36-4B-A7-CC ○ MAC 11-DF-36-4B-A7-CC Wildcard 11-DF-36-4B-A7-CC

Destination: ● Any ○ Host 11-DF-36-4B-A7-CC ○ MAC 11-DF-36-4B-A7-CC Wildcard 11-DF-36-4B-A7-CC

Port

Source Port: Please Select

Please Select (0-65535) Please Select (0-65535)

Destination Port: Please Select

Please Select (0-65535) Please Select (0-65535)

IPv4 DSCP

● IP Precedence: Please Select Value (0-7) Mask (0x0-0x7)

ToS: Please Select Value (0-15) Mask (0x0-0xF)

○ DSCP (0-63): Please Select Value (0-63) Mask (0x0-0x3F)

TCP Flag

Figure 8-10 ACL Configuration Wizard (Extended Expert ACL) Window

The fields that can be configured are described below:

Parameter	Description
Sequence No.	Enter the ACL rule number here. The range is from 1 to 65535. Select **Auto Assign** to automatically generate an ACL rule number for this entry.
Protocol Type	Select the protocol type option here. Options to choose from are **TCP**, **UDP**, **ICMP**, **EIGRP** (88), **ESP** (50), **GRE** (47), **IGMP** (2), **OSPF** (89), **PIM** (103), **VRRP** (112), **IP-in-IP** (94), **PCP** (108), **Protocol ID**, and **None**. • **Value** - The protocol ID can also manually be entered here. The range is from 0 to 255.

Parameter	Description
	• **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.

The fields that can be configured in **Assign rule criteria** are described below:

Parameter	Description
Source IPv4 Address	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host IP address here. • **IP** - The **Wildcard** option will 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 IPv4 Address	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host IP address here. • **IP** - The **Wildcard** option will 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 MAC Address	Select and enter the source MAC address information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host -** Enter the source host MAC address here. • **MAC** - The **Wildcard** option will be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination MAC Address	Select and enter the destination MAC address information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host -** Enter the destination host MAC address here. • **MAC** - The **Wildcard** option will 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: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Mask** - 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: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used.

Parameter	Description
	- **Mask** - 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-override** (4), **critical** (5), **internet** (6), and **network** (7). - **Value** - The IP precedence value can also manually be entered here. The range is from 0 to 7. - **Mask** - Enter the IP precedence mask value here. The range is from 0x0 to 0x7.
ToS	Select the Type-of-Service (**ToS**) value that will be used here. Options to choose from are **normal** (0), **min monetary cost** (1), **max reliability** (2), **max throughput** (4), and **min delay** (8). - **Value** - The ToS value can also manually be entered here. The range is from 0 to 15. - **Mask** - Enter the ToS mask value here. The range is from 0x0 to 0xF.
DSCP	Select the DSCP value that will be used here. Options to choose from are **default** (0), **af11** (10), **af12** (12), **af13** (14), **af21** (18), **af22** (20), **af23** (22), **af31** (26), **af32** (28), **af33** (30), **af41** (34), **af42** (36), **af43** (38), **cs1** (8), **cs2** (16), **cs3** (24), **cs4** (32), **cs5** (40), **cs6** (48), **cs7** (56), and **ef** (46). - **Value** - The DSCP value can also manually be entered here. The range is from 0 to 63. - **Mask** - Enter the DSCP mask value here. The range is from 0x0 to 0x3F.
TCP Flag	Select the 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**.
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.

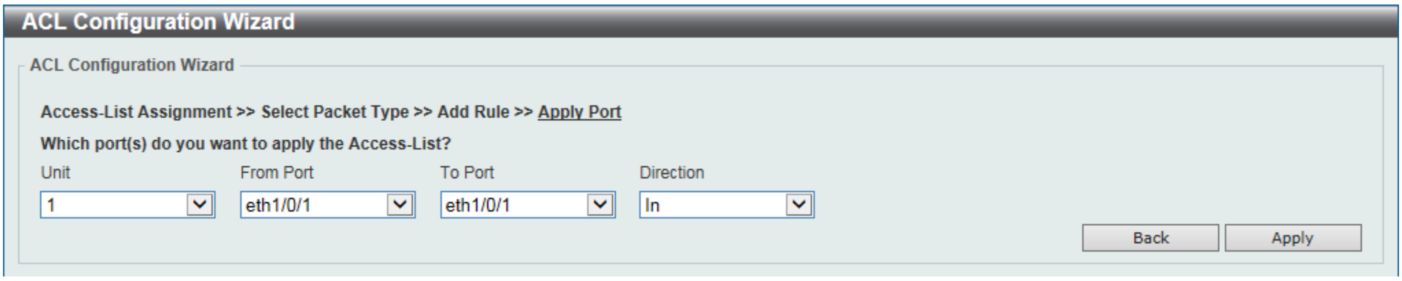
Parameter	Description
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.

Click the **Back** button to return to the previous step.

Click the **Next** button to continue to the next step.

Step 4 - Apply Port

After clicking the **Next** button, the following window will appear.



ACL Configuration Wizard

ACL Configuration Wizard

Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port

Which port(s) do you want to apply the Access-List?

Unit	From Port	To Port	Direction
1	eth1/0/1	eth1/0/1	In

Figure 8-11 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**.

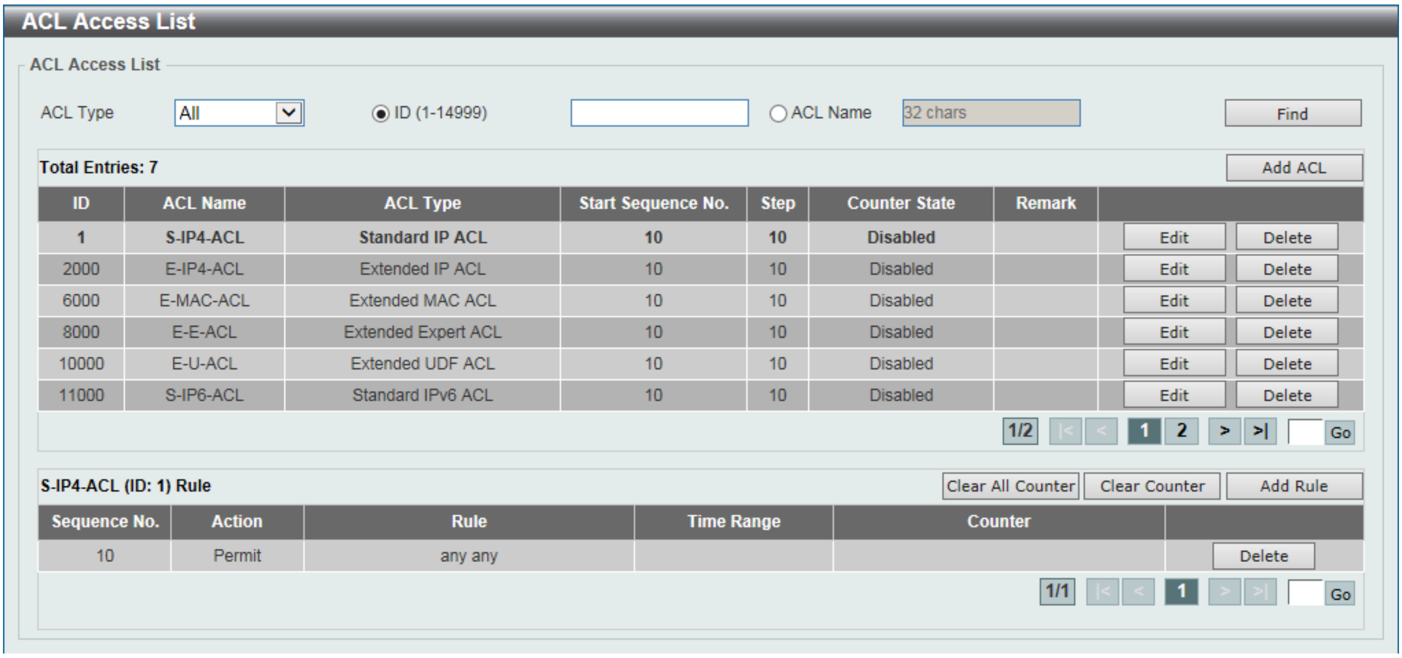
Click the **Back** button to return to the previous step.

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:



ACL Access List

ACL Access List

ACL Type: All | ● ID (1-14999) | ○ ACL Name: 32 chars

Total Entries: 7

ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	
1	S-IP4-ACL	Standard IP ACL	10	10	Disabled		Edit Delete
2000	E-IP4-ACL	Extended IP ACL	10	10	Disabled		Edit Delete
6000	E-MAC-ACL	Extended MAC ACL	10	10	Disabled		Edit Delete
8000	E-E-ACL	Extended Expert ACL	10	10	Disabled		Edit Delete
10000	E-U-ACL	Extended UDF ACL	10	10	Disabled		Edit Delete
11000	S-IP6-ACL	Standard IPv6 ACL	10	10	Disabled		Edit Delete

S-IP4-ACL (ID: 1) Rule

Sequence No.	Action	Rule	Time Range	Counter	
10	Permit	any any			Delete

Figure 8-12 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**, **Expert ACL**, and **UDF ACL**.
ID	Select and enter the access list ID here. The range is from 1 to 14999.
ACL Name	Select and enter the access list name here. This name can be up to 32 characters long.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Add ACL** button to create a new ACL.

Click the **Edit** button to re-configure the specific ACL.

Click the **Delete** button, next to the ACL, to remove the specific ACL.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **Clear All Counter** button to clear all the counter information displayed.

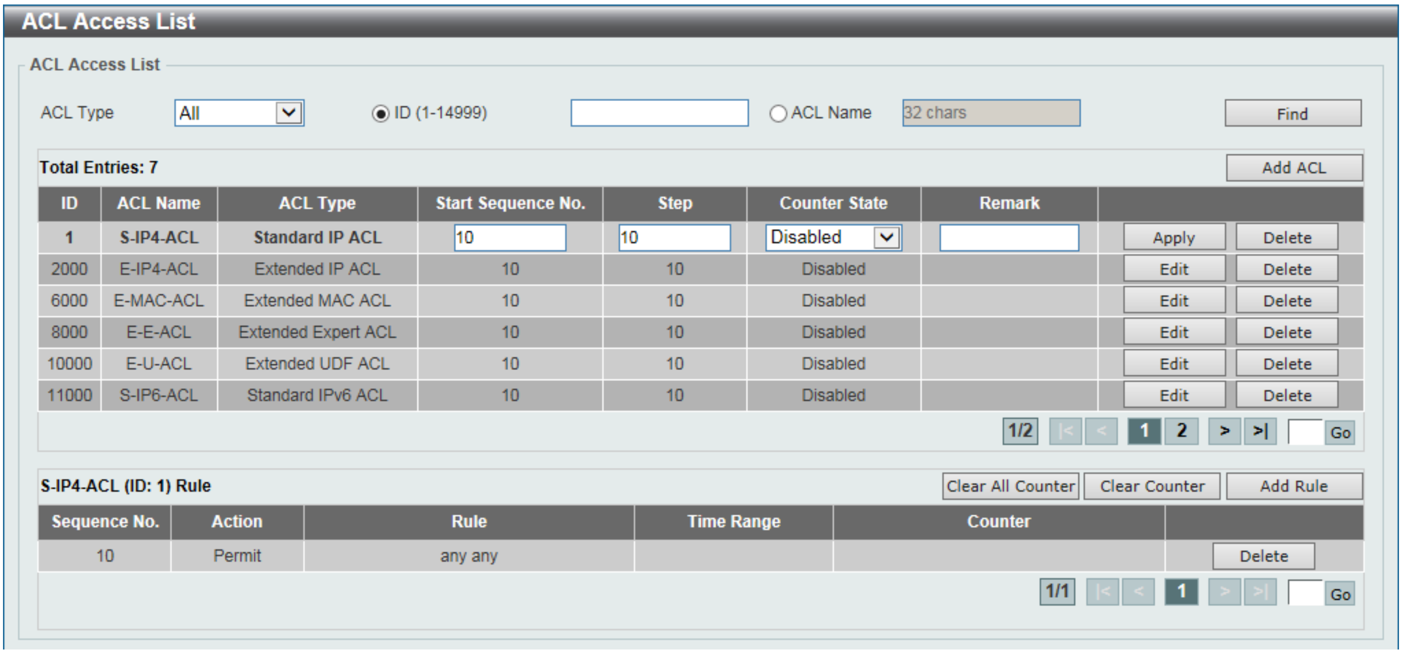
Click the **Clear Counter** button to clear the counter information for the rule displayed.

Click the **Add Rule** button to create an ACL rule for the ACL selected.

Click the **Delete** button, next to the ACL rule, to remove the specific ACL rule.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Edit** button, the following page will appear.



ACL Access List

ACL Access List

ACL Type: All ● ID (1-14999) ○ ACL Name: 32 chars

Total Entries: 7

ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	
1	S-IP4-ACL	Standard IP ACL	10	10	Disabled		Apply Delete
2000	E-IP4-ACL	Extended IP ACL	10	10	Disabled		Edit Delete
6000	E-MAC-ACL	Extended MAC ACL	10	10	Disabled		Edit Delete
8000	E-E-ACL	Extended Expert ACL	10	10	Disabled		Edit Delete
10000	E-U-ACL	Extended UDF ACL	10	10	Disabled		Edit Delete
11000	S-IP6-ACL	Standard IPv6 ACL	10	10	Disabled		Edit Delete

S-IP4-ACL (ID: 1) Rule

Sequence No.	Action	Rule	Time Range	Counter	
10	Permit	any any			Delete

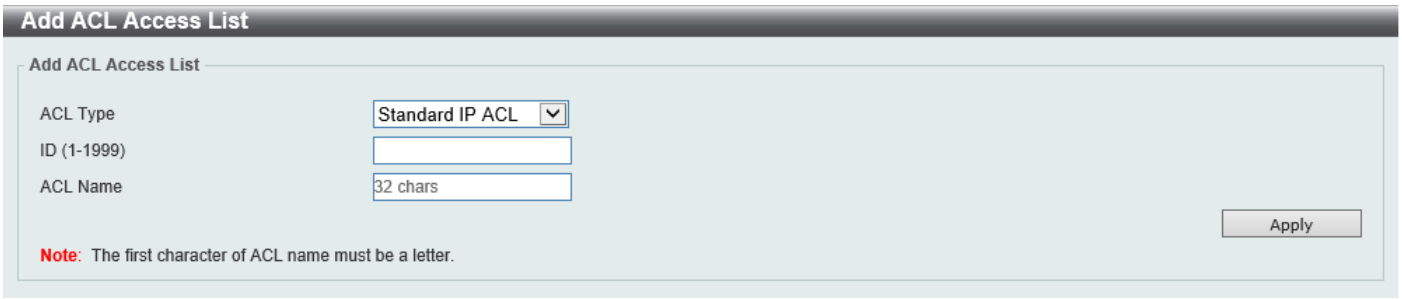
Figure 8-13 ACL Access List (Edit) Window

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. 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. By default, this value is 10.
Counter State	Select to enable or disable the counter state option here.
Remark	Enter an optional remark that will be associated with this ACL here.

Click the **Apply** button to accept the changes made.

After clicking the **Add ACL** button, the following page will appear.



Add ACL Access List

Add ACL Access List

ACL Type: Standard IP ACL

ID (1-1999):

ACL Name: 32 chars

Note: The first character of ACL name must be a letter.

Figure 8-14 ACL Access List (Add ACL) Window

After clicking the **Add ACL** button, the fields that can be configured are described below:

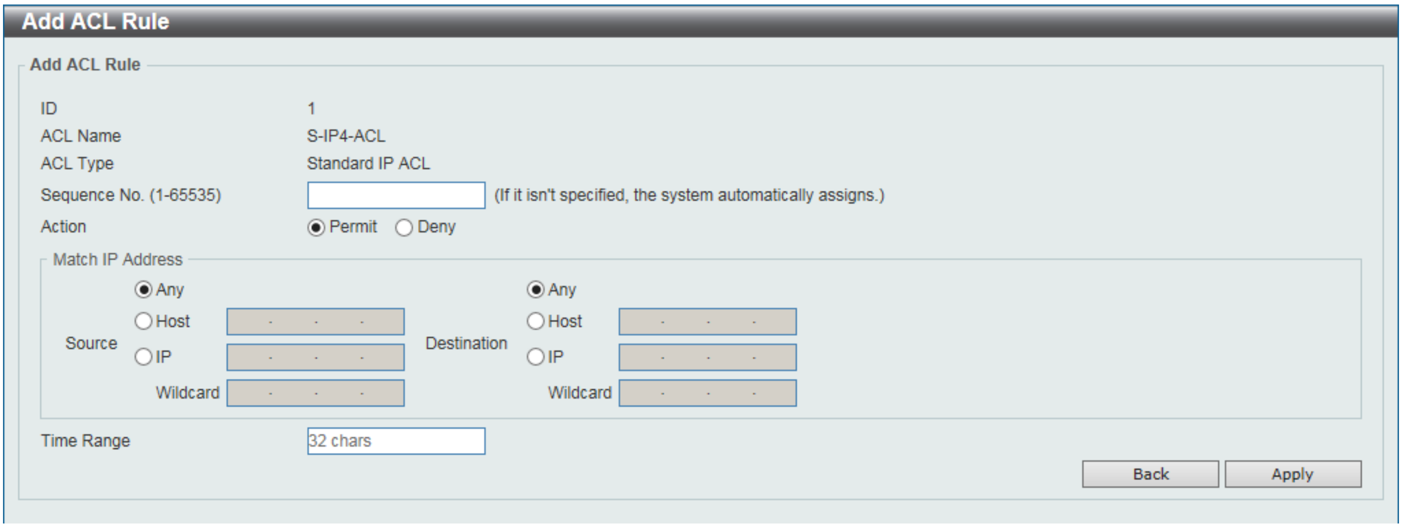
Parameter	Description
ACL Type	Select the ACL type that will be created here. Options to choose from are **Standard IP ACL**, **Extended IP ACL**, **Standard IPv6 ACL**, **Extended IPv6 ACL**, **Extended MAC ACL**, **Extended Expert ACL**, and **Extended UDF ACL**.
ID	Enter the ID for the ACL here.

Parameter	Description
	- 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. - For an **Extended UDF ACL**, the range from 10000 to 10999.
ACL Name	Enter the name of the ACL here. This name can be up to 32 characters long.

Click the **Apply** button to accept the changes made.

Standard IP ACL

After selecting a Standard IP ACL and clicking the **Add Rule** button, the following page will appear.



Add ACL Rule

Add ACL Rule

ID 1

ACL Name S-IP4-ACL

ACL Type Standard IP ACL

Sequence No. (1-65535) (If it isn't specified, the system automatically assigns.)

Action ● Permit ○ Deny

Match IP Address

Source: ● Any ○ Host ○ IP Wildcard

Destination: ● Any ○ Host ○ IP Wildcard

Time Range 32 chars

Figure 8-15 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** - Any source traffic will be evaluated according to the conditions of this rule. - **Host** - Enter the source host IP address here. - **IP** - The **Wildcard** option will 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** - Any destination traffic will be evaluated according to the conditions of this rule. - **Host** - Enter the destination host IP address here.

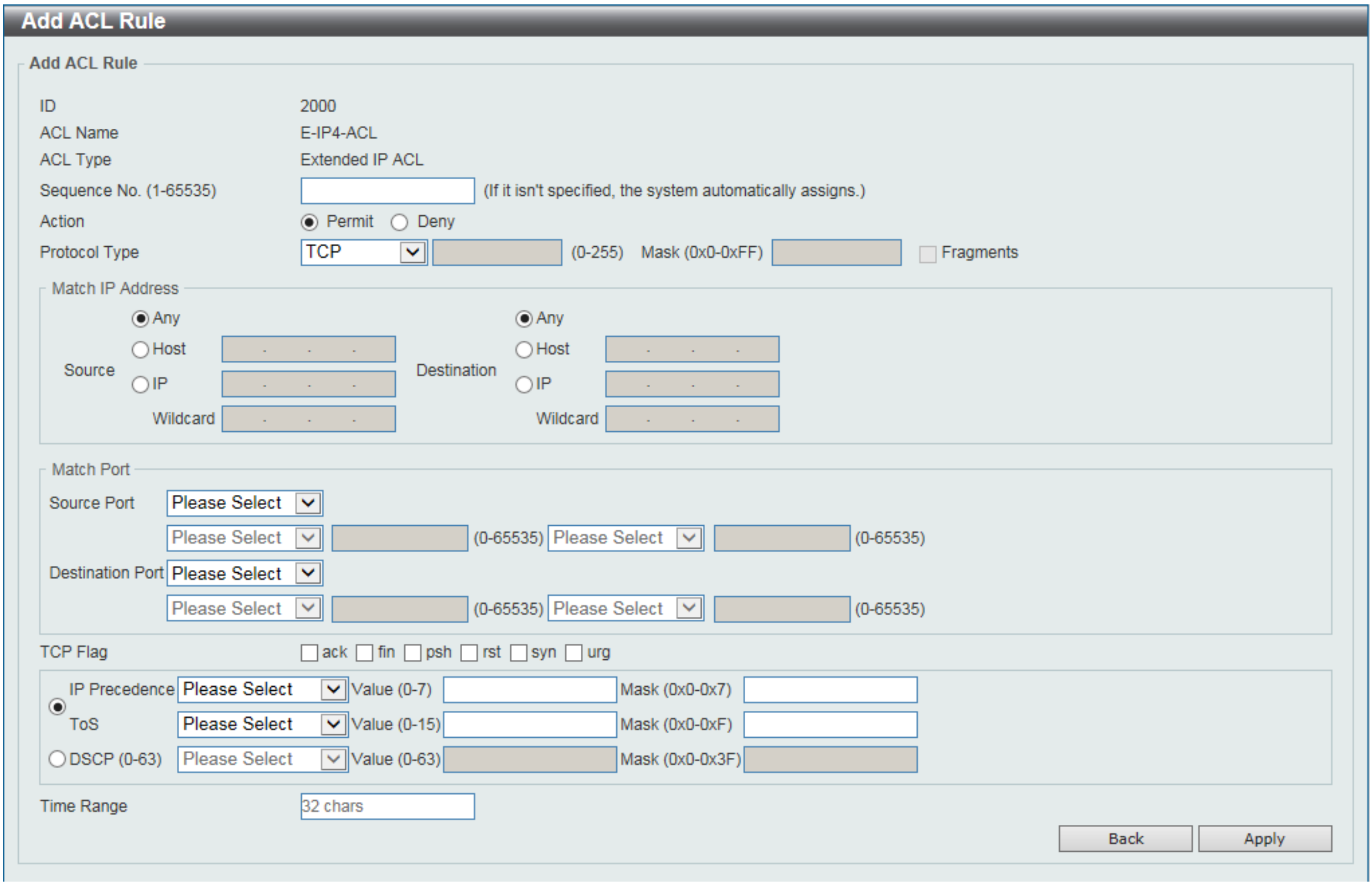
Parameter	Description
	• **IP** - The **Wildcard** option will be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.

Click the **Apply** button to accept the changes made.

Click the **Back** button to discard the changes made and return to the previous page.

Extended IP ACL

After selecting an Extended IP ACL and clicking the **Add Rule** button, the following page will appear.



Add ACL Rule

Add ACL Rule

ID 2000

ACL Name E-IP4-ACL

ACL Type Extended IP ACL

Sequence No. (1-65535) (If it isn't specified, the system automatically assigns.)

Action ● Permit ○ Deny

Protocol Type TCP (0-255) Mask (0x0-0xFF) □ Fragments

Match IP Address

Source ● Any ○ Host ○ IP Wildcard

Destination ● Any ○ Host ○ IP Wildcard

Match Port

Source Port Please Select

Please Select (0-65535) Please Select (0-65535)

Destination Port Please Select

Please Select (0-65535) Please Select (0-65535)

TCP Flag □ ack □ fin □ psh □ rst □ syn □ urg

● IP Precedence Please Select Value (0-7) Mask (0x0-0x7)

ToS Please Select Value (0-15) Mask (0x0-0xF)

○ DSCP (0-63) Please Select Value (0-63) Mask (0x0-0x3F)

Time Range 32 chars

Figure 8-16 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.

Parameter	Description
	• **Mask** - After selecting the **Protocol ID** option, manually enter the protocol mask value here. The range is from 0x0 to 0xFF. • **Fragments -** Select this option to include packet fragment filtering.
Source	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host -** Enter the source host IP address here. • **IP** - The **Wildcard** option will 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** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host -** Enter the destination host IP address here. • **IP** - The **Wildcard** option will be available. Enter the group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
Source Port	Select and enter the source port value here. Options to choose from are: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Mask** - 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: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Mask -** 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**.
TCP Flag	Select 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**.

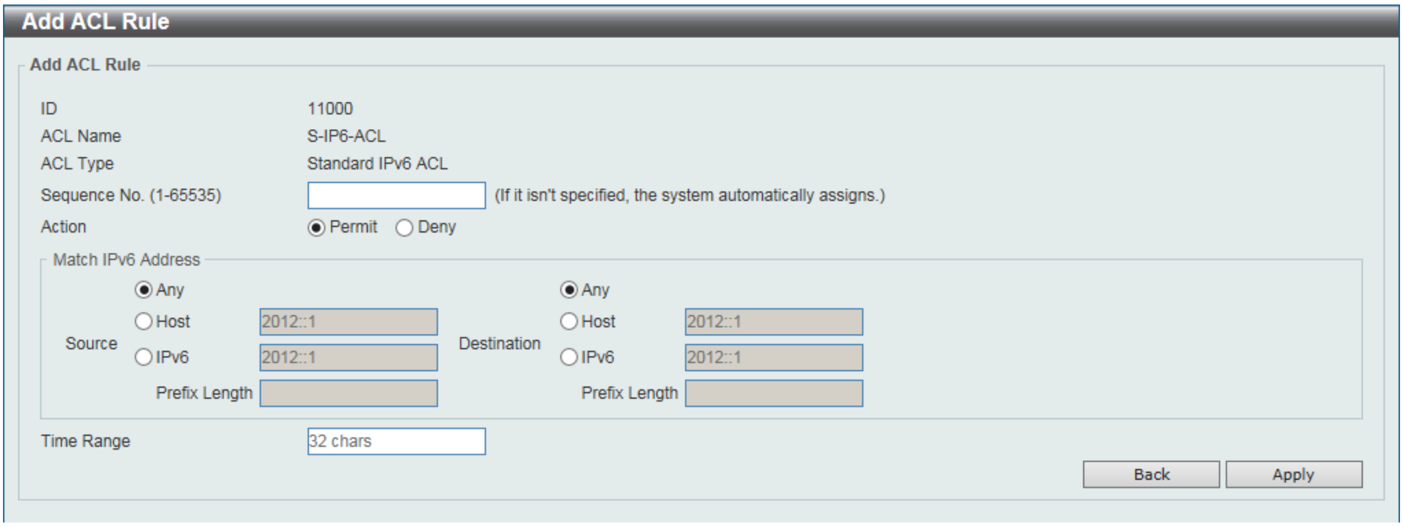
Parameter	Description
IP Precedence	Select the IP precedence value used here. Options to choose from are **routine** (0), **priority** (1), **immediate** (2), **flash** (3), **flash-override** (4), **critical** (5), **internet** (6), and **network** (7). • **Value** - The IP precedence value can also 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.

Click the **Apply** button to accept the changes made.

Click the **Back** button to discard the changes made and return to the previous page.

Standard IPv6 ACL

After selecting a Standard IPv6 ACL and clicking the **Add Rule** button, the following page will appear.



Add ACL Rule

Add ACL Rule

ID 11000

ACL Name S-IP6-ACL

ACL Type Standard IPv6 ACL

Sequence No. (1-65535) (If it isn't specified, the system automatically assigns.)

Action ● Permit ○ Deny

Match IPv6 Address

Source: ● Any ○ Host 2012::1 ○ IPv6 2012::1 Prefix Length

Destination: ● Any ○ Host 2012::1 ○ IPv6 2012::1 Prefix Length

Time Range 32 chars

Figure 8-17 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.

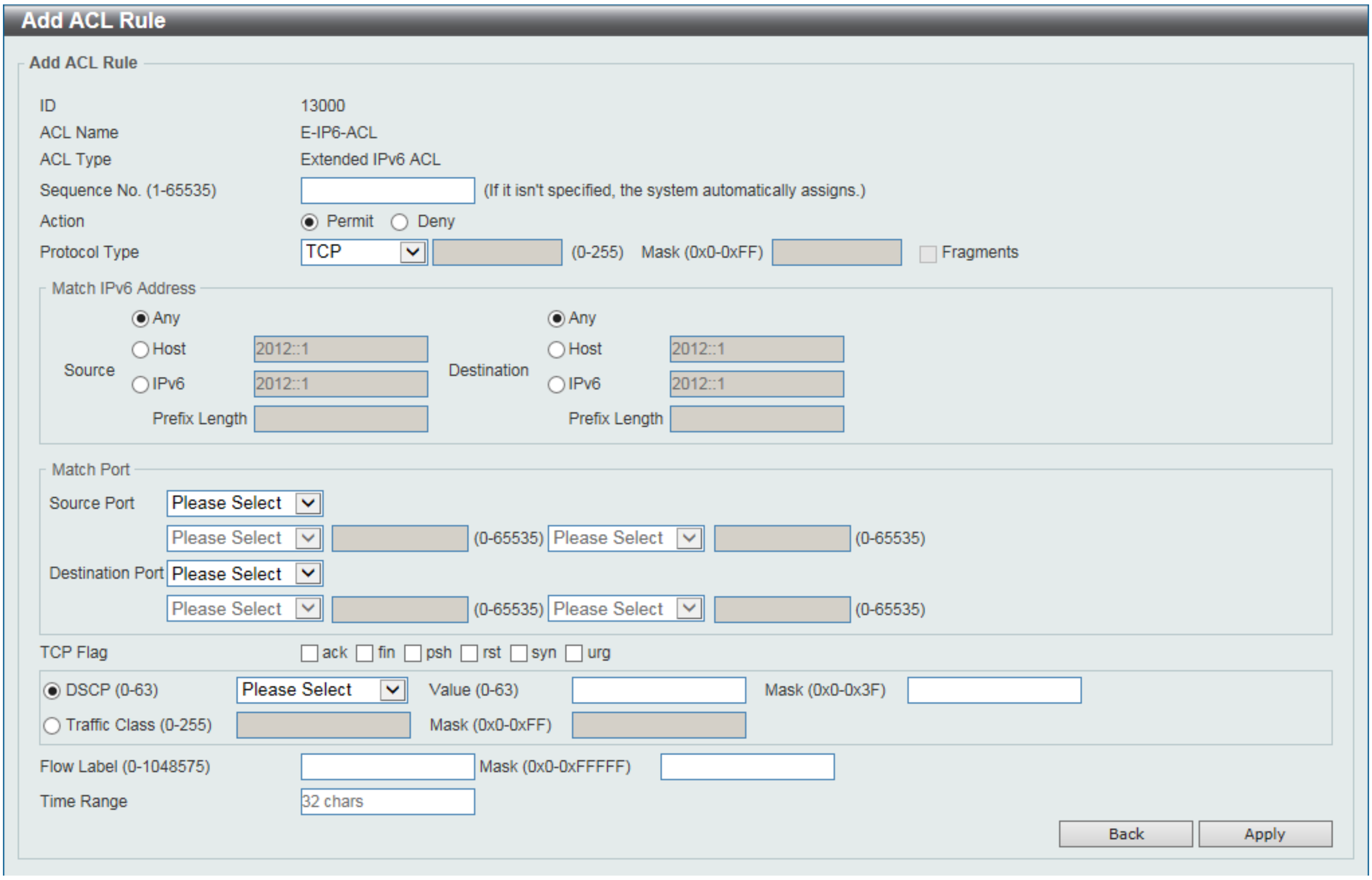
Parameter	Description
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.
Source	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host IPv6 address here. • **IPv6** - The **Prefix Length** option will be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host IPv6 address here. • **IPv6** - The **Prefix Length** option will be available. Enter the destination IPv6 address and prefix length value in the spaces provided.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.

Click the **Apply** button to accept the changes made.

Click the **Back** button to discard the changes made and return to the previous page.

Extended IPv6 ACL

After selecting an Extended IPv6 ACL and clicking the **Add Rule** button, the following page will appear.



Add ACL Rule

Add ACL Rule

ID 13000

ACL Name E-IP6-ACL

ACL Type Extended IPv6 ACL

Sequence No. (1-65535) (If it isn't specified, the system automatically assigns.)

Action ● Permit ○ Deny

Protocol Type TCP (0-255) Mask (0x0-0xFF) □ Fragments

Match IPv6 Address

Source ● Any ○ Host 2012::1 ○ IPv6 2012::1 Prefix Length

Destination ● Any ○ Host 2012::1 ○ IPv6 2012::1 Prefix Length

Match Port

Source Port Please Select
Please Select (0-65535) Please Select (0-65535)

Destination Port Please Select
Please Select (0-65535) Please Select (0-65535)

TCP Flag □ ack □ fin □ psh □ rst □ syn □ urg

● DSCP (0-63) Please Select Value (0-63) Mask (0x0-0x3F)

○ Traffic Class (0-255) Mask (0x0-0xFF)

Flow Label (0-1048575) Mask (0x0-0xFFFFF)

Time Range 32 chars

Figure 8-18 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 information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host IPv6 address here. • **IPv6** - The **Prefix Length** option will be available. Enter the source IPv6 address and prefix length value in the spaces provided.
Destination	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host IPv6 address here. • **IPv6** - The **Prefix Length** option will 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: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Mask** - 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: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Mask** - 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**.
TCP Flag	Select the appropriate TCP flag option to include the flag in this rule. Options to choose from are **ack**, **fin**, **psh**, **rst**, **syn**, and **urg**. This parameter is only available in the protocol type **TCP**.
Specify ICMP Message Type	Select the ICMP message type used here. This parameter is only available in the protocol type **ICMP**.
ICMP Message Type	When the **ICMP Message Type** is not selected, enter the ICMP Message Type numerical value used here.

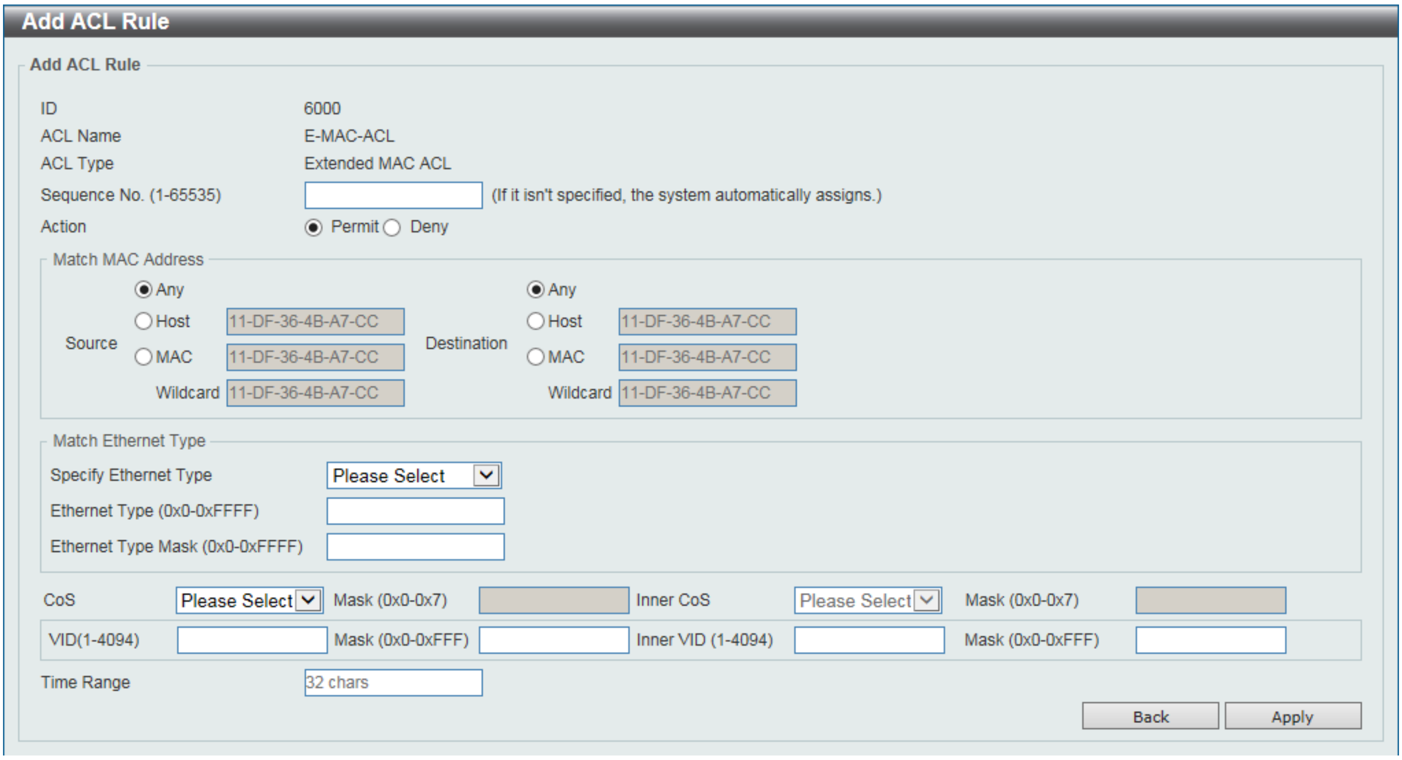
Parameter	Description
	When the **ICMP Message Type** is selected, this numerical value will automatically be entered. This parameter is only available in the protocol type **ICMP**.
Message Code	When the **ICMP Message Type** is not selected, enter the Message Code numerical value used here. When the **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. The range is from 0 to 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.

Click the **Apply** button to accept the changes made.

Click the **Back** button to discard the changes made and return to the previous page.

Extended MAC ACL

After selecting an Extended MAC ACL and clicking the **Add Rule** button, the following page will appear.



Add ACL Rule

Add ACL Rule

ID 6000

ACL Name E-MAC-ACL

ACL Type Extended MAC ACL

Sequence No. (1-65535) (If it isn't specified, the system automatically assigns.)

Action ● Permit ○ Deny

Match MAC Address

Source: ● Any; ○ Host 11-DF-36-4B-A7-CC; ○ MAC 11-DF-36-4B-A7-CC; Wildcard 11-DF-36-4B-A7-CC

Destination: ● Any; ○ Host 11-DF-36-4B-A7-CC; ○ MAC 11-DF-36-4B-A7-CC; Wildcard 11-DF-36-4B-A7-CC

Match Ethernet Type

Specify Ethernet Type: Please Select

Ethernet Type (0x0-0xFFFF)

Ethernet Type Mask (0x0-0xFFFF)

CoS: Please Select — Mask (0x0-0x7) — Inner CoS: Please Select — Mask (0x0-0x7)

VID(1-4094) — Mask (0x0-0xFFF) — Inner VID (1-4094) — Mask (0x0-0xFFF)

Time Range: 32 chars

Figure 8-19 Extended MAC ACL (Add Rule) Window

The fields that can be configured are described below:

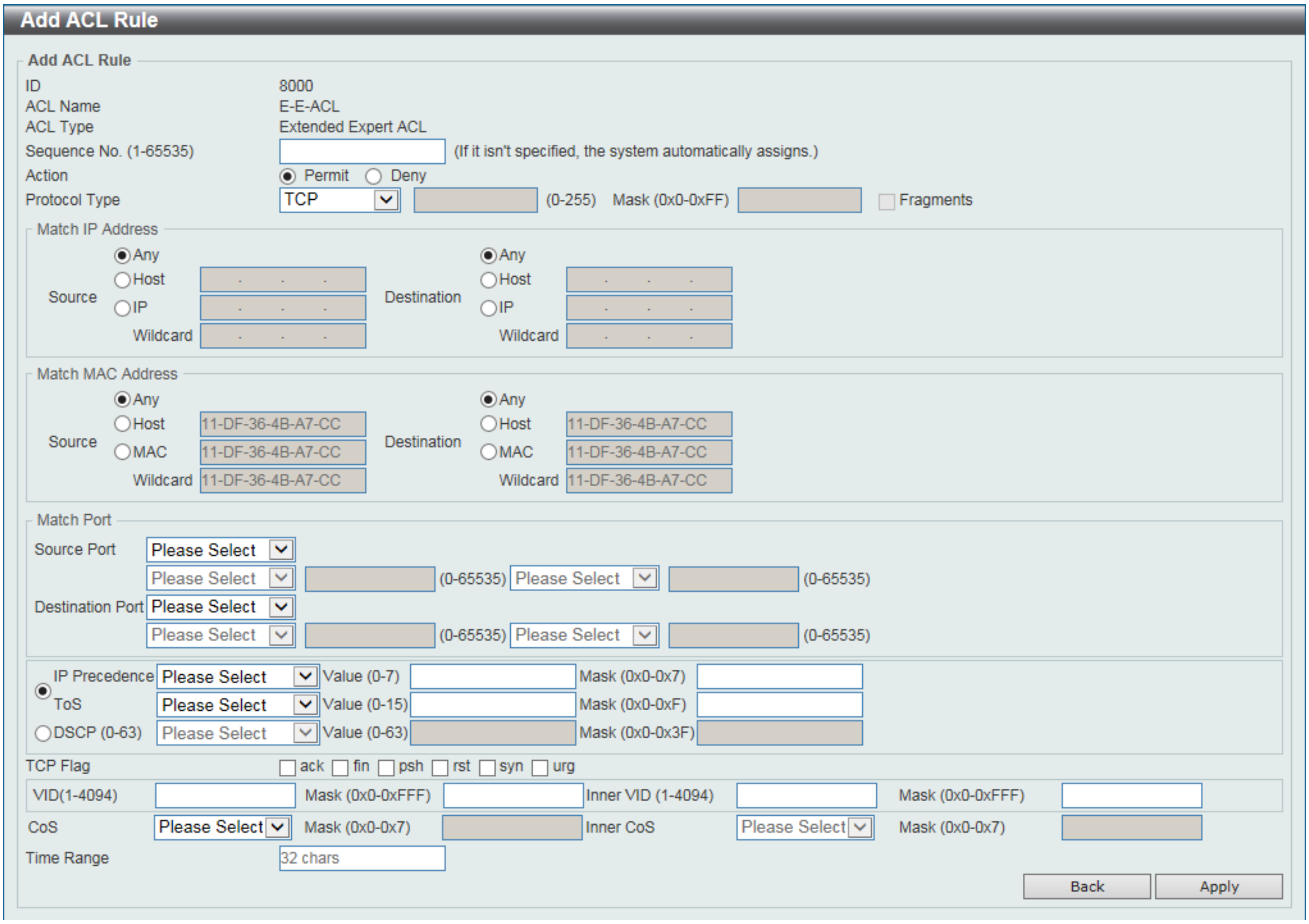
Parameter	Description
Sequence No.	Enter the sequence number of this ACL rule here. The range is from 1 to 65535. If this value is not specified, the system will automatically generate an ACL rule number for this entry.
Action	Select the action that this rule will take here. Options to choose from are **Permit** and **Deny**.
Source	Select and enter the source MAC address information here. Options to choose from are: • **Any -** Any source traffic will be evaluated according to the conditions of this rule. • **Host -** Enter the source host MAC address here. • **MAC** - The **Wildcard** option will 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 -** Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host MAC address here. • **MAC** - The **Wildcard** option will 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. The range is from 0x0 to 0xFFFF. When the Ethernet type profile is selected, above, the appropriate hexadecimal value will automatically be entered.
Ethernet Type Mask	Enter the Ethernet type mask hexadecimal value here. The range is from 0x0 to 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.

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.



Add ACL Rule

Add ACL Rule

ID	8000
ACL Name	E-E-ACL
ACL Type	Extended Expert ACL
Sequence No. (1-65535)	(If it isn't specified, the system automatically assigns.)
Action	● Permit ○ Deny
Protocol Type	TCP (0-255) Mask (0x0-0xFF) □ Fragments

Match IP Address

Source: ● Any ○ Host ○ IP Wildcard

Destination: ● Any ○ Host ○ IP Wildcard

Match MAC Address

Source: ● Any ○ Host 11-DF-36-4B-A7-CC ○ MAC 11-DF-36-4B-A7-CC Wildcard 11-DF-36-4B-A7-CC

Destination: ● Any ○ Host 11-DF-36-4B-A7-CC ○ MAC 11-DF-36-4B-A7-CC Wildcard 11-DF-36-4B-A7-CC

Match Port

Source Port: Please Select; Please Select (0-65535) Please Select (0-65535)

Destination Port: Please Select; Please Select (0-65535) Please Select (0-65535)

● IP Precedence: Please Select Value (0-7) Mask (0x0-0x7)

ToS: Please Select Value (0-15) Mask (0x0-0xF)

○ DSCP (0-63): Please Select Value (0-63) Mask (0x0-0x3F)

TCP Flag: □ ack □ fin □ psh □ rst □ syn □ urg

VID(1-4094) Mask (0x0-0xFFF) Inner VID (1-4094) Mask (0x0-0xFFF)

CoS: Please Select Mask (0x0-0x7) Inner CoS: Please Select Mask (0x0-0x7)

Time Range: 32 chars

Figure 8-20 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 IP Address	Select and enter the source information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host IP address here.

Parameter	Description
	• **IP** - The **Wildcard** option will 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 IP Address	Select and enter the destination information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host IP address here. • **IP** - The **Wildcard** option will 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 MAC Address	Select and enter the source MAC address information here. Options to choose from are: • **Any** - Any source traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the source host MAC address here. • **MAC** - The **Wildcard** option will be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination MAC Address	Select and enter the destination MAC address information here. Options to choose from are: • **Any** - Any destination traffic will be evaluated according to the conditions of this rule. • **Host** - Enter the destination host MAC address here. • **MAC** - The **Wildcard** option will 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: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Mask** - 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: • **=** - The specific selected port number will be used. • **>** - All ports greater than the selected port, will be used. • **<** - All ports smaller than the selected port, will be used. • **≠** - All ports, excluding the selected port, will be used. • **Mask** - 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.

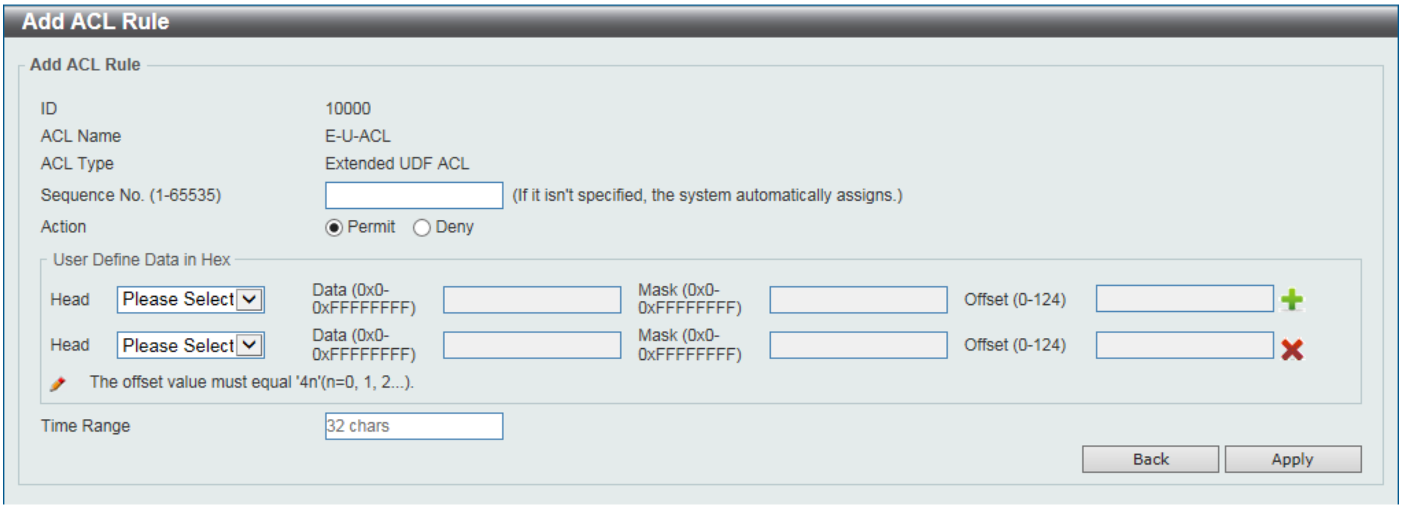
Parameter	Description
	When the **ICMP Message Type** is selected, this numerical value will automatically be entered. This parameter is only available in the protocol type **ICMP**.
IP Precedence	Select the IP precedence value used here. Options to choose from are **routine** (0), **priority** (1), **immediate** (2), **flash** (3), **flash-override** (4), **critical** (5), **internet** (6), and **network** (7). • **Value** - The IP precedence value can also manually be entered here. The range is from 0 to 7. • **Mask** - Enter the IP precedence mask value here. The range is from 0x0 to 0x7.
ToS	Select the Type-of-Service (**ToS**) value that will be used here. Options to choose from are **normal** (0), **min monetary-cost** (1), **max reliability** (2), **max throughput** (4), and **min delay** (8). • **Value** - The ToS value can also manually be entered here. The range is from 0 to 15. • **Mask** - Enter the ToS mask value here. The range is from 0x0 to 0xF.
DSCP	Select the DSCP value that will be used here. Options to choose from are **default** (0), **af11** (10), **af12** (12), **af13** (14), **af21** (18), **af22** (20), **af23** (22), **af31** (26), **af32** (28), **af33** (30), **af41** (34), **af42** (36), **af43** (38), **cs1** (8), **cs2** (16), **cs3** (24), **cs4** (32), **cs5** (40), **cs6** (48), **cs7** (56), and **ef** (46). • **Value** - The DSCP value can also manually be entered here. The range is from 0 to 63. • **Mask** - Enter the DSCP mask value here. The range is from 0x0 to 0x3F.
TCP Flag	Select the 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.
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.

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 UDF ACL

After selecting an Extended UDF ACL and clicking the **Add Rule** button, the following page will appear.



Add ACL Rule

Add ACL Rule

ID 10000

ACL Name E-U-ACL

ACL Type Extended UDF ACL

Sequence No. (1-65535) (If it isn't specified, the system automatically assigns.)

Action ● Permit ○ Deny

User Define Data in Hex

Head Please Select Data (0x0-0xFFFFFFFF) Mask (0x0-0xFFFFFFFF) Offset (0-124)

Head Please Select Data (0x0-0xFFFFFFFF) Mask (0x0-0xFFFFFFFF) Offset (0-124)

The offset value must equal '4n'(n=0, 1, 2...).

Time Range 32 chars

Figure 8-21 Extended UDF 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**.
Head	Select the offset value specified by the header. Options to choose from are **L2**, **L3**, and **L4**.
Data	Enter the UDF fields per rule to match the content of the packet. • **Mask** - Enter the data mask value here. The bit corresponding to bit value 0 will be ignored, and the bit corresponding to bit value 1 will be checked. The range is from **0x0** to **0xFFFFFFFF**.
Offset	Specifies the offset value specified by the header. The offset reference can be one of the following: • **L2** - Specifies the offset starts from the L2 header. • **L3** - Specifies the offset starts from the L3 header minus 2 bytes. • **L4** - Specifies the offset starts from the L4 header.
Time Range	Enter the name of the time range profile that will be used in this ACL rule here. This name can be up to 32 characters long.

Click the ✚ button to add more data entries.

Click the ✖ button to remove the specific entry.

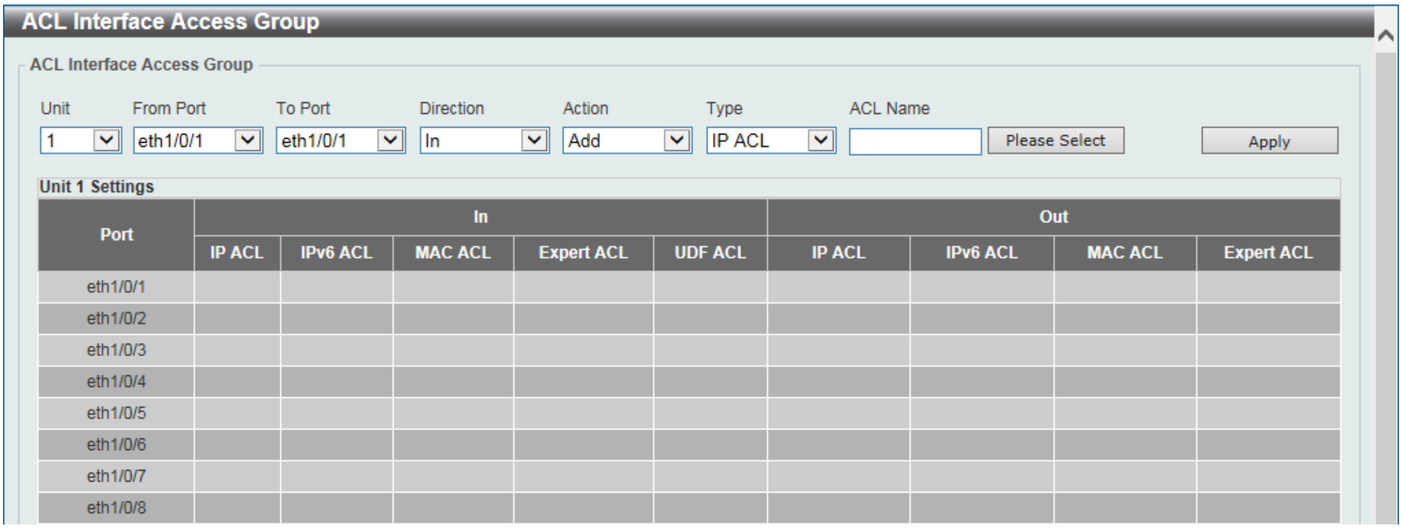
Click the **Apply** button to accept the changes made.

Click the **Back** button to discard the changes made and return to the previous page.

ACL Interface Access Group

This window is used to display and configure the ACL interface access group settings.

To view the following window, click **ACL > ACL Interface Access Group**, as shown below:



ACL Interface Access Group

ACL Interface Access Group

Unit	From Port	To Port	Direction	Action	Type	ACL Name		
1	eth1/0/1	eth1/0/1	In	Add	IP ACL		Please Select	Apply

Unit 1 Settings

Port	In					Out			
	IP ACL	IPv6 ACL	MAC ACL	Expert ACL	UDF ACL	IP ACL	IPv6 ACL	MAC ACL	Expert ACL
eth1/0/1									
eth1/0/2									
eth1/0/3									
eth1/0/4									
eth1/0/5									
eth1/0/6									
eth1/0/7									
eth1/0/8									

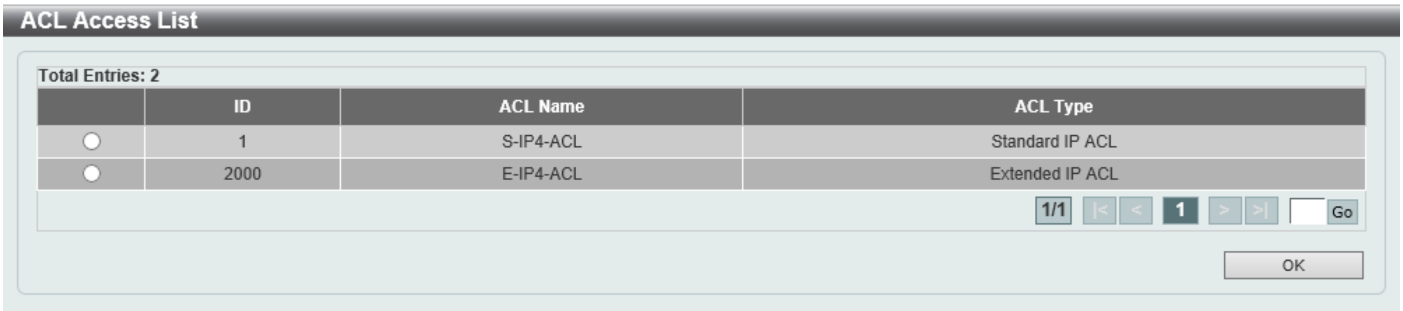
Figure 8-22 ACL Interface Access Group Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
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**.
Type	Select the ACL type here. Options to choose from are **IP ACL**, **IPv6 ACL**, **MAC ACL**, **Expert ACL**, and **UDF ACL**.
ACL Name	Enter the ACL name here. This name can be up to 32 characters long. Click the **Please Select** button to select an existing ACL from the list.

Click the **Apply** button to accept the changes made.

After clicking the **Please Select** button, the following window will appear:



ACL Access List

Total Entries: 2

	ID	ACL Name	ACL Type
○	1	S-IP4-ACL	Standard IP ACL
○	2000	E-IP4-ACL	Extended IP ACL

Figure 8-23 ACL Interface Access Group (Please Select) Window

Select the radio button next to the entry to use that ACL in the configuration.

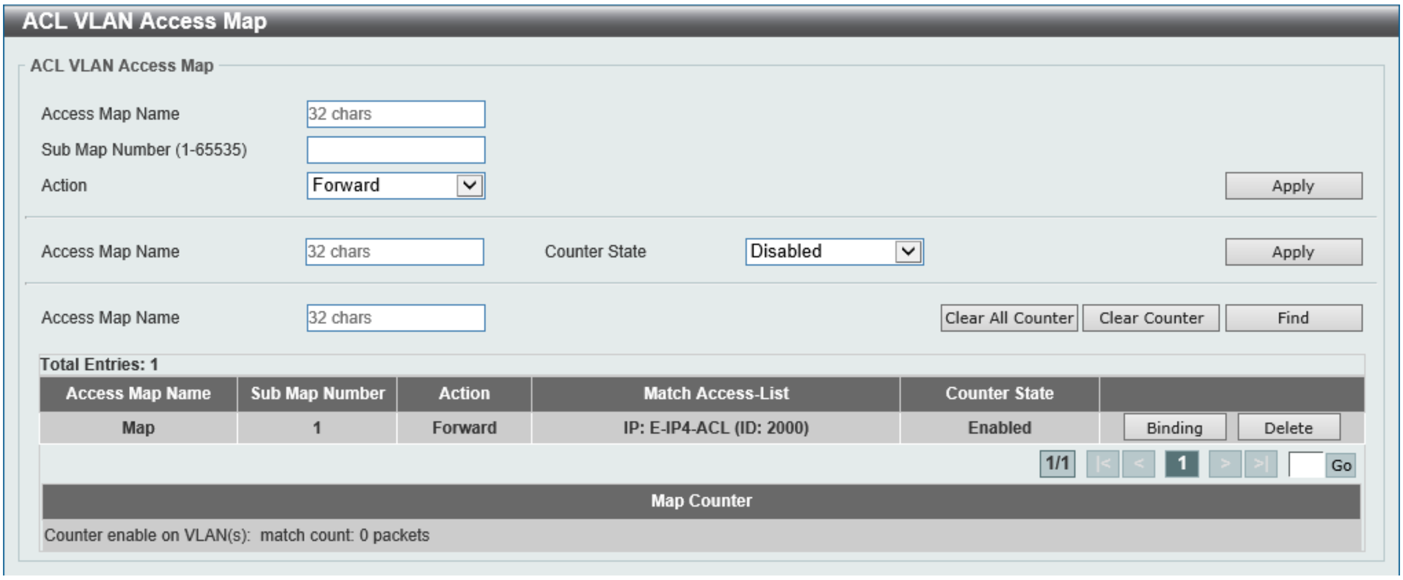
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

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:



ACL VLAN Access Map

ACL VLAN Access Map

Access Map Name: 32 chars

Sub Map Number (1-65535):

Action: Forward

Access Map Name: 32 chars   Counter State: Disabled

Access Map Name: 32 chars

Total Entries: 1

Access Map Name	Sub Map Number	Action	Match Access-List	Counter State	
Map	1	Forward	IP: E-IP4-ACL (ID: 2000)	Enabled	Binding Delete

Map Counter
Counter enable on VLAN(s): match count: 0 packets

Figure 8-24 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. The range is from 1 to 65535.
Action	Select the action that will be taken here. Options to choose from are **Forward**, **Drop**, and **Redirect**. When the **Redirect** option is selected, select the redirected interface from the drop-down list.
Counter State	Select whether to enable or disable the counter state.

Click the **Apply** button to 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.

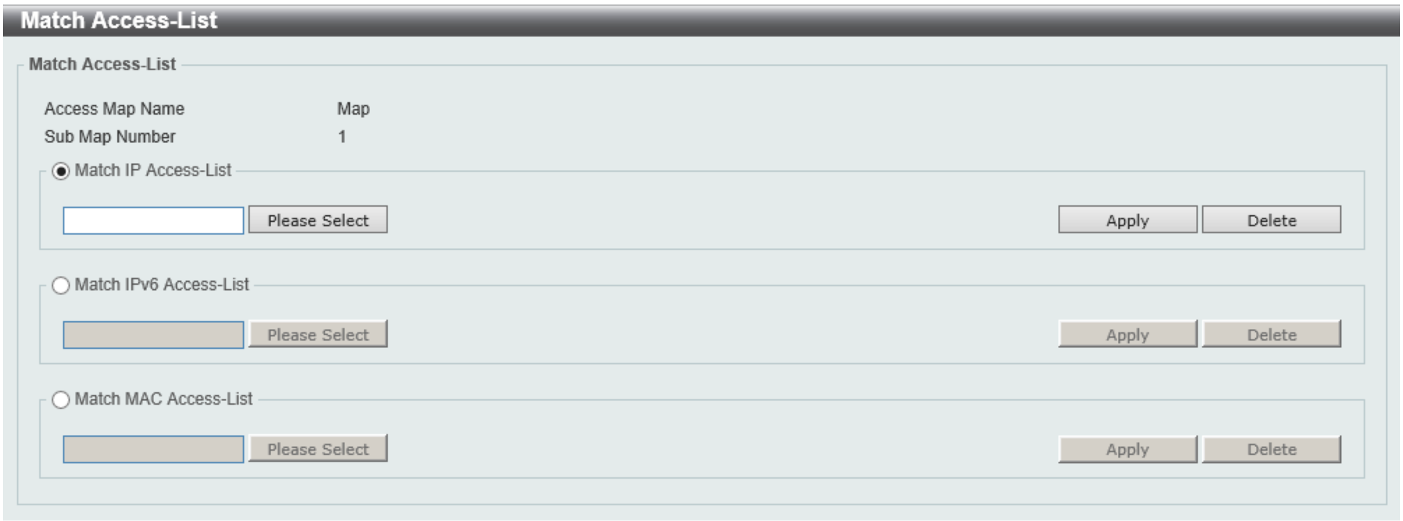
Click the **Find** button to locate a specific entry based on the information entered.

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:



Match Access-List

Match Access-List

Access Map Name Map

Sub Map Number 1

● Match IP Access-List

○ Match IPv6 Access-List

○ Match MAC Access-List

Figure 8-25 ACL VLAN Access Map (Binding) Window

The fields that can be configured are described below:

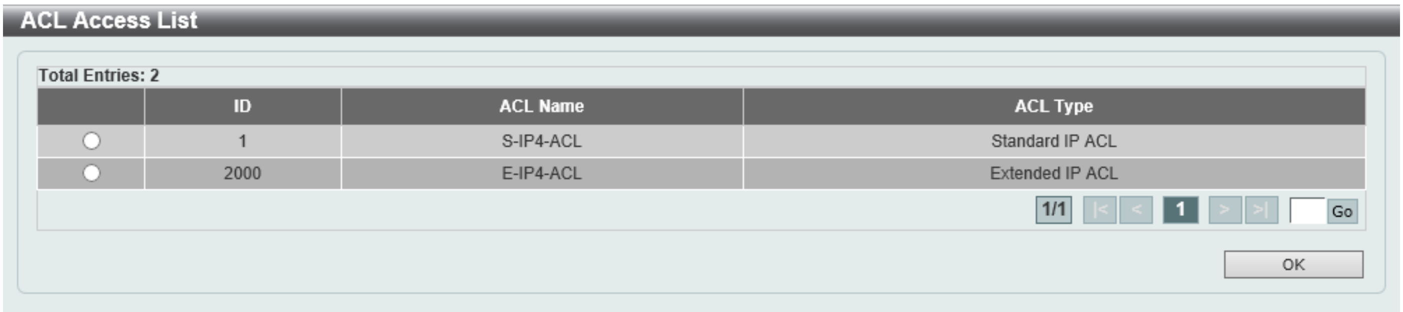
Parameter	Description
Match IP Access-List	Here the IP access list that will be matched will be displayed.
Match IPv6 Access-List	Here the IPv6 access list that will be matched will be displayed.
Match MAC Access-List	Here the MAC access list that will be matched will be displayed.

Click the **Please Select** button navigate to a list of access lists 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:



ACL Access List

Total Entries: 2

	ID	ACL Name	ACL Type
○	1	S-IP4-ACL	Standard IP ACL
○	2000	E-IP4-ACL	Extended IP ACL

Figure 8-26 ACL VLAN Access Map (Binding, Selection) Window

Select the radio button next to the entry to use that access list in the configuration.

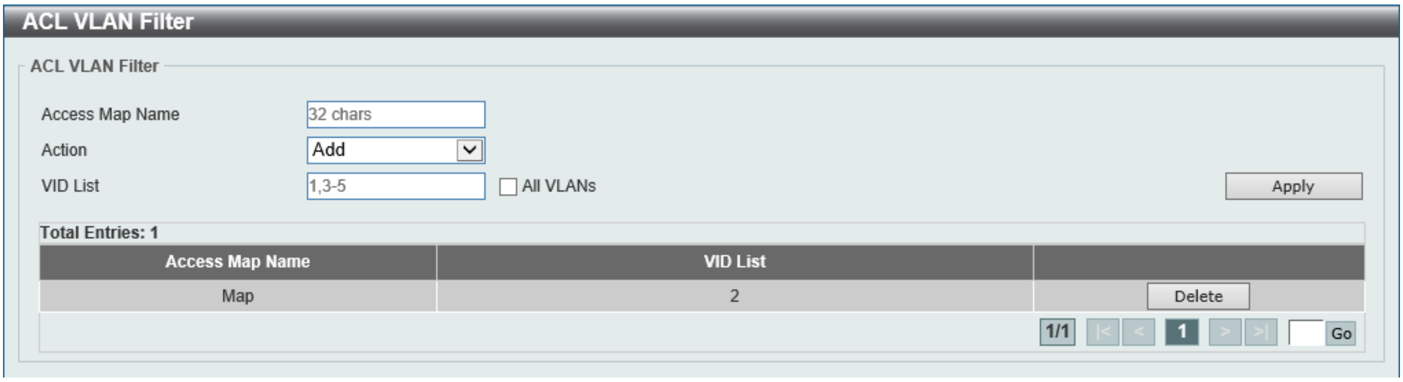
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

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.

To view the following window, click **ACL > ACL VLAN Filter**, as shown below:



ACL VLAN Filter

ACL VLAN Filter

Access Map Name: 32 chars

Action: Add

VID List: 1,3-5 □ All VLANs

Total Entries: 1

Access Map Name	VID List	
Map	2	Delete

Figure 8-27 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.
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. Select the **All VLANs** option to apply this configuration to all the VLANs configured on this Switch.

Click the **Apply** button to accept the changes made.

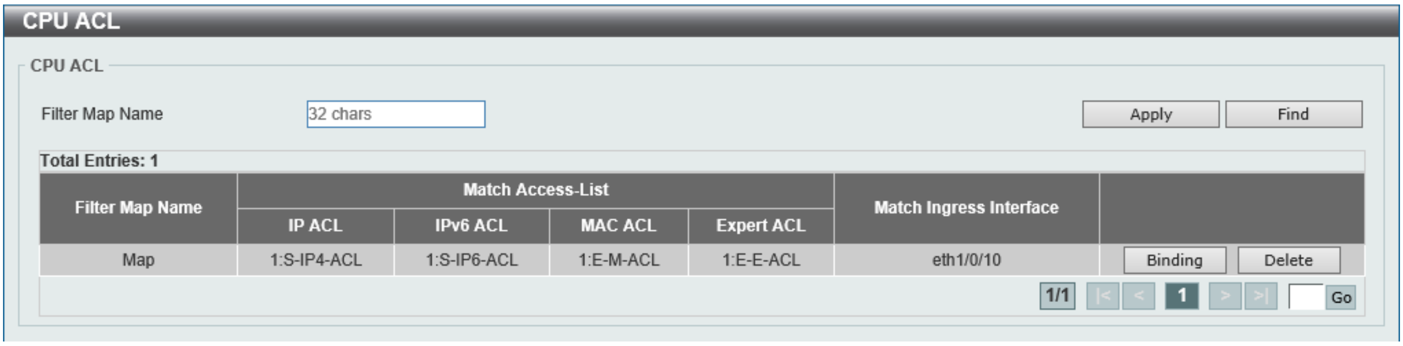
Click the **Delete** button to remove the specific entry.

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:



CPU ACL

CPU ACL

Filter Map Name: 32 chars

Total Entries: 1

Filter Map Name	Match Access-List				Match Ingress Interface	
	IP ACL	IPv6 ACL	MAC ACL	Expert ACL		
Map	1:S-IP4-ACL	1:S-IP6-ACL	1:E-M-ACL	1:E-E-ACL	eth1/0/10	Binding Delete

Figure 8-28 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.

Click the **Apply** button to accept the changes made.

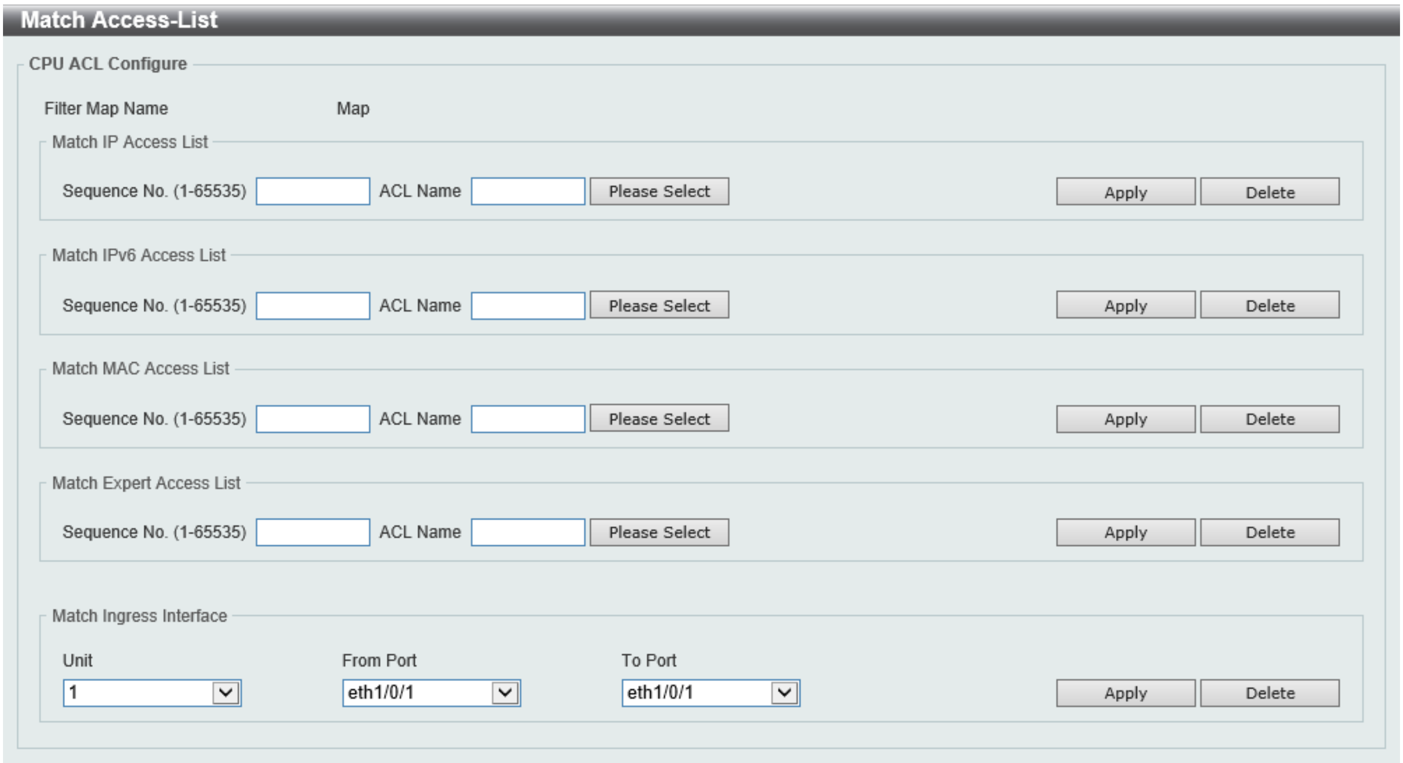
Click the **Find** button to locate a specific entry based on the information entered.

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.


Match Access-List

CPU ACL Configure

Filter Map Name: Map

Match IP Access List

Sequence No. (1-65535) ACL Name

Match IPv6 Access List

Sequence No. (1-65535) ACL Name

Match MAC Access List

Sequence No. (1-65535) ACL Name

Match Expert Access List

Sequence No. (1-65535) ACL Name

Match Ingress Interface

Unit: 1

From Port: eth1/0/1

To Port: eth1/0/1

Figure 8-29 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.

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.

Parameter	Description
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.

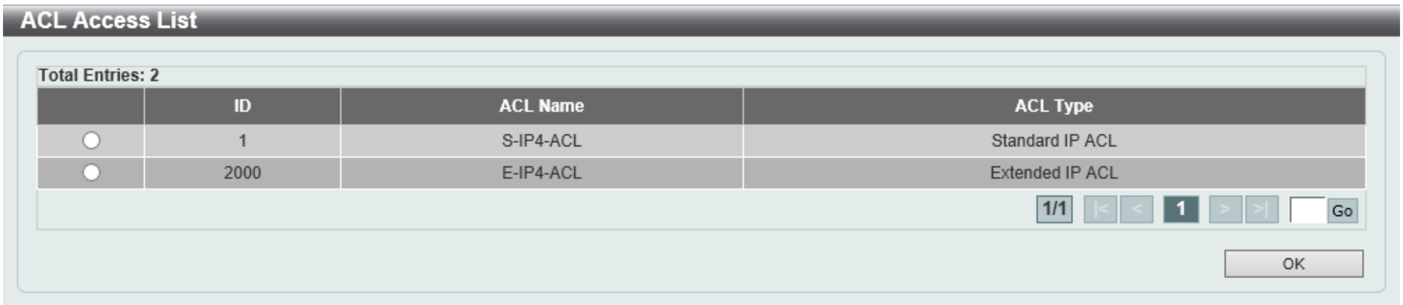
The fields that can be configured in **Match Ingress Interface** are described below:

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.

After clicking the **Please Select** button, the following window will appear:



ACL Access List

Total Entries: 2

	ID	ACL Name	ACL Type
○	1	S-IP4-ACL	Standard IP ACL
○	2000	E-IP4-ACL	Extended IP ACL

Figure 8-30 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.

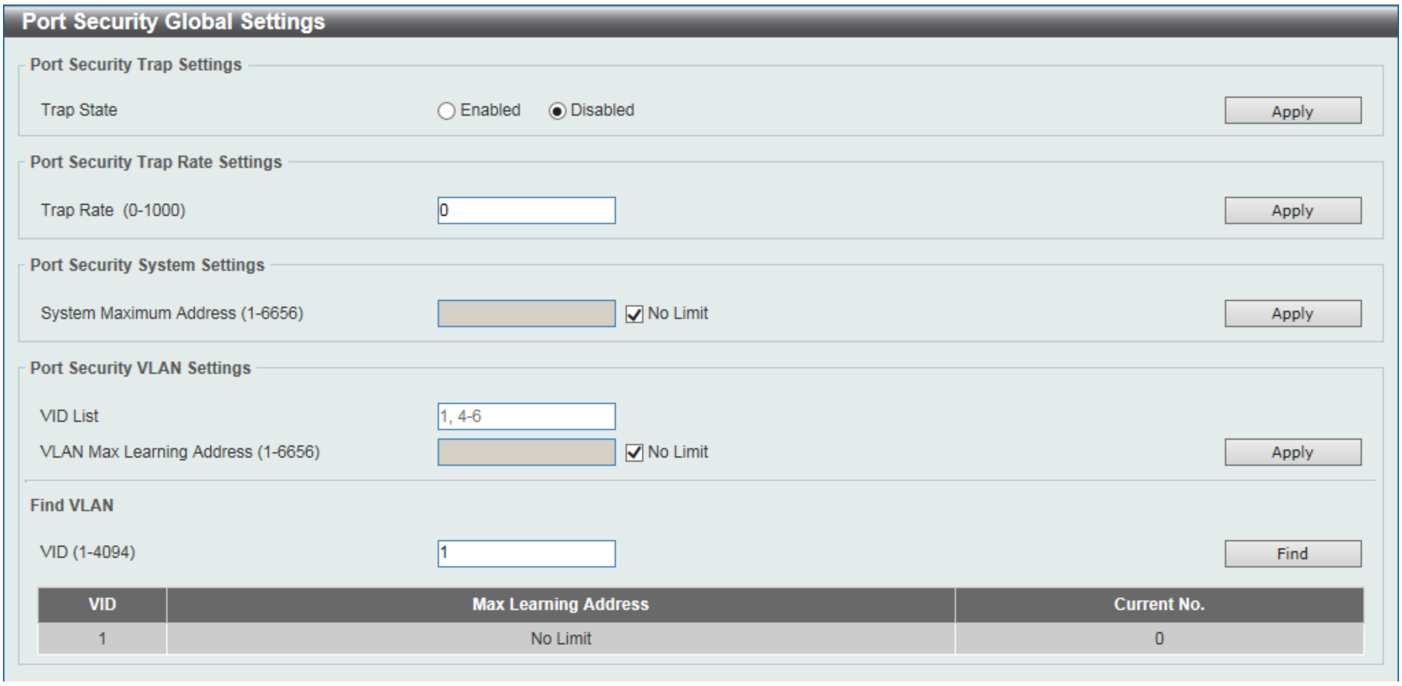
9. Security

Port Security

Port Security Global Settings

This window is used to display and configure the global port security settings. Port Security is a security feature that prevents unauthorized computers (with source MAC addresses) unknown to the Switch prior to locking the port (or ports) from connecting to the Switch's locked ports and gaining access to the network.

To view the following window, click **Security > Port Security > Port Security Global Settings**, as shown below:



Port Security Global Settings

Port Security Trap Settings

Trap State ○ Enabled ● Disabled [Apply]

Port Security Trap Rate Settings

Trap Rate (0-1000) 0 [Apply]

Port Security System Settings

System Maximum Address (1-6656) ☑ No Limit [Apply]

Port Security VLAN Settings

VID List 1, 4-6

VLAN Max Learning Address (1-6656) ☑ No Limit [Apply]

Find VLAN

VID (1-4094) 1 [Find]

VID	Max Learning Address	Current No.
1	No Limit	0

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. By default, this value is 0. This indicates that an SNMP trap is 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. The range is from 1 to 6656. By default, there is no limit.

Parameter	Description
	Select 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.
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 6656. 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:

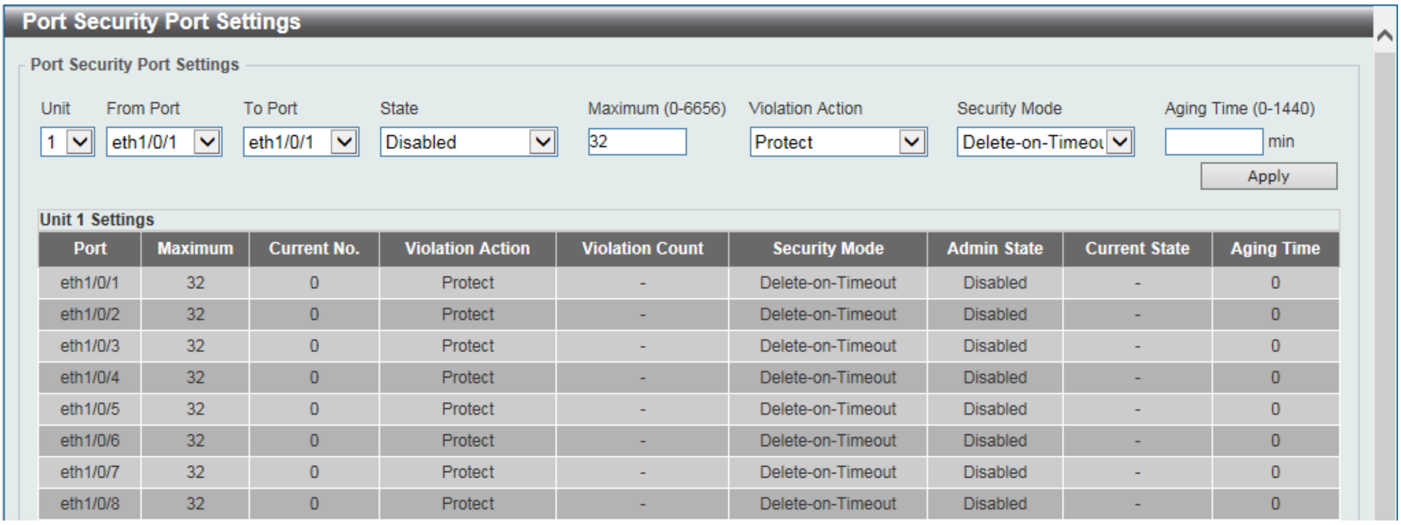
Parameter	Description
VID	Enter the VLAN ID that will be located here.

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:



Port Security Port Settings

Port Security Port Settings

Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1
State: Disabled
Maximum (0-6656): 32
Violation Action: Protect
Security Mode: Delete-on-Timeou
Aging Time (0-1440): min

Unit 1 Settings

Port	Maximum	Current No.	Violation Action	Violation Count	Security Mode	Admin State	Current State	Aging Time
eth1/0/1	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0
eth1/0/2	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0
eth1/0/3	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0
eth1/0/4	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0
eth1/0/5	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0
eth1/0/6	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0
eth1/0/7	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0
eth1/0/8	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0

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.
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. The range is from 0 to 6656. By default, this value is 32.

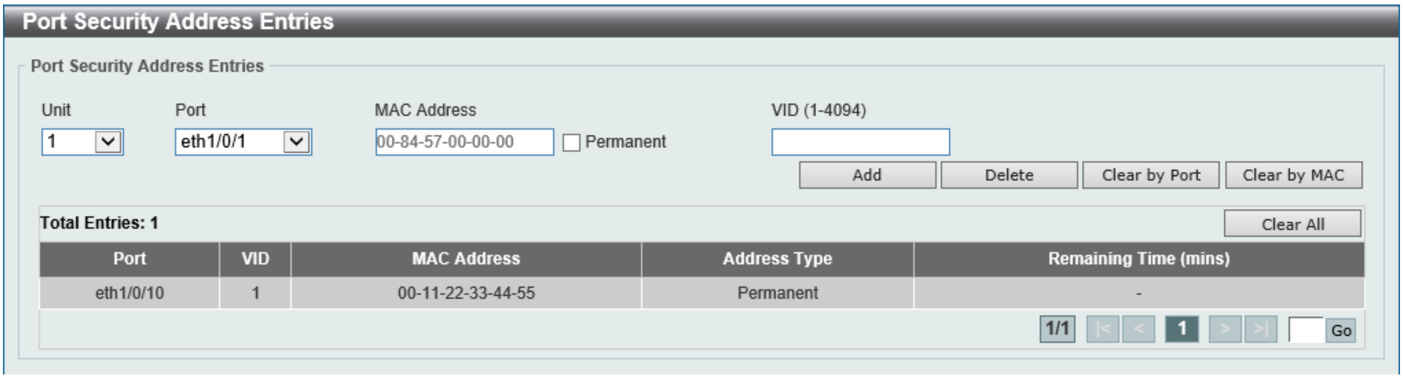
Parameter	Description
Violation Action	Select the violation action that will be taken here. Options to choose from are: • **Protect** - Specifies to drop all packets from the insecure hosts at the port-security process level, but does not increment the security-violation count. • **Restrict** - Specifies to drop all packets from the insecure hosts at the port-security process level and increments the security-violation count and record the system log. • **Shutdown** - Specifies to shut down the port if there is a security violation and record the system log.
Security Mode	Select the security mode option here. Options to choose from are: • **Permanent** - Specifies that under this mode, all learned MAC addresses are not be purged out unless the user manually deletes those entries. • **Delete-on-Timeout** - Specifies that under this mode, all learned MAC addresses are purged out when an entry is aged out or when the user manually deletes these entries.
Aging Time	Enter the aging time value used for auto-learned dynamic secured addresses on the specified port here. The range is from 0 to 1440 minutes.

Click the **Apply** button to accept the changes made.

Port Security Address Entries

This window is used to view, clear, and configure the port security address entries.

To view the following window, click **Security > Port Security > Port Security Address Entries**, as shown below:



Port Security Address Entries

Port Security Address Entries

Unit: 1
Port: eth1/0/1
MAC Address: 00-84-57-00-00-00 □ Permanent
VID (1-4094):

Total Entries: 1

Port	VID	MAC Address	Address Type	Remaining Time (mins)
eth1/0/10	1	00-11-22-33-44-55	Permanent	-

Figure 9-3 Port Security Address Entries Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
Port	Select the appropriate port range used for the configuration here.
MAC Address	Enter the MAC address here. Select **Permanent** to specify that all learned MAC addresses are not purged out unless the user manually delete those entries.
VID	Enter the VLAN ID here. The range is from 1 to 4094.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove a new entry based on the information entered.

Click the **Clear by Port** button to clear the information based on the port selected.

Click the **Clear by MAC** button to clear the information based on the MAC address entered.

Click the **Clear All** button to clear all the information in this table.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

802.1X

802.1X (Port-based and Host-based Access Control)

The IEEE 802.1X standard is a security measure for authorizing and authenticating users to gain access to various wired or wireless devices on a specified Local Area Network by using a Client and Server based access control model. This is accomplished by using a RADIUS server to authenticate users trying to access a network by relaying Extensible Authentication Protocol over LAN (EAPOL) packets between the Client and the Server.

The following figure represents a basic EAPOL packet:

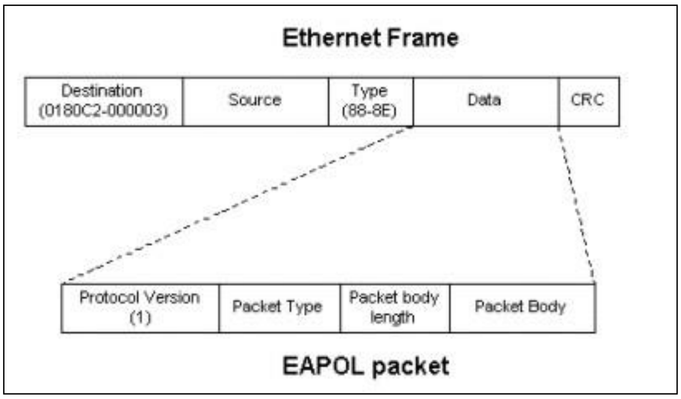


Figure 9-4 The EAPOL Packet

Utilizing this method, unauthorized devices are restricted from connecting to a LAN through a port to which the user is connected. EAPOL packets are the only traffic that can be transmitted through the specific port until authorization is granted. The 802.1X access control method has three roles, each of which are vital to creating and up keeping a stable and working Access Control security method.

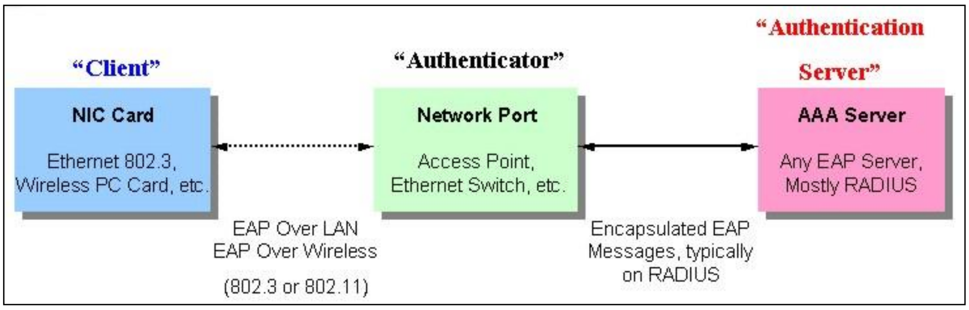

"Client"
NIC Card
Ethernet 802.3, Wireless PC Card, etc.
"Authenticator"
Network Port
Access Point, Ethernet Switch, etc.
"Authentication Server"
AAA Server
Any EAP Server, Mostly RADIUS
EAP Over LAN
EAP Over Wireless
(802.3 or 802.11)
Encapsulated EAP Messages, typically on RADIUS

Figure 9-5 The three roles of 802.1X

The following section will explain the three roles of Client, Authenticator, and Authentication Server in greater detail.

Authentication Server

The Authentication Server is a remote device that is connected to the same network as the Client and Authenticator, must be running a RADIUS Server program and must be configured properly on the Authenticator (Switch). Clients connected to a port on the Switch must be authenticated by the Authentication Server (RADIUS) before attaining any services offered by the Switch on the LAN. The role of the Authentication Server is to certify the identity of the Client attempting to access the network by exchanging secure information between the RADIUS server and the Client through EAPOL packets and, in turn, informs the Switch whether or not the Client is granted access to the LAN and/or Switches services.

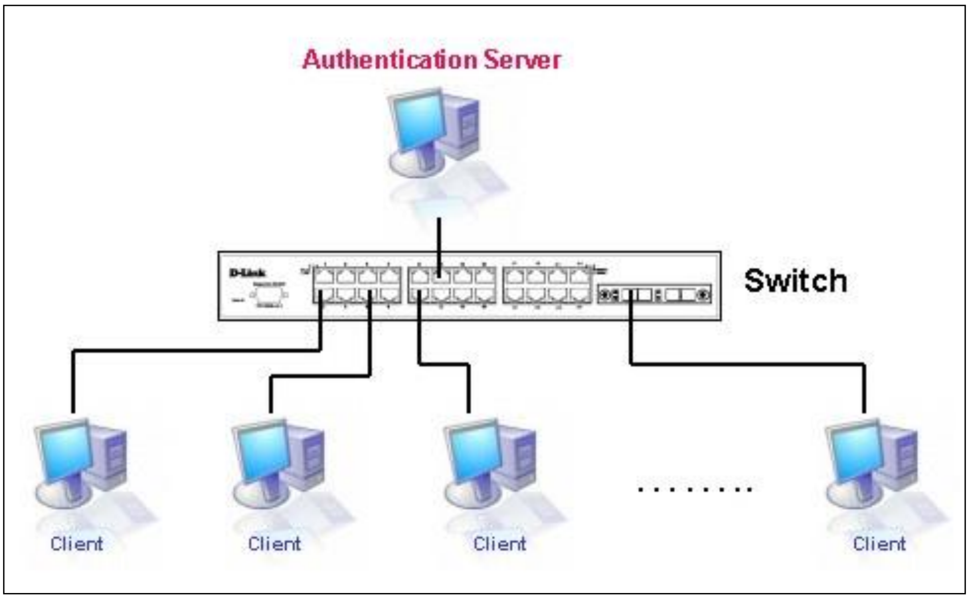


Figure 9-6 The Authentication Server

Authenticator

The Authenticator (the Switch) is an intermediary between the Authentication Server and the Client. The Authenticator serves two purposes when utilizing the 802.1X function. The first purpose is to request certification information from the Client through EAPOL packets, which is the only information allowed to pass through the Authenticator before access is granted to the Client. The second purpose of the Authenticator is to verify the information gathered from the Client with the Authentication Server, and to then relay that information back to the Client.

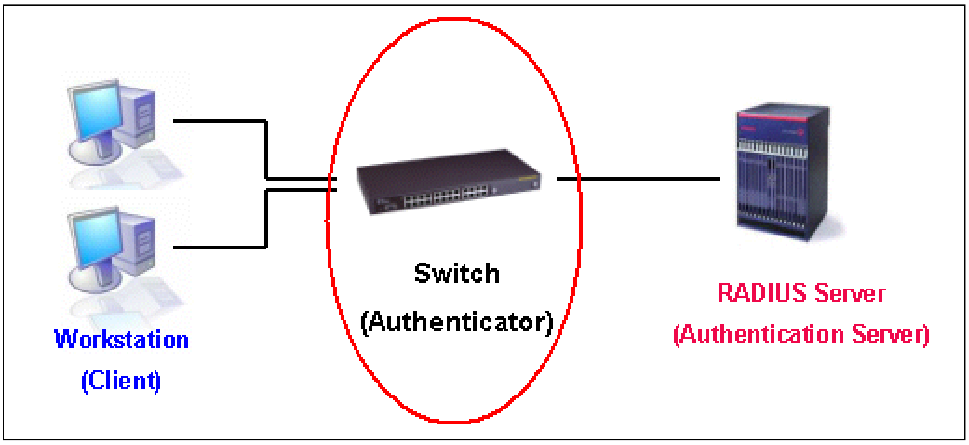


Figure 9-7 The Authenticator

Three steps must be implemented on the Switch to properly configure the Authenticator.

- The 802.1X State must be Enabled. (**Security > 802.1X > 802.1X Global Settings**)
- The 802.1X settings must be implemented by port (**Security > 802.1X > 802.1X Port Settings**)
- A RADIUS server must be configured on the Switch. (**Security > RADIUS > RADIUS Server Settings**)

Client

The Client is simply the end station that wishes to gain access to the LAN or Switch services. All end stations must be running software that is compliant with the 802.1X protocol. For users running Windows 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.

