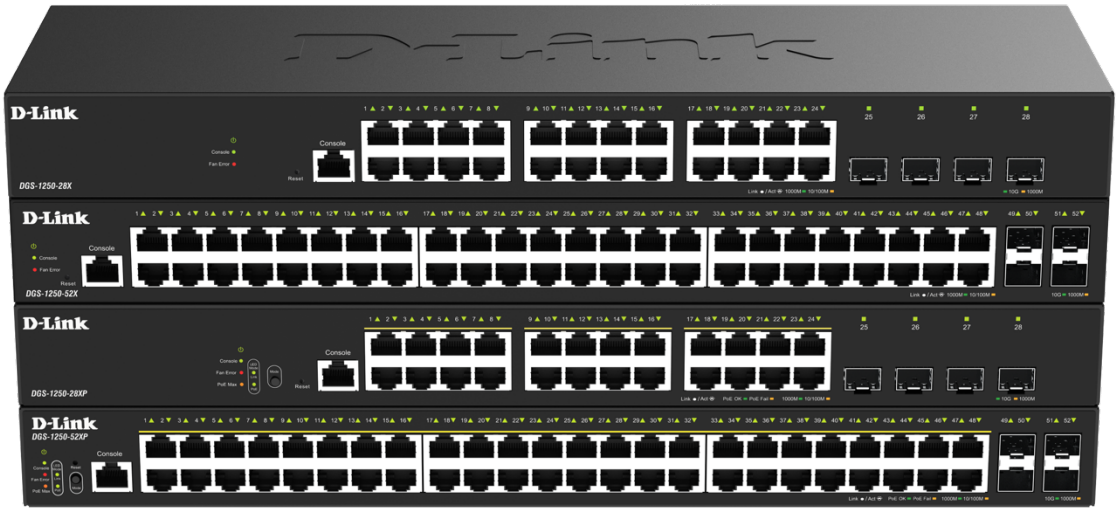
Version 1.01 | 05/28/2026



User Manual

L2 Gigabit Ethernet (PoE) Smart Managed Switch

DGS-1250 Series

Table of Contents

Table of Contents **1**
About This Guide **8**
Terms/Usage 8
Copyright and Trademarks 8
1 Product Introduction **9**
DGS-1250-28X 10
Front Panel 10
Rear Panel 10
DGS-1250-28XP 11
Front Panel 11
Rear Panel 12
DGS-1250-52X 13
Front Panel 13
Rear Panel 13
DGS-1250-52XP 14
Front Panel 14
Rear Panel 15
2 Hardware Installation **16**
Safety Cautions 16
Step 1: Unpacking 17
Step 2: Switch Installation 17
Desktop or Shelf Installation 17
Rack Installation 17
Step 3 – Plugging in the AC Power Cord 18
Power Failure 18
Grounding the Switch 18
3 Getting Started **20**
Management Options 20
Using Web-based Management 20
Supported Web Browsers 20
Connecting to the Switch 20
Login Web-based Management 20
Smart Wizard 21
Web-based Management 21
Web User Interface (Web UI) 21
Areas of the User Interface 21
Standard Mode 22
Surveillance Mode 23
4 Configuration **24**
Smart Wizard Configuration 24
Web Mode 24
IPv4 Information 25
SNMP Settings 25
User Accounts Settings 26
Web-based Management 27
Tool Bar > Save Menu 27
Save Configuration 27

Tool Bar > Tool Menu 28
Firmware Information 28
Configuration Information 28
Firmware Upgrade & Backup > Firmware Upgrade from HTTP 28
Firmware Upgrade & Backup > Firmware Upgrade from TFTP 29
Firmware Backup to HTTP & Backup > Firmware Backup to HTTP 29
Firmware Backup to HTTP & Backup > Firmware Backup to TFTP 29
Configuration Restore & Backup > Configuration Restore from HTTP 29
Configuration Restore & Backup > Configuration Restore from TFTP 29
Configuration Restore & Backup > Configuration Backup to HTTP 30
Configuration Restore & Backup > Configuration Backup to TFTP 30
Log Backup > Log Backup to HTTP 30
Log Backup > Log Backup to TFTP 30
Ping 30
Traceroute 31
Reset 31
Reboot System 31
Nuclias Connect Setting 32
Upload Nuclias Connect File 33
Tool Bar > Smart Wizard 33
Tool Bar > Online Help 34
Function Tree 35
Device Information 35
System > System Information 35
System > Peripheral 36
System > Port Configuration > Port Settings 36
System > Port Configuration > Port Status 37
System > Port Configuration > Port GBIC 37
System > Port Configuration > Error Disable Settings 38
System > Port Configuration > Jumbo Frame 39
System > PoE > PoE System 39
System > PoE > PoE Status 40
System > PoE > PoE Configuration 40
System > PoE > PoE Statistics 41
System > PoE > PoE Measurement 41
System > PoE > PD Alive 41
System > System Log > System Log Settings 42
System > System Log > System Log Server Settings 43
System > System Log > System Log 43
System > Time and SNTP > Clock Settings 43
System > Time and SNTP > Time Zone Settings 43
System > Time and SNTP > SNTP Settings 45
System > Time Range 45
Management > User Accounts Settings 45
Management > Password Encryption 46
Management > SNMP > SNMP Global Settings 47
Management > SNMP > SNMP View Table Settings 48
Management > SNMP > SNMP Community Table Settings 48
Management > SNMP > SNMP Group Table Settings 49

Management > SNMP > SNMP Engine ID Local Settings 49
Management > SNMP > SNMP User Table Settings 50
Management > SNMP > SNMP Host Table Settings 51
Management > RMON > RMON Global Settings 51
Management > RMON > RMON Statistics Settings 51
Management > RMON > RMON History Settings 52
Management > RMON > RMON Alarm Settings 52
Management > RMON > RMON Event Settings 53
Management > DHCP > Service DHCP 53
Management > DHCP > DHCP Class Settings 54
Management > DHCP > DHCP Relay > DHCP Relay Global Settings 55
Management > DHCP > DHCP Relay > DHCP Relay Pool Settings 55
Management > DHCP > DHCP Relay > DHCP Relay Information Settings 57
Management > DHCP > DHCP Relay > DHCP Relay Information Option Format Settings 58
Management > DHCP > DHCP Relay > DHCP Relay Port Settings 59
Management > DHCP > DHCP Relay > DHCP Local Relay VLAN Settings 60
Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Global Settings 60
Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Interface Settings 62
Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Format Type Settings 62
Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Port Settings 63
Management > DHCP > DHCPv6 Relay > DHCPv6 Local Relay VLAN Settings 63
Management > DHCP Auto Configuration 64
Management > DHCP Auto Image Settings 64
Management > Telnet/Web 65
Management > Session Timeout 65
Management > D-Link Discover Protocol Settings 65
L2 Features > FDB > Static FDB > Unicast Static FDB 66
L2 Features > FDB > Static FDB > Multicast Static FDB 66
L2 Features > FDB > MAC Address Table Settings 66
L2 Features > FDB > MAC Address Table 67
L2 Features > FDB > MAC Notification 68
L2 Features > VLAN Configuration Wizard 68
L2 Features > 802.1Q VLAN 71
L2 Features > Asymmetric VLAN 71
L2 Features > VLAN Interface 71
L2 Features > VLAN Tunnel > Dot1q Tunnel 72
L2 Features > VLAN Tunnel > VLAN Mapping 74
L2 Features > VLAN Tunnel > VLAN Mapping Profile 75
L2 Features > GVRP > GVRP Global 79
L2 Features > GVRP > GVRP Port 80
L2 Features > GVRP > GVRP Advertise VLAN 80
L2 Features > GVRP > GVRP Forbidden VLAN 81
L2 Features > GVRP > GVRP Statistics Table 81
L2 Features > Auto Surveillance VLAN > Auto Surveillance Properties 81
L2 Features > Auto Surveillance VLAN > MAC Settings and Surveillance Device 82
L2 Features > Voice VLAN > Voice VLAN Global 83
L2 Features > Voice VLAN > Voice VLAN Port 83
L2 Features > Voice VLAN > Voice VLAN OUI 84
L2 Features > Voice VLAN > Voice VLAN Device 84

L2 Features > Voice VLAN > Voice VLAN LLDP-MED Device 84
L2 Features > STP > STP Global Settings 84
L2 Features > STP > STP Port Settings 86
L2 Features > STP > MST Configuration Identification 87
L2 Features > STP > STP Instance 87
L2 Features > STP > MSTP Port Information 88
L2 Features > ERPS(G.8032) > ERPS 88
L2 Features > ERPS(G.8032) > ERPS Profile 90
L2 Features > Loopback Detection 91
L2 Features > Link Aggregation 91
L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Settings 92
L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Groups Settings 93
L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Mrouter Settings 94
L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Statistics Settings 95
L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Setting 95
L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Groups Setting 96
L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Mrouter Settings 97
L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Statistics Settings 98
L2 Features > L2 Multicast Control > Multicast VLAN 98
L2 Features > L2 Multicast Control > Multicast VLAN Group Settings 100
L2 Features > L2 Multicast Control > Multicast Filtering 101
L2 Features > LLDP > LLDP Global Settings 102
L2 Features > LLDP > LLDP Port Settings 103
L2 Features > LLDP > LLDP Management Address List 103
L2 Features > LLDP > LLDP Basic TLVs Settings 104
L2 Features > LLDP > LLDP Dot1 TLVs Settings 104
L2 Features > LLDP > LLDP Dot3 TLVs Settings 105
L2 Features > LLDP > LLDP-MED Port Settings 105
L2 Features > LLDP > LLDP Statistics Information 106
L2 Features > LLDP > LLDP Local Port Information 107
L2 Features > LLDP > LLDP Neighbor Port Information 107
L3 Features > ARP > ARP Aging Time 108
L3 Features > ARP > Static ARP 108
L3 Features > ARP > ARP Table 108
L3 Features > IPv4 Interface 109
L3 Features > IPv4 Static/Default Route 110
L3 Features > IPv4 Route Table 110
L3 Features > IPv6 Interface 111
L3 Features > IPv6 Neighbor 112
L3 Features > IPv6 Static/Default Route 112
L3 Features > IPv6 Route Table 113
L3 Features > DNS Server Settings 113
QoS > Port Default CoS 114
QoS > Port Scheduler Method 114
QoS > Queue Settings 115
QoS > CoS to Queue Mapping 115
QoS > Port Rate Limiting 116
QoS > Queue Rate Limiting 116
QoS > Port Trust State 117

QoS > DSCP CoS Mapping 117
QoS > Advanced Settings> Class Map 118
QoS > Advanced Settings> Policy Map 119
QoS > Advanced Settings> Policy Binding 120
ACL > ACL Configuration Wizard 122
ACL > ACL Access List 141
ACL > ACL Interface Access Group 141
Security > Port Security > Port Security Global Settings 142
Security > Port Security > Port Security Port Settings 143
Security > Port Security > Port Security Address Entries 143
Security > 802.1X > 802.1X Global Settings 144
Security > 802.1X > 802.1X Port Settings 144
Security > 802.1X > Authentication Sessions Information 145
Security > 802.1X > Authenticator Statistics 145
Security > 802.1X > Authenticator Session Statistics 146
Security > 802.1X > Authenticator Diagnostics 146
Security > AAA > AAA Global Settings 147
Security > AAA > Application Authentication Settings 147
Security > AAA > Authentication Settings 147
Security > RADIUS > RADIUS Global Settings 149
Security > RADIUS > RADIUS Server Settings 149
Security > RADIUS > RADIUS Group Server Settings 150
Security > RADIUS > RADIUS Statistic 150
Security > TACACS > TACACS Server Settings 151
Security > TACACS > TACACS Group Server Settings 151
Security > TACACS > TACACS Statistic 152
Security > IMPB > DHCPv4 Snooping > DHCP Snooping Global Settings 152
Security > IMPB > DHCPv4 Snooping > DHCP Snooping Port Settings 153
Security > IMPB > DHCPv4 Snooping > DHCP Snooping VLAN Settings 154
Security > IMPB > DHCPv4 Snooping > DHCP Snooping Database 154
Security > IMPB > DHCPv4 Snooping > DHCP Snooping Binding Entry 155
Security > IMPB > Dynamic ARP Inspection > ARP Access List 155
Security > IMPB > Dynamic ARP Inspection > ARP Inspection Settings 156
Security > IMPB > Dynamic ARP Inspection > ARP Inspection Port Settings 156
Security > IMPB > Dynamic ARP Inspection > ARP Inspection VLAN 157
Security > IMPB > Dynamic ARP Inspection > ARP Inspection Statistics 157
Security > IMPB > Dynamic ARP Inspection > ARP Inspection Log 157
Security > IMPB > IP Source Guard > IP Source Port Settings 158
Security > IMPB > IP Source Guard > IP Source Guard Binding 158
Security > IMPB > IP Source Guard > IP Source Guard HW Entry 159
Security > IMPB >Advanced Settings > IP-MAC-Port Binding Settings 160
Security > IMPB >Advanced Settings > IP-MAC-Port Blocked Entry 160
Security > IMPB >IPv6 > IPv6 Snooping 161
Security > IMPB >IPv6 > IPv6 ND Inspection 162
Security > IMPB >IPv6 > IPv6 RA Guard 163
Security > IMPB >IPv6 > IPv6 DHCP Guard 164
Security > IMPB >IPv6 > IPv6 Source Guard > IPv6 Source Guard Settings 165
Security > IMPB >IPv6 > IPv6 Source Guard > IPv6 Neighbor Binding 166
Security > Network Access Authentication > Guest VLAN 167

Security > Network Access Authentication > Network Access Authentication Global Settings 167
Security > Network Access Authentication > Network Access Authentication Port Settings 168
Security > Network Access Authentication > Network Access Authentication Sessions Information 168
Security > DHCP Server Screening > DHCP Server Screening Global Settings 169
Security > DHCP Server Screening > DHCP Server Screening Port Settings 170
Security > ARP Spoofing Prevention 170
Security > MAC Authentication 171
Security > Safeguard Engine > Safeguard Engine Settings 172
Security > Safeguard Engine > CPU Protect Counters 172
Security > Safeguard Engine > CPU Protect Sub-Interface 173
Security > Safeguard Engine > CPU Protect Type 173
Security > Trusted Host 174
Security > Traffic Segmentation Settings 174
Security > Storm Control Settings 175
Security > DoS Attack Prevention Settings 176
Security > SSH > SSH Global Settings 177
Security > SSH > Host Key 178
Security > SSH > SSH Server Algorithm 178
Security > SSH > SSH Server Connection 178
Security > SSH > SSH User Authentication List 179
Security > SSH > SSH Public Key Settings 179
Security > SSL > SSL Global Setting 179
Security > SSL > Crypto PKI Trustpoint 180
Security > SSL > SSL Service Policy 181
OAM > Cable Diagnostics 181
OAM > DDM > DDM Settings 182
OAM > DDM > DDM Temperature Threshold Settings 182
OAM > DDM > DDM Voltage Threshold Settings 183
OAM > DDM > DDM Bias Current Threshold Settings 183
OAM > DDM > DDM TX Power Threshold Settings 183
OAM > DDM > DDM RX Power Threshold Settings 184
OAM > DDM > DDM Status Table 184
Monitoring > Statistics > Port 185
Monitoring > Statistics > Port Counters 186
Monitoring > Statistics > Counters 187
Monitoring > Mirror Settings 188
Green > Power Saving 188
Green > EEE 189
Surveillance Mode 190
Surveillance Overview 190
Surveillance Topology 190
Device Information 195
Port Information 196
IP-Camera Information 198
NVR Information 199
PoE Information 200
PoE Scheduling 201
Time 203
Clock Settings 203

SNTP Settings 204
Surveillance Settings 205
Surveillance Log 207
Health Diagnostic 207
Toolbar 209
Wizard 209
Tools 209
Save 213
Help 214
Online Help 215
Standard Mode 215
Appendix A - Technical Specifications 216
Hardware Specifications 216
Key Components / Performance 216
Port Functions 216
Physical & Environment 216
Emission (EMI) Certifications 216
Safety Certifications 216
Features 217
L2 Features 217
L3 Features 217
D-Link Green Technology 217
VLAN 217
QoS (Quality of Service) 217
Security 217
Management 218

About This Guide

This guide provides installation and instructions for the D-Link L2 Gigabit Ethernet Smart Managed Switch (DGS-1250-28X/28XP/52X/52XP).

Note: The model you have purchased may appear slightly different from the illustrations shown in the document. Refer to the sections for detailed information about your switch, its components, network connections, and technical specifications.

This guide is divided into four parts:

1. Hardware Installation: Step-by-step hardware installation procedures.
2. Getting Started: A startup guide for basic switch installation and settings.
3. D-Link Network Assistant: An introduction to the central configuration utility.
4. Configuration: Information about the function descriptions and configuration settings.

Terms/Usage

In this guide, the term “Switch” (first letter capitalized) refers to the DGS-1250 Series switch and “switch” (first letter lower case) refers to other Ethernet switches. Some technologies use “switch”, “bridge” and “switching hubs” interchangeably, and all are commonly accepted terms for Ethernet switches.

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

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

Copyright and Trademarks

Information in this document is subjected to change without notice.

© 2025 D-Link Corporation. All rights reserved.

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

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

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

1 Product Introduction

Thank you and congratulations on your purchase of D-Link DGS-1250 Series Switch.

D-Link's latest generation L2 Gigabit Ethernet switch series blends plug-and-play simplicity with exceptional value and reliability for small and medium-sized business (SMB) networking. All models are housed in a new style rack-mount metal case with easy-to-view front panel diagnostic LEDs, and provide advance features including network security, traffic segmentation, QoS and versatile management.

Flexible Port Configurations: The DGS-1250 Series is D-Link's latest Gigabit switch which provides 24-port, 48-port GBASE-T and 4-port SFP+ models. The DGS-1250 Series switches, have the advantage of using intuitive feature-rich software and utilizing a neat and simplified Web GUI allowing users to access and configure the Switch from everywhere via a web browser. GBASE-T provides the requisite backward compatibility that allows end users to transparently upgrade from 10/100Mbps to 1 Gbps, using Cat 5e, 6, 6A, 7 unshielded and shielded twisted-pair cables. 10G SFP+ has the advantage of lower power consumption, longer cable distance, and better latency performance. Direct Attach Cables (DACs) can be used to provide a cost effective way of connecting switches at 10 Gbps that are in close proximity to each other.

D-Link Green Technology: D-Link Green devices aim to provide eco-friendly alternatives without compromising performance. D-Link Green Technology includes a number of innovations to reduce energy consumption on DGS-1250 series switches, such as reducing power when a port does not have a device attached, or adjusting the power usage according to the length of Ethernet cable connected to it.

Extensive Layer 2 Features: Implemented as complete L2 devices, these switches include functions such as IGMP snooping, port mirroring, Spanning Tree, ERPS, 802.3ad LACP, SNTP, LLDP and Loopback Detection to enhance performance and network reliability.

Extensive Layer 3 Features: These switches include functions such as IP interfaces, static routes, IPv6 static routes, and ARP to enhance performance and network resiliency.

QoS: The switches support bandwidth control and 802.1p priority queues, enabling users to run bandwidth-sensitive applications such as voice and video on the network. These functions allow the switches to work seamlessly with VLANs, 802.1p traffic and IPv6 Traffic Class priority to prioritize traffic on the network.

Network Security: D-Link's innovative Safeguard Engine function protects the switches against traffic flooding caused by virus attacks. Additional features such as Storm Control can help to keep the network from being overwhelmed by abnormal traffic. Port Security is another simple but useful authentication method to maintain the network device integrity. Also supports DHCP Server Screening, SSL and IP-MAC-Port Binding features.

Versatile Management: The new generation of D-Link Gigabit Ethernet Switches provide growing businesses with a simple and easy management of their network, using a web-based management interface that allows administrators to remotely control their network down to the port level. Adding a console port with RJ-45 for command line interface management. The Switch can be managed, out-of-band, by using the console port on the front panel of the Switch. Alternatively, the Switch can also be managed, in-band, by using a Telnet connection to any of the LAN ports on the Switch. And the command line interface provides complete access to all switch management features.

Users can also access the switch via Telnet. Some basic tasks can be performed such as changing the Switch IP address, resetting the settings to factory defaults, setting the administrator password, rebooting the Switch, or upgrading the Switch firmware by using the Command Line Interface (CLI).

In addition, users can utilize the SNMP MIB (*Management Information Base*) to poll the switches for information about the status, or send out traps of abnormal events. SNMP support allows users to integrate the switches with other third-party devices for management in an SNMP-enabled environment. D-Link Smart Managed Switches provides easy-to-use graphic interface and facilitates the operation efficiency.

DGS-1250-28X

24-port GE with 4-port SFP+ Smart managed switch

Front Panel



DGS-1250-28X Front Panel

Power LED : The Power LED lights up when the Switch is connected to a power source.

Console: The console LED lights up when the console port is connected.

Fan error: The Fan error LED lights up when the fan has runtime failure and is brought offline.

Port Link/Act/Speed LED (1-24, 25F-28F): The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port.

1GBase-T (Port 1 ~ Port 24)		
	Green	Amber
LED RIGHT	1000M	10M/100M

SFP+ (Port 25~ Port 28)	
Green	Amber
10G	1000M

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

ATTENTION: Ce produit est destiné à être utilisé avec un transceiveur optique homologué UL,tension DC3.3V, classe laser I.

CAUTION: The equipment is designed for building installation and not intended to be connected to exposed (outside plant) networks including campus environment and the ITE is to be connected only to PoE networks without routing to the outside plant." or equivalent.

ATTENTION: L'équipement est conçu pour une installation dans un bâtiment et ne doit pas être connecté à des réseaux exposés (installations extérieures), notamment des environnements de campus, et l'ITE doit être connecté uniquement à des réseaux PoE sans acheminement vers une installation extérieure." ou équivalent.

Reset: By pressing the Reset button, the Switch will change back to the default configuration and all changes will be lost.

Rear Panel



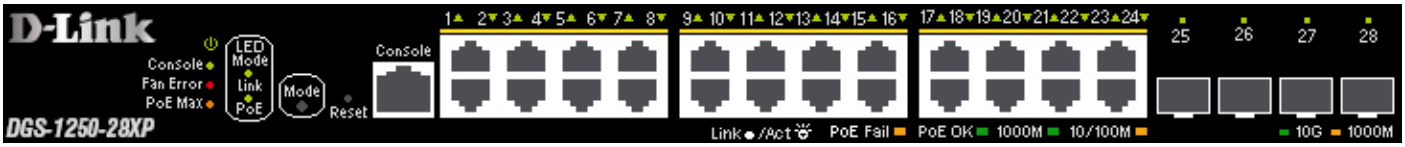
DGS-1250-28X Rear Panel

Power: Connect the AC power cord to this port.

DGS-1250-28XP

24-port GE POE with 4-port SFP+ Smart managed switch

Front Panel



DGS-1250-28XP Front Panel

Power LED : The Power LED lights up when the Switch is connected to a power source.

Console: The console LED lights up when the console port is connected.

PoE: Switch the LED in front panel to PoE mode by push PoE button.

In PoE mode:

Solid Green represents the PD successfully obtained the power from PSE.

Solid Amber represents failure occurred.

PoE Max: When the power requested exceeds guard band threshold, this LED lights in **solid amber**. When power available is more than guard band power, this LED lights in **blinking amber**.

Fan error: The Fan error LED lights up when the fan has runtime failure and is brought offline.

Port Link/Act/Speed LED (1-24, 25F-28F): The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port.

1GBase-T (Port 1 ~ Port 24)		
	Green	Amber
LED RIGHT	1000M	10M/100M

SFP+ (Port 25 ~ Port 28)	
Green	Amber
10G	1000M

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

ATTENTION: Ce produit est destiné à être utilisé avec un transceiveur optique homologué UL,tension DC3.3V, classe laser I.

CAUTION: The equipment is designed for building installation and not intended to be connected to exposed (outside plant) networks including campus environment and the ITE is to be connected only to PoE networks without routing to the outside plant." or equivalent.

ATTENTION: L'équipement est conçu pour une installation dans un bâtiment et ne doit pas être connecté à des réseaux exposés (installations extérieures), notamment des environnements de campus, et l'ITE doit être connecté uniquement à des réseaux PoE sans acheminement vers une installation extérieure." ou équivalent.

Reset: By pressing the Reset button, the Switch will change back to the default configuration and all changes will be lost.

Rear Panel



DGS-1250-28XP Rear Panel

Power: Connect the AC power cord to this port.

DGS-1250-52X

48-port GE with 4-port SFP+ Smart managed switch

Front Panel



DGS-1250-52X Front Panel

Power LED : The Power LED lights up when the Switch is connected to a power source.

Console: The console LED lights up when the console port is connected.

Fan error: The Fan error LED lights up when the fan has runtime failure and is brought offline.

Port Link/Act/Speed LED (1-28, 49F~52F): The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port.

1GBase-T (Port 1 ~ Port 48)		
	Green	Amber
LED RIGHT	1000M	10M/100M

SFP+ (Port 49~ Port 52)	
Green	Amber
10G	1000M

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

ATTENTION: Ce produit est destiné à être utilisé avec un transceiveur optique homologué UL,tension DC3.3V, classe laser I.

CAUTION: The equipment is designed for building installation and not intended to be connected to exposed (outside plant) networks including campus environment and the ITE is to be connected only to PoE networks without routing to the outside plant." or equivalent.

ATTENTION: L'équipement est conçu pour une installation dans un bâtiment et ne doit pas être connecté à des réseaux exposés (installations extérieures), notamment des environnements de campus, et l'ITE doit être connecté uniquement à des réseaux PoE sans acheminement vers une installation extérieure." ou équivalent.

Reset: By pressing the Reset button, the Switch will change back to the default configuration and all changes will be lost.

Rear Panel



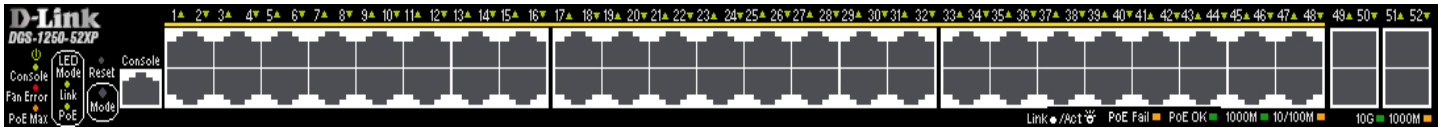
DGS-1250-52X Rear Panel

Power: Connect the AC power cord to this port.

DGS-1250-52XP

48-port GE POE with 4-port SFP+ Smart managed switch

Front Panel



DGS-1250-52XP Front Panel

Power LED : The Power LED lights up when the Switch is connected to a power source.

Console: The console LED lights up when the console port is connected.

PoE: Switch the LED in front panel to PoE mode by push PoE button.

In PoE mode:

Solid Green represents the PD successfully obtained the power from PSE.

Solid Amber represents failure occurred.

PoE Max: When the power requested exceeds guard band threshold, this LED lights in **solid amber**. When power available is more than guard band power, this LED lights in **blinking amber**.

Fan error: The Fan error LED lights up when the fan has runtime failure and is brought offline.

Port Link/Act/Speed LED (1-48, 49F~52F): The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port.

1GBase-T (Port 1 ~ Port 48)		
	Green	Amber
LED RIGHT	1000M	10M/100M

SFP+ (Port 49 ~ Port 52)	
Green	Amber
10G	1000M

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

ATTENTION: Ce produit est destiné à être utilisé avec un transceiveur optique homologué UL,tension DC3.3V, classe laser I.

CAUTION: The equipment is designed for building installation and not intended to be connected to exposed (outside plant) networks including campus environment and the ITE is to be connected only to PoE networks without routing to the outside plant." or equivalent.

ATTENTION: L'équipement est conçu pour une installation dans un bâtiment et ne doit pas être connecté à des réseaux exposés (installations extérieures), notamment des environnements de campus, et l'ITE doit être connecté uniquement à des réseaux PoE sans acheminement vers une installation extérieure." ou équivalent.

Reset: By pressing the Reset button, the Switch will change back to the default configuration and all changes will be lost.

Rear Panel



DGS-1250-52XP Rear Panel

Power: Connect the AC power cord to this port.

2 Hardware Installation

This chapter provides unpacking and installation information for the D-Link DGS-1250 Series Switch.

Safety Cautions

To reduce the risk of bodily injury, electrical shock, fire and damage to the equipment, observe the following precautions:

- Observe and follow service markings.
  - Do not service any product except as explained in your system documentation.
  - Opening or removing covers that are marked with the triangular symbol with a lightning bolt may expose you to electrical shock.
- Only a trained service technician should service components inside these compartments.
- If any of the following conditions occur, unplug the product from the electrical outlet and replace the part or contact your trained service provider:
  - The power cable, extension cable, or plug is damaged.
  - An object has fallen into the product.
  - The product has been exposed to water.
  - The product has been dropped or damaged.
  - The product does not operate correctly when you follow the operating instructions.
- Keep your system away from radiators and heat sources. Also, do not block cooling vents.
- Do not spill food or liquids on your system components, and never operate the product in a wet environment. If the system gets wet, contact your trained service provider.
- Do not push any objects into the openings of your system. Doing so can cause fire or electric shock by shorting out interior components.
- Use the product only with approved equipment.
- Allow the product to cool before removing covers or touching internal components.
- Operate the product only from the type of external power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service provider or local reseller.
- Also, be sure that attached devices are electrically rated to operate with the power available in your location.
- Use only approved power cable(s). If you have not been provided with a power cable for your system or for any AC powered option intended for your system, purchase a power cable that is approved for use in your country. The power cable must be rated for the product and for the voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the product.
- To help prevent electric shock, plug the system and peripheral power cables into properly grounded electrical outlets.
- These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a 3-wire cable with properly grounded plugs.
- Observe extension cable and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80 percent of the ampere ratings limit for the extension cable or power strip.
- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position system cables and power cables carefully; route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications.
- Always follow your local/national wiring rules.
- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:
  - Install the power supply before connecting the power cable to the power supply.
  - Unplug the power cable before removing the power supply.
  - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supplies.
- Move products with care; ensure that all casters and/or stabilizers are firmly connected to the system. Avoid sudden stops and uneven surfaces.

Step 1: Unpacking

Open the shipping carton and carefully unpack its contents. Please consult the packing list located in the User Manual to make sure all items are present and undamaged.

- One D-Link DGS-1250 Series switch
- One Multilingual Getting Started Guide
- One RJ-45 console cable
- Power Cord and Power Cord Retainer
- Rack-mount kit and Rubber Feet

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

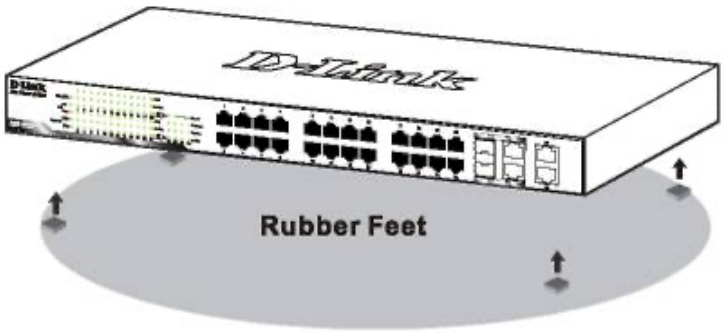
Step 2: Switch Installation

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

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

Desktop or Shelf Installation

When installing the switch on a desktop or shelf, the rubber feet included with the device must be attached on the bottom at each corner of the device's base. Allow enough ventilation space between the device and the objects around it.



Attach the adhesive rubber pads to the bottom

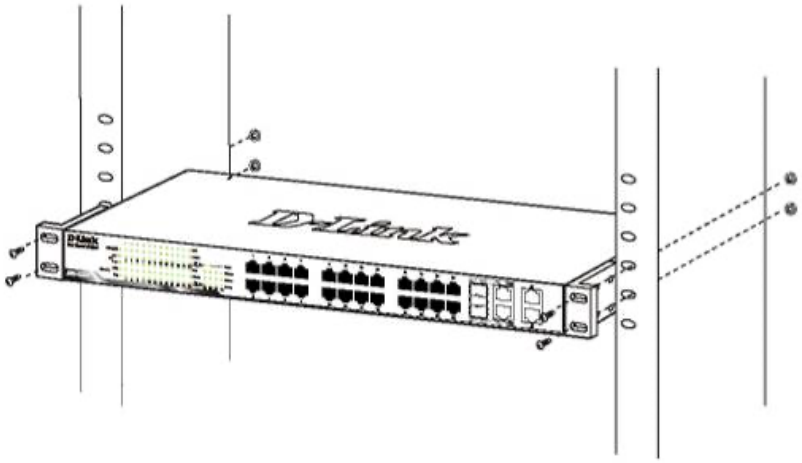
Rack Installation

The switch can be mounted in an EIA standard size 19-inch rack, which can be placed in a wiring closet with other equipment. To install, attach the mounting brackets to the switch's side panels (one on each side) and secure them with the screws provided (with 8 M3*6.0 size screws).



Attach the mounting brackets to the Switch

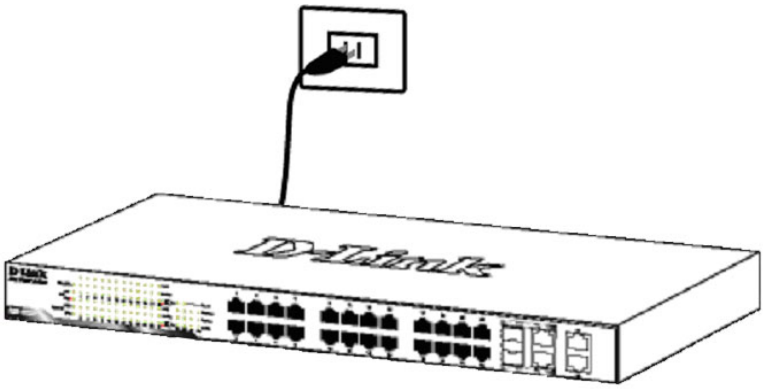
Then, use the screws provided with the equipment rack to mount the switch in the rack.



Mount the Switch in the rack or chassis

Step 3 – Plugging in the AC Power Cord

The Switch can now be connected to the AC power. Connect the AC power cord to the rear of the switch and to an electrical outlet (preferably one that is grounded and surge protected).



Plugging the switch into an outlet

Power Failure

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

Grounding the Switch

This section describes how to connect the DGS-1250 Series Switch to ground. You must complete this procedure before powering your switch.

Required Tools and Equipment

- Ground screws (included in the accessory kit): One M4 x 6 mm (metric) pan-head screw.
- Ground cable (not included in the accessory kit): The grounding cable should be sized according to local and national installation requirements. Depending on the power supply and system, a 12 to 6 AWG copper conductor is required for U.S installation. Commercially available 6 AWG wire is recommended. The length of the cable depends on the proximity of the switch to proper grounding facilities.
- A screwdriver (not included in the accessory kit)

The following steps let you connect the switch to a protective ground:

Step 1: Verify if the system power is off.

Step 2: Use the ground cable to place the #8 terminal lug ring on top of the ground-screw opening, as seen in the figure below.

Step 3: Insert the ground screw into the ground-screw opening.

Step 4: Using a screwdriver, tighten the ground screw to secure the ground cable to the switch.

Step 5: Attach the terminal lug ring at the other end of the grounding cable to an appropriate grounding stud or bolt on rack where the switch is installed.

Step 6: Verify if the connections at the ground connector on the switch and the rack are securely attached.

Connect a Grounding Cable

CAUTION: The equipment power supply cord shall be connected to a socket-outlet with earthing connection.

ATTENTION: Le cordon d'alimentation de l'équipement doit être branché sur une prise de courant dotée d'une connexion à la terre.

3 Getting Started

This chapter introduces the management interface of D-Link DGS-1250 Series Switch.

Management Options

The D-Link DGS-1250 Series Switch can be managed through any port by using the Web-based Management, or through any PC using CLI commands.

Each switch must be assigned its own IP Address, which is used for communication with the Web-Based Management or a SNMP network manager. The PC should have an IP address in the same subnet as the switch. Each switch can allow up to four users to access the Web-Based Management concurrently.

Please refer to the following installation instructions for the Web-based Management.

Using Web-based Management

After a successful physical installation, you can configure the Switch, monitor the network status, and display statistics using a web browser.

Supported Web Browsers

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

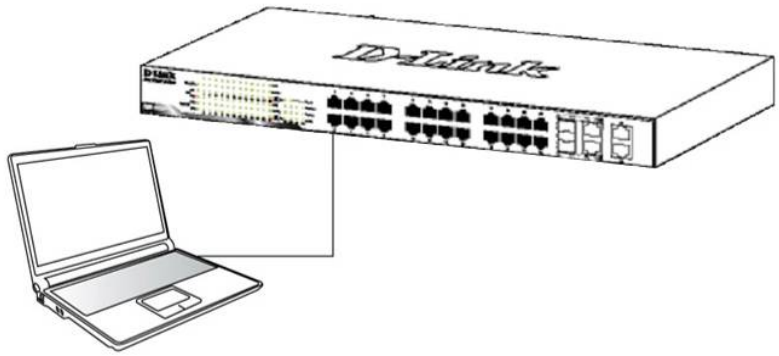
- Edge
- Chrome
- Firefox
- Safari

Connecting to the Switch

You will need the following equipment to begin the web configuration of your device:

1. A PC with a RJ-45 Ethernet connection
2. A standard Ethernet cable

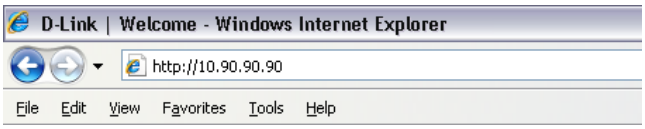
Connect the Ethernet cable to any of the ports on the front panel of the switch and to the Ethernet port on the PC.



Connected Ethernet cable

Login Web-based Management

In order to login and configure the switch via Web-based GUI, the PC must have an IP address in the same subnet as the switch. For example, if the switch has an IP address of **10.90.90.90**, the PC should have an IP address of **10.x.y.z** (where x/y is a number between 0 ~ 254 and z is a number between 1 ~ 254), and a subnet mask of **255.0.0.0**. There are two ways to launch the Web-based Management.

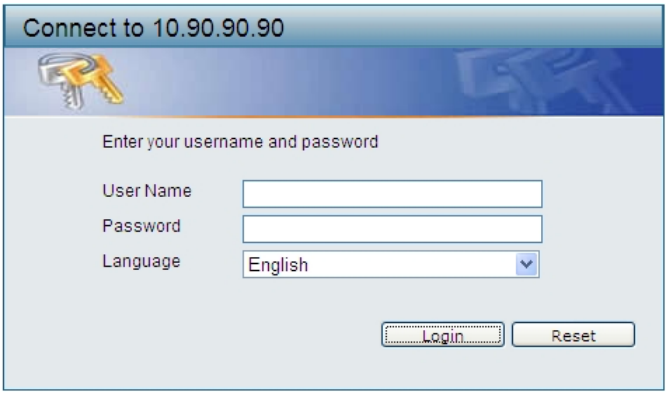


Enter the IP address 10.90.90.90 in the web browser

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

When the following login dialog box appears, enter the password and choose the language of the Web-based Management interface then click **Login**. [Default User name/password: admin/admin]

The switch supports 10 languages including English, Traditional Chinese, Simplified Chinese, German, Spanish, French, Italian, Portuguese, Japanese and Russian. By default, the Username and Password are empty and the language is **English**.



Login Dialog Box

Smart Wizard

After a successful login, the Smart Wizard will guide you through essential settings of the D-Link DGS-1250 Series Switch. Please refer to the Smart Wizard Configuration section for details.

Web-based Management

By clicking the **Exit** button in the Smart Wizard, you will enter the Web-based Management interface. Please refer to Chapter 4 Configuration for detailed instructions.

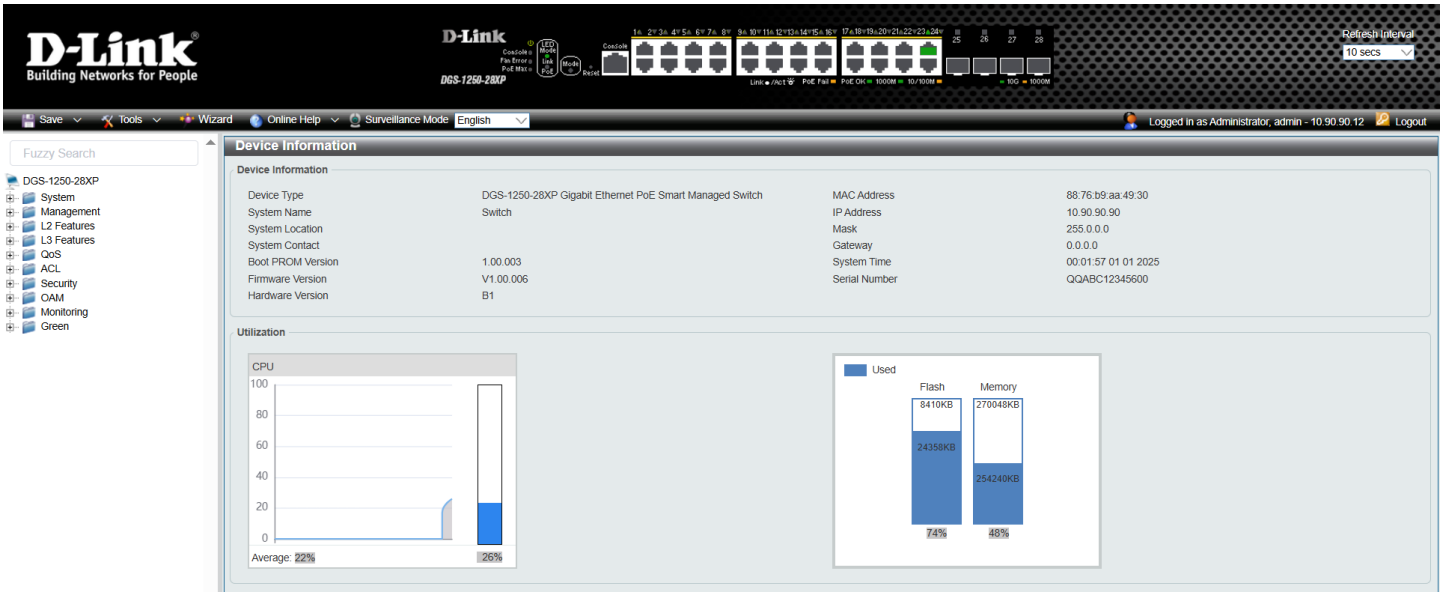
Web User Interface (Web UI)

Areas of the User Interface

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

Standard Mode

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

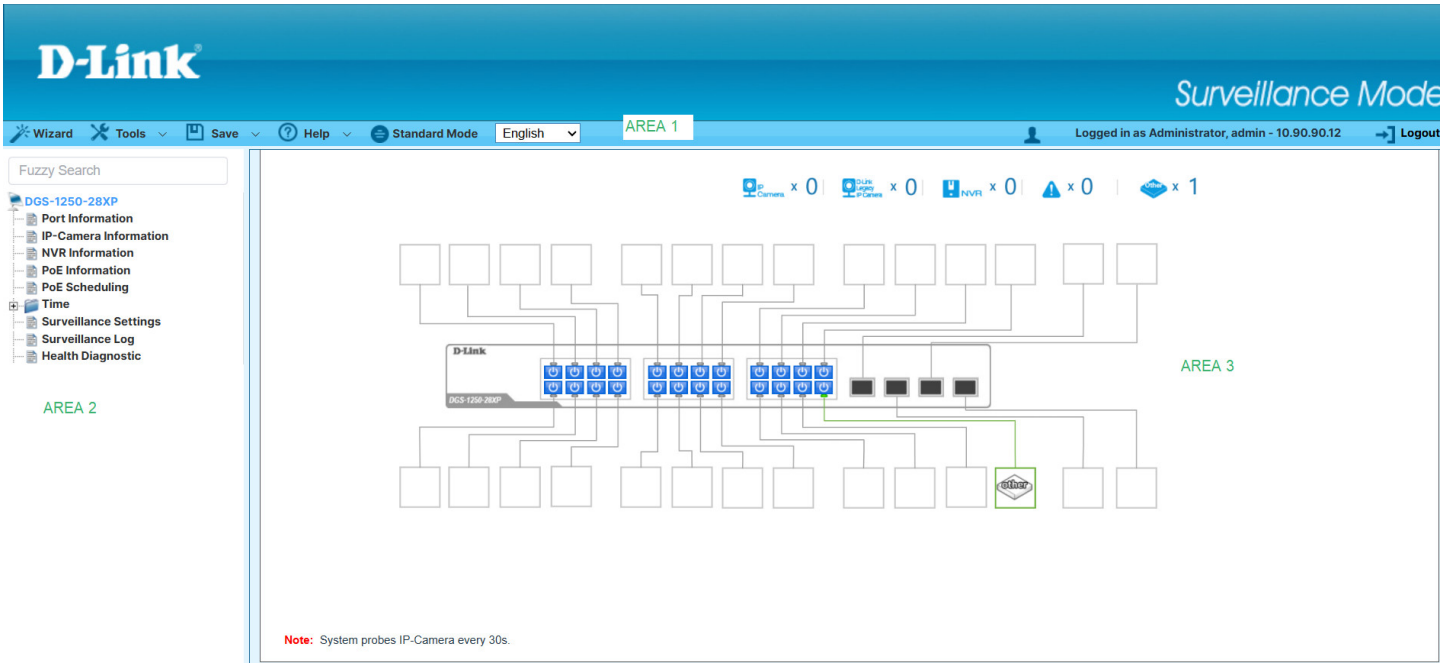


Web UI (Standard Mode)

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

Surveillance Mode

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



Web UI (Surveillance Mode)

Area Number	Description
AREA 1	In this area is a toolbar used to access functions like the **Wizard**, **Tools**, **Save**, **Help**, **Online Help**, accessing the Web UI in the **Standard Mode**, customized **Language** preference, and a **Logout** option. Click the **Standard Mode** option to change the switch mode from Surveillance Mode to Standard Mode. The user account and IP address currently logged into the Web UI will also be displayed in this toolbar.
AREA 2	In this area, the software features available in the Web UI of the Switch are grouped into folders containing hyperlinks that will open window frames in Area 3. There is also a search option in this area that can be used to search for specific feature keywords in the Web UI to find the link to the set of features.
AREA 3	In this area, configuration and monitoring window frames are available based on the selections made in Area 2. The status of devices, IP cameras, and NVRs discovered on the switch will also be displayed in this area.

NOTE: For more information about the Surveillance Mode, refer to **Surveillance Mode** on page 177.

4 Configuration

The features and functions of the D-Link DGS-1250 Series Switch can be configured for optimum use through the Web-based Management Utility.

Smart Wizard Configuration

After a successful login, the Smart Wizard will guide you through essential settings of the D-Link DGS-1250 Series Switch. If you do not plan to change anything, click **Exit** to leave the Wizard and enter the Web Interface. You can also skip it by clicking **Ignore the wizard next time** for the next time you logon to the Web-based Management.

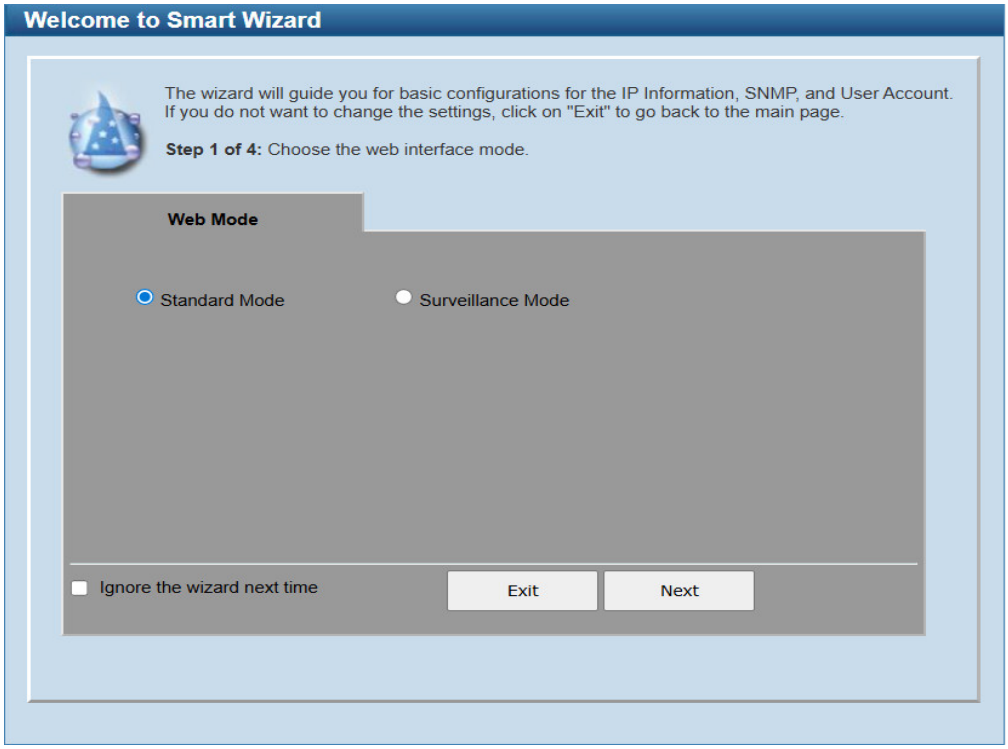
Web Mode

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

The **Standard Mode** is used to configure, manage, and monitor most of the software features on the Switch.

The **Surveillance Mode** is an additional web mode specifically designed to assist the user with surveillance features supported by the Switch.

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



The fields that can be configured are described below:

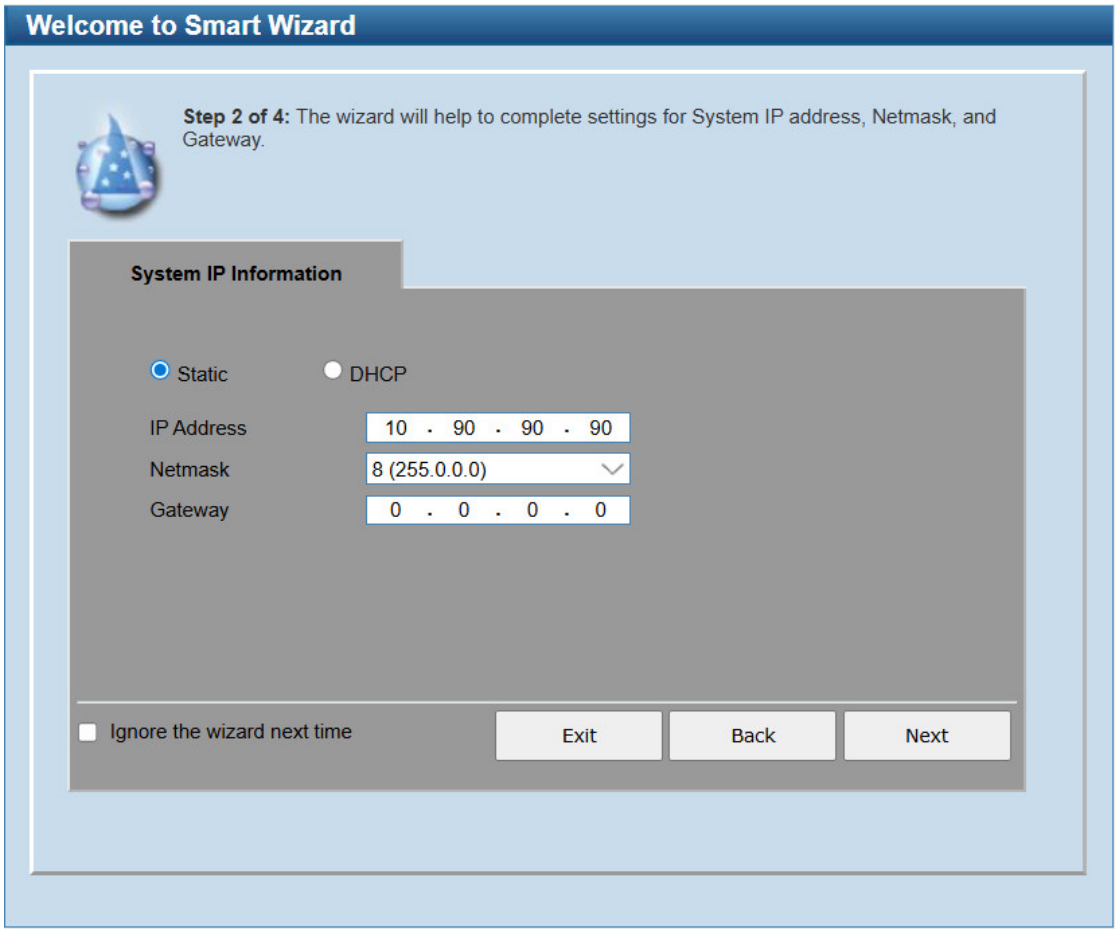
Parameter	Description
Standard Mode	Select this option to access the Standard Mode after the Smart Wizard was completed.
Surveillance Mode	Select this option to access the Surveillance Mode after the Smart Wizard was completed.

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

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

IPv4 Information

IPv4 Information will guide you to do basic configurations on 3 steps for the IP Information, access password, and SNMP. Select **Static**, to manually enter a new **IP Address**, **Netmask** and **Gateway** address, or select DHCP to automatically receive IP settings from a DHCP server. Click the **Next** button to enter the SNMP settings page The IP address is allowed for IPv4 and IPv6 address. If you are not changing the settings, click **Exit** button to go back to the main page. Or you can click on **Ignore the wizard next time** to skip wizard setting when the switch boots up.

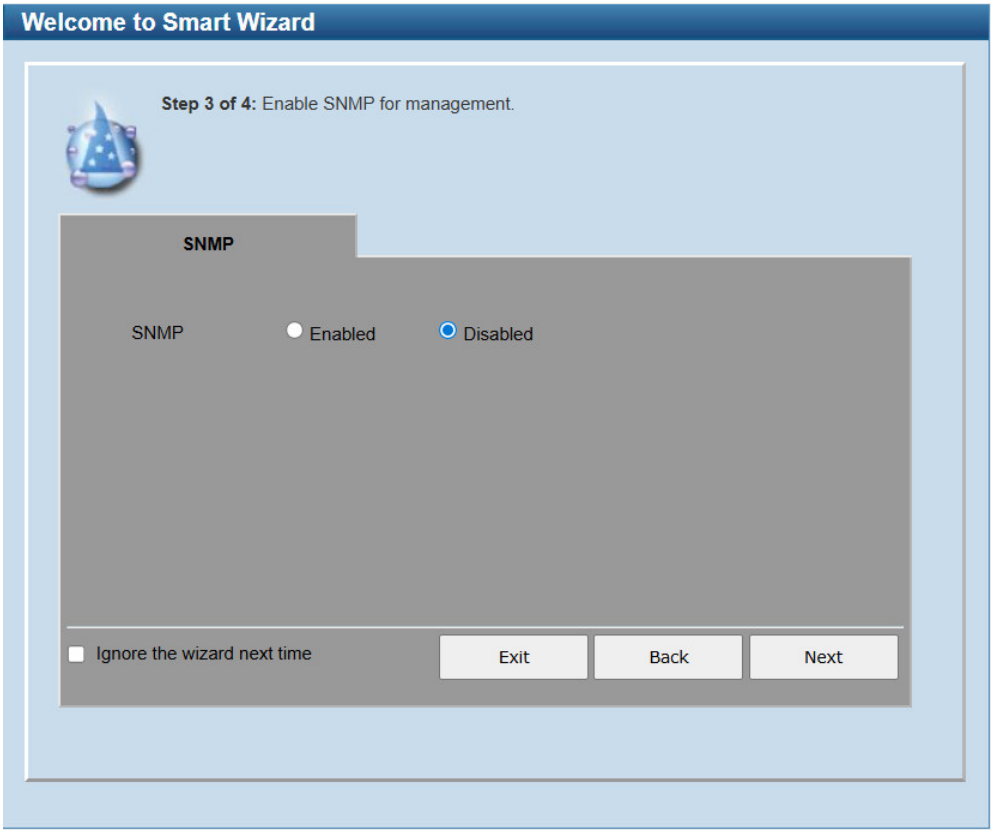


IPv4 Information in Smart Wizard

NOTE: The IPv4 Information of Smart Wizard does not support IPv6 address.

SNMP Settings

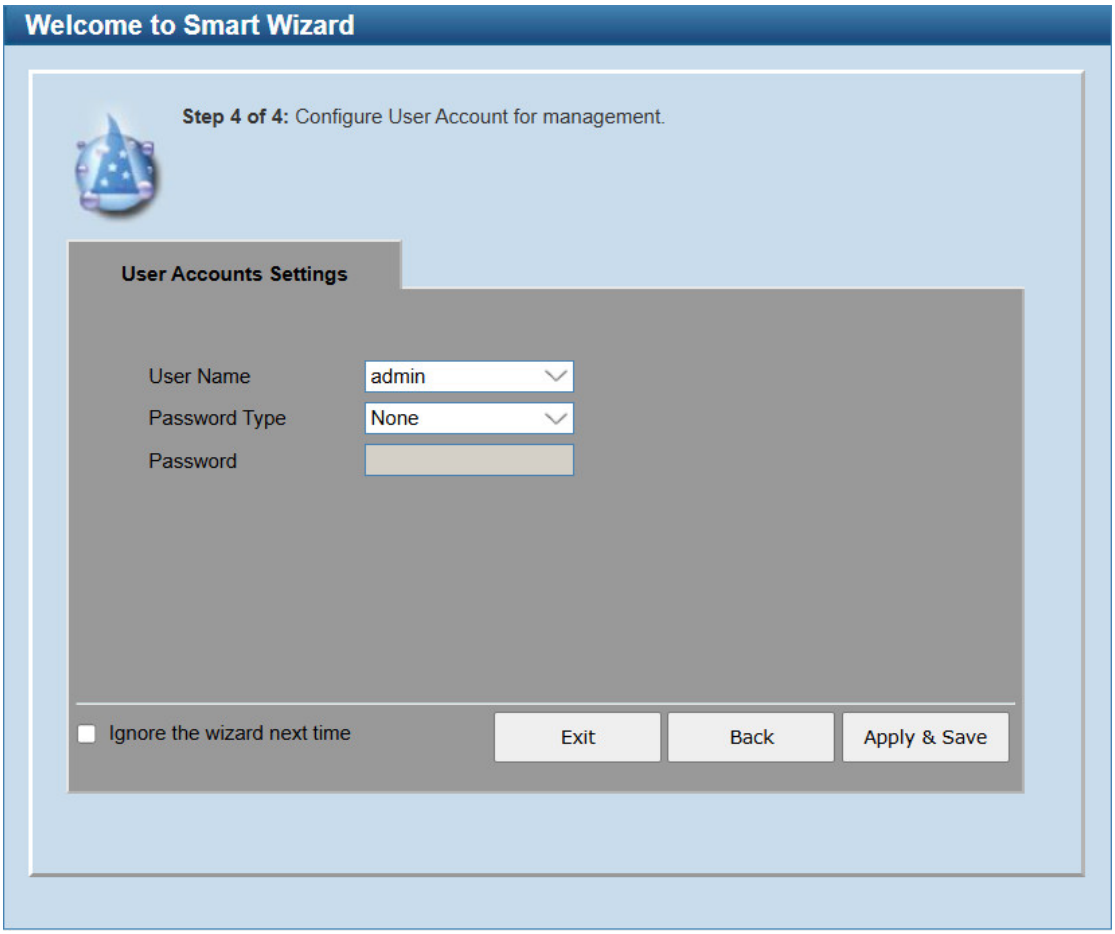
The SNMP Settings page allows you to quickly enable/disable the SNMP function. The default SNMP Setting is **Disabled**. Click **Enabled** and then click **Next**, then it will enter the **User Accounts Settings** page.



SNMP Settings in Smart Wizard

User Accounts Settings

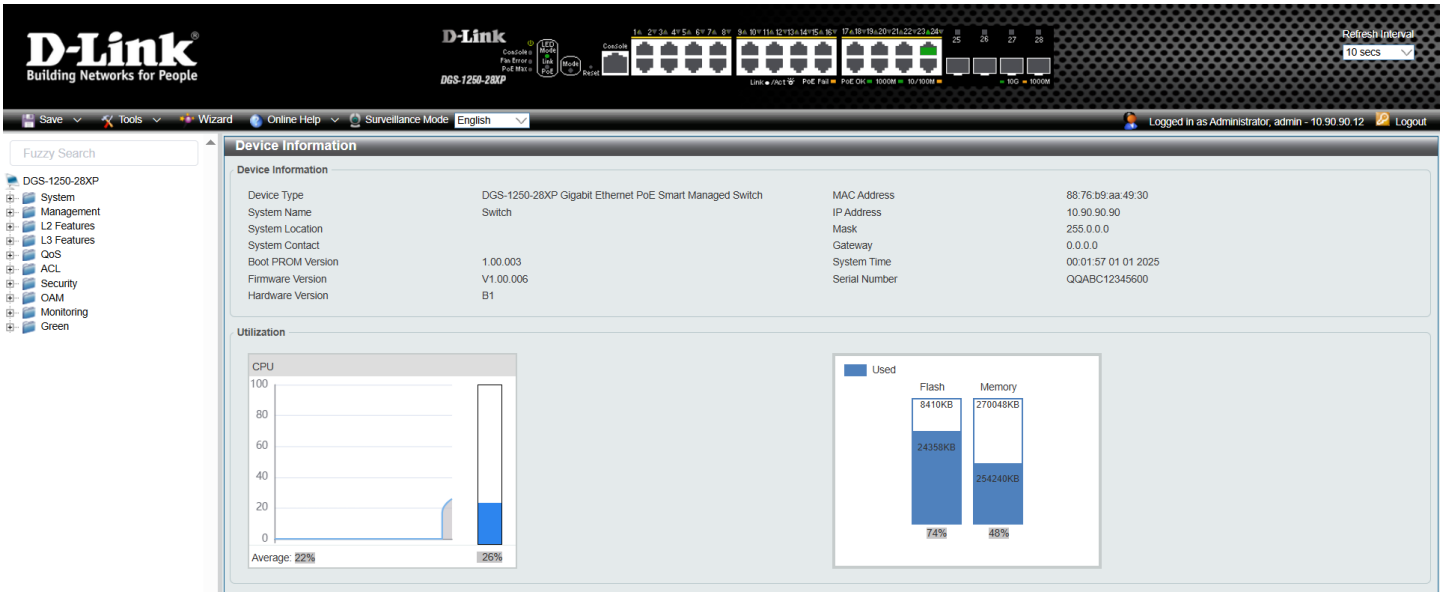
The User Accounts Settings page allows you to quickly specify the user account function. Enter the **User Name**, **Password Type** and **Password**. Click **Apply & Save** to save the configuration.



User Accounts Setting in Smart Wizard

Web-based Management

After clicking the **Exit** button in the Smart Wizard you will see the screen below:



Web-based Management

The above image is the Web-based Management screen. The three main areas are the **Tool Bar** on top, the **Function Tree**, and the **Main Configuration Screen**.

The **Tool Bar** provides a quick and convenient way for essential utility functions like firmware and configuration management.

By choosing different functions in the **Function Tree**, you can change all the settings in the **Main Configuration Screen**. The main configuration screen will show the current status of your Switch by clicking the model name on top of the function tree.

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

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

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

Click the D-Link logo at the upper-left corner of the screen to be redirected to the local D-Link website.

Tool Bar > Save Menu

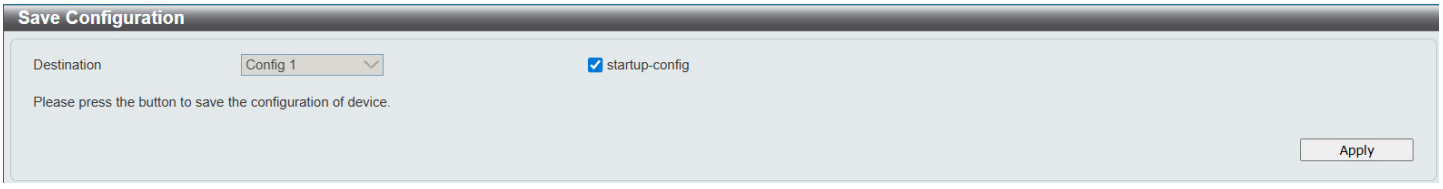
The Save Menu provides Save Configuration and Save Log functions.



Save Menu

Save Configuration

Select Save configuration to save the configuration changes to the Switch's non-volatile RAM.



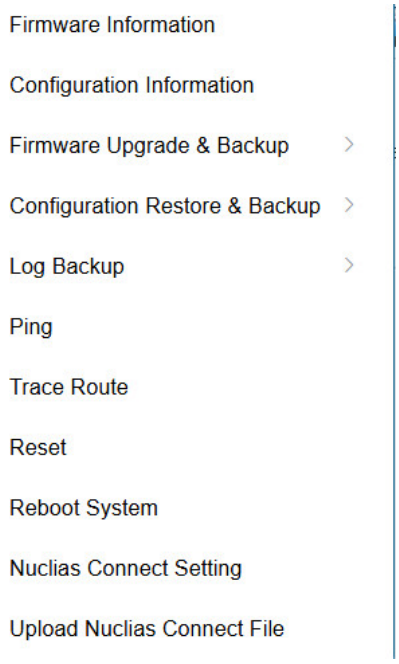
Save Configuration

Destination: Select the destination to save the configuration to.
Startup-config: Check the box to enable the startup configuration function.

Click the **Apply** button to save your settings.

Tool Bar > Tool Menu

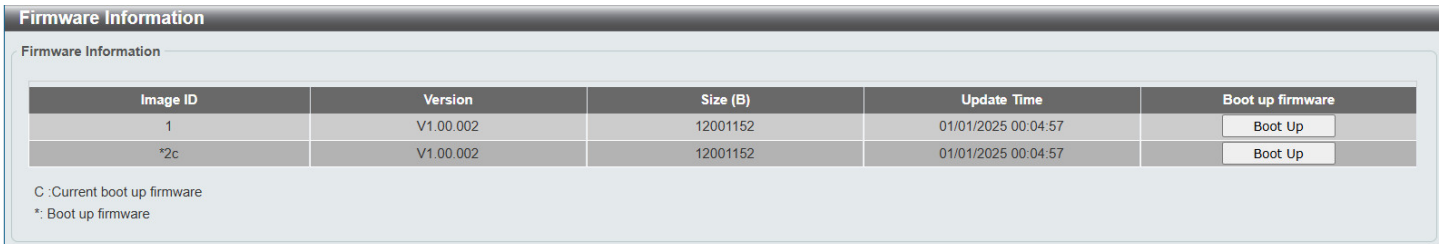
The Tool Menu offers global functions controls such as Reset, Reboot Device, Configuration Backup and Restore, Firmware Backup and Upgrade.



Tool Menu

Firmware Information

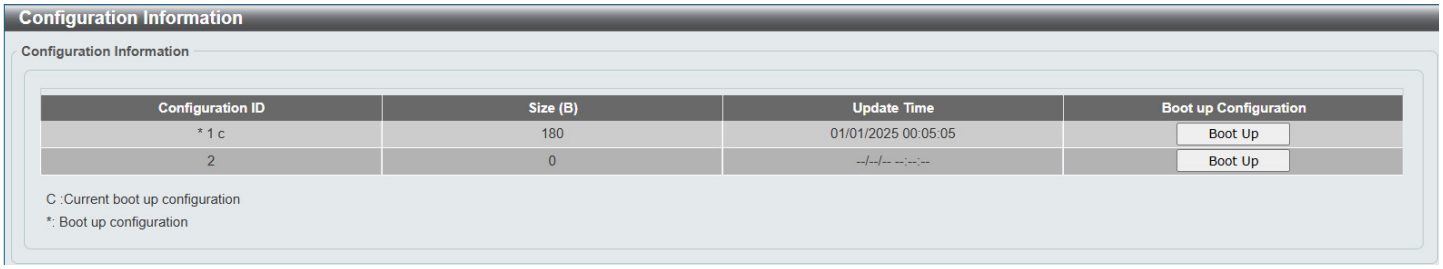
Display the firmware for the 2 firmware images, including the image that has been booted and the image that is selected for the next reboot.



Tool Menu > Firmware Information

Configuration Information

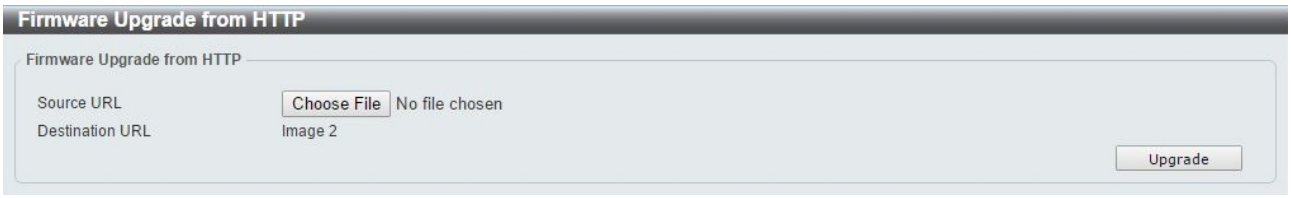
Display information for the Switch configuration. This includes the configuration that has been loaded and the configuration that is selected for the next reboot.



Tool Menu > Configuration Information

Firmware Upgrade & Backup > Firmware Upgrade from HTTP

To upgrade the firmware of Switch from a firmware file, select a **Source URL**, firmware **Destination URL** and click **Upgrade**. The specified firmware file will be uploaded to the Switch via **HTTP**.



Tool Menu > Firmware Upgrade & Backup > Firmware Upgrade from HTTP

Note: The Switch will reboot after restoring the firmware.

Firmware Upgrade & Backup > Firmware Upgrade from TFTP

Upgrade firmware using TFTP. Enter the TFTP IP address, source URL, and select a Destination URL. Click **Upgrade**.

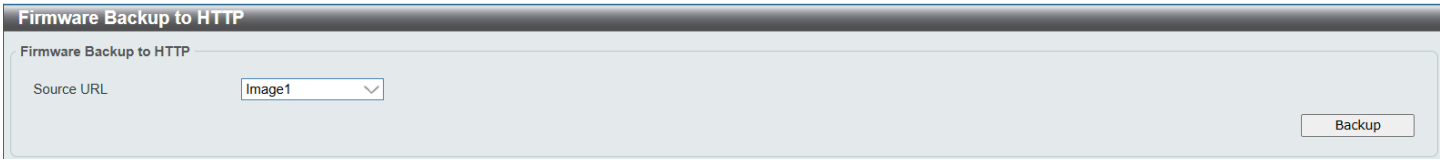


Tool Menu > Firmware Upgrade & Backup > Firmware Upgrade from TFTP

Note: The Switch will reboot after restoring the firmware.

Firmware Backup to HTTP & Backup > Firmware Backup to HTTP

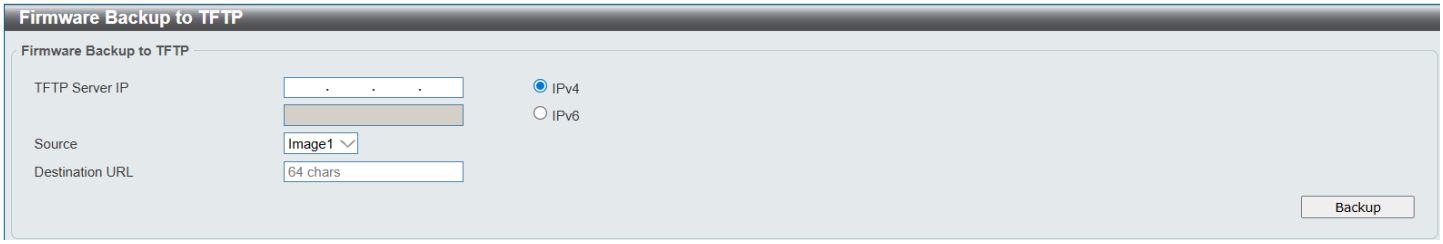
To save a backup of the firmware, select the source URL and then click **Backup**.



Tool Menu > Firmware Upgrade & Backup > Firmware Backup to HTTP

Firmware Backup to HTTP & Backup > Firmware Backup to TFTP

To save a backup of the firmware using TFTP, enter the TFTP server IP address, the source URL, and the destination URL. Click **Backup**.



Tool Menu > Firmware Upgrade & Backup > Firmware Backup to TFTP

Configuration Restore & Backup > Configuration Restore from HTTP

To restore the Switch from a saved configuration file, select a **Source URL**, configuration **Destination** and click **Restore**.



Tool Menu > Configuration Upgrade & Backup > Configuration Restore from HTTP

Startup-config: Check the box to enable the startup configuration function.

Configuration Restore & Backup > Configuration Restore from TFTP

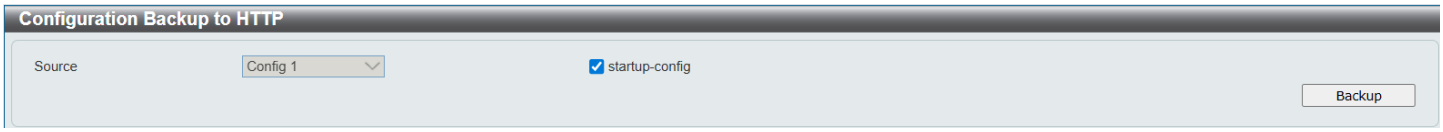
To load the Switch's configuration from a saved configuration file using TFTP, enter the TFTP server IP address, destination image and source URL, then click **Restore**.



Tool Menu > Configuration Upgrade & Backup > Configuration Restore from TFTP

Configuration Restore & Backup > Configuration Backup to HTTP

To save the current configuration to a file, click **Backup**.



Tool Menu > Configuration Upgrade & Backup > Configuration Backup to HTTP

Configuration Restore & Backup > Configuration Backup to TFTP

To save the current configuration to a file using TFTP, click **Backup**.

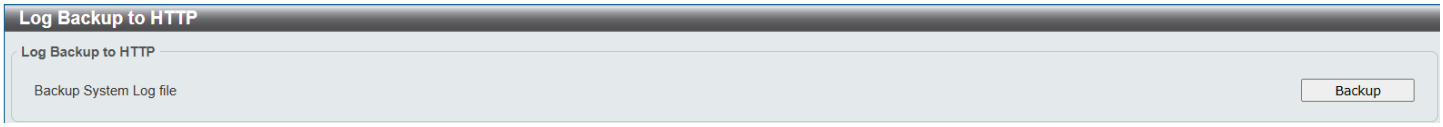


Tool Menu > Configuration Upgrade & Backup > Configuration Backup to TFTP

TFTP Server IP: Select **IPv4** or **IPv6** and enter the IP address.
Source: Select the source configuration file.
Startup-config: when checking the box, only the current startup configuration file will be backed up, which may be stored in the “Config 1” or “Config 2” location.
Destination URL: Enter the destination URL for the backup.

Log Backup > Log Backup to HTTP

To save the log to a file and click **Backup.**



Tool Menu > Log Backup > Log Backup to HTTP

Log Backup > Log Backup to TFTP

To save the log to a file using TFTP, enter the TFTP server IP address and destination URL then click **Backup**.

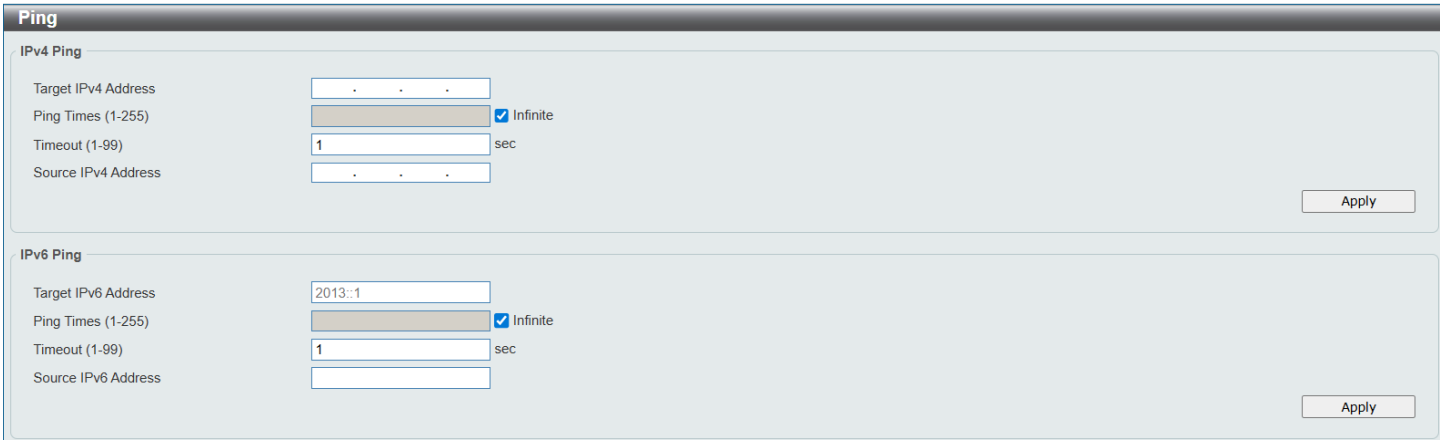


Tool Menu > Log Backup > Log Backup to TFTP

TFTP Server IP: Select **IPv4** or **IPv6** and enter the IP address.
Destination URL: Enter the destination URL for the backup.

Ping

To ping a computer or device, enter either **Target IPv4 Address or Target IPv6 Address**, **Ping Times, Timeout** and **Source IPv4 Address or Source IPv6 Address**. Enter the required information, tick the **Infinite** option to disable the **Ping Times** feature, and click **Apply**. The results will be displayed in the **Result** box.



Ping

Traceroute

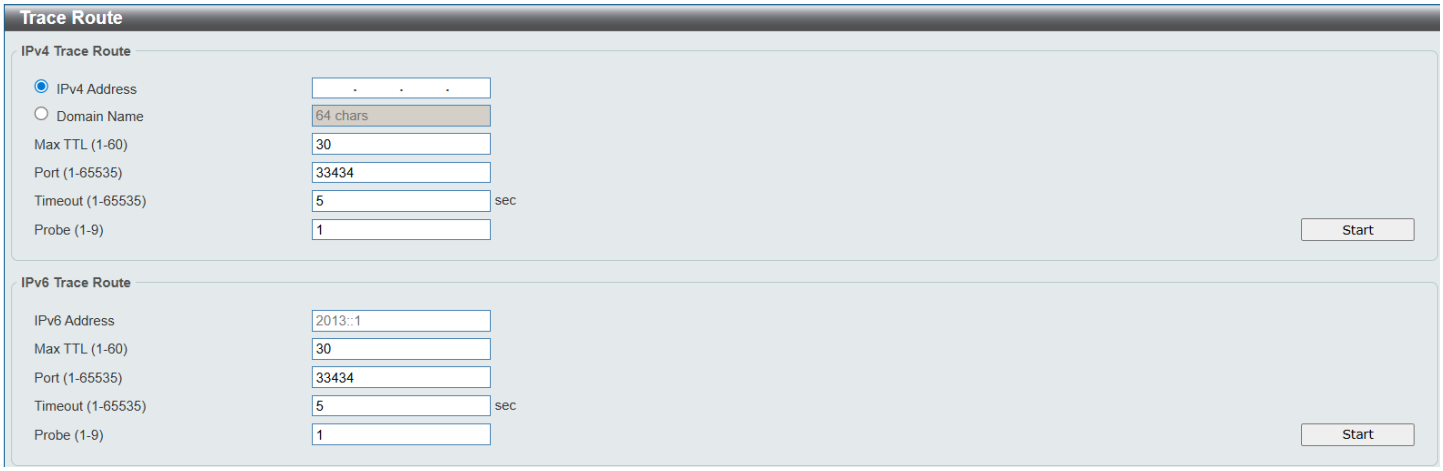
Ping is a small program that sends ICMP Echo packets to the IP address you specify. The destination node then responds to or "echoes" the packets sent from the Switch. This is very useful to verify connectivity between the Switch and other nodes on the network.

Max TTL: Enter the Time-To-Live (TTL) value of the trace route request here.

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.

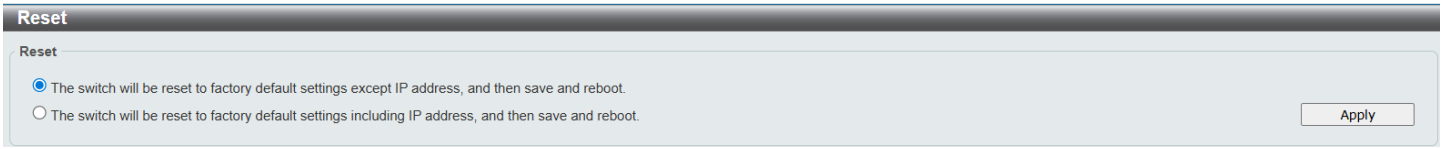
Probe: Enter the probe time number here. The range is from 1 to 8.



Traceroute

Reset

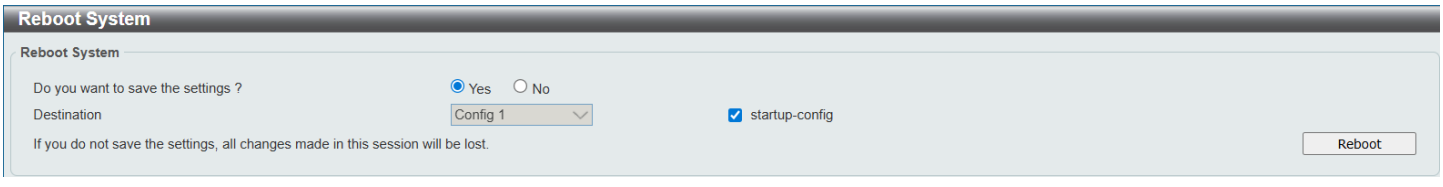
Select which reset option you want to perform and click **Apply.**



Tool Menu > Reset

Reboot System

Select to save your current settings and then click **Reboot** to restart the Switch.



Tool Menu > Reboot System

Destination: Select the configuration destination to be saved.

Startup-config: When checking the box, only the current startup configuration file will be backed up which may be stored in the “Config 1” or “Config 2” location.

Nuclias Connect Setting

This page contains the Nuclias Connect Settings of the Switch.



Tool Menu > Nuclias Connect Setting

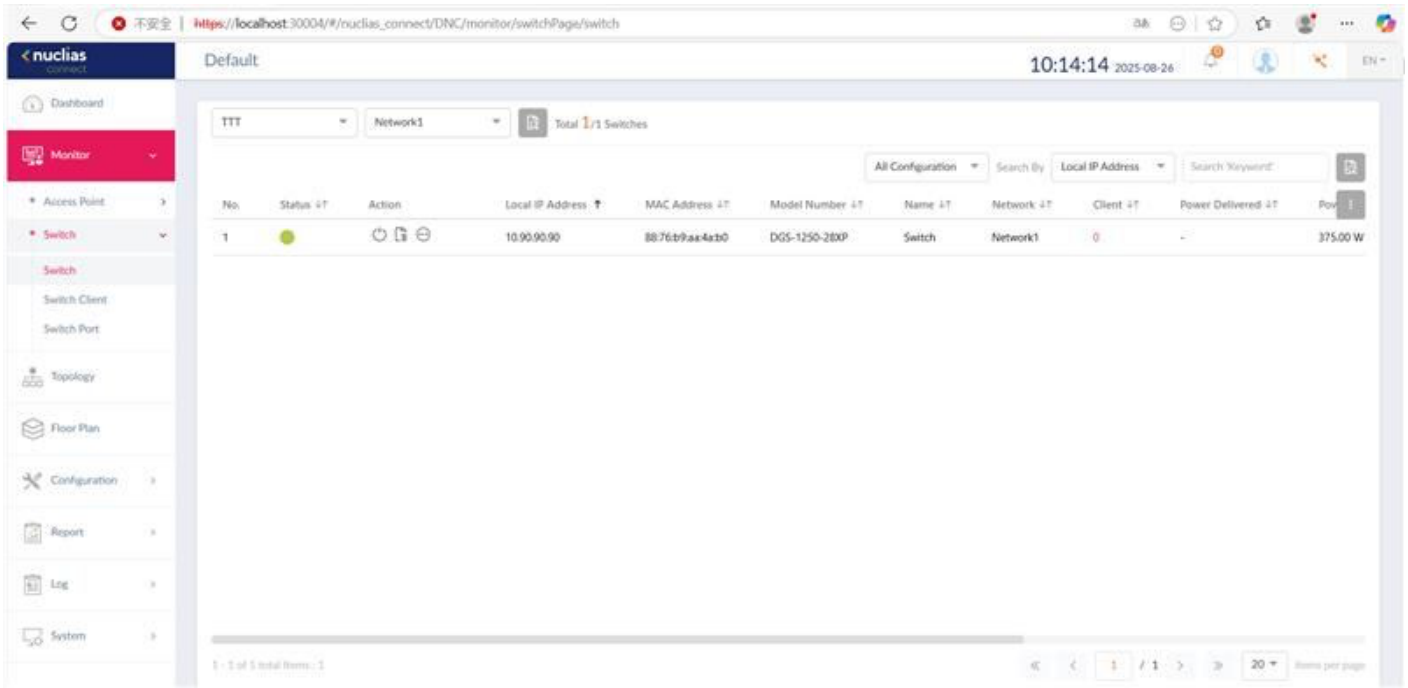


Tool Menu > Nuclias Connect Setting (mDNS Server Information)

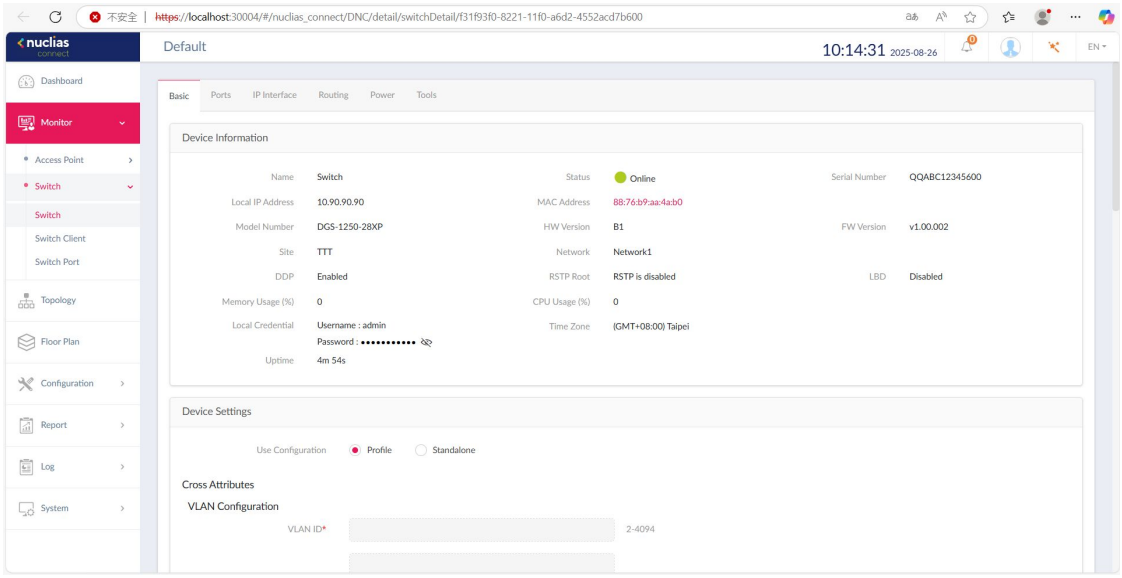
Nuclias Connect, D-Link’s centralized management solution for Small-to-Medium-Sized Business (SMB) networks. Nuclias Connect makes it easier to analyze, automate, configure, optimize, scale, and secure your network — delivering the convenience of an Enterprise-wide management solution, at an SMB price.

Nuclias Connect State: Enable/Disable the Nuclias Connect State.

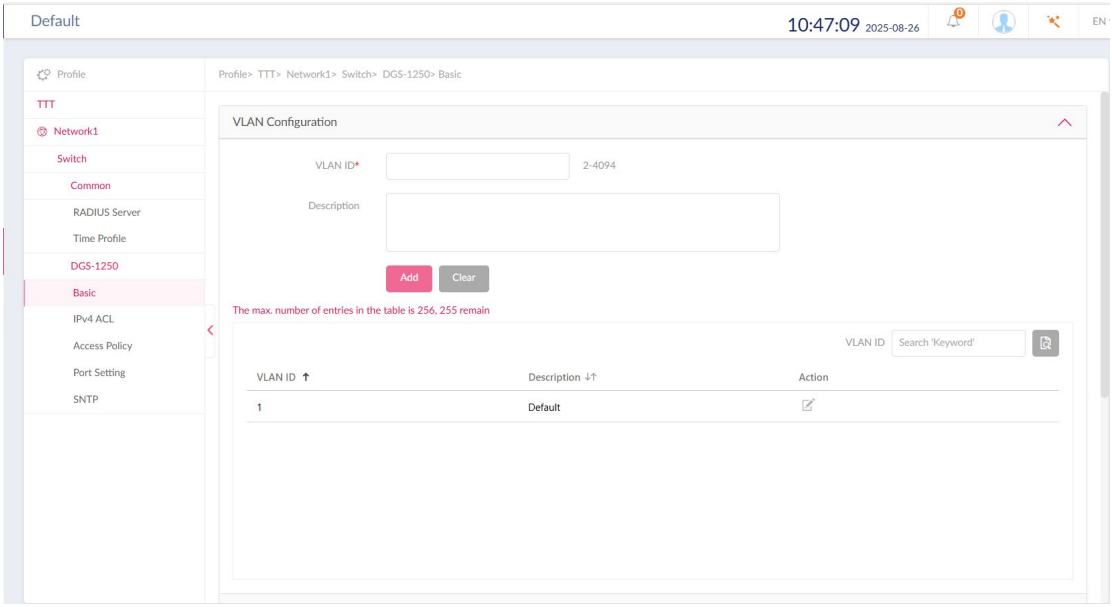
Nuclias Connect Status: Presents the Nuclias Connection Status which includes “Connection Status”, “Server IP/Port” and “Group ID”. The DNC server supports mDNS protocol which can be configured in Nuclias Connect Setting page.



On Nuclias Connect, user would be able to retrieve the device information.



Majority features would be able to be configured thru Nuclias Connect.

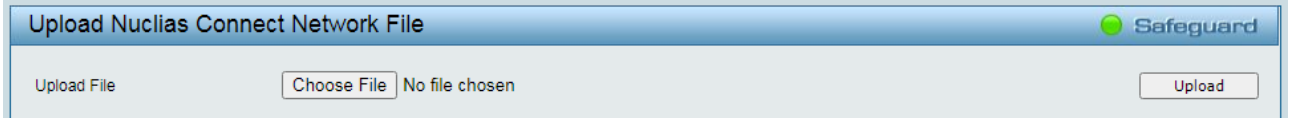


Please visit website Nuclias Connect (https://www.dlink.com/en/business/nuclias/nuclias-connect) for more information.

CAUTION: DGS-1250 series is designed to compatible with DNC-100 version 1.3.2.7 (and later). Please check DNC-100 (Nuclias Connect) version before use.

Upload Nuclias Connect File

This page used to load the previous saved Nuclias Connect Network file



Tool Menu > Upload Nuclias Connect File

Select File: Select the specific DNC file for Nuclias Connect Network. This specific type of file was created and saved via Nuclias Connect Network Profile which provided an easy method for device to rejoin the DNC.

Tool Bar > Smart Wizard

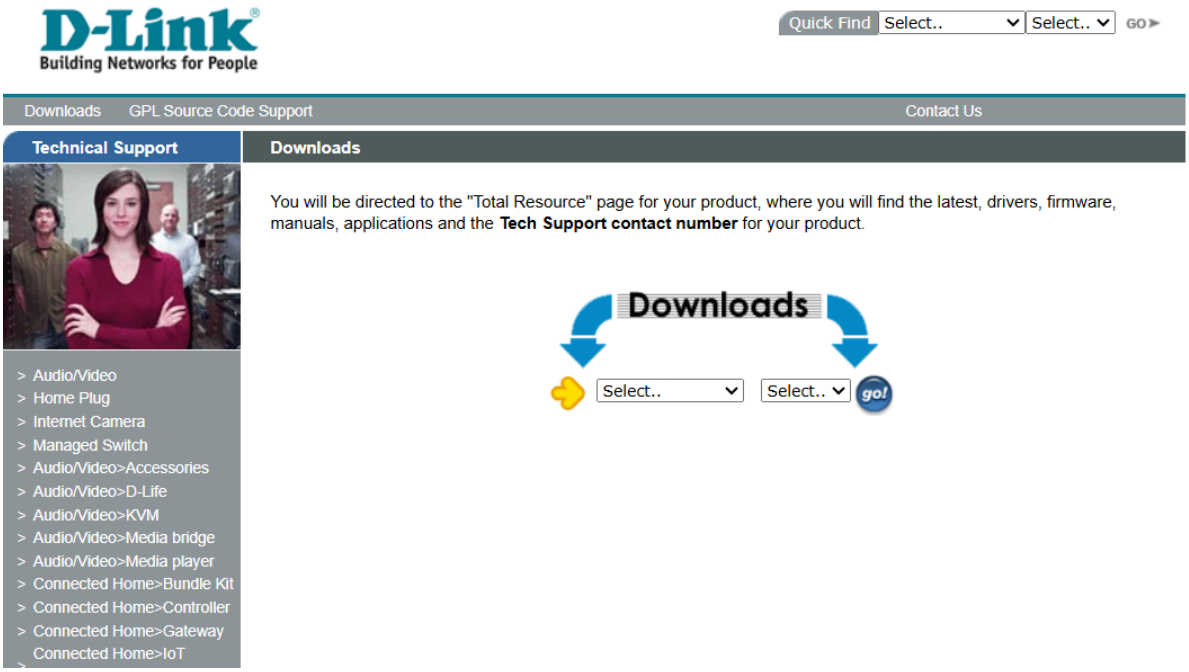
By clicking the **Smart Wizard** button, you can re-run to the Smart Wizard if you wish to make any changes.

Tool Bar > Online Help

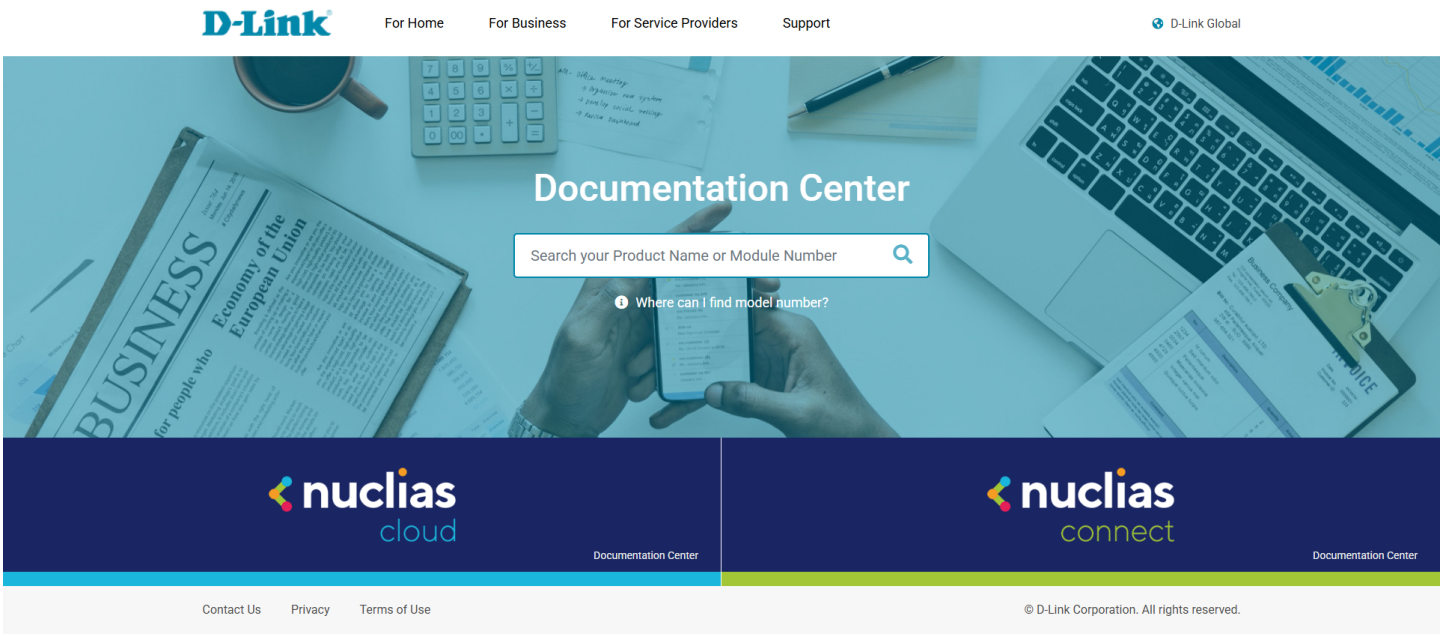
The Online Help provides two ways of online support: **D-link Support Site** will lead you to the D-Link website where you can find online resources such as updated firmware; **User Guide** can offer an immediate reference for the feature definition or configuration guide.