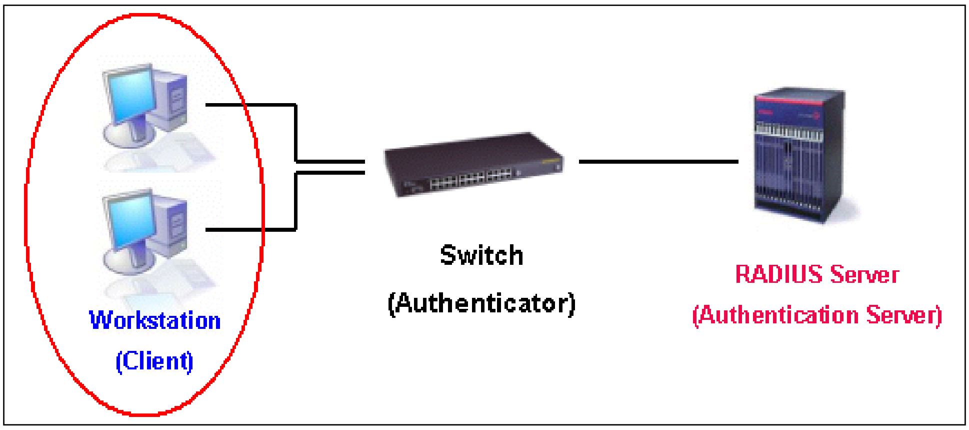


Figure 9-8 The Client

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 detailed explanation of how the authentication process is completed between the three roles stated above.

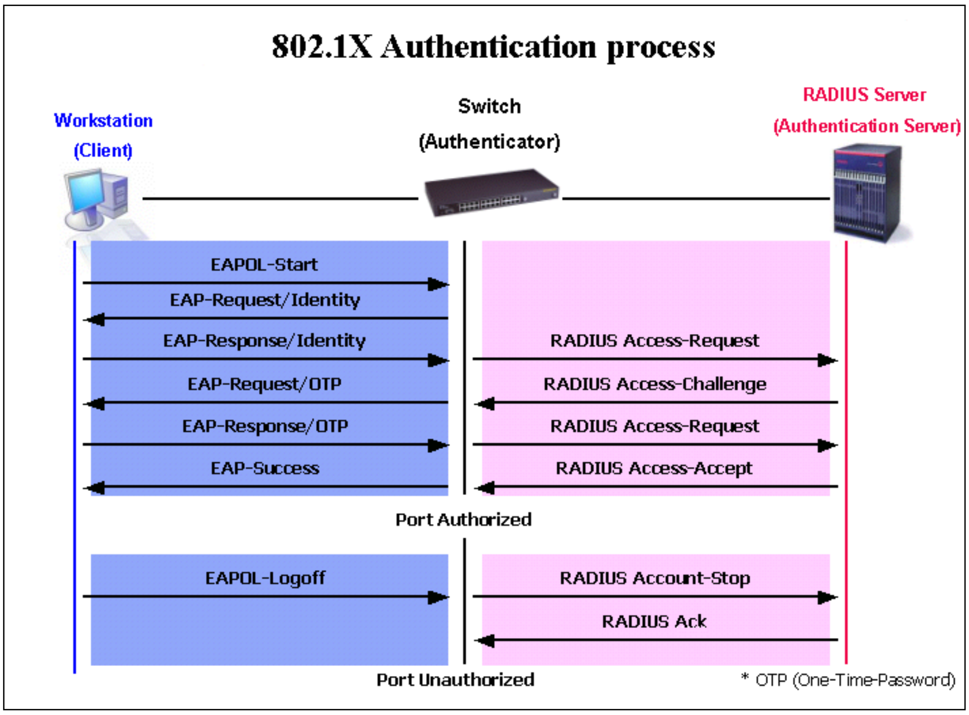


Figure 9-9 The 802.1X Authentication Process

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 448 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.

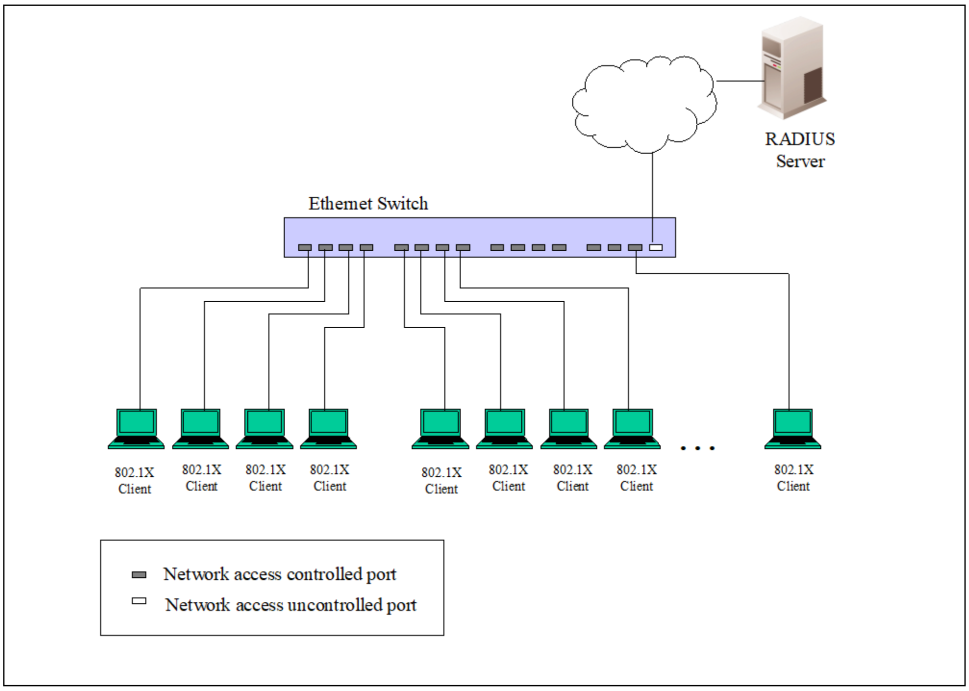


Figure 9-10 Example of Typical Port-based Configuration

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.

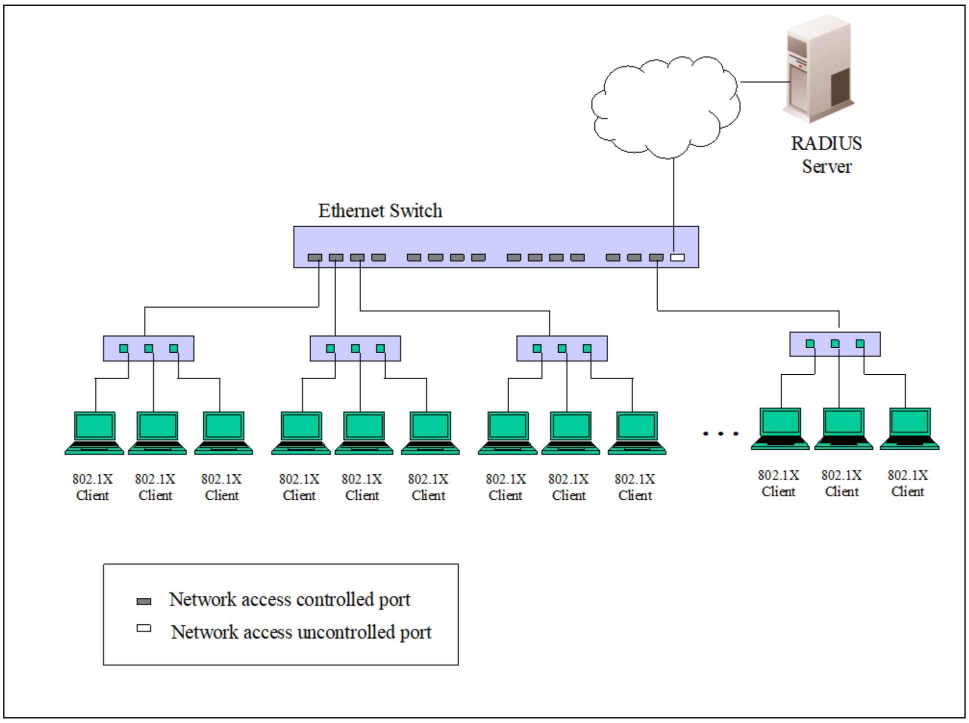
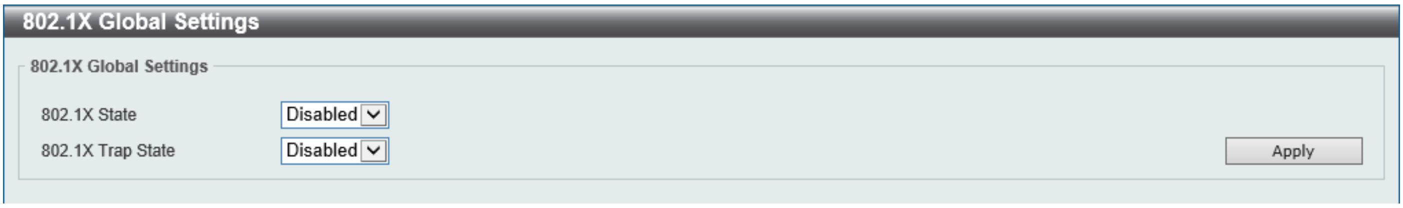


Figure 9-11 Example of Typical Host-based Configuration

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:


802.1X Global Settings

802.1X Global Settings

802.1X State: Disabled

802.1X Trap State: Disabled

Figure 9-12 802.1X Global Settings Window

The fields that can be configured are described below:

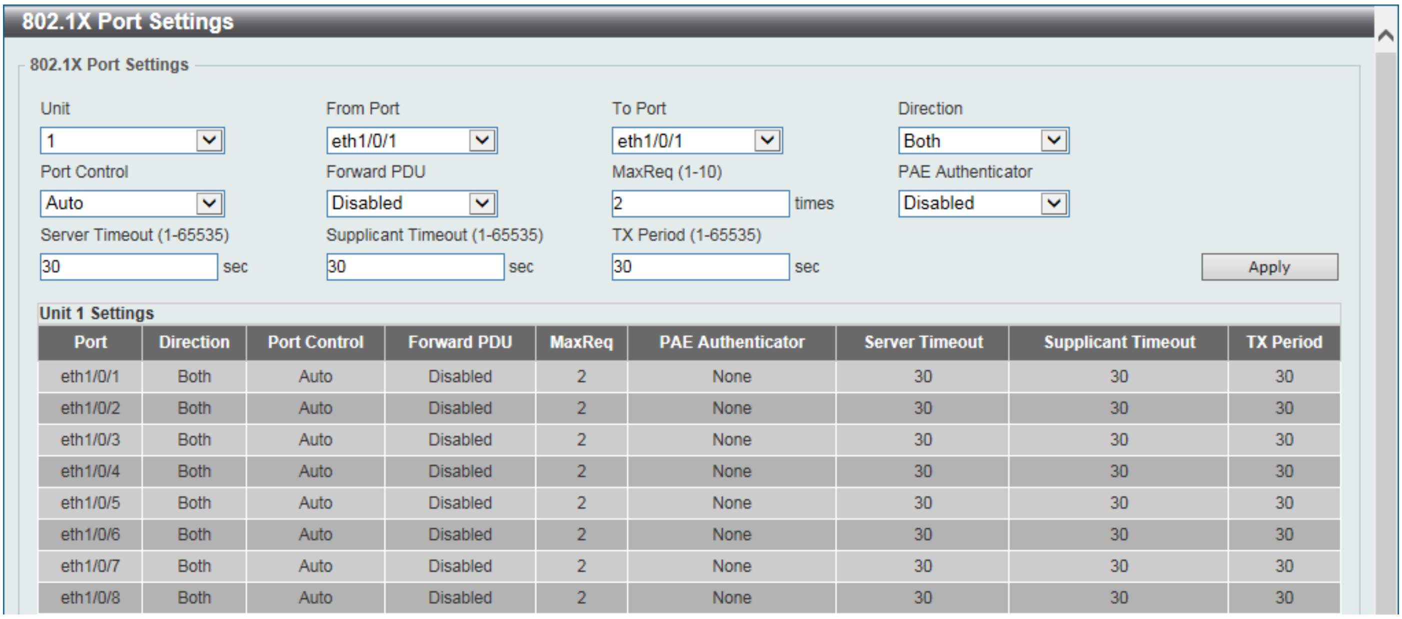
Parameter	Description
802.1X State	Select to enable or disable the global 802.1X state here.
802.1X Trap State	Select to enable or disable the 802.1X trap state here.

Click the **Apply** button to accept the changes made.

802.1X Port Settings

This window is used to display and configure the 802.1X port settings.

To view the following window, click **Security > 802.1X > 802.1X Port Settings**, as shown below:



802.1X Port Settings

802.1X Port Settings

Unit	From Port	To Port	Direction
1	eth1/0/1	eth1/0/1	Both
Port Control	Forward PDU	MaxReq (1-10)	PAE Authenticator
Auto	Disabled	2 times	Disabled
Server Timeout (1-65535)	Supplicant Timeout (1-65535)	TX Period (1-65535)	
30 sec	30 sec	30 sec	Apply

Unit 1 Settings

Port	Direction	Port Control	Forward PDU	MaxReq	PAE Authenticator	Server Timeout	Supplicant Timeout	TX Period
eth1/0/1	Both	Auto	Disabled	2	None	30	30	30
eth1/0/2	Both	Auto	Disabled	2	None	30	30	30
eth1/0/3	Both	Auto	Disabled	2	None	30	30	30
eth1/0/4	Both	Auto	Disabled	2	None	30	30	30
eth1/0/5	Both	Auto	Disabled	2	None	30	30	30
eth1/0/6	Both	Auto	Disabled	2	None	30	30	30
eth1/0/7	Both	Auto	Disabled	2	None	30	30	30
eth1/0/8	Both	Auto	Disabled	2	None	30	30	30

Figure 9-13 802.1X Port Settings Window

The fields that can be configured are described below:

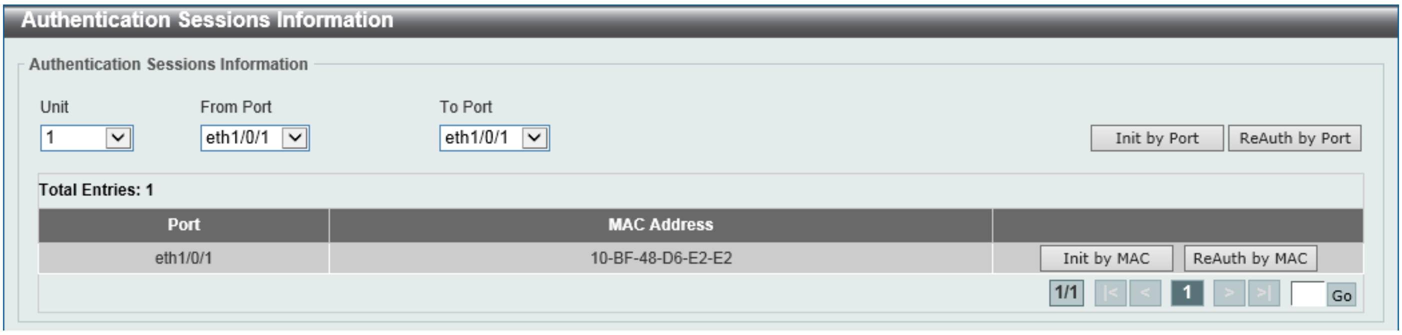
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
Direction	Select the direction here. Options to choose from are **Both** and **In**. This option configures the direction 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. The range is from 1 to 10. By default, this value is 2. This option configures the maximum number of times that the backend authentication state machine will retransmit an Extensible Authentication Protocol (EAP) request frame to the supplicant before restarting the authentication process.
PAE Authenticator	Select to enable or disable the PAE authenticator option here. This option configures a specific port as an IEEE 802.1X port access entity (PAE) authenticator.
Server Timeout	Enter the server timeout value here. The range is from 1 to 65535 seconds. By default, this value is 30 seconds.
Supplicant Timeout	Enter the supplicant timeout value here. The range is from 1 to 65535 seconds. By default, this value is 30 seconds.
TX Period	Enter the transmission period value here. The range is from 1 to 65535 seconds. By default, this value is 30 seconds.

Click the **Apply** button to accept the changes made.

Authentication Sessions Information

This window is used to display and configure the authentication session information.

To view the following window, click **Security > 802.1X > Authentication Sessions Information**, as shown below:



Authentication Sessions Information

Authentication Sessions Information

Unit: 1

From Port: eth1/0/1

To Port: eth1/0/1

Total Entries: 1

Port	MAC Address	
eth1/0/1	10-BF-48-D6-E2-E2	Init by MAC ReAuth by MAC

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.
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.

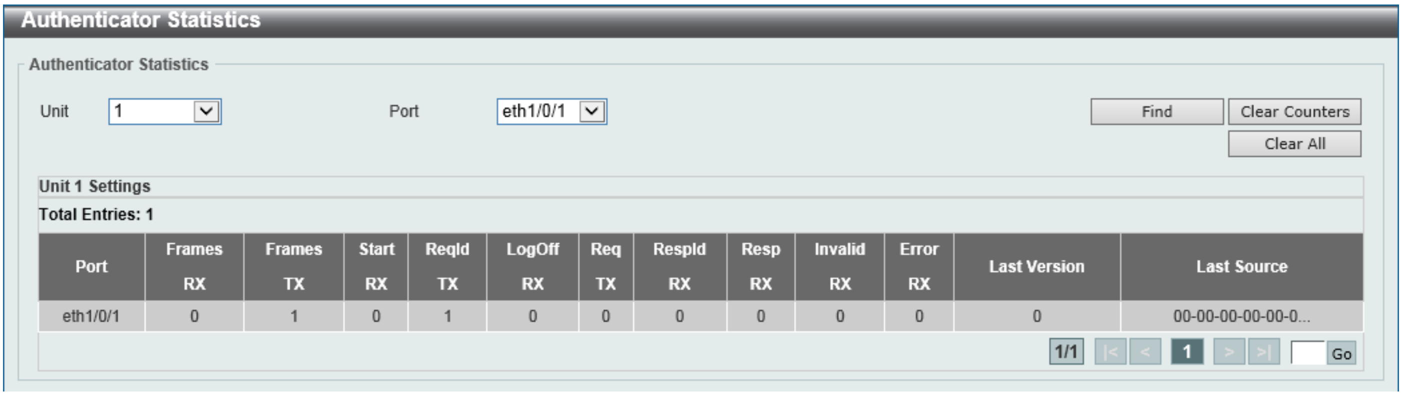
Click the **ReAuth by MAC** button to re-authenticate the session information based on the MAC address.

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:



Authenticator Statistics

Authenticator Statistics

Unit: 1

Port: eth1/0/1

Unit 1 Settings

Total Entries: 1

Port	Frames RX	Frames TX	Start RX	ReqId TX	LogOff RX	Req TX	RespId RX	Resp RX	Invalid RX	Error RX	Last Version	Last Source
eth1/0/1	0	1	0	1	0	0	0	0	0	0	0	00-00-00-00-00-0...

Figure 9-15 Authenticator Statistics Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this query here.
Port	Select the appropriate port used for the query here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear Counters** button to clear the counter information based on the selections made.

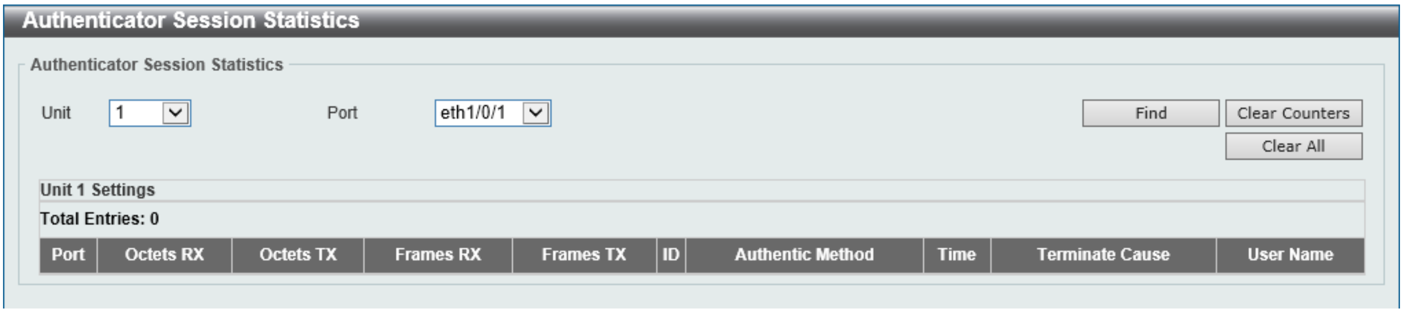
Click the **Clear All** button to clear all the information in this table.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Authenticator Session Statistics

This window is used to view and clear the authenticator session statistics.

To view the following window, click **Security > 802.1X > Authenticator Session Statistics**, as shown below:


Authenticator Session Statistics
Authenticator Session Statistics
Find
Clear Counters
Clear All

Unit 1 Port eth1/0/1

Unit 1 Settings

Total Entries: 0

Port	Octets RX	Octets TX	Frames RX	Frames TX	ID	Authentic Method	Time	Terminate Cause	User Name

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.
Port	Select the appropriate port used for the query here.

Click the **Find** button to locate a specific entry based on the information entered.

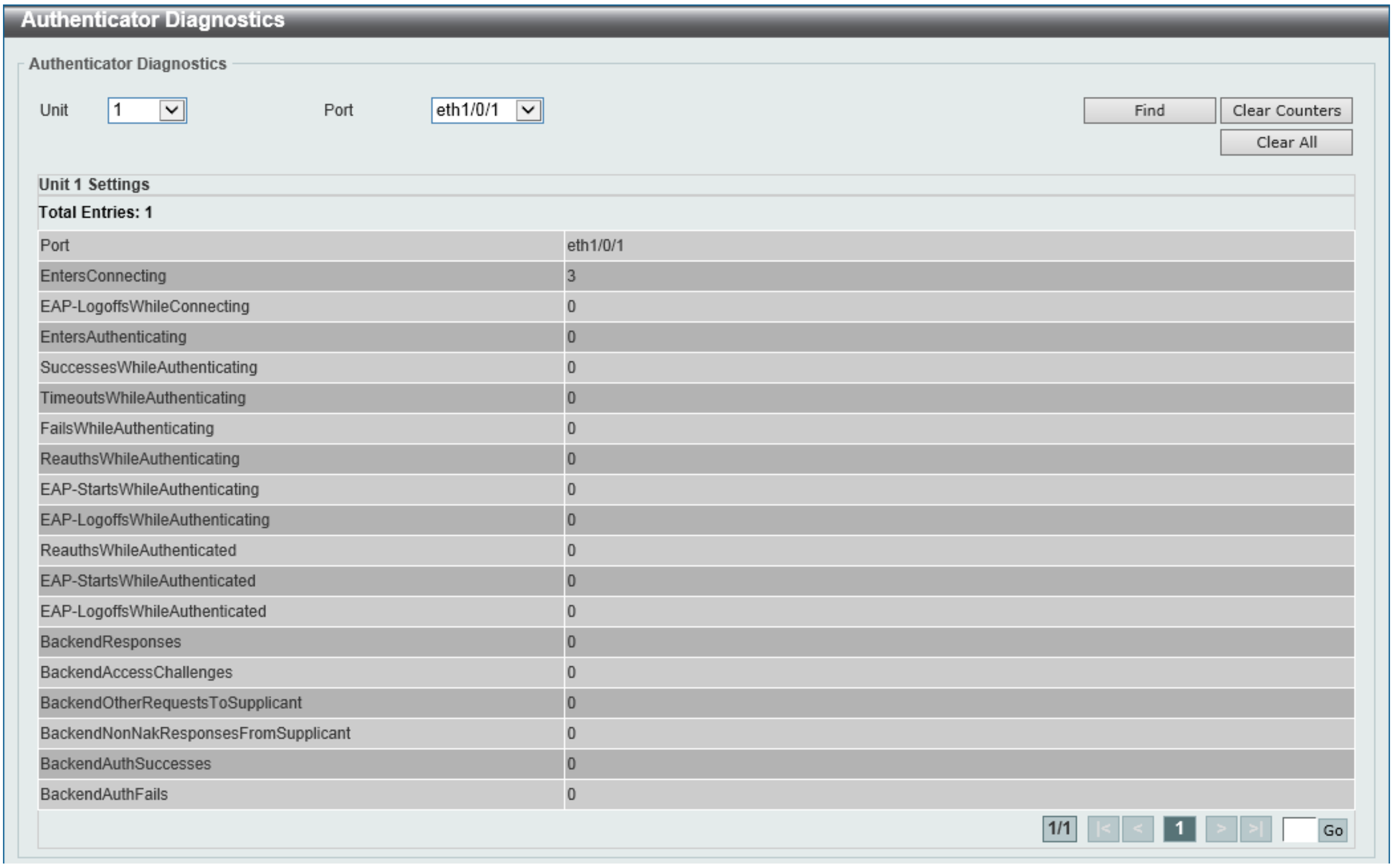
Click the **Clear Counters** button to clear the counter information based on the selections made.

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:



Unit: 1
Port: eth1/0/1

Unit 1 Settings

Total Entries: 1

Port	eth1/0/1
EntersConnecting	3
EAP-LogoffsWhileConnecting	0
EntersAuthenticating	0
SuccessesWhileAuthenticating	0
TimeoutsWhileAuthenticating	0
FailsWhileAuthenticating	0
ReauthsWhileAuthenticating	0
EAP-StartsWhileAuthenticating	0
EAP-LogoffsWhileAuthenticating	0
ReauthsWhileAuthenticated	0
EAP-StartsWhileAuthenticated	0
EAP-LogoffsWhileAuthenticated	0
BackendResponses	0
BackendAccessChallenges	0
BackendOtherRequestsToSupplicant	0
BackendNonNakResponsesFromSupplicant	0
BackendAuthSuccesses	0
BackendAuthFails	0

Figure 9-17 Authenticator Diagnostics Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this query here.
Port	Select the appropriate port used for the query here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear Counters** button to clear the counter information based on the selections made.

Click the **Clear All** button to clear all the information in this table.

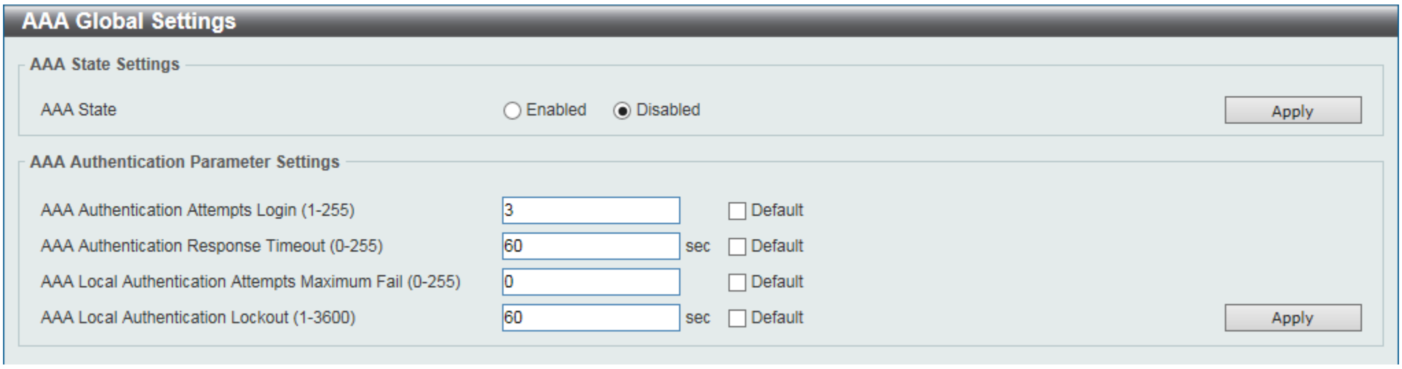
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

AAA

AAA Global Settings

This window is used to enable or disable the global Authentication, Authorization, and Accounting (AAA) state.

To view the following window, click **Security > AAA > AAA Global Settings**, as shown below:


AAA Global Settings

AAA State Settings

AAA State ○ Enabled ● Disabled

AAA Authentication Parameter Settings

AAA Authentication Attempts Login (1-255)	3		□ Default
AAA Authentication Response Timeout (0-255)	60	sec	□ Default
AAA Local Authentication Attempts Maximum Fail (0-255)	0		□ Default
AAA Local Authentication Lockout (1-3600)	60	sec	□ Default

Figure 9-18 AAA Global Settings Window

The fields that can be configured in **AAA State Settings** 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.

The fields that can be configured in **AAA Authentication Parameter Settings** are described below:

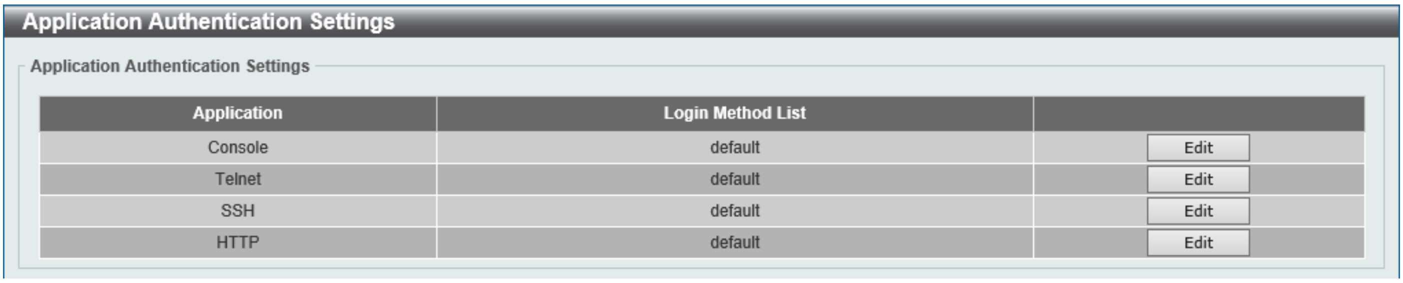
Parameter	Description
AAA Authentication Attempts Login	Enter the number of allowed AAA authentication login attempts here. The range is from 1 to 255. By default, this value is 3. Select the **Default** option to use the default value.
AAA Authentication Response Timeout	Enter the AAA authentication response timeout value here. The range is from 0 to 255 seconds. By default, this value is 60 seconds. Select the **Default** option to use the default value.
AAA Local Authentication Attempts Maximum Fail	Enter the maximum amount of times local AAA authentication attempts are allowed to fail here. If this value is 0, this feature is disabled. The range is from 0 to 255. By default, this value is 0. Select the **Default** option to use the default value.
AAA Local Authentication Lockout	Enter the local AAA authentication lockout time here. The range is from 1 to 3600 seconds. By default, this is 60 seconds. Select the **Default** option to use the default value.

Click the **Apply** button to accept the changes made.

Application Authentication Settings

This window is used to display and configure the application authentication settings.

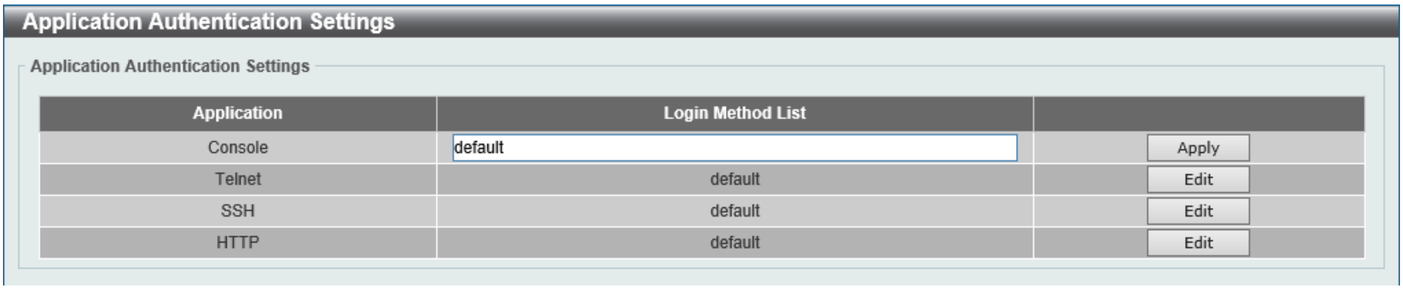
To view the following window, click **Security > AAA > Application Authentication Settings**, as shown below:


Application Authentication Settings
Application Authentication Settings
Edit
Edit
Edit
Edit

Application	Login Method List	
Console	default	Edit
Telnet	default	Edit
SSH	default	Edit
HTTP	default	Edit

Figure 9-19 Application Authentication Settings Window

Click the **Edit** button to re-configure the specific entry.


Application Authentication Settings
Application Authentication Settings
Apply
Edit
Edit
Edit

Application	Login Method List	
Console	default	Apply
Telnet	default	Edit
SSH	default	Edit
HTTP	default	Edit

Figure 9-20 Application Authentication Settings (Edit) Window

The fields that can be configured are described below:

Parameter	Description
Login Method List	After clicking the **Edit** button for the specific entry, enter the login method list name used here.

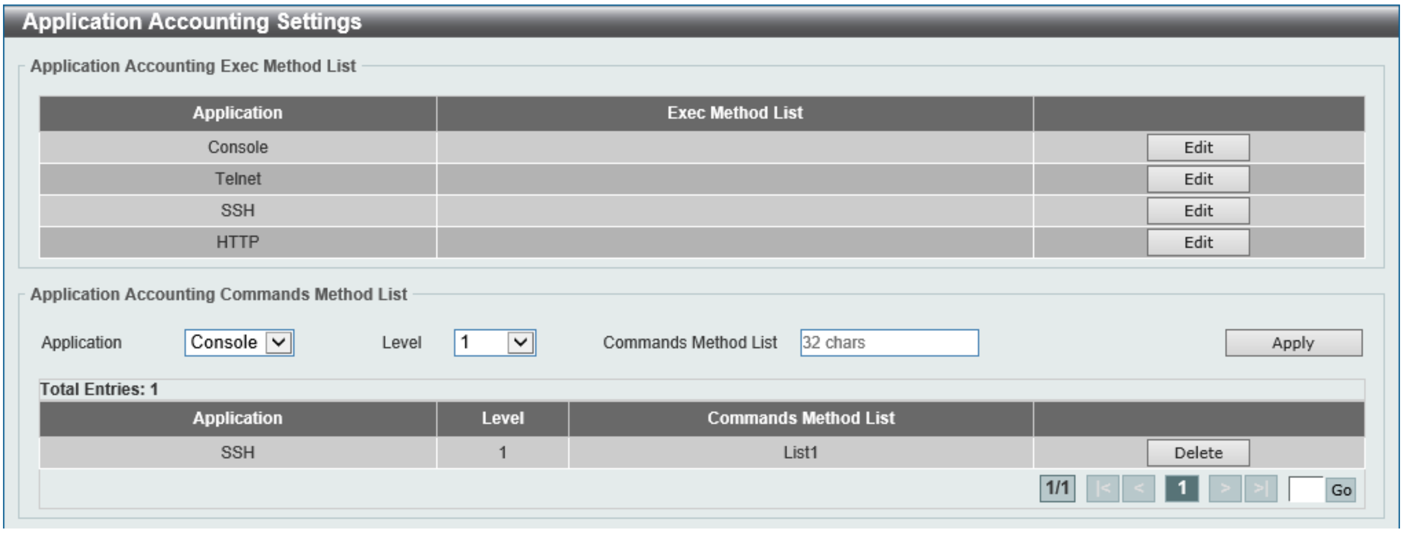
Click the **Edit** button to re-configure the specific entry.

Click the **Apply** button to accept the changes made.

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:



Application Accounting Settings

Application Accounting Exec Method List

Application	Exec Method List	
Console		Edit
Telnet		Edit
SSH		Edit
HTTP		Edit

Application Accounting Commands Method List

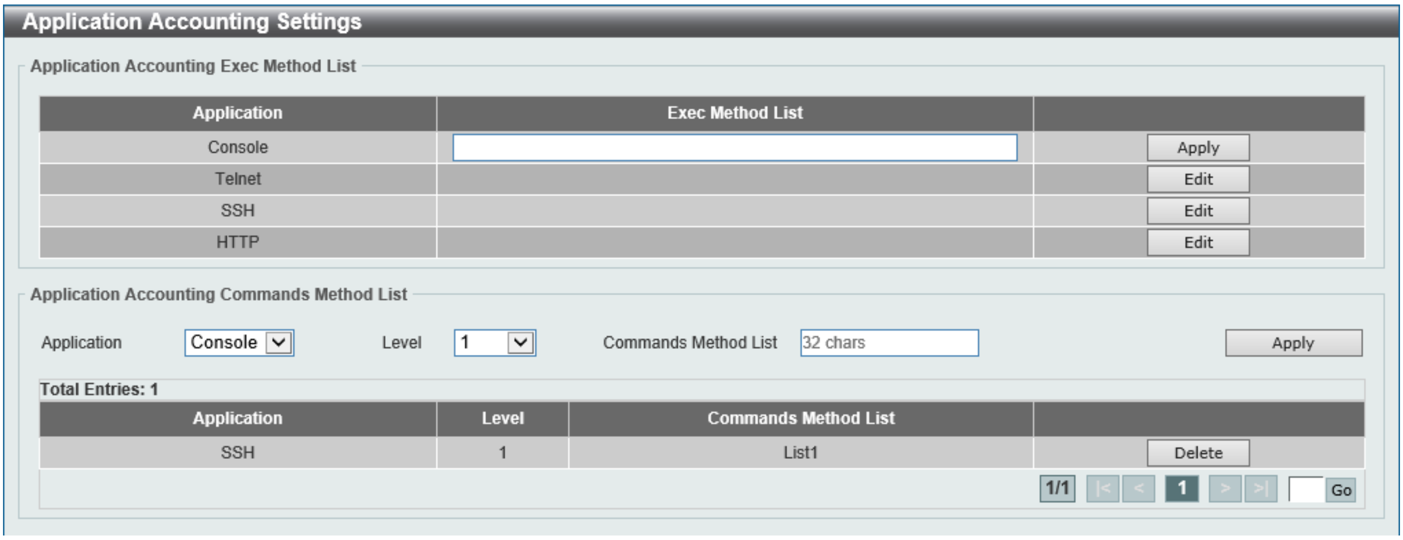
Application: Console Level: 1 Commands Method List: 32 chars

Total Entries: 1

Application	Level	Commands Method List	
SSH	1	List1	Delete

Figure 9-21 Application Accounting Settings Window

Click the **Edit** button to re-configure the specific entry.



Application Accounting Settings

Application Accounting Exec Method List

Application	Exec Method List	
Console		Apply
Telnet		Edit
SSH		Edit
HTTP		Edit

Application Accounting Commands Method List

Application: Console Level: 1 Commands Method List: 32 chars

Total Entries: 1

Application	Level	Commands Method List	
SSH	1	List1	Delete

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.

Parameter	Description
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.

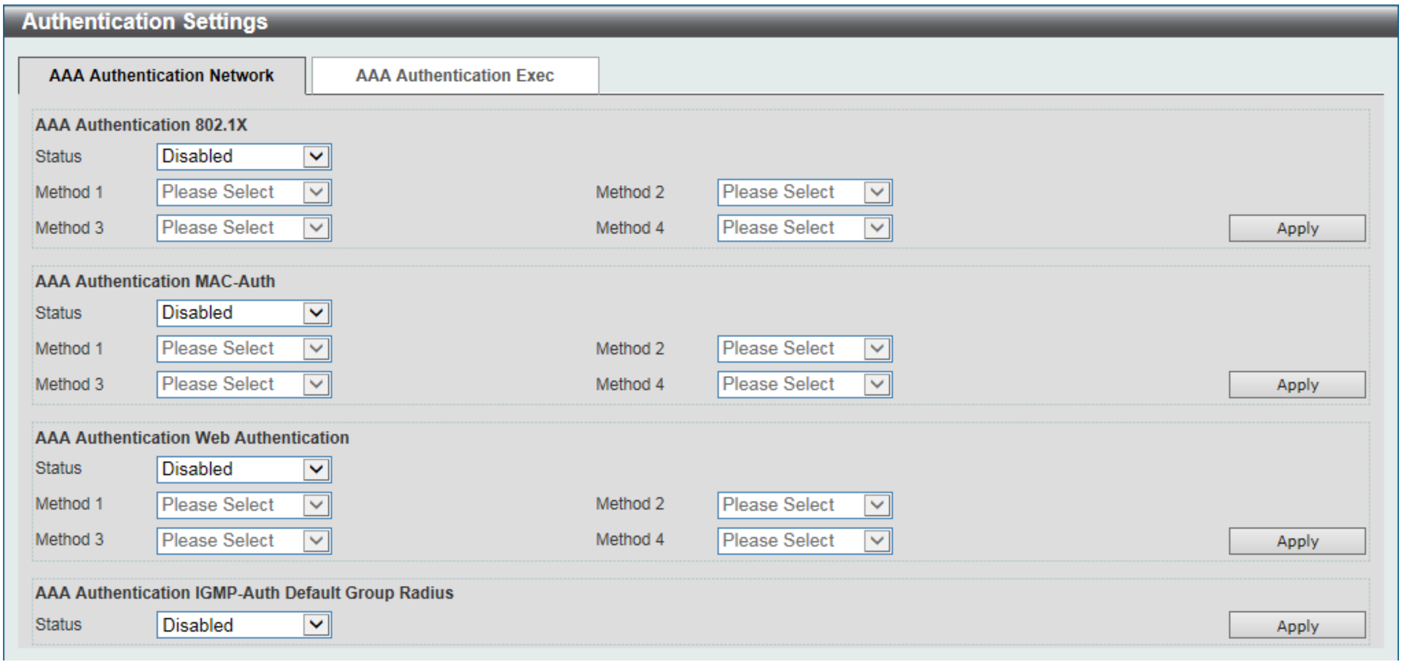
Click the **Delete** button to remove the specified entry.

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** and select the **AAA Authentication Network** tab, as shown below:



Authentication Settings

AAA Authentication 802.1X

Status: Disabled

Method 1: Please Select   Method 2: Please Select

Method 3: Please Select   Method 4: Please Select

AAA Authentication MAC-Auth

Status: Disabled

Method 1: Please Select   Method 2: Please Select

Method 3: Please Select   Method 4: Please Select

AAA Authentication Web Authentication

Status: Disabled

Method 1: Please Select   Method 2: Please Select

Method 3: Please Select   Method 4: Please Select

AAA Authentication IGMP-Auth Default Group Radius

Status: Disabled

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. • **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 Authentication** 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.

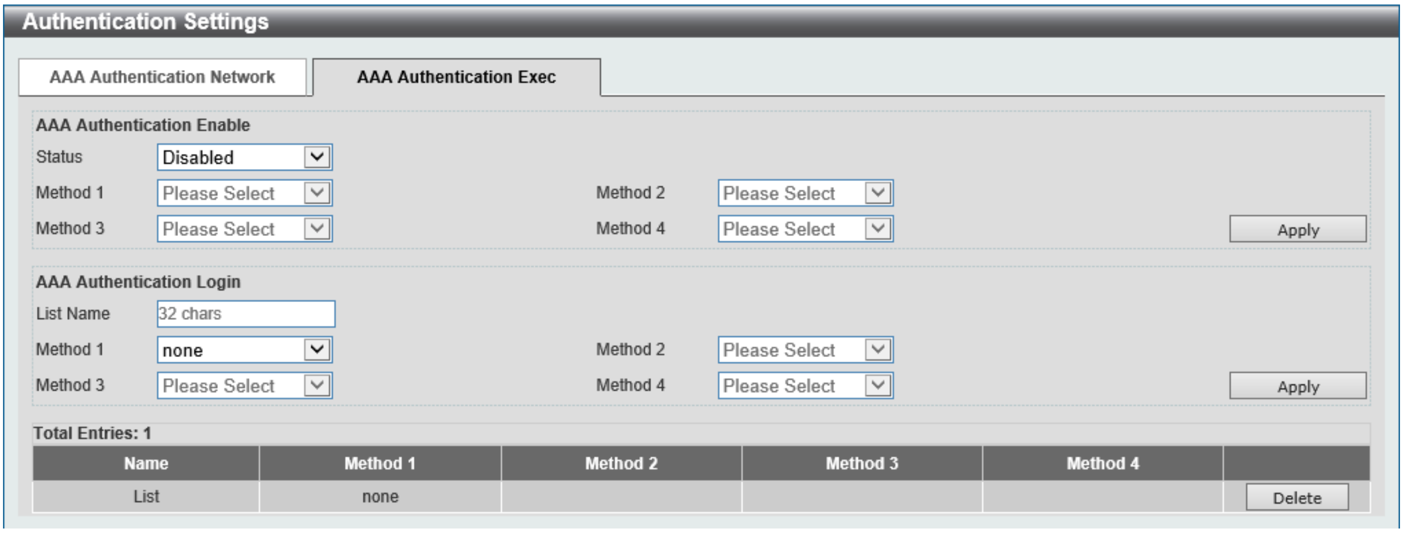
Click the **Apply** button to accept the changes made.

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 default method list for IGMP authentication here.

Click the **Apply** button to accept the changes made.

To view the following window, select the **AAA Authentication Exec** tab, as shown below:



Status: Disabled
Method 1: Please Select
Method 2: Please Select
Method 3: Please Select
Method 4: Please Select

List Name: 32 chars
Method 1: none
Method 2: Please Select
Method 3: Please Select
Method 4: Please Select

Total Entries: 1

Name	Method 1	Method 2	Method 3	Method 4	
List	none				Delete

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.

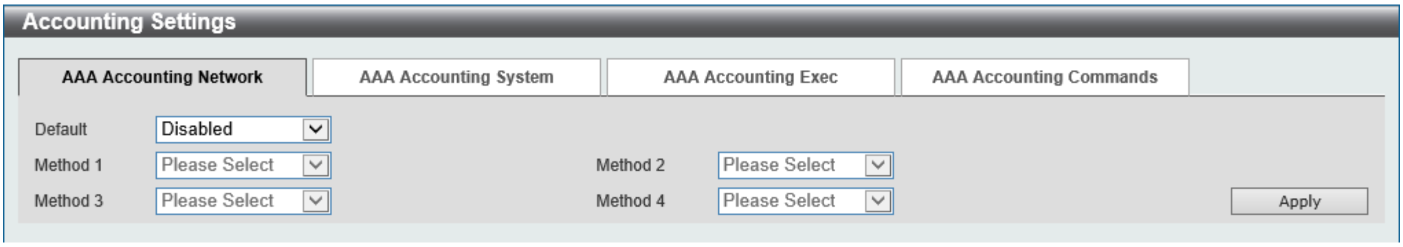
Click the **Apply** button to accept the changes made.

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** and select the **AAA Accounting Network** tab, as shown below:



Default: Disabled
Method 1: Please Select
Method 2: Please Select
Method 3: Please Select
Method 4: Please Select

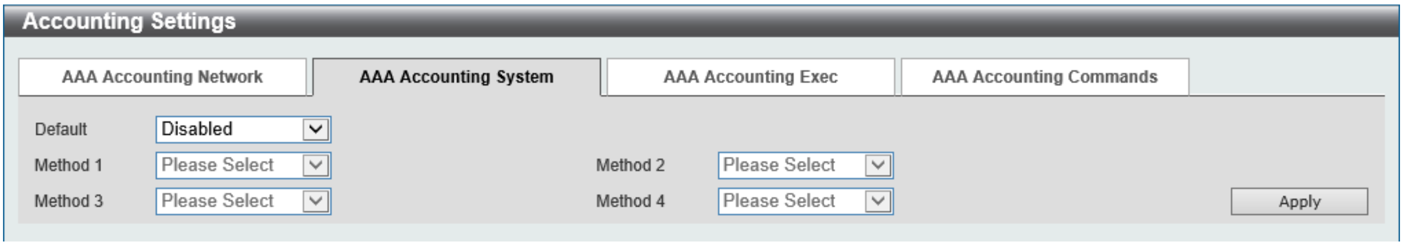
Figure 9-25 Accounting Settings Window

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+**. **None** is only available for **Method 1**.

Click the **Apply** button to accept the changes made.

To view the following window, select the **AAA Accounting System** tab, as shown below:



Default: Disabled
Method 1: Please Select
Method 2: Please Select
Method 3: Please Select
Method 4: Please Select

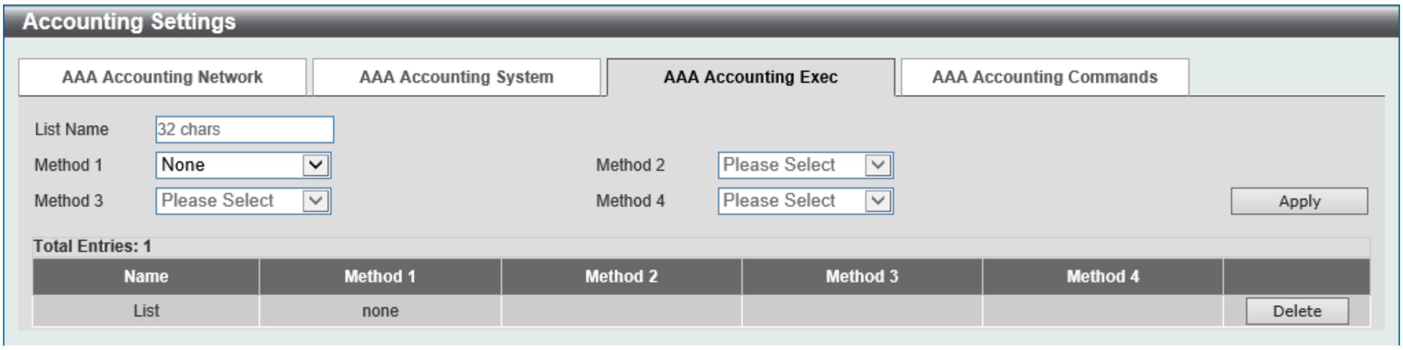
Figure 9-26 Accounting Settings (AAA Accounting System) Window

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+**. **None** is only available for **Method 1**.

Click the **Apply** button to accept the changes made.

To view the following window, select the **AAA Accounting Exec** tab, as shown below:



Accounting Settings

List Name: 32 chars

Method 1: None

Method 2: Please Select

Method 3: Please Select

Method 4: Please Select

Total Entries: 1

Name	Method 1	Method 2	Method 3	Method 4	
List	none				Delete

Figure 9-27 Accounting Settings (AAA Accounting Exec) Window

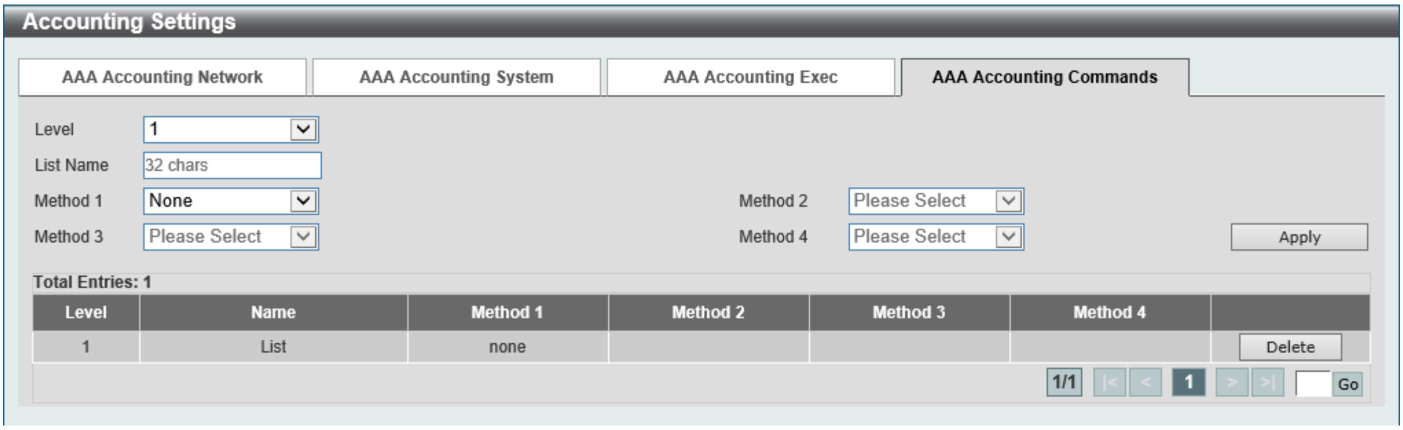
The fields that can be configured in **AAA Accounting Exec** are described below:

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+**. **None** is only available for **Method 1**.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

To view the following window, select the **AAA Accounting Commands** tab, as shown below:



Accounting Settings

Level: 1

List Name: 32 chars

Method 1: None

Method 2: Please Select

Method 3: Please Select

Method 4: Please Select

Total Entries: 1

Level	Name	Method 1	Method 2	Method 3	Method 4	
1	List	none				Delete

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+**. **None** is only available for **Method 1**.

Click the **Apply** button to accept the changes made.

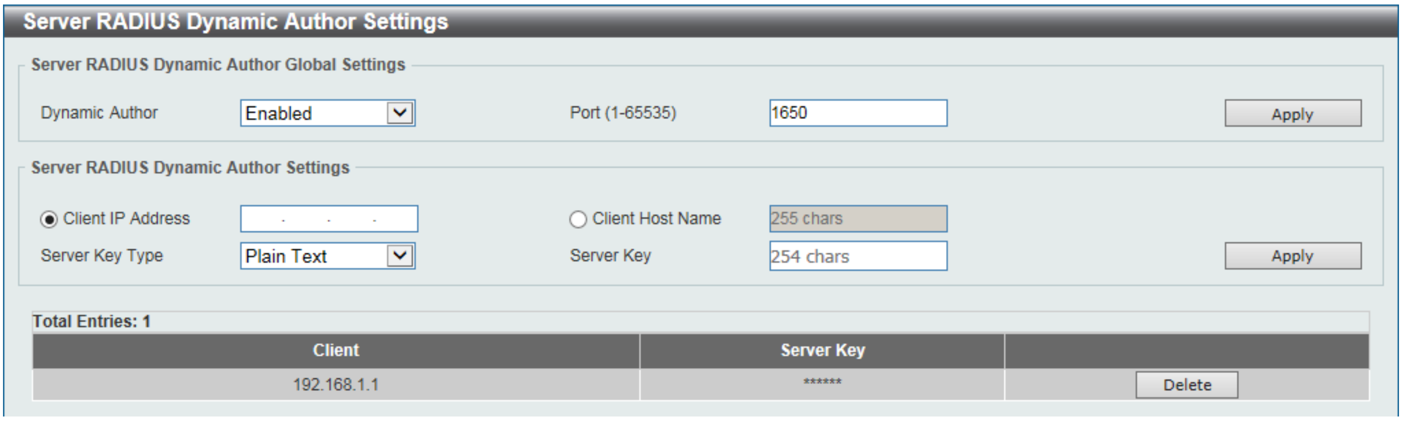
Click the **Delete** button to remove the specified entry.

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 Switch as an AAA server to facilitate the inter-action with an external policy server.

To view the following window, click **Security > AAA > Server RADIUS Dynamic Author Settings**, as shown below:



Server RADIUS Dynamic Author Settings

Server RADIUS Dynamic Author Global Settings

Dynamic Author: Enabled
Port (1-65535): 1650

Server RADIUS Dynamic Author Settings

● Client IP Address: . . .
○ Client Host Name: 255 chars
Server Key Type: Plain Text
Server Key: 254 chars

Total Entries: 1

Client	Server Key	
192.168.1.1	******	Delete

Figure 9-29 Server RADIUS Dynamic Author Settings Window

The fields that can be configured in **Server RADIUS Dynamic Author Global Settings** are described below:

Parameter	Description
Dynamic Author	Select to enable or disable the dynamic authorization.
Port	Enter the port number for the Switch to listen to RADIUS requests from the RADIUS client.

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	Select and enter the client IP address here.
Client Host Name	Select and enter the client host name here.
Server Key Type	Select the key type that will be used here. Options to choose from are **Plain Text** and **Encrypted**.
Server Key	Enter the key, used to communicate with the RADIUS server, here. This key can be up to 254 characters long.

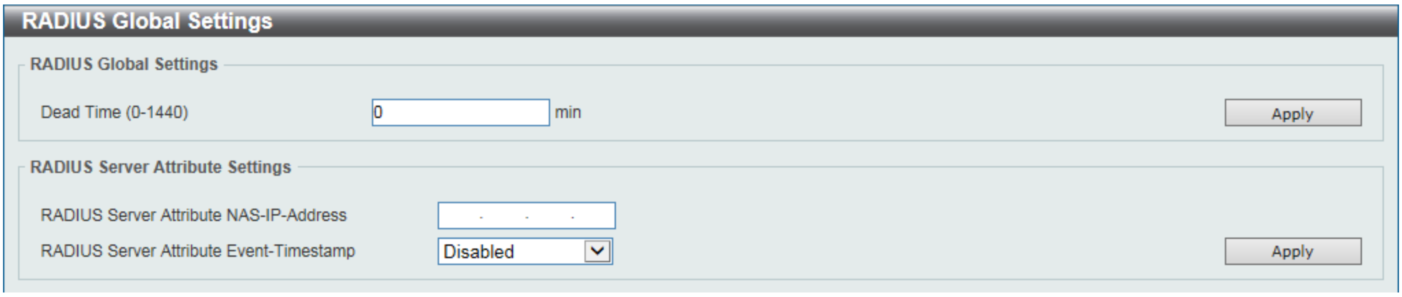
Click the **Apply** button to accept the changes made.

RADIUS

RADIUS Global Settings

This window is used to display and configure the global RADIUS settings.

To view the following window, click **Security > RADIUS > RADIUS Global Settings**, as shown below:



RADIUS Global Settings

RADIUS Global Settings

Dead Time (0-1440): 0 min

RADIUS Server Attribute Settings

RADIUS Server Attribute NAS-IP-Address: . . .

RADIUS Server Attribute Event-Timestamp: Disabled

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. The range is from 1 to 1440 minutes. By default, this value is 0 minutes. When this option is 0, the unresponsive server will not be marked as dead. This setting can be used to improve the authentication processing time by setting the dead time to skip the unresponsive server host entries. 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 Server Attribute Settings** are described below:

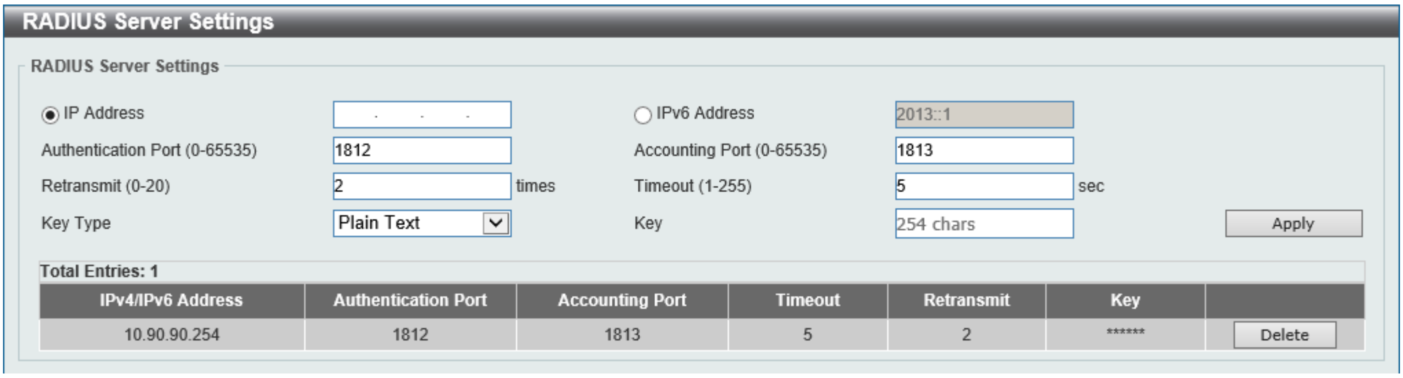
Parameter	Description
RADIUS Server Attribute NAS-IP-Address	Enter the IPv4 address of the RADIUS server attribute 4 in the RADIUS packet here.
RADIUS Server Attribute Event-Timestamp	Select to enable or disable the RADIUS server attribute event-timestamp function here.

Click the **Apply** button to accept the changes made.

RADIUS Server Settings

This window is used to display and configure the RADIUS server settings.

To view the following window, click **Security > RADIUS > RADIUS Server Settings**, as shown below:



RADIUS Server Settings

RADIUS Server Settings

● IP Address: . . .

○ IPv6 Address: 2013::1

Authentication Port (0-65535): 1812

Accounting Port (0-65535): 1813

Retransmit (0-20): 2 times

Timeout (1-255): 5 sec

Key Type: Plain Text

Key: 254 chars

Total Entries: 1

IPv4/IPv6 Address	Authentication Port	Accounting Port	Timeout	Retransmit	Key	
10.90.90.254	1812	1813	5	2	******	Delete

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. The range is from 0 to 65535. By default, this value is 1812. If no authentication is used, use the value 0.
Accounting Port	Enter the accounting port number used here. The range is from 0 to 65535. By default, this value is 1813. If no accounting is used, use the value 0.
Retransmit	Enter the retransmit value used here. The range is from 0 to 20. By default, this value is 2. To disable this option, enter the value 0.
Timeout	Enter the timeout value used here. The range is from 1 to 255 seconds. By default, this value is 5 seconds.
Key Type	Select the key type that will be used here. Options to choose from are **Plain Text** and **Encrypted**.
Key	Enter the key, used to communicate with the RADIUS server, here. This key can be up to 254 characters long.

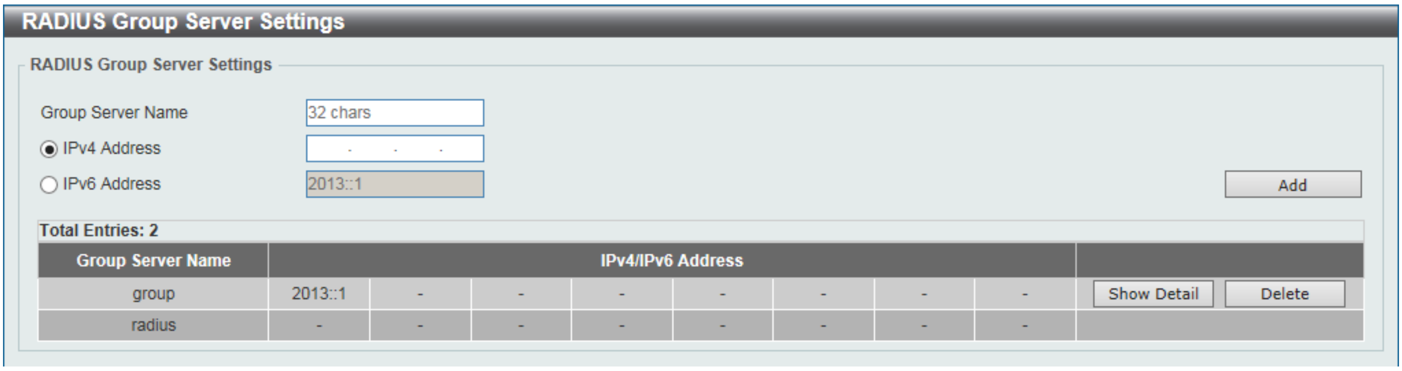
Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

RADIUS Group Server Settings

This window is used to display and configure the RADIUS group server settings.

To view the following window, click **Security > RADIUS > RADIUS Group Server Settings**, as shown below:



RADIUS Group Server Settings

RADIUS Group Server Settings

Group Server Name: 32 chars

● IPv4 Address: . . .

○ IPv6 Address: 2013::1

Total Entries: 2

Group Server Name	IPv4/IPv6 Address								
group	2013::1	-	-	-	-	-	-	-	Show Detail Delete
radius	-	-	-	-	-	-	-	-	

Figure 9-32 RADIUS Group Server Settings Window

The fields that can be configured are described below:

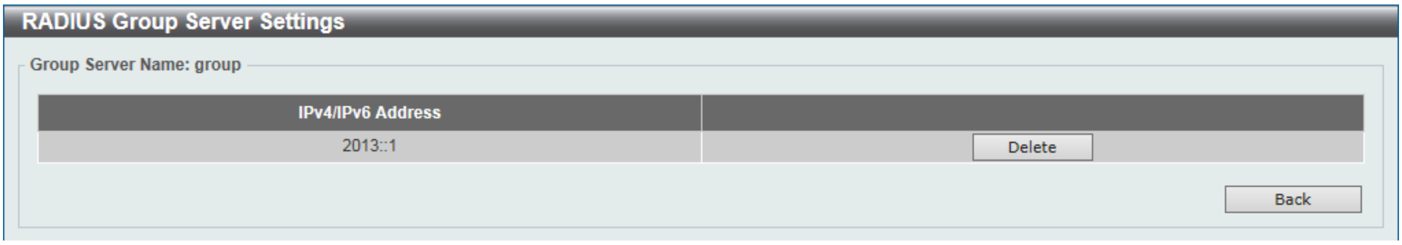
Parameter	Description
Group Server Name	Enter the RADIUS group server name here. This name can be up to 32 characters long.
IPv4 Address	Enter the group server IPv4 address here.
IPv6 Address	Enter the group server IPv6 address here.

Click the **Add** button to add a new entry based on the information entered.

Click the **Show Detail** button to view and configure detailed settings for the RADIUS group server.

Click the **Delete** button to remove the specified entry.

After clicking the **Show Detail** button, the following page will be available.



RADIUS Group Server Settings

Group Server Name: group

IPv4/IPv6 Address	
2013::1	Delete

Figure 9-33 RADIUS Group Server Settings (Detail) Window

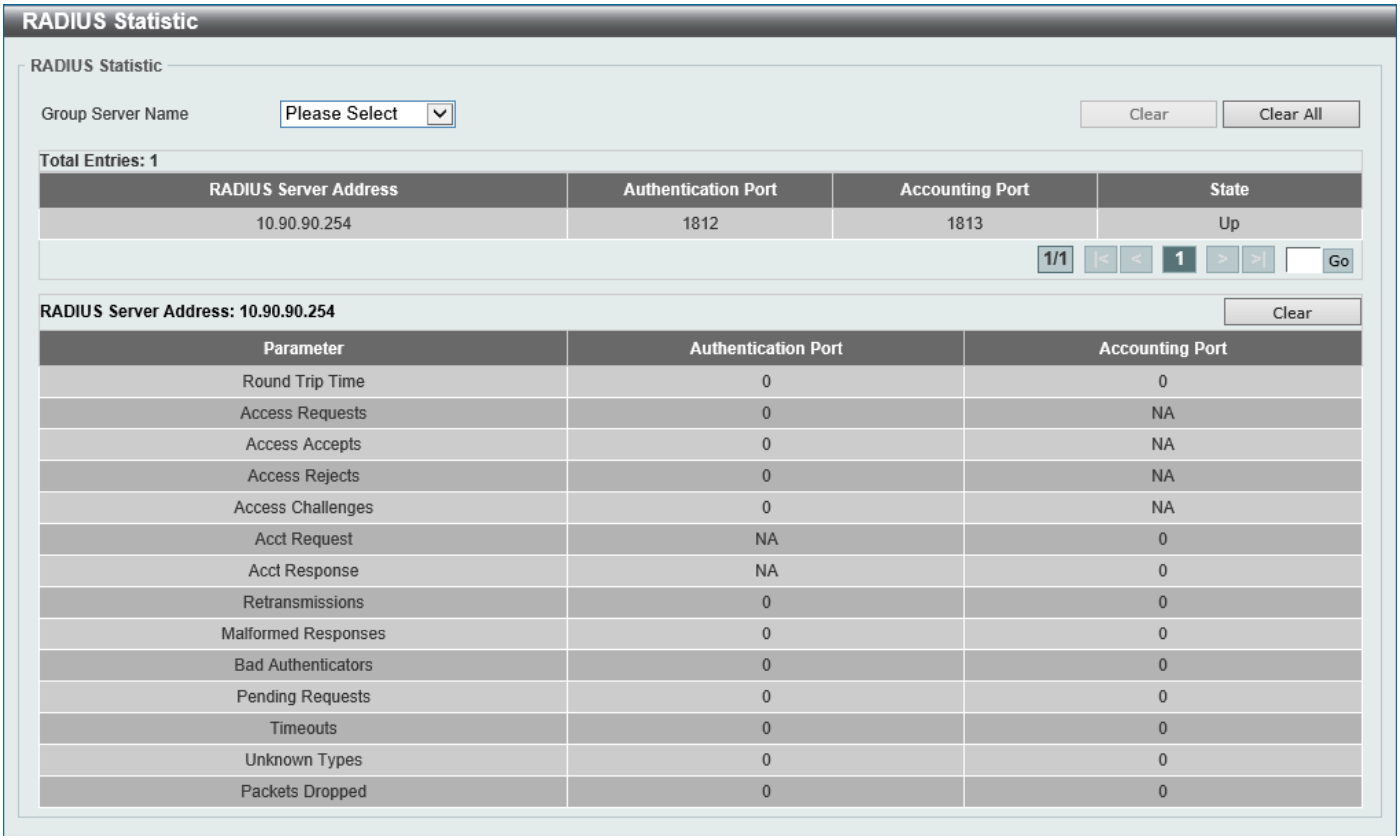
Click the **Delete** button to remove the specified entry.

Click the **Back** button to return to the previous window.

RADIUS Statistic

This window is used to view and clear the RADIUS statistics information.

To view the following window, click **Security > RADIUS > RADIUS Statistic**, as shown below:



Total Entries: 1

RADIUS Server Address	Authentication Port	Accounting Port	State
10.90.90.254	1812	1813	Up

RADIUS Server Address: 10.90.90.254

Parameter	Authentication Port	Accounting Port
Round Trip Time	0	0
Access Requests	0	NA
Access Accepts	0	NA
Access Rejects	0	NA
Access Challenges	0	NA
Acct Request	NA	0
Acct Response	NA	0
Retransmissions	0	0
Malformed Responses	0	0
Bad Authenticators	0	0
Pending Requests	0	0
Timeouts	0	0
Unknown Types	0	0
Packets Dropped	0	0

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.

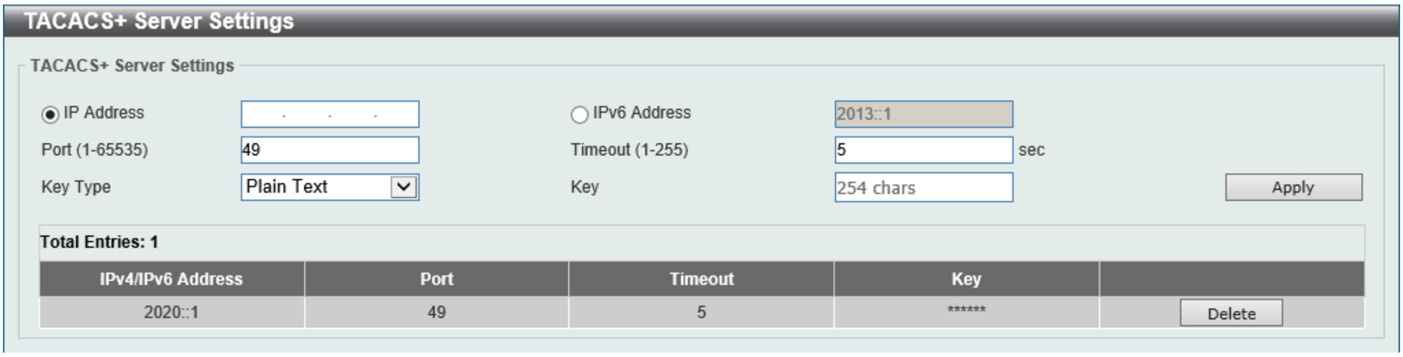
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

TACACS+

TACACS+ Server Settings

This window is used to display and configure the TACACS+ server settings.

To view the following window, click **Security > TACACS+ > TACACS+ Server Settings**, as shown below:



TACACS+ Server Settings

TACACS+ Server Settings

● IP Address: . . .
○ IPv6 Address: 2013::1
Port (1-65535): 49
Timeout (1-255): 5 sec
Key Type: Plain Text
Key: 254 chars

Total Entries: 1

IPv4/IPv6 Address	Port	Timeout	Key	
2020::1	49	5	******	Delete

Figure 9-35 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. The range is from 1 to 65535. By default, this value is 49.
Timeout	Enter the timeout value here. The range is from 1 to 255 seconds. By default, this value is 5 seconds.
Key Type	Select the key type that will be used here. Options to choose from are **Plain Text** and **Encrypted**.
Key	Enter the key, used to communicate with the TACACS+ server, here. This key can be up to 254 characters long.

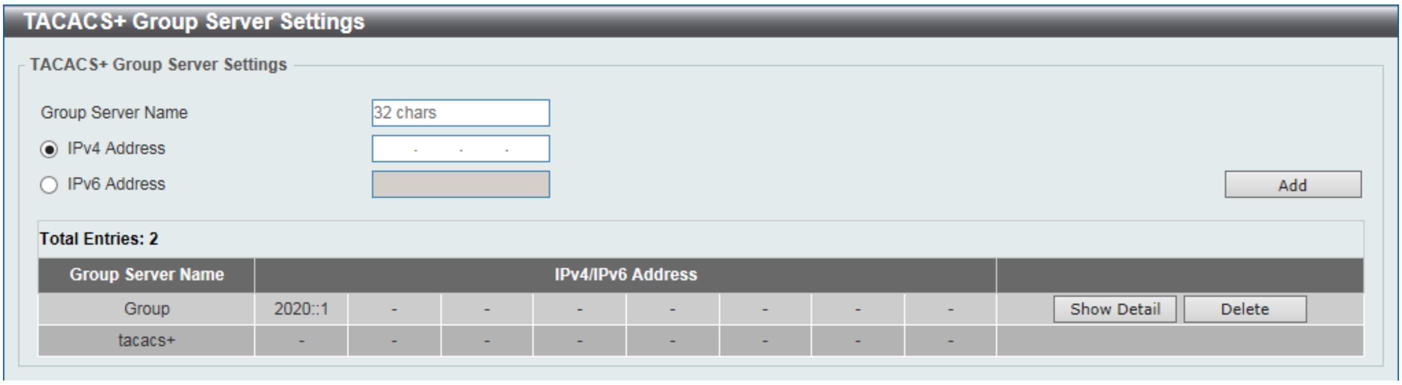
Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

TACACS+ Group Server Settings

This window is used to display and configure the TACACS+ group server settings.

To view the following window, click **Security > TACACS+ > TACACS+ Group Server Settings**, as shown below:



TACACS+ Group Server Settings

TACACS+ Group Server Settings

Group Server Name: 32 chars

● IPv4 Address: . . .

○ IPv6 Address

Total Entries: 2

Group Server Name	IPv4/IPv6 Address								
Group	2020::1	-	-	-	-	-	-	-	Show Detail Delete
tacacs+	-	-	-	-	-	-	-	-	

Figure 9-36 TACACS+ Group Server Settings Window

The fields that can be configured are described below:

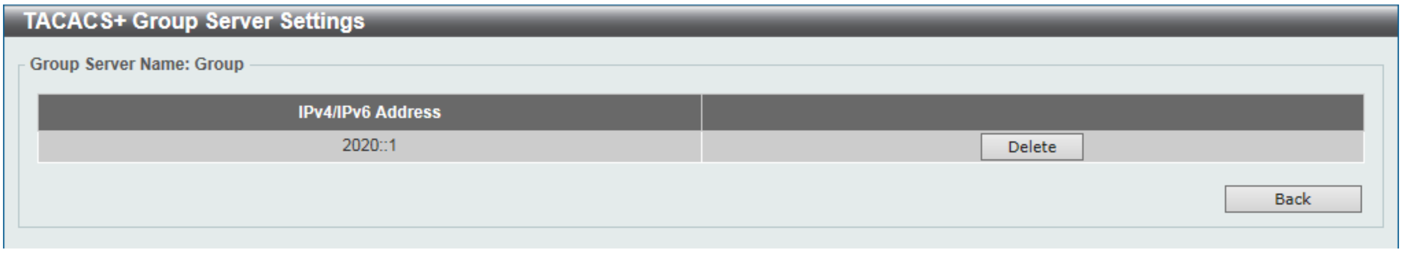
Parameter	Description
Group Server Name	Enter the TACACS+ group server name here. This name can be up to 32 characters long.
IPv4 Address	Enter the IPv4 address of the TACACS+ group server here.
IPv6 Address	Enter the IPv6 address of the TACACS+ group server here.

Click the **Add** button to add a new entry based on the information entered.

Click the **Show Detail** button to view and configure detailed settings for the TACACS+ group server.

Click the **Delete** button to remove the specified entry.

After clicking the **Show Detail** button, the following page will be available.



TACACS+ Group Server Settings

Group Server Name: Group

IPv4/IPv6 Address	
2020::1	Delete

Figure 9-37 TACACS+ Group Server Settings (Show Detail) Window

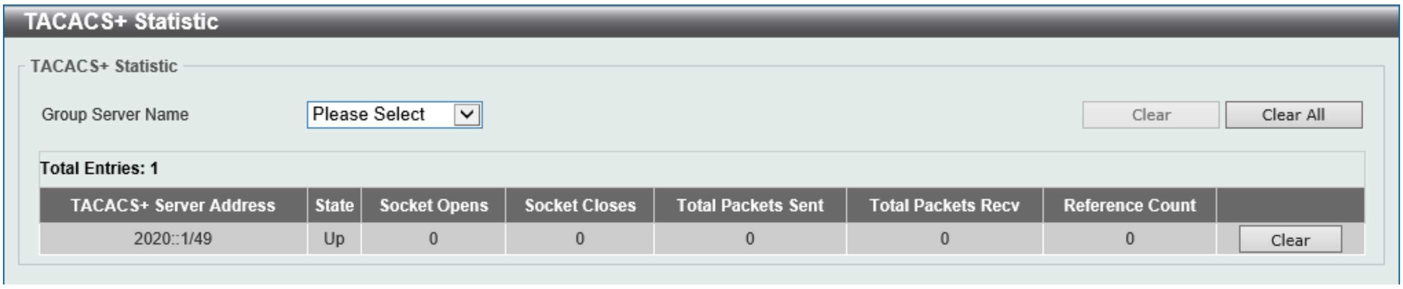
Click the **Delete** button to remove the specified entry.

Click the **Back** button to return to the previous window.

TACACS+ Statistic

This window is used to view and clear the TACACS+ statistic information.

To view the following window, click **Security > TACACS+ > TACACS+ Statistic**, as shown below:



Group Server Name: Please Select

Total Entries: 1

TACACS+ Server Address	State	Socket Opens	Socket Closes	Total Packets Sent	Total Packets Recv	Reference Count	
2020::1/49	Up	0	0	0	0	0	Clear

Figure 9-38 TACACS+ Statistic Window

The fields that can be configured are described below:

Parameter	Description
Group Server Name	Select the TACACS+ group server name from this list here.

Click the first **Clear** button to clear the information based on the group selected.

Click the **Clear All** button to clear all the information in this table.

Click the second **Clear** button to clear all the information for the specific entry.

IMPB

The IP network layer uses a four-byte address. The Ethernet link-layer uses a six-byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP-MAC-Port Binding (IMPB) is to restrict the access to a Switch to a number of authorized users. Authorized clients can access a Switch's port by either checking the pair of IP-MAC addresses with the pre-configured database or if DHCP snooping has been enabled in which case the Switch will automatically learn the IP/MAC pairs by snooping DHCP packets and saving them to the IMPB white list. If an unauthorized user tries to access an IP-MAC binding enabled port, the system will block the access by dropping its packet. Active and inactive entries use the same database. The function is port-based, meaning a user can enable or disable the function on the individual port.

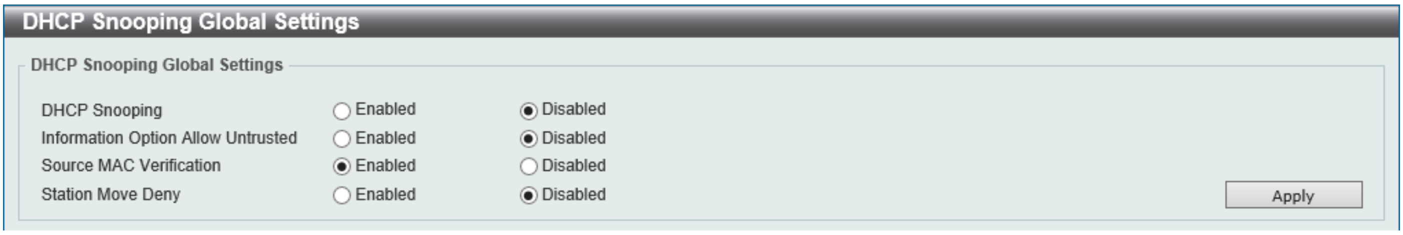
IPv4

DHCPv4 Snooping

DHCP Snooping Global Settings

This window is used to display and configure the global DHCP snooping settings.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Global Settings**, as shown below:



DHCP Snooping	○ Enabled	● Disabled
Information Option Allow Untrusted	○ Enabled	● Disabled
Source MAC Verification	● Enabled	○ Disabled
Station Move Deny	○ Enabled	● Disabled

Figure 9-39 DHCP Snooping Global Settings Window

The fields that can be configured are described below:

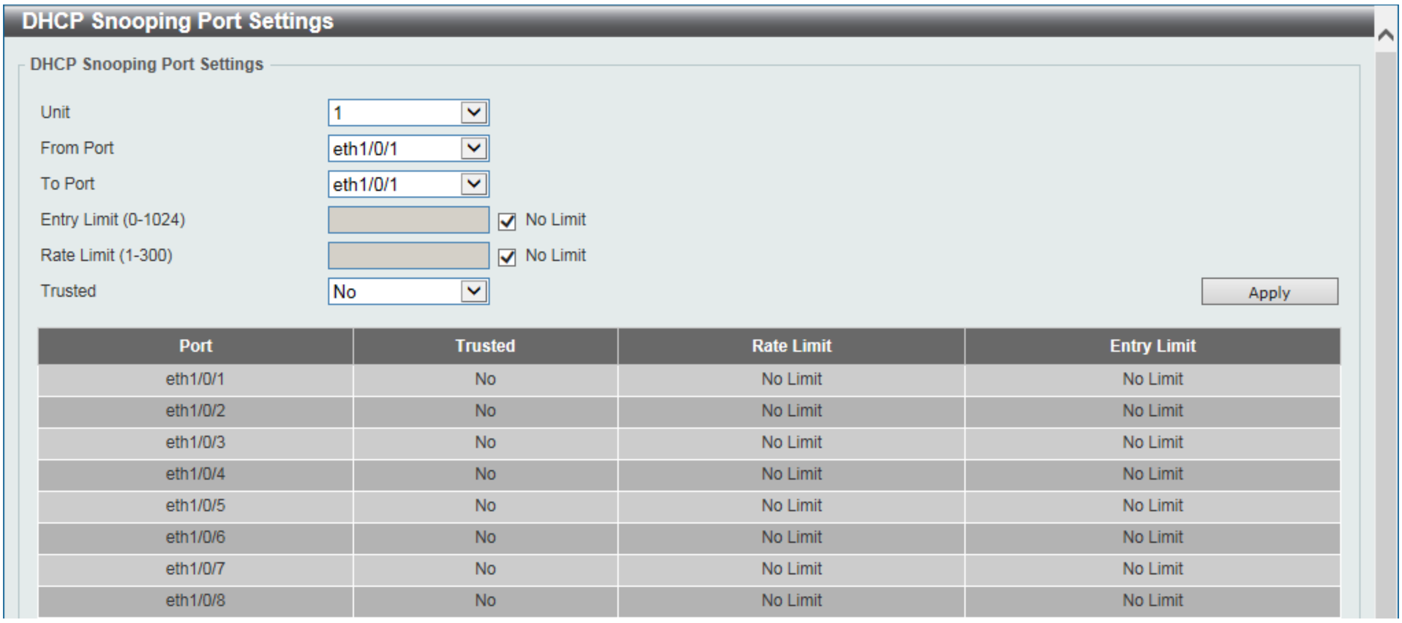
Parameter	Description
DHCP Snooping	Select to enable or disable the global DHCP snooping status.
Information Option Allow Untrusted	Select to enable or disable the option to globally allow DHCP packets with the relay Option 82 on the untrusted interface.
Source MAC Verification	Select to enable or disable the verification that the source MAC address in a DHCP packet matches the client hardware address.
Station Move Deny	Select to enable or disable the DHCP snooping station move state. When DHCP snooping station move is enabled, the dynamic DHCP snooping binding entry with the same VLAN ID and MAC address on the specific port can move to another port if it detects that a new DHCP process belong to the same VLAN ID and MAC address.

Click the **Apply** button to accept the changes made.

DHCP Snooping Port Settings

This window is used to display and configure the DHCP snooping port settings.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Port Settings**, as shown below:



DHCP Snooping Port Settings

DHCP Snooping Port Settings

Unit: 1

From Port: eth1/0/1

To Port: eth1/0/1

Entry Limit (0-1024): ☑ No Limit

Rate Limit (1-300): ☑ No Limit

Trusted: No

Port	Trusted	Rate Limit	Entry Limit
eth1/0/1	No	No Limit	No Limit
eth1/0/2	No	No Limit	No Limit
eth1/0/3	No	No Limit	No Limit
eth1/0/4	No	No Limit	No Limit
eth1/0/5	No	No Limit	No Limit
eth1/0/6	No	No Limit	No Limit
eth1/0/7	No	No Limit	No Limit
eth1/0/8	No	No Limit	No Limit

Figure 9-40 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.
From Port - To Port	Select the appropriate port range used for the configuration here.
Entry Limit	Enter the entry limit value here. The range is from 0 to 1024. Select the **No Limit** option to use the default value.
Rate Limit	Enter the rate limit value here. The range is from 1 to 300. Select the **No Limit** option to disable the function.

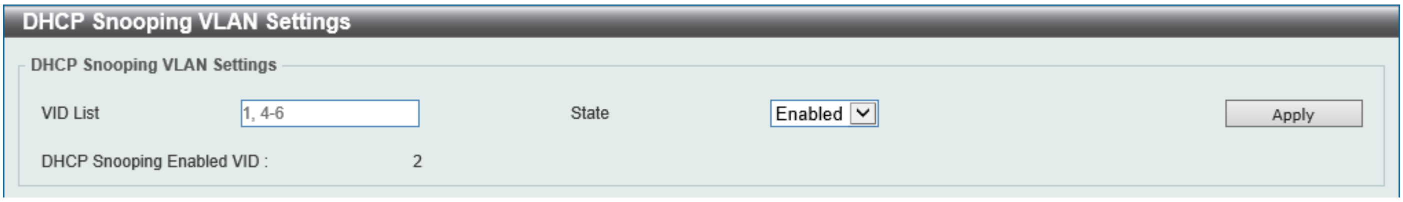
Parameter	Description
Trusted	Select the trusted option here. Options to choose from are **No** and **Yes**. Ports connected to the DHCP server or to other Switches should be configured as trusted interfaces. The ports connected to DHCP clients should be configured as untrusted interfaces. DHCP snooping acts as a firewall between untrusted interfaces and DHCP servers.

Click the **Apply** button to accept the changes made.

DHCP Snooping VLAN Settings

This window is used to display and configure the DHCP snooping VLAN settings.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping VLAN Settings**, as shown below:



DHCP Snooping VLAN Settings

DHCP Snooping VLAN Settings

VID List: 1, 4-6

State: Enabled

DHCP Snooping Enabled VID : 2

Figure 9-41 DHCP Snooping VLAN Settings Window

The fields that can be configured are described below:

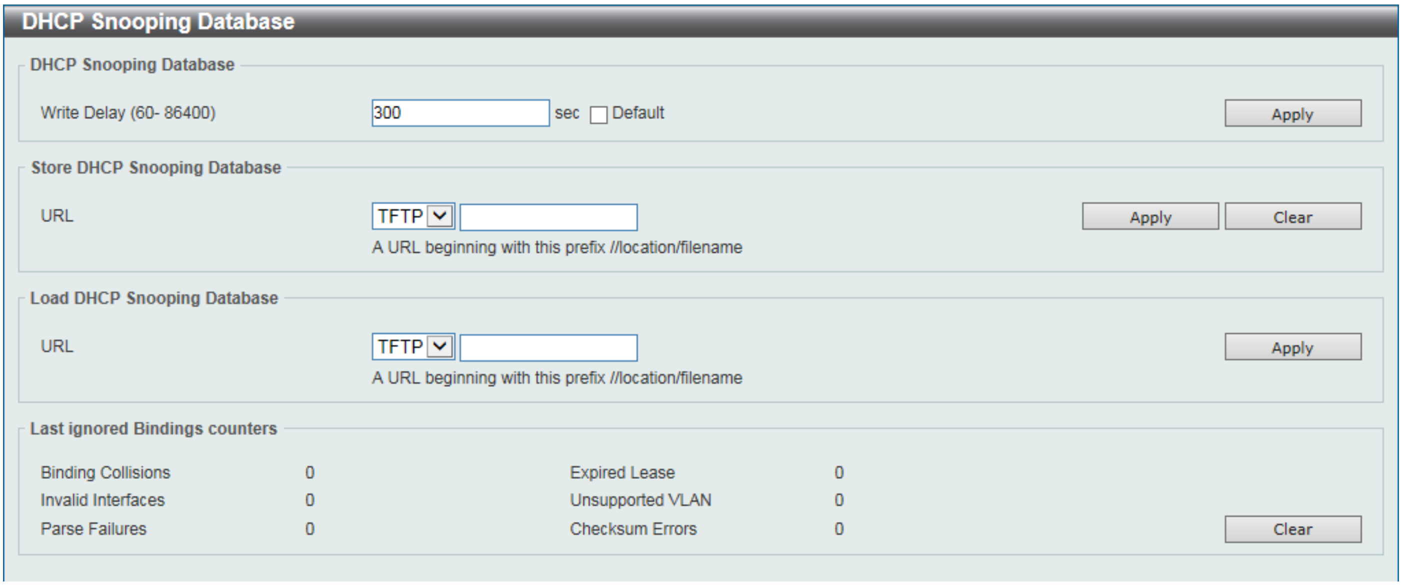
Parameter	Description
VID List	Enter the VLAN ID list used here.
State	Select to enable or disable the DHCP snooping VLAN setting here.

Click the **Apply** button to accept the changes made.

DHCP Snooping Database

This window is used to display and configure the DHCP snooping database settings.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Database**, as shown below:


DHCP Snooping Database
DHCP Snooping Database
sec
□ Default
Apply
Store DHCP Snooping Database
Apply
Clear
Load DHCP Snooping Database
Apply
Last ignored Bindings counters
Clear

Write Delay (60- 86400): 300

URL: TFTP

A URL beginning with this prefix //location/filename

URL: TFTP

A URL beginning with this prefix //location/filename

Binding Collisions	0	Expired Lease	0
Invalid Interfaces	0	Unsupported VLAN	0
Parse Failures	0	Checksum Errors	0

Figure 9-42 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. The range is from 60 to 86400 seconds. By default, this value is 300 seconds.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Store DHCP Snooping Database** are described below:

Parameter	Description
URL	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.

Click the **Clear** button to clear the information.

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.

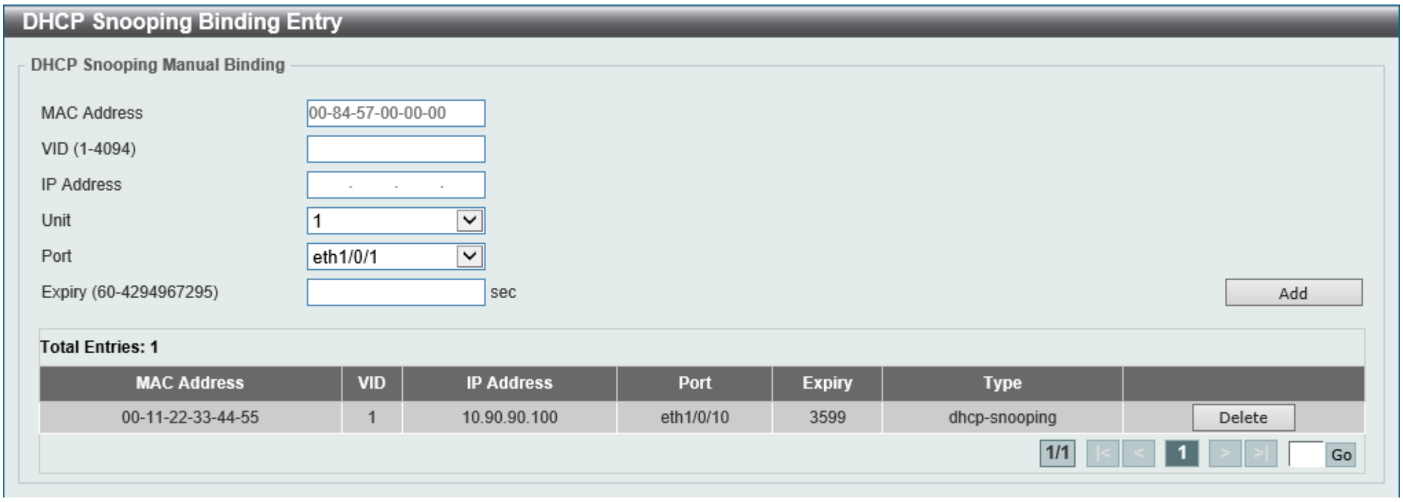
Click the **Apply** button to accept the changes made.