Online Help



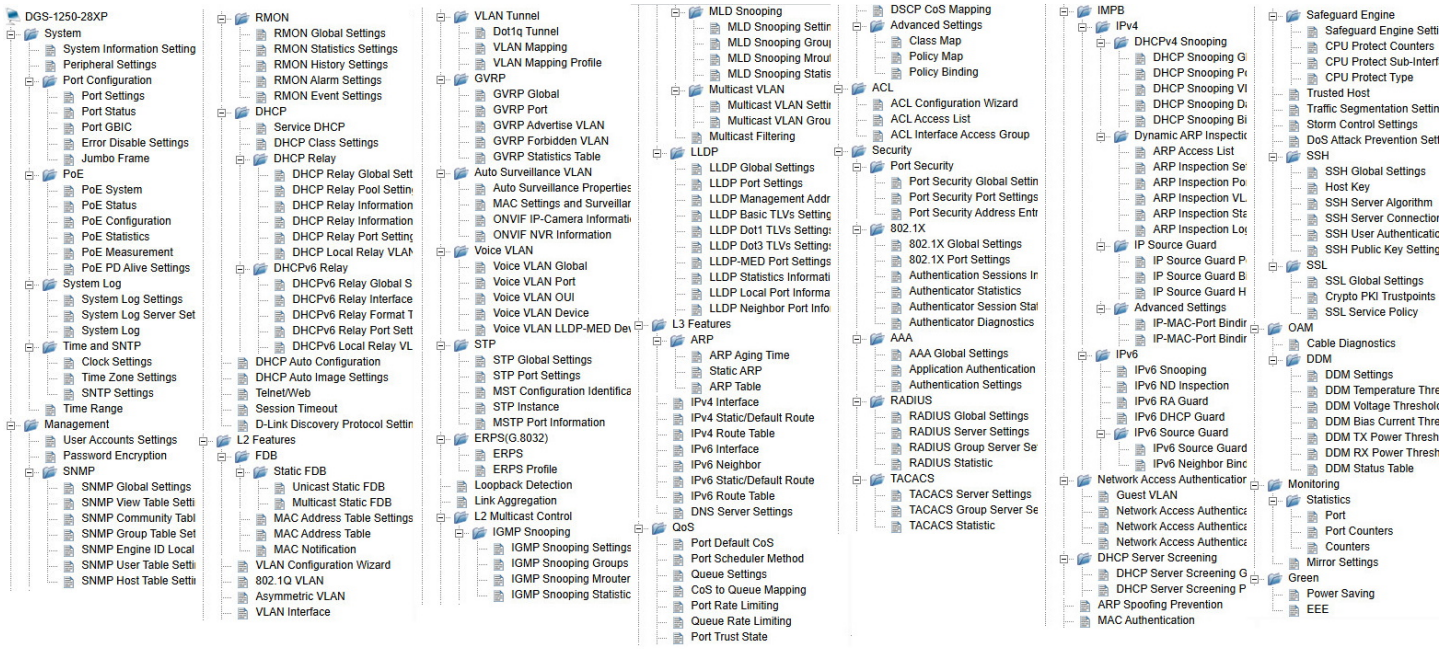
D-Link Support Site



User Guide Micro Site

Function Tree

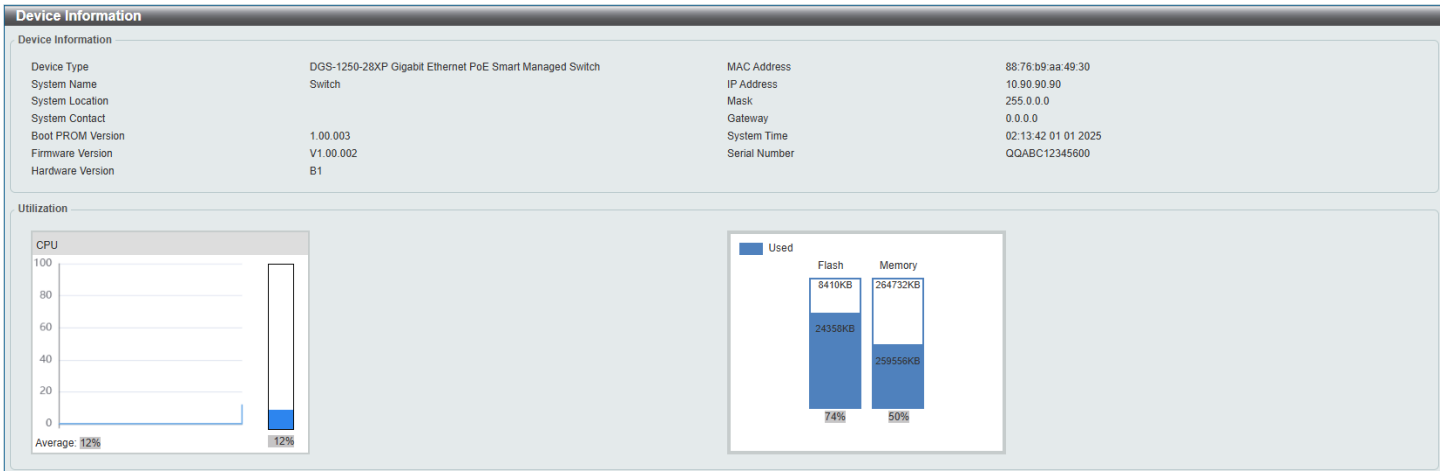
All configuration options on the switch are accessed through the Setup menu on the left side of the main window. Click on the setup item that you want to configure. The following sections provide more detailed description of each feature and function.



Function Tree

Device Information

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

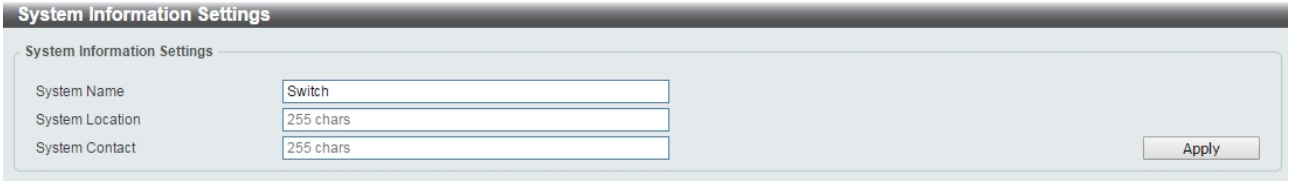


Device Information

System > System Information

The System Setting page allows you to configure basic system information.

System Information Settings: Enter a **System Name**, **System Location** and **System Contact**.

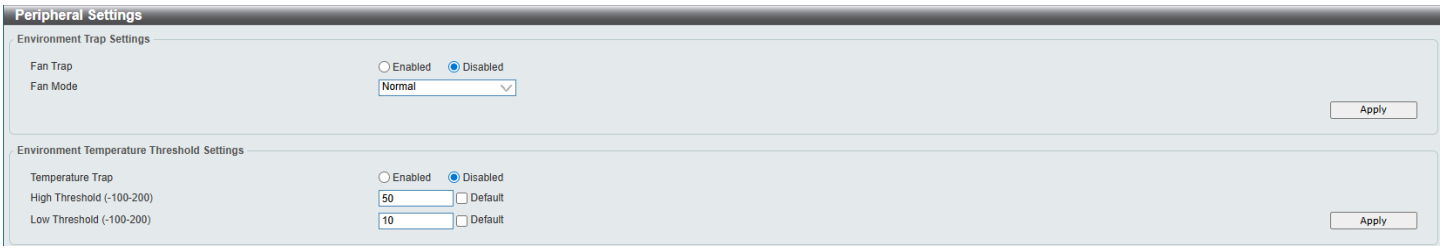


System > System Information

System > Peripheral

The Peripheral page allows user to configure the environment trap settings and environment temperature threshold settings.

System Information Settings: Enter a **System Name**, **System Location** and **System Contact**.



System > Peripheral

Environment Traps Settings:

Fan Trap: Select to enable or disable the fan trap state for waning fan event (fan failed or fan recover).

Fan Mode: Select to change Fan Normal mode or Quiet mode mode.

Environment Temperature Threshold Settings:

Temperature Trap: Select to enable or disable the temperature trap state for waning temperature event (temperature exceeds the thresholds or temperature recover).

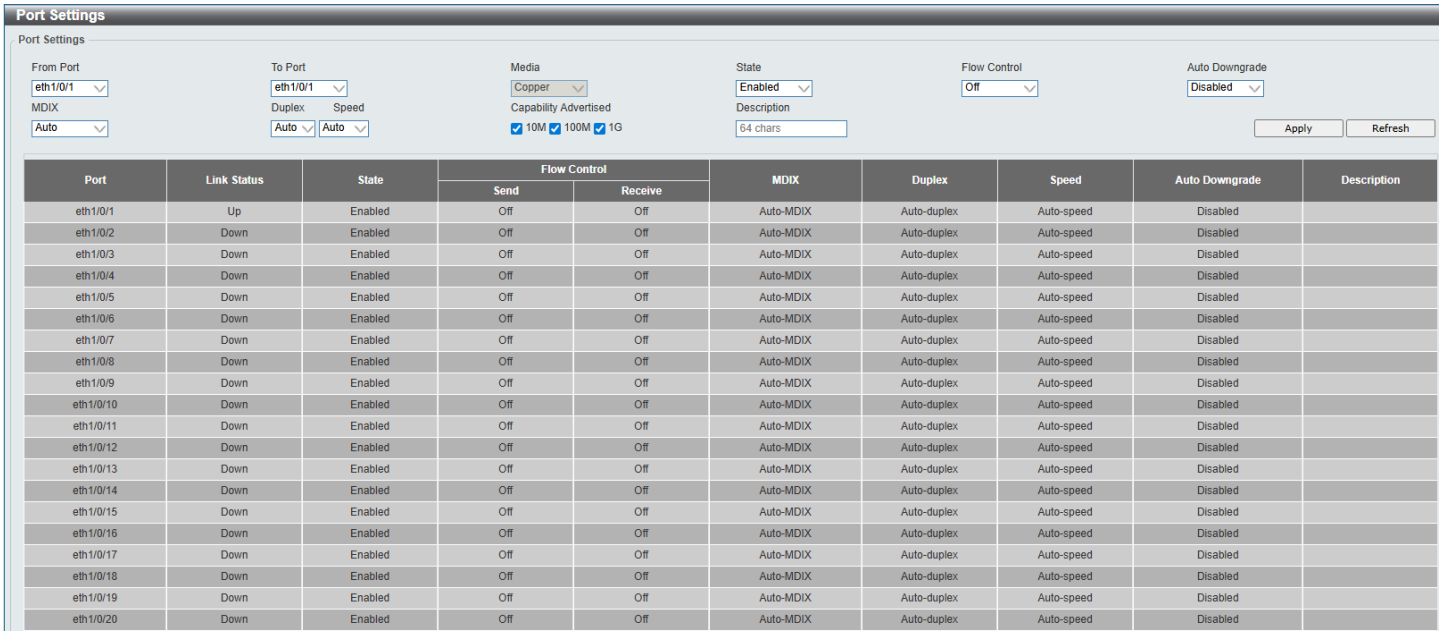
High Threshold (-100-200): Enter the high threshold value of the warning temperature setting. The range is from -100 to 200 Celsius degree. Tick the Default check box to return to the default value.

Low Threshold (-100-200): Enter the low threshold value of the warning temperature setting. The range is from -100 to 200 Celsius degree. Tick the Default check box to return to the default value.

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

System > Port Configuration > Port Settings

In the **Port Settings** page, the status of all ports can be monitored and adjusted for optimum configuration.



System > Port Configuration > Port Settings

From Port / To Port: Select the appropriate port range to be configured.
Media: Display selected interface media type belong to copper or fiber.
State: Enable or disable the physical port.
Flow Control: Select **On** or **Off**. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use back-pressure flow control, and Auto ports use an automatic selection of the two.
Auto Downgrade: To enable or disable automatically downgrading the advertised speed, in-case a link cannot be established at the available speed.
MDIX: Select the Medium Dependent Interface Crossover (MDIX) option here. Options to choose from are:

- Auto - Select this option for auto-sensing of the optimal type of cabling.

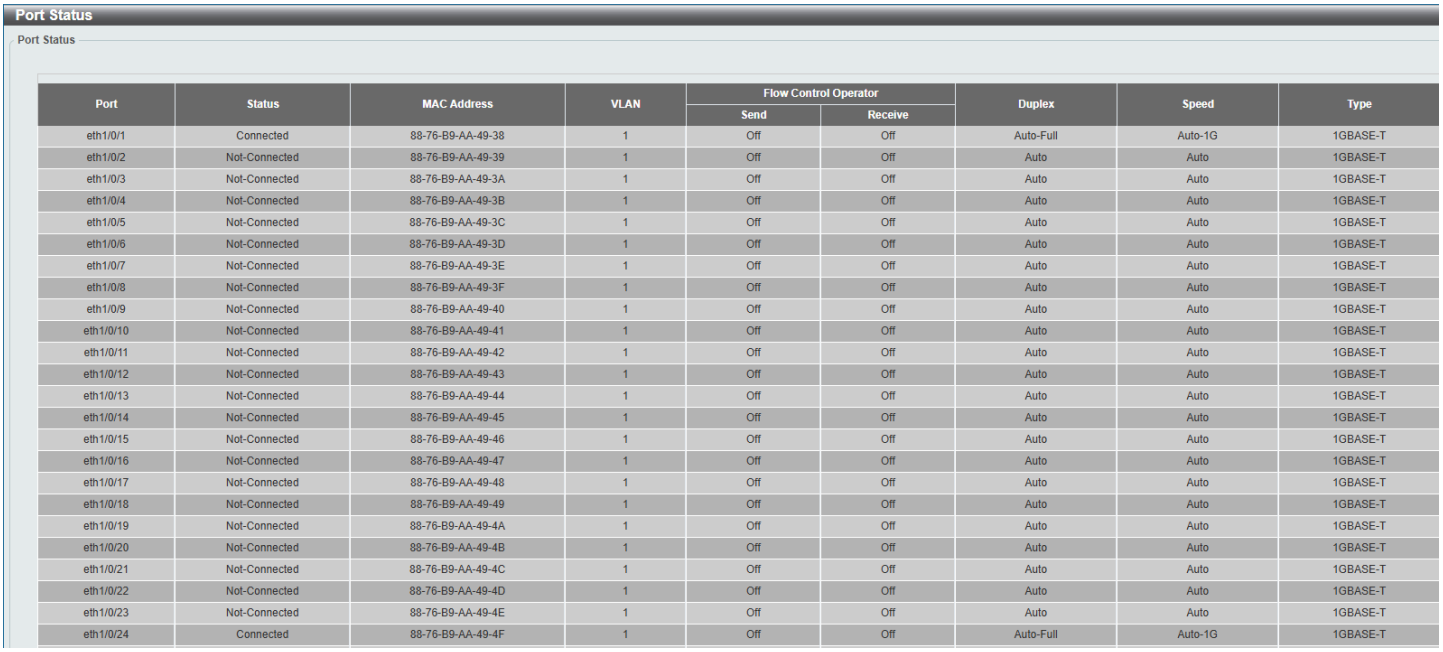
- Normal - Select this option for normal cabling. If this option is selected, the port is in the MDIX mode and can be connected to a PC NIC using a straight-through cable or a port (in the MDI mode) on another Switch through a crossover cable.
- Cross - Select this option for crossover cabling. If this option is selected, the port is in the MDI mode and can be connected to a port (in the MDIX mode) on another Switch through a straight cable.

Note: This option is only available on the 10/100/1000 Mbps RJ45 ports.
Duplex: Select the duplex mode used. Options to choose from are **Auto** and **Full**.
Speed: Select the speed for the ports. The speed values are **Auto**,1**0M**, **100M**, **1000M** for copper ports. **1G** and **10G** available for Fiber ports.
Capability Advertised: When the **Speed** is set to **Auto**, these capabilities are advertised during auto-negotiation.
Description: Enter a 64 characters description for the corresponding port.

Click **Apply** button to save your settings.
Click the **Refresh** button to refresh the display table.

System > Port Configuration > Port Status

The Port Settings page allows you to view the Switch's physical port status and settings. The table will display the Port, Status, MAC Address, VLAN, Flow Control Operator, Duplex, Speed and Type.


Port Status

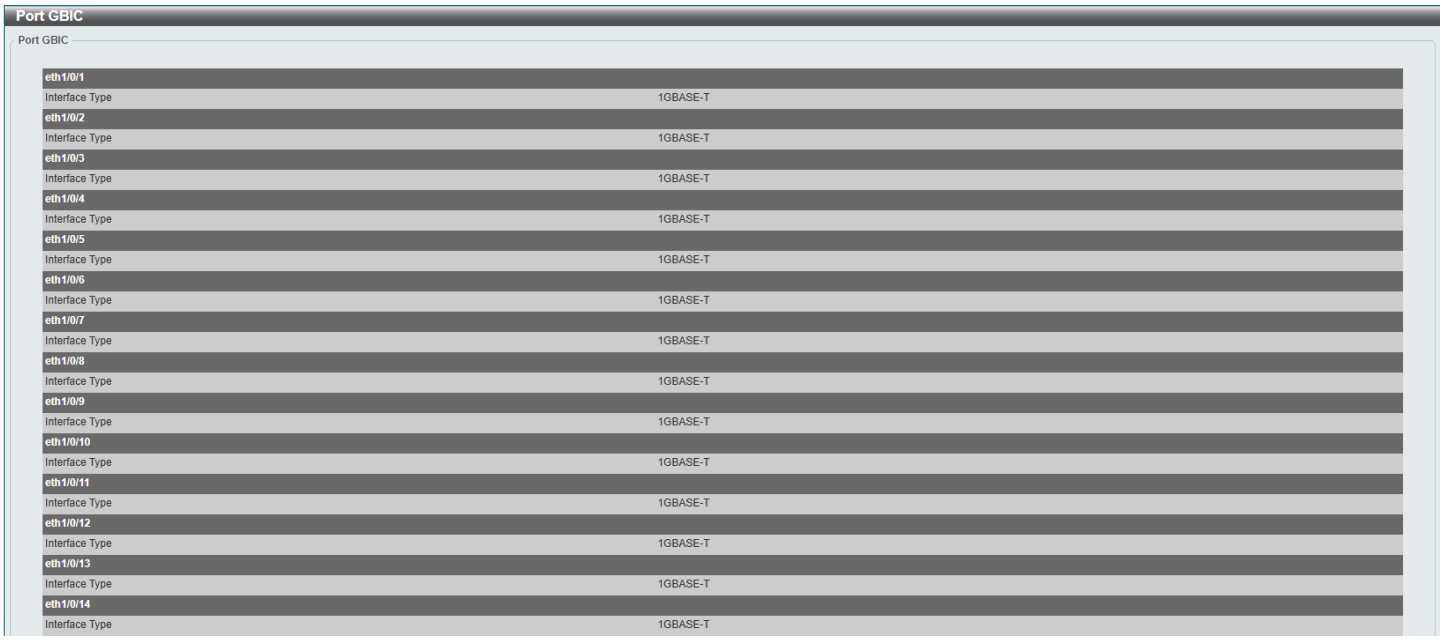
Port Status

Port	Status	MAC Address	VLAN	Flow Control Operator		Duplex	Speed	Type
				Send	Receive			
eth1/0/1	Connected	88-76-B9-AA-49-38	1	Off	Off	Auto-Full	Auto-1G	1GBASE-T
eth1/0/2	Not-Connected	88-76-B9-AA-49-39	1	Off	Off	Auto	Auto	1GBASE-T
eth1/0/3	Not-Connected	88-76-B9-AA-49-3A	1	Off	Off	Auto	Auto	1GBASE-T
eth1/0/4	Not-Connected	88-76-B9-AA-49-3B	1	Off	Off	Auto	Auto	1GBASE-T
eth1/0/5	Not-Connected	88-76-B9-AA-49-3C	1	Off	Off	Auto	Auto	1GBASE-T
eth1/0/6	Not-Connected	88-76-B9-AA-49-3D	1	Off	Off	Auto	Auto	1GBASE-T
eth1/0/7	Not-Connected	88-76-B9-AA-49-3E	1	Off	Off	Auto	Auto	1GBASE-T
eth1/0/8	Not-Connected	88-76-B9-AA-49-3F	1	Off	Off	Auto	Auto	1GBASE-T
eth1/0/9	Not-Connected	88-76-B9-AA-49-40	1	Off	Off	Auto	Auto	1GBASE-T
eth1/0/10	Not-Connected	88-76-B9-AA-49-41	1	Off	Off	Auto	Auto	1GBASE-T
eth1/0/11	Not-Connected	88-76-B9-AA-49-42	1	Off	Off	Auto	Auto	1GBASE-T
eth1/0/12	Not-Connected	88-76-B9-AA-49-43	1	Off	Off	Auto	Auto	1GBASE-T
eth1/0/13	Not-Connected	88-76-B9-AA-49-44	1	Off	Off	Auto	Auto	1GBASE-T
eth1/0/14	Not-Connected	88-76-B9-AA-49-45	1	Off	Off	Auto	Auto	1GBASE-T
eth1/0/15	Not-Connected	88-76-B9-AA-49-46	1	Off	Off	Auto	Auto	1GBASE-T
eth1/0/16	Not-Connected	88-76-B9-AA-49-47	1	Off	Off	Auto	Auto	1GBASE-T
eth1/0/17	Not-Connected	88-76-B9-AA-49-48	1	Off	Off	Auto	Auto	1GBASE-T
eth1/0/18	Not-Connected	88-76-B9-AA-49-49	1	Off	Off	Auto	Auto	1GBASE-T
eth1/0/19	Not-Connected	88-76-B9-AA-49-4A	1	Off	Off	Auto	Auto	1GBASE-T
eth1/0/20	Not-Connected	88-76-B9-AA-49-4B	1	Off	Off	Auto	Auto	1GBASE-T
eth1/0/21	Not-Connected	88-76-B9-AA-49-4C	1	Off	Off	Auto	Auto	1GBASE-T
eth1/0/22	Not-Connected	88-76-B9-AA-49-4D	1	Off	Off	Auto	Auto	1GBASE-T
eth1/0/23	Not-Connected	88-76-B9-AA-49-4E	1	Off	Off	Auto	Auto	1GBASE-T
eth1/0/24	Connected	88-76-B9-AA-49-4F	1	Off	Off	Auto-Full	Auto-1G	1GBASE-T

System > Port Configuration > Port Status

System > Port Configuration > Port GBIC

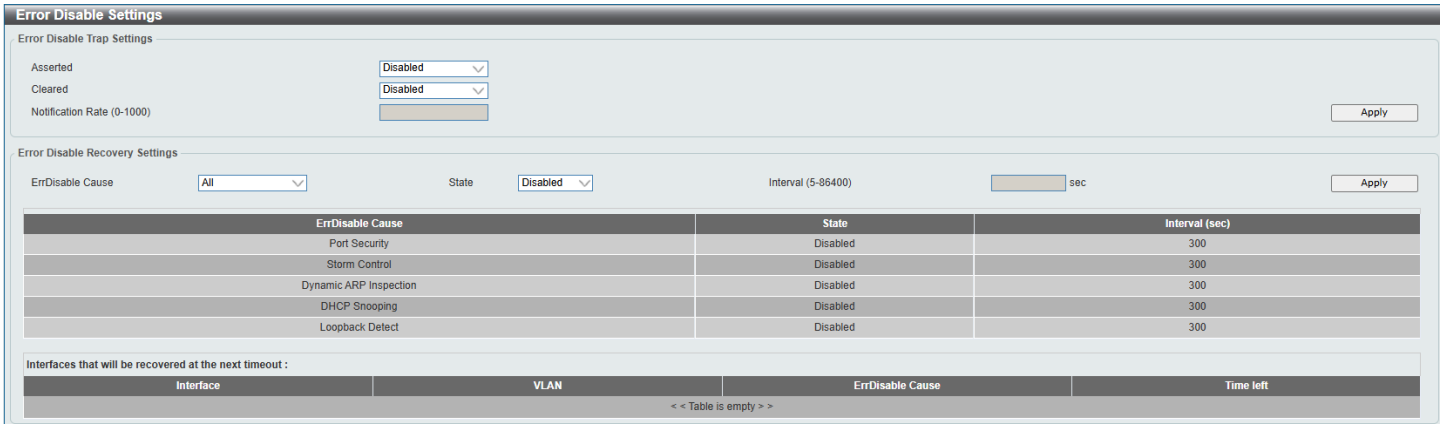
The Port Settings page allows you to view the Switch's physical port interface type.



System > Port Configuration > Port GBIC

System > Port Configuration > Error Disable Settings

The Error Disable Settings page allows you to configure the sending of SNMP notifications for error disable state.



System > Port Configuration > Error Disable Settings

Error Disable Trap Settings:
Asserted: Select to enable or disable the notifications when entering into the error disabled state.
Cleared: Select to enable or disable the notifications when exiting from the error disabled state.
Notification Rate (0-1000): Enter the number of traps per minute. The packets that exceed the rate will be dropped. The value is between 0 and 1000.

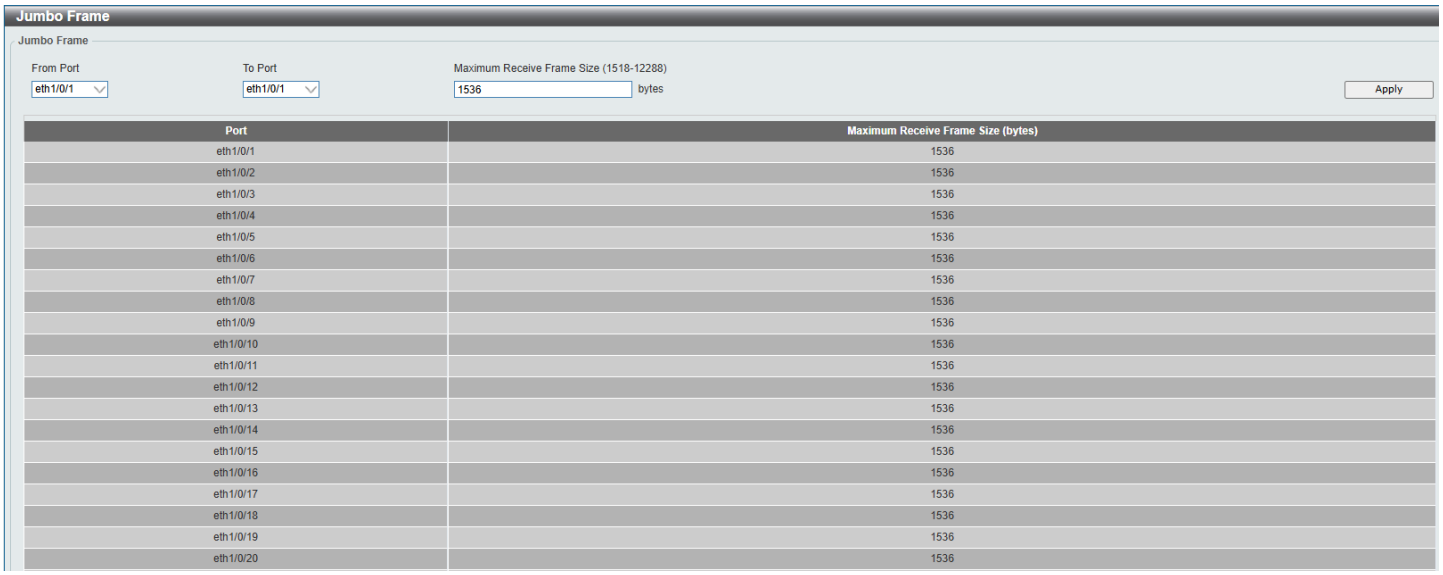
Click the **Apply** button to save your settings.

Error Disable Recovery Settings:
ErrDisable Cause: Specify the error disable causes. Options to choose from are **All**, **Port Security**, **Storm Control**, **Dynamic ARP Inspection, DHCP Snooping** and **Loopback Detect.**
State: Select to enable or disable the auto-recovery for an error port caused by the specified cause.
Interval (5-86400): Enter the time interval. The values are between 5 and 86400 seconds.

Click the **Apply** button to save your settings.

System > Port Configuration > Jumbo Frame

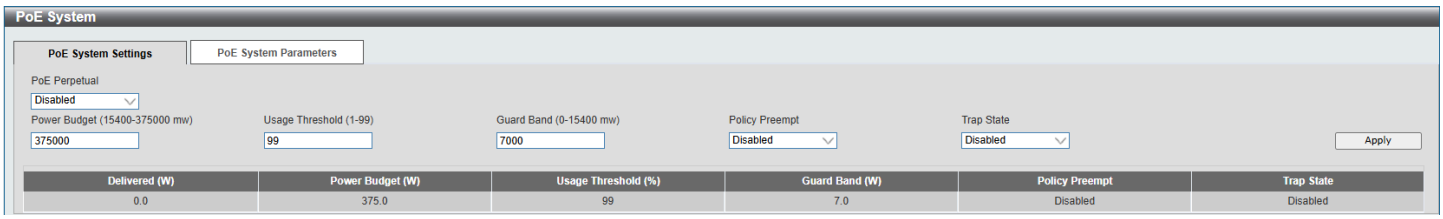
The Jumbo Frame page allows you to view and configure the Jumbo Frame size and settings. Jumbo frames are Ethernet frames with more than 1518 bytes of payload. The Switch supports jumbo frames with a maximum frame size of up to 12288 bytes. (Default 1536 bytes)



System > Port Configuration > Jumbo Frame

System > PoE > PoE System

The PoE System page allows you to view and configure system PoE settings.



System > PoE > PoE System Settings



System > PoE > PoE System Parameters

PoE System Settings:

PoE Perpetual: Select to enable or disable the mechanism of uninterrupted power to PD even which switch is in booting process.

Power Budget (15400-375000 mw): Configure the total PoE power budget of this switch. Default value is 240000 mW.

Usage Threshold (1-99): Configure the total power usage threshold to send SNMP traps. Range from 1~99 in percentage rate.

Guard Band (0-15400 mw): Configurable value for PoE guard band. This specific amount of reserved power helps to protect sudden spike of PD power usage. (Default 7000 mW)

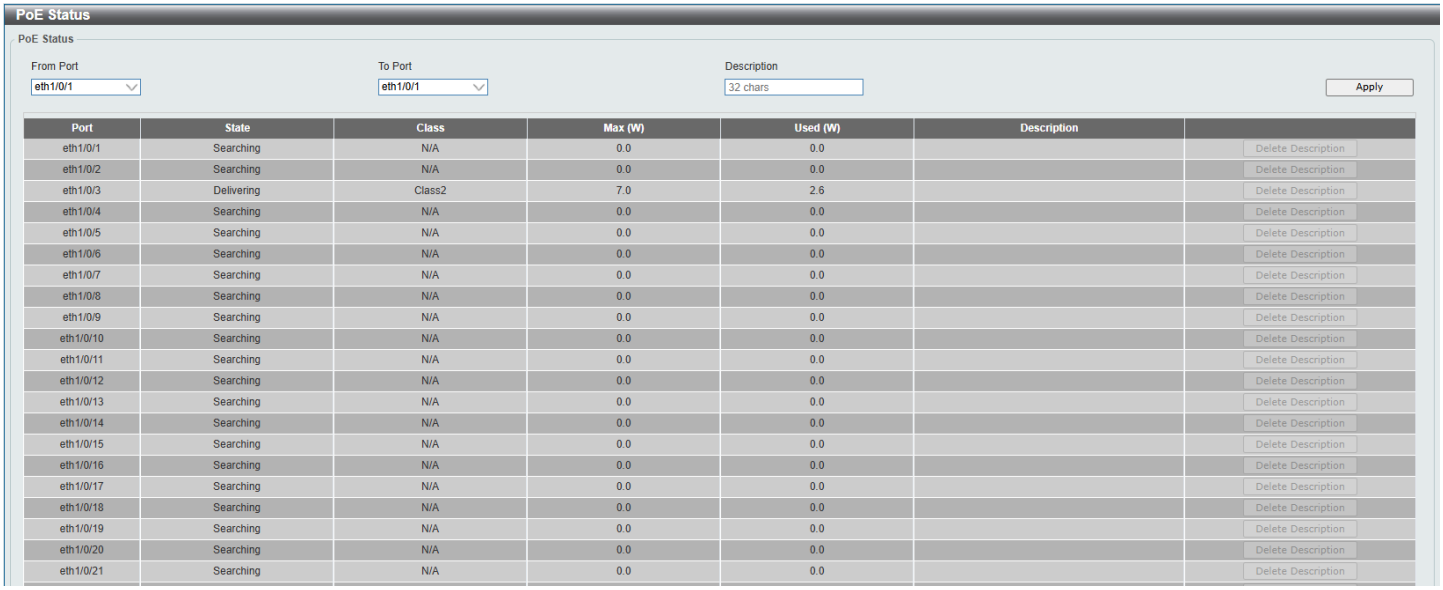
Policy Preempt: Select **Enable** or **Disable** to apply the preemption policy of PoE function. (Default Disable)

Trap State: Select **Enable** or **Disable** to send SNMP traps for PoE events. (Default Disable)

Click the **Apply** button to save your settings.

System > PoE > PoE Status

The PoE Status page display current PoE status on interfaces.



System > PoE > PoE Status

Ports: List of interfaces that supports PoE.

State: Current state of interface. States: Disabled, Searching, Requesting, Delivering, Time-based Off, Failure (Failure event listed)

Class: Current PD class classification. This switch compliant with IEEE 802.3af/802.3at PoE standard which supports 5 classes (Class0~Class4).

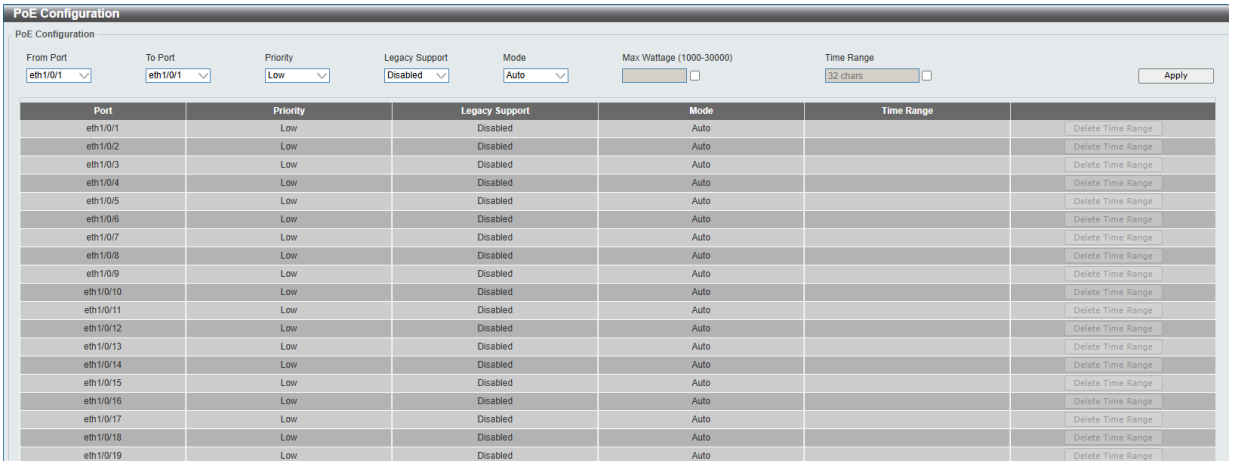
Max (W): Display the Max power based on classification.

Used (W): Display the current power usage on the interface.

Description: Display the description string configured.

System > PoE > PoE Configuration

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



System > PoE > PoE Configuration

From Port - To Port: Select the appropriate port range used for the configuration here.

Priority: Select the priority for provisioning power to the port. Options to choose from are Critical, High and Low.

Legacy Support: Select this option to enable or disable the support of legacy PD.

Mode: Select the power management mode for the PoE ports. Options to choose from are **Auto** and **Never**.

Max Wattage: When selecting **Auto** in the Mode drop-down list, this option appears. Tick the check box and enter the maximum wattage of power that can be provisioned to the auto-detected PD. If the value is not entered, the class of the PD automatically determines the maximum wattage which can be provisioned. The valid range for maximum wattage is between 1000 mW and 30000 mW

Time Range: Display the current power usage on the interface.

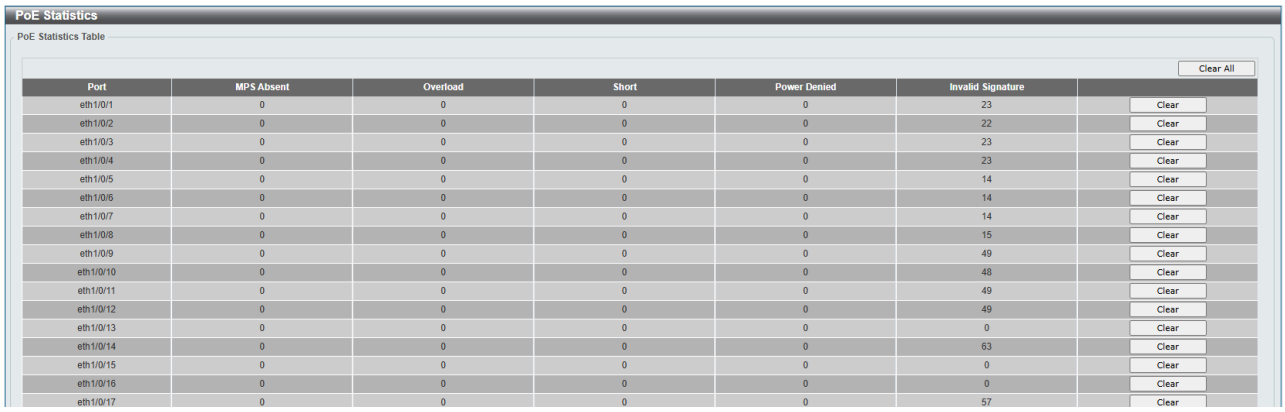
Description: Display the description string configured.

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

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

System > PoE > PoE Statistics

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



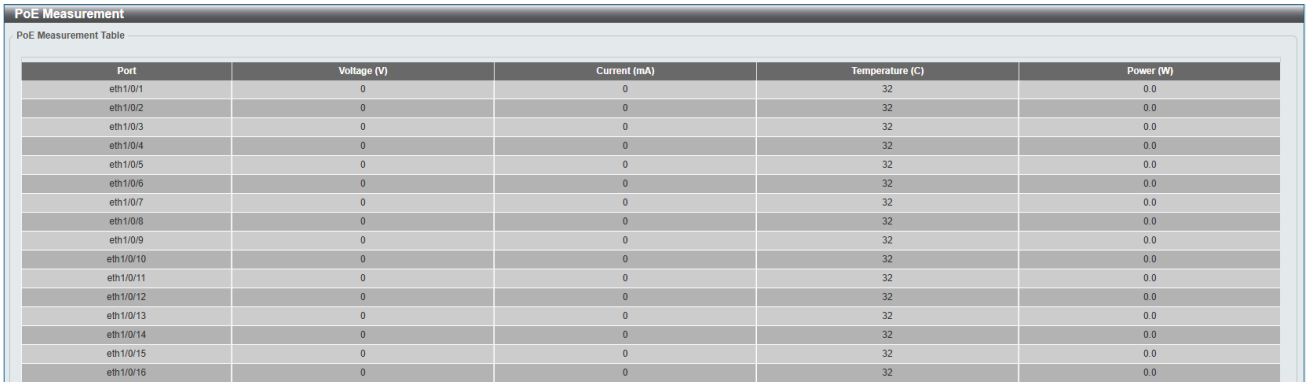
System > PoE > PoE Statistics

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.

System > PoE > PoE Measurement

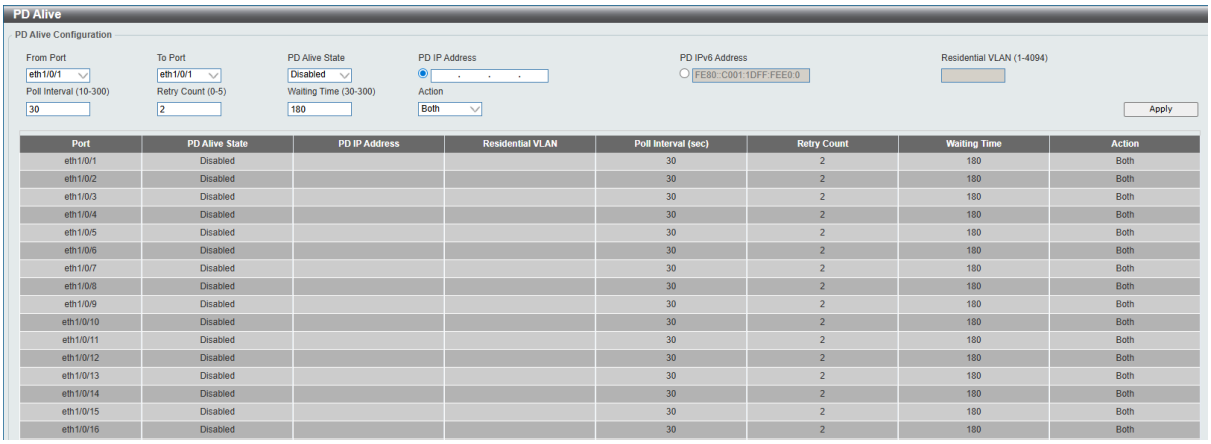
This page is used to display and clear the PoE statistics on the Switch ports.



System > PoE > PoE Measurement

System > PoE > PD Alive

This page 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.



System > PoE > PD Alive

From Port - To Port: Select the appropriate port range used for the configuration here.

PD Alive State: Select to enable or disable the state of the PoE alive function on the specified port(s) here.

PD IP Address: Enter the IPv4 address of the target PD here.

PD IPv6 Address: Enter the IPv6 address of the target PD here.

Residential VLAN (1-4094): Enter VLAN ID for **IPv6 link-local** destination.

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.

System > System Log > System Log Settings

The System Log Settings page allows you to view and configure the system's log settings.



System > System Log > System Log Settings

Global State:

Source Interface State: Select to enable or disable the source interface's global state.

Type: Select the type of interface that will be used. The default option is **VLAN**.

VID (1-4094): Specifies the VLAN ID. The possible range is *1 – 4094*.

Click the **Apply** button to save your settings.

Buffer Log Settings:

Buffer Log State: Select to enable or disable the buffer log state.

Severity: Select the severity value of the type of information that will be logged. The values are 0 (Emergencies), **1 (Alerts)**, **2 (Critical)**, **3 (Errors)**, **4 (Warnings)**, **5 (Notifications)**, **6 (Informational)**, and **7 (Debugging)**.

Write Delay (0-65535): Enter the interval for periodic writing of the logging buffer to flash. The value is between 0 and 65535 seconds. And default is 300 seconds. Tick the Infinite option, to disable the write delay feature.

Click the **Apply** button to save your settings.

System > System Log > System Log Server Settings

The System Log Server Settings page allows you to view and configure the system log's server settings.



System > System Log > System Log Server Settings

IP Address: Select and enter the IPv4 address or IPv6 Address.

UDP Port (514 or 1024-65535): Enter the system log server's UDP port number. This value must be 514 or between 1024 and 65535. The default value is 514.

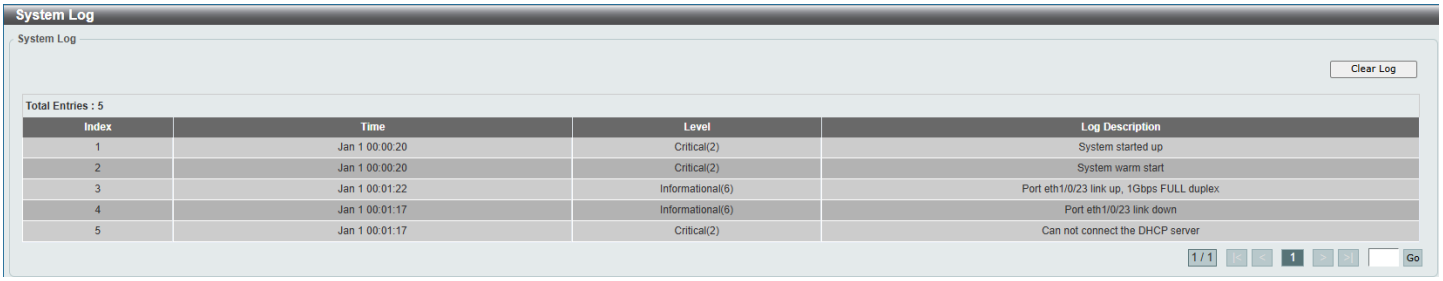
Severity: Select the severity value of the type of information that will be logged. Options to choose from are **0 (Emergencies)**, **1 (Alerts)**, **2 (Critical)**, **3 (Errors)**, **4 (Warnings)**, **5 (Notifications)**, **6 (Informational)**, and **7 (Debugging)**.

Facility: Select the facility value. The values must be between 0 and 23.

Click the **Apply** button to save your settings and click the **Delete** button to remove the entry.

System > System Log > System Log

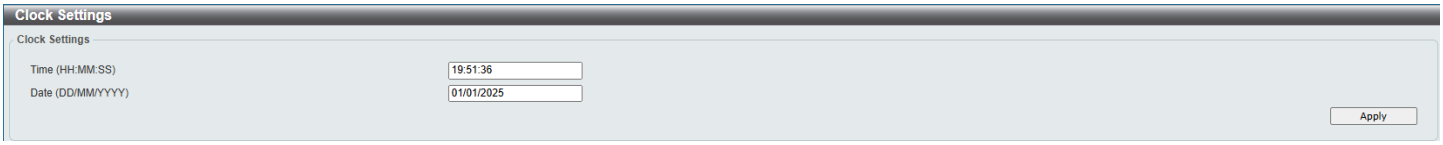
The System Log page displays the system logs on the Switch.



System > System Log > System Log

System > Time and SNTP > Clock Settings

The Clock Settings page allows you to configure the time settings for the Switch.



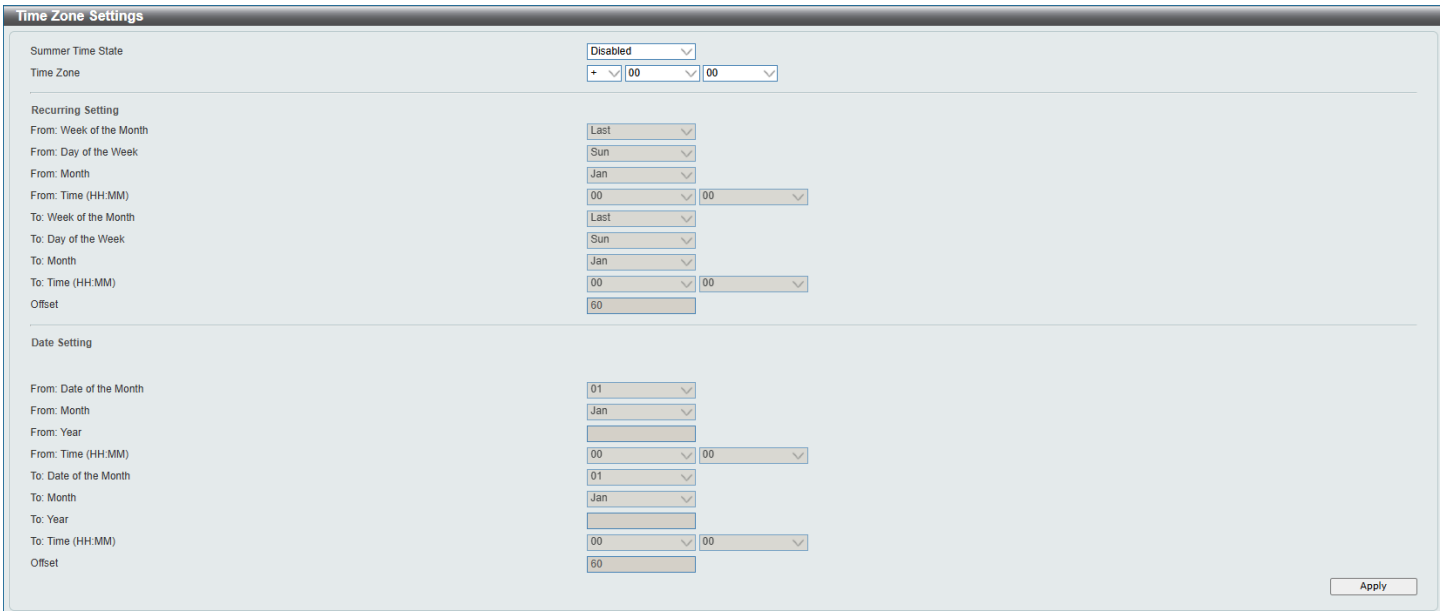
System > Time and SNTP > Clock Settings

Time (HH:MM:SS): Enter the current time in hours, minutes, and seconds.
Data (DD/MM/YYYY): Enter the current day, month, and year to update the system clock.

Click the **Apply** button to save your settings.

System > Time and SNTP > Time Zone Settings

The Time Zone Settings page allows you to configure time zones and Daylight Saving Time settings for SNTP.



System > Time and SNTP > Time Zone Settings

Summer Time State: Select **Summer Time State** setting. Options to choose from are **Disabled**, **Recurring Setting**, and **Date Setting**.

Time Zone: Select the local time zone's offset from Coordinated Universal Time (UTC).

The **Recurring Setting** can be configured below:

From: Week of the Month – Select week of the month that daylight saving time will start.

From: Day of the Week - Select day of the week that daylight saving time will start.

From: Month – Select the month that daylight time will start.

From: Time in HH MM – Select the time of the day that daylight saving time will start.

To: Week of the Month – Select week of the month that daylight saving time will end.

To: Day of the Week – Specify day of the week that daylight saving time will end.

To: Month – Select the month that daylight saving time will end.

To: Time In HH MM – Select the time of the day that daylight saving time will end.

Offset – Enter the number of minutes to add during daylight saving time. The default value is 60. The range of this offset is 30, 60, 90 and 120.

The **Date Setting** can be configured below:

From: Date of the Month – Select date of the month that daylight saving time will start.

From: Month – Select the month that daylight saving time will start.

From: Year – Select the year that the daylight saving time will start.

From: Time In HH MM – Select the time of the day that daylight saving time will start.

To: Date of the Month – Select the date of the month that daylight saving time will end.

To: Month – Select the month that daylight saving time will end.

To: Year – Select the year that the daylight saving time will end.

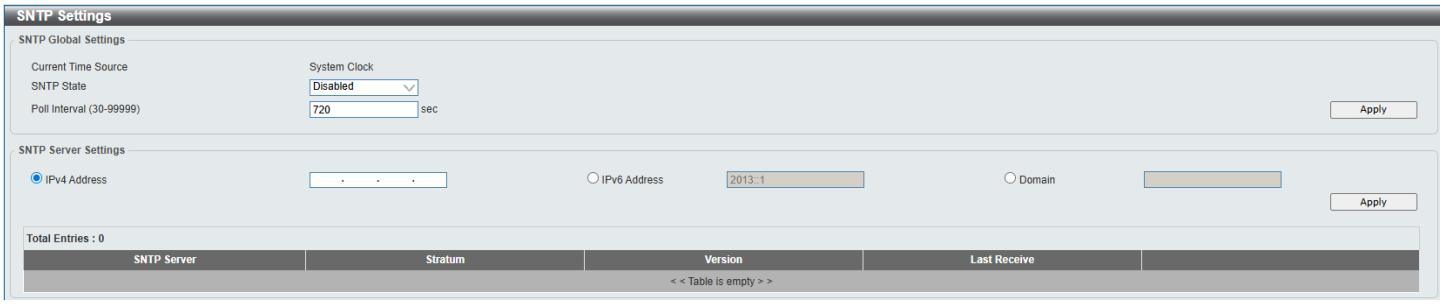
To: Time In HH MM – Select the time of the day that daylight time will end.

Offset – Select the number of minutes to add during daylight saving time. The default value is 60. The range of this offset is 30, 60, 90 and 120.

Click the **Apply** button to save your settings.

System > Time and SNTP > SNTP Settings

The SNTP Settings page allows you to configure the time settings for the Switch.



System > Time and SNTP > SNTP Settings

SNTP Global Settings:

SNTP State: Select to enable or disable the SNTP state.

Poll Interval (30-99999): Enter the poll interval. The value is from 30 to 99999 seconds. The default interval is 720 seconds.

Click the **Apply** button to save your settings.

SNTP Server Setting:

IPv4 Address: Enter the IPv4 address of the SNTP server which provides the clock synchronization.

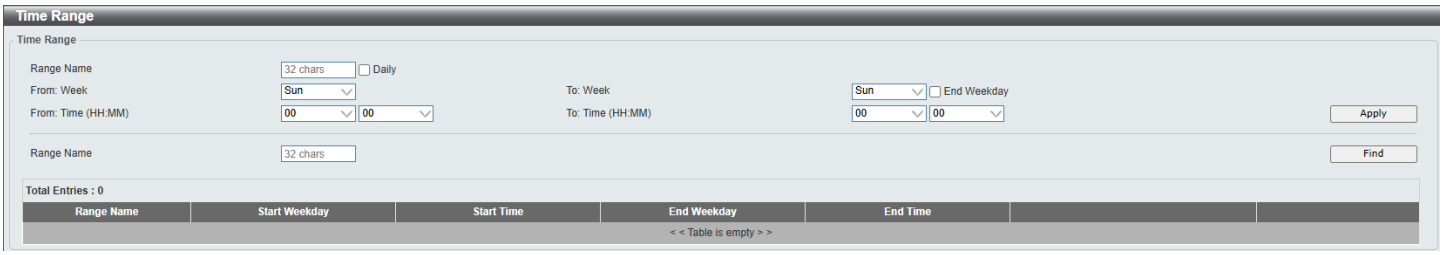
IPv6 Address: Enter the IPv6 address of the SNTP server which provides the clock synchronization.

Domain: Enter SNTP Server domain name which provides the clock synchronization.

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

System > Time Range

The Time Range page allows you to view and configure the time range settings for the Switch.



System > Time Range

Range Name: Enter a name for the time range. The name can be up to 32 characters long.

From Week / To Week: Select the starting and ending days of the week that will be used for this time range. Tick the **Daily** option to use this time range for every day of the week. Tick the **End Week Day** option to use this time range from the starting day of the week until the end of the week, which is Sunday.

From Time (HH:MM) / To Time (HH:MM): Select the starting and ending time of the day that will be used for this time range. The first drop-down menu selects the hour and the second drop-down menu selects the minute.

Click the **Apply** button to save your settings.

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

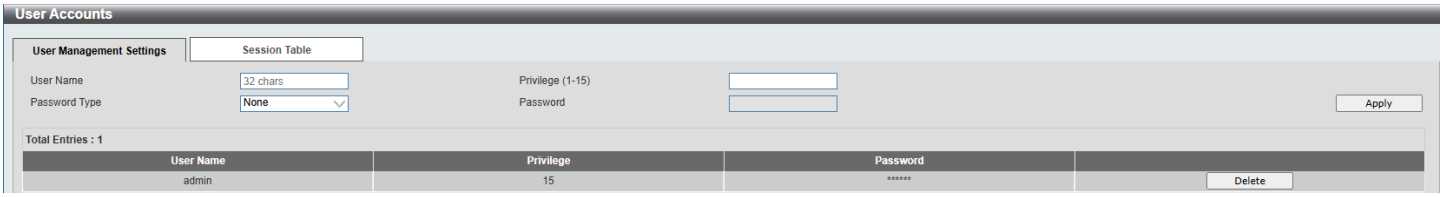
Management > User Accounts Settings

The User Accounts Settings page allows you to create and configure user accounts. Active user account sessions can be viewed. By default, there is no user account created on the Switch.

The pre-defined user account privilege levels supported by this switch are:

- Basic User – Privilege Level 1. This user account level has the lowest priority of the user accounts. The purpose of this type of user account level is for basic system checking.
- Operator – Privilege Level 12. This user account level is used to grant system configuration information for users who need to change or monitor system configuration, except for security related information such as user accounts and SNMP account settings.

- Administrator – Privilege Level 15. This administrator user account level can monitor all system information and change any of the system configuration settings expressed in this guide.



Management > User Accounts Settings

User Name: Enter the name of the user name. The name can be up to 32 characters long.
Privilege (1-15): Select the privilege level for this account. The value is between 1 and 15.

Radius assign D-Link User-Level mapping DGS-1250 series User-Level info:

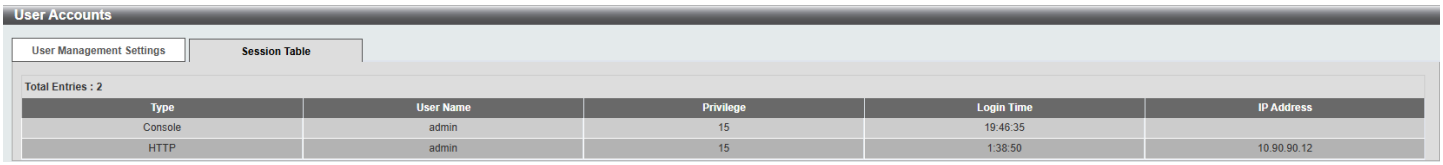
Privilege shown in RADIUS server	Privilege used in switch FW	User Level
3	1	User
4	12	Operator
5	15	Administrator

Password Type: Select a password type for this user account. The options are **None**, **Plain Text**, and **Encrypted**.
Password: If you selected either **Plain Text** or **Encrypted** for the password type, please enter a password for this user account.

Password rules:
1. Password: 8 – 30 UTF-8 characters (Unicode hex range 0x0021 - 0x007e).
2. MUST contains at least one alphabet upper and lower case.
3. MUST contains at least one digit.
4. MUST contains at least one special symbol.
5. MUST NOT as same as user name.
6. MUST be non-consecutive characters.
7. MUST NOT include default login account & default IP address.

Click the **Apply** button to save your settings.
Click the **Delete** button to remove the specified user account entry.

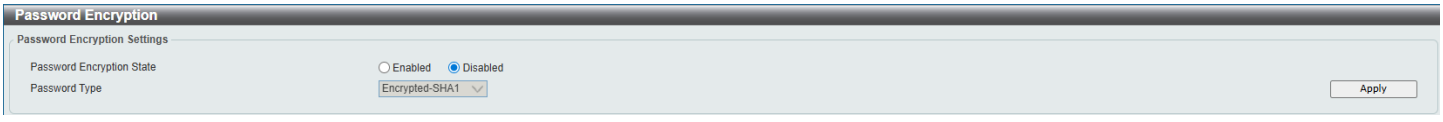
After clicking the **Session Table** tab, the following page will appear:



Management > User Accounts Settings – Session Table

Management > Password Encryption

The Password Encryption page allows you to enable or disable password encryption.



Management > Password Encryption

Password Encryption State: Specify to enable or disable the password encryption.
Password Type: Specify the password encryption type to Encrypted-SHA1 or Encrypted-MD5.

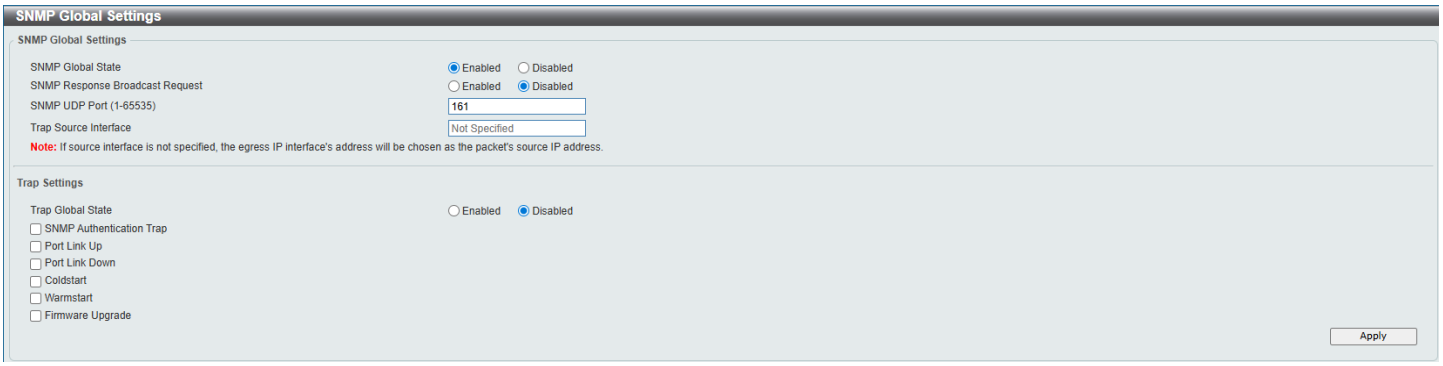
Click the **Apply** button to save your settings.

Management > SNMP > SNMP Global Settings

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) protocol designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems on the Switch or your local 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 default SNMP global state is disabled. Select **Enable** and then select **Trap Settings**. Click **Apply** to enable the SNMP function.



Management > SNMP > SNMP Global Settings

SNMP Global Settings:

SNMP Global State: Select to enable or disable the SNMP feature.

SNMP Response Broadcast Request: Select to enable or disable the server to response to broadcast SNMP GetRequest packets.

SNMP UDP Port (0-65535): Enter the SNMP UDP port number. The value is between 0 and 65535.

Trap Source Interface: Specify the interface whose IP address will be used as the source address for sending the SNMP trap packet.

Trap Settings:

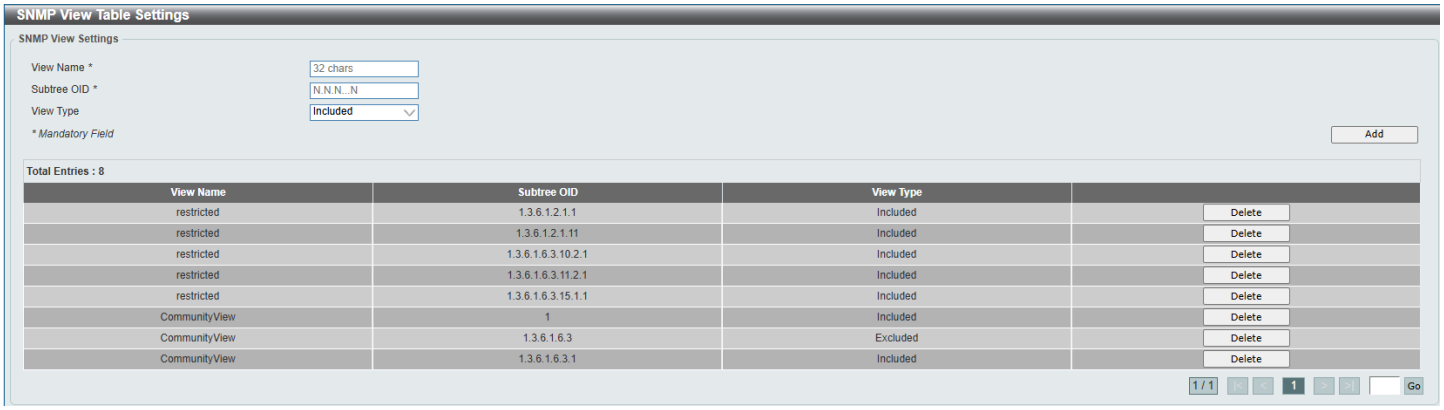
Trap Global State: Select to enable or disable the sending of all or specific SNMP notifications.

SNMP Authentication Trap: Tick this option to control the sending of SNMP authentication failure notifications. An authenticationFailuretrap is generated when the device receives an SNMP message that is not properly authenticated. The authentication method depends on the version of SNMP being used. For SNMPv1 or SNMPv2c, authentication failure occurs if packets are formed with an incorrect community string. For SNMPv3, authentication failure occurs if packets are formed with an incorrect SHA/MD5 authentication key.
Port Link Up: Tick this option to control the port link up notifications.
Port Link Down: Tick this option to control the port link down notifications.
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 save your settings.

Management > SNMP > SNMP View Table Settings

The SNMP View page allows you to define SNMP Views, which can be used to manage the MIB objects that are accessible to a remote SNMP manager.



Management > SNMP > SNMP View Table Settings

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

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

View Type: Select the OIDs that can accessed by a SNMP manager.

Click **Add** to create a new view or **Delete** to remove an existing view.

Management > SNMP > SNMP Community Table Settings

The SNMP Community page allows you to set the SNMP community string of the Switch. SNMP managers using the same community string are permitted access to the Switch's SNMP agent.



Management > SNMP > SNMP Community Table Settings

Key Type: Select the key type for the SNMP community. Select either **Plain Text** or **Encrypted**.

Community Name: Select 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 access to on the Switch. The view name must exist in the SNMP View Table.

Access Right: Select the user's access rights from the drop-down menu:

Read Only - SNMP community members can read the contents of the MIBs on the Switch.

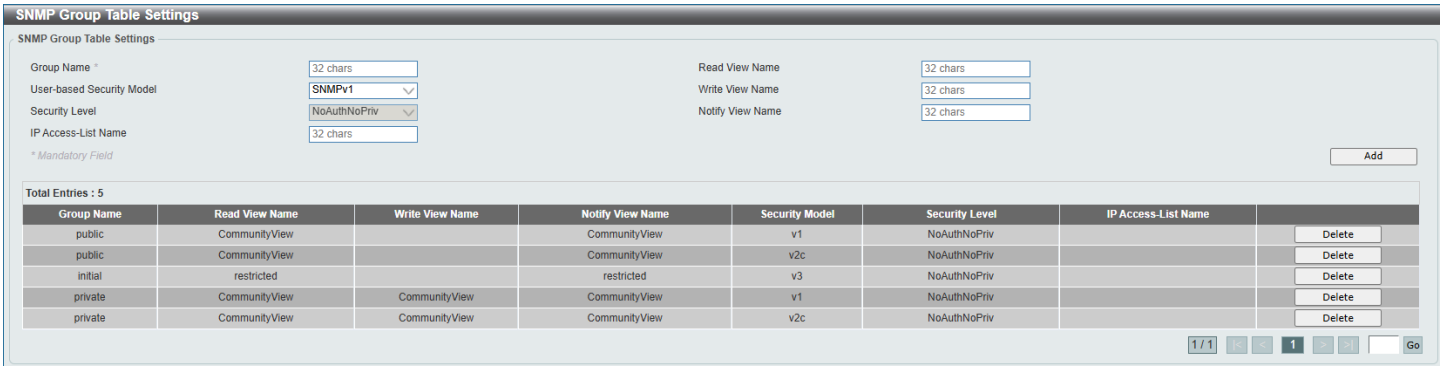
Read Write - SNMP community members can read and write the contents of the MIBs on the Switch.

IP Access-List Name: Enter the name of the standard access list to control access to the SNMP agent using this community string.

Click **Add** to a new entry based on the information entered or **Delete** to remove the specified entry.

Management > SNMP > SNMP Group Table Settings

The SNMP Group page allows you to manage SNMP Groups. Access to SNMP OIDs and security policies can be controlled on a per group basis.



Management > SNMP > SNMP Group Table Settings

Group Name: Enter a SNMP group name of up to 32 characters.

User-based Security Model: Select the SNMP security model.

SNMPv1 - SNMPv1 does not support any security features.

SNMPv2c - SNMPv2 supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.

SNMPv3 - SNMPv3 provides secure access to devices through a combination of authentication and encryption.

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

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

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

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

IP Address-List Name:

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

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

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

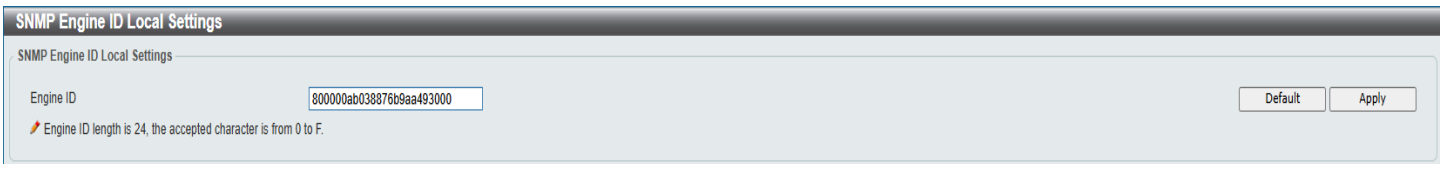
Click the **Add** button to add a new entry based on the information entered.

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

Management > SNMP > SNMP Engine ID Local Settings

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

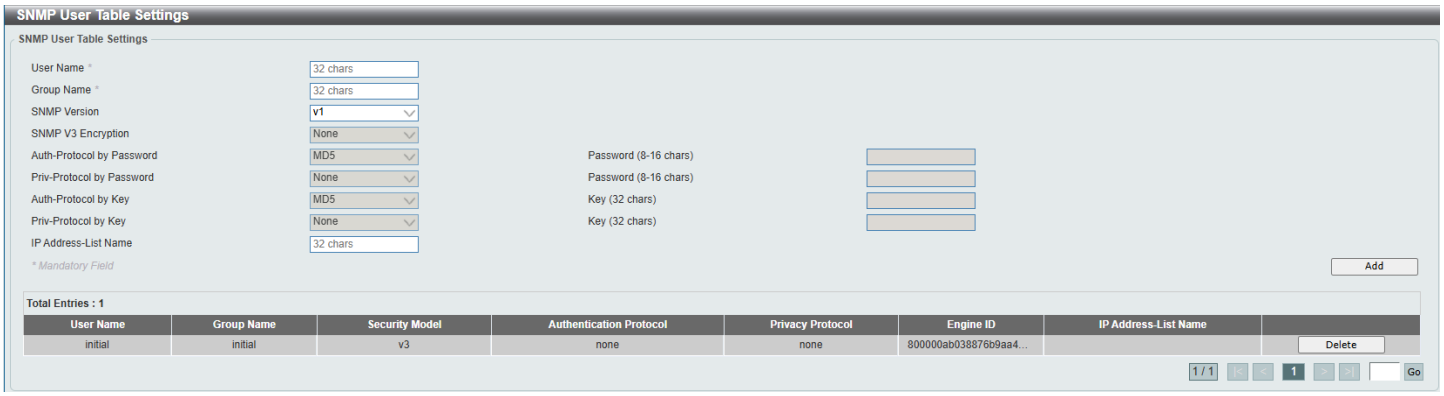
Input the Engine ID then click **Apply** to apply the changes or click **Default** to change back to the default value.



Management > SNMP > SNMP Engine ID Local Settings

Management > SNMP > SNMP User Table Settings

The SNMP User Table Settings page allows you to manage the SNMP users that can access the Switch. It allows you to set the Group, SNMP version, and authentication and encryption type for a user.



Management > SNMP > SNMP User Table Settings

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

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

SNMP Version: Select the SNMP version of the user. The options to choose are **v1**, **v2c** and **v3**.

SNMP V3 Encryption: When selecting **v3** in the **SNMP Version** drop-down list, this option is available. Options to choose from are **None**, **Password**, and **Key**.

Auth-Protocol by Password: Select either **MD5** or **SHA** to be the authentication protocol. Enter a password for SNMPv3 encryption in the right column.

MD5 – Select to use the HMAC-MD5-96 authentication level. This field will require the user to enter a password.

SHA - Select that the HMAC-SHA authentication protocol will be used. This field will require the user to enter a password.

Priv-Protocol by Password: Select either **None** or **DES56** and then enter a password for SNMPv3 encryption in the right column.

None – Select to not use any authorization.

DES56 – Select to use DES 56-bit encryption, based on the CBC-DES (DES-56) standard. This field will require you to enter a password.

Auth-Protocol by Key: Select either **MD5** or **SHA** to be the authentication protocol. Enter a key for SNMPv3 encryption in the right column.

MD5 – Select to use the HMAC-MD5-96 authentication level. This field will require the user to enter a key.

SHA – Select to use the HMAC-SHA authentication protocol. This field will require you to enter a key.

Priv-Protocol by Key: Select either **None** or **DES56** and then enter a password for SNMPv3 encryption in the right column.

None – Select to not use any authorization.

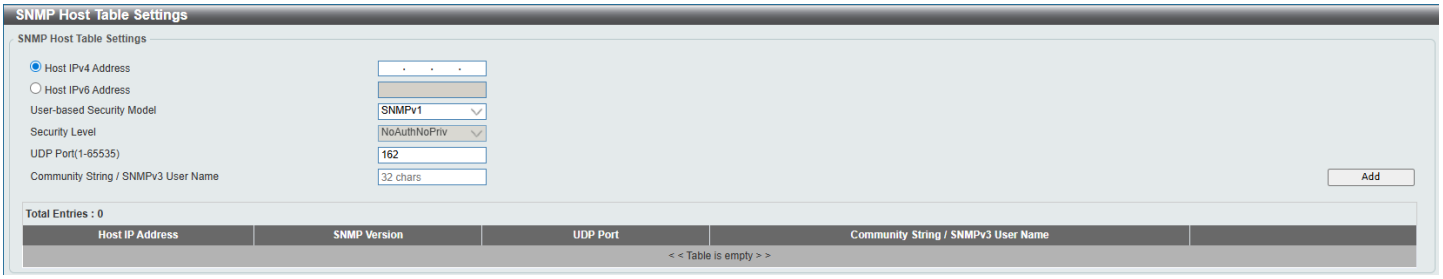
DES56 – Select to use DES 56-bit encryption, based on the CBC-DES (DES-56) standard. This field will require the user to enter a key.

IP Address-List Name: Enter the standard IP Access Control List (ACL) to associate with the user.

Click **Add** to create a new SNMP user account or click **Delete** to remove any existing data.

Management > SNMP > SNMP Host Table Settings

The SNMP Host Table Settings page allows you to configure the SNMP trap recipients.



Management > SNMP > SNMP Host Table Settings

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

User-based Security Model: Specify the SNMP version to be used to the management host. The options are **SNMPv1**, **SNMPv2C** and **SNMPv3**.

Security Level: When selecting **SNMPv3** in the **User-based Security Model** drop-down list, this option is available.

NoAuthNoPriv – Select to have no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.

AuthNoPriv – Select to require authorization, but with no encryption of packets sent between the Switch and a remote SNMP manager.

AuthPriv – Select to require authorization, and packets sent between the Switch and a remote SNMP manger will be encrypted.

UDP Port (0-65535): Enter the UDP port number. The default trap UDP port number is 162. The range of **UDP port numbers is from 0 to 65535.**

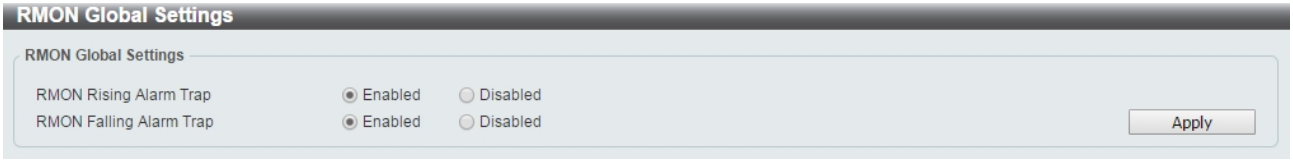
NOTE: Some port numbers may conflict with other protocols.

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

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

Management > RMON > RMON Global Settings

You can enable and disable remote monitoring (RMON) status for the SNMP function on the Switch. In addition, RMON Rising and Falling Alarm Traps can be enabled and disabled.



Management > RMON > RMON Global Settings

Management > RMON > RMON Statistics Settings

The RMON Statistics Settings page displays RMON Ethernet statistics and allows you to configure the settings.



Management > RMON > RMON Statistics Settings

The RMON Ethernet Statistics Configuration contains the following fields:

Port: Select the port from which the RMON information was taken.

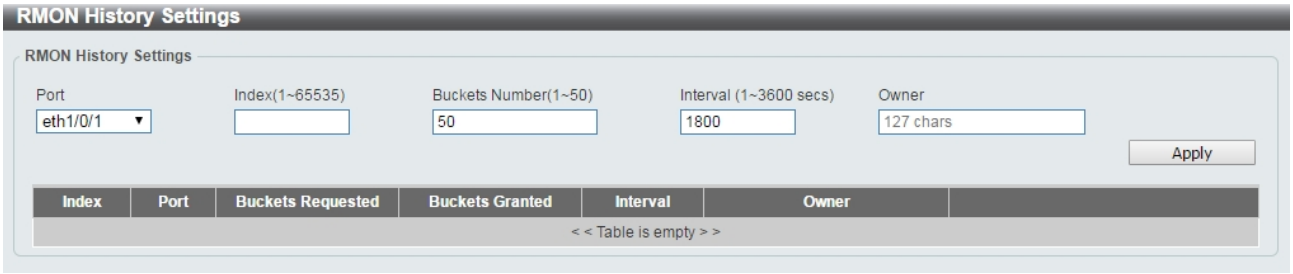
Index (1 - 65535): Indicates the RMON Ethernet Statistics entry number.

Owner: Displays the RMON station or user that requested the RMON information.

Click **Add** to activate your entry or click to renew the details collected and displayed.

Management > RMON > RMON History Settings

The RMON History Settings page contains information about samples of data taken from ports, such as interface definitions or polling periods.



Management > RMON > RMON History Settings

The History Control Configuration contains the following fields:

Port: Select the port from which the RMON information was taken.

Index (1 - 65535): Indicates the history control entry number.

Buckets Number (1 ~ 50): Enter the number of buckets that the device saves.

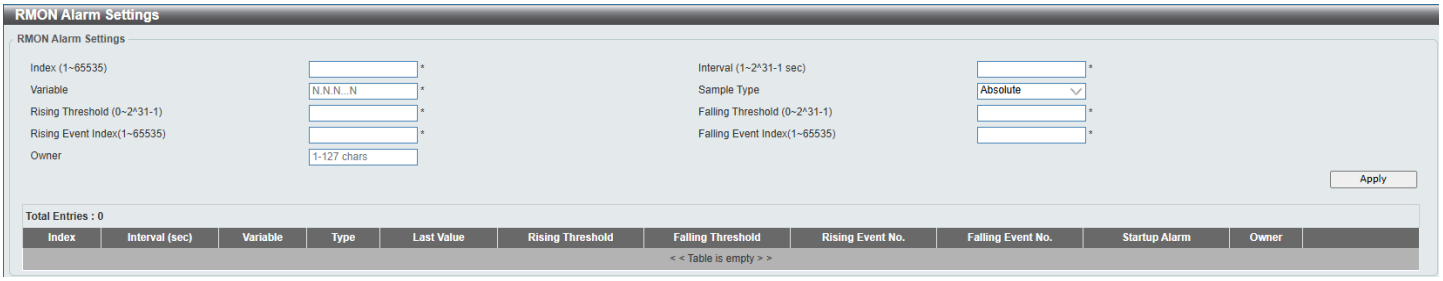
Interval (1 ~ 3600 secs): Indicates in seconds the time period that samplings are taken from the ports. The field range is *1-3600*. The default is *1800* seconds (equal to 30 minutes).

Owner: Displays the RMON station or user that requested the RMON information.

Click **Apply** to activate your entry.

Management > RMON > RMON Alarm Settings

The RMON Alarm Settings page allows you to configure the network alarms. Network alarms occur when a network problem or event is detected.



Management > RMON > RMON Alarm Settings

The configuration contains the following fields:

Index (1 - 65535): Enter a specific alarm.

Variable: Select the selected MIB variable value.

Rising Threshold (0 ~ 2^31-1): Displays the rising counter value that triggers the rising threshold alarm.

Rising Event Index (1 ~ 65535): Displays the event that triggers the specific alarm. The possible field values are user defined RMON events.

Owner: Enter the owner string. The string can be up to 127 characters.

Interval (1 ~ 2^31-1): Defines the alarm interval time in seconds.

Sample type: Defines the sampling method for the selected variable and comparing the value against the thresholds. The possible field values are:

Delta value – Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.

Absolute value – Compares the values directly with the thresholds at the end of the sampling interval.

Falling Threshold (0 ~ 2^31-1): Displays the falling counter value that triggers the falling threshold alarm.

Falling Event Index (1 ~ 65535): Displays the event that triggers the specific alarm. The possible field values are user defined RMON events.

Click **Apply** to activate your alarm entry.

Management > RMON > RMON Event Settings

The RMON Event Settings page contains fields for defining, modifying and viewing RMON event statistics.



Management > RMON > RMON Event Settings

The RMON Events Page contains the following fields:

Index (1~ 65535): Enter the event index.

Description: Enter an event description.

Type: Select the event type. The possible values are:

None – Indicates that no event occurred.

Log – Indicates that the event is a log entry.

SNMP Trap – Indicates that the event is a trap.

Log and Trap – Indicates that the event is both a log entry and a trap.

Community: Enter the community to which the event belongs.

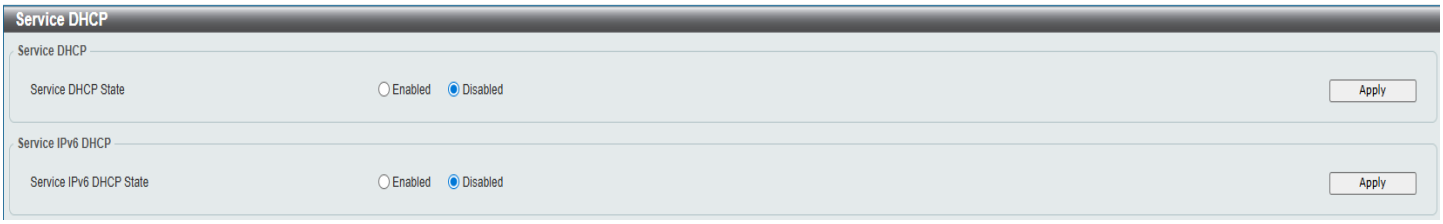
Owner: Enter the time that the event occurred.

Click **Add** to add a new RMON event.

Management > DHCP > Service DHCP

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

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



Management > DHCP > Service DHCP Window

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

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

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

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

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

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

Management > DHCP > 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:



Management > DHCP > DHCP Class Settings Window

The fields that can be configured are described below:

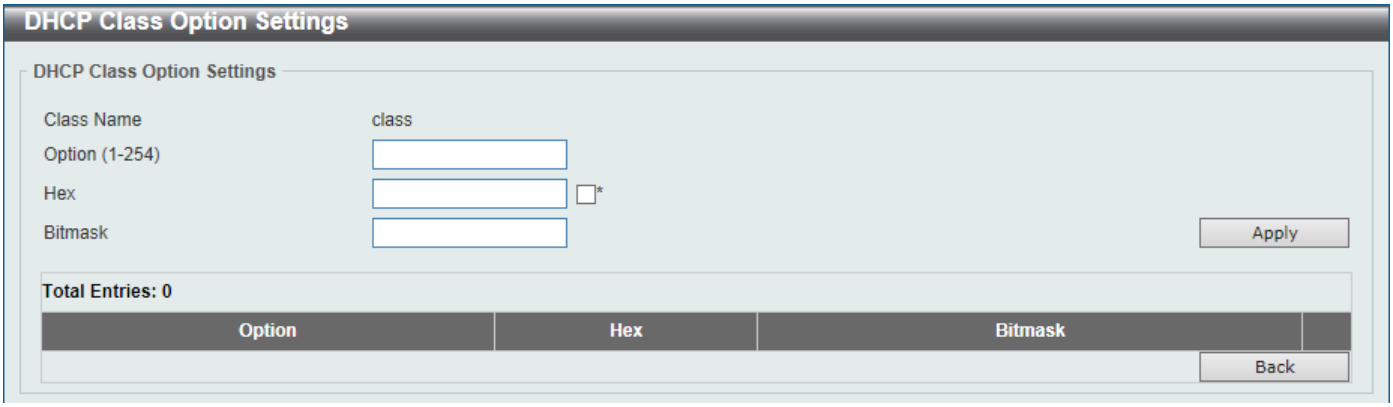
Parameter	Description
Class Name	Enter the DHCP class name with a maximum of 32 characters.

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.



Management > DHCP > DHCP Class Settings (Edit) Window

The fields that can be configured are described below:

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

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

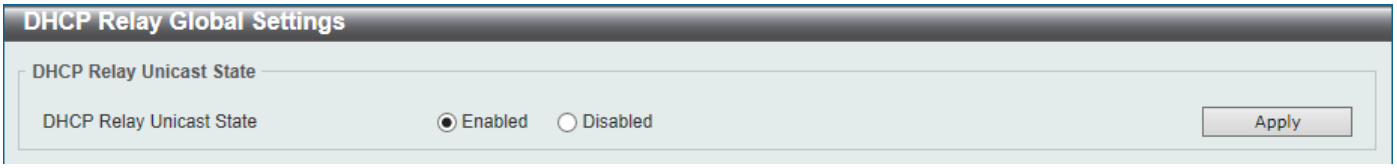
Click the **Delete** button to remove the specified entry.

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

Management > DHCP > DHCP Relay > DHCP Relay Global Settings

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

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



Management > DHCP > DHCP Relay > DHCP Relay Global Settings Window

The fields that can be configured are described below:

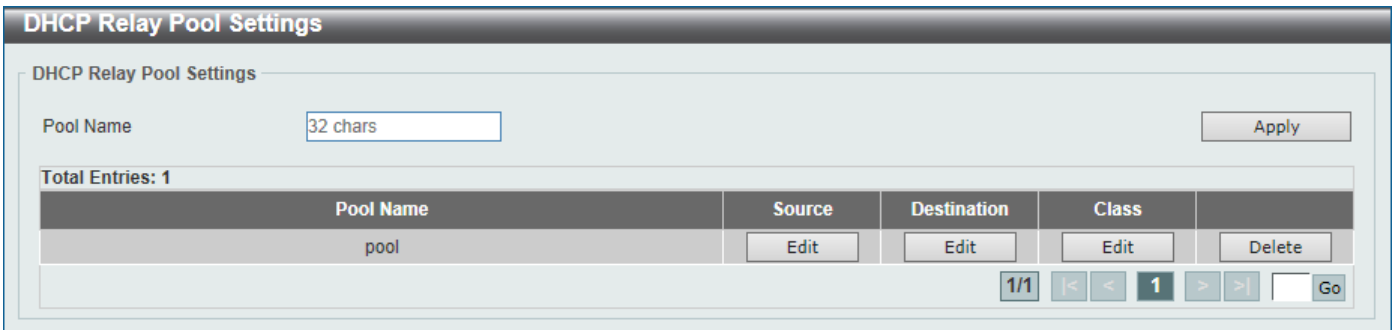
Parameter	Description
DHCP Relay Unicast State	Select to globally enable or disable the DHCP relay unicast state here.

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

Management > DHCP > 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:



Management > DHCP > DHCP Relay > DHCP Relay Pool Settings Window

The fields that can be configured are described below:

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

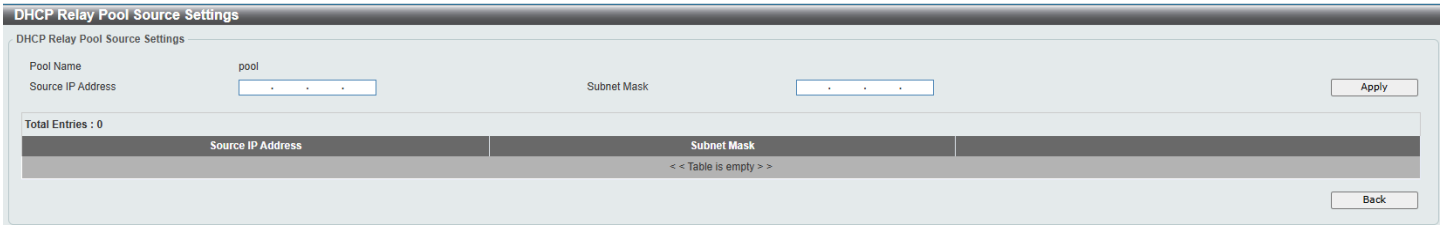
Click the **Apply** button to accept the changes made.

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

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

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

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



Management > DHCP > DHCP Relay > DHCP Relay Pool Source Settings Window

The fields that can be configured are described below:

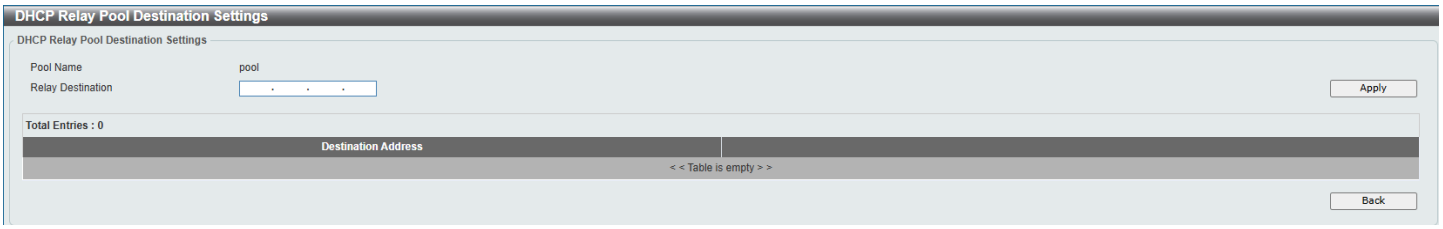
Parameter	Description
Source IP Address	Enter the source subnet of client packets.
Subnet Mask	Enter the network mask of the source subnet.

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.



Management > DHCP > DHCP Relay > DHCP Relay Pool (Destination Edit) Window

The fields that can be configured are described below:

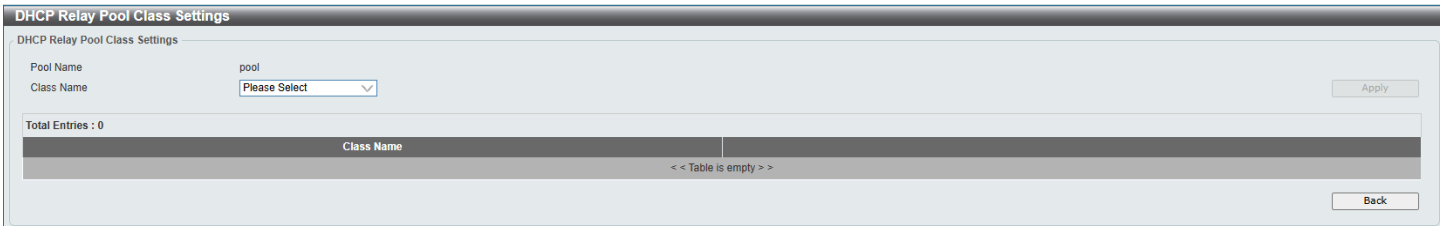
Parameter	Description
Relay Destination	Enter the relay destination DHCP server IP address.

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

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

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

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



Management > DHCP > DHCP Relay > DHCP Relay Pool (Class Edit) Window

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

The fields that can be configured are described below:

Parameter	Description
Class Name	Select the DHCP class name.

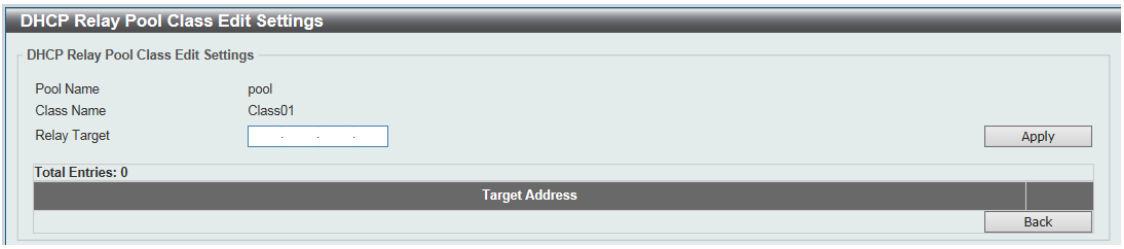
To edit a class, select it then click **Apply** to display its information below.

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

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

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

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



Management > DHCP > DHCP Relay > DHCP Relay Pool (Class Edit, Edit) Window

The fields that can be configured are described below:

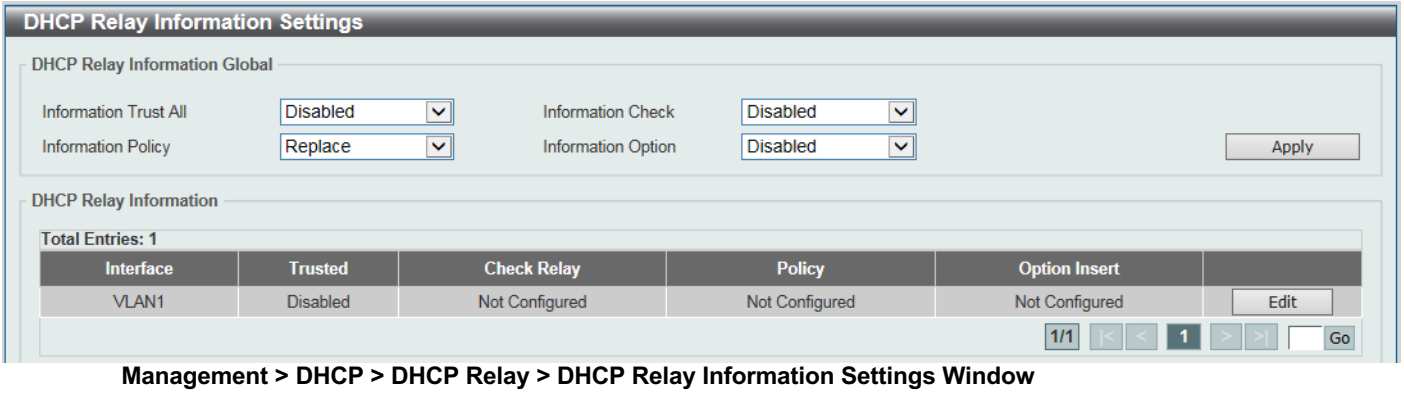
Parameter	Description
Relay Target	Enter the DHCP relay target for relaying packets that matches the value pattern of the option defined in the DHCP class.

Click the **Apply** button to accept the changes made. Click the **Delete** button to remove the specified entry. Click the **Back** button to return to the previous window.

Management > DHCP > DHCP Relay > 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:



Management > DHCP > DHCP Relay > DHCP Relay Information Settings Window

The fields that can be configured are described below:

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

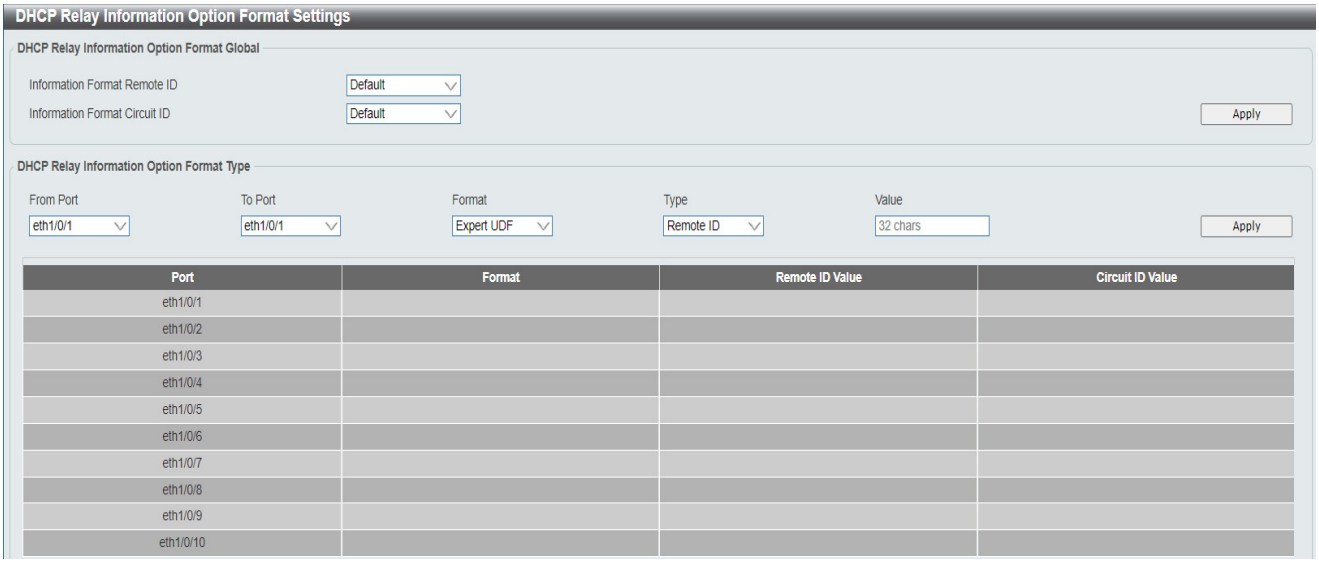
Click the **Edit** button to modify the corresponding interface.

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

Management > DHCP > DHCP Relay > 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:



Management > DHCP > DHCP Relay > DHCP Relay Information Option Format Settings Window

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

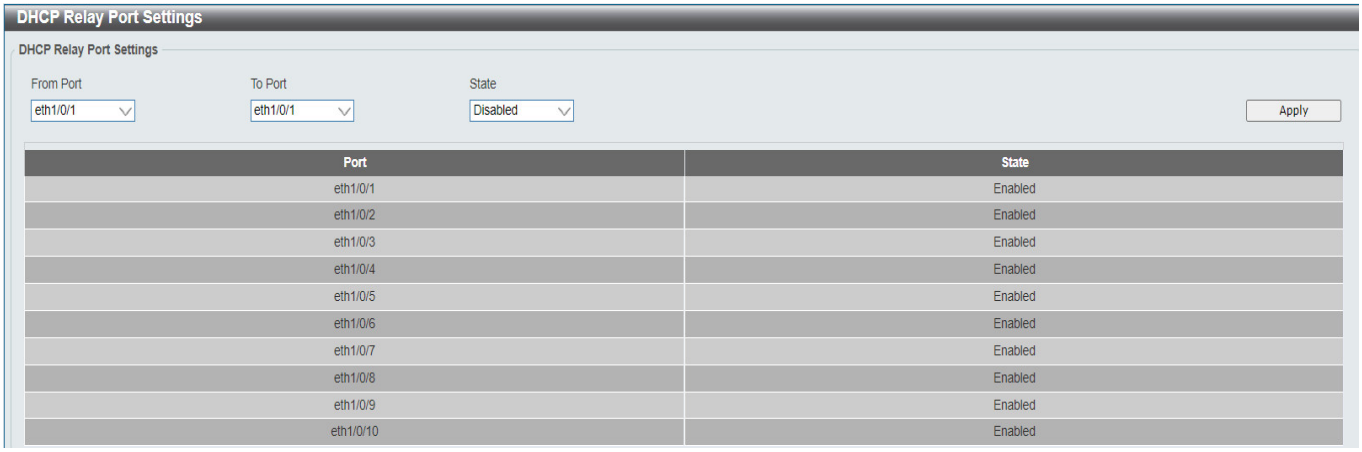
Parameter	Description
Information Format Remote ID	Select the DHCP information remote ID sub-option. Options to choose from are: • **Default** - Select to use the Switch's system MAC address as the remote ID. • **User Define** - Select to use a user-defined remote ID. Enter the user-defined string with the maximum of 32 characters in the text box. • **Vendor2** - Select to use vendor 2 as the remote ID. • **Expert UDF** - Select to use the expert UDF remote ID. Select the stand-alone unit format after this selection here.
Information Format Circuit ID	Select the DHCP information circuit ID sub-option. Options to choose from are: • **Default** - Select to use the default circuit ID sub-option. • **User Define** - Select to use a user-defined circuit ID. Enter the user-defined string with the maximum of 32 characters in the text box. • **Vendor1** - Select to use vendor 1 as the circuit ID. • **Expert UDF** - Select to use the expert UDF circuit ID. Select the stand-alone unit format after this selection here.
From Port - To Port	Select the range of ports that will be used for this configuration here.
Format	Specifies that the expert UDF format will be used.
Type	Select to use the **Remote ID** type or **Circuit ID** type here.
Value	Enter the vendor-defined string for Option 82 information in the remote/circuit ID sub-option here. This string can be up to 32 characters long.

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

Management > DHCP > DHCP Relay > 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:



Management > DHCP > DHCP Relay > DHCP Relay Port Settings Window

The fields that can be configured are described below:

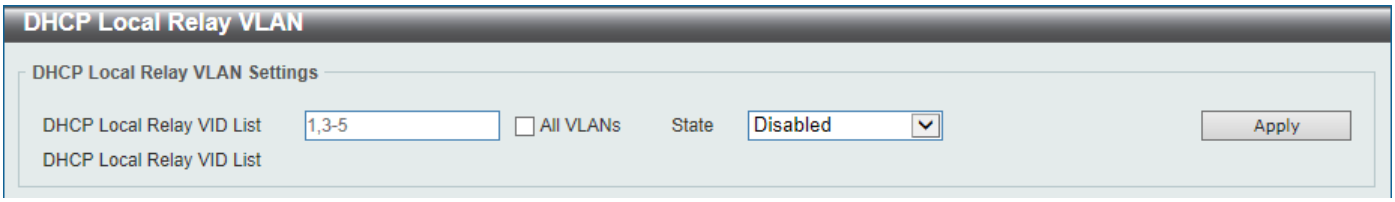
Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
State	Select to enable or disable the DHCP Relay feature on the specified port(s).

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

Management > DHCP > DHCP Relay > DHCP Local Relay VLAN Settings

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

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



Management > DHCP > DHCP Relay > DHCP Local Relay VLAN Window

The fields that can be configured are described below:

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

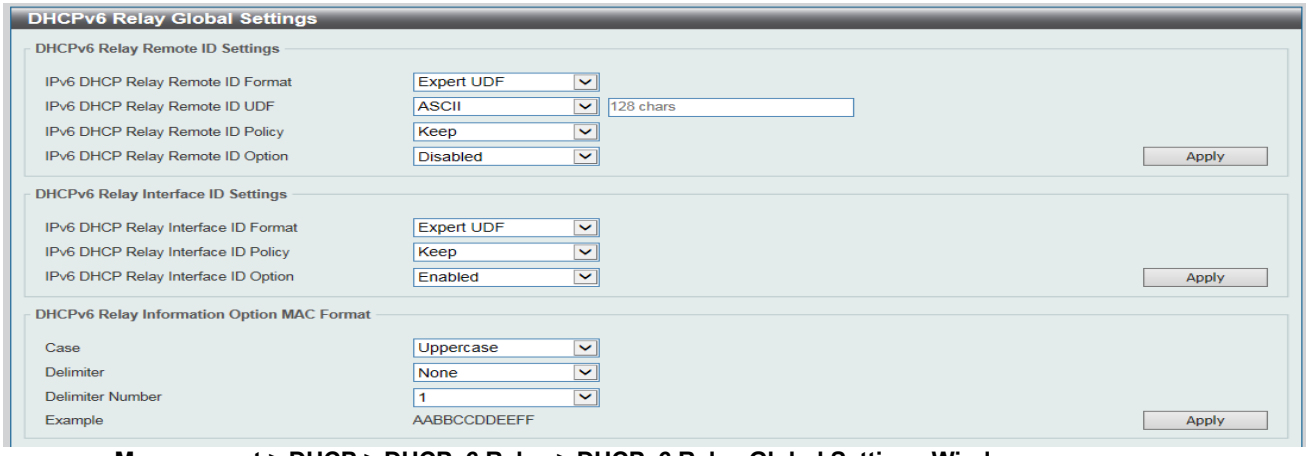
Click the **Apply** button to accept the changes made.

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

Management > DHCP > 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:



Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Global Settings Window

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

Parameter	Description
IPv6 DHCP Relay Remote ID Format	Select the IPv6 DHCP Relay remote ID format that will be used here. Options to choose from are **Default, CID with User Define,** and **User Define**.
IPv6 DHCP Relay Remote ID UDF	Select to choose the User Define Field (UDF) for remote ID. Options to choose from are **ASCII**, and **Hex**. • **ASCII** - Select to enter the ASCII string with a maximum of 128 characters in the text box. • **HEX** - Select to enter the hexadecimal string with a maximum of 256 characters in the text box.

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

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

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

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

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

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

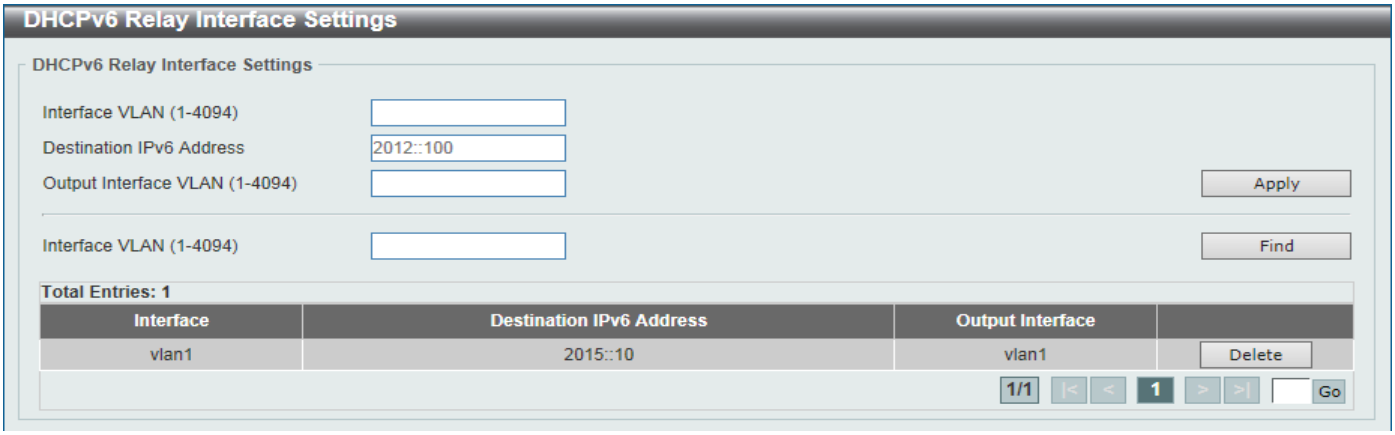
Parameter	Description
Case	Select the case that will be used here. Options to choose from are: • **Lowercase** - Specifies that the MAC format will be lowercase. For example: aa-bb-cc-dd-ee-ff. • **Uppercase** - Specifies that the MAC format will be uppercase. For example: AA-BB-CC-DD-EE-FF.
Delimiter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

Management > DHCP > DHCPv6 Relay > 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:



Management > DHCP > DHCPv6 Relay > 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.

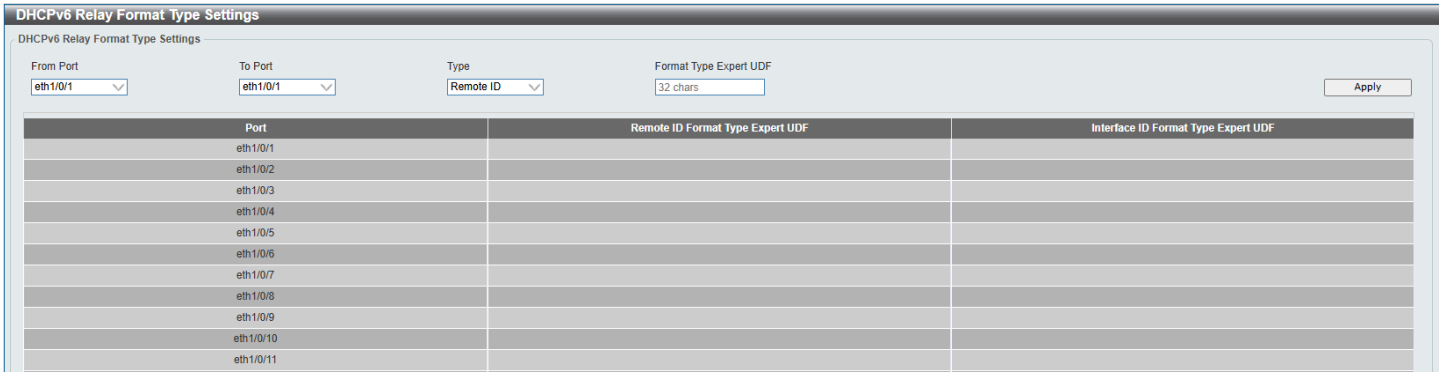
Click the **Delete** button to remove the specified entry.

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

Management > DHCP > DHCPv6 Relay > 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:



Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Format Type Settings Window

The fields that can be configured are described below:

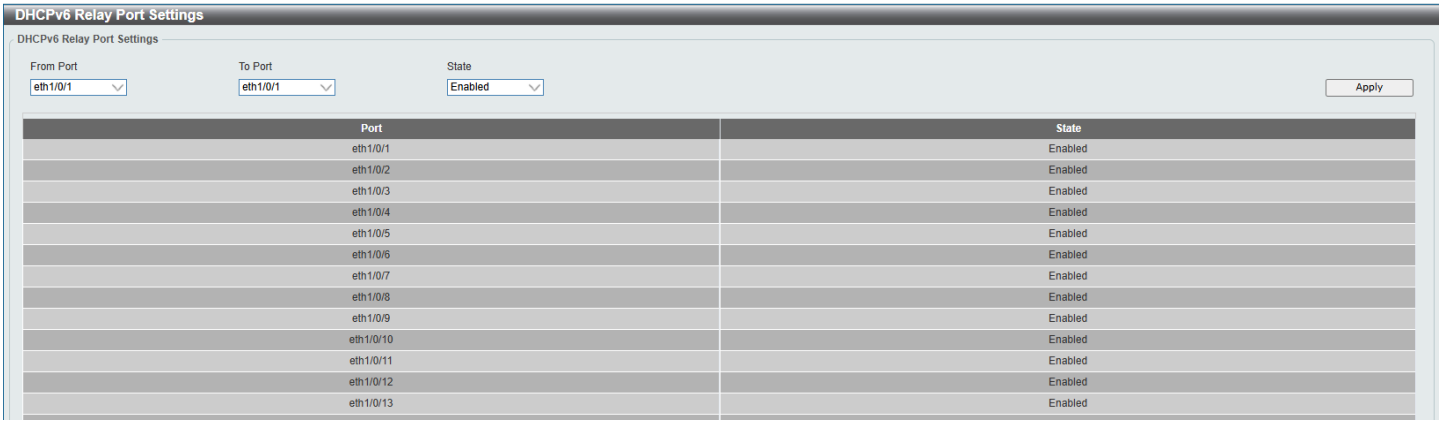
Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
Type	Select the type here. Options to choose from are: • **Remote ID** - Specifies to configure the Expert UDF format type string for DHCPv6 Option 37. • **Interface ID** - Specifies to 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.

Management > DHCP > DHCPv6 Relay > 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:



Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Port Settings Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
State	Select to enable or disable the DHCPv6 relay port feature on the specified port(s) here.

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

Management > DHCP > DHCPv6 Relay > DHCPv6 Local Relay VLAN Settings

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

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



Figure 4-60 DHCPv6 Local Relay VLAN Window

The fields that can be configured are described below:

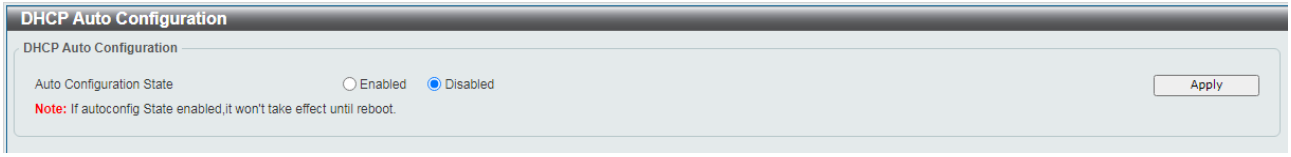
Parameter	Description
DHCPv6 Local Relay VID List	Enter the DHCPv6 local relay VLAN ID(s) here. More than one VLAN ID can be entered here. Select the **All VLANs** option to apply this setting on all configured VLANs on this Switch.
State	Select to enable or disable the DHCPv6 local relay feature on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

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

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

Management > DHCP Auto Configuration

In the DHCP Auto Configuration Page, users can enable or disable automatic download of the configuration files from the DHCP server. During reboot, if DHCP Auto Configuration is enabled, the device retrieves the config file the TFTP Server.



Management > DHCP Auto Configuration

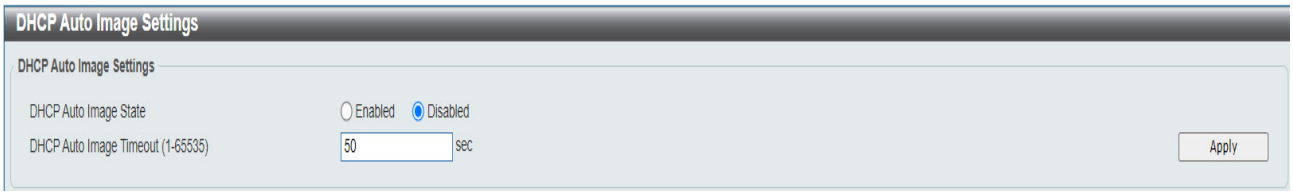
The fields that can be configured are described below:

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

Click the **Apply** button to save your settings.

Management > DHCP Auto Image Settings

In the DHCP Auto Image Settings Page, users can enable or disable automatic download of the firmware files from the DHCP server. During reboot, if DHCP Auto Image state is enabled, the device retrieves the firmware file the TFTP Server.



Management > DHCP Auto Image Settings

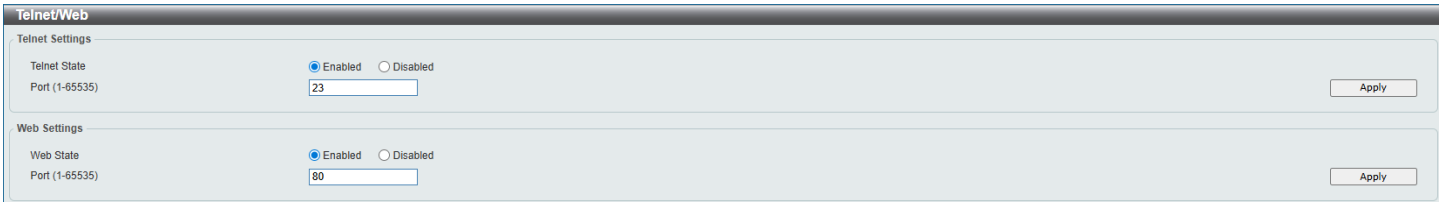
The fields that can be configured are described below:

Parameter	Description
DHCP Auto Image State	Select this option to enable or disable the auto-image function.
DHCP Auto Image Timeout	Settings range (1-65535) sec, default value: 50 sec.

Click the **Apply** button to save your settings.

Management > Telnet/Web

The Telnet/Web page allows you to configure Telnet and Web settings on the Switch.



Management > Telnet/Web

Telnet Settings:

Telnet State: Select to enable or disable the configuration through Telnet.

Port (1-65535): Enter the TCP port number used for Telnet management of the Switch. The standard TCP port for the Telnet protocol is 23.

Click **Apply** to save your settings.

Web Settings:

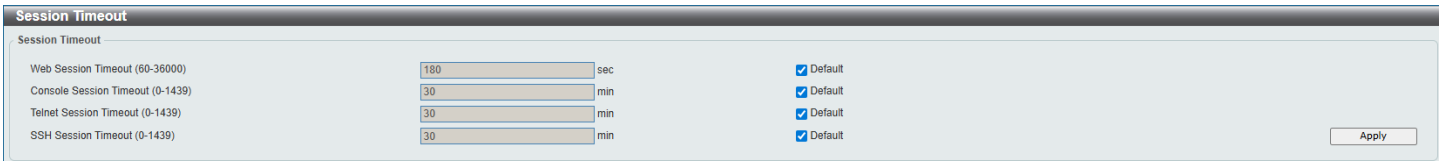
Web State: Select to enable or disable Web-based configuration.

Port (1-65535): Enter the TCP port number used for Web management of the Switch. The standard TCP port for the HTTP protocol is 80.

Click the **Apply** button to save your settings.

Management > Session Timeout

The Session Timeout page allows you to configure the session timeout on the Switch.



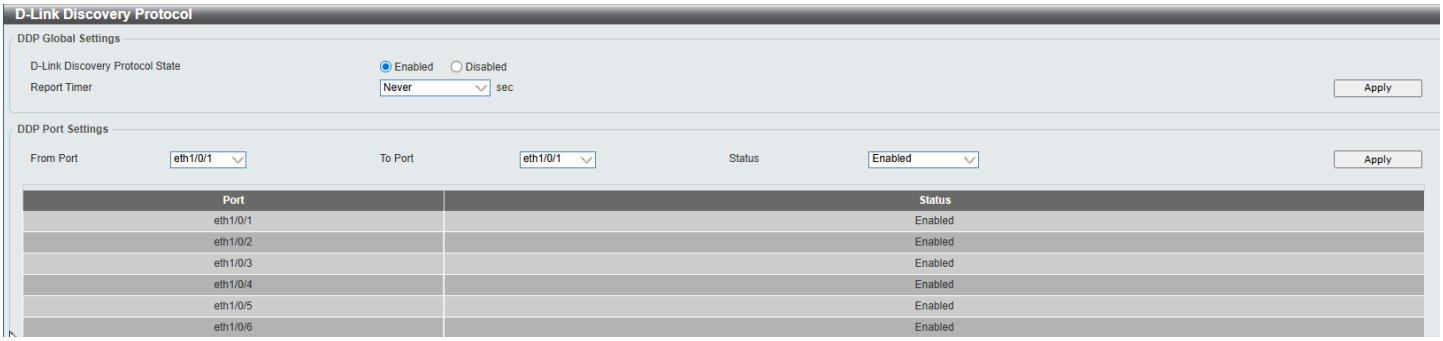
Management > Session Timeout

Web Session Timeout (60-36000): Enter the time in seconds of the web session timeout. Tick the **Default** check box. The default value is 180 sec.
Console Session Timeout (0-1439): Enter the time in minutes of the Console session timeout. Tick the **Default** check box to return to the default setting. The value is from 0 to 1439 minutes. 0 means never timeout. The default value is 30 minutes.
Telnet Session Timeout (0-1439): Enter the time in minutes of the Telnet session timeout. Tick the **Default** check box to return to the default setting. The value is from 0 to 1439 minutes. 0 means never timeout. The default value is 30 minutes.
SSH Session Timeout (0-1439): Enter the time in minutes of the Telnet session timeout. Tick the **Default** check box to return to the default setting. The value is from 0 to 1439 minutes. 0 means never timeout. The default value is 30 minutes.

Click the **Apply** button to save your settings.

Management > D-Link Discover Protocol Settings

The D-Link Discover Protocol Settings page allows you to configure and display D-Link Discovery Protocol (DDP).



Management > D-Link Discover Protocol Settings

D-Link Discovery Protocol State: Enter the enable or disable the D-Link Discovery Protocol state.

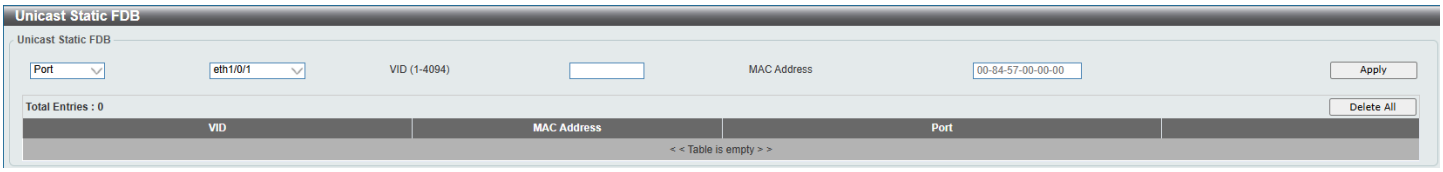
Report Timer: Specify the interval in seconds between two consecutive DDP report messages. Options to choose from are **30**, **60**, **90**,**120**, and **Never**.

DDP Port Settings:
From Port / To Port: Enter the appropriate port range used for the configuration.
State: Select to enable or disable the DDP port state.

Click the **Apply** button to save your settings.

L2 Features > FDB > Static FDB > Unicast Static FDB

The Unicast Static FDB page allows you to view and configure the static unicast forwarding settings on the Switch.



L2 Features > FDB > Static FDB > Unicast Static FDB

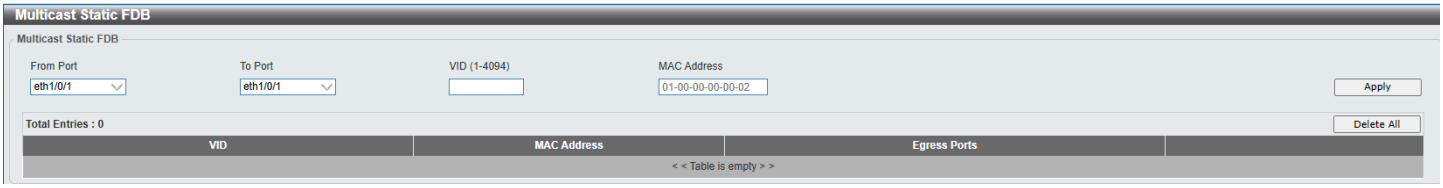
Port / Drop: Allows the selection of the port number on which the MAC address entered resides. This option could also drop the MAC address from the unicast static FDB. When selecting **Port**, select the switch unit and port number.
VID (1-4094): Enter the VLAN ID on which the associated unicast MAC address resides.
MAC Address: Enter the MAC address to which packets will be statically forwarded or dropped. This must be a unicast MAC address.

Click the **Apply** button to save your settings or click the **Delete All** button to delete all the entries found in the display table.

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

L2 Features > FDB > Static FDB > Multicast Static FDB

The Multicast Static FDB page allows you to view and configure the static multicast forwarding settings on the Switch.



L2 Features > FDB > Static FDB > Multicast Static FDB

From Port / To Port: Enter the appropriate port range used for the configuration.
VID (1-4094): Enter the VLAN ID of the VLAN the corresponding MAC address belongs to.
MAC Address: Enter the static destination MAC address of the multicast packets. This must be a multicast MAC address. The format of the destination MAC address is 01-XX-XX-XX-XX-XX.

Click the **Apply** button to save your settings. And 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.

L2 Features > FDB > MAC Address Table Settings

The **MAC Address Table Settings** page allows you to view and configure the MAC address table's global settings.



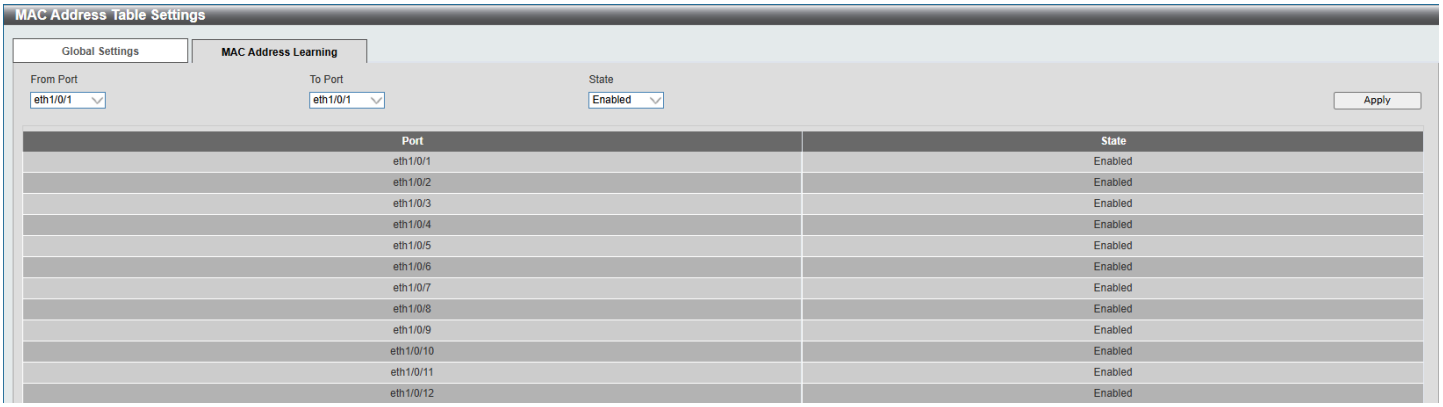
L2 Features > FDB > MAC Address Table Settings – Global Setting

Aging Time: Enter the MAC address table's aging time value. This value must be between 10 and 1000000 seconds.

Entering 0 will disable MAC address aging. By default, this value is 300 seconds.

Click the **Apply** button to save your settings.

After clicking the MAC Address Learning tab, the following page will appear.



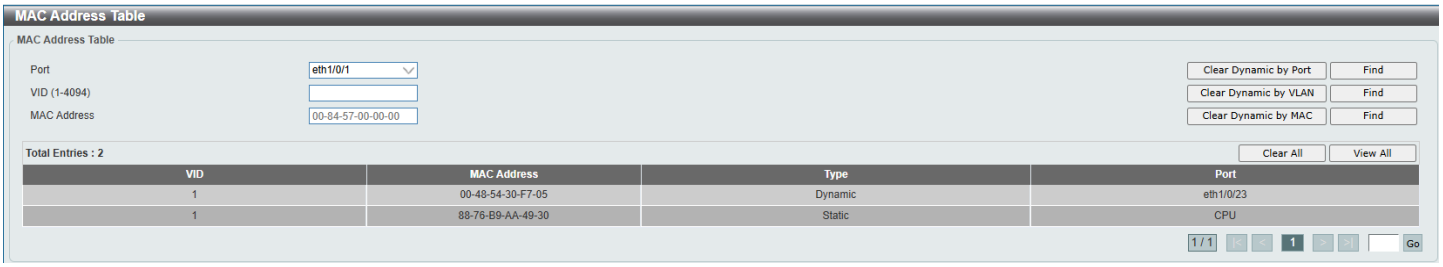
L2 Features > FDB > MAC Address Table Settings – MAC Address Learning

From Port / To Port: Enter the range of ports that will be used for this configuration.
State: Select to enable or disable the MAC address learning function on the specified ports.

Click the **Apply** button to save your settings.

L2 Features > FDB > MAC Address Table

The **MAC Address Table** page allows you to view the entries listed in the MAC address table.



L2 Features > FDB > MAC Address Table

Port: Select the port that will be used for this configuration.
VID (1-4094): Enter the VLAN ID that will be used for this configuration.
MAC Address: Enter the MAC address that will be used for this configuration

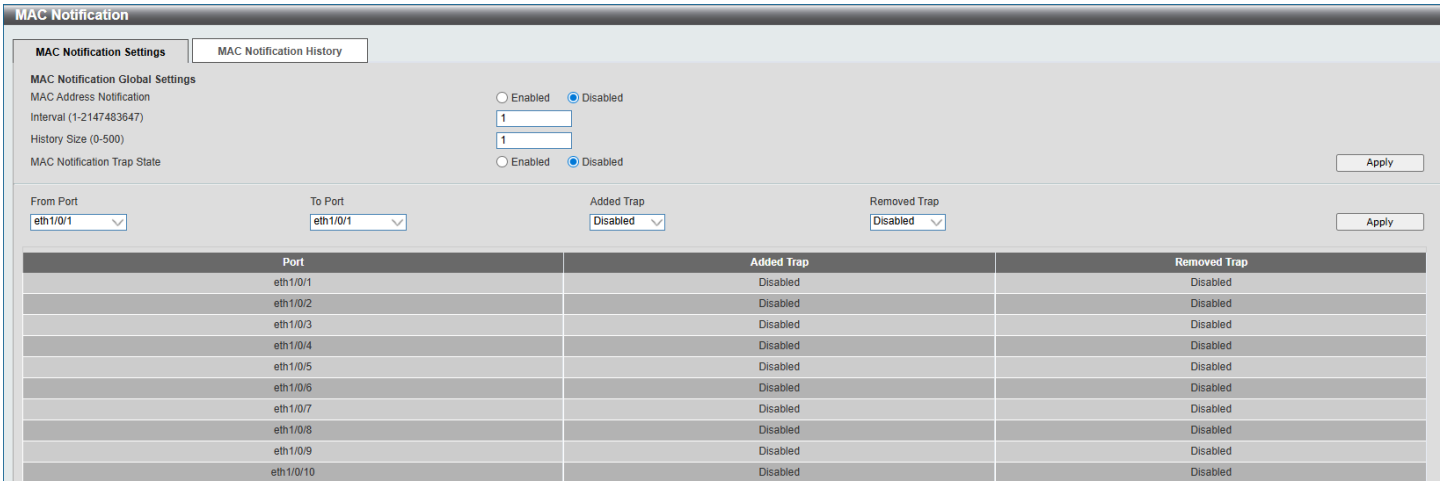
Click the **Find** button to locate a specific entry based on the information entered.

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

L2 Features > FDB > MAC Notification

This window is used to display and configure **MAC notification**. Switch alarms when new MAC entry learned.



L2 Features > FDB > MAC Address Table

MAC Address Notification Global Settings: Select to enable or disable MAC notification globally on the Switch

Interval: Enter the time value between notifications. This value must be between 1 and 2147483647 seconds. By default, this value is 1 second.

History Size: Enter the maximum number of entries listed in the history log used for notification. This value must be between 0 and 500. By default, this value is 1.

MAC Notification Trap State: Select to enable or disable MAC notification trap state on the Switch

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.



L2 Features > FDB > MAC Notification History

L2 Features > 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 (Step 1) Window

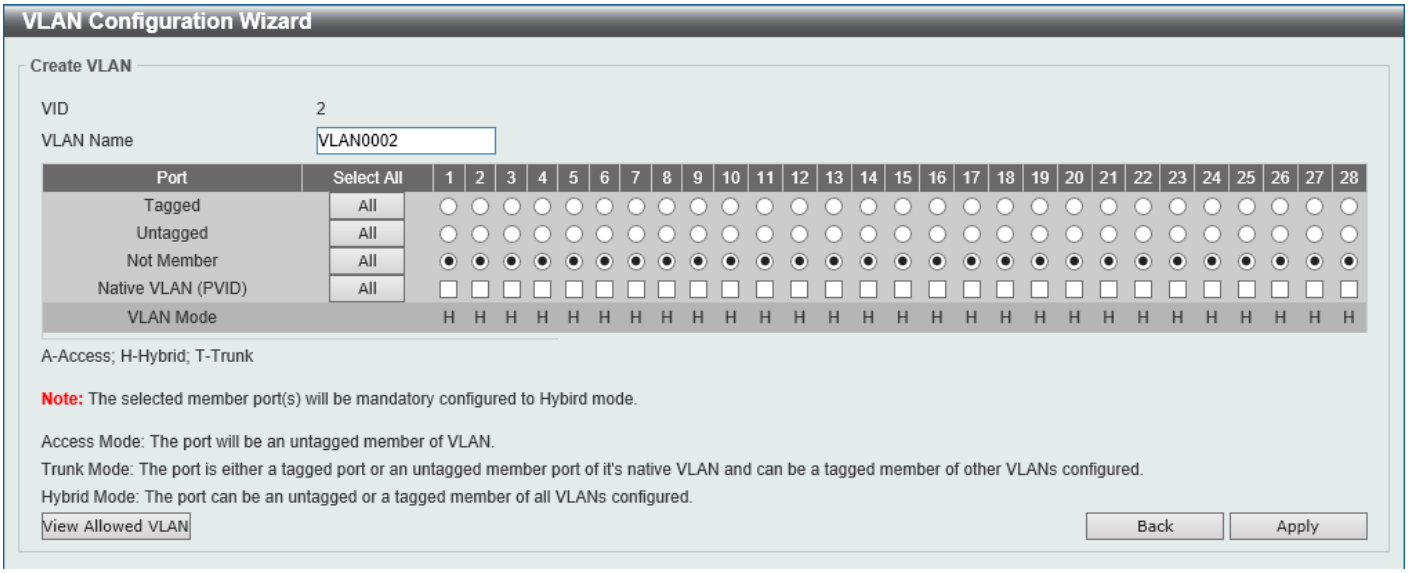
The fields that can be configured are described below:

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.



VLAN Configuration Wizard (Create VLAN) Window

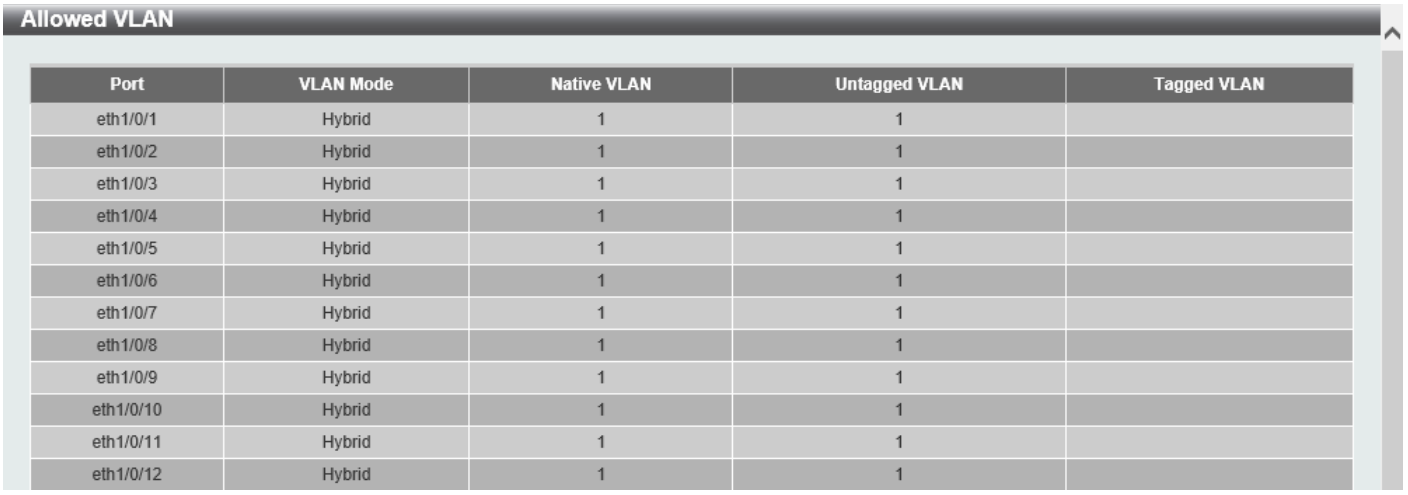
The fields that can be configured are described below:

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

Click the **View Allowed VLAN** button view the allowed VLAN settings. Click the **Back** button to return to the previous step.

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

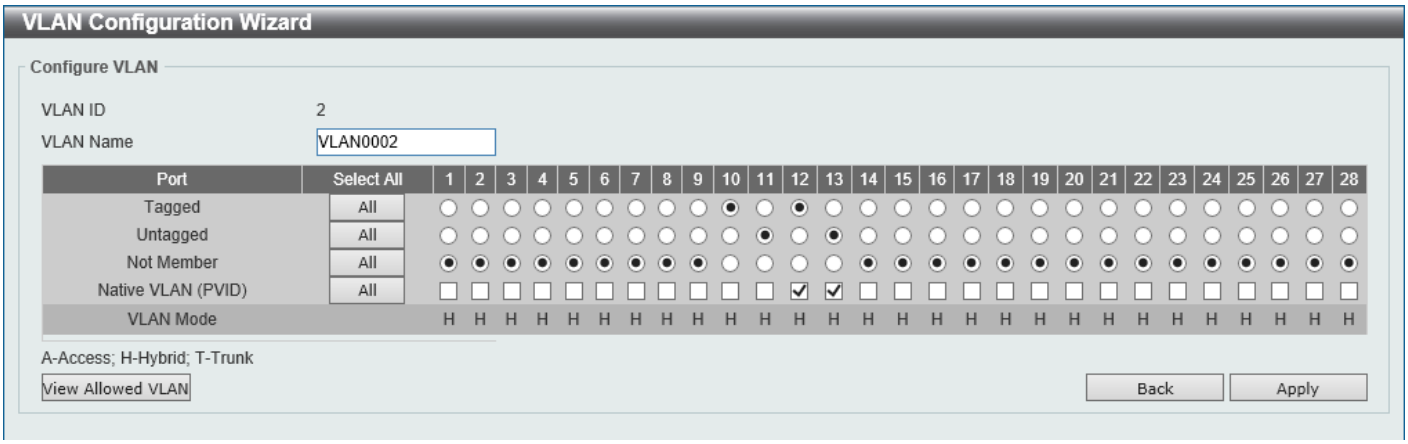
After clicking the **View Allowed VLAN** button, the following window will appear.



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) Window

The fields that can be configured are described below:

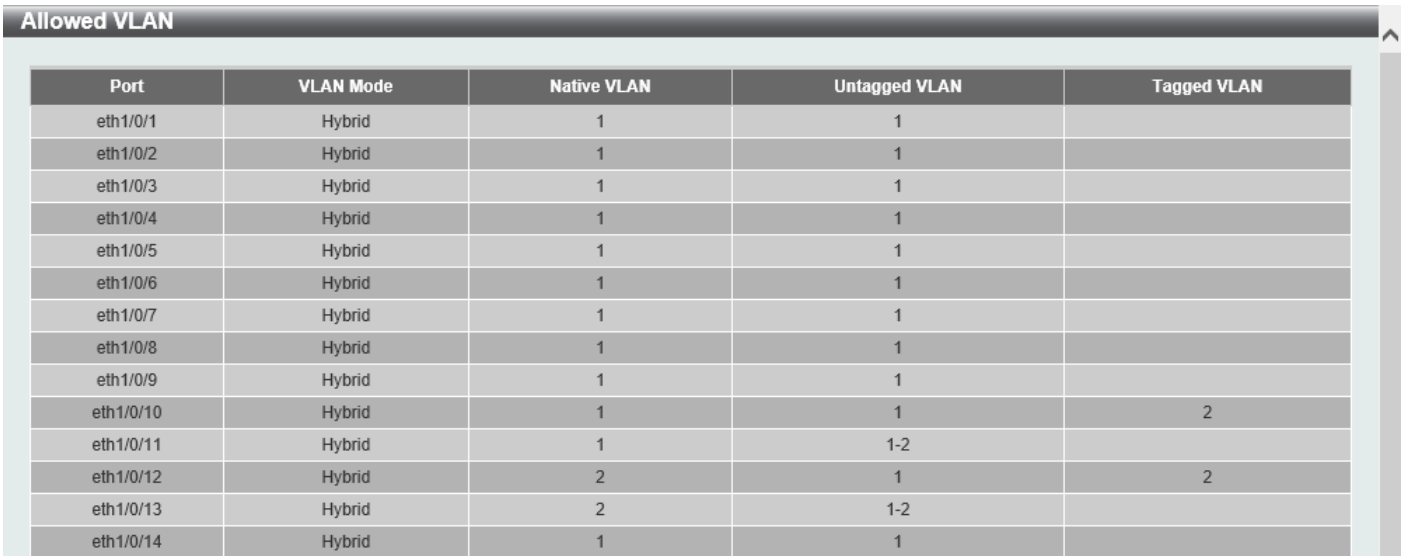
Parameter	Description
VLAN Name	Enter the name for the VLAN here.
Tagged	Select the switch ports that are tagged members of this VLAN here.
Untagged	Select the switch ports that are untagged members of this VLAN here.
Not Member	Select the switch ports that are not members of this VLAN here.
Native VLAN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

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

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

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

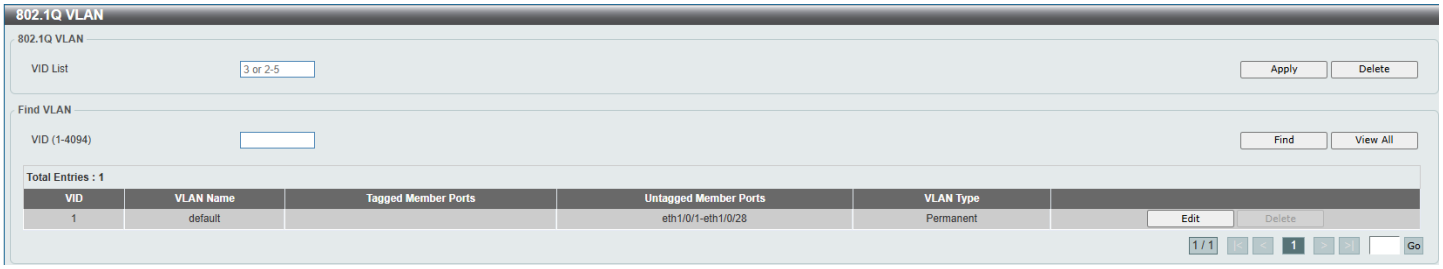
After clicking the **View Allowed VLAN** button, the following window will appear.



Allowed VLAN Window

L2 Features > 802.1Q VLAN

The 802.1Q VLAN page allows you to view and configure the VLAN settings on this switch.



L2 Features > 802.1Q VLAN

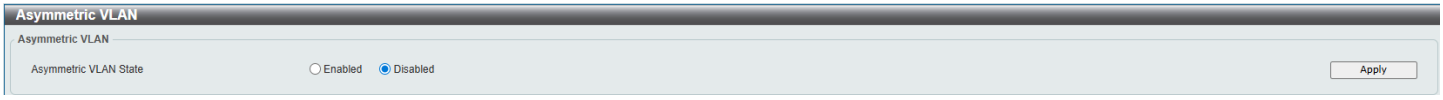
802.1Q VLAN:

VID List: Enter the VLAN ID list that will be created.
Click the **Apply** button to save your settings.
Click the **Delete** button to remove the specific entry.

Find VLAN:
VID (1-4094): Enter the VLAN ID to be displayed.
Click the **Find** button to locate a specific entry based on the information entered.
Click the **View All** button to locate all the entries.
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.

L2 Features > Asymmetric VLAN

The Asymmetric VLAN page allows you to configure the asymmetric VLAN function on this switch.

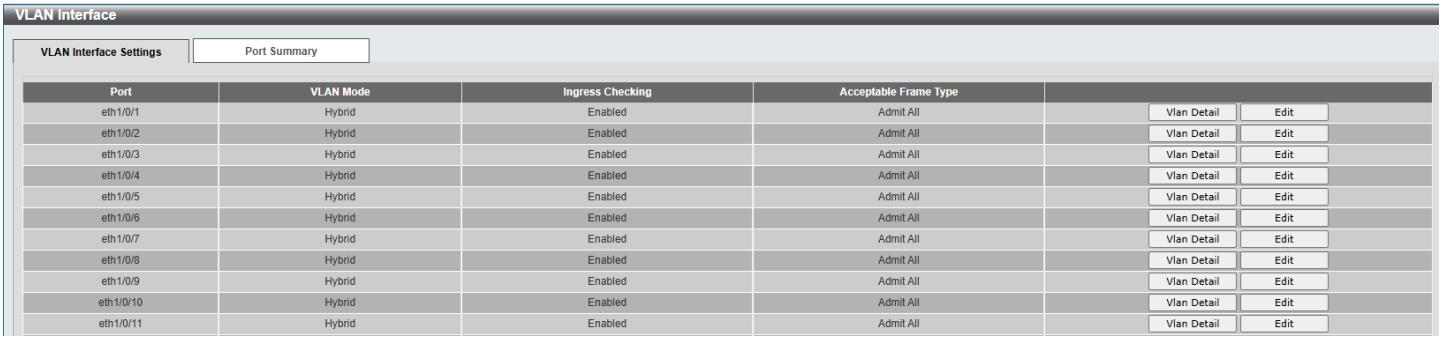


L2 Features > Asymmetric VLAN

Asymmetric VLAN State: Select to enable or disable the Asymmetric VLAN function.
Click the **Apply** button to save your settings.

L2 Features > VLAN Interface

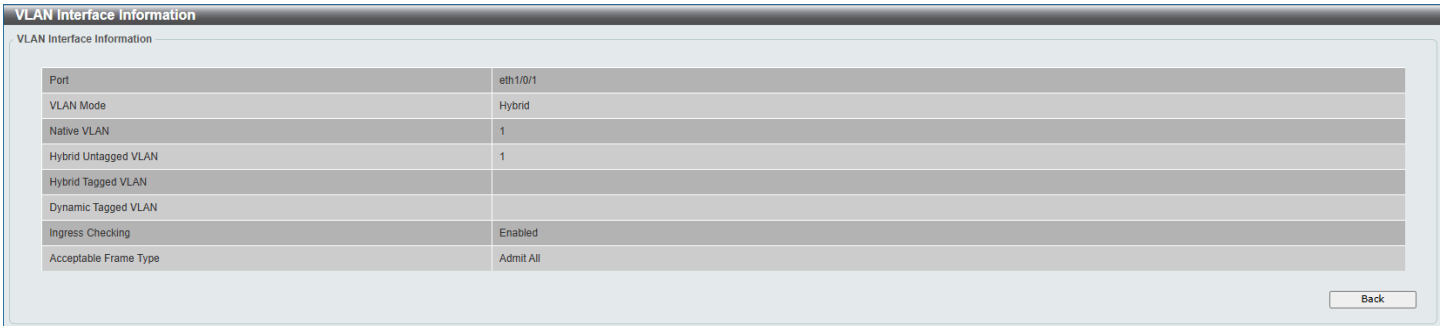
The VLAN Interface page allows you to view and configure the VLAN interface settings on this switch.



L2 Features > VLAN Interface

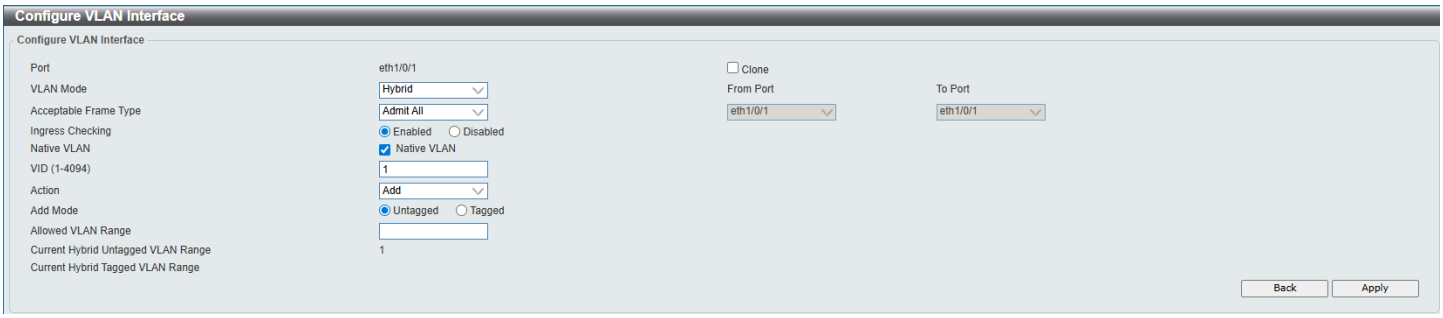
Unit: Select the switch unit that will be used for this configuration.
Click the **VLAN Detail** button to view more detailed information about the VLAN on the specific interface.
Click the **Edit** button to re-configure the specific entry.

After clicking the **VLAN Detail** button, the following page will appear:



L2 Features > VLAN Interface – VLAN Detail

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



L2 Features > VLAN Interface – VLAN Detail

Port: Display the VLAN port number.

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

Acceptable Frame Type: Select the acceptable frame type behavior option. Options to choose from are Tagged **Only**, **Untagged Only**, and **Admit All**.

Ingress Checking: Select to enable or disable the ingress checking function.

Native VLAN: Tick the option to enable the native VLAN function.

VID (1-4094): After ticking the **Native VLAN** check box, this option will be available. Enter the VLAN ID used for this configuration. This value must be between 1 and 4094.

Action: Select the action that will be taken here. Options to choose from are **Add, Remove, Tagged,** and **Untagged.**

Add Mode: Select whether to add an **Untagged** or **Tagged** parameters.

Allowed VLAN Range: Enter the allowed VLAN range information.

Clone: Tick the **Clone** check box to copy the configuration to specified ports.

From Port / To Port: Copy the configuration of VLAN interface for specified port ranges.

Click the **Apply** button to save your settings.

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

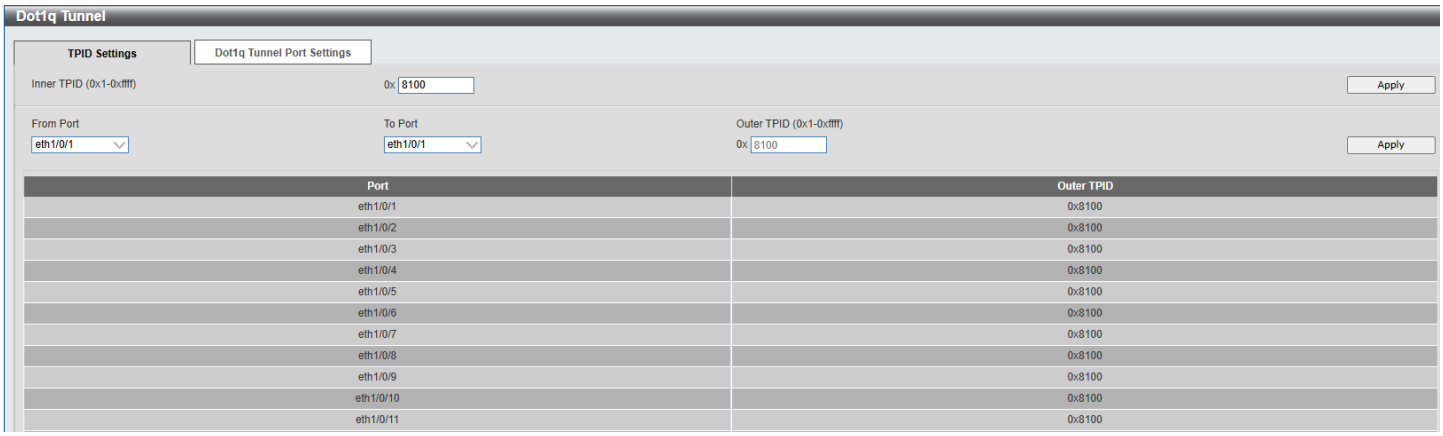
L2 Features > VLAN Tunnel > Dot1q Tunnel

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

An 802.1Q tunnel port behaves as a User Network Interface (UNI) port of a service VLAN. The trunk ports which are tagged members of the service VLAN behave as the Network Node Interface (NNI) ports of the service VLAN.

Only configure the 802.1Q tunneling Ethernet type on ports that are connected to the provider bridge network, which receives and transmits the service VLAN tagged frames. If the tunnel Ethernet type is configured, the specified value will be the Tag Protocol ID (TPID) in the outer VLAN tag of the transmitted frames of the port. The specified TPID is also used to identify the service VLAN tag for the received frame on this port.

To view the following window, click **L2 Features > VLAN Tunnel > Dot1q Tunnel**, as shown below:



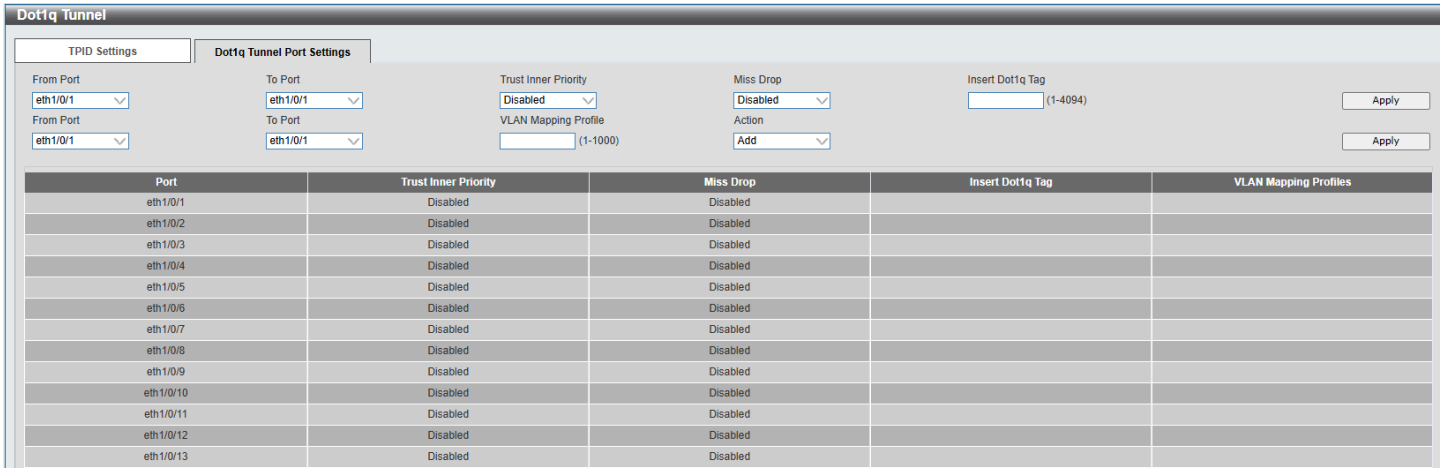
L2 Features > VLAN Tunnel > Dot1q Tunnel Settings Window

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.
From Port - To Port	Select the port range that will be used here.
Outer TPID	Enter the outer TPID value here. This value is in the hexadecimal form. The range is from 0x1 to 0xFFFF.

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

After clicking the **Dot1q Tunnel Port Settings** tab, the following page will appear:



L2 Features > VLAN Tunnel > Dot1q Tunnel Settings (Dot1q Tunnel Port Settings) Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the port range that will be used here.
Trust Inner Priority	Select to enable or disable the 802.1Q Inner Trust Priority feature here. When the trusting priority option is enabled on an 802.1Q tunnel port, the priority of the VLAN tag in the received packets will be copied to the service VLAN tag.
Miss Drop	Select to enable or disable the Miss Drop feature here. If the VLAN mapping Miss Drop option is enabled on the receiving port, when the original VLAN of the received packets cannot match the VLAN mapping entries or rules on this port, the received packets will be dropped.
Insert Dot1q Tag	Enter the 802.1Q VLAN ID that is inserted to the untagged packets which are received on the 802.1Q tunnel port(s) here. The range is from 1 to 4094.

VLAN Mapping Profile	Enter the ID of the VLAN mapping profile here. A lower ID has a higher priority. The ID range is from 1 to 1000.
Action	Select **Add** to add a new entry based in the information entered. Select **Remove** to remove an entry based in the information entered.

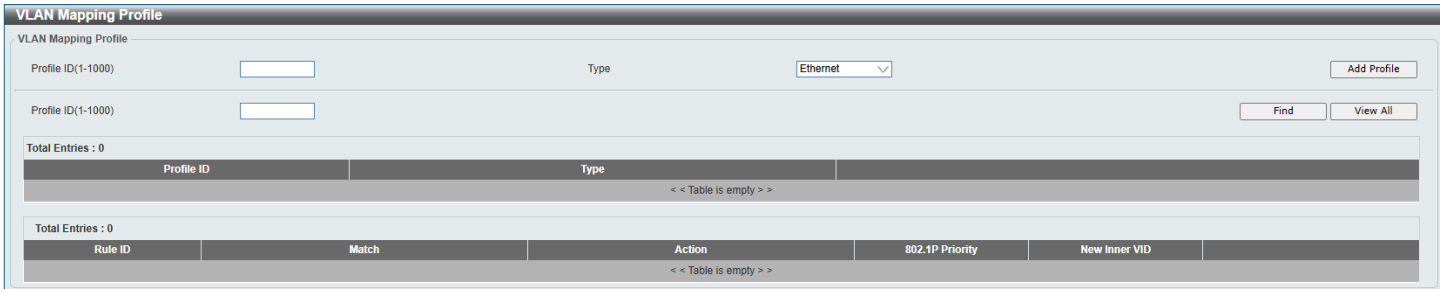
Click the **Apply** button to accept the changes made.

L2 Features > VLAN Tunnel > VLAN Mapping

This window is used to display and configure the VLAN mapping settings. If a profile is applied on an interface, the Switch matches the incoming packets according to the rules of the profile. If the packet matches a rule, the action of the rule will be taken. This action may be adding or replacing the outer-VID, specifying the priority of the new outer- TAG or specifying the packet's new inner-VID.

The match order depends on the rule's sequence number in the profile and stopped when first matched. If the sequence number is not specified, it will be allocated automatically. The sequence number begins from 10 and increments 10. Multiple different types of profiles can be configured on one interface.

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



L2 Features > VLAN Tunnel > VLAN Mapping Window

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the port range that will be used here.
Port	Select the port that will be used for the search here.
Original VID List	Enter the original VLAN ID list here. The range is from 1 to 4094.
Original Inner VID	Enter the original inner VLAN ID here. The range is from 1 to 4094.
Action	Select the action that will be taken here. Options to choose from are **Translate** and **Dot1q-tunnel**. • **Translate** - Specifies that the VID will replace the VID of the matched packets. • **Dot1q-tunnel** - Specifies that the outer-VID will be added for matched packets.
VID	Enter the VLAN ID to be translated here. The range is from 1 to 4094.
Inner VID	Enter the inner VLAN ID to be translated here. The range is from 1 to 4094.
Priority	Select the 802.1p priority value here. The range is from 0 to 7. A higher value has a higher priority.

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

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

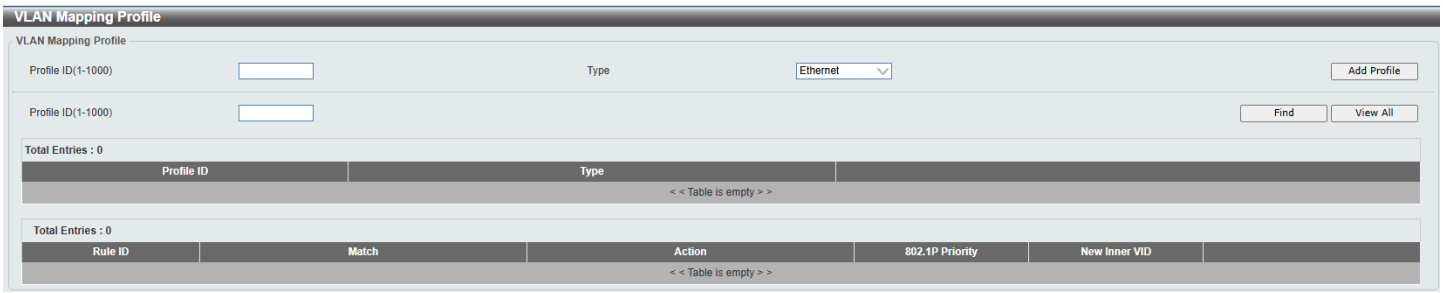
Click the **Delete** button to delete the specified entry.

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

L2 Features > VLAN Tunnel > VLAN Mapping Profile

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

To view the following window, click **L2 Features > VLAN Tunnel > VLAN Mapping Profile**, after clicking an entry of the VLAN Mapping Profile, the rules of Profile 1 will appear.



L2 Features > VLAN Tunnel > VLAN Mapping Profile Window

The fields that can be configured are described below:

Parameter	Description
Profile ID	Enter the ID of the VLAN mapping profile here. A lower ID has a higher priority. The ID range is from 1 to 1000.
Type	Select the profile type here. Different profiles can match different fields. Options to choose from are **Ethernet**, **IP**, **IPv6**, and **Ethernet-IP**. • **Ethernet** - The profile can match Layer 2 fields. • **IP** - The profile can match Layer 3 IP fields. • **IPv6** - The profile can match IPv6 destination or source addresses. • **Ethernet-IP** - The profile can match Layer 2 and Layer 3 IP fields.

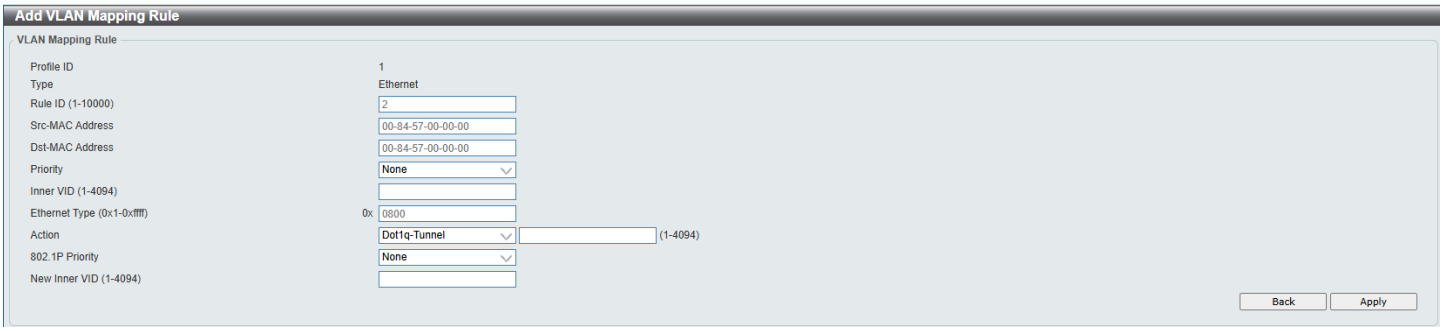
Click the Add Profile button to add a new VLAN mapping profile.

Click the Find button to locate a specific entry based on the information entered. Click the Add Rule button to create a new rule.

Click the Delete button to remove the specified entry.

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

After clicking the Add Rule button next to an Ethernet type profile, the following page will appear.



L2 Features > VLAN Tunnel > VLAN Mapping Profile (Ethernet, Add Rule) Window

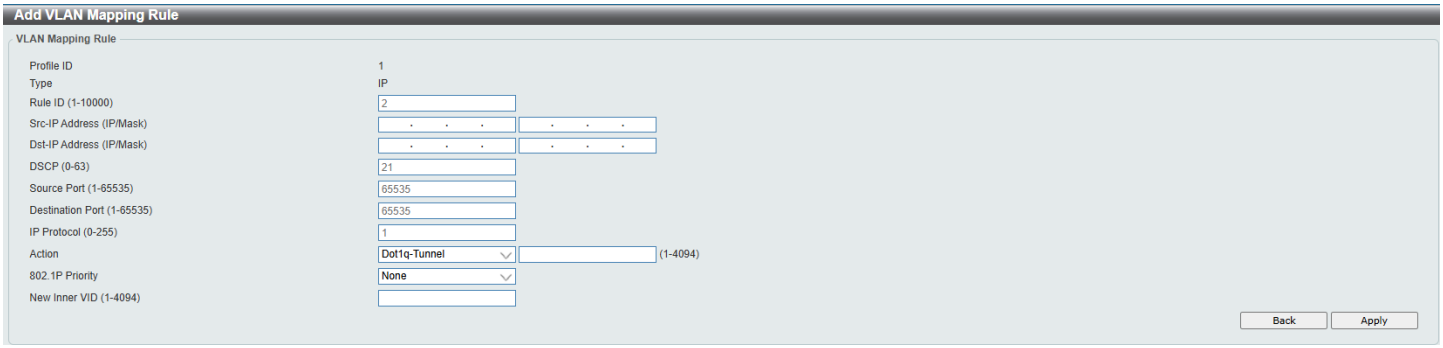
The fields that can be configured are described below:

Parameter	Description
Rule ID	Enter the VLAN mapping rule ID here. If not specified, the rule ID begins from 10 and is incremented by 10 for every new rule. The range is from 1 to 10000.
Src-MAC Address	Enter the source MAC address here.
Dst-MAC Address	Enter the destination MAC address here.
Priority	Select the 802.1p priority value here. The range is from 0 to 7. A higher value has a higher priority.
Inner VID	Enter the inner VLAN ID here. The range is from 1 to 4094.
Ethernet Type	Enter the Ethernet type value here. The range is from 0x0 to 0xFFFF.
Action	Select the action that will be taken here. Options to choose from are **Dot1q-Tunnel** and **Translate**. • **Dot1q-Tunnel** - Specifies that the outer-VID will be added for matched packets. • **Translate** - Specifies that the outer-VID will replace the outer-VID of the matched packets.
New Outer VID	Enter the new outer VLAN ID here. The range is from 1 to 4094.
802.1P Priority	Select the 802.1p priority value here. The range is from 0 to 7. A higher value has a higher priority.
New Inner VID	After selecting Dot1q-Tunnel as the action, enter the new inner VLAN ID here. The range is from 1 to 4094. This option is only available when Dot1q-Tunnel is selected as the action.

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

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

After clicking the **Add** Rule button next to an **IP** type profile, the following page will appear.



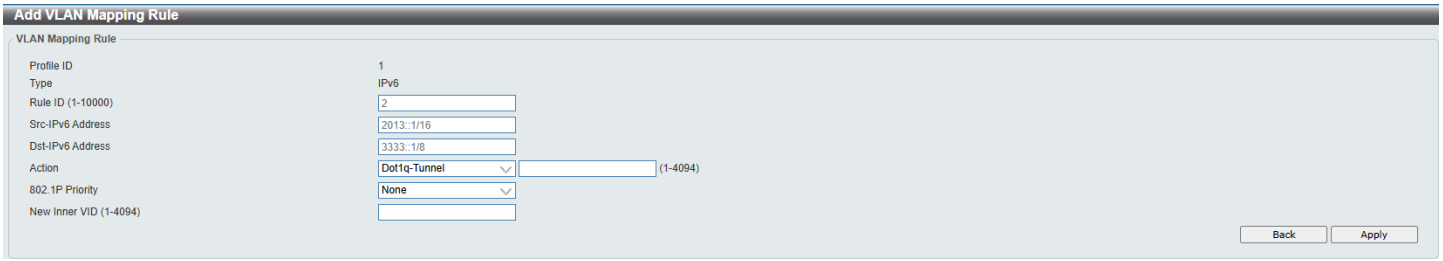
L2 Features > VLAN Tunnel > VLAN Mapping Profile (IP, Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Rule ID	Enter the VLAN mapping rule ID here. If not specified, the rule ID begins from 10 and is incremented by 10 for every new rule. The range is from 1 to 10000.
Src-IP Address (IP/Mask)	Enter the source IPv4 address and subnet mask here.
Dst-IP Address (IP/Mask)	Enter the destination IPv4 address and subnet mask here.
DSCP	Enter the differentiated services code point (DSCP) value here. The range is from 0 to 63.
Source Port	Enter the source TCP/UDP port number here. The range is from 1 to 65535.
Destination Port	Enter the destination TCP/UDP port number here. The range is from 1 to 65535.
IP Protocol	Enter the Layer 3 IP protocol value here. The range is from 0 to 255.
Action	Select the action that will be taken here. Options to choose from are **Dot1q-Tunnel** and **Translate**. • **Dot1q-Tunnel** - Specifies that the VID will be added for matched packets. • **Translate** - Specifies that the outer-VID will replace the outer-VID of the matched packets.
New Outer VID	Enter the new outer VLAN ID here. The range is from 1 to 4094.
802.1P Priority	Select the 802.1p priority value here. The range is from 0 to 7. A higher value has a higher priority.
New Inner VID	After selecting Dot1q-Tunnel as the action, enter the new inner VLAN ID here. The range is from 1 to 4094. This option is only available when Dot1q-Tunnel is selected as the action.

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

After clicking the Add Rule button next to an IPv6 type profile, the following page will appear.



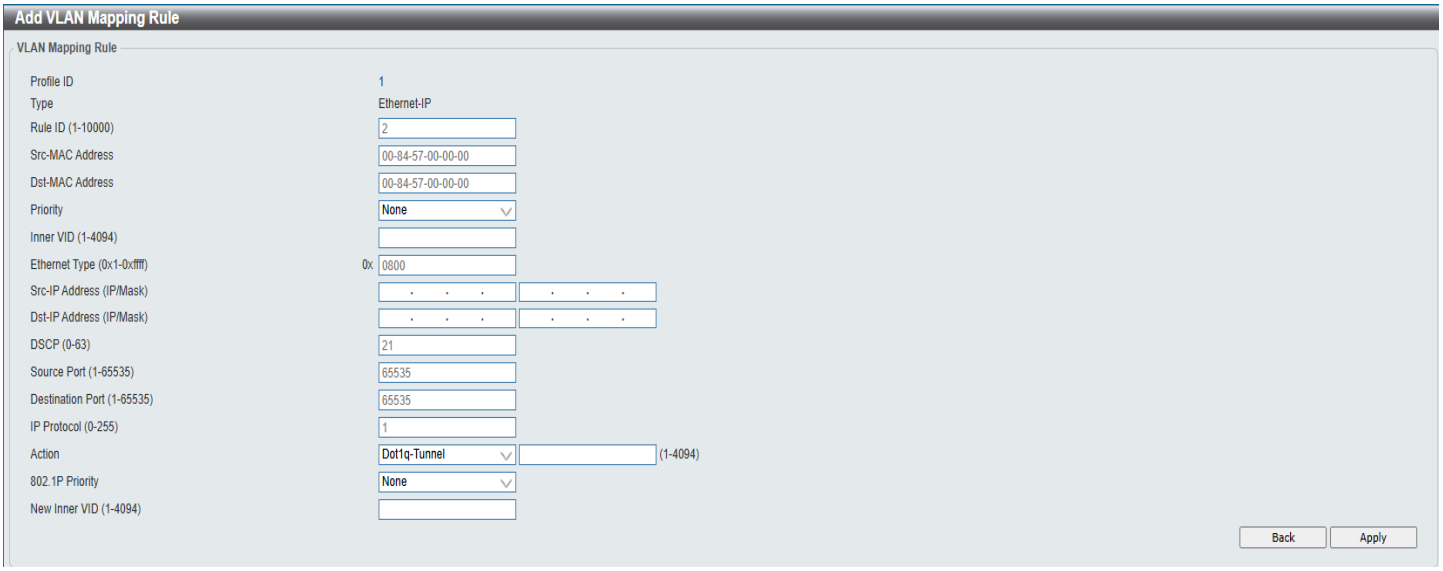
L2 Features > VLAN Tunnel > VLAN Mapping Profile (IPv6, Add Rule) Window

The fields that can be configured are described below:

Parameter	Description
Rule ID	Enter the VLAN mapping rule ID here. If not specified, the rule ID begins from 10 and is incremented by 10 for every new rule. The range is from 1 to 10000
Src-IPv6 Address	Enter the source IPv6 address and prefix length here.
Dst-IPv6 Address	Enter the destination IPv6 address and prefix length here.
Action	Select the action that will be taken here. Options to choose from are **Dot1q-Tunnel** and **Translate**. • **Dot1q-Tunnel** - Specifies that the outer-VID will be added for matched packets. • **Translate** - Specifies that the outer-VID will replace the outer-VID of the matched packets.
New Outer VID	Enter the new outer VLAN ID here. The range is from 1 to 4094.
802.1P Priority	Select the 802.1p priority value here. The range is from 0 to 7. A higher value has a higher priority.
New Inner VID	After selecting Dot1q-Tunnel as the action, enter the new inner VLAN ID here. The range is from 1 to 4094. This option is only available when Dot1q-Tunnel was selected as the action.

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

After clicking the **Add Rule** button next to an **Ethernet-IP** type profile, the following page will appear.



L2 Features > VLAN Tunnel > VLAN Mapping Profile (Ethernet-IP, Add Rule) Window

The fields that can be configured are described below:

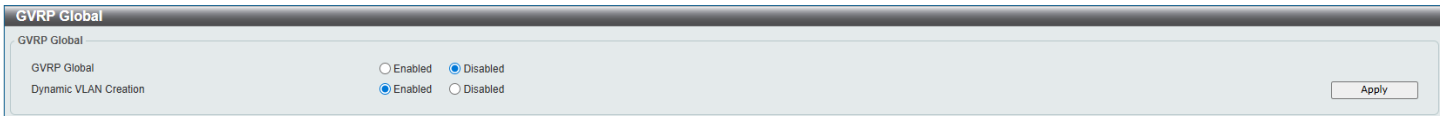
Parameter	Description
Rule ID	Enter the VLAN mapping rule ID here. If not specified, the rule ID begins from 10 and is incremented by 10 for every new rule. The range is from 1 to 10000
Src-MAC Address	Enter the source MAC address here.
Dst-MAC Address	Enter the destination MAC address here.
Priority	Select the 802.1p priority value here. The range is from 0 to 7. A higher value has a higher priority.
Inner VID	Enter the inner VLAN ID here. The range is from 1 to 4094.
Ethernet Type	Enter the Ethernet type value here. The range is from 0x0 to 0xFFFF.
Src-IP Address	Enter the source IPv4 address and subnet mask here.
Address	Enter the destination IPv4 address and subnet mask here.
DSCP	Enter the differentiated services code point (DSCP) value here. The range is from 0 to 63.
Source Port	Enter the source TCP/UDP port number here. The range is from 1 to 65535.
Destination Port	Enter the destination TCP/UDP port number here. The range is from 1 to 65535.
IP Protocol	Enter the Layer 3 IP protocol value here. The range is from 0 to 255.
Action	Select the action that will be taken here. Options to choose from are **Dot1q-Tunnel** and **Translate**. **Dot1q-Tunnel** - Specifies that the outer-VID will be added for matched packets. **Translate** - Specifies that the outer-VID will replace the outer-VID of the matched packets.
New Outer VID	Enter the new outer VLAN ID here. The range is from 1 to 4094.
802.1P Priority	Select the 802.1p priority value here. The range is from 0 to 7. A higher value has a higher priority.
New Inner VID	After selecting Dot1q-Tunnel as the action, enter the new inner VLAN ID here. The range is from 1 to 4094. This option is only available when **Dot1q-Tunnel** was selected as the action.

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

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

L2 Features > GVRP > GVRP Global

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



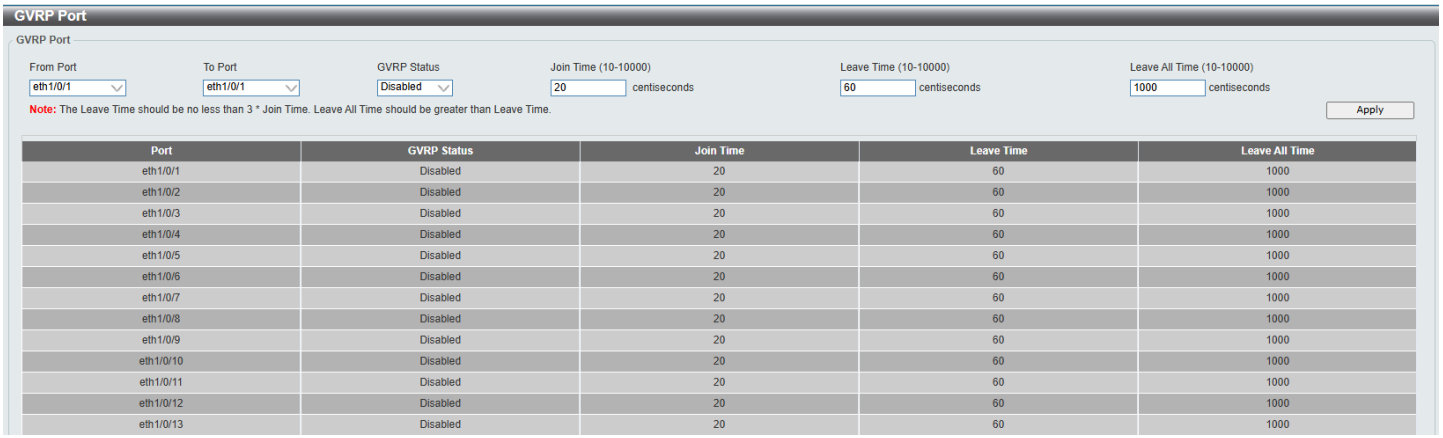
L2 Features > GVRP > GVRP Global

GVRP Global: Select enable/disable for GVRP Global state.
Dynamic VLAN Creation: Select enable/disable for Dynamic VLAN Creation state.

Click the **Apply** button to apply the configuration.

L2 Features > GVRP > GVRP Port

The page is used to configure the parameters of GVRP in ports.



L2 Features > GVRP > GVRP Port

From Port/To Port: Indicates the interface.
GVRP Status: Select enable/disable for port based GVRP state.

Join Time (10-100000): Indicates the time in milliseconds that PDUs are transmitted. The default value is *200ms*.

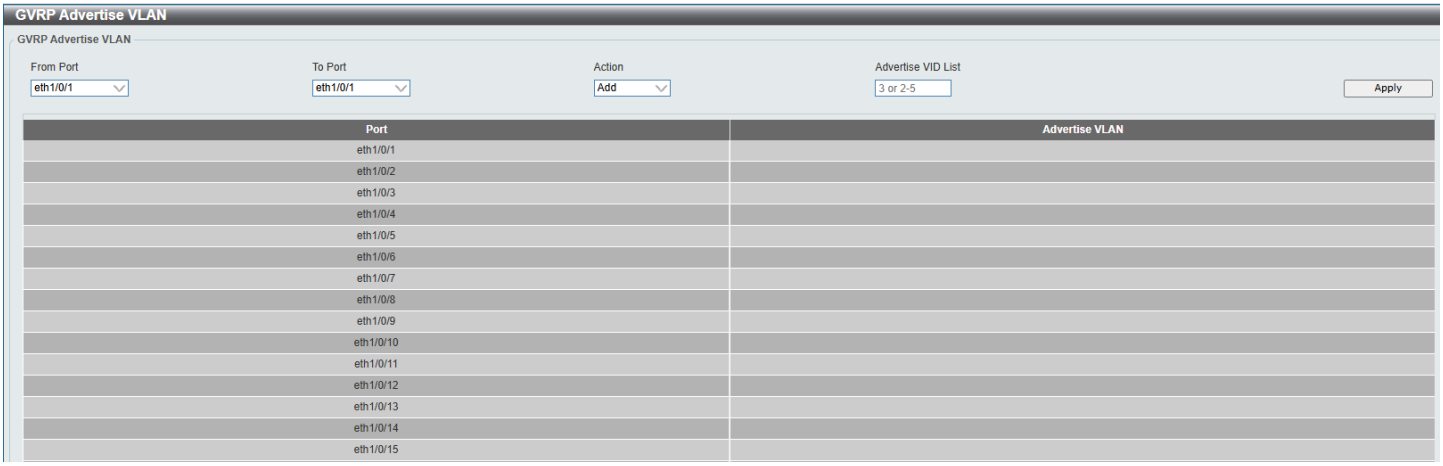
Leave Time (100-100000): Indicates the amount of time in milliseconds that the device waits before leaving its GARP state. The leave time is activated by a leave all time message sent/received, and cancelled by the Join message. The default value is *600ms*.

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

Click the **Apply** button to apply the configuration.

L2 Features > GVRP > GVRP Advertise VLAN

This page is used to configure the VLAN ID to be advertised.



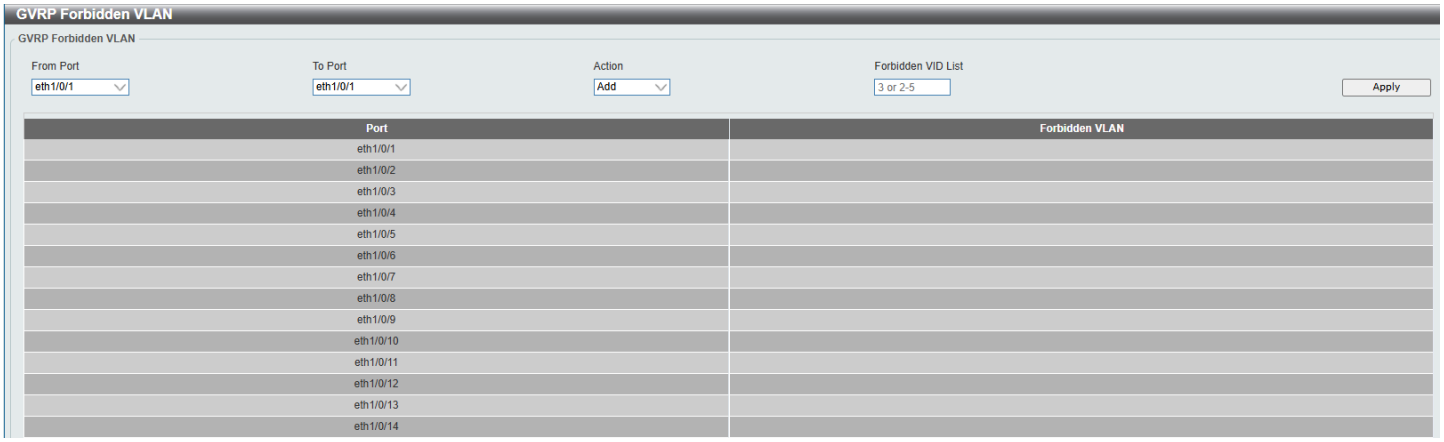
L2 Features > GVRP > GVRP Advertise VLAN

From Port/To Port: Indicates the interface.
Action: Selectable **Add**, **Remove**, **Replace** or **ALL** (adding all VLAN IDs)

Click the **Apply** button to apply the configuration.

L2 Features > GVRP > GVRP Forbidden VLAN

This page is used to configure the VLAN ID that forbid to register.

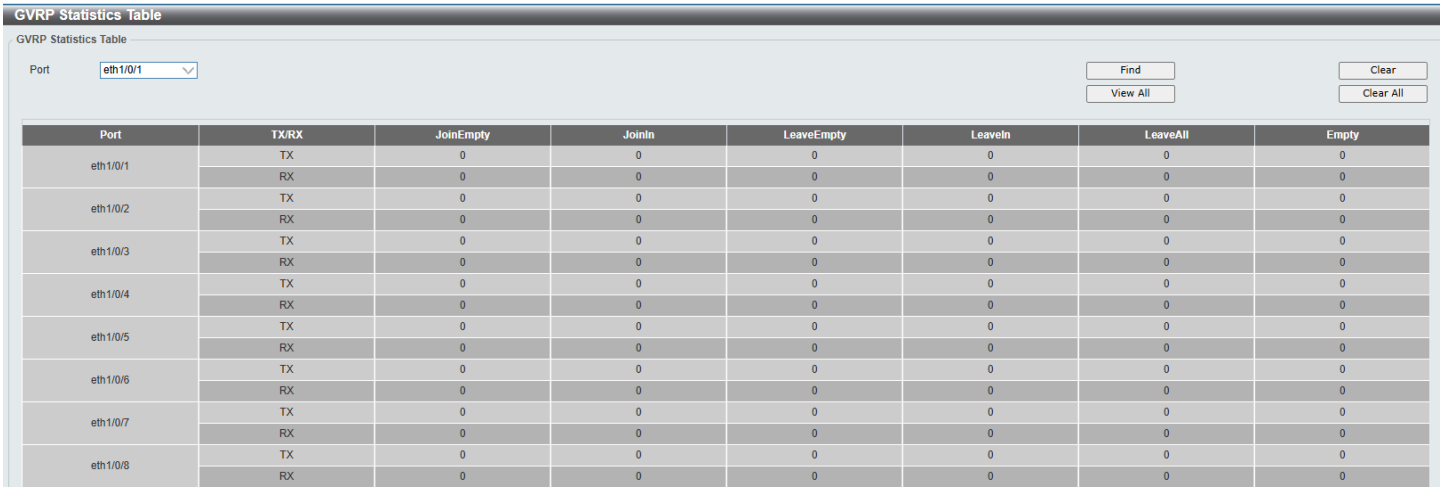


L2 Features > GVRP > GVRP Forbidden VLAN

From Port/To Port: Indicates the interface.
Action: Selectable **Add**, **Remove**, **Replace** or **ALL** (adding all VLAN IDs)
Click the **Apply** button to apply the configuration.

L2 Features > GVRP > GVRP Statistics Table

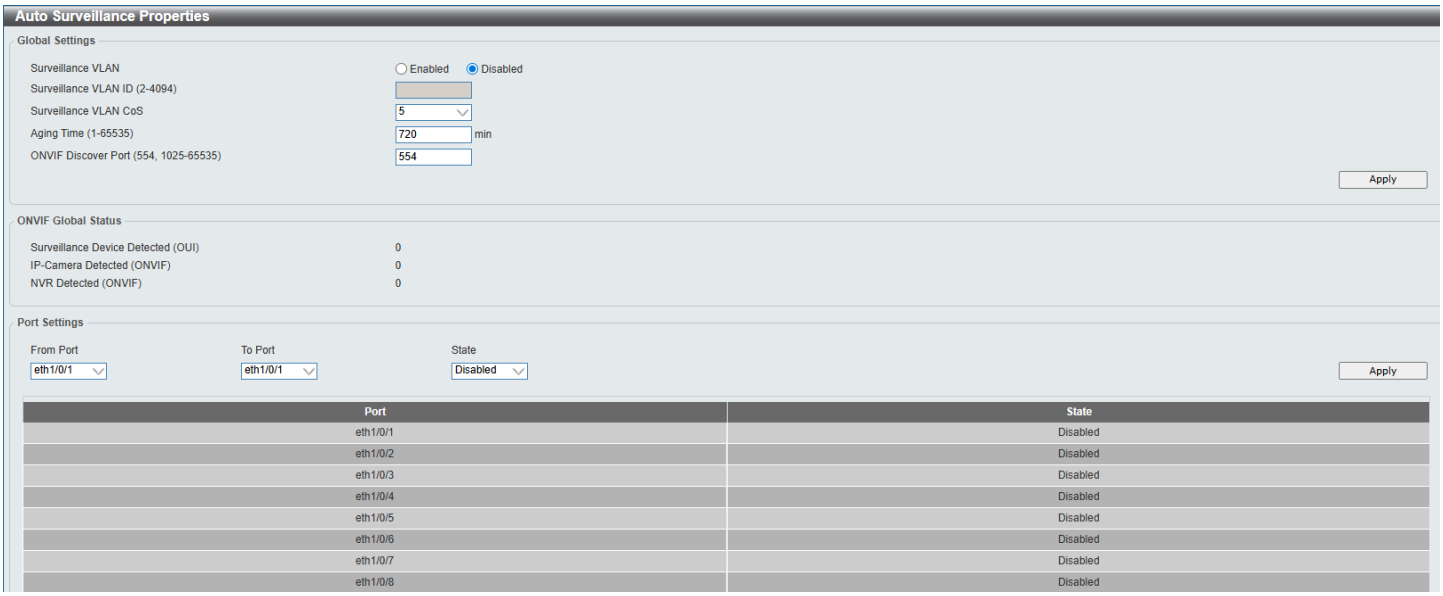
This page shows the GVRP related statistics counters.



L2 Features > GVRP > GVRP Statistics Table

L2 Features > Auto Surveillance VLAN > Auto Surveillance Properties

The Auto Surveillance Properties page is used to configure the auto surveillance VLAN global settings and display the ports surveillance VLAN information.



L2 Features > Auto Surveillance VLAN > Auto Surveillance Properties

Global Settings:

Surveillance VLAN: Specify to enable or disable the surveillance VLAN state.

Surveillance VLAN ID: Enter the surveillance VLAN ID. The range is from 1 to 4094.

Surveillance VLAN CoS: Specify the priority of the surveillance VLAN from 0 to 7.

Aging Time: Specify the aging time of the surveillance VLAN. The range is from 1 to 65535 minutes. The default value is 720 minutes. The aging time is used to remove a port from surveillance VLAN if the port is an automatic surveillance VLAN member. When the last surveillance device 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 counter will be reset and the timer will stop.

Click the **Apply** button to save your settings.

Port Settings:

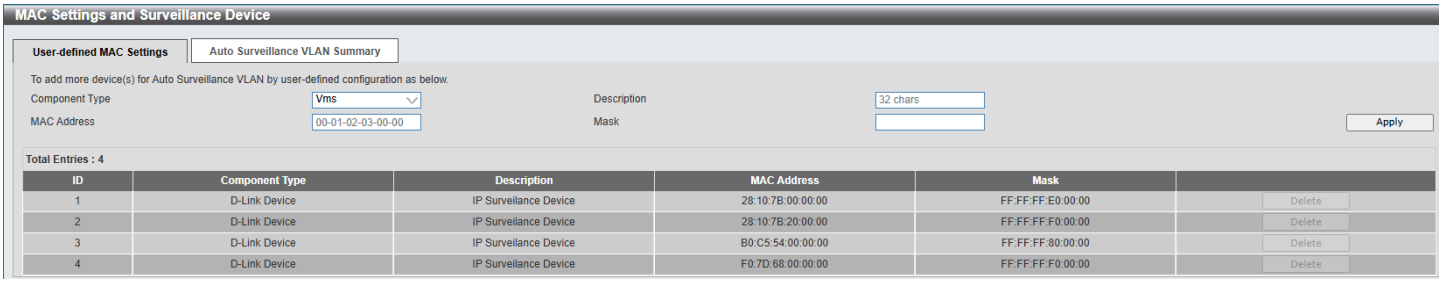
From Port/To Port: Specify the port range used for the configuration.

State: Specify to enable or disable the state of the port.

Click the **Apply** button to save your settings.

L2 Features > Auto Surveillance VLAN > MAC Settings and Surveillance Device

The MAC Settings and Surveillance Device page is used to configure the user-defined surveillance device OUI and display the surveillance VLAN information.



L2 Features > Auto Surveillance VLAN > MAC Settings and Surveillance Device

Component Type: Specify the surveillance component type. Option to choose from are **Vms**, **VmsClient**, **VideoEncoder**, **NetworkStorage** and **Other**.

Description: Enter the description for the user-defined OUI with a maximum of 32 characters.

MAC Address: Enter the OUI MAC address.

Mask: Enter the OUI MAC address matching bitmask.

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

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

After click the **Auto Surveillance VLAN Summary** tab, the following page will appear.

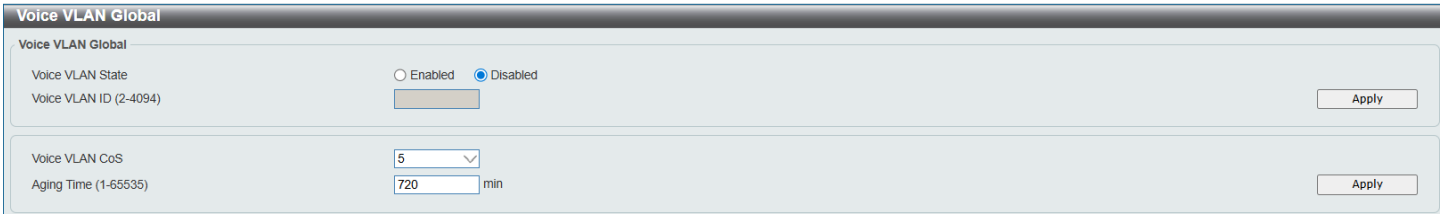


L2 Features > Auto Surveillance VLAN > MAC Settings and Surveillance Device

L2 Features > Voice VLAN > Voice VLAN Global

The Voice VLAN is a VLAN used to carry voice traffic from an IP phone. As the sound quality of Voice over IP, is sensitive to delay Quality of service (QoS) for voice traffic should be configured to ensure that voice traffic is handled with a higher priority.

The switches determine whether a received packet is a voice packet by checking its source MAC address. If the source MAC addresses of a packet complies with the organizationally unique identifier (OUI) addresses configured by the system, the packets are determined as voice packets and transmitted in voice VLAN.



L2 Features > Voice VLAN > Voice VLAN Global Settings

Voice VLAN State: Select to enable or disable Voice VLAN.

VLAN ID (1-4094): Enter the voice VLAN ID. The value is range from 1 to 4094.

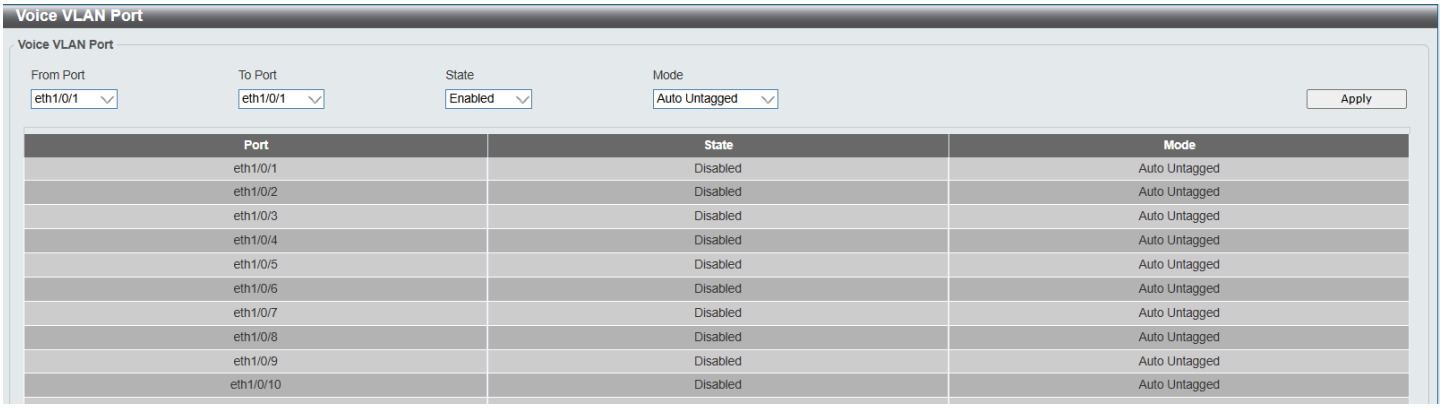
Voice VLAN CoS: Specify the priority of the voice VLAN from 0 to 7.

Aging Time: Enter the aging time of voice VLAN. The range is from 1 to 65535 minutes. The default value is 720 minutes. The aging time is used to remove a port from voice VLAN if the port is an automatic VLAN member. When the last voice device stops sending traffic and the MAC address of this voice device is aged out, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after expiration of voice VLAN aging timer. If the voice traffic resumes during the aging time, the aging counter will be reset and the timer will stop.

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

L2 Features > Voice VLAN > Voice VLAN Port

The Voice VLAN Port page is used to show the ports voice VLAN information.



L2 Features > Voice VLAN > Voice VLAN Port

From Port / To Port: Select the appropriate port range used for the configuration.

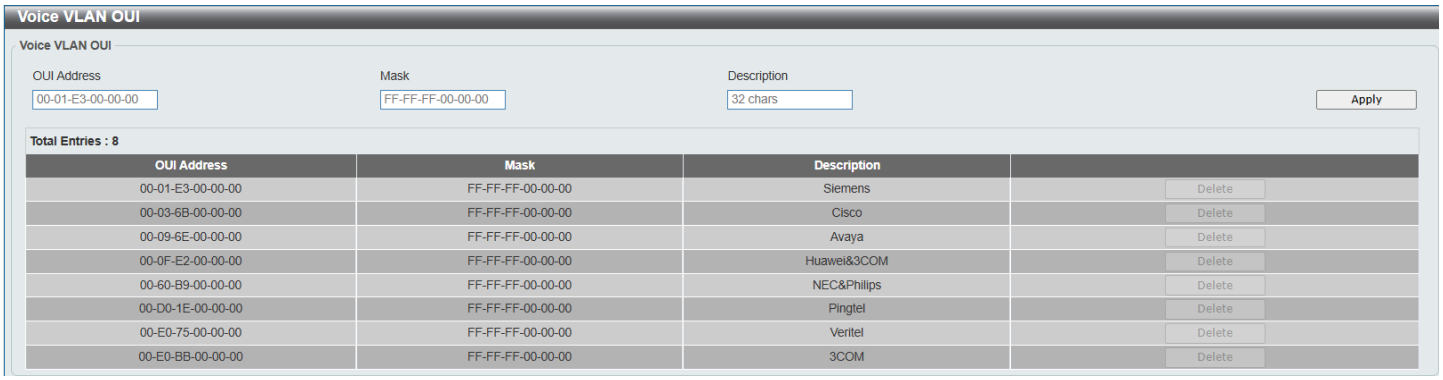
State: Specify to enable or disable the state of the port.

Mode: Specify the mode of the port. Options to choose from are **Auto Untagged**, **Auto Tagged**, and **Manual**.

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

L2 Features > Voice VLAN > Voice VLAN OUI

The Voice VLAN OUI page is used to configure the user-defined voice traffic's OUI. The OUI is used to identify voice traffic. There are a number of pre-defined OUIs. The user can further define the user-defined OUIs if needed. The user-defined OUI cannot be the same as the pre-defined OUI.



L2 Features > Voice VLAN > Voice VLAN OUI

OUI Address: Specify the OUI MAC address.

Mask: Specify the OUI MAC address matching bitmask.

Description: Enter the description for the user-defined OUI with a maximum of 32 characters.

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

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

L2 Features > Voice VLAN > Voice VLAN Device

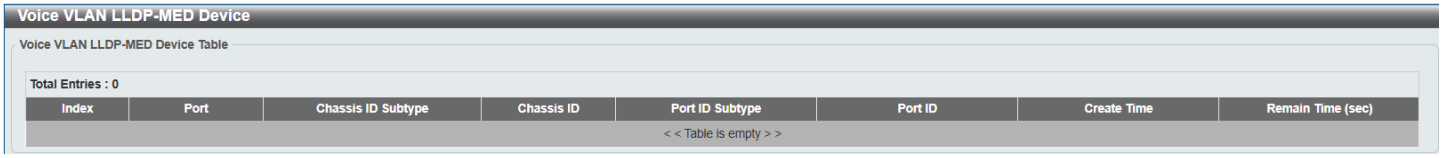
The Voice VLAN Device page is used to show voice devices that are connected to the Switch. The Start Time is the time when the device was detected on the port and the Status displays the voice VLAN status of the port.



L2 Features > Voice VLAN > Voice VLAN Device

L2 Features > Voice VLAN > Voice VLAN LLDP-MED Device

The page displays the Voice VLAN LLDP-MED voice devices connected to the Switch.



L2 Features > Voice VLAN > Voice VLAN LLDP-MED Device

L2 Features > STP > STP Global Settings

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

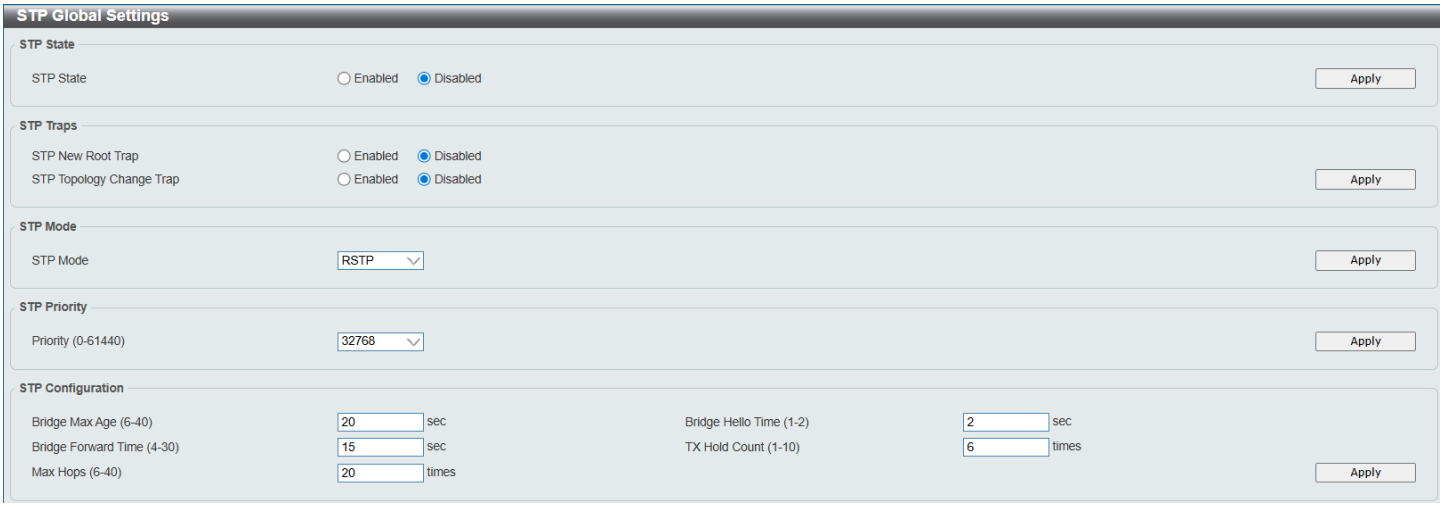
The Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1D STP standard and was developed in order to overcome some of the limitations of STP that impede the function of some recent switching innovations. The basic function and much of the terminology is the same and most of the settings configured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

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

By default, Rapid Spanning Tree is disabled. If enabled, the Switch will listen for Bridge Protocol Data Unit (BPDU) packets and its accompanying Hello packet. The BPDU packets are sent even if a BPDU packet is 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.

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

After enabling STP, configure the STP Global Settings (shown below).



L2 Features > STP > STP Global Settings

STP State:

STP State: Select to enable or disable the Spanning Tree Protocol.

Click the **Apply** button to save your settings.

STP Traps:

STP New Root Trap: Select to enable or disable the STP new root trap option.

STP Topology Change Trap: Select to enable or disable the STP topology change trap option.

Click the **Apply** button to save your settings.

STP Mode:

STP Mode: Select the STP mode. The options to choose from are MSTP, RSTP and STP.

Click the **Apply** button to save your settings.

STP Priority:

Priority (0-61440): Enter the STP priority value. This value is between 0 and 61440. By default, this value is 32768. The lower the value, the higher the priority.

Click the **Apply** button to save your settings.

STP Configuration:

Bridge Max Age (6-40): Enter the bridge's maximum age value here. This value must be between 6 and 40 seconds. By default, this value is 20 seconds. The maximum age value may be set to ensure that old information does not endlessly circulate throughout the network. Set by the root bridge, this value ensures that the Switch has spanning tree configuration consistent with other devices on the LAN.

Bridge Forward Time (4-30): Enter the bridge's forwarding time value. This value must be between 4 and 30 seconds. By default, this value is 15 seconds. Any port on the Switch spends this time in the listening state while moving from the blocking state to the forwarding state.

Max Hops (1-40): Enter the maximum number of hops that are allowed. This value must be between 1 and 40 hops. By default, this value is 20 hops. This value is used to set the number of hops between devices in a spanning tree region before the BPDU packet sent by the Switch will is 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.

Bridge Hello Time (0-2): After selecting **RSTP/STP** as the **STP Mode**, this parameter will be available. Enter the bridge's hello time value here. This value must be between 1 and 2 seconds. By default, this value is 2 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to all switches. This field will only appear when STP or RSTP is selected for the STP Version.