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:



DHCP Snooping Binding Entry

DHCP Snooping Manual Binding

MAC Address	00-84-57-00-00-00
VID (1-4094)	
IP Address	. . .
Unit	1
Port	eth1/0/1
Expiry (60-4294967295)	sec

Total Entries: 1

MAC Address	VID	IP Address	Port	Expiry	Type	
00-11-22-33-44-55	1	10.90.90.100	eth1/0/10	3599	dhcp-snooping	Delete

Figure 9-43 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. The range is from 1 to 4094.
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.
Port	Select the appropriate port used for the configuration here.
Expiry	Enter the expiry time value used here. The range is from 60 to 4294967295 seconds.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove the specified entry.

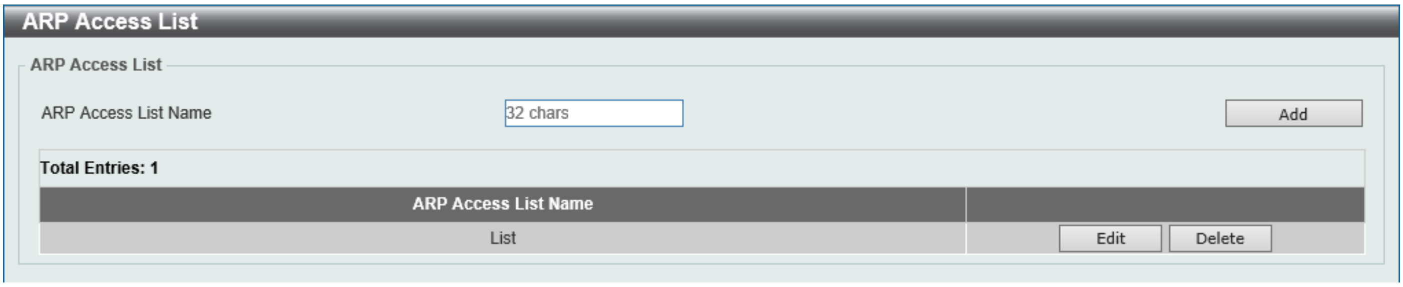
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Dynamic ARP Inspection

ARP Access List

This window is used to display and configure the dynamic ARP inspection settings.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Access List**, as shown below:



ARP Access List

ARP Access List

ARP Access List Name: 32 chars

Total Entries: 1

ARP Access List Name	
List	Edit Delete

Figure 9-44 ARP Access List Window

The fields that can be configured are described below:

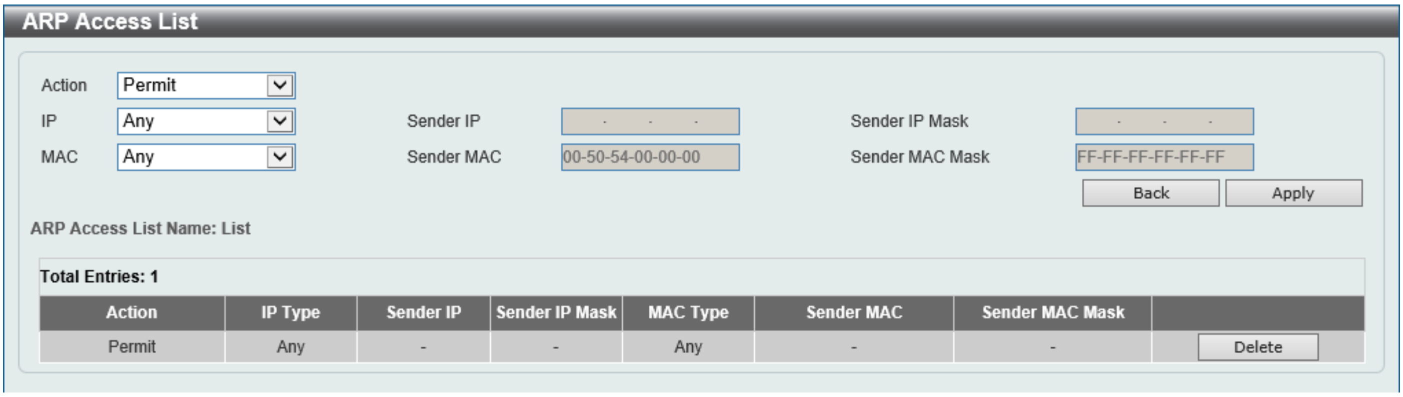
Parameter	Description
ARP Access List Name	Enter the ARP access list name used here. This name can be up to 32 characters long.

Click the **Add** button to add a new entry based on the information entered.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

After clicking the **Edit** button, the following window will appear.



ARP Access List

Action: Permit
IP: Any
MAC: Any
Sender IP: . . .
Sender MAC: 00-50-54-00-00-00
Sender IP Mask: . . .
Sender MAC Mask: FF-FF-FF-FF-FF-FF

ARP Access List Name: List

Total Entries: 1

Action	IP Type	Sender IP	Sender IP Mask	MAC Type	Sender MAC	Sender MAC Mask	
Permit	Any	-	-	Any	-	-	Delete

Figure 9-45 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.

Parameter	Description
Sender IP Mask	After selecting the **IP with Mask** option as the type of **IP**, enter the sender IP mask used here.
MAC	Select the type of sender MAC address that will be used here. Options to choose from are **Any**, **Host**, and **MAC with Mask**.
Sender MAC	After selecting the **Host** or **MAC with Mask** options as the type of **MAC**, enter the sender MAC address used here.
Sender MAC Mask	After selecting the **MAC with Mask** option as the type of **MAC**, enter the sender MAC mask used here.

Click the **Back** button to return to the previous page.

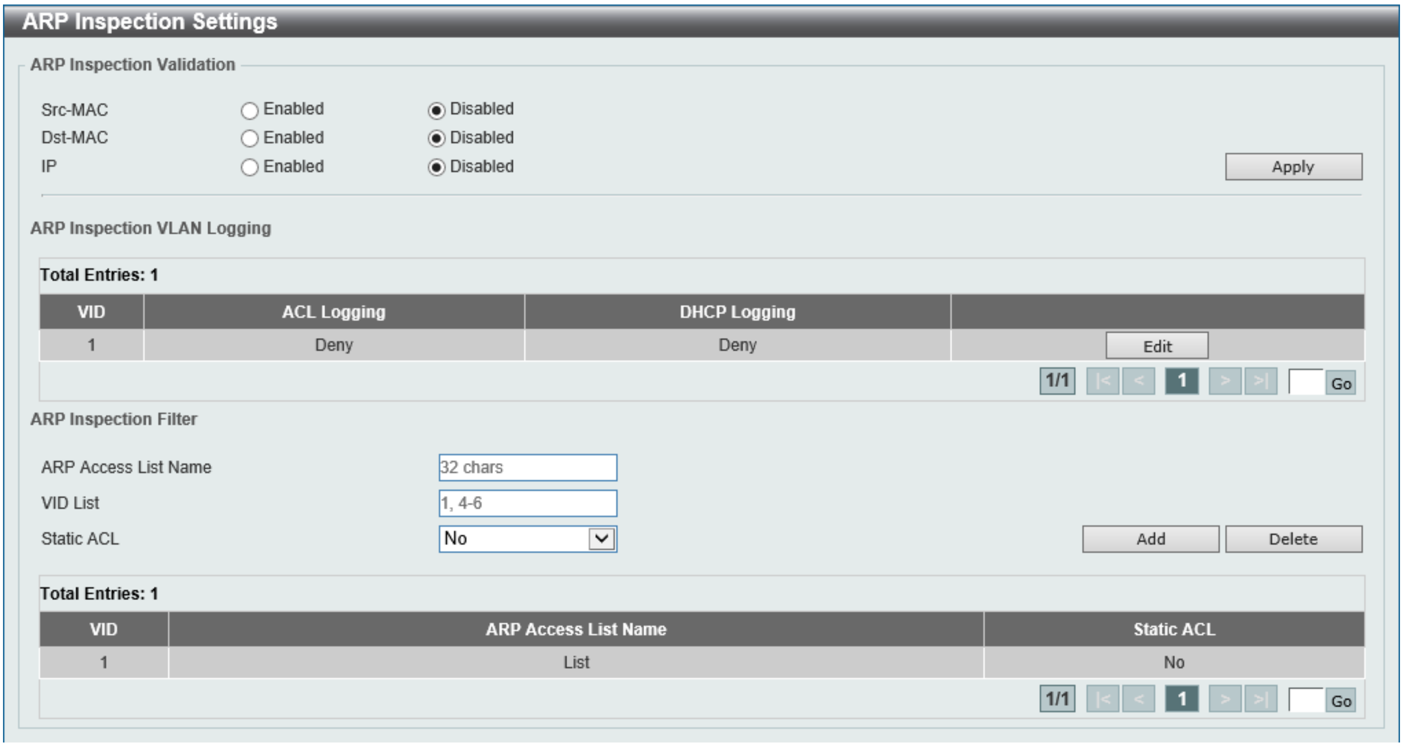
Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

ARP Inspection Settings

This window is used to display and configure the ARP inspection settings.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Settings**, as shown below:



ARP Inspection Settings

ARP Inspection Validation

Src-MAC ○ Enabled ● Disabled

Dst-MAC ○ Enabled ● Disabled

IP ○ Enabled ● Disabled

ARP Inspection VLAN Logging

Total Entries: 1

VID	ACL Logging	DHCP Logging	
1	Deny	Deny	Edit

ARP Inspection Filter

ARP Access List Name: 32 chars

VID List: 1, 4-6

Static ACL: No

Total Entries: 1

VID	ARP Access List Name	Static ACL
1	List	No

Figure 9-46 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

Parameter	Description
	address in the Ethernet header against the target MAC address in the ARP payload.
IP	Select to enable or disable the IP option here. This option specifies to check the ARP body for invalid and unexpected IP addresses. It also specifies to check the validity of IP address in the ARP payload. The sender IP in both the ARP request and response and target IP in the ARP response are validated. Packets destined for the IP addresses 0.0.0.0, 255.255.255.255, and all IP multicast addresses are dropped. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to configure the ACL/DHCP logging actions.

The fields that can be configured in **ARP Inspection VLAN Logging** are described below:

Parameter	Description
ACL Logging	After clicking the **Edit** button, select the ACL logging action here. Options to choose from are **Deny**, **Permit**, **All**, and **None**.
DHCP Logging	After clicking the **Edit** button, select the DHCP logging action here. Options to choose from are **Deny**, **Permit**, **All**, and **None**.

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.

The fields that can be configured in **ARP Inspection Filter** are described below:

Parameter	Description
ARP Access List Name	Enter the ARP access list name used here. This name can be up to 32 characters long.
VID List	Enter the VLAN ID list used here.
Static ACL	Select whether to use a static ACL or not here by either selecting **Yes** or **No**.

Click the **Add** button to add a new entry based on the information entered.

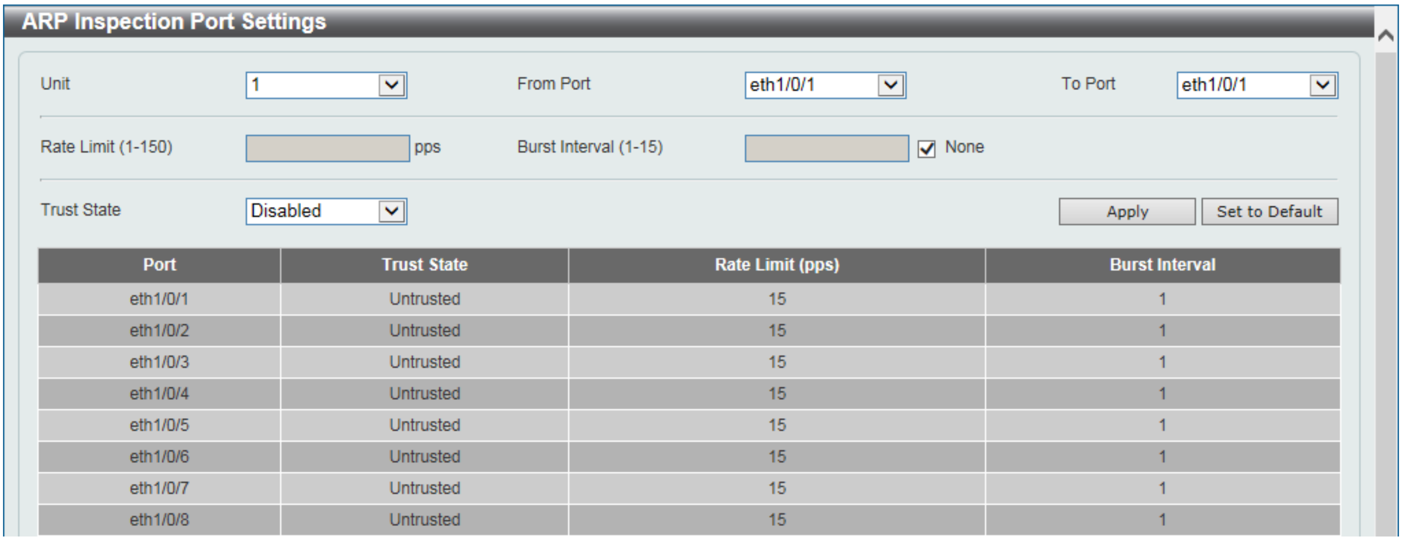
Click the **Delete** button to remove an entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

ARP Inspection Port Settings

This window is used to display and configure the ARP inspection port settings.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Port Settings**, as shown below:



ARP Inspection Port Settings

Unit: 1 — From Port: eth1/0/1 — To Port: eth1/0/1

Rate Limit (1-150): pps — Burst Interval (1-15): ☑ None

Trust State: Disabled

Port	Trust State	Rate Limit (pps)	Burst Interval
eth1/0/1	Untrusted	15	1
eth1/0/2	Untrusted	15	1
eth1/0/3	Untrusted	15	1
eth1/0/4	Untrusted	15	1
eth1/0/5	Untrusted	15	1
eth1/0/6	Untrusted	15	1
eth1/0/7	Untrusted	15	1
eth1/0/8	Untrusted	15	1

Figure 9-47 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.
From Port - To Port	Select the appropriate port range used for the configuration here.
Rate Limit	Enter the rate limit value here. The range is from 1 to 150 packets per seconds.
Burst Interval	Enter the burst interval value here. The range is from 1 to 15. Select the **None** option to disable the option.
Trust State	Select to enable or disable the trust state here.

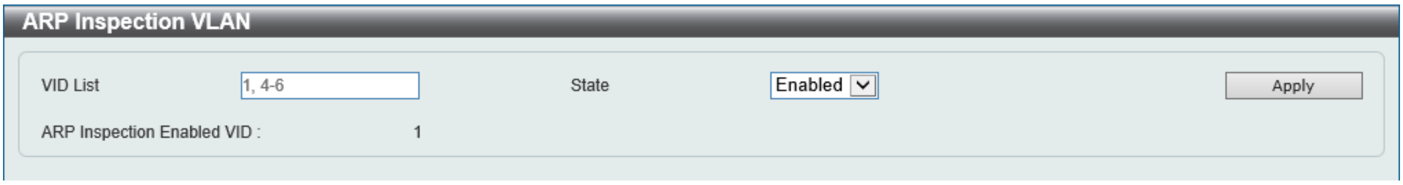
Click the **Apply** button to accept the changes made.

Click the **Set to Default** button to change the information to the default values.

ARP Inspection VLAN

This window is used to display and configure the ARP inspection VLAN settings.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection VLAN**, as shown below:



ARP Inspection VLAN

VID List: 1, 4-6 — State: Enabled

ARP Inspection Enabled VID : 1

Figure 9-48 ARP Inspection VLAN Window

The fields that can be configured are described below:

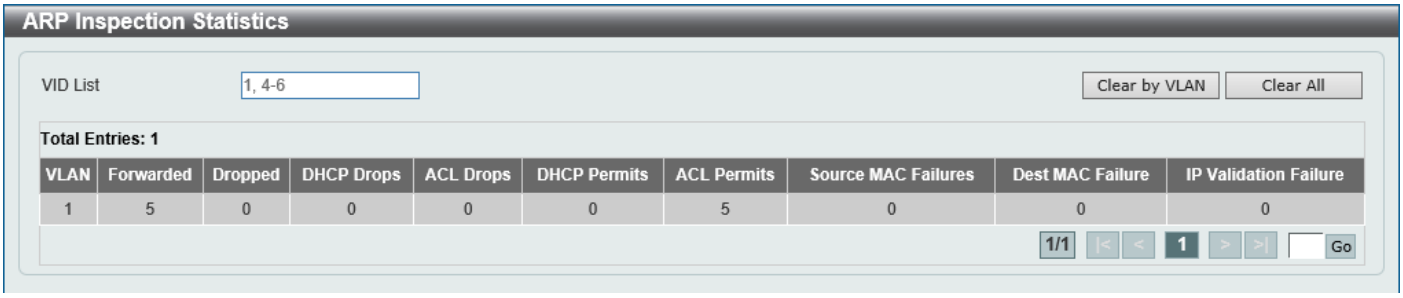
Parameter	Description
VID List	Enter the VLAN ID list used here.
State	Select to enable or disable the ARP inspection option’s state for the specified VLAN here.

Click the **Apply** button to accept the changes made.

ARP Inspection Statistics

This window is used to view and clear the ARP inspection statistics information.

To view the following window, click **Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Statistics**, as shown below:



VID List: 1, 4-6

Total Entries: 1

VLAN	Forwarded	Dropped	DHCP Drops	ACL Drops	DHCP Permits	ACL Permits	Source MAC Failures	Dest MAC Failure	IP Validation Failure
1	5	0	0	0	0	5	0	0	0

Figure 9-49 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.

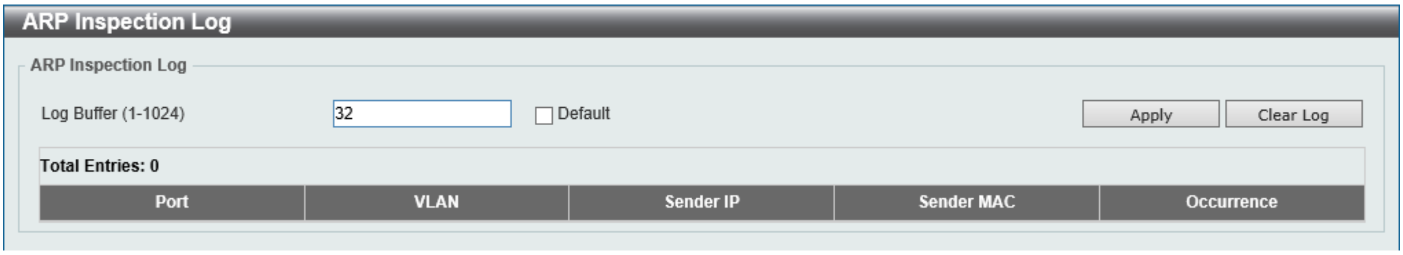
Click the **Clear All** button to clear all the information in this table.

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:



Log Buffer (1-1024): 32 □ Default

Total Entries: 0

Port	VLAN	Sender IP	Sender MAC	Occurrence

Figure 9-50 ARP Inspection Log Window

The fields that can be configured are described below:

Parameter	Description
Log Buffer	Enter the log buffer value used here. The range is from 1 to 1024. By default, this value is 32.

Click the **Apply** button to accept the changes made.

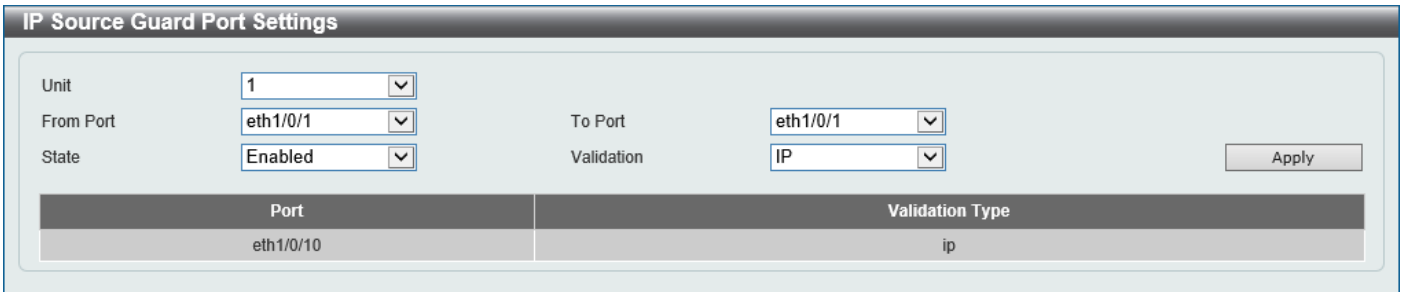
Click the **Clear Log** button to clear the log.

IP Source Guard

IP Source Guard Port Settings

This window is used to display and configure the IP Source Guard (IPSG) port settings.

To view the following window, click **Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Port Settings**, as shown below:



IP Source Guard Port Settings

Unit: 1

From Port: eth1/0/1 To Port: eth1/0/1

State: Enabled Validation: IP

Port	Validation Type
eth1/0/10	ip

Figure 9-51 IP Source Guard Port Settings Window

The fields that can be configured are described below:

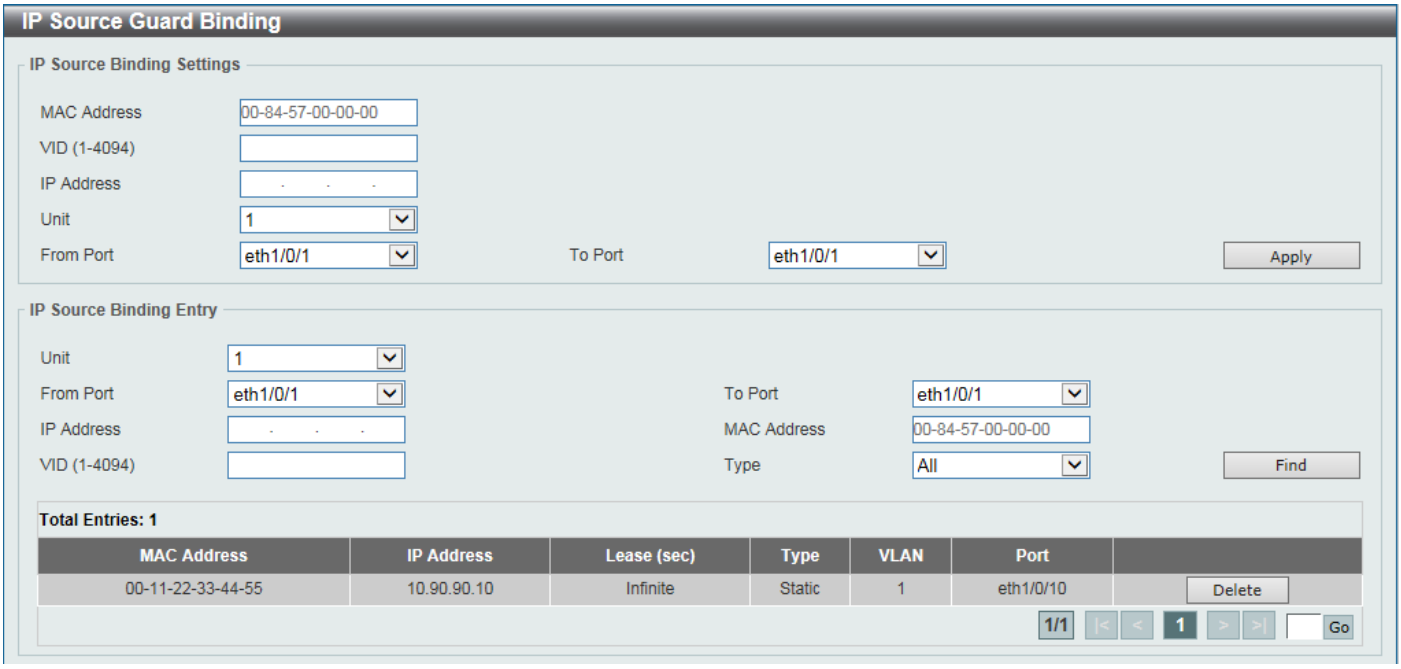
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the IPSG's state for the specified port(s) here.
Validation	Select the validation method used here. Options to choose from are: • **IP -** Specifies that the IP address of the received packets will be checked. • **IP-MAC -** Specifies that the IP address and the MAC address of the received packets will be checked.

Click the **Apply** button to accept the changes made.

IP Source Guard Binding

This window is used to display and configure the IPSG binding settings.

To view the following window, click **Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Binding**, as shown below:



IP Source Guard Binding

IP Source Binding Settings

MAC Address: 00-84-57-00-00-00
VID (1-4094):
IP Address: . . .
Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1

IP Source Binding Entry

Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1
IP Address: . . .
MAC Address: 00-84-57-00-00-00
VID (1-4094):
Type: All

Total Entries: 1

MAC Address	IP Address	Lease (sec)	Type	VLAN	Port	
00-11-22-33-44-55	10.90.90.10	Infinite	Static	1	eth1/0/10	Delete

Figure 9-52 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.
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.
From Port - To Port	Select the appropriate port range used for the query here.
IP Address	Enter the IP address of the binding entry here.
MAC Address	Enter the MAC address of the binding entry here.
VID	Enter the VLAN ID of the binding entry here.
Type	Select the type of binding entry to find here. Options to choose from are: • **All** - Specifies that all the DHCP binding entries will be displayed. • **DHCP Snooping** - Specifies to display the IP-source guard binding entry learned by DHCP binding snooping. • **Static** - Specifies to display the IP-source guard binding entry that is manually configured.

Click the **Find** button to locate a specific entry based on the information entered.

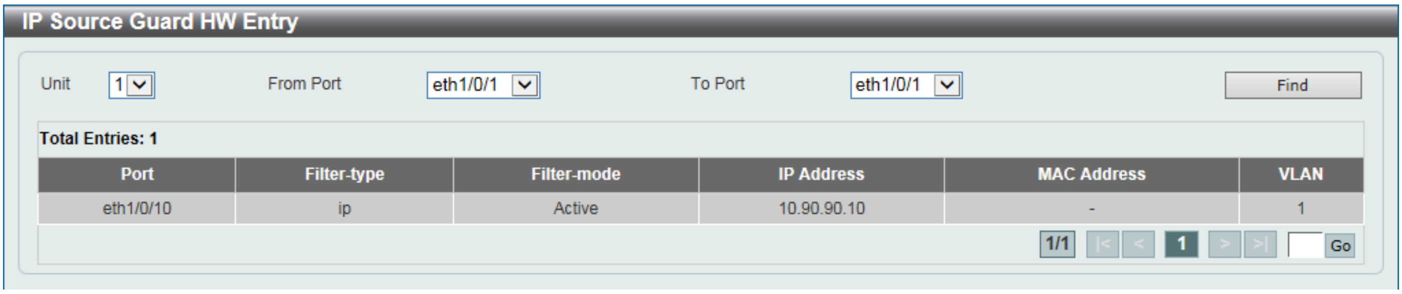
Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IP Source Guard HW Entry

This window is used to view the IPSG hardware entries.

To view the following window, click **Security > IMPB > IPv4 > IP Source Guard > IP Source Guard HW Entry**, as shown below:



IP Source Guard HW Entry

Unit 1 From Port eth1/0/1 To Port eth1/0/1 Find

Total Entries: 1

Port	Filter-type	Filter-mode	IP Address	MAC Address	VLAN
eth1/0/10	ip	Active	10.90.90.10	-	1

Figure 9-53 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.
From Port - To Port	Select the appropriate port range used for the query here.

Click the **Find** button to locate a specific entry based on the information entered.

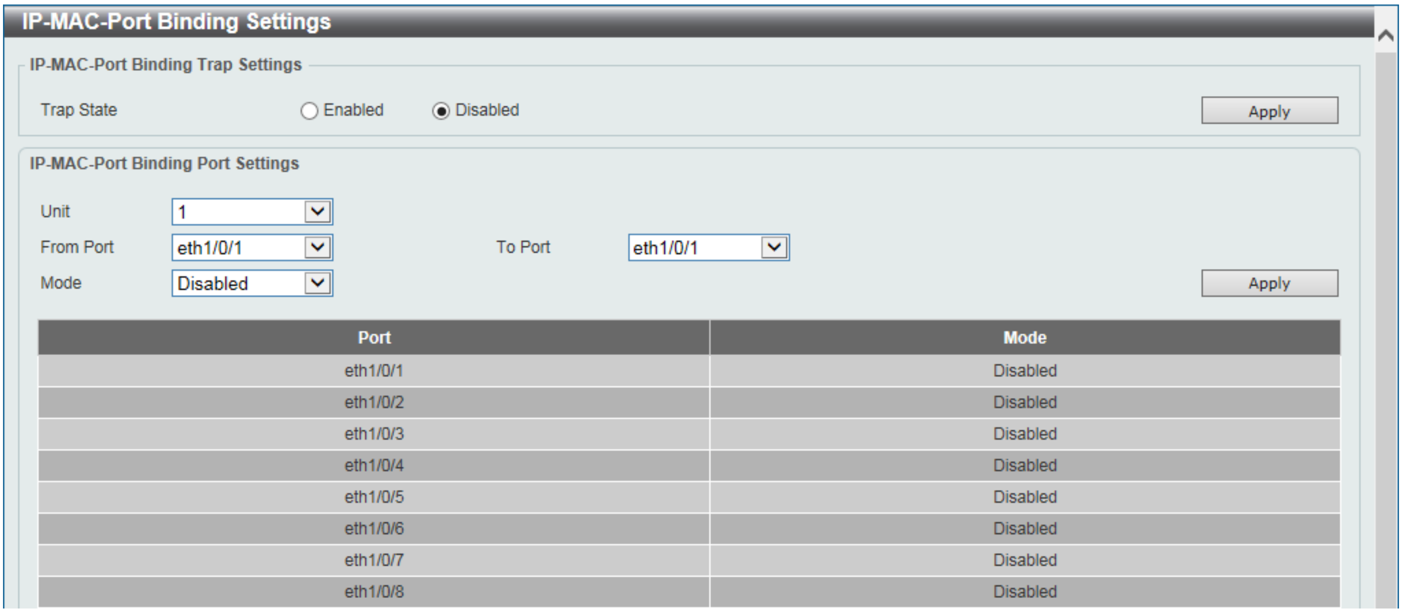
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Advanced Settings

IP-MAC-Port Binding Settings

This window is used to display and configure the IP-MAC-Port binding settings.

To view the following window, click **Security > IMPB > IPv4 > Advanced Settings > IP-MAC-Port Binding Settings**, as shown below:



IP-MAC-Port Binding Settings

IP-MAC-Port Binding Trap Settings

Trap State ○ Enabled ● Disabled

IP-MAC-Port Binding Port Settings

Unit: 1

From Port: eth1/0/1 To Port: eth1/0/1

Mode: Disabled

Port	Mode
eth1/0/1	Disabled
eth1/0/2	Disabled
eth1/0/3	Disabled
eth1/0/4	Disabled
eth1/0/5	Disabled
eth1/0/6	Disabled
eth1/0/7	Disabled
eth1/0/8	Disabled

Figure 9-54 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.
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** - Specifies that IP-MAC-Port binding function is disabled on the specified port(s). • **Strict** - When a port is enabled for IMPB strict-mode access control, a host can only access the port after the host sends ARP or IP packets and the ARP packet or IP packet sent by the host passes the binding check. To pass the binding check, the source IP address, source MAC address, VLAN ID, and arrival port number must match any of the entries defined by either the IPSG static binding entry or the DHCP snooping learned dynamic binding entry. • **Loose** - 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

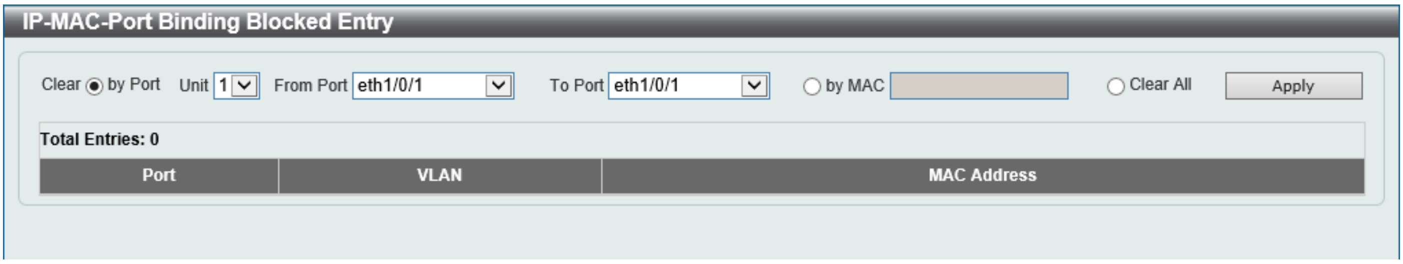
Parameter	Description
	either the IPSG static binding entry or the DHCP snooping learned dynamic binding entry.

Click the **Apply** button to accept the changes made.

IP-MAC-Port Binding Blocked Entry

This window is used to view and clear the IP-MAC-Port binding blocked entry table.

To view the following window, click **Security > IMPB > IPv4 > Advanced Settings > IP-MAC-Port Binding Blocked Entry**, as shown below:


IP-MAC-Port Binding Blocked Entry
Clear ● by Port Unit 1 From Port eth1/0/1 To Port eth1/0/1 ○ by MAC ○ Clear All
Apply

Total Entries: 0

Port	VLAN	MAC Address

Figure 9-55 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.
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.

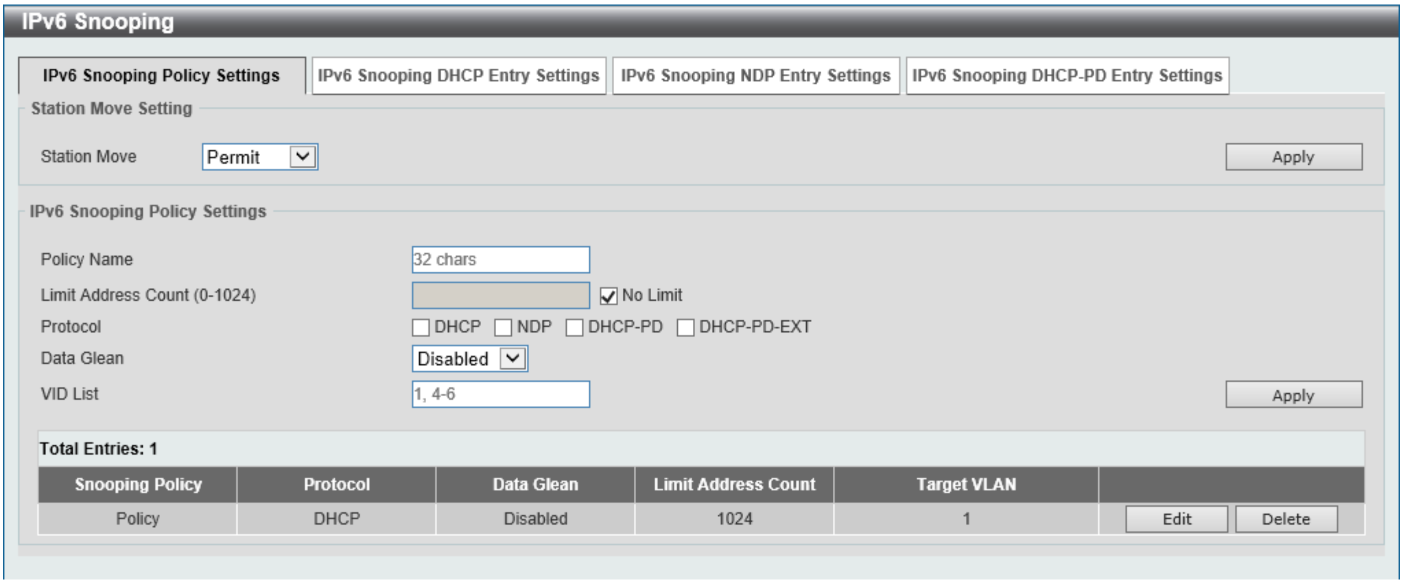
Click the **Apply** button to accept the changes made.

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** and select the **IPv6 Snooping Policy Settings** tab, as shown below:


IPv6 Snooping
IPv6 Snooping Policy Settings
IPv6 Snooping DHCP Entry Settings
IPv6 Snooping NDP Entry Settings
IPv6 Snooping DHCP-PD Entry Settings
Station Move Setting
Apply
IPv6 Snooping Policy Settings
Apply
Edit
Delete

Station Move: Permit

Policy Name: 32 chars

Limit Address Count (0-1024): ☑ No Limit

Protocol: □ DHCP □ NDP □ DHCP-PD □ DHCP-PD-EXT

Data Glean: Disabled

VID List: 1, 4-6

Total Entries: 1

Snooping Policy	Protocol	Data Glean	Limit Address Count	Target VLAN	
Policy	DHCP	Disabled	1024	1	Edit Delete

Figure 9-56 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**. • **DHCP** - Specifies that addresses should be snooped in DHCPv6 packets. • **NDP** - Specifies that addresses should be snooped in NDP packets. • **DHCP-PD** - Specified that IPv6 prefix should be snooped in DHCPv6 PD packets. • **DHCP-PD-EXT** Specified that IPv6 prefix should be snooped in DHCPv6 PD packets. PD snooping runs in the extension mode. 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

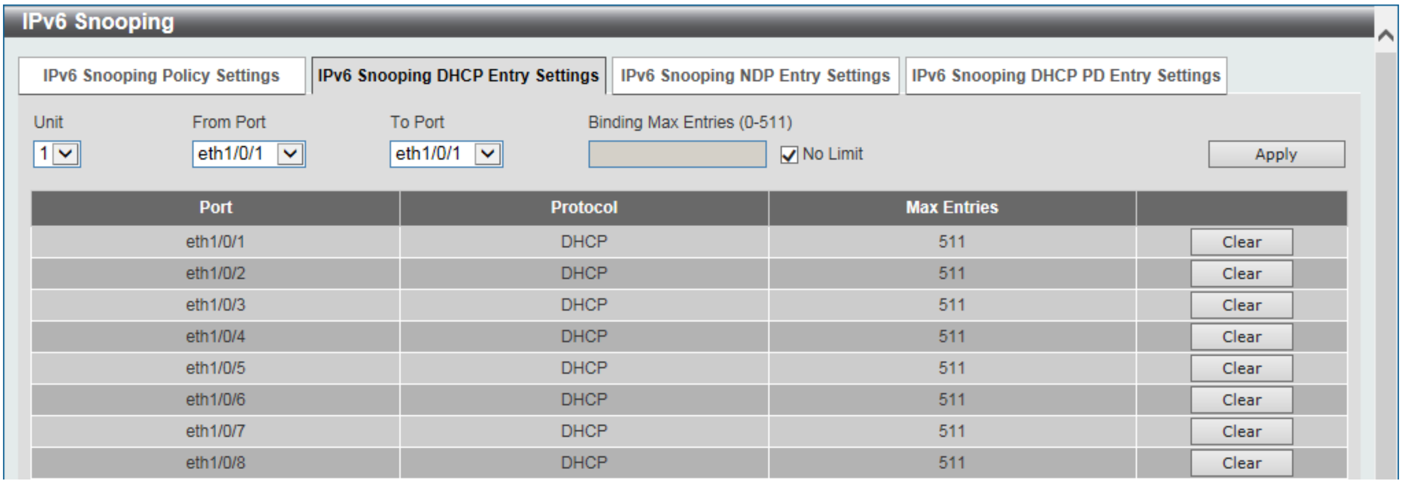
Parameter	Description
	IPv6 address and manually configured IPv6 address. Before assigning an IPv6 address, the host must perform Duplicate Address Detection first. ND snooping detects DAD messages (DAD Neighbor Solicitation (NS) and DAD Neighbor Advertisement (NA)) to build its binding database. The 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.
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.


IPv6 Snooping
IPv6 Snooping Policy Settings
IPv6 Snooping DHCP Entry Settings
IPv6 Snooping NDP Entry Settings
IPv6 Snooping DHCP PD Entry Settings
Apply

Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1
Binding Max Entries (0-511):
☑ No Limit

Port	Protocol	Max Entries	
eth1/0/1	DHCP	511	Clear
eth1/0/2	DHCP	511	Clear
eth1/0/3	DHCP	511	Clear
eth1/0/4	DHCP	511	Clear
eth1/0/5	DHCP	511	Clear
eth1/0/6	DHCP	511	Clear
eth1/0/7	DHCP	511	Clear
eth1/0/8	DHCP	511	Clear

Figure 9-57 IPv6 Snooping (IPv6 Snooping DHCP Entry Settings) Window

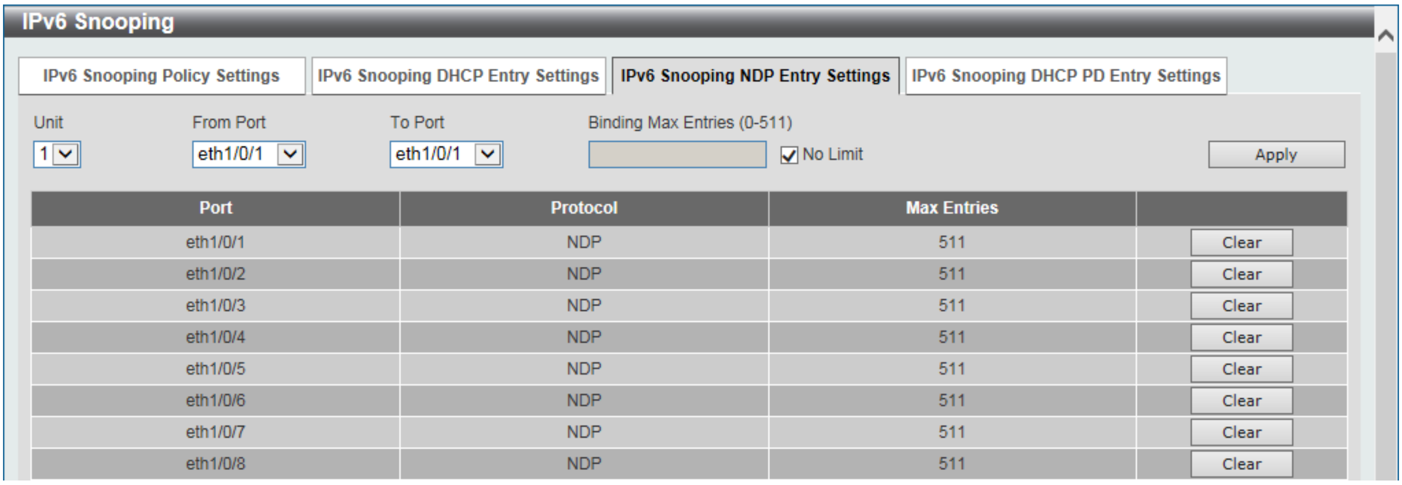
The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch stacking unit ID here.
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 511. Select the **No Limit** option to use the default value.

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.


IPv6 Snooping
IPv6 Snooping Policy Settings
IPv6 Snooping DHCP Entry Settings
IPv6 Snooping NDP Entry Settings
IPv6 Snooping DHCP PD Entry Settings
Apply

Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1
Binding Max Entries (0-511): ☑ No Limit

Port	Protocol	Max Entries	
eth1/0/1	NDP	511	Clear
eth1/0/2	NDP	511	Clear
eth1/0/3	NDP	511	Clear
eth1/0/4	NDP	511	Clear
eth1/0/5	NDP	511	Clear
eth1/0/6	NDP	511	Clear
eth1/0/7	NDP	511	Clear
eth1/0/8	NDP	511	Clear

Figure 9-58 IPv6 Snooping (IPv6 Snooping NDP Entry Settings) Window

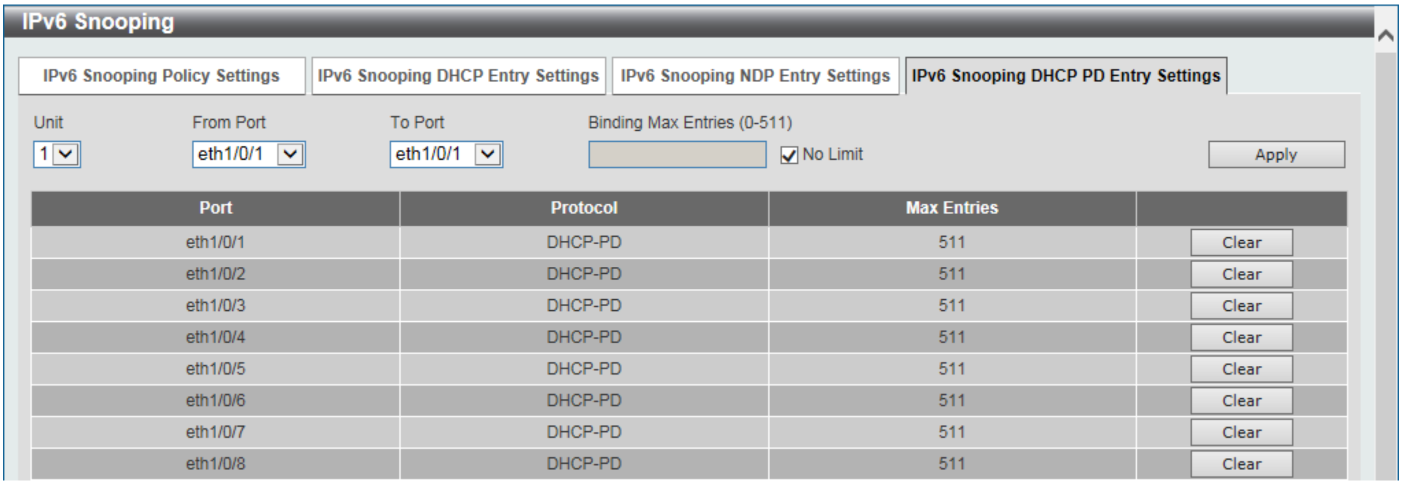
The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch stacking unit ID here.
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 511. Select the **No Limit** option to use the default value.

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.


IPv6 Snooping
IPv6 Snooping Policy Settings
IPv6 Snooping DHCP Entry Settings
IPv6 Snooping NDP Entry Settings
IPv6 Snooping DHCP PD Entry Settings
Apply

Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1
Binding Max Entries (0-511): ☑ No Limit

Port	Protocol	Max Entries	
eth1/0/1	DHCP-PD	511	Clear
eth1/0/2	DHCP-PD	511	Clear
eth1/0/3	DHCP-PD	511	Clear
eth1/0/4	DHCP-PD	511	Clear
eth1/0/5	DHCP-PD	511	Clear
eth1/0/6	DHCP-PD	511	Clear
eth1/0/7	DHCP-PD	511	Clear
eth1/0/8	DHCP-PD	511	Clear

Figure 9-59 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.
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 511. Select the **No Limit** option to use the default value.

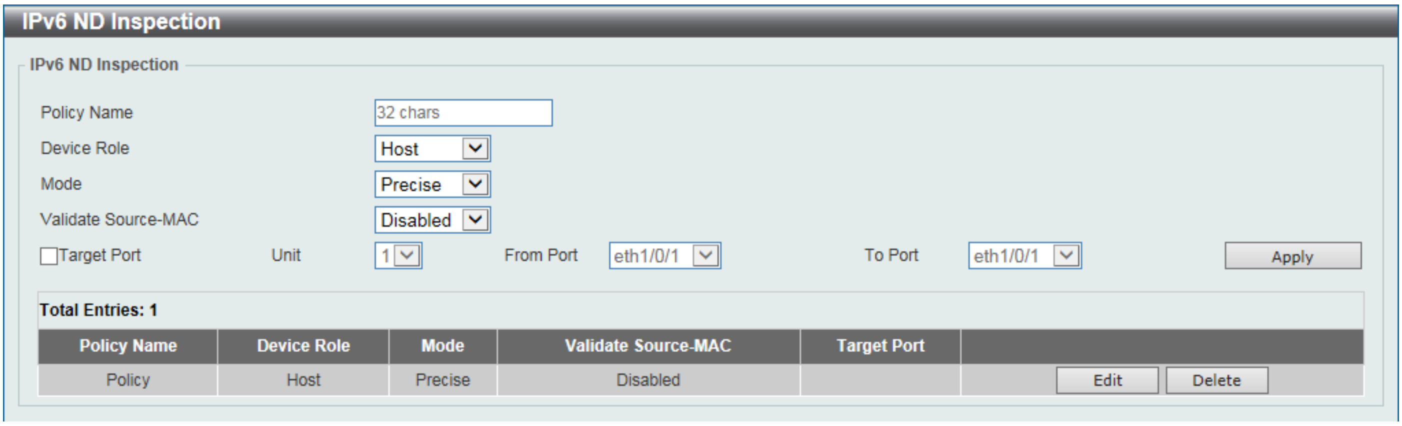
Click the **Apply** button to accept the changes made.

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:



IPv6 ND Inspection

IPv6 ND Inspection

Policy Name: 32 chars
Device Role: Host
Mode: Precise
Validate Source-MAC: Disabled
□ Target Port Unit: 1 From Port: eth1/0/1 To Port: eth1/0/1

Total Entries: 1

Policy Name	Device Role	Mode	Validate Source-MAC	Target Port	
Policy	Host	Precise	Disabled		Edit Delete

Figure 9-60 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** and **Fuzzy**.
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.
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.

Click the **Apply** button to accept the changes made.

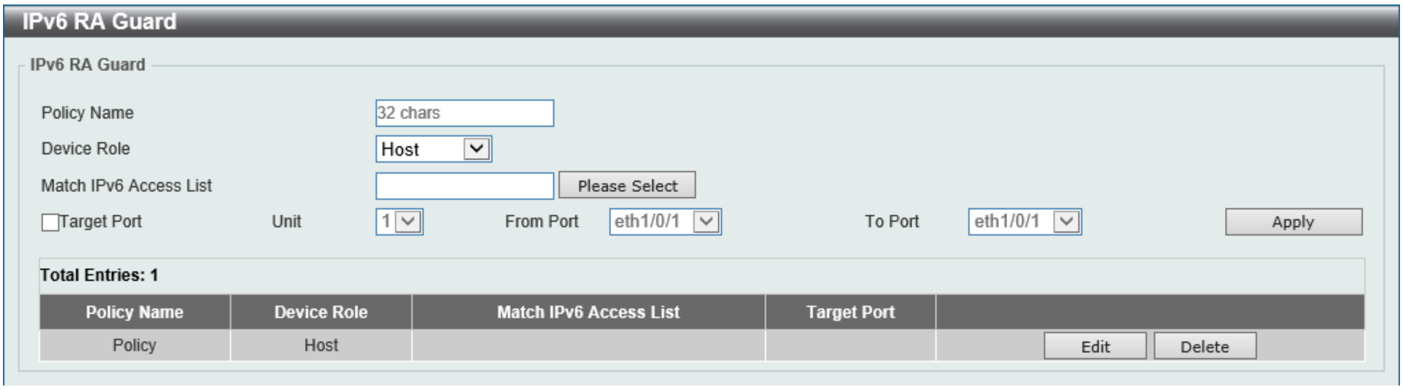
Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

IPv6 RA Guard

This window is used to display and configure the IPv6 Router Advertisement (RA) guard settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 RA Guard**, as shown below:



IPv6 RA Guard

IPv6 RA Guard

Policy Name: 32 chars

Device Role: Host

Match IPv6 Access List:

□ Target Port Unit: 1 From Port: eth1/0/1 To Port: eth1/0/1

Total Entries: 1

Policy Name	Device Role	Match IPv6 Access List	Target Port	
Policy	Host			Edit Delete

Figure 9-61 IPv6 RA Guard Window

The fields that can be configured are described below:

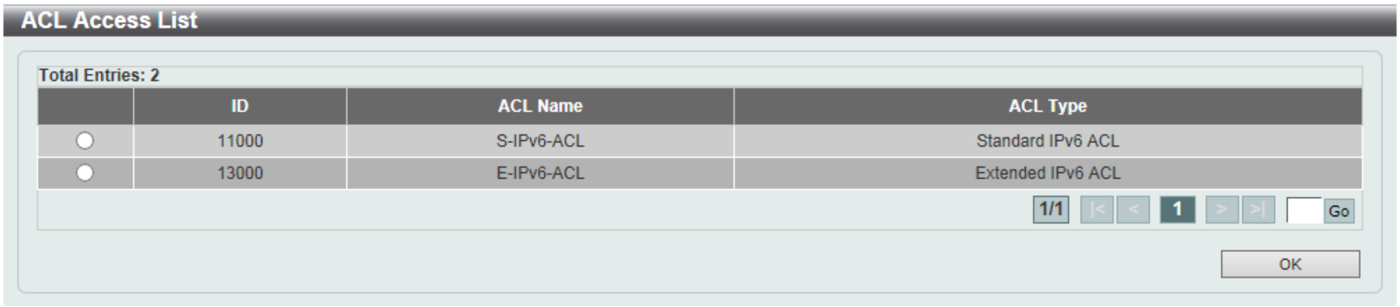
Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Device Role	Select the device role here. Options to choose from are **Host** and **Router**. By default, the device's role is **Host**, which will block all the RA packets. If the device's role is **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.
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.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

After clicking the **Please Select** button, the following window will appear:



ACL Access List

Total Entries: 2

	ID	ACL Name	ACL Type
○	11000	S-IPv6-ACL	Standard IPv6 ACL
○	13000	E-IPv6-ACL	Extended IPv6 ACL

Figure 9-62 ACL Access List Window

Select the radio button next to the entry to use that ACL in the configuration.

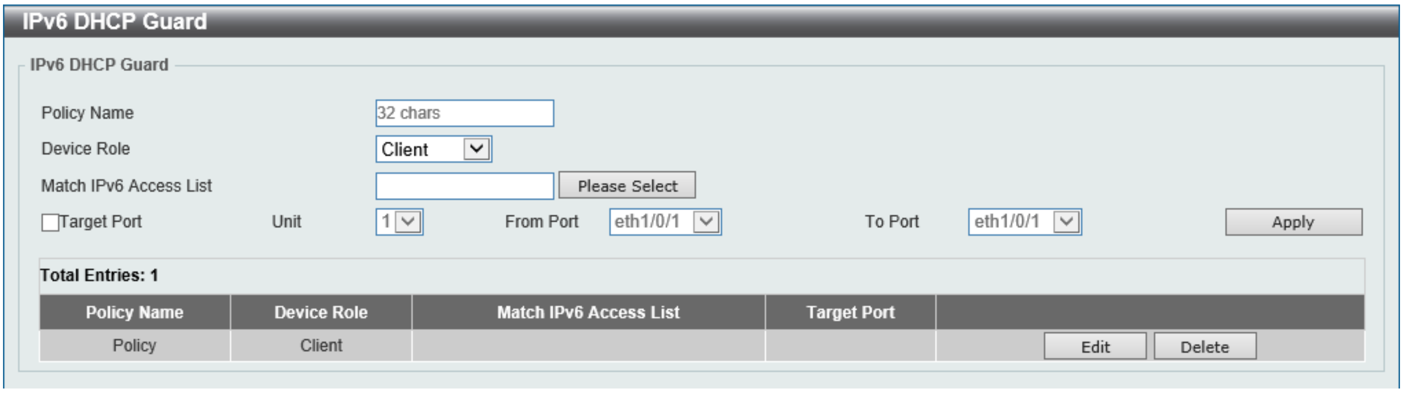
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **OK** button to accept the selection made.

IPv6 DHCP Guard

This window is used to display and configure the IPv6 DHCP guard settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 DHCP Guard**, as shown below:



IPv6 DHCP Guard

IPv6 DHCP Guard

Policy Name: 32 chars

Device Role: Client

Match IPv6 Access List:

□ Target Port Unit: 1 From Port: eth1/0/1 To Port: eth1/0/1

Total Entries: 1

Policy Name	Device Role	Match IPv6 Access List	Target Port	
Policy	Client			Edit Delete

Figure 9-63 IPv6 DHCP Guard Window

The fields that can be configured are described below:

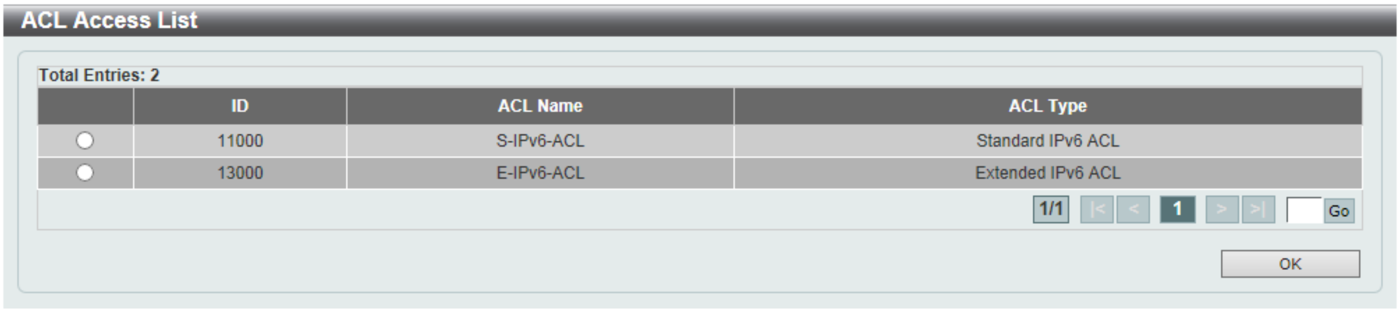
Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Device Role	Select the device role here. Options to choose from are: • **Client** - Specifies to block all the DHCPv6 packets from the DHCPv6 server. • **Server** - Specifies that DHCPv6 Server packets 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.
From Port - To Port	Select the appropriate port range used for the configuration here.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

After clicking the **Please Select** button, the following window will appear:



ACL Access List

Total Entries: 2

	ID	ACL Name	ACL Type
○	11000	S-IPv6-ACL	Standard IPv6 ACL
○	13000	E-IPv6-ACL	Extended IPv6 ACL

Figure 9-64 ACL Access List Window

Select the radio button next to the entry to use that ACL in the configuration.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

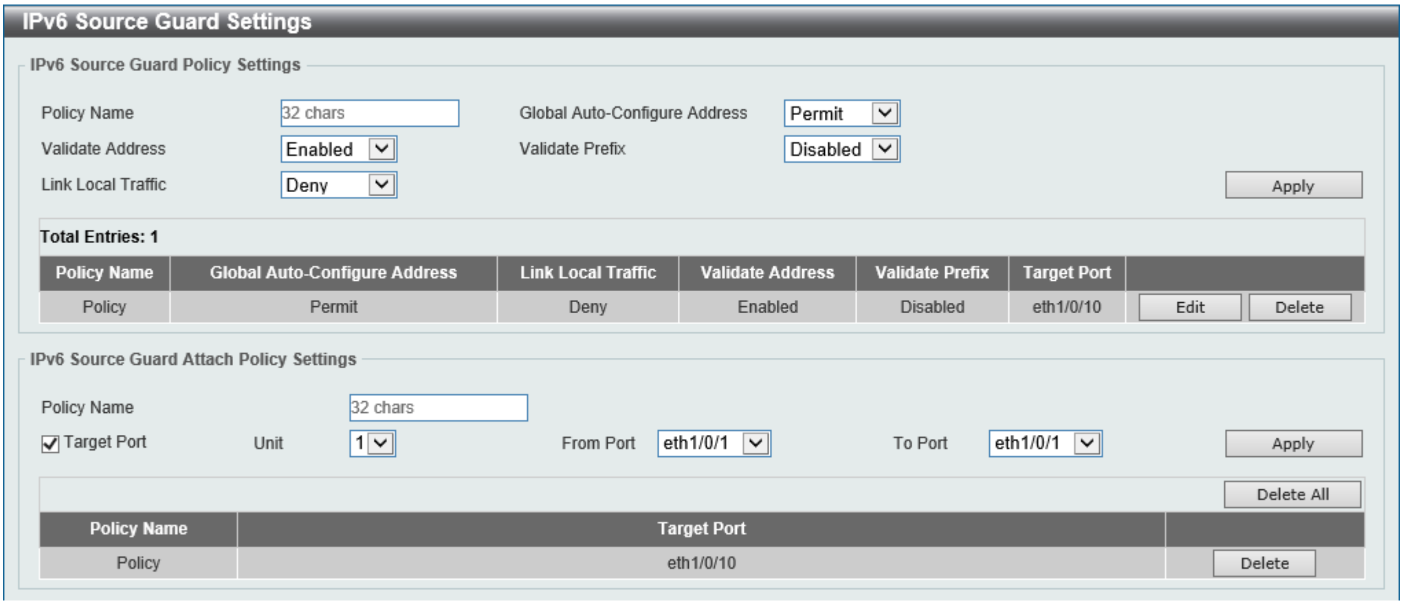
Click the **OK** button to accept the selection made.

IPv6 Source Guard

IPv6 Source Guard Settings

This window is used to display and configure the IPv6 source guard settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 Source Guard > IPv6 Source Guard Settings**, as shown below:



IPv6 Source Guard Settings

IPv6 Source Guard Policy Settings

Policy Name: 32 chars
Global Auto-Configure Address: Permit
Validate Address: Enabled
Validate Prefix: Disabled
Link Local Traffic: Deny

Total Entries: 1

Policy Name	Global Auto-Configure Address	Link Local Traffic	Validate Address	Validate Prefix	Target Port	
Policy	Permit	Deny	Enabled	Disabled	eth1/0/10	Edit Delete

IPv6 Source Guard Attach Policy Settings

Policy Name: 32 chars
☑ Target Port   Unit: 1   From Port: eth1/0/1   To Port: eth1/0/1

Policy Name	Target Port	
Policy	eth1/0/10	Delete

Figure 9-65 IPv6 Source Guard Settings Window

The fields that can be configured in **IPv6 Source Guard Policy Settings** are described below:

Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Global Auto-Configure Address	Select to permit of deny data traffic from the auto-configured global address. It is useful when all global addresses on a link are assigned by DHCP and the administrator that wants to block hosts with self-configured addresses from sending traffic.
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.
Link Local Traffic	Select to permit of deny hardware permitted data traffic send by the link-local address.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

The fields that can be configured in **IPv6 Source Guard Attach Policy Settings** are described below:

Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Target Port	Select this option to specify the target port.

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.

Click the **Apply** button to accept the changes made.

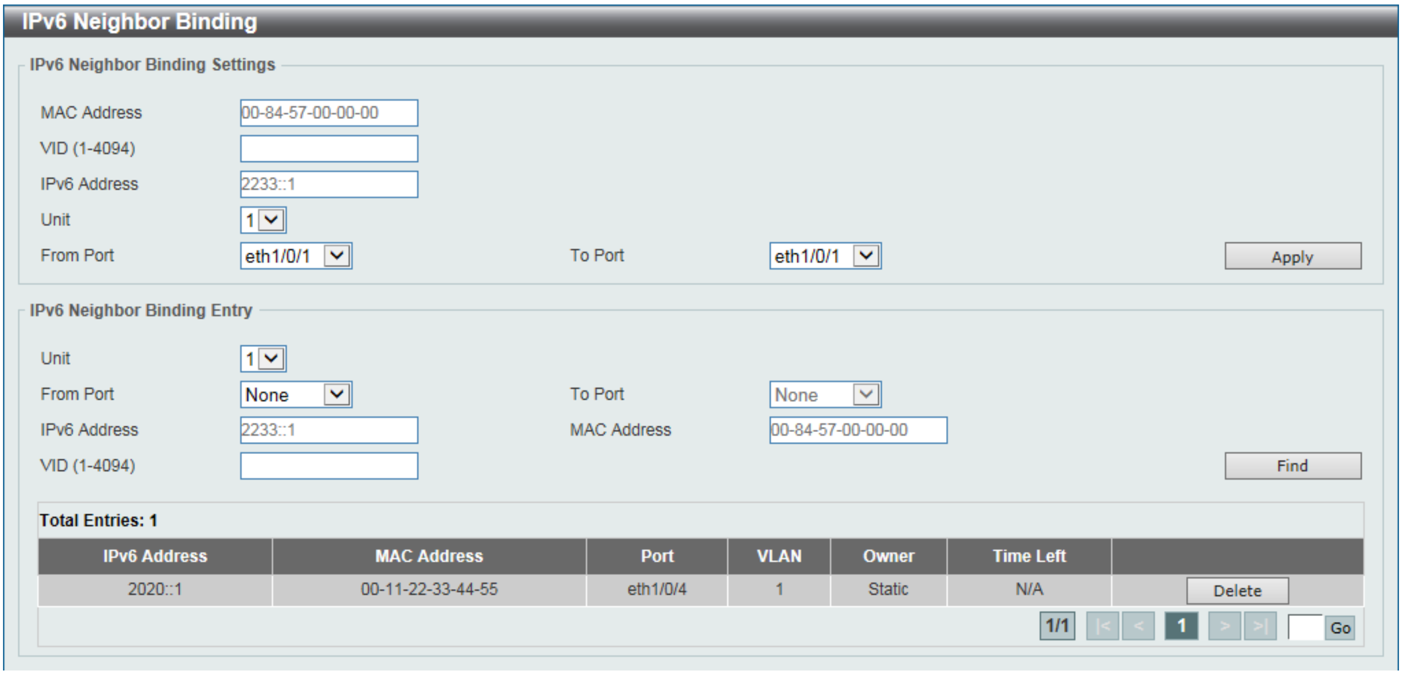
Click the **Delete All** button to remove all the entries.

Click the **Delete** button to remove the specified entry.

IPv6 Neighbor Binding

This window is used to display and configure the IPv6 neighbor binding settings.

To view the following window, click **Security > IMPB > IPv6 > IPv6 Source Guard > IPv6 Neighbor Binding**, as shown below:



IPv6 Neighbor Binding

IPv6 Neighbor Binding Settings

MAC Address: 00-84-57-00-00-00
VID (1-4094):
IPv6 Address: 2233::1
Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1

IPv6 Neighbor Binding Entry

Unit: 1
From Port: None
To Port: None
IPv6 Address: 2233::1
MAC Address: 00-84-57-00-00-00
VID (1-4094):

Total Entries: 1

IPv6 Address	MAC Address	Port	VLAN	Owner	Time Left	
2020::1	00-11-22-33-44-55	eth1/0/4	1	Static	N/A	Delete

Figure 9-66 IPv6 Neighbor Binding Window

The fields that can be configured in **IPv6 Neighbor Binding Settings** are described below:

Parameter	Description
MAC Address	Enter the MAC address used here.
VID	Enter the VLAN ID used here. The range is from 1 to 4094.
IPv6 Address	Enter the IPv6 address used here.
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.

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.
From Port - To Port	Select the appropriate port range used for the search here.

Parameter	Description
IPv6 Address	Enter the IPv6 address to find here.
MAC Address	Enter the MAC address to find here.
VID	Enter the VLAN ID to find here.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

DHCP Server Screening

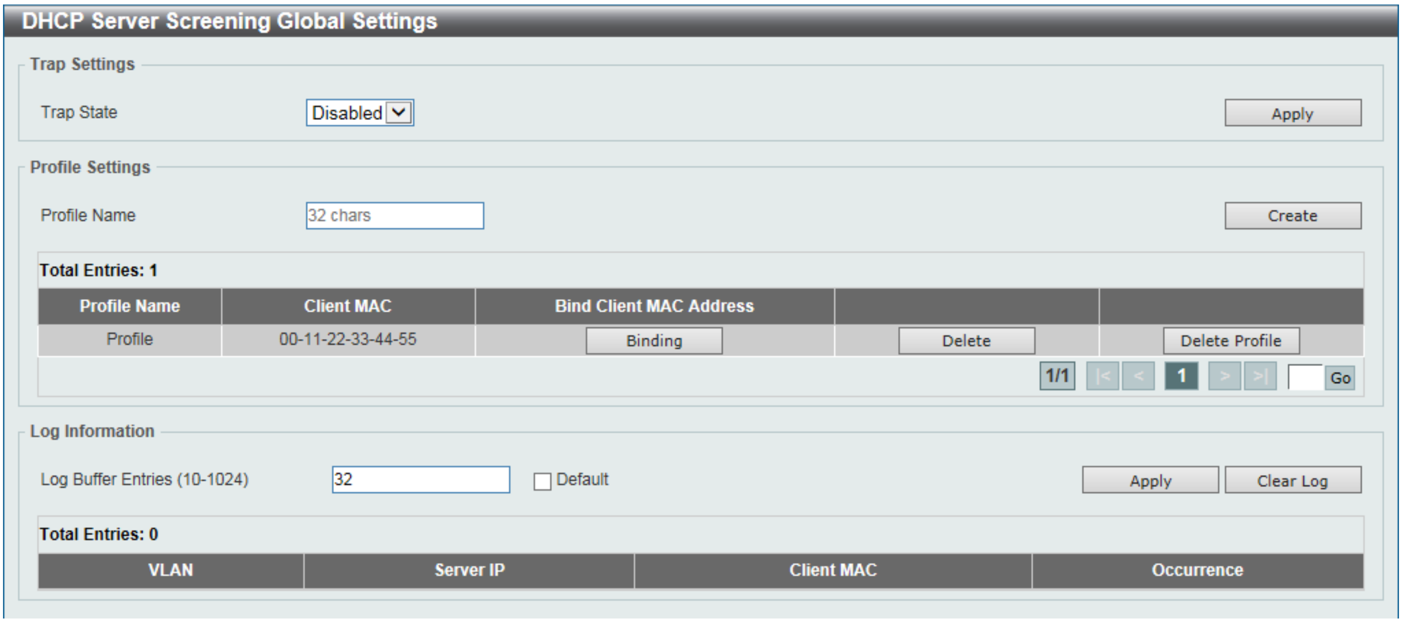
This function allows users to not only to restrict all DHCP server packets but also to receive any specified DHCP server packet by any specified DHCP client. It is useful when one or more DHCP servers are present on the network and both provide DHCP services to different distinct groups of clients.

When the DHCP Server Screening function is enabled on a port, all DHCP server packets received on this ports will be redirected to the CPU for a software-based check. Legal DHCP server packets will be forwarded out and illegal DHCP server packets will be dropped. When DHCP Server Screening function is enabled, all DHCP server packets will be filtered from a specific port.

DHCP Server Screening Global Settings

This window is used to display and configure the global DHCP server screening settings.

To view the following window, click **Security > DHCP Server Screening > DHCP Server Screening Global Settings**, as shown below:



DHCP Server Screening Global Settings

Trap Settings

Trap State: Disabled

Profile Settings

Profile Name: 32 chars

Total Entries: 1

Profile Name	Client MAC	Bind Client MAC Address		
Profile	00-11-22-33-44-55	Binding	Delete	Delete Profile

Log Information

Log Buffer Entries (10-1024): 32 □ Default

Total Entries: 0

VLAN	Server IP	Client MAC	Occurrence

Figure 9-67 DHCP Server Screening Global Settings Window

The fields that can be configured in **Trap Settings** are described below:

Parameter	Description
Trap State	Select to enable or disable the DHCP server-screening trap here.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Profile Settings** are described below:

Parameter	Description
Profile Name	Enter the DHCP server screening profile name here. This name can be up to 32 characters long.

Click the **Create** button to create a new profile.

Click the **Binding** button to configure the client MAC address in the profile.

Click the **Delete** button to remove the specified entry.

Click the **Delete Profile** button to remove the specified profile.

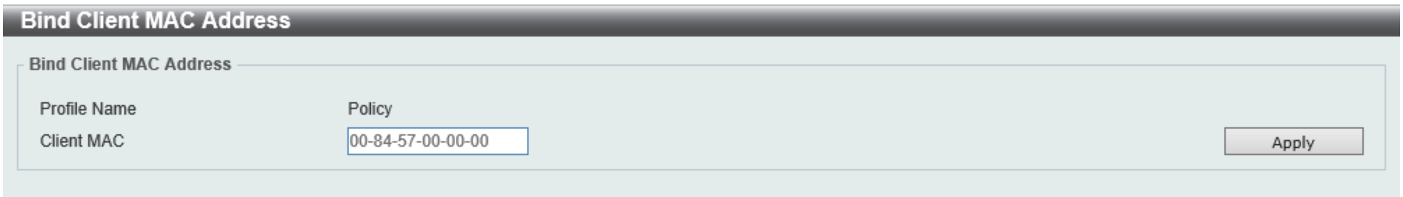
The fields that can be configured in **Log Information** are described below:

Parameter	Description
Log Buffer Entries	Enter the logged buffer entries value here. The range is from 10 to 1024. By default, this value is 32. Select the **Default** option to use the default value.

Click the **Apply** button to accept the changes made.

Click the **Clear Log** button to clear the log.

After clicking the **Binding** button, the following window will appear:



Bind Client MAC Address

Bind Client MAC Address

Profile Name: Policy

Client MAC: 00-84-57-00-00-00

Figure 9-68 Bind Client MAC Address Window

The fields that can be configured are described below:

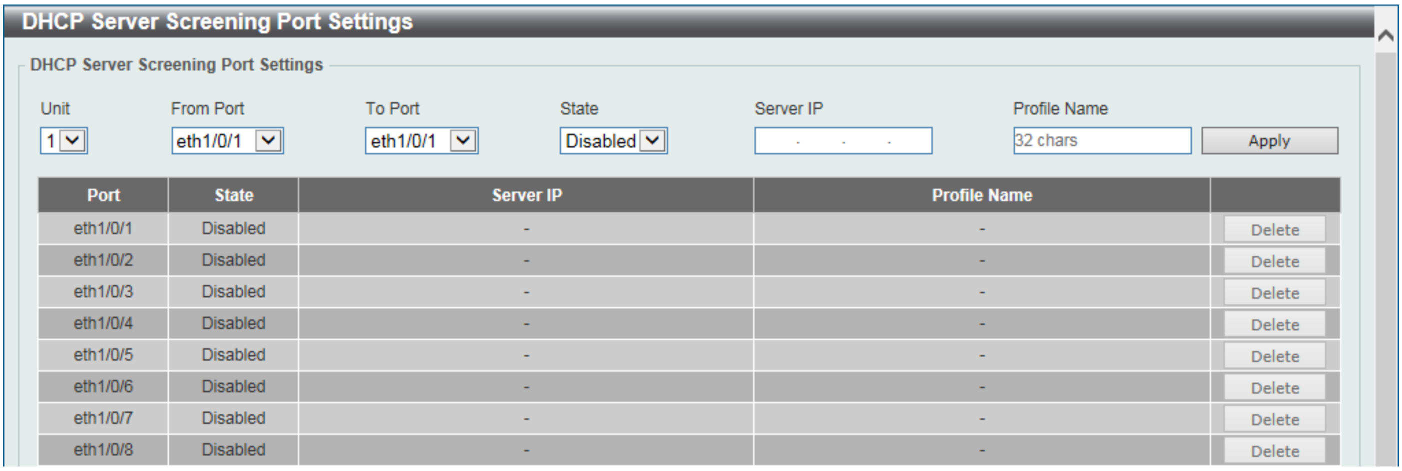
Parameter	Description
Client MAC	Enter the MAC address used here.

Click the **Apply** button to accept the changes made.

DHCP Server Screening Port Settings

This window is used to display and configure the DHCP server screening port settings.

To view the following window, click **Security > DHCP Server Screening > DHCP Server Screening Port Settings**, as shown below:



DHCP Server Screening Port Settings

DHCP Server Screening Port Settings

Unit	From Port	To Port	State	Server IP	Profile Name	
1	eth1/0/1	eth1/0/1	Disabled	. . .	32 chars	Apply

Port	State	Server IP	Profile Name	
eth1/0/1	Disabled	-	-	Delete
eth1/0/2	Disabled	-	-	Delete
eth1/0/3	Disabled	-	-	Delete
eth1/0/4	Disabled	-	-	Delete
eth1/0/5	Disabled	-	-	Delete
eth1/0/6	Disabled	-	-	Delete
eth1/0/7	Disabled	-	-	Delete
eth1/0/8	Disabled	-	-	Delete

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.
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.

Click the **Apply** button to accept the changes made.

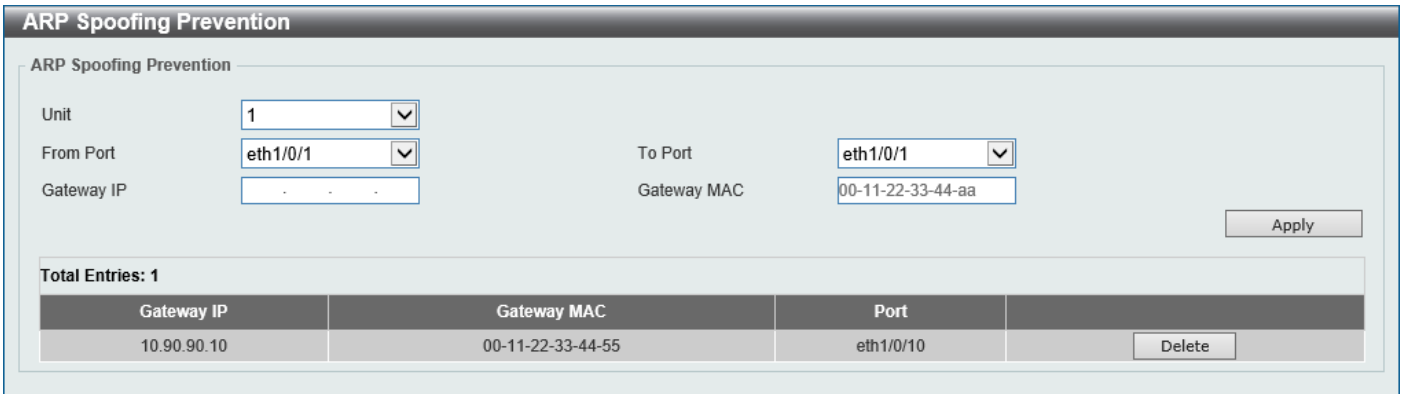
Click the **Delete** button to remove the specified entry.

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:



Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1
Gateway IP: . . .
Gateway MAC: 00-11-22-33-44-aa

Total Entries: 1

Gateway IP	Gateway MAC	Port	
10.90.90.10	00-11-22-33-44-55	eth1/0/10	Delete

Figure 9-70 ARP Spoofing Prevention Window

The fields that can be configured in **ARP Spoofing Prevention** 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.
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.

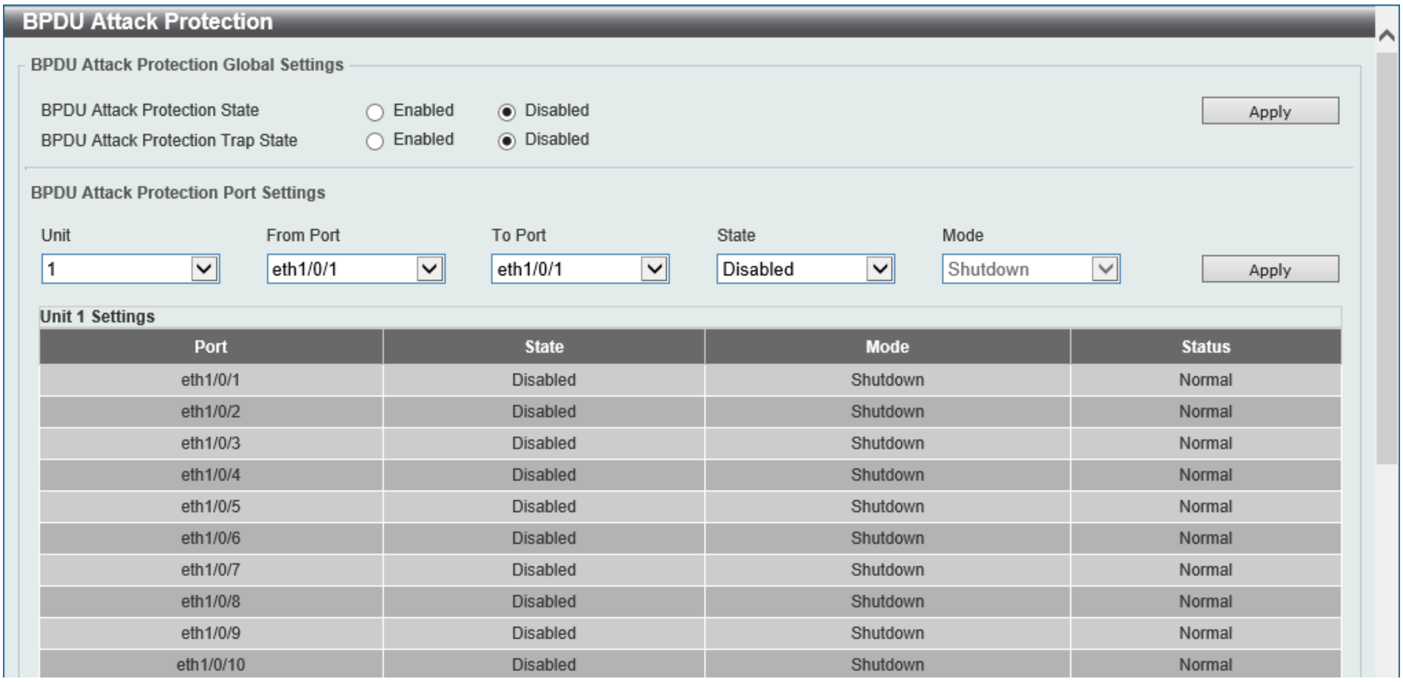
BPDU Attack Protection

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. However, 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:



BPDU Attack Protection

BPDU Attack Protection Global Settings

BPDU Attack Protection State ○ Enabled ● Disabled

BPDU Attack Protection Trap State ○ Enabled ● Disabled

BPDU Attack Protection Port Settings

Unit	From Port	To Port	State	Mode
1	eth1/0/1	eth1/0/1	Disabled	Shutdown

Unit 1 Settings

Port	State	Mode	Status
eth1/0/1	Disabled	Shutdown	Normal
eth1/0/2	Disabled	Shutdown	Normal
eth1/0/3	Disabled	Shutdown	Normal
eth1/0/4	Disabled	Shutdown	Normal
eth1/0/5	Disabled	Shutdown	Normal
eth1/0/6	Disabled	Shutdown	Normal
eth1/0/7	Disabled	Shutdown	Normal
eth1/0/8	Disabled	Shutdown	Normal
eth1/0/9	Disabled	Shutdown	Normal
eth1/0/10	Disabled	Shutdown	Normal

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:

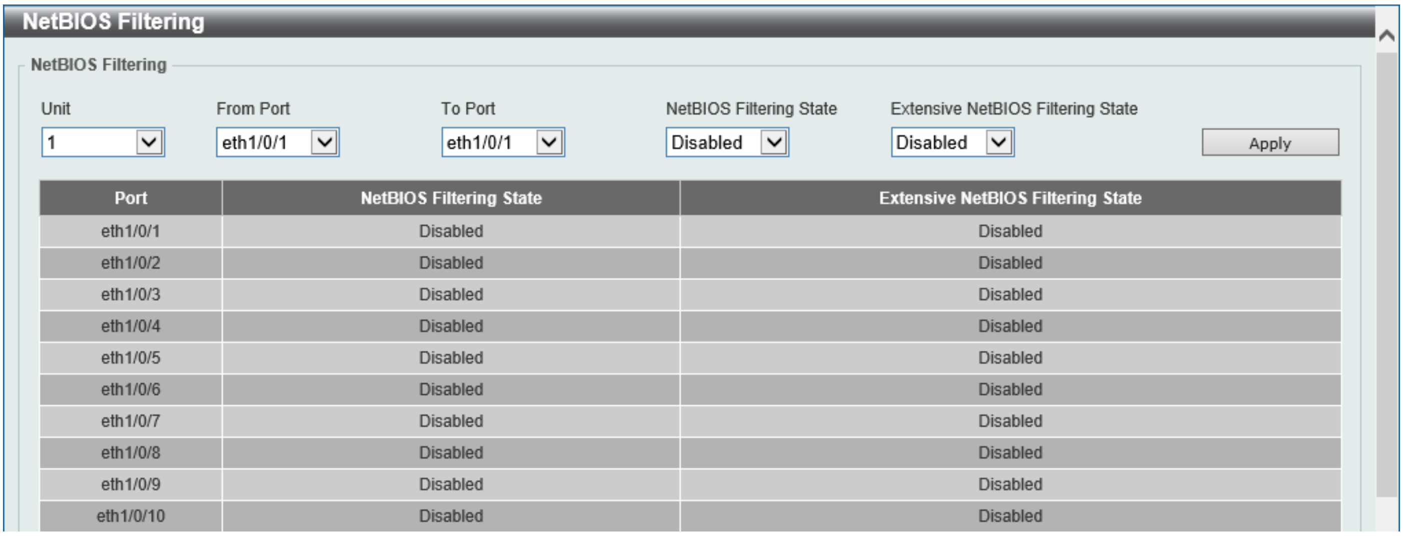
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the BPDU attack protection state on the specified ports.
Mode	Select the BPDU attack protection mode that will be applied to the specified ports. Options to choose from are: • **Drop** - Drop all received BPDU packets when the port enters under attack state. • **Block** - Drop all packets (include BPDU and normal packets) when the port enters under attack state. • **Shutdown** - Shut down the port when the port enters under attack state.

Click the **Apply** button to accept the changes made.

NetBIOS Filtering

This window is used to display and configure the NetBIOS filtering settings.

To view the following window, click **Security > NetBIOS Filtering**, as shown below:



NetBIOS Filtering

NetBIOS Filtering

Unit: 1; From Port: eth1/0/1; To Port: eth1/0/1; NetBIOS Filtering State: Disabled; Extensive NetBIOS Filtering State: Disabled

Port	NetBIOS Filtering State	Extensive NetBIOS Filtering State
eth1/0/1	Disabled	Disabled
eth1/0/2	Disabled	Disabled
eth1/0/3	Disabled	Disabled
eth1/0/4	Disabled	Disabled
eth1/0/5	Disabled	Disabled
eth1/0/6	Disabled	Disabled
eth1/0/7	Disabled	Disabled
eth1/0/8	Disabled	Disabled
eth1/0/9	Disabled	Disabled
eth1/0/10	Disabled	Disabled

Figure 9-72 NetBIOS Filtering 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 range of ports that will be used for this configuration here.
NetBIOS Filtering State	Select to enable or disable the NetBIOS filtering state on the specified ports. This is used to permit or deny NetBIOS packets on physical ports.
Extensive NetBIOS Filtering State	Select to enable or disable the extensive NetBIOS filtering state on the specified ports. This is used to permit or deny NetBIOS packets over 802.3 frames on physical ports.

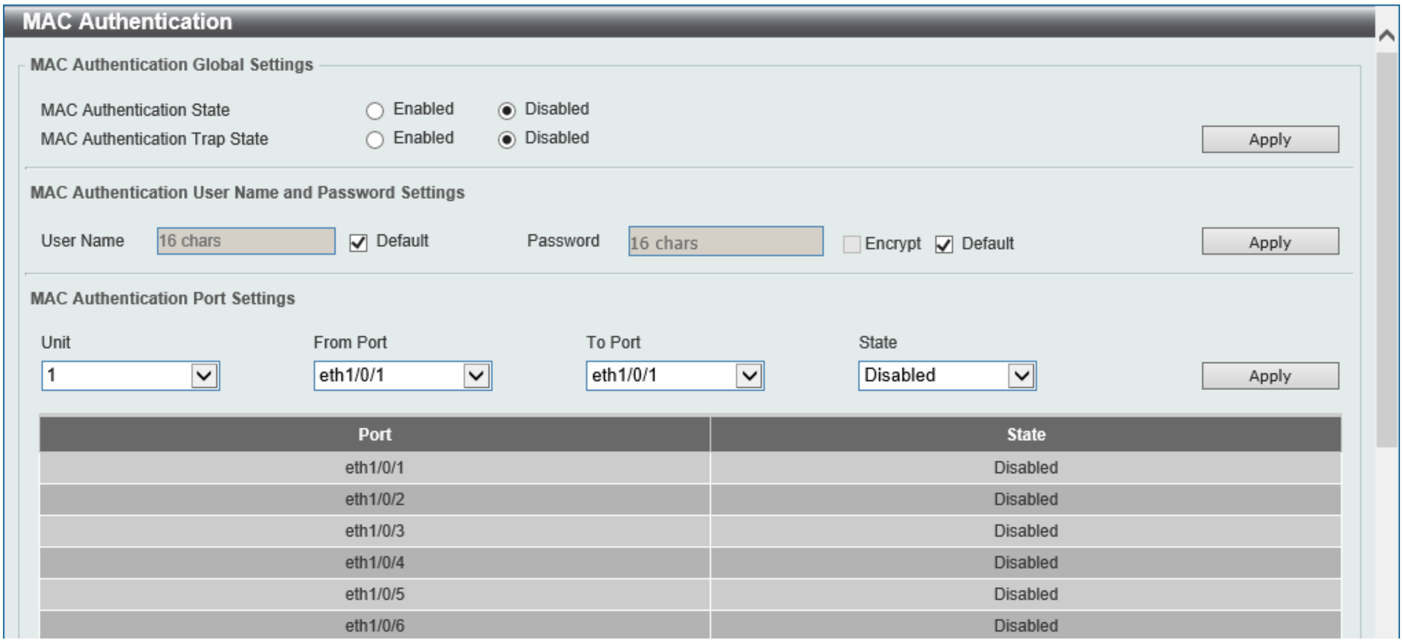
Click the **Apply** button to accept the changes made.

MAC Authentication

This window is used to display and configure the MAC authentication settings. MAC authentication is a feature designed to authenticate a user by MAC address when the user is trying to access the network via the Switch. The

Switch itself can perform the authentication based on a local database or be a RADIUS client and perform the authentication process via the RADIUS protocol with a remote RADIUS server.

To view the following window, click **Security > MAC Authentication**, as shown below:



MAC Authentication

MAC Authentication Global Settings

MAC Authentication State ○ Enabled ● Disabled

MAC Authentication Trap State ○ Enabled ● Disabled

Apply

MAC Authentication User Name and Password Settings

User Name 16 chars ☑ Default Password 16 chars □ Encrypt ☑ Default

Apply

MAC Authentication Port Settings

Unit	From Port	To Port	State
1	eth1/0/1	eth1/0/1	Disabled

Apply

Port	State
eth1/0/1	Disabled
eth1/0/2	Disabled
eth1/0/3	Disabled
eth1/0/4	Disabled
eth1/0/5	Disabled
eth1/0/6	Disabled

Figure 9-73 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. Select the **Default** option to restore the username to the client MAC address here.
Password	Enter the password used for MAC authentication here. Select the **Encrypt** option save this password in the encrypted form. Select 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.
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 launch a pop-up user name and password window to query users. 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. By default, HTTP is used. By default, the HTTP port number is 80, and HTTPS port number is 443.

The following diagram illustrates the basic six steps all parties go through in a successful Web Authentication process:

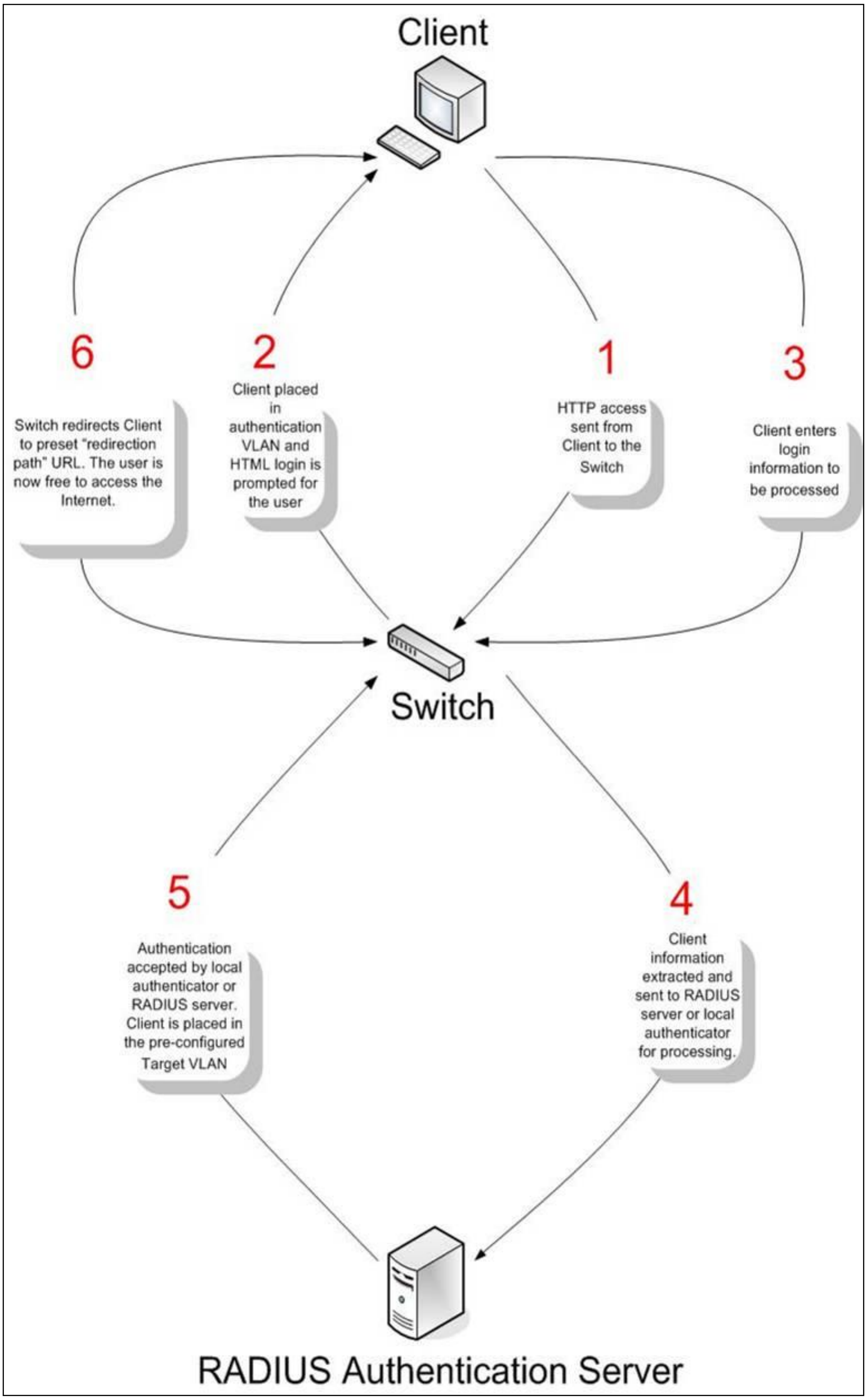

Client
6
Switch redirects Client to preset "redirection path" URL. The user is now free to access the Internet.
2
Client placed in authentication VLAN and HTML login is prompted for the user
1
HTTP access sent from Client to the Switch
3
Client enters login information to be processed
Switch
5
Authentication accepted by local authenticator or RADIUS server. Client is placed in the pre-configured Target VLAN
4
Client information extracted and sent to RADIUS server or local authenticator for processing.
RADIUS Authentication Server

Figure 9-74 RADIUS Authentication Server

Conditions and Limitations

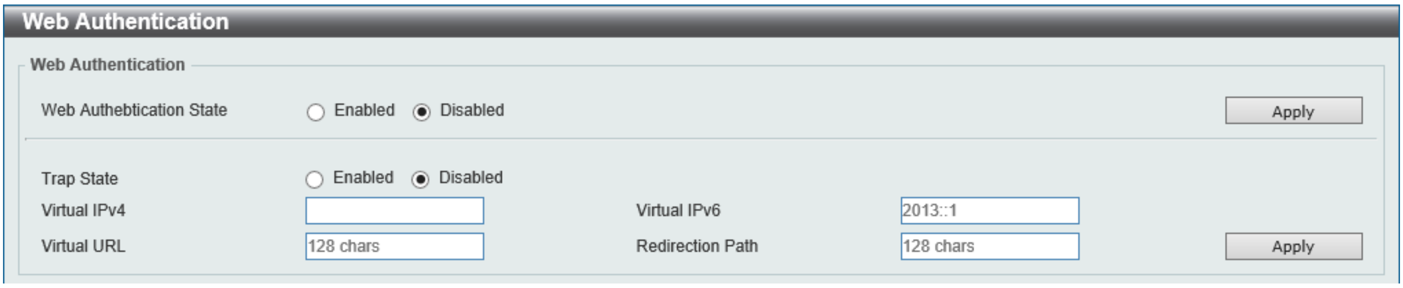
- If the client is utilizing DHCP to attain an IP address, the authenticating VLAN must provide a DHCP server or a DHCP relay function so that client may obtain an IP address.
- Certain functions exist on the Switch that will filter HTTP packets, such as the ACL function. The user needs to be very careful 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:



Web Authentication

Web Authentication

Web Authebtication State ○ Enabled ● Disabled

Trap State ○ Enabled ● Disabled

Virtual IPv4

Virtual IPv6 2013::1

Virtual URL 128 chars

Redirection Path 128 chars

Figure 9-75 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. Therefore, 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 virtual URL used here. This URL can be up to 128 characters long.
Redirection Path	Enter the redirection path here. This path can be up to 128 characters long.