For MSTP, the Hello Time must be set on a port by port basis in "STP Port Settings" page (please refer to the following section).

TX Hold Count (1-10): Enter the transmit hold count value. This value must be between 1 and 10. The default value is 6. This value is used to set the maximum number of Hello packets transmitted per interval.

MPT Instance ID Settings:

Instance ID (1-32): Instance ID for Multi-Process RSTP

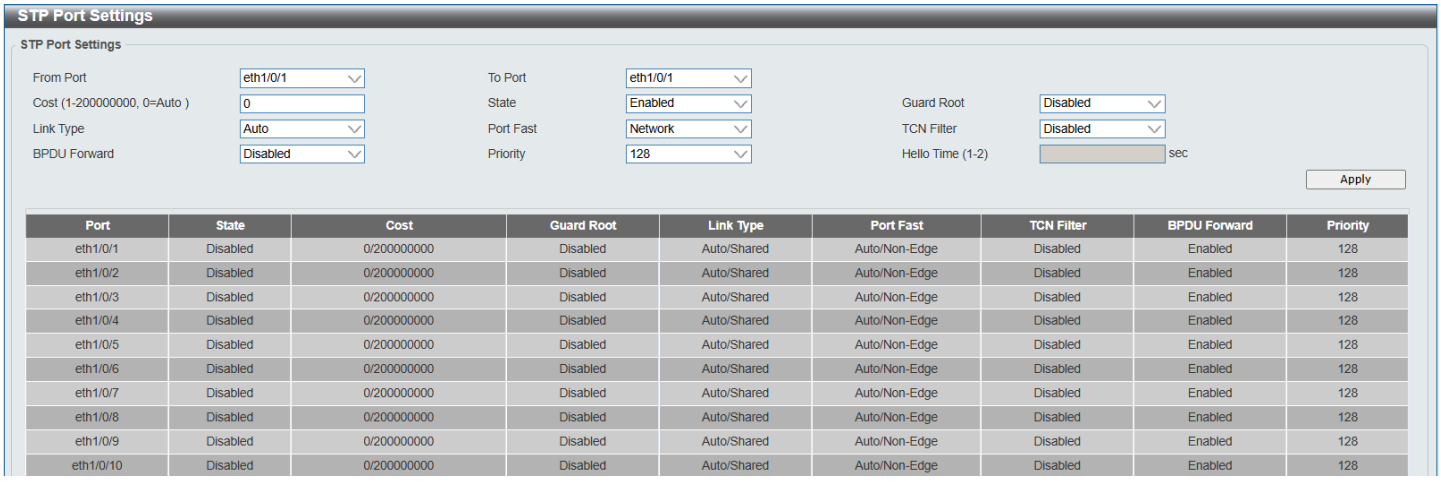
Click the **Apply** button to save your settings.

L2 Features > STP > STP Port Settings

In addition to setting spanning tree parameters for use on the switch level, the Switch allows for the configuration of STP on a port level Groups of ports can be configured in a port group, each of which can have its own spanning tree instance and configuration settings.

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

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



L2 Features > STP > STP Port Settings

From Port/To Port: Enter a consecutive group of ports to be configured starting with the selected port.

Cost: This is the STP port cost, which is used to calculate the spanning tree topology. tf represents the relative interface bandwidth and is the desirability of the link. The port cost can be set automatically or set manually as a metric value. The default value is *0* (auto).

> **0 (auto):** Setting 0 for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = 200000. Gigabit port = 20000. 2.5G = 8,000, 5G = 4,000, 10G = 2,000
>
> **Value 1-200000000:** Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets.

State: Select to enable or disable port based STP. It will be selectable after STP is enabled globally on the Switch.

Guard Root: Select to enable or disable the guard root function.

Link Type: Select the link type option. The options to choose from are **Auto**, **P2P**, and **Shared**. A full-duplex port is considered to have a point-to-point (**P2P**) connection. A half-duplex port is considered to have a **Shared** connection. The port cannot rapidly transition to the forwarding state if the link type is set to **Shared**. By default this option is **Auto**.

Port Fast: Select the port fast option. The options are **Network**, **Disabled**, and **Edge**. In the **Network** mode the port will remain in the non-port, fast state for three seconds. If no BPDUs are received the port will be put into the forwarding state.

If the port receives a BPDU, it will change back to the non-port fast state. This is the default port fast mode. In the **Disabled** mode, the port will always be in the non-port fast state. It will wait for the forward-time delay to change to the forwarding state. In the **Edge** mode, the port will directly change to the forwarding state without waiting for the forward-time delay. If the interface receives a BPDU, its operation state changes to the non-port fast state.

TCN Filter: Select to enable or disable the TCN filter option. Enabling TCN filtering on a port is useful for connecting to an external network, which may not be under full control of the administrator. When a port is set to the TCN filter mode, the topology change event received by the port will be ignored. By default, this option is disabled.

BPDU Forward: Bridges use Bridge Protocol Data Units (BPDUs) in the operation of spanning tree, BPDU. Forwarding is useful when a bridge interconnects two regions, with each region requiring a separate spanning tree. BPDU filtering functions only when STP is disabled either globally or on a single interface. The possible field values are:

Disabled: BPDU filtering is enabled on the port.

Enabled: BPDU forwarding is enabled on the port (STP must be disabled).

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

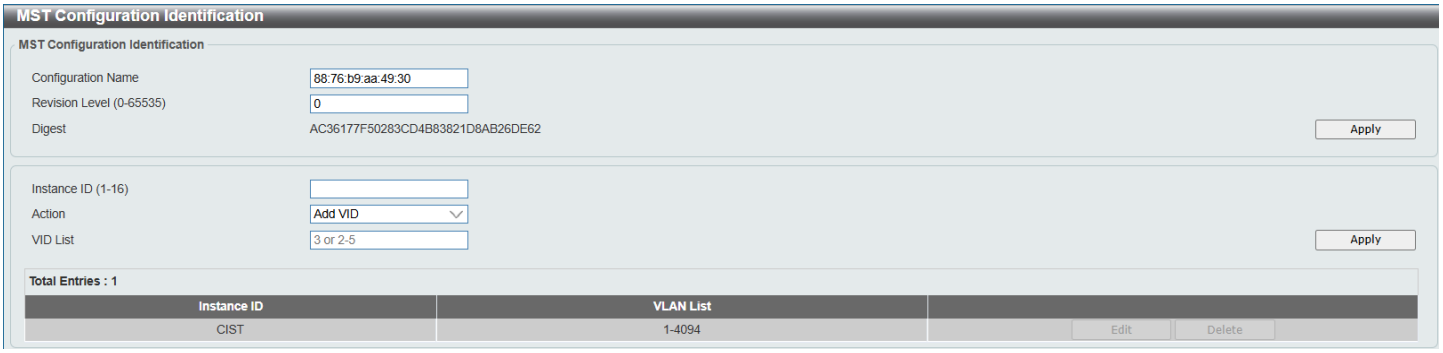
Hello Time: The interval between two transmissions of BPDU packets sent by the Root Bridge to indicate to all other switches that it is indeed the Root Bridge. This parameter applied in **MSTP** mode only. The default value is 2.

Click the **Apply** button to save your settings.

L2 Features > STP > MST Configuration Identification

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

The MST Configuration Identification page is for defining global MSTP settings, including region names, MSTP revision level.



L2 Features > STP > MST Configuration Identification

MST Configuration Identification:

Configuration Name: Enter a name set on the switch to uniquely identify the MSTI (multiple spanning tree instance). If a configuration name is not set, this field shows the MAC address of the device running MSTP.

Revision Level(0 - 65535): This value, together with the configuration name and identical VLANs mapped for STP instance IDs identifies the MST region configured on the switch.

Click **Apply** to define the configuration name and revision level.

Instance ID Settings:

Instance ID (1 - 64): Enter the MSTI ID associated with the VID List. The possible field range is 1-64.

Action: The possible values are:

Add VID - Indicates that the edit type is add.

Remove VID - Indicates that the edit type is removed.

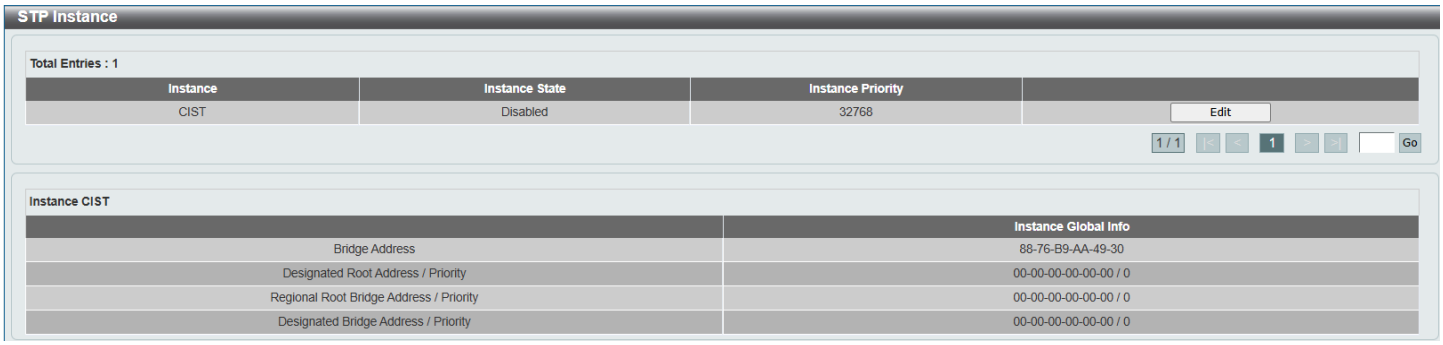
VID List: Enter the VID range from configured VLANs set on the Switch.

Click the **Apply** button to save your settings.

Click the **Edit** to modify the setting of VID or click **Delete** to remove it.

L2 Features > STP > STP Instance

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



L2 Features > STP > STP Instance

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

L2 Features > STP > MSTP Port Information

The MSTP Port Information page allows you to configure the MSTP Interface settings.



L2 Features > STP > MSTP Port Information

Port: Enter the port to find.

Click the **Clear Detected Protocol** button to clear the detected protocol settings for the port selected.

Click **Find** to search the MSTP port information.

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

L2 Features > ERPS(G.8032) > ERPS

ERPS (Ethernet Ring Protection Switching) is the first industry standard (ITU-T G.8032) for Ethernet ring protection switching. It is achieved by integrating mature Ethernet Operations, Administration, and Maintenance (OAM)* functions and a simple automatic protection switching (APS) protocol for Ethernet ring networks. ERPS provides sub-50ms failover for Ethernet traffic in a ring topology. It ensures that there are no loops formed at the Ethernet layer.

One link within a ring, the ring Protection Link (RPL), will be blocked to avoid a Layer 2 loop. When there is a failure, 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.

The ERPS page allows you to configure the ERPS instance and profile configuration of the Switch.



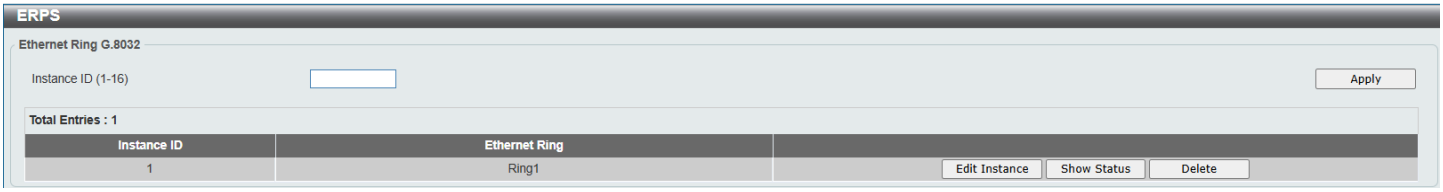
L2 Features > ERPS(G.8032) > ERPS

Instance ID (1-16): Specify the Instance ID to be created.

Click the **Apply** button to save your settings.

NOTE: STP and LBD should be disabled on the ring ports before enabling ERPS.

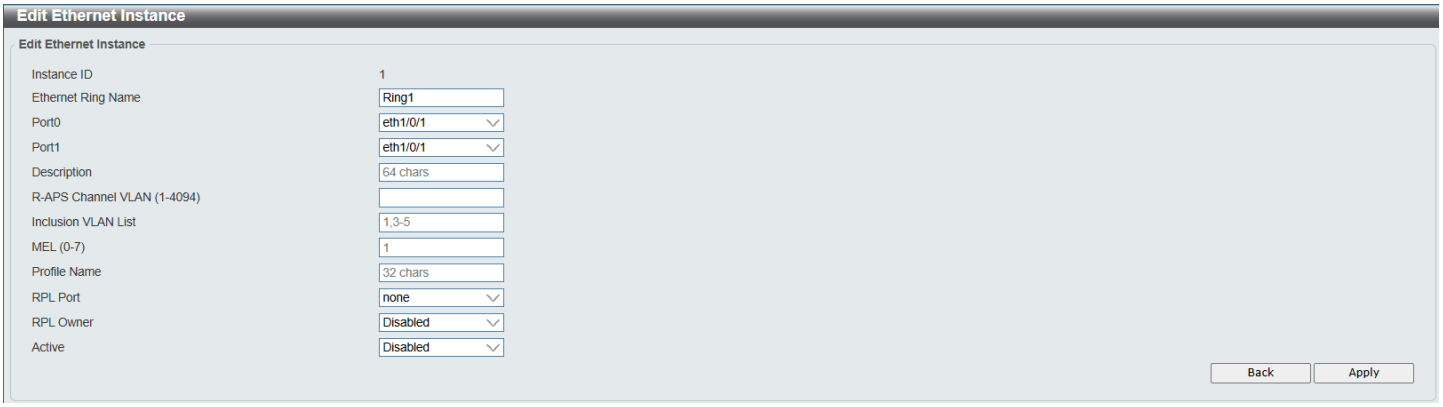
Enter instance ID 1 and click **Apply** to create ERPS physical ring. Then the following page will be displayed.



L2 Features > ERPS(G.8032) > ERPS - Create

Click **Edit Instance** button to modify the ERP instance, click **Show Status** button to display the ERPS physical ring's status information, or click **Delete** button to remove the Ethernet instance.

Click **Edit Instance** to modify the Ethernet Instance configuration:



L2 Features > ERPS(G.8032) > ERPS – Edit Instance

Ethernet Ring Name: Enter the Ethernet ring name for the specified instance.

Port0: Specifies the port as the first ring port and also specifies the virtual port channel used.

Port1: Specifies the port as the second ring port and also specifies the virtual port channel used.

Description: Enter the description for the specified instance.

R-APS Channel VLAN (1-4094): Specifies the R-APS channel of ERP instance. The range is between 1 and 4094.

Inclusion VLAN List: Specifies to add or delete the inclusion VLAN group. The VLANs specified here will be protected by the ERP mechanism.

MEL(0-7): Specifies the ring MEL of the R-APS function. The default ring MEL is 1.

Profile Name: Specifies the profile name of Ethernet Instance.

RPL Port: Specifies the RPL port used. Options to choose from are Port0, Port1, and None.

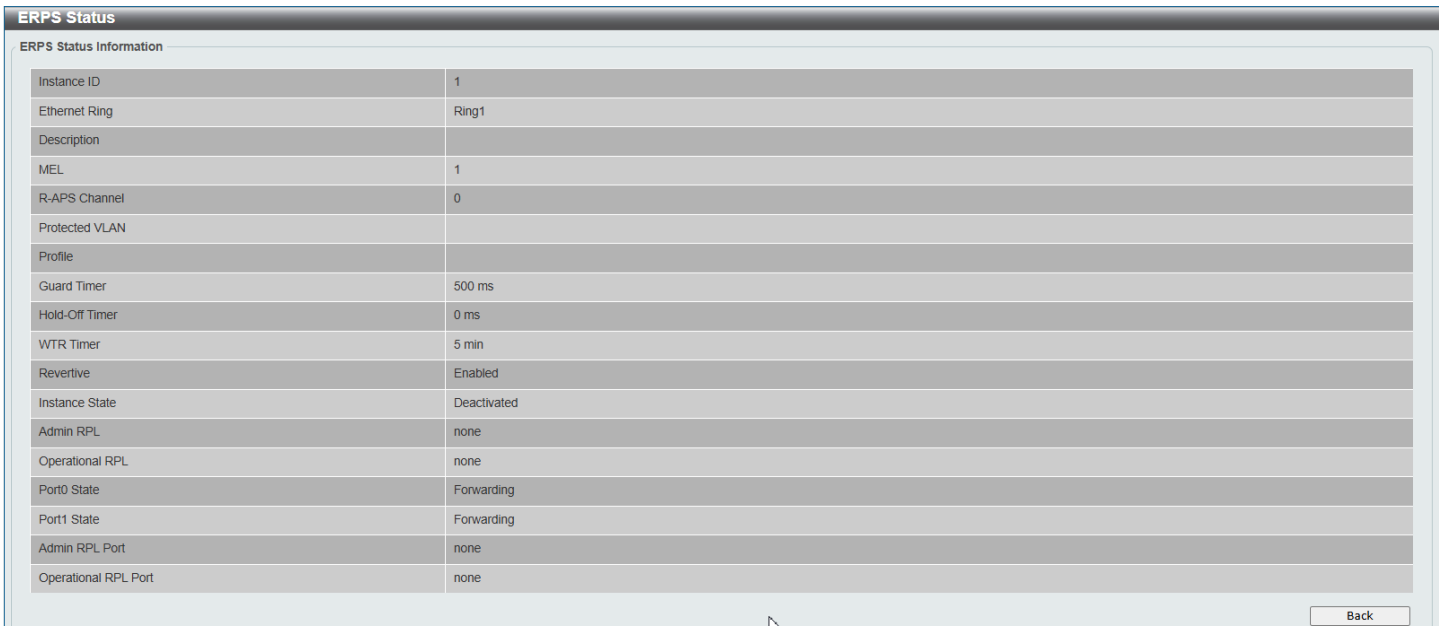
RPL Owner: Specifies to enable or disable the RPL owner node.

Active: Specifies enable or disable to active this ERP instance.

Click the **Apply** button to save your settings.

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

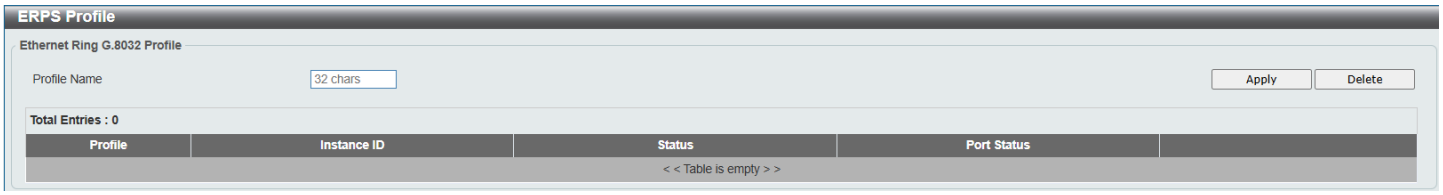
Click **Show Status** button to display the ERPS status information.



L2 Features > ERPS(G.8032) > ERPS – Show Status

L2 Features > ERPS(G.8032) > ERPS Profile

The ERPS Profile page allows you to configure the ERPS profile information of the Switch.

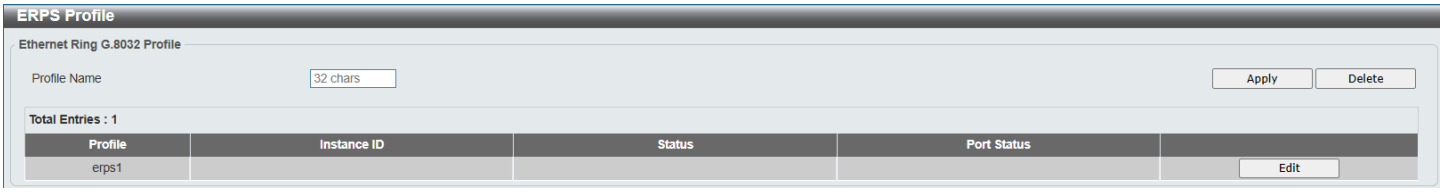


L2 Features > ERPS(G.8032) > ERPS Profile

Profile Name: Specify the profile name to be created on the Switch.

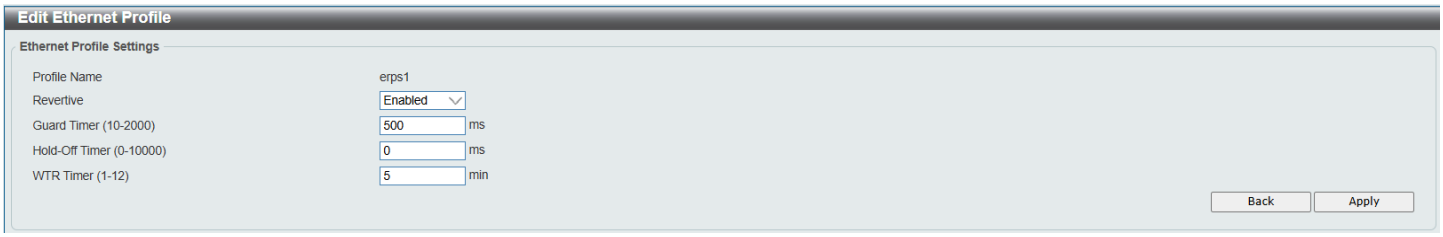
Click the **Apply** button to save your settings.
Click the **Delete** button to remove the profile.

Enter **Profile Name** and click **Apply** button to associate the G.8032 profile with the ERP instance created.



L2 Features > ERPS(G.8032) > ERPS Profile - created

Click **Edit** button to configure the Ethernet Profile settings:



L2 Features > ERPS(G.8032) > ERPS Profile - Edit

Revertive: Specifies whether to enable or disable to the original state after a failure, for example, when the RPL was blocked.

Guard Time (10-2000): Specifies the guard time of the R-APS function. The value is between 10 and 2000 milliseconds. The default guard time is 500 milliseconds.

Hold-Off Timer (0-10000): Specifies the hold-off time of the R-APS function. The value is between 0 and 10000 milliseconds. The default hold-off time is 0 milliseconds.

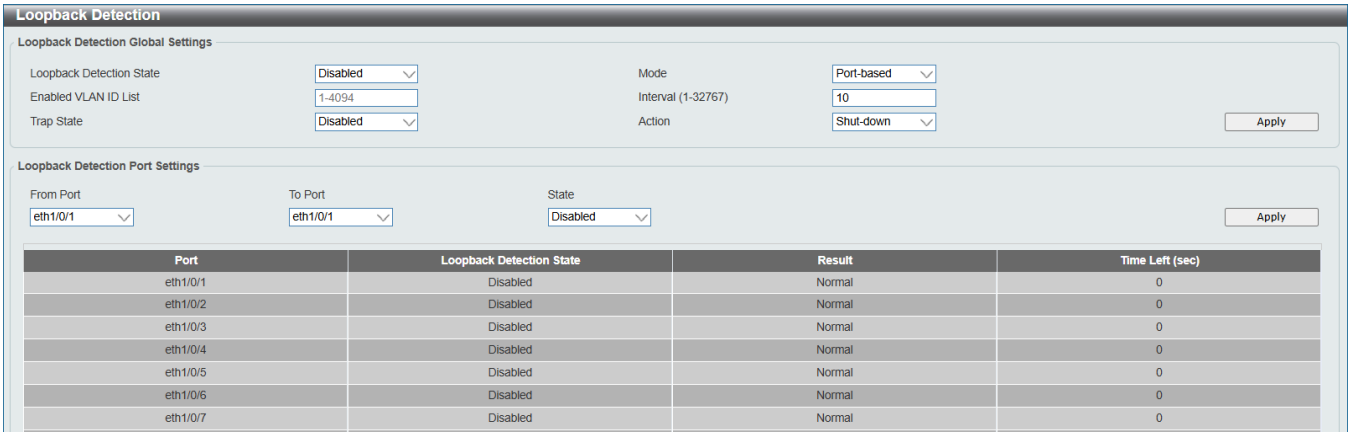
WTR Timer (1-12): Specifies the WTR time of the R-APS function. The value is between 1 and 12 minutes. The default WTR time is 5 minutes.

Click the **Apply** button to save your settings.

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

L2 Features > Loopback Detection

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



L2 Features > Loopback Detection Settings

Loopback Detection State: Enable or disable loopback detection. The default is *disabled.*

Mode: Select either Port-based or VLAN-based loopback detection.

Enabled VLAN ID List: Enter the VLAN ID for loopback detection. This only takes effect when **VLAN-based** is selected in the **Mode** drop-down list.

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

Trap State: Select to enable or disable the loopback detection trap state.
Action: Select **Shut-down** or **None** for loopback detection.

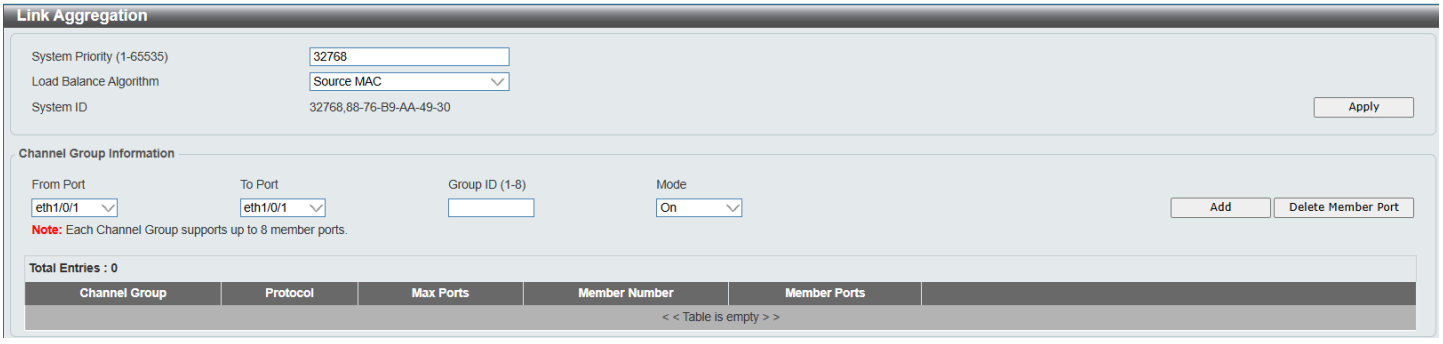
From Port / To Port: Enter a consecutive group of ports to be configured starting with the selected port.

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

Click the **Apply** button to save your settings.

L2 Features > Link Aggregation

The Link Aggregation page allows you to view and configure the link aggregation settings.



L2 Features > Link Aggregation

System Priority (1-65535): Enter the system's priority value. This must be between 1 and 65535. By default, the value is 32768. The system priority determines which system turns into "Actor" role. 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: Specify the load balancing algorithm that will be used. Options to choose from are: **Source MAC**, **Destination MAC**, **Source Destination MAC**, **Source IP**, **Destination IP**, and **Source Destination IP**. By default, this option is **Source MAC**.
System ID: The **System ID** information.

Click the **Apply** button to save your settings.

Channel Group Information:

From Port / To Port: Select the appropriate port range used for the configuration.
Group ID: Enter the channel-group number. This value must be between 1 and 8. The system will automatically create the port-channel when a physical port first joins a channel-group. An interface can only join one channel-group.
Mode: Select either **On**, **Active**, or **Passive**. If you selected **On**, the channel-group type is static. If **Active** or **Passive** is selected, 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.

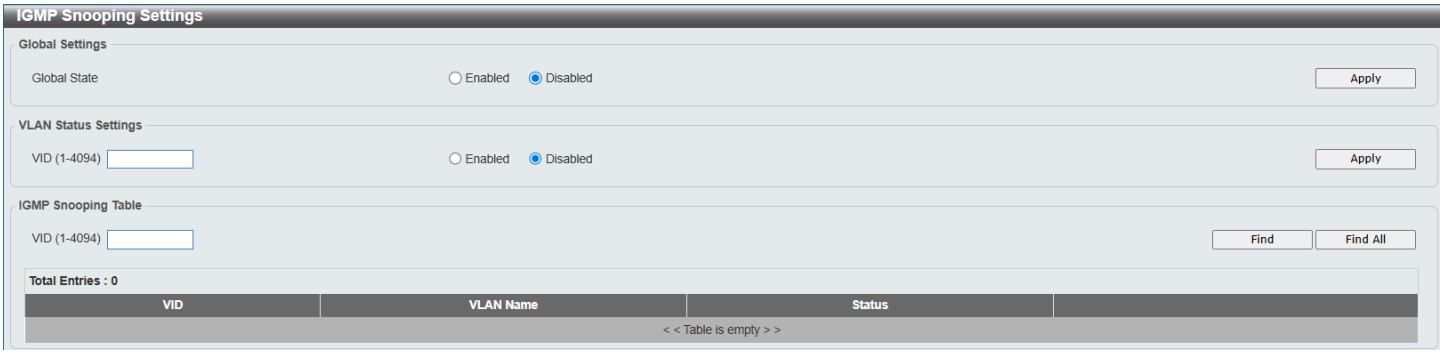
Click the **Add** button to add a new entry based on the information entered.
Click the **Delete Member Port** button to remove the specific member port.
Click the **Delete Channel** button to remove the specific entry.
Click the **Channel Detail** button to view more detailed information about the channel.

L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Settings

With Internet Group Management Protocol (IGMP) snooping, the DGS-1250 Series Switch can make intelligent multicast forwarding decisions by examining the contents of each frame's Layer 2 MAC header.

IGMP snooping can help reduce cluttered traffic on the LAN. With IGMP snooping enabled globally, the DGS-1250 Series Switch will forward multicast traffic only to connections that have group members attached.

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



L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Settings

Global Settings:

Global State: Select to enable or disable the IGMP Snooping global state.

Click the **Apply** button to save your settings.

VLAN Status Settings:

VID (1-4094): Enter the VLAN ID and select to enable or disable the IGMP snooping on the VLAN.

Click the **Apply** button to save your settings.

IGMP Snooping Table:

VID (1-4094): Enter the VLAN ID between 1 and 4094.

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

Click the **Find All** button to display all the entries.

Click the **Show Detail** button to display the detail information of the specified VLAN.

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

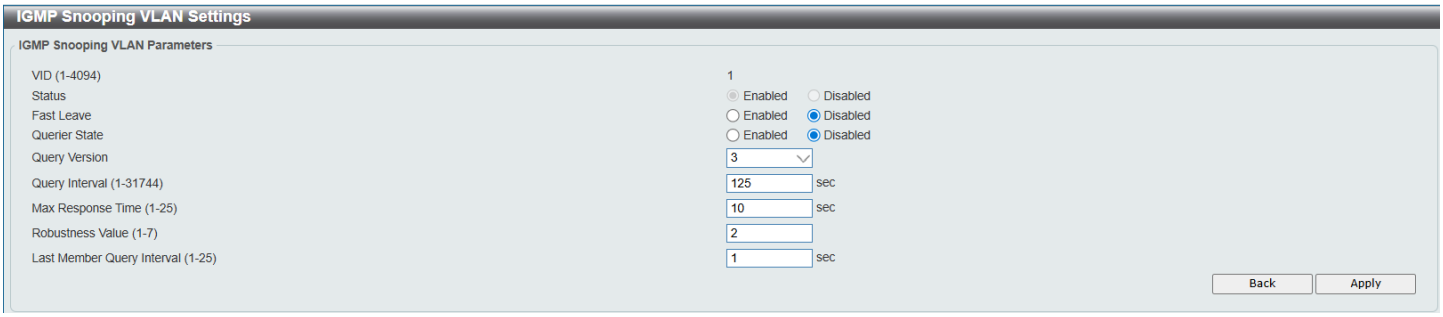
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

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



L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping – Show Detail

Click the **Modify** button to edit the information in the following window:



L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping – Modify

The following parameters can be configured:

Fast Leave: Select to enable or disable the IGMP snooping fast leave function.

Querier State: Select to enable or disable the querier state.

Query Version: Select the general query packet version sent by the IGMP snooping querier.

Query Interval (1-31744): Enter the interval at which the IGMP snooping querier sends IGMP general query messages periodically.

Max. Response Time (1-25): Enter the maximum response time. The range is between 1 and 25 seconds.

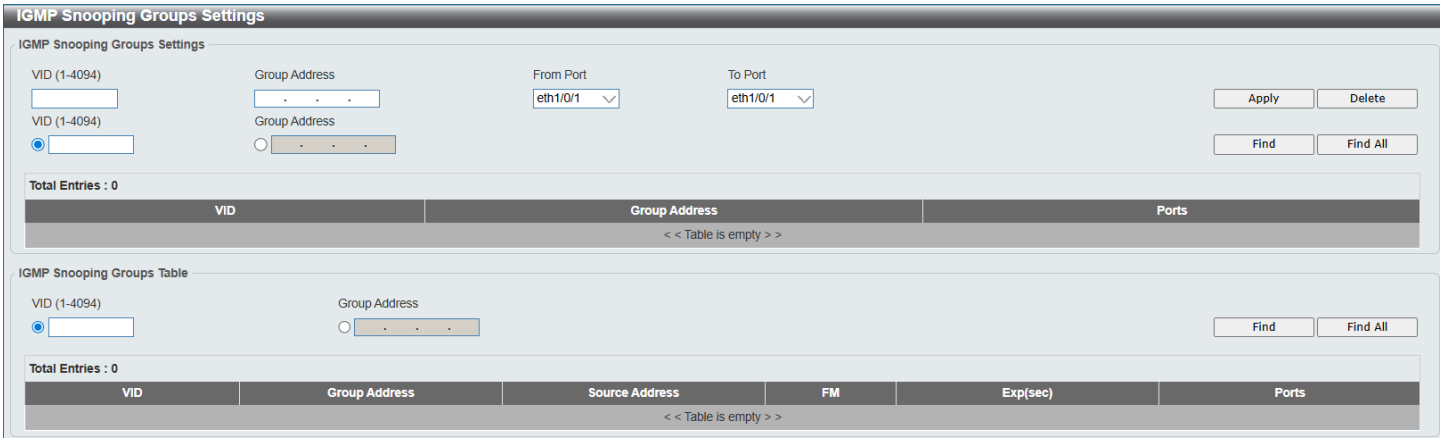
Robustness Value (1-7): Enter the robustness variable used in IGMP snooping.

Last Member Query Interval (1-25): Enter the interval at which the IGMP snooping querier sends IGMP group-specific or group-source-specific query messages.

Click the **Apply** button to save your settings.

L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Groups Settings

The IGMP snooping Groups Settings page allows you to configure and view the IGMP snooping static group, and view IGMP snooping group.



L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Group Settings

VID (1-4094): Enter the VLAN ID.
Group Address: Enter the IP multicast group address.
From Port / To Port: Select the range of ports to be configured.

Click the **Apply** button to save your settings.
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 **Find 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.

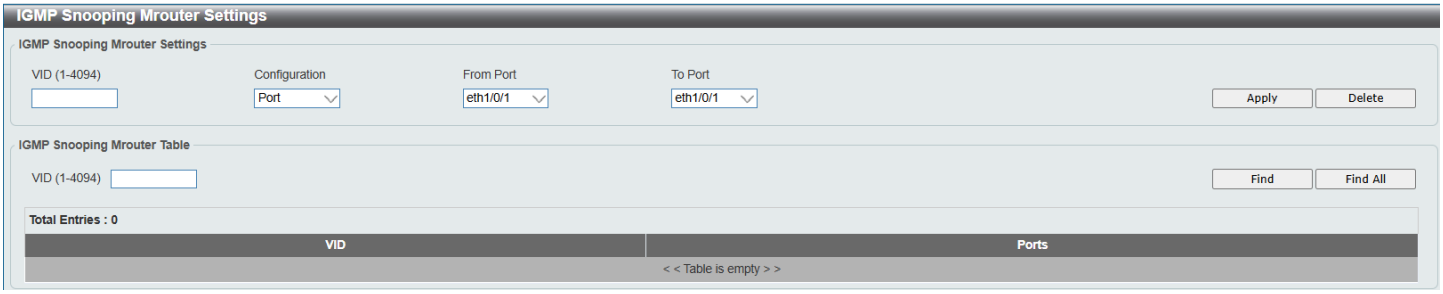
The fields that can be configured for **IGMP Snooping Groups Table** are described below:

IGMP Snooping Group Table:
VID (1-4094): Specify the VLAN ID.
Group Address: Click the radio button and enter an IP multicast group address.

Click the **Find** button to locate a specific entry based on the information entered.
Click the **Find All** button to view all the entries.

L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Mrouter Settings

The IGMP Snooping Mrouter Settings page allows you to configure interfaces as multicast router ports or ports that cannot be multicast router ports on the Switch.



L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Mrouter Settings

VID (1-4094): Enter the VLAN ID in the range 1 to 4094.
Configuration: Select the port configuration type.
- **Port:** Select to configure the port as a static multicast router port.
- **Forbidden Port:** Select to configure the port as a port that cannot be a static multicast router port.

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

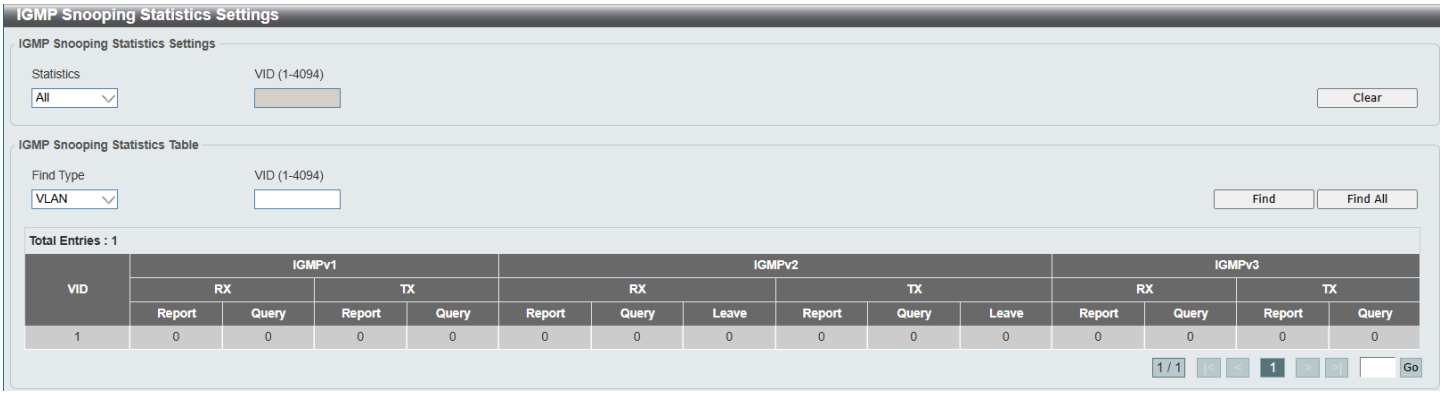
Click the **Apply** button to save your settings.
Click the **Delete** button to remove the specified entry.

The IGMP Snooping Mrouter Table is showed as below:
VID (1-4094): Enter the VLAN ID to be searched.

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

L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Statistics Settings

The IGMP Snooping Statistics Settings page allows you to clear and display the IGMP snooping related statistics.



L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Statistics Settings

Statistics: Select the interface to be cleared. The options are All and VLAN.
VID (1-4094): Enter the VLAN ID.
Click the **Clear** button to clear the IGMP snooping related statistics.

The fields that can be configured for **IGMP Snooping Statistics Table** are listed below:
Find Type: Select the interface to be searched. The options are **VLAN** and **Port**.
VID (1-4094): Enter the VLAN ID.

Click the **Find** button to locate a specific entry based on the information entered.
Click the **Find All** button to view all the entries.

L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Setting

The MLD Snooping Settings page allows you to configure the MLD snooping settings.



L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Setting

Global Settings:
Global State: Select to enable or disable the MLD Snooping state.
Click the **Apply** button to save your settings.

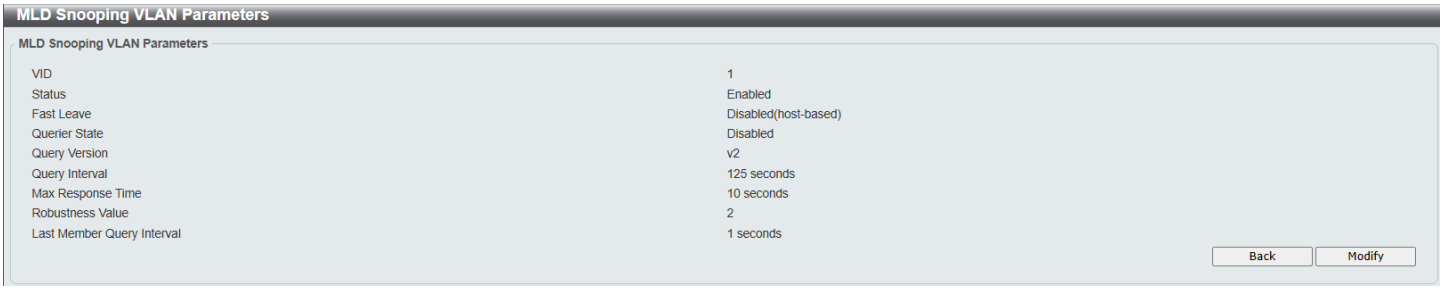
VLAN Status Settings:
VID (1-4094): Enter the VLAN ID and select to enable or disable MLD snooping on the VLAN.
Click the **Apply** button to save your settings.

MLD Snooping Table:
VID (1-4094): Enter the VLAN ID to be searched.

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

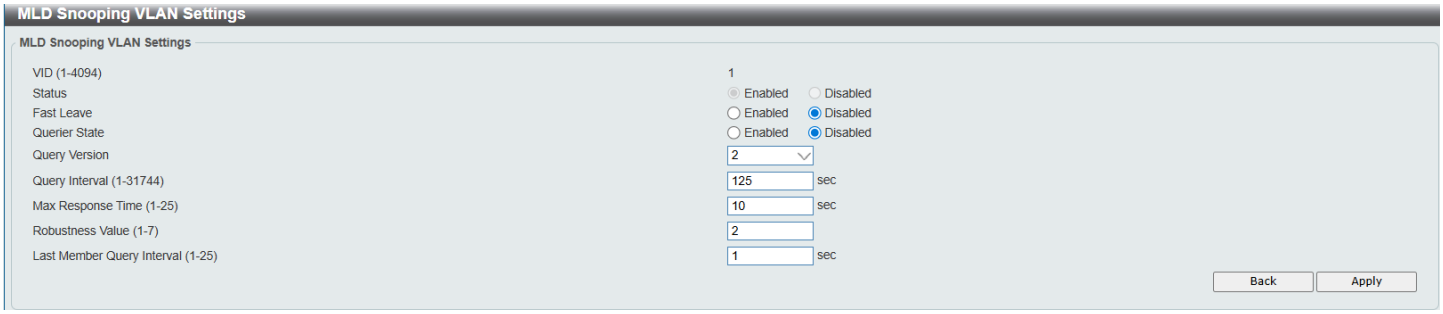
After clicking the **Show Detail** button, the following window will appear.



L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Setting – Show Detail

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 **Edit** button in MLD Snooping Settings window, the following window will appear.



L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Setting – Edit

Fast Leave: Select to enable or disable the MLD snooping fast leave function.

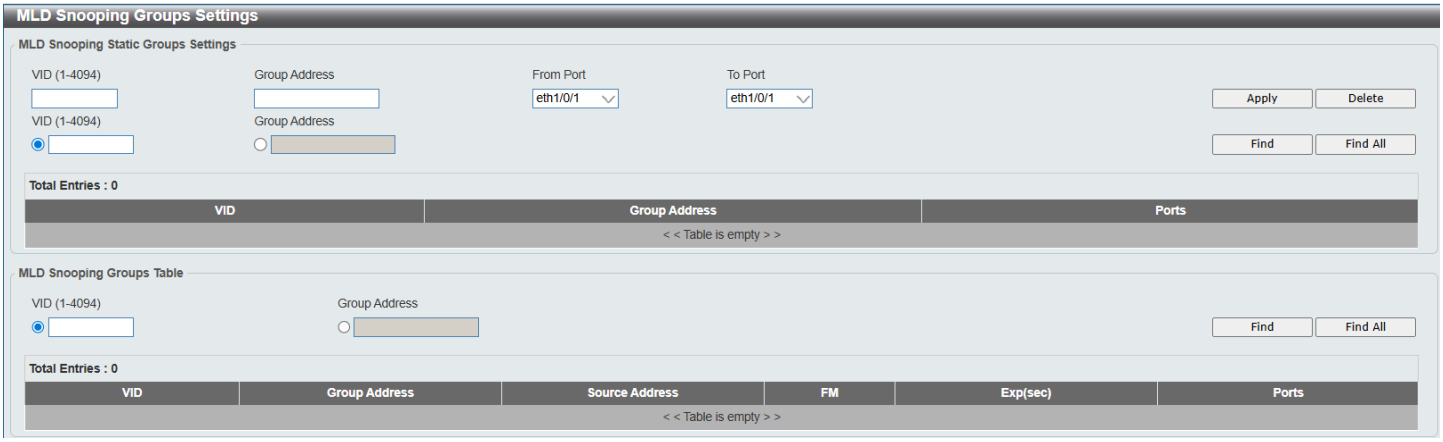
Querier State: Select to enable or disable the querier state.

Query Version: Select the general query packet version sent by the MLD snooping querier.
Query Interval (1-31744): Enter the interval at which the MLD snooping querier sends MLD general query messages periodically.
Max. Response Time (1-25): Enter the maximum response time, in seconds, advertised in MLD snooping queries. The range is 1 to 25.
Robustness Value (1-7): Enter the robustness variable used in MLD snooping.
Last Member Query Interval (1-25): Enter the interval at which the MLD snooping querier sends MLD group-specific or group-source-specific (channel) query messages.

Click the **Apply** button to save your settings.

L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Groups Setting

The MLD Snooping Groups Settings page allows you to configure and view the MLD snooping static group, and view MLD snooping group.



L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Group Setting

VID (1-4094): Enter the VLAN ID.
Group Address: Enter the IP multicast group address.
From Port / To Port: Select the range of ports to be configured.

Click the **Apply** button to save your settings.
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 **Find 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 for the **MLD Snooping Groups Table** are described below:
VID (1-4094): Enter the VLAN ID.
Group Address: Enter the IP multicast group address.
Click the **Find Snooping** button to locate a specific entry based on the information entered.
Click the **Find All Snooping** button to view all the entries.

L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Mrouter Settings

The MLD Snooping Mrouter Settings page allows you to configure the interfaces as router ports or ports that cannot be multicast router ports on the Switch.



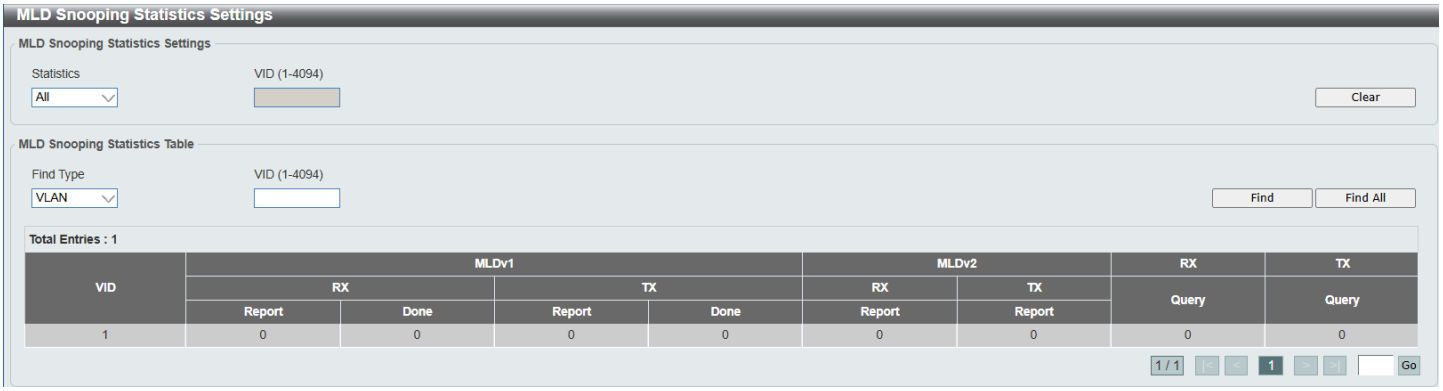
L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Mrouter Settings

VID (1-4094): Enter the VLAN ID.
Configuration: Select the port configuration type.
Port: Select to configure the port as being connected to a multicast-enabled router.
Forbidden Port: Select to configure the port as not being connected to a multicast-enabled router.
From Port / To Port: Select the range of ports to be configured.

Click the **Apply** button to save your settings.
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 **Find 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.

L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Statistics Settings

The MLD Snooping Statistics Settings page allows you to clear and display the MLD snooping related statistics.



L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Statistics Settings

Statistics: Select the type of statistics to display. Available options are **All** and **VLAN.**

VID (1-4094): Enter the VLAN ID.

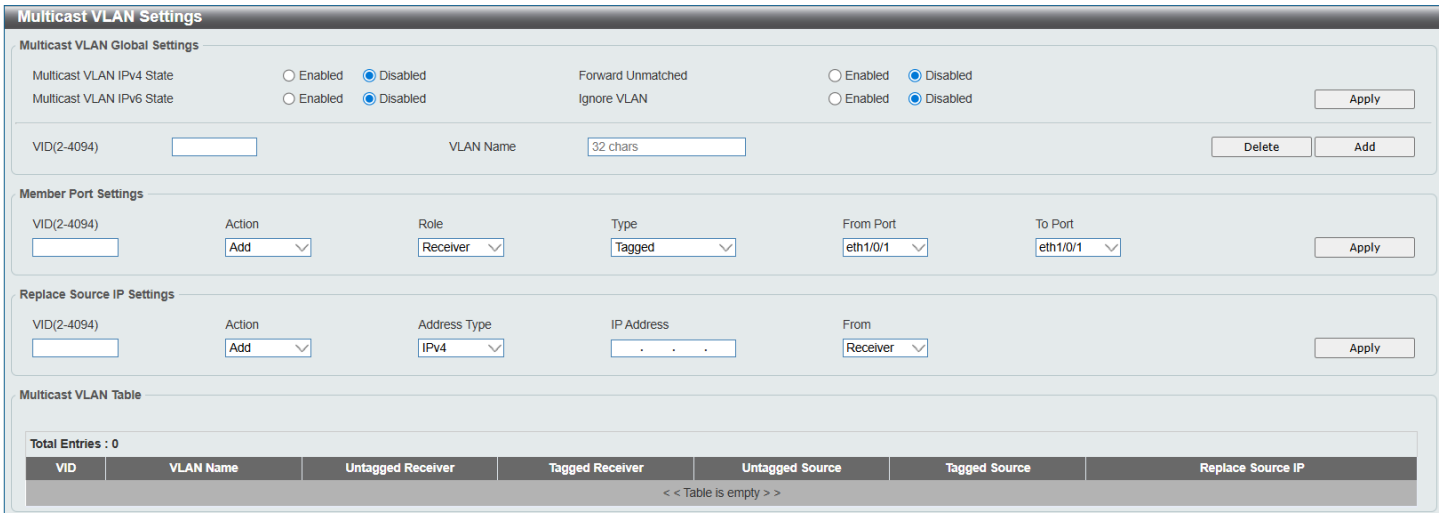
Click the **Find** button to locate a specific entry based on the information entered.

Click the **Find All** button to view all the entries.

L2 Features > L2 Multicast Control > Multicast VLAN

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:



L2 Features > L2 Multicast Control > Multicast VLAN > Multicast VLAN Settings

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

Parameter	Description
Multicast VLAN IPv4 State	Select to enable or disable the IPv4 IGMP control packet process in multicast VLANs.
Forward Unmatched	Select the enable or disable the Forward Unmatched feature here. This specifies that if the received IGMP or MLD control packet is untagged, does not match any profile, and the associated default VLAN is a multicast VLAN, or is tagged with a multicast VLAN, but does not match the associated profile, then the packet will be forwarded or dropped based on this setting. By default, the packet will be dropped.
Multicast VLAN IPv6 State	Select to enable or disable the IPv6 MLD control packet process in multicast VLANs.

Ignore VLAN	Select the enable or disable the ignore VLAN feature here. This specifies the setting for tagged IGMP or MLD control packets. If enabled, then the packet's VLAN is ignored and taken to match the profile to find its multicast VLAN. When this option is enabled, the Switch will ignore the VLAN of the receiving IGMP or MLD control packet and try to find a match profile.
VID	Enter the VLAN ID of the multicast VLAN that will be created or deleted here. The range is 2 to 4094.
VLAN Name	Enter the VLAN name of the multicast VLAN that will be created or deleted here.

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

Click the **Delete** button to delete an entry based on the information entered.

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

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

Parameter	Description
VID	Enter the multicast VLAN ID that will be used here. The range is 2 to 4094.
Action	Select **Add** to add a new entry based in the information entered. Select **Delete** to delete an entry based in the information entered.
Role	Select the role here. Options to choose from are **Receiver** and **Source**. • **Receiver** - Specifies to configure the port as a subscriber port that can only receive multicast data in the multicast VLAN. • **Source** - Specifies to configure the port as an uplink port that can send multicast data in the multicast VLAN.
Type	Select the type here. Options to choose from are **Tagged** and **Untagged**. • **Tagged** - Specifies that if a port is a tagged member, the packets sent from the port are tagged with the Multicast VLAN ID. • **Untagged** - Specifies that if the port is an untagged member, then the packets will be forwarded in the untagged form.
From Port - To Port	Select the Switch port range that will be used here.

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

The fields that can be configured in **Replace Source IP Settings** are described below:

Parameter	Description
VID	Enter the multicast VLAN ID that will be used here. The range is 2 to 4094.
Action	Select **Add** to add a new entry based in the information entered. Select **Delete** to delete an entry based in the information entered.
Address Type	Select the address type here. Options to choose from are **IPv4** and **IPv6**. • **IPv4** - Specifies to enter the source IPv4 address for IGMP control packet reporting. • **IPv6** - Specifies to enter the source IPv6 address for MLD control packet reporting.
IP Address	Enter the IPv4/IPv6 address here.

From	Select the “from” option here. Options to choose from are **Receiver**, **Source**, and **Both**. • **Receiver** - Specifies that the source IPv4/IPv6 address of the IGMP/MLD report/leave packet received on any multicast VLAN receiver port will be replaced. • **Source** - Specifies that the source IPv4/IPv6 address of the IGMP/MLD report/leave packet received on any multicast VLAN source port will be replaced. • **Both** - Specifies that the source IPv4/IPv6 address of the IGMP/MLD report/leave packet received on any port in the multicast VLAN will be replaced.

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

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

Parameter	Description
VID	Enter the multicast VLAN ID that will be used here. The range is 2 to 4094.

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

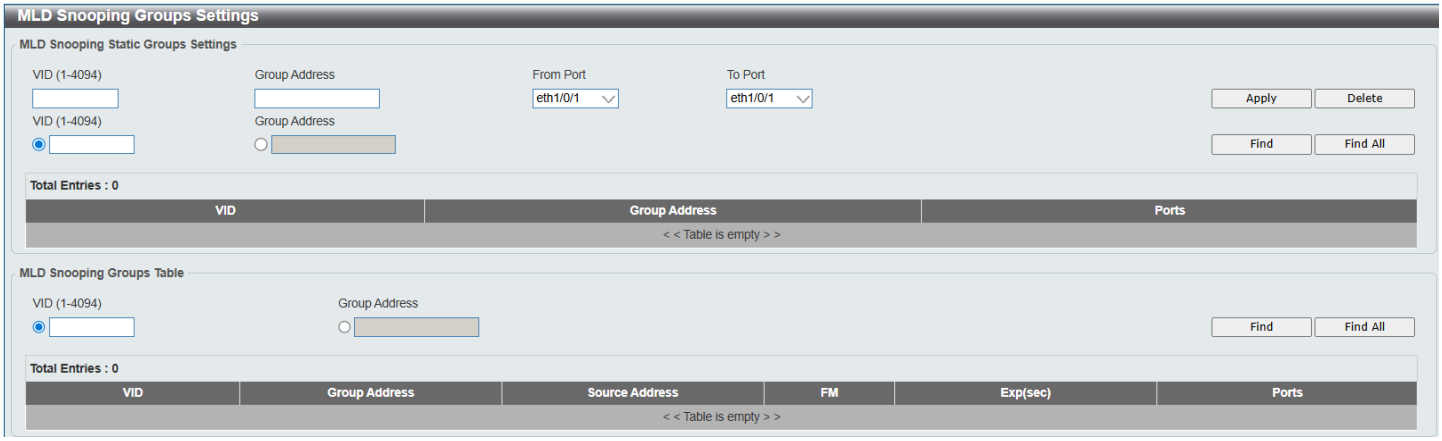
Click the **Show All** button to view all the entries.

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

L2 Features > L2 Multicast Control > Multicast VLAN Group Settings

This widow is used to view and configure the multicast VLAN group settings.

To view the following window, click **L2 Features > L2 Multicast Control > Multicast VLAN > Multicast VLAN Group Settings**, as shown below:



L2 Features > L2 Multicast Control > Multicast VLAN > Multicast VLAN Group Settings

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** and **IPv6**. • **IPv4** - Specifies to use IPv4 multicast addresses in the range. • **IPv6** - Specifies to use IPv6 multicast addresses in the range.

From IP Address	Enter the source IPv4/IPv6 address here.
To IP Address	Enter the destination IPv4/IPv6 address here.

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

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

Parameter	Description
VID	Enter the multicast VLAN ID that will be used here. The range is 2 to 4094.
Profile Name	Enter the group profile name for the multicast VLAN feature here. This name can be up to 32 characters long.
Action	Select the action that will be taken here. Options to choose from are **Add** and **Delete**. This is to add or delete the multicast group entirely.

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

The fields that can be configured in **Group Profile Table** are described below:

Parameter	Description
Profile Name	Enter the group profile name for the multicast VLAN feature here. This name can be up to 32 characters long.

Click the **Find** button to locate a specific entry based on the information entered.
Click the **Show All** button to display all the entries.
Click the **Delete All** button to delete all the entries found in the display table.
Click the **Delete** button to delete the specified entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

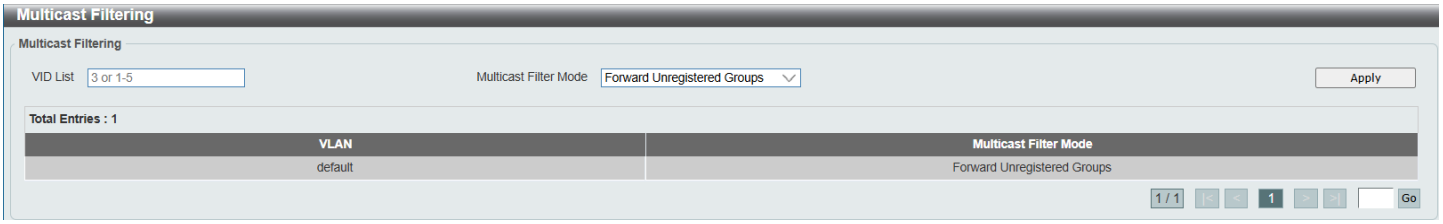
The fields that can be configured in **Access Group Table** are described below:

Parameter	Description
VID	Enter the multicast VLAN ID that will be used here. The range is 2 to 4094.

Click the **Find** button to locate a specific entry based on the information entered.
Click the **Show All** button to display all the entries.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

L2 Features > L2 Multicast Control > Multicast Filtering

The Multicast Filtering page allows you to view and configure multicast filtering settings.



L2 Features > L2 Multicast Control > Multicast Filtering

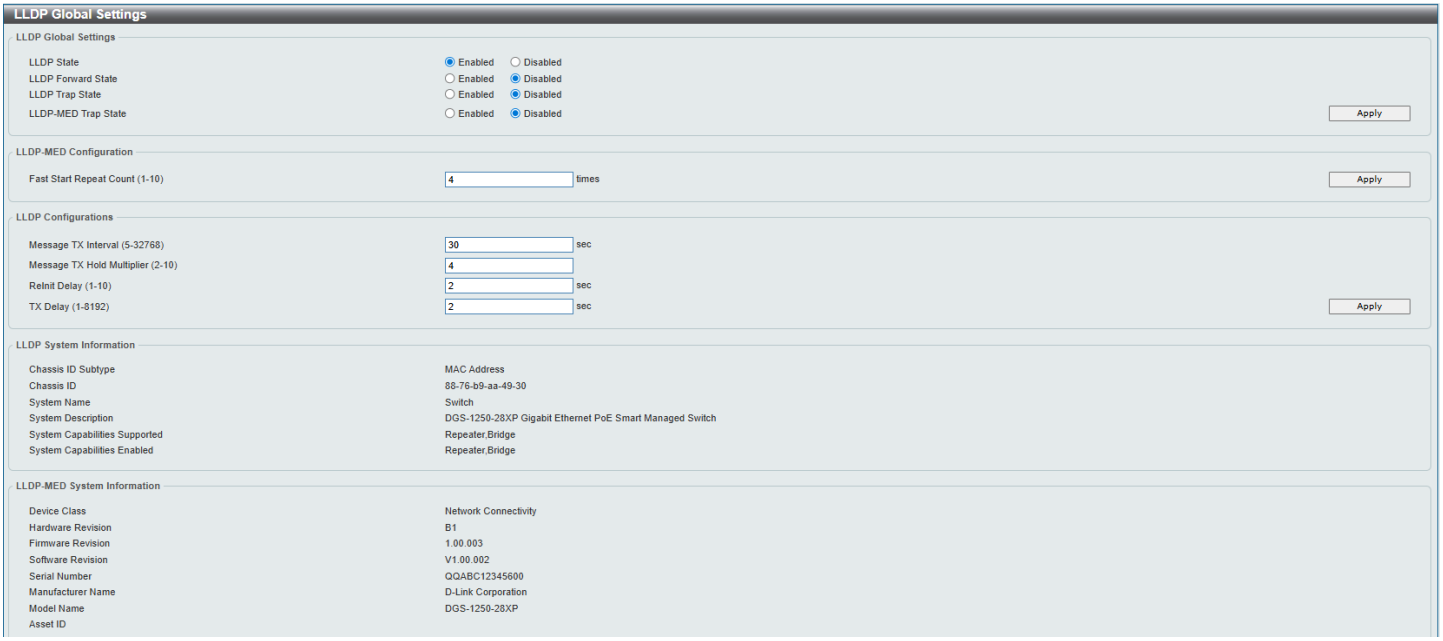
VID List: Enter the VLAN ID.

Multicast Filter Mode: Select the multicast filter mode. Options to choose from are **Forward Unregistered**, **Forward All**, and **Filter Unregistered**. When selecting the **Forward Unregistered** option, registered multicast packets will be forwarded based on the forwarding table and all unregistered multicast packets will be flooded based on the VLAN domain. When selecting the **Forward All** option, all multicast packets will be flooded based on the VLAN domain. When selecting the **Filter Unregistered** option, registered packets will be forwarded based on the forwarding table and all unregistered multicast packets will be filtered.

Click the **Apply** button to save your settings.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

L2 Features > LLDP > LLDP Global Settings

Link Layer Discovery Protocol (LLDP) is and IEEE 802.1AB standards-compliant method for switches to advertise themselves to neighbor devices, as well as to learn about neighbor LLDP devices. SNMP utilities can learn the network topology by obtaining the MIB information for each LLDP device. The LLDP function is enabled by default.



L2 Features > LLDP > LLDP Global Settings

LLDP Global Settings:

LLDP State: Select to enable or disable LLDP globally on the Switch. With this enabled, the Switch will transmit receive and process LLDP packets.

LLDP Forward State: Select 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 to enable or disable the LLDP trap state.

LLDP-MED Trap State: Select to enable or disable the LLDP-MED trap state.

Click the **Apply** button to save your settings.

LLDP-MED Configuration:

Fast Start Repeat Count (1-10): Enter the LLDP-MED fast start repeat count value. This value must be between 1 and 10.

Click the **Apply** button to save your settings.

LLDP Configurations:

Message TX Interval (5-32768): This parameter indicates the interval at which LLDP frames are transmitted on behalf of this LLDP agent. The default value is 30 seconds.

Message TX Hold Multiplier (2-10): This parameter is a multiplier that determines the actual TTL value used in an LLDPDU. The default value is 4.

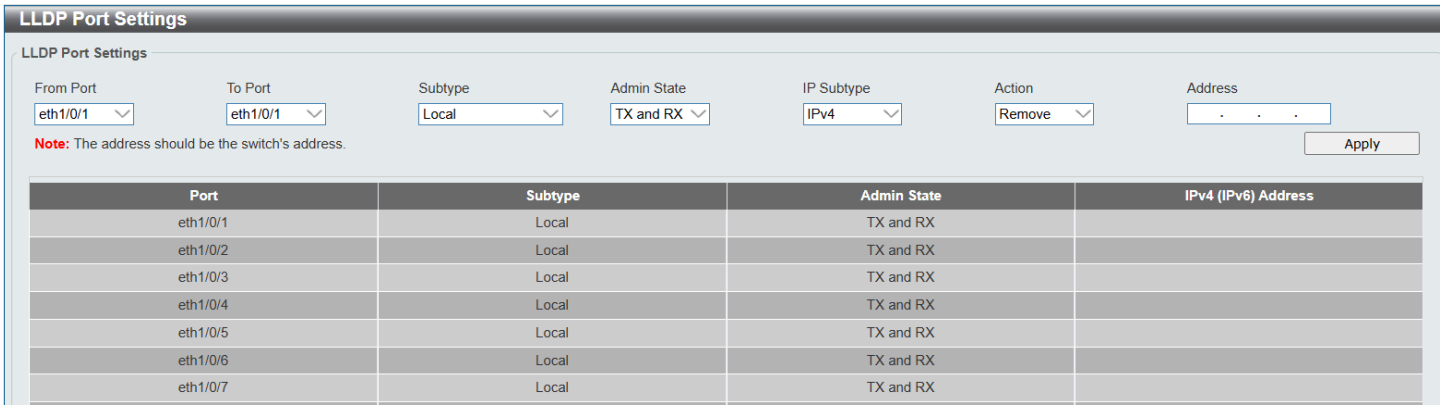
LLDP ReInit Delay (1-10): This parameter indicates the amount of delay from the time adminStatus becomes disabled until re-initialization is attempted. The default value is 2 seconds.

LLDP TX Delay (1-8192): This parameter indicates the delay between successive LLDP frame transmissions initiated by value or status changes in the LLDP local systems MIB. The value for txDelay is set by the following range formula: 1 < txDelay < (0.25 °— msgTxInterval). The default value is 2 seconds.

Click the **Apply** button to save your settings.

L2 Features > LLDP > LLDP Port Settings

The Basic LLDP Port Settings page displays LLDP port information and contains parameters for configuring LLDP port settings.



L2 Features> LLDP > LLDP Port Settings

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

Subtype: Select the subtype of LLDP Type Length Value (TLV). Options to choose from are **MAC Address**, and **Local**.

Admin Status: Select the LLDP transmission mode on the port. The available options are:

TX: Enables transmitting LLDP packets only.

RX: Enables receiving LLDP packets only.

TX and RX: Enables transmitting and receiving LLDP packets. This is the default value.

Disabled: Disables LLDP on the port.

IP Subtype: Select the type of the IP address information to be sent. Options to choose from are **All**, **IPv4** and **IPv6**.

Action: Select to remove or add the action field.

Address: Enter the IP address to be sent.

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

L2 Features > LLDP > LLDP Management Address List

The LLDP Management Address List page displays the detailed management address information for the entry.



L2 Features > LLDP >LLDP Management Address List

Management Address: Select IPv4, IPv6 or All address to be displayed. Click **Find** and the table will update and display the values required.

Subtype: Displays the managed address subtype (e.g. MAC or IPv4)

Address: Displays the IP address.

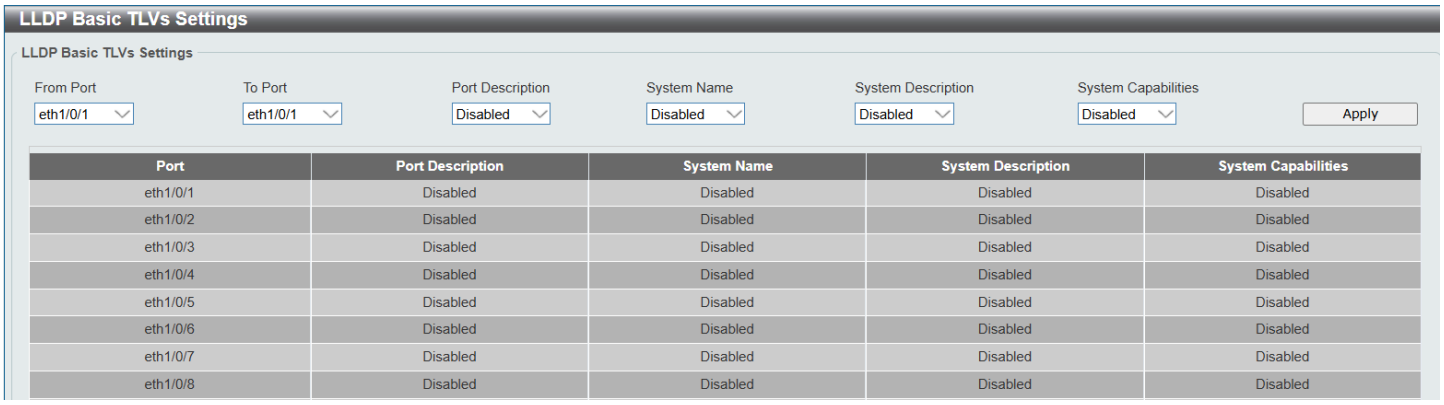
IF Type: Displays the IF Type.

OID: Displays the SNMP OID.

Advertising Ports: Displays the advertising ports.

L2 Features > LLDP > LLDP Basic TLVs Settings

This LLDP Basic TLVs Settings page allows you to configure the LLDP Port settings.



L2 Features > LLDP > LLDP Basic TLVs Settings

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

Port Description: Select to enable or disable the Port Description option.

System Name: Select the system name to be enabled or disabled in the LLDP port. If enabled is selected, users can specify the content of the system Name.

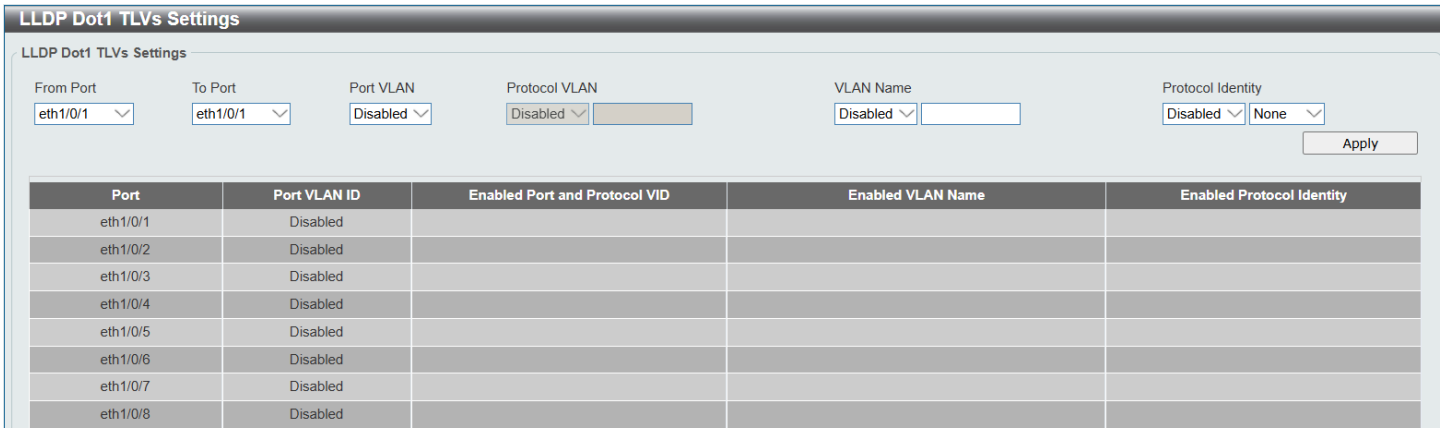
System Description: Select to enable or disable the System Description option.

System Capabilities: Select to enable or disable the System Capabilities option.

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

L2 Features > LLDP > LLDP Dot1 TLVs Settings

This LLDP Dot1 TLVs Settings page allows you to configure an individual port or group of ports to exclude one or more of the IEEE 802.1 organizational port VLAN ID TLV data types from outbound LLDP advertisements.



L2 Features > LLDP > LLDP Dot1 TLVs Settings

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

Port VLAN: Select to enable or disable the port VLAN ID TLV to send. The Port VLAN ID TLV is an optional fixed length TLV that allows a VLAN bridge port to advertise the port's VLAN identifier (PVID) that will be associated with untagged or priority tagged frames.

Protocol VLAN: Select to enable or disable Port and Protocol VLAN ID (PPVID) TLV to send, and enter the VLAN ID in PPVID TLV. [No support in current Firmware stage]

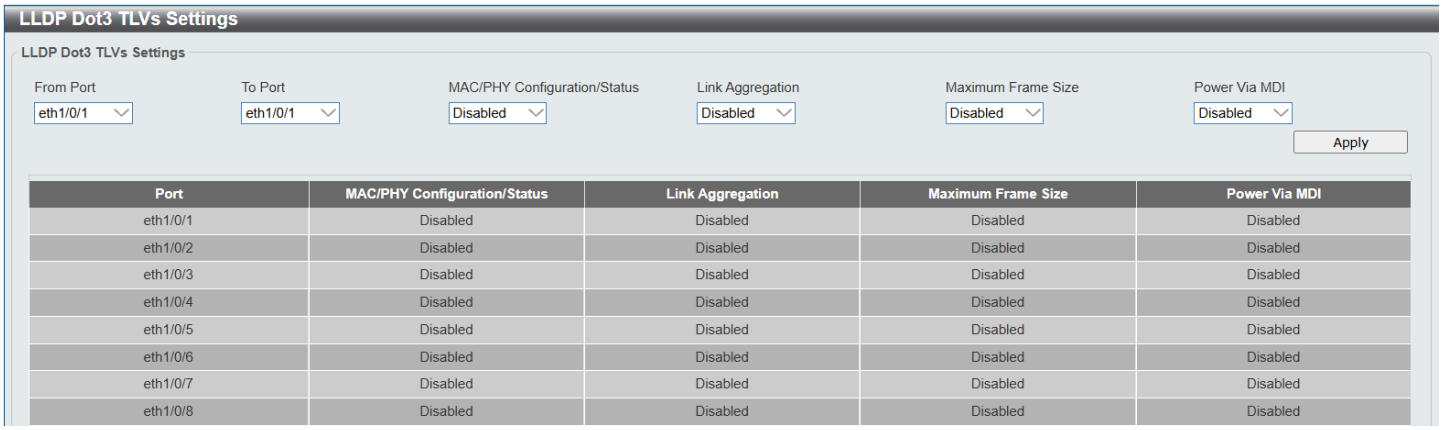
VLAN Name: Select to enable or disable the VLAN name TLV to send, and enter the ID of the VLAN in the VLAN name TLV.

Protocol Identity: Select to enable or disable the Protocol Identity TLV to send, and the protocol name. Options for protocol name to choose from are **None**, **EAPOL**, **LACP**, **GVRP**, **STP**, and **All**.

Click the **Apply** button to save your settings.

L2 Features > LLDP > LLDP Dot3 TLVs Settings

The LLDP Dot3 TLVs Settings page allows you to configure an individual port or group of ports to exclude one or more IEEE 802.3 organizational specific TLV data type from outbound LLDP advertisements.



L2 Features > LLDP > LLDP Dot3 TLVs Settings

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

MAC/PHY Configuration/Status: Select whether the MAC/PHY Configuration Status is enabled on the port. The possible field values are:

Enabled: Enables the MAC/PHY Configuration Status on the port.

Disabled: Disables the MAC/PHY Configuration Status on the port.

Link Aggregation: Specifies whether the link aggregation is enabled on the port. The possible field values are:

Enabled: Enables the link aggregation configured on the port.

Disabled: Disables the link aggregation configured on the port.

Maximum Frame Size: Specifies whether the Maximum Frame Size is enabled on the port. The possible field values are:

Enabled: Enables the Maximum Frame Size configured on the port.

Disabled: Disables the Maximum Frame Size configured on the port.

Power via MDI: Advertises the Power via MDI implementations supported by the port. The possible field values are:

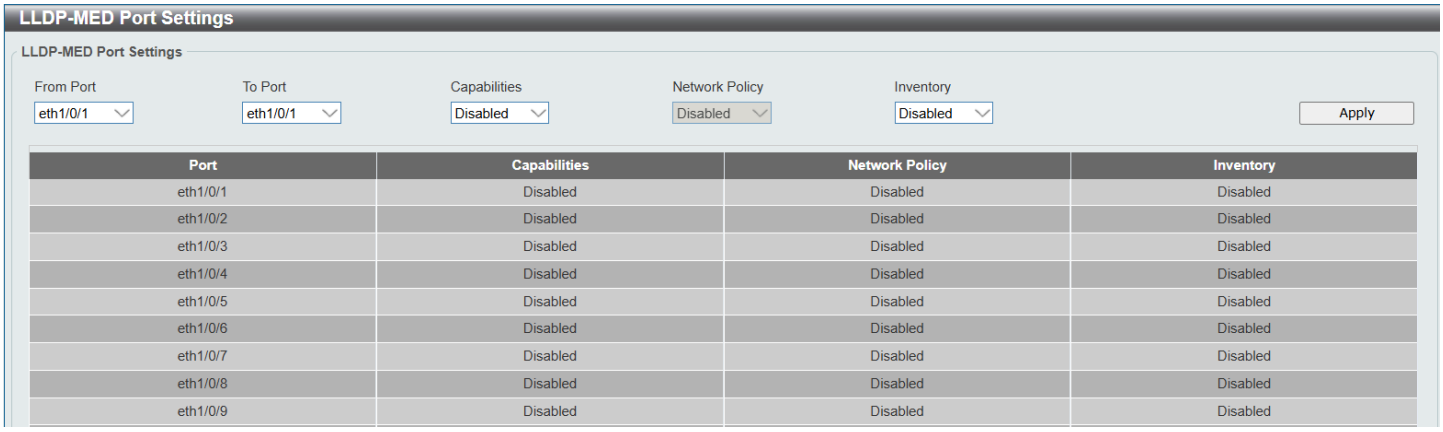
Enabled: Enables the Power via MDI configured on the port.

Disabled: Disables the Power via MDI configured on the port.

Click **Apply** to implement changes made.

L2 Features > LLDP > LLDP-MED Port Settings

The LLDP-MED Port Settings page allows you to enable or disable transmitting LLDP-MED TLVs.



L2 Features > LLDP > LLDP-MED Port Settings

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

Capabilities: Select to enable or disable transmitting the LLDP-MED capabilities TLV.

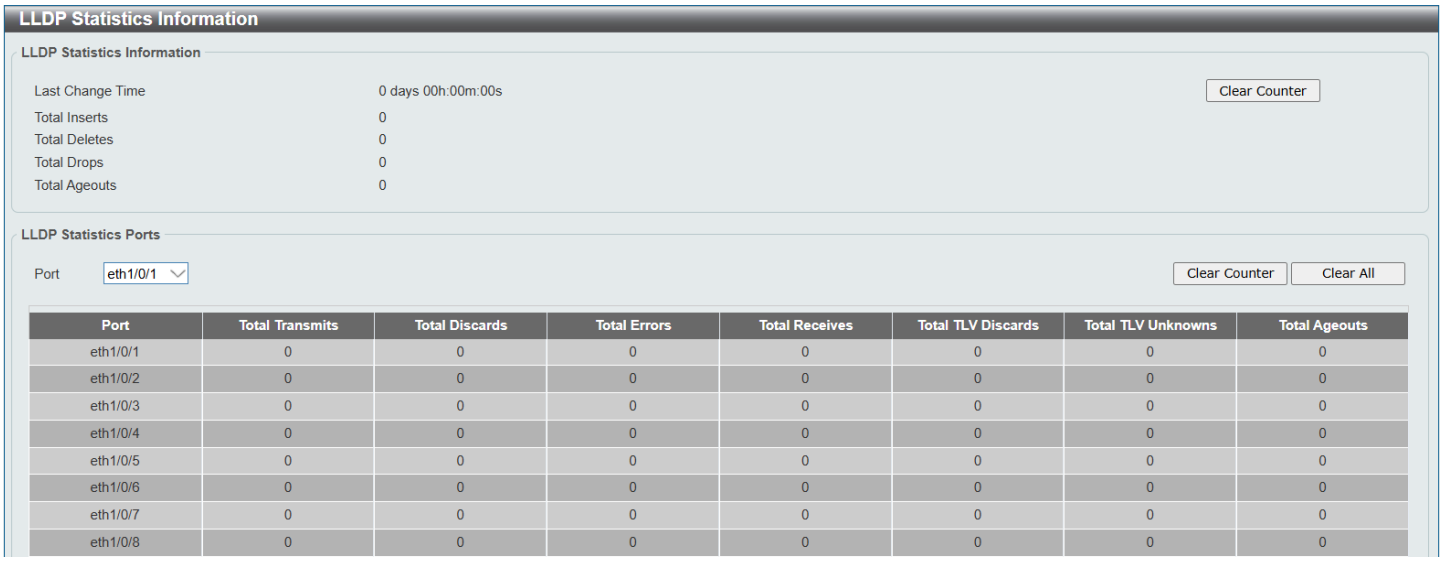
Network Policy: Select to enable or disable transmitting the LLDP-MED network policy TLV. [No support in current Firmware stage]

Inventory: Select to enable or disable transmitting the LLDP-MED inventory management TLV.

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

L2 Features > LLDP > LLDP Statistics Information

The LLDP Statistics Information page displays an overview of the LLDP information.



L2 Features > LLDP > LLDP Statistics Information

The following statistics can be viewed:

LLDP Statistics Information: Displays the counters that refer to the whole switch.

Last Change Time: The amount of time since the last update to the remote table in days, hours, minutes, and seconds.

Total Inserts: Displays the number of new entries, since the last switch reboot.

Total Deletes: Displays the number of new entries, since the last switch reboot.

Total Drops: Displays the number of LLDP frames dropped due to the table was full.

Total Ageouts: Displays the number of entries deleted due to the Time-To-Live expiring.

LLDP Statistics Ports: Displays LLDP port statistics.

Port: Select the port to be displayed.

Total Transmits: Displays the total number of LLDP frames transmitted on the port.

Total Discards: Displays the total discarded frame number of LLDP frames received on the port.

Total Errors: Displays the Error frame number of LLDP frames received on the port.

Total Receives: Displays the total number of LLDP frames received on the port.

Total TLV Discards: Each LLDP frame can contain multiple pieces of information, known as TLVs. If a TLV is malformed, it is counted and discarded.

Total TLV Unknowns: Displays the number of well-formed TLVs, but with a unknown type value.

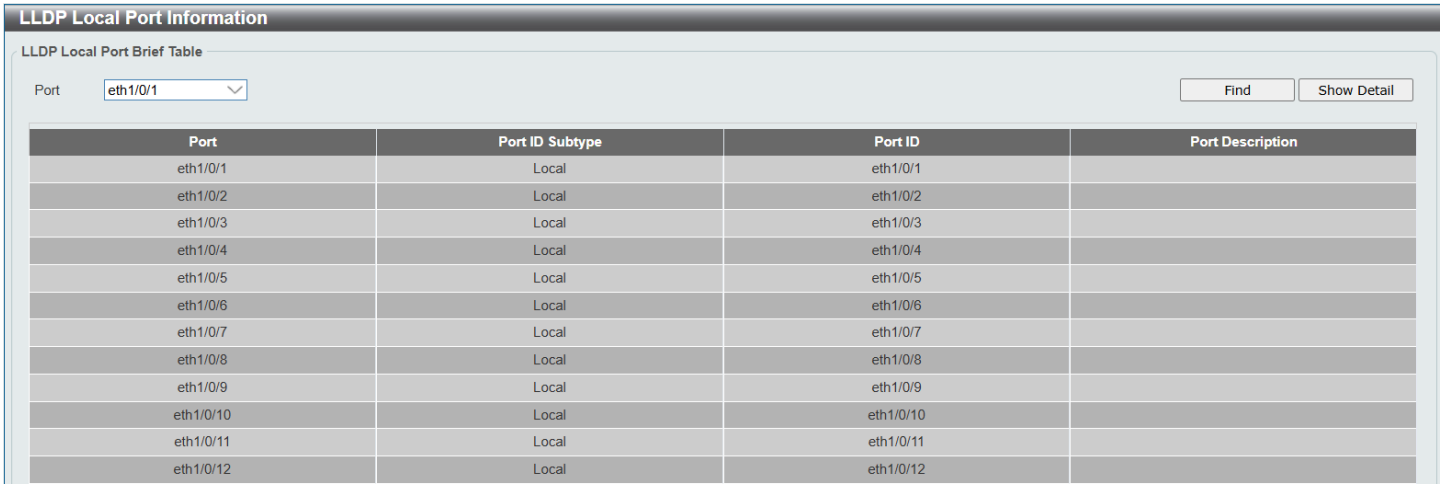
Total Ageouts: Each LLDP frame contains information about how long time the LLDP information is valid. If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.

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.

L2 Features > LLDP > LLDP Local Port Information

The LLDP Local Port Information page displays LLDP local port information.

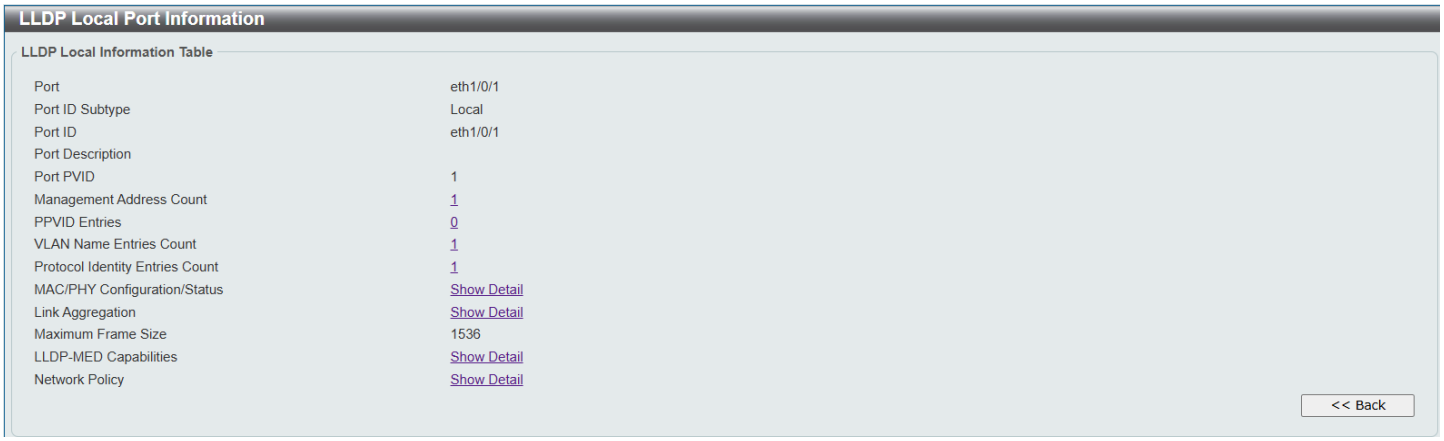


L2 Features > LLDP > LLDP Local Port Information

Port: Displays the port number.
Port ID Subtype: Displays the port ID subtype.
Port ID: Displays the port ID (Unit number/Port number).
Port Description: Displays the port description.

Click **Find** to displays more information for the specified port.

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



L2 Features > LLDP > LLDP Local Port Information – Show Detail

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

L2 Features > LLDP > 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.



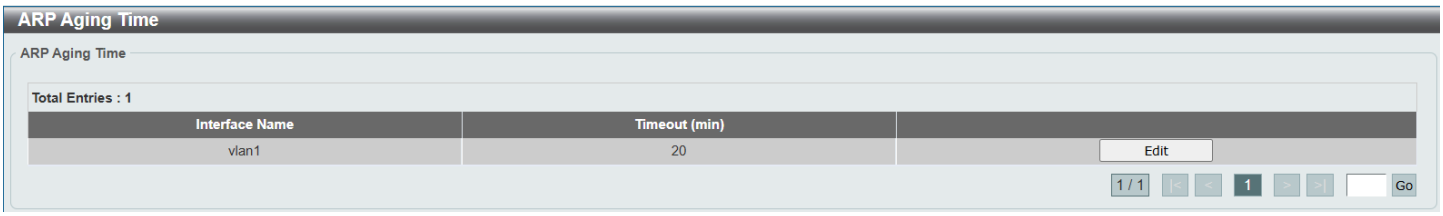
L2 Features > LLDP > LLDP Neighbors Port Information

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

Click the **Clear** button to remove the specified port of LLDP neighbor port or click **Clear All** button to remove all LLDP neighbor ports.

L3 Features > ARP > ARP Aging Time

The ARP Aging Time page allows you to view and configure the ARP aging time settings.



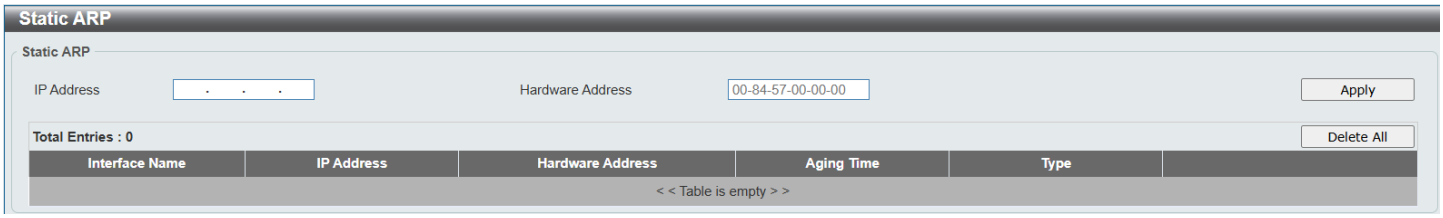
L3 Features > ARP > ARP Aging Time

Timeout(min): Specifies the aging time of the ARP entry. The default is 5 minutes.

Click the **Apply** button to save your settings.
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.

L3 Features > ARP > Static ARP

The Static ARP page provides information regarding each interface, including the IP address mapped to a MAC address. Enter an **IP Address** or **Hardware Address** and then click **Apply** to create a new ARP entry.

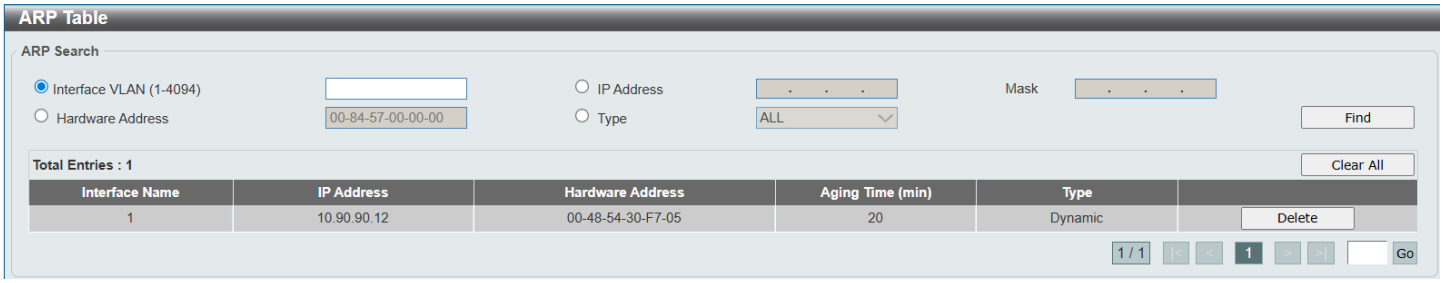


L3 Features > ARP > Static ARP

Click **Edit** to modify the **Hardware Address**.
Click **Delete** to remove the information from ARP table.
Click **Delete All** to remove all information from ARP table.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

L3 Features > ARP > ARP Table

The ARP Table page allows you to view and configure the ARP table settings.



L3 Features > ARP > ARP Table

Interface VLAN (1-4094): Select and enter the interface's VLAN ID.
IP address: Select and enter the IP address to be displayed.
Mask: Enter the mask address for the specified IP address.
Hardware Address: Select and enter the MAC address.
Type: Select the type.
Click the **Find** button to locate a specific entry based on the information entered.
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.

L3 Features > IPv4 Interface

The IPv4 Interface page allows you to configure the IPv4 Interface settings.



L3 Features > IPv4 Interface

Interface VLAN (1-4094): Enter the VLAN ID of the IPv4 interface.

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

Click the **Find** button to display the specific entry.

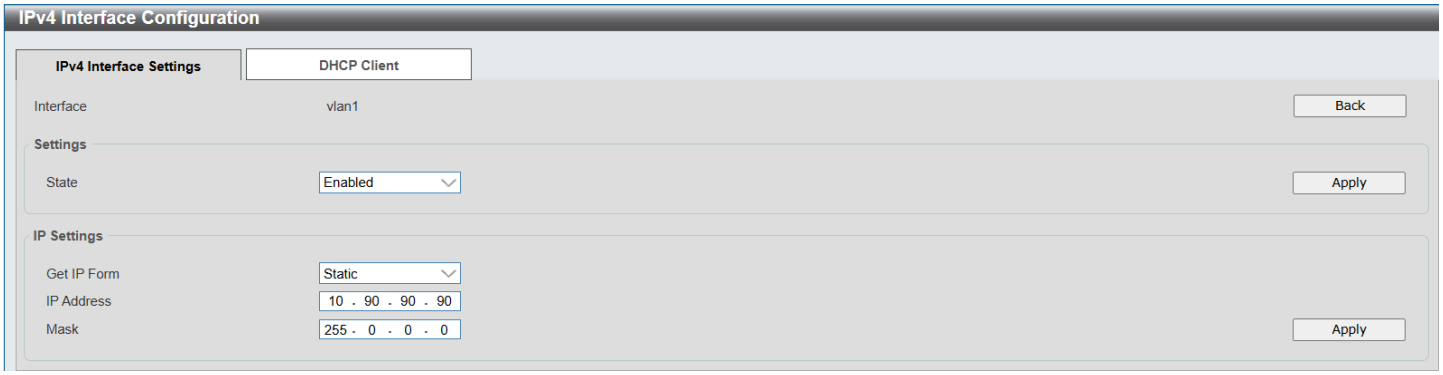
Click the **Edit** button to re-configure the specific entry.

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.

NOTE: When user delete or disable all Switch VLAN IP interface which user cannot log-in via Telnet, Web UI and SNMP Switch control interface.

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



L3 Features > IPv4 Interface - Edit

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

State: Select to enable or disable the IPv4 interface's global state.

Click the **Apply** button to save your settings.

IP Settings:

Get IP From: Select Static or DHCP. When the **Static** option is selected, users can enter the IPv4 address of this interface manually. When the **DHCP** option is selected, this interface will obtain IPv4 information from a DHCP server located on the local network.

IP Address: Enter the IPv4 Address for this interface.

Mask: Enter the IPv4 subnet mask for this interface.

Click the **Apply** button to save your settings.

After clicking the **DHCP Client** tab, the following page will appear.



L3 Features > IPv4 Interface – DHCP Client

DHCP Client Client-ID (1-4094): Enter the VLAN interface, whose hexadecimal MAC address will be used as the client ID to be sent with the discover message.
Class ID String: Enter the vendor class identifier with the maximum of 32 characters. Tick the **Hex** check box to have the class identifier in the hexadecimal form.

Host Name: Enter the host name.

Lease: Enter the preferred lease time for the IP address to request from the DHCP server. Enter the day duration of the lease, or select the hour and minute duration of the lease.
DHCP Retry Times (5-120): Enter the DHCP retry times. The value is between 5 and 120 and default is 7 times.

Click the **Apply** button to save your settings.

L3 Features > IPv4 Static/Default Route

The IPv4 Static/Default Route page allows you to view and configure the IPv4 static and default route settings.



L3 Features > IPv4 Static/Default Route

IP Address: Specify the network address for the IPv4 static route.

Mask: Specify the mask address for the IPv4 static route. If this is a default route, select the **Default Route** checkbox.

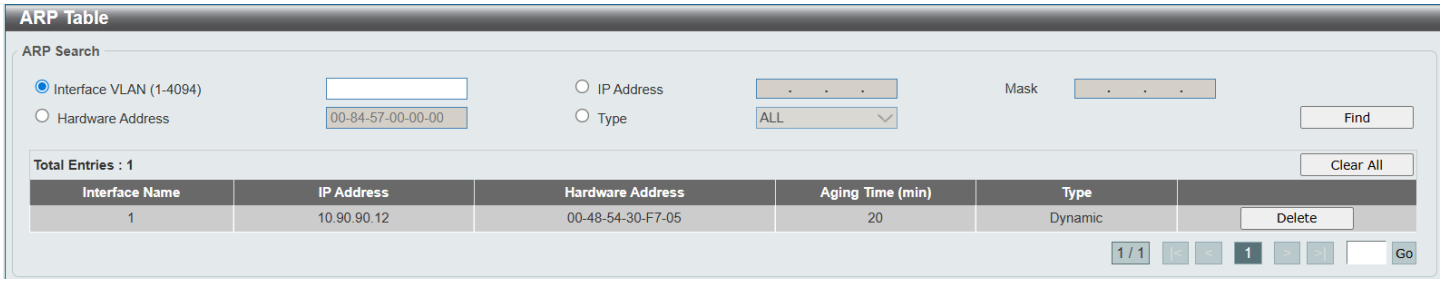
Gateway: Enter the gateway address for IPv4 route. If this is a default route, then this is the default gateway.

Backup State: Each network can only have one primary route, and any other routes should be assigned to the backup state. When the primary route failed, the switch also supports a floating static route, which means that the user may create an alternative static route to a different next hop. This secondary next hop device route is considered as a backup static route for when the primary static route is down. If the primary route is lost, the backup route will become active.

Click **Apply** button to accept the changes made.
Click the **Delete** button to remove the specific entry.

L3 Features > IPv4 Route Table

The IPv4 Route Table page is used to view and configure the IPv4 route table settings.



L3 Features > IPv4 Route Table

IP Address: Click the radio button and enter the destination IP address of the route to be displayed. The longest prefix matched will be displayed.

Network Address: Click the radio button and enter the destination network address of the route to be displayed.

Connected: Select this option to display only connected routes.

Hardware: Select this option to display only the routes that have been written into hardware.

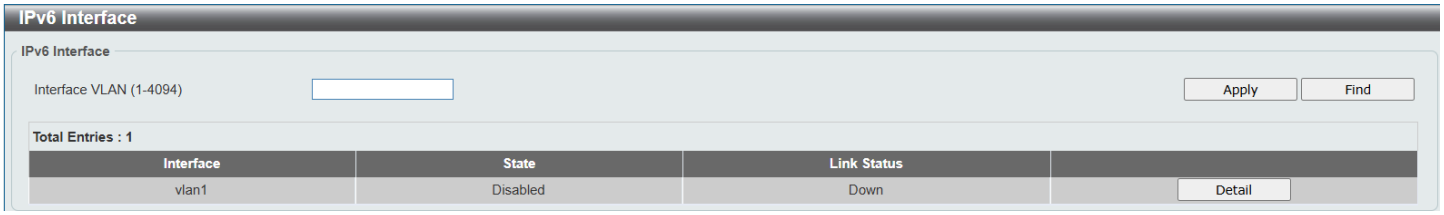
Summary: Display a summary of the active routing entries.

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.

L3 Features > IPv6 Interface

The IPv6 Interface page is used to view and configure the IPv6 interface's settings.



L3 Features > IPv6 Interface

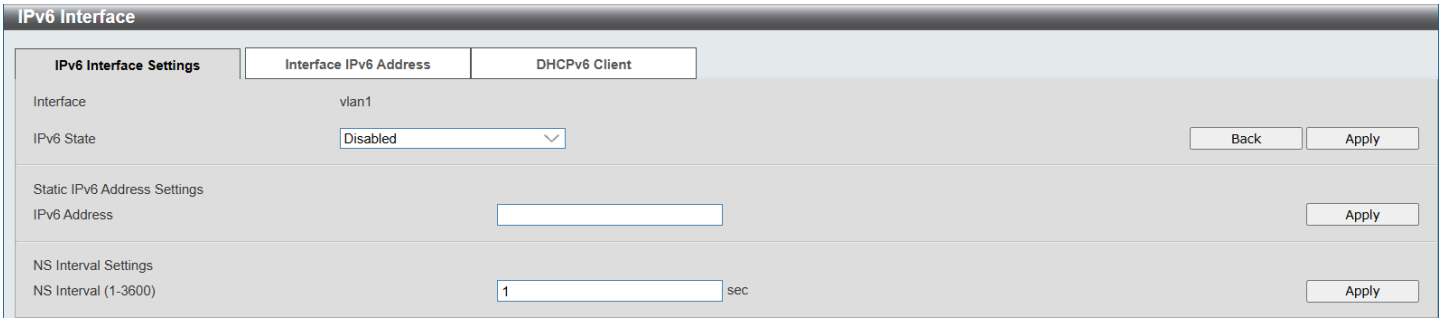
Interface VLAN (1-4094): Enter the VLAN ID of the IPv6 interface.

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

Click the **Find** button to display the specific entry.

Click the **Detail** button to view and configure more detailed settings for the IPv6 interface entry.

After clicking the **Detail** button, the following window will be appeared.



L3 Features > IPv6 Interface - Detail

IPv6 State: Select to enable or disable the IPv6 interface's global state.
Click the **Apply** button to save your settings.

Static IPv6 Address Setting:
IPv6 Address: Enter the IPv6 address for this IPv6 interface.
Click the **Apply** button to save your settings.

NS Interval Settings:
NS Interval (1-3600): Specify the NS interval and the values are between 1 and 3600.
Click the **Apply** button to save your settings.

After clicking the **Interface Address** tab located at the top of the page, the following page will appear



L3 Features > IPv6 Interface – Interface IPv6 Address

After clicking the **DHCPv6 Client** tab located at the top of the page, the following page will appear



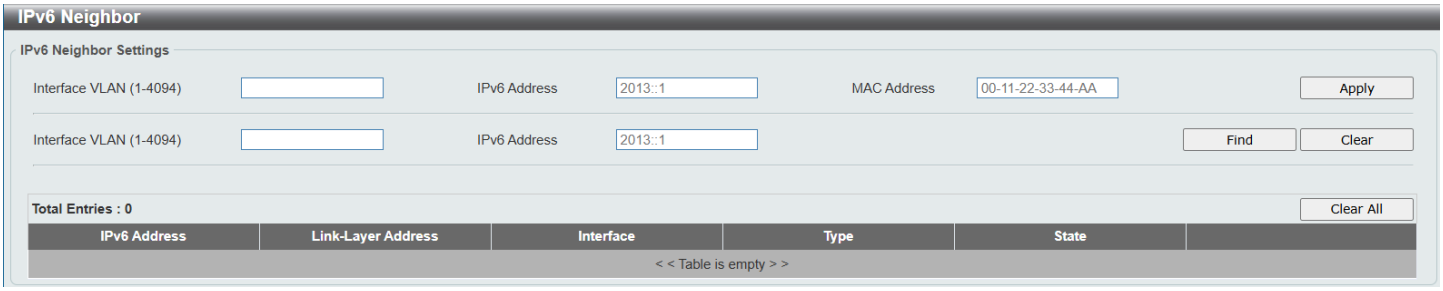
L3 Features > IPv6 Interface – DHCPv6 Client

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

Client State: Select to enable or disable the DHCPv6 client state.
Click the **Apply** button to save your settings.

L3 Features > IPv6 Neighbor

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



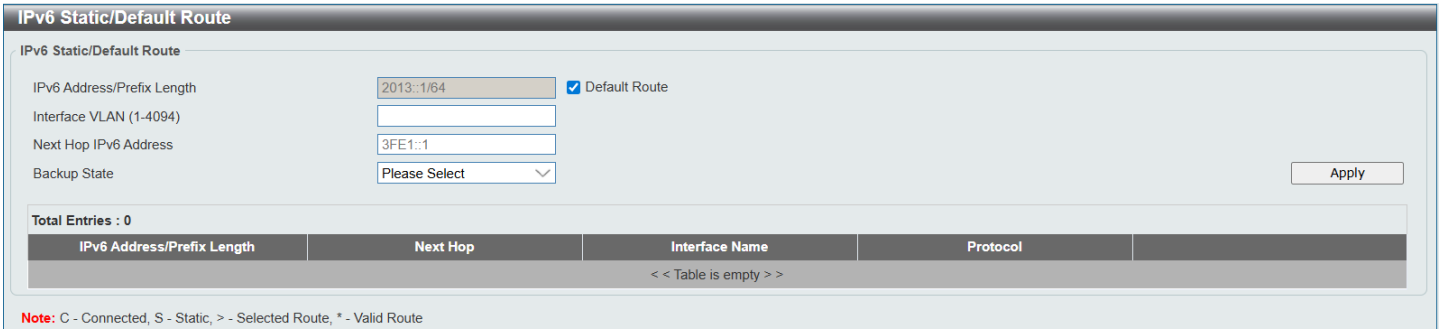
L3 Features > IPv6 Neighbor

Interface VLAN (1-4094): Enter the VLAN ID of the IPv6 neighbor.
IPv6 Address: Specifies the neighbor IPv6 address.
MAC Address: Specifies the link layer MAC address.

Click the **Apply** button to save your settings.
Click **Find** to locate a specific entry based on the information entered.
Click **Clear** to clear the specified information entered in the fields.
Click **Clear all** to clear all the information entered in the fields.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

L3 Features > IPv6 Static/Default Route

The IPv6 Static/Default Route is used to configure the IPv6 static or default routes.



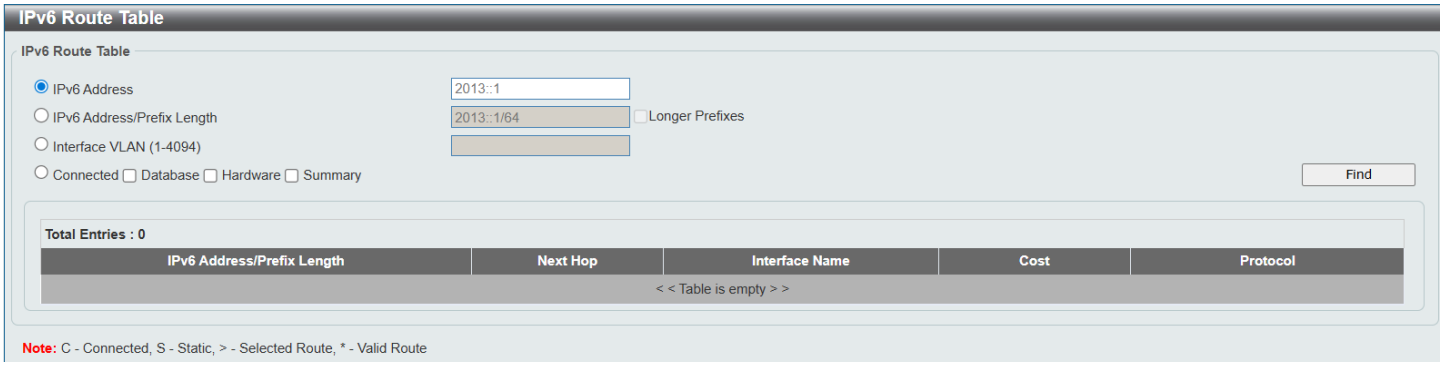
L3 Features > IPv6 Static/Default Route

IPv6 Address/Prefix Length: Enter the destination network for the route, or tick the **Defult Route** check box to be assigned to the default route.
Interface VLAN (1-4094): Enter interface's VLAN ID that will be associated with this route.
Next Hop IPv6 Address: Enter the router's next hop IPv6 address.
Backup State: Select the backup state option here. Options to choose from are **Primary**, and **Backup**. When the Primary option is selected, the route is specified as the primary route to the destination. When the Backup option is selected, the route is specified as the backup route to the destination.

Click the **Apply** button to save your settings.

L3 Features > IPv6 Route Table

The IPv6 Route Table page is used to view and configure the IPv6 route table.



L3 Features > IPv6 Route Table

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 the route and all of the more specific routes.

Interface VLAN (1-4094): Select and enter the interface's VLAN ID to display here.

Connected: Select this option to display only connected routes.

Database: Select to view 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: Display the brief information of the active routing entries.

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

L3 Features > DNS Server Settings

This page is used to configure Domain Name Server IP address.



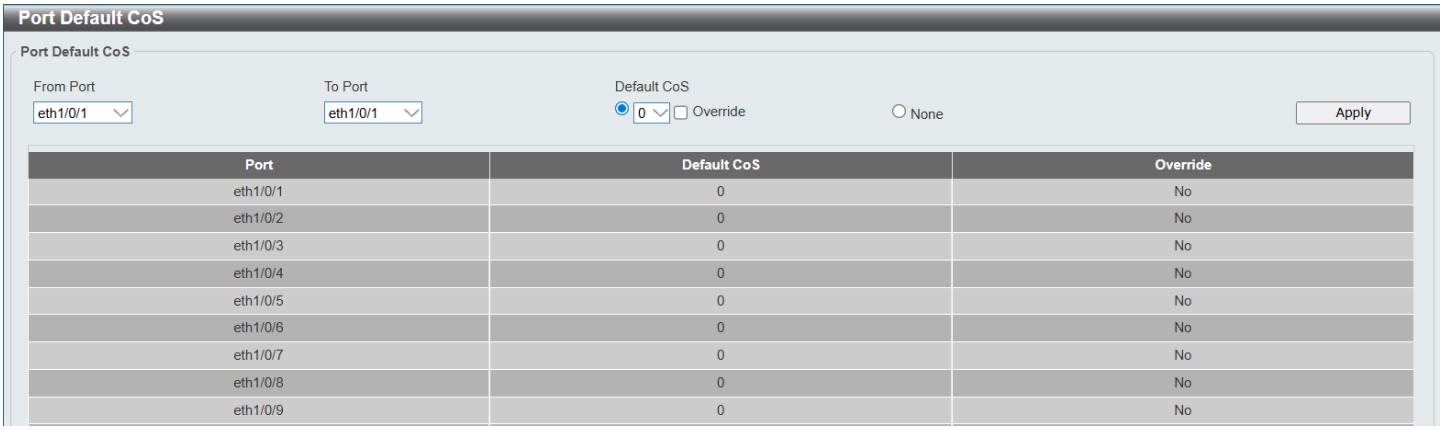
L3 Features > DNS Server Settings

Domain Names Server is the database for transferring domain name string to Internet Protocol addresses.
DGS-1250 series supports up to 3 DNS servers.

Click the **Apply** button to add/remove the DNS server IP address.

QoS > Port Default CoS

The Port Default CoS page allows you to view and configure the port's default CoS settings.



QoS > Port Default CoS

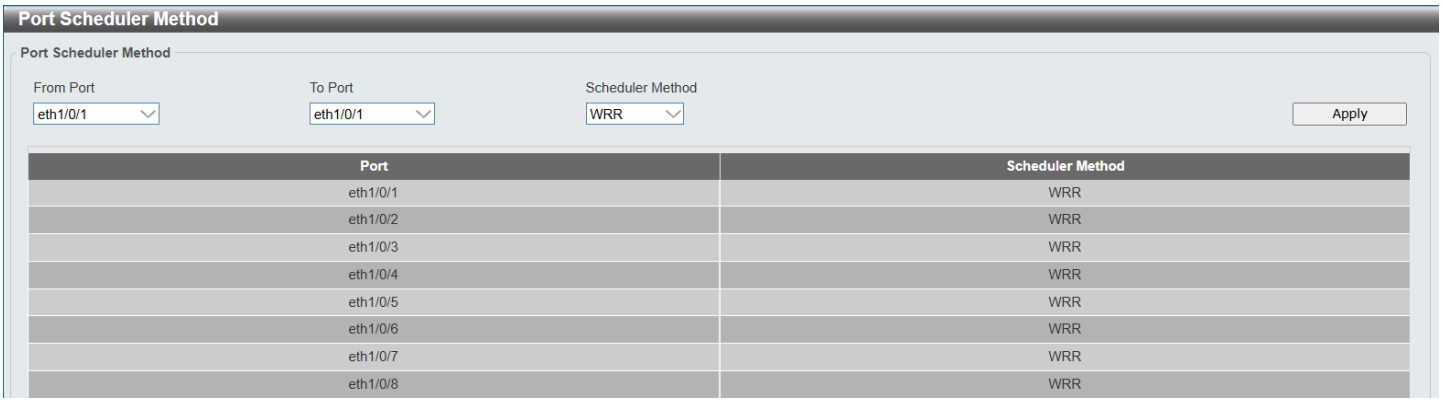
From Port / To Port: Select the range of ports to be configured.

Default CoS: Select the default CoS option for the specified ports. The values are from 0 to 7. Click the **Override** check box to apply the port's default CoS to all packets (tagged or untagged) received by the port. Select the **None** option to use the default settings.

Click the **Apply** button to save your settings.

QoS > Port Scheduler Method

The Port Scheduler Method page allows you to view and configure the port scheduler method settings.



QoS > Port Scheduler Method

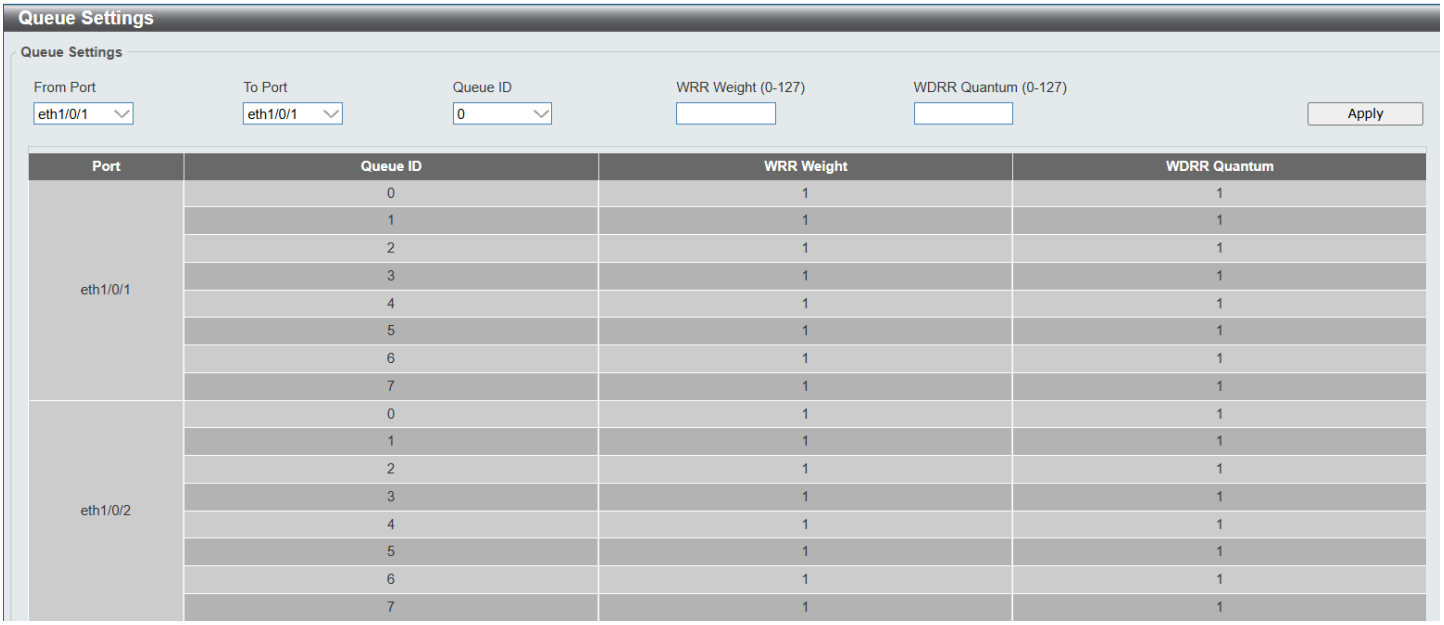
From Port / To Port: Select the range of ports to be configured.

Scheduler Method: Select the scheduler method for the specified ports. Available options are Strict Priority (**SP**), Round-Robin (**RR**), Weighted Round-Robin (**WRR**), and Weighted Deficit Round-Robin (**WDRR**). By default, the output queue scheduling algorithm is **WRR**.

Click the **Apply** button to save your settings.

QoS > Queue Settings

The Queue Settings page allows you to configure the queue settings.



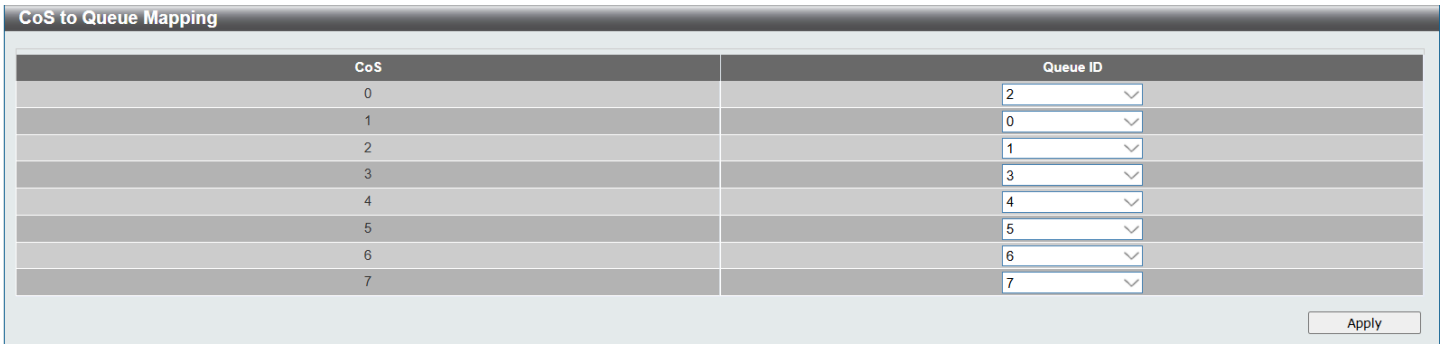
QoS > Queue Settings

From Port / To Port: Select the range of ports to be configured.
Queue ID: Select the queue ID value. The range is between 0 and 7.
WRR Weight (0-127): Enter the WRR weight value. The value is between 0 and 127.
WDRR Quantum (0-127): Enter the WRR quantum value. The value is between 0 and 127.

Click the **Apply** button to save your settings.

QoS > CoS to Queue Mapping

The CoS to Queue Mapping page allows you to view and configure the CoS-to-Queue mapping settings.



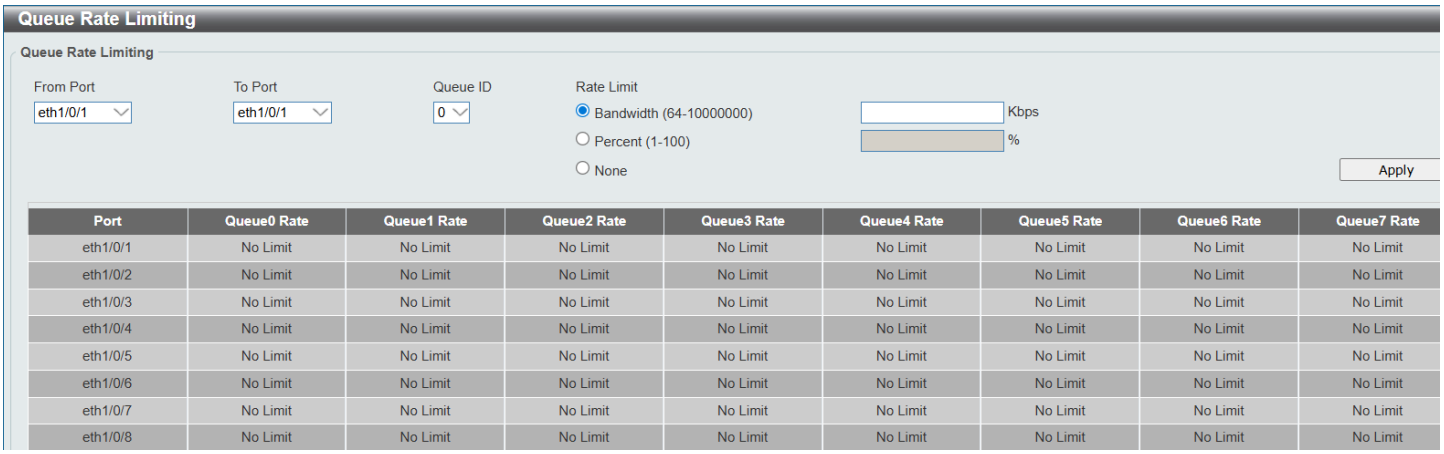
QoS > CoS to Queue Mapping

Queue ID: Select the queue ID that will be mapped to the corresponding CoS value. The value is from are 0 to 7.

Click the **Apply** button to save your settings.

QoS > Port Rate Limiting

The Port Rate Limiting page allows you to view and configure the port rate limiting settings.



QoS > Port Rate Limiting

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

Direction: Select the direction. Available options are **Input** and **Output**. When **Input** is selected, the rate limit for ingress packets is configured. When **Output** is selected, the rate limit for egress packets is configured.

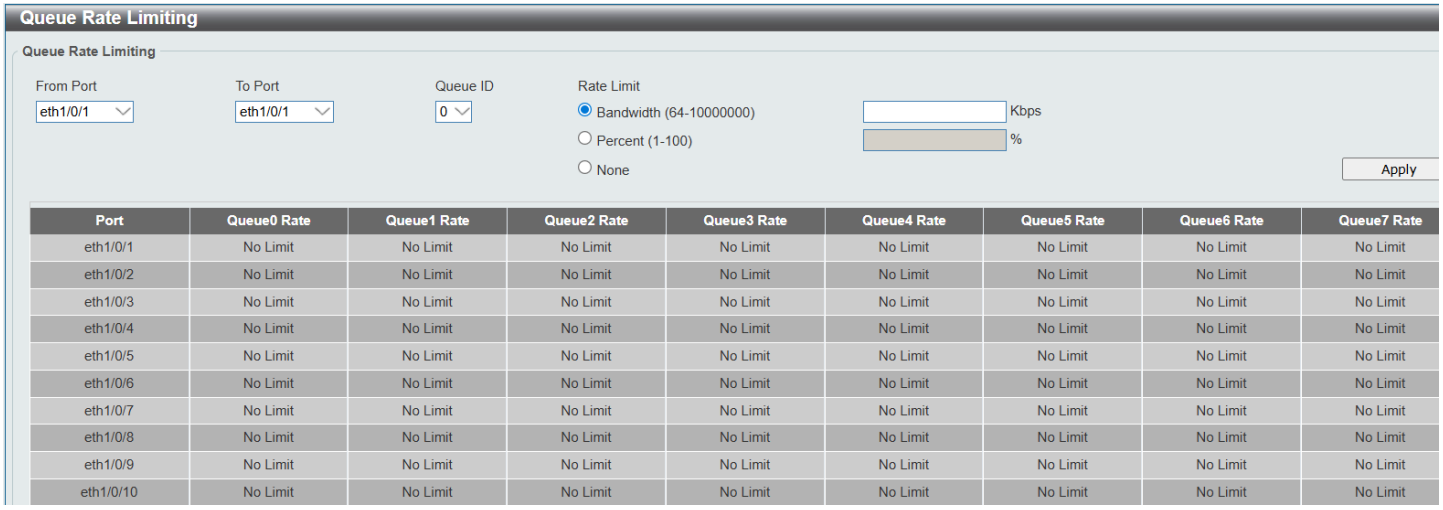
Rate Limit: Enter the Rate Limit for the specified port.

When **Bandwidth** is selected, enter the input/output bandwidth value used in the space provided. This value must be between 64 and 10000000 kbps. Also, enter the **Burst Size** value in the space provided. This value must be between 0 and 128000 kilobytes.
When **Percent** is selected, enter the input/output bandwidth percentage value used in the space provided. This value must be between 1 and 100 percent (%). Also, enter the **Burst Size** value in the space provided. This value must be between 0 and 128000 kilobytes.
Select the **None** option to remove the rate limit on the specified port(s). The specified limitation cannot exceed the maximum speed of the specified interface. For the ingress bandwidth limitation, the ingress can trigger a pause frame or a flow control frame when the received traffic exceeds the limitation.

Click the **Apply** button to save your settings.

QoS > Queue Rate Limiting

The Queue Rate Limiting page allows you to view and configure the queue rate limiting settings.



QoS > Queue Rate Limiting

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

Queue ID: Select the queue ID for the specified ports. The value is between 0 and 7.

Rate Limit: Specify the Rate limit option.

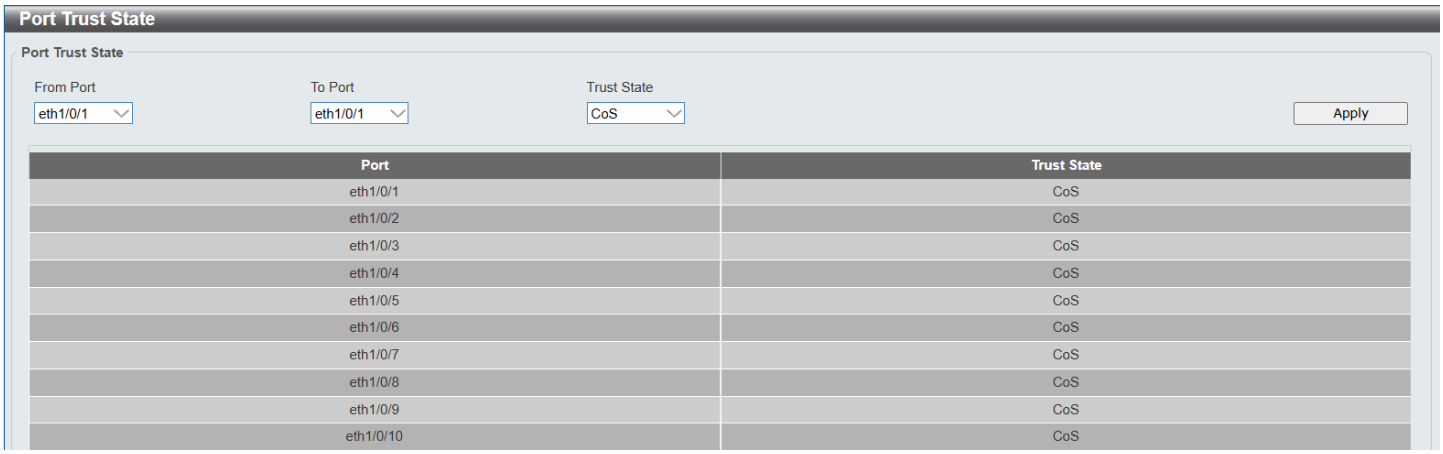
If you selected the **Min Bandwidth** option, enter the minimum bandwidth rate limit value in the space provided. This value must be between 8 and 10000000 kbps. Also enter the maximum bandwidth (**Max Bandwidth**) rate

limit in the space provided. This value must be between 8 and 10000000 kbps.
If you selected the **Min Percent** option, enter the minimum bandwidth percentage value in the space provided. This value must be between 1 and 100 percent (%). Also enter the maximum percentage value (**Max Percent**) in the space provided. This value must be between **1** and **100** percent (%).

Click the **Apply** button to save your settings.

QoS > Port Trust State

The Port Trust State page allows you to view and configure the port trust state settings.



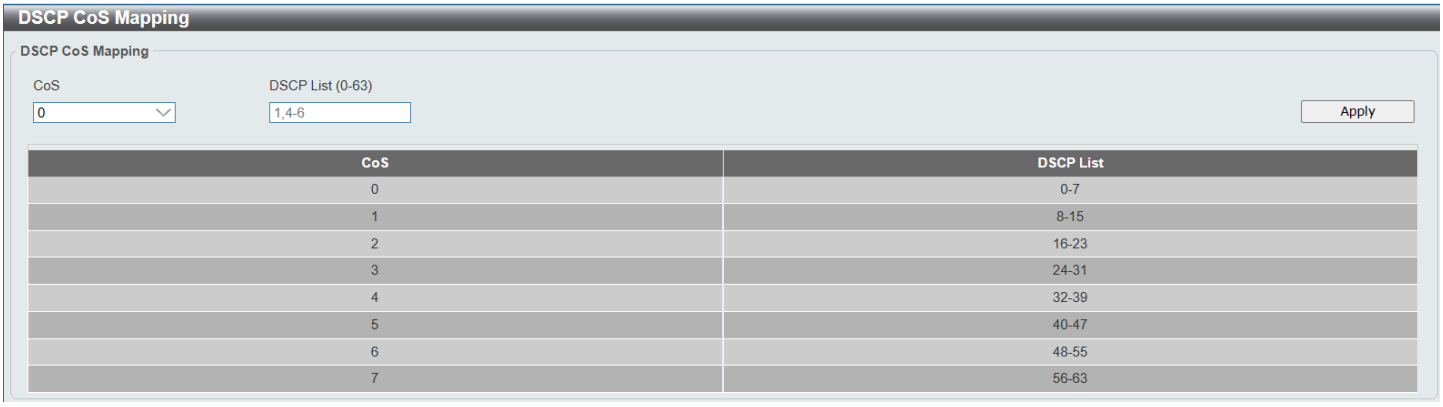
QoS > Port Trust State

From Port / To Port: Select the range of ports to be configured.
Trust State: Select the trust state to be **CoS** or **DSCP**.

Click the **Apply** button to save your settings.

QoS > DSCP CoS Mapping

The DSCP CoS Mapping page allows you to view and configure the DSCP CoS mapping settings.



QoS > DSCP CoS Mapping

From Port / To Port: Select the range of ports to be configured.
CoS: Select the **CoS** priority.
DSCP List (0-63): Enter the DSCP list number.

Click the **Apply** button to save your settings.

QoS > Advanced Settings> Class Map

This window is used to display and configure the class map settings.



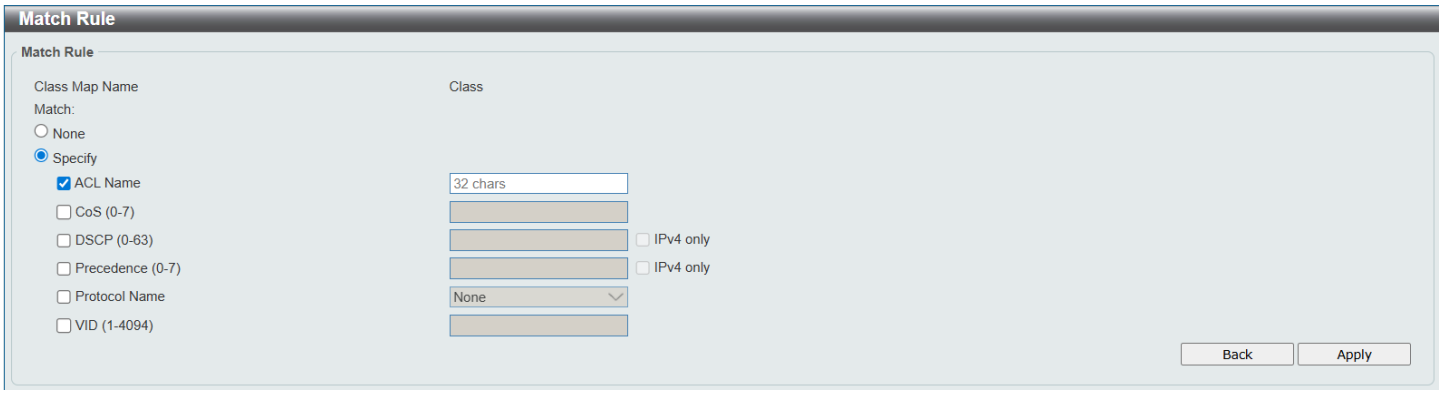
QoS > Advanced Settings>Class Map

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.

After clicking the **Match** button, the following page will be available.



Class Map (Match) Window

The fields that can be configured are described below:

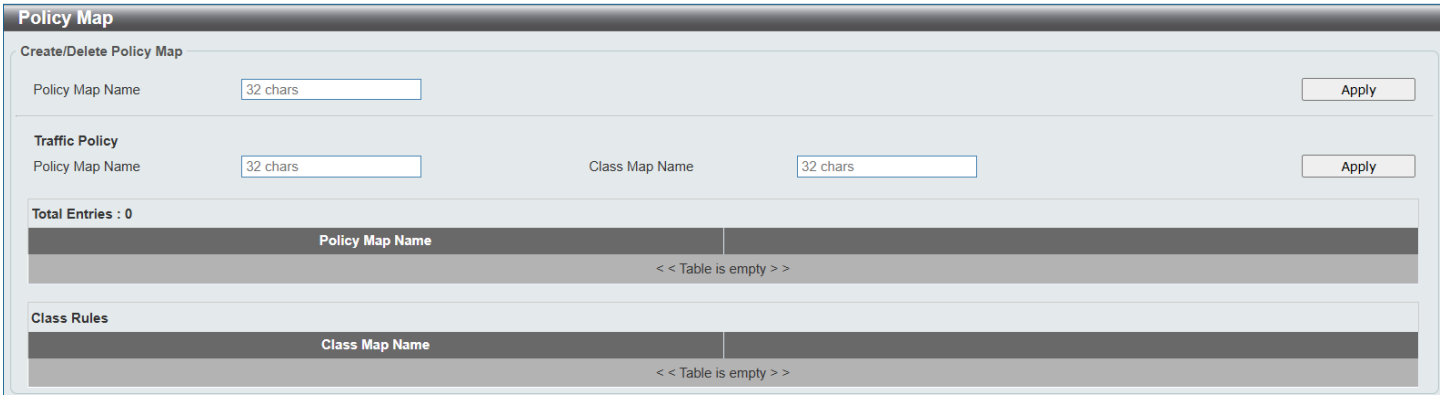
Parameter	Description
None	Select this option to match nothing to this class map.
Specify	Select the option to match something to this class map.
ACL Name	Select and enter the access list name that will be matched with this class map here. This name can be up to 32 characters long.
CoS List	Select and enter the CoS list value that will be matched with this class map here. This value must be between 0 and 7.
DSCP List	Select and enter the DSCP list value that will be matched with this class map here. This value must be between 0 and 63. Tick the **IPv4 only** option to match IPv4 packets only. If not specified, the match is for both IPv4 and IPv6 packets.
Precedence List	Select and enter the precedence list value that will be matched with this class map here. This value must be between 0 and 7. Tick the **IPv4 only** option to match IPv4 packets only. If not specified, the match is for both IPv4 and IPv6 packets. For IPv6 packets, the precedence is most three significant bits of traffic class of IPv6 header.
Protocol Name	Select the protocol name that will be matched with the class map here. Options to choose from are **ARP**, **BGP**, **DHCP**, **DNS**, **EGP**, **FTP**, **IPv4**, **IPv6**, **NetBIOS**, **NFS**, **NTP**, **OSPF**, **PPPOE**, **RIP**, **RTSP**, **SSH**, **Telnet**, and **TFTP**.

VLAN List	Select and enter the VLAN list value that will be matched with the class map here. This value must be between 1 and 4094.

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

QoS > Advanced Settings> Policy Map

This window is used to display and configure the policy map settings.



QoS > Advanced Settings>Policy Map

The fields that can be configured for **Create/Delete Policy Map** are described below:

Parameter	Description
Policy Map Name	Enter the name of the policy map that will be created here. This name can be up to 32 characters long.

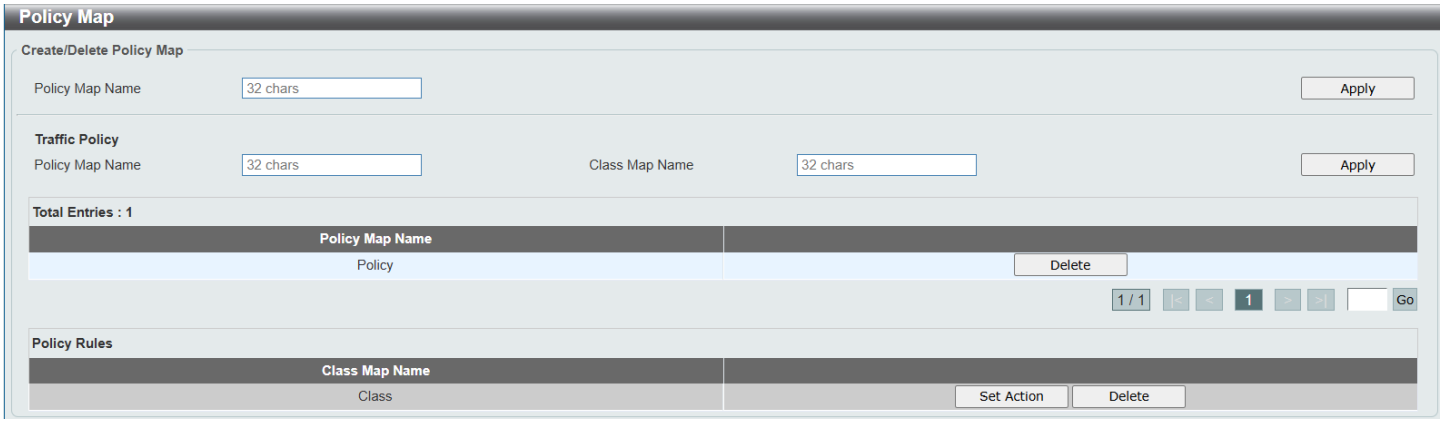
Click the **Apply** button to accept the changes made.

The fields that can be configured for **Traffic Policy** are described below:

Parameter	Description
Policy Map Name	Enter the policy map name here. This name can be up to 32 characters long.
Class Map Name	Enter the class map name here. This name can be up to 32 characters long.

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

To view the **Class Rules** assigned to a Policy, select the **Policy Map** entry in the Policy Map table. The class rules assigned to the Policy will be displayed in the **Class Rules** table, as shown below:

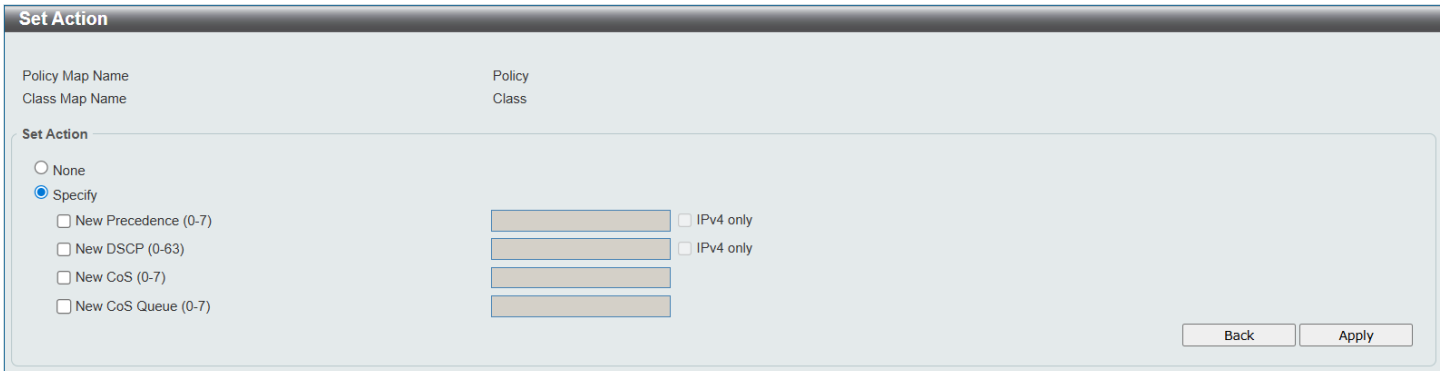


Policy Map (Class Rules) Window

Click the **Set Action** button to configure the set action settings for the specified entry.

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

After clicking the **Set Action** button, the following page will appear.



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 packets here. The range is from 0 to 7. Setting the CoS will not affect the CoS queue selection. The CoS will only be marked.
New Cos Queue	Select the new CoS queue value to packets here. This will overwrite the original CoS queue selection. Setting the CoS queue will take effect if the policy map is applied on the interface.

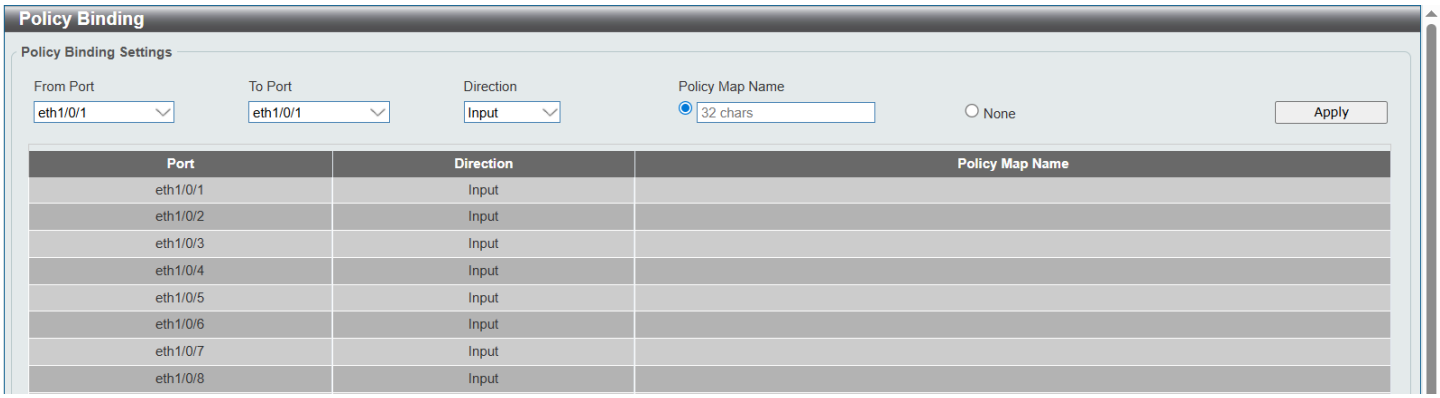
Click the **Back** button to return to the previous window.

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

QoS > Advanced Settings> 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:



QoS > Advanced Settings>Policy Binding

The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the range of ports that will be used for this configuration here.
Direction	Select the direction option here. **Input** specifies ingress traffic.
Policy Map Name	Enter the policy map name here. This name can be up to 32 characters long. Select the **None** option to not tie a policy map to this entry.

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

ACL > ACL Configuration Wizard

The ACL Configuration Wizard page allows you to create a new ACL access list or configure an existing ACL access list.

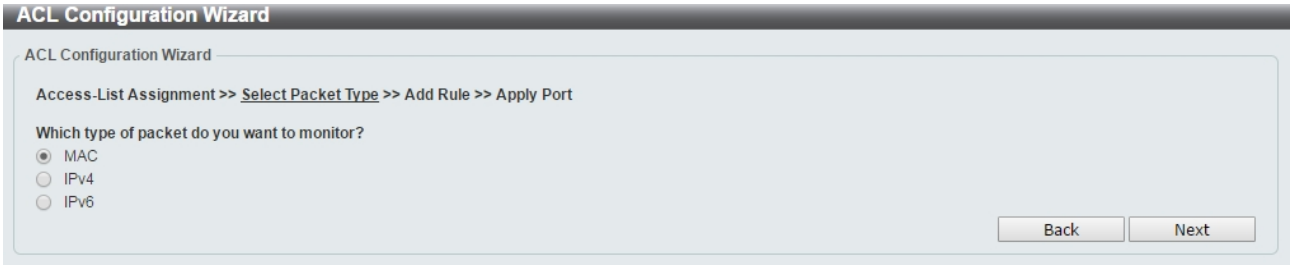


ACL > ACL Configuration Wizard

Create: Select **Create** and enter the ACL Name with a maximum of 32 characters.
Update: Select **Update** to see a table containing the existing access lists. Select the entry to re-configure it.

Click the **Next** button to continue.

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



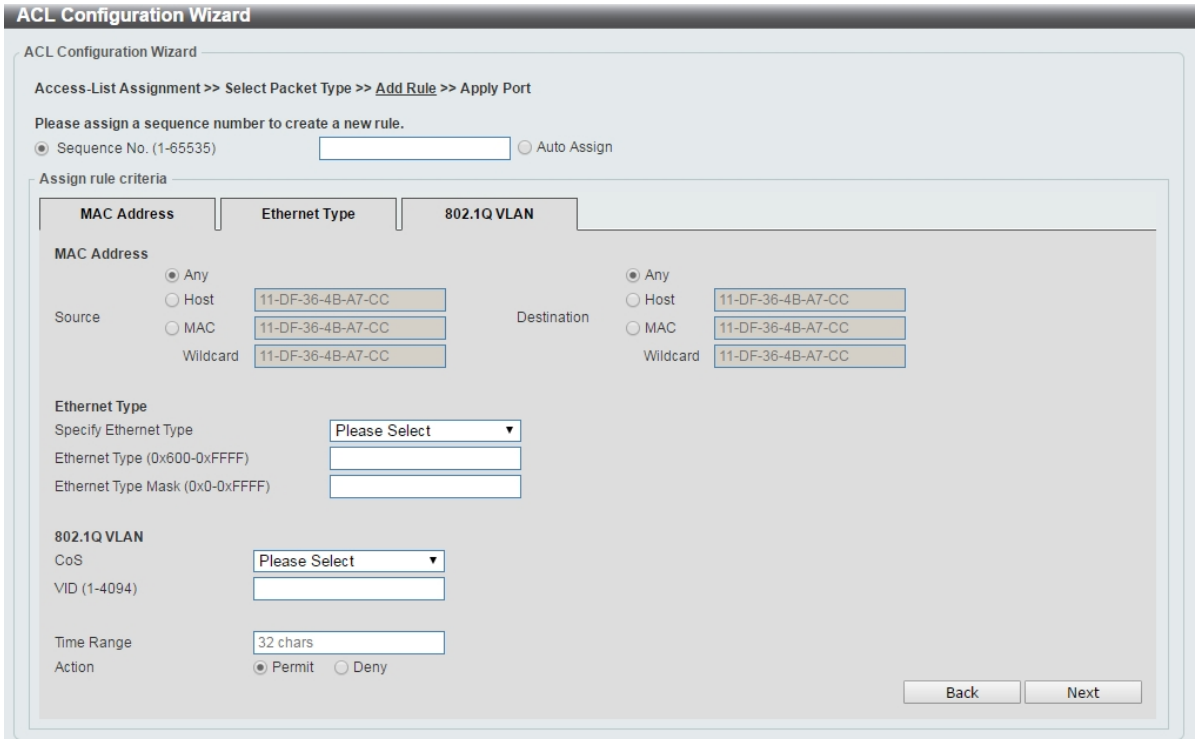
ACL > ACL Configuration Wizard – Packet Type

MAC: Select to create a MAC ACL.
IPv4: Select to create an IPv4 ACL.
IPv6: Select to create an IPv6 ACL.

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

Click the **Next** button to continue.

To define the MAC ACL: Select **MAC** and then click the **Next** button. Click the **MAC Address**, **Ethernet Type** and **802.1Q VLAN** tabs to display the following page:



ACL > ACL Configuration Wizard – Create MAC ACL

The Add ACL Profile **MAC** ACL contains the following fields:

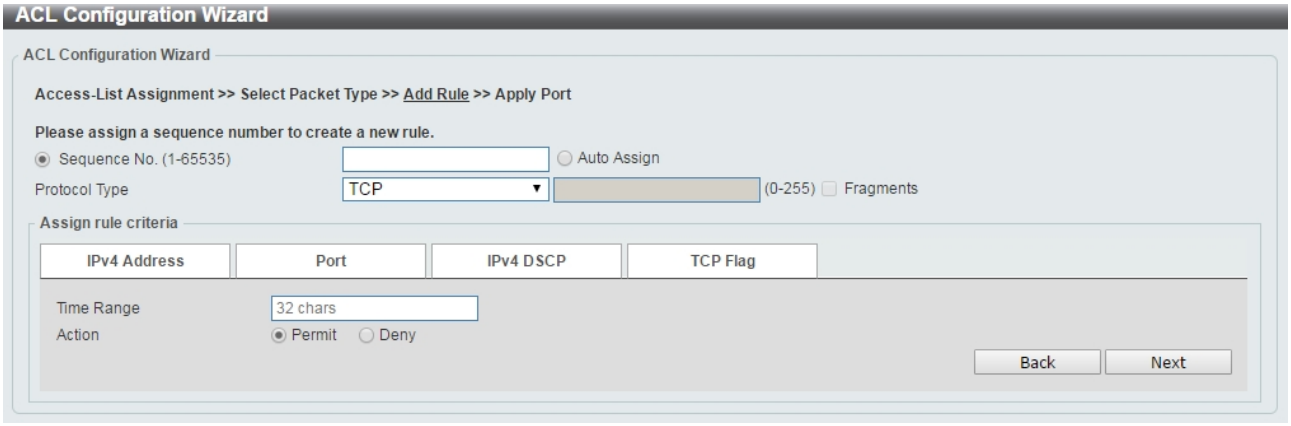
Sequence No.(1-65535): Select the ACL rule number. The value is between 1 and 65535. Select **Auto Assign** to automatically generate an ACL rule number for this entry.
Source: Select and enter the source information. Available options are **Any**, **Host**, and **MAC**. When **Any** is selected, any source traffic will be evaluated according to the conditions of this rule. When **Host** is specified, enter the source host's MAC address. When **MAC** is selected, the **Wildcard** will also be available. Enter the source MAC address and wildcard value in the spaces provided.
Destination: Select and enter the destination information. Available options are **Any**, **Host**, and **MAC**. When **Any** option is selected, any destination traffic will be evaluated according to the conditions of this rule. When **Host** is selected, enter the destination host's MAC address. When **MAC** is selected, the **Wildcard** will also be available. Enter the destination MAC address and wildcard value in the spaces provided.

Specify Ethernet Type: Select the Ethernet type option. 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 (0x600-0xFFFF): Enter the Ethernet type hexadecimal value. The value is between 0x600 and 0xFFFF. When any Ethernet type profile is selected in the **Specify Ethernet Type** drop-down list, the appropriate hexadecimal value will automatically be entered.
Ethernet Type Mask (0x0-0xFFFF): Enter the Ethernet type mask hexadecimal value. The value is between 0x0 and 0xFFFF. When any Ethernet type profile is selected in the **Specify Ethernet Type** drop-down list, the appropriate hexadecimal value will automatically be entered.

CoS: Select the CoS value used. This value is between 0 and 7.
VID (1-4094): Enter the VLAN ID that will be associated with this ACL rule. The value should be between 1 and 4094.
Time Range: Enter the time range.
Action: Select the action that this rule will take. The values are Permit and Deny.

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

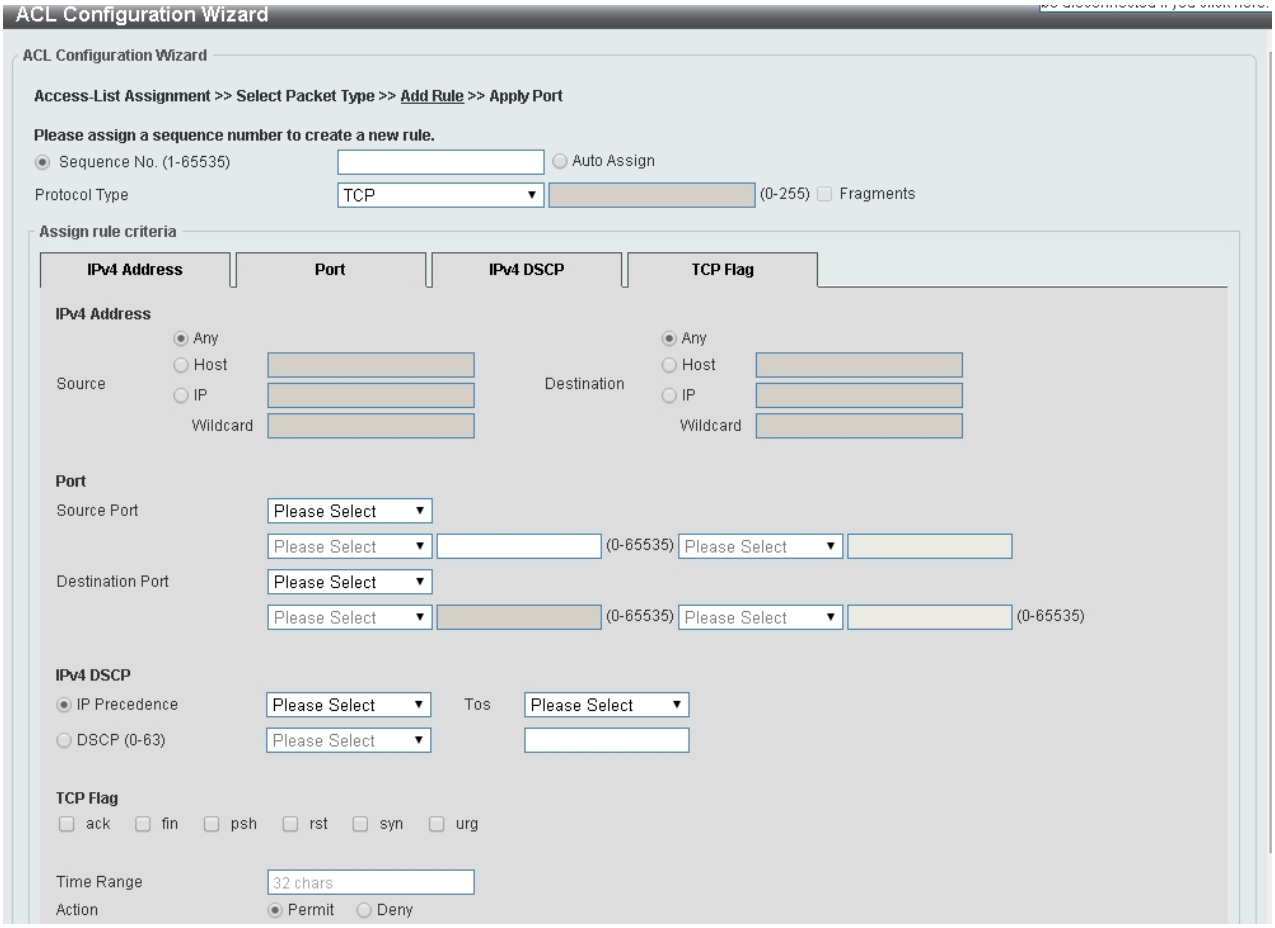
To define the IPv4 ACL: Select **IPv4** and then click the **Next** button. Click the **IPv4 Address**, **Port**, **IPv4 DSCP** and **TCP Flag** tabs to display the following page:



ACL > ACL Configuration Wizard – Create IPv4 ACL

Sequence No. (1-65535): Select and enter the ACL rule number. This value must be between 1 and 65535. Select **Auto Assign** to automatically generate an ACL rule number for this entry.
Protocol Type: Select the protocol type option. Options to choose from are **TCP**, **UDP**, **ICMP**, **EIGRP**, **ESP**, **GRE**, **IGMP**, **OSPF**, **PIM**, **VRRP**, **IP-in-IP**, **PCP**, **Protocol ID**, and **None**.

After selecting **TCP** as the **Protocol Type**, Click the **IPv4 Address**, **Port, IPv4 DSCP** and **TCP Flag** tabs to display the following page:



ACL > ACL Configuration Wizard – Create IPv4 ACL-TCP

Source: Select the source information. The values are **Any**, **Host** and **IP**.

Destination: Select the destination information. The values are **Any**, **Host** and **IP**.

Source Port: Select the source port value.

Destination Port: Select the destination port value.

IP Precedence: Select the IP precedence value. Options to choose from are **0 (routine)**, **1 (priority)**, **2 (immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.

ToS: Specify the Type-of-Service (**ToS**) value that will be used. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.

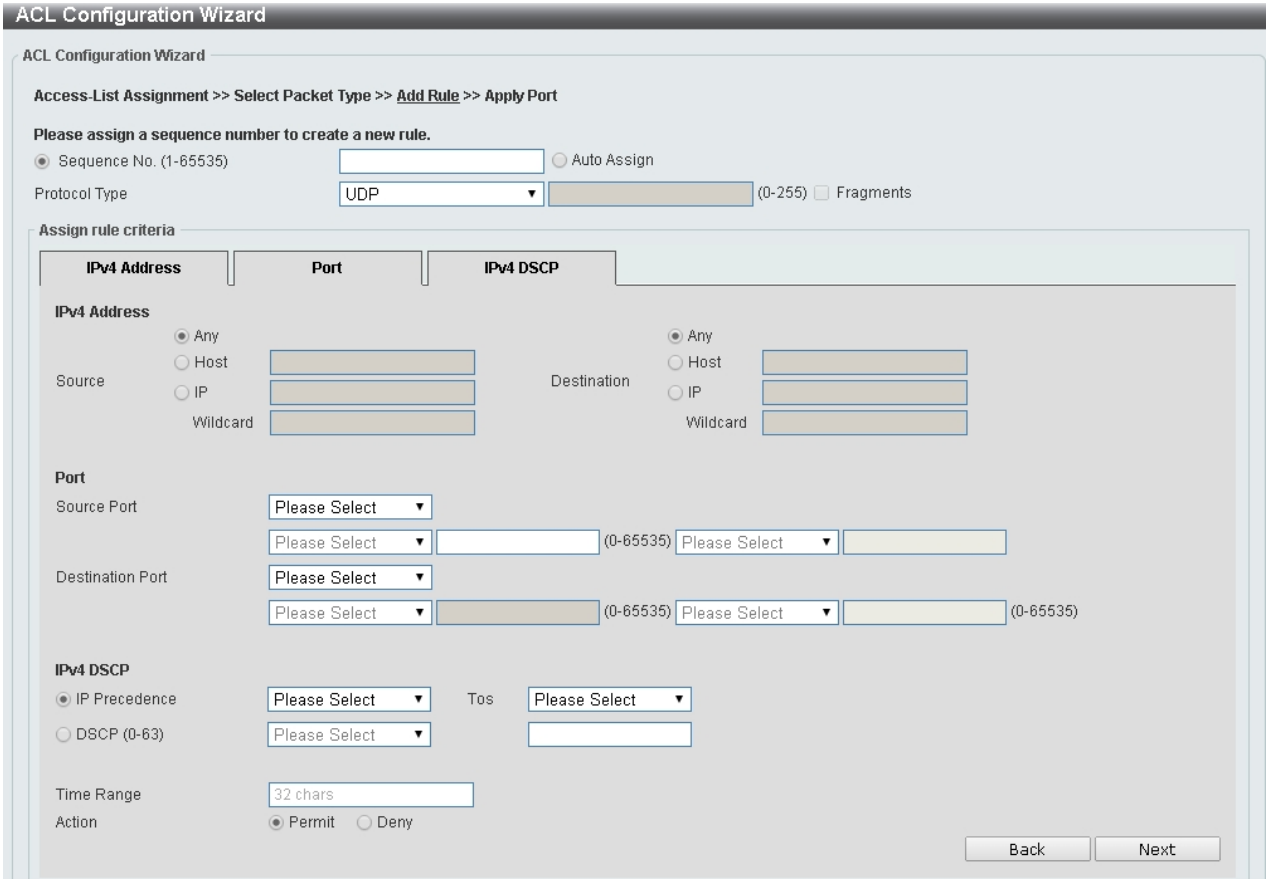
DSCP (0-63): Enter the DSCP value. And the range is between 0 and 63.

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**.

Time Range: Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting **UDP** as the **Protocol Type**, click the **IPv4 Address**, **Port** and **IPv4 DSCP** tabs to display the following page:



ACL > ACL Configuration Wizard – Create IPv4 ACL-UDP

Source: Select the source information. The values are **Any**, **Host** and **IP**.

Destination: Select the destination information. The values are **Any**, **Host** and **IP**.

Source Port: Select the source port value.

Destination Port: Select the destination port value.

IP Precedence: Select the IP precedence value. Options to choose from are **0 (routine)**, **1 (priority)**, **2 (immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.

ToS: Specify the Type-of-Service (**ToS**) value that will be used. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.

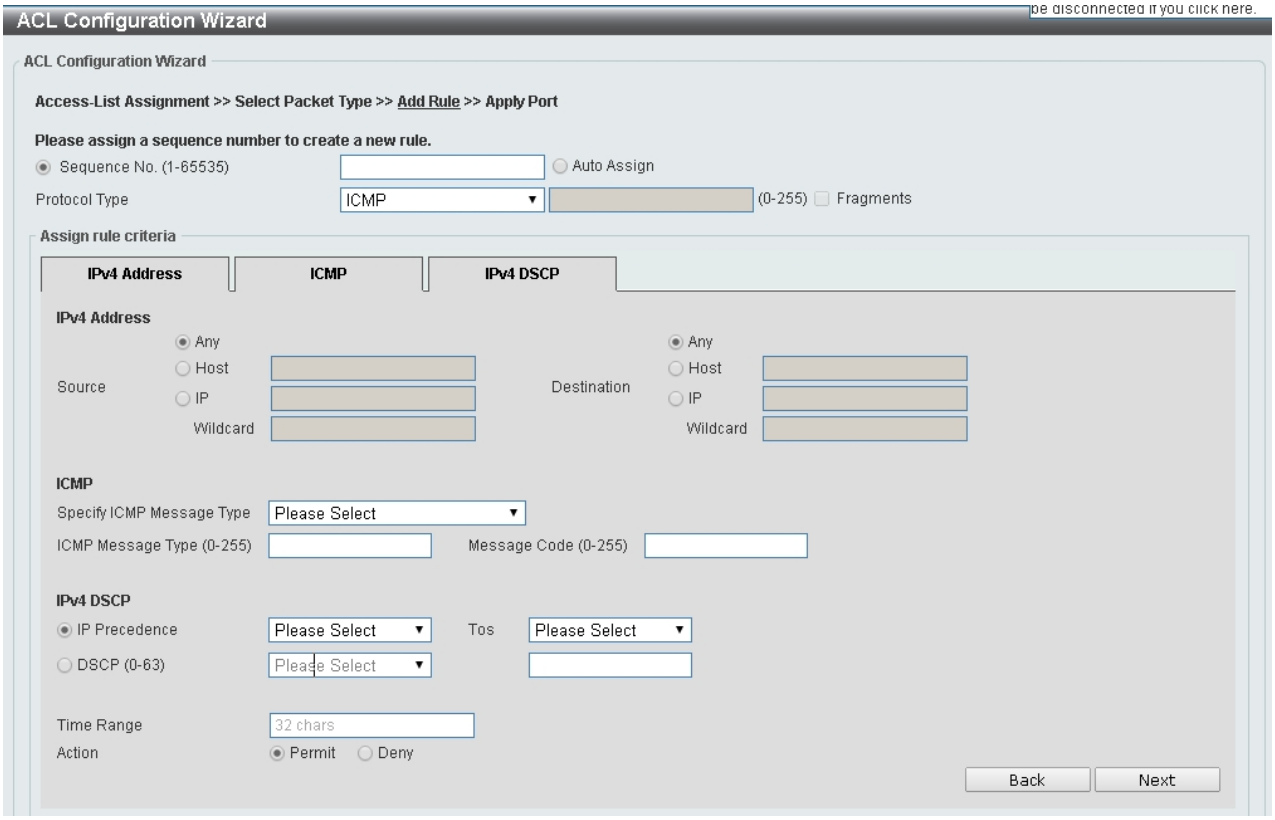
DSCP (0-63): Enter the DSCP value. And the range is between 0 and 63.

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**.

Time Range: Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting **ICMP** as the **Protocol Type**, click the **IPv4 Address**, **ICMP** and **IPv4 DSCP** tabs to display the following page:



ACL > ACL Configuration Wizard – Create IPv4 ACL-ICMP

Source: Select the source information. The values are **Any**, **Host** and **IP**.

Destination: Select the destination information. The values are **Any**, **Host** and **IP**.

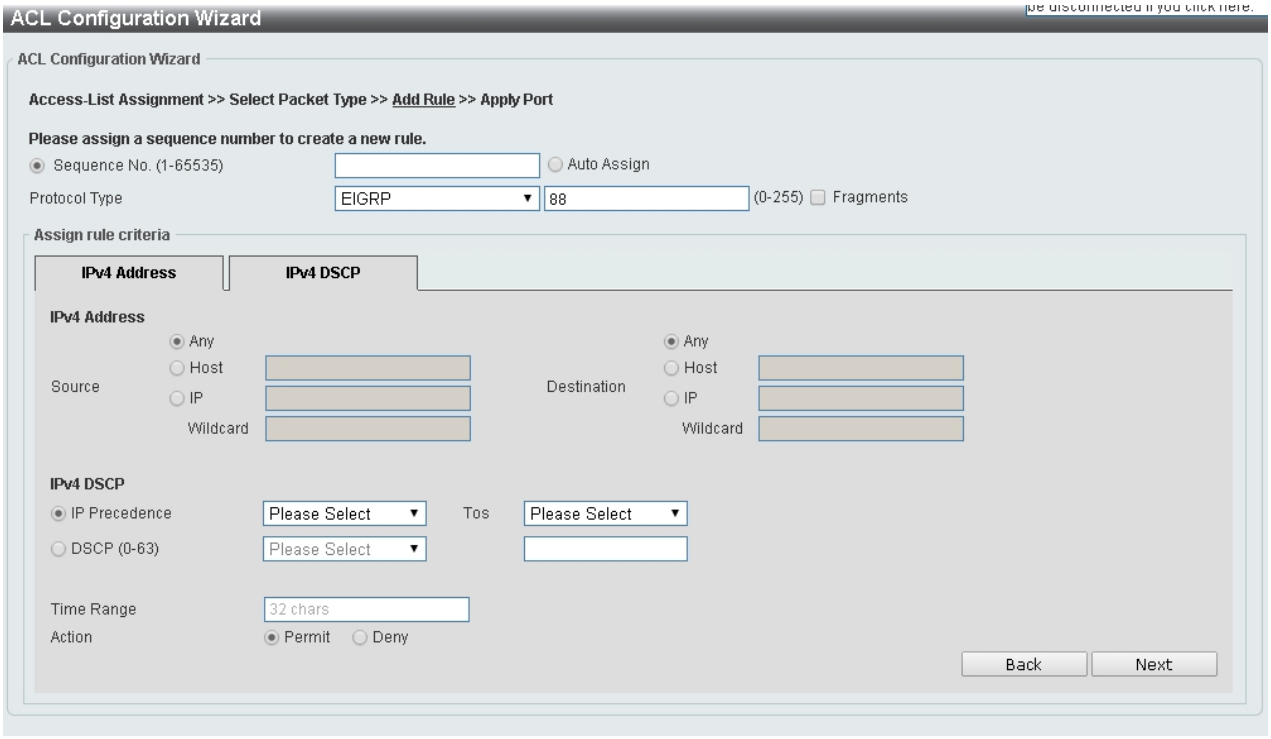
IP Precedence: Select the IP precedence value. Options to choose from are **0 (routine)**, **1 (priority)**, **2 (immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.
ToS: Select the Type-of-Service (**ToS**) value that will be used. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.

DSCP (0-63): Select the DSCP value. And the range is between 0 and 63.

Specify ICMP Message Type: Specify the ICMP message type.
ICMP Message Type (0-255): When the **ICMP Message Type** is not selected, enter the ICMP Message Type numerical value used. When the **ICMP Message Type** is selected, this numerical value will automatically be entered.
Message Code (0-255): When the **ICMP Message Type** is not selected, enter the Message Code numerical value used. When the **ICMP Message Type** is selected, this numerical value will automatically be entered.
Time Range: Enter the time range.

Action: Specify the action for the rule. The values are Permit and Deny.

After selecting **EIGRP** as the **Protocol Type**, click the **IPv4 Address** and **IPv4 DSCP** tabs to display the following page:



ACL > ACL Configuration Wizard – Create IPv4 ACL-EIGRP

Source: Select the source information. The values are **Any**, **Host** and **IP**.

Destination: Select the destination information. The values are **Any**, **Host** and **IP**.

Fragments: Specify the **Fragments** option to include packet fragment filtering.

Source: Select the source information. The values are **Any**, **Host** and **IP**.

Destination: Select the destination information. The values are **Any**, **Host** and **IP**.

IP Precedence: Select the IP precedence value. Options to choose from are **0 (routine)**, **1 (priority)**, **2 (immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.

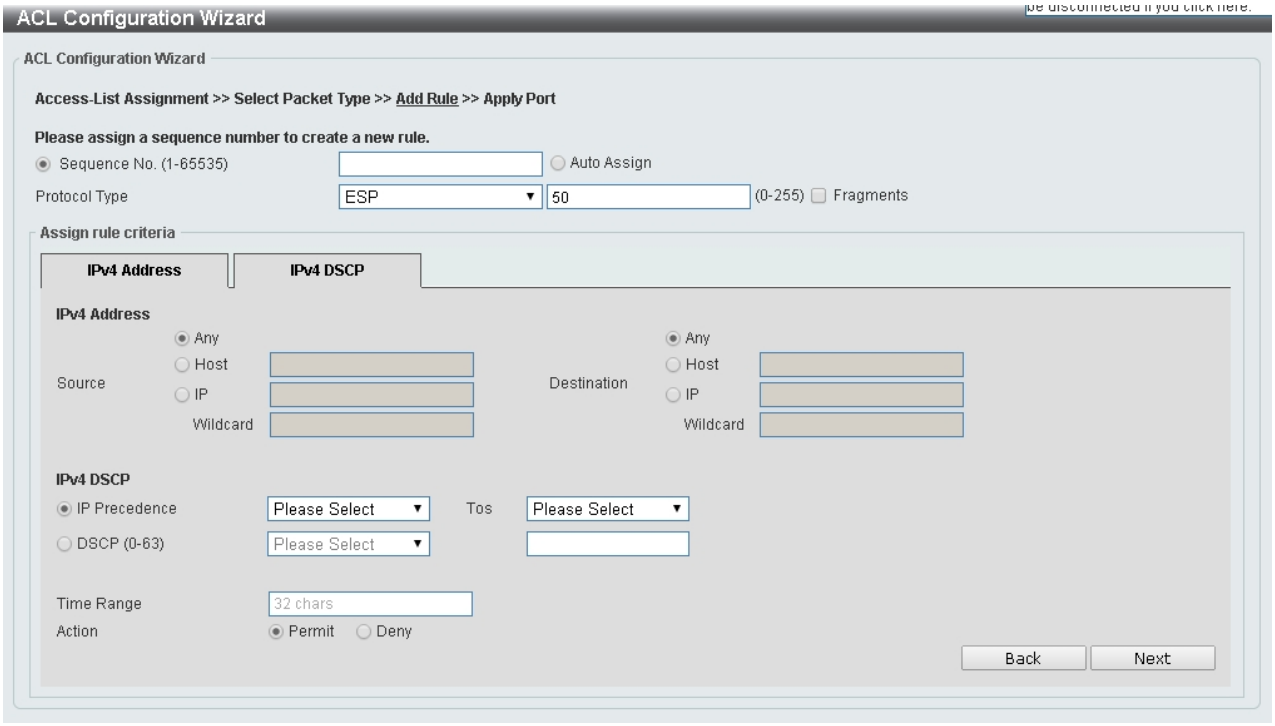
ToS: Select the Type-of-Service (**ToS**) value that will be used. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.

DSCP (0-63): Select the DSCP value. And the range is between 0 and 63.

Time Range: Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting **ESP** as the **Protocol Type**, click the **IPv4 Address** and **IPv4 DSCP** tabs to display the following page:



ACL > ACL Configuration Wizard – Create IPv4 ACL-ESP

Source: Select the source information. The values are **Any**, **Host** and **IP**.

Destination: Select the destination information. The values are **Any**, **Host** and **IP**.

IP Precedence: Select the IP precedence value. Options to choose from are **0 (routine)**, **1 (priority)**, **2 (immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.

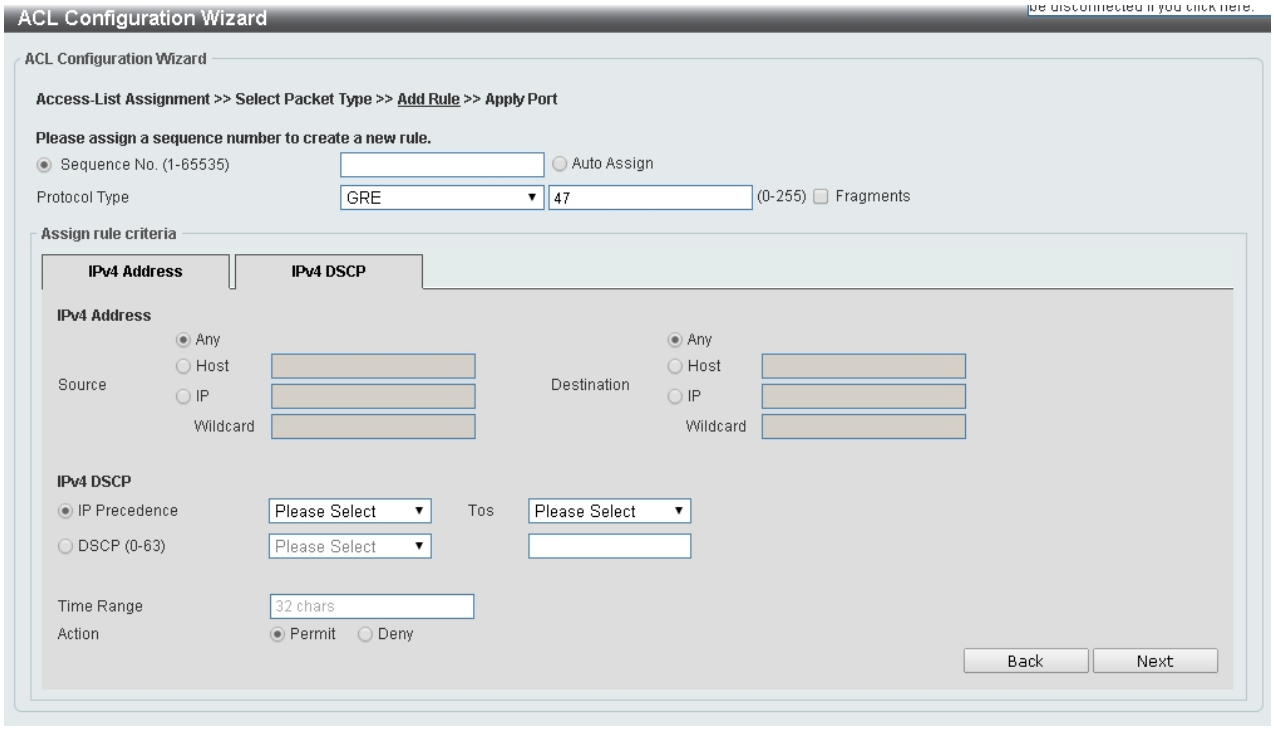
ToS: Select the Type-of-Service (**ToS**) value that will be used. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.

DSCP (0-63): Select the DSCP value. And the range is between 0 and 63.

Time Range: Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting **GRE** as the **Protocol Type**, click the **IPv4 Address** and **IPv4 DSCP** tabs to display the following page:



ACL > ACL Configuration Wizard – Create IPv4 ACL-GRE

Fragments: Select the **Fragments** option to include packet fragment filtering.

Source: Select the source information. The values are **Any**, **Host** and **IP**.

Destination: Select the destination information. The values are **Any**, **Host** and **IP**.

IP Precedence: Select the IP precedence value. Options to choose from are **0 (routine)**, **1 (priority)**, **2 (immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.

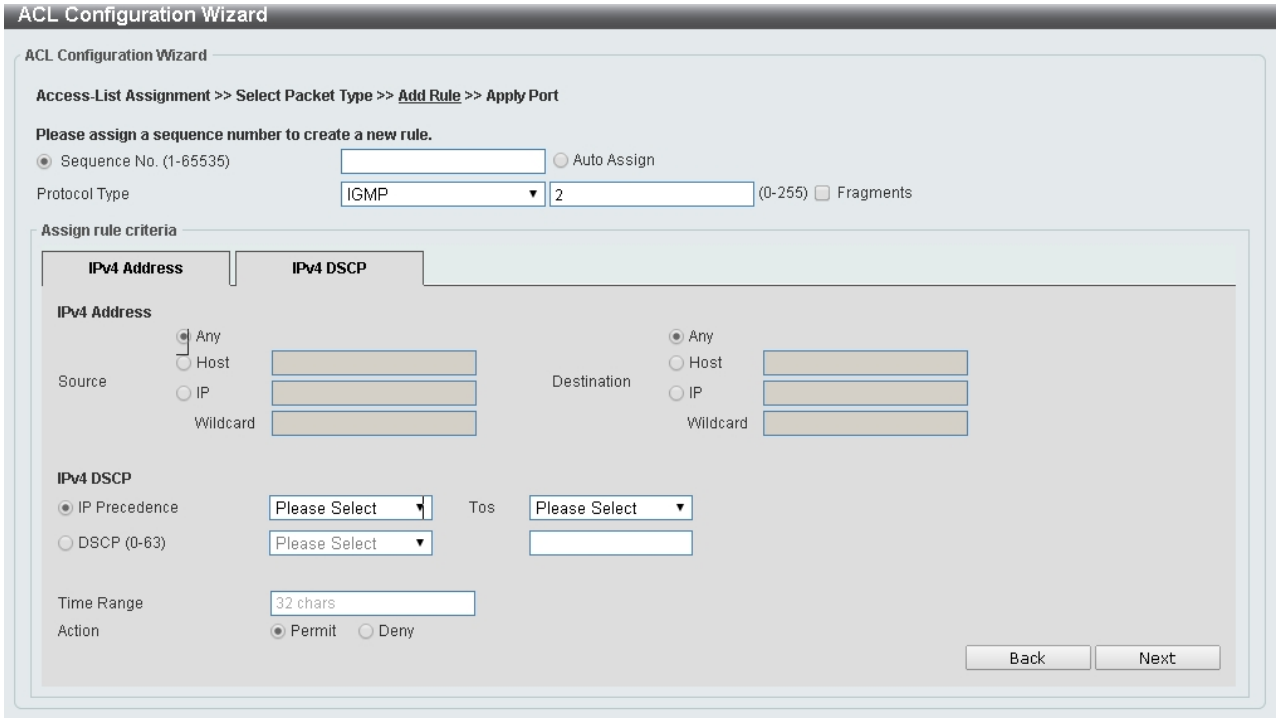
ToS: Specify the Type-of-Service (**ToS**) value that will be used. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.

DSCP (0-63): Select the DSCP value. And the range is between 0 and 63.

Time Range: Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting **IGMP** as the **Protocol Type**, click the **IPv4 Address**, and **IPv4 DSCP** tabs to display the following page:



ACL > ACL Configuration Wizard – Create IPv4 ACL-IGMP

Fragments: Select the **Fragments** option to include packet fragment filtering.

Source: Select the source information. The values are **Any**, **Host** and **IP**.

Destination: Select the destination information. The values are **Any**, **Host** and **IP**.

IP Precedence: Select the IP precedence value. Options to choose from are **0 (routine)**, **1 (priority)**, **2 (immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.

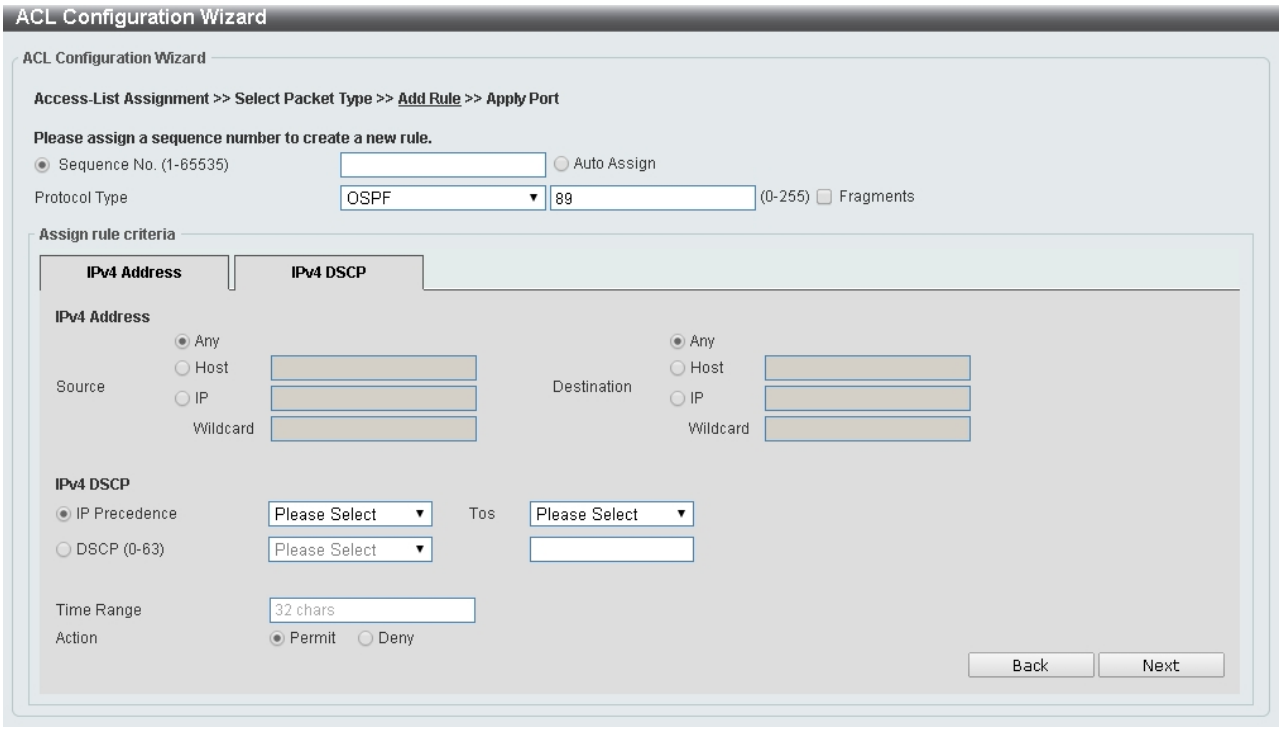
ToS: Specify the Type-of-Service (**ToS**) value that will be used. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.

DSCP (0-63): Select the DSCP value. And the range is between 0 and 63.

Time Range: Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting **OSPF** as the **Protocol Type,** click the **IPv4 Address**, and **IPv4 DSCP** to display the following page:



ACL > ACL Configuration Wizard – Create IPv4 ACL-OSPF

Fragments: Select the **Fragments** option to include packet fragment filtering.

Source: Select the source information. The values are **Any**, **Host** and **IP**.

Destination: Select the destination information. The values are **Any**, **Host** and **IP**.

IP Precedence: Select the IP precedence value. Options to choose from are **0 (routine)**, **1 (priority)**, **2 (immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.

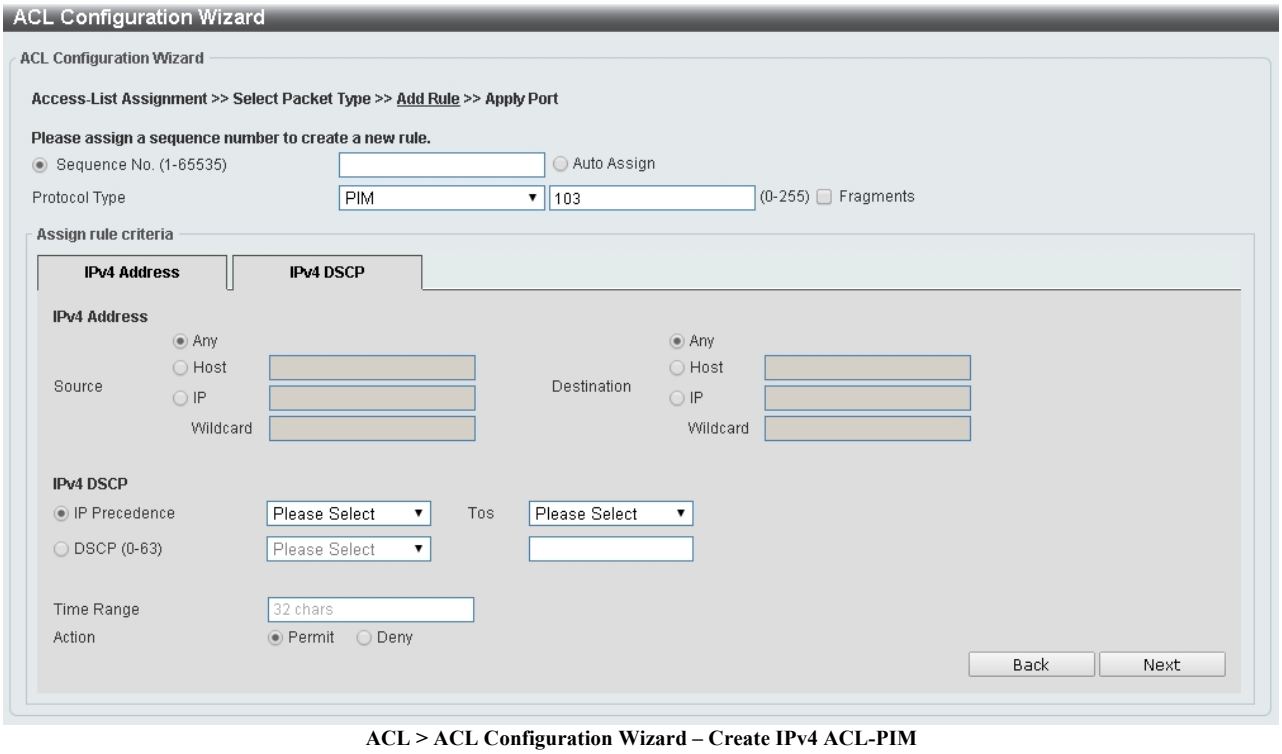
ToS: Specify the Type-of-Service (**ToS**) value that will be used. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.

DSCP (0-63): Select the DSCP value. And the range is between 0 and 63.

Time Range: Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting **PIM** as the **Protocol Type,** click the **IPv4 Address**, and **IPv4 DSCP** tabs to display the following page**:**



ACL > ACL Configuration Wizard – Create IPv4 ACL-PIM

Fragments: Select the **Fragments** option to include packet fragment filtering.

Source: Select the source information. The values are **Any**, **Host** and **IP**.

Destination: Select the destination information. The values are **Any**, **Host** and **IP**.

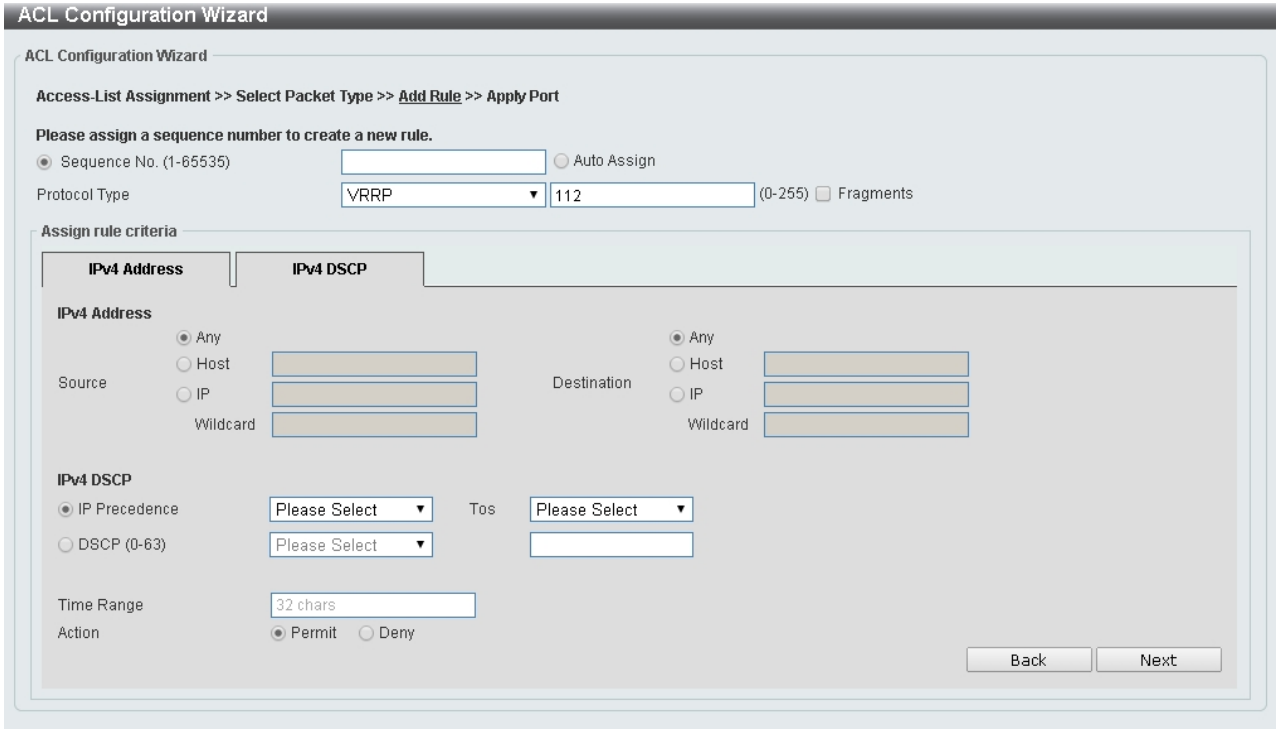
IP Precedence: Select the IP precedence value used. Options to choose from are **0 (routine)**, **1 (priority)**, **2 (immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.
ToS: Select the Type-of-Service (**ToS**) value that will be used. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.

DSCP (0-63): Select the DSCP value. And the range is between 0 and 63.

Time Range: Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting **VRRP** as the **Protocol Type,** click the **IPv4 Address**, and **IPv4 DSCP** tabs to display the following page**:**



ACL > ACL Configuration Wizard – Create IPv4 ACL-VRRP

Fragments: Select the **Fragments** option to include packet fragment filtering.

Source: Select the source information. The values are **Any**, **Host** and **IP**.

Destination: Select the destination information. The values are **Any**, **Host** and **IP**.

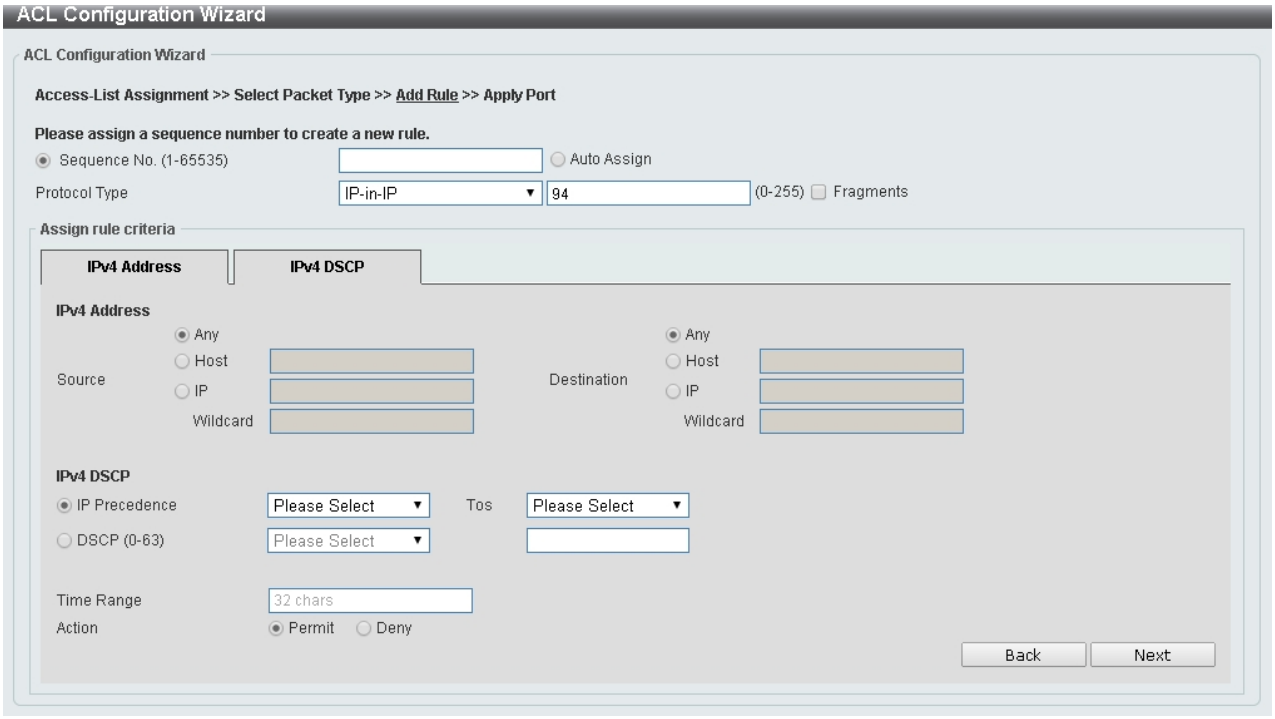
IP Precedence: Select the IP precedence value. Options to choose from are **0 (routine)**, **1 (priority)**, **2 (immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.
ToS: Select the Type-of-Service (**ToS**) value that will be used. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.

DSCP (0-63): Select the DSCP value. And the range is between 0 and 63.

Time Range: Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting **IP-in-IP** as the **Protocol Type,** click the **IPv4 Address**, and **IPv4 DSCP** tabs to display the following page**:**



ACL > ACL Configuration Wizard – Create IPv4 ACL-IP in IP

Fragments: Select the **Fragments** option to include packet fragment filtering.

Source: Select the source information. The values are **Any**, **Host** and **IP**.

Destination: Select the destination information. The values are **Any**, **Host** and **IP**.

IP Precedence: Select the IP precedence value. Options to choose from are **0 (routine)**, **1 (priority)**, **2 (immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.

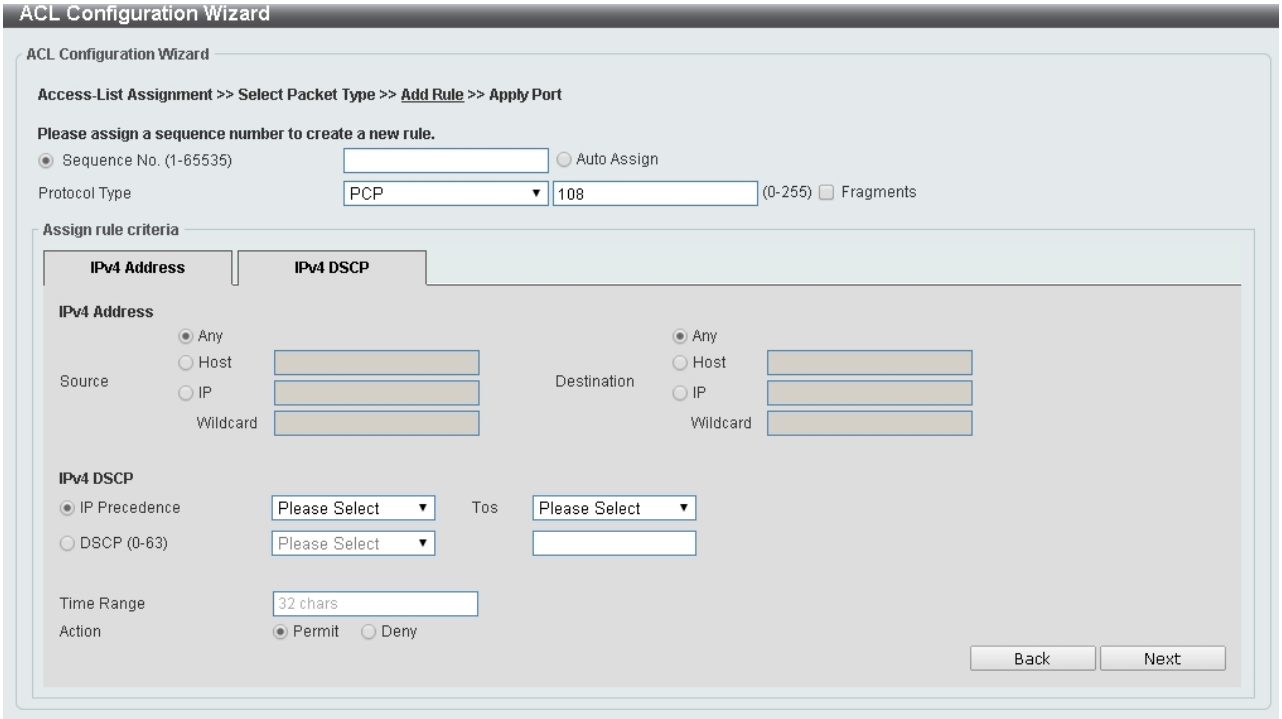
ToS: Select the Type-of-Service (**ToS**) value that will be used. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.

DSCP (0-63): Select the DSCP value. And the range is between 0 and 63.

Time Range: Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting **PCP** as the **Protocol Type,** click the **IPv4 Address**, and **IPv4 DSCP** tabs to display the following page**:**



ACL > ACL Configuration Wizard – Create IPv4 ACL-PCP

Fragments: Select the **Fragments** option to include packet fragment filtering.

Source: Select the source information. The values are **Any**, **Host** and **IP**.

Destination: Select the destination information. The values are **Any**, **Host** and **IP**.

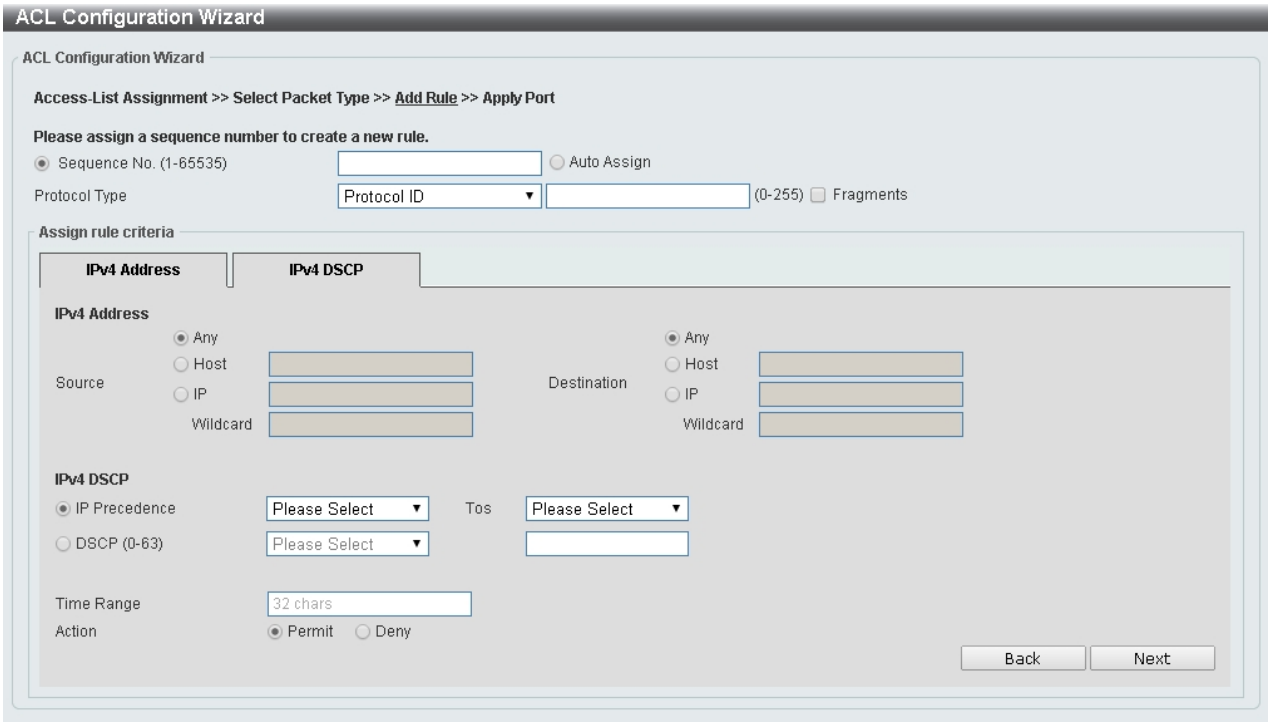
IP Precedence: Select the IP precedence value. Options to choose from are **0 (routine)**, **1 (priority)**, **2 (immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.
ToS: Select the Type-of-Service (**ToS**) value that will be used. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.