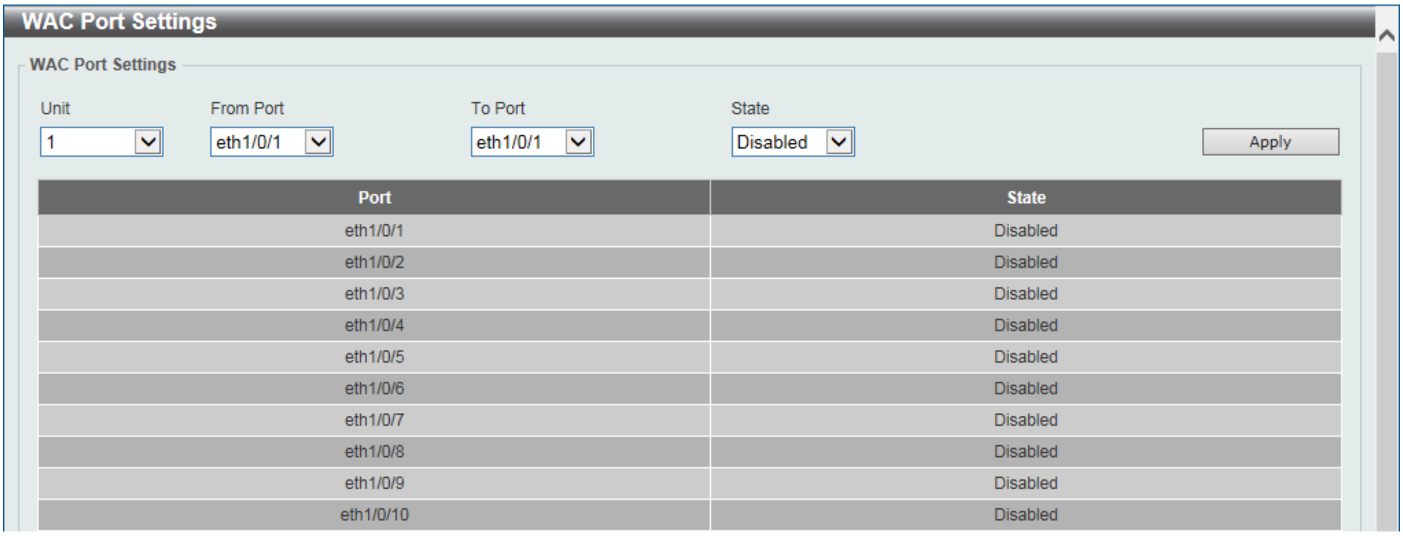
Click the **Apply** button to accept the changes made.

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:



Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1
State: Disabled

Port	State
eth1/0/1	Disabled
eth1/0/2	Disabled
eth1/0/3	Disabled
eth1/0/4	Disabled
eth1/0/5	Disabled
eth1/0/6	Disabled
eth1/0/7	Disabled
eth1/0/8	Disabled
eth1/0/9	Disabled
eth1/0/10	Disabled

Figure 9-76 WAC Port Settings Window

The fields that can be configured are described below:

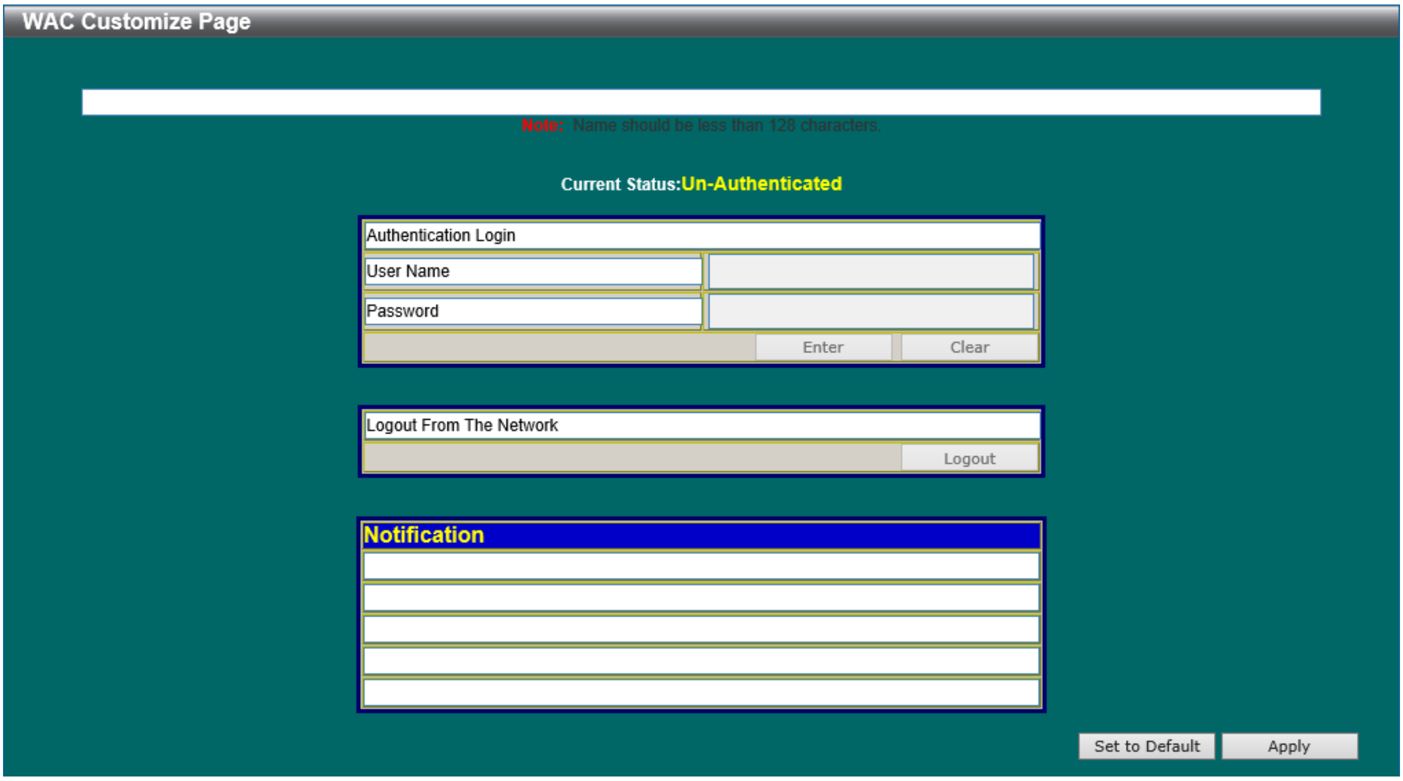
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the WAC feature on the port(s) specified.

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:



WAC Customize Page

Note: Name should be less than 128 characters.

Current Status:Un-Authenticated

Authentication Login

User Name

Password

Logout From The Network

Notification

Figure 9-77 WAC Customize Page Window

The fields that can be configured are described below:

Parameter	Description
Page Title	Enter a custom page title message here. This message can be up to 128 characters long.
Login Window Title	Enter a custom login window title here. This title can be up to 64 characters long.
User Name Title	Enter a custom username title here. This title can be up to 32 characters long.
Password Title	Enter a custom password title here. This title can be up to 32 characters long.
Logout Window Title	Enter a custom logout window title here. This title can be up to 64 characters long.
Notification	Enter additional information to display in the notification area here. This information can be up to 128 characters long for each line. There a 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 made.

Network Access Authentication

Guest VLAN

This window is used to display and configure the network access authentication guest VLAN settings.

To view the following window, click **Security > Network Access Authentication > Guest VLAN**, as shown below:

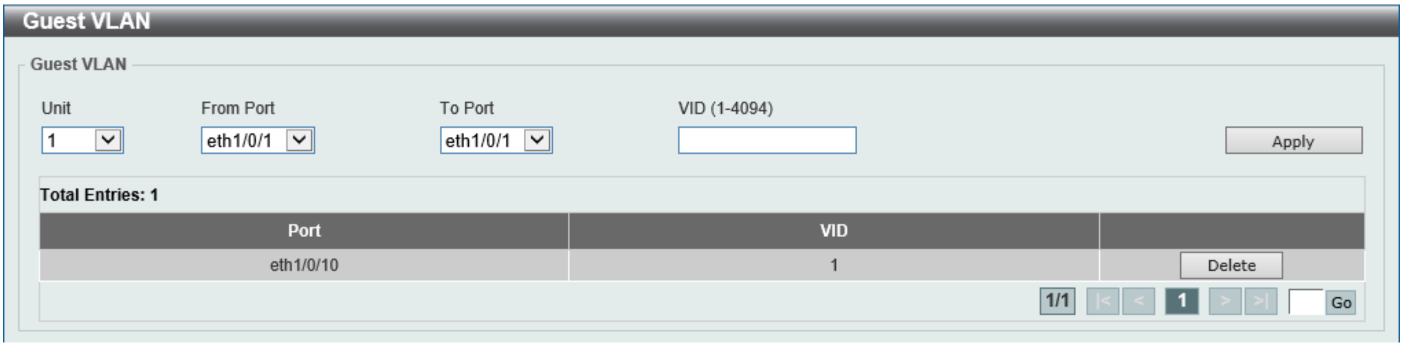


Figure 9-78 Guest VLAN Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
VID	Enter the VLAN ID used here. The range is from 1 to 4094.

Click the **Apply** button to accept the changes made.

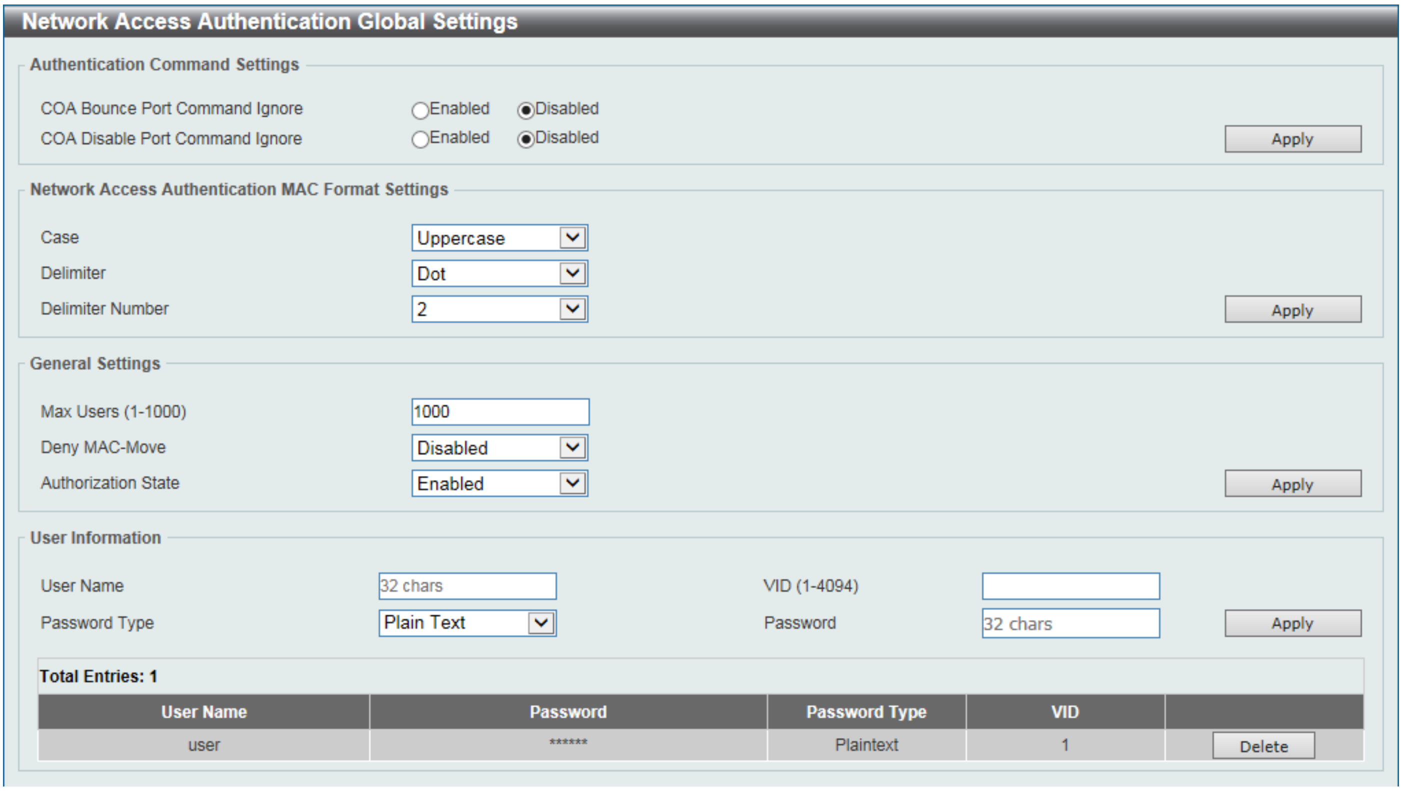
Click the **Delete** button to remove the specified entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Network Access Authentication Global Settings

This window is used to display and configure the global Network Access Authentication settings.

To view the following window, click **Security > Network Access Authentication > Network Access Authentication Global Settings**, as shown below:



Network Access Authentication Global Settings

Authentication Command Settings

COA Bounce Port Command Ignore ○Enabled ●Disabled

COA Disable Port Command Ignore ○Enabled ●Disabled

Network Access Authentication MAC Format Settings

Case: Uppercase

Delimiter: Dot

Delimiter Number: 2

General Settings

Max Users (1-1000): 1000

Deny MAC-Move: Disabled

Authorization State: Enabled

User Information

User Name: 32 chars

VID (1-4094):

Password Type: Plain Text

Password: 32 chars

Total Entries: 1

User Name	Password	Password Type	VID	
user	******	Plaintext	1	Delete

Figure 9-79 Network Access Authentication Global Settings Window

The fields that can be configured in **Authentication Aommand Settings** are described below:

Parameter	Description
COA Bounce Port Command Ignore	Select to enable (ignore) or disable (accept) a RADIUS CoA bounce port command.
COA Disable Port Command Ignore	Select to enable (ignore) or disable (accept) a RADIUS CoA disable port command.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Network Access Authentication MAC Format Settings** are described below:

Parameter	Description
Case	Select the case format that will be used for the network access authentication MAC address here. Options to choose from are **Lowercase** and **Uppercase**.
Delimiter	Select the delimiter that will be used for the network access authentication MAC address here. Options to choose from are **Hyphen**, **Colon**, **Dot**, and **None**.
Delimiter Number	Select the delimiter number option here. Options to choose from are **1**, **2**, and **5**.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **General Settings** are described below:

Parameter	Description
Max Users	Enter the maximum amount of users allowed here. The range is from 1 to 1000. By default, this value is 1000.
Deny MAC-Move	Select to enable or disable the deny MAC-move feature here. This option controls whether to allow authenticated hosts to do roaming across different Switch ports and only controls whether a host, which is authenticated at a port set to the multi-authenticate mode, is allowed to move to another port. If a station is allowed to move, there are two situations. It may either need to be re-authenticated or directly moved to the new port without re-authentication based on the following rule. If the new port has the same authentication configuration as the original port, 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. The range is form 1 to 4094.
Password Type	Select the password type option here. Options to choose from are **Plain Text** and **Encrypted**.
Password	Enter the password used here.

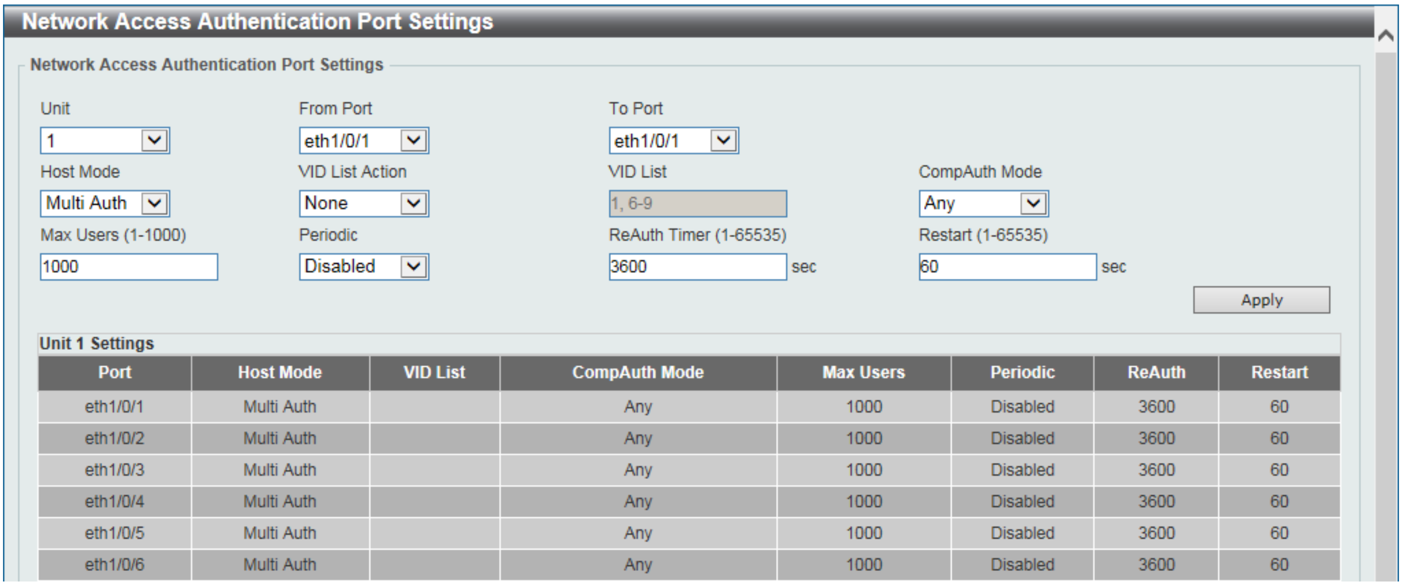
Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Network Access Authentication Port Settings

This window is used to display and configure the network access authentication port settings.

To view the following window, click **Security > Network Access Authentication > Network Access Authentication Port Settings**, as shown below:



Network Access Authentication Port Settings

Network Access Authentication Port Settings

Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1
Host Mode: Multi Auth
VID List Action: None
VID List: 1, 6-9
CompAuth Mode: Any
Max Users (1-1000): 1000
Periodic: Disabled
ReAuth Timer (1-65535): 3600 sec
Restart (1-65535): 60 sec

Unit 1 Settings

Port	Host Mode	VID List	CompAuth Mode	Max Users	Periodic	ReAuth	Restart
eth1/0/1	Multi Auth		Any	1000	Disabled	3600	60
eth1/0/2	Multi Auth		Any	1000	Disabled	3600	60
eth1/0/3	Multi Auth		Any	1000	Disabled	3600	60
eth1/0/4	Multi Auth		Any	1000	Disabled	3600	60
eth1/0/5	Multi Auth		Any	1000	Disabled	3600	60
eth1/0/6	Multi Auth		Any	1000	Disabled	3600	60

Figure 9-80 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.
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 ports here. Options to choose from are: • **Multi Host** - 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. • **Multi Auth** - 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.
VID List Action	Select the VID list action here. Options to choose from are **None**, **Add**, and **Delete**.
VID List	After selecting the **Multi Auth** option as the **Host Mode**, the following parameter is available. 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 here. Options to choose from are: • **Any** - Select to pass if any of the authentication methods passes. If **Any** is selected, MAC-based access control is disabled and 802.1X is enabled, 802.1X authentication will be required. • **MAC-WAC** – Select to verify MAC-based access control first. If the client passes MAC authentication, Web-based access control (WAC) will be verify.

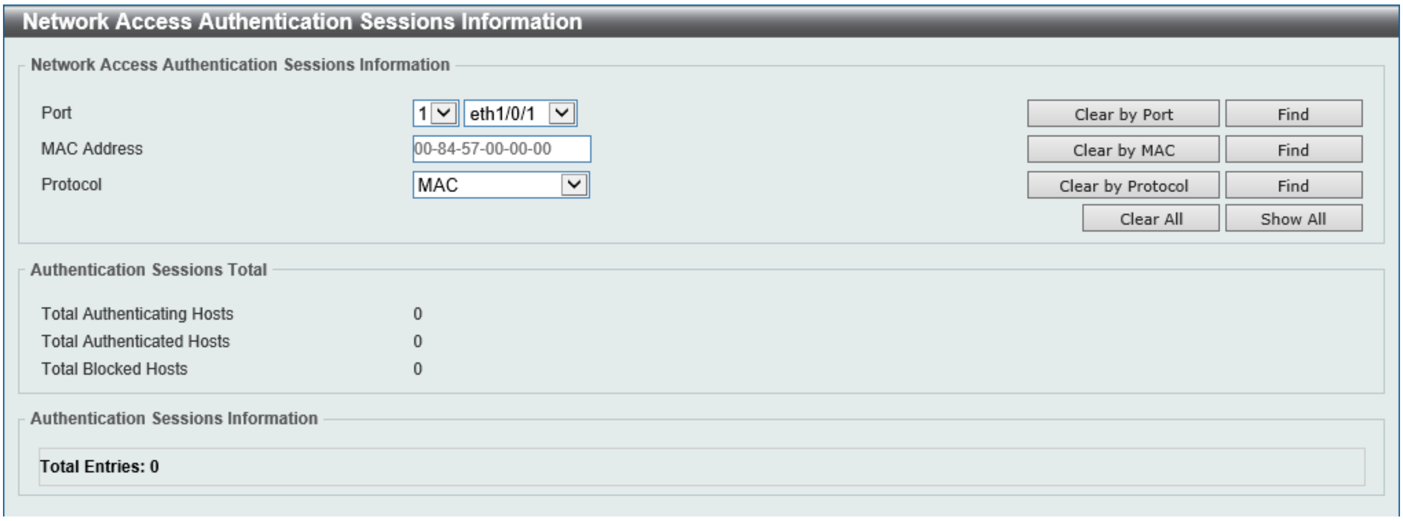
Parameter	Description
	Both authentication methods need to be passed to have a successful authentication.
Max Users	Enter the maximum users value used here. The range is from 1 to 1000.
Periodic	Select to enable or disable periodic re-authentication for the selected port here.
ReAuth Timer	Enter the re-authentication timer value here. The range is from 1 to 65535 seconds. By default, this value is 3600 seconds.
Restart	Enter the restart time value used here. The range is from 1 to 65535 seconds. By default, this value is 60 seconds.

Click the **Apply** button to accept the changes made.

Network Access Authentication Sessions Information

This window is used to view and clear the network access authentication session information.

To view the following window, click **Security > Network Access Authentication > Network Access Authentication Sessions Information**, as shown below:



Network Access Authentication Sessions Information

Network Access Authentication Sessions Information

Port: 1 eth1/0/1

MAC Address: 00-84-57-00-00-00

Protocol: MAC

Authentication Sessions Total

Total Authenticating Hosts	0
Total Authenticated Hosts	0
Total Blocked Hosts	0

Authentication Sessions Information

Total Entries: 0

Figure 9-81 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 are displayed with their respective sub-interfaces (groups):

Protocol Name	Sub-interface (Group)	Description
802.1X	Protocol	Port-based Network Access Control
ARP	Protocol	Address resolution Protocol
DHCP	Protocol	Dynamic Host Configuration Protocol
DNS	Protocol	Domain Name System
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
PPPoE	Protocol	Point-to-point protocol over Ethernet
SNMP	Manage	Simple Network Management Protocol
SSH	Manage	Secure Shell
STP	Protocol	Spanning Tree Protocol
Telnet	Manage	Telnet
TFTP	Manage	Trivial File Transfer Protocol
Web	Manage	Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS)

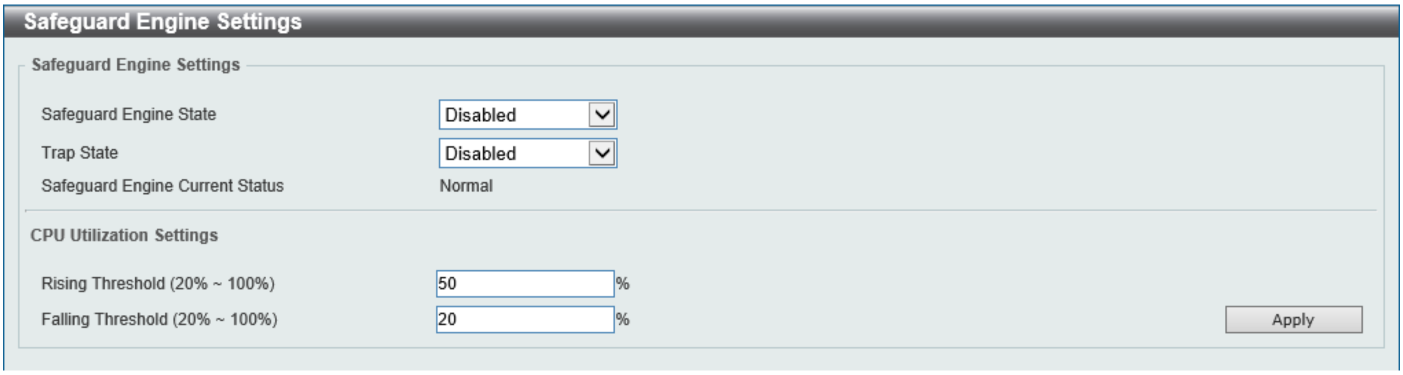
A customized rate limit (in packets per second) can be assigned to the Safeguard Engine's sub-interfaces as a whole or to individual protocols specified by the user in the management interface. Be careful when customizing the rate limit for individual protocols, using this function, as improper rate limits can cause the Switch to process packets abnormally.

NOTE: When Safeguard Engine is enabled, the Switch will allot bandwidth to various traffic flows (ARP, IP) using the FFP (Fast Filter Processor) metering table to control the CPU utilization and limit traffic. This may limit the speed of routing traffic over the network.

Safeguard Engine Settings

This window is used to display and configure the safeguard engine settings.

To view the following window, click **Security > Safeguard Engine > Safeguard Engine Settings**, as shown below:



Safeguard Engine Settings

Safeguard Engine Settings

Safeguard Engine State: Disabled

Trap State: Disabled

Safeguard Engine Current Status: Normal

CPU Utilization Settings

Rising Threshold (20% ~ 100%): 50 %

Falling Threshold (20% ~ 100%): 20 %

Figure 9-82 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:

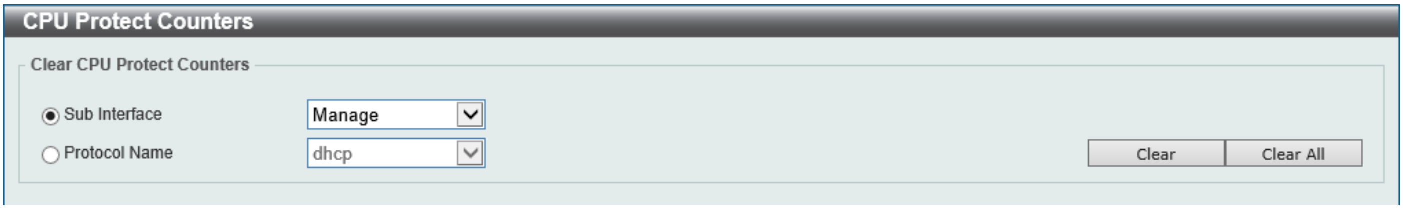
Parameter	Description
Rising Threshold	Enter the rising threshold value here. The range is from 20% to 100%. This value is used to configure the acceptable level of CPU utilization before the Safeguard Engine mechanism is enabled. Once the CPU utilization reaches this percentage level, the Switch will move into Exhausted mode, based on the parameters provided in this window.
Falling Threshold	Enter the falling threshold value here. The range is from 20% to 100%. This value is used to configure the acceptable level of CPU utilization as a percentage, where the Switch leaves the Safeguard Engine state and returns to normal mode.

Click the **Apply** button to accept the changes made.

CPU Protect Counters

This window is used to view and clear the CPU protection counter information.

To view the following window, click **Security > Safeguard Engine > CPU Protect Counters**, as shown below:



CPU Protect Counters

Clear CPU Protect Counters

● Sub Interface: Manage

○ Protocol Name: dhcp

Figure 9-83 CPU Protect Counters Window

The fields that can be configured are described below:

Parameter	Description
Sub Interface	Select the sub-interface option here. Options to choose from are **Manage**, **Protocol**, **Route**, and **All**. This option specifies to clear the CPU protect related counters of sub-interfaces.
Protocol Name	Select the protocol name option here.

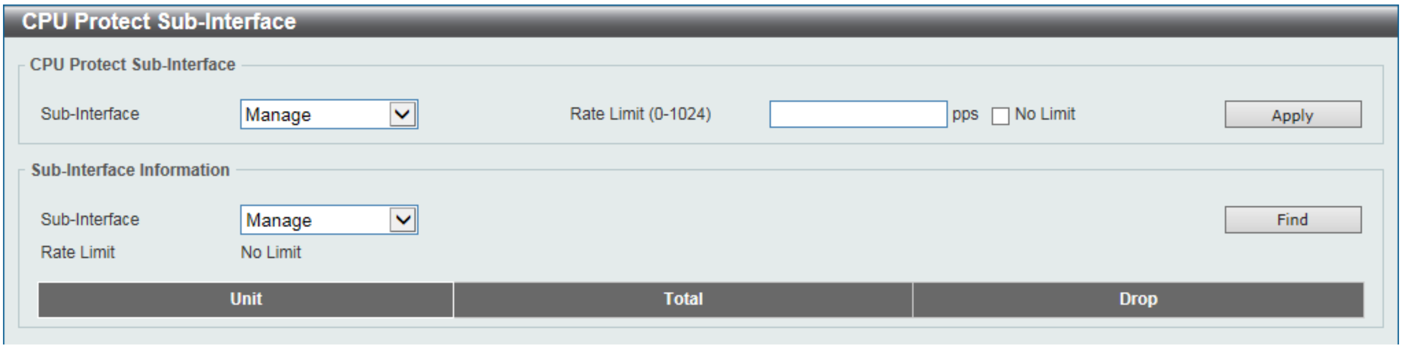
Click the **Clear** button to clear the information based on the selections made.

Click the **Clear All** button to clear all the information in this table.

CPU Protect Sub-Interface

This window is used to display and configure the CPU protection sub-interface settings.

To view the following window, click **Security > Safeguard Engine > CPU Protect Sub-Interface**, as shown below:



CPU Protect Sub-Interface

CPU Protect Sub-Interface

Sub-Interface: Manage

Rate Limit (0-1024): pps □ No Limit

Sub-Interface Information

Sub-Interface: Manage

Rate Limit: No Limit

Unit	Total	Drop

Figure 9-84 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. The range is from 0 to 1024 packets per second. Select 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:

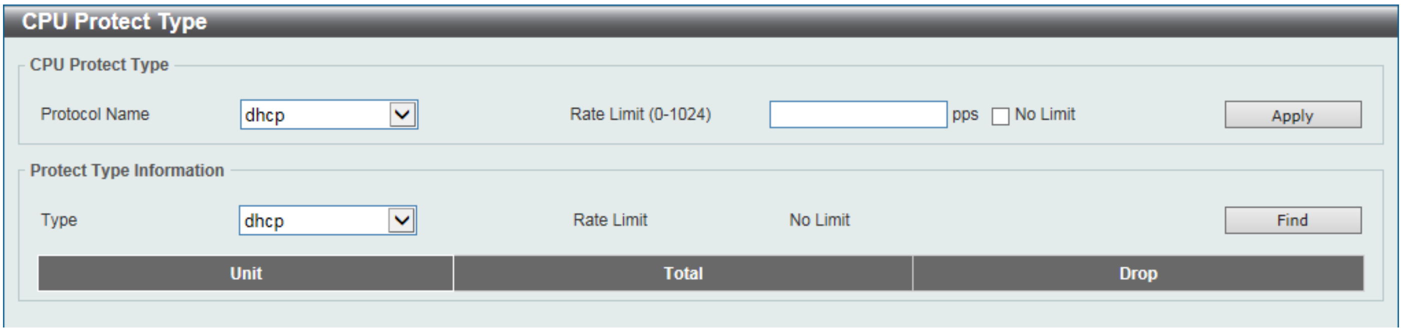


Figure 9-85 CPU Protect Type Window

The fields that can be configured in **CPU Protect Type** are described below:

Parameter	Description
Protocol Name	Select the protocol name option here.
Rate Limit	Enter the rate limit value used here. The range is from 0 to 1024 packets per second. Select 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:

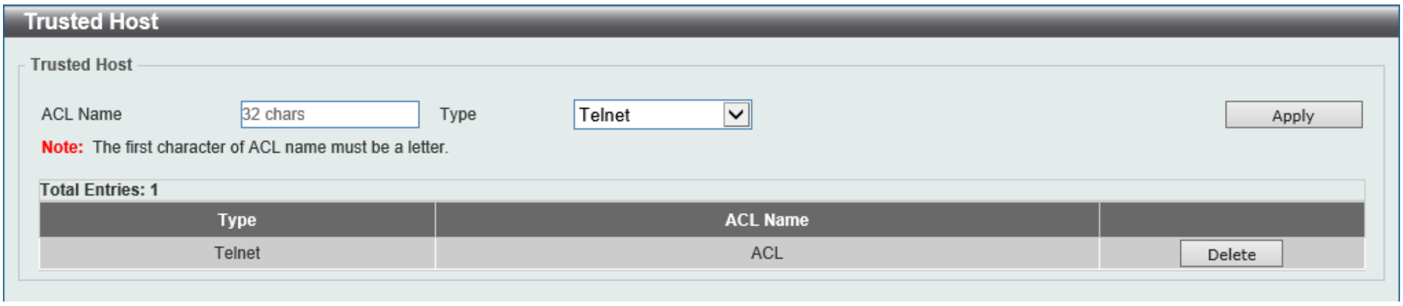
Parameter	Description
Type	Select the protocol type here. After selecting the protocol type, the **Rate Limit** assigned to the protocol type will be displayed. Select the **Unit** option to specify the unit ID of the Switch in the physical stack.

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:



ACL Name: 32 chars   Type: Telnet

Note: The first character of ACL name must be a letter.

Total Entries: 1

Type	ACL Name	
Telnet	ACL	Delete

Figure 9-86 Trusted Host Window

The fields that can be configured are described below:

Parameter	Description
ACL Name	Enter the access class' name here. This name can be up to 32 characters long.
Type	Select the trusted host type here. Options to choose from are **Telnet**, **SSH**, **Ping**, **HTTP**, and **HTTPS**.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

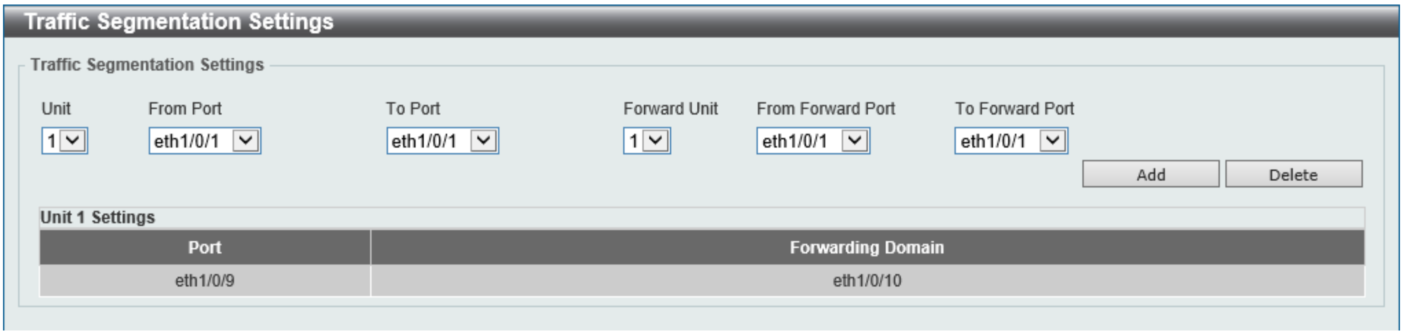
Traffic Segmentation Settings

This window is used to display and configure the traffic segmentation settings. When the traffic segmentation forwarding domain is specified, packets received by the port will be restricted in Layer 2 packet forwarding to interfaces within the domain. When the forwarding domain of a port is empty, Layer 2 forwarding for packets received by the port is not restricted.

The traffic segmentation member list can be comprised of different interface types, for example port and port-channel in the same forwarding domain. If the interfaces specified by the command include a port-channel, all the member ports of this port-channel will be included in the forwarding domain.

If the forwarding domain of an interface is empty, then there is no restriction on Layer 2 forwarding of packets received by the port.

To view the following window, click **Security > Traffic Segmentation Settings**, as shown below:



Unit	From Port	To Port	Forward Unit	From Forward Port	To Forward Port
1	eth1/0/1	eth1/0/1	1	eth1/0/1	eth1/0/1

Unit 1 Settings

Port	Forwarding Domain
eth1/0/9	eth1/0/10

Figure 9-87 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.
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.
From Forward Port ~ To Forward Port	Select the forward port range used for the configuration here.

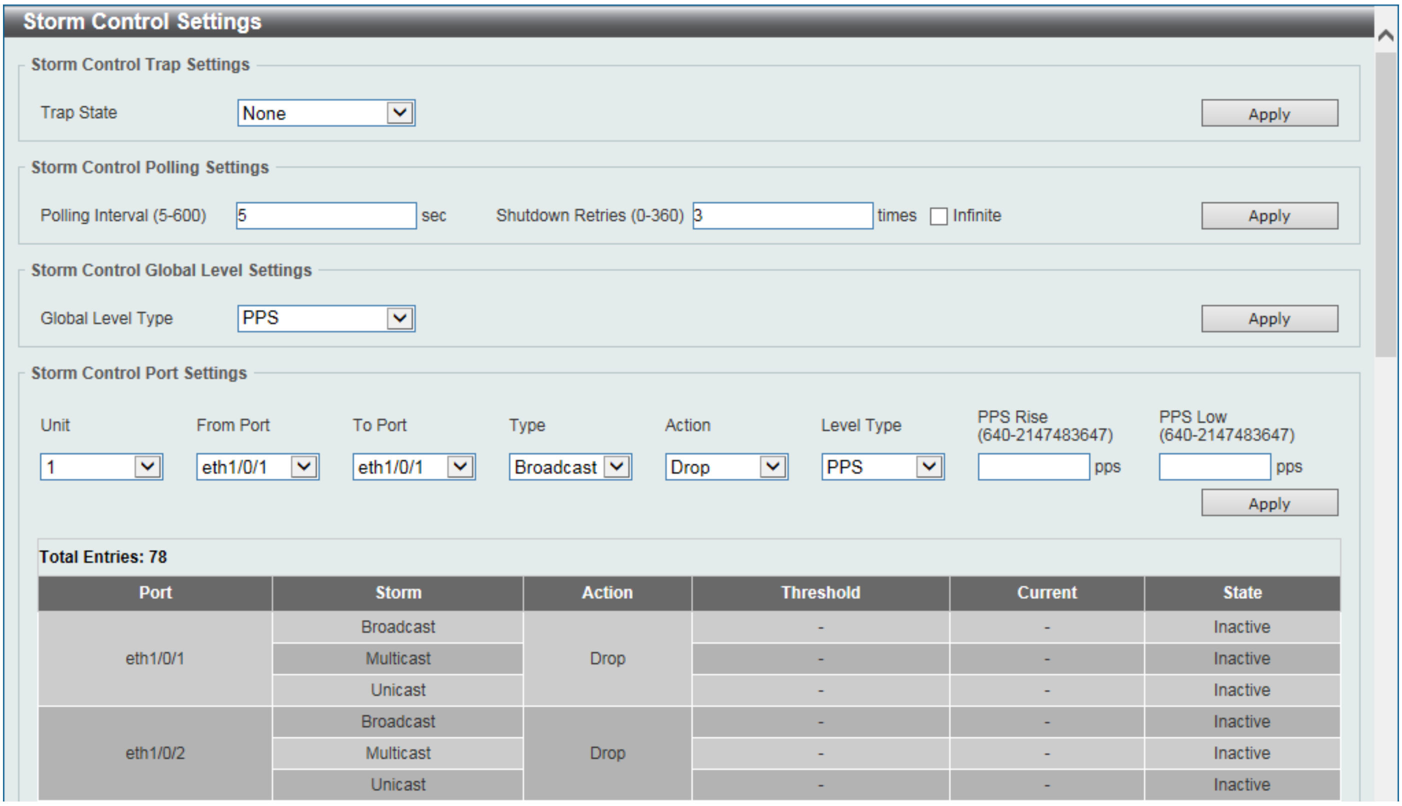
Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove an entry based on the information entered.

Storm Control Settings

This window is used to display and configure the storm control settings.

To view the following window, click **Security > Storm Control Settings**, as shown below:



Storm Control Settings

Storm Control Trap Settings

Trap State: None

Storm Control Polling Settings

Polling Interval (5-600): 5 sec

Shutdown Retries (0-360): 3 times ☐ Infinite

Storm Control Global Level Settings

Global Level Type: PPS

Storm Control Port Settings

Unit	From Port	To Port	Type	Action	Level Type	PPS Rise (640-2147483647)	PPS Low (640-2147483647)
1	eth1/0/1	eth1/0/1	Broadcast	Drop	PPS	pps	pps

Total Entries: 78

Port	Storm	Action	Threshold	Current	State
eth1/0/1	Broadcast	Drop	-	-	Inactive
	Multicast		-	-	Inactive
	Unicast		-	-	Inactive
eth1/0/2	Broadcast	Drop	-	-	Inactive
	Multicast		-	-	Inactive
	Unicast		-	-	Inactive

Figure 9-88 Storm Control Settings Window

The fields that can be configured in **Storm Control Trap Settings** are described below:

Parameter	Description
Trap State	Select the storm control trap option here. Options to choose from are: • **None** - No traps are sent. • **Storm Occur** - A trap notification is sent when a storm event is detected. • **Storm Clear** - A trap notification is sent when a storm event is cleared. • **Both** - A trap notification is sent when a storm event is detected and cleared.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Storm Control Polling Settings** are described below:

Parameter	Description
Polling Interval	Enter the interval value used here. The range is from 5 to 600 seconds. By default, this value is 5 seconds.
Shutdown Retries	Enter the shutdown retries value used here. The range is from 0 to 360. By default, this value is 3. Select 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 Global Level Settings** are described below:

Parameter	Description
Global Level Type	Select the storm control global meter type here. Options to choose from are: • **PPS** - Select the type as packets per second. • **Kbps** - Select the type as the rate of bits per second. • **Percentage** - Select the type as a percentage of the total bandwidth.

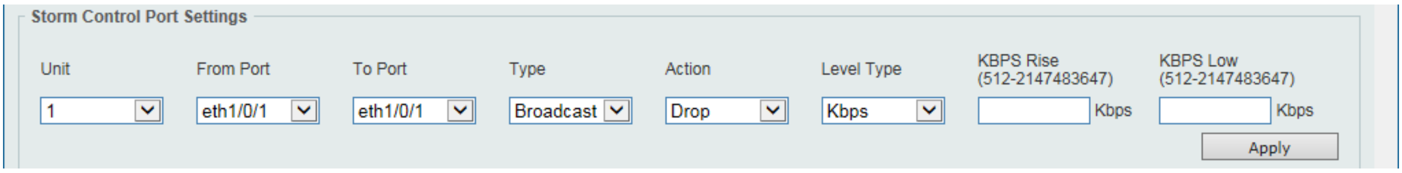
Click the **Apply** button to accept the changes made.

The fields that can be configured in **Storm Control Port Settings** are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
From Port - To Port	Select the appropriate port range used for the configuration here.
Type	Select the type of storm attack that will be controlled here. Options to choose from are **Broadcast**, **Multicast**, and **Unicast**. When the action is configured as the shutdown mode, the unicast refers to both known and unknown unicast packets; that is, if the known and unknown unicast packets hit the specified threshold, the port will be shutdown. Otherwise, unicast refers to unknown unicast packets.
Action	Select the action that will be taken here. Options to choose from are: • **None** - Specifies not to filter the storm packets. • **Shutdown** - Specifies to shut down the port when the value specified for rise threshold is reached. • **Drop** - Specifies to discards packets that exceed the risen threshold.
Level Type	Select the level type option here. Options to choose from are **PPS**, **Kbps**, and **Level**.
PPS Rise	Enter the rise packets per second value here. This option specifies the rise threshold value in packets count per second. The range is from 640 to 2147483647 packets per second.
PPS Low	Enter the low packets per second value here. This option specifies the low threshold value in packets count per second. The range is from 640 to 2147483647 packets per second. By default, this is 80% of the specified **PPS Rise** value.

Click the **Apply** button to accept the changes made.

After selecting the **Kbps** option as the **Level Type**, the following parameters are available.



Storm Control Port Settings

Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1
Type: Broadcast
Action: Drop
Level Type: Kbps
KBPS Rise (512-2147483647): Kbps
KBPS Low (512-2147483647): Kbps

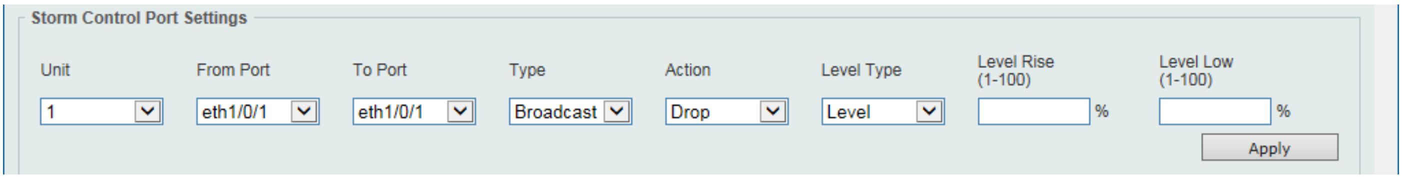
Figure 9-89 Storm Control Settings (Level Type - Kbps) Window

The additional fields that can be configured in **Storm Control Port Settings** are described below:

Parameter	Description
KBPS Rise	Enter the rise KBPS value used here. This option specifies the rise threshold value as a rate of kilobits per second at which traffic is received on the port. The range is from 512 to 2147483647 Kbps.
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. The range is from 512 to 2147483647 Kbps. By default, this is 80% of the specified **KBPS Rise** value.

Click the **Apply** button to accept the changes made.

After selecting the **Level** option as the **Level Type**, the following parameters are available.



Storm Control Port Settings

Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1
Type: Broadcast
Action: Drop
Level Type: Level
Level Rise (1-100): %
Level Low (1-100): %

Figure 9-90 Storm Control Settings (Level Type - Level) Window

The additional fields that can be configured in **Storm Control Port Settings** are described below:

Parameter	Description
Level Rise	Enter the rise level value used here. This option specifies the rise threshold value as a percentage of the total bandwidth per port at which traffic is received on the port. The range is from 0% to 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. The range is from 0% to 100%. By default, this is 80% of the **Level Rise** value.

Click the **Apply** button to accept the changes made.

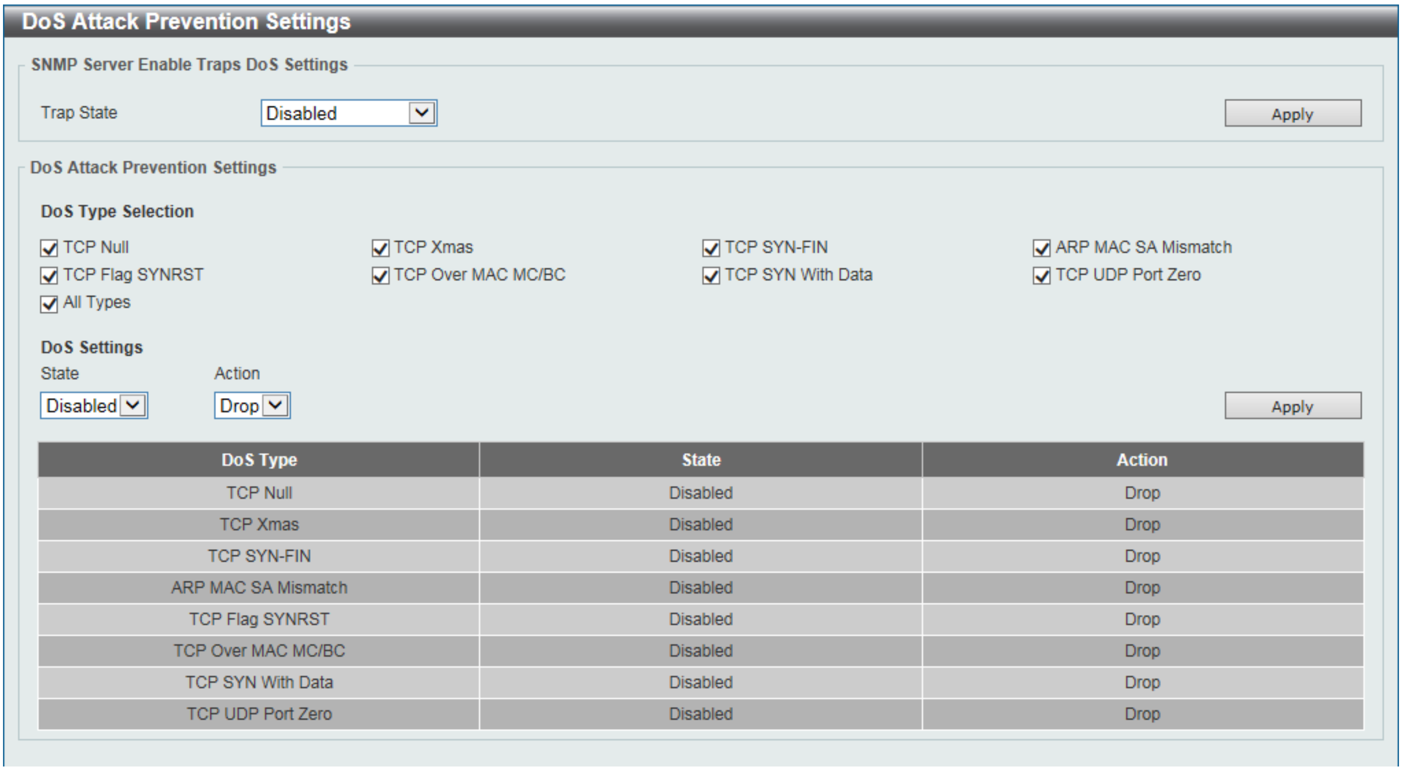
DoS Attack Prevention Settings

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:

- **TCP Null:** This detects and prevents TCP NULL scans. A TCP NULL scan is a scanning technique where the attacker sends packets with no TCP flags set.
- **TCP Xmas:** This detects and prevents TCP Xmas scans. A TCP Xmas scan is a scanning technique where the attacker sends packets with various TCP flags set, making the packet appear "lit up like a Christmas tree."
- **TCP SYN-FIN:** This detects and prevents TCP SYN/FIN scans. This type of scan sends TCP packets with both SYN and FIN flags set.
- **ARP MAC SA Mismatch:** This detects and prevents ARP mismatch attacks. ARP mismatch attacks involve spoofing ARP packets to associate an attacker's MAC address with the IP address of another network node.

- **TCP Flag SYNRST:** This detects and prevents TCP SYN/RST scans. This type of scan sends TCP packets with SYN and RST flags set.
- **TCP Over MAC MC/BC:** This detects and prevents TCP packets over MAC MCBC (multicast MAC addresses). It helps prevent multicast traffic from being used to amplify attacks.
- **TCP SYN With Data:** This detects and prevents TCP SYN/Data scans. This type of scan sends TCP packets with both SYN and data payload.
- **TCP UDP Port Zero:** This detects and prevents TCP/UDP packets with port zero. Packets with port zero may be used in certain types of attacks or as part of reconnaissance efforts.
- **All Types:** All of above types.

To view the following window, click **Security > DoS Attack Prevention Settings**, as shown below:



DoS Attack Prevention Settings

SNMP Server Enable Traps DoS Settings

Trap State: Disabled

DoS Attack Prevention Settings

DoS Type Selection

☑ TCP Null ☑ TCP Xmas ☑ TCP SYN-FIN ☑ ARP MAC SA Mismatch
☑ TCP Flag SYNRST ☑ TCP Over MAC MC/BC ☑ TCP SYN With Data ☑ TCP UDP Port Zero
☑ All Types

DoS Settings

State: Disabled
Action: Drop

DoS Type	State	Action
TCP Null	Disabled	Drop
TCP Xmas	Disabled	Drop
TCP SYN-FIN	Disabled	Drop
ARP MAC SA Mismatch	Disabled	Drop
TCP Flag SYNRST	Disabled	Drop
TCP Over MAC MC/BC	Disabled	Drop
TCP SYN With Data	Disabled	Drop
TCP UDP Port Zero	Disabled	Drop

Figure 9-91 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	Select the DoS type option that will be prevented here.
State	Select to enable or disable the global DoS attack prevention state here.
Action	Select the action that will be taken when the DoS attack was detected here. The only option to select here is **Drop**.

Click the **Apply** button to accept the changes made.

SSH

Secure Shell (SSH) is a program allowing secure remote login and secure network services over an insecure network that allows a secure login to remote host computers, a safe method of executing commands on a remote end node, and will provide secure encrypted and authenticated communication between two non-trusted hosts. SSH, with its array of unmatched security features is an essential tool in today's networking environment. It is a powerful guardian against numerous existing security hazards that now threaten network communications.

The steps required to use the SSH protocol for secure communication between a remote PC (the SSH client) and the Switch (the SSH server) are as follows:

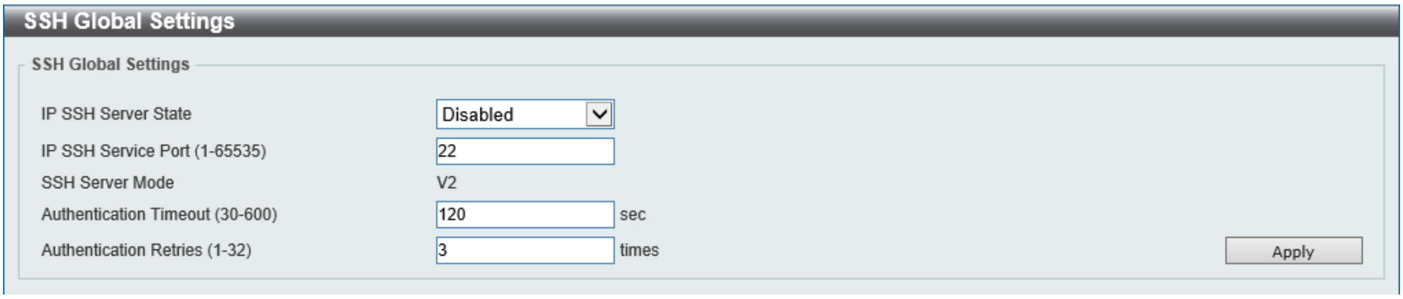
- Create a user account with admin-level access using the User Accounts window. This is identical to creating any other admin-level User Account on the Switch, including specifying a password. This password is used to logon to the Switch, once a secure communication path has been established using the SSH protocol.
- Configure the User Account to use a specified authorization method to identify users that are allowed to establish SSH connections with the Switch using the SSH User Authentication Mode window. There are three choices as to the method SSH will use to authorize the user, which are Host Based, Password, and Public Key.
- Configure the encryption algorithm that SSH will use to encrypt and decrypt messages sent between the SSH client and the SSH server, using the SSH Authentication Method and Algorithm Settings window.
- Finally, enable SSH on the Switch using the SSH Configuration window.

After completing the preceding steps, a SSH Client on a remote PC can be configured to manage the Switch using a secure, in band connection.

SSH Global Settings

This window is used to display and configure the global SSH settings.

To view the following window, click **Security > SSH > SSH Global Settings**, as shown below:



SSH Global Settings

SSH Global Settings

IP SSH Server State: Disabled

IP SSH Service Port (1-65535): 22

SSH Server Mode: V2

Authentication Timeout (30-600): 120 sec

Authentication Retries (1-32): 3 times

Figure 9-92 SSH Global Settings Window

The fields that can be configured are described below:

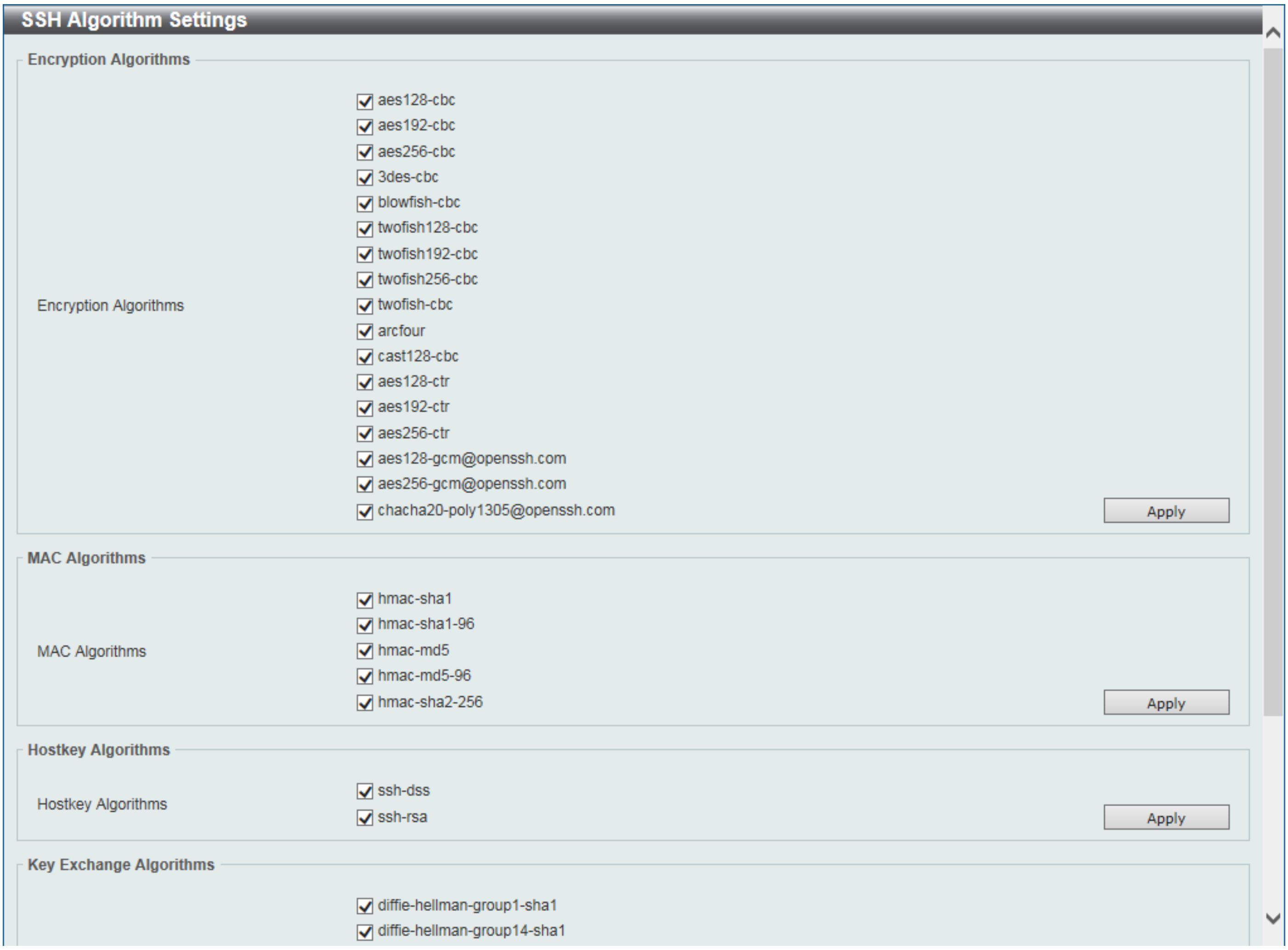
Parameter	Description
IP SSH Server State	Select to enable or disable the global SSH server state.
IP SSH Service Port	Enter the SSH service port number used here. The range is from 1 to 65535. By default, this value is 22.
Authentication Timeout	Enter the authentication timeout value here. The range is from 30 to 600 seconds. By default, this value is 120 seconds.
Authentication Retries	Enter the authentication retries value here. The range is from 1 to 32. By default, this value is 3.

Click the **Apply** button to accept the changes made.

SSH Algorithm Settings

This window is used to display and configure the SSH algorithm settings.

To view the following window, click **Security > SSH > SSH Algorithm Settings**, as shown below:



SSH Algorithm Settings

Encryption Algorithms

Encryption Algorithms
☑ aes128-cbc
☑ aes192-cbc
☑ aes256-cbc
☑ 3des-cbc
☑ blowfish-cbc
☑ twofish128-cbc
☑ twofish192-cbc
☑ twofish256-cbc
☑ twofish-cbc
☑ arcfour
☑ cast128-cbc
☑ aes128-ctr
☑ aes192-ctr
☑ aes256-ctr
☑ aes128-gcm@openssh.com
☑ aes256-gcm@openssh.com
☑ chacha20-poly1305@openssh.com

MAC Algorithms

MAC Algorithms
☑ hmac-sha1
☑ hmac-sha1-96
☑ hmac-md5
☑ hmac-md5-96
☑ hmac-sha2-256

Hostkey Algorithms

Hostkey Algorithms
☑ ssh-dss
☑ ssh-rsa

Key Exchange Algorithms

☑ diffie-hellman-group1-sha1
☑ diffie-hellman-group14-sha1

Figure 9-93 SSH Algorithm Settings Window

The fields that can be configured are described below:

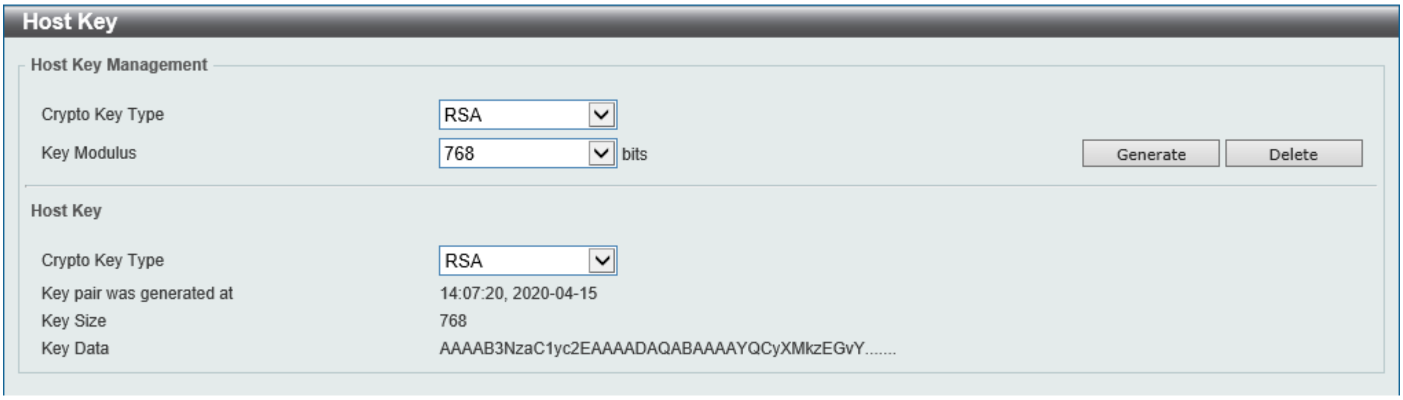
Parameter	Description
Encryption Algorithms	Select to define the allowed encryption key algorithm list in the SSH server.
MAC Algorithms	Select to define the allowed Message Authentication Code (MAC) key algorithm list in the SSH server.
Hostkey Algorithms	Select to define the allowed host key algorithm list in the SSH server.
Key Exchange Algorithms	Select to define the allowed key exchange algorithm list in the SSH server.

Click the **Apply** button to accept the changes made.

Host Key

This window is used to view and generate the SSH host key.

To view the following window, click **Security > SSH > Host Key**, as shown below:



Host Key

Host Key Management

Crypto Key Type: RSA

Key Modulus: 768 bits

Host Key

Crypto Key Type: RSA

Key pair was generated at: 14:07:20, 2020-04-15

Key Size: 768

Key Data: AAAAB3NzaC1yc2EAAAADAQABAAAAYQCyXMkzEGvY.......

Figure 9-94 Host Key Window

The fields that can be configured in **Host Key Management** are described below:

Parameter	Description
Crypto Key Type	Select the crypto key type used here. Options to choose from are the Rivest Shamir Adleman (**RSA**) key type and the Digital Signature Algorithm (**DSA**) key type.
Key Modulus	Select the key modulus value here. Options to choose from are **512**, **768**, **1024**, and **2048** bit.

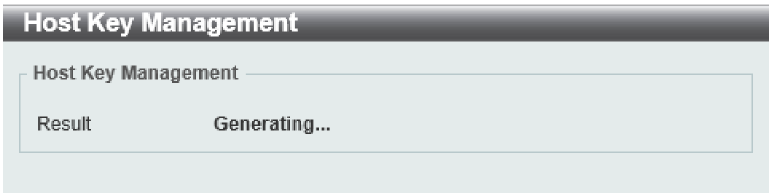
Click the **Generate** button to generate a host key based on the selections made.

Click the **Delete** button to remove a host key based on the selections made.

The fields that can be configured in **Host Key** are described below:

Parameter	Description
Crypto Key Type	Select the crypto key type used here. Options to choose from are the Rivest Shamir Adleman (**RSA**) key type and the Digital Signature Algorithm (**DSA**) key type.

After clicking the **Generate** button, the following window will appear:



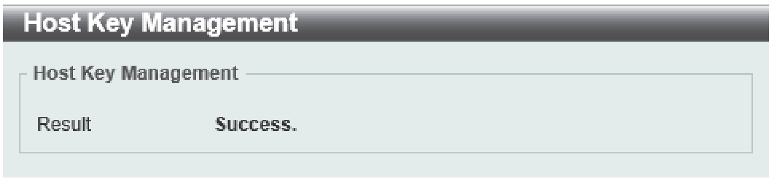
Host Key Management

Host Key Management

Result: Generating...

Figure 9-95 Host Key (Generating) Window

After the key was successfully generated, the following window will appear.



Host Key Management

Host Key Management

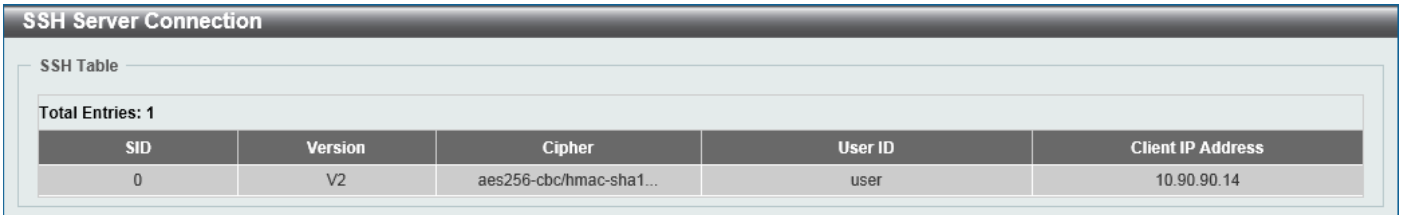
Result: Success.

Figure 9-96 Host Key (Generating, Success) Window

SSH Server Connection

This window is used to view the SSH server connections table.

To view the following window, click **Security > SSH > SSH Server Connection**, as shown below:



SSH Server Connection

SSH Table

Total Entries: 1

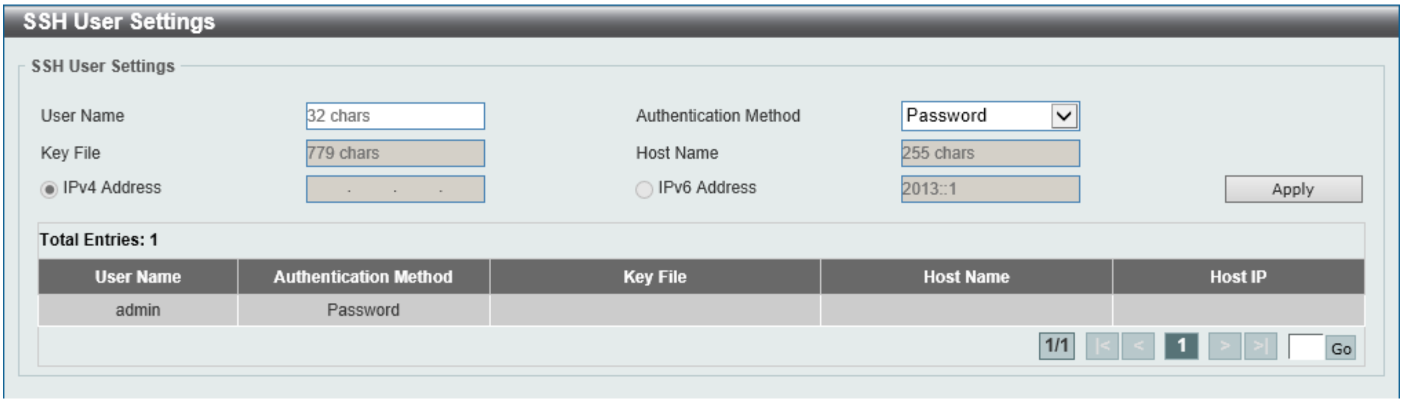
SID	Version	Cipher	User ID	Client IP Address
0	V2	aes256-cbc/hmac-sha1...	user	10.90.90.14

Figure 9-97 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:



SSH User Settings

SSH User Settings

User Name	32 chars	Authentication Method	Password	
Key File	779 chars	Host Name	255 chars	
● IPv4 Address	. . .	○ IPv6 Address	2013::1	Apply

Total Entries: 1

User Name	Authentication Method	Key File	Host Name	Host IP
admin	Password			

Figure 9-98 SSH User Settings Window

The fields that can be configured are described below:

Parameter	Description
User Name	Enter the SSH user's username used here. This name can be up to 32 characters long.
Authentication Method	Select the authentication methods used here. Options to choose from are **Password**, **Public Key**, and **Host-based**.
Key File	After selecting the **Public Key** or **Host-based** option as the **Authentication Method**, enter the public key here.
Host Name	After selecting the **Host-based** option as the **Authentication Method**, enter the host name here.
IPv4 Address	After selecting the **Host-based** option as the **Authentication Method**, select and enter the IPv4 address here.
IPv6 Address	After selecting the **Host-based** option as the **Authentication Method**, select and enter the IPv6 address here.

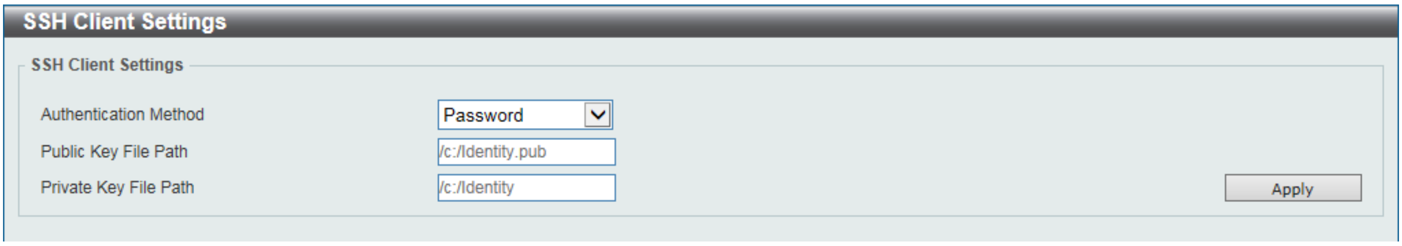
Click the **Apply** button to accept the changes made.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

SSH Client Settings

This window is used to display and configure the SSH client settings.

To view the following window, click **Security > SSH > SSH Client Settings**, as shown below:



SSH Client Settings

SSH Client Settings

Authentication Method: Password

Public Key File Path: /c:/Identity.pub

Private Key File Path: /c:/Identity

Figure 9-99 SSH Client Settings Window

The fields that can be configured are described below:

Parameter	Description
Authentication Method	Select the authentication methods used here. Options to choose from are: • **Password** - Select to use the password authentication method for this user account. This is the default authentication method. • **Public Key** - Select to use the public key authentication method for this user account. Enter the URL of a local file to be used as the public key of this user.
Public Key File Path	Enter the path and filename of the local file to be used as the public key here.
Private Key File Path	Enter the path of the local file to be used as the private key here.

Click the **Apply** button to accept the changes made.

SSL

Secure Sockets Layer (SSL) is a security feature that will provide a secure communication path between a server and client through the use of authentication, digital signatures, and encryption. These security functions are implemented through the use of a cipher suite, which is a security string that determines the exact cryptographic parameters, specific encryption algorithms, and key sizes to be used for an authentication session and consists of three levels:

- **Key Exchange:** The first part of the cipher suite string specifies the public key algorithm to be used. This Switch utilizes the Rivest Shamir Adleman (RSA) public key algorithm and the Digital Signature Algorithm (DSA), specified here as the DHE DSS Diffie-Hellman (DHE) public key algorithm. This is the first authentication process between client and server as they "exchange keys" in looking for a match and therefore authentication to be accepted to negotiate encryptions on the following level.
- **Encryption:** The second part of the cipher suite that includes the encryption used for encrypting the messages sent between client and host. The Switch supports two types of cryptology algorithms:
    - **Stream Ciphers** - There are two types of stream ciphers on the Switch, RC4 with 40-bit keys, and RC4 with 128-bit keys. These keys are used to encrypt messages and need to be consistent between client and host for optimal use.
    - **CBC Block Ciphers** - CBC refers to Cipher Block Chaining, which means that a portion of the previously encrypted block of encrypted text is used in the encryption of the current block. The Switch supports the 3DES EDE encryption code defined by the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) to create the encrypted text.
- **Hash Algorithm:** This part of the cipher suite allows the user to choose a message digest function, 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 three hash algorithms, MD5 (Message Digest 5), SHA (Secure Hash Algorithm), and SHA256.

These three parameters are uniquely assembled in four choices on the Switch to create a three-layered encryption code for secure communication between the server and the client. The user may implement any one or combination of the cipher suites available, yet different cipher suites will affect the security level and the performance of the secured connection. The information included in the cipher suites is not included with the Switch and requires downloading from a third source in a file form called a certificate. This function of the Switch cannot be executed without the presence and implementation of the certificate file and can be downloaded to the Switch by utilizing a TFTP server or the Switch file system. The Switch supports TLS 1.0, TLS 1.1, and TLS 1.2. Other versions of SSL may not be compatible with this Switch and may cause problems upon authentication and transfer of messages from client to server.

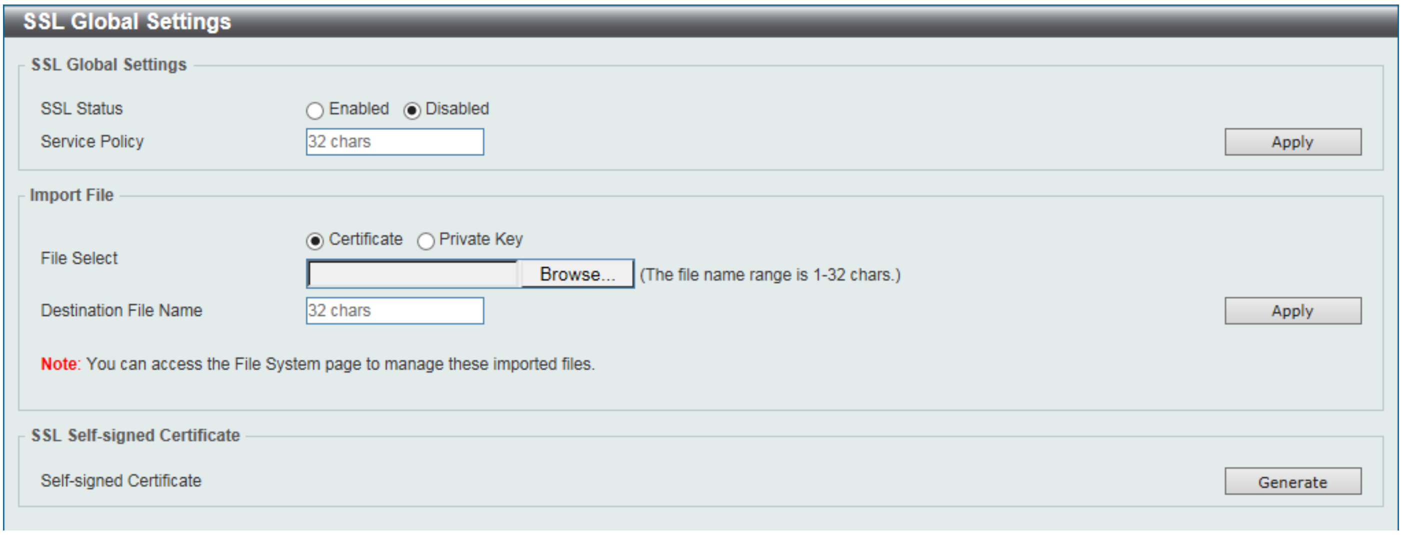
When the SSL function has been enabled, the web will become disabled. To manage the Switch through the web-based management while utilizing the SSL function, the web browser must support SSL encryption and the header of the URL must begin with https:// (Ex. https://xx.xx.xx.xx). Any other method will result in an error and no access can be authorized for the web-based management.

Users can download a certificate file for the SSL function on the Switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the client must have consistent certificate files for optimal use of the SSL function. Currently, the Switch comes with a certificate pre-loaded though the user may need to download more, depending on user circumstances.

SSL Global Settings

This window is used to display and configure the global SSL settings.

To view the following window, click **Security > SSL > SSL Global Settings**, as shown below:



SSL Global Settings

SSL Global Settings

SSL Status ○ Enabled ● Disabled

Service Policy 32 chars

Import File

File Select ● Certificate ○ Private Key

(The file name range is 1-32 chars.)

Destination File Name 32 chars

Note: You can access the File System page to manage these imported files.

SSL Self-signed Certificate

Self-signed Certificate

Figure 9-100 SSL Global Settings Window

The fields that can be configured in **SSL Global Settings** are described below:

Parameter	Description
SSL Status	Select to enable or disable the global SSL status here.
Service Policy	Enter the service policy name here. This name can be up to 32 characters long.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **Import File** are described below:

Parameter	Description
File Select	Select the file type that will be loaded here. Options to choose from are **Certificate** and **Private Key**. After selecting the file type, browse to the appropriate file, located on the local computer, by pressing the **Browse** button.
Destination File Name	Enter the destination file name used here. This name can be up to 32 characters long.

Click the **Apply** button to accept the changes made.

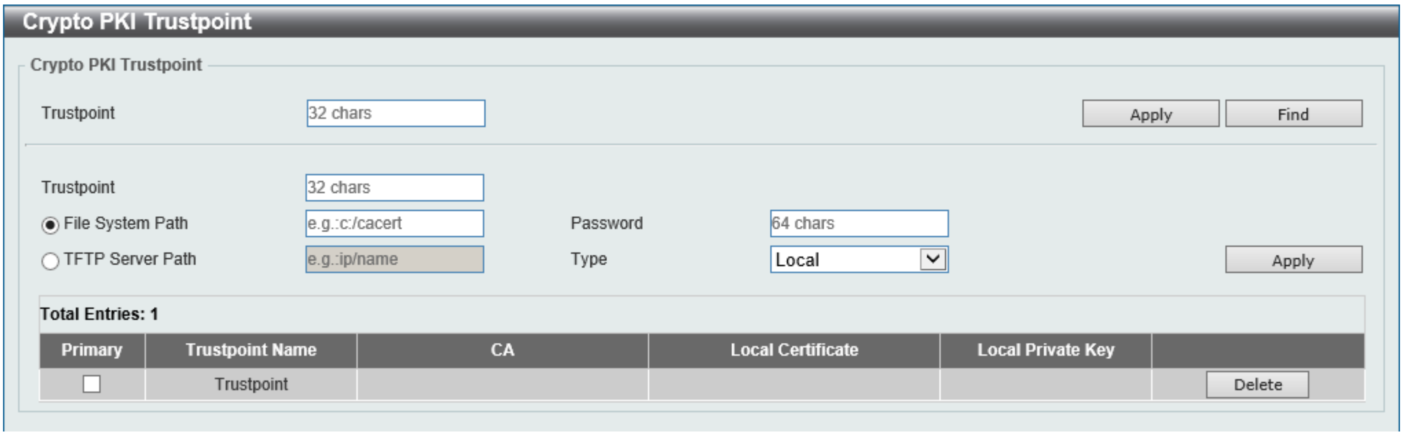
Click the **Generate** button in the **SSL-Self-signed Certificate** section to generate a new self-signed certificate, regardless if there is a built-in self-signed certificate or not. The certificate generated does not affect the user-downloaded certificates.

NOTE: The SSL self-signed certificate only supports self-signature RSA certificates with a key length of 2048 bits.

Crypto PKI Trustpoint

This window is used to display and configure the crypto PKI trust point settings.

To view the following window, click **Security > SSL > Crypto PKI Trustpoint**, as shown below:



Crypto PKI Trustpoint

Crypto PKI Trustpoint

Trustpoint: 32 chars

Trustpoint: 32 chars

● File System Path: e.g.:c:/cacert

Password: 64 chars

○ TFTP Server Path: e.g.:ip/name

Type: Local

Total Entries: 1

Primary	Trustpoint Name	CA	Local Certificate	Local Private Key	
□	Trustpoint				Delete

Figure 9-101 Crypto PKI Trustpoint Window

The fields that can be configured are described below:

Parameter	Description
Trustpoint	Enter the name of the trust-point that is associated with the imported certificates and key pairs here. This name can be up to 32 characters long.
File System Path	Enter the file system path for certificates and key pairs here.
Password	Enter the encrypted password phrase that is used to undo encryption when the private keys are imported here. The password phrase is a string of up to 64 characters. If the password phrase is not specified, the NULL string will be used.
TFTP Server Path	Enter the TFTP server path here.
Type	Select the type of certificate that will be imported here. Options to choose from are: • **Both** - Specifies to import the CA certificate, local certificate, and key pairs. • **CA** - Specifies to import the CA certificate only.

Parameter	Description
	• **Local** - Specifies to import local certificate and key pairs only.

Click the **Apply** button to accept the changes made.

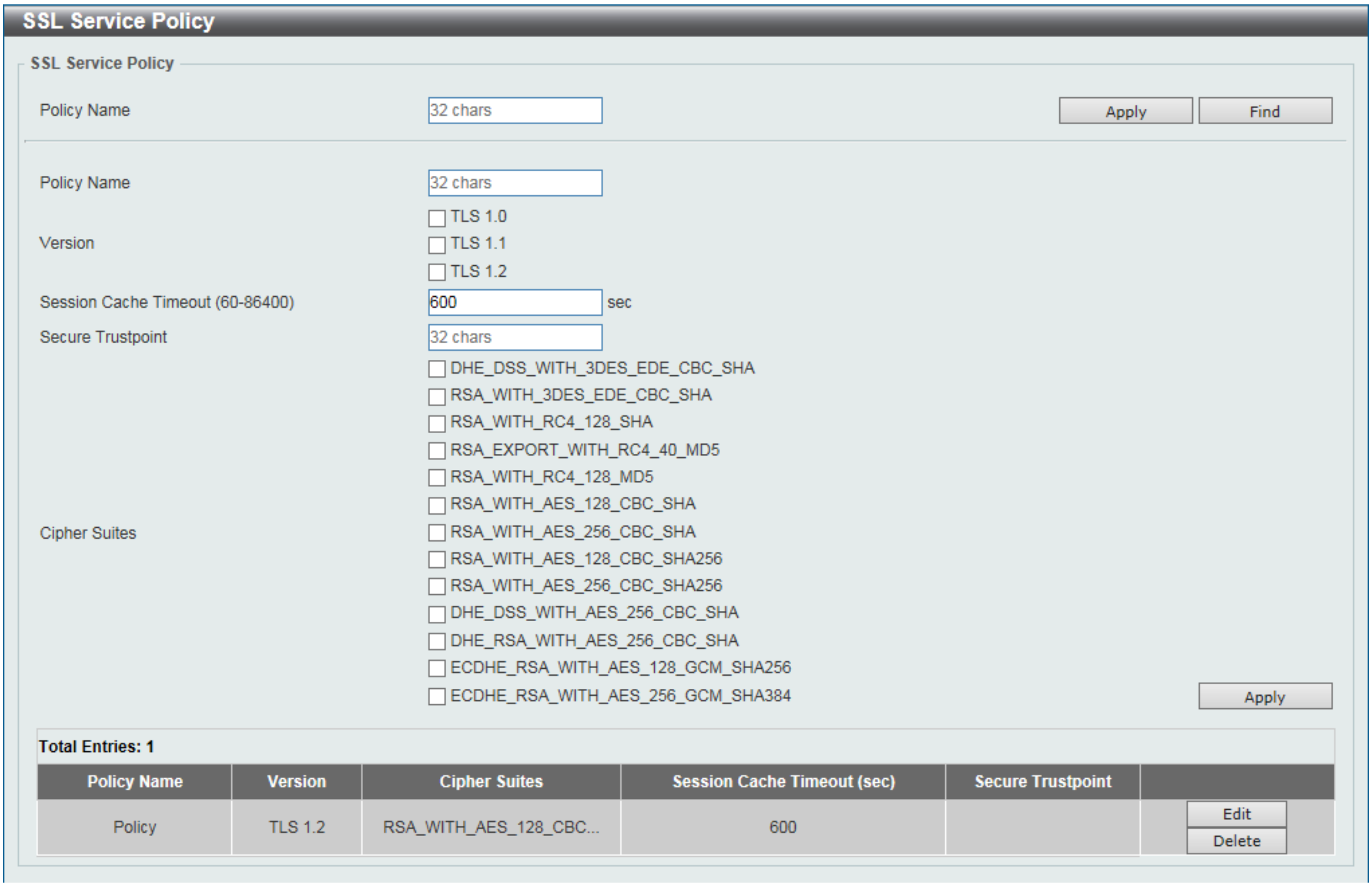
Click the **Find** button to locate a specific entry based on the information entered.

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:



SSL Service Policy

SSL Service Policy

Policy Name: 32 chars [Apply] [Find]

Policy Name: 32 chars

Version:
□ TLS 1.0
□ TLS 1.1
□ TLS 1.2

Session Cache Timeout (60-86400): 600 sec

Secure Trustpoint: 32 chars

Cipher Suites:
□ DHE_DSS_WITH_3DES_EDE_CBC_SHA
□ RSA_WITH_3DES_EDE_CBC_SHA
□ RSA_WITH_RC4_128_SHA
□ RSA_EXPORT_WITH_RC4_40_MD5
□ RSA_WITH_RC4_128_MD5
□ RSA_WITH_AES_128_CBC_SHA
□ RSA_WITH_AES_256_CBC_SHA
□ RSA_WITH_AES_128_CBC_SHA256
□ RSA_WITH_AES_256_CBC_SHA256
□ DHE_DSS_WITH_AES_256_CBC_SHA
□ DHE_RSA_WITH_AES_256_CBC_SHA
□ ECDHE_RSA_WITH_AES_128_GCM_SHA256
□ ECDHE_RSA_WITH_AES_256_GCM_SHA384

[Apply]

Total Entries: 1

Policy Name	Version	Cipher Suites	Session Cache Timeout (sec)	Secure Trustpoint	
Policy	TLS 1.2	RSA_WITH_AES_128_CBC...	600		Edit Delete

Figure 9-102 SSL Service Policy Window

The fields that can be configured are described below:

Parameter	Description
Policy Name	Enter the SSL service policy name here. This name can be up to 32 characters long.
Version	Select the Transport Layer Security (TLS) version here. Options to choose from are **TLS 1.0**, **TLS 1.1**, and **TLS 1.2**.
Session Cache Timeout	Enter the session cache timeout value used here. The range is from 60 to 86400 seconds. By default, this value is 600 seconds.
Secure Trustpoint	Enter the secure trust point name here. This name can be up to 32 characters long.
Cipher Suites	Select the cipher suites that will be associated with this profile here.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

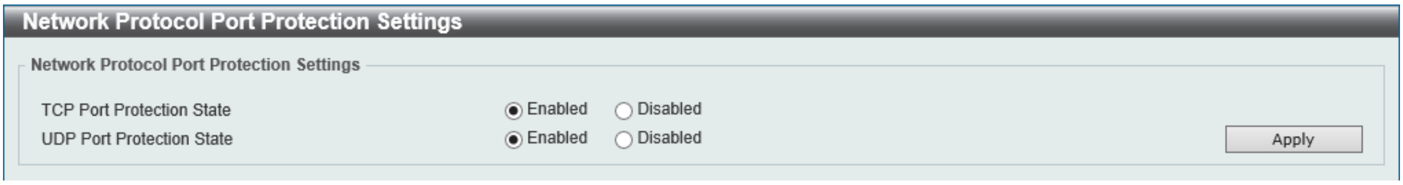
Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specified entry.

Network Protocol Port Protection Settings

This window is used to display and configure the network protocol port protection settings.

To view the following window, click **Security > Network Protocol Port Protection Settings**, as shown below:



Network Protocol Port Protection Settings

Network Protocol Port Protection Settings

TCP Port Protection State ● Enabled ○ Disabled

UDP Port Protection State ● Enabled ○ Disabled

Figure 9-103 Network Protocol Port Protect Settings Window

The fields that can be configured are described below:

Parameter	Description
TCP Port Protect State	Select to enable or disable the TCP port network protocol protection function here.
UDP Port Protect State	Select to enable or disable the UDP port network protocol protection function here.

Click the **Apply** button to accept the changes made.