DSCP (0-63): Select the DSCP value. And the range is between 0 and 63.

Time Range: Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting **Protocol ID** as the **Protocol Type,** click the **IPv4 Address**, and **IPv4 DSCP** tabs to display the following page**:**



ACL > ACL Configuration Wizard – Create IPv4 ACL-Protocol ID

Fragments: Select the **Fragments** option to include packet fragment filtering.

Source: Select the source information. The values are **Any**, **Host** and **IP**.

Destination: Select the destination information. The values are **Any**, **Host** and **IP**.

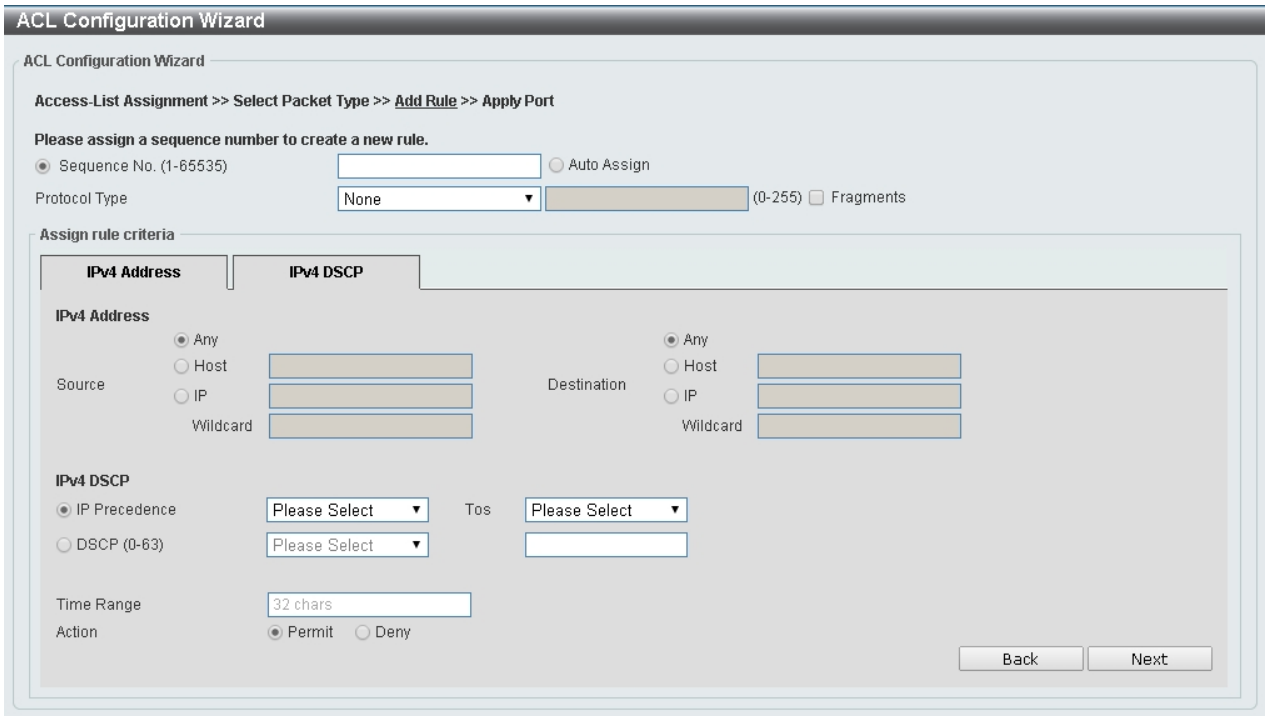
IP Precedence: Select the IP precedence value used. Options to choose from are **0 (routine)**, **1 (priority)**, **2 (immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.
ToS: Select the Type-of-Service (**ToS**) value that will be used. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.

DSCP (0-63): Select the DSCP value. And the range is between 0 and 63.

Time Range: Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting **None** as the **Protocol Type,** click the associated tabs with **IPv4 Address**, and **IPv4 DSCP** tabs to display the following page**:**



ACL > ACL Configuration Wizard – Create IPv4 ACL-None

Fragments: Select the **Fragments** option to include packet fragment filtering.

Source: Select the source information. The values are **Any**, **Host** and **IP**.

Destination: Select the destination information. The values are **Any**, **Host** and **IP**.

IP Precedence: Select the IP precedence value. Options to choose from are **0 (routine)**, **1 (priority)**, **2 (immediate)**, **3 (flash)**, **4 (flash-override)**, **5 (critical)**, **6 (internet)**, and **7 (network)**.

ToS: Select the Type-of-Service (**ToS**) value that will be used. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.

DSCP (0-63): Select the DSCP value. And the range is between 0 and 63.

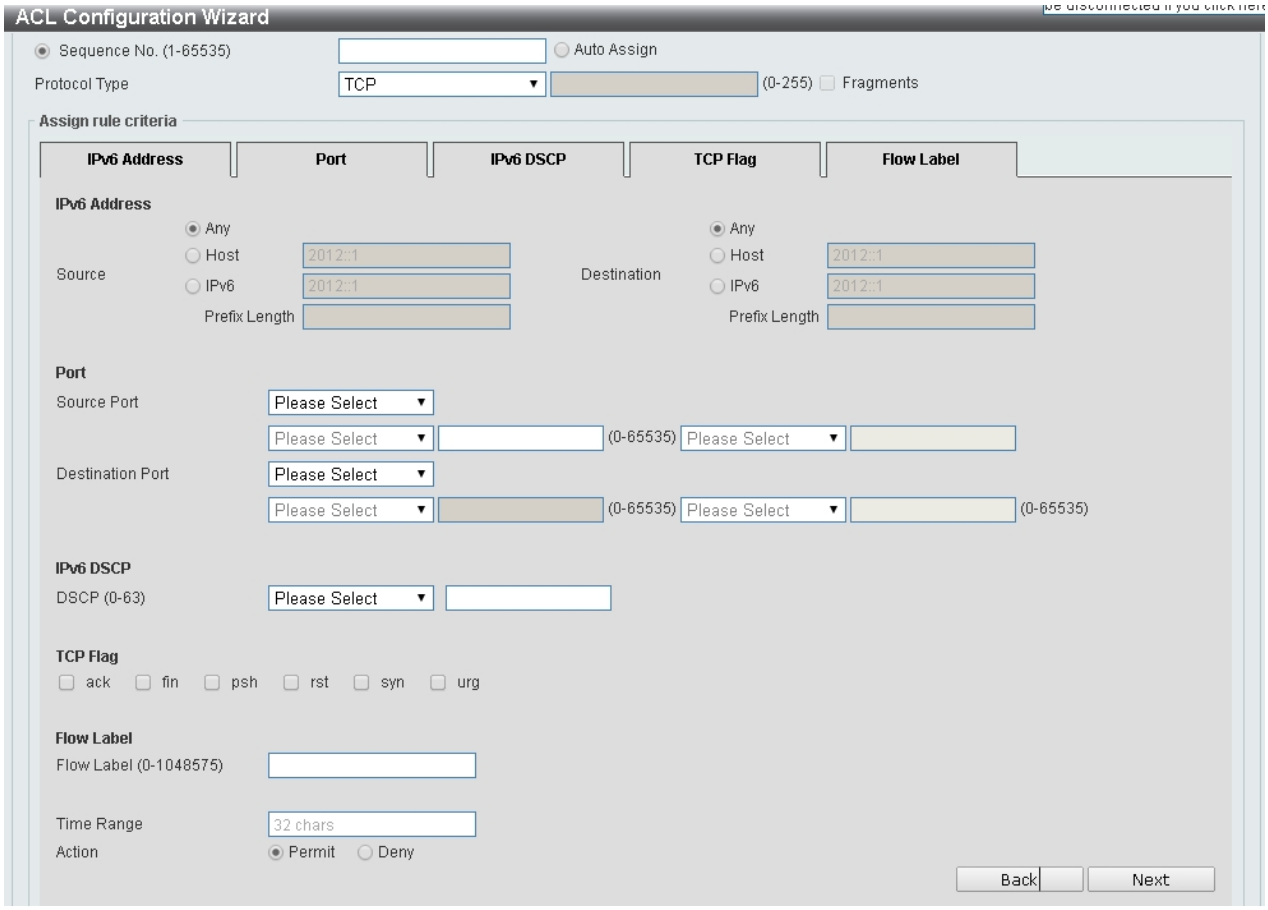
Time Range: Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

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

Click the **Next** button to continue.

To define the IPv6 ACL: Select **IPv6** and then click the **Next** button. Select **TCP** option as the **Protocol Type** and click the **IPv6 Address**, **Port**, **IPv6 DSCP**, **TCP Flag** and **Flow Label** tabs to display the following page**:**



ACL > ACL Configuration Wizard – Create IPv6 ACL-TCP

Source Port: Select the source port value.

Destination Port: Select the destination port value.

IPv6 DSCP (0-63): Select the DSCP value. And the range is between 0 and 63.

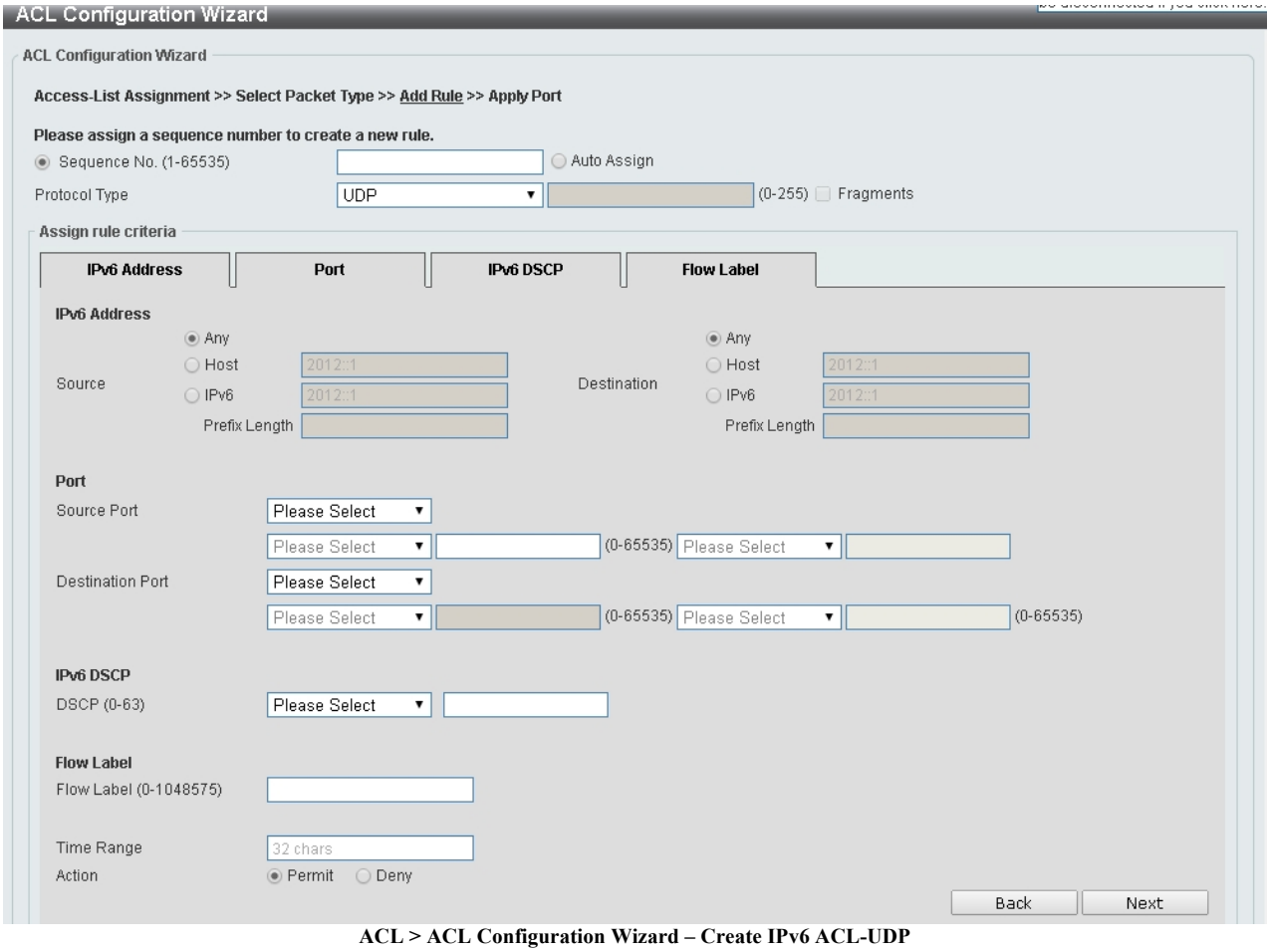
TCP Flag: Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are **ack**, **fin**, **psh**, **rst**, **syn**, and **urg**.

Flow Label (0-1048575): Enter the flow label value. This value must be between 0 and 1048575.

Time Range: Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting **UDP** as the **Protocol Type,** click the **IPv6 Address**, **Port**, **IPv6 DSCP** and **Flow Label** tabs to display the following page**:**



ACL > ACL Configuration Wizard – Create IPv6 ACL-UDP

Source Port: Select the source port value.

Destination Port: Select the destination port value.

Source: Select the source information. The values are **Any**, **Host** and **IP**.

Destination: Select the destination information. The values are **Any**, **Host** and **IP**.

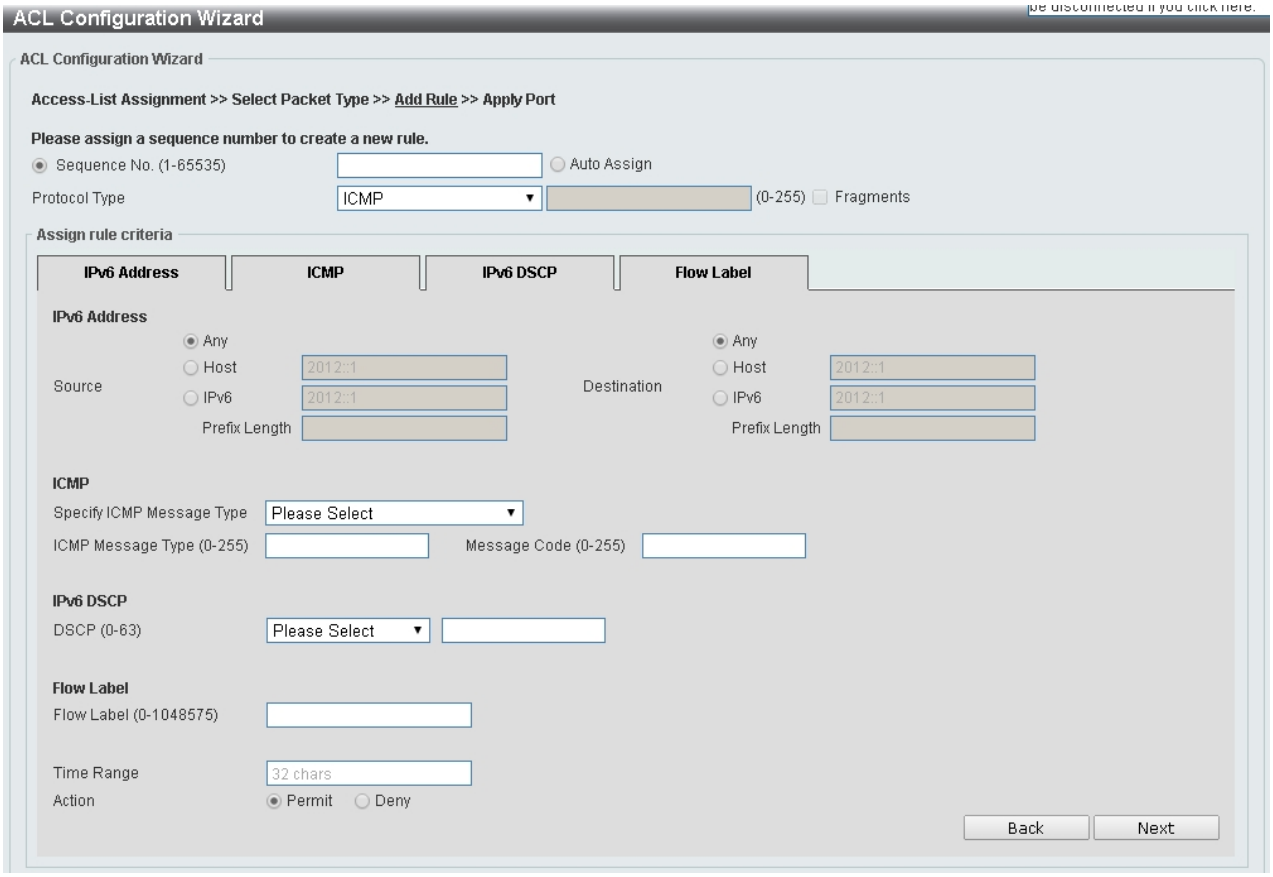
DSCP (0-63): Select the DSCP value. And the range is between 0 and 63.

Flow Label (0-1048575): Enter the flow label value. This value must be between 0 and 1048575.

Time Range: Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting **ICMP** as the **Protocol Type,** click the **IPv6 Address**, **ICMP**, **IPv6 DSCP** and **Flow Label** tabs to display the following page**:**



ACL > ACL Configuration Wizard – Create IPv6 ACL-ICMP

Source: Select the source information. The values are **Any**, **Host** and **IP**.

Destination: Select the destination information. The values are **Any**, **Host** and **IP**.

DSCP (0-63): Select the DSCP value. And the range is between 0 and 63.

Flow Label (0-1048575): Enter the flow label value. This value must be between 0 and 1048575.

Specify ICMP Message Type: Select the ICMP message type used.

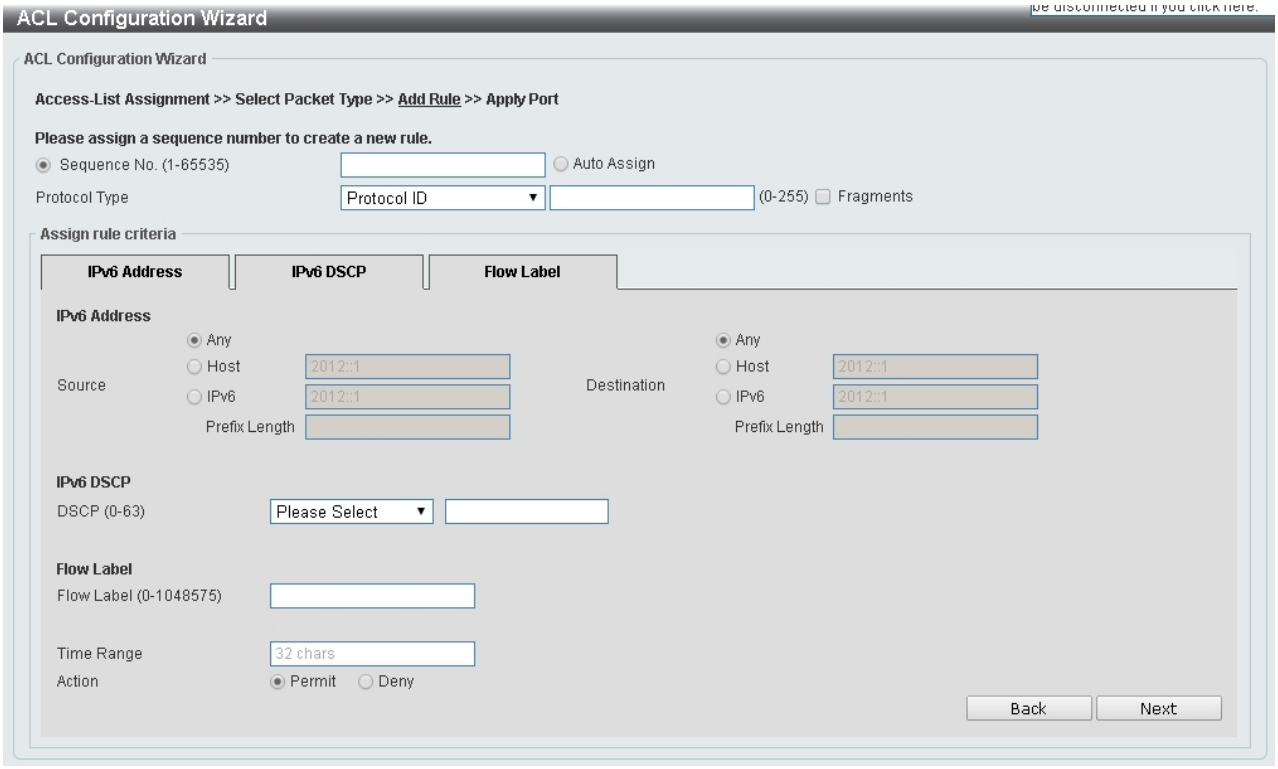
ICMP Message Type **(0-255):** When the **ICMP Message Type** is not selected, enter the ICMP Message Type numerical value. When the **ICMP Message Type** is selected, this numerical value will automatically be entered.

Message Code (0-255): When the **ICMP Message Type** is not selected, enter the Message Code numerical value. When the **ICMP Message Type** is selected, this numerical value will automatically be entered.

Time Range: Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

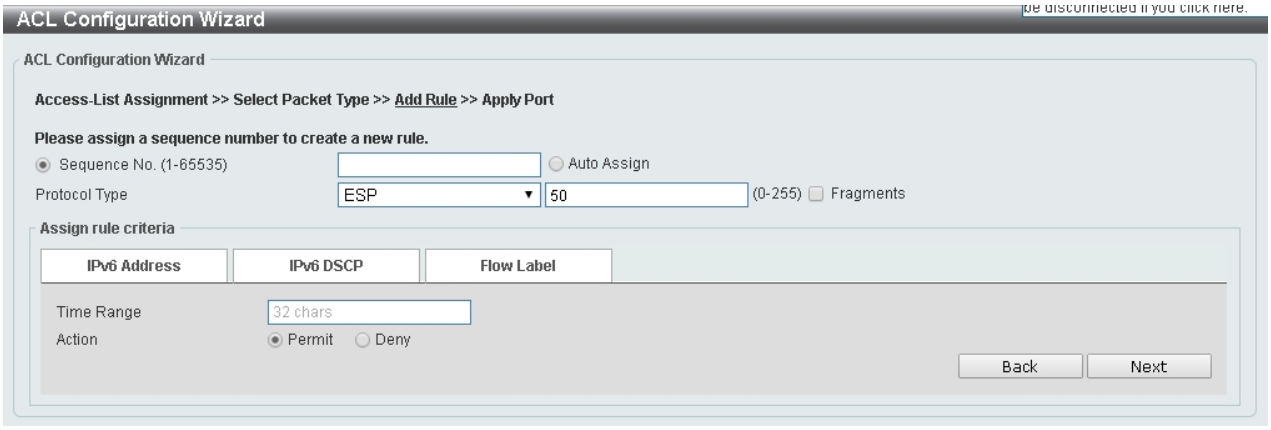
After selecting **Protocol ID** as the **Protocol Type,** click the **IPv6 Address**, **IPv6 DSCP** and **Flow Label** tabs to display the following page**:**



ACL > ACL Configuration Wizard – Create IPv6 ACL-Protocol ID

Source: Select the source information. The values are **Any**, **Host** and **IP**.
Destination: Select the destination information. The values are **Any**, **Host** and **IP**.
DSCP (0-63): Enter the DSCP value. And the range is between 0 and 63.
Flow Label (0-1048575): Enter the flow label value. This value must be between 0 and 1048575.
Action: Select the action for the rule. The values are **Permit** and **Deny**.

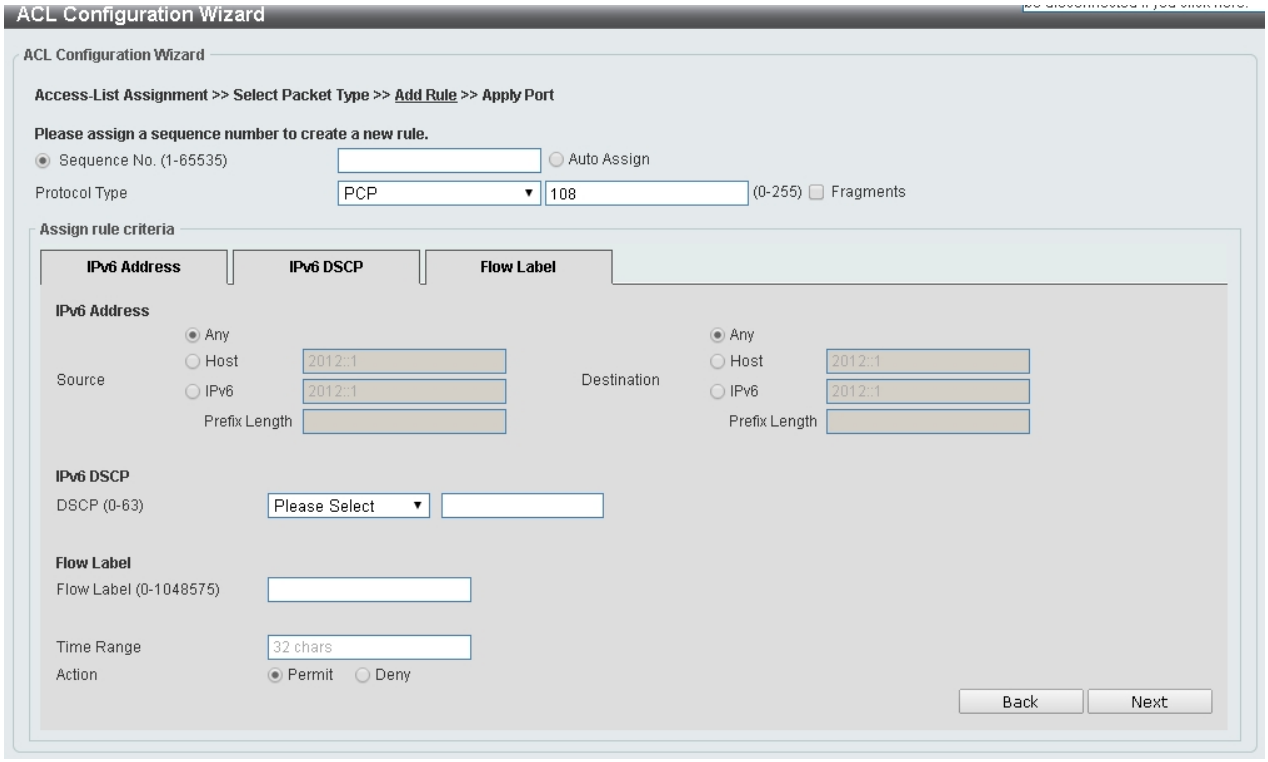
After selecting **ESP** as the **Protocol Type,** click the **IPv6 Address**, **IPv6 DSCP** and **Flow Label** tabs to display the following page**:**



ACL > ACL Configuration Wizard – Create IPv6 ACL-ESP

Source: Select the source information. The values are **Any**, **Host** and **IP**.
Destination: Select the destination information. The values are **Any**, **Host** and **IP**.
DSCP (0-63): Enter the DSCP value. And the range is between 0 and 63.
Flow Label (0-1048575): Enter the flow label value. This value must be between 0 and 1048575.
Time Range: Enter the time range.
Action: Select the action for the rule. The values are **Permit** and **Deny**.

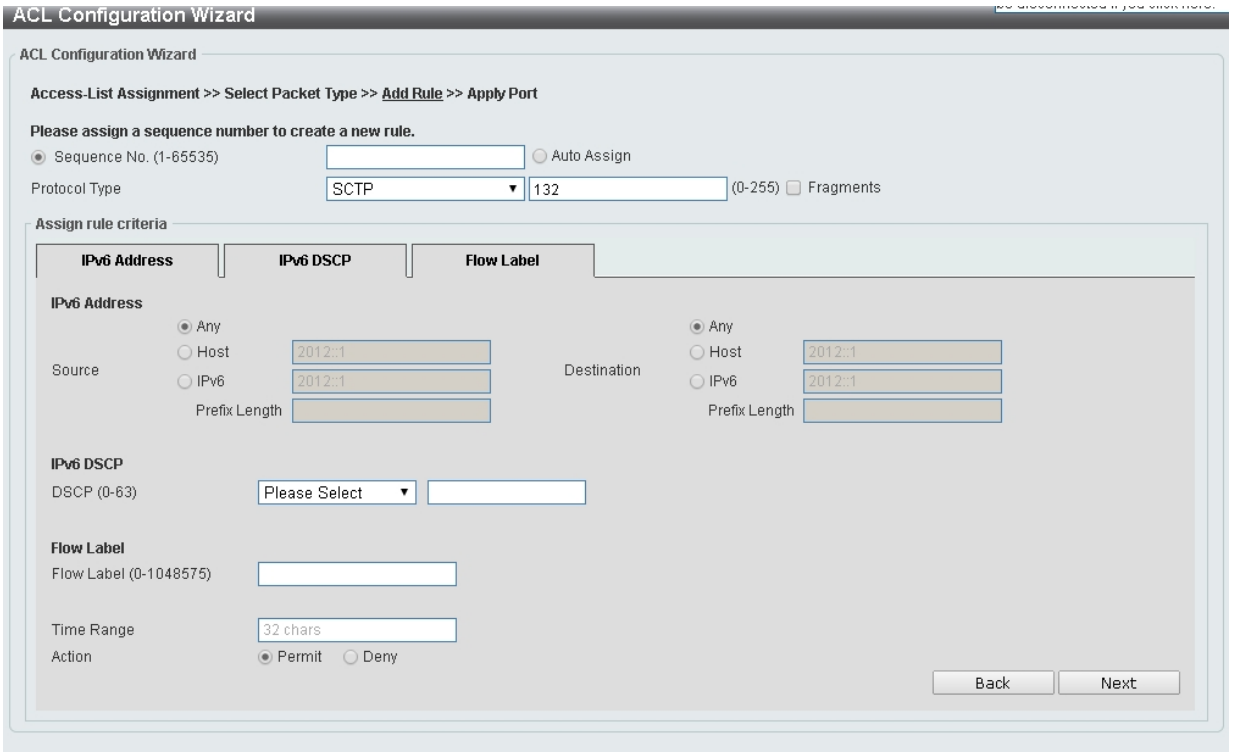
After selecting **PCP** as the **Protocol Type,** click the **IPv6 Address**, **IPv6 DSCP** and **Flow Label** tabs to display the following page**:**



ACL > ACL Configuration Wizard – Create IPv6 ACL-PCP

Source: Select the source information. The values are **Any**, **Host** and **IP**.
Destination: Select the destination information. The values are **Any**, **Host** and **IP**.
DSCP (0-63): Enter the DSCP value. And the range is between 0 and 63.
Flow Label (0-1048575): Enter the flow label value. This value must be between 0 and 1048575.
Time Range: Enter the time range.
Action: Select the action for the rule. The values are **Permit** and **Deny**.

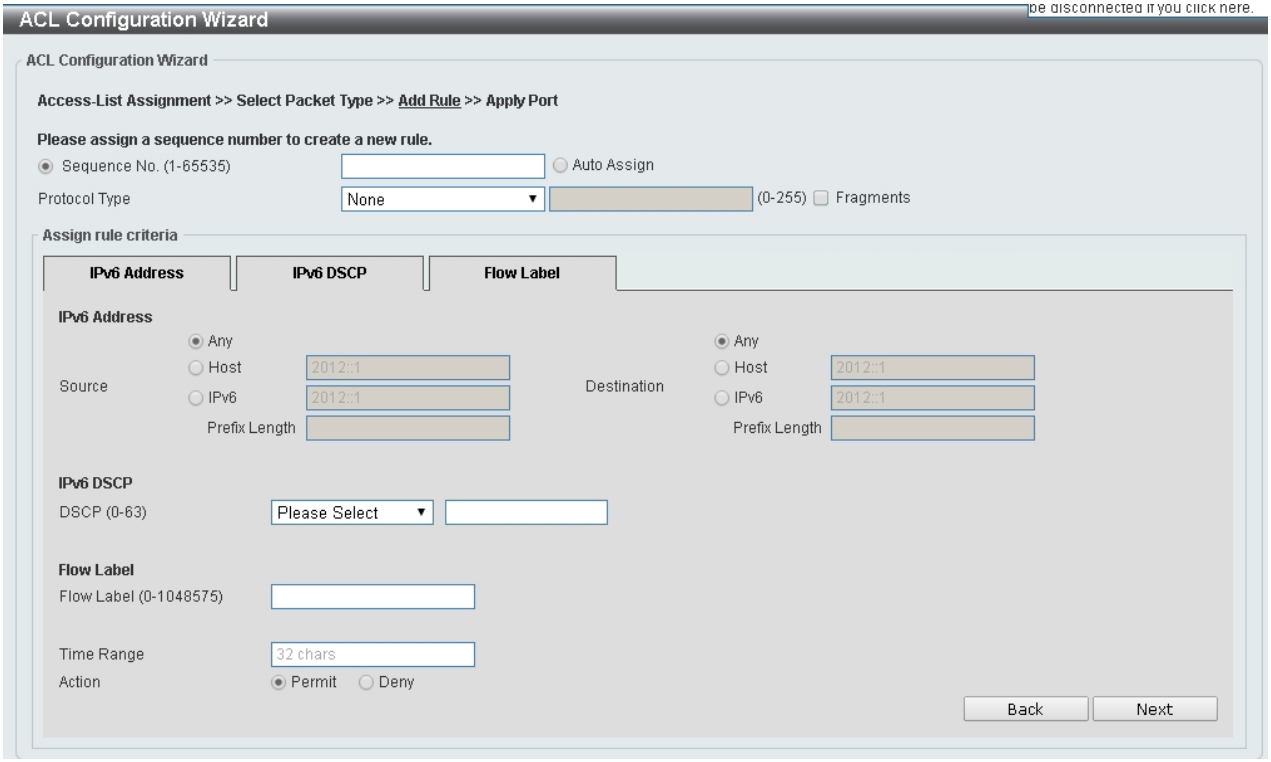
After selecting **SCTP** as the **Protocol Type,** click the **IPv6 Address**, **IPv6 DSCP** and **Flow Label** tabs to display the following page:



ACL > ACL Configuration Wizard – Create IPv6 ACL-SCTP

Source: Select the source information. The values are **Any**, **Host** and **IP**.
Destination: Select the destination information. The values are **Any**, **Host** and **IP**.
DSCP (0-63): Enter the DSCP value. And the range is between 0 and 63.
Flow Label (0-1048575): Enter the flow label value. This value must be between 0 and 1048575.
Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting the **None** as the **Protocol Type,** click the **IPv6 Address**, **IPv6 DSCP** and **Flow Label** tabs to display the following page:

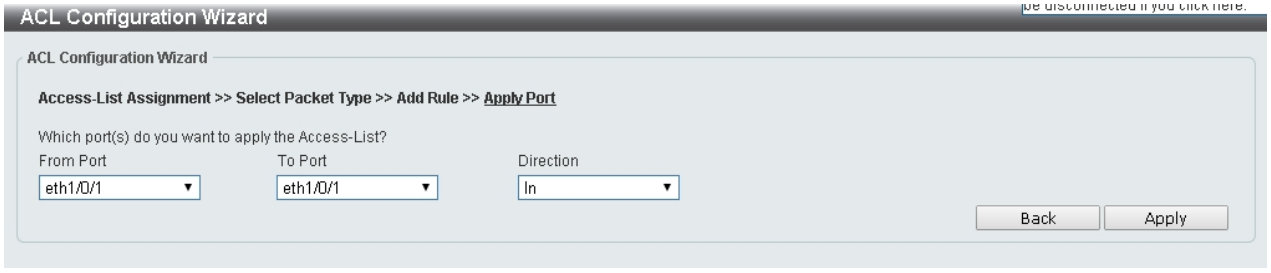


ACL > ACL Configuration Wizard – Create IPv6 ACL-None

Source: Select the source information. The values are **Any**, **Host** and **IP**.
Destination: Select the destination information. The values are **Any**, **Host** and **IP**.
DSCP (0-63): Enter the DSCP value. And the range is between 0 and 63.
Flow Label (0-1048575): Enter the flow label value. This value must be between 0 and 1048575.
Time Range: Enter the time range.
Action: Select the action for the rule. The values are **Permit** and **Deny**.

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

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



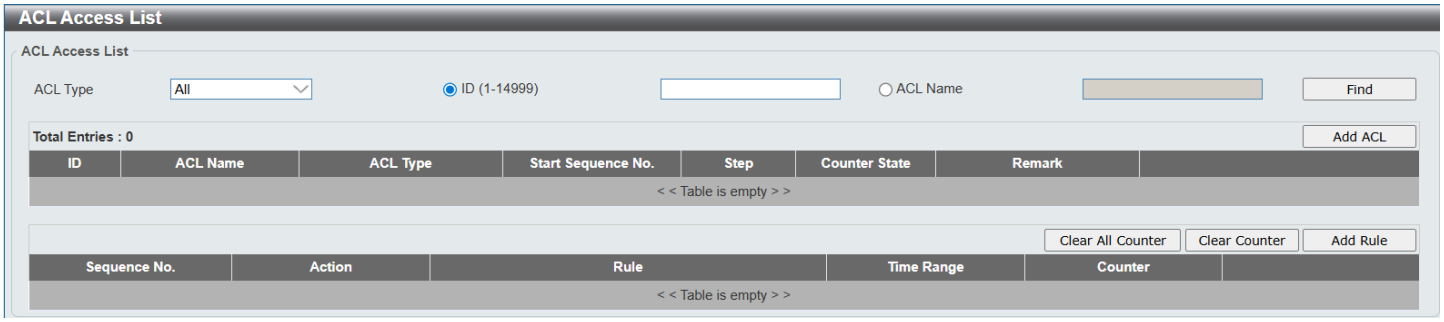
ACL > ACL Configuration Wizard – Create IPv6 ACL-Next

From Port / To Port: Select the range of ports to be configured.
Direction: Select either **In** or **Out**.

Click the **Back** button to return to the previous window.
Click the **Apply** button to save your settings.

ACL > ACL Access List

The ACL Access List page allows you to view and configure the access list settings.



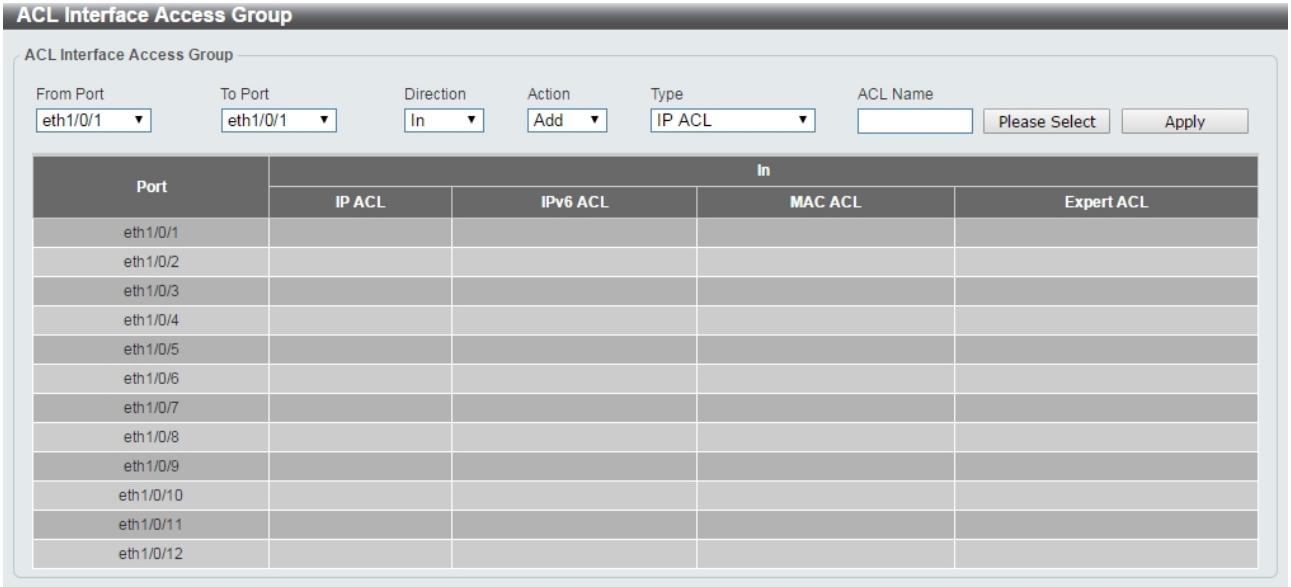
ACL > ACL Access List

ACL Type: Select the ACL profile type to find. Options to choose from are **All**, **IP ACL**, **IPv6 ACL**, **MAC ACL**, and **Expert ACL**.
ID (1-14999): Select and enter ACL ID. The range is between 1 and 14999.
ACL Name: Select and enter ACL name. The 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 profile.
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 profile selected.

ACL > ACL Interface Access Group

The ACL Interface Access Group page allows you to view and configure the interface access group settings.

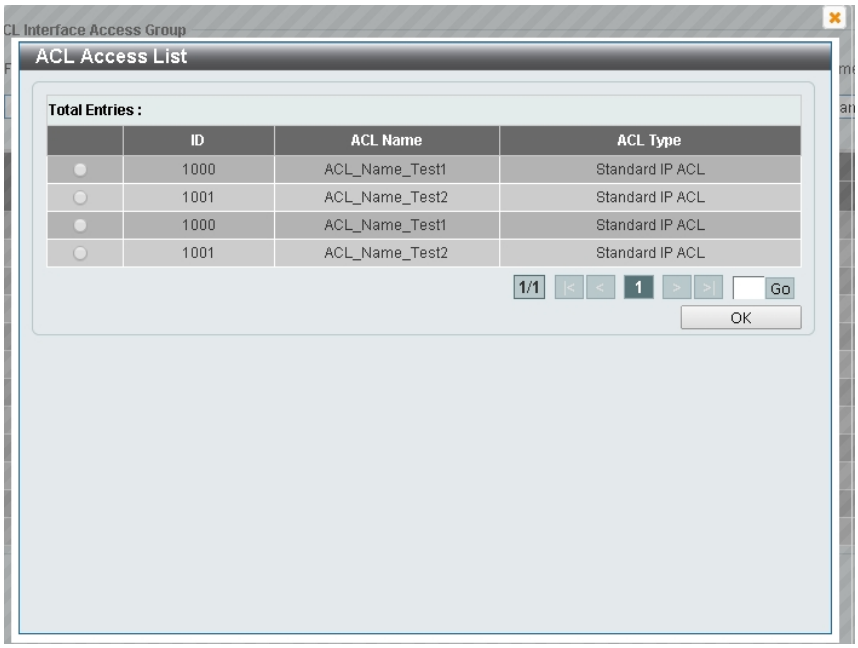


ACL > ACL Interface Access Group

From Port / To Port: Select the range of ports to be configured.
Direction: Select the direction.
Action: Select the action to be **Add** or **Delete**.
ACL Type: Select the ACL profile type to find. Options to choose from are **All**, **IP ACL**, **IPv6 ACL**, **MAC ACL**, and **Expert ACL**.
ACL Name: Enter ACL name. The name can be up to 32 characters long.

Click the **Apply** button to save your settings.

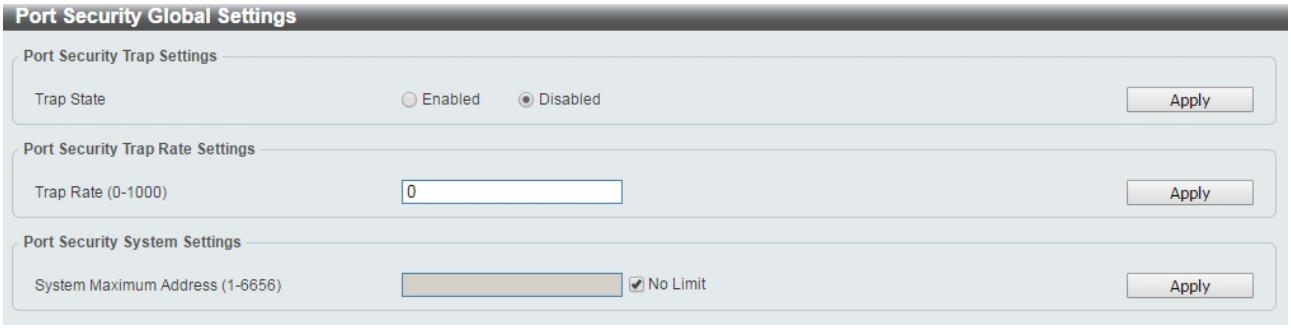
After clicking the **Please Select** button, the following page will appear.



ACL > ACL Interface Access Group - Select

Security > Port Security > Port Security Global Settings

The Port Security Global Settings page allows you to view and configure the global port security settings. Port Security is a feature that prevents unauthorized computers (with source MAC addresses) unknown to the Switch from connection and gaining access to the network.



Security > Port Security > Port Security Global Settings

Trap Security Trap Settings:

Trap State: Select to enable or disable the port security trap of the Switch.

Click the **Apply** button to save your settings.

Port Security Trap Rate Settings:

Trap Rate (0-1000): Enter the number of traps per second. The range is from 0 to 1000.

Click the **Apply** button to save your settings.

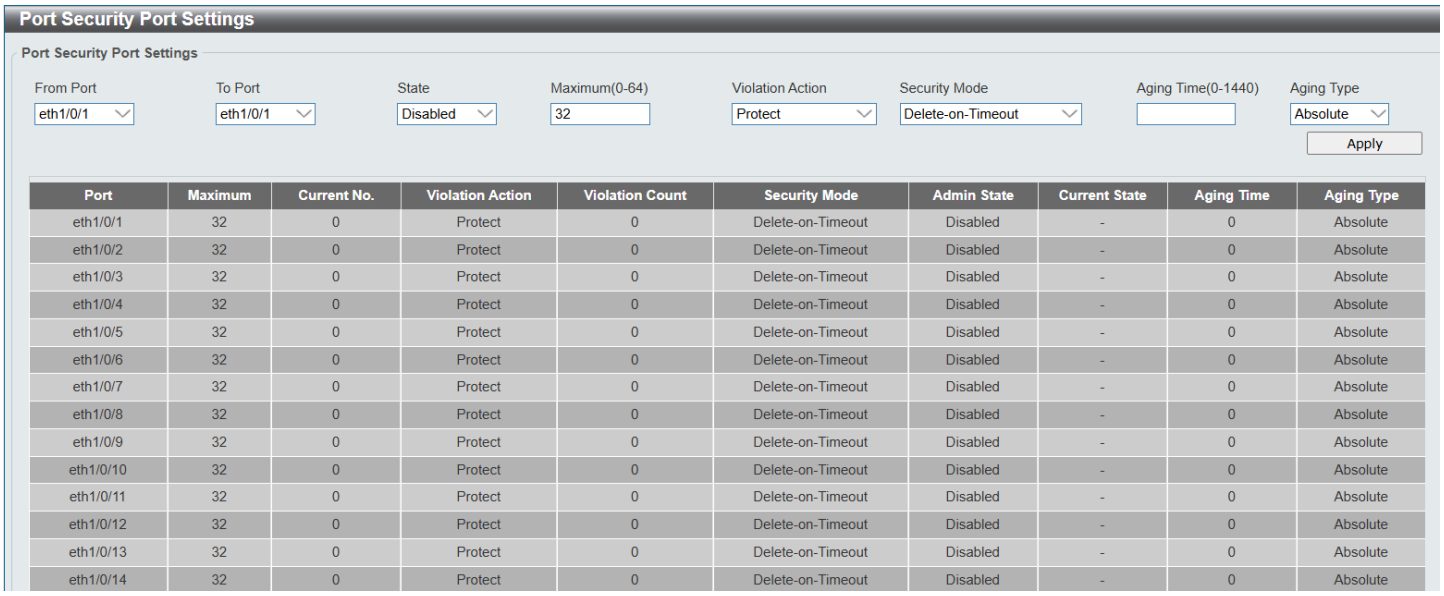
Port Security System Settings:

System Maximum Address (1-6656): Enter the maximum number of secure MAC addresses allowed. If not specified, the default value is **No Limit**. The valid range is from 1 to 6656. Tick the **No Limit** checkbox to allow the maximum number of secure MAC addresses.

Click the **Apply** button to save your settings.

Security > Port Security > Port Security Port Settings

The Port Security Port Settings page allows you to view and configure the port security port settings of the Switch.



Security > Port Security > Port Security Port Settings

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

State: Select to enable or disable the port security state of specified ports.

Maximum (0-6556): Enter the maximum number of secure MAC addresses that will be allowed on the specified ports. The value is between 0 and 6656.

Violation Action: Select the violation action that will be taken. The values are **Protect**, **Restrict**, and **Security Mode:** Select the security mode option. The values are **Permanent** and **Delete-on-Timeout**. If you select **Permanent,** the MAC addresses that have been learned by the Switch will not be purged unless you manually delete them. If you select **Delete-on-Timeout**, all learned MAC addresses will be purged when an entry is aged out or when you manually delete them.

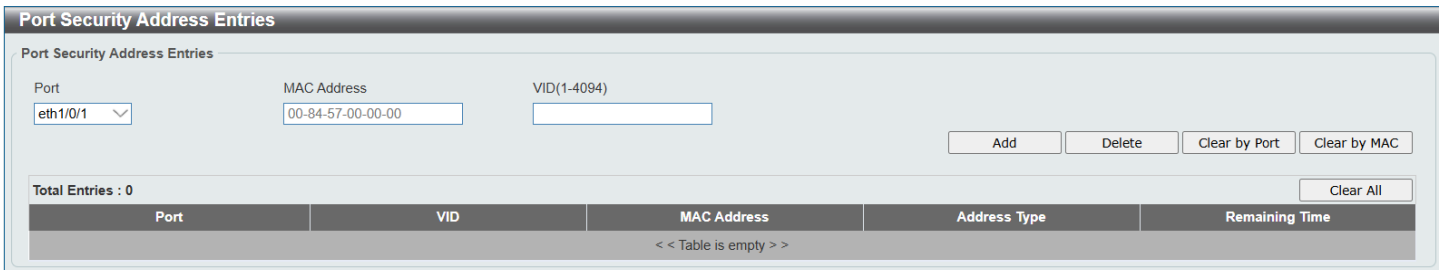
Aging Time (0-1440): Enter the aging time for auto-learned dynamic addresses on the specified ports.

Aging Type: Select the aging type. The values are **Absolute** and **Inactivity**. Select **Absolute** so that all the dynamic addresses on this port age out exactly after the time specified and are removed from the secure address list. This is the default option. Select **Inactivity** so that the dynamic addresses on this port age out only if there is no traffic from the addresses for the specified time period.

Click the **Apply** button to save your settings.

Security > Port Security > Port Security Address Entries

The Port Security Address Entries page allows you to view, clear and configure the port security address entries.



Security > Port Security > Port Security Address Entries

Port: Select the port to be configured.

MAC Address: Enter the MAC address for the specified port.

VID (1-4094): Enter the VLAN ID. The range is between 1 and 4094.

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

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

Click the **Clear by Port** button to clear the information based on the port selected.

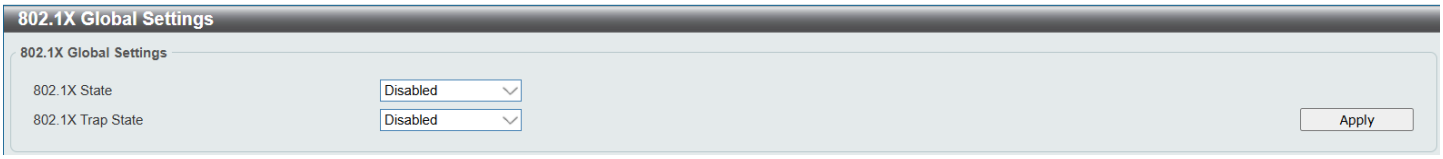
Click the **Clear by MAC** button to clear the information based on the MAC address entered.

Click the **Clear All** button to clear all the information in this table.

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

Security > 802.1X > 802.1X Global Settings

The 802.1X Global Settings page allows you to configure the 802.1X feature.



Security > 802.1X > 802.1X Global Settings

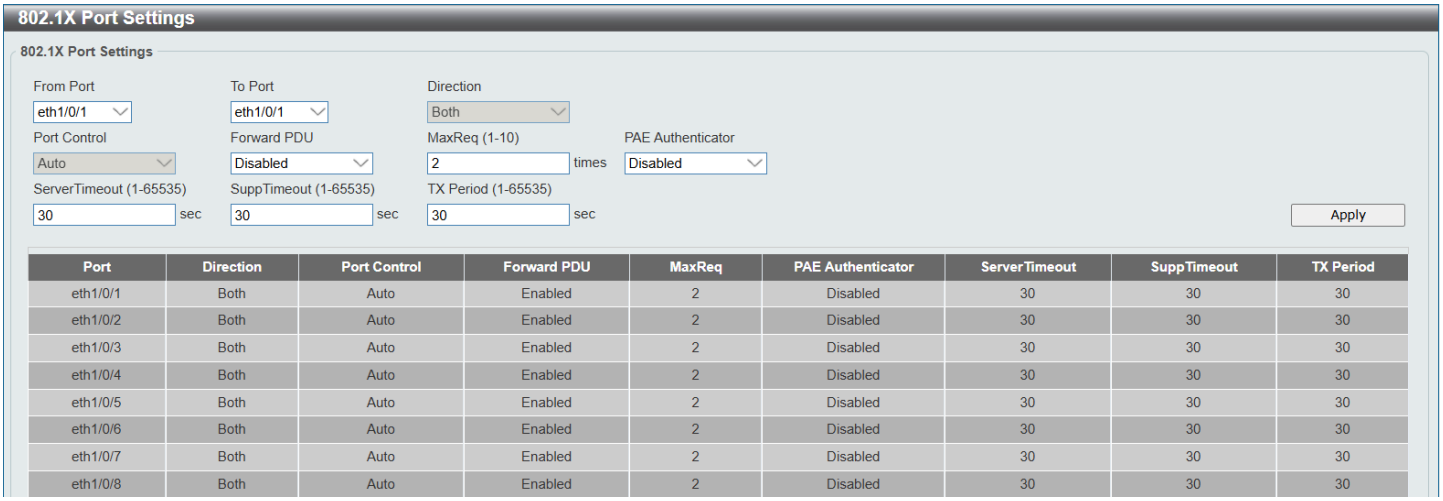
802.1X State: Specify to enable or disable the 802.1X state.

802.1X Trap State: Specify to enable or disable the 802.1X trap state.

Click the **Apply** button to save your settings.

Security > 802.1X > 802.1X Port Settings

The 802.1X Port Settings page allow you to configure the port settings.



Security > 802.1X > 802.1X Port Settings

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

Direction: Sets the administratively-controlled direction on the port. The possible field values are:

Both: Specify the control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field.

In: Disables the support in the present firmware release.

Port Control: This allows user to control the port authorization state.

Select **ForceAuthorized** to disable 802.1X and cause the port to transition to the authorized state without any authentication exchange required. This means the port transmits and receives normal traffic without 802.1X-based authentication of the client.
If **ForceUnauthorized** is selected, the port will remain in the unauthorized state, ignoring all attempts by the client to authenticate. The Switch cannot provide authentication services to the client through the interface.
If **Auto** is selected, it will enable 802.1X and cause the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state, transitions from down to up, or when an EAPOL-start frame is received. The Switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server. The default setting is **Auto**.

Forward PDU: Select to enable or disable the forward PDU option here.

MaxReq(1-10): This parameter specifies the maximum number of times that the switch retransmits an EAP request (md5-challenge) to the client before it times out the authentication session. Default is 2 times.

PAE Authenticator: Select to enable or disable the Port Access Entity (PAE) authenticator option here. This option configures a specific port as an IEEE 802.1X PAE authenticator.

ServerTimeout(1-65535): Specify the number of seconds that the Switch will wait for the request from the authentication server before timing out the server. On timeout,authenticator will send EAP-Request packet to client. The range is 1to 65535. The default is 30 seconds.

SuppTimeout(1-65535): Specify the number of seconds that the Switch will wait for the response from the supplicant before timing out the supplicant messages other than EAP requestID. The range is 1 to 65535. The default is 30 seconds..

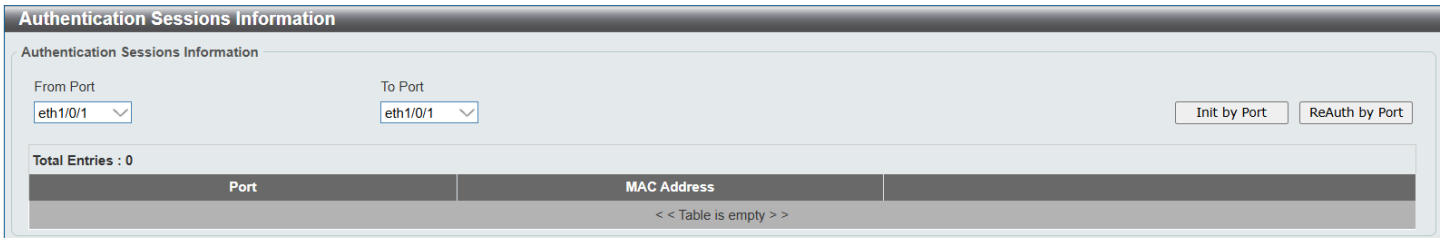
TX Peiord(1-65535): This sets the TxPeriod of time for the authenticator PAE state machine. This value determines the period of an EAP Request/Identity packet transmitted to the client. The default is 30 seconds.

Click the **Apply** button to save your settings.

NOTE: For 802.1X authentication, Dynamic VLAN is only supported in "Multi-Host" mode (port based).

Security > 802.1X > Authentication Sessions Information

The Authentication Sessions Information page is used to view and configure the authentication session information.



Security > 802.1X > Authentication Sessions Information

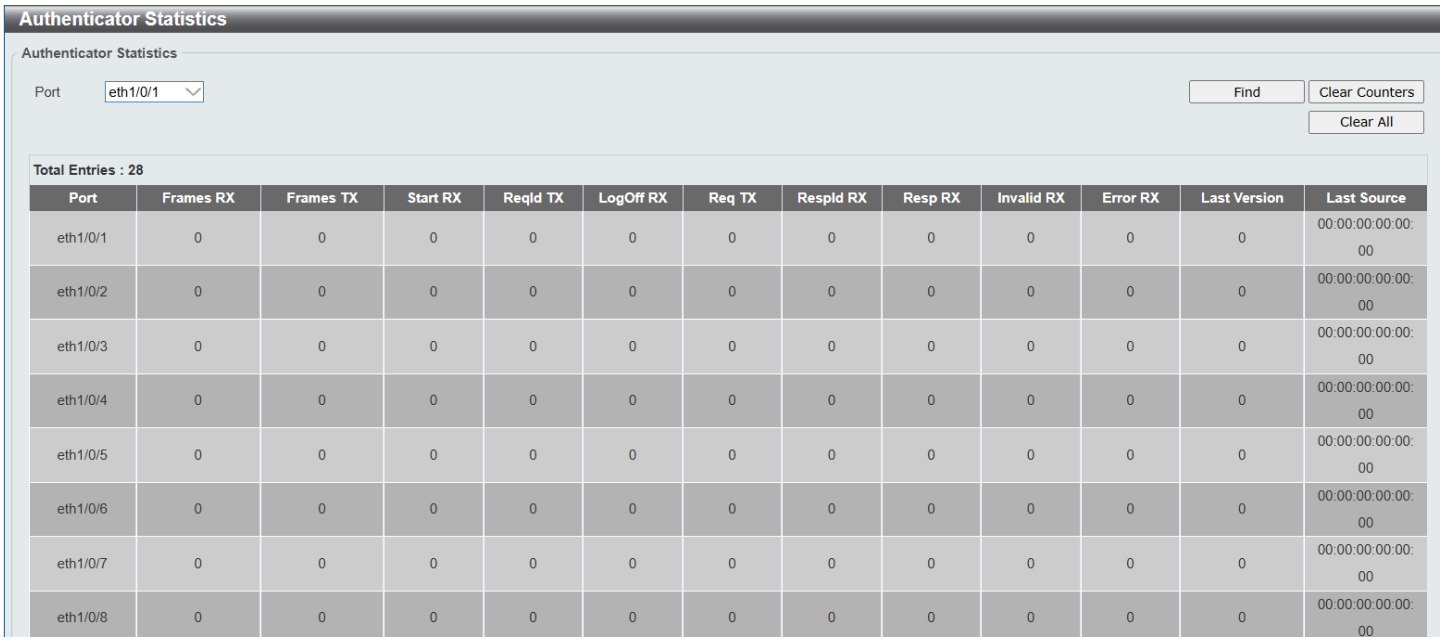
From Port / To Port: Select the port to be queried.

Click the **Init by Port** button to initiate the session information based on the selections made.

Click the **ReAuth by Port** button to re-authenticate the session information based on the selections made.

Security > 802.1X > Authenticator Statistics

The Authenticator Statistics page is used to view and clear the authenticator statistics.



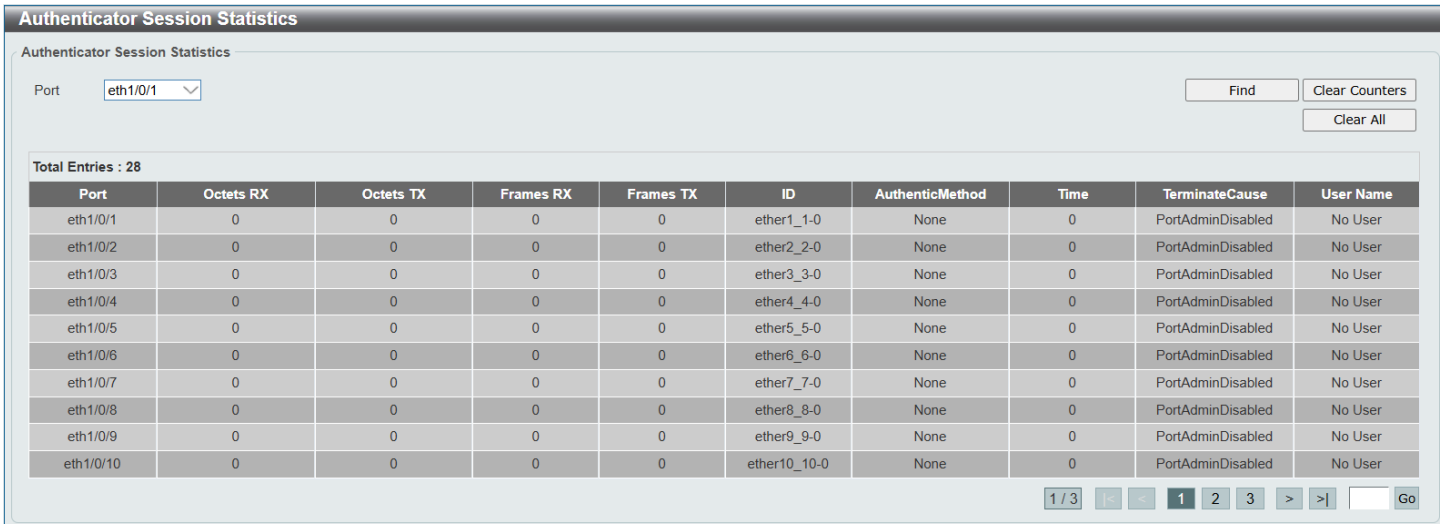
Security > 802.1X > Authenticator Statistics

Port: Select the port to be queried.

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.

Security > 802.1X > Authenticator Session Statistics

The Authenticator Session Statistics is used to view and clear the authenticator session statistics.

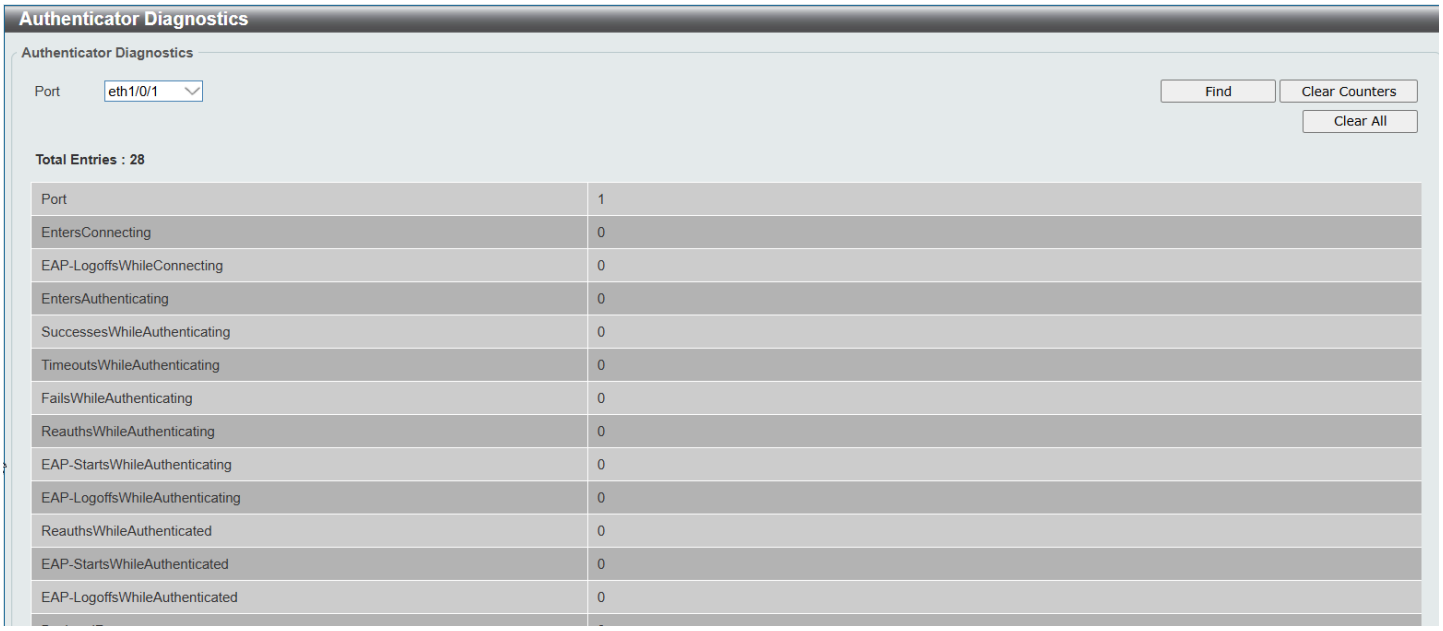


Security > 802.1X > Authenticator Sessions Statistics

Port: Select the port to be queried.
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.

Security > 802.1X > Authenticator Diagnostics

The authenticator Diagnostics is used to view and clear the authenticator diagnostics information.



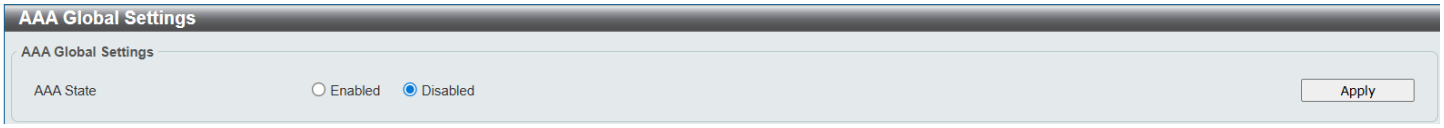
Security > 802.1X > Authenticator Diagnostics

Port: Select the port to be queried.

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.

Security > AAA > AAA Global Settings

The AAA Global Settings is used to enable or disable the global Authentication, Authorization, and Accounting (AAA) state.



Security > AAA > AAA Global Settings

The fields that can be configured are described below:

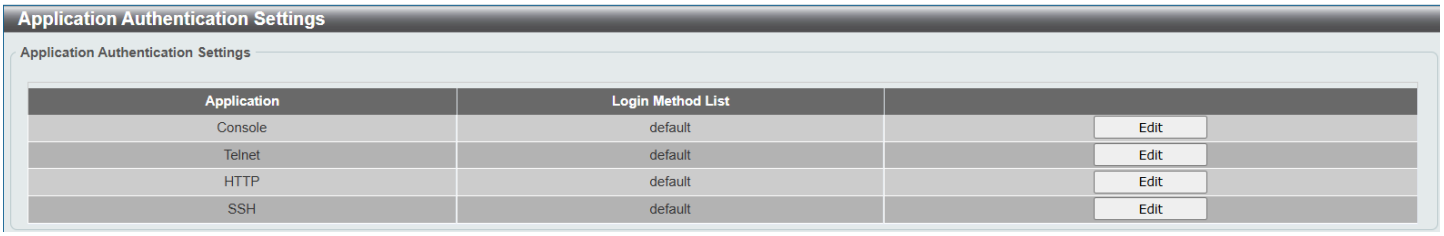
Parameter	Description
AAA State	Select to enable or disable the global Authentication, Authorization, and Accounting (AAA) state. By default, this is disabled.

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

Security > AAA > Application Authentication Settings

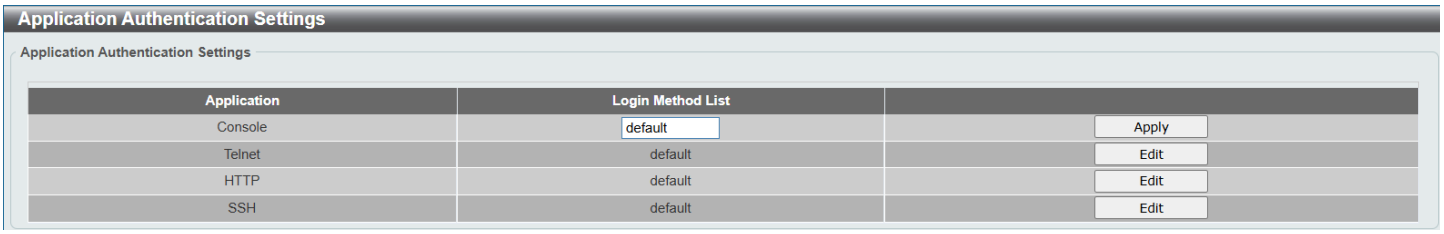
This window is used to display and configure the application authentication settings.

To view the following window, click **Security > AAA > Application Authentication Settings**, as shown below:



Security > AAA > AAA Authentication Settings

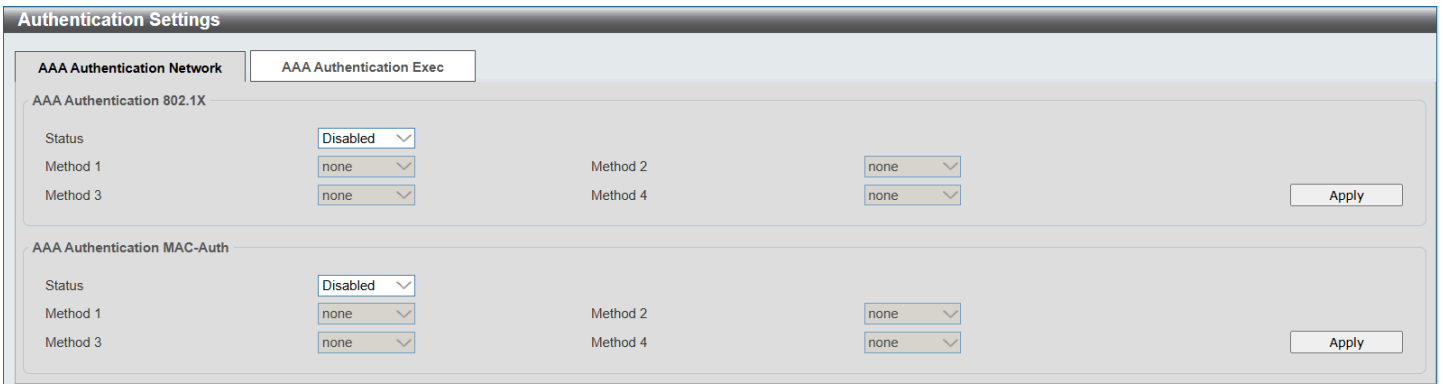
Application: Lists the configuration applications on the Switch. The user may configure the Login Method List for Console, Telnet application, SSH and the WEB (HTTP) application. Click **Edit** to specify the Login Method name.



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

Security > AAA > Authentication Settings

The Authentication Settings is used to view and configure the application authentication settings.



Authentication Settings (AAA Authentication Network) 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.

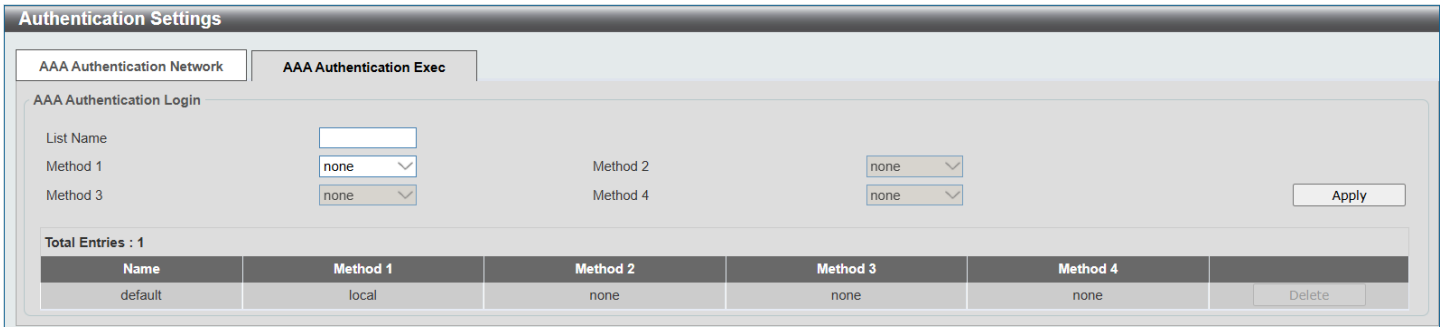
Click the **Apply** button to accept the changes made.

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.

After clicking the **AAA Authentication Exec** tab, the following page will appear.



Authentication Settings (AAA Authentication EXEC) Window

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

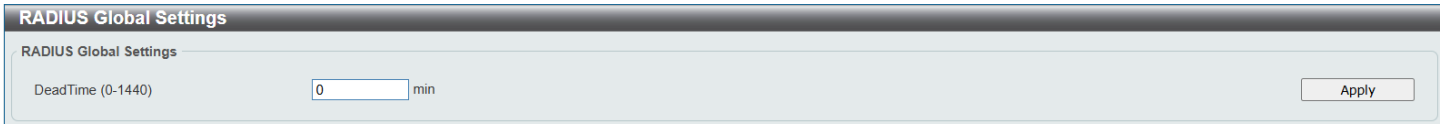
Parameter	Description
List Name	Enter the method list name that will be used with the AAA authentication login option here.
Method 1 ~ Method 4	Select the method lists that will be used for this configuration here. Options to choose from are:

Parameter	Description
	• **none** - Normally, the method is listed as the last method. The user will pass authentication if it is not denied by previous method's authentication. • **local** - Specifies to use the local database for authentication. • **group** - Specifies to use the server groups defined by the AAA group server command. Enter the AAA group server name in the space provided. This string can be up to 32 characters long. • **radius** - Specifies to use the servers defined by the RADIUS server host command. • **tacacs+** - Specifies to use the servers defined by the TACACS+ server host command.

Click the **Apply** button to accept the changes made. Click the **Delete** button to remove the specified entry.

Security > RADIUS > RADIUS Global Settings

The RADIUS Global Settings page allows you to view and configure the RADIUS global settings.



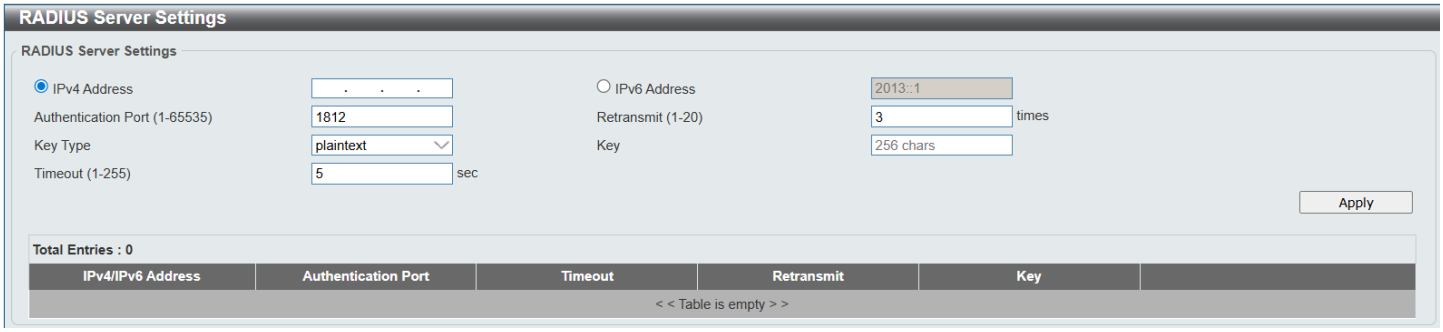
Security > RADIUS > RADIUS Global Settings

Dead Time: Enter the dead time value here. This value must be between 0 and 1440 minutes. By default, this value is 0 minutes. When this option is 0, the unresponsive server will not be marked as dead. This setting can be used to improve the authentication processing time by setting the dead time to skip the unresponsive server host entries. When the system performs authentication with the authentication server, it attempts one server at a time. If the attempted server does not respond, the system will attempt the next server. When the system finds a server does not respond, it will mark the server as down, start a dead time timer, and skip them in authentication of the following requests until expiration of the dead time.

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

Security > RADIUS > RADIUS Server Settings

The RADIUS feature of the Switch allows the user to facilitate centralized user administration and provide protection against hacking attacks.



Security > RADIUS > RADIUS Server Settings

Click the **IPv4 Address** or **IPv6 Address** and enter the IP address to be configured.

Authentication Port (1-65535): Enter the authentication port number used here. This value must be between 0 and 65535. By default, this value is 1812. If no authentication is used, use the value 0.

Retransmit (1-20): Enter the accounting value used here. This value must be between 0 and 20. By default, the value is 3. To disable this option, enter the value 0.

Key Type: Select the key type that will be used. Options to choose from are **Plain Text** and **Encrypted**.

Key: Enter the key used to communicate with the RADIUS server. This key can be up to 32 characters long.

Timeout (1-255): Enter the timeout value. This value must be between 1 and 255 seconds. By default, this value is 5 seconds.

Click the **Apply** button to save your settings.

Security > RADIUS > RADIUS Group Server Settings

The RADIUS Group Server Settings page is used to view and configure the RADIUS group server setting.



Security > RADIUS > RADIUS Group Server Settings

Group Server name: Enter the RADIUS group server's name. This name can be up to 15 characters long.

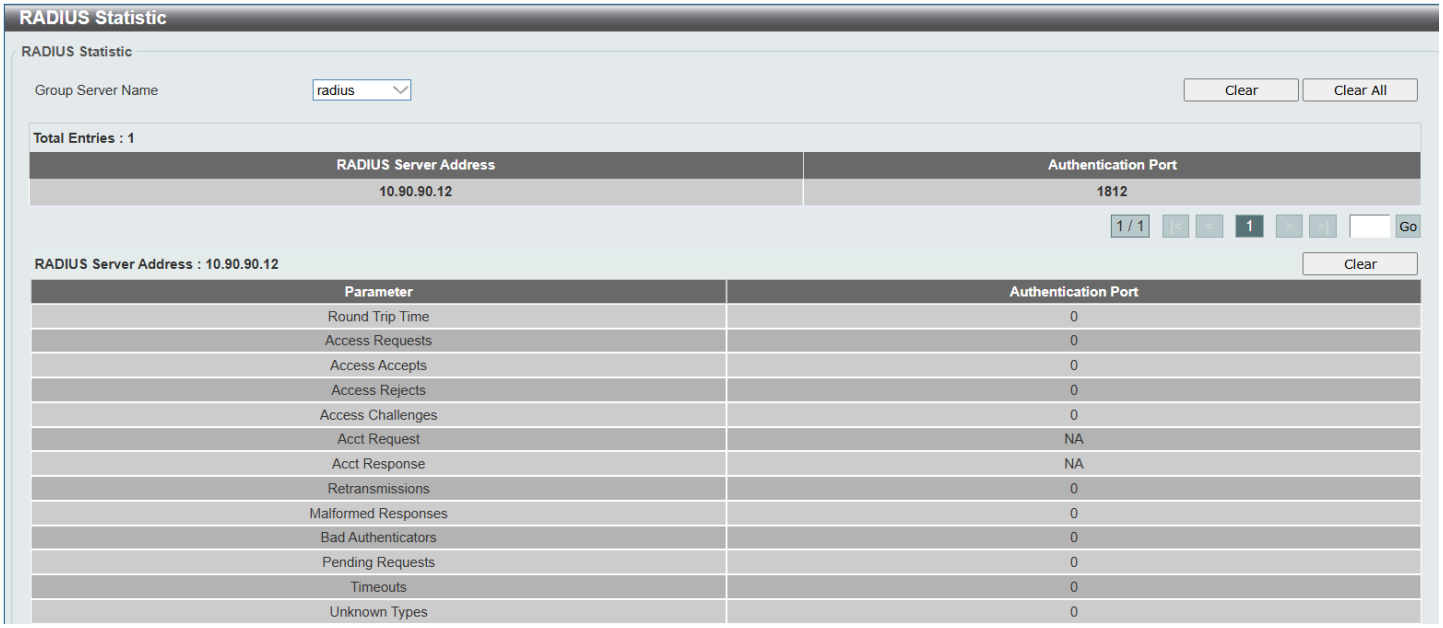
IP Address: Enter the group server's IPv4 address.

IPv6 Address: Enter the group server's IPv6 address.

Click the **Apply** button to save your settings.

Security > RADIUS > RADIUS Statistic

The RADIUS Statistic page is used to view and clear the RADIUS statistics information.



Security > RADIUS > RADIUS Statistic

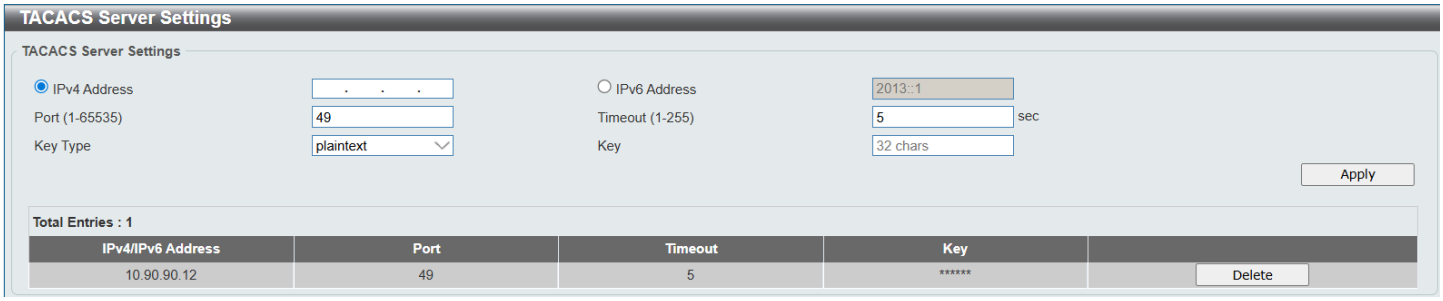
Group Server Name: Select the RADIUS group server name from this list here.

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.

Security > TACACS > TACACS Server Settings

The TACAS feature of the Switch allows the user to facilitate centralized user administration and provide protection against hacking attacks.



Security > TACACS > TACACS Server Settings

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the TACACS+ server IPv4 address here.
IPv6 Address	Enter the TACACS+ server IPv6 address here.
Port	Enter the port number used here. This value must be between 1 and 65535. By default, this value is 49.
Timeout	Enter the timeout value here. This value must be between 1 and 255 seconds. By default, this value is 5 seconds.
Key Type	Select the key type that will be used here. Options to choose from are **Plain Text** and **Encrypted**.
Key	Enter the key, used to communicate with the TACACS+ server, here. This key can be up to 254 characters long.

Click the **Apply** button to save your settings.

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

Security > TACACS > TACACS Group Server Settings

The TACACS Group Server Settings page is used to view and configure the TACACS group server setting.



Security > TACACS > TACACS Group Server Settings

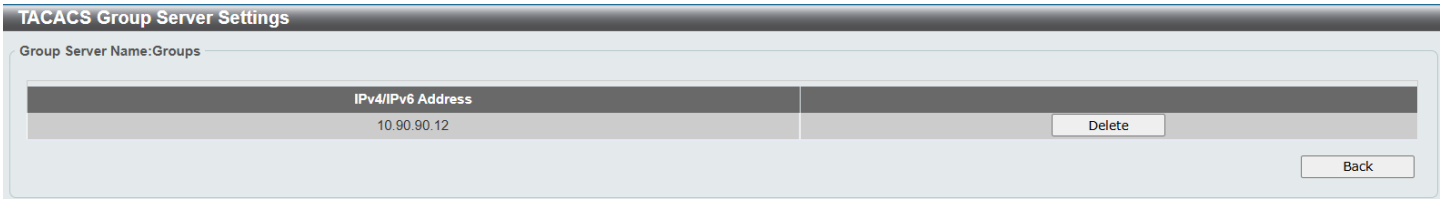
The fields that can be configured are described below:

Parameter	Description
Group Server Name	Enter the TACACS+ group server name here. This name can be up to 32 characters long.
IPv4 Address	Enter the IPv4 address of the TACACS+ group server here.
IPv6 Address	Enter the IPv6 address of the TACACS+ group server here.

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

Click the **Show Detail** button to view and configure more detailed settings for the TACACS+ group server. Click the **Delete** button to remove the specified entry.

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

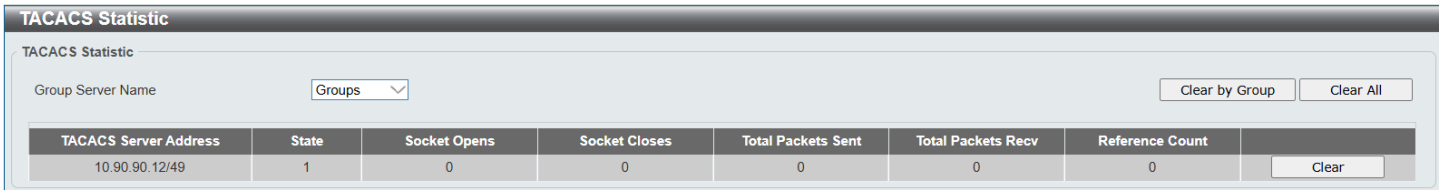


TACACS+ Group Server Settings (Show Detail) Window

Click the **Delete** button to remove the specified entry.
Click the **Back** button to return to the previous window.

Security > TACACS > TACACS Statistic

The TACACS Statistic page is used to view and clear the TACACS statistics information.



Security > TACACS > TACACS Statistic

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

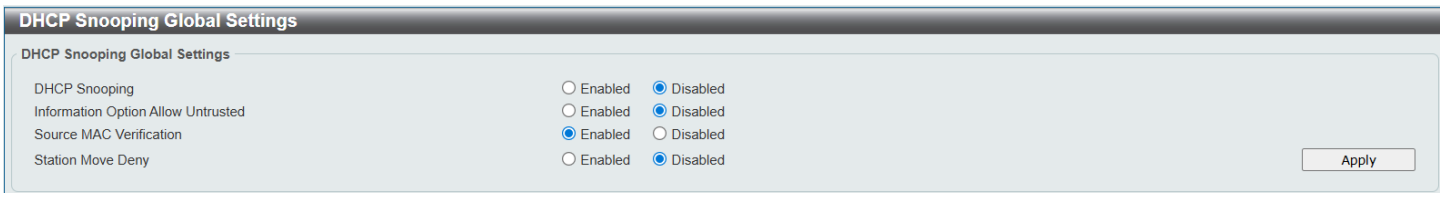
the **Clear All** button to clear all the information in this table.

Click the second **Clear** button to clear all the information for the specific entry.

Security > IMPB > DHCPv4 Snooping > DHCP Snooping Global Settings

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.

To view the following window, click **Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Global Settings**, as shown below:



Security > IMPB > DHCPv4 Snooping > DHCP Snooping Global Settings

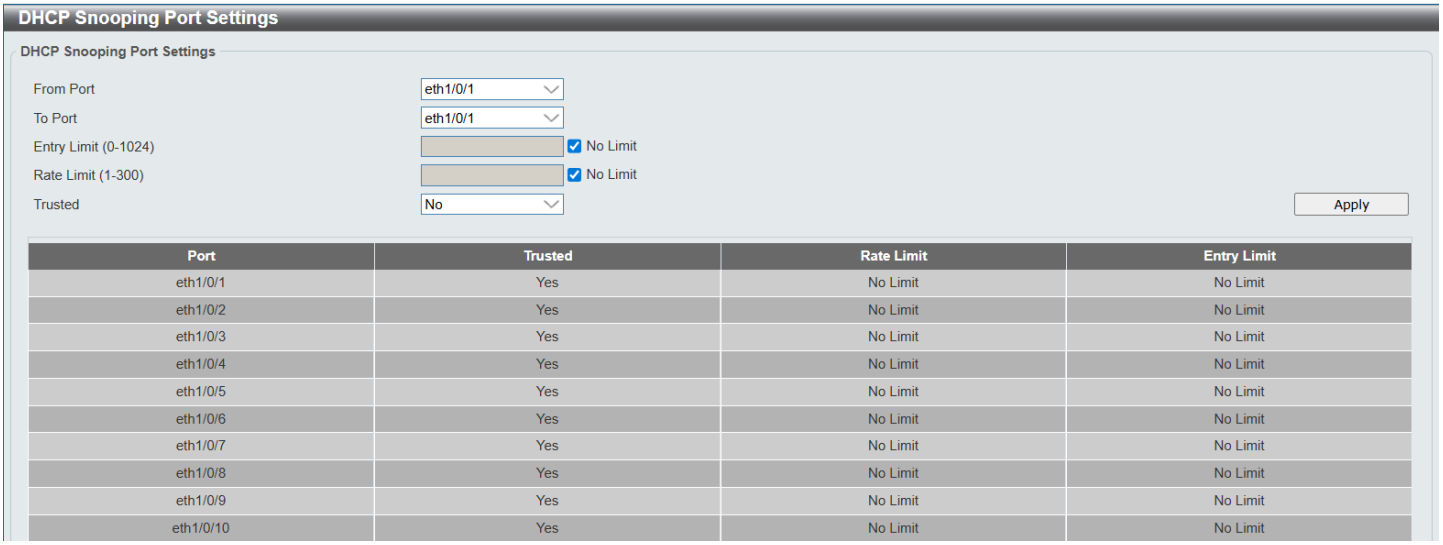
The fields that can be configured are described below:

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.

Security > IMPB > DHCPv4 Snooping > DHCP Snooping Port Settings

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



Security > IMPB > DHCPv4 Snooping > DHCP Snooping Port Settings

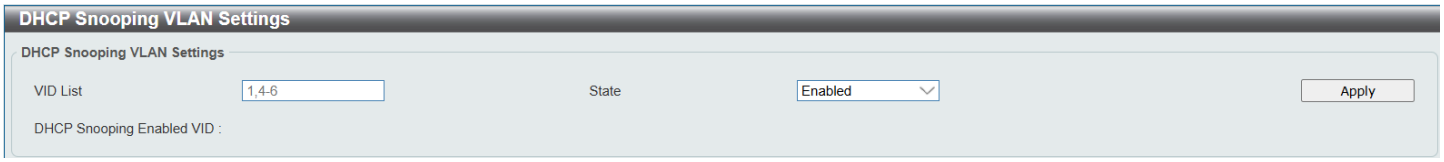
The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Entry Limit	Enter the entry limit value here. This value must be between 0 and 1024. Tick the **No Limit** option to disable the function.
Rate Limit	Enter the rate limit value here. This value must be between 1 and 300. Tick the **No Limit** option to disable the function.
Trusted	Select the trusted option here. Options to choose from are **No** and **Yes**. Ports connected to the DHCP server or to other Switches should be configured as 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.

Security > IMPB > DHCPv4 Snooping > DHCP Snooping VLAN Settings

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



Security > IMPB > DHCPv4 Snooping > DHCP Snooping VLAN Settings

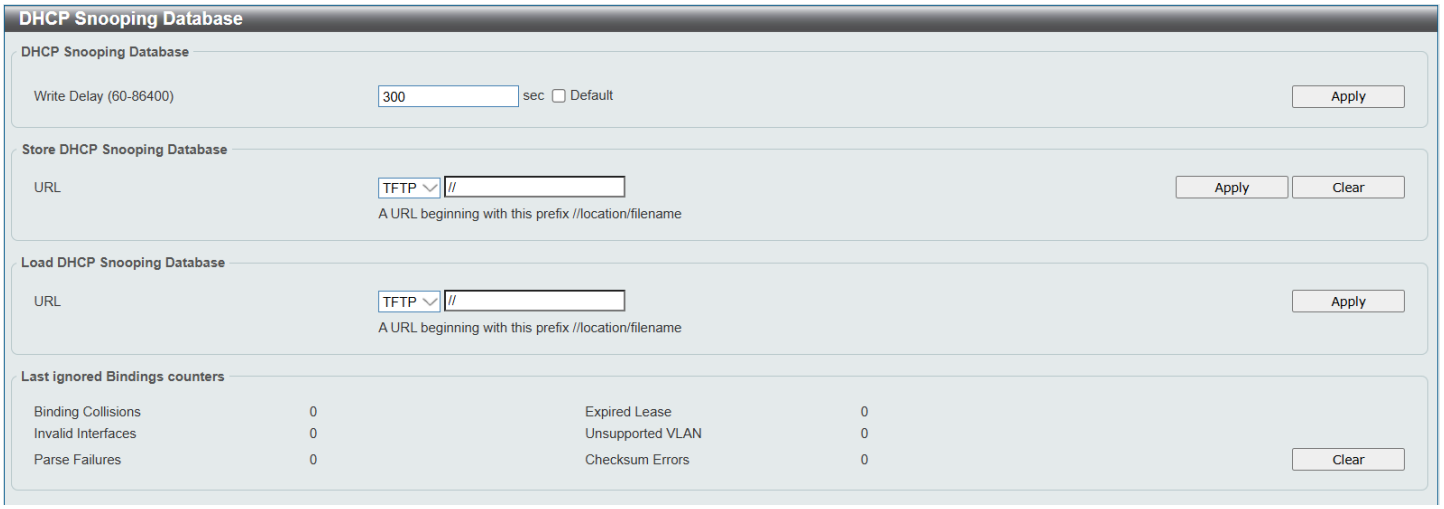
The fields that can be configured are described below:

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.

Security > IMPB > DHCPv4 Snooping > DHCP Snooping Database

This window is used to display and configure the DHCP snooping database settings.



Security > IMPB > DHCPv4 Snooping > DHCP Snooping Database

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

Parameter	Description
Write Delay	Enter the write delay time value here. This value must be between 60 and 86400 seconds. By default, this value is 300 seconds.

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

The fields that can be configured in **Store DHCP Snooping Database** are described below:

Parameter	Description
URL	Specifies to store the DHCP snooping database on a **TFTP** server. Enter the URL in the space provided.

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

The fields that can be configured in **Load DHCP Snooping Database** are described below:

Parameter	Description
URL	Specifies to load the DHCP snooping database from a **TFTP** server. Enter the URL in the space provided.

Click the **Apply** button to accept the changes made. Click the **Clear** button to clear all the counter information.

Security > IMPB > DHCPv4 Snooping > DHCP Snooping Binding Entry

This window is used to display and configure the DHCP snooping binding entries.



Security > IMPB > DHCPv4 Snooping > DHCP Snooping Binding Entry

MAC Address: Enter the MAC address of the DHCP snooping binding entry here.
VID: Enter the VLAN ID of the DHCP snooping binding entry here. This value must be between 1 and 4094.
IP Address: Enter the IP address of the DHCP snooping binding entry here.
Port: Select the appropriate port used for the configuration here.
Expiry: Enter the expiry time value used here. This value must be between 60 and 4294967295 seconds.

Security > IMPB > Dynamic ARP Inspection > ARP Access List

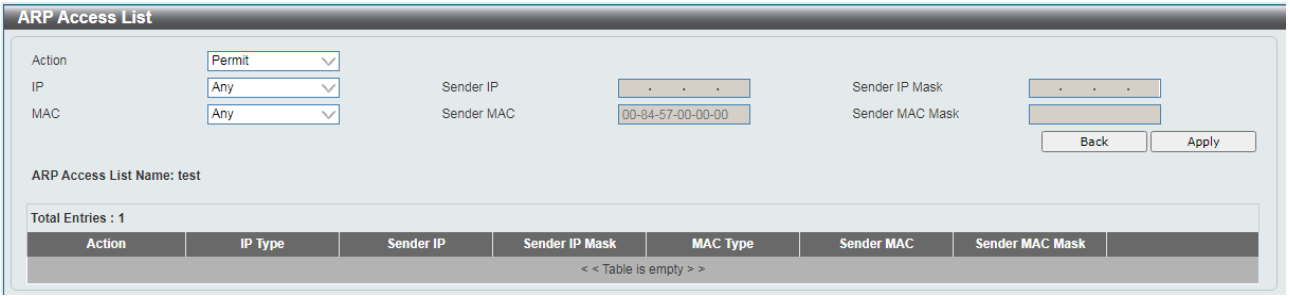
This window is used to display and configure the dynamic ARP inspection settings.



Security > IMPB > Dynamic ARP Inspection > ARP Access List

ARP Access: List Name Enter the ARP access list name used here. This name can be up to 32 characters long.

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



Action: Select the action that will be taken here. Options to choose from are Permit and Deny.
IP: Select the type of sender IP address that will be used here. Options to choose from are Any, Host, and IP with Mask.
Sender IP: After selecting the Host or IP with Mask options as the type of IP, enter the sender IP address used here.
Sender IP Mask: After selecting the IP with Mask option as the type of IP, enter the sender IP mask used here.

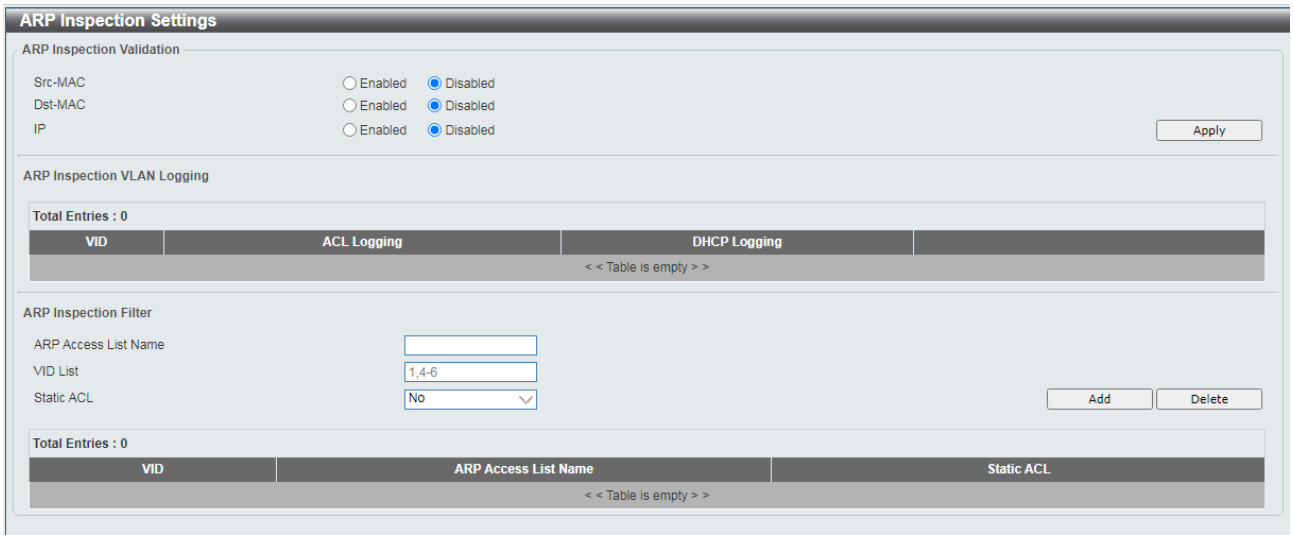
MAC: Select the type of sender MAC address that will be used here. Options to choose from are Any, Host, and MAC with Mask.

Sender MAC: After selecting the Host or MAC with Mask options as the type of MAC, enter the sender MAC address used here.

Sender MAC Mask: After selecting the MAC with Mask option as the type of MAC, enter the sender MAC mask used here.

Security > IMPB > Dynamic ARP Inspection > ARP Inspection Settings

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



Security > IMPB > Dynamic ARP Inspection > ARP Inspection Settings

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 packet.

Dst-MAC: Select to enable or disable the destination MAC option here. This option specifies to check for ARP response packets and the consistency of the destination MAC address in the Ethernet header against the target MAC address in the ARP payload.

IP: Select to enable or disable the IP option here. This option specifies to check the ARP body for invalid and unexpected IP addresses. It also specifies to check the validity of IP address in the ARP payload. The sender IP in both the ARP request and response and target IP in the ARP response are validated. Packets destined for the IP addresses 0.0.0.0, 255.255.255.255, and all IP multicast addresses are dropped. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses.

The fields that can be configured in **ARP Inspection Filter** are described:

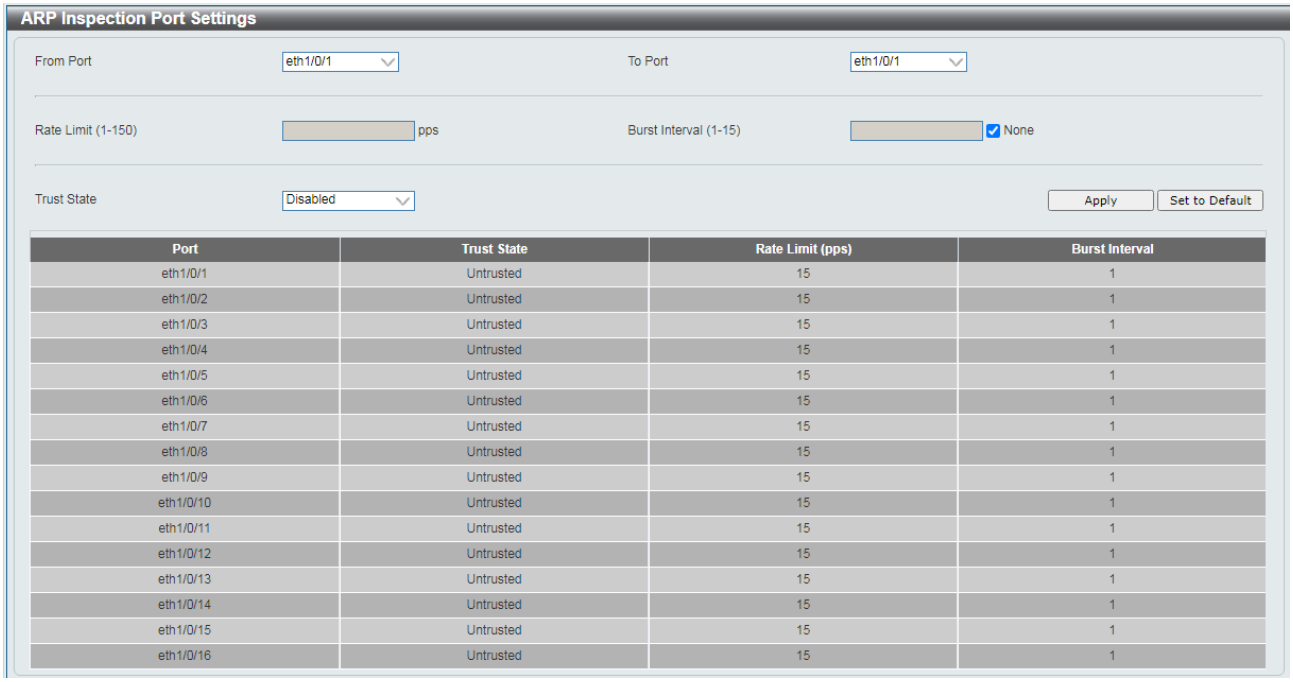
ARP: Access List Name Enter the ARP access list name used here. This name can be up to 32 characters long.

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.

Security > IMPB > Dynamic ARP Inspection > ARP Inspection Port Settings

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



Port	Trust State	Rate Limit (pps)	Burst Interval
eth1/0/1	Untrusted	15	1
eth1/0/2	Untrusted	15	1
eth1/0/3	Untrusted	15	1
eth1/0/4	Untrusted	15	1
eth1/0/5	Untrusted	15	1
eth1/0/6	Untrusted	15	1
eth1/0/7	Untrusted	15	1
eth1/0/8	Untrusted	15	1
eth1/0/9	Untrusted	15	1
eth1/0/10	Untrusted	15	1
eth1/0/11	Untrusted	15	1
eth1/0/12	Untrusted	15	1
eth1/0/13	Untrusted	15	1
eth1/0/14	Untrusted	15	1
eth1/0/15	Untrusted	15	1
eth1/0/16	Untrusted	15	1

Security > IMPB > Dynamic ARP Inspection > ARP Inspection Port Settings

From Port ~ To Port: Select the appropriate port range used for the configuration here.
Rate Limit: Enter the rate limit value here. This value must be between 1 and 150 packets per seconds.
Burst Interval: Enter the burst interval value here. This value must be between 1 and 15. Tick the None option to disable the option.
Trust State: Select to enable or disable the trust state here.

Security > IMPB > Dynamic ARP Inspection > ARP Inspection VLAN

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



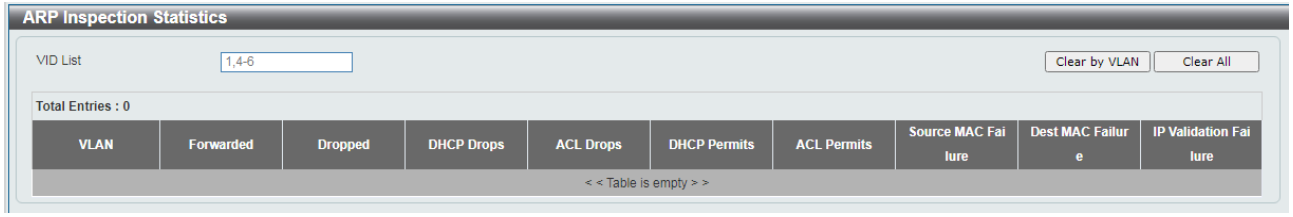
Security > IMPB > Dynamic ARP Inspection > ARP Inspection VLAN

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

Security > IMPB > Dynamic ARP Inspection > ARP Inspection Statistics

This window is used to display and clear the ARP inspection statistics information.

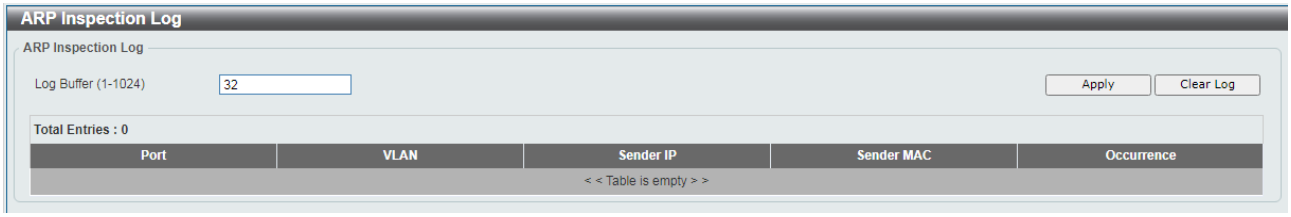


Security > IMPB > Dynamic ARP Inspection > ARP Inspection Statistics

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.

Security > IMPB > Dynamic ARP Inspection > ARP Inspection Log

This window is used to display, configure and clear the ARP inspection log information.

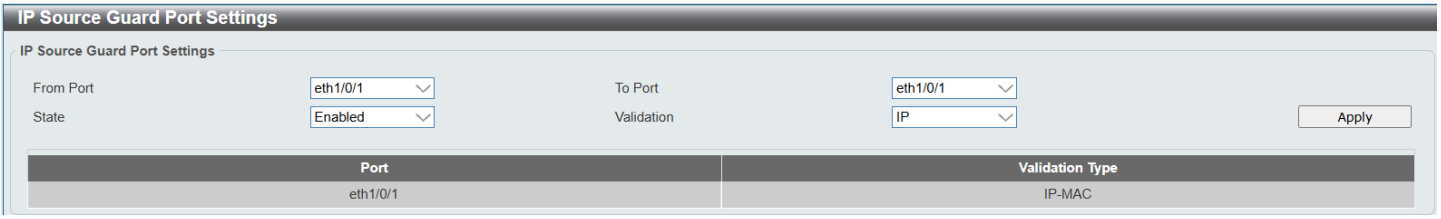


Security > IMPB > Dynamic ARP Inspection > ARP Inspection Log

Log Buffer: Enter the log's buffer value used here. This value must be between 1 and 1024. By default, this value is 32.
Click the **Clear Log** button to clear all the information in this table.

Security > IMPB > IP Source Guard > IP Source 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:



Security > IMPB > IP Source Guard > IP Source Guard Port Settings

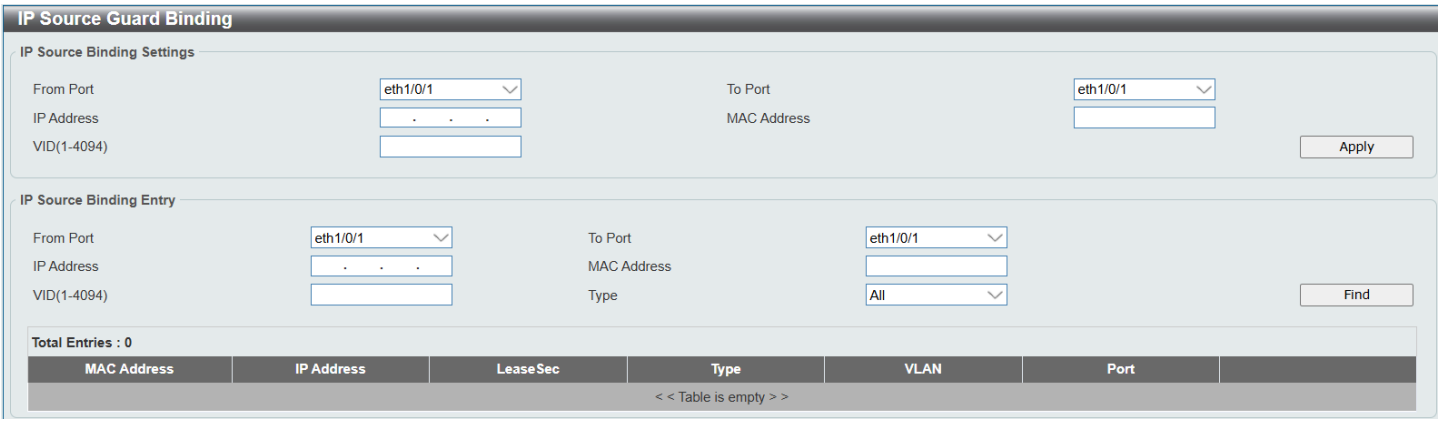
The fields that can be configured are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable the IPSG's state for the specified port(s) here.
Validation	Select the validation method used here. Options to choose from are **IP** and **IP-MAC**. Selecting **IP** means that the IP address of the received packets will be checked. Selecting **IP-MAC** means that the IP address and the MAC address of the received packets will be checked.

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

Security > IMPB > IP Source Guard > 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:



Security > IMPB > IP Source Guard > IP Source Guard Binding

The fields that can be configured in **IP Source Binding Settings** are described below:

Parameter	Description
MAC Address	Enter the MAC address of the binding entry here.
VID	Enter the VLAN ID of the binding entry here.
IP Address	Enter the IP address of the binding entry here.
From Port - To Port	Select the appropriate port range used for the configuration here.

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

The fields that can be configured in **IP Source Binding Entry** are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the query here.
IP Address	Enter the IP address of the binding entry here.
MAC Address	Enter the MAC address of the binding entry here.
VID	Enter the VLAN ID of the binding entry here.
Type	Select the type of binding entry to find here. Options to choose from are: • **All** - Specifies that all the DHCP binding entries will be displayed. • **DHCP Snooping** - Specifies to display the IP-source guard binding entry learned by DHCP binding snooping. • **Static** - Specifies to display the IP-source guard binding entry that is manually configured.

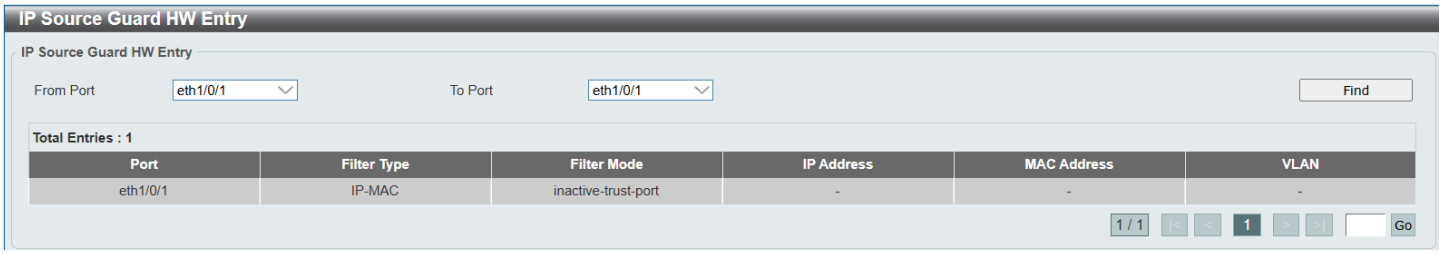
Click the **Find** button to locate a specific entry based on the information entered. Click the **Delete** button to remove the specified entry.

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

Security > IMPB > IP Source Guard > 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:



Security > IMPB > IP Source Guard > IP Source Guard HW Entry

The fields that can be configured are described below:

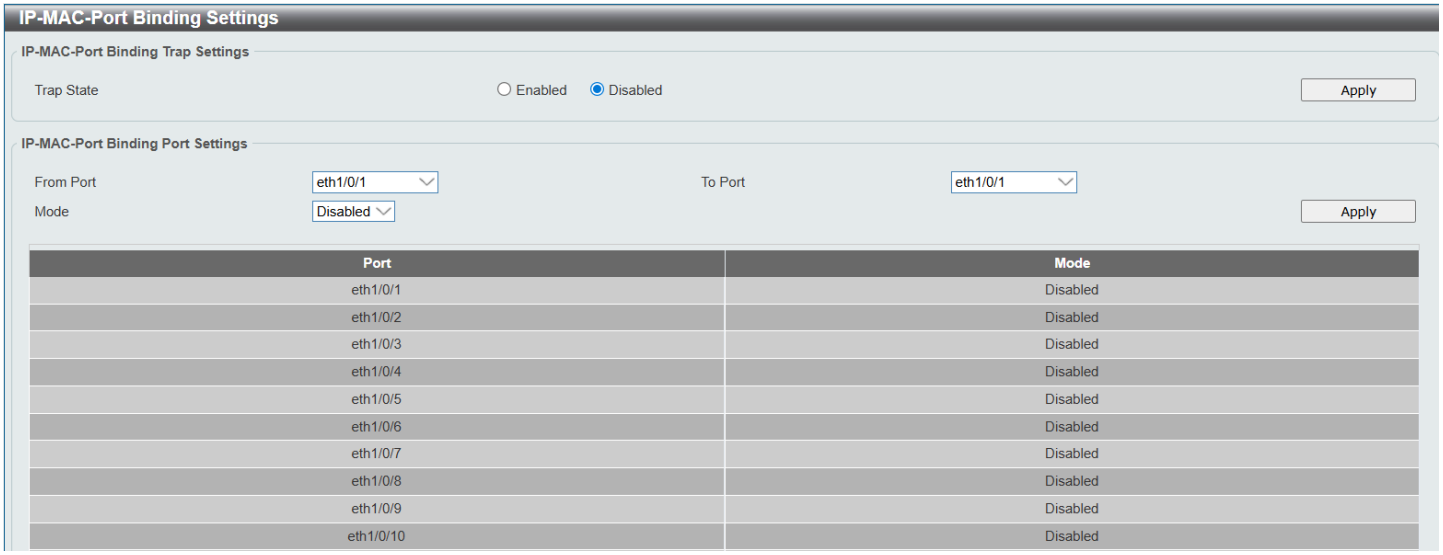
Parameter	Description
From Port - To Port	Select the appropriate port range used for the query here.

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

Security > IMPB >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:



Security > IMPB > Advanced Settings > IP-MAC-Port Binding Settings

The fields that can be configured in **IP-MAC-Port Binding Trap Settings** are described below:

Parameter	Description
Trap State	Select the enable or disable the IP-MAC-Port binding option's trap state.

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

The fields that can be configured in **IP-MAC-Port Binding Port Settings** are described below:

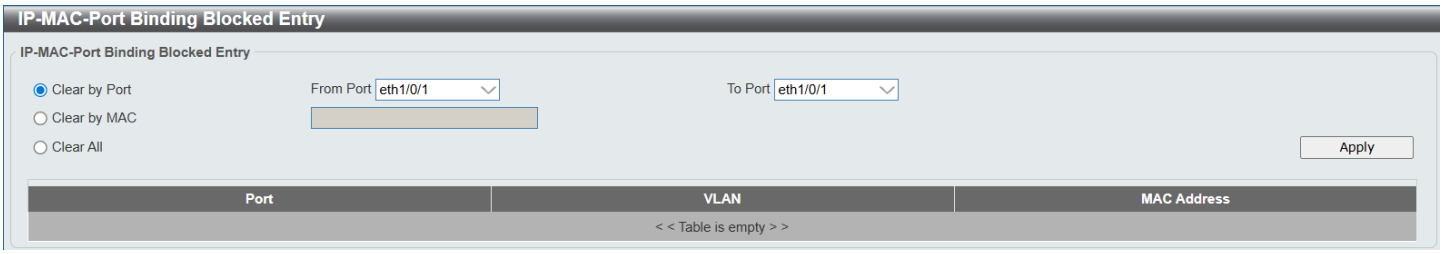
Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Mode	Select the mode of access control that will be used here. Options to choose from are **Disabled**, **Strict**, and **Loose**. When a port is enabled for IMPB strict-mode access control, a host can only access the port after the host sends ARP or IP packets and the ARP packet or IP packet sent by the host passes the binding check. To pass the binding check, the source IP address, source MAC address, VLAN ID, and arrival port number must match any of the entries defined by either the IPSG static binding entry or the DHCP snooping learned dynamic binding entry. When a port is enabled for IMPB loose-mode access control, a host will be denied to access the port after the host sends ARP or IP packets and the ARP packet or IP packet sent by the host does not pass the binding check. To pass the binding check, the source IP address, source MAC address, VLAN ID, and arrival port must match any of the entries defined by either the IPSG static binding entry or the DHCP snooping learned dynamic binding entry.

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

Security > IMPB >Advanced Settings > IP-MAC-Port 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:



Security > IMPB > Advanced Settings > IP-MAC-Port Blocked Entry

The fields that can be configured are described below:

Parameter	Description
Clear by Port	Select this option to clear the entry table based on the port(s) selected.
From Port - To Port	Select the appropriate port range that will be cleared here.
Clear by MAC	Select this option to clear the entry table based on the MAC address entered. Enter the MAC address that will be cleared in the space provided.
Clear All	Select this option to clear all entries that contain MAC addresses.

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

Security > IMPB >IPv6 > IPv6 Snooping

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

To view the following window, click **Security > IMPB > IPv6 > IPv6 Snooping**, as shown below:



IPv6 Snooping Window

The fields that can be configured in **Station Move Setting** are described below:

Parameter	Description
Station Move	Select the station move options here. Options to choose from are **Permit** and **Deny**.

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

The fields that can be configured in **IPv6 Snooping Policy Settings** are described below:

Parameter	Description
Policy Name	Enter the IPv6 snooping policy name used here. This name can be up to 32 characters long.
Limit Address Count	Enter the address count limit value used here. This value must be between 0 and 511. Tick the **No Limit** option to disable this option.

Protocol	Select the protocol state here. Options to choose from are **Enabled** and **Disabled**. • **DHCP** - Specifies that addresses should be snooped in DHCPv6 packets. • **NDP** - Specifies that addresses should be snooped in NDP packets. DHCPv6 snooping sniffs the DHCPv6 packets sent between the DHCPv6 client and server in the address assigning procedure. When a DHCPv6 client successfully got a valid IPv6 address, DHCPv6 snooping creates its binding database. ND Snooping is designed for a stateless auto-configuration assigned IPv6 address and manually configured IPv6 address. Before assigning an IPv6 address, the host must perform Duplicate Address Detection first. ND snooping detects DAD messages (DAD Neighbor Solicitation (NS) and DAD Neighbor Advertisement (NA)) to build its binding database. The NDP packet (NS and NA) is also used to detect whether a host is still reachable and determine whether to delete a binding or not.
VID List	Enter the VLAN ID list used here.

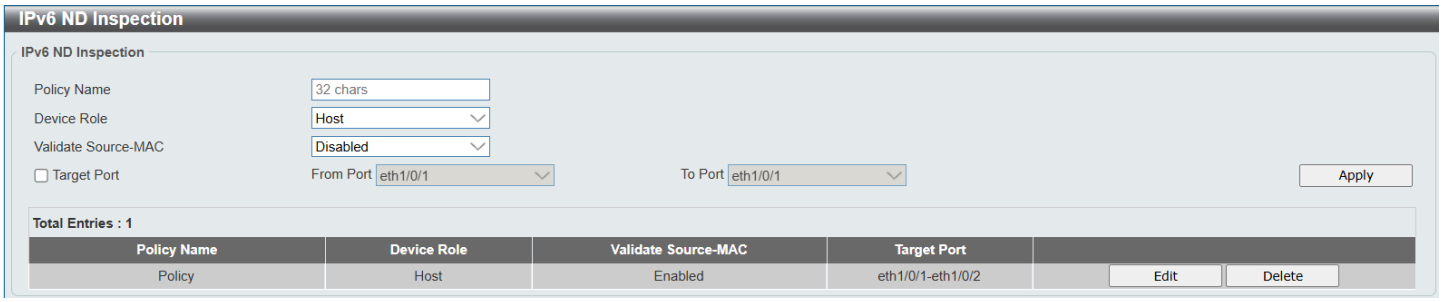
Click the **Apply** button to accept the changes made.

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

Security > IMPB >IPv6 > 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 Window

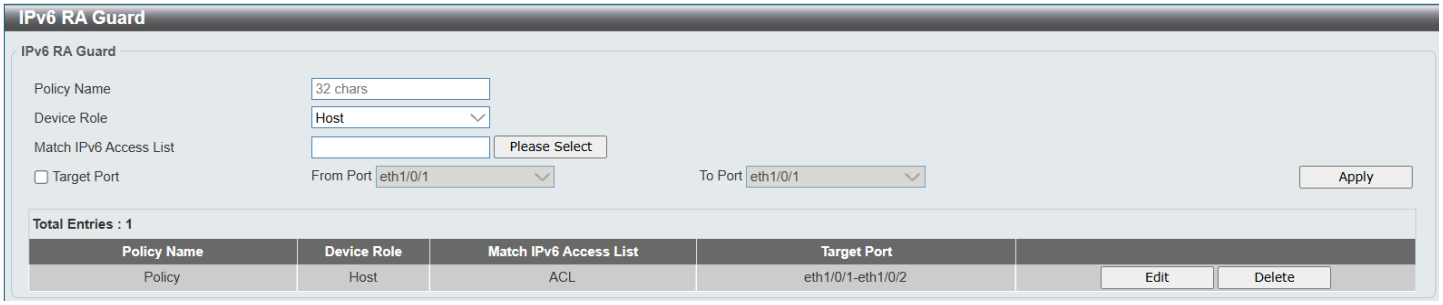
The fields that can be configured are described below:

Parameter	Description
Policy Name	Enter the policy name used here. This name can be up to 32 characters long.
Device Role	Select the device role here. Options to choose from are **Host** and **Router**. By default, the device's role is set as host and inspection for NS and NA messages are performed. If the device role is set as router, the NS and NA inspection is not performed. When performing NS/NA inspection, the message will be verified against the dynamic binding table learned from the ND protocol or from the DHCP.
Validate Source-MAC	Select to enable or disable the validation of the source MAC address option here. When the Switch receives an ND message that contains a link-layer address, the source MAC address is checked against the link-layer address. The packet will be dropped if the link-layer address and the MAC addresses are different from each other.
Target Port	Tick this option to specify the target port.
From Port - To Port	Select the appropriate port range used for the configuration here.

Click the **Apply** button to accept the changes made.
Click the **Edit** button to re-configure the specific entry.
Click the **Delete** button to remove the specified entry.

Security > IMPB >IPv6 > 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:



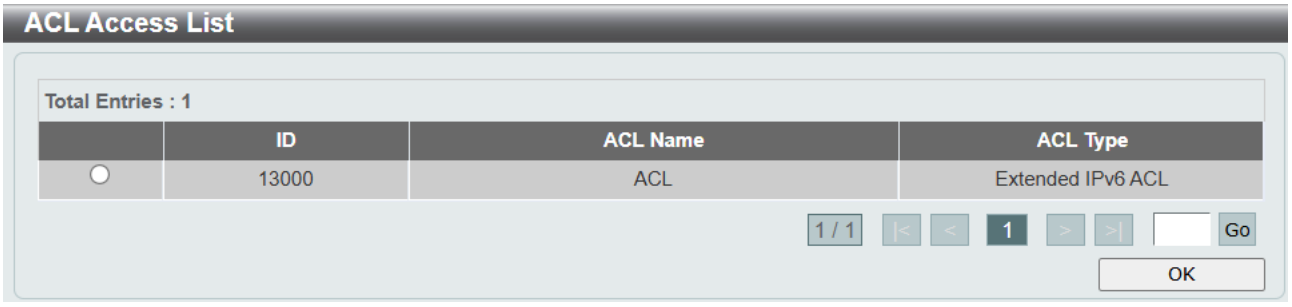
IPv6 RA Guard Window

The fields that can be configured are described below:

Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Device Role	Select the device role here. Options to choose from are **Host** and **Router**. By default, the device's role is **Host**, which will block all the RA packets. If the device's role is **Router**, RA packets will be forwarded according to the port's bound ACL.
Match IPv6 Access List	Enter or select the IPv6 access list to match here. Click the **Please Select** button to select an existing ACL from the list.
Target Port	Tick this option to specify the target port.
From Port - To Port	Select the appropriate port range used for the configuration here.

Click the **Apply** button to accept the changes made.
Click the **Edit** button to re-configure the specific entry.
Click the **Delete** button to remove the specified entry.

After clicking the **Please Select** button, the following window will appear:



ACL Access List Window

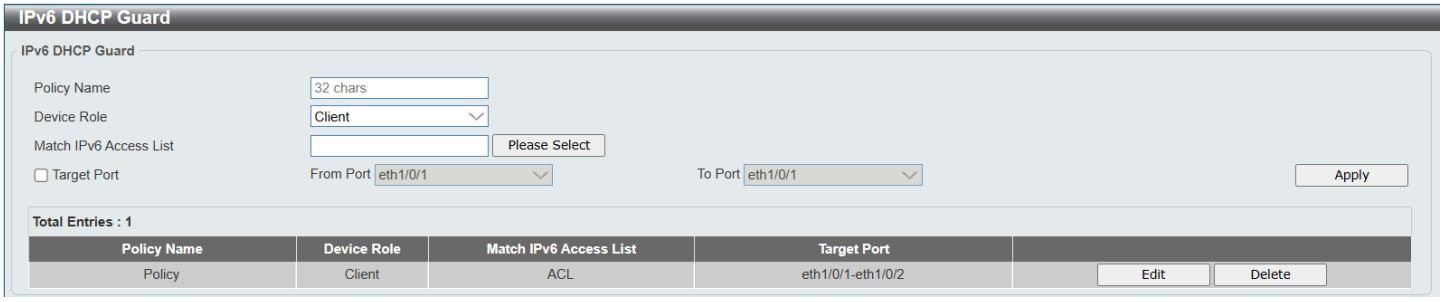
Select the radio button next to the entry to use that ACL in the configuration.

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.

Security > IMPB >IPv6 > 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 Window

The fields that can be configured are described below:

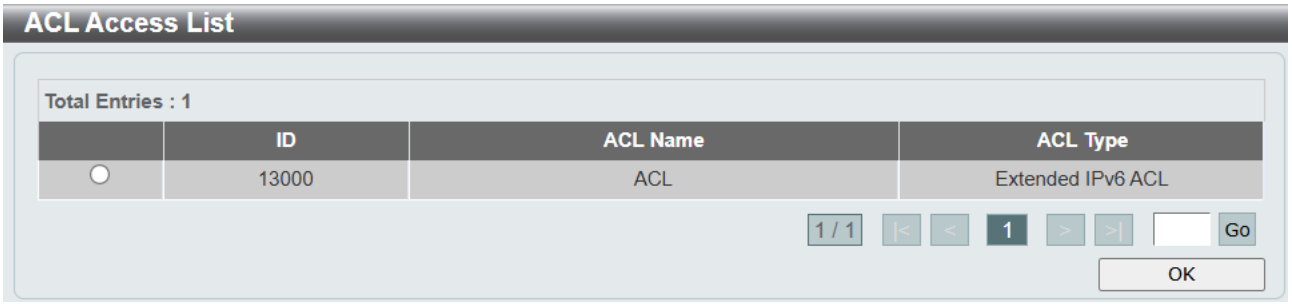
Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Device Role	Select the device role here. Options to choose from are **Host** and **Router**. By default, the device's role is **Host**, which will block all the RA packets. If the device's role is **Router**, RA packets will be forwarded according to the port's bound ACL.
Match IPv6 Access List	Enter or select the IPv6 access list to match here. Click the **Please Select** button to select an existing ACL from the list.
Target Port	Tick this option to specify the target port.
From Port - To Port	Select the appropriate port range used for the configuration here.

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

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

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

After clicking the **Please Select** button, the following window will appear:



ACL Access List Window

Select the radio button next to the entry to use that ACL in the configuration.

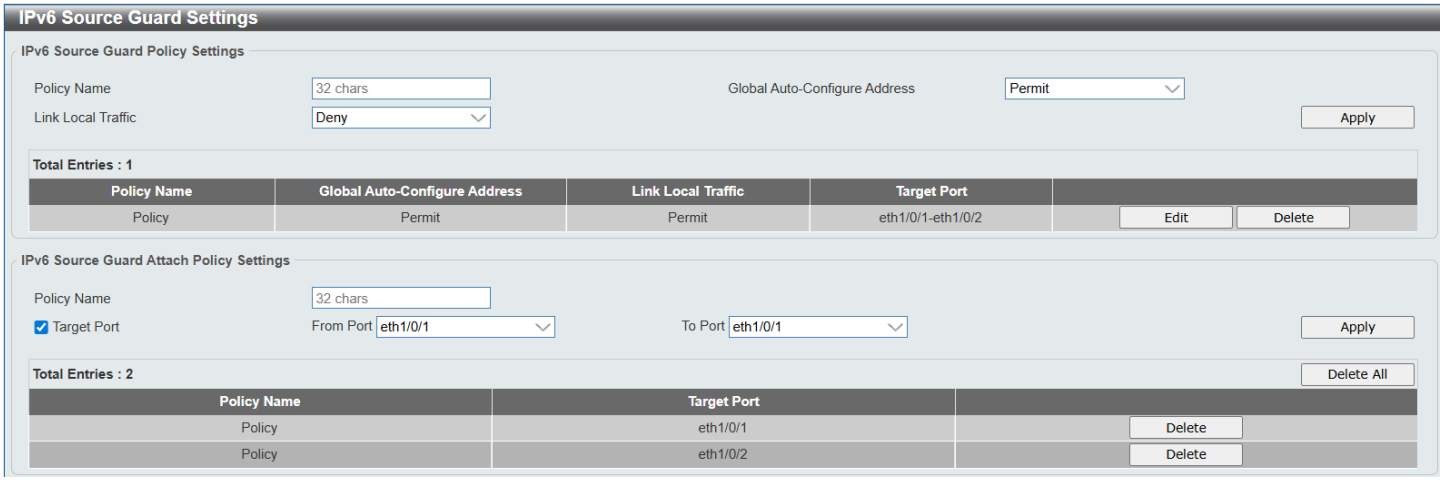
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

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

Security > IMPB >IPv6 > 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 Window

The fields that can be configured in **IPv6 Source Guard Policy Settings** are described below:

Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Global Auto-Configure Address	Select to **Permit** of **Deny** data traffic from the auto-configured global address. It is useful when all global addresses on a link are assigned by DHCP and the administrator that wants to block hosts with self-configured addresses from sending traffic. By default, **Permit** is used.
Link Local Traffic	Select to **Permit** of **Deny** hardware permitted data traffic send by the link-local address. By default, **Deny** is used.

Click the **Apply** button to accept the changes made. Click the **Edit** button to re-configure the specific entry. Click the **Delete** button to remove the specified entry.

The fields that can be configured in **IPv6 Source Guard Attach Policy Settings** are described below:

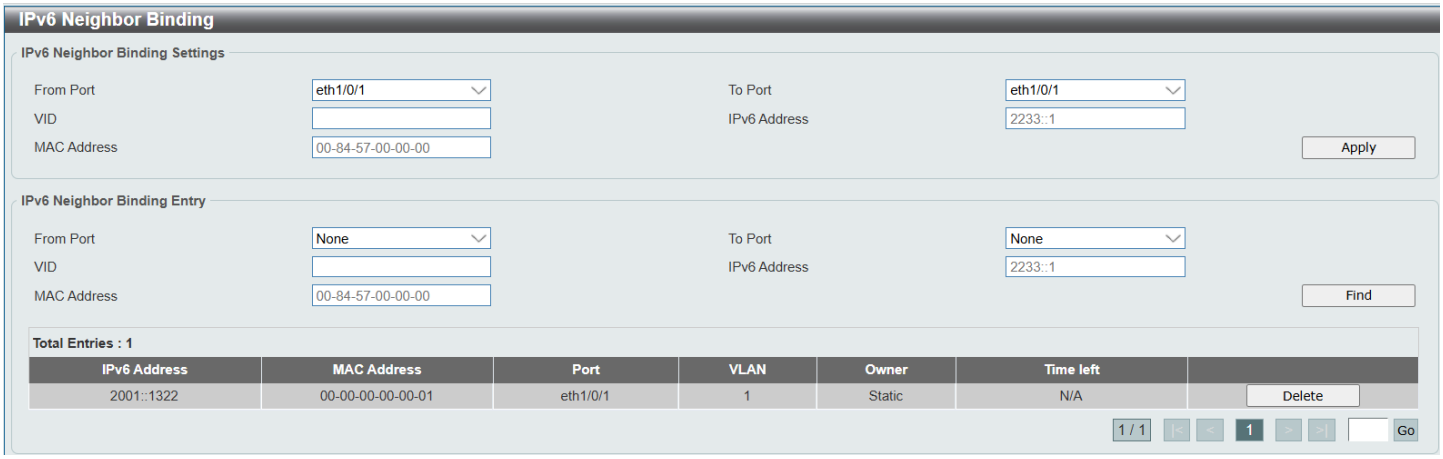
Parameter	Description
Policy Name	Enter the policy name here. This name can be up to 32 characters long.
Target Port	Select this option to specify the target port.
From Port - To Port	Select the appropriate port range used for the configuration here.

Click the **Apply** button to accept the changes made.
Click the **Delete All** button to remove all the entries.
Click the **Delete** button to remove the specified entry.

Security > IMPB >IPv6 > IPv6 Source Guard > 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 Window

The fields that can be configured in **IPv6 Neighbor Binding Settings** are described below:

Parameter	Description
MAC Address	Enter the MAC address used here.
VID	Enter the VLAN ID used here. This value must be between 1 and 4094.
IPv6 Address	Enter the IPv6 address used here.
From Port - To Port	Select the appropriate port range used for the configuration here.

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

The fields that can be configured in **IPv6 Neighbor Binding Entry** are described below:

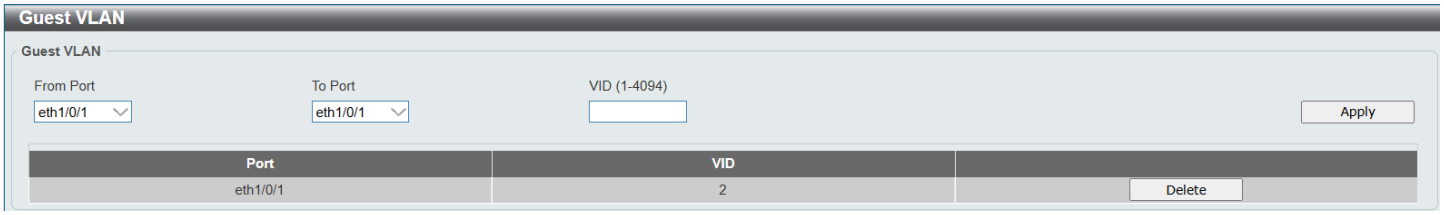
Parameter	Description
From Port - To Port	Select the appropriate port range used for the search here.
IPv6 Address	Enter the IPv6 address to find here.
MAC Address	Enter the MAC address to find here.
VID	Enter the VLAN ID to find here.

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

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

Security > Network Access Authentication > Guest VLAN

The Guest VLAN page is used to view and configure the network access authentication guest VLAN settings.



Security > Network Access Authentication > Guest VLAN

From Port / To Port: Select the appropriate port range used for the configuration here.

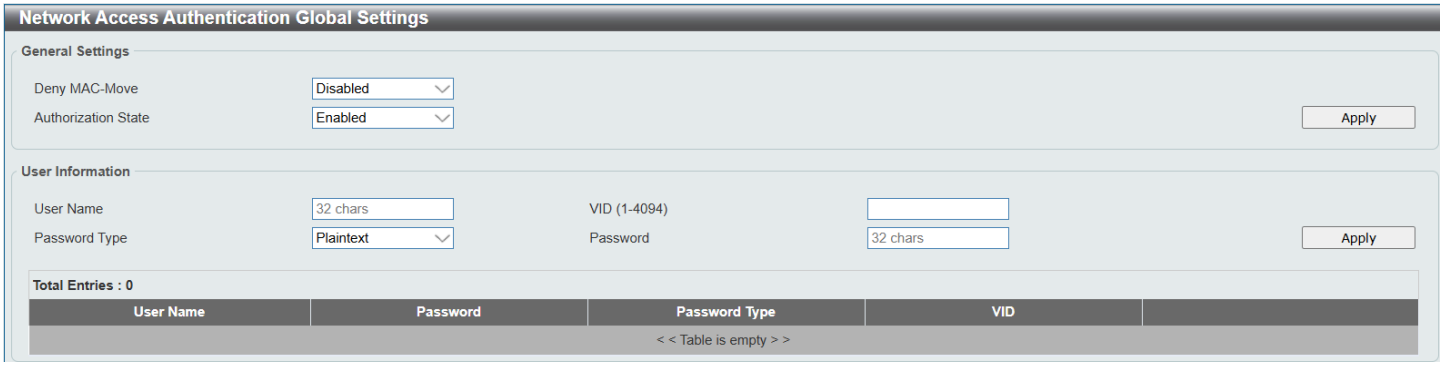
VID (1-4094): Enter the VLAN ID used here. This value must be between 1 and 4094.

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

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

Security > Network Access Authentication > Network Access Authentication Global Settings

The Network Access Authentication global Settings page is used to view and configure the network access authentication global settings.



Security > Network Access Authentication > Network Access Authentication Global Settings

General Settings:

Deny MAC–Move: Select to enable or disable the Deny MAC-Move feature here. This option controls whether authenticated hosts can move between switch ports and whether a host configured for multi-authenticate mode can move to another port.

When Deny MAC-Move is set to enablement, authorized host does NOT allow to move to other ports of Switch.

When Deny MAC-Move is set to disablement, authorized host would be permitted to move to other ports of Switch for re-authentication.

Authorization State: Select to enable or disable the Authorized State. This is used to enable or disable the acceptance of an authorized configuration and apply this to the host or port. When authorization state is enabled, the attributes assigned by the RADIUS server, for example: VLAN, 802.1p default priority, bandwidth, and ACL will be accepted.

The bandwidth and ACL attributes are assigned on a per-port basis. If the Network Access Authentication Port Settings Host Mode is set to Multi Auth, the VLAN and 802.1p attributes are assigned on a per-host basis.

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

User Information:

User Name: Enter the user name used here. This name can be up to 32 characters long.

VID (1-4094): Enter the VLAN ID used here.

Password Type: Select the password type option here. Options to choose from are **Plain Text** and **Encrypted**.

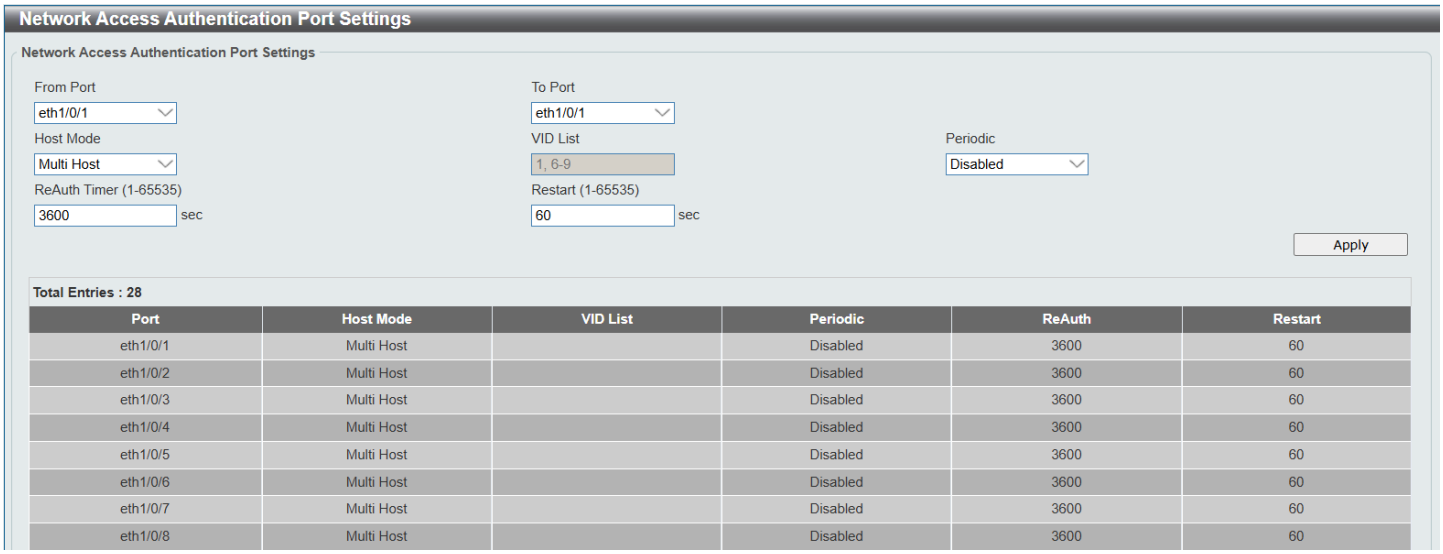
Password: Enter the password used here. This Password can be up to 32 characters long.

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

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

Security > Network Access Authentication > Network Access Authentication Port Settings

The Network Access Authentication Port Settings page is used to view and configure the network access authentication port settings.



Security > Network Access Authentication > Network Access Authentication Port Settings

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

Host Mode: Select the host mode option that will be associated with the selected port(s) here. Options to choose from are **Multi Host** and **Multi Auth.** If the port is operated in the multi-host mode, and if one of the hosts is authenticated, then all other hosts are allowed to access the port. According to 802.1X authentication, if the re-authentication fails or the authenticated user logs off, the port will be blocked for a specified period. The port restores the processing of EAPOL packets after the specified period. If the port is operated in the multi-authenticated mode, then each host needs to be authenticated individually to access the port. A host is represented by its MAC address and is only hosts that can be authenticated are allowed network access.

VID List: After selecting the Multi Auth option as the host mode, the following parameter is available. Enter the VLAN ID to be enabled for authentication. After the client is authenticated, the client will not be re-authenticated when present on other VLANs. When a port's authentication mode is changed to Multi Host, the previous authentication VLAN(s) on this port will be cleared..

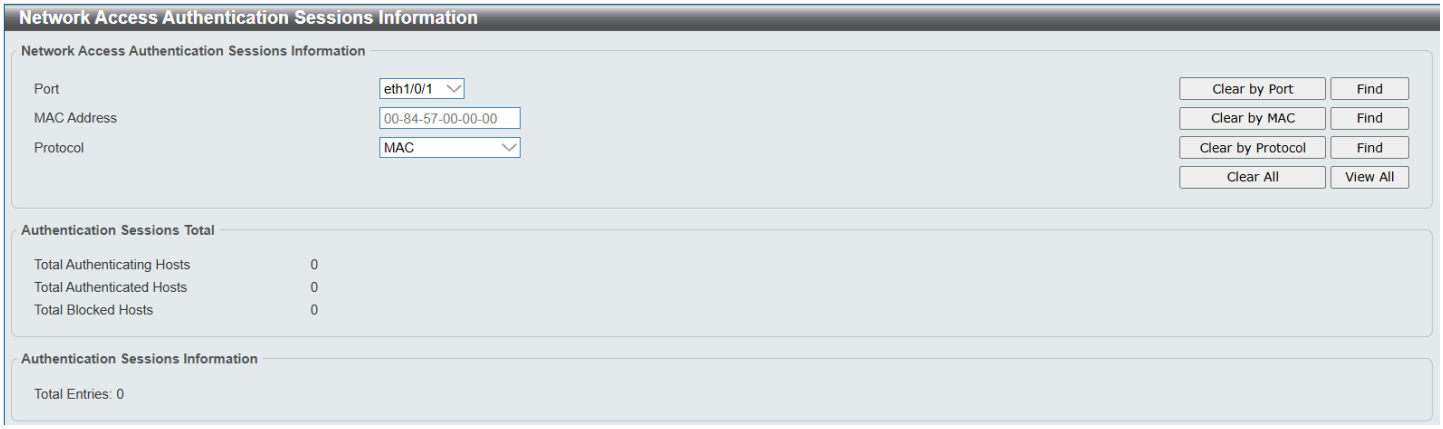
ReAuth Timer (1-65535): Enter the re-authentication timer value. This value must be between 1 and 65535 seconds. By default, this value is 3600 seconds.

Restart (1-65535): Enter the restart time value used. This value must be between 1 and 65535 seconds.

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

Security > Network Access Authentication > Network Access Authentication Sessions Information

The Network Access Authentication Sessions Information is used to view and clear the network access authentication session information.



Security > Network Access Authentication > Network Access Authentication Sessions Information

Port: Select the port to be queried.

MAC Address: Enter the MAC address of the client.

Protocol: Select the authentication protocol used. Options to choose from are **MAC**, **WAC**, and **DOT1X**.

Clear by Port: Click the **Clear by Port** button to clear the authentication session information by selected port.

Clear by MAC: Click the **Clear by MAC** button to clear the authentication session information by selected MAC address.

Clear by Protocol: Click the **Clear by Protocol** button to clear the authentication session information by selected protocol.

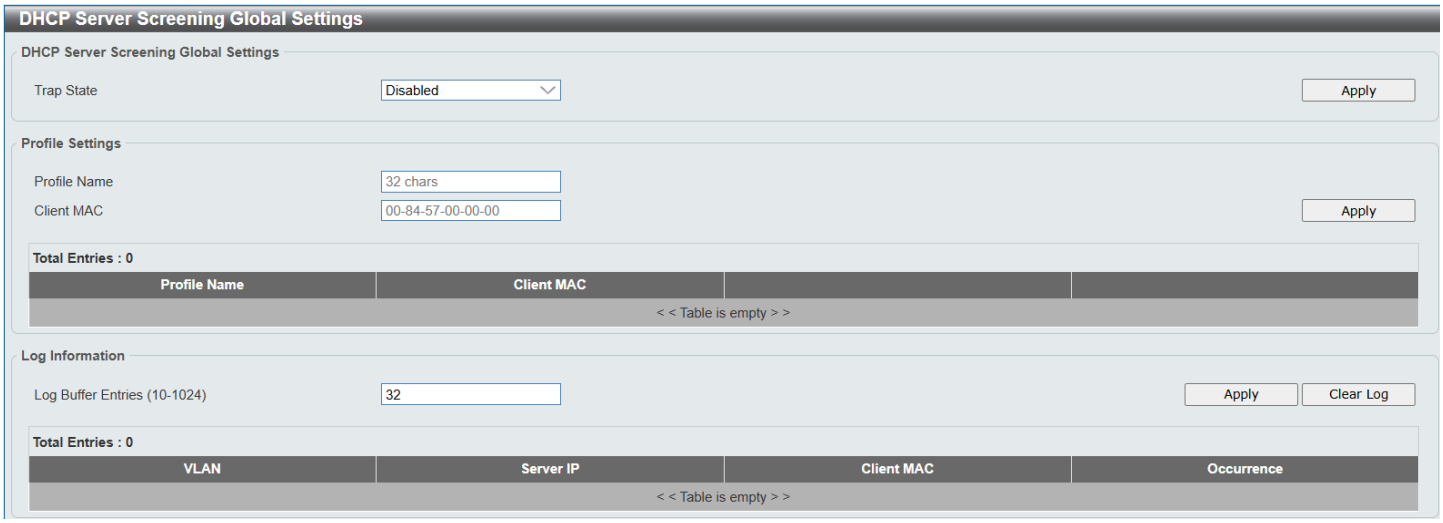
Clear ALL: Click the **Clear ALL** button to clear all authentication session information.

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

Click the **View All** button to locate and display all the entries.

Security > DHCP Server Screening > DHCP Server Screening Global Settings

DHCP Server Screening function allows you to restrict an illegal DHCP server by discarding DHCP packets from distrusted ports.



Security > DHCP Server Screening > DHCP Server Screening Global Settings

DHCP Server Screening Global Settings:

Trap State: Select to enable or disable the trap state.

Click the **Apply** button to save your settings.

Profile Settings:

Profile Name: Enter the profile name.

Client MAC: Enter the MAC address.

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

Click the **Delete Profile** button to remove the specified profile.

Click the **Apply** button to save your settings.

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

Log Information:

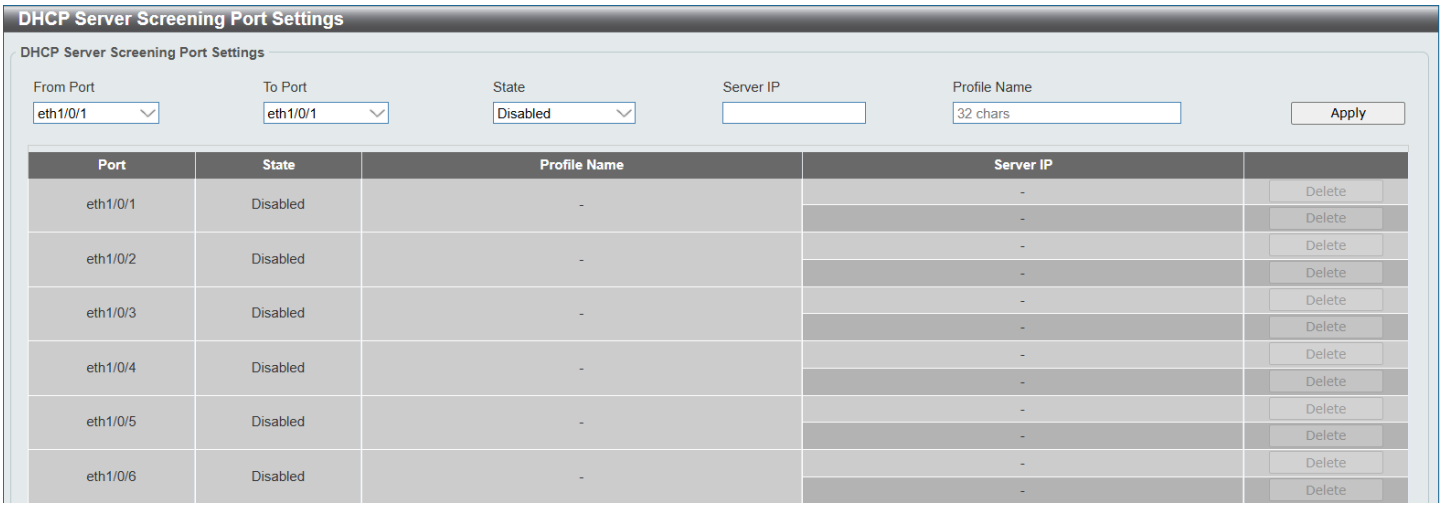
Log Buffer Entries (10-1024): Enter the logged buffer entries. The value is between 10 and 1024.

Click the **Apply** button to save your settings.

Click the **Clear Log** button to clear the log.

Security > DHCP Server Screening > DHCP Server Screening Port Settings

The DHCP Server Screening Port Settings page allows you to view and configure DHCP server screening ports.



Security > DHCP Server Screening > DHCP Server Screening Port Settings

From Port / To Port: Select the range of ports to be configured.
State: Select to enable or disable the DHCP server screening port state.
Profile Name: Enter the profile name of specified ports.
Server IP: Select **IPv4 Address** or **IPv6 Address** and enter the DHCP server IP.

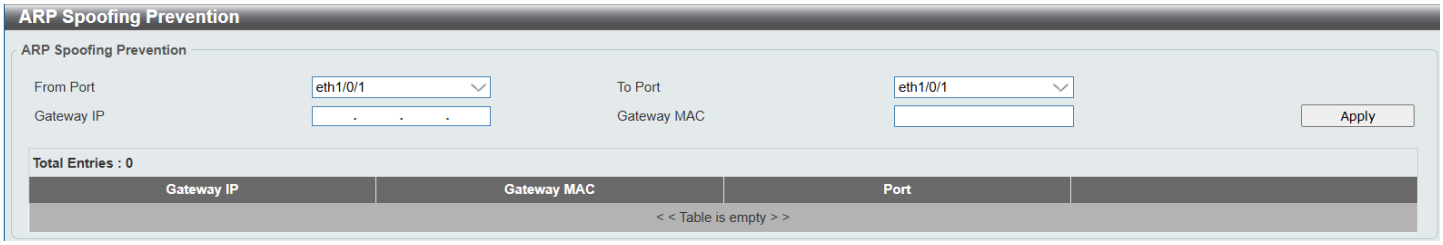
Click the **Apply** button to save your settings.

Security > ARP Spoofing Prevention

This window is used to display and configure the ARP spoofing prevention settings. When an entry is created, ARP packets whose sender IP address matches the gateway IP address, of an entry, but its sender MAC address field does not match the gateway MAC address, of the entry, will be dropped by the system. The ASP will bypass the ARP packets whose sender IP address doesn't match the configured gateway IP address.

If an ARP address matches a configured gateway's IP address, MAC address, and port list, then bypass the Dynamic ARP Inspection (DAI) check no matter if the receiving port is ARP trusted or untrusted.

To view the following window, click **Security > ARP Spoofing Prevention**, as shown below:



ARP Spoofing Prevention Window

The fields that can be configured in **ARP Spoofing Prevention** are described below:

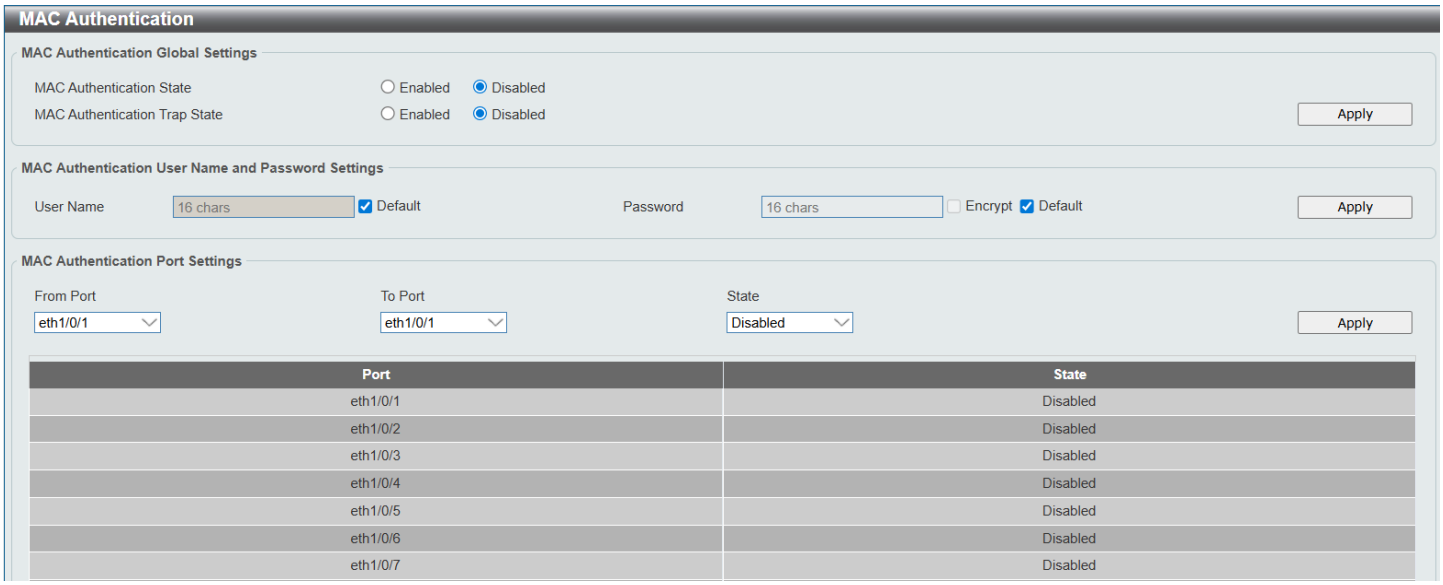
Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Gateway IP	Enter the gateway IP address used here.
Gateway MAC	Enter the gateway MAC address used here.

Click the **Apply** button to accept the changes made. Click the **Delete** button to remove the specified entry.

Security > 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 Window

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

Parameter	Description
MAC Authentication State	Select to enable or disable the global MAC authentication state.
MAC Authentication Trap State	Select to enable or disable the MAC authentication trap state.

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

The fields that can be configured in **MAC Authentication User Name and Password Settings** are described below:

Parameter	Description
User Name	Enter the username used for MAC authentication here. This name can be up to 16 characters long. Tick the **Default** option to restore the username to the client MAC address here.
Password	Enter the password used for MAC authentication here. Tick the **Encrypt** option save this password in the encrypted form. Tick the **Default** option to restore the password to the client MAC address here.

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

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

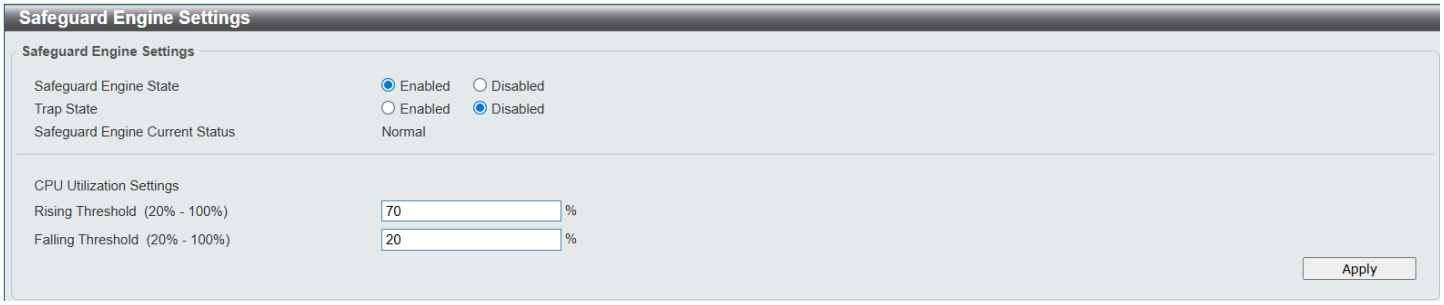
Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
State	Select to enable or disable MAC authentication for the port(s) specified here.

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

Security > Safeguard Engine > 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:



Security > Safeguard Engine > Safeguard Engine Settings

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

Parameter	Description
Safeguard Engine State	Select to enable or disable the safeguard engine feature here.
Trap State	Select to enable or disable the safeguard engine trap state here.

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

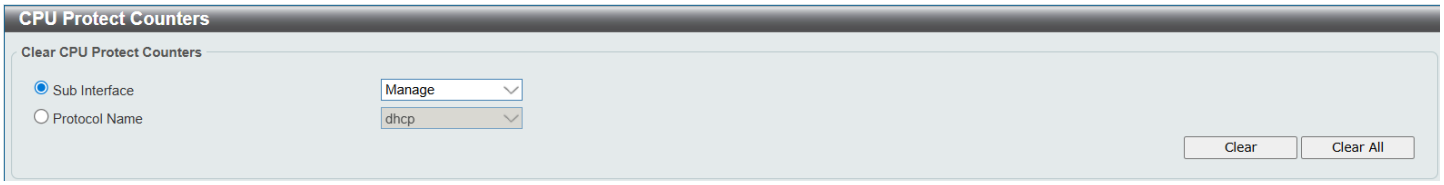
Parameter	Description
Rising Threshold	Enter the rising threshold value here. This value must be between 20% and 100%. This value is used to configure the acceptable level of CPU utilization before the Safeguard Engine mechanism is enabled. Once the CPU utilization reaches this percentage level, the Switch will move into Exhausted mode, based on the parameters provided in this window.
Falling Threshold	Enter the falling threshold value here. This value must be between 20% and 100%. This value is used to configure the acceptable level of CPU utilization as a percentage, where the Switch leaves the Safeguard Engine state and returns to normal mode.

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

Security > Safeguard Engine > 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:



Security > Safeguard Engine > CPU Protect Counters

The fields that can be configured are described below:

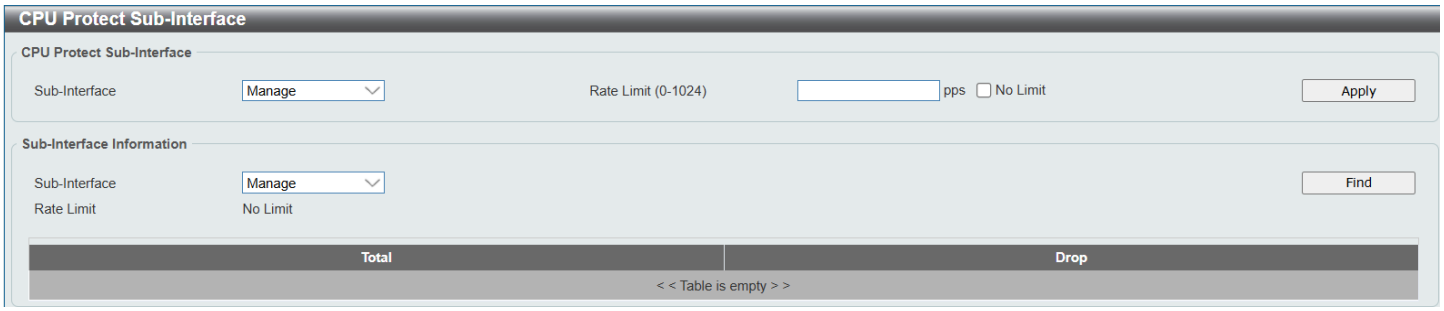
Parameter	Description
Sub Interface	Select the sub-interface option here. Options to choose from are **Manage**, **Protocol**, **Route**, and **All**. This option specifies to clear the CPU protect related counters of sub-interfaces.
Protocol Name	Select the protocol name option here.

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.

Security > Safeguard Engine > 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:



Security > Safeguard Engine > CPU Protect Sub-Interface

The fields that can be configured in **CPU Protect Sub-Interface** are described below:

Parameter	Description
Sub-Interface	Select the sub-interface option here. Options to choose from are **Manage**, **Protocol**, and **Route**.
Rate Limit	Enter the rate limit value used here. This value must be between 0 and 1024 packets per second. Tick the **No Limit** option to disable the rate limit.

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

The fields that can be configured in **Sub-Interface Information** are described below:

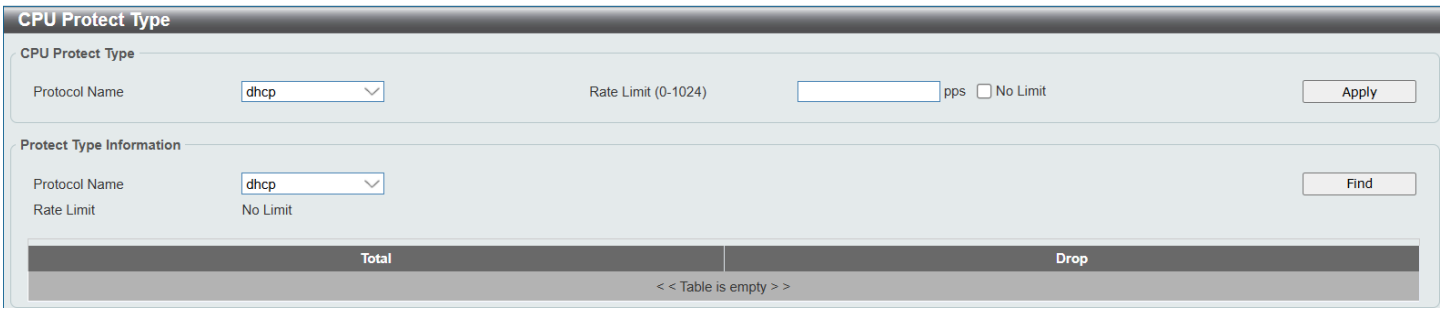
Parameter	Description
Sub-Interface	Select the sub-interface option here. Options to choose from are **Manage**, **Protocol**, and **Route**.

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

Security > Safeguard Engine > 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:



Security > Safeguard Engine > CPU Protect Type

The fields that can be configured in **CPU Protect Type** are described below:

Parameter	Description
Protocol Name	Select the protocol name option here.
Rate Limit	Enter the rate limit value used here. This value must be between 0 and 1024 packets per second. Tick the **No Limit** option to disable the rate limit.

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

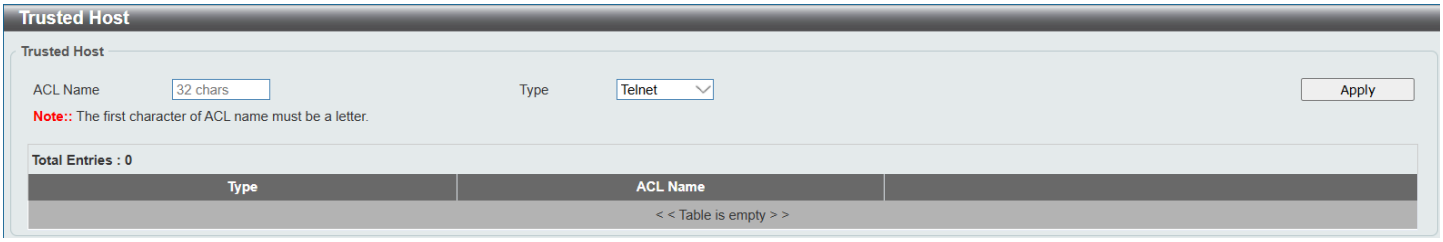
The fields that can be configured in **Protect Type Information** are described below:

Parameter	Description
Protocol Name	Select the protocol name here. After selecting the protocol name, the **Rate Limit** assigned to the protocol type will be displayed.

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

Security > Trusted Host

The Trusted Host page allows you to view and configure the trusted host settings.



Security > Trusted Host

ACL Name: Specify the ACL name. The name can be up to 32 characters long.
Type: Specify the trusted host type. The options are **Telnet**, **Ping**, **HTTP** and **HTTPS**.

Click the **Apply** button to save your settings.

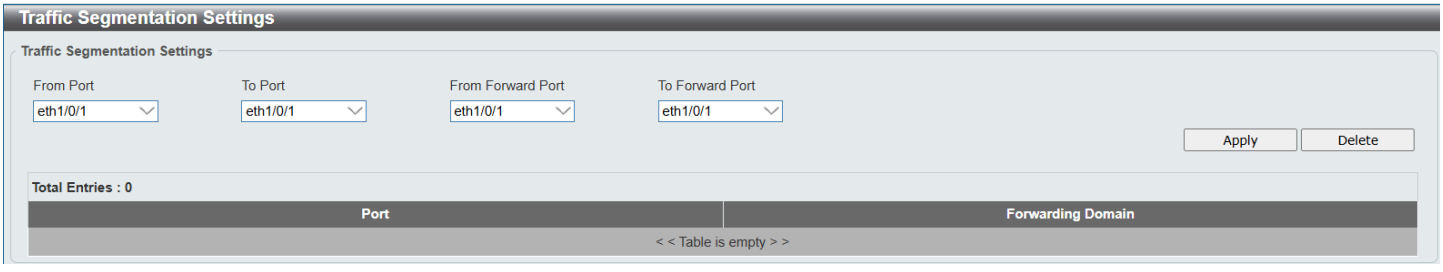
Security > Traffic Segmentation Settings

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:



Security > Traffic Segmentation Settings

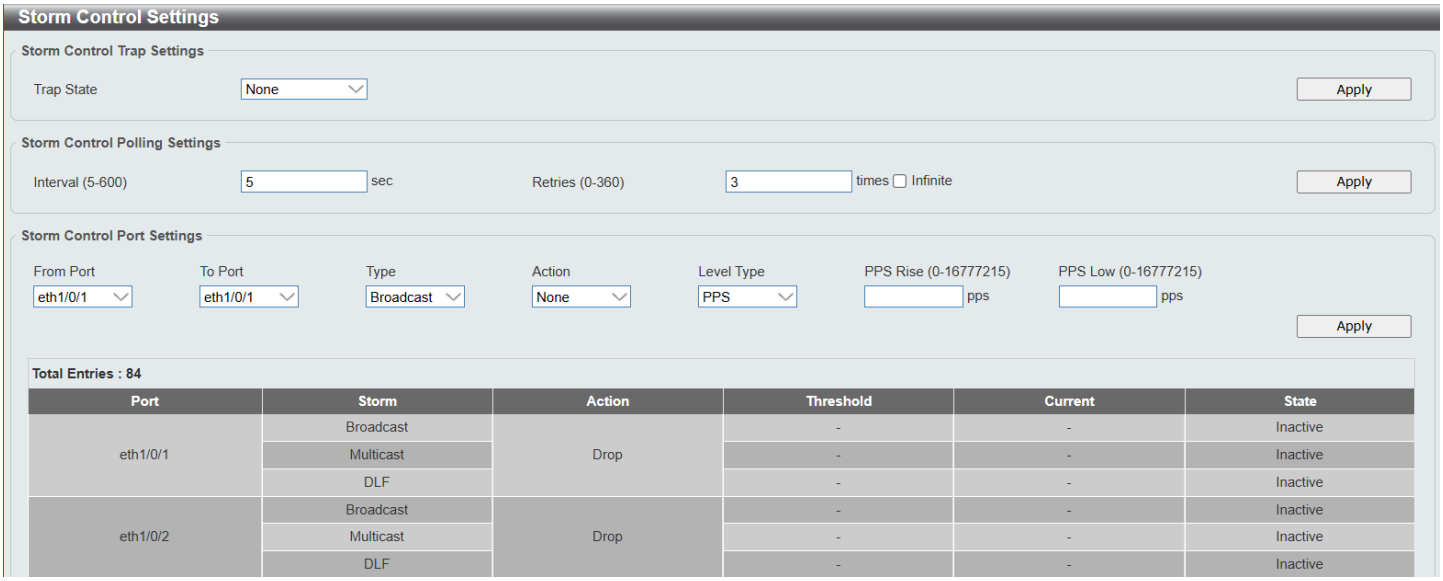
From Port / To Port: Select the range of ports to be configured.
From Forward Port / To Forward Port: Select the range of forward ports to be configured.

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

Security > 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:



Security > Storm Control Settings-PPS

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

Parameter	Description
Trap State	Select the storm control trap option here. Options to choose from are: • **None** - Specifies that no traps will be sent. • **Storm Occur** - Specifies that a trap notification is sent when a storm event is detected. • **Storm Clear** - Specifies that a trap notification is sent when a storm event is cleared. • **Both** - Specifies that a trap notification is sent when a storm event is detected and/or cleared.

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

The fields that can be configured in **Storm Control Polling Settings** are described below:

Parameter	Description
Polling Interval	Enter the interval value used here. This value must be between 5 and 600 seconds. By default, this value is 5 seconds.
Shutdown Retries	Enter the shutdown retries value used here. This value must be between 0 and 360. By default, this value is 3. Tick the **Infinite** option to disable this feature.

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

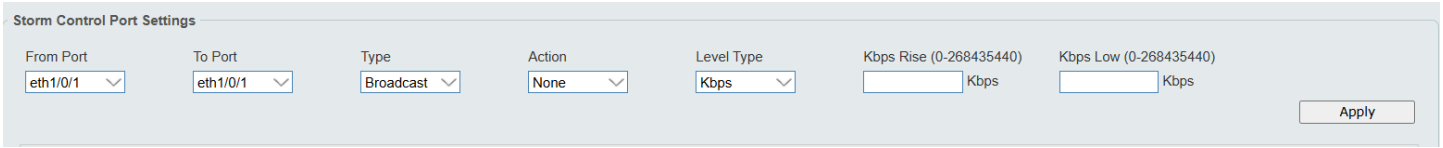
The fields that can be configured in **Storm Control Port Settings** are described below:

Parameter	Description
From Port - To Port	Select the appropriate port range used for the configuration here.
Type	Select the type of storm attack that will be controlled here. Options to choose from are **Broadcast**, **Multicast**, and **DLF**. 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** and **Kbps**.
PPS Rise	Enter the rise packets per second value here. This option specifies the rise threshold value in packets count per second. This value must be between 0 and 16777215 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. This value must be between 0 and 16777215 packets per second.

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

After selecting the **Kbps** option as the **Level Type**, the following parameters are available.



Security > Storm Control Settings-Kbps

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 value must be between 0 and 268435440.
KBPS Low	Enter the rise KBPS value used here. This value must be between 0 and 268435440.

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

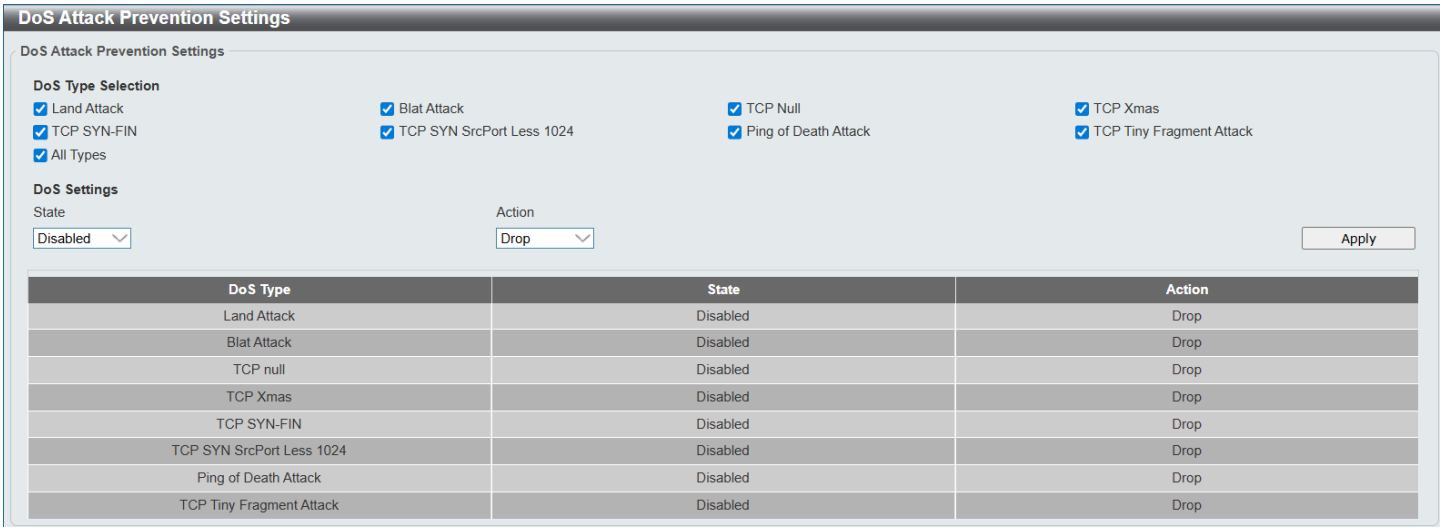
Security > DoS Attack Prevention Settings

This window is used to display and configure the Denial-of-Service (DoS) attack prevention settings. The following well-known DoS types that can be detected by most Switches:

- **Land Attack:** This type of attack involves IP packets where the source and destination address are set to the address of the target device. It may cause the target device to reply to itself continuously.
- **Blat Attack**: This type of attack will send packets with the TCP/UDP source port equal to the destination port of the target device. It may cause the target device to respond to itself.
- **TCP-Null:** This type of attack involves port scanning by using specific packets that contain a sequence number of 0 and no flags.
- **TCP-Xmas:** This type of attack involves port scanning by using specific packets that contain a sequence number of 0 and the Urgent (URG), Push (PSH), and FIN flags.
- **TCP SYN-FIN:** This type of attack involves port scanning by using specific packets that contain SYN and FIN flags.
- **TCP SYN SrcPort Less 1024:** This type of attack involves port scanning by using specific packets that contain source port 0 to 1023 and SYN flag.
- **Ping of Death Attack:** A ping of death is a type of attack on a computer that involves sending a malformed or otherwise a malicious ping to a computer. A ping is normally 64 bytes in size (many computers cannot handle a ping larger than the maximum IP packet size which is 65535 bytes). The sending of a ping of this size can crash the target computer. Traditionally, this bug has been relatively easy to exploit. Generally, sending a 65536 byte ping packet is illegal according to networking protocol, but a packet of such a size can be sent if it is fragmented; when the target computer reassembles the packet, a buffer overflow can occur, which often causes a system crash.
- **TCP Tiny Fragment Attack:** The Tiny TCP Fragment attacker uses IP fragmentation to create extremely small fragments and force the TCP header information into a separate packet fragment to pass through the check

function of the router and issue an attack.

To view the following window, click **Security > DoS Attack Prevention Settings**, as shown below:



Security > DoS Attack Prevention Settings

The fields that can be configured in **DoS Attack Prevention Settings** are described below:

Parameter	Description
DoS Type Selection	Tick the DoS type option that will be prevented here.
State	Select to enable or disable the global DoS attack prevention state here.
Action	Select the action that will be taken when the DoS attack was detected here. The only option to select here is **Drop**.

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

Security > SSH > SSH Global Settings

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



Security > SSH > SSH Global Settings

IP SSH Server State: Select to enable or disable the SSH server's global state.

IP SSH Service Port: Enter the SSH service port number used here. This value must be between 1 and 65535. By default, this number is 22.

Authentication Timeout: Enter the authentication timeout value here. This value must be between 30 and 600 seconds. By default, this value is 120 seconds.

Authentication Retries: Enter the authentication retries value here. This value must be between 1 and 32. By default, this value is 3.

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

Security > SSH > Host Key

This window is used to display and generate the SSH host key.



Security > SSH > SSH Host Key

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 1024 and 2048 bit.

Click the **Generate** button to generate a host key based on the selections made.

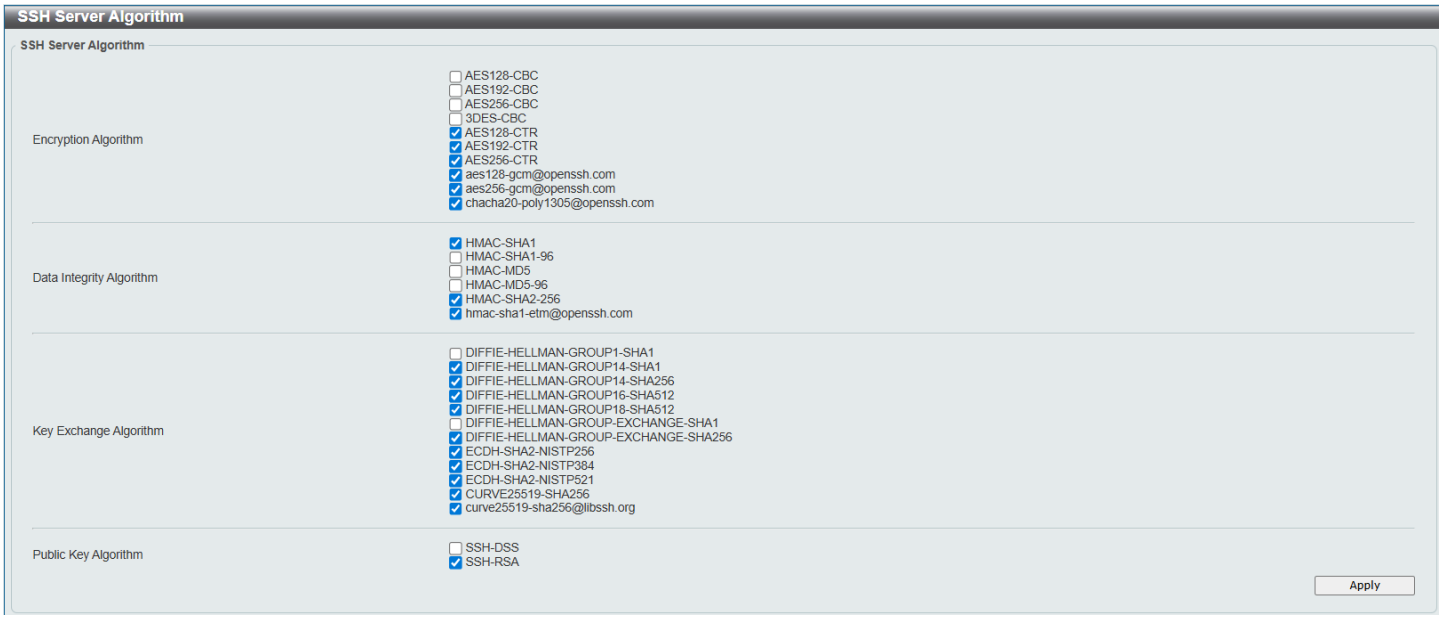
Click the **Delete** button to remove a host key based on the selections made.

The fields that can be configured in **Host Key** are described:

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.

Security > SSH > SSH Server Algorithm

The SSH Algorithm window allows the configuration of the desired types of SSH algorithms used for authentication encryption. There are four categories of algorithms listed and specific algorithms of each may be enabled or disabled by using their corresponding pull-down menus. All algorithms are enabled by default. To open the following window, click Security > SSH > SSH Algorithm:

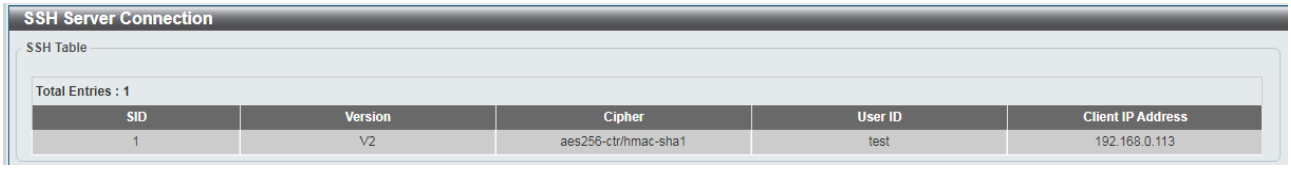


Security > SSH > SSH Server Algorithm

Security > SSH > SSH Server Connection

This window is used to view the SSH server connections table.

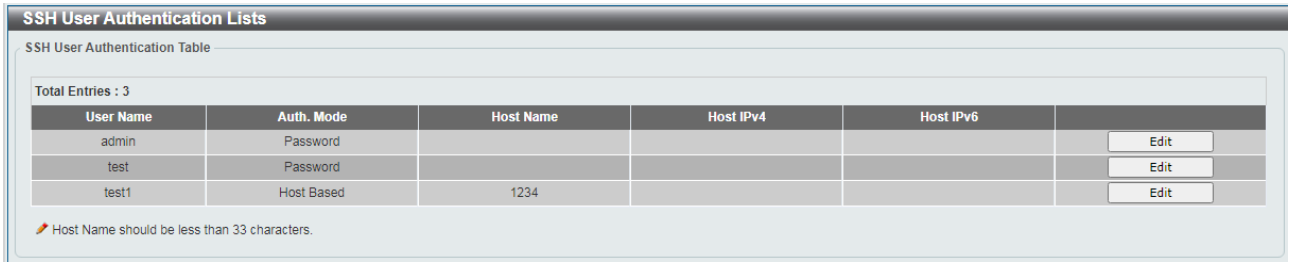
To view the following window, click Security > SSH > SSH Server Connection, as shown below:



Security > SSH > SSH Server Connection

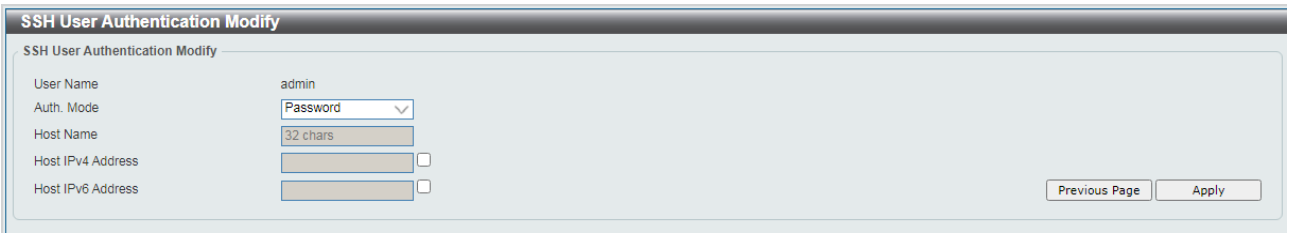
Security > SSH > SSH User Authentication List

This window is used to display SSH User List.



Security > SSH > SSH User Authentication List

By Click **Edit**, the following page shown:



Host Name: After selecting the Host-based option as the Authentication Method, enter the host name here.

Host IPv4 Address: After selecting the Host-based option as the Authentication Method, select and enter the IPv4 address here.

Host 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.

Security > SSH > SSH Public Key Settings

This window is used to configure the SSH public Key settings.



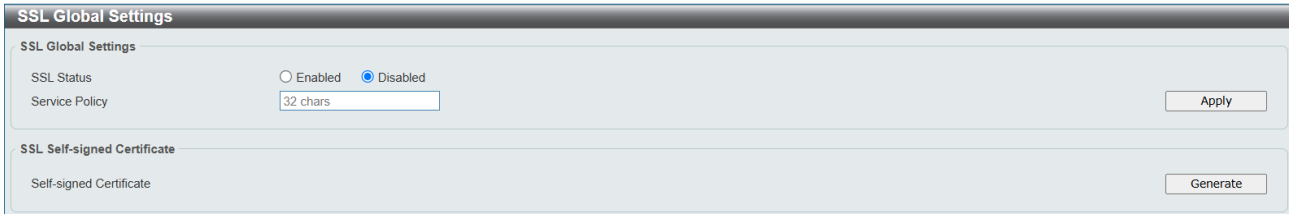
Security > SSH > SSH Public Key Settings

Click the **Download** button to download the specific public key to switch.

Security > SSL > SSL Global Setting

Secure Sockets Layer (SSL) is a security feature that provides a secure communication path between the management PC and the Switch Web UI by using authentication, digital signatures and encryption. These security functions are implemented by Ciphersuite, a security string that determines the cryptographic parameters, encryption algorithms and key sizes.

This page allows you to configure the SSL global state settings.



Security > SSL > SSL Settings

SSL Global Settings:

SSL Status: Select to enable or disable the SSL feature's global status.

Service Policy: Enter service policy name.

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

SSL-Self-signed Certificate: Apply "Generate" will update new Certificate.

NOTE: When SSL is enabled, it will take longer to open a web page due to the extra processing required for encryption. After saving, please wait about 10 seconds for the system summery page to load.

Security > SSL > Crypto PKI Trustpoint

The SSL Service Policy page allows you to view and configure the SSL service policy settings.



Security > SSL > Crypto PKI Trustpoint

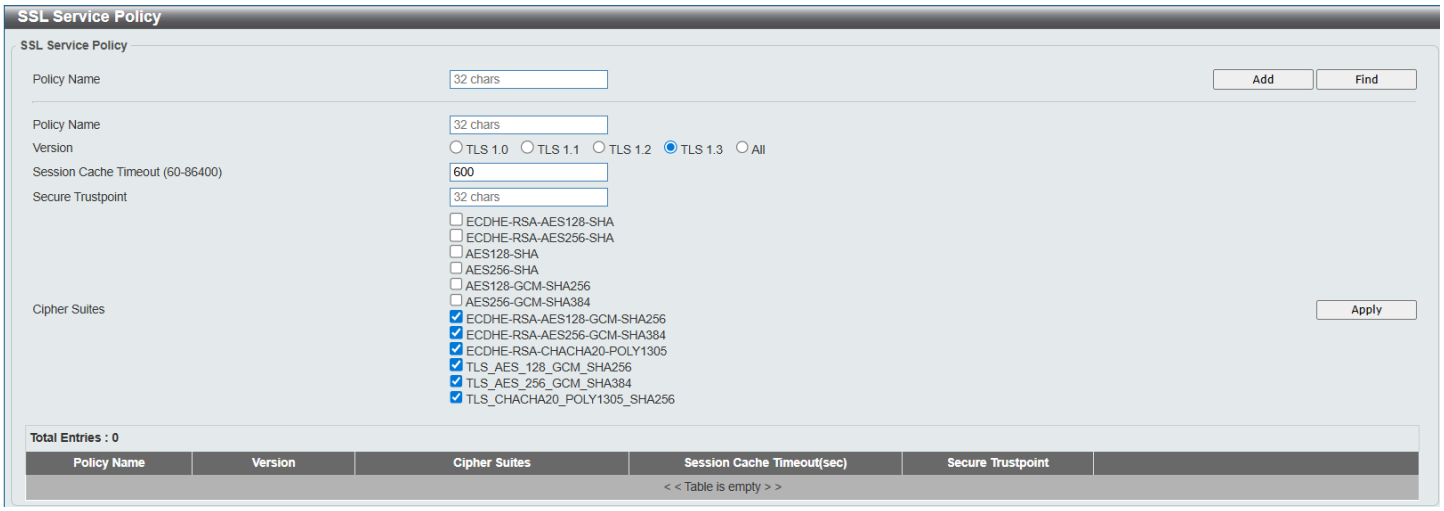
Trustpoint: Enter the name of the trust-point that is associated with the imported certificates and key pairs here. This name can be up to 32 characters long.
TFTP Server Path: Enter the TFTP server path here.
Password: Enter the encrypted password phrase that is used to undo encryption when the private 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.
Type: Select the type of certificate that will be imported here. Options to choose from are **Both, CA,** and **Local**.

- Selecting **Both** specifies to import the CA certificate, local certificate and key pairs.
- Selecting **CA** specifies to import the CA certificate only.
- Selecting **Local** specifies to import local certificate and key pairs only.

Click the **Apply** button to accept the changes made.
Click the **Find** button to locate a specific entry based on the information entered.
Click the **Delete** button to remove the specified entry

Security > SSL > SSL Service Policy

The SSL Service Policy page allows you to view and configure the SSL service policy settings.



Security > SSL > SSL Service Policy

Policy Name: Enter a policy name for SSL.

Click the **Add** button to save your settings.

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

Version: Select the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) version here. Options to choose from are TLS 1.0, TLS 1.1, TLS 1.2 and TLS 1.3.

Session Cache Timeout (60-86400): Enter the session cache timeout value. The value is between 60 and 86400 seconds.

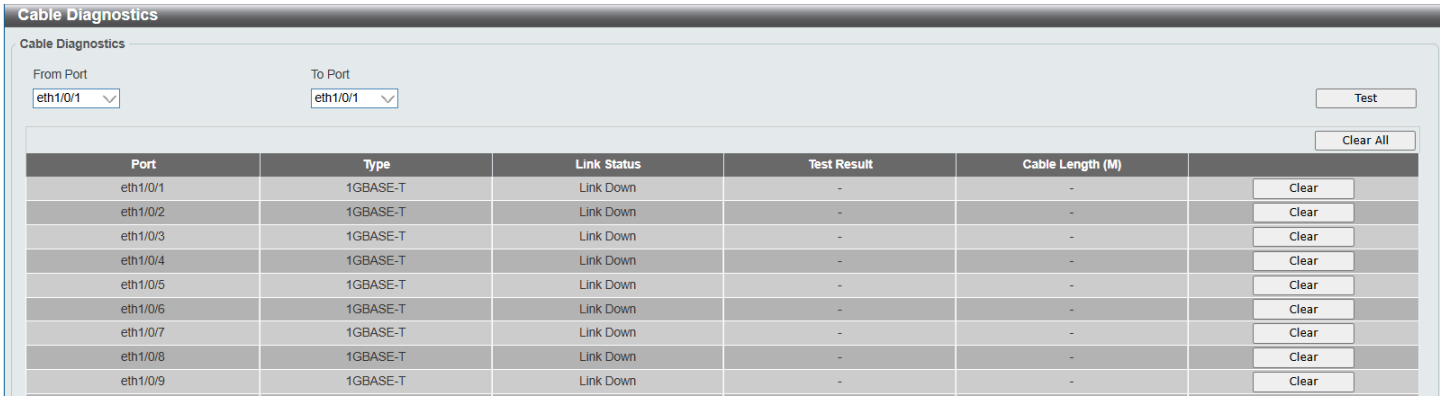
Secure Trustpoint (32 chars): Enter the secure trust point name here. This name can be up to 32 characters long.

Cipher Suites: Select the cipher suites that will be associated with this profile.

Click the **Apply** button to save your settings.

OAM > Cable Diagnostics

The Cable Diagnostics page is designed primarily for administrators and customer service representatives to examine the copper cable quality. It determines the type of cable errors in the cable. Select the range of ports and then click the **Test** button to start the diagnosis.



OAM > Cable Diagnostic

Click the **Clear** button to clear all the information for the specific port.

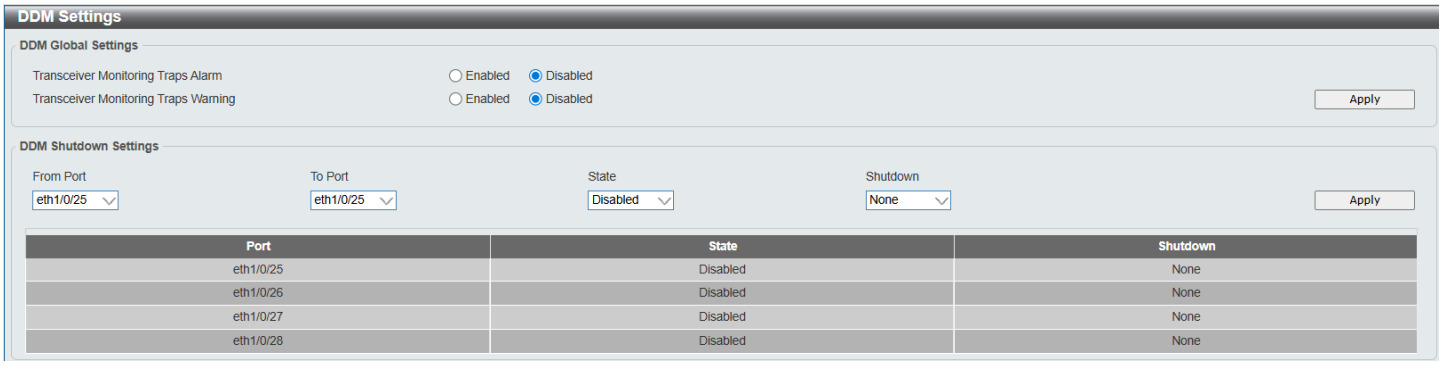
Click the **Clear All** button to clear all the information in this table.

NOTE: For more accurate test results, use the TIA/EIA-568B pin assignment on the RJ45 connectors.

NOTE: The Switch (RTCT) distance deviation is about +/- 20m.

OAM > DDM > 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.



OAM > DDM > DDM Settings

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.

The fields that can be configured in **DDM Shutdown Settings** are described:

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 shutdown the port, when the operating parameter exceeds the Alarm or Warning threshold.

Alarm - Shutdown the port when the configured alarm threshold range is exceeded.

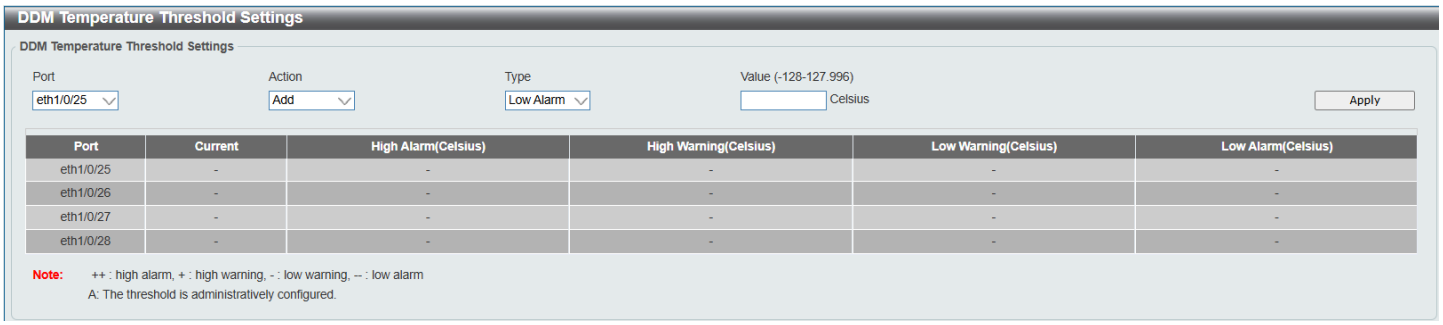
Warning - Shutdown the port when the configured warning threshold range is exceeded.