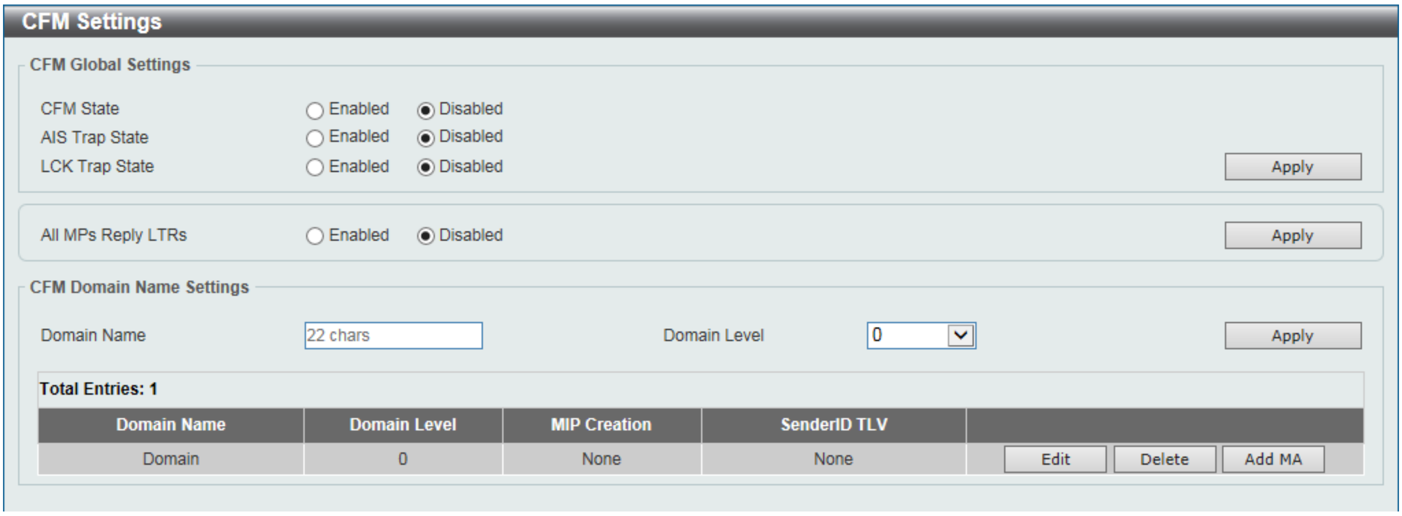
10. OAM

CFM

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:



CFM Settings

CFM Global Settings

CFM State ○ Enabled ● Disabled

AIS Trap State ○ Enabled ● Disabled

LCK Trap State ○ Enabled ● Disabled

All MPs Reply LTRs ○ Enabled ● Disabled

CFM Domain Name Settings

Domain Name: 22 chars

Domain Level: 0

Total Entries: 1

Domain Name	Domain Level	MIP Creation	SenderID TLV	
Domain	0	None	None	Edit Delete Add MA

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.

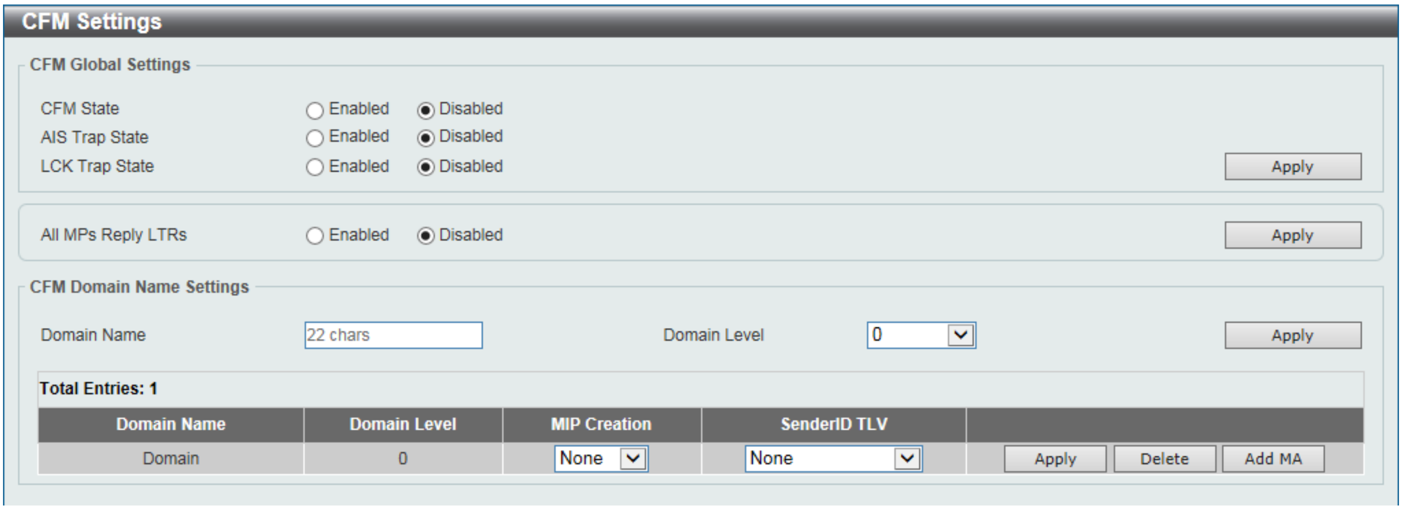
Click the **Apply** button to accept the changes made.

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 following page will appear.



CFM Settings

CFM Global Settings

CFM State ○ Enabled ● Disabled

AIS Trap State ○ Enabled ● Disabled

LCK Trap State ○ Enabled ● Disabled

All MPs Reply LTRs ○ Enabled ● Disabled

CFM Domain Name Settings

Domain Name: 22 chars

Domain Level: 0

Total Entries: 1

Domain Name	Domain Level	MIP Creation	SenderID TLV	
Domain	0	None	None	Apply Delete Add MA

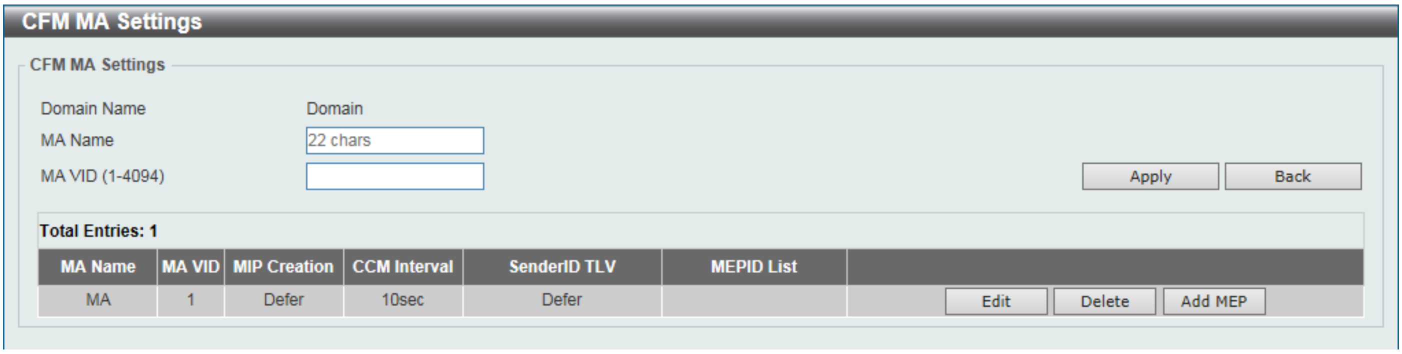
Figure 10-2 CFM Settings (Edit) Window

The fields that can be configured in the table are described below:

Parameter	Description
MIP Creation	Select the Maintenance domain 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** - 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 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. Options to choose from are: • **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.



CFM MA Settings

CFM MA Settings

Domain Name: Domain

MA Name: 22 chars

MA VID (1-4094):

Total Entries: 1

MA Name	MA VID	MIP Creation	CCM Interval	SenderID TLV	MEPID List	
MA	1	Defer	10sec	Defer		Edit Delete Add MEP

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.

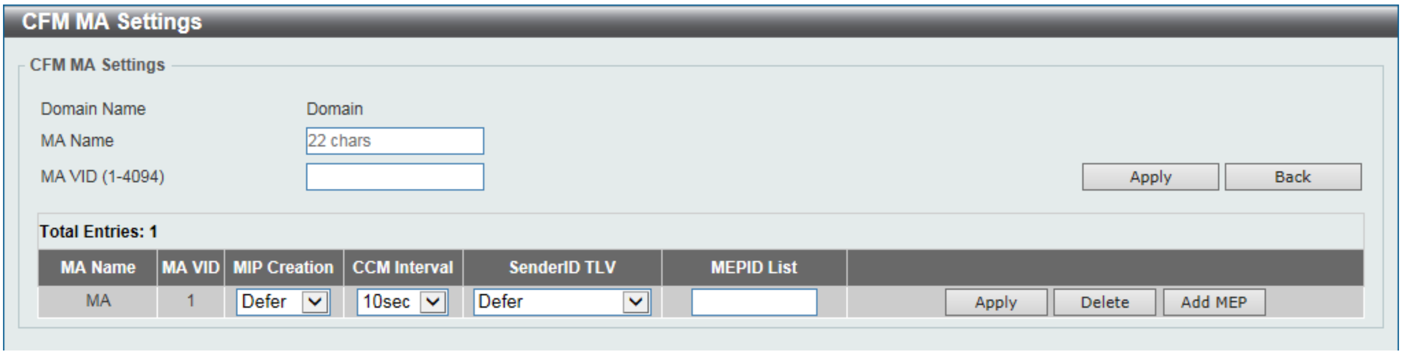
Click the **Back** button to return to the previous window.

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.



CFM MA Settings

CFM MA Settings

Domain Name: Domain

MA Name: 22 chars

MA VID (1-4094):

Total Entries: 1

MA Name	MA VID	MIP Creation	CCM Interval	SenderID TLV	MEPID List	
MA	1	Defer	10sec	Defer		Apply Delete Add MEP

Figure 10-4 CFM Settings (Add MA, Edit) Window

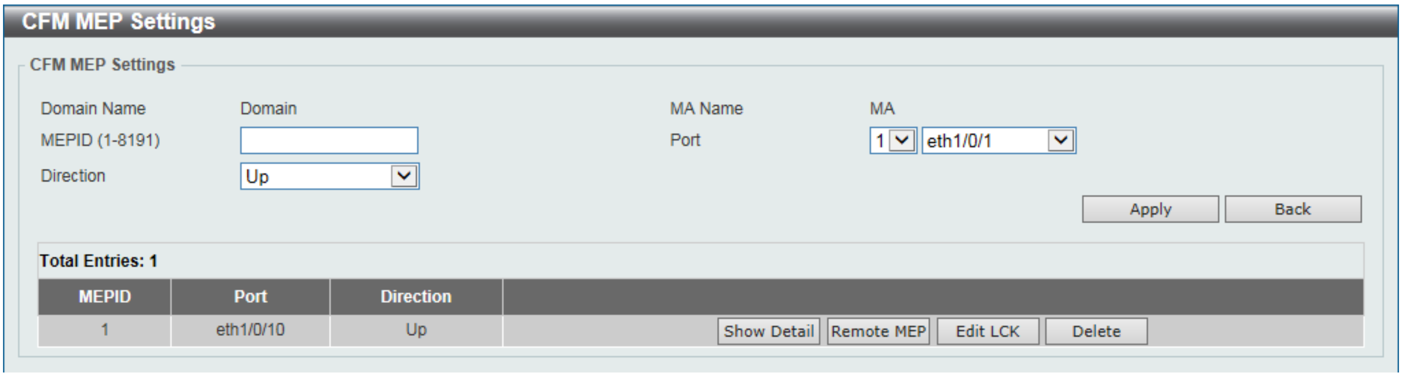
The fields that can be configured in the table are described below:

Parameter	Description
MIP Creation	This option is used to configure the MIP creation for an MA. Options to choose from are: • **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

Parameter	Description
	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 **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.
SenderID TLV	This option is used to configure the transmission of the sender ID TLV by MPs for an MA. Options to choose from are: • **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.



CFM MEP Settings

CFM MEP Settings

Domain Name: Domain

MA Name: MA

MEPID (1-8191):

Port: 1 eth1/0/1

Direction: Up

Total Entries: 1

MEPID	Port	Direction	
1	eth1/0/10	Up	Show Detail Remote MEP Edit LCK Delete

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.

Parameter	Description
	• **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.

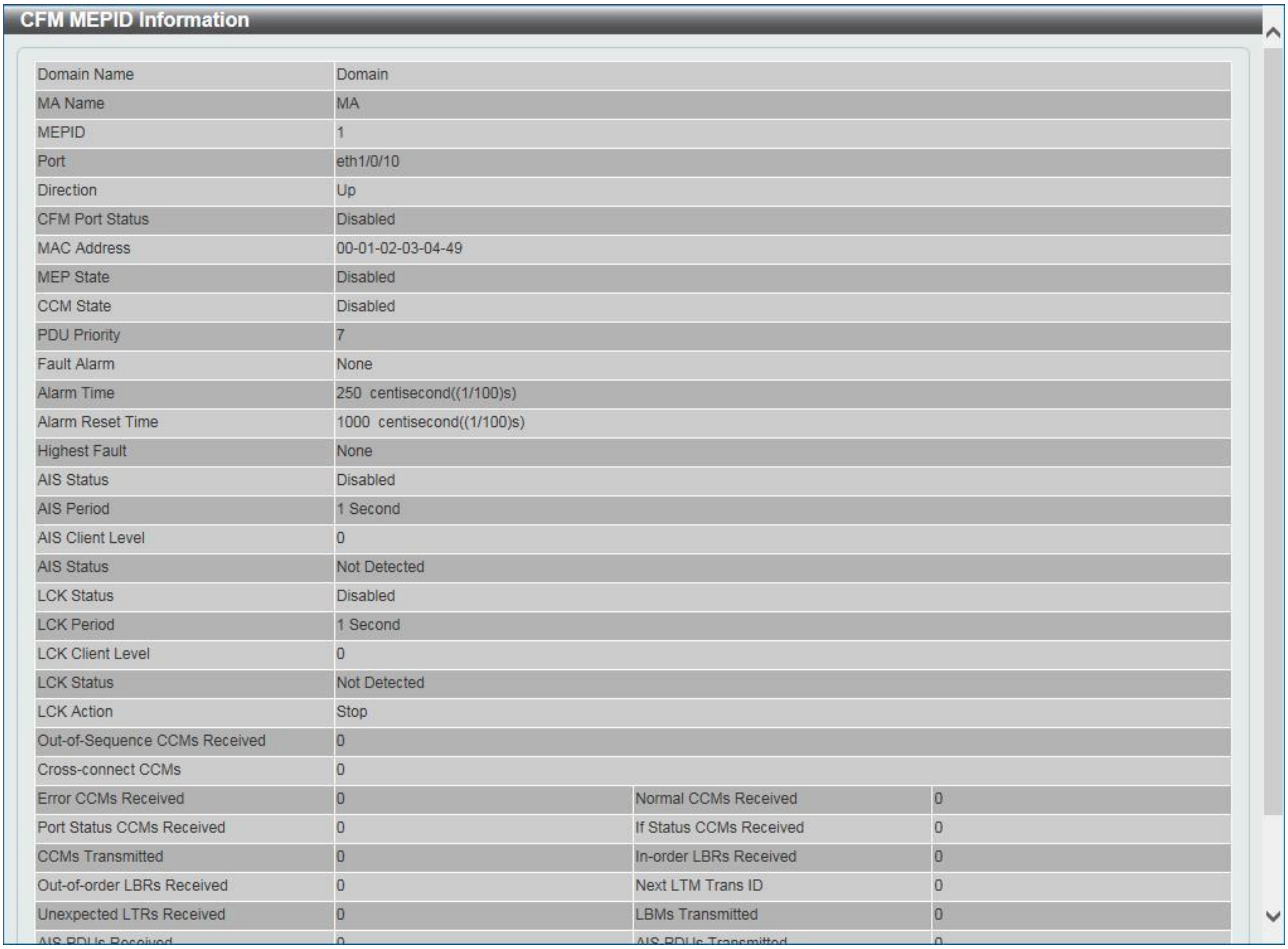
Click the **Show Detail** button to view more detailed information about the specified MEP.

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 **Delete** button to delete the specified entry.

After clicking the **Show Detail** button, the following page will appear.



CFM MEPID Information

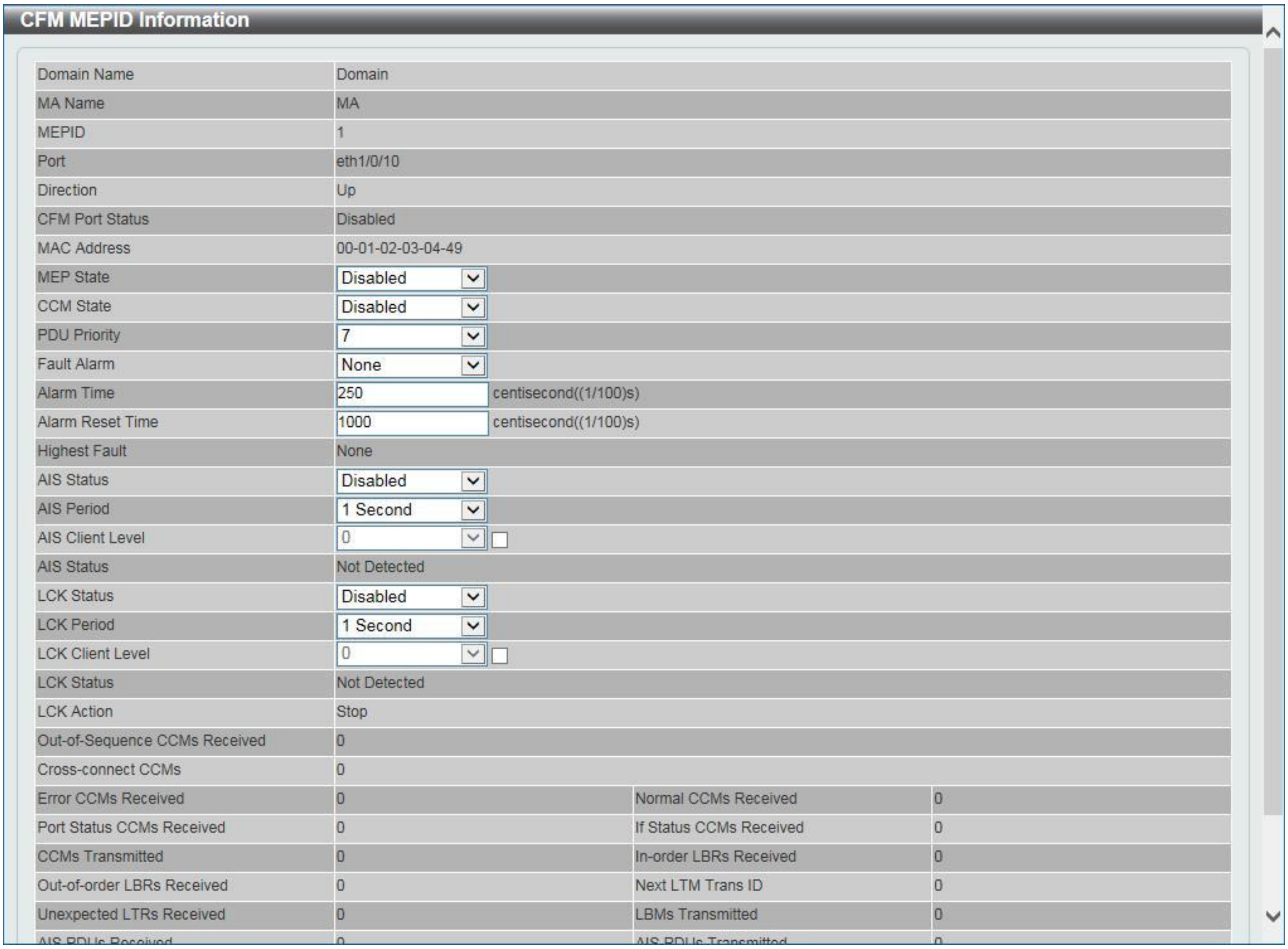
Domain Name	Domain		
MA Name	MA		
MEPID	1		
Port	eth1/0/10		
Direction	Up		
CFM Port Status	Disabled		
MAC Address	00-01-02-03-04-49		
MEP State	Disabled		
CCM State	Disabled		
PDU Priority	7		
Fault Alarm	None		
Alarm Time	250 centisecond((1/100)s)		
Alarm Reset Time	1000 centisecond((1/100)s)		
Highest Fault	None		
AIS Status	Disabled		
AIS Period	1 Second		
AIS Client Level	0		
AIS Status	Not Detected		
LCK Status	Disabled		
LCK Period	1 Second		
LCK Client Level	0		
LCK Status	Not Detected		
LCK Action	Stop		
Out-of-Sequence CCMs Received	0		
Cross-connect CCMs	0		
Error CCMs Received	0	Normal CCMs Received	0
Port Status CCMs Received	0	If Status CCMs Received	0
CCMs Transmitted	0	In-order LBRs Received	0
Out-of-order LBRs Received	0	Next LTM Trans ID	0
Unexpected LTRs Received	0	LBMs Transmitted	0
AIS PDUs Received	0	AIS PDUs Transmitted	0

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.



CFM MEPID Information

Domain Name	Domain		
MA Name	MA		
MEPID	1		
Port	eth1/0/10		
Direction	Up		
CFM Port Status	Disabled		
MAC Address	00-01-02-03-04-49		
MEP State	Disabled		
CCM State	Disabled		
PDU Priority	7		
Fault Alarm	None		
Alarm Time	250 centisecond((1/100)s)		
Alarm Reset Time	1000 centisecond((1/100)s)		
Highest Fault	None		
AIS Status	Disabled		
AIS Period	1 Second		
AIS Client Level	0 □		
AIS Status	Not Detected		
LCK Status	Disabled		
LCK Period	1 Second		
LCK Client Level	0 □		
LCK Status	Not Detected		
LCK Action	Stop		
Out-of-Sequence CCMs Received	0		
Cross-connect CCMs	0		
Error CCMs Received	0	Normal CCMs Received	0
Port Status CCMs Received	0	If Status CCMs Received	0
CCMs Transmitted	0	In-order LBRs Received	0
Out-of-order LBRs Received	0	Next LTM Trans ID	0
Unexpected LTRs Received	0	LBMs Transmitted	0
AIS PDUs Received	0	AIS PDUs Transmitted	0

Figure 10-7 CFM Settings (Add MA, Add MEP, MEPID Detail, Edit) Window

The fields that can be configured are described below:

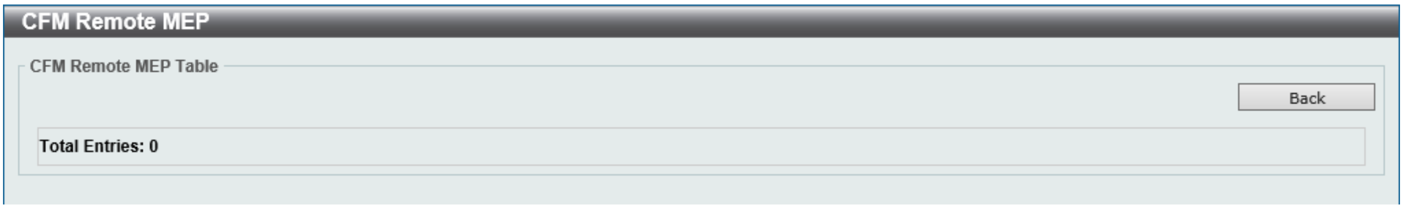
Parameter	Description
MEP State	Select to enable or disable the MEP state on the interface here.
CCM State	Select to enable or disable the CCM state here.
PDU Priority	Select the PDU priority value here. The range is from 0 to 7. This feature is used to define the 802.1p priority that is set in the CCM 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** - 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*. • **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.

Parameter	Description
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 Status	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	Tick the check box and select the client level ID to which the MEP sends the AIS PDUs here. The range is from 0 to 7. The default client MD level is that the most immediate client layer MIPs and MEPs exist on.
LCK Status	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	Tick the check box and select the client level ID to which the MEP sends the LCK PDU here. The range is from 0 to 7. The default client MD level is that the most immediate client layer MIPs and MEPs exist on.

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.

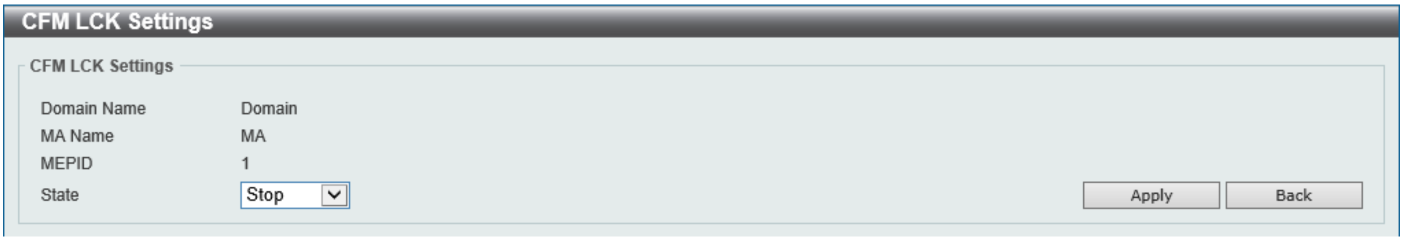


Total Entries: 0

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.



Domain Name Domain
MA Name MA
MEPID 1
State Stop

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.

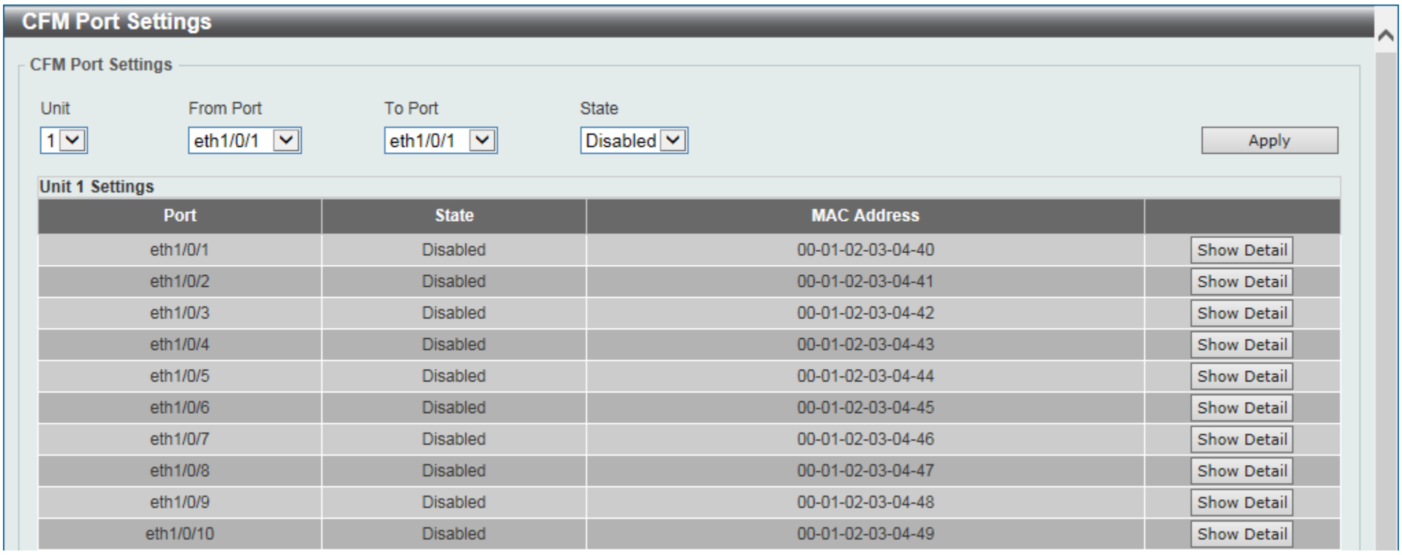
Click the **Apply** button to accept the changes made.

Click the **Back** button to return to the previous window.

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:



CFM Port Settings

CFM Port Settings

Unit: 1 | From Port: eth1/0/1 | To Port: eth1/0/1 | State: Disabled | Apply

Unit 1 Settings

Port	State	MAC Address	
eth1/0/1	Disabled	00-01-02-03-04-40	Show Detail
eth1/0/2	Disabled	00-01-02-03-04-41	Show Detail
eth1/0/3	Disabled	00-01-02-03-04-42	Show Detail
eth1/0/4	Disabled	00-01-02-03-04-43	Show Detail
eth1/0/5	Disabled	00-01-02-03-04-44	Show Detail
eth1/0/6	Disabled	00-01-02-03-04-45	Show Detail
eth1/0/7	Disabled	00-01-02-03-04-46	Show Detail
eth1/0/8	Disabled	00-01-02-03-04-47	Show Detail
eth1/0/9	Disabled	00-01-02-03-04-48	Show Detail
eth1/0/10	Disabled	00-01-02-03-04-49	Show Detail

Figure 10-10 CFM Port Settings Window

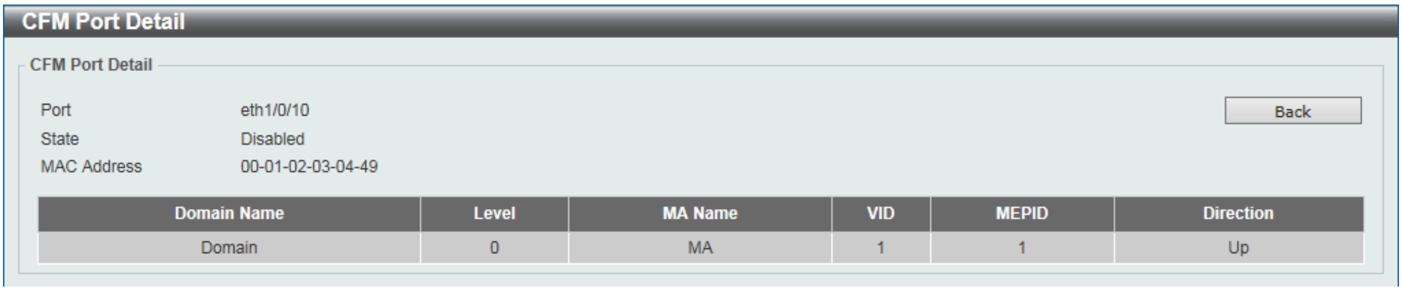
The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit ID that will be used here.
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.



CFM Port Detail

CFM Port Detail

Port: eth1/0/10

State: Disabled

MAC Address: 00-01-02-03-04-49

Back

Domain Name	Level	MA Name	VID	MEPID	Direction
Domain	0	MA	1	1	Up

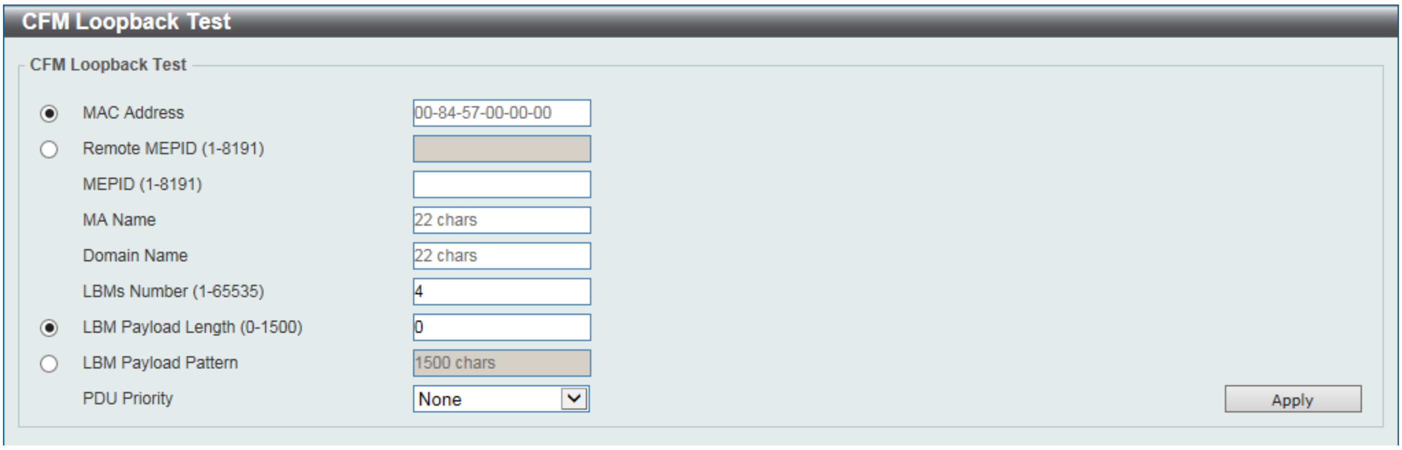
Figure 10-11 CFM Port Settings (View Detail) Window

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:



CFM Loopback Test

CFM Loopback Test

● MAC Address: 00-84-57-00-00-00
○ Remote MEPID (1-8191):
MEPID (1-8191):
MA Name: 22 chars
Domain Name: 22 chars
LBMs Number (1-65535): 4
● LBM Payload Length (0-1500): 0
○ LBM Payload Pattern: 1500 chars
PDU Priority: None

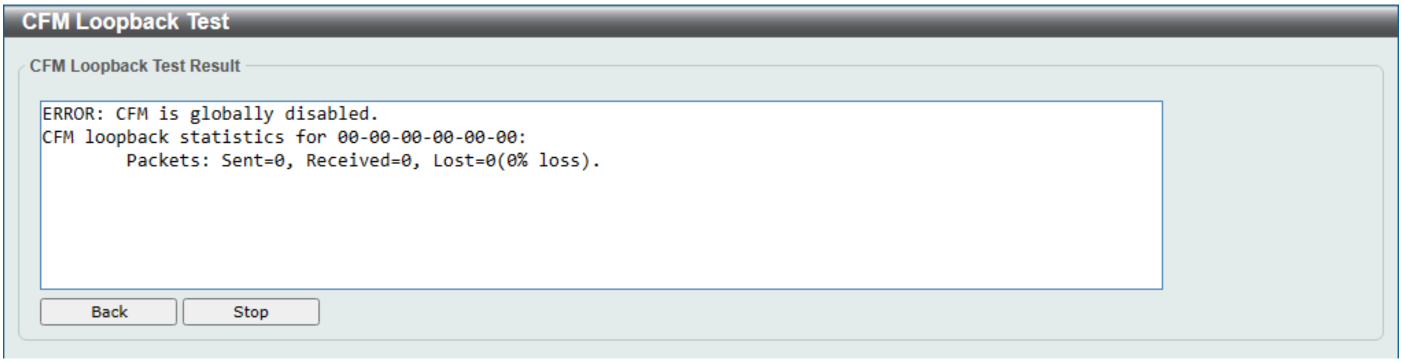
Figure 10-12 CFM Loopback Test Window

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 to 1500. 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. No spaces are allowed.
PDU Priority	Select the 802.1p priority to be set in the transmitted LBMs here. If **None** is selected, it uses the same priority as the CCMs sent by the MEP. The range is from 0 to 7.

Click the **Apply** button to accept the changes made.

After clicking the **Apply** button, the following **CFM Loopback Test Result** will appear:



```
ERROR: CFM is globally disabled.
CFM loopback statistics for 00-00-00-00-00-00:
       Packets: Sent=0, Received=0, Lost=0(0% loss).
```

Figure 10-13 CFM Loopback Test Result Window

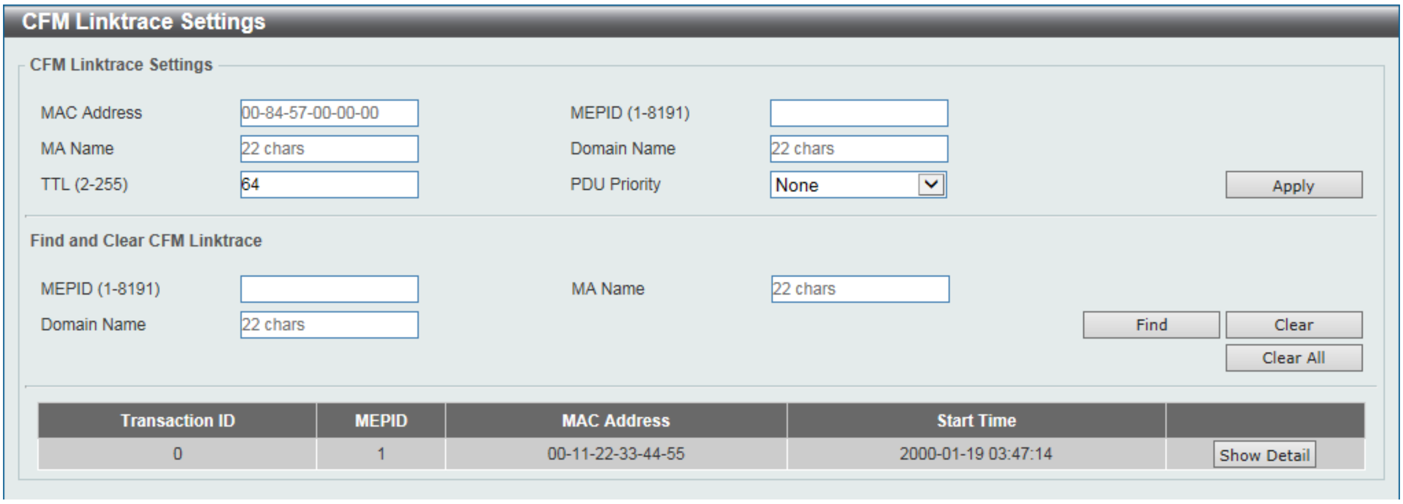
Click the **Stop** button to halt the CFM Loopback Test.

Click the **Back** button to return to the CFM Loopback Test window.

CFM Linktrace Settings

This window is used to display and configure the CFM link-trace settings.

To view the following window, click **OAM > CFM > CFM Linktrace Settings**, as shown below:



MAC Address: 00-84-57-00-00-00
MEPID (1-8191):
MA Name: 22 chars
Domain Name: 22 chars
TTL (2-255): 64
PDU Priority: None

MEPID (1-8191):
MA Name: 22 chars
Domain Name: 22 chars

Transaction ID	MEPID	MAC Address	Start Time	
0	1	00-11-22-33-44-55	2000-01-19 03:47:14	Show Detail

Figure 10-14 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 LTMs here. **If None** is selected, it uses the same priority as the CCMs sent by the MEP. The range is from 0 to 7.

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.

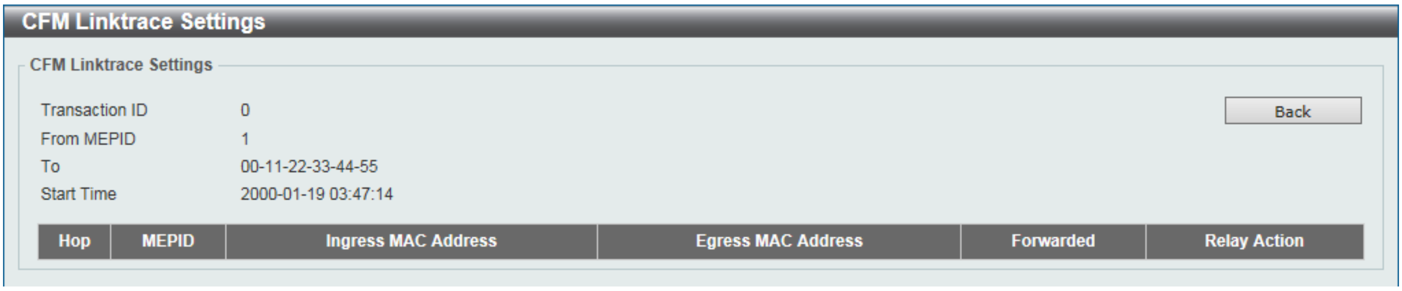
Click the **Find** button to locate a specific entry based on the information entered.

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.



CFM Linktrace Settings

CFM Linktrace Settings

Transaction ID 0

From MEPID 1

To 00-11-22-33-44-55

Start Time 2000-01-19 03:47:14

Hop	MEPID	Ingress MAC Address	Egress MAC Address	Forwarded	Relay Action

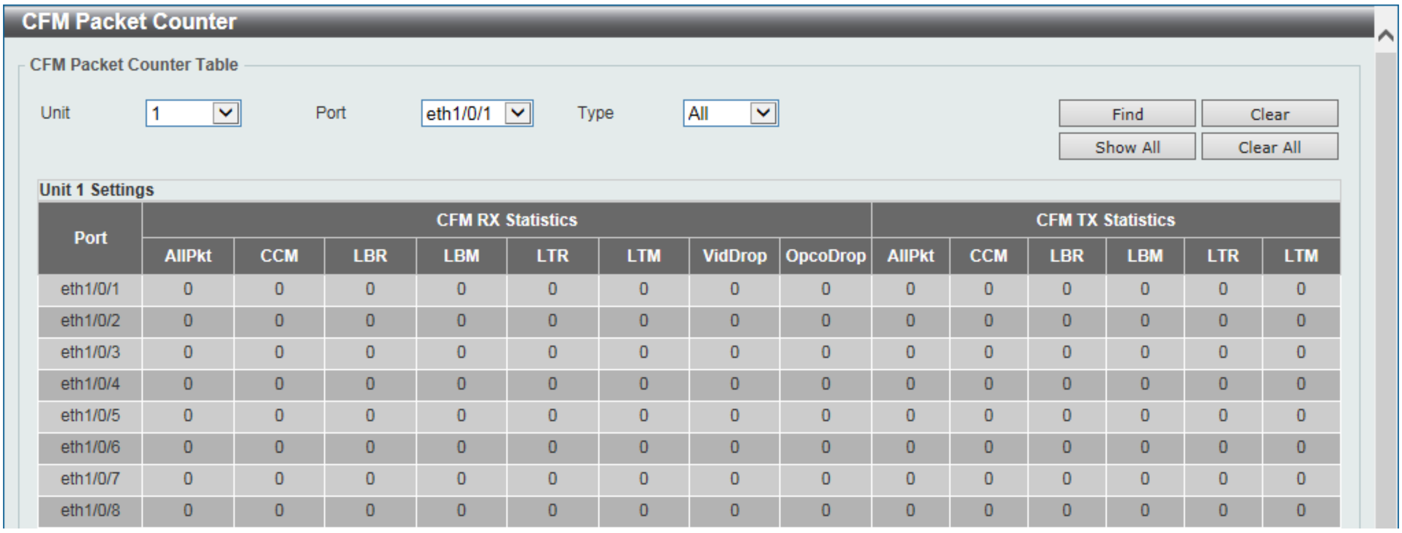
Figure 10-15 CFM Linktrace Settings (Show Detail) Window

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:



CFM Packet Counter

CFM Packet Counter Table

Unit 1 Port eth1/0/1 Type All

Unit 1 Settings

Port	CFM RX Statistics								CFM TX Statistics					
	AllPkt	CCM	LBR	LBM	LTR	LTM	VidDrop	OpcoDrop	AllPkt	CCM	LBR	LBM	LTR	LTM
eth1/0/1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth1/0/2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth1/0/3	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth1/0/4	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth1/0/5	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth1/0/6	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth1/0/7	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth1/0/8	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 10-16 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.
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.

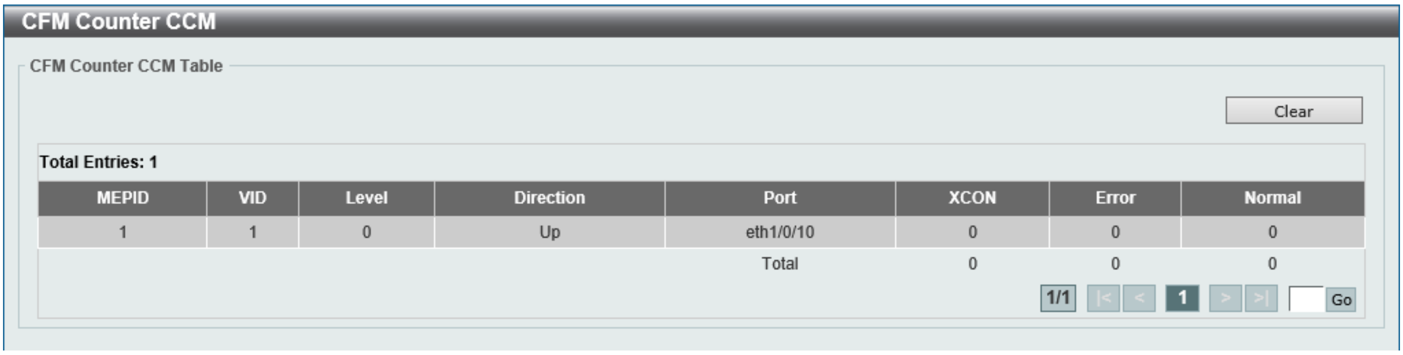
Click the **Show All** button to display all the entries.

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:



CFM Counter CCM

CFM Counter CCM Table

Total Entries: 1

MEPID	VID	Level	Direction	Port	XCON	Error	Normal
1	1	0	Up	eth1/0/10	0	0	0
				Total	0	0	0

Figure 10-17 CFM Counter CCM Window

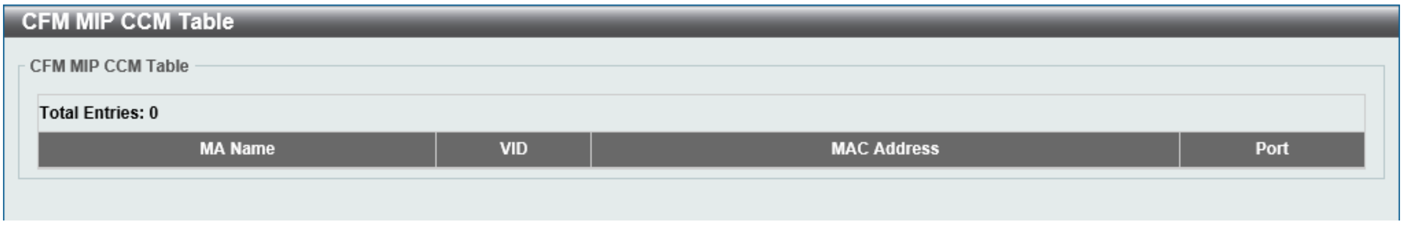
Click the **Clear** button to clear the counter information associated with all entries.

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:



CFM MIP CCM Table

CFM MIP CCM Table

Total Entries: 0

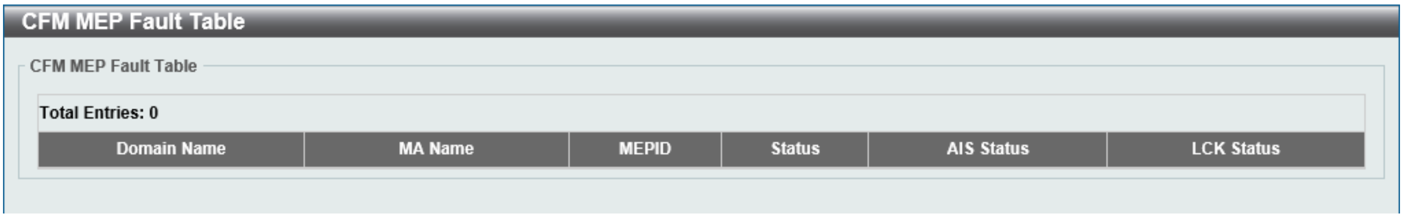
MA Name	VID	MAC Address	Port

Figure 10-18 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:



CFM MEP Fault Table

CFM MEP Fault Table

Total Entries: 0

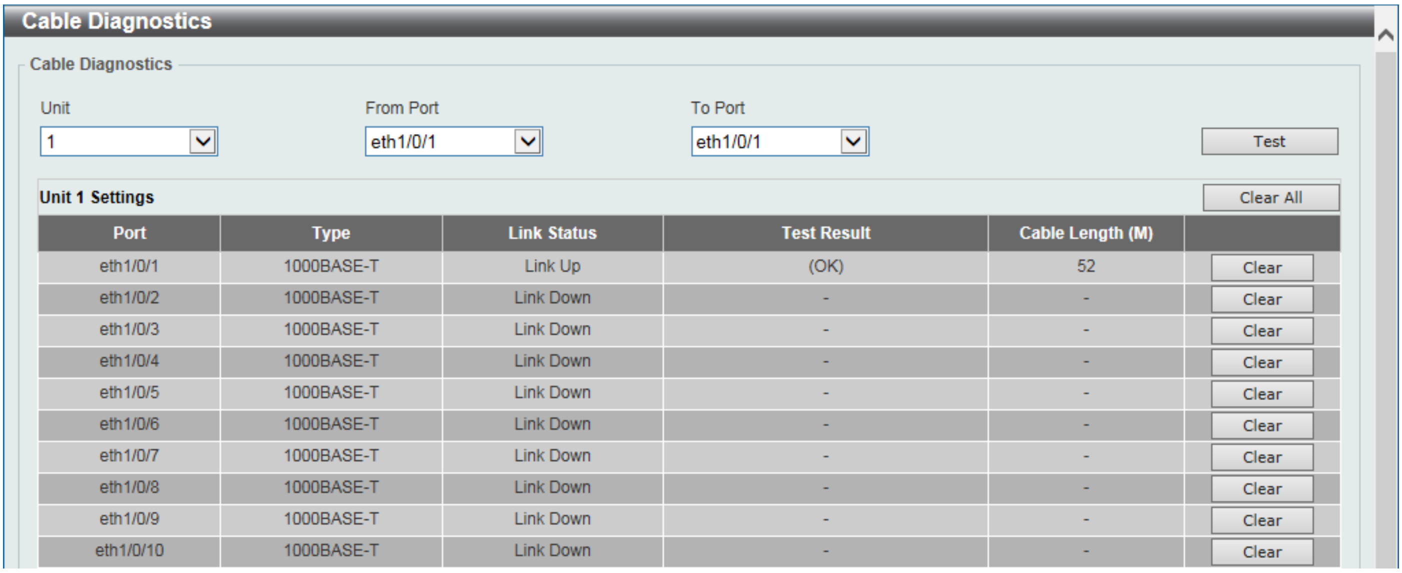
Domain Name	MA Name	MEPID	Status	AIS Status	LCK Status

Figure 10-19 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:



Cable Diagnostics

Cable Diagnostics

Unit: 1

From Port: eth1/0/1

To Port: eth1/0/1

Unit 1 Settings

Port	Type	Link Status	Test Result	Cable Length (M)	
eth1/0/1	1000BASE-T	Link Up	(OK)	52	Clear
eth1/0/2	1000BASE-T	Link Down	-	-	Clear
eth1/0/3	1000BASE-T	Link Down	-	-	Clear
eth1/0/4	1000BASE-T	Link Down	-	-	Clear
eth1/0/5	1000BASE-T	Link Down	-	-	Clear
eth1/0/6	1000BASE-T	Link Down	-	-	Clear
eth1/0/7	1000BASE-T	Link Down	-	-	Clear
eth1/0/8	1000BASE-T	Link Down	-	-	Clear
eth1/0/9	1000BASE-T	Link Down	-	-	Clear
eth1/0/10	1000BASE-T	Link Down	-	-	Clear

Figure 10-20 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.
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 All** button to clear all the information in this table.

Click the **Clear** button to clear all the information for the specific port.

NOTE: Cable diagnostic function limitations. Cable length detection is only supported on copper ports.

NOTE: For more accurate test results, use the TIA/EIA-568B pin assignment on the RJ45 connectors.

Test Result messages:

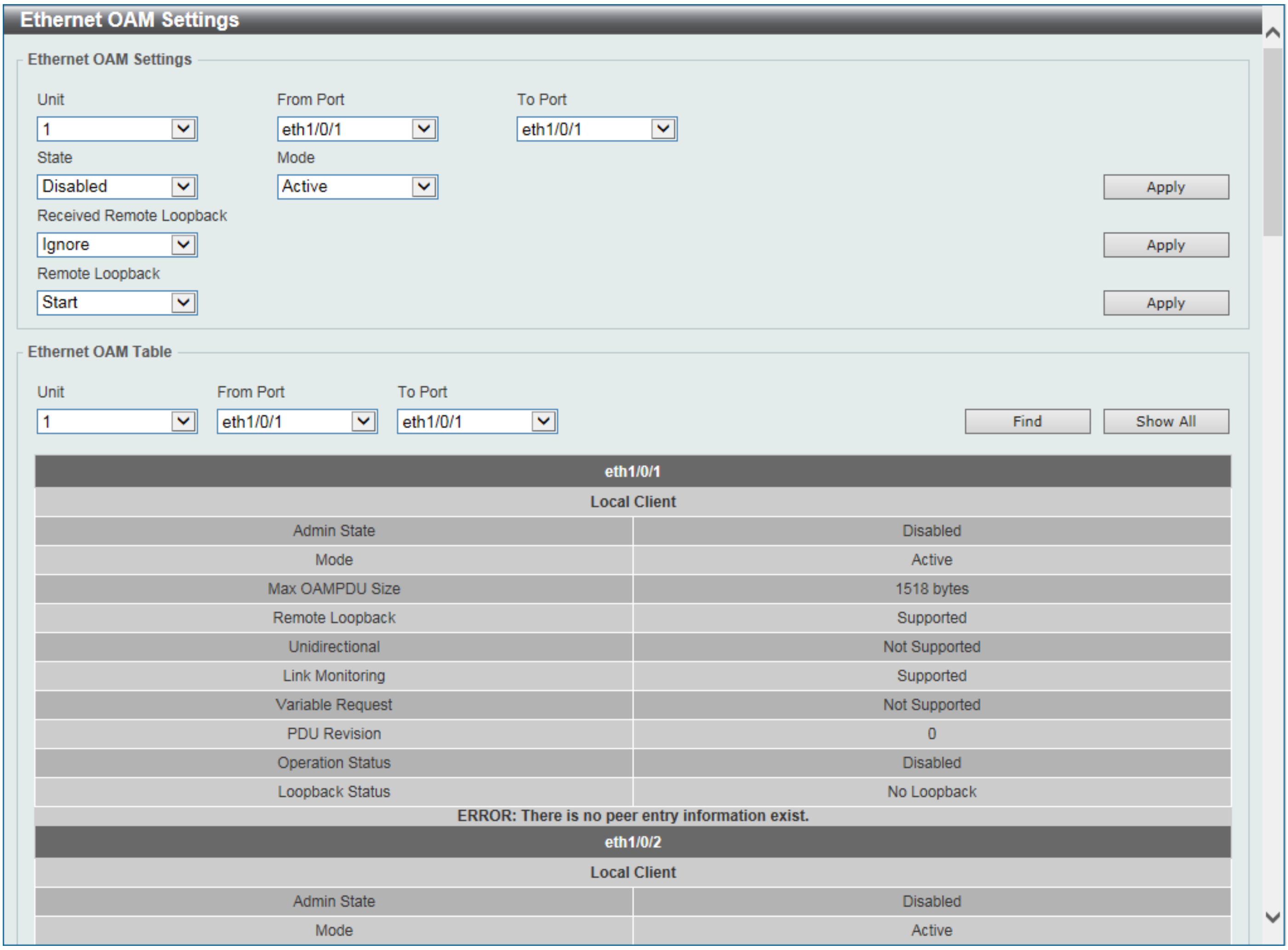
- **Open** - The cable in the error pair does not have a connection at the specified position.
- **Short** - The cable in the error pair has a short problem at the specified position.
- **Open or Short** - The cable has an open or short problem, but the PHY has no capability to distinguish between them.
- **Shutdown** - The remote partner is powered off.
- **OK**- The pair or cable has no error.
- **No Cable** - The port does not have any cable connection to the remote partner.

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:



Ethernet OAM Settings

Ethernet OAM Settings

Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1
State: Disabled
Mode: Active
Received Remote Loopback: Ignore
Remote Loopback: Start

Ethernet OAM Table

Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1

eth1/0/1	
Local Client	
Admin State	Disabled
Mode	Active
Max OAMPDU Size	1518 bytes
Remote Loopback	Supported
Unidirectional	Not Supported
Link Monitoring	Supported
Variable Request	Not Supported
PDU Revision	0
Operation Status	Disabled
Loopback Status	No Loopback
ERROR: There is no peer entry information exist.	
eth1/0/2	
Local Client	
Admin State	Disabled
Mode	Active

Figure 10-21 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.
From Port - To Port	Select the Switch port range that will be used here.
State	Select to enable or disable the Ethernet OAM feature on the specified ports 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** - 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** - 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.
From Port - To Port	Select the Switch port range that will be used here.

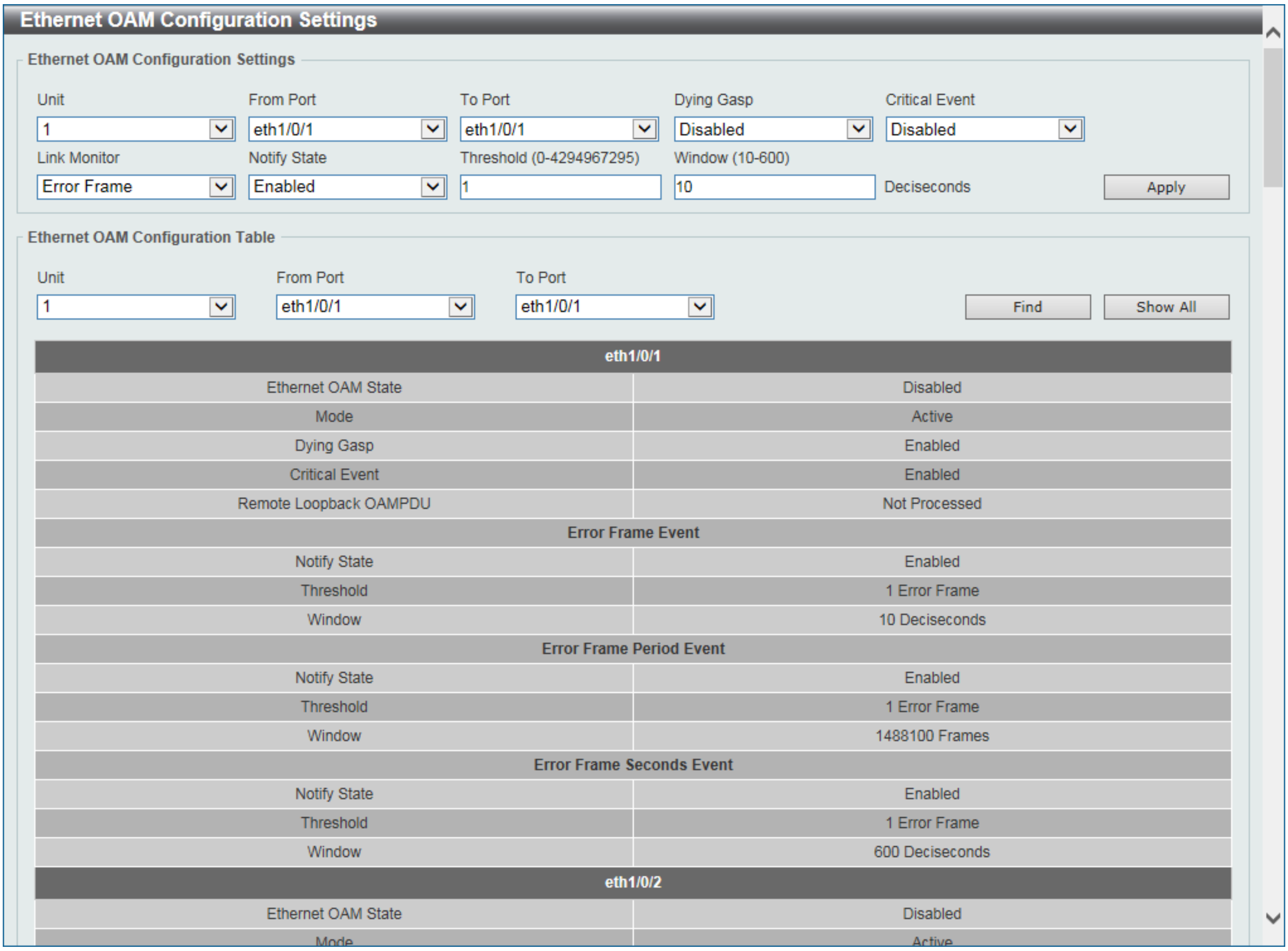
Click the **Find** button to locate a specific entry based on the information entered.

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:



Ethernet OAM Configuration Settings

Ethernet OAM Configuration Settings

Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1
Dying Gasp: Disabled
Critical Event: Disabled
Link Monitor: Error Frame
Notify State: Enabled
Threshold (0-4294967295): 1
Window (10-600): 10 Deciseconds

Ethernet OAM Configuration Table

Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1

eth1/0/1	
Ethernet OAM State	Disabled
Mode	Active
Dying Gasp	Enabled
Critical Event	Enabled
Remote Loopback OAMPDU	Not Processed
Error Frame Event	
Notify State	Enabled
Threshold	1 Error Frame
Window	10 Deciseconds
Error Frame Period Event	
Notify State	Enabled
Threshold	1 Error Frame
Window	1488100 Frames
Error Frame Seconds Event	
Notify State	Enabled
Threshold	1 Error Frame
Window	600 Deciseconds
eth1/0/2	
Ethernet OAM State	Disabled
Mode	Active

Figure 10-22 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.
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 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.

Parameter	Description
	• **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 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 4294967295. • 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. • 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 4294967295.
Window	Enter the window value here. • 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. • 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. • 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 frames.

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.
From Port - To Port	Select the Switch port range that will be used here.

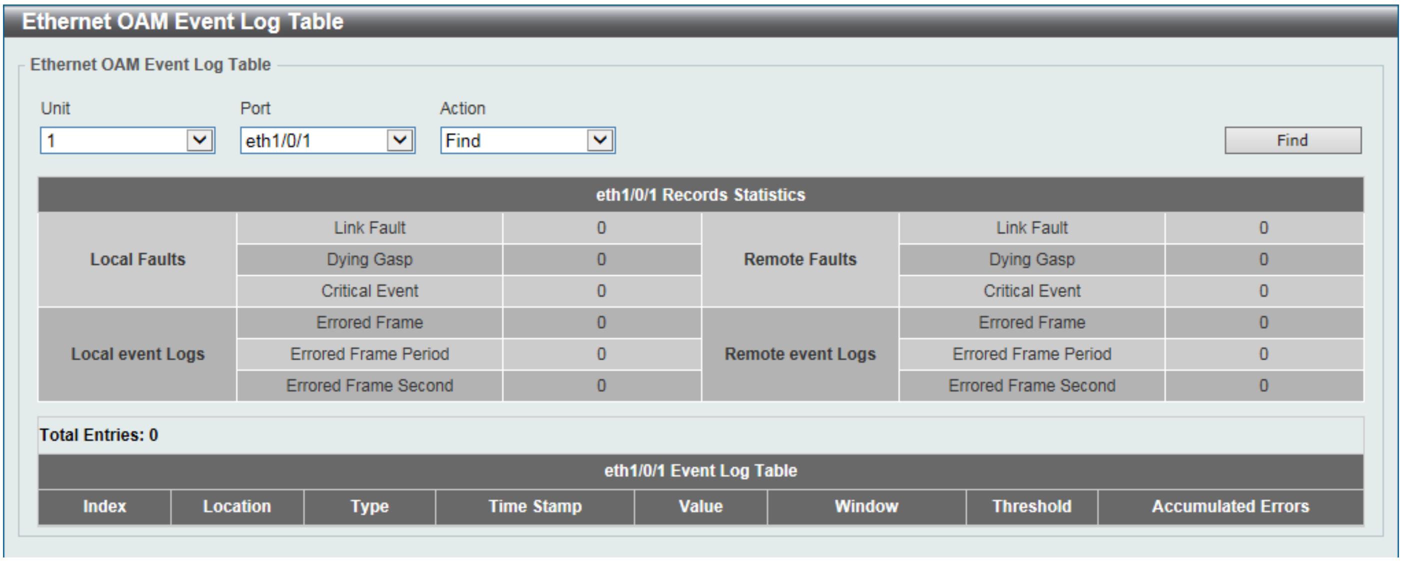
Click the **Find** button to locate a specific entry based on the information entered.

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:



Ethernet OAM Event Log Table

Ethernet OAM Event Log Table

Unit: 1
Port: eth1/0/1
Action: Find

eth1/0/1 Records Statistics

Local Faults	Link Fault	0	Remote Faults	Link Fault	0
	Dying Gasp	0		Dying Gasp	0
	Critical Event	0		Critical Event	0
Local event Logs	Errored Frame	0	Remote event Logs	Errored Frame	0
	Errored Frame Period	0		Errored Frame Period	0
	Errored Frame Second	0		Errored Frame Second	0

Total Entries: 0

eth1/0/1 Event Log Table

Index	Location	Type	Time Stamp	Value	Window	Threshold	Accumulated Errors

Figure 10-23 Ethernet OAM Event Log Table Window

The fields that can be configured are described below:

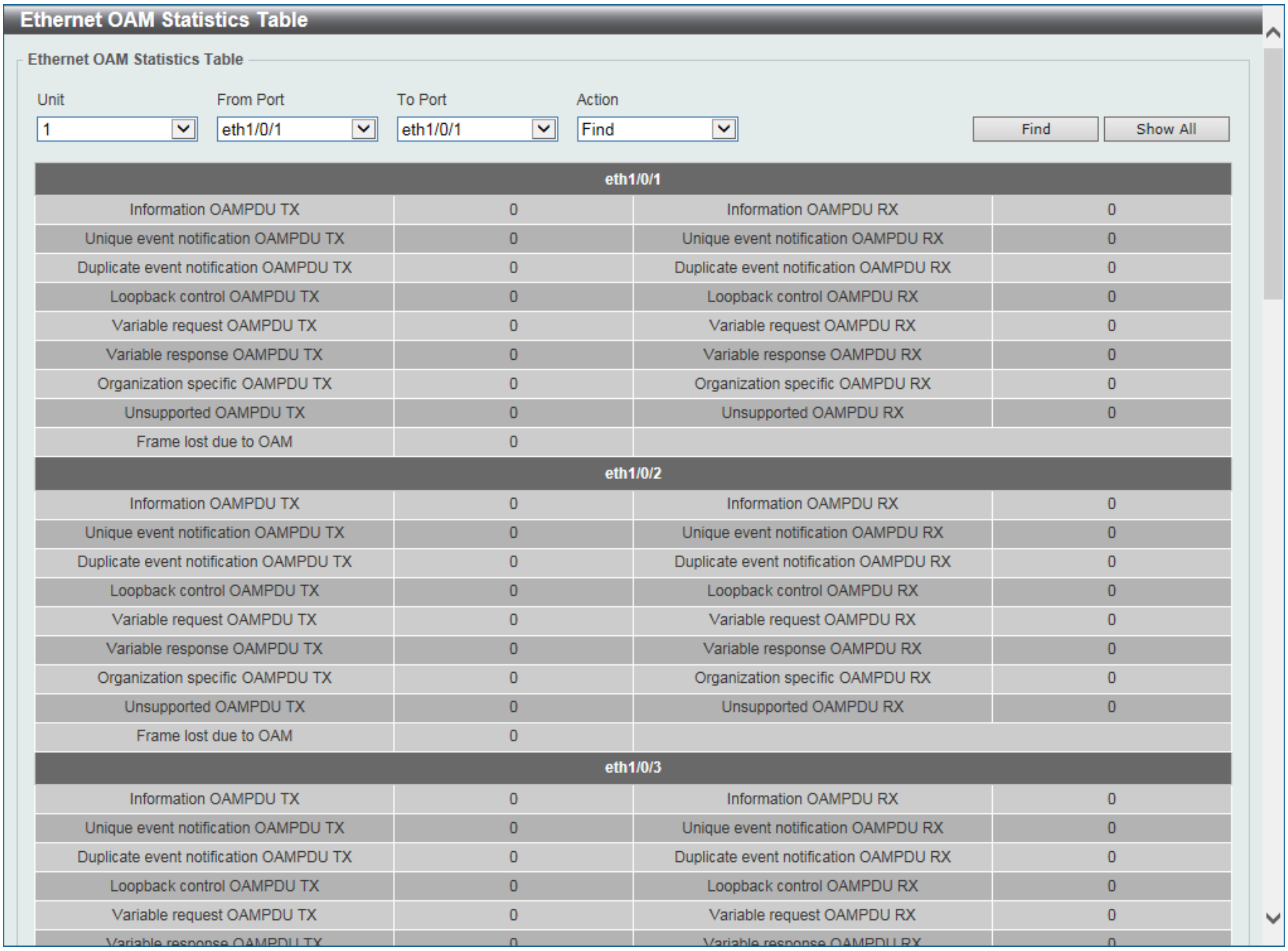
Parameter	Description
Unit	Select the Switch unit ID that will be used here.
Port	Select the Switch port that will be used here.
Action	Select the **Find** option to find and display the log entries associated with the specified port. Select the **Clear** option to clear the log entries associated with 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:



Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1
Action: Find

eth1/0/1			
Information OAMPDU TX	0	Information OAMPDU RX	0
Unique event notification OAMPDU TX	0	Unique event notification OAMPDU RX	0
Duplicate event notification OAMPDU TX	0	Duplicate event notification OAMPDU RX	0
Loopback control OAMPDU TX	0	Loopback control OAMPDU RX	0
Variable request OAMPDU TX	0	Variable request OAMPDU RX	0
Variable response OAMPDU TX	0	Variable response OAMPDU RX	0
Organization specific OAMPDU TX	0	Organization specific OAMPDU RX	0
Unsupported OAMPDU TX	0	Unsupported OAMPDU RX	0
Frame lost due to OAM	0		
eth1/0/2			
Information OAMPDU TX	0	Information OAMPDU RX	0
Unique event notification OAMPDU TX	0	Unique event notification OAMPDU RX	0
Duplicate event notification OAMPDU TX	0	Duplicate event notification OAMPDU RX	0
Loopback control OAMPDU TX	0	Loopback control OAMPDU RX	0
Variable request OAMPDU TX	0	Variable request OAMPDU RX	0
Variable response OAMPDU TX	0	Variable response OAMPDU RX	0
Organization specific OAMPDU TX	0	Organization specific OAMPDU RX	0
Unsupported OAMPDU TX	0	Unsupported OAMPDU RX	0
Frame lost due to OAM	0		
eth1/0/3			
Information OAMPDU TX	0	Information OAMPDU RX	0
Unique event notification OAMPDU TX	0	Unique event notification OAMPDU RX	0
Duplicate event notification OAMPDU TX	0	Duplicate event notification OAMPDU RX	0
Loopback control OAMPDU TX	0	Loopback control OAMPDU RX	0
Variable request OAMPDU TX	0	Variable request OAMPDU RX	0
Variable response OAMPDU TX	0	Variable response OAMPDU RX	0

Figure 10-24 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.
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).

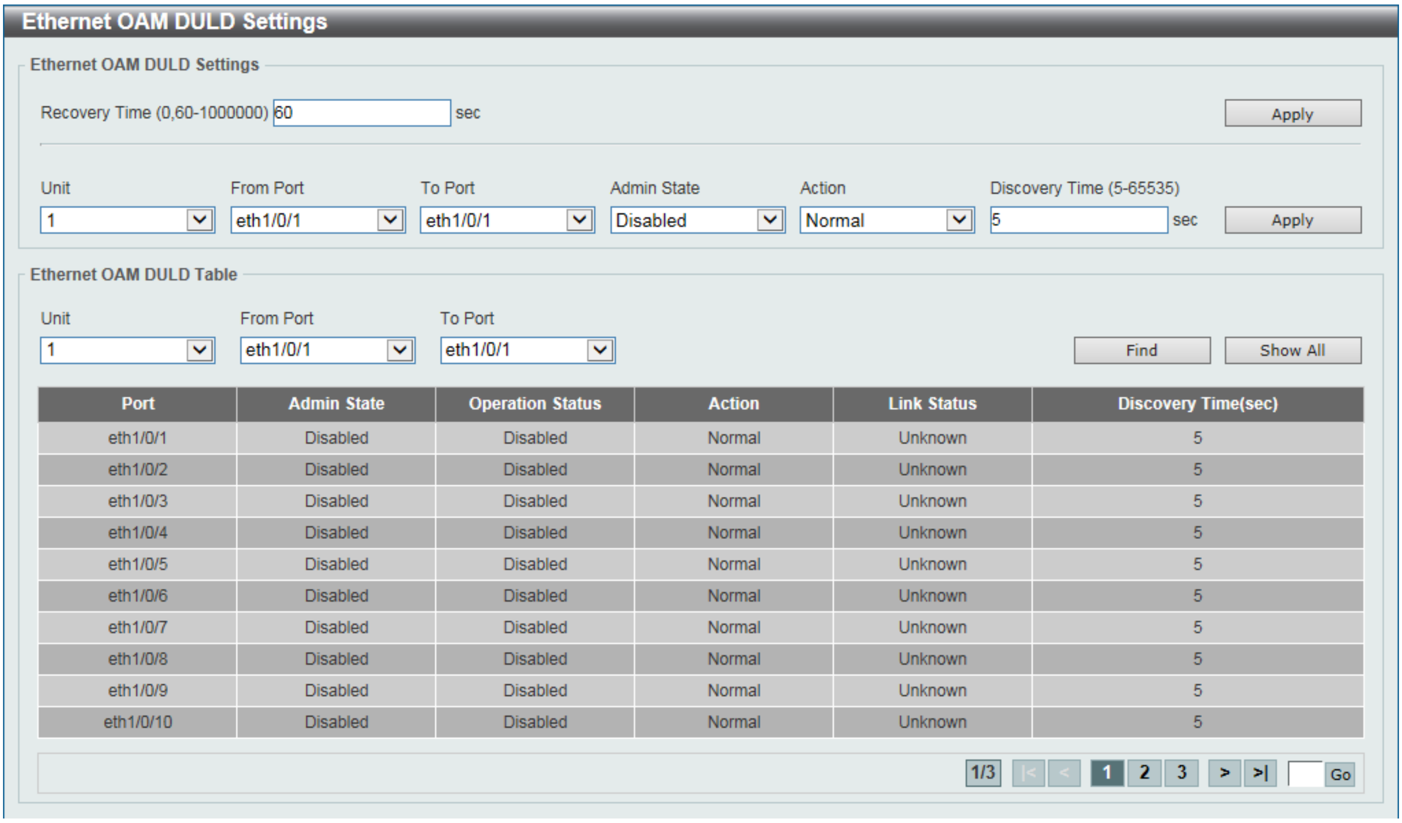
Click the **Show All** button to display all the statistics information.

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:



Ethernet OAM DULD Settings

Ethernet OAM DULD Settings

Recovery Time (0,60-1000000) 60 sec

Unit	From Port	To Port	Admin State	Action	Discovery Time (5-65535)
1	eth1/0/1	eth1/0/1	Disabled	Normal	5 sec

Ethernet OAM DULD Table

Unit	From Port	To Port
1	eth1/0/1	eth1/0/1

Port	Admin State	Operation Status	Action	Link Status	Discovery Time(sec)
eth1/0/1	Disabled	Disabled	Normal	Unknown	5
eth1/0/2	Disabled	Disabled	Normal	Unknown	5
eth1/0/3	Disabled	Disabled	Normal	Unknown	5
eth1/0/4	Disabled	Disabled	Normal	Unknown	5
eth1/0/5	Disabled	Disabled	Normal	Unknown	5
eth1/0/6	Disabled	Disabled	Normal	Unknown	5
eth1/0/7	Disabled	Disabled	Normal	Unknown	5
eth1/0/8	Disabled	Disabled	Normal	Unknown	5
eth1/0/9	Disabled	Disabled	Normal	Unknown	5
eth1/0/10	Disabled	Disabled	Normal	Unknown	5

Figure 10-25 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 Ethernet OAM unidirectional link detection automatic recovery time here. The range is 0, and from 60 to 1000000 seconds. If this value is 0, this feature is disabled. By default, this value is 60 seconds.
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.
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).
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.

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.
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.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

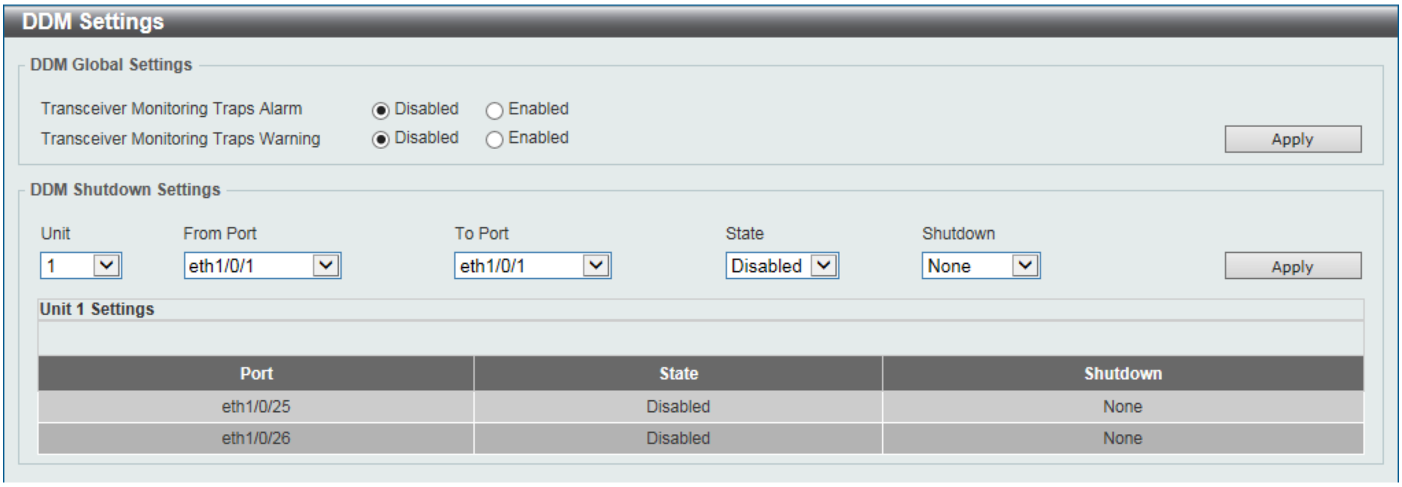
DDM

This folder contains windows that perform Digital Diagnostic Monitoring (DDM) functions on the Switch. There are windows that allow the user to view the digital diagnostic monitoring status of SFP/SFP+ modules inserting to the Switch and to configure alarm settings, warning settings, temperature threshold settings, voltage threshold settings, bias current threshold settings, Tx power threshold settings, and Rx power threshold settings.

DDM Settings

The window is used to view and configure the action that will occur for specific ports when an exceeding alarm threshold or warning threshold event is encountered.

To view the following window, click **OAM > DDM > DDM Settings**, as shown below:



DDM Settings

DDM Global Settings

Transceiver Monitoring Traps Alarm ● Disabled ○ Enabled

Transceiver Monitoring Traps Warning ● Disabled ○ Enabled

DDM Shutdown Settings

Unit: 1 From Port: eth1/0/1 To Port: eth1/0/1 State: Disabled Shutdown: None

Unit 1 Settings

Port	State	Shutdown
eth1/0/25	Disabled	None
eth1/0/26	Disabled	None

Figure 10-26 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.
Transceiver Monitoring Traps Warning	Select to enable or disable the transceiver monitoring traps warning feature here.

Click the **Apply** button to accept the changes made.

The fields that can be configured in **DDM Shutdown Settings** are described below:

Parameter	Description
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.
State	Use the drop-down menu to enable or disable the DDM state.
Shutdown	Specify whether to shut down the port, when the operating parameter exceeds the alarm or warning threshold. Options to choose from are: • **Alarm** - Shutdown the port when the configured alarm threshold range is exceeded.

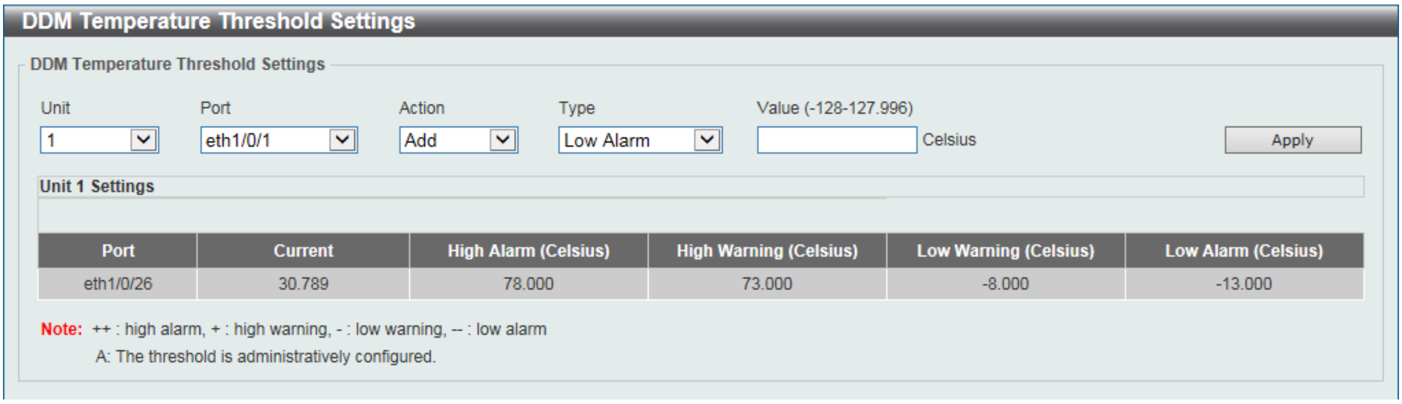
Parameter	Description
	• **Warning** - Shutdown the port when the configured warning threshold range is exceeded. • **None** - The port will never shutdown regardless if the threshold ranges are exceeded or not. By default, the **None** option is used.

Click the **Apply** button to accept the changes made.

DDM Temperature Threshold Settings

This window is used to display and configure the DDM Temperature Threshold Settings for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM Temperature Threshold Settings**, as shown below:



DDM Temperature Threshold Settings

DDM Temperature Threshold Settings

Unit: 1
Port: eth1/0/1
Action: Add
Type: Low Alarm
Value (-128-127.996): Celsius

Unit 1 Settings

Port	Current	High Alarm (Celsius)	High Warning (Celsius)	Low Warning (Celsius)	Low Alarm (Celsius)
eth1/0/26	30.789	78.000	73.000	-8.000	-13.000

Note: ++ : high alarm, + : high warning, - : low warning, -- : low alarm
A: The threshold is administratively configured.

Figure 10-27 DDM Temperature Threshold Settings Window

The fields that can be configured are described below:

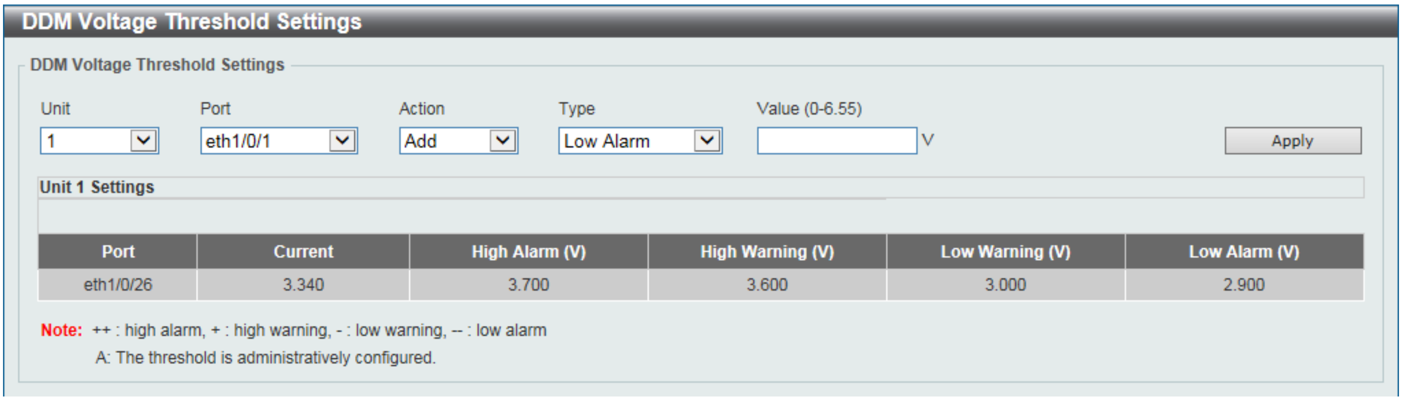
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**.
Type	Select the type of temperature threshold. Options to choose from are **Low Alarm**, **Low Warning**, **High Alarm**, and **High Warning**.
Value	Enter the threshold value. The range is from -128 to 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:



DDM Voltage Threshold Settings

DDM Voltage Threshold Settings

Unit	Port	Action	Type	Value (0-6.55)	
1	eth1/0/1	Add	Low Alarm	V	Apply

Unit 1 Settings

Port	Current	High Alarm (V)	High Warning (V)	Low Warning (V)	Low Alarm (V)
eth1/0/26	3.340	3.700	3.600	3.000	2.900

Note: ++ : high alarm, + : high warning, - : low warning, -- : low alarm
A: The threshold is administratively configured.

Figure 10-28 DDM Voltage Threshold Settings Window

The fields that can be configured are described below:

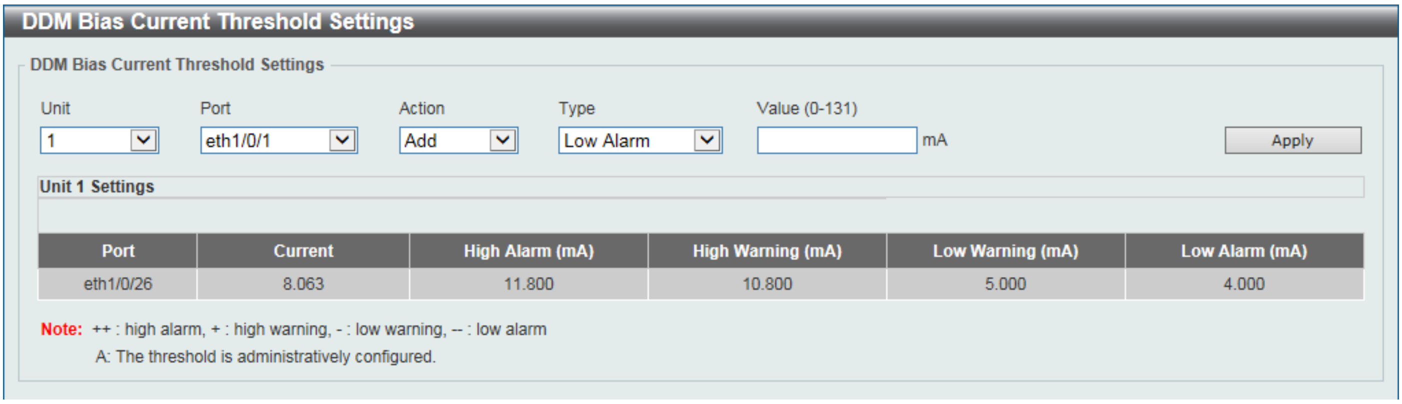
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**.
Type	Select the type of voltage threshold. Options to choose from are **Low Alarm**, **Low Warning**, **High Alarm**, and **High Warning**.
Value	Enter the threshold value. The range is from 0 to 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:



DDM Bias Current Threshold Settings

DDM Bias Current Threshold Settings

Unit	Port	Action	Type	Value (0-131)	
1	eth1/0/1	Add	Low Alarm	mA	Apply

Unit 1 Settings

Port	Current	High Alarm (mA)	High Warning (mA)	Low Warning (mA)	Low Alarm (mA)
eth1/0/26	8.063	11.800	10.800	5.000	4.000

Note: ++ : high alarm, + : high warning, - : low warning, -- : low alarm
A: The threshold is administratively configured.

Figure 10-29 DDM Bias Current Threshold Settings Window

The fields that can be configured are described below:

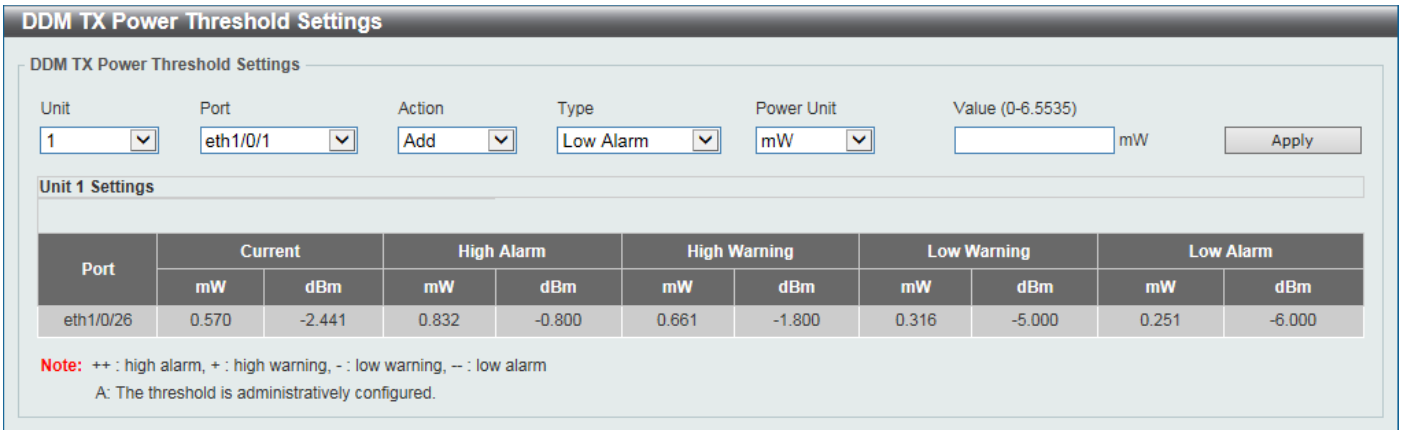
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**.
Type	Select the type of bias current threshold. Options to choose from are **Low Alarm**, **Low Warning**, **High Alarm**, and **High Warning**.
Value	Enter the threshold value. The range is from 0 to 131 mA.

Click the **Apply** button to accept the changes made.

DDM TX Power Threshold Settings

This window is used to display and configure the threshold of TX power for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM TX Power Threshold Settings**, as shown below:



DDM TX Power Threshold Settings

DDM TX Power Threshold Settings

Unit: 1
Port: eth1/0/1
Action: Add
Type: Low Alarm
Power Unit: mW
Value (0-6.5535): mW

Unit 1 Settings

Port	Current		High Alarm		High Warning		Low Warning		Low Alarm	
	mW	dBm	mW	dBm	mW	dBm	mW	dBm	mW	dBm
eth1/0/26	0.570	-2.441	0.832	-0.800	0.661	-1.800	0.316	-5.000	0.251	-6.000

Note: ++ : high alarm, + : high warning, - : low warning, -- : low alarm
A: The threshold is administratively configured.

Figure 10-30 DDM TX Power Threshold Settings Window

The fields that can be configured are described below:

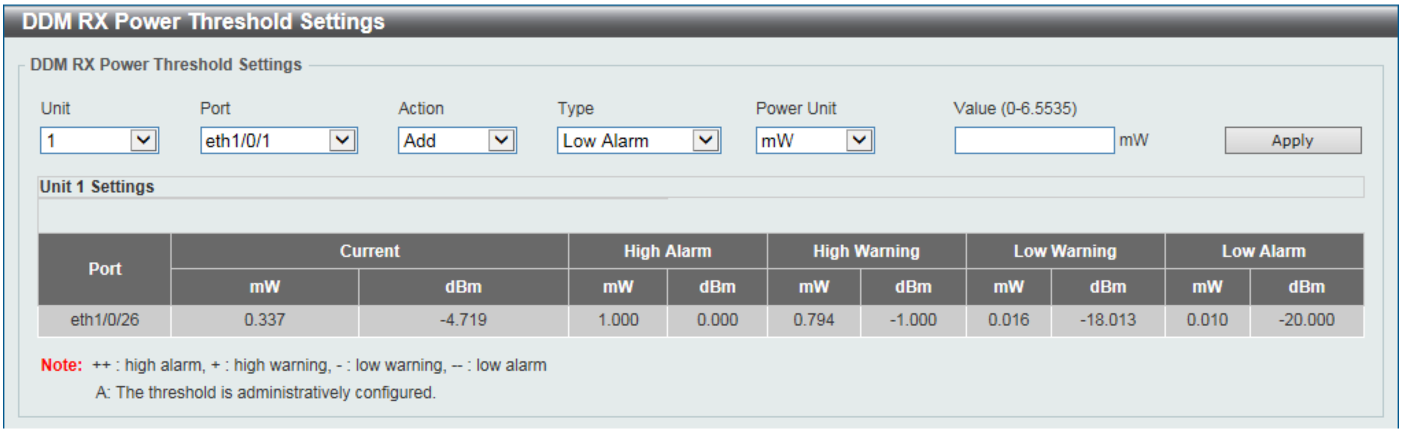
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**.
Type	Select the type of TX power threshold. Options to choose from are **Low Alarm**, **Low Warning**, **High Alarm**, and **High Warning**.
Power Unit	Select the power unit here. Options to choose from are **mW** and **dBm**.
Value	Enter the threshold value either in **mW** or **dBm** here. • When selecting **mW** in the **Power Unit** drop-down list, The range is from 0 to 6.5535. • When selecting **dBm** in the **Power Unit** drop-down list, this value must be from -40 to 8.1647.

Click the **Apply** button to accept the changes made.

DDM RX Power Threshold Settings

This window is used to display and configure the threshold of RX power for specific ports on the Switch.

To view the following window, click **OAM > DDM > DDM RX Power Threshold Settings**, as shown below:



DDM RX Power Threshold Settings

DDM RX Power Threshold Settings

Unit: 1
Port: eth1/0/1
Action: Add
Type: Low Alarm
Power Unit: mW
Value (0-6.5535): mW

Unit 1 Settings

Port	Current		High Alarm		High Warning		Low Warning		Low Alarm	
	mW	dBm	mW	dBm	mW	dBm	mW	dBm	mW	dBm
eth1/0/26	0.337	-4.719	1.000	0.000	0.794	-1.000	0.016	-18.013	0.010	-20.000

Note: ++ : high alarm, + : high warning, - : low warning, -- : low alarm
A: The threshold is administratively configured.

Figure 10-31 DDM RX Power Threshold Settings Window

The fields that can be configured are described below:

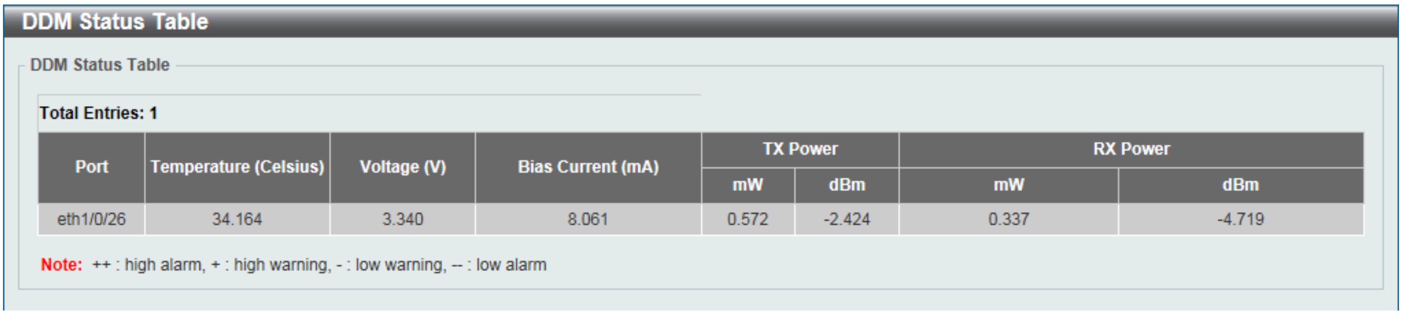
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
Port	Select the port used for the configuration here.
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**.
Type	Select the type of RX power threshold. Options to choose from are **Low Alarm**, **Low Warning**, **High Alarm**, and **High Warning**.
Power Unit	Select the power unit here. Options to choose from are **mW** and **dBm**.
Value	Enter the threshold value either in **mW** or **dBm** here. • When selecting **mW** in the **Power Unit** drop-down list, The range is from 0 to 6.5535. • When selecting dBm in the Power Unit drop-down list, this value must be from -40 to 8.1647.

Click the **Apply** button to accept the changes made.

DDM Status Table

This window is used to display the current operating digital diagnostic monitoring parameters and their values on the SFP module for specified ports.

To view the following window, click **OAM > DDM > DDM Status Table**, as shown below:



DDM Status Table

DDM Status Table

Total Entries: 1

Port	Temperature (Celsius)	Voltage (V)	Bias Current (mA)	TX Power		RX Power	
				mW	dBm	mW	dBm
eth1/0/26	34.164	3.340	8.061	0.572	-2.424	0.337	-4.719

Note: ++ : high alarm, + : high warning, - : low warning, -- : low alarm

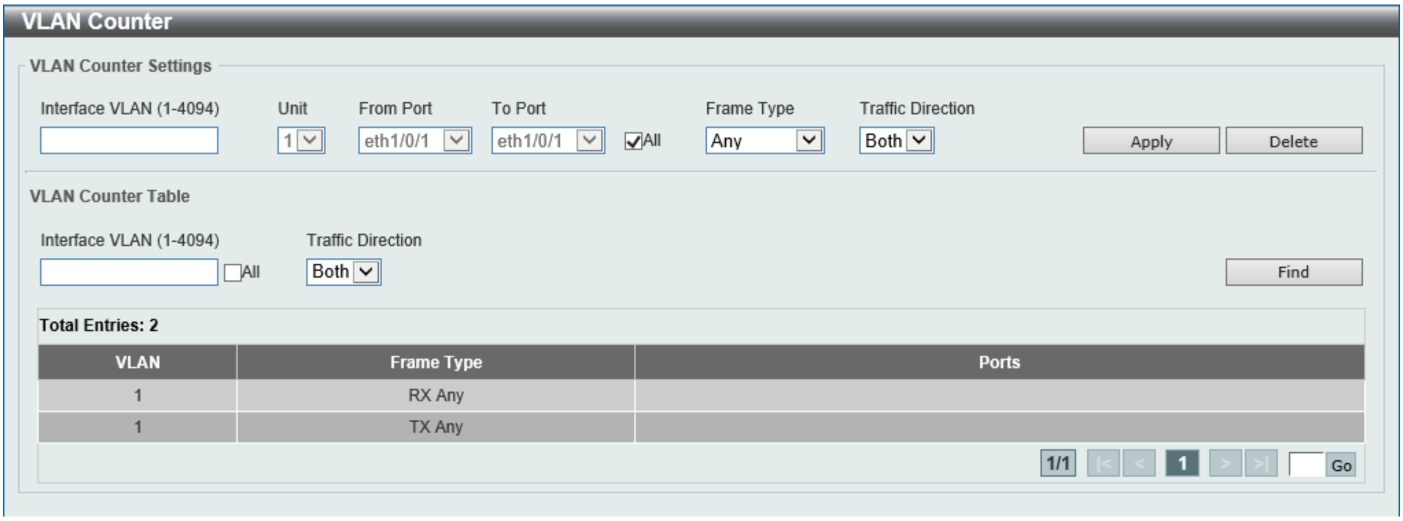
Figure 10-32 DDM Status Table Window

11. Monitoring

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:



VLAN Counter

VLAN Counter Settings

Interface VLAN (1-4094):
Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1 ☑All
Frame Type: Any
Traffic Direction: Both

VLAN Counter Table

Interface VLAN (1-4094): □All
Traffic Direction: Both

Total Entries: 2

VLAN	Frame Type	Ports
1	RX Any	
1	TX Any	

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.
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 the four frame types mentioned above.
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 (or entries) 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 in the display 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 to display here. Options to choose from are: • **RX -** Specifies to display ingress traffic count settings. • **TX** - Specifies to display egress traffic count settings. • **Both** - Specifies to display ingress and egress traffic count settings.

Click the **Find** button to display entries in the table based on the information entered/selected.

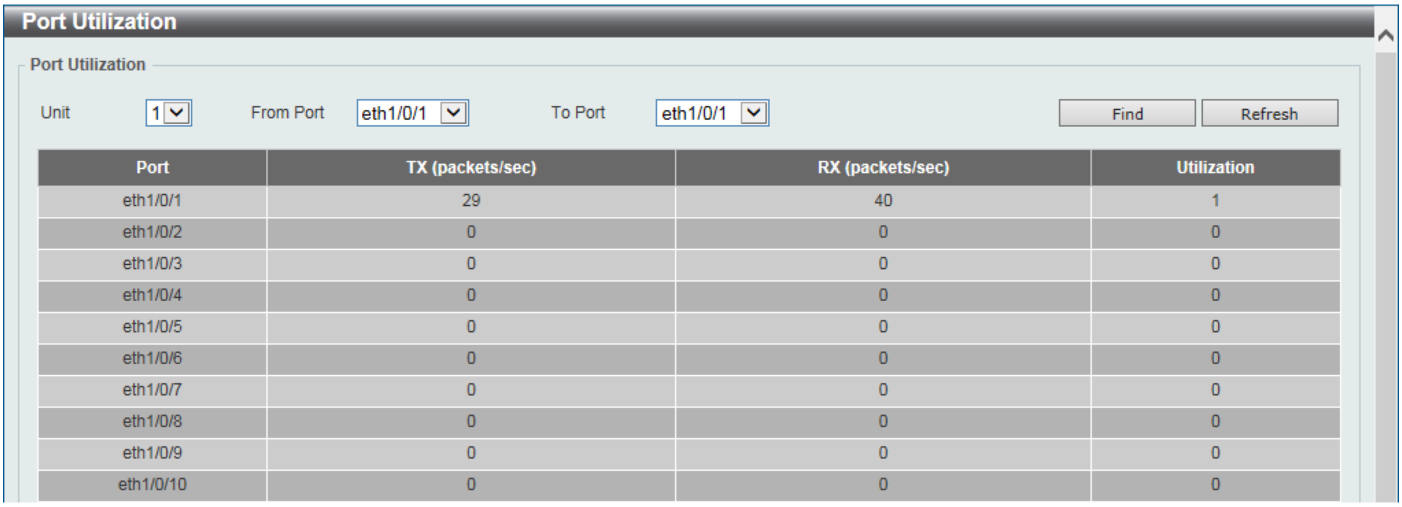
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

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:



Port Utilization

Port Utilization

Unit: 1 From Port: eth1/0/1 To Port: eth1/0/1

Port	TX (packets/sec)	RX (packets/sec)	Utilization
eth1/0/1	29	40	1
eth1/0/2	0	0	0
eth1/0/3	0	0	0
eth1/0/4	0	0	0
eth1/0/5	0	0	0
eth1/0/6	0	0	0
eth1/0/7	0	0	0
eth1/0/8	0	0	0
eth1/0/9	0	0	0
eth1/0/10	0	0	0

Figure 11-2 Port Utilization Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used here.
From Port - To Port	Select the range of ports that will be used here.

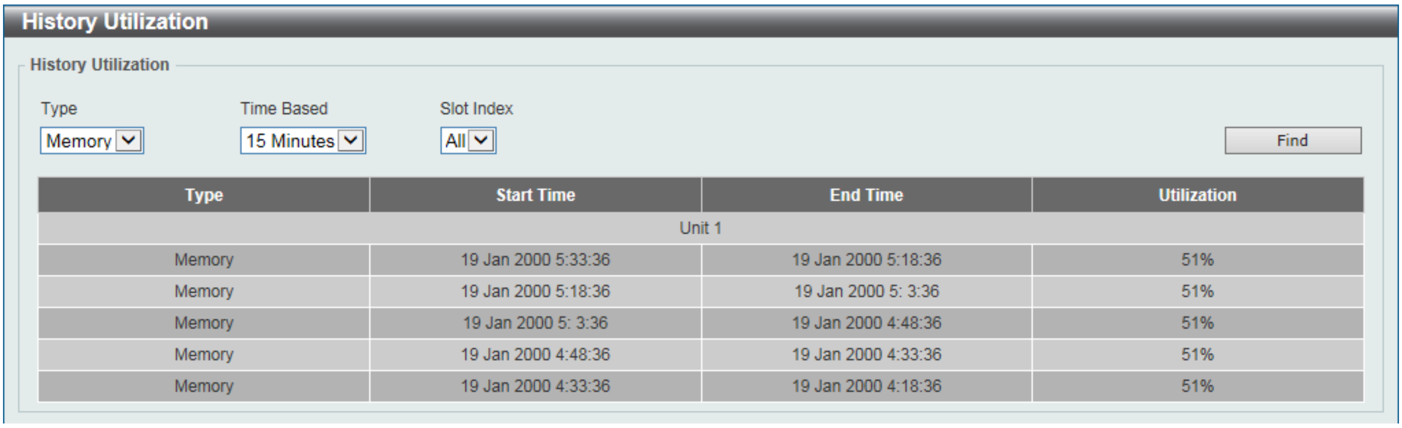
Click the **Find** button to display entries in the table based on the information entered/selected.

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:



History Utilization

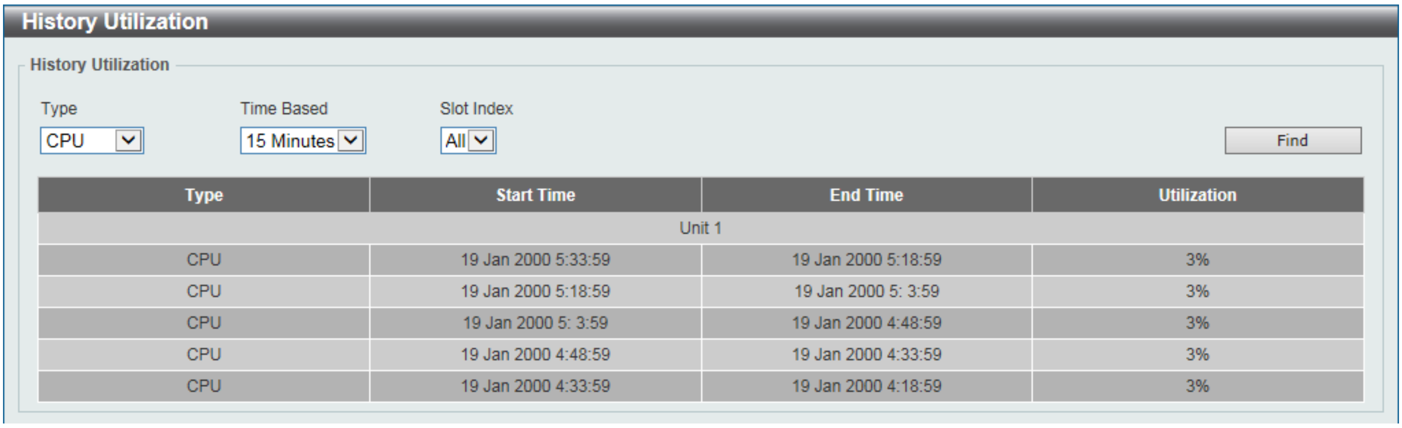
History Utilization

Type	Time Based	Slot Index
Memory	15 Minutes	All

Type	Start Time	End Time	Utilization
Unit 1			
Memory	19 Jan 2000 5:33:36	19 Jan 2000 5:18:36	51%
Memory	19 Jan 2000 5:18:36	19 Jan 2000 5: 3:36	51%
Memory	19 Jan 2000 5: 3:36	19 Jan 2000 4:48:36	51%
Memory	19 Jan 2000 4:48:36	19 Jan 2000 4:33:36	51%
Memory	19 Jan 2000 4:33:36	19 Jan 2000 4:18:36	51%

Figure 11-3 History Utilization (Memory) Window

After selecting **CPU** as the **Type**, the following window will appear:



History Utilization

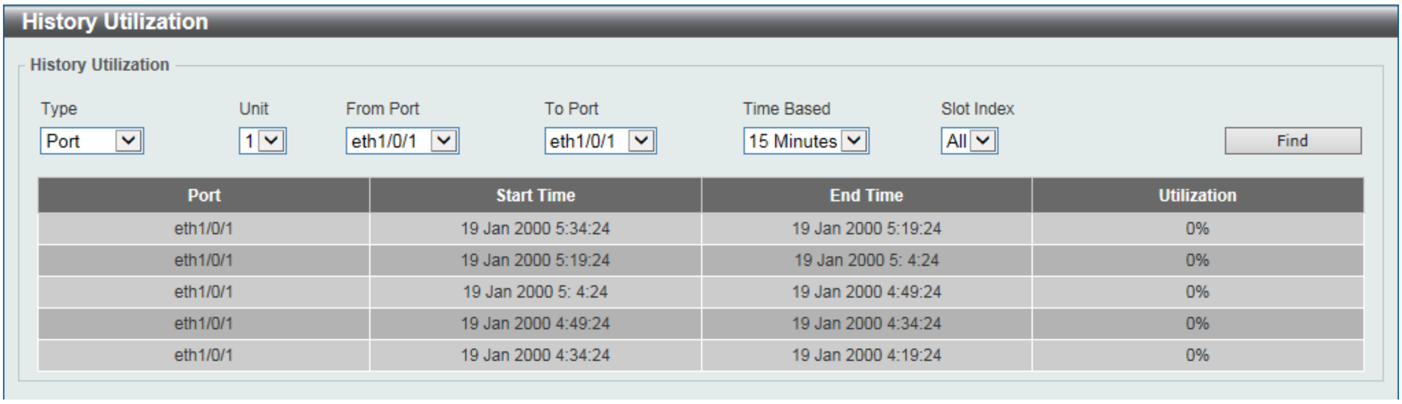
History Utilization

Type	Time Based	Slot Index
CPU	15 Minutes	All

Type	Start Time	End Time	Utilization
Unit 1			
CPU	19 Jan 2000 5:33:59	19 Jan 2000 5:18:59	3%
CPU	19 Jan 2000 5:18:59	19 Jan 2000 5: 3:59	3%
CPU	19 Jan 2000 5: 3:59	19 Jan 2000 4:48:59	3%
CPU	19 Jan 2000 4:48:59	19 Jan 2000 4:33:59	3%
CPU	19 Jan 2000 4:33:59	19 Jan 2000 4:18:59	3%

Figure 11-4 History Utilization (CPU) Window

After selecting **Port** as the **Type**, the following window will appear:



History Utilization

History Utilization

Type	Unit	From Port	To Port	Time Based	Slot Index
Port	1	eth1/0/1	eth1/0/1	15 Minutes	All

Port	Start Time	End Time	Utilization
eth1/0/1	19 Jan 2000 5:34:24	19 Jan 2000 5:19:24	0%
eth1/0/1	19 Jan 2000 5:19:24	19 Jan 2000 5: 4:24	0%
eth1/0/1	19 Jan 2000 5: 4:24	19 Jan 2000 4:49:24	0%
eth1/0/1	19 Jan 2000 4:49:24	19 Jan 2000 4:34:24	0%
eth1/0/1	19 Jan 2000 4:34:24	19 Jan 2000 4:19:24	0%

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.

Parameter	Description
	- **CPU** - Specifies to display the historical CPU utilization information. - **Port** - Specifies to display the historical port utilization information.
Unit	Select the Switch unit that will be used here.
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 slots of 15-minute based information. - **1 Day** - Specifies to display slots of daily-based information. 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. - After selecting to use 15-minute slots, the options to choose from are **All**, and **1** to **5**. - After selecting to use 1-day slots, the options to choose from are **All**, **1**, and **2**.

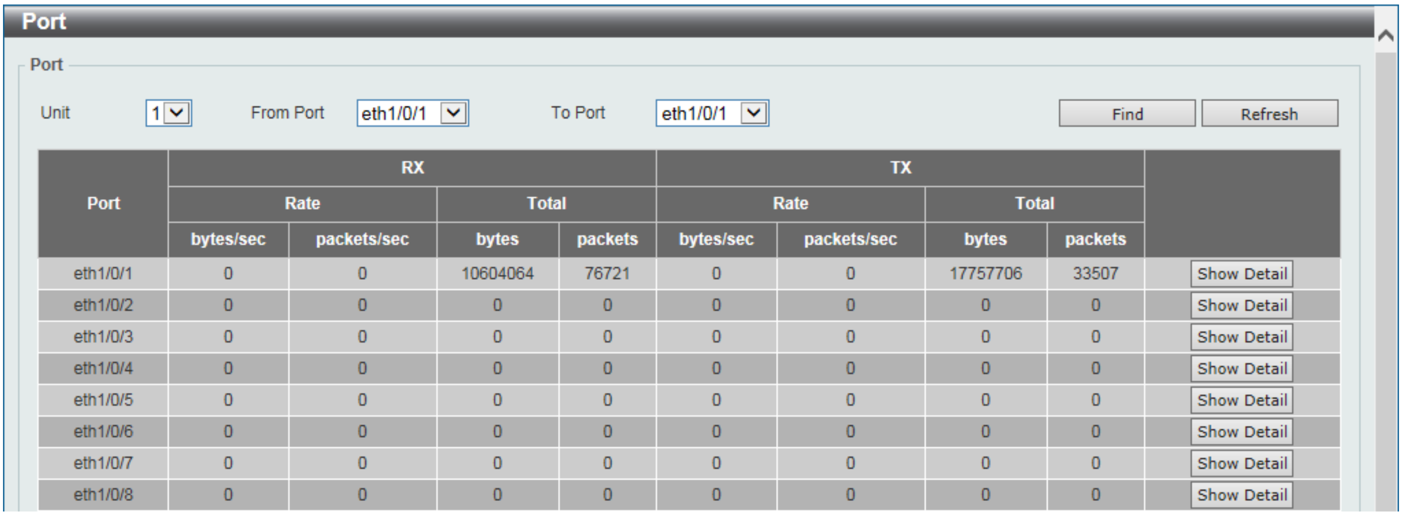
Click the **Find** button to display entries in the table based on the information selected.

Statistics

Port

This window is used to view the port statistics information.

To view the following window, click **Monitoring > Statistics > Port**, as shown below:



Unit 1
From Port eth1/0/1
To Port eth1/0/1

Port	RX				TX				
	Rate		Total		Rate		Total		
	bytes/sec	packets/sec	bytes	packets	bytes/sec	packets/sec	bytes	packets	
eth1/0/1	0	0	10604064	76721	0	0	17757706	33507	Show Detail
eth1/0/2	0	0	0	0	0	0	0	0	Show Detail
eth1/0/3	0	0	0	0	0	0	0	0	Show Detail
eth1/0/4	0	0	0	0	0	0	0	0	Show Detail
eth1/0/5	0	0	0	0	0	0	0	0	Show Detail
eth1/0/6	0	0	0	0	0	0	0	0	Show Detail
eth1/0/7	0	0	0	0	0	0	0	0	Show Detail
eth1/0/8	0	0	0	0	0	0	0	0	Show Detail

Figure 11-6 Port Window

The fields that can be configured are described below:

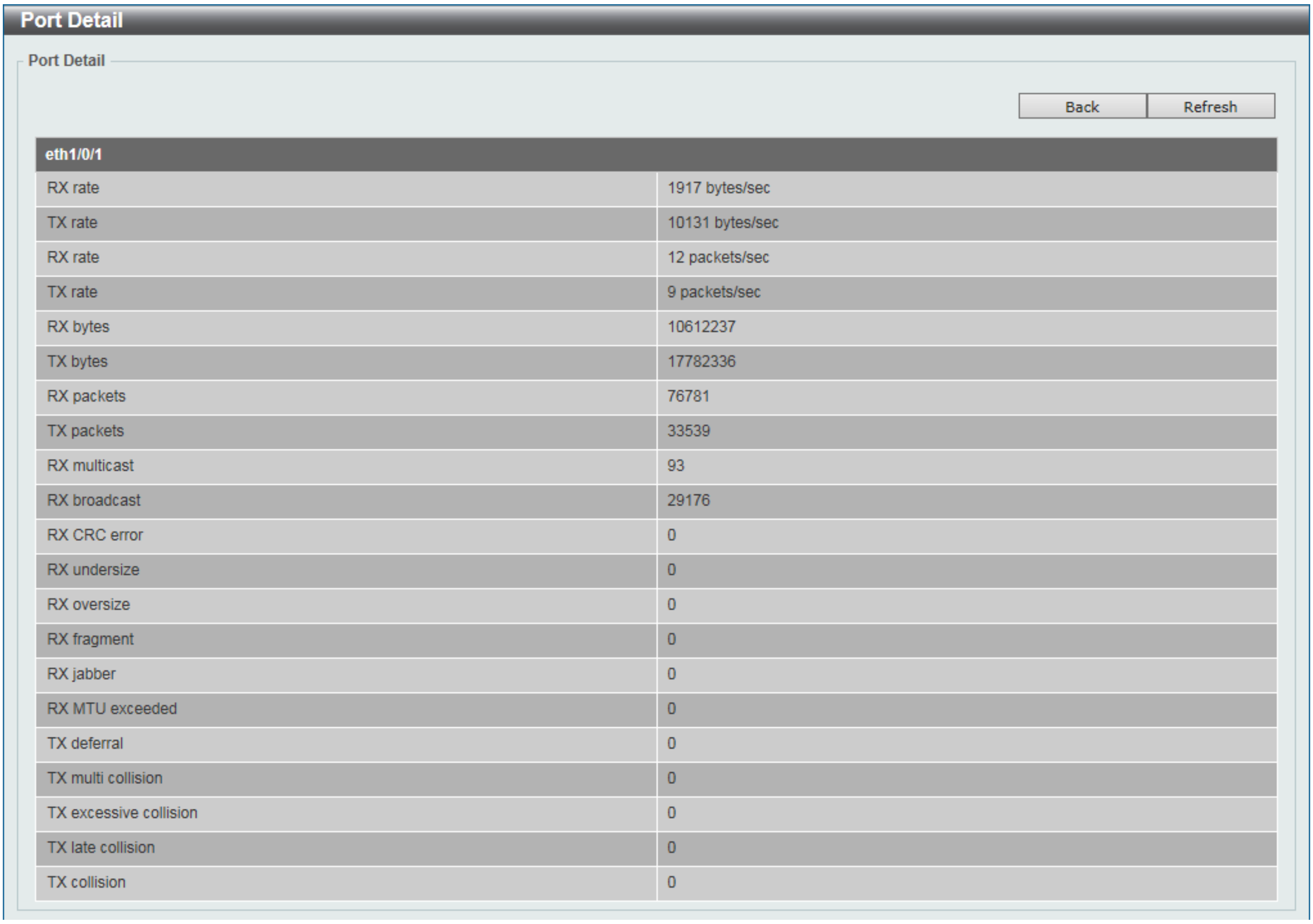
Parameter	Description
Unit	Select the Switch unit that will be used in this display here.
From Port - To Port	Select the range of ports that will be used in this display here.

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 detailed statistics information on the specified port.

After clicking the **Show Detail** button, the following window will appear:



eth1/0/1	
RX rate	1917 bytes/sec
TX rate	10131 bytes/sec
RX rate	12 packets/sec
TX rate	9 packets/sec
RX bytes	10612237
TX bytes	17782336
RX packets	76781
TX packets	33539
RX multicast	93
RX broadcast	29176
RX CRC error	0
RX undersize	0
RX oversize	0
RX fragment	0
RX jabber	0
RX MTU exceeded	0
TX deferral	0
TX multi collision	0
TX excessive collision	0
TX late collision	0
TX collision	0

Figure 11-7 Port (Show Detail) Window

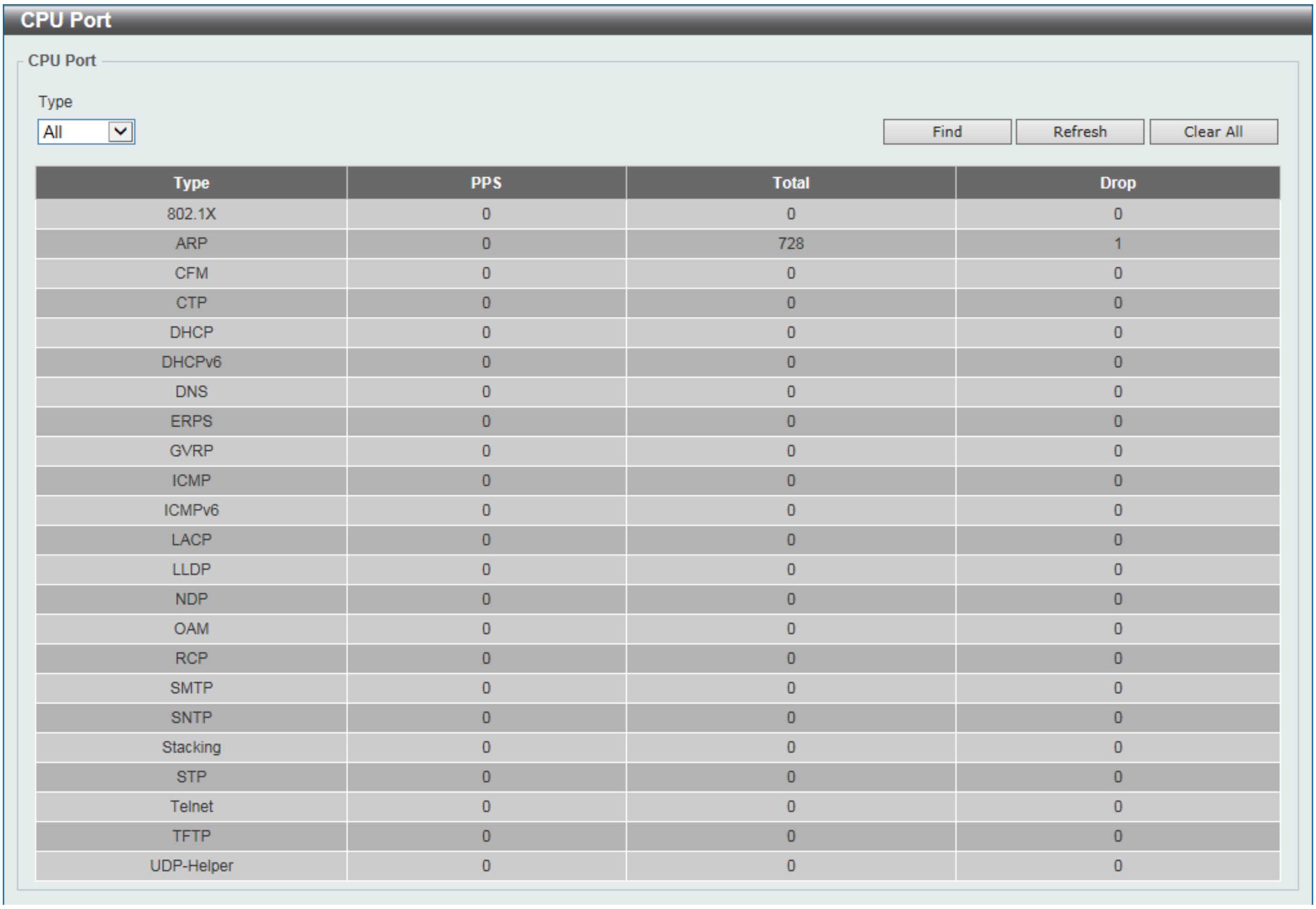
Click the **Back** button to return to the previous window.

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:



Type	PPS	Total	Drop
802.1X	0	0	0
ARP	0	728	1
CFM	0	0	0
CTP	0	0	0
DHCP	0	0	0
DHCPv6	0	0	0
DNS	0	0	0
ERPS	0	0	0
GVRP	0	0	0
ICMP	0	0	0
ICMPv6	0	0	0
LACP	0	0	0
LLDP	0	0	0
NDP	0	0	0
OAM	0	0	0
RCP	0	0	0
SMTP	0	0	0
SNTP	0	0	0
Stacking	0	0	0
STP	0	0	0
Telnet	0	0	0
TFTP	0	0	0
UDP-Helper	0	0	0

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**.

Click the **Find** button to display entries in the table based on the information selected.

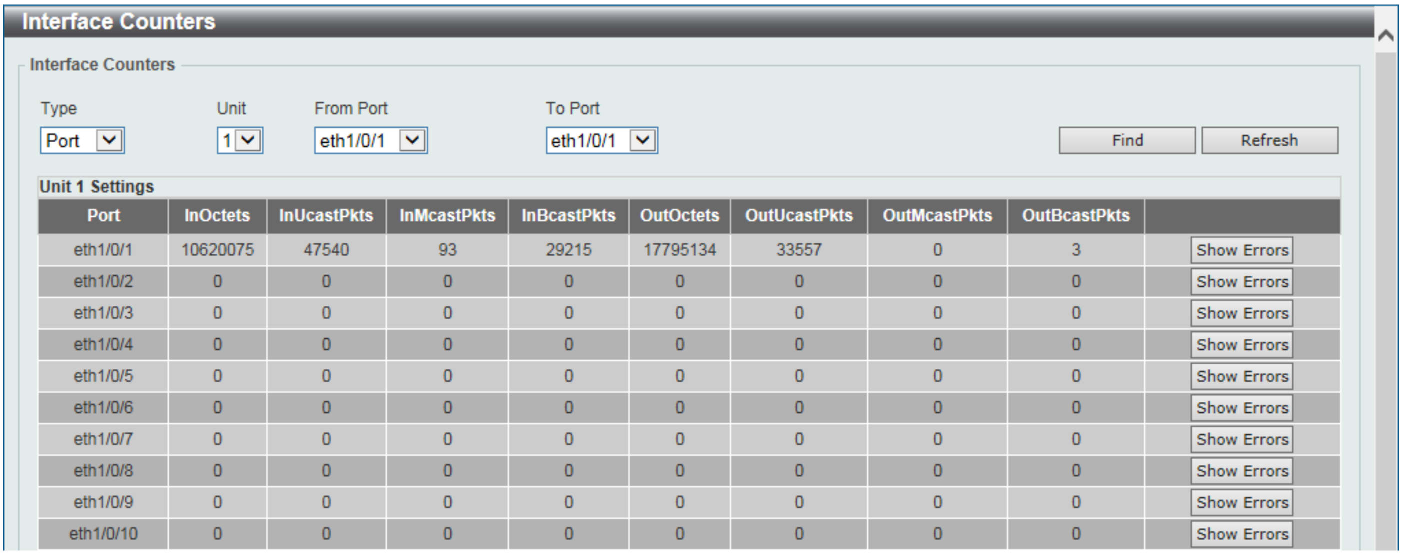
Click the **Refresh** button to refresh the information displayed in the table.

Click the **Clear All** button 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:

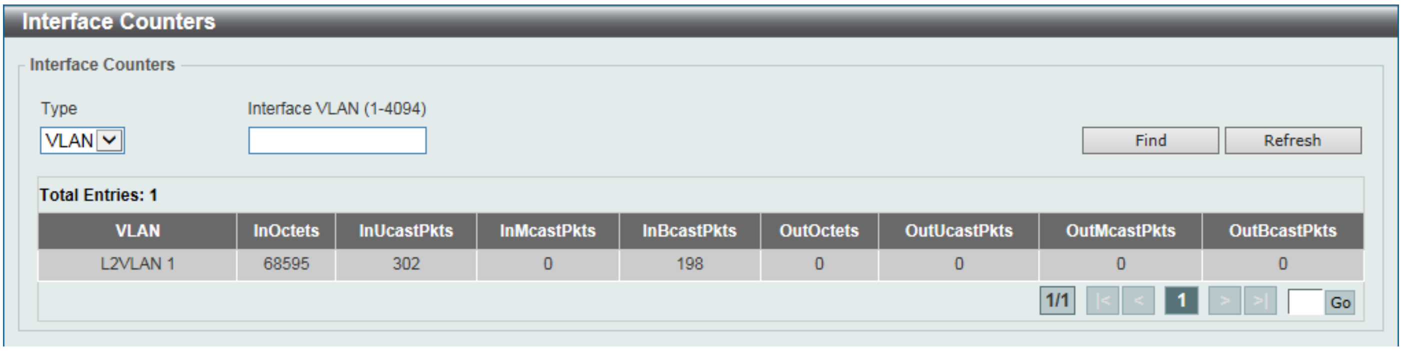


Type: Port
Unit: 1
From Port: eth1/0/1
To Port: eth1/0/1

Unit 1 Settings

Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts	
eth1/0/1	10620075	47540	93	29215	17795134	33557	0	3	Show Errors
eth1/0/2	0	0	0	0	0	0	0	0	Show Errors
eth1/0/3	0	0	0	0	0	0	0	0	Show Errors
eth1/0/4	0	0	0	0	0	0	0	0	Show Errors
eth1/0/5	0	0	0	0	0	0	0	0	Show Errors
eth1/0/6	0	0	0	0	0	0	0	0	Show Errors
eth1/0/7	0	0	0	0	0	0	0	0	Show Errors
eth1/0/8	0	0	0	0	0	0	0	0	Show Errors
eth1/0/9	0	0	0	0	0	0	0	0	Show Errors
eth1/0/10	0	0	0	0	0	0	0	0	Show Errors

Figure 11-9 Interface Counters (Port) Window



Type: VLAN
Interface VLAN (1-4094):

Total Entries: 1

VLAN	InOctets	InUcastPkts	InMcastPkts	InBcastPkts	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
L2VLAN 1	68595	302	0	198	0	0	0	0

Figure 11-10 Interface Counters (VLAN) Window

The fields that can be configured are described below:

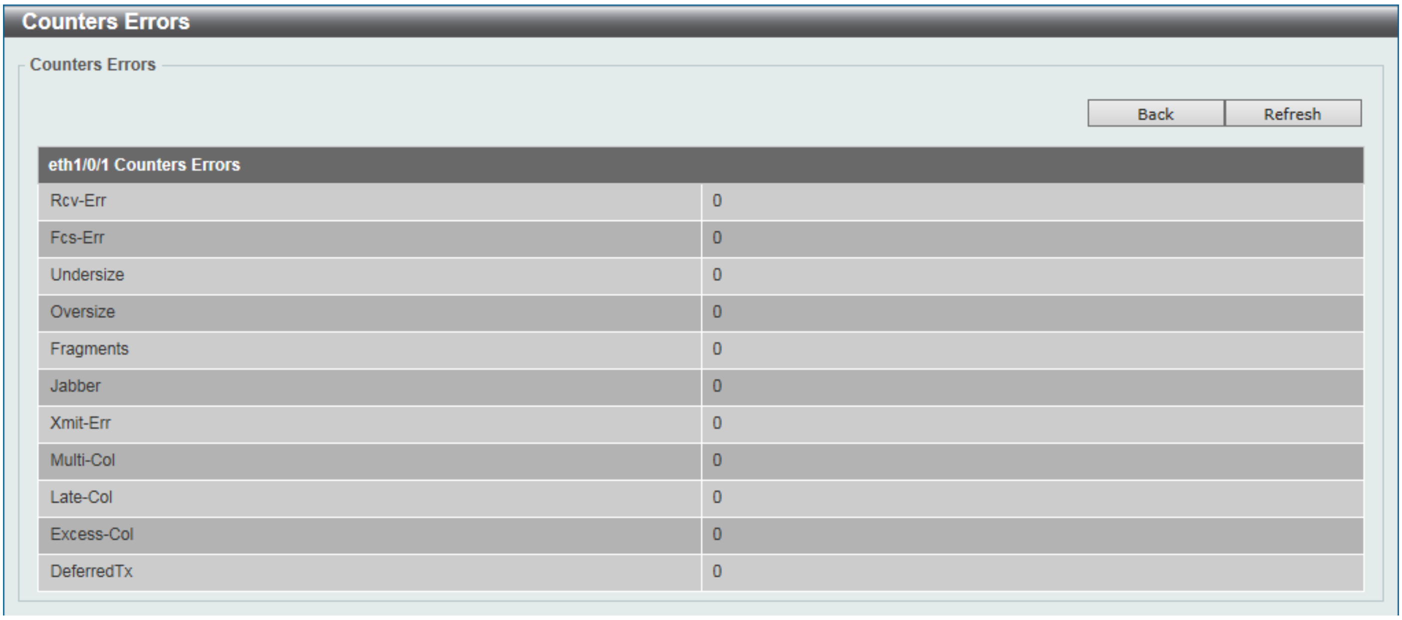
Parameter	Description
Type	Select the type of information to display here. Options to choose from are **Port** and **VLAN**.
Port	Select this option to display interface counters per-port. • **Unit** - Select the Switch unit that will be used in this display here. • **From Port / To Port** - Select the range of ports that will be used in this display here.
VLAN	Select this option to display interface counters per-VLAN. • **Interface VLAN** - Enter the ID of the interface VLAN to display here.

Click the **Find** button to display entries in the table based on the information selected.

Click the **Refresh** button to refresh the information displayed in the table.

Click the **Show Errors** button to view detailed error information on the specified port.

After clicking the **Show Errors** button, the following window will appear:



eth1/0/1 Counters Errors	
Rcv-Err	0
Fcs-Err	0
Undersize	0
Oversize	0
Fragments	0
Jabber	0
Xmit-Err	0
Multi-Col	0
Late-Col	0
Excess-Col	0
DeferredTx	0

Figure 11-11 Interface Counters (Show Errors) Window

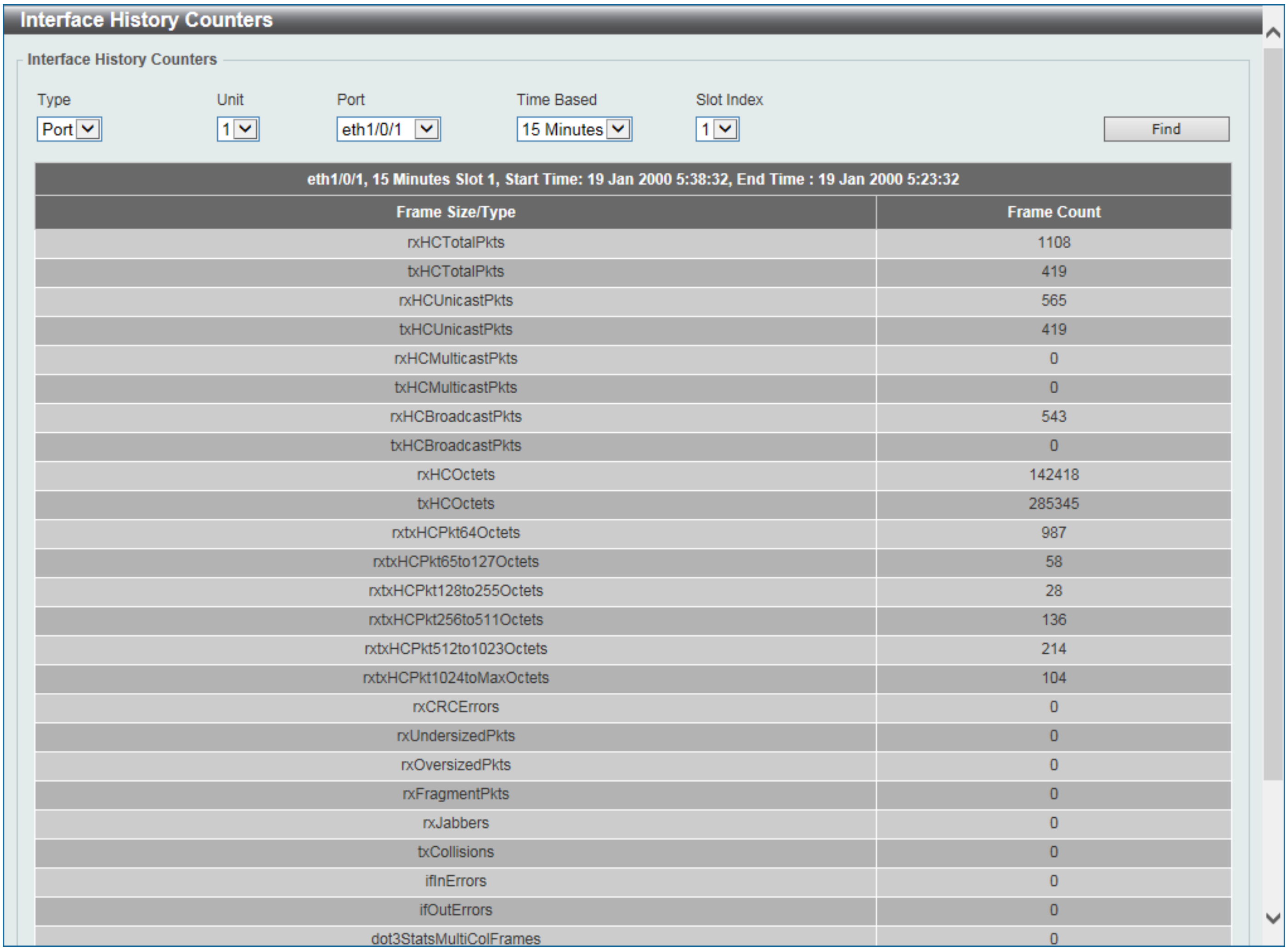
Click the **Back** button to return to the previous window.

Click the **Refresh** button to refresh the information displayed in the table.

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:



Interface History Counters

Interface History Counters

Type: Port
Unit: 1
Port: eth1/0/1
Time Based: 15 Minutes
Slot Index: 1

eth1/0/1, 15 Minutes Slot 1, Start Time: 19 Jan 2000 5:38:32, End Time : 19 Jan 2000 5:23:32

Frame Size/Type	Frame Count
rxHCTotalPkts	1108
txHCTotalPkts	419
rxHCUnicastPkts	565
txHCUnicastPkts	419
rxHCMulticastPkts	0
txHCMulticastPkts	0
rxHCBroadcastPkts	543
txHCBroadcastPkts	0
rxHCOctets	142418
txHCOctets	285345
rxtxHCPkt64Octets	987
rxtxHCPkt65to127Octets	58
rxtxHCPkt128to255Octets	28
rxtxHCPkt256to511Octets	136
rxtxHCPkt512to1023Octets	214
rxtxHCPkt1024toMaxOctets	104
rxCRCErrors	0
rxUndersizedPkts	0
rxOversizedPkts	0
rxFragmentPkts	0
rxJabbers	0
txCollisions	0
ifInErrors	0
ifOutErrors	0
dot3StatsMultiColFrames	0

Figure 11-12 Interface History Counters (Port) Window

The fields that can be configured are described below:

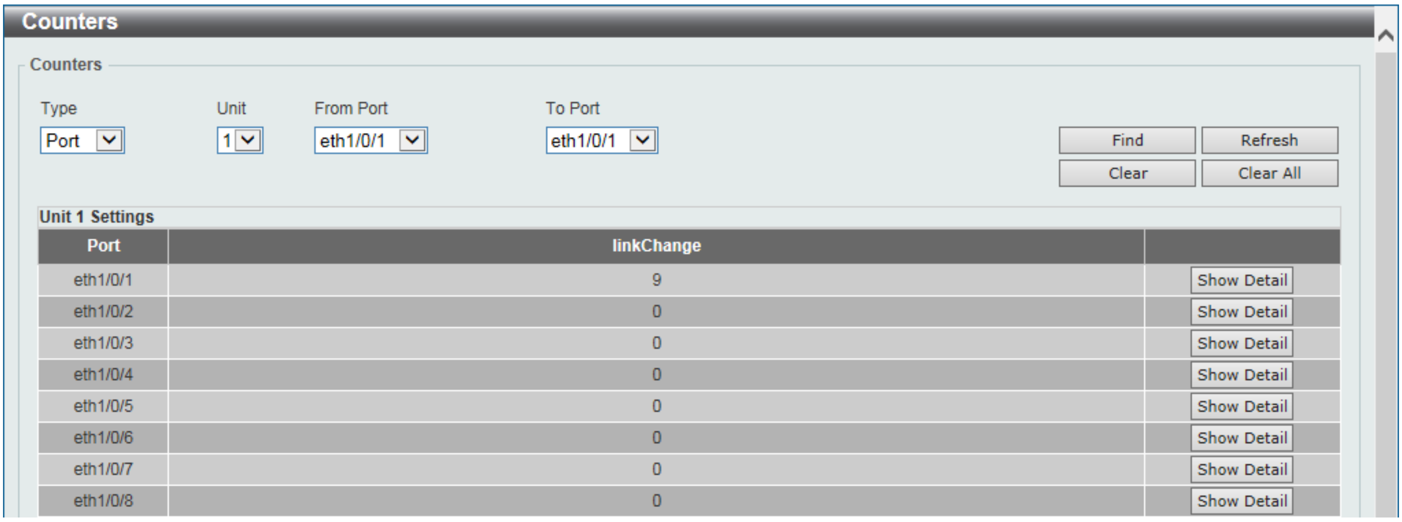
Parameter	Description
Type	Select the type of information to display here.
Unit	Select the Switch unit that will be used in this display here.
Port	Select the port that will be used in this display here.
Time Based	Select the time-based statistical count value here. Options to choose from are: • **15 Minutes -** Specifies to display slots of 15-minute based information. • **1 Day -** Specifies to display slots of daily-based information. 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. • After selecting to use 15-minute slots, the options to choose from are **All**, and **1** to **5**. • After selecting to use 1-day slots, the options to choose from are **1** and **2**.

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:



Counters

Counters

Type: Port

Unit: 1

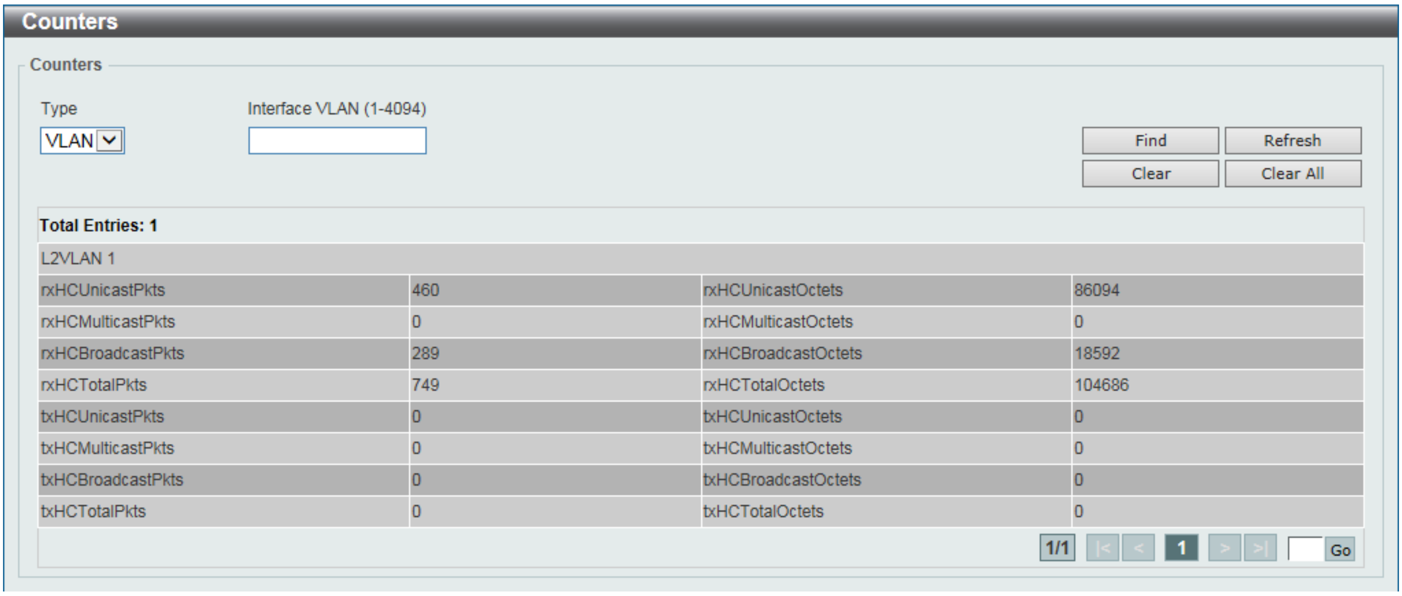
From Port: eth1/0/1

To Port: eth1/0/1

Unit 1 Settings

Port	linkChange	
eth1/0/1	9	Show Detail
eth1/0/2	0	Show Detail
eth1/0/3	0	Show Detail
eth1/0/4	0	Show Detail
eth1/0/5	0	Show Detail
eth1/0/6	0	Show Detail
eth1/0/7	0	Show Detail
eth1/0/8	0	Show Detail

Figure 11-13 Counters (Port) Window



Counters

Counters

Type: VLAN

Interface VLAN (1-4094):

Total Entries: 1

L2VLAN 1

rxHCUnicastPkts	460	rxHCUnicastOctets	86094
rxHCMulticastPkts	0	rxHCMulticastOctets	0
rxHCBroadcastPkts	289	rxHCBroadcastOctets	18592
rxHCTotalPkts	749	rxHCTotalOctets	104686
txHCUnicastPkts	0	txHCUnicastOctets	0
txHCMulticastPkts	0	txHCMulticastOctets	0
txHCBroadcastPkts	0	txHCBroadcastOctets	0
txHCTotalPkts	0	txHCTotalOctets	0

Figure 11-14 Counters (VLAN) 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 **Port** and **VLAN**.
Port	Select this option to display counters per-port. • **Unit** - Select the Switch unit that will be used in this display here. • **From Port / To Port** - Select the range of ports that will be used in this display here.
VLAN	Select this option to display counters per-VLAN.

Parameter	Description
	- **Interface VLAN** - Enter the ID of the interface VLAN to display here.

Click the **Find** button to display entries in the table based on the information selected.

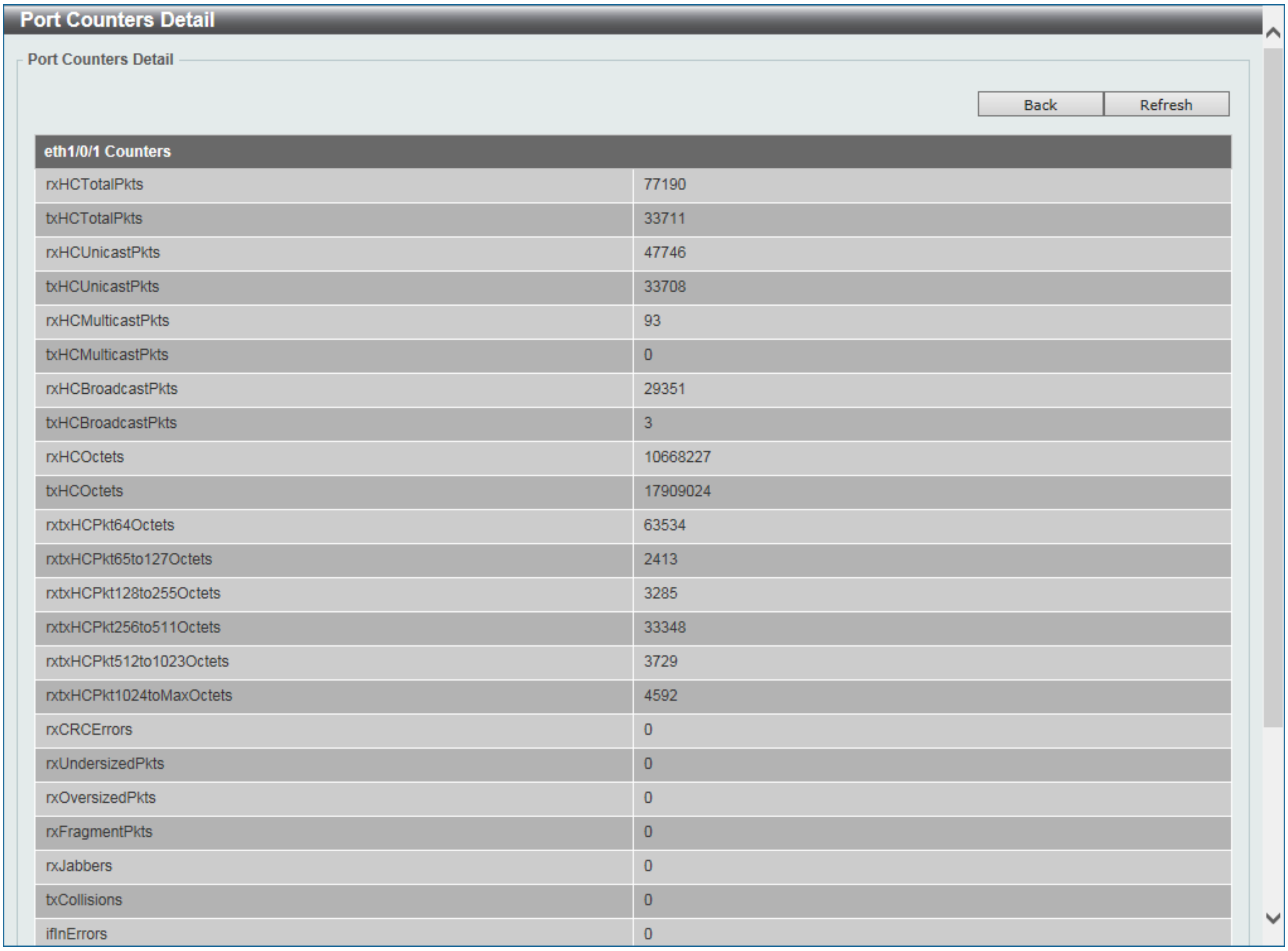
Click the **Refresh** button to refresh the counter information displayed in the table.

Click the **Clear** button clear the counter information displayed in the table based on the information selected.

Click the **Clear All** button clear all the counter information displayed in the table.

Click the **Show Detail** button to view detailed counter information on the specified port.

After clicking the **Show Detail** button, the following window will appear:



eth1/0/1 Counters	
rxHCTotalPkts	77190
txHCTotalPkts	33711
rxHCUnicastPkts	47746
txHCUnicastPkts	33708
rxHCMulticastPkts	93
txHCMulticastPkts	0
rxHCBroadcastPkts	29351
txHCBroadcastPkts	3
rxHCOctets	10668227
txHCOctets	17909024
rxtxHCPkt64Octets	63534
rxtxHCPkt65to127Octets	2413
rxtxHCPkt128to255Octets	3285
rxtxHCPkt256to511Octets	33348
rxtxHCPkt512to1023Octets	3729
rxtxHCPkt1024toMaxOctets	4592
rxCRCErrors	0
rxUndersizedPkts	0
rxOversizedPkts	0
rxFragmentPkts	0
rxJabbers	0
txCollisions	0
ifInErrors	0

Figure 11-15 Counters (Show Detail) Window

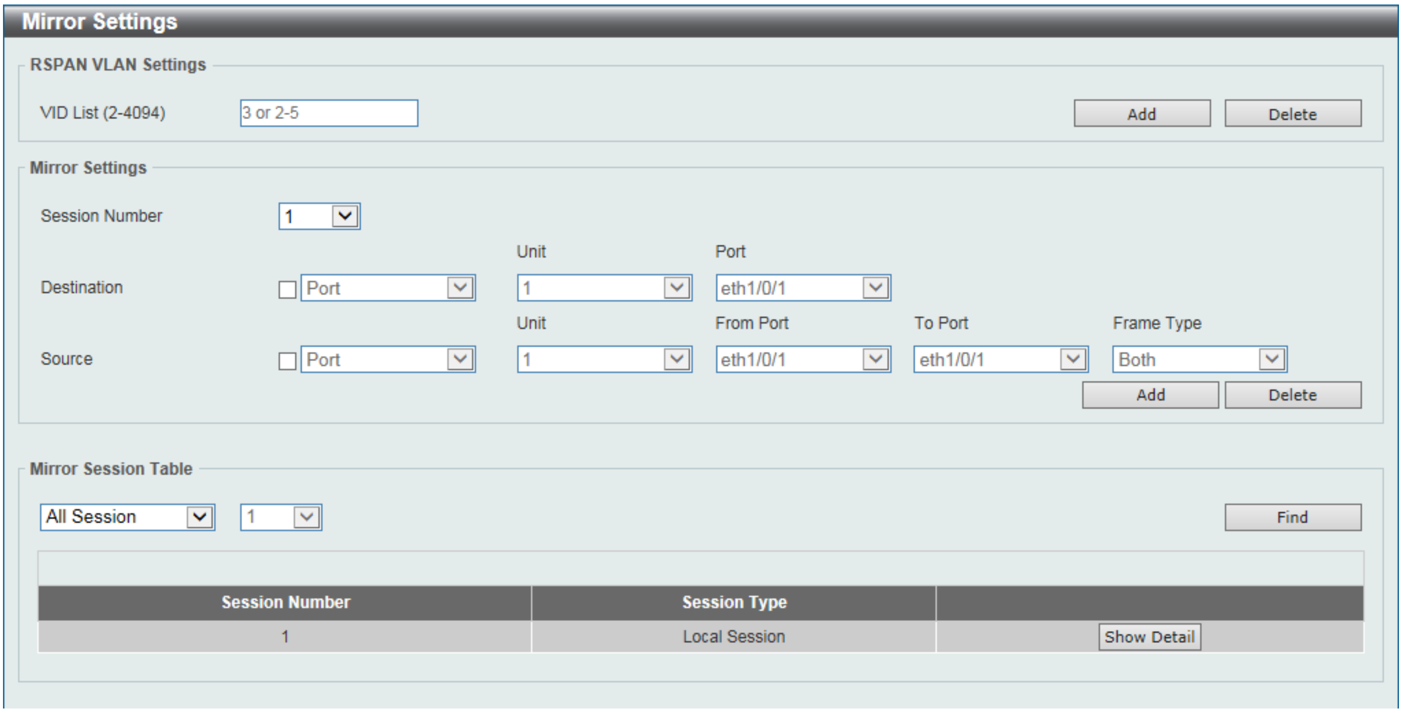
Click the **Back** button to return to the previous window.

Click the **Refresh** button to refresh the information displayed in the table.

Mirror Settings

This window is used to display and configure the mirror feature's settings. The Switch allows users to copy frames transmitted and received on a port and redirect the copies to another port. Attach a monitoring device to the mirroring port, such as a sniffer or an RMON probe, to view details about the packets passing through the first port. This is useful for network monitoring and troubleshooting purposes.

To view the following window, click **Monitoring > Mirror Settings**, as shown below:



Mirror Settings

RSPAN VLAN Settings

VID List (2-4094): 3 or 2-5

Add | Delete

Mirror Settings

Session Number: 1

Destination: □ Port; Unit: 1; Port: eth1/0/1

Source: □ Port; Unit: 1; From Port: eth1/0/1; To Port: eth1/0/1; Frame Type: Both

Add | Delete

Mirror Session Table

All Session; 1

Find

Session Number	Session Type	
1	Local Session	Show Detail

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. The range is from 1 to 4.
Destination	Select 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** - After selecting this option, select the Switch **Unit** ID, and destination **Port** number from the drop-down menus. • **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 range is from 2 to 4094.
Source	Select 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** - 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**, and **TX**. When selecting **Both**, traffic in both the incoming and outgoing

Parameter	Description
	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. • **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. The only frame type supported is **RX**. • **Remote VLAN** - After selecting this option, enter the **VID** in the space provided. The range is from 2 to 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.

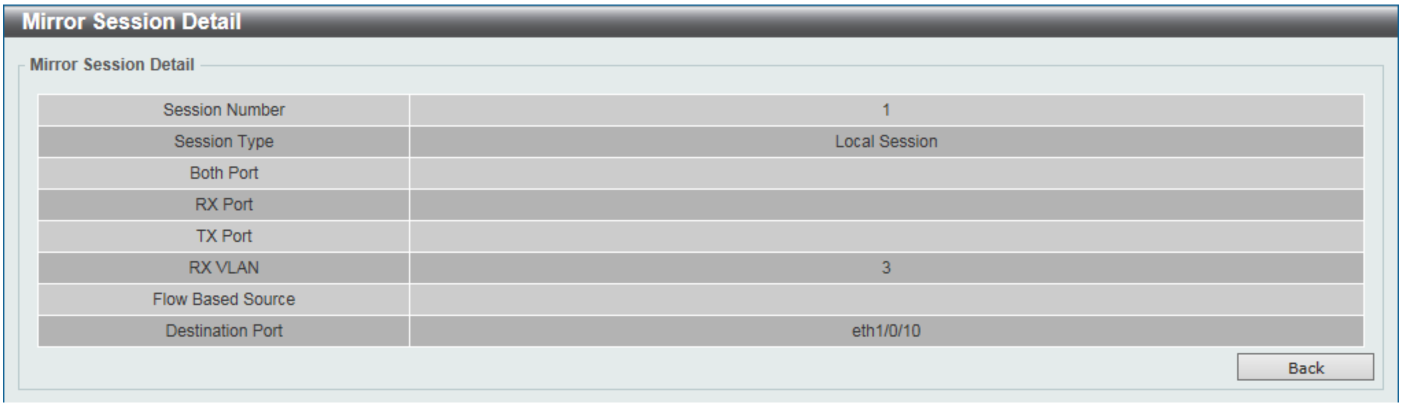
The fields that can be configured for **Mirror Session Table** are described below:

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 detailed information about the mirror session.

After clicking the **Show Detail** button, the following window will appear:



Mirror Session Detail

Mirror Session Detail

Session Number	1
Session Type	Local Session
Both Port	
RX Port	
TX Port	
RX VLAN	3
Flow Based Source	
Destination Port	eth1/0/10

Figure 11-17 Mirror Settings (Show Detail) Window

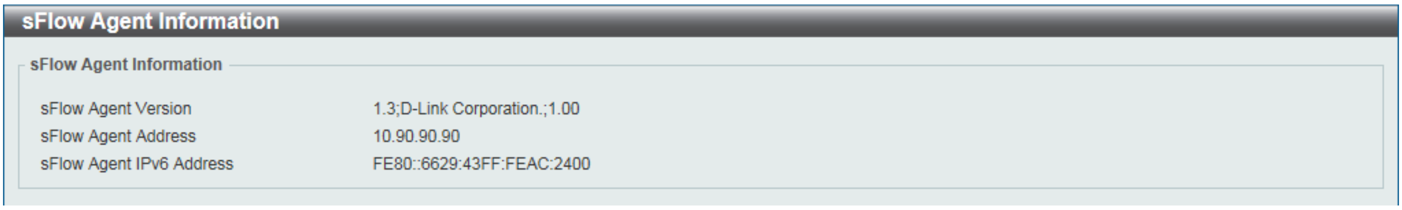
Click the **Back** button to return to the previous page.

sFlow

sFlow Agent Information

This window is used to view the sFlow agent information.

To view the following window, click **Monitoring > sFlow > sFlow Agent Information**, as shown below:



sFlow Agent Information

sFlow Agent Information

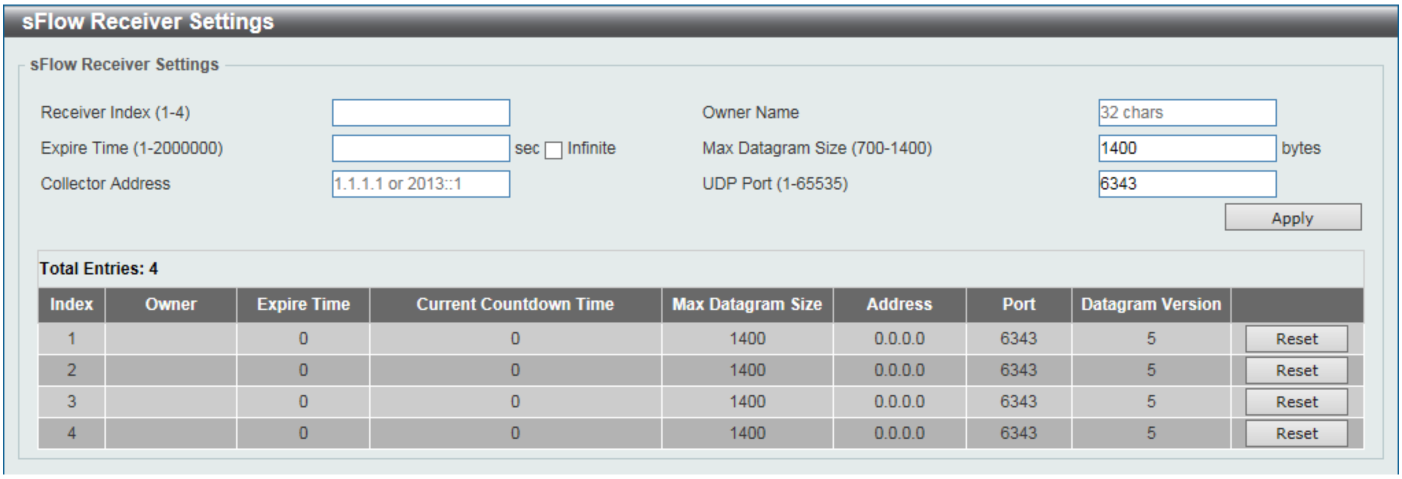
sFlow Agent Version	1.3;D-Link Corporation.;1.00
sFlow Agent Address	10.90.90.90
sFlow Agent IPv6 Address	FE80::6629:43FF:FEAC:2400

Figure 11-18 sFlow Agent Information Window

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:



sFlow Receiver Settings

sFlow Receiver Settings

Receiver Index (1-4)		Owner Name	32 chars
Expire Time (1-2000000)	sec □ Infinite	Max Datagram Size (700-1400)	1400 bytes
Collector Address	1.1.1.1 or 2013::1	UDP Port (1-65535)	6343

Total Entries: 4

Index	Owner	Expire Time	Current Countdown Time	Max Datagram Size	Address	Port	Datagram Version	
1		0	0	1400	0.0.0.0	6343	5	Reset
2		0	0	1400	0.0.0.0	6343	5	Reset
3		0	0	1400	0.0.0.0	6343	5	Reset
4		0	0	1400	0.0.0.0	6343	5	Reset

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. The range is from 1 to 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. The range is from 1 to 65535. By default, this value is 6343.

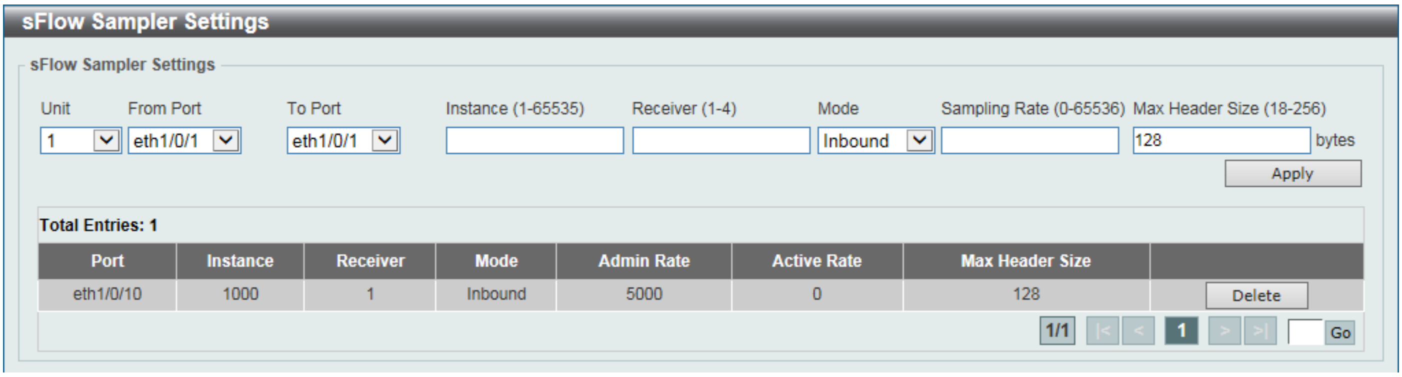
Click the **Apply** button to accept the changes made.

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:



sFlow Sampler Settings

sFlow Sampler Settings

Unit	From Port	To Port	Instance (1-65535)	Receiver (1-4)	Mode	Sampling Rate (0-65536)	Max Header Size (18-256)
1	eth1/0/1	eth1/0/1			Inbound		128 bytes

Total Entries: 1

Port	Instance	Receiver	Mode	Admin Rate	Active Rate	Max Header Size	
eth1/0/10	1000	1	Inbound	5000	0	128	Delete

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.
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 range is from 1 to 65535.
Receiver	Enter the receiver index for this sampler. If not specified, the value is 0. The range is from 1 to 4.
Mode	Select the mode here. Options to choose from are: • Selecting **Inbound** specifies to sample ingress packets. • Selecting **Outbound** specifies to sample egress packets. By default, the **Inbound** option is used.
Sampling Rate	Enter the packet-sampling rate here. The range is from 0 to 65536. Entering 0 will disable this function. By default, this value is 0.
Max Header Size	Enter the maximum number of bytes that should be copied from sampled packets. The range is from 18 to 256 bytes. By default, this value is 128 bytes.

Click the **Apply** button to accept the changes made.

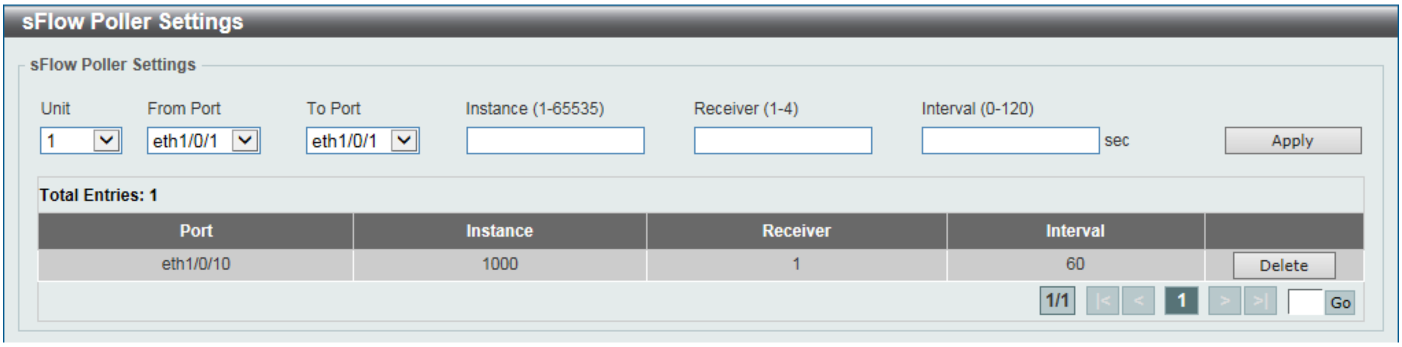
Click the **Delete** button to remove the specified entry.

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:



sFlow Poller Settings

sFlow Poller Settings

Unit: 1

From Port: eth1/0/1

To Port: eth1/0/1

Instance (1-65535):

Receiver (1-4):

Interval (0-120): sec

Total Entries: 1

Port	Instance	Receiver	Interval	
eth1/0/10	1000	1	60	Delete

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.
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 range is from 1 to 65535.
Receiver	Enter the receiver index value for this poller here. The range is from 1 to 4.
Interval	Enter the maximum number of seconds between successive polling samples. The range is from 0 to 120 seconds. Entering 0 will disable this feature. By default, this value is 0.

Click the **Apply** button to accept the changes made.

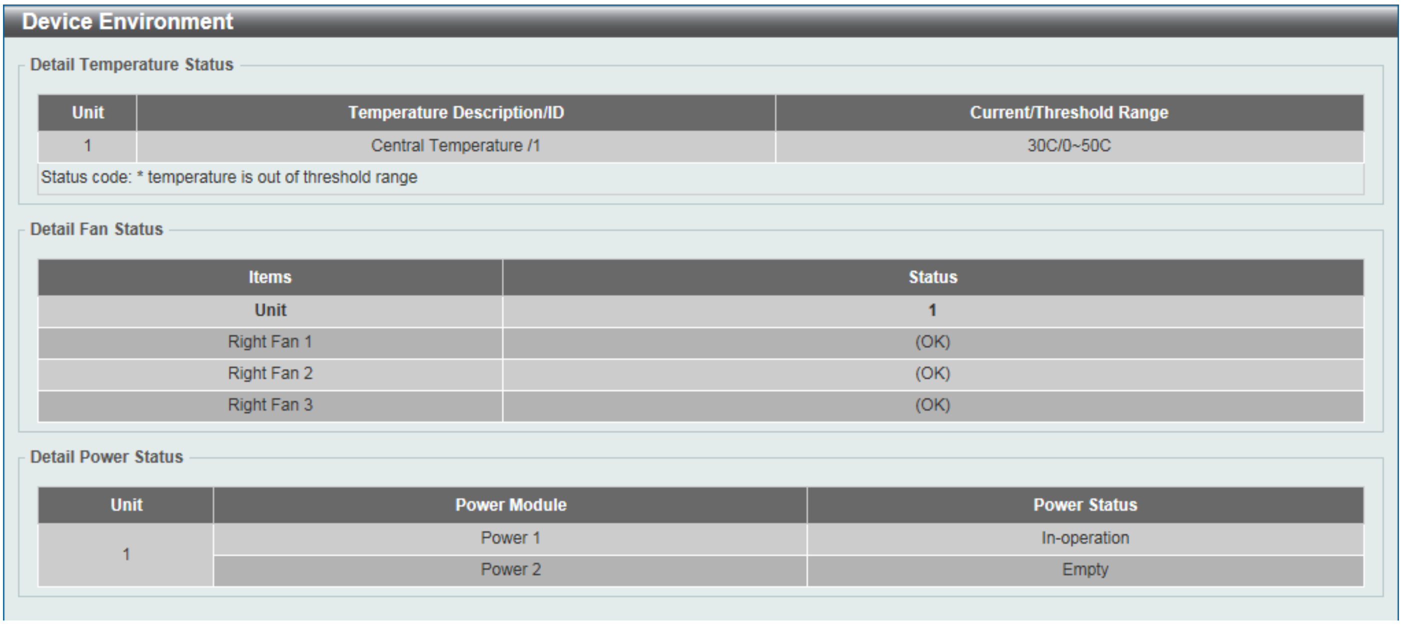
Click the **Delete** button to remove the specified entry.

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.

To view the following window, click **Monitoring > Device Environment**, as shown below:



Device Environment

Detail Temperature Status

Unit	Temperature Description/ID	Current/Threshold Range
1	Central Temperature /1	30C/0~50C

Status code: * temperature is out of threshold range

Detail Fan Status

Items	Status
Unit	**1**
Right Fan 1	(OK)
Right Fan 2	(OK)
Right Fan 3	(OK)

Detail Power Status

Unit	Power Module	Power Status
1	Power 1	In-operation
	Power 2	Empty

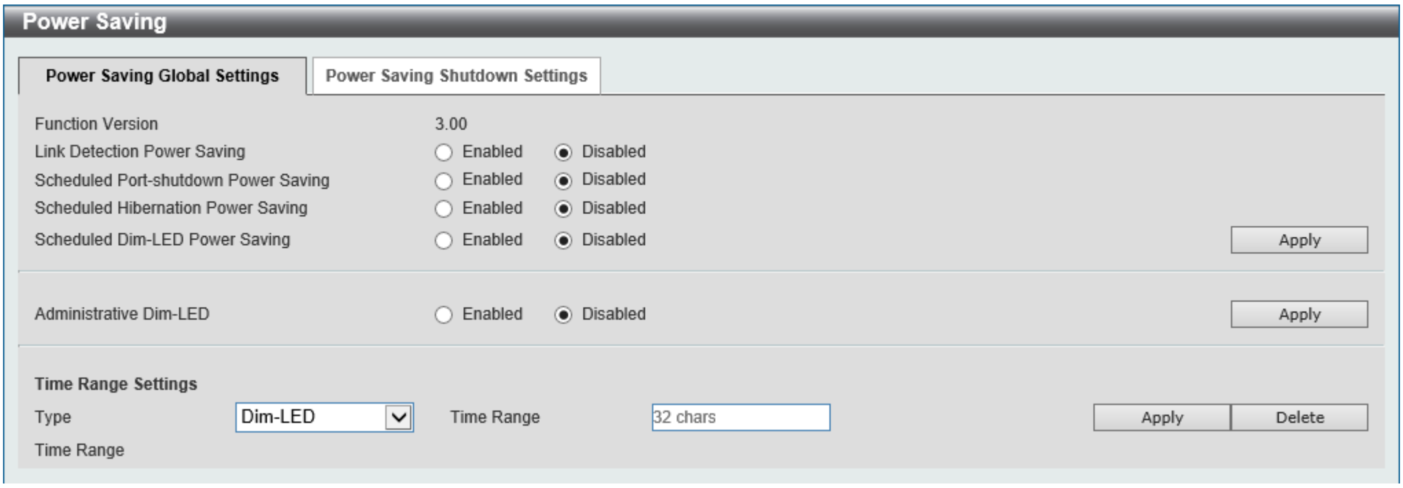
Figure 11-22 Device Environment Window

12. Green

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** and select the **Power Saving Global Settings** tab, as shown below:



Function Version 3.00

Link Detection Power Saving ○ Enabled ● Disabled

Scheduled Port-shutdown Power Saving ○ Enabled ● Disabled

Scheduled Hibernation Power Saving ○ Enabled ● Disabled

Scheduled Dim-LED Power Saving ○ Enabled ● Disabled

Administrative Dim-LED ○ Enabled ● Disabled

Time Range Settings

Type: Dim-LED   Time Range: 32 chars

Time Range

Figure 12-1 Power Saving Global Settings Window

The fields that can be configured in **Power Saving Global Settings** are described below:

Parameter	Description
Link Detection Power Saving	Select to enable or disable the link detection 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.
Scheduled Port-shutdown Power Saving	Select to enable or disable applying the power saving by scheduled port shutdown.
Scheduled Hibernation Power Saving	Select to enable or disable the scheduled hibernation power saving function here. This parameter is only available when physical stacking is *disabled*.
Scheduled Dim-LED Power Saving	Select to enable or disable applying the power saving by scheduled dimming LEDs.
Administrative Dim-LED	Select to enable or disable the port LED function.

Click the **Apply** button to accept the changes made.

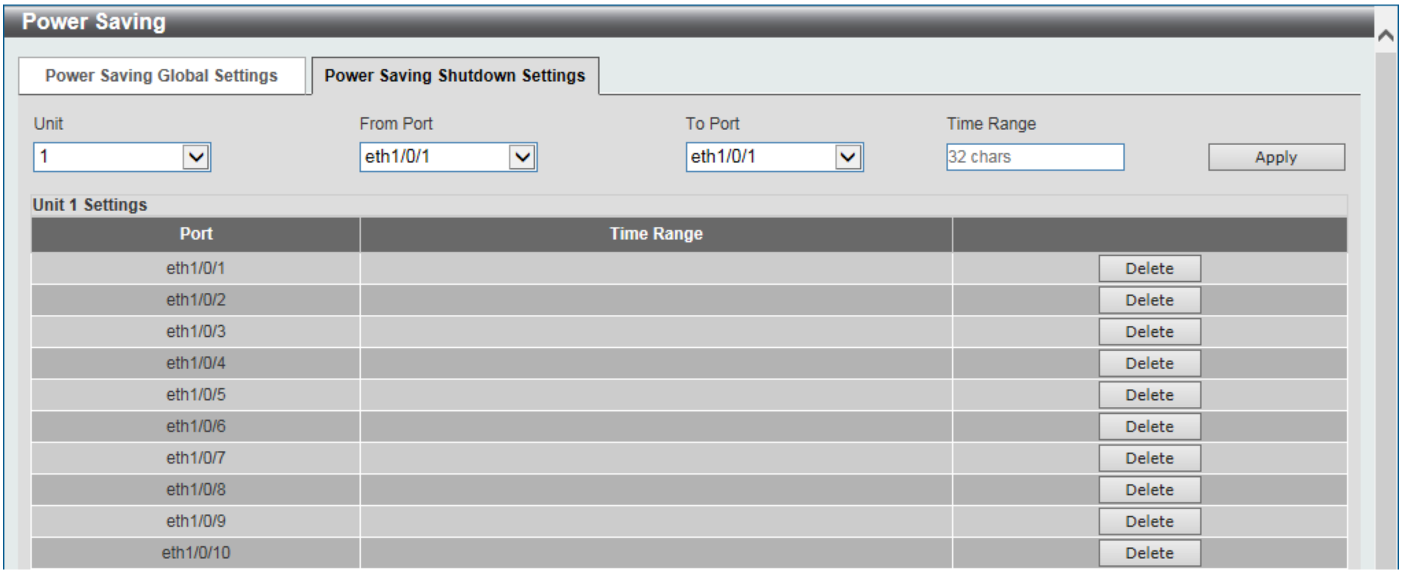
The fields that can be configured in **Time Range Settings** are described below:

Parameter	Description
Type	Select the type of power saving. Options to choose from are **Dim-LED** and **Hibernation**. **Hibernation** is only available when physical stacking is *disabled*.
Time Range	Enter the name of the time range to associate with the power saving type.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Delete** button to remove the specified entry.

To view the following window, select the **Power Saving Shutdown Settings** tab, as shown below:



Unit: 1 | From Port: eth1/0/1 | To Port: eth1/0/1 | Time Range: 32 chars

Unit 1 Settings

Port	Time Range	
eth1/0/1		Delete
eth1/0/2		Delete
eth1/0/3		Delete
eth1/0/4		Delete
eth1/0/5		Delete
eth1/0/6		Delete
eth1/0/7		Delete
eth1/0/8		Delete
eth1/0/9		Delete
eth1/0/10		Delete

Figure 12-2 Power Saving Shutdown Settings Window

The fields that can be configured are described below:

Parameter	Description
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.
Time Range	Enter the name of the time range to associate with the ports.

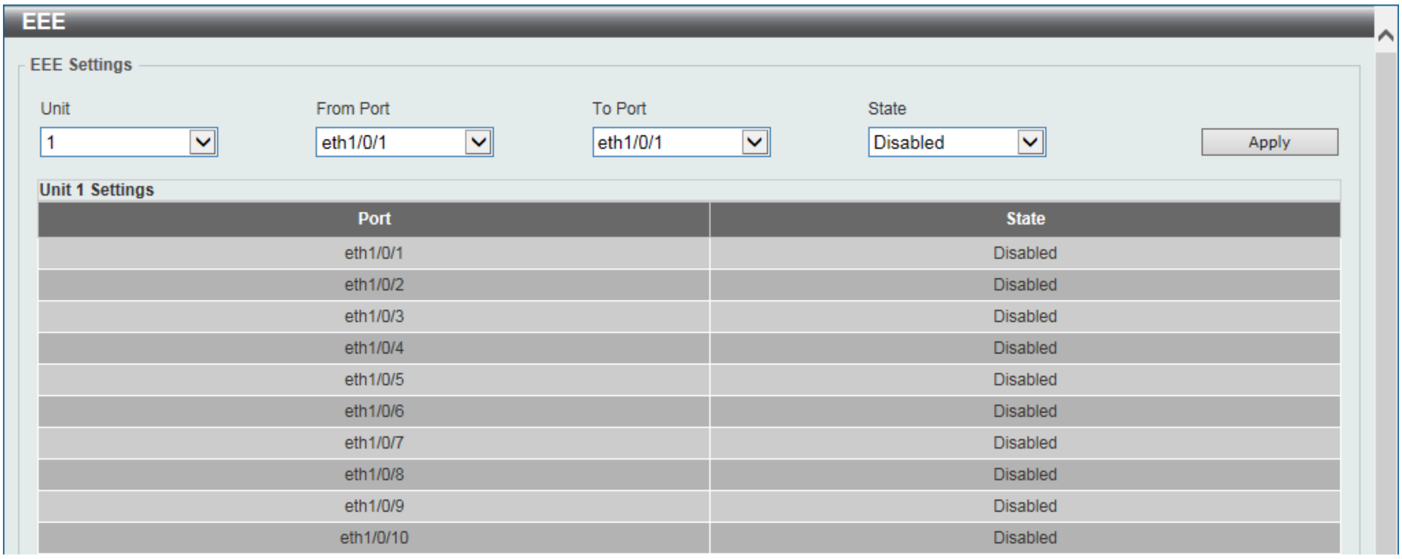
Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

EEE

Energy Efficient Ethernet (EEE) is defined in IEEE 802.3az. It is designed to reduce the energy consumption of a link when no packets are being sent.

To view the following window, click **Green > EEE**, as shown below:



Unit: 1 | From Port: eth1/0/1 | To Port: eth1/0/1 | State: Disabled

Unit 1 Settings

Port	State
eth1/0/1	Disabled
eth1/0/2	Disabled
eth1/0/3	Disabled
eth1/0/4	Disabled
eth1/0/5	Disabled
eth1/0/6	Disabled
eth1/0/7	Disabled
eth1/0/8	Disabled
eth1/0/9	Disabled
eth1/0/10	Disabled

Figure 12-3 EEE Window

The fields that can be configured are described below:

Parameter	Description
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.
State	Select this option to enable or disable the state of this feature here.

Click the **Apply** button to accept the changes made.

13. Toolbar

Save

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:

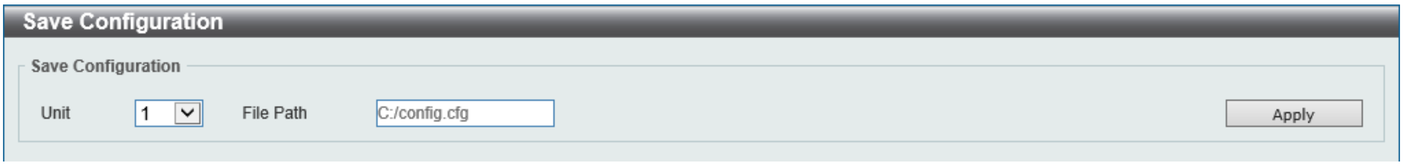


Figure 13-1 Save Configuration Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
File Path	Enter the filename and path in the space provided.

Click the **Apply** button to save the configuration.

Tools

Firmware Upgrade & Backup

Firmware Upgrade from HTTP

This window is used to initiate a firmware upgrade from a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP**, as shown below:

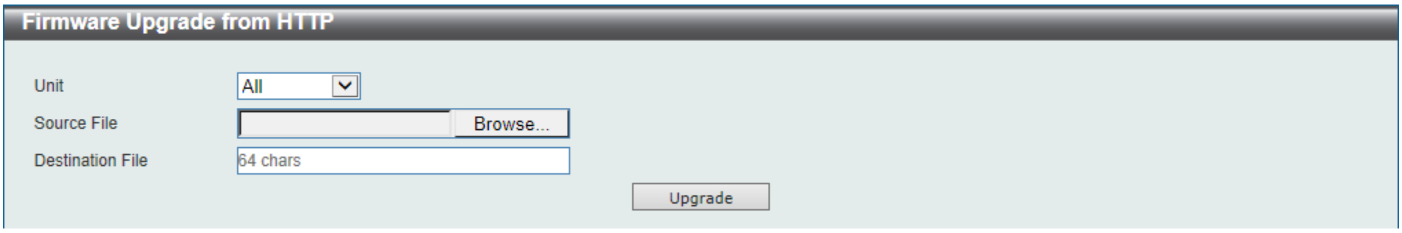


Figure 13-2 Firmware Upgrade from HTTP Window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.

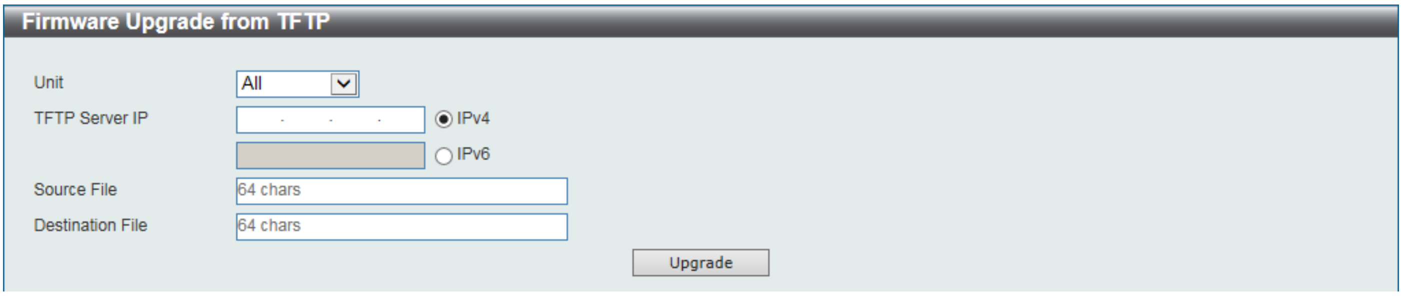
Parameter	Description
Source File	In this field the source firmware file's filename and path will be displayed after selection. To navigate to the location of the firmware file located on the local PC, either double click in the text box or click the **Browse** button.
Destination File	Enter the destination path and location where the new firmware should be stored on the Switch. This field can be up to 64 characters long.

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Upgrade from TFTP

This window is used to initiate a firmware upgrade from a TFTP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from TFTP**, as shown below:



Firmware Upgrade from TFTP

Unit	All
TFTP Server IP	. . . ● IPv4
	○ IPv6
Source File	64 chars
Destination File	64 chars

Figure 13-3 Firmware Upgrade from TFTP Window

The fields that can be configured are described below:

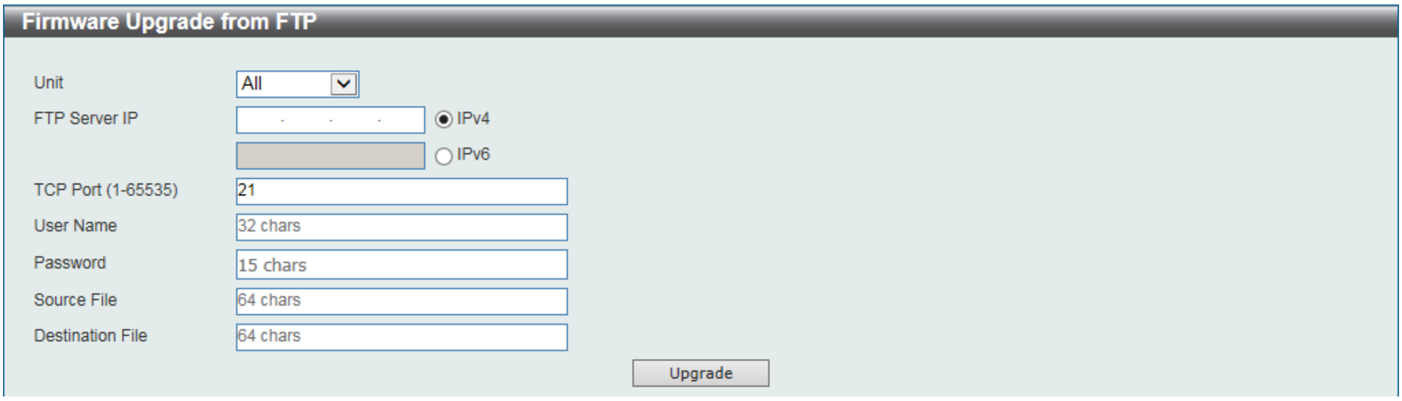
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
TFTP Server IP	Enter the TFTP server IP address here. When select the **IPv4** option, enter the IPv4 address of the TFTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 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.

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Upgrade from FTP

This window is used to initiate a firmware upgrade from an FTP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from FTP**, as shown below:



Firmware Upgrade from FTP

Unit: All

FTP Server IP: . . . ● IPv4

○ IPv6

TCP Port (1-65535): 21

User Name: 32 chars

Password: 15 chars

Source File: 64 chars

Destination File: 64 chars

Figure 13-4 Firmware Upgrade from FTP Window

The fields that can be configured are described below:

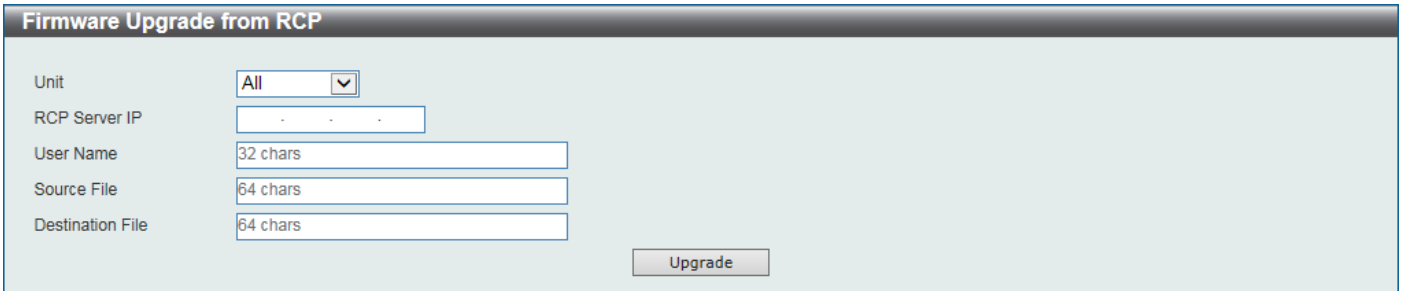
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
FTP Server IP	Enter the FTP server IP address here. When select the **IPv4** option, enter the IPv4 address of the FTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 address of the FTP server in the space provided.
TCP Port	Enter the TCP port number used for the FTP connection here. The range is from 1 to 65535.
User Name	Enter the user name used for the FTP connection here. This name can be up to 32 characters long.
Password	Enter the password used for the FTP connection here. This password can be up to 15 characters long.
Source File	Enter the source filename and path of the firmware file located on the FTP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the new firmware should be stored on the Switch. This field can be up to 64 characters long.

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Upgrade from RCP

This window is used to initiate a firmware upgrade from an RCP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from RCP**, as shown below:



Firmware Upgrade from RCP

Unit	All
RCP Server IP	. . .
User Name	32 chars
Source File	64 chars
Destination File	64 chars

Figure 13-5 Firmware Upgrade from RCP Window

The fields that can be configured are described below:

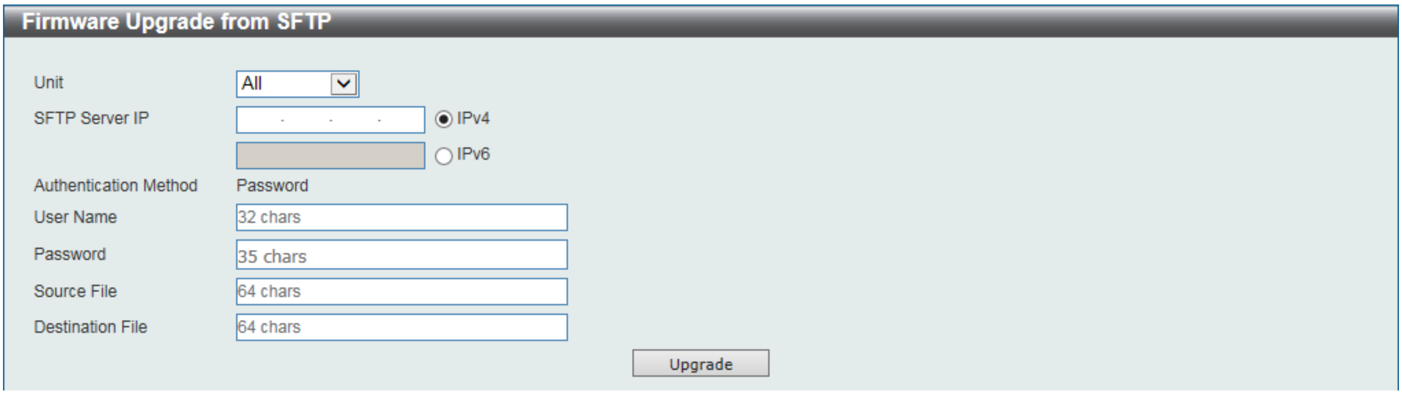
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
RCP Server IP	Enter the RCP server IP address here.
User Name	Enter the user name used for the RCP connection here. This name can be up to 32 characters long.
Source File	Enter the source filename and path of the firmware file located on the RCP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the new firmware should be stored on the Switch. This field can be up to 64 characters long.

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Upgrade from SFTP

This window is used to initiate a firmware upgrade from an SFTP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from SFTP**, as shown below:



Firmware Upgrade from SFTP

Unit	All
SFTP Server IP	. . . ● IPv4 ○ IPv6
Authentication Method	Password
User Name	32 chars
Password	35 chars
Source File	64 chars
Destination File	64 chars

Figure 13-6 Firmware Upgrade from SFTP Window

The fields that can be configured are described below:

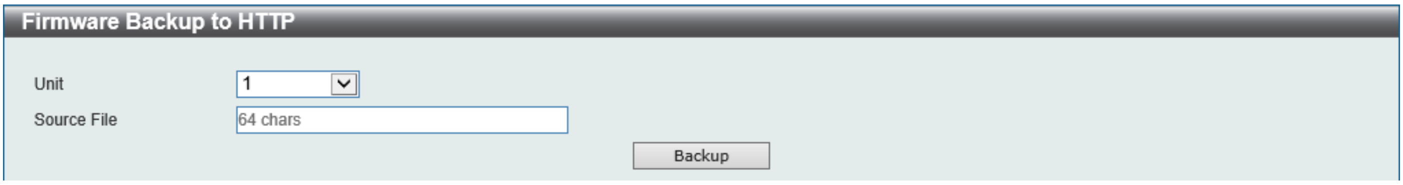
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
SFTP Server IP	Enter the SFTP server IP address here. When select the **IPv4** option, enter the IPv4 address of the SFTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 address of the SFTP server in the space provided.
User Name	Enter the user name used for the SFTP connection here. This name can be up to 32 characters long.
Password	Enter the password used for the SFTP connection here. This password can be up to 35 characters long.
Source File	Enter the source filename and path of the firmware file located on the SFTP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the new firmware should be stored on the Switch. This field can be up to 64 characters long.

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Backup to HTTP

This window is used to initiate a firmware backup to a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to HTTP**, as shown below:



Firmware Backup to HTTP

Unit: 1

Source File: 64 chars

Figure 13-7 Firmware Backup to HTTP Window

The fields that can be configured are described below:

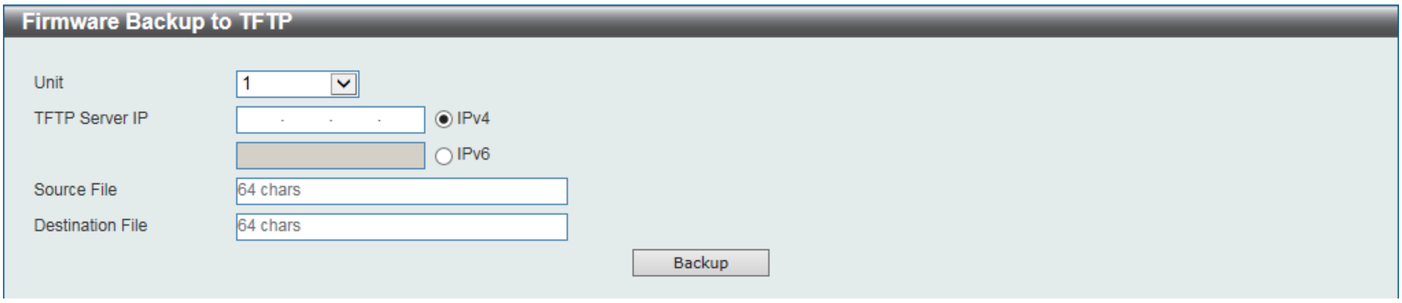
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
Source File	Enter the source filename and path of the firmware file located on the Switch here. This field can be up to 64 characters long.

Click the **Backup** button to 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:



Firmware Backup to TFTP

Unit: 1

TFTP Server IP: . . . ● IPv4

○ IPv6

Source File: 64 chars

Destination File: 64 chars

Figure 13-8 Firmware Backup to TFTP Window

The fields that can be configured are described below:

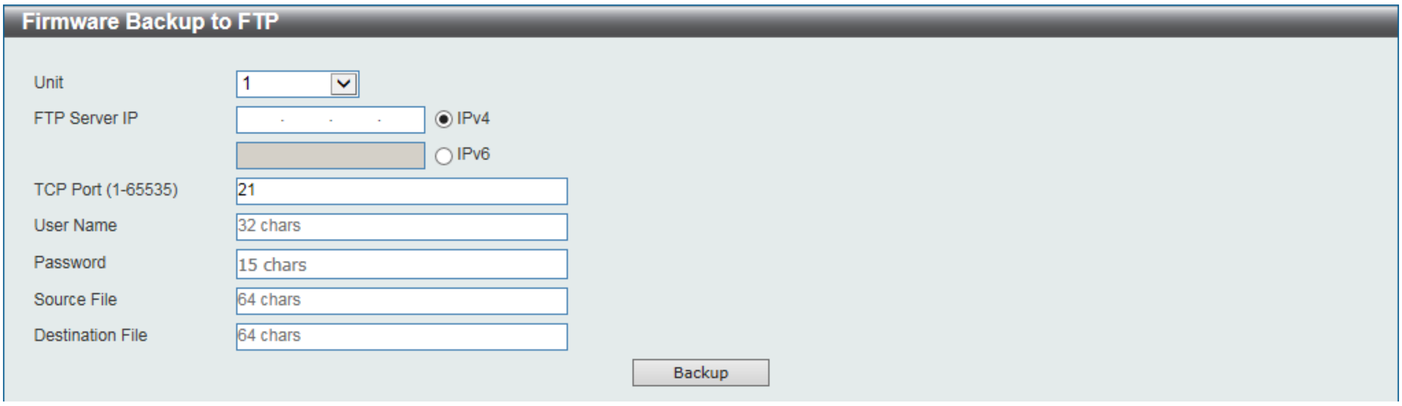
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
TFTP Server IP	Enter the TFTP server IP address here. When select the **IPv4** option, enter the IPv4 address of the TFTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 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.
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.

Firmware Backup to FTP

This window is used to initiate a firmware backup to an FTP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to FTP**, as shown below:



Firmware Backup to FTP

Unit: 1

FTP Server IP: . . . ● IPv4

○ IPv6

TCP Port (1-65535): 21

User Name: 32 chars

Password: 15 chars

Source File: 64 chars

Destination File: 64 chars

Figure 13-9 Firmware Backup to FTP Window

The fields that can be configured are described below:

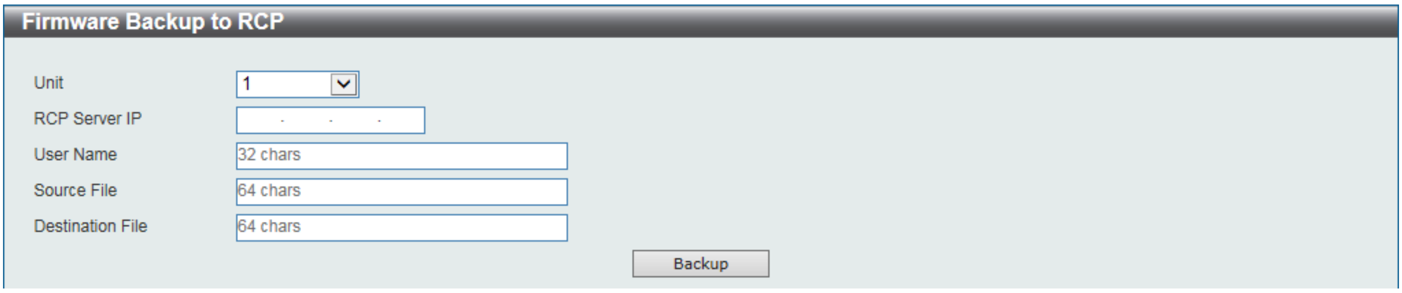
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
FTP Server IP	Enter the FTP server IP address here. When select the **IPv4** option, enter the IPv4 address of the FTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 address of the FTP server in the space provided.
TCP Port	Enter the TCP port number used for the FTP connection here. The range is from 1 to 65535.
User Name	Enter the user name used for the FTP connection here. This name can be up to 32 characters long.
Password	Enter the password used for the FTP connection here. This password can be up to 15 characters long.
Source File	Enter the source filename and path of the firmware file located on the Switch here. This field can be up to 64 characters long.
Destination File	Enter the destination filename and path of the firmware file to be backed up to the FTP server here. This field can be up to 64 characters long.

Click the **Backup** button to initiate the firmware backup.

Firmware Backup to RCP

This window is used to initiate a firmware backup to an RCP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to RCP**, as shown below:



Firmware Backup to RCP

Unit: 1

RCP Server IP: . . .

User Name: 32 chars

Source File: 64 chars

Destination File: 64 chars

Figure 13-10 Firmware Backup to RCP Window

The fields that can be configured are described below:

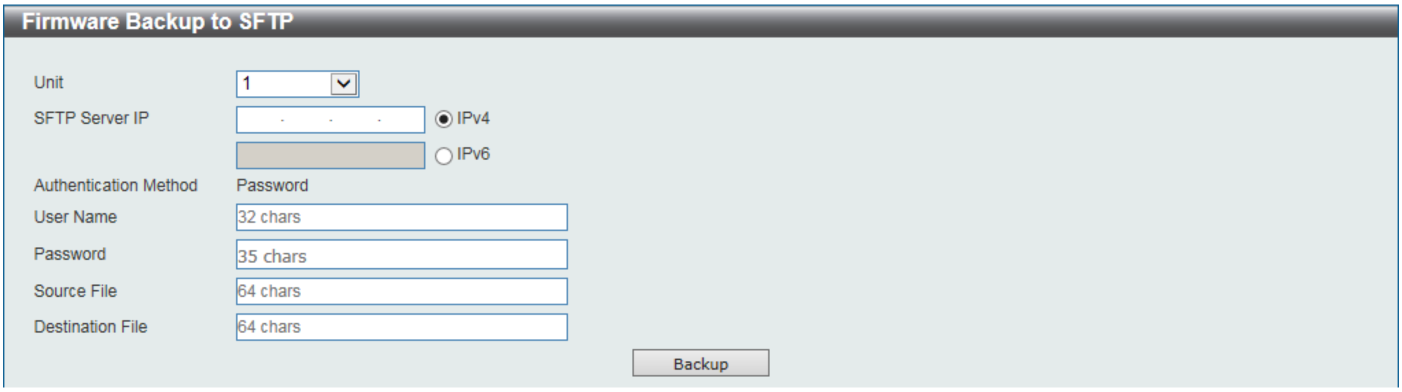
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
RCP Server IP	Enter the RCP server IP address here.
User Name	Enter the user name used for the RCP connection here. This name can be up to 32 characters long.
Source File	Enter the source filename and path of the firmware file located on the Switch here. This field can be up to 64 characters long.
Destination File	Enter the destination filename and path of the firmware file to be backed up to the RCP server here. This field can be up to 64 characters long.

Click the **Backup** button to initiate the firmware backup.

Firmware Backup to SFTP

This window is used to initiate a firmware backup to a SFTP server.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to SFTP**, as shown below:



Firmware Backup to SFTP

Unit: 1

SFTP Server IP: . . . ● IPv4

○ IPv6

Authentication Method: Password

User Name: 32 chars

Password: 35 chars

Source File: 64 chars

Destination File: 64 chars

Figure 13-11 Firmware Backup to SFTP 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.
SFTP Server IP	Enter the SFTP server IP address here. When select the **IPv4** option, enter the IPv4 address of the SFTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 address of the SFTP server in the space provided.
User Name	Enter the user name used for the SFTP connection here. This name can be up to 32 characters long.
Password	Enter the password used for the SFTP connection here. This password can be up to 35 characters long.
Source File	Enter the source filename and path of the firmware file located on the Switch here. This field can be up to 64 characters long.
Destination File	Enter the destination filename and path of the firmware file to be backed up to the SFTP server here. This field can be up to 64 characters long.

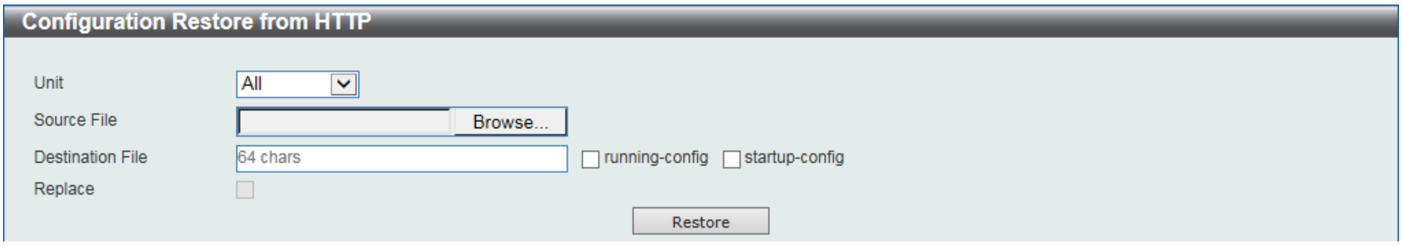
Click the **Backup** button to initiate the firmware backup.

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:



Configuration Restore from HTTP

Unit: All

Source File: Browse...

Destination File: 64 chars □ running-config □ startup-config

Replace: □

Figure 13-12 Configuration Restore from HTTP Window

The fields that can be configured are described below:

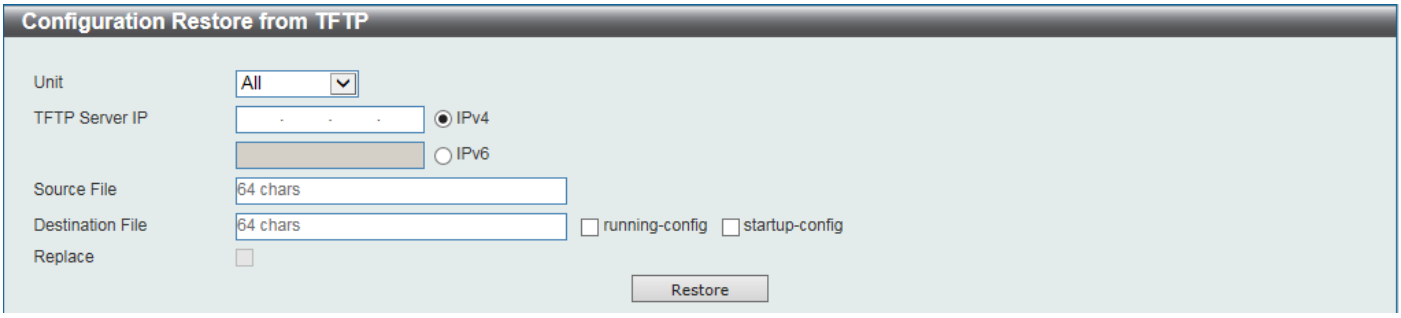
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
Source File	In this field the source configuration file’s filename and path will be displayed after selection. To navigate to the location of the configuration file located on the local PC, either double 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. This field can be up to 64 characters long. Select the **running-config** option to restore and overwrite the running configuration file on the Switch. Select the **startup-config** option to restore and overwrite the start-up configuration file on the Switch.
Replace	Select this option to replace the configuration file on the Switch with this one.

Click the **Restore** button to initiate the configuration restore.

Configuration Restore from TFTP

This window is used to initiate a configuration restore from a TFTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from TFTP**, as shown below:



Configuration Restore from TFTP

Unit: All

TFTP Server IP: . . . ● IPv4

○ IPv6

Source File: 64 chars

Destination File: 64 chars ☐ running-config ☐ startup-config

Replace: ☐

Figure 13-13 Configuration Restore from TFTP Window

The fields that can be configured are described below:

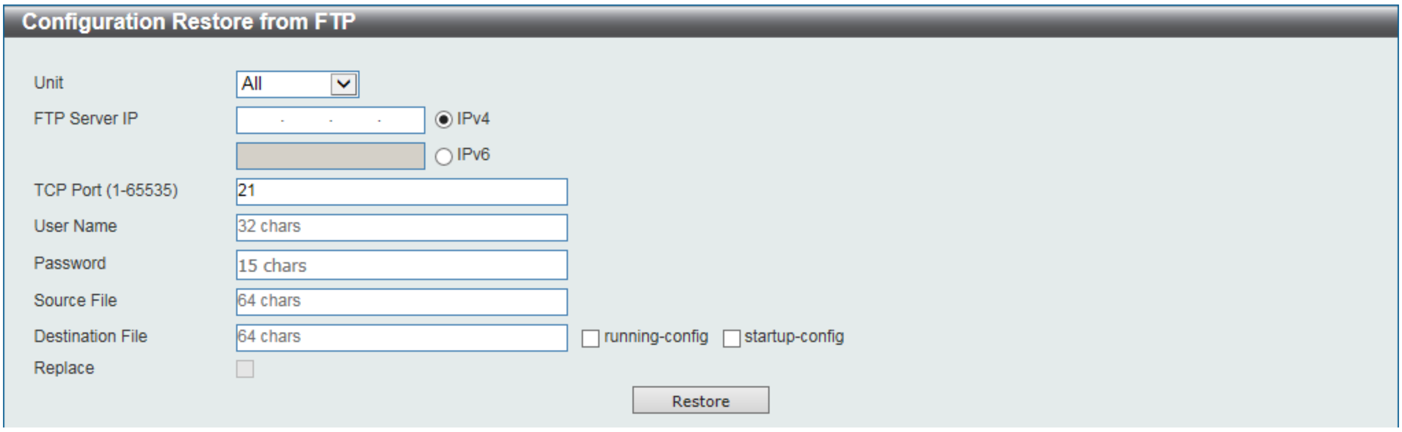
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
TFTP Server IP	Enter the TFTP server IP address here. When select the **IPv4** option, enter the IPv4 address of the TFTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 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. This field can be up to 64 characters long. Select the **running-config** option to restore and overwrite the running configuration file on the Switch. Select the **startup-config** option to restore and overwrite the start-up configuration file on the Switch.
Replace	Select this option to replace the configuration file on the Switch with this one.

Click the **Restore** button to initiate the configuration restore.

Configuration Restore from FTP

This window is used to initiate a configuration restore from an FTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from FTP**, as shown below:



Configuration Restore from FTP

Unit	All	
FTP Server IP	. . .	● IPv4
		○ IPv6
TCP Port (1-65535)	21	
User Name	32 chars	
Password	15 chars	
Source File	64 chars	
Destination File	64 chars	□ running-config □ startup-config
Replace	□	

Figure 13-14 Configuration Restore from FTP Window

The fields that can be configured are described below:

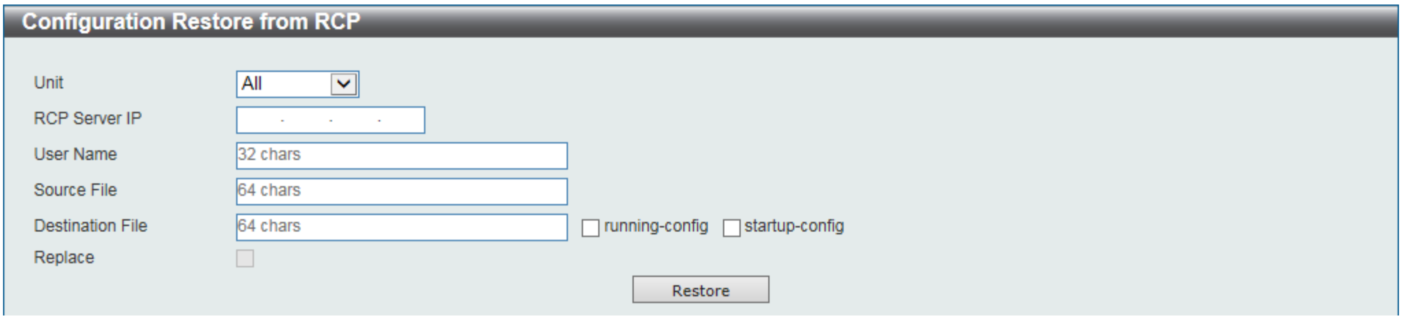
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
FTP Server IP	Enter the FTP server IP address here. When select the **IPv4** option, enter the IPv4 address of the FTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 address of the FTP server in the space provided.
TCP Port	Enter the TCP port number used for the FTP connection here. The range is from 1 to 65535.
User Name	Enter the user name used for the FTP connection here. This name can be up to 32 characters long.
Password	Enter the password used for the FTP connection here. This password can be up to 15 characters long.
Source File	Enter the source filename and path of the configuration file located on the FTP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the configuration file should be stored on the Switch. This field can be up to 64 characters long. Select the **running-config** option to restore and overwrite the running configuration file on the Switch. Select the **startup-config** option to restore and overwrite the start-up configuration file on the Switch.
Replace	Select this option to replace the configuration file on the Switch with this one.

Click the **Restore** button to initiate the configuration restore.

Configuration Restore from RCP

This window is used to initiate a configuration restore from an RCP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from RCP**, as shown below:



Configuration Restore from RCP

Unit	All
RCP Server IP	. . .
User Name	32 chars
Source File	64 chars
Destination File	64 chars □ running-config □ startup-config
Replace	□

Figure 13-15 Configuration Restore from RCP Window

The fields that can be configured are described below:

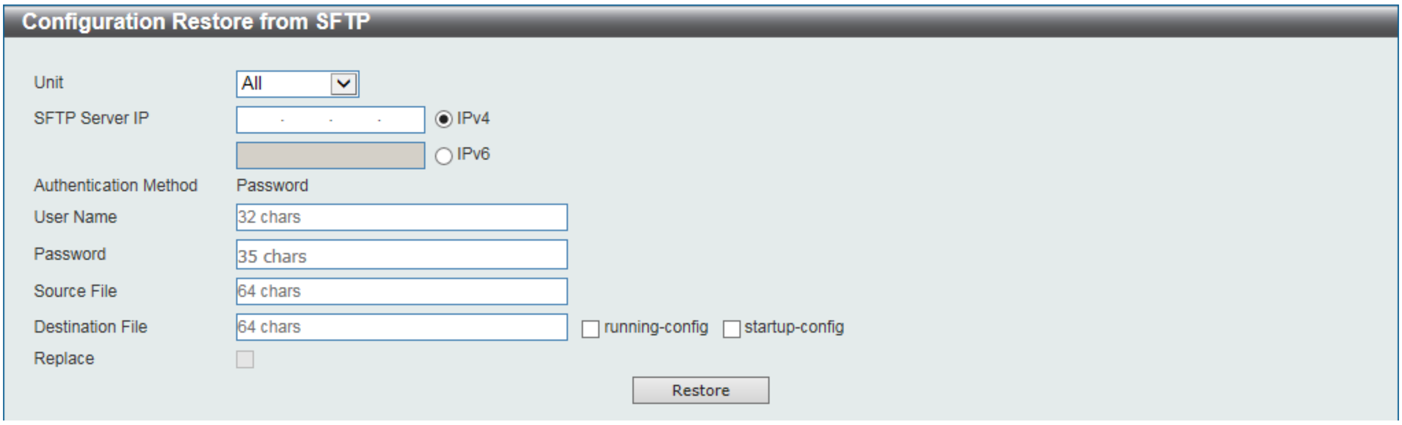
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
RCP Server IP	Enter the RCP server IP address here.
User Name	Enter the user name used for the RCP connection here. This name can be up to 32 characters long.
Source File	Enter the source filename and path of the configuration file located on the RCP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the configuration file should be stored on the Switch. This field can be up to 64 characters long. Select the **running-config** option to restore and overwrite the running configuration file on the Switch. Select the **startup-config** option to restore and overwrite the start-up configuration file on the Switch.
Replace	Select this option to replace the configuration file on the Switch with this one.

Click the **Restore** button to initiate the configuration restore.

Configuration Restore from SFTP

This window is used to initiate a configuration restore from an SFTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from SFTP**, as shown below:



Configuration Restore from SFTP

Unit: All

SFTP Server IP: . . . ● IPv4 ○ IPv6

Authentication Method: Password

User Name: 32 chars

Password: 35 chars

Source File: 64 chars

Destination File: 64 chars □ running-config □ startup-config

Replace: □

Figure 13-16 Configuration Restore from SFTP Window

The fields that can be configured are described below:

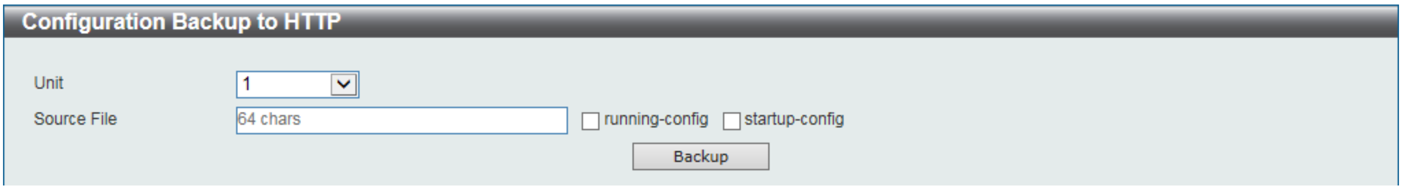
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
SFTP Server IP	Enter the SFTP server IP address here. When select the **IPv4** option, enter the IPv4 address of the SFTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 address of the SFTP server in the space provided.
User Name	Enter the user name used for the SFTP connection here. This name can be up to 32 characters long.
Password	Enter the password used for the SFTP connection here. This password can be up to 35 characters long.
Source File	Enter the source filename and path of the configuration file located on the SFTP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the configuration file should be stored on the Switch. This field can be up to 64 characters long. Select the **running-config** option to restore and overwrite the running configuration file on the Switch. Select the **startup-config** option to restore and overwrite the start-up configuration file on the Switch.
Replace	Select this option to replace the configuration file on the Switch with this one.

Click the **Restore** button to initiate the configuration restore.

Configuration Backup to HTTP

This window is used to initiate a configuration file backup to a local PC using HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to HTTP**, as shown below:



Configuration Backup to HTTP

Unit: 1

Source File: 64 chars □ running-config □ startup-config

Figure 13-17 Configuration Backup to HTTP Window

The fields that can be configured are described below:

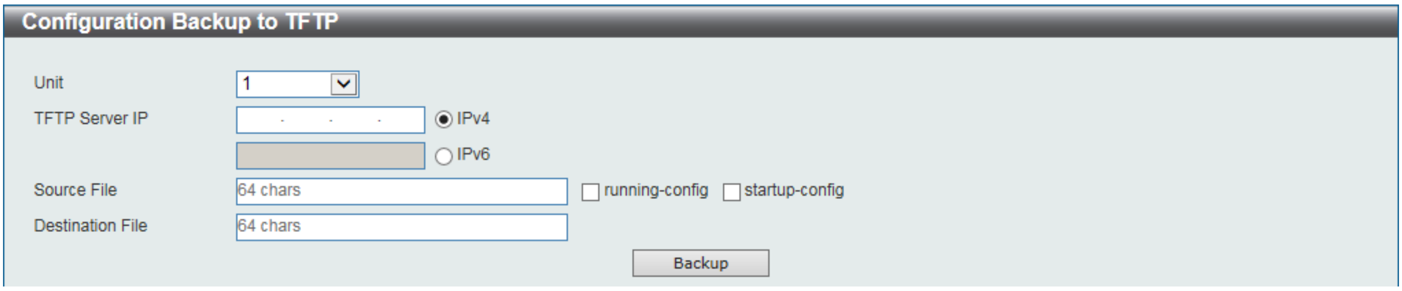
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
Source File	Enter the source filename and path of the configuration file located on the Switch here. This field can be up to 64 characters long. Select the **running-config** option to back up the running configuration file from the Switch. Select the **startup-config** option to back up the start-up configuration file from the Switch.

Click the **Backup** button to initiate the configuration file backup.

Configuration Backup to TFTP

This window is used to initiate a configuration file backup to a TFTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to TFTP**, as shown below:



Configuration Backup to TFTP

Unit: 1

TFTP Server IP: . . . ● IPv4

○ IPv6

Source File: 64 chars □ running-config □ startup-config

Destination File: 64 chars

Figure 13-18 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. Select the **startup-config** option to back up the start-up configuration file from the Switch.
Destination File	Enter the destination path and location where the configuration file should be stored on the TFTP server. This field can be up to 64 characters long.

Click the **Backup** button to initiate the configuration file backup.

Configuration Backup to FTP

This window is used to initiate a configuration file backup to an FTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to FTP**, as shown below:

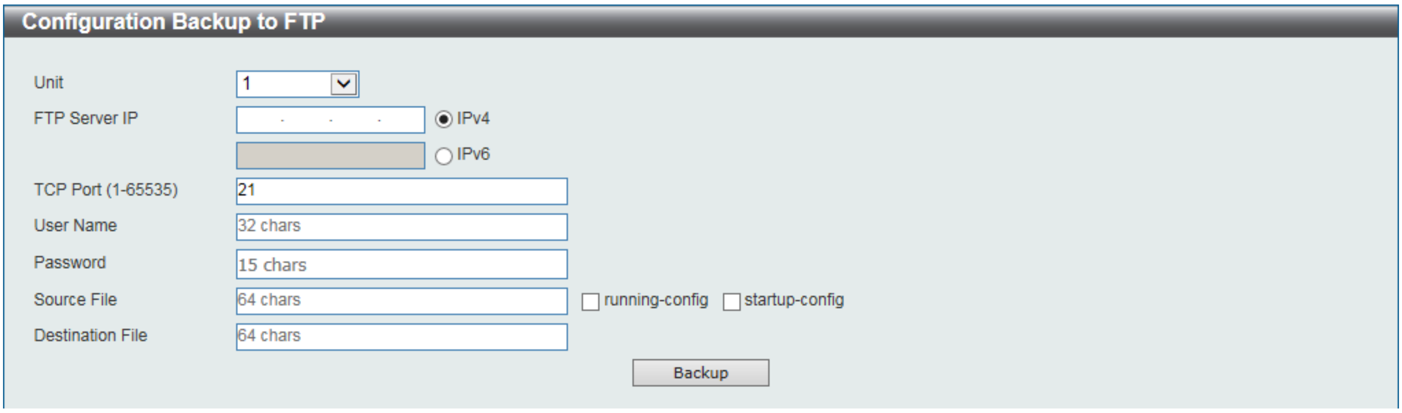


Figure 13-19 Configuration Backup to FTP Window

The fields that can be configured are described below:

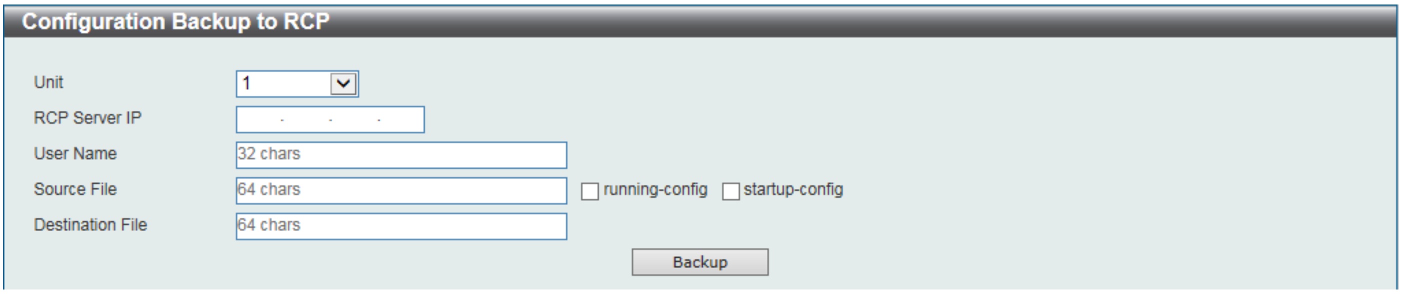
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
FTP Server IP	Enter the FTP server IP address here. When select the **IPv4** option, enter the IPv4 address of the FTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 address of the FTP server in the space provided.
TCP Port	Enter the TCP port number used for the FTP connection here. The range is from 1 to 65535.
User Name	Enter the user name used for the FTP connection here. This name can be up to 32 characters long.
Password	Enter the password used for the FTP connection here. This password can be up to 15 characters long.
Source File	Enter the source filename and path of the configuration file located on the Switch here. This field can be up to 64 characters long. Select the **running-config** option to back up the running configuration file from the Switch. Select the **startup-config** option to back up the start-up configuration file from the Switch.
Destination File	Enter the destination path and location where the configuration file should be stored on the FTP server. This field can be up to 64 characters long.

Click the **Backup** button to initiate the configuration file backup.

Configuration Backup to RCP

This window is used to initiate a configuration file backup to an RCP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to RCP**, as shown below:



Configuration Backup to RCP

Unit: 1

RCP Server IP: . . .

User Name: 32 chars

Source File: 64 chars □ running-config □ startup-config

Destination File: 64 chars

Figure 13-20 Configuration Backup to RCP Window

The fields that can be configured are described below:

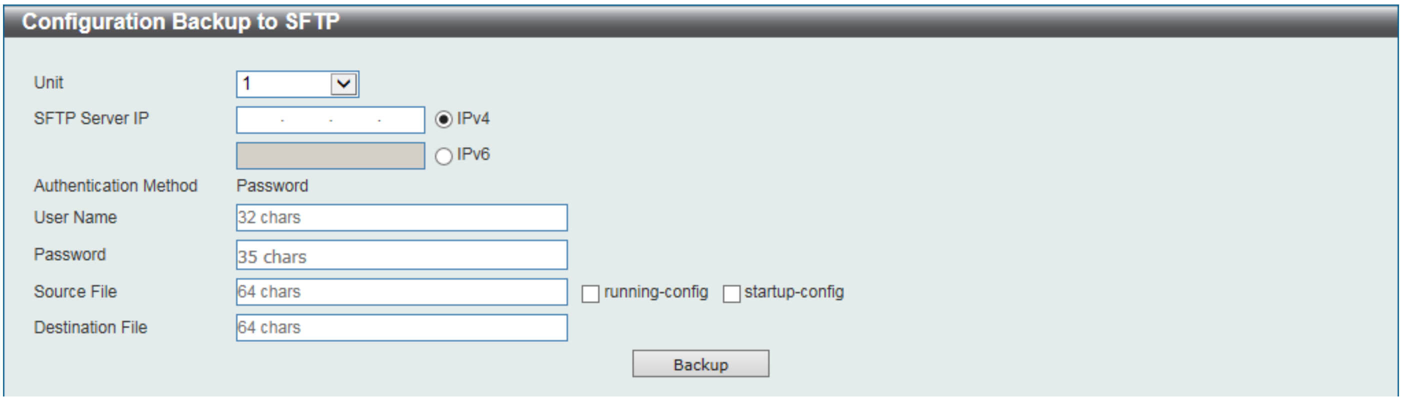
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
RCP Server IP	Enter the RCP server IP address here.
User Name	Enter the user name used for the RCP connection here. This name can be up to 32 characters long.
Source File	Enter the source filename and path of the configuration file located on the Switch here. This field can be up to 64 characters long. Select the **running-config** option to back up the running configuration file from the Switch. Select the **startup-config** option to back up the start-up configuration file from the Switch.
Destination File	Enter the destination path and location where the configuration file should be stored on the RCP server. This field can be up to 64 characters long.

Click the **Backup** button to initiate the configuration file backup.

Configuration Backup to SFTP

This window is used to initiate a configuration file backup to an SFTP server.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to SFTP**, as shown below:



Configuration Backup to SFTP

Unit: 1

SFTP Server IP: . . . ● IPv4

○ IPv6

Authentication Method: Password

User Name: 32 chars

Password: 35 chars

Source File: 64 chars □ running-config □ startup-config

Destination File: 64 chars

Figure 13-21 Configuration Backup to SFTP 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.
SFTP Server IP	Enter the SFTP server IP address here. When select the **IPv4** option, enter the IPv4 address of the SFTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 address of the SFTP server in the space provided.
User Name	Enter the user name used for the SFTP connection here. This name can be up to 32 characters long.
Password	Enter the password used for the SFTP connection here. This password can be up to 35 characters long.
Source File	Enter the source filename and path of the configuration file located on the Switch here. This field can be up to 64 characters long. Select the **running-config** option to back up the running configuration file from the Switch. Select the **startup-config** option to back up the start-up configuration file from the Switch.
Destination File	Enter the destination path and location where the configuration file should be stored on the SFTP server. This field can be up to 64 characters long.

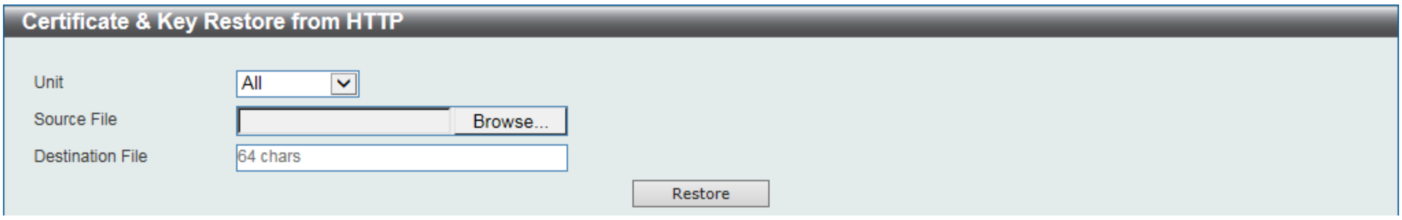
Click the **Backup** button to initiate the configuration file backup.

Certificate & Key Restore & Backup

Certificate & Key Restore from HTTP

This window is used to initiate a certificate and key restore from a local PC using HTTP.

To view the following window, click **Tools > Certificate & Key Restore & Backup > Certificate & Key Restore from HTTP**, as shown below:



Certificate & Key Restore from HTTP

Unit: All

Source File:

Destination File: 64 chars

Figure 13-22 Certificate & Key Restore from HTTP Window

The fields that can be configured are described below:

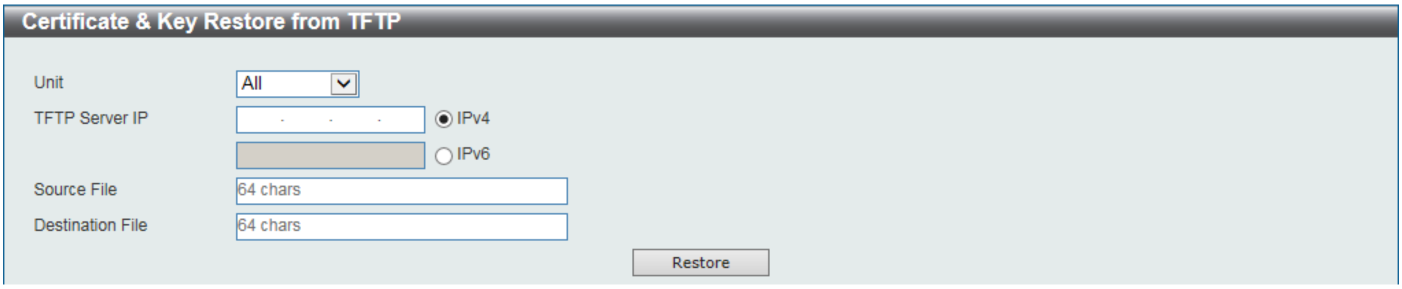
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
Source File	In this field the source certificate and key file’s filename and path will be displayed after selection. To navigate to the location of the certificate and key file located on the local PC, either double click in the text box or click the **Browse** button.
Destination File	Enter the destination path and location where the new certificate and key should be stored on the Switch. This field can be up to 64 characters long.

Click the **Restore** button to initiate the certificate and key restore.

Certificate & Key Restore from TFTP

This window is used to initiate a certificate and key restore from a TFTP server.

To view the following window, click **Tools > Certificate & Key Restore & Backup > Certificate & Key Restore from TFTP**, as shown below:



Certificate & Key Restore from TFTP

Unit: All

TFTP Server IP: ● IPv4 ○ IPv6

Source File: 64 chars

Destination File: 64 chars

Figure 13-23 Certificate & Key Restore from TFTP Window

The fields that can be configured are described below:

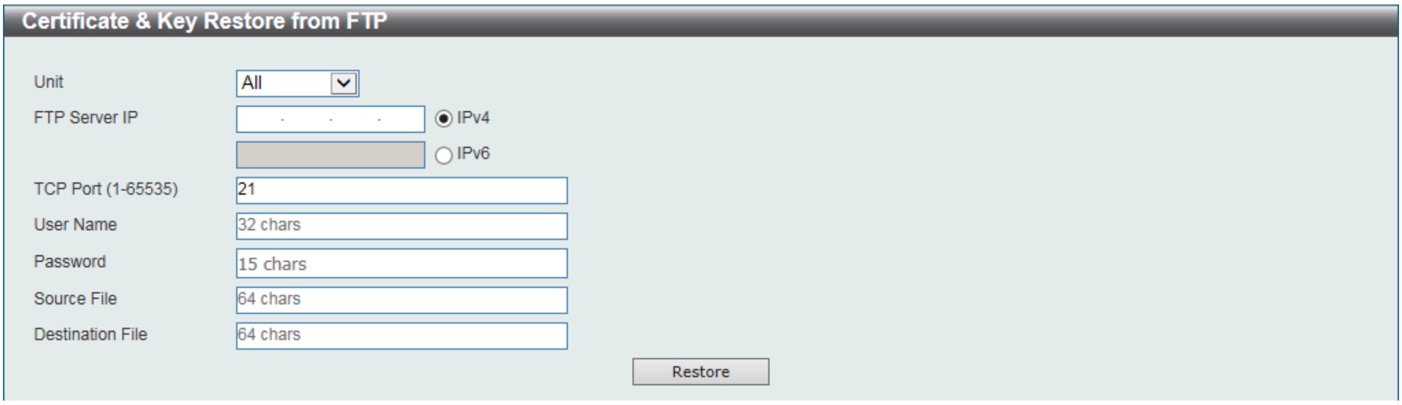
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
TFTP Server IP	Enter the TFTP server IP address here. When select the **IPv4** option, enter the IPv4 address of the TFTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 address of the TFTP server in the space provided.
Source File	Enter the source filename and path of the certificate and key 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 certificate and key should be stored on the Switch. This field can be up to 64 characters long.

Click the **Restore** button to initiate the certificate and key restore.

Certificate & Key Restore from FTP

This window is used to initiate a certificate and key restore from an FTP server.

To view the following window, click **Tools > Certificate & Key Restore & Backup > Certificate & Key Restore from FTP**, as shown below:



Certificate & Key Restore from FTP

Unit: All

FTP Server IP: ● IPv4 ○ IPv6

TCP Port (1-65535): 21

User Name: 32 chars

Password: 15 chars

Source File: 64 chars

Destination File: 64 chars

Figure 13-24 Certificate & Key Restore from FTP 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.
FTP Server IP	Enter the FTP server IP address here. When select the **IPv4** option, enter the IPv4 address of the FTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 address of the FTP server in the space provided.
TCP Port	Enter the TCP port number used for the FTP connection here. The range is from 1 to 65535.
User Name	Enter the user name used for the FTP connection here. This name can be up to 32 characters long.
Password	Enter the password used for the FTP connection here. This password can be up to 15 characters long.
Source File	Enter the source filename and path of the certificate and key file located on the FTP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the new certificate and key should be stored on the Switch. This field can be up to 64 characters long.

Click the **Restore** button to initiate the certificate and key restore.

Certificate & Key Restore from RCP

This window is used to initiate a certificate and key restore from an RCP server.

To view the following window, click **Tools > Certificate & Key Restore & Backup > Certificate & Key Restore from RCP**, as shown below:

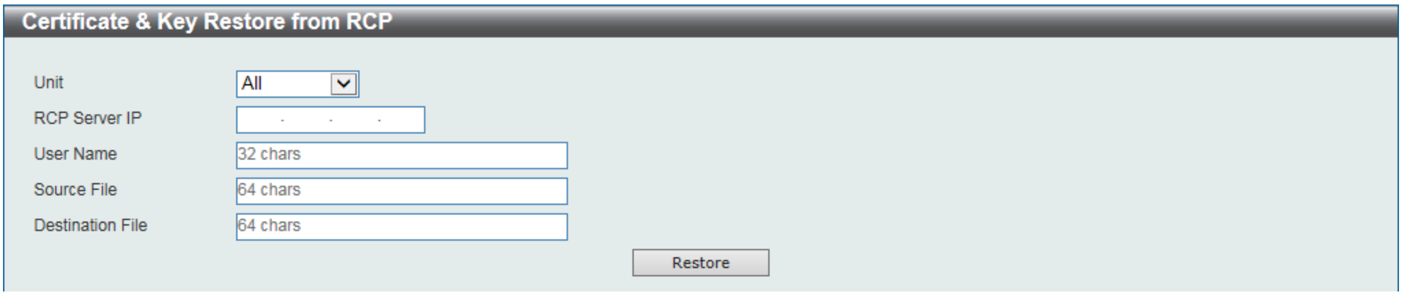


Figure 13-25 Certificate & Key Restore from RCP Window

The fields that can be configured are described below:

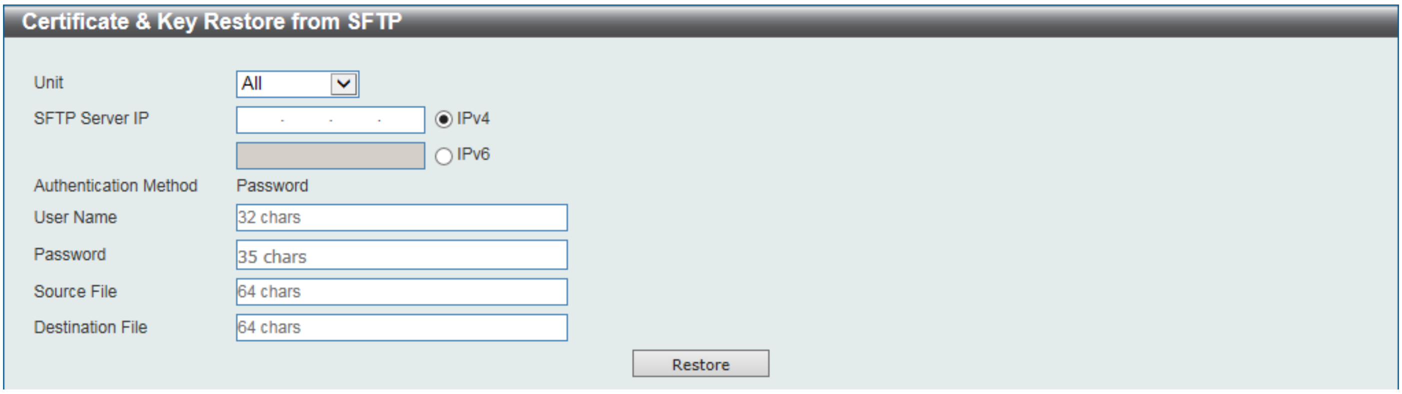
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
RCP Server IP	Enter the RCP server IP address here.
User Name	Enter the user name used for the RCP connection here. This name can be up to 32 characters long.
Source File	Enter the source filename and path of the certificate and key file located on the RCP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the new certificate and key should be stored on the Switch. This field can be up to 64 characters long.

Click the **Restore** button to initiate the certificate and key restore.

Certificate & Key Restore from SFTP

This window is used to initiate a certificate and key restore from an SFTP server.

To view the following window, click **Tools > Certificate & Key Restore & Backup > Certificate & Key Restore from SFTP**, as shown below:



Certificate & Key Restore from SFTP

Unit	All
SFTP Server IP	. . . ● IPv4
	○ IPv6
Authentication Method	Password
User Name	32 chars
Password	35 chars
Source File	64 chars
Destination File	64 chars

Figure 13-26 Certificate & Key Restore from SFTP Window

The fields that can be configured are described below:

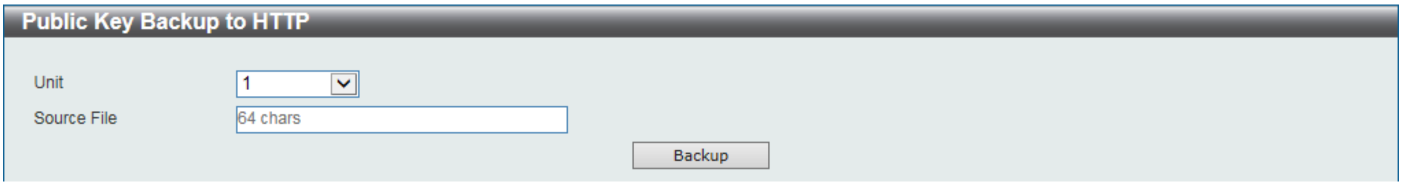
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
SFTP Server IP	Enter the SFTP server IP address here. When select the **IPv4** option, enter the IPv4 address of the SFTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 address of the SFTP server in the space provided.
User Name	Enter the user name used for the SFTP connection here. This name can be up to 32 characters long.
Password	Enter the password used for the SFTP connection here. This password can be up to 35 characters long.
Source File	Enter the source filename and path of the certificate and key file located on the SFTP server here. This field can be up to 64 characters long.
Destination File	Enter the destination path and location where the new certificate and key should be stored on the Switch. This field can be up to 64 characters long.

Click the **Restore** button to initiate the certificate and key restore.

Public Key Backup to HTTP

This window is used to initiate a public key backup to a local PC using HTTP.

To view the following window, click **Tools > Certificate & Key Upgrade & Backup > Public Key Backup to HTTP**, as shown below:



Public Key Backup to HTTP

Unit	1
Source File	64 chars

Figure 13-27 Public Key Backup to HTTP Window

The fields that can be configured are described below:

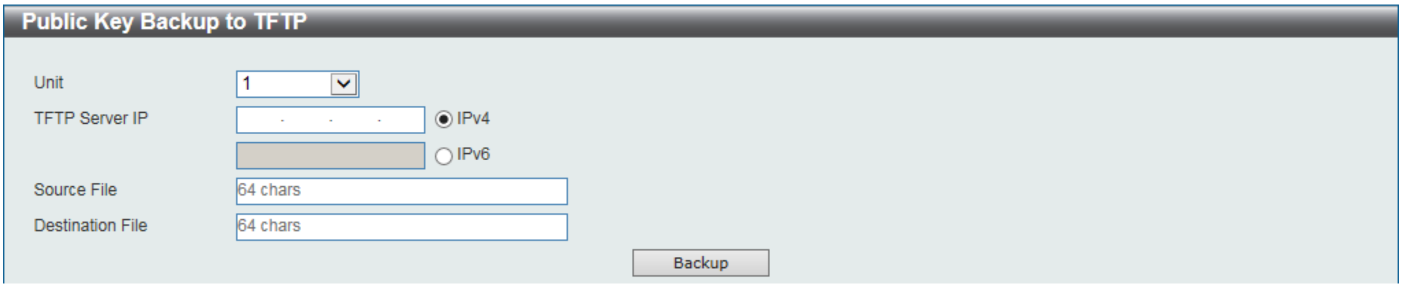
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
Source File	Enter the source filename and path of the certificate and key file located on the Switch here. This field can be up to 64 characters long.

Click the **Backup** button to initiate the certificate and key backup.

Public Key Backup to TFTP

This window is used to initiate a public key backup to a TFTP server.

To view the following window, click **Tools > Certificate & Key Upgrade & Backup > Public Key Backup to TFTP**, as shown below:



Public Key Backup to TFTP

Unit	1	
TFTP Server IP	. . .	● IPv4
		○ IPv6
Source File	64 chars	
Destination File	64 chars	

Figure 13-28 Public Key Backup to TFTP Window

The fields that can be configured are described below:

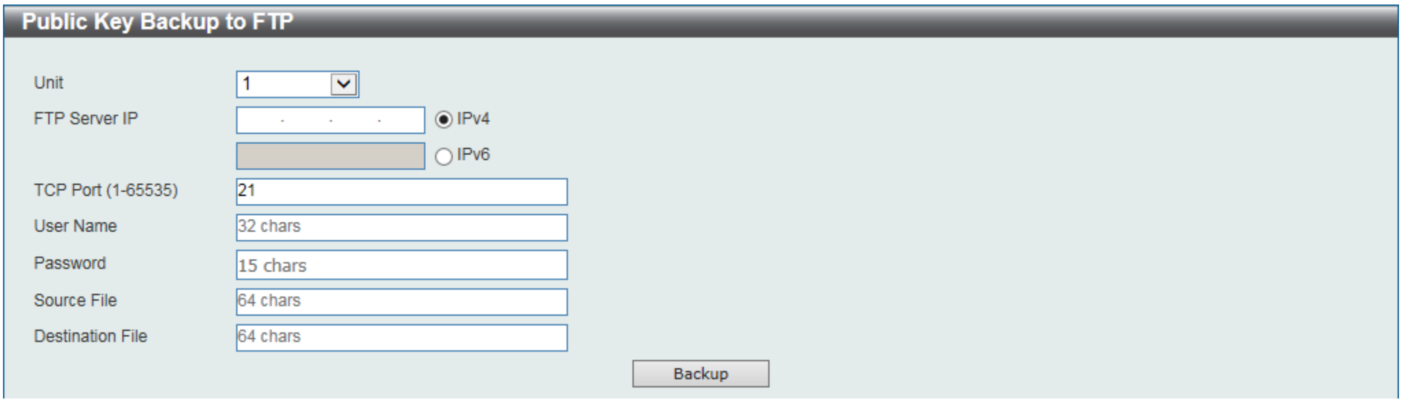
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
TFTP Server IP	Enter the TFTP server IP address here. When select the **IPv4** option, enter the IPv4 address of the TFTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 address of the TFTP server in the space provided.
Source File	Enter the source filename and path of the certificate and key file located on the Switch here. This field can be up to 64 characters long.
Destination File	Enter the destination filename and path of the certificate and key 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 certificate and key backup.

Public Key Backup to FTP

This window is used to initiate a public key backup to an FTP server.

To view the following window, click **Tools > Certificate & Key Upgrade & Backup > Public Key Backup to FTP**, as shown below:



Public Key Backup to FTP

Unit: 1

FTP Server IP: ● IPv4 ○ IPv6

TCP Port (1-65535): 21

User Name: 32 chars

Password: 15 chars

Source File: 64 chars

Destination File: 64 chars

Figure 13-29 Public Key Backup to FTP Window

The fields that can be configured are described below:

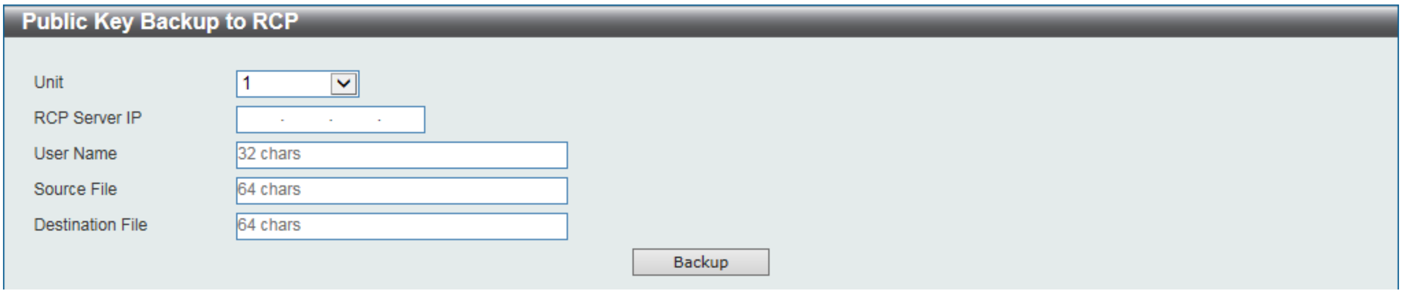
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
FTP Server IP	Enter the FTP server IP address here. When select the **IPv4** option, enter the IPv4 address of the FTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 address of the FTP server in the space provided.
TCP Port	Enter the TCP port number used for the FTP connection here. The range is from 1 to 65535.
User Name	Enter the user name used for the FTP connection here. This name can be up to 32 characters long.
Password	Enter the password used for the FTP connection here. This password can be up to 15 characters long.
Source File	Enter the source filename and path of the certificate and key file located on the Switch here. This field can be up to 64 characters long.
Destination File	Enter the destination filename and path of the certificate and key file to be backed up to the FTP server here. This field can be up to 64 characters long.

Click the **Backup** button to initiate the certificate and key backup.

Public Key Backup to RCP

This window is used to initiate a public key backup to an RCP server.

To view the following window, click **Tools > Certificate & Key Upgrade & Backup > Public Key Backup to RCP**, as shown below:



Public Key Backup to RCP

Unit	1
RCP Server IP	. . .
User Name	32 chars
Source File	64 chars
Destination File	64 chars

Figure 13-30 Public Key Backup to RCP Window

The fields that can be configured are described below:

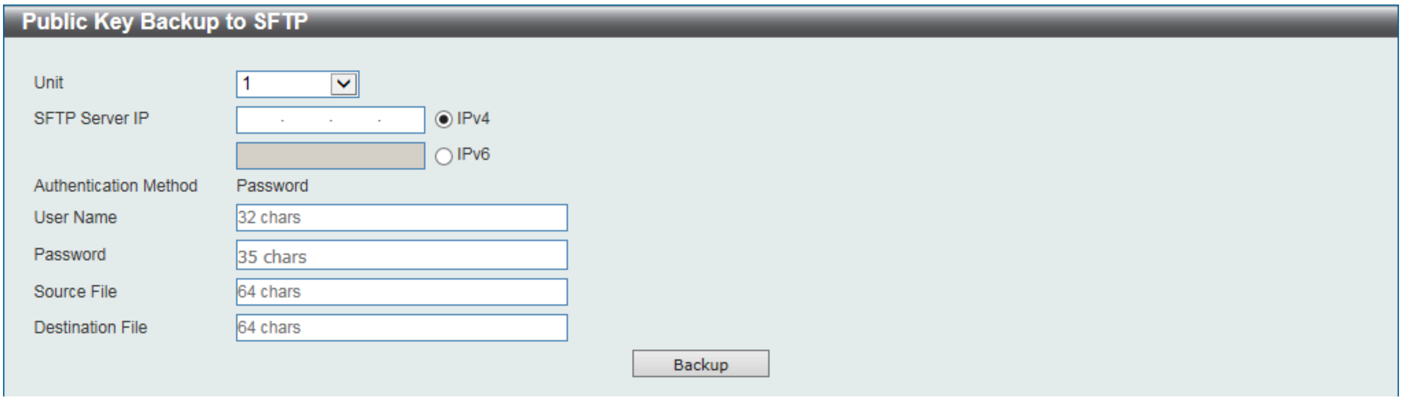
Parameter	Description
Unit	Select the Switch unit that will be used for this configuration here.
RCP Server IP	Enter the RCP server IP address here.
User Name	Enter the user name used for the RCP connection here. This name can be up to 32 characters long.
Source File	Enter the source filename and path of the certificate and key file located on the Switch here. This field can be up to 64 characters long.
Destination File	Enter the destination filename and path of the certificate and key file to be backed up to the RCP server here. This field can be up to 64 characters long.

Click the **Backup** button to initiate the certificate and key backup.

Public Key Backup to SFTP

This window is used to initiate a public key backup to an SFTP server.

To view the following window, click **Tools > Certificate & Key Upgrade & Backup > Public Key Backup to SFTP**, as shown below:



Public Key Backup to SFTP

Unit	1
SFTP Server IP	. . . ● IPv4
	○ IPv6
Authentication Method	Password
User Name	32 chars
Password	35 chars
Source File	64 chars
Destination File	64 chars

Figure 13-31 Public Key Backup to SFTP 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.
SFTP Server IP	Enter the SFTP server IP address here. When select the **IPv4** option, enter the IPv4 address of the SFTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 address of the SFTP server in the space provided.
User Name	Enter the user name used for the SFTP connection here. This name can be up to 32 characters long.
Password	Enter the password used for the SFTP connection here. This password can be up to 35 characters long.
Source File	Enter the source filename and path of the certificate and key file located on the Switch here. This field can be up to 64 characters long.
Destination File	Enter the destination filename and path of the certificate and key file to be backed up to the SFTP server here. This field can be up to 64 characters long.

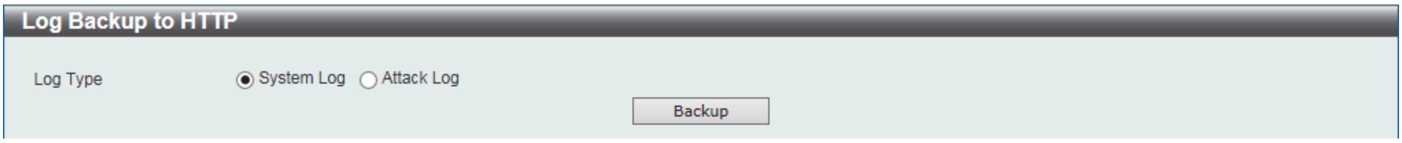
Click the **Backup** button to initiate the certificate and key backup.

Log Backup

Log Backup to HTTP

This window is used to initiate a system log backup to a local PC using HTTP.

To view the following window, click **Tools > Log Backup > Log Backup to HTTP**, as shown below:



Log Backup to HTTP

Log Type ● System Log ○ Attack Log

Figure 13-32 Log Backup to HTTP Window

The fields that can be configured are described below:

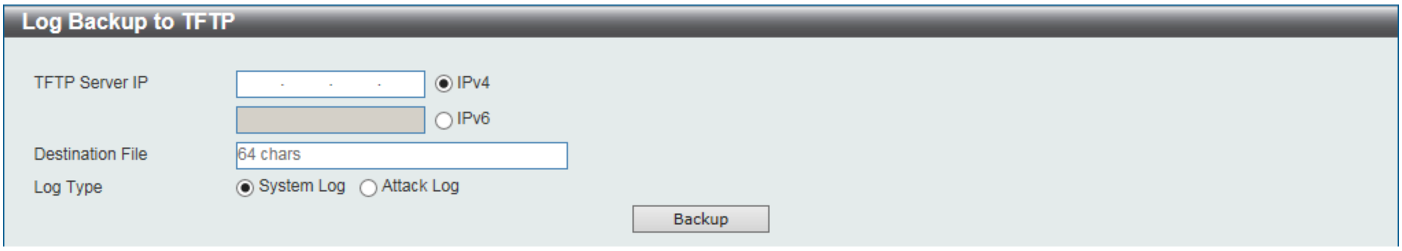
Parameter	Description
Log Type	Select the log type that will be backed up to the local PC using HTTP. • When the **System Log** option is selected, the system log will be backed up. • When the **Attack Log** is selected, the attack log will be backed up.

Click the **Backup** button to initiate the system log backup.

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:



Log Backup to TFTP

TFTP Server IP ● IPv4 ○ IPv6

Destination File: 64 chars

Log Type: ● System Log ○ Attack Log

Figure 13-33 Log Backup to TFTP Window

The fields that can be configured are described below:

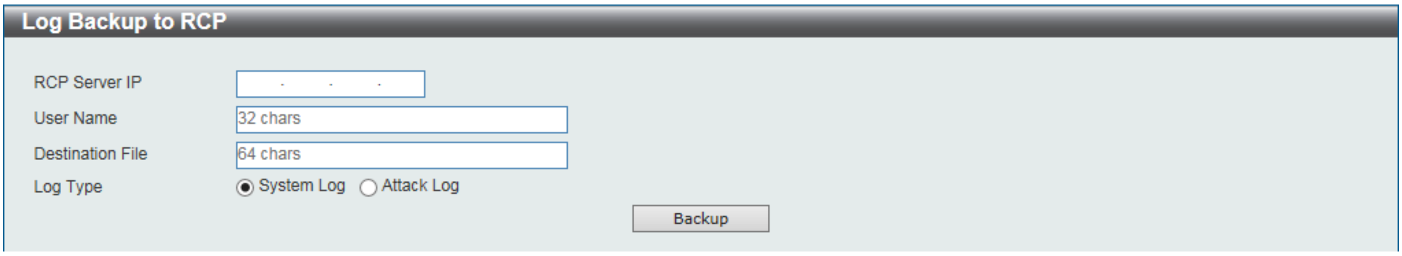
Parameter	Description
TFTP Server IP	Enter the TFTP server IP address here. When select the **IPv4** option, enter the IPv4 address of the TFTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 address of the TFTP server in the space provided.
Destination File	Enter the 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.

Log Backup to RCP

This window is used to initiate a system log backup to an RCP server.

To view the following window, click **Tools > Log Backup > Log Backup to RCP**, as shown below:



Log Backup to RCP

RCP Server IP

User Name: 32 chars

Destination File: 64 chars

Log Type: ● System Log ○ Attack Log

Figure 13-34 Log Backup to RCP Window

The fields that can be configured are described below:

Parameter	Description
RCP Server IP	Enter the RCP server IP address here.
User Name	Enter the user name used for the RCP connection here. This name can be up to 32 characters long.
Destination File	Enter the destination path and location where the log file should be stored on the RCP server. This field can be up to 64 characters long.
Log Type	Select the log type that will be backed up to the RCP server.

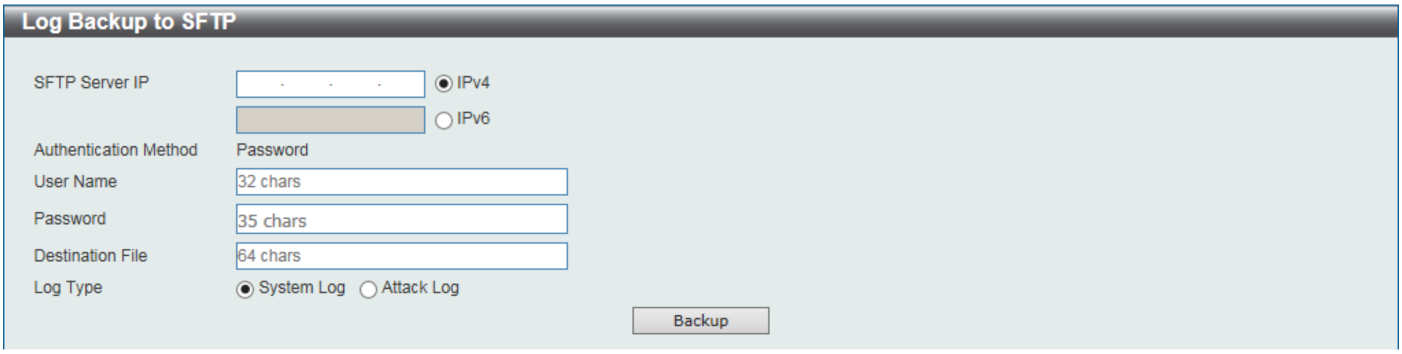
Parameter	Description
	• When the **System Log** option is selected, the system log will be backed up. • When the **Attack Log** is selected, the attack log will be backed up.

Click the **Backup** button to initiate the system log backup.

Log Backup to SFTP

This window is used to initiate a system log backup to an SFTP server.

To view the following window, click **Tools > Log Backup > Log Backup to SFTP**, as shown below:


Log Backup to SFTP

SFTP Server IP: . . . ● IPv4
○ IPv6
Authentication Method: Password
User Name: 32 chars
Password: 35 chars
Destination File: 64 chars
Log Type: ● System Log ○ Attack Log

Figure 13-35 Log Backup to SFTP Window

The fields that can be configured are described below:

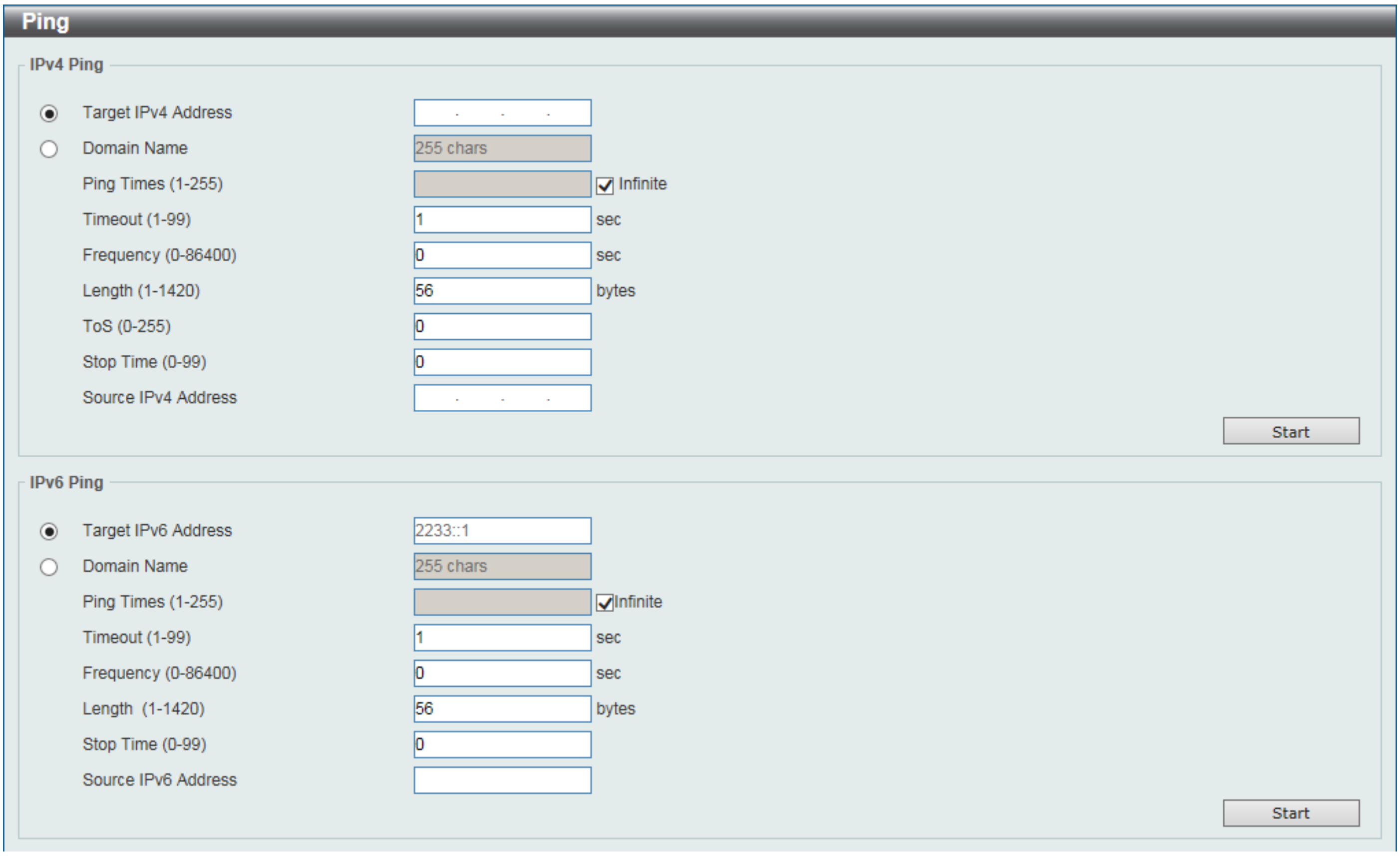
Parameter	Description
SF Server IP	Enter the SFTP server IP address here. When select the **IPv4** option, enter the IPv4 address of the SFTP server in the space provided. When the **IPv6** option is selected, enter the IPv6 address of the SFTP server in the space provided.
User Name	Enter the user name used for the SFTP connection here. This name can be up to 32 characters long.
Password	Enter the password used for the SFTP connection here. This password can be up to 35 characters long.
Destination File	Enter the destination path and location where the log file should be stored on the SFTP server. This field can be up to 64 characters long.
Log Type	Select the log type that will be backed up to the SFTP 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:



Ping

IPv4 Ping

● Target IPv4 Address	. . .	
○ Domain Name	255 chars	
Ping Times (1-255)		☑ Infinite
Timeout (1-99)	1	sec
Frequency (0-86400)	0	sec
Length (1-1420)	56	bytes
ToS (0-255)	0	
Stop Time (0-99)	0	
Source IPv4 Address	. . .	

IPv6 Ping

● Target IPv6 Address	2233::1	
○ Domain Name	255 chars	
Ping Times (1-255)		☑Infinite
Timeout (1-99)	1	sec
Frequency (0-86400)	0	sec
Length (1-1420)	56	bytes
Stop Time (0-99)	0	
Source IPv6 Address		

Figure 13-36 Ping Window

The fields that can be configured in **IPv4 Ping** are described below:

Parameter	Description
Target IPv4 Address	Select and enter an IP address to be pinged.
Domain Name	Select and enter the domain name of the system to discover.
Ping Times	Enter the number of times desired to attempt to Ping the IPv4 address configured in this window. The range is from 1 to 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 here. The range is from 1 to 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 frequency time for ping. The range is from 0 to 86400 seconds.
Length	Enter the number of data bytes to be sent. The value does not include any VLAN or IEEE 802.1Q tag length. The range is from 1 to 1420 bytes.
ToS	Enter to configure ToS in the IP header of the outgoing datagrams. The range is from 0 to 255.
Stop Time	Enter to stop pining after the specified time. If the value is 0, the pinging will never stop. The range is from 0 to 99.
Source IPv4 Address	Enter the source IPv4 address. If the current Switch has more than one IP address, you can enter one of them to this field. When entered, this IPv4 address

Parameter	Description
	will be used as the packets' source IP address sent to the remote host, or as primary IP address.

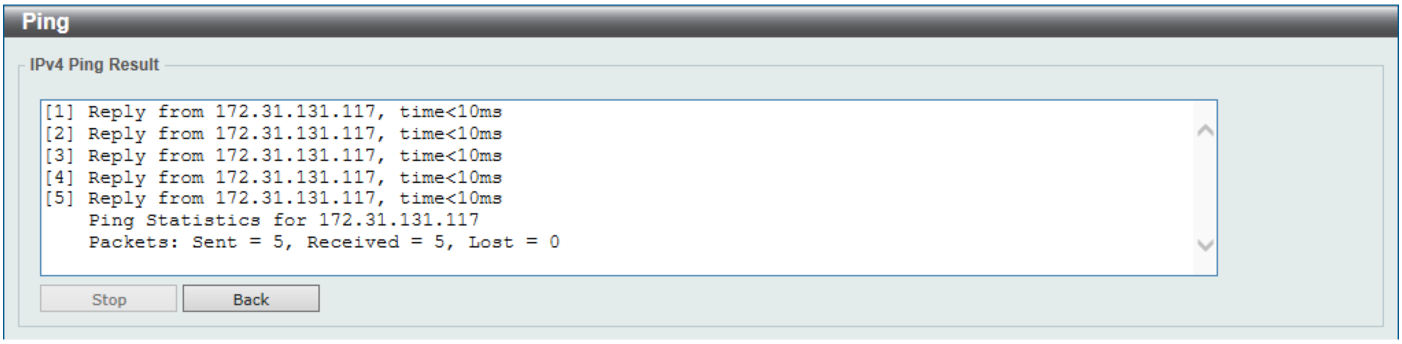
Click the **Start** button to initiate the Ping Test for each individual section.

The fields that can be configured in **IPv6 Ping** are described below:

Parameter	Description
Target IPv6 Address	Enter an IPv6 address to be pinged.
Domain Name	Select and enter the domain name of the system to discover.
Ping Times	Enter the number of times desired to attempt to Ping the IPv6 address configured in this window. The range is from 1 to 255. Tick the **Infinite** check box to keep sending ICMPv6 Echo packets to the specified IPv6 address until the program is stopped.
Timeout	Select a timeout period here. The range is from 1 to 99 seconds for this Ping message to reach its destination. If the packet fails to find the IPv6 address in this specified time, the Ping packet will be dropped.
Frequency	Enter the frequency time for ping. The range is from 0 to 86400 seconds.
Length	Enter the number of data bytes to be sent. The value does not include any VLAN or IEEE 802.1Q tag length. The range is from 1 to 1420 bytes.
Stop Time	Enter to stop pining after the specified time. If the value is 0, the pinging will never stop. 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 IPv6 address sent to the remote host, or as primary IPv6 address.

Click the **Start** button to initiate the Ping Test for each individual section.

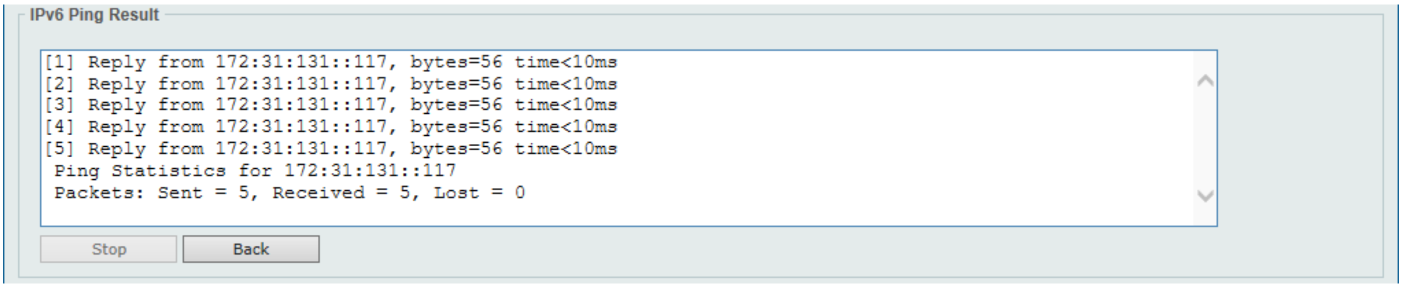
After clicking the **Start** button in **IPv4 Ping** section, the following **IPv4 Ping Result** will appear:



```
[1] Reply from 172.31.131.117, time<10ms
[2] Reply from 172.31.131.117, time<10ms
[3] Reply from 172.31.131.117, time<10ms
[4] Reply from 172.31.131.117, time<10ms
[5] Reply from 172.31.131.117, time<10ms
    Ping Statistics for 172.31.131.117
    Packets: Sent = 5, Received = 5, Lost = 0
```

Figure 13-37 IPv4 Ping Result Window

After clicking the **Start** button in **IPv6 Ping** section, the following **IPv6 Ping Result** will appear:



```
[1] Reply from 172:31:131::117, bytes=56 time<10ms
[2] Reply from 172:31:131::117, bytes=56 time<10ms
[3] Reply from 172:31:131::117, bytes=56 time<10ms
[4] Reply from 172:31:131::117, bytes=56 time<10ms
[5] Reply from 172:31:131::117, bytes=56 time<10ms
 Ping Statistics for 172:31:131::117
 Packets: Sent = 5, Received = 5, Lost = 0
```

Figure 13-38 IPv6 Ping Result Window

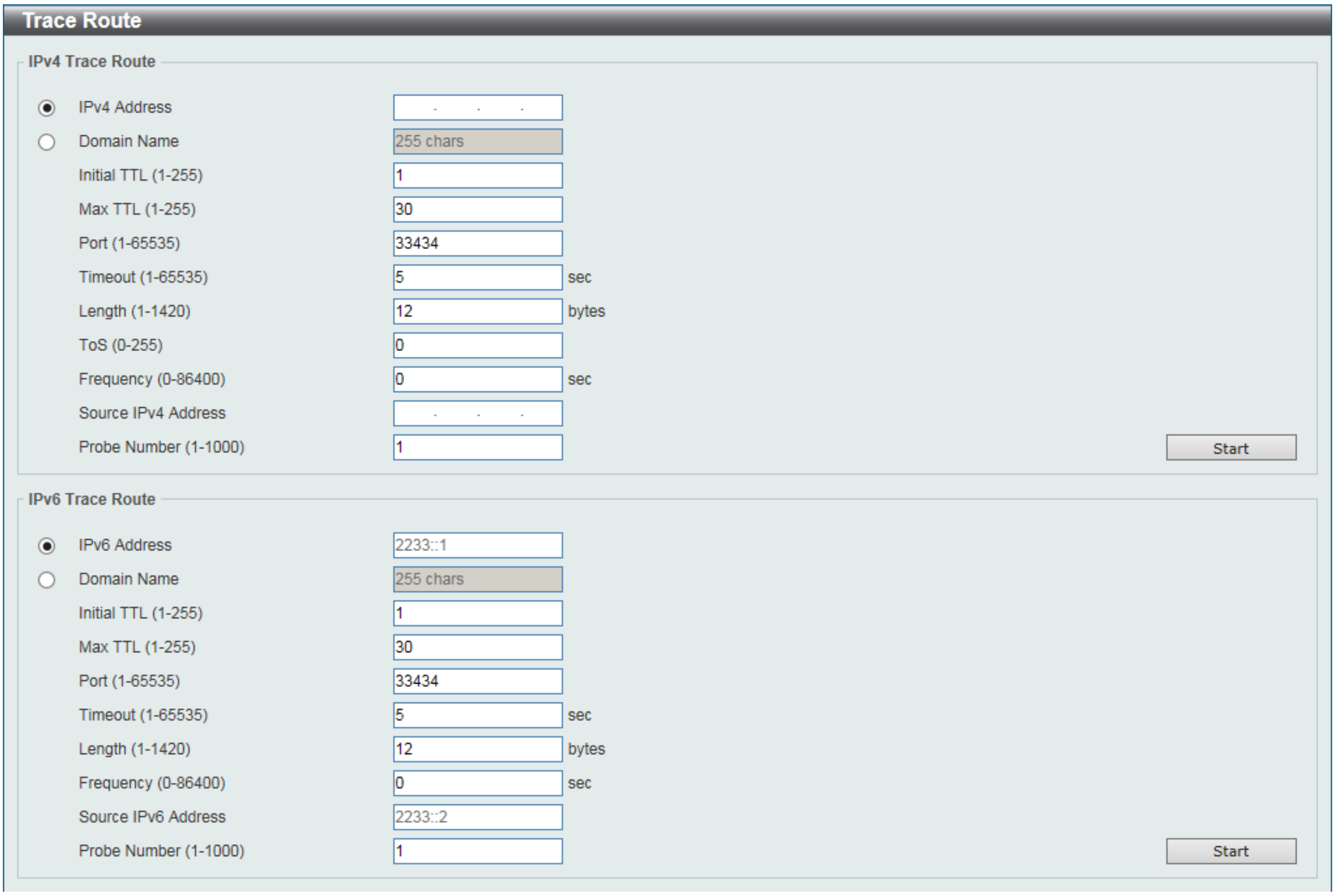
Click the **Stop** button to halt the Ping Test.

Click the **Back** button to return to the 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:



Trace Route

IPv4 Trace Route

● IPv4 Address	. . .	
○ Domain Name	255 chars	
Initial TTL (1-255)	1	
Max TTL (1-255)	30	
Port (1-65535)	33434	
Timeout (1-65535)	5	sec
Length (1-1420)	12	bytes
ToS (0-255)	0	
Frequency (0-86400)	0	sec
Source IPv4 Address	. . .	
Probe Number (1-1000)	1	

IPv6 Trace Route

● IPv6 Address	2233::1	
○ Domain Name	255 chars	
Initial TTL (1-255)	1	
Max TTL (1-255)	30	
Port (1-65535)	33434	
Timeout (1-65535)	5	sec
Length (1-1420)	12	bytes
Frequency (0-86400)	0	sec
Source IPv6 Address	2233::2	
Probe Number (1-1000)	1	

Figure 13-39 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 to send UDP datagrams with the specified value. The allowed range is from 1 to 255.
Max TTL	Enter the 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 number of bytes of the outgoing datagrams. The range is from 1 to 1420 bytes.

Parameter	Description
ToS	Enter to configure ToS in the IP header of the outgoing datagrams. The range is from 0 to 255.
Frequency	Enter the frequency time for trace route. The range is from 0 to 86400 seconds.
Source IPv4 Address	Enter the source IP address used for the trace route packet.
Probe Number	Enter the probe time number here. The range is from 1 to 1000. If unspecified, the default value is 1.

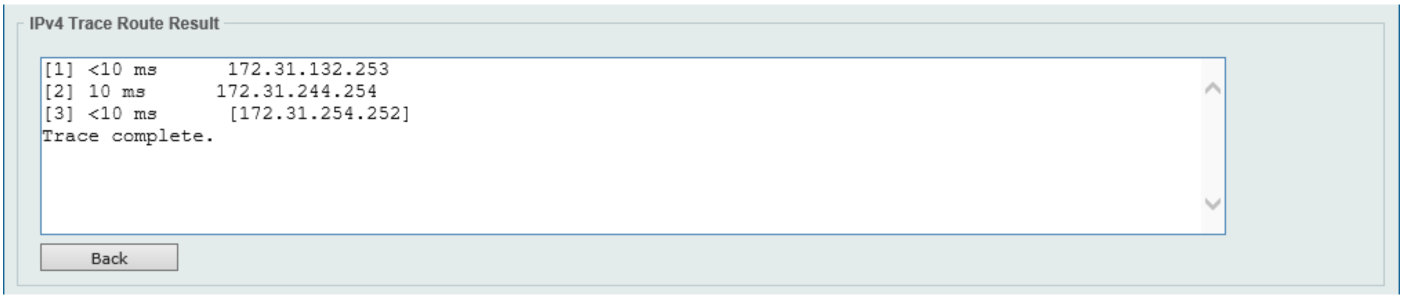
Click the **Start** button to initiate the route trace for each individual section.

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 to send UDP datagrams with the specified value. The allowed range is from 1 to 255.
Max TTL	Enter the 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 number of bytes of the outgoing datagrams. The range is from 1 to 1420 bytes.
Frequency	Enter the frequency time for trace route. The range is from 0 to 86400 seconds.
Source IPv6 Address	Enter the source IP address used for the trace route packet.
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.

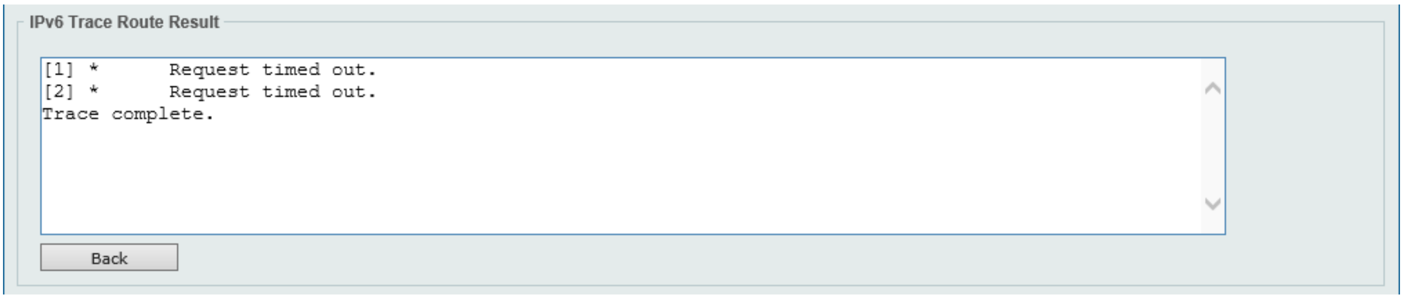
After clicking the **Start** button in **IPv4 Trace Route** section, the following **IPv4 Trace Route Result** will appear:



```
[1] <10 ms      172.31.132.253
[2] 10 ms      172.31.244.254
[3] <10 ms      [172.31.254.252]
Trace complete.
```

Figure 13-40 IPv4 Trace Route Result Window

After clicking the **Start** button in **IPv6 Trace Route** section, the following **IPv6 Trace Route Result** will appear:



IPv6 Trace Route Result

```
[1] *      Request timed out.
[2] *      Request timed out.
Trace complete.
```

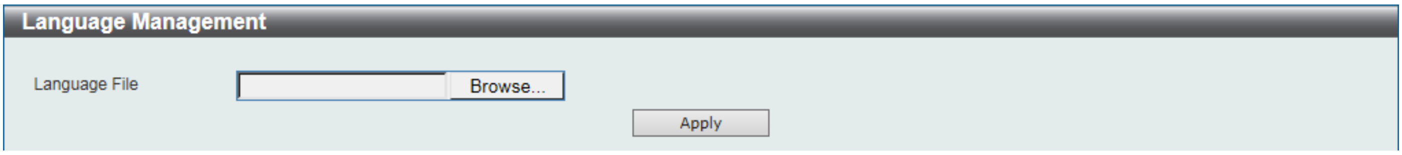
Figure 13-41 IPv6 Trace Route Result Window

Click the **Back** button to stop the trace route and return to the Trace Route section.

Language Management

This window is used to download a language file to the Switch.

To view the following window, click **Tools > Language Management**, as shown below:



Language Management

Language File

Figure 13-42 Language Management Window

The fields that can be configured are described below:

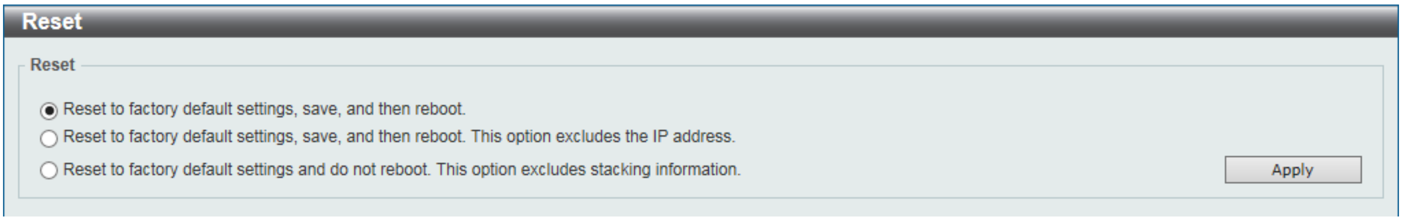
Parameter	Description
Language File	In this field the language filename and path will be displayed after selection. To navigate to the location of the language file located on the local PC, either double click in the text box or click the **Browse** button.

Click the **Apply** button to save the configuration.

Reset

This window is used to reset the Switch's configuration to the factory default settings.

To view the following window, click **Tools > Reset**, as shown below:



Reset

Reset

● Reset to factory default settings, save, and then reboot.
○ Reset to factory default settings, save, and then reboot. This option excludes the IP address.
○ Reset to factory default settings and do not reboot. This option excludes stacking information.

Figure 13-43 Reset Window

Select one of the following options:

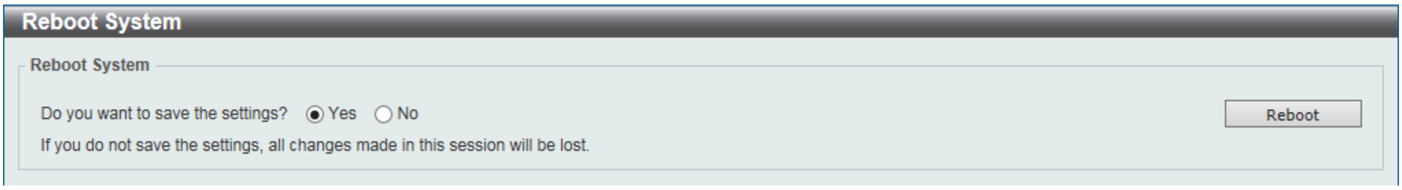
- Reset to factory default settings, save, and then reboot.
- Reset to factory default settings, save, and then reboot. This option excludes the IP address.
- Reset to factory default settings and do not reboot. This option excludes stacking information.

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:


Reboot System

Reboot System

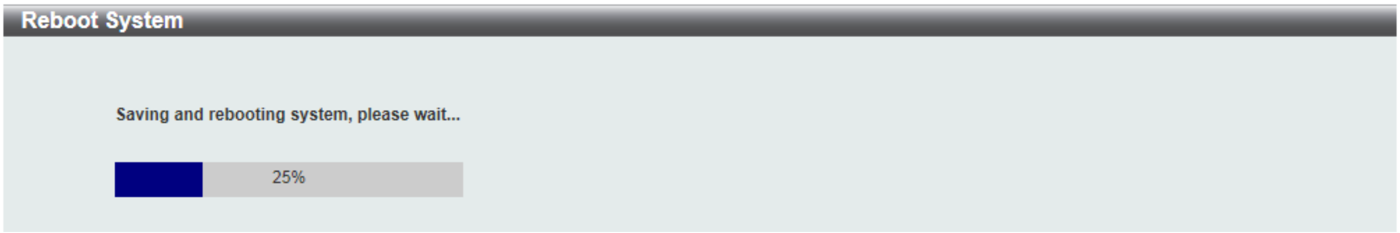
Do you want to save the settings? ● Yes ○ No

If you do not save the settings, all changes made in this session will be lost.

Figure 13-44 Reboot System Window

When rebooting the Switch, any configuration changes that was made during this session, will be lost unless the **Yes** option is selected when asked to save the settings.

Click the **Reboot** button to alternatively save the settings and reboot the Switch.


Reboot System

Saving and rebooting system, please wait...

25%

Figure 13-45 Reboot System (Rebooting) Window

Language

Select the language to be used on the Web UI in the drop-down list.

Logout

Click this option to log out of the Web UI of the Switch.

Appendix A - Password Recovery Procedure

Authenticating any user attempting to access networks is crucial. The primary authentication method used to grant access to qualified users is through a local login, which involves using a username and password. Occasionally, passwords are forgotten or lost, requiring network administrators to reset them. This section will elucidate how the **Password Recovery** feature can assist network administrators in achieving this goal.

Follow these steps to access the **Password Recovery Mode**:

- For security reasons, the administrator must physically connect to the **Console** port of the Switch to initiate password recovery. Power on the Switch.
- While the system is booting up, and when the **Starting runtime image** message appears, press Shift+6 (^) to enter the Password Recovery Mode. In Password Recovery Mode, all ports on the Switch will be disabled.

```
  Loader Procedure
--------------------------------------------------------------------------------
  Please Wait, Loading 1.00.032 Runtime Image ..............  100 %
  UART init .................................................  100 %
  Starting runtime image
```

```
Password Recovery Mode

Switch(reset-config)#
```

In the **Password Recovery Mode**, the following commands can be used.

Command	Description
`no enable password`	This command is used to delete all account level passwords.
`no login console`	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 System Log entries are listed in this appendix.

802.1X

Log	Description	Severity
1	Event Description: This log is recorded when IEEE 802.1X authentication fails. Log Message: 802.1X authentication fail [due to <reason>] from (Username: <username>, <interface-id>, MAC: <mac-address>) Parameters Description: reason: The reason for the authentication failure. Possible reasons include: (1) User authentication failure (2) No server(s) responding (3) No servers configured (4) Insufficient resources (5) User timeout expired username: The user being authenticated. interface-id: The switch interface number. mac-address: The MAC address of the authenticated device.	Critical
2	Event Description: This log is recorded when IEEE 802.1X authentication is successful. Log Message: 802.1X authentication success (Username: <username>, <interface-id>, MAC: <mac-address>) Parameters Description: username: The user being authenticated. interface-id: The interface name. mac-address: The MAC address of the authenticated device.	Informational
3	Event Description: This log is recorded when IEEE 802.1X authentication cannot function due to ACL hardware exhaustion. Log Message: 802.1X cannot work correctly because ACL rule resource is not available	Alert

AAA

Log	Description	Severity
1	Event Description: This log is recorded when the AAA global state is enabled or disabled. Log Message: AAA is <status> Parameters Description: status: The AAA status.	Informational
2	Event Description: This log is recorded when a login is successful. Log Message: Successful login through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>) Parameters Description: exec-type: The EXEC types, for example, Console, Telnet, SSH, Web, or Web (SSL). client-ip: The IP address of the client if valid through IP protocol. aaa-method: The authentication method, for example, none, local, or server. server-ip: The IP address of the AAA server if the authentication method is a remote server. username: The username for authentication.	Informational
3	Event Description: This log is recorded when a login fails. Log Message: Login failed through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>) Parameters Description: exec-type: The EXEC types, for example, Console, Telnet, SSH, Web, or Web (SSL). client-ip: The IP address of the client if valid through IP protocol. aaa-method: The authentication method, for example, local or server. server-ip: The IP address of the AAA server if the authentication method is a remote server.	Warning

Log	Description	Severity
	username: The username for authentication.	
4	Event Description: This log is recorded when RADIUS assigns valid VLAN ID attributes. Log Message: RADIUS server <server-ip> assigned VID: <vid> to port <interface-id> (Username: <username>) Parameters Description: server-ip: The IP address of the RADIUS server. vid: The VLAN ID assigned by the RADIUS server. interface-id: The port number of the authenticated client. username: The username for authentication.	Informational
5	Event Description: This log is recorded when RADIUS assigns valid bandwidth attributes. Log Message: RADIUS server <server-ip> assigned <direction> bandwidth: <threshold> to port <interface-id> (Username: <username>) Parameters Description: server-ip: The IP address of the RADIUS server. direction: The direction for bandwidth control, for example, ingress or egress. threshold: The bandwidth threshold assigned by the RADIUS server. interface-id: The port number of the authenticated client. username: The username for authentication.	Informational
6	Event Description: This log is recorded when RADIUS assigns 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: The IP address of the RADIUS server. priority: The priority assigned by the RADIUS server. interface-id: The port number of the authenticated client. username: The username for authentication.	Informational
7	Event Description: This log is recorded when RADIUS assigns an ACL script but fails to apply it to the system due to insufficient resources. Log Message: RADIUS server <server-ip> assigns <username> ACL failure at port <interface-id> (<acl-script>) Parameters Description: server-ip: The IP address of the RADIUS server. username: The username for authentication. interface-id: The port number of the authenticated client. acl-script: The ACL script assigned by the RADIUS server.	Warning
8	Event Description: This log is recorded when the remote server does not respond to the login authentication request. Log Message: Login failed through <exec-type> <from client-ip> due to AAA server <server-ip> timeout (Username: <username>) Parameters Description: exec-type: The EXEC types, such as Console, Telnet, SSH, Web, or Web (SSL). client-ip: The IP address of the client if valid through the IP protocol. aaa-method: The authentication method, for example, local or server. server-ip: The IP address of the AAA server if the authentication method is a remote server. username: The username for authentication.	Warning
9	Event Description: This log is recorded when enable privilege is successfully enabled. Log Message: Successful enable privilege through <exec-type> <from client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>) Parameters Description: exec-type: The EXEC types, for example, Console, Telnet, SSH, Web, or Web (SSL). client-ip: The IP address of the client if valid through the IP protocol. aaa-method: The authentication method, for example, local or server. server-ip: The IP address of the AAA server if the authentication method is a remote server. username: The username for authentication.	Informational
10	Event Description: This log is recorded when enable privilege fails.	Warning

Log	Description	Severity
	Log Message: Enable privilege failed through <exec-type> <from client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>) Parameters Description: exec-type: The EXEC types, for example, Console, Telnet, SSH, Web, or Web (SSL). client-ip: The IP address of the client if valid through the IP protocol. aaa-method: The authentication method, for example, local or server. server-ip: The IP address of the AAA server if the authentication method is a remote server. username: The username for authentication.	
11	Event Description: This log is recorded when the remote server does not respond to the enable password authentication request. Log Message: Enable privilege failed through <exec-type> <from client-ip> due to AAA server <server-ip> timeout (Username: <username>) Parameters Description: exec-type: The EXEC types, for example, Console, Telnet, SSH, Web, or Web (SSL). client-ip: The IP address of the client if valid through the IP protocol. aaa-method: The authentication method, for example, local or server. server-ip: The IP address of the AAA server if the authentication method is a remote server. username: The username for authentication.	Warning
12	Event Description: This log is recorded when a local user is locked out. Log Message: User <username> locked out on authentication failure Parameters Description: username: The username of the locked-out user.	Notice
13	Event Description: This log is recorded when a local user is unlocked. Log Message: User <username> unlocked Parameters Description: username: The username of the previously locked-out user.	Notice
14	Event Description: This log is recorded when RADIUS assigned an ACL script success. Log Message: RADIUS server <server-ip> assigns <username> ACL success at port <interface-id> (<acl-script>) Parameters Description: server-ip: The IP address of the RADIUS server. username: The username for authentication. interface-id: The port number of the authenticated client. acl-script: The assign ACL script authorized by the RADIUS server.	Informational

ARP

Log	Description	Severity
1	Event Description: This log is recorded when gratuitous ARP detects a duplicate IP address. Log Message: Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <port-num>, Interface: <ipif-name>) Parameters Description: ipaddr: The duplicated IP address. macaddr: The MAC address of the duplicated IP address. port-num: The port number of the device. ipif-name: The name of the interface on the switch that contains the duplicated IP address.	Warning

Auto Image

Log	Description	Severity
1	Event Description: This log is recorded when the auto-image firmware upgrade is successful. Log Message: The downloaded firmware was successfully executed by DHCP AutoImage update (TFTP Server IP: <ipaddr>)	Informational

Log	Description	Severity
	Parameters Description: ipaddr: The IP address of the TFTP server.	
2	Event Description: This log is recorded when the auto-image firmware upgrade fails. Log Message: The downloaded firmware was not successfully executed by DHCP AutoImage update (TFTP Server IP: <ipaddr>) Parameters Description: ipaddr: The IP address of the TFTP server.	Informational

Auto Save Config

Log	Description	Severity
1	Event Description: This log is generated when the DDP configuration is automatically saved. Log Message:CONFIG-6-DDPSAVECONFIG: Configuration automatically saved to flash due to configuring from DDP(Username: <username>, IP: <ipaddr>) username: The current logged-in user. ipaddr: The IP address of the client.	Informational

Auto Surveillance VLAN

Log	Description	Severity
1	Event Description: This log is recorded when a new surveillance device is detected on an interface. Log Message: New surveillance device detected (<interface-id>, MAC: <mac-address>) Parameters Description: interface-id: The name of the interface. mac-address: The MAC address of the surveillance device.	Informational
2	Event Description: This log is recorded when an interface, which is part of an enabled surveillance VLAN, automatically joins the surveillance VLAN. Log Message: <interface-id> add into surveillance VLAN <vid> Parameters Description: interface-id: The name of the interface. vid: The VLAN ID.	Informational
3	Event Description: This log is recorded when an interface leaves the surveillance VLAN, and no surveillance device is detected during the aging interval for that interface. Log Message: <interface-id> remove from surveillance VLAN <vid> Parameters Description: interface-id: The name of the interface. vid: The VLAN ID.	Informational

BPDU Protection

Log	Description	Severity
1	Event Description: Record the event when a BPDU attack occurs. Log Message: <interface-id> enter STP BPDU under protection state (mode: <mode>) Parameters Description: interface-id: The interface on which the STP BPDU attack was detected. mode: The BPDU Protection mode of the interface. The mode can be set to drop, block, or shutdown.	Informational
2	Event Description: Record the event when the STP BPDU attack is resolved. Log Message: <interface-id> recover from BPDU under protection state. Parameters Description: interface-id: The interface on which the STP BPDU attack was detected.	Informational

CFM

Log	Description	Severity
1	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 an unknown MEPID. macaddr: Represents the MAC address of the MEP. The value "all zeros" means an unknown MAC address.	Critical
2	Event Description: An 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. 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 an unknown MEPID. macaddr: Represents the MAC address of the MEP. The value "all zeros" means an unknown MAC address.	Warning
3	Event Description: Unable to 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."	Warning
4	Event Description: The 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."	Warning
5	Event Description: The 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."	Informational

CFM Extension

Log	Description	Severity
1	Event Description: AIS condition detected.	Notice

Log	Description	Severity
	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. 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.	
2	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.	Notice
3	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.	Notice
4	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.	Notice

Configuration/Firmware

Log	Description	Severity
1	Event Description: This log is recorded when a firmware upgrade is successful. Log Message: [Unit <unitID>,]Firmware upgraded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) Parameters Description: unitID: The unit ID. If the switch is in standalone state, there will be no unitID information for logging. session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client. server-ip: The IP address of the server. pathfile: The path and file name on the server.	Informational
2	Event Description: This log is recorded when a firmware upgrade fails. Log Message: [Unit <unitID>,]Firmware upgraded by <session> unsuccessfully (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) Parameters Description:	Warning

Log	Description	Severity
	unitID: The unit ID. If the switch is in standalone state, there will be no unitID information for logging. session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client. server-ip: The IP address of the server. pathfile: The path and file name on the server.	
3	Event Description: This log is recorded when a firmware upload is successful. Log Message: [Unit <unitID>,]Firmware uploaded by <session> successfully (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) Parameters Description: unitID: The unit ID. If the switch is in standalone state, there will be no unitID information for logging. session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client. server-ip: The IP address of the server. pathfile: The path and file name on the server.	Informational
4	Event Description: This log is recorded when a firmware upload fails. Log Message: [Unit <unitID>,]Firmware uploaded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) Parameters Description: unitID: The unit ID. If the switch is in standalone state, there will be no unitID information for logging. session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client. server-ip: The IP address of the server. pathfile: The path and file name on the server.	Warning
5	Event Description: This log is recorded when a configuration is downloaded successfully. Log Message: [Unit <unitID>,]Configuration downloaded by <session> successfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) Parameters Description: unitID: The unit ID. If the switch is in standalone state, there will be no unitID information for logging. session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client. server-ip: The IP address of the server. pathfile: The path and file name on the server.	Informational
6	Event Description: This log is recorded when a configuration download fails. Log Message: [Unit <unitID>,]Configuration downloaded by <session> unsuccessfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) Parameters Description: unitID: The unit ID. If the switch is in standalone state, there will be no unitID information for logging. session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client. server-ip: The IP address of the server. pathfile: The path and file name on the server.	Warning
7	Event Description: This log is recorded when the configuration is uploaded successfully. Log Message: [Unit <unitID>,]Configuration uploaded by <session> successfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) Parameters Description:	Informational

Log	Description	Severity
	unitID: The unit ID. If the switch is in a standalone state, there will be no unitID information for logging. session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client. server-ip: The IP address of the server. pathfile: The path and file name on the server.	
8	Event Description: This log is recorded when the configuration upload fails. Log Message: [Unit <unitID>,]Configuration uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) Parameters Description: unitID: The unit ID. If the switch is in a standalone state, there will be no unitID information for logging. session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client. server-ip: The IP address of the server. pathfile: The path and file name on the server.	Warning
9	Event Description: This log is recorded when a log message is uploaded successfully. Log Message: [Unit <unitID>,]Configuration saved to flash by console (Username: <username>) Parameters Description: unitID: The unit ID. If the switch is in standalone state, there will be no unitID information for logging. username: The current login user.	Informational
10	Event Description: This log is recorded when a configuration is saved to the flash remotely. Log Message: [Unit <unitID>,]Configuration saved to flash (Username: <username>, IP: <ipaddr>) Parameters Description: unitID: The unit ID. If the switch is in standalone state, there will be no unitID information for logging. username: The current login user. ipaddr: The IP address of the client.	Informational
11	Event Description: This log is recorded when a log message is uploaded successfully. Log Message: Log message uploaded by <session> successfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>]) Parameters Description: session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client.	Informational
12	Event Description: This log is recorded when a log message upload fails. Log Message: Log message uploaded by <session> unsuccessfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>]) Parameters Description: session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client.	Warning
13	Event Description: This log is recorded when an unknown file type download fails. Log Message: [Unit <unitID>,]Downloaded by <session> unsuccessfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) Parameters Description: unitID: The unit ID. If the switch is in standalone state, there will be no unitID information for logging. session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client.	Warning

Log	Description	Severity
	server-ip: The IP address of the server. pathfile: The path and file name on the server.	

NOTE:

1. The user's session indicates Console, Web, SNMP, Telnet, or SSH.
2. If updating configuration/firmware through Console, there will be no IP and MAC information available for logging.

DAD

Log	Description	Severity
1	Event Description: This log is recorded when the DUT receives a Neighbor Solicitation (NS) message with a duplicate address during the Duplicate Address Detection (DAD) duration. The DUT will add this log. Log Message: Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Solicitation Messages Parameters Description: ipv6address: The IPv6 address in NS messages. interface-id: The interface name.	Warning
2	Event Description: This log is recorded when the DUT receives a Neighbor Advertisement (NA) message with a duplicate address during the Duplicate Address Detection (DAD) duration. The DUT will add this log. Log Message: Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Advertisement Messages Parameters Description: ipv6address: The IPv6 address in NA messages. interface-id: The interface name.	Warning

DAI

Log	Description	Severity
1	Event Description: This log is recorded when DAI detects invalid ARP packets. 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, indicating whether it is an ARP packet request or response. ip-address: The IP address. mac-address: The MAC address. vlan-id: The VLAN ID. interface-id: The name of the interface.	Warning
2	Event Description: This log is recorded when DAI detects valid ARP packets. Log Message: Legal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>) Parameters Description: type: The type of ARP packet, indicating whether it is an ARP packet request or response. ip-address: The IP address. mac-address: The MAC address. vlan-id: The VLAN ID. interface-id: The name of the interface.	Informational

DDM

Log	Description	Severity
1	Event Description: When any of the SFP parameters exceed the warning threshold.	Warning

Log	Description	Severity
	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.	
2	Event Description: When any of the SFP parameters exceed the alarm threshold. Log Message: Optical transceiver <interface-id> <component> <high-low> alarm threshold exceeded Parameters Description: interface-id: Port interface ID. component: DDM threshold type. It can be one of the following types: • temperature • supply voltage • bias current • TX power • RX power high-low: High or low threshold.	Critical
3	Event Description: When any of the SFP parameters recover 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

DHCP Snooping

Log	Description	Severity
1	Event Description: This message indicates that the reload of DHCP snooping entry from external storage has failed. Log Message: DHCP snooping entry reload failure (URL: <url-string>) Parameters Description: URL: URL string.	Informational

DHCPv6 Client

Log	Description	Severity
1	Event Description: DHCPv6 Client Interface Administrator State Change. Log Message: DHCPv6 client on interface <ipif-name> changed state to [enabled | disabled] Parameters Description: ipif-name: The name of the DHCPv6 client interface affected by the state change.	Informational
2	Event Description: DHCPv6 Client Obtains IPv6 Address. Log Message: DHCPv6 client obtains an IPv6 address <ipv6address> on interface <ipif-name> Parameters Description:	Informational

Log	Description	Severity
	ipv6address: The IPv6 address obtained by the DHCPv6 client. ipif-name: The name of the interface where the DHCPv6 client obtained the IPv6 address.	
3	Event Description: IPv6 Address Renewal Initiated. Log Message: The IPv6 address <ipv6address> on interface <ipif-name> starts renewing Parameters Description: ipv6address: The IPv6 address that is initiating the renewal process. ipif-name: The name of the interface where the IPv6 address is located.	Informational
4	Event Description: IPv6 Address Renewal Successful. Log Message: The IPv6 address <ipv6address> on interface <ipif-name> renews success Parameters Description: ipv6address: The IPv6 address that successfully renewed. ipif-name: The name of the interface where the IPv6 address is located.	Informational
5	Event Description: IPv6 Address Rebinding Initiated. Log Message: The IPv6 address <ipv6address> on interface <ipif-name> starts rebinding Parameters Description: ipv6address: The IPv6 address that is initiating the rebinding process. ipif-name: The name of the interface where the IPv6 address is located.	Informational
6	Event Description: IPv6 Address Rebinding Successful. Log Message: The IPv6 address <ipv6address> on interface <ipif-name> rebinds success Parameters Description: ipv6address: The IPv6 address that successfully rebound. ipif-name: The name of the interface where the IPv6 address is located.	Informational
7	Event Description: IPv6 Address Deletion. Log Message: The IPv6 address <ipv6address> on interface <ipif-name> was deleted Parameters Description: ipv6address: The IPv6 address that was deleted. ipif-name: The name of the interface from which the IPv6 address was deleted.	Informational
8	Event Description: DHCPv6 Client PD Interface Administrator State Change. Log Message: DHCPv6 client PD on interface <intf-name> changed state to <enabled | disabled> Parameters Description: intf-name: The name of the DHCPv6 client PD interface affected by the state change.	Informational
9	Event Description: DHCPv6 Client PD Obtains IPv6 Prefix. Log Message: DHCPv6 client PD obtains an ipv6 prefix < ipv6networkaddr> on interface <intf-name> Parameters Description: ipv6networkaddr: The IPv6 prefix obtained by the DHCPv6 client PD. intf-name: The name of the interface where the DHCPv6 client PD obtained the IPv6 prefix.	Informational
10	Event Description: IPv6 Prefix Renewal Initiated. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts renewing Parameters Description: ipv6networkaddr: The IPv6 prefix that is initiating the renewal process. intf-name: The name of the interface where the IPv6 prefix is located.	Informational
11	Event Description: IPv6 Prefix Renewal Successful. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> renews success Parameters Description: ipv6networkaddr: The IPv6 prefix that successfully renewed. intf-name: The name of the interface where the IPv6 prefix is located.	Informational
12	Event Description: IPv6 Prefix Rebinding Initiated. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts rebinding Parameters Description: ipv6networkaddr: The IPv6 prefix that is initiating the rebinding process. intf-name: The name of the interface where the IPv6 prefix is located.	Informational
13	Event Description: IPv6 Prefix Rebinding Successful.	Informational

Log	Description	Severity
	Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> rebinds success Parameters Description: ipv6networkaddr: The IPv6 prefix that successfully rebound. intf-name: The name of the interface where the IPv6 prefix is located.	
14	Event Description: IPv6 Prefix Deletion. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> was deleted Parameters Description: ipv6networkaddr: The IPv6 prefix that was deleted. intf-name: The name of the interface from which the IPv6 prefix was deleted.	Informational

DHCPv6 Relay

Log	Description	Severity
1	Event Description: DHCPv6 relay on a specify interface's administrator state changed. Log Message: DHCPv6 relay on interface <ipif-name> changed state to [enabled | disabled] Parameters Description: <ipif-name>: Name of the DHCPv6 relay agent interface.	Informational

DHCPv6 Server

Log	Description	Severity
1	Event Description: The addresses in the DHCPv6 server pool have been used up. Log Message: The address of the DHCPv6 Server pool <pool-name> is used up Parameters Description: pool-name: The name of the DHCPv6 Server pool.	Informational
2	Event Description: The number of allocated IPv6 addresses is equal to 256. Log Message: The number of allocated ipv6 addresses of the DHCPv6 Server pool is equal to 256	Informational

DNS Resolver

Log	Description	Severity
1	Event Description: This log is recorded when a duplicate domain name is added to the cache, resulting in the deletion of the dynamic domain name cache. Log Message: Duplicate Domain name case name: <domain-name>, static IP: <ipaddr>, dynamic IP:<ipaddr> Parameters Description: domain-name: The domain name string. ipaddr: The static/dynamic IP address.	Informational

DoS Prevention

Log	Description	Severity
1	Event Description: This log is recorded when a DoS attack is detected. Log Message: <dos-type> is dropped from (Port <interface-id>) Parameters Description: dos-type: The DoS attack type. interface-id: The name of the interface.	Notice

DULD

Log	Description	Severity
1	Event Description: A unidirectional link has been detected on this port. Log Message: DULD <INTERFACE-ID> is detected as unidirectional link Parameters Description: INTERFACE-ID: The interface name.	Warning

ERPS

Log	Description	Severity
1	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
2	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
3	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
4	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
5	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
6	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

ErrDisable

Log	Description	Severity
1	Event Description: When a port enters an error-disable state. Log Message: Port <interface-id> enters error disable state due to <reason-id> Parameters Description: interface-id: The port number. reason-id: Loopback Detection, Port Security Violation, Storm Control, BPDU Protected, ARP Rate Limit, DHCP Rate Limit, L2 Protocol Tunneling, Scheduled Port Shutdown by Power Saving, Scheduled Hibernation by Power Saving.	Warning

Log	Description	Severity
2	Event Description: When a port leaves the error-disable state. Log Message: Port <interface-id> leaves the error disable state which is previously caused by <reason-id> Parameters Description: interface-id: The port number. reason-id: Loopback Detection, Port Security Violation, Storm Control, BPDU Protected, ARP Rate Limit, DHCP Rate Limit, L2 Protocol Tunneling, Scheduled Port Shutdown by Power Saving, Scheduled Hibernation by Power Saving.	Warning
3	Event Description: When a port enters an error-disable state. Log Message: Port <interface-id> VLAN <vid> enters error disable state due to <reason-id> Parameters Description: interface-id: The port number. reason-id: Loopback Detection, Port Security Violation, Storm Control, Scheduled Port Shutdown by Power Saving, Scheduled Hibernation by Power Saving. vid: VLAN ID	Warning
4	Event Description: When a port leaves the error-disable state. Log Message: Port <interface-id> VLAN <vid> leaves the error disable state which is previously caused by <reason-id> Log Message: Port <interface-id> in VLAN <vid> leaves the error-disable state, which was previously caused by <reason-id>. Parameters Description: interface-id: The port number. reason-id: Loopback Detection, Port Security Violation, Storm Control, Scheduled Port Shutdown by Power Saving, Scheduled Hibernation by Power Saving. vid: VLAN ID	Warning

Ethernet OAM

Log	Description	Severity
1	Event Description: Dying Gasp Event (Remote) Log Message: OAM dying gasp event received (Port<interface-id>) Parameters Description: interface-id: The interface name.	Warning
2	Event Description: Dying Gasp Event (Local) Log Message: Device encountered an OAM dying gasp event	Warning
3	Event Description: Critical Event (Remote) Log Message: OAM critical event received (Port <interface-id>) Parameters Description: interface-id: The interface name.	Warning
4	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 a critical link event, e.g., OAM disable, Port shutdown, Port link down, Packet overload.	Warning
5	Event Description: Errored Frame Event (Remote) Log Message: Errored frame event received (Port <interface-id>) Parameters Description: interface-id: The interface name.	Warning
6	Event Description: Errored Frame Period Event (Remote) Log Message: Errored frame period event received (Port <interface-id>) Parameters Description: interface-id: The interface name.	Warning
7	Event Description: Errored Frame Seconds Summary Event (Remote)	Warning

Log	Description	Severity
	Log Message: Errored frame seconds summary event received (Port <interface-id>) Parameters Description: interface-id: The interface name.	
8	Event Description: Remote Loopback Start Log Message: OAM Remote loopback started (Port <interface-id>) Parameters Description: interface-id: The interface name.	Warning
9	Event Description: Remote Loopback Stop Log Message: OAM Remote loopback stopped (Port <interface-id>) Parameters Description: interface-id: The interface name.	Warning
10	Event Description: Errored Frame Event (Local) Log Message: Device encountered an errored frame event (Port <interface-id>) Parameters Description: interface-id: The interface name.	Warning
11	Event Description: Errored Frame Period Event (Local) Log Message: Device encountered an errored frame period event (Port <interface-id>) Parameters Description: interface-id: The interface name.	Warning
12	Event Description: Errored Frame Seconds Summary Event (Local) Log Message: Device encountered an errored frame seconds summary event (Port <interface-id>) Parameters Description: interface-id: The interface name.	Warning

Interface

Log	Description	Severity
1	Event Description: This log is recorded when the port link is down. Log Message: Port <port-type><interface-id> link down Parameters Description: port-type: The port type. interface-id: The interface name.	Informational
2	Event Description: This log is recorded when the port link is up. Log Message: Port <port-type><interface-id> link up, <link-speed> Parameters Description: port-type: The port type. interface-id: The interface name. link-speed: The port link speed.	Informational

IPSG

Log	Description	Severity
1	Event Description: This log is recorded when there are no hardware rule resources to set the DHCP snooping entry into the IPSG table. Log Message: Failed to set IPSG entry due to no hardware rule resource. (IP: <ipaddr>, MAC: <macaddr>, VID: <vlanid>, Interface <interface-id>) Parameters Description: ipaddr: The IP address. macaddr: The MAC address. vlanid: The VLAN ID. interface-id: The interface name.	Warning

IPv6SG

Log	Description	Severity
1	Event Description: This log is recorded when there are no hardware rule resources to set the IPv6 snooping entry into the IPv6SG table. Log Message: Failed to set IPv6SG entry due to no hardware rule resource. (IP: <ipaddr>, MAC: <macaddr>, VID: <vlan-id>, Interface <interface-id>) Parameters Description: ipaddr: The IPv6 address of the IPv6 snooping entry. macaddr: The MAC address of the IPv6 snooping entry. vlan-id: The VLAN ID of the IPv6 snooping entry. interface-id: The interface of the IPv6 snooping entry.	Warning

IPv6 Snooping

Log	Description	Severity
1	Event Description: IPv6 data glean failed. Log Message: Failed to glean (IP: <IPADDR>, MAC: <MACADDR>, VID: <VLANID>, Port <INTERFACE-ID>) Parameters Description: IPADDR: The IP address of the IPv6 Snooping entry. MACADDR: The MAC address of the IPv6 Snooping entry. VLANID: The VID of the IPv6 Snooping entry. INTERFACE-ID: The port of the IPv6 Snooping entry.	Notice
2	Event Description: IPv6 data glean succeeded. Log Message: Glean to recover (IP: <IPADDR>, MAC: <MACADDR>, VID: <VLANID>, Port <INTERFACE-ID>) Parameters Description: IPADDR: The IP address of the IPv6 Snooping entry. MACADDR: The MAC address of the IPv6 Snooping entry. VLANID: The VID of the IPv6 Snooping entry. INTERFACE-ID: The port of the IPv6 Snooping entry.	Informational

LACP

Log	Description	Severity
1	Event Description: This log is recorded when the link aggregation group link is up. Log Message: Link Aggregation Group <group-id> link up Parameters Description: group-id: The group ID of the link aggregation group.	Informational
2	Event Description: This log is recorded when the link aggregation group link is down. Log Message: Link Aggregation Group <group-id> link down Parameters Description: group-id: The group ID of the link aggregation group.	Informational
3	Event Description: This log is recorded when a member port is attached to the link aggregation group. Log Message: <ifname> attach to Link Aggregation Group <group-id> Parameters Description: ifname: The interface name of the port that is attached to the aggregation group. group-id: The group ID of the aggregation group that the port is attached to.	Informational
4	Event Description: This log is recorded when a member port is detached from the link aggregation group. Log Message: <ifname> detach from Link Aggregation Group <group-id> Parameters Description:	Informational

Log	Description	Severity
	ifname: The interface name of the port that is detached from the aggregation group. group-id: The group ID of the aggregation group that the port is detached from.	

LBD

Log	Description	Severity
1	Event Description: This log is recorded when an interface detects a loop. Log Message: <interface-id> LBD loop occurred Parameters Description: interface-id: The interface on which a loop is detected.	Critical
2	Event Description: This log is recorded when an interface detects a loop in a VLAN. Log Message: <interface-id> VLAN <vlan-id> LBD loop occurred Parameters Description: interface-id: The interface on which the loop is detected. vlan-id: The VLAN in which the loop is detected.	Critical
3	Event Description: This log is recorded when an interface loop is recovered. Log Message: <interface-id> LBD loop recovered Parameters Description: interface-id: The interface on which the loop is recovered.	Critical
4	Event Description: This log is recorded when an interface loop is recovered in a VLAN. Log Message: <interface-id> VLAN <vlan-id> LBD loop recovered Parameters Description: interface-id: The interface on which the loop is recovered. vlan-id: The VLAN in which the loop is recovered.	Critical
5	Event Description: This log is recorded when the number of VLANs that loop back exceeds the reserved number. Log Message: Loop VLAN numbers overflow	Critical

LLDP/LLDP-MED

Log	Description	Severity
1	Event Description: This log is recorded when an LLDP-MED topology change is 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: The chassis ID subtype. This can be chassisComponent (1), interfaceAlias (2), portComponent (3), macAddress (4), networkAddress (5), interfaceName (6), or local (7). chassisID: The chassis ID. portType: The port ID subtype. This can be interfaceAlias (1), portComponent (2), macAddress (3), networkAddress (4), interfaceName (5), agentCircuitId (6), or local (7). portID: The port ID. deviceClass: The LLDP-MED device type.	Notice
2	Event Description: This log is recorded when an LLDP-MED device type conflict is detected. Log Message: Conflict LLDP-MED device type detected (on port <portNum>, chassis ID: <chassisType>, <chassisID>, port ID: <portType>, <portID>, device class: <deviceClass>) Parameters Description: portNum: The port number. chassisType: The chassis ID subtype. This can be chassisComponent (1), interfaceAlias (2), portComponent (3), macAddress (4), networkAddress (5), interfaceName (6), or local (7). chassisID: The chassis ID. portType: The port ID subtype. This can be interfaceAlias (1), portComponent (2), macAddress (3), networkAddress (4), interfaceName (5), agentCircuitId (6), or local (7).	Notice

Log	Description	Severity
	portID: The port ID. deviceClass: The LLDP-MED device type.	
3	Event Description: This log is recorded when an incompatible LLDP-MED TLV set is detected. Log Message: Incompatible LLDP-MED TLV set detected (on port <portNum>, chassis ID: <chassisType>, <chassisID>, port ID: <portType>, <portID>, device class: <deviceClass>) Parameters Description: portNum: The port number. chassisType: The chassis ID subtype. This can be chassisComponent (1), interfaceAlias (2), portComponent (3), macAddress (4), networkAddress (5), interfaceName (6), or local (7). chassisID: The chassis ID. portType: The port ID subtype. This can be interfaceAlias (1), portComponent (2), macAddress (3), networkAddress (4), interfaceName (5), agentCircuitId (6), or local (7). portID: The port ID. deviceClass: The LLDP-MED device type.	Notice

Login/Logout CLI

Log	Description	Severity
1	Event Description: This log is recorded when login through the console is successful. Log Message: Successful login through Console (Username: <username>) Parameters Description: username: The current login user.	Informational
2	Event Description: This log is recorded when login through the console failed. Log Message: Login failed through Console (Username: <username>) Parameters Description: username: The current login user.	Warning
3	Event Description: This log is recorded when the console session timed out. Log Message: Console session timed out (Username: <username>) Parameters Description: username: The current login user.	Informational
4	Event Description: This log is recorded when logout from the console occurred. Log Message: Logout through Console (Username: <username>) Parameters Description: username: The current login user.	Informational
5	Event Description: This log is recorded when login through Telnet is successful. Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: The current login user. ipaddr: The IP address of the client.	Informational
6	Event Description: This log is recorded when login through Telnet failed. Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: The current login user. ipaddr: The IP address of the client.	Warning
7	Event Description: This log is recorded when the Telnet session timed out. Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: The current login user. ipaddr: The IP address of the client.	Informational
8	Event Description: This log is recorded when logout from Telnet occurred. Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description:	Informational

Log	Description	Severity
	username: The current login user. ipaddr: The IP address of the client.	
9	Event Description: This log is recorded when login through SSH is successful. Log Message: Successful login through SSH (Username: <username>, IP: <ipaddr>) Parameters Description: username: The current login user. ipaddr: The IP address of the client.	Informational
10	Event Description: This log is recorded when login through SSH failed. Log Message: Login failed through SSH (Username: <username>, IP: <ipaddr>) Parameters Description: username: The current login user. ipaddr: The IP address of the client.	Critical
11	Event Description: This log is recorded when the SSH session timed out. Log Message: SSH session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: The current login user. ipaddr: The IP address of the client.	Informational
12	Event Description: This log is recorded when logout from SSH occurred. Log Message: Logout through SSH (Username: <username>, IP: <ipaddr>) Parameters Description: username: The current login user. ipaddr: The IP address of the client.	Informational

MAC-based Access Control

Log	Description	Severity
1	Event Description: A host has passed the authentication. Log Message: MAC-based Access Control host login success (MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Parameters Description: mac-address: The host MAC address. interface-id: The interface on which the host is authenticated. vlan-id: The VLAN ID on which the host exists after it is authenticated.	Informational
2	Event Description: A 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 address. interface-id: The interface on which the host is authenticated. vlan-id: The VLAN ID on which the host exists before it is aged out.	Informational
3	Event Description: A host failed to pass the authentication. Log Message: MAC-based Access Control host login fail (MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Parameters Description: mac-address: The host MAC address. interface-id: The interface on which the host is authenticated. vlan-id: The originated VLAN ID on which the host exists.	Critical
4	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
5	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

Log	Description	Severity
6	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
7	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

Log	Description	Severity
1	Event Description: This log is recorded when the Spanning Tree Protocol is enabled. Log Message: Spanning Tree Protocol is enabled	Informational
2	Event Description: This log is recorded when the Spanning Tree Protocol is disabled. Log Message: Spanning Tree Protocol is disabled	Informational
3	Event Description: This log is recorded when an MSTP instance topology change event occurs. Log Message: Topology changed (Instance: <instance-id>,<interface-id>, MAC:<macaddr>) Parameters Description: instance-id: The MST instance ID. Instance 0 represents the default instance, CIST. interface-id: The port number that detects or receives topology change information. macaddr: The MAC address of the bridge.	Notice
4	Event Description: This log is recorded when a new MSTP instance root bridge is selected. Log Message: [CIST | CIST Region | MSTI Region] New Root bridge selected ([Instance: <instance-id>] MAC: <macaddr> Priority:<priority>) Log Message: [CIST | CIST Region | MSTI Region] New Root bridge selected ([Instance: <instance-id>] MAC: <macaddr> Priority:<priority>) Parameters Description: instance-id: The MST instance ID. Instance 0 represents the default instance, CIST. macaddr: The MAC address of the bridge. priority: The bridge priority value. This value is divisible by 4096.	Informational
5	Event Description: This log is recorded when a new MSTP instance root port is selected. Log Message: New root port selected (Instance:<instance-id>, <interface-id>) Parameters Description: instance-id: The MST instance ID. Instance 0 represents the default instance, CIST. interface-id: The port number that detects or receives topology change information.	Notice
6	Event Description: This log is recorded when an MSTP instance port state change event occurs. Log Message: Spanning Tree port status change (Instance:<instance-id>, <interface-id>) <old-status> -> <new-status> Parameters Description: instance-id: The MST instance ID. Instance 0 represents the default instance, CIST. interface-id: The port number that detects or receives topology change information. old-status: The old status of the port. This can be Disable, Discarding, Learning, or Forwarding. new-status: The new status of the port. This can be Disable, Discarding, Learning, or Forwarding.	Notice
7	Event Description: This log is recorded when an MSTP instance port role change event occurs. Log Message: Spanning Tree port role change (Instance:<instance-id>, <interface-id>) <old-role> -> <new-role> Parameters Description: instance-id: The MST instance ID. Instance 0 represents the default instance, CIST. interface-id: The port number that detects or receives topology change information. old-role: The old STP role. This can be DisablePort, AlternatePort, BackupPort, RootPort, DesignatedPort, NonstpPort, or MasterPort.	Informational

Log	Description	Severity
	new-role: The new STP role. This can be DisablePort, AlternatePort, BackupPort, RootPort, DesignatedPort, NonstpPort, or MasterPort.	
8	Event Description: This log is recorded when an MST instance is created. Log Message: Spanning Tree instance created (Instance:<instance-id>) Parameters Description: instance-id: The MST instance ID. Instance 0 represents the default instance, CIST.	Informational
9	Event Description: This log is recorded when an MST instance is deleted. Log Message: Spanning Tree instance deleted (Instance:<instance-id>) Parameters Description: instance-id: The MST instance ID. Instance 0 represents the default instance, CIST.	Informational
10	Event Description: This log is recorded when STP version changes. Log Message: Spanning Tree version change (new version:<new-version>) Parameters Description: new-version: The active STP version.	Informational
11	Event Description: This log is recorded when the configuration name and revision level changed in the MST configuration identification. Log Message: Spanning Tree MST configuration ID name and revision level change (name:<name> revision level <revision-level>) Parameters Description: name: The name given for the specified MST region. revision-level: The revision level. Switches using the same given name but with a different revision level are considered members of different MST regions.	Informational
12	Event Description: This log is recorded when a VLAN is mapped to an MST instance. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <instance-id> add vlan <startvlanid> [- <endvlanid>]) Parameters Description: instance-id: The MST instance ID. Instance 0 represents the default instance, CIST. startvlanid: The starting VLAN ID in the VLAN range to be added. endvlanid: The ending VLAN ID in the VLAN range to be added.	Informational
13	Event Description: This log is recorded when a VLAN is deleted from an MST instance. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <instance-id> delete vlan <startvlanid> [- <endvlanid>]) Parameters Description: instance-id: The MST instance ID. Instance 0 represents the default instance, CIST. startvlanid: The starting VLAN ID in the VLAN range to be deleted. endvlanid: The ending VLAN ID in the VLAN range to be deleted.	Informational
14	Event Description: This log is recorded when the port role changes to alternate due to guard root. Log Message: Spanning Tree port role change (Instance:<instance-id>, <interface-id>) to alternate port due to the guard root Parameters Description: instance-id: The MST instance ID. Instance 0 represents the default instance, CIST. interface-id: The port number that detects the event.	Informational

OSPFv2

Log	Description	Severity
1	Event Description: OSPF interface link state changed. Log Message: OSPF interface <intf-name> changed state to [Up | Down] Parameters Description: intf-name: Name of OSPF interface.	Informational
2	Event Description: OSPF interface administrator state changed. Log Message: OSPF protocol on interface <intf-name> changed state to [Enabled | Disabled] Parameters Description:	Informational

Log	Description	Severity
	intf-name: Name of OSPF interface.	
3	Event Description: One OSPF interface changed from one area to another. Log Message: OSPF interface <intf-name> changed from area <area-id> to area <area-id> Parameters Description: intf-name: Name of OSPF interface. area-id: OSPF area ID.	Informational
4	Event Description: One OSPF neighbor state changed from Loading to Full. Log Message: OSPF nbr <nbr-id> on interface <intf-name> changed state from Loading to Full Parameters Description: intf-name: Name of OSPF interface. nbr-id: Neighbor's router ID.	Notice
5	Event Description: One OSPF neighbor state changed from Full to Down. Log Message: OSPF nbr <nbr-id> on interface <intf-name> changed state from Full to Down Parameters Description: intf-name: Name of OSPF interface. nbr-id: Neighbor's router ID.	Notice
6	Event Description: One OSPF neighbor state’s dead timer expired. Log Message: OSPF nbr <nbr-id> on interface <intf-name> dead timer expired Parameters Description: intf-name: Name of OSPF interface. nbr-id: Neighbor's router ID.	Notice
7	Event Description: One OSPF virtual neighbor state changed from Loading to Full. Log Message: OSPF nbr <nbr-id> on virtual link changed state from Loading to Full Parameters Description: nbr-id: Neighbor's router ID.	Notice
8	Event Description: One OSPF virtual neighbor state changed from Full to Down. Log Message: OSPF nbr <nbr-id> on virtual link changed state from Full to Down Parameters Description: nbr-id: Neighbor's router ID.	Notice
9	Event Description: OSPF router ID was changed. Log Message: OSPF router ID changed to <router-id> Parameters Description: router-id: OSPF router ID.	Informational
10	Event Description: Enable OSPF. Log Message: OSPF state changed to Enabled	Informational
11	Event Description: Disable OSPF. Log Message: OSPF state changed to Disabled	Informational
12	Event Description: One OSPF neighbor state changed. Log Message: OSPF NBR <nbr-id> on interface <intf-name> changed state from <state> to <state>, <event> Parameters Description: nbr-id: Neighbor's router ID. intf-name: Name of OSPF interface. state: Neighbor state. event: The event that caused the neighbor state to change.	Informational
13	Event Description: One OSPF virtual neighbor state changed. Log Message: OSPF NBR <nbr-id> on virtual link changed state from <state> to <state>, <event> Parameters Description: nbr-id: Neighbor's router ID. state: Neighbor state. event: The event that caused the virtual neighbor state to change.	Informational

Peripheral

Log	Description	Severity
1	Event Description: This log is recorded when the fan is recovered. Log Message: Unit <unit-id> <fan-descr> back to normal Parameters Description: Unit <unit-id>: The unit ID. fan-descr: The fan ID and position.	Critical
2	Event Description: This log is recorded when a fan failed. Log Message: Unit <unit-id> <fan-descr> failed Parameters Description: Unit <unit-id>: The unit ID. fan-descr: The fan ID and position.	Critical
3	Event Description: This log is recorded when the temperature sensor enters the alarm state. Log Message: Unit <unit-id> <thermal-sensor-descr> detects abnormal temperature <degree> Parameters Description: Unit <unit-id>: The unit ID. thermal-sensor-descr: The sensor ID and position. degree: The current temperature.	Critical
4	Event Description: This log is recorded when the temperature recovers to normal. Log Message: Unit <unit-id> <thermal-sensor-descr> temperature back to normal Parameters Description: Unit <unit-id>: The unit ID. thermal-sensor-descr: The sensor ID and position.	Critical
5	Event Description: Power failed. Log Message: Unit <unit-id> <power-descr> failed Parameters Description: Unit <unit-id>: The unit ID. power-descr: Describe the power.	Critical
6	Event Description: Power is recovered. Log Message: Unit <unit-id> <power-descr> back to normal Parameters Description: Unit <unit-id>: The unit ID. power-descr: Describe the power.	Critical
7	Event Description: Manually change the fan control mode. Log Message: Unit <unit-id> Fan control mode changed from <mode> to <mode> Parameters Description: Unit <unit-id>: The unit ID. <mode>: fan control mode.	Informational
8	Event Description: Fan control mode returns to normal. Log Message: Unit <unit-id> Fan control mode returns to normal mode Parameters Description: Unit <unit-id>: The unit ID.	Warning

PoE

Log	Description	Severity
1	Event Description: Total power usage threshold is exceeded. Log Message: Unit <unit-id> usage threshold <percentage> is exceeded Parameters Description: unit-id: The box ID. percentage: The usage threshold.	Warning
2	Event Description: Total power usage threshold is recovered.	Warning

Log	Description	Severity
	Log Message: Unit <unit-id> usage threshold <percentage> is recovered Parameters Description: unit-id: The box ID. percentage: The usage threshold.	
3	Event Description: PD doesn’t reply to the ping request. Log Message: PD alive check failed. (Port: <portNum>, PD: <ipaddr>) Parameters Description: portNum: The port number. ipaddr: The IP (IPv4/IPv6) address of PD.	Warning

Port Security

Log	Description	Severity
1	Event Description: This log is generated when a MAC address triggers a port security violation. Log Message: MAC address <macaddr> causes port security violation on <interface-id> Parameters Description: macaddr: The MAC address that caused the violation. interface-id: The interface identifier.	Warning
2	Event Description: This log is generated when the system's address table becomes full. Log Message: Limit on system entry number has been exceeded	Warning

Reboot Schedule

Log	Description	Severity
1	Event Description: This event is about scheduling a switch reboot within a specified time. Log Message: Display “Reboot scheduled in 5 minutes” when the countdown equals 5 minutes	Warning
2	Event Description: This event is about scheduling a switch reboot within a specified time. Log Message: Display ”Reboot scheduled in 1 minute” when the countdown equals 1 minute	Critical
3	Event Description: This event occurs after a scheduled reboot in a specific interval. Log Message: System was restarted by schedule in an interval time	Informational
4	Event Description: This event occurs after a scheduled reboot at a specific time. Log Message: System was restarted by schedule at specific time	Informational
5	Event Description: This event occurs after a periodic scheduled reboot at a specific time. Log Message: System was restarted by periodic schedule at specific time	Informational
6	Event Description: This event occurs after a scheduled reboot with "save_before_reboot" configured. Log Message: Configuration was saved by schedule	Informational

Safeguard

Log	Description	Severity
1	Event Description: This log is generated when the host transitions into the exhausted mode. Log Message: Safeguard Engine enters EXHAUSTED mode	Warning
2	Event Description: This log is generated when the host transitions into the normal mode. Log Message: Safeguard Engine enters NORMAL mode	Informational

SIM

Log	Description	Severity
1	Event Description: Download Firmware OK. Log Message: Firmware upgraded by <session-name> successfully (Username: <username>) Parameters Description: session-name: The name of the session during the firmware upgrade. username: The user who initiated the firmware upgrade (GMUSER).	Informational
2	Event Description: Download Firmware fail. Log Message: Firmware upgrade by <session-name> was unsuccessful! (Username: <username>) Parameters Description: session-name: The name of the session during the firmware upgrade. username: The user who attempted the firmware upgrade (GMUSER).	Warning
3	Event Description: Download Slave Firmware OK. Log Message: Firmware upgraded to SLAVE successfully (Username: <username>) Parameters Description: username: The user who initiated the slave firmware upgrade (GMUSER).	Informational
4	Event Description: Download Slave Firmware fail. Log Message: Firmware upgraded to SLAVE unsuccessfully! (Username: <username>) Parameters Description: username: The user who attempted the slave firmware upgrade (GMUSER).	Warning
5	Event Description: Download Configuration OK. Log Message: Configuration successfully downloaded by <session-name> (Username: <username>) Parameters Description: session-name: The name of the session during the configuration download. username: The user who initiated the configuration download (GMUSER).	Informational
6	Event Description: Download Configuration fail. Log Message: Configuration download by <session-name> was unsuccessful! (Username: <username>) Parameters Description: session-name: The name of the session during the configuration download. username: The user who attempted the configuration download (GMUSER).	Warning
7	Event Description: Upload Configuration OK. Log Message: Configuration successfully uploaded by <session-name> (Username: <username>) Parameters Description: session-name: The name of the session during the configuration upload. username: The user who initiated the configuration upload (GMUSER).	Informational
8	Event Description: Upload Configuration fail. Log Message: Configuration upload by <session-name> was unsuccessful! (Username: <username>) Parameters Description: session-name: The name of the session during the configuration upload. username: The user who attempted the configuration upload (GMUSER).	Warning
9	Event Description: Upload Log OK. Log Message: Log message successfully uploaded by <session-name> (Username: <username>) Parameters Description: session-name: The name of the session during the log upload. username: The user who initiated the log upload (GMUSER).	Informational
10	Event Description: Upload Log fail. Log Message: Log message upload by <session-name> was unsuccessful! (Username: <username>) Parameters Description: session-name: The name of the session during the log upload. username: The user who attempted the log upload (GMUSER).	Warning

SNMP

Log	Description	Severity
1	Event Description: This log is generated when an SNMP request is received with an incorrect community string. Log Message: SNMP request received from <ipaddr> with invalid community string Parameters Description: ipaddr: The IP address.	Informational

SSH

Log	Description	Severity
1	Event Description: This log is created when the SSH server is enabled. Log Message: SSH server is enabled	Informational
2	Event Description: This log is generated when the SSH server is disabled. Log Message: SSH server is disabled	Informational

Stacking

Log	Description	Severity
1	Event Description: Hot insertion. Log Message: Unit: <unitID>, MAC: <macaddr> Hot insertion Parameters Description: unitID: Box ID. macaddr: MAC address.	Informational
2	Event Description: Hot removal. Log Message: Unit: <unitID>, MAC: <macaddr> Hot removal Parameters Description: unitID: Box ID. macaddr: MAC address.	Informational
3	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 can be one of the following: Ring Chain unitID: Box ID. macaddr: MAC address.	Critical
4	Event Description: Backup master changed to master. Log Message: Backup master changed to master. Master (Unit: <unitID>) Parameters Description: unitID: Box ID.	Informational
5	Event Description: Slave changed to master. Log Message: Slave changed to master. Master (Unit: <unitID>) Parameters Description: unitID: Box ID.	Informational
6	Event Description: Box ID conflict. Log Message: Hot insert failed, box ID conflict: Unit <unitID> conflict (MAC: <macaddr> and MAC: <macaddr>) Parameters Description: unitID: Box ID. macaddr: The MAC addresses of the conflicting boxes.	Critical

Log	Description	Severity
7	Event Description: Stacking port link up. Log Message: Stacking port <port> link up Parameters Description: port: SIO port ID.	Critical
8	Event Description: Stacking port link down. Log Message: Stacking port <port> link down Parameters Description: port: SIO port ID.	Critical
9	Event Description: SIO link up. Log Message: SIO interface Unit <unitID> <SIOn > link up Parameters Description: unitID: Box ID. SIOn: The SIO interface number. The currently supported SIO interface numbers should be SIO1 and SIO2.	Critical
10	Event Description: SIO link down. Log Message: SIO interface Unit <unitID> <SIOn > link down Parameters Description: unitID: Box ID. macaddr: The MAC addresses of the conflicting boxes.	Critical

Storm Control

Log	Description	Severity
1	Event Description: This log is generated when a storm is detected. Log Message: <Broadcast | Multicast | Unicast> storm is occurring on <interface-id> Parameters Description: Broadcast: A broadcast storm is detected. Broadcast packets (DA = FF:FF:FF:FF:FF:FF). Multicast: A multicast storm is detected. Multicast packets may include unknown L2 multicast, known L2 multicast, unknown IP multicast, and known IP multicast. Unicast: A unicast storm is detected. Unicast packets may include both known and unknown unicast packets. interface-id: The identifier of the affected interface where the storm is detected.	Warning
2	Event Description: This log is generated when the storm is resolved. Log Message: <Broadcast | Multicast | Unicast> storm is cleared on <interface-id> Parameters Description: Broadcast: The broadcast storm is resolved. Multicast: The multicast storm is resolved. Unicast: The unicast storm is resolved. This includes both known and unknown unicast packets. interface-id: The identifier of the interface where the storm is resolved.	Informational
3	Event Description: This log is generated when a port is 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 that was error-disabled due to the storm. Broadcast: The interface is disabled due to a broadcast storm occurrence. Multicast: The interface is disabled due to a multicast storm occurrence. Unicast: The interface is disabled due to a unicast storm occurrence. This includes both known and unknown unicast packets.	Warning

System

Log	Description	Severity
1	Event Description: This log is generated when the system performs a warm start.	Critical

Log	Description	Severity
	Log Message: Unit <unit-id> System warm start Parameters Description: <unit-id>: The unit ID. Note: If the switch is in standalone mode, there will be no unitID information available for logging.	
2	Event Description: This log is generated when the system performs a cold start. Log Message: Unit <unit-id> System cold start Parameters Description: <unit-id>: The unit ID. Note: If the switch is in standalone mode, there will be no unitID information available for logging.	Critical
3	Event Description: This log is generated when the system starts up. Log Message: Unit <unit-id> System started up Parameters Description: <unit-id>: The unit ID. Note: If the switch is in standalone mode, there will be no unitID information available for logging.	Critical

Telnet

Log	Description	Severity
1	Event Description: This log is generated when a successful Telnet login occurs. Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username of the Telnet client. ipaddr: The IP address of the Telnet client.	Informational
2	Event Description: This log is generated when a Telnet login attempt fails. Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username of the Telnet client. ipaddr: The IP address of the Telnet client.	Warning
3	Event Description: This log is generated when a successful Telnet logout occurs. Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username of the Telnet client. ipaddr: The IP address of the Telnet client.	Informational
4	Event Description: This log is generated when a Telnet session times out. Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username of the Telnet client. ipaddr: The IP address of the Telnet client.	Informational

Voice VLAN

Log	Description	Severity
1	Event Description: This log is generated when a new voice device is detected on an interface. Log Message: New voice device detected (<interface-id>, MAC: <mac-address>) Parameters Description: interface-id: The interface name. mac-address: The MAC address of the voice device.	Informational
2	Event Description: This log is generated when an interface, in auto-voice VLAN mode, joins the voice VLAN. Log Message: <interface-id> add into voice VLAN <vid> Parameters Description:	Informational

Log	Description	Severity
	interface-id: The interface name. vid: The VLAN ID.	
3	Event Description: This log is generated when an interface leaves the voice VLAN, and no voice device is detected during the aging interval for that interface. Log Message: <interface-id> remove from voice VLAN <vid> Parameters Description: interface-id: The interface name. vid: The VLAN ID.	Informational

VRRP Debug

Log	Description	Severity
1	Event Description: This log is generated when one virtual router state becomes Master. Log Message: VR <vr-id> at interface <intf-name> switch to Master role Parameters Description: vr-id: VRRP virtual router ID. intf-name: Interface name on which the virtual router is based.	Informational
2	Event Description: This log is generated when one virtual router state becomes Backup. Log Message: VR <vr-id> at interface <intf-name> switch to Backup state Parameters Description: vr-id: VRRP virtual router ID. intf-name: Interface name on which the virtual router is based.	Informational
3	Event Description: This log is generated when one virtual router state becomes Init. Log Message: VR <vr-id> at interface <intf-name> switch to Init state Parameters Description: vr-id: VRRP virtual router ID. intf-name: Interface name on which the virtual router is based.	Informational
4	Event Description: This log is generated when there is an authentication type mismatch in a received VRRP advertisement message. Log Message: Authentication type mismatch on VR <vr-id> at interface <intf-name> Parameters Description: vr-id: VRRP virtual router ID. intf-name: Interface name on which the virtual router is based.	Warning
5	Event Description: This log is generated when authentication checking fails for a received VRRP advertisement message. Log Message: Authentication fail on VR <vr-id> at interface <intf-name>. Auth type <auth-type> Parameters Description: vr-id: VRRP virtual router ID. intf-name: Interface name on which the virtual router is based. auth-type: VRRP interface authentication type.	Warning
6	Event Description: This log is generated when there is a checksum error in a received VRRP advertisement message. Log Message: Received an ADV msg with incorrect checksum on VR <vr-id> at interface <intf-name> Parameters Description: vr-id: VRRP virtual router ID. intf-name: Interface name on which the virtual router is based.	Warning
7	Event Description: This log is generated when there is a Virtual Router ID mismatch in a received VRRP advertisement message. Log Message: Received ADV msg virtual router ID mismatch. VR <vr-id> at interface <intf-name> Parameters Description: vr-id: VRRP virtual router ID. intf-name: Interface name on which the virtual router is based.	Warning

Log	Description	Severity
8	Event Description: This log is generated when there is an advertisement interval mismatch in a received VRRP advertisement message. Log Message: Received ADV msg adv interval mismatch. VR <vr-id> at interface <intf-name> Parameters Description: vr-id: VRRP virtual router ID. intf-name: Interface name on which the virtual router is based.	Warning
9	Event Description: A virtual MAC address is added to the switch's L2 table. Log Message: Added a virtual MAC <vrrp-mac-addr> into L2 table Parameters Description: vrrp-mac-addr: VRRP virtual MAC address.	Notice
10	Event Description: A virtual MAC address is deleted from the switch's L2 table. Log Message: Deleted a virtual MAC <vrrp-mac-addr> from L2 table Parameters Description: vrrp-mac-addr: VRRP virtual MAC address.	Notice
11	Event Description: A virtual MAC address is added to the switch's L3 table. Log Message: Added a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table Parameters Description: vrrp-ip-addr: VRRP virtual IP address. vrrp-mac-addr: VRRP virtual MAC address.	Notice
12	Event Description: A virtual MAC address is deleted from the switch's L3 table. Log Message: Deleted a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from L3 table Parameters Description: vrrp-ip-addr: VRRP virtual IP address. vrrp-mac-addr: VRRP virtual MAC address.	Notice
13	Event Description: Failed to add a virtual MAC address to the switch's L2 table. The L2 table is full. Log Message: Failed to add virtual MAC <vrrp-mac-addr> into chip L2 table. Errcode <vrrp-errcode> Parameters Description: vrrp-mac-addr: VRRP virtual MAC address. vrrp-errcode: Errcode of VRRP protocol behavior.	Error
14	Event Description: Failed to delete a virtual MAC address from the switch's L2 table. The L2 table is full. Log Message: Failed to delete virtual MAC <vrrp-mac-addr> from chip L2 table. Errcode <vrrp-errcode> Parameters Description: vrrp-mac-addr: VRRP virtual MAC address. vrrp-errcode: Errcode of VRRP protocol behavior.	Error
15	Event Description: Failed to add a virtual MAC address to the switch's L3 table. The L3 table is full. Log Message: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. L3 table is full Parameters Description: vrrp-ip-addr: VRRP virtual IP address. vrrp-mac-addr: VRRP virtual MAC address.	Error
16	Event Description: Failed to add a virtual MAC address to the switch's L3 table. The port from which the MAC is learned is invalid. Log Message: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Port <mac-port> is invalid Parameters Description: vrrp-ip-addr: VRRP virtual IP address. vrrp-mac-addr: VRRP virtual MAC address. mac-port: Port number of VRRP virtual MAC.	Error
17	Event Description: Failed to add a virtual MAC address to the switch's L3 table. The interface from which the MAC is learned is invalid. Log Message: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Interface <mac-intf> is invalid Parameters Description: vrrp-ip-addr: VRRP virtual IP address. vrrp-mac-addr: VRRP virtual MAC address.	Error

Log	Description	Severity
	mac-intf: Interface ID on which VRRP virtual MAC address is based.	
18	Event Description: Failed to add a virtual MAC address to the switch's L3 table. The box from which the MAC is learned is invalid. Log Message: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Box id <mac-box> is invalid Parameters Description: vrrp-ip-addr: VRRP virtual IP address. vrrp-mac-addr: VRRP virtual MAC address. mac-box: Stacking box number of VRRP virtual MAC.	Error
19	Event Description: Failed to add a virtual MAC address to the switch chip's L3 table. Log Message: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into chip L3 table. Errcode <vrrp-errcode> Parameters Description: vrrp-ip-addr: VRRP virtual IP address. vrrp-mac-addr: VRRP virtual MAC address. vrrp-errcode: Err code of VRRP protocol behavior.	Error
20	Event Description: Failed to delete a virtual MAC address from the switch chip's L3 table. Log Message: Failed to delete virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from chip L3 table. Errcode <vrrp-errcode> Parameters Description: vrrp-ip-addr: VRRP virtual IP address. vrrp-mac-addr: VRRP virtual MAC address. vrrp-errcode: Err code of VRRP protocol behavior.	Error

WAC

Log	Description	Severity
1	Event Description: Client Host Authentication Failure. Log Message: Web-Authentication host login fail(Username: <string>, IP: <ipaddr | ipv6address>, MAC: <macaddr>, Port: <portNum>, VID: <vlanid>) Parameters Description: string: The username of the client attempting to log in. ipaddr: The IPv4 address of the client. ipv6address: The IPv6 address of the client. macaddr: The MAC address of the client's device. portNum: The network port number the client is connected to. vlanid: The VLAN ID associated with the client's connection.	Critical
2	Event Description: Maximum Authorized Users Reached. Log Message: Web-Authentication enters stop learning state	Warning
3	Event Description: Authorized Users Below Maximum Limit Log Message: Web-Authentication recovered from stop learning state	Warning
4	Event Description: Client Host Authentication Success. Log Message: Web-Authentication host login success(Username: <string>, IP: <ipaddr | ipv6address>, MAC: <macaddr>, Port: <portNum>, VID: <vlanid>) Parameters Description: string: The username of the client who successfully logged in. ipaddr: The IPv4 address of the client. ipv6address: The IPv6 address of the client. macaddr: The MAC address of the client's device. portNum: The network port number the client is connected to. vlanid: The VLAN ID associated with the client's connection.	Informational
5	Event Description: ACL Hardware Resource Exhaustion. Log Message: Web-Authentication cannot work correctly because ACL rule resource is not available	Alert

Web

Log	Description	Severity
1	Event Description: Successful Web Login. Log Message: Successful login through Web (Username: <username>, IP: <ipaddr>) Parameters Description: username: The user who successfully logged in. ipaddr: The IP address from which the login was made.	Informational
2	Event Description: Failed Web Login. Log Message: Login failed through Web (Username: <username>, IP: <ipaddr>) Parameters Description: username: The user who attempted to log in. ipaddr: The IP address from which the login attempt was made.	Warning
3	Event Description: Web Session Timeout. Log Message: Web session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: The user whose session timed out. ipaddr: The IP address from which the session was initiated.	Informational
4	Event Description: Successful Web Logout. Log Message: Logout through Web (Username: <username>, IP: <ipaddr>) Parameters Description: username: The user who logged out. ipaddr: The IP address from which the logout was made.	Informational
5	Event Description: Successful Web (SSL) Login. Log Message: Successful login through Web(SSL) (Username: <username>, IP: <ipaddr>) Parameters Description: username: The user who successfully logged in using SSL. ipaddr: The IP address from which the SSL login was made.	Informational
6	Event Description: Failed Web (SSL) Login. Log Message: Login failed through Web(SSL) (Username: <username>, IP: <ipaddr>) Parameters Description: username: The user who attempted to log in using SSL. ipaddr: The IP address from which the SSL login attempt was made.	Warning
7	Event Description: Web (SSL) Session Timeout. Log Message: Web(SSL) session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: The user whose SSL session timed out. ipaddr: The IP address from which the SSL session was initiated.	Informational
8	Event Description: Successful Web (SSL) Logout. Log Message: Logout through Web(SSL) (Username: <username>, IP: <ipaddr>) Parameters Description: username: The user whose SSL session timed out. ipaddr: The IP address from which the SSL session was initiated.	Informational

ZTP

Log	Description	Severity
1	Event Description: This log is generated when the reset button on the unit is pressed, triggering the function. Log Message: Unit <UnitID> reset button pressed, trigger <Name> function. Parameters Description: UnitID: The unit ID.	Critical

Log	Description	Severity
	Name: Reboot, ZTP, Factory Reset.	
2	Event Description: This log is generated when the ZTP firmware is upgraded successfully. Log Message: The downloaded firmware was successfully executed by ZTP update (TFTP Server IP: <ipaddr>) Parameters Description: ipaddr: The IP address of the TFTP server.	Informational
3	Event Description: This log is generated when the ZTP firmware upgrade fails. Log Message: The downloaded firmware was not successfully executed by ZTP update (TFTP Server IP: <ipaddr>) Parameters Description: ipaddr: The IP address of the TFTP server.	Warning

Appendix C - Trap Entries

The Trap Log entries are listed in this appendix.

802.1X

Trap Name		Description	OID
1	dDot1xExtLoggedSuccess	This trap is sent when a host successfully passes IEEE 802.1X authentication (login successful). Binding Objects: • ifIndex • dnaSessionClientMacAddress • dnaSessionAuthVlan • dnaSessionAuthUserName	1.3.6.1.4.1.171.14.30.0.1
2	dDot1xExtLoggedFail	This trap is sent when a host fails to pass IEEE 802.1X authentication (login failed). Binding Objects: • ifIndex • dnaSessionClientMacAddress • dnaSessionAuthVlan • dnaSessionAuthUserName • dDot1xExtNotifyFailReason	1.3.6.1.4.1.171.14.30.0.2

802.3ah OAM

Trap Name		Description	OID
1	dot3OamThresholdEvent	This trap is sent when a local or remote threshold crossing event is detected. Binding Objects: • dot3OamEventLogTimestamp • dot3OamEventLogOui • dot3OamEventLogType • dot3OamEventLogLocation • dot3OamEventLogWindowHi • dot3OamEventLogWindowLo • dot3OamEventLogThresholdHi • dot3OamEventLogThresholdLo • dot3OamEventLogValue • dot3OamEventLogRunningTotal • dot3OamEventLogEventTotal	1.3.6.1.2.1.158.0.1
2	dot3OamNonThresholdEvent	This trap is sent when a local or remote non-threshold crossing event is detected. Binding Objects: • dot3OamEventLogTimestamp • dot3OamEventLogOui • dot3OamEventLogType • dot3OamEventLogLocation • dot3OamEventLogEventTotal	1.3.6.1.2.1.158.0.2

Authentication Fail

Trap Name		Description	OID
1	authenticationFailure	This trap is sent to signify that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of 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
1	dBpduProtectionAttackOccur	This trap is sent when a BPDU attack occurs on an interface. Binding Objects: • ifIndex • dBpduProtectionIfCfgMode	1.3.6.1.4.1.171.14.47.0.1
2	dBpduProtectionAttackRecover	This trap is sent when a BPDU attack is resolved on an interface. Binding Objects: • ifIndex	1.3.6.1.4.1.171.14.47.0.2

CFM

Trap Name		Description	OID
1	dot1agCfmFaultAlarm	This trap is sent when a connectivity defect is detected. Binding Objects: • dot1agCfmMepHighestPrDefect	1.3.111.2.802.1.1.8.0.1
2	dCfmAisOccurred	This trap is sent when the local MEP enters AIS status. Binding Objects: • dCfmEventMdIndex • dCfmEventMaIndex • dCfmEventMepIdentifier	1.3.6.1.4.1.171.14.86.0.1
3	dCfmAisCleared	This trap is sent when the local MEP exits AIS status. Binding Objects: • dCfmEventMdIndex • dCfmEventMaIndex • dCfmEventMepIdentifier	1.3.6.1.4.1.171.14.86.0.2
4	dCfmLockOccurred	This trap is sent when the local MEP enters lock status. Binding Objects: • dCfmEventMdIndex • dCfmEventMaIndex • dCfmEventMepIdentifier	1.3.6.1.4.1.171.14.86.0.3
5	dCfmLockCleared	This trap is sent when the local MEP exits lock status. Binding Objects: • dCfmEventMdIndex • dCfmEventMaIndex • dCfmEventMepIdentifier	1.3.6.1.4.1.171.14.86.0.4

DDM

Trap Name		Description	OID
1	dDdmAlarmTrap	This trap is sent when an abnormal alarm situation occurs or recovers from an abnormal alarm situation to normal status. Only when the current value is greater than the low warning or less than the high warning, a recover trap will be sent. Binding Objects: • dDdmNotifyInfoIfIndex • dDdmNotifyInfoComponent • dDdmNotifyInfoAbnormalLevel • dDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.171.14.72.0.1
2	dDdmWarningTrap	This trap is sent when an abnormal warning situation occurs or recovers from an abnormal warning situation to normal status. Binding Objects: • dDdmNotifyInfoIfIndex • dDdmNotifyInfoComponent • dDdmNotifyInfoAbnormalLevel • dDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.171.14.72.0.2

DHCP Server Screen Prevention

Trap Name		Description	OID
1	dDhcpFilterAttackDetected	This trap is sent when the DHCP server screen is enabled, and the switch receives a forged DHCP Server packet. Binding Objects: • dDhcpFilterLogBufServerIpAddr • dDhcpFilterLogBufClientMacAddr • dDhcpFilterLogBufferVlanId • dDhcpFilterLogBufferOccurTime	1.3.6.1.4.1.171.14.133.0.1

DoS Attack Prevention

Trap Name		Description	OID
1	dDosPreveAttackDetectedPacket2	This trap is sent when a DoS attack is detected. Binding Objects: • dDoSPrevCtrlAttackType • dDosPrevNotiInfoDropPortNumber	1.3.6.1.4.1.171.14.59.0.4

ERPS

Trap Name		Description	OID
1	dErpsFailuredetectedNotif	This trap is sent when a signal failure is detected.	1.3.6.1.4.1.171.14.78.0.1
2	dErpsFailureClearedNotif	This trap is sent when a signal failure is cleared.	1.3.6.1.4.1.171.14.78.0.2
3	dErpsRPLOwnerConflictNotif	This trap is sent when an RPL owner conflict is detected.	1.3.6.1.4.1.171.14.78.0.3

ErrDisable

Trap Name		Description	OID
1	dErrDisNotifyPortDisabledAssert	This trap is sent when a port enters the error-disabled state. Binding Objects: • dErrDisNotifyInfoPortIfIndex • dErrDisNotifyInfoLoopDetectedVID • dErrDisNotifyInfoReasonID	1.3.6.1.4.1.171.14.45.0.1
2	dErrDisNotifyPortDisabledClear	This trap is sent when a port-loop restarts after the interval time. Binding Objects: • dErrDisNotifyInfoPortIfIndex • dErrDisNotifyInfoLoopDetectedVID • dErrDisNotifyInfoReasonID	1.3.6.1.4.1.171.14.45.0.2

General Management

Trap Name		Description	OID
1	dGenMgmtLoginFail	This trap is sent when a user login to the switch fails. Binding Objects: • dGenMgmtNotifyInfoLoginType • dGenMgmtNotifyInfoUserName	1.3.6.1.4.1.171.14.165.0.1

Gratuitous ARP

Trap Name		Description	OID
1	agentGratuitousARPTrap	This trap is sent when an IP address conflict occurs. Binding Objects: • ipaddr • macaddr • portNumber • agentGratuitousARPInterfaceName	1.3.6.1.4.1.171.14.75.0.1

IMPB

Trap Name		Description	OID
1	dImpbViolationTrap	This trap is sent when the switch detects an IPMB address violation. Binding Objects: • ifIndex • dImpbViolationIpAddrType • dImpbViolationIpAddress • dImpbViolationMacAddress • dImpbViolationVlan	1.3.6.1.4.1.171.14.22.0.1

LACP

Trap Name		Description	OID
1	linkup	This trap is sent when the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links has transitioned from the down state to	1.3.6.1.6.3.1.1.5.4

Trap Name		Description	OID
		another state (not the notPresent state). The new state is indicated in ifOperStatus. Binding Objects: • ifIndex • ifAdminStatus • ifOperStatus	
2	linkDown	This trap is sent when the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to transition from another state (not from the notPresent state) to the down state. The old state is indicated in ifOperStatus. Binding Objects: • ifIndex • ifAdminStatus • ifOperStatus	1.3.6.1.6.3.1.1.5.3

LBD

Trap Name		Description	OID
1	dLbdLoopOccurred	This trap is sent when an interface loop occurs. Binding Objects: • dLbdNotifyInfoIfIndex	1.3.6.1.4.1.171.14.46.0.1
2	dLbdLoopRestart	This trap is sent when an interface loop restarts after the interval time. Binding Objects: • dLbdNotifyInfoIfIndex	1.3.6.1.4.1.171.14.46.0.2
3	dLbdVlanLoopOccurred	This trap is sent when an interface with a VID loop occurs. Binding Objects: • dLbdNotifyInfoIfIndex • dLbdNotifyInfoVlanId	1.3.6.1.4.1.171.14.46.0.3
4	dLbdVlanLoopRestart	This trap is sent when an interface loop with a VID restarts after the interval time. Binding Objects: • dLbdNotifyInfoIfIndex • dLbdNotifyInfoVlanId	1.3.6.1.4.1.171.14.46.0.4

LLDP/LLDP-MED

Trap Name		Description	OID
1	lldpRemTablesChange	This trap is sent when the value in lldpStatsRemTableLastChangeTime changes. Binding Objects: • lldpStatsRemTablesInserts • lldpStatsRemTablesDeletes • lldpStatsRemTablesDrops • lldpStatsRemTablesAgeouts	1.0.8802.1.1.2.0.0.1
2	lldpXMedTopologyChangeDetected	This trap is sent when the local device senses a change in the topology that indicates a new remote device attached to a local port, or a remote device has been disconnected or moved from one port to another. Binding Objects: • lldpRemChassisIdSubtype • lldpRemChassisId	1.0.8802.1.1.2.1.5.4795.0.1

Trap Name		Description	OID
		• lldpXMedRemDeviceClass	

MAC-based Access Control

Trap Name		Description	OID
1	dMacAuthLoggedSuccess	This trap is sent when a MAC-based Access Control host successfully logs in. Binding Objects: • ifIndex • dnaSessionClientMacAddress • dnaSessionAuthVlan	1.3.6.1.4.1.171.14.153.0.1
2	dMacAuthLoggedFail	This trap is sent when a MAC-based Access Control host login fails. Binding Objects: • ifIndex • dnaSessionClientMacAddress • dnaSessionAuthVlan	1.3.6.1.4.1.171.14.153.0.2
3	dMacAuthLoggedAgesOut	This trap is sent when a MAC-based Access Control host ages out. Binding Objects: • ifIndex • dnaSessionClientMacAddress • dnaSessionAuthVlan	1.3.6.1.4.1.171.14.153.0.3

MAC Notification

Trap Name		Description	OID
1	swL2macNotification	This trap is sent to indicate a MAC address change in the MAC address table. Binding Objects: • swL2macNotifyInfo	1.3.6.1.4.1.171.14.3.0.1
2	dL2FdbMacNotificationWithVID	This trap is sent to indicate a MAC address change in the MAC address table. Binding Objects: • dL2FdbMacChangeNotifyInfoWithVID	1.3.6.1.4.1.171.14.3.0.2

MSTP

Trap Name		Description	OID
1	newRoot	This trap is sent to indicate that the sending agent has become the new root of the Spanning Tree. This trap is sent by a bridge after its election as the new root, for example, upon the expiration of the Topology Change Timer or immediately subsequent to its election. Implementation of this trap is optional.	1.3.6.1.2.1.17.0.1
2	topologyChange	This trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state or from the Forwarding state to the Blocking state. This 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
1	dEntityExtFanStatusChg	This trap is sent from the commander switch when a fan fails (dEntityExtEnvFanStatus is 'fault') or recovers (dEntityExtEnvFanStatus is 'ok'). Binding Objects: • dEntityExtEnvFanUnitId • dEntityExtEnvFanIndex • dEntityExtEnvFanStatus	1.3.6.1.4.1.171.14.5.0.1
2	dEntityExtThermalStatusChg	This trap is sent from the commander switch when a thermal alarms (dEntityExtEnvTempStatus is 'abnormal') or recovers (dEntityExtEnvTempStatus is 'ok'). Binding Objects: • dEntityExtEnvTempUnitId • dEntityExtEnvTempIndex • dEntityExtEnvTempStatus	1.3.6.1.4.1.171.14.5.0.2
3	dEntityExtPowerStatusChg	This trap is sent when the commander switch sends a notification indicating a power module failure, recovery, or removal. Binding Objects: • dEntityExtEnvPowerUnitId • dEntityExtEnvPowerIndex • dEntityExtEnvPowerStatus	1.3.6.1.4.1.171.14.5.0.3

PIM6-SM

Trap Name		Description	OID
1	pimNeighborLoss	A pimNeighborLoss notification signifies the loss of an adjacency with a neighbor. This notification should be generated when the neighbor timer expires, and the router has no other neighbor on the same interface with the same IP version and a lower IP address than itself. This notification is generated whenever the counter pimNeighborLossCount is incremented, subject to the rate limit specified by pimNeighborLossNotificationsPeriod. Binding Objects: • pimNeighborUpTime	1.3.6.1.2.1.157.0.1
2	pimInvalidRegister	A pimInvalidRegister notification signifies that an invalid PIM Register message was received by this device. This notification is generated whenever the counter pimInvalidRegisterMsgsRcvd is incremented, subject to the rate limit specified by pimInvalidRegisterNotificationPeriod. Binding Objects: • pimGroupMappingPimMode • pimInvalidRegisterAddressType • pimInvalidRegisterOrigin • pimInvalidRegisterGroup • pimInvalidRegisterRp	1.3.6.1.2.1.157.0.2
3	pimInvalidJoinPrune	A pimInvalidJoinPrune notification signifies that an invalid PIM Join/Prune message was received by this device. This notification is generated whenever the counter pimInvalidJoinPruneMsgsRcvd is incremented, subject to the rate limit specified by pimInvalidJoinPruneNotificationPeriod. Binding Objects: • pimGroupMappingPimMode • pimInvalidJoinPruneAddressType • pimInvalidJoinPruneOrigin	1.3.6.1.2.1.157.0.3

Trap Name		Description	OID
		• pimInvalidJoinPruneGroup • pimInvalidJoinPruneRp • pimNeighborUpTime	
4	pimRPMappingChage	A pimRPMappingChange notification signifies a change to the active RP mapping on this device. This notification is generated whenever the counter pimRPMappingChangeCount is incremented, subject to the rate limit specified by pimRPMappingChangeNotificationPeriod. Binding Objects: • pimGroupMappingPimMode • pimGroupMappingPrecedence	1.3.6.1.2.1.157.0.4
5	pimInterfaceElection	A pimInterfaceElection notification signifies that a new DR or DF has been elected on a network. This notification is generated whenever the counter pimInterfaceElectionWinCount is incremented, subject to the rate limit specified by pimInterfaceElectionNotificationPeriod. Binding Objects: • pimInterfaceAddressType • pimInterfaceAddress	1.3.6.1.2.1.157.0.5

PoE

Trap Name		Description	OID
1	pethMainPowerUsageOnNotification	This trap indicates that the PSE Threshold usage indication is on, and the power usage is above the threshold. There must be at least 500 msec between notifications emitted by the same object instance. Binding Objects: • pethMainPseConsumptionPower	1.3.6.1.2.1.105.0.2
2	pethMainPowerUsageOffNotification	This trap indicates that the PSE Threshold usage indication is off, and the power usage is below the threshold. There must be at least 500 msec between notifications emitted by the same object instance. Binding Objects: • pethMainPseConsumptionPower	1.3.6.1.2.1.105.0.3
3	dPoeIfPowerDeniedNotification	This notification indicates if the PSE state diagram enters the state *POWER_DENIED*. There must be at least 500 msec between notifications emitted by the same object instance. Binding Objects: • pethPsePortPowerDeniedCounter	1.3.6.1.4.1.171.14.24.0.1
4	dPoeIfPowerOverLoadNotification	This trap indicates if the PSE state diagram enters the state *ERROR_DELAY_OVER*. There must be at least 500 msec between notifications emitted by the same object instance. Binding Objects: • pethPsePortOverLoadCounter	1.3.6.1.4.1.171.14.24.0.2
5	dPoeIfPowerShortCircuitNotification	This trap indicates if the PSE state diagram enters the state *ERROR_DELAY_SHORT*. There must be at least 500 msec between notifications emitted by the same object instance. Binding Objects: • pethPsePortShortCounter	1.3.6.1.4.1.171.14.24.0.3
6	dPoeIfPdAliveFailOccurNotification	This trap indicates if the PD device has stopped working or is unresponsive. There must be at least 500 msec between notifications emitted by the same object instance.	1.3.6.1.4.1.171.14.24.0.4

Port

Trap Name		Description	OID
1	linkup	This trap is sent when the port link status changes to up. Binding Objects: • ifIndex • ifAdminStatus • ifOperStatus	1.3.6.1.6.3.1.1.5.4
2	linkDown	This trap is sent when the port link status changes to down. Binding Objects: • ifIndex • ifAdminStatus • ifOperStatus	1.3.6.1.6.3.1.1.5.3

Port Security

Trap Name		Description	OID
1	dPortSecMacAddrViolation	This trap is sent when new MAC addresses violate the pre-defined port security configuration. Binding Objects: • ifIndex • dPortSecIfCurrentStatus • dPortSecIfLastMacAddress	1.3.6.1.4.1.171.14.8.0.1

Reboot Schedule

Trap Name		Description	OID
1	dPortSecMacAddrViolation	This trap is sent when new MAC addresses violate the predefined port security configuration. Binding Objects: • ifIndex • dPortSecIfCurrentStatus • dPortSecIfLastMacAddress	1.3.6.1.4.1.171.14.8.0.1

RMON

Trap Name		Description	OID
1	risingAlarm	This trap is sent when an alarm entry crosses its rising threshold and generates an event configured for sending SNMP traps. Binding Objects: • alarmIndex • alarmVariable • alarmSampleType • alarmValue • alarmRisingThreshold	1.3.6.1.2.1.16.0.1
2	fallingAlarm	This trap is sent when an alarm entry crosses its falling threshold and generates an event configured for sending SNMP traps. Binding Objects: • alarmIndex • alarmVariable	1.3.6.1.2.1.16.0.2

Trap Name		Description	OID
		• alarmSampleType • alarmValue • alarmFallingThreshold	

Safeguard

Trap Name		Description	OID
1	dSafeguardChgToExhausted	This trap is sent to indicate a change in the system operation mode from normal to exhaust. Binding Objects: • dSafeguardEngineCurrentMode	1.3.6.1.4.1.171.14.19.1.1.0.1
2	dSafeguardChgToNormal	This trap is sent to indicate a change in the system operation mode from exhausted to normal. Binding Objects: • dSafeguardEngineCurrentMode	1.3.6.1.4.1.171.14.19.1.1.0.2

SIM

Trap Name		Description	OID
1	swSingleIPMSColdStart	This trap is sent when the commander switch's member generates a cold start notification. Binding Objects: • swSingleIPMSID • swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.11
2	swSingleIPMSWarmStart	This trap is sent when the commander switch sends a notification because its member generates a warm start notification. Binding Objects: • swSingleIPMSID • swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.12
3	swSingleIPMSLinkDown	This trap is sent when the commander switch sends a notification because its member generates a link down notification. Binding Objects: • swSingleIPMSID • swSingleIPMSMacAddr • ifIndex	1.3.6.1.4.1.171.12.8.6.0.13
4	swSingleIPMSLinkUp	This trap is sent when the commander switch sends a notification because its member generates a link up notification. Binding Objects: • swSingleIPMSID • swSingleIPMSMacAddr • ifIndex	1.3.6.1.4.1.171.12.8.6.0.14
5	swSingleIPMSAuthFail	This trap is sent when the commander switch sends a notification because its member generates an authentication failure notification. Binding Objects: • swSingleIPMSID • swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.15
6	swSingleIPMSnewRoot	This trap is sent when the commander switch sends a notification because its member generates a new root notification.	1.3.6.1.4.1.171.12.8.6.0.16

Trap Name		Description	OID
		Binding Objects: • swSingleIPMSID • swSingleIPMSMacAddr	
7	swSingleIPMSTopologyChange	This trap is sent when the commander switch sends a notification because its member generates a topology change notification. Binding Objects: • swSingleIPMSID • swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.17

Stack

Trap Name		Description	OID
1	dStackInsertNotification	This trap is sent for the Unit Hot Insert notification. Binding Objects: • dStackNotifyInfoBoxId • dStackInfoMacAddr	1.3.6.1.4.1.171.14.9.0.1
2	dStackRemoveNotification	This trap is sent for the Unit Hot Remove notification. Binding Objects: • dStackNotifyInfoBoxId • dStackInfoMacAddr	1.3.6.1.4.1.171.14.9.0.2
3	dStackFailureNotification	This trap is sent for the Unit Failure notification. Binding Objects: • dStackNotifyInfoBoxId	1.3.6.1.4.1.171.14.9.0.3
4	dStackTPChangeNotification	This trap is sent for the Stacking Topology Change notification. Binding Objects: • dStackNotifyInfoTopologyType • dStackNotifyInfoBoxId • dStackInfoMacAddr	1.3.6.1.4.1.171.14.9.0.4
5	dStackRoleChangeNotification	This trap is sent for the Stacking Unit Role Change notification. Binding Objects: • dStackNotifyInfoRoleChangeType • dStackNotifyInfoBoxId	1.3.6.1.4.1.171.14.9.0.5

Start

Trap Name		Description	OID
1	coldStart	This trap is sent to signify that the SNMPv2 entity, acting in an agent role, is reinitializing itself, and its configuration may have been altered.	1.3.6.1.6.3.1.1.5.1
2	warmStart	This trap is sent to signify that the SNMPv2 entity, acting in an agent role, is reinitializing itself in a way that its configuration remains unaltered.	1.3.6.1.6.3.1.1.5.2

Storm Control

Trap Name		Description	OID
1	dStormCtrlOccurred	This trap is sent when dStormCtrlNotifyEnable is set to stormOccurred or 'both,' and a storm is detected.	1.3.6.1.4.1.171.14.25.0.1

Trap Name		Description	OID
		Binding Objects: • ifIndex • dStormCtrlNotifyTrafficType	
2	dStormCtrlStormCleared	This trap is sent when dStormCtrlNotifyEnable is set to stormCleared or 'both,' and a storm is cleared. Binding Objects: • ifIndex • dStormCtrlNotifyTrafficType	1.3.6.1.4.1.171.14.25.0.2

System File

Trap Name		Description	OID
1	dsfUploadImage	This trap is sent when the user successfully uploads an image file.	1.3.6.1.4.1.171.14.14.0.1
2	dsfDownloadImage	This trap is sent when the user successfully downloads an image file.	1.3.6.1.4.1.171.14.14.0.2
3	dsfUploadCfg	This trap is sent when the user successfully uploads a configuration file.	1.3.6.1.4.1.171.14.14.0.3
4	dsfDownloadCfg	This trap is sent when the user successfully downloads a configuration file.	1.3.6.1.4.1.171.14.14.0.4
5	dsfSaveCfg	This trap is sent when the user successfully saves the configuration file.	1.3.6.1.4.1.171.14.14.0.5

VRRP

Trap Name		Description	OID
1	vrrpTrapNewMaster	This trap is sent when the newMaster trap indicates that the sending agent has transitioned to the 'Master' state. Binding Objects: • vrrpOperMasterIpAddr	1.3.6.1.2.1.68.0.1
2	vrrpTrapAuthFailure	This trap is sent when 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: • vrrpTrapPacketSrc • vrrpTrapAuthErrorType	1.3.6.1.2.1.68.0.2

Web Authentication

Trap Name		Description	OID
1	dWebAuthLoggedSuccess	The trap is sent when a host has successfully logged in (passed Web-Authentication). Binding Objects: • ifIndex • dnaSessionAuthVlan • dnaSessionClientMacAddress • dnaSessionClientAddrType • dnaSessionClientAddress • dnaSessionAuthUserName	1.3.6.1.4.1.171.14.154.0.1

Trap Name		Description	OID
2	dWebAuthLoggedFail	The trap is sent when a host has failed to pass Web-Authentication (login failed). Binding Objects: • ifIndex • dnaSessionAuthVlan • dnaSessionClientMacAddress • dnaSessionClientAddrType • dnaSessionClientAddress • dnaSessionAuthUserName	1.3.6.1.4.1.171.14.154.0.2

ZTP

Trap Name		Description	OID
1	swResetButtonPressedTrap	This trap is sent when the reset button is pressed. Binding Objects: • Unit ID • swResetButtonMode	1.3.6.1.4.1.171.12.120.2.0.1

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.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Type      |    Length     |     Tag       |   String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The table below shows the definition of Tag field (different with RFC 2868):

Tag Field Value	String Field Format
0x01	VLAN name (ASCII)
0x02	VLAN ID (ASCII)
Others (0x00, 0x03 ~ 0x1F, >0x1F)	When the Switch receives the VLAN setting string, it will think it is the VLAN ID first. In other words, the Switch will check all existing VLAN IDs and check if there is one matched. If the Switch can find one matched, it will move to that VLAN. If the Switch cannot find the matched VLAN ID, it will think the VLAN setting string as a "VLAN Name". Then it will check that it can find out a matched VLAN Name.

NOTE: A tag field of greater than 0x1F is interpreted as the first octet of the following field.

If the user has configured the VLAN attribute of the RADIUS server (for example, VID 3) and the 802.1X, or MAC based Access Control, 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, there are two types of parameters that can be configured on the RADIUS server. (1) VSA14 ACL and (2) NAS-Filter-Rule.

VSA14 ACL Script

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, MAC-based Access Control or WAC authentication 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.

NAS-Filter-Rule (92)

The parameters of the NAS-Filter-Rule are:

RADIUS Tunnel Attribute	Description	Value	Usage
NAS-Filter-Rule	This attribute indicates the filter rules to be applied for the user.	A string (concatenating the individual filter rules, separated by a null (0x00) octet)	Required

Filter Rule Format

Use the permit rule to add a permit entry. Use the deny rule to add a deny entry.

{permit | deny} in tcp from any to {any | *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR* **} [***TCP-PORT-RANGE***]**

{permit | deny} in udp from any to {any | *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR* **} [***UDP-PORT-RANGE***]**

{permit | deny} in icmp from any to {any | *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR* **} [***ICMP-TYPE***]**

{permit | deny} in ip from any to {any | *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR* **} {permit | deny} in** *IP-PROT-VALUE* **from any to {any |** *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR* **}**

Syntax Description

Parameter	Description
tcp, udp, icmp, ip, *IP-PROT-VALUE*	Filter rule can match TCP, UDP, ICMP, IP, or user-specified protocol value. The valid value of IP-PROT-VALUE is from 0 to 255.
any	Use the keyword **any** to match any destination addresses.
DST-IP-ADDR	Specifies a specific destination host IP address.
DST-IP-NET-ADDR	Specifies a group of destination IP addresses with a mask width in the form 1.2.3.4/24.
DST-IPV6-ADDR	Specifies a specific destination host IPv6 address.
DST-IPV6-NET-ADDR	Specifies a group of destination IPv6 networks in the form 2000::1/64.
TCP-PORT-RANGE	(Optional) Specifies to match the TCP port or port range. The format is like 22-23, 80.
UDP-PORT-RANGE	(Optional) Specifies to match the UDP port or port range. The format is like 56, 67-68.
ICMP-TYPE	(Optional) Specifies the ICMP message type. The valid number for the message type is from 0 to 255.

Examples

This example shows how to deny a host’s Telnet service on the RADIUS server.

```
Nas-filter-Rule="deny in tcp from any to any 23"
Nas-filter-Rule+="permit in ip from any to any"
```

This example shows how to limit a host to access a group of IP address on the RADIUS server.

```
Nas-filter-Rule="permit in ip from any to 10.10.10.1/24"
Nas-filter-Rule+="permit in ip from any to fe80::d1:1/64"
```

The parameters of the Vendor-Specific Attribute are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	24	Required
Attribute-Specific Field	IPv6 filter rule. Used to accept IPv6 address related inputs.	This attribute indicates one of the following IP modes for the NAS-Filter-Rule. 1=Forward IPv4 and IPv6 traffic	Required

Vendor-Specific Attribute	Description	Value	Usage
		2=Forward IPv4 traffic only (drop any IPv6 traffic) If this attribute is not assigned by the RADIUS server, forward IPv4 traffic only. IPv6 packets will be dropped.	

Note: If both proprietary ACL script (VSA14) and standard NAS-Filter-Rule (92) are assigned at the same time, the NAS-Filter-Rule (92) will take effect, and VSA14 will be ignored.

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
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