None - The port will never shutdown regardless if the threshold ranges are exceeded or not. This is the default.

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

OAM > DDM > DDM Temperature Threshold Settings

This window is used to display and configure the DDM Temperature Threshold Settings for specific ports on the Switch.



OAM > DDM > DDM Temperature Threshold Settings

Port: Select the port used for the configuration here.

Action: Select the action that will be taken here. Options to choose from are Add and Delete.

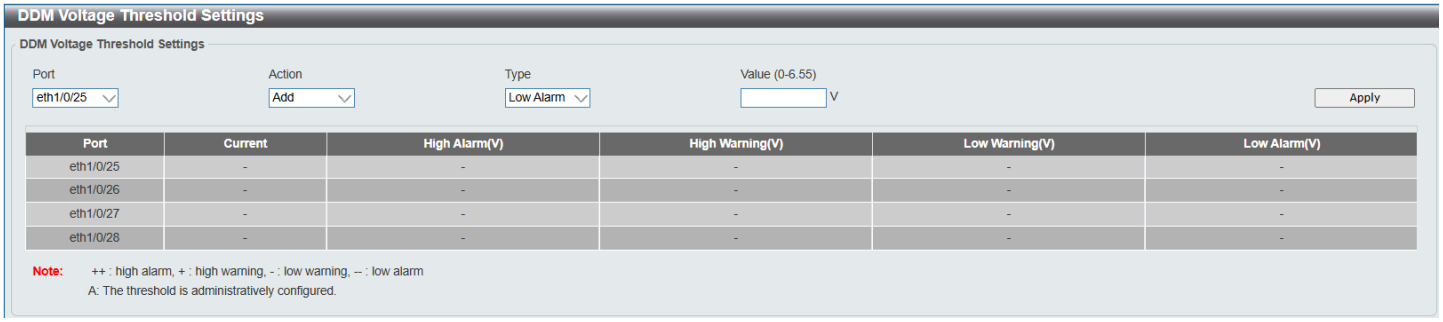
Type: Select the type of temperature threshold. Options to choose from are Low Alarm, Low Warning, High Alarm, and High Warning.

Value: Enter the threshold value. This value must be between -128 and 127.996 °C..

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

OAM > DDM > DDM Voltage Threshold Settings

This window is used to display and configure the DDM Voltage Threshold Settings for specific ports on the Switch.



OAM > DDM > DDM Voltage Threshold Settings

Port: Select the port used for the configuration here.

Action: Select the action that will be taken here. Options to choose from are Add and Delete.

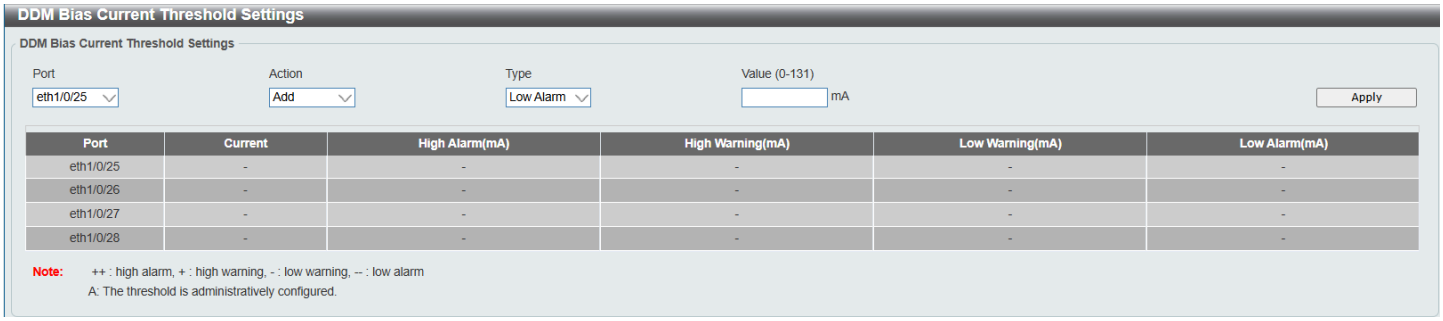
Type: Select the type of voltage threshold. Options to choose from are Low Alarm, Low Warning, High Alarm, and High Warning.

Value: Enter the threshold value. This value must be between 0 and 6.55 Volt.

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

OAM > DDM > 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.



OAM > DDM > DDM Bias Current Threshold Settings

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.

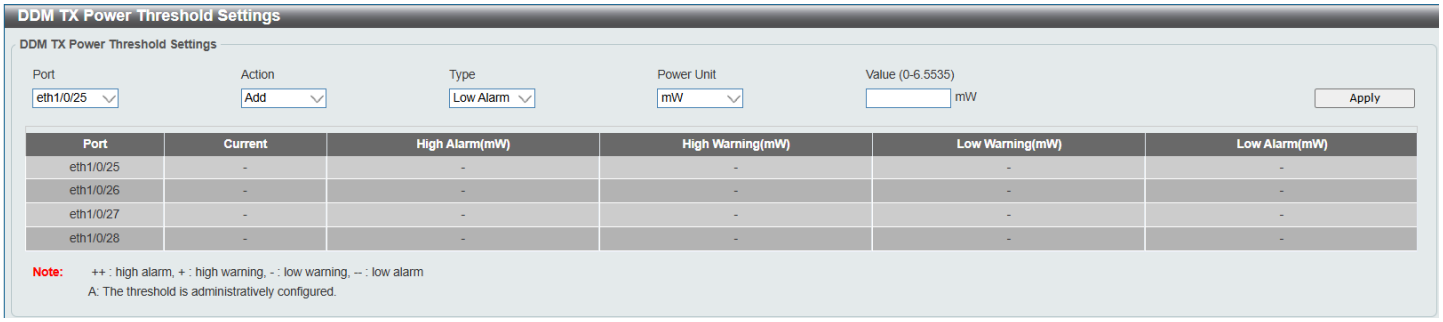
Type: Select the type of bias current threshold. Options to choose from are Low Alarm, Low Warning, High Alarm, and High Warning.

Value: Enter the threshold value. This value must be between 0 and 131 mA.

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

OAM > DDM > DDM TX Power Threshold Settings

This window is used to display and configure the threshold of TX power for specific ports on the Switch.



OAM > DDM > DDM TX Power Threshold Settings

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.

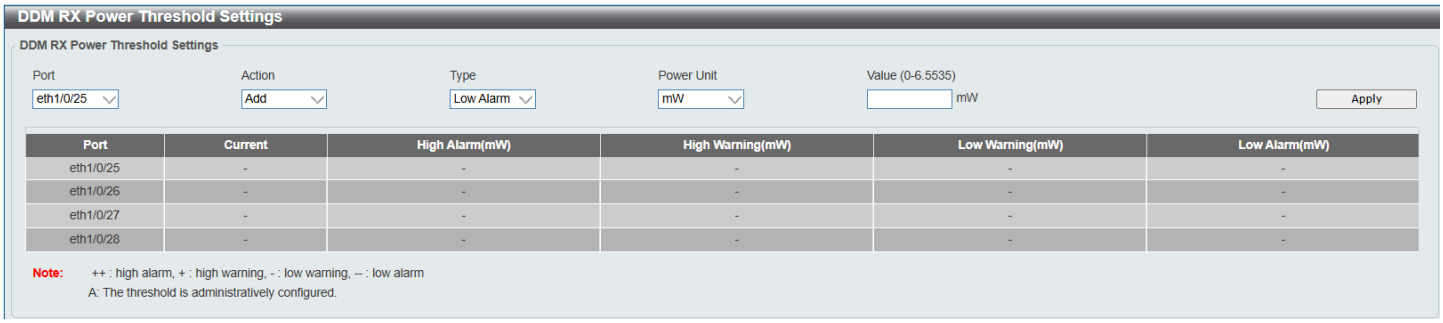
Power Unit: Select the power unit here. Options to choose from are mW and dBm.

Value: Enter the threshold value either in **mW** or **dBm** here.

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

OAM > DDM > DDM RX Power Threshold Settings

This window is used to display and configure the threshold of RX power for specific ports on the Switch.



OAM > DDM > DDM RX Power Threshold Settings

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.

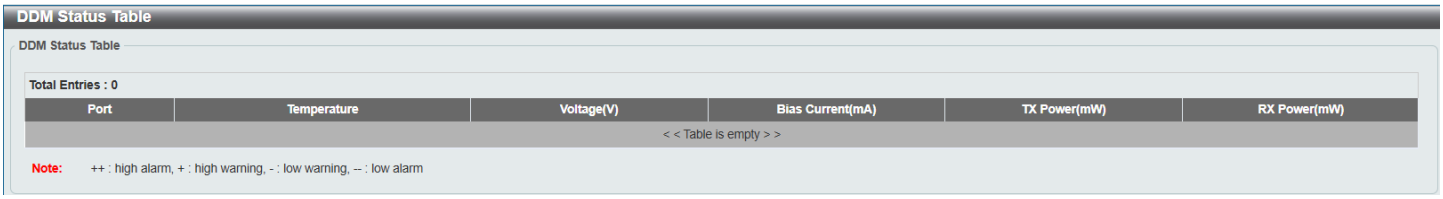
Power Unit: Select the power unit here. Options to choose from are mW and dBm.

Value: Enter the threshold value either in **mW** or **dBm** here.

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

OAM > DDM > DDM Status Table

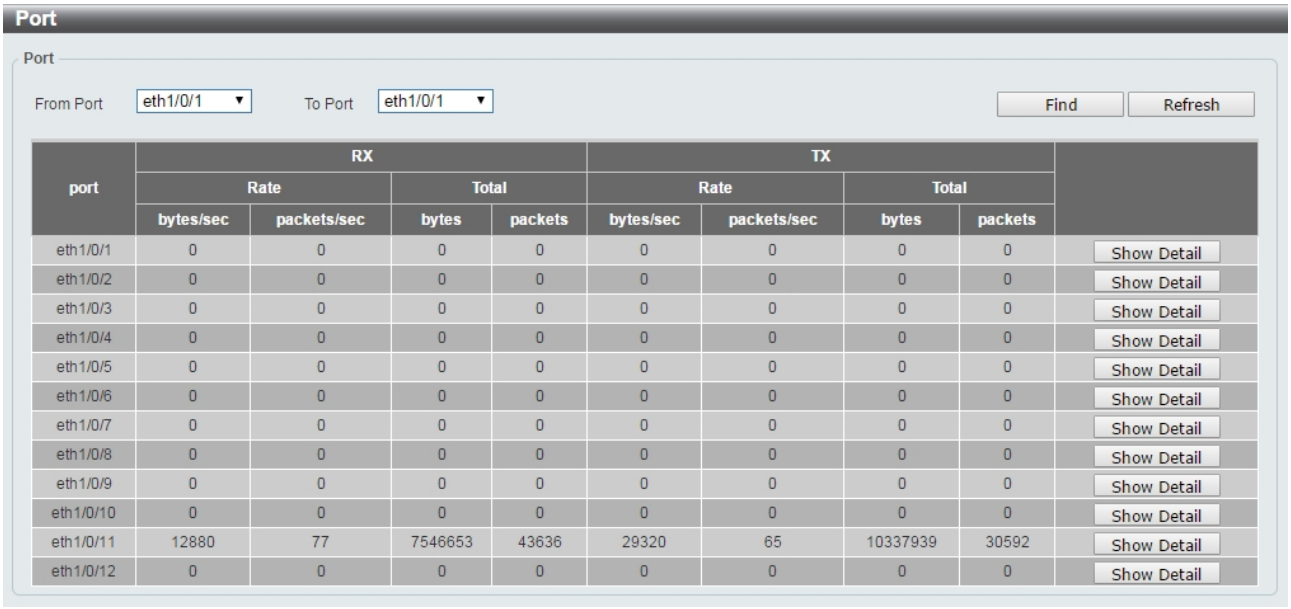
This window is used to display the current operating digital diagnostic monitoring parameters and their values on the SFP module for specified ports.



OAM > DDM > DDM Status Table

Monitoring > Statistics > Port

This page allows you to display the port traffic statistics.

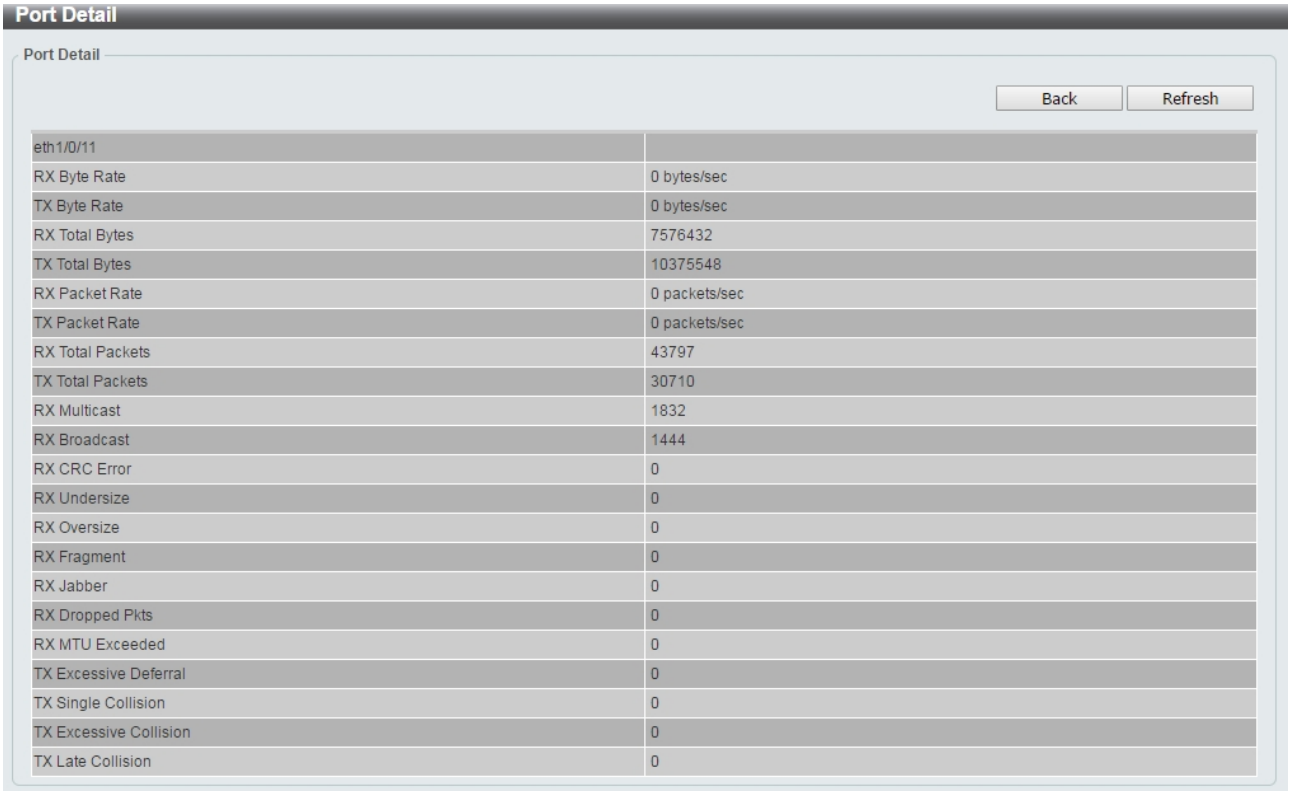


Monitoring > Statistics > Port

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

Click the **Find** button to locate a specific entry based on the information entered.
Click the **Refresh** button to refresh the display table.

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

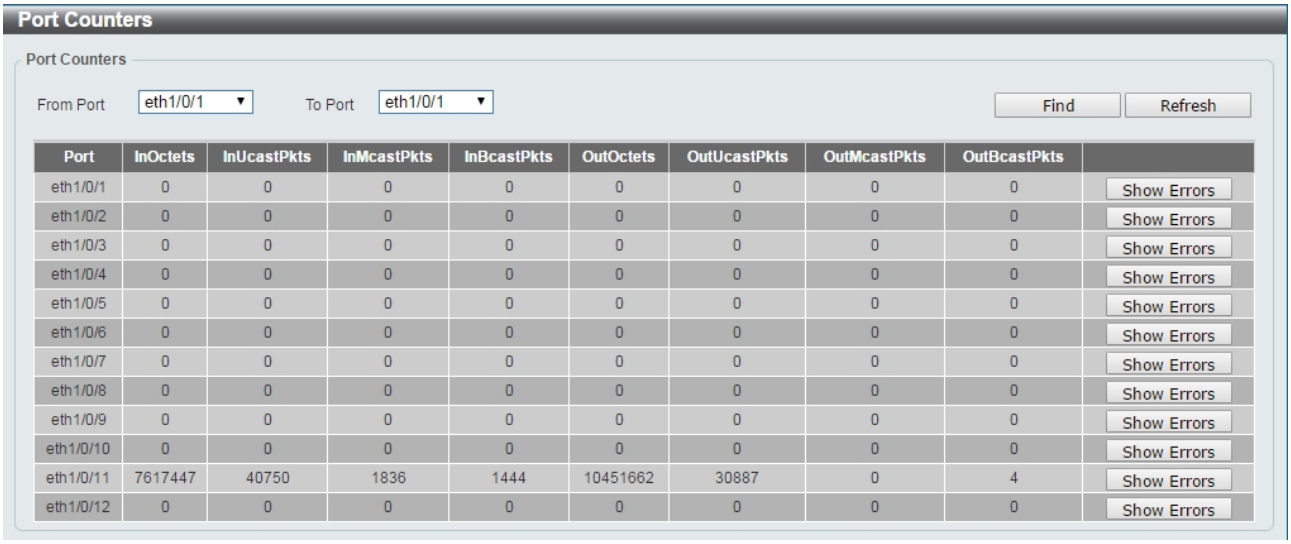


Monitoring > Statistics > Port – Show Detail

Click the **Back** button to return to the previous window.
Click the **Refresh** button to refresh the display table.

Monitoring > Statistics > Port Counters

The Port Counters page allows you to display port counter statistics.



Monitoring > Statistics > Port Counters

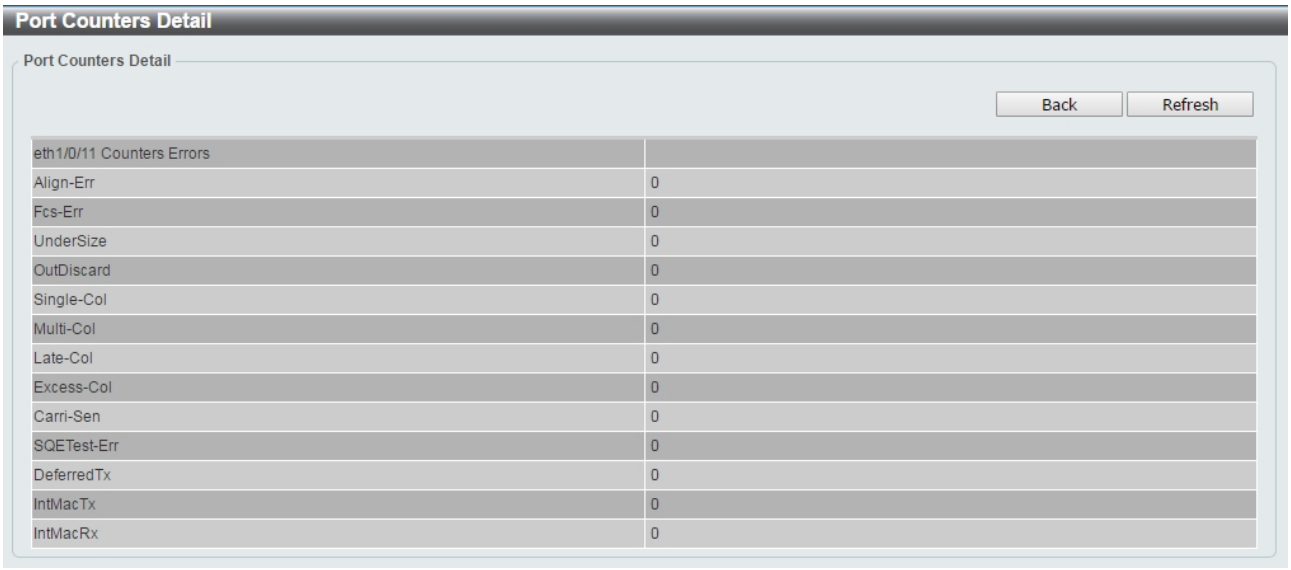
From Port / To Port: Select the range of ports to be viewed.

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

Click the **Refresh** button to refresh the display table.

Click the **Show Errors** button to see all error counters of the specific port.

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



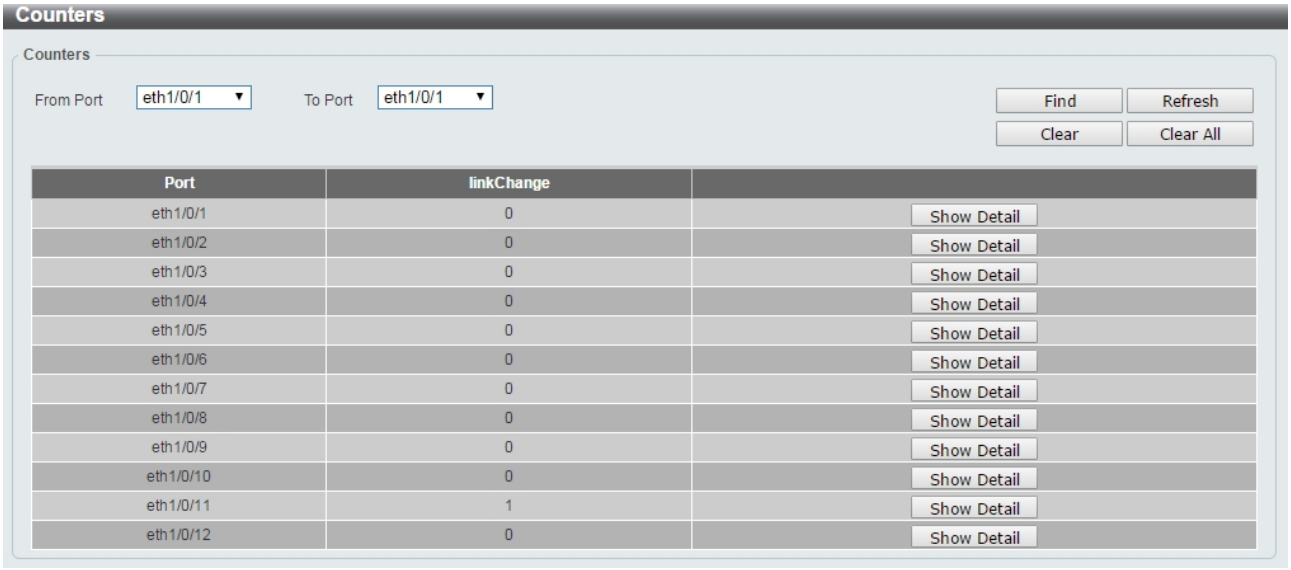
Monitoring > Statistics > Port Counters – Show Errors

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

Click the **Refresh** button to refresh the display table.

Monitoring > Statistics > Counters

The Counters page allows you to display all port counters, and clear the port counters of the specified or all ports.



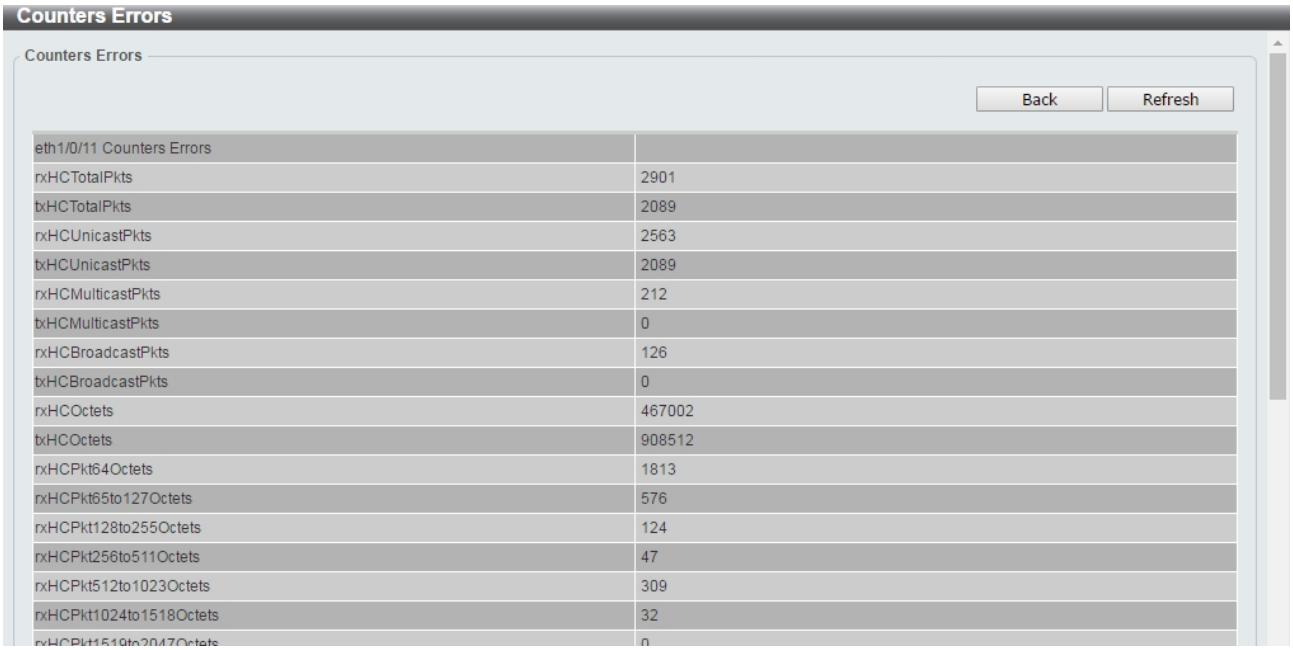
Monitoring > Statistics > Counters

From Port / To Port: Select the range of ports to be viewed.

Click the **Find** button to locate a specific entry based on the information entered.
Click the **Refresh** button to refresh the display table.
Click the **Clear** button to clear all the information for the specific ports.
Click the **Clear All** button to clear all the information in this table.

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

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

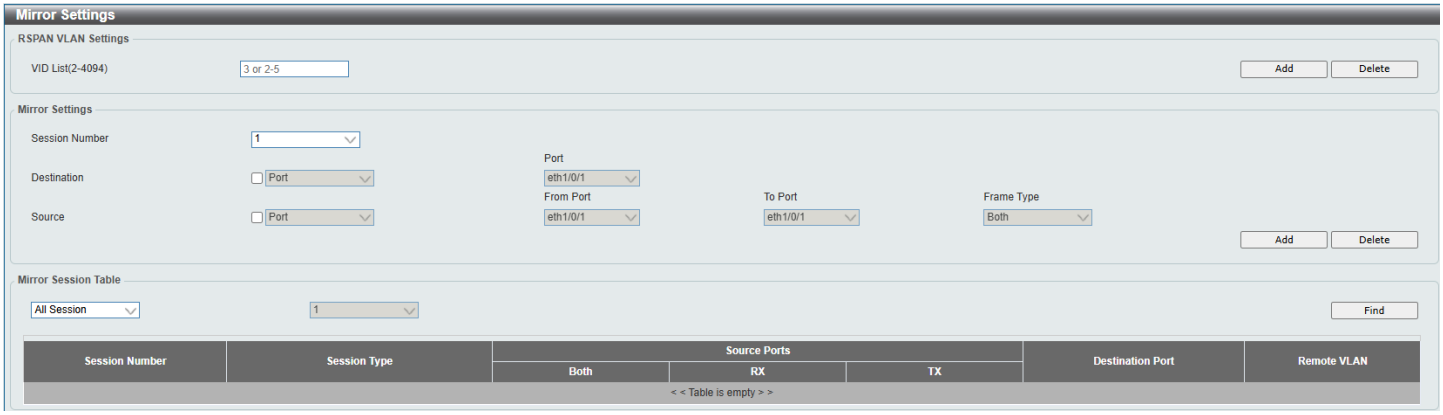


Monitoring > Statistics > Counters – Show Detail

Click the **Back** button to return to the previous window.
Click the **Refresh** button to refresh the display table.

Monitoring > Mirror Settings

The Mirror Settings page allows you to view and configure the port mirroring feature.



Monitoring > Mirror Settings

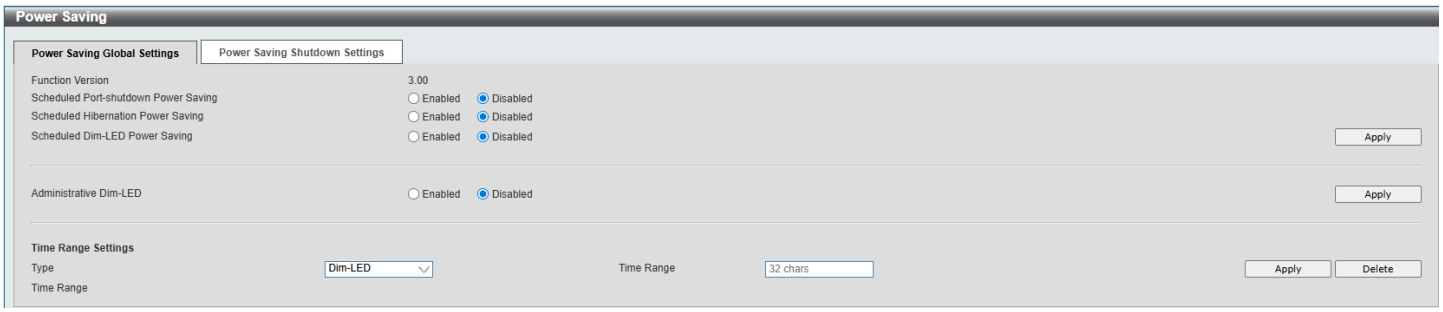
Session Number: Select the mirror session number for the entry.
Destination: Select the destination port for mirror settings.
Source: Select the range of ports to be the source port and Frame Type to be mirrored.

Click the **Add** button to add the newly configured mirror entry based on the information entered.
Click the **Delete** button to delete an existing mirror entry based on the information entered.

Mirror Session Table: Select the Mirror Session Type to be displayed.
Click the **Find** button to locate a specific entry based on the information entered.

Green > Power Saving

The Power Saving page allows you to configure the power saving settings of the Switch.

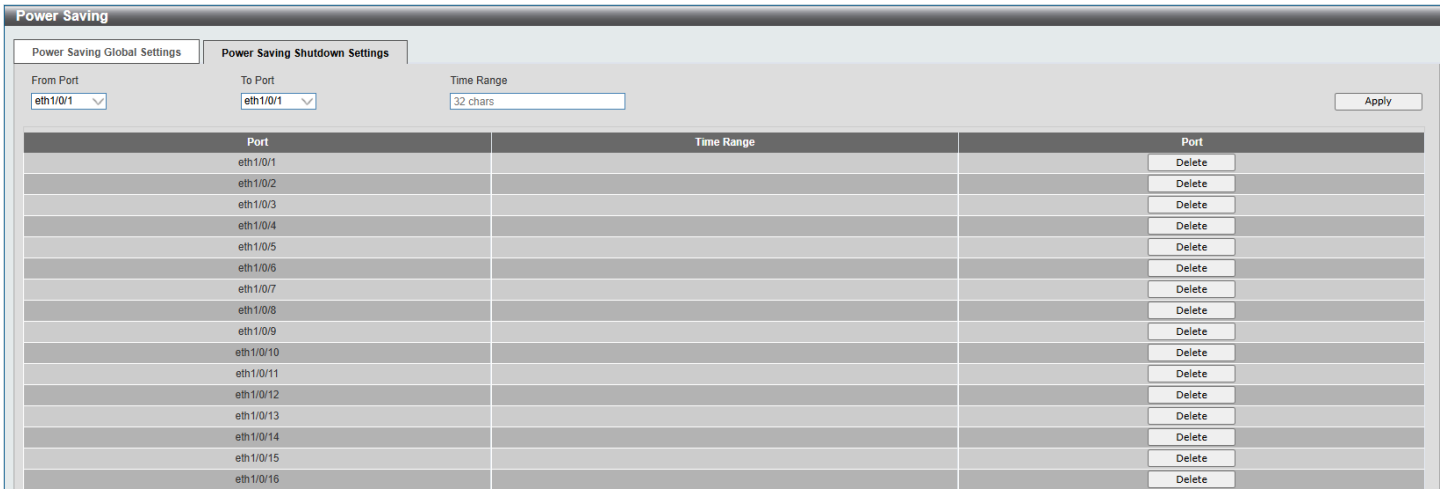


Green > Power Saving

Scheduled Port-shutdown Power Saving: Select to enable or disable the scheduled port shutdown power saving feature.
Scheduled Hibernation Power Saving: Select to enable or disable the scheduled hibernation power saving feature. When this option is enabled, the system will enter into the hibernation mode based on the specified time range. When the system enters the hibernation mode, the switch will go into a low power state and idle. It will shut down all the ports and LEDs and all network function will be disabled. If the Switch is an endpoint type Power Sourcing Equipment (PSE), the Switch will not provide power to the port.
Scheduled Dim-LED Power Saving: Select to enable or disable applying the power saving by scheduled dimming of the Switch LEDs.
Administrative Dim-LED: Select to enable or disable the port LED dimming function.
Type: Select the type of power saving. Options to choose from are **Dim-LED** and **Hibernation**.
Time Range: Select the name of the time range to associate with the power saving type.

Click the **Apply** button to save your settings for each individual section.
Click the **Delete** button to remove the specified entry.

After clicking the **Power Saving Shutdown Settings** tab, the following page will appear.



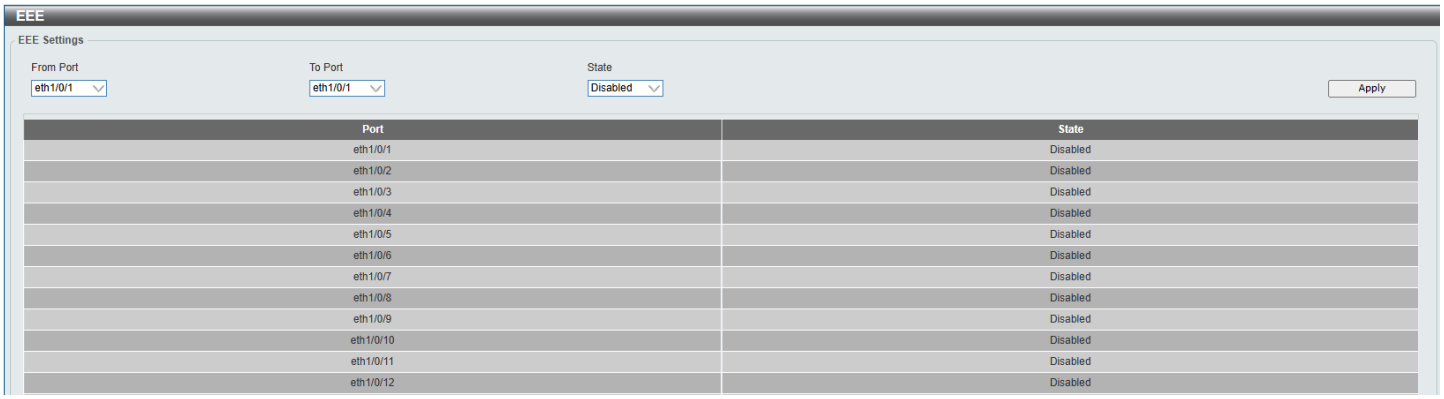
Green > Power Saving – Shutdown Settings

From Port / To Port: Select the range of ports to be configured.
Time Range: Enter the time range to associate with the specified ports.

Click the **Apply** button to save your settings.

Green > EEE

The 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.



Green > EEE

From Port / To Port: Select the range of ports to be configured.
State: Select to enable or disable the EEE feature.

Click the **Apply** button to save your settings.

Surveillance Mode

SURVEILLANCE OVERVIEW PORT INFORMATION

IP-Camera Information
NVR Information

PoE Information
PoE Scheduling
Management
Time

Surveillance Settings
Surveillance Log
Health Diagnostic
Toolbar

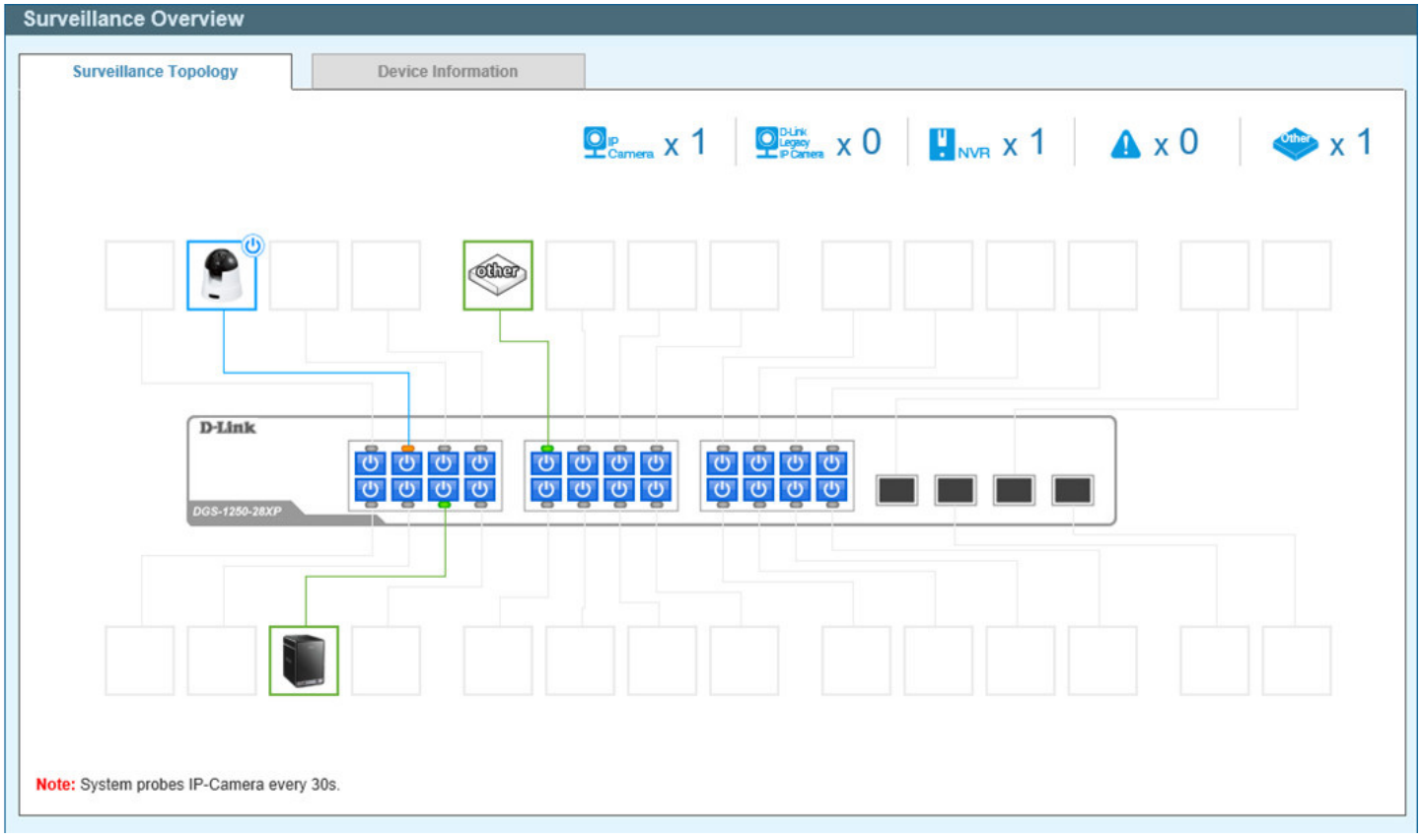
Surveillance Overview

In this window, the **Surveillance Topology** and **Device Information** are displayed. It appears automatically when you access the Surveillance Mode in the Web UI of the Switch.

Surveillance Topology

This window provides more information about what is connected to each port. Hover with the mouse pointer over each device icon to get more information about the recognized device (such as the number of devices, device type, IP address, power consumption, link speed, and errors).

To return to the Surveillance Overview window after viewing other windows, click the **DGS-1250-28XP** link.

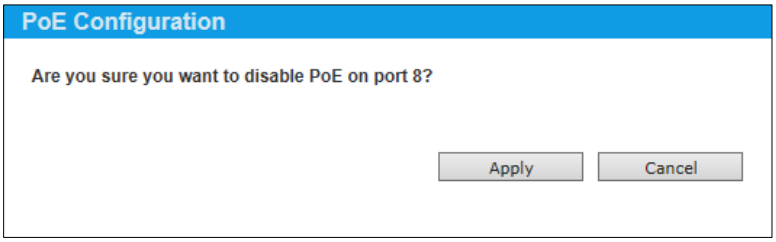


Surveillance Overview Window

The following icons are available in this window and are described below:

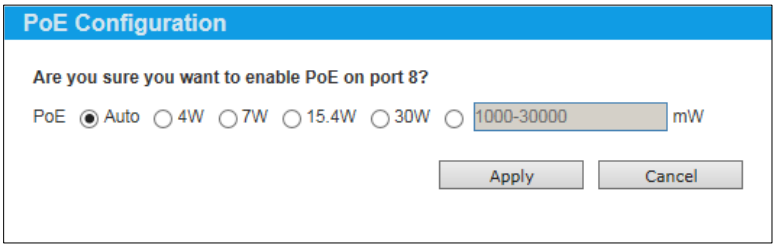
Icon	Description
IP Camera x 1	This displays the total amount of ONVIF IP cameras connected to the Ethernet ports on the Switch.
D-Link Legacy IP Camera x 0	This displays the total amount of D-Link legacy IP cameras (detected by ASV 1.0) connected to the Ethernet ports on the Switch.
NVR x 1	This displays the total amount of Network Video Recorders (NVRs) connected to the Ethernet ports on the Switch.
x 0	This displays the amount of surveillance warnings generated on the Switch.
Other x 1	This displays the amount of other devices connected to the Ethernet ports on the Switch.
	This displays the device connected to the Ethernet port on the Switch. The green border around the image indicates that the device is a non-PoE device.
	This displays the device connected to the Ethernet port on the Switch. The blue border around the image indicates that the device is a PoE device and is receiving power from the Switch using PoE. The PD Alive function can be used on this device.
	Click this icon to disable PoE on the port.
	Click this icon to enable PoE on the port.

After clicking the  icon, the following window will appear:



PoE Configuration (To Disable) Window

After clicking the  icon, the following window will appear:



PoE Configuration (To Enable) Window

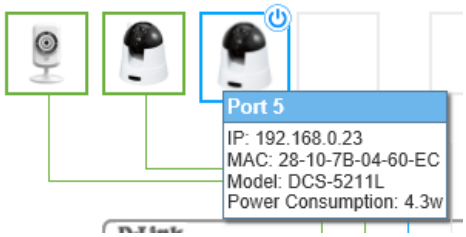
The fields that can be configured are described below:

Parameter	Description
PoE	Select the maximum power that will be supplied on the PoE port. Options to choose from are **Auto**, **4W**, **7W**, **15.4W**, **30W**, and a configurable value from 1000 mW to 30000 mW. The unit is either in watt or milliwatt.

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

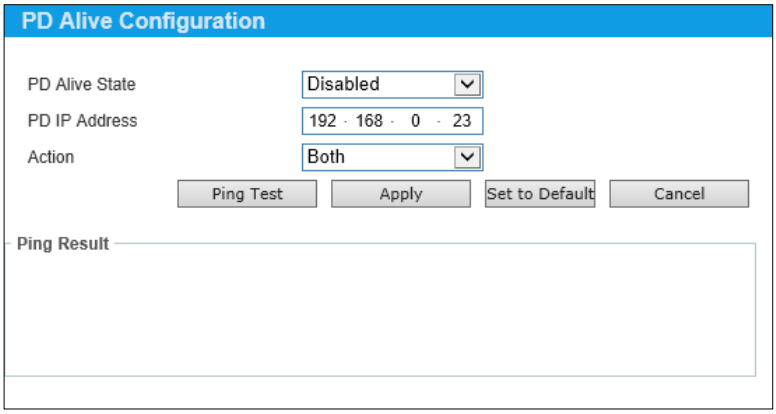
Click the **Cancel** button to discard the changes made.

After hovering (with the mouse pointer) over the network device icon, the following additional information will be displayed:



Additional Device Information

After clicking (left-click) the network device icon, the following window will appear.

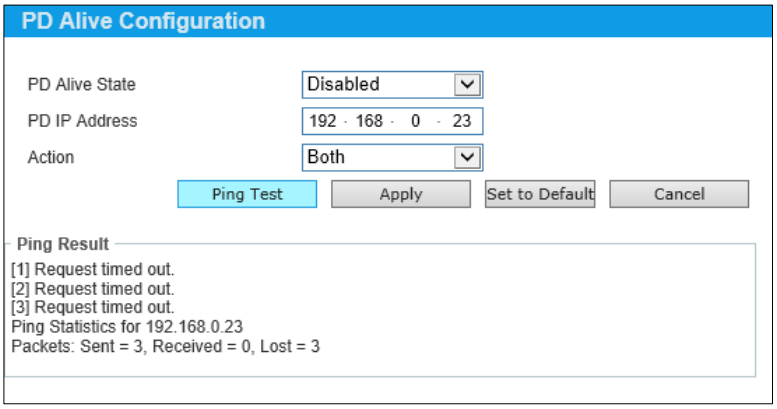


P
D Alive Configuration Window

The fields that can be configured are described below:

Parameter	Description
PD Alive State	Select to enable or disable the PD Alive function here.
PD IP Address	Enter the IP address of the PD here.
Action	Select the action that will be taken here. Options to choose from are: • **Reset** - Specifies to reset the PoE port state (turn PoE off and on). • **Notify** - Specifies to send logs and traps to notify the administrator. • **Both** - Specifies to send logs and traps to notify the administrator and to reset the PoE port state (turn PoE off and on).

After clicking **Ping Test** button, the following window will appear.



PD Alive Configuration Window (Ping Result)

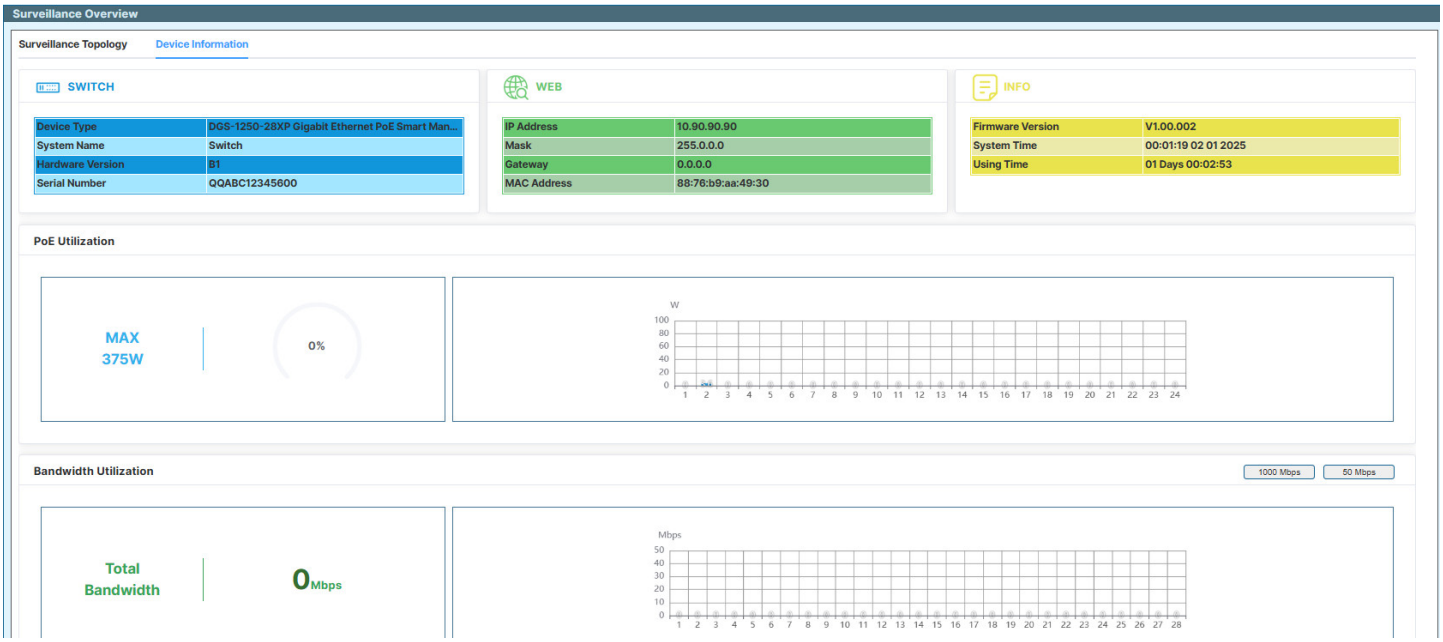
The **Ping Result** will be displayed.

NOTE: A breakdown of the device icons can be found by clicking the **Help** menu in the toolbar.

NOTE: The Switch uses ONVIF traffic to monitor the status of the surveillance device, but some third party devices do not fully comply with the ONVIF standard. If you are having problems with surveillance devices not being detected, please check ONVIF compatibility with the manufacturer of the original surveillance device.

Device Information

After clicking the **Device Information** tab, the following window will appear.



Device Information Window

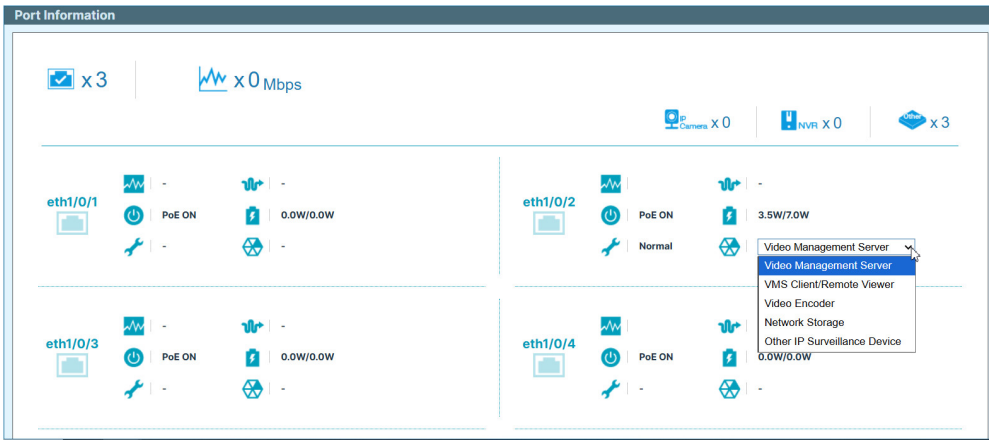
Click the **1000 Mbps** button to change the maximum bandwidth displayed in the **Bandwidth Utilization** chart to 1 Gbps.

Click the **50 Mbps** button to change the maximum bandwidth displayed in the **Bandwidth Utilization** chart to 50 Mbps.

Port Information

This window is used to display port information like throughput, distance of the network cable, PoE provisioning status, power consumption; loopback detection status, group, and how many IP cameras, NVRs, and other devices are connected to the ports.

To view the following window, click **Port Information**, as shown below:



Port Information Window

The following icons are available in this window and are described below:

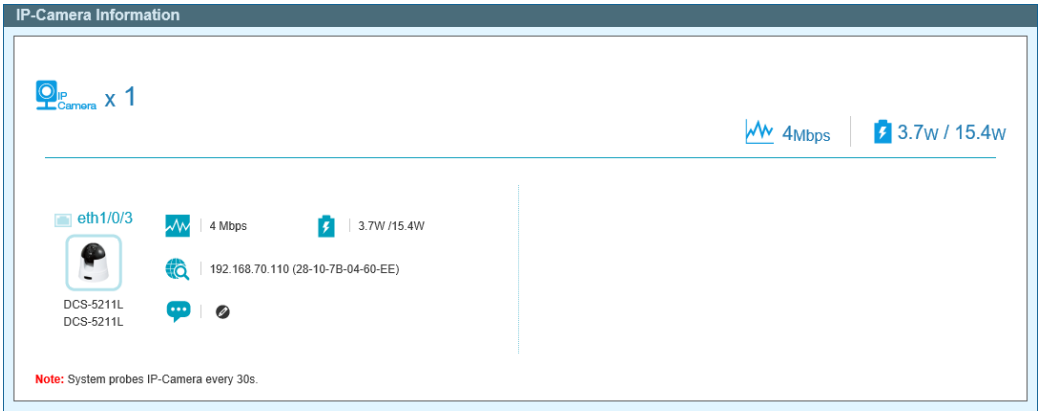
Icon	Description
x 5	This displays the total amount of Ethernet devices connected to the Ethernet ports on the Switch.
6 Mbps	The displays the total amount of inbound bandwidth that is being used by the Ethernet devices connected to the Ethernet ports on the Switch.
IP Camera x 3	This displays the total amount of ONVIF IP cameras connected to the Ethernet ports on the Switch.
NVR x 1	This displays the total amount of NVRs connected to the Ethernet ports on the Switch.
Other x 1	This displays the total amount of other Ethernet devices connected to the Ethernet ports on the Switch.
eth1/0/1	This displays the Ethernet port number on the Switch.
0 Mbps	This displays the amount of inbound bandwidth that is being used by the Ethernet device connected to the respective Ethernet port.

Icon	Description
 -	This displays the Ethernet cable length between the device and the Ethernet port on the Switch.
 PoE ON	This displays the PoE status on the port.
 3.9W/15.4W	This displays the power consumption and power class of the PD connected to the Ethernet port.
 Normal  Loop	This displays the Loopback Detection status on the Ethernet port. • **Normal** - Specifies that there are no loops in the network. • **Loop** - Specifies that there is a loop in the network. Click the **Loop** link to navigate to the **Health Diagnostic** window.
 Group Details	If an ONVIF IP camera or NVR is connected to the port, the **Group Details** link will be available. Select the **Group Details** link to access the Group Details window.
 Video Management Server	If a network device is connected to the port that is neither an ONVIF IP camera nor NVR, the device type can be selected. Options to choose from are **Video Management Server**, **VMS Client/Remote Viewer**, **Video Encoder**, **Network Storage**, and **Other IP Surveillance Device**.

IP-Camera Information

This window is used to display IP camera information.

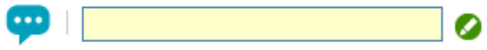
To view the following window, click **IP-Camera Information**, as shown below:



IP-Camera Information Window

The following icons are available in this window and are described below:

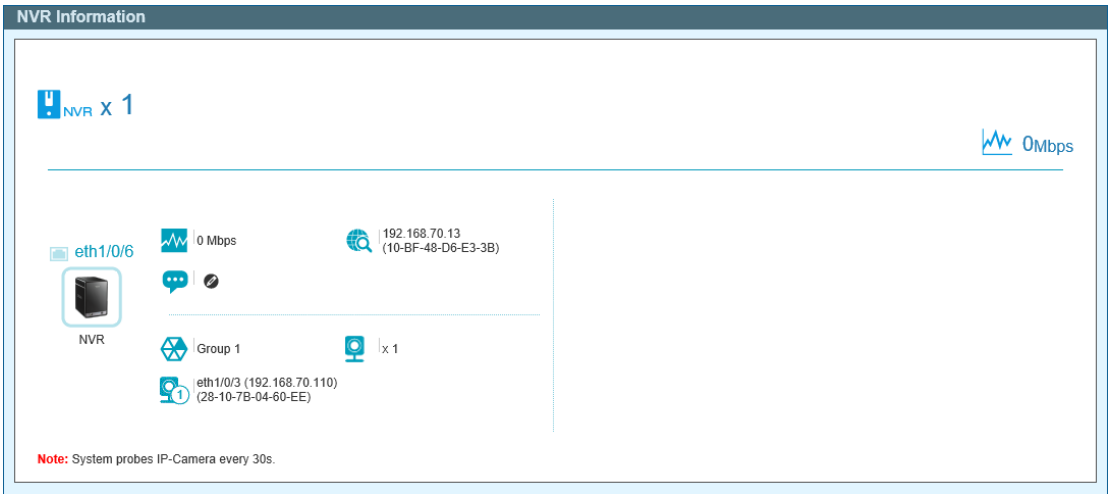
Icon	Description
x 3	This displays the total amount of ONVIF IP cameras connected to the Ethernet ports on the Switch.
0Mbps	The displays the total amount of inbound bandwidth that is being used by the ONVIF IP cameras connected to the Ethernet ports on the Switch.
4.4W / 15.4W	The displays the total power consumption and power class (of PDs) used by the ONVIF IP cameras connected to the Ethernet ports on the Switch.
eth1/0/1	This displays the Ethernet port number on the Switch.
DCS-942LB1 DCS-942LB1	This displays a photo, manufacturer, and model name of the IP camera connected to the port. D-Link IP cameras will display the photo of the specific model connected to the port. Non-D-Link camera will display a generic IP camera photo.
0 Mbps	This displays the amount of inbound bandwidth that is being used by the IP camera.
4.4W /15.4W	This displays the power consumption and power class of the IP camera.
192.168.0.21 (B0-C5-54-26-B7-A3)	This displays the IP address and MAC address of the IP camera.
DCS-942LB1	This displays the description for the IP camera. Click the icon to modify the description.

Icon	Description
	Enter the description for the IP camera here. Click the icon to apply the modified description.

NVR Information

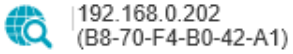
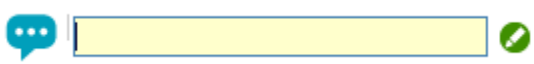
This window is used to display NVR information.

To view the following window, click **NVR Information**, as shown below:



NVR Information Window

The following icons are available in this window and are described below:

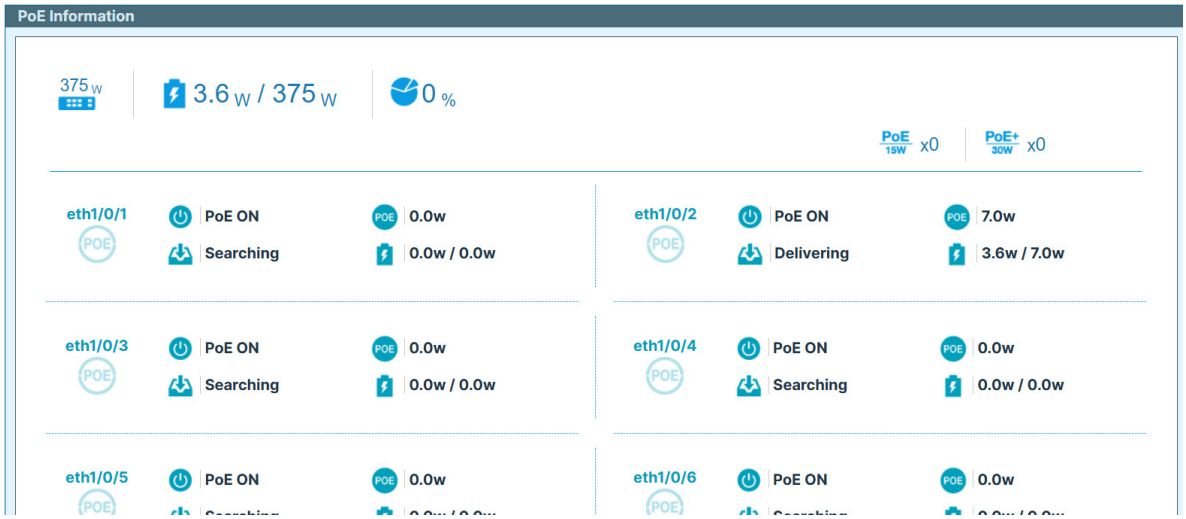
Icon	Description
	This displays the total amount of NVRs connected to the Ethernet ports on the Switch.
	The displays the total amount of inbound bandwidth that is being used by the NVRs connected to the Ethernet ports on the Switch.
	This displays the Ethernet port number on the Switch.
	This displays a generic photo of the NVR connected to the port.
	This displays the amount of inbound bandwidth that is being used by the NVR.
	This displays the IP address and MAC address of the NVR.
	This displays the description for the NVR. Click the icon to modify the description.
	Enter the description for the NVR here. Click the icon to apply the modified description.

Icon	Description
Group 1	This displays the group ID of the NVR.
x 3	This displays the number of ONVIF IP cameras managed by this NVR.
eth1/0/5 (192.168.0.23) (28-10-7B-04-60-EC)	This displays information about the ONVIF IP camera that is managed by this NVR.

PoE Information

This window is used to display Power-over-Ethernet (PoE) information.

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



PoE Information Window

The following icons are available in this window and are described below:

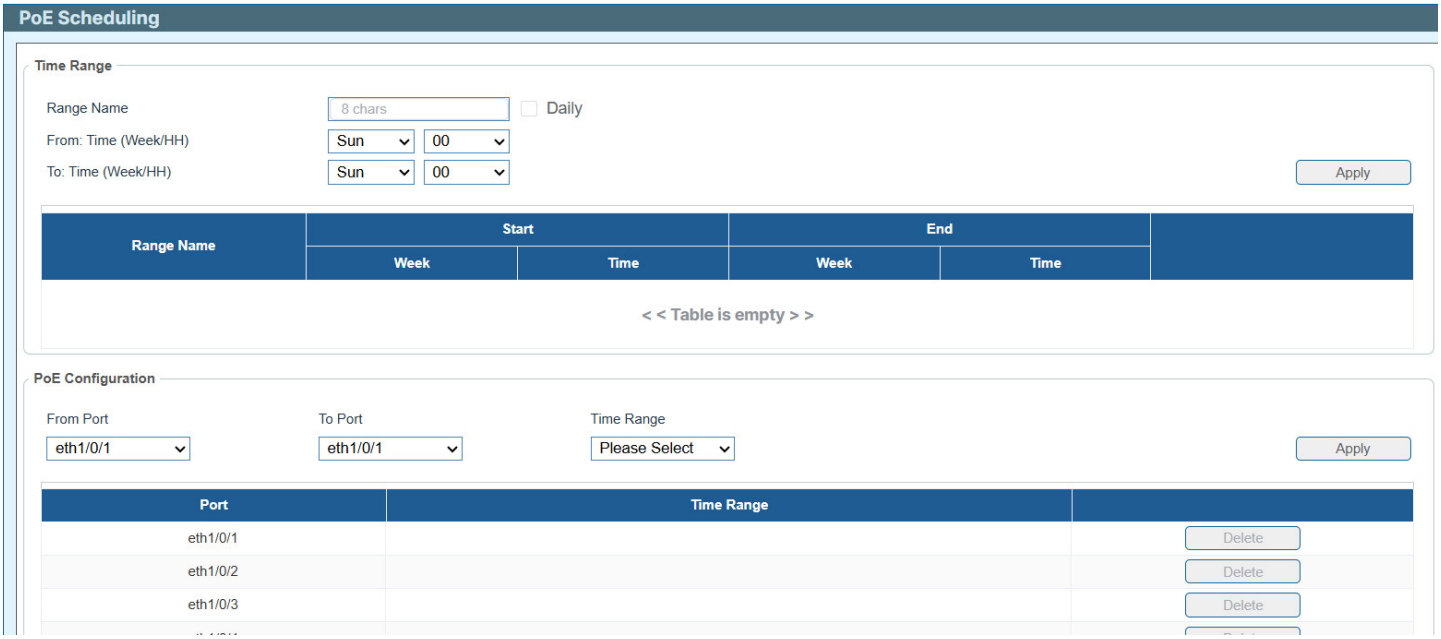
Icon	Description
375 W	This displays the maximum PoE budget that can be provided by the Switch.
3.6 W / 375 W	This displays the total PoE consumption and power class of PDs connected to the Switch.
22 %	This displays the current PoE utilization (in percentage).
PoE 15W x 1	This displays the number of PoE devices connected to the Switch that is using 15 Watts of power per port.
PoE+ 30W x 0	This displays the number of PoE devices connected to the Switch that is using 30 Watts of power per port.
eth1/0/5 POE	This displays the Ethernet port number on the Switch.
PoE ON	This displays the PoE state on the port. This can be either **PoE ON** or **PoE OFF**.

Icon	Description
POE | 15.4W	This displays the maximum PoE budget available on this port.
Delivering Power Denied	This displays the current PoE status on the port. This status can be one of the following: **Disabled**, **Requesting**, **Searching**, **Delivering**, **MPS (Maintain Power Signature) Absent**, **PD Short**, **Overload**, **Power Denied**, **Thermal Shutdown**, **Startup Failure**, or **Classification Failure**. When the **Power Denied** message is displayed, click on the link to redirect the **Health Diagnostic** window for more information.
3.5W/ 15.4W	This displays the PoE consumption and power class of the PD connected to the port.

PoE Scheduling

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

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



PoE Scheduling Window

The fields that can be configured in the **Time Range** section are described below:

Parameter	Description
Range Name	Enter the name of the time range schedule here. Tick the **Daily** option to use this schedule for every day of the week.
From: Time (Week/HH)	Select the starting day and hour in the time range schedule here. Alternatively.
To: Time (Week/HH)	Select the ending day and hour in the time range schedule here. The schedule will end at the end of the selected hour.

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

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

The fields that can be configured in the **PoE Configuration** section are described below:

Parameter	Description
From Port / To Port	Select the port range that will be used here.
Time Range	Select the time range schedule that will be applied to the selected port(s) here.

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

Click the **Delete** button to remove the time range schedule from the specified port.

Time

Clock Settings

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

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



Clock Settings Window

The fields that can be configured are described below:

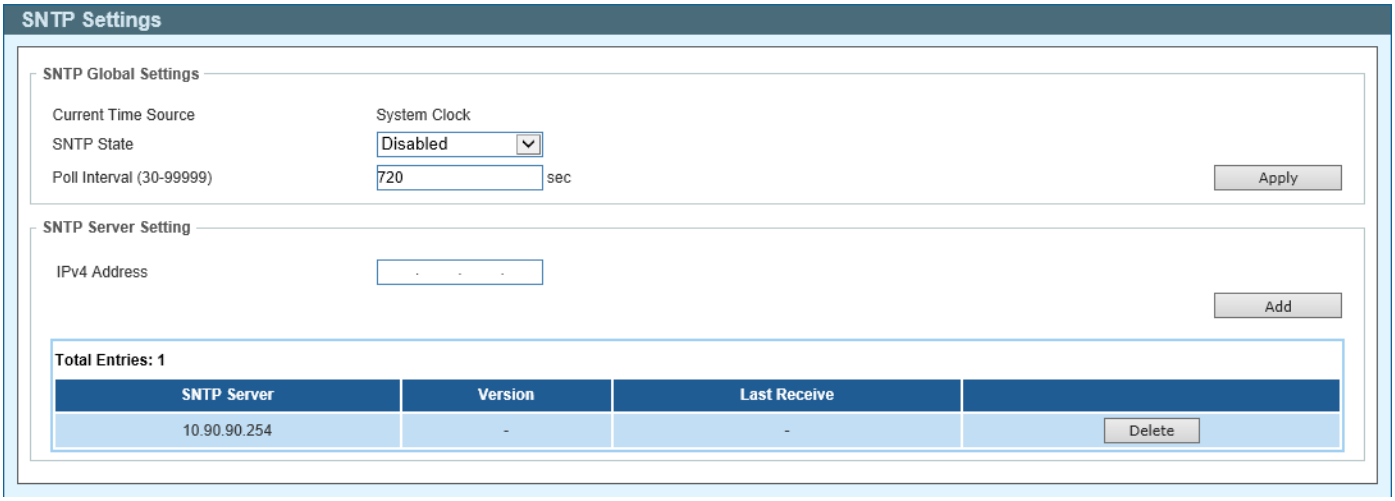
Parameter	Description
Time (HH:MM:SS)	Enter the current time in hours, minutes, and seconds.
Date (DD/MM/YYYY)	Enter the current day, month, and year to update the system clock.

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

SNTP Settings

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

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



SNTP Settings Window

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

Parameter	Description
SNTP State	Select to enable or disable the SNTP feature here.
Poll Interval	Enter the poll interval value here. The range is from 30 to 99999 seconds. By default, this value is 720 seconds.

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

The fields that can be configured in the **SNTP Server Setting** section are described below:

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

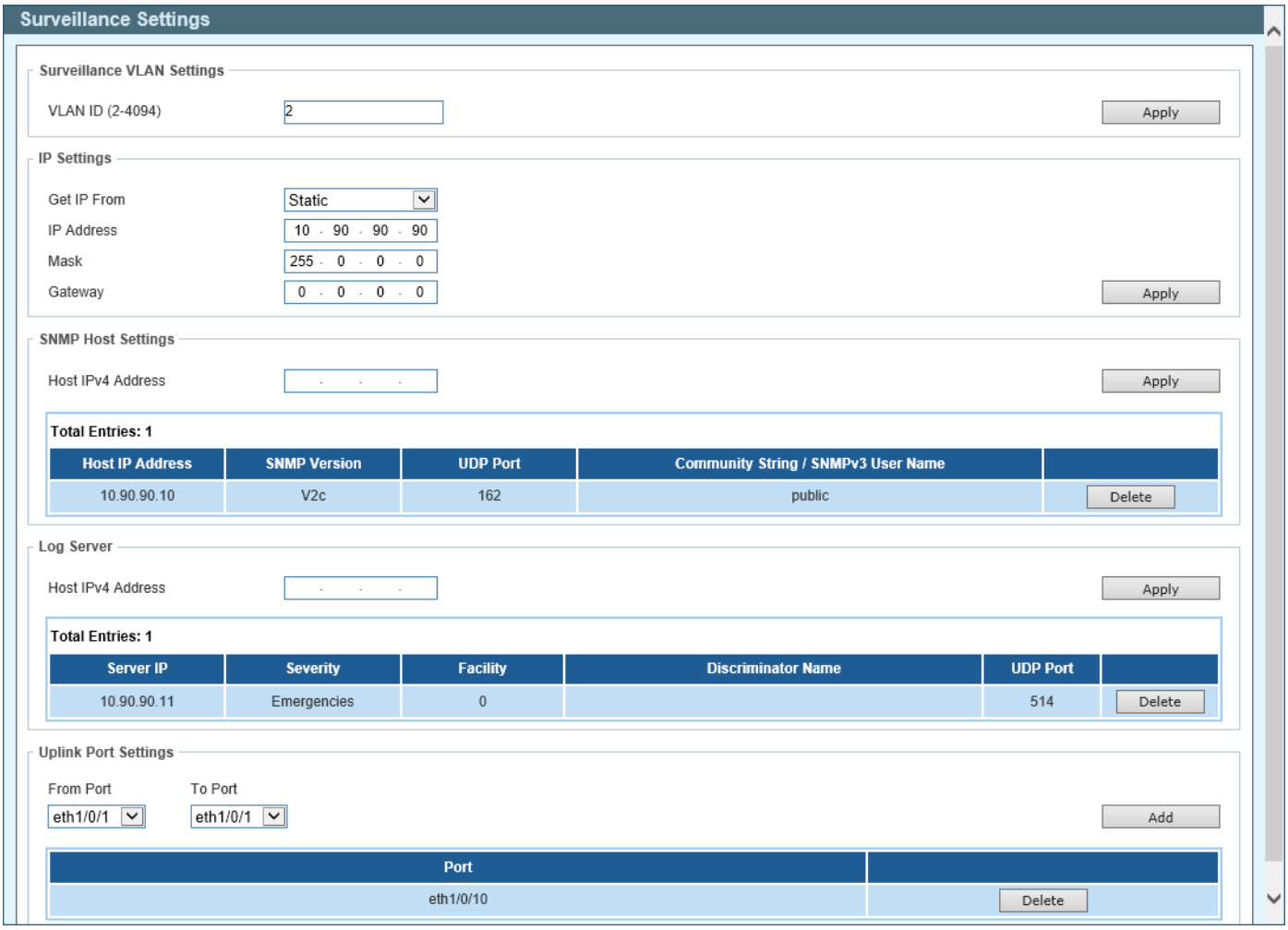
Click the **Add** button to add the SNTP server to the configuration.

Click the **Delete** button to remove the SNTP server from the configuration.

Surveillance Settings

This window is used to display and configure the surveillance settings. The Switch has only one Surveillance VLAN. This surveillance VLAN also supports to recognize the surveillance devices, like IP Cameras (IPC) and Network Video Recorders (NVR), using the ONVIF protocol.

To view the following window, click **Surveillance Settings**, as shown below:



Surveillance Settings Window

The fields that can be configured in the **Surveillance VLAN Settings** section are described below:

Parameter	Description
VLAN ID	Enter the ID of the surveillance VLAN here. The range is from 2 to 4094.

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

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

Parameter	Description
Get IP From	Select the method used to configure the IP address settings on the Switch here. Options to choose from are: • **Static** - Specifies that the IP address settings will be manually configured. • **DHCP** - Specifies that the IP address settings will be automatically obtained from a DHCP server on the network.
IP Address	Enter the IPv4 address of the Switch here.
Mask	Enter the IPv4 subnet mask of the Switch here.

Parameter	Description
Gateway	Enter the IPv4 address of the default gateway here.

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

The fields that can be configured in the **SNMP Host Settings** section are described below:

Parameter	Description
Host IPv4 Address	Enter the IPv4 address of the SNMP host here.

Click the **Apply** button to accept the changes made. Click the **Delete** button to remove the specified entry.

The fields that can be configured in the **Log Server** section are described below:

Parameter	Description
Host IPv4 Address	Enter the IPv4 address of the SNMP server here.

Click the **Apply** button to accept the changes made. Click the **Delete** button to remove the specified entry.

The uplink ports join all surveillance VLANs since they forward surveillance traffic to other switches. It is recommended to connect uplink ports to the other switches because the discovery process is disabled on these ports.

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

Parameter	Description
From Port / To Port	Select the uplink port range that will be used here.

Click the **Apply** button to accept the changes made. Click the **Delete** button to remove the specified entry.

Surveillance Log

This window is used to display the surveillance log.

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



Surveillance Log Window

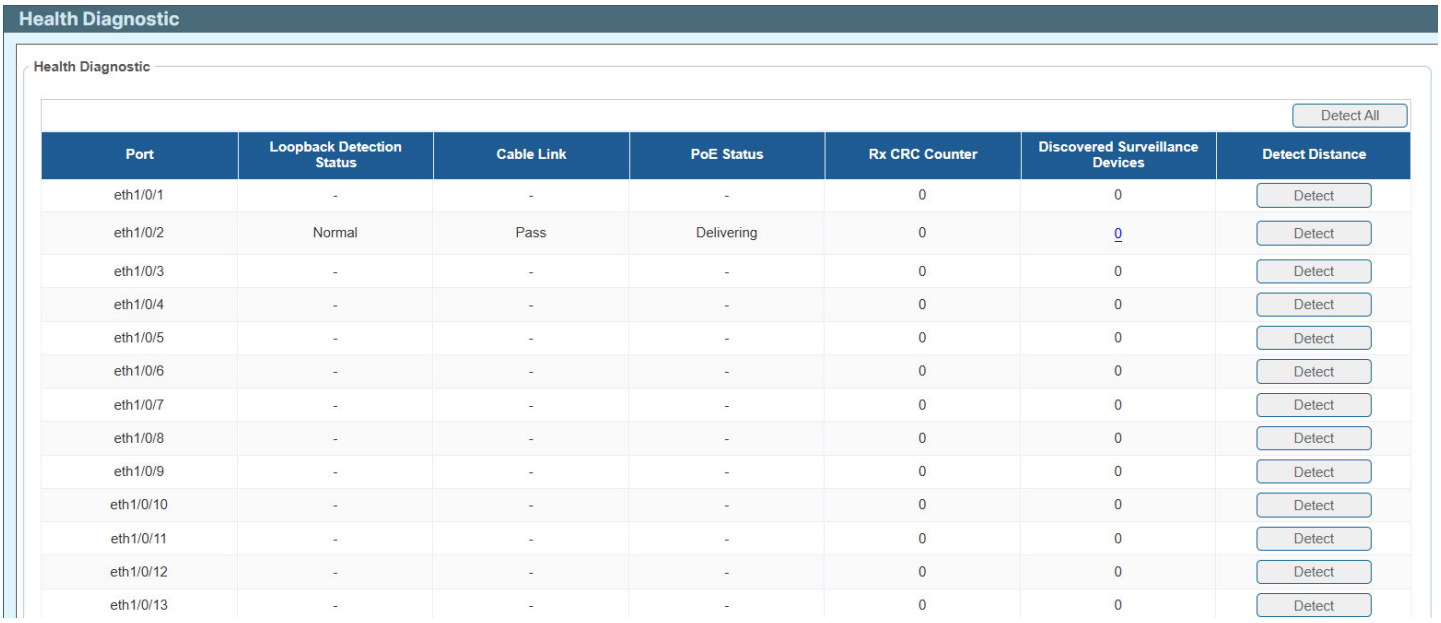
Click the **Refresh** button to refresh the information displayed in the table. Click the **Backup** button to upload the surveillance log to the PC using HTTP.

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

Health Diagnostic

This window is used to display Health Diagnostics information, Discovered Surveillance Devices information, and initiate a cable distance test on all or selected ports on the Switch. For each link-up port, the system will check the link status, PoE status and error counters periodically. This page will refresh every 30s.

To view the following window, click **Health Diagnostic**, as shown below:



Health Diagnostic Window

The fields that are displayed in the table are described below:

Parameter	Description
Port	This field displays the Ethernet port number.
Loopback Detection Status	This field displays the Loopback Detection status on the Ethernet port. It can be one of the following: • **Normal** - No loop is detected on the port. • **Loop** - A loop is detected on the port.
Cable Link	This field displays the cable link status. It can be one of the following: • **Pass** - The port link is up and operating in the full-duplex mode. • **10M Half** - The port link is up and operating at 10 Mbps speed and in the half-duplex mode. • **100M Half** - The port link is up and operating at 100 Mbps speed and in the half-duplex mode.
PoE Status	This field displays the PoE status. It can be one of the following: **Delivering**, **Searching**, **Pass**, **MPS (Maintain Power Signature) Absent**, **PD Short**, **Overload**, **Power Denied**, **Thermal Shutdown**, **Startup Failure**, or **Classification Failure**.
Rx CRC Counter	This field displays the RX CRC counter.

Parameter	Description
Discovered Surveillance Devices	This field displays the number of ONVIF IP cameras and NVRs discovered on the port. Click the hyperlink (1) to view the group details associated with IP camera or NVR connected to the port.
Detect Distance	Click the **Detect** button to initiate a cable distance test on the specified port.

Click the **Detect All** button to initiate a cable distance test on all the ports of the Switch.

Toolbar

Wizard

Click this option to start the Smart Wizard. For more information about the Smart Wizard, refer to **Smart Wizard** on page 5.

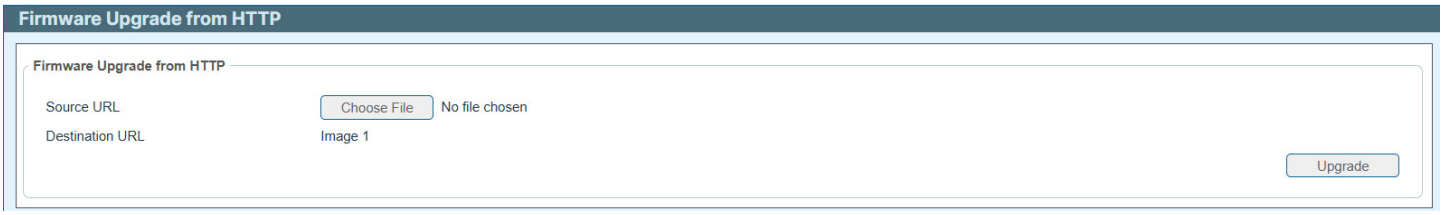
Tools

Firmware Upgrade & Backup

Firmware Upgrade from HTTP

This window is used to initiate a firmware upgrade from a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP**, as shown below:



Firmware Upgrade from HTTP Window

The fields that can be configured are described below:

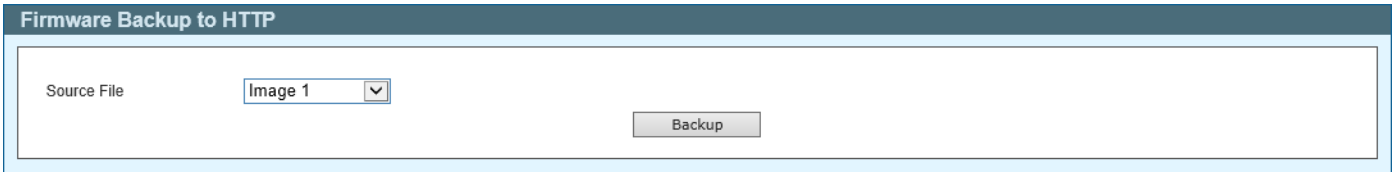
Parameter	Description
Source File	Click the **Browse** button and navigate to the firmware file on the local PC here. This file will be uploaded to the Switch.
Destination File	Select the destination where the firmware file will be saved on the Switch here. Options to choose from are **Image 1** and **Image 2**.

Click the **Upgrade** button to initiate the firmware upgrade.

Firmware Backup to HTTP

This window is used to initiate a firmware backup to a local PC using HTTP.

To view the following window, click **Tools > Firmware Upgrade & Backup > Firmware Backup to HTTP**, as shown below:



Firmware Backup to HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source File	Select the firmware on the Switch that will be backed up to the local PC here. Options to choose from are **Image 1** and **Image 2**.

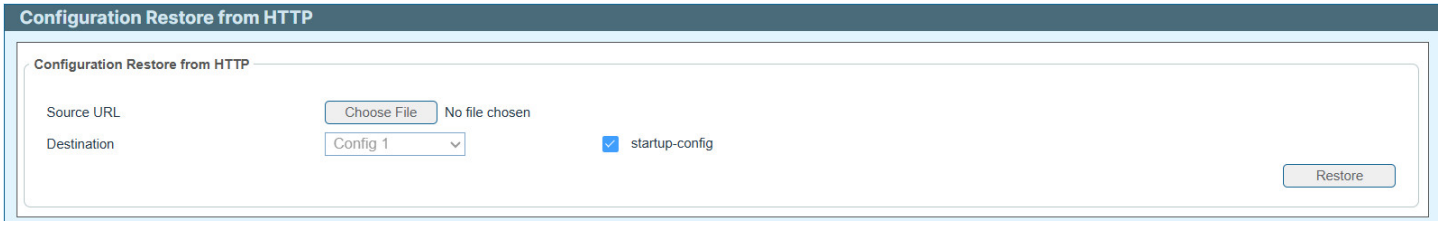
Click the **Backup** button to initiate the firmware backup. Wait for the Web browser to prompt where to save the file on the local PC.

Configuration Restore & Backup

Configuration Restore from HTTP

This window is used to initiate a configuration restore from a local PC using HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Restore from HTTP**, as shown below:



Configuration Restore from HTTP Window

The fields that can be configured are described below:

Parameter	Description
Source File	Click the **Browse** button and navigate to the configuration file on the local PC here. This file will be uploaded to the Switch.
Destination File	Select the destination for the configuration file on the Switch here. Options to choose from are: • **Configuration 1** - Select this option to use configuration 1 as the destination. • **Configuration 2** - Select this option to use configuration 2 as the destination. • **running-config** - Select this option to use the running configuration as the destination. • **startup-config** - Select this option to use the start-up configuration as the destination.

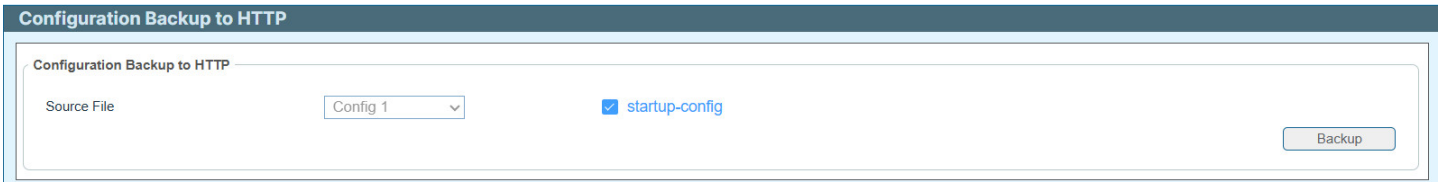
Parameter	Description
Replace	Select this option to replace the running configuration on the Switch with this one.

Click the **Restore** button to initiate the configuration restore.

Configuration Backup to HTTP

This window is used to initiate a configuration file backup to a local PC using HTTP.

To view the following window, click **Tools > Configuration Restore & Backup > Configuration Backup to HTTP**, as shown below:



Configuration Backup to HTTP Window

The fields that can be configured are described below:

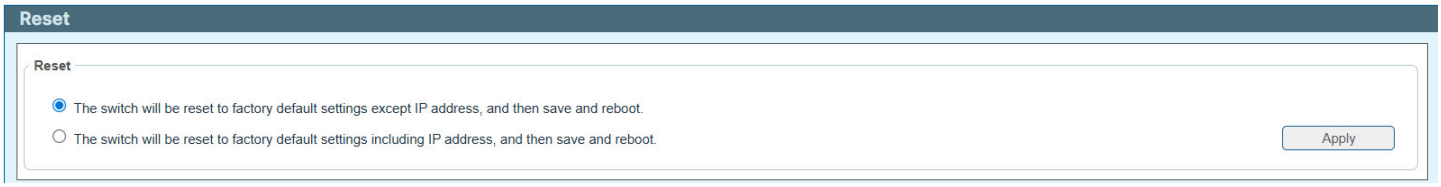
Parameter	Description
Source File	Select the configuration on the Switch that will be backed up to the local PC here. Options to choose from are: • **Configuration 1** - Select this option to backup configuration 1. • **Configuration 2** - Select this option to backup configuration 2. • **running-config** - Select this option to backup the running configuration. • **startup-config** - Select this option to backup the start-up configuration.

Click the **Backup** button to initiate the configuration file backup. Wait for the Web browser to prompt where to save the file on the local PC.

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 Window

Select one of the following options:

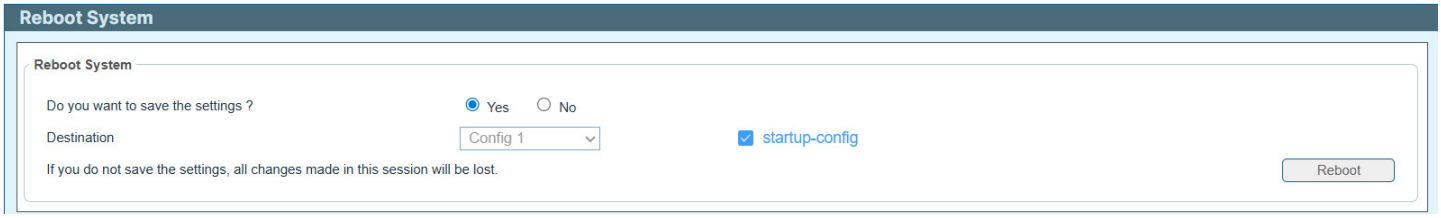
- The Switch will reset to its factory default settings and then save, reboot.
- The Switch will reset to its factory default settings and then save, reboot. This option excludes the IP address.
- The Switch will reset to its factory default settings and not reboot.

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

Reboot System

This window is used to reboot the Switch and alternatively save the configuration before doing so.

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



Reboot System Window

When rebooting the Switch, any configuration changes that was made during this session, will be lost unless the **Yes** option is selected when asked to save the settings.

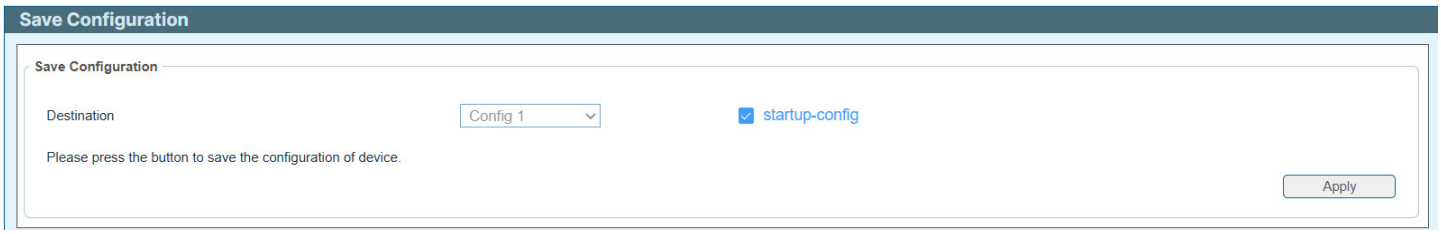
Click the **Reboot** button to alternatively save the settings and reboot the Switch.

Save

Save Configuration

This window is used to save the running configuration to the start-up configuration. This is to prevent the loss of configuration in the event of a power failure.

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



Save Configuration Window

The fields that can be configured are described below:

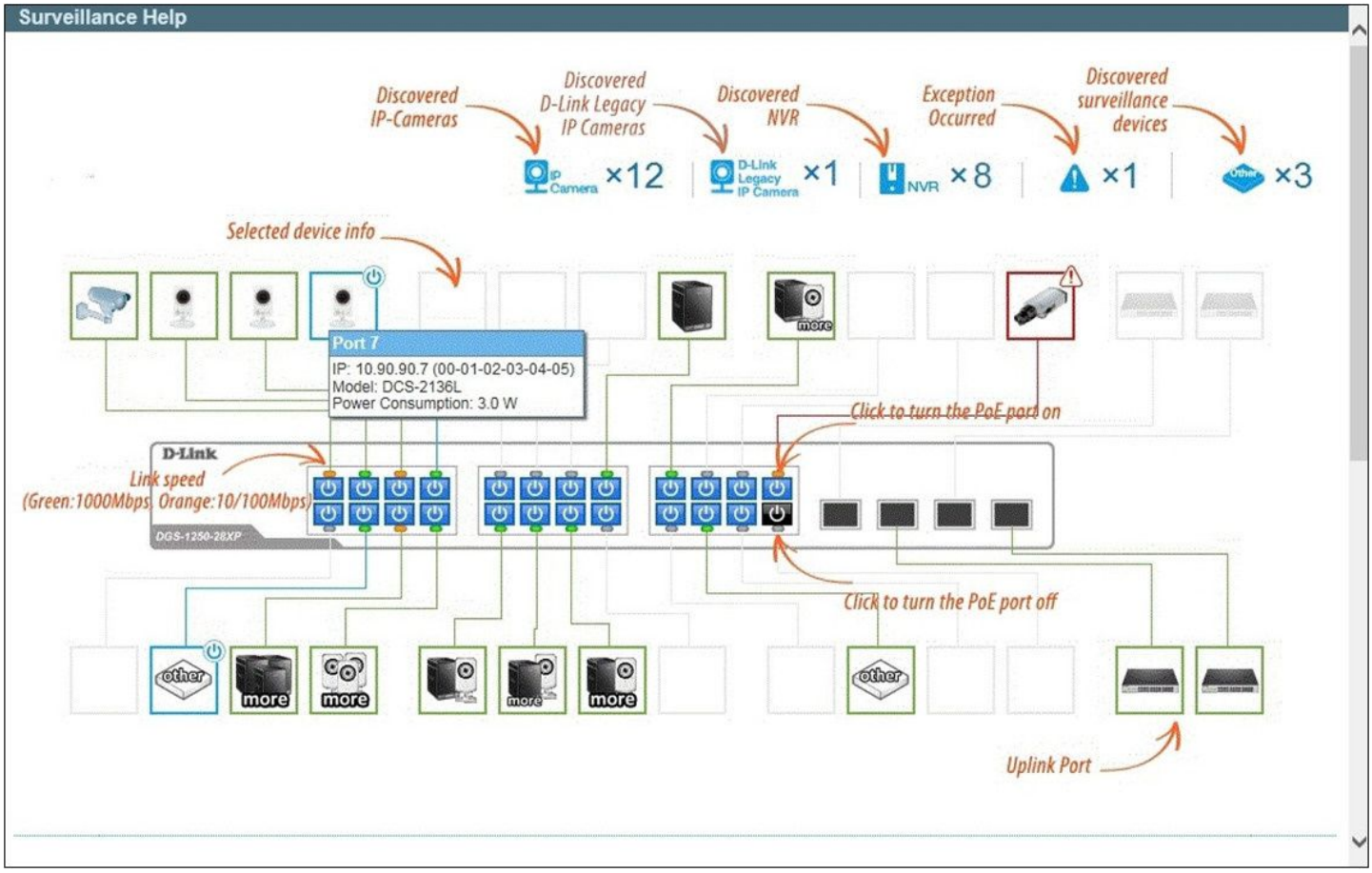
Parameter	Description
File Path	Select the destination where the configuration will be saved here. Options to choose from are **startup-config**, **Configuration 1**, and **Configuration 2**.

Click the **Apply** button to save the configuration.

Help

Click this option to access the built-in Surveillance Help window.

After clicking the **Help** option, the following window will appear.



Help (Diagram) Window

Device Status

Icon	Description	Icon	Description	Icon	Description
	The device is operational but is not powered by PoE.		The device is operational and is powered by PoE.		The device may malfunction. Some problem detected on this port or device.
	This icon indicates that the designated device is operational and is powered by PoE. It also indicates that the PD Alive function is enabled.		The device was rebooted successfully. Please click the icon to recover to its operational state.		The device has malfunctioned. A problem has been detected on this port or device. PD Alive function may have malfunctioned.

IP-Camera/NVR Status

Icon	Description	Icon	Description	Icon	Description
	One D-Link ONVIF IP-Camera discovered on this port. For D-Link IP-Camera, a specific icon will be displayed.		One ONVIF IP-Camera discovered on this port.	more	Multiple ONVIF IP-Cameras discovered on this port.
	One NVR discovered on this port. Any device connect to IP-Camera via HTTP, HTTPS and RTSP will be recognized as an NVR.	more	Multiple NVRs discovered on this port.		One ONVIF IP-Camera and one NVR discovered on this port.
more	Multiple ONVIF IP-Cameras and one NVR discovered on this port.	more	One ONVIF IP-Camera and multiple NVRs discovered on this port.	more	Multiple ONVIF IP-Cameras and multiple NVRs discovered on this port.
other	The port is up and no ONVIF IP-Camera, NVR, or other surveillance device has been discovered on this port.		This port is set as uplink port and the port status is up. Uplink port joins all VLANs and surveillance discovery process is disabled on this port.		This port is set as uplink port and the port status is down.

Help (Table) Window

Online Help

D-Link Support Site

Click this option to connect to the D-Link support website. An Internet connection is required.

User Guide

Click this option to connect to the online user guide for the Switch. An Internet connection is required.

Standard Mode

Click the **Standard Mode** button in the toolbar to change the Web UI mode and style from Surveillance Mode to Standard Mode.



NOTE: All active Web UI user sessions can only access the same Web UI mode at the same time.

The mode can only be changed when one user session is active. The mode cannot be changed when another user session is connected to the Web UI.

Logout

Click this option to log out of the Web UI of the Switch

Appendix A - Technical Specifications

Hardware Specifications

Key Components / Performance

- Switching Capacity:
- - DGS-1250-28X: 128Gbps
- - DGS-1250-28XP: 128Gbps
- - DGS-1250-52X: 176Gbps
- - DGS-1250-52XP: 176Gbps
- DDRIII for CPU: 512MBytes
- Flash Memory: 32MBytes

Port Functions

- 1GBASE-T ports compliant with the following standards:

- 100BASE-TX: IEEE 802.3u compliance
- 1000BASE-T: IEEE 802.3ab compliance
- Supports Full-Duplex operations
- IEEE 802.3x Flow Control support for Full-Duplex mode
- Auto MDI/MDIX
- Auto-negotiation
- Head-of-line blocking prevention

- 10GE SFP/SFP+ ports compliant with the following standards:

- IEEE 802.3z
- IEEE 802.3ae
- IEEE 802.3aq

1000BASE-T transceivers supported:

- DGS-712 (1000BASE-TX)

SFP transceivers:

- DEM-310GT (1000BASE-LX, 10km)
- DEM-311GT (1000BASE-SX, 550m)
- DEM-312GT2 (1000BASE-SX, 2km)
- DEM-314GT (1000BASE-LHX, 50km)
- DEM-315GT (1000BASE-ZX, 80km)

SFP WDM Transceiver:

- DEM-330T/R (1000BASE-BX, 10km)
- DEM-331T/R (1000BASE-BX, 40km)
- DEM-302S-BXD (1000BASE-BX-D Single-Mode, 2KM(TX-1550/RX-1310 nm))
- DEM-302S-BXU (1000BASE-BX-U Single-Mode, 2KM(TX-1310/RX-1550 nm))

SFP+ Transceiver:

- DEM-431XT: 10GBASE-SR 80m
- DEM431XT-DD: 10GBASE-SR, 80m
- DEM-432XT: 10BASE-LR, 10km
- DEM-432XT-DD: 10GBASE-LR, 10km
- DEM-433XT: 10GBASE-ER, 40km
- DEM-433XT-DD: 10GBASE-ER, 40km
- DEM-434XT: 10GBASE-ZR, 80km

WDM SFP+ Transceiver:

- DEM-436XT-BXU: 10GBASE-LR 20km
- DEM-436XT-BXD: 10GBASE-LR 20km

CWDM SFP+ Transceiver:

- DEM-X10CS-1271: 10G Single-Mode 10KM CWDM SFP+ Transceiver
- DEM-X10CS-1291: 10G Single-Mode 10KM CWDM SFP+ Transceiver
- DEM-X10CS-1311: 10G Single-Mode 10KM CWDM SFP+ Transceiver
- DEM-X10CS-1331: 10G Single-Mode 10KM CWDM SFP+ Transceiver
- DEM-X40CS-1471: 10G Single-Mode 40KM CWDM SFP+ Transceiver
- DEM-X40CS-1491: 10G Single-Mode 40KM CWDM SFP+ Transceiver
- DEM-X40CS-1511: 10G Single-Mode 40KM CWDM SFP+ Transceiver
- DEM-X40CS-1571: 10G Single-Mode 40KM CWDM SFP+ Transceiver

- Support following Direct Attach Cable(DAC):

- DEM-CB100S
- DEM-CB300S

Physical & Environment

- AC input, 100~240 VAC, 50/60Hz, internal universal power supply
- Acoustic Value:

- DGS-1250-28X: 1 Fans
- DGS-1250-28XP: 1 Fans
- DGS-1250-52X: 2 Fans
- DGS-1250-52XP: 2 Fans

- Operation Temperature -5~50°C
- Storage Temperature -40~70°C
- Operation Humidity: 0%~95% RH
- Storage Humidity: 0%~95% RH

Emission (EMI) Certifications

- FCC class A
- CE Class A
- VCCI Class A
- IC Class A
- C-Ticket Class A
- BSMI Class A
- CCC Class A

Safety Certifications

- cUL, CB, CE, CCC, BSMI

Features

L2 Features

- Supports up to 16K MAC address
- Jumbo frame: Supports up to 12KB
- IGMP snooping: Supports 128 multicast group
- MLD Snooping
- 802.1D Spanning Tree
- 802.1s MSTP
- 802.1w Rapid Spanning Tree
- ERPS
- Loopback Detection
- 802.3ad Link Aggregation:
  - DGS-1250 Rev.B1 Series 8 groups per device and 8 ports per group
- Port mirroring
- ERPS
- Voice VLAN
- Auto Surveillance VLAN
- GVRP
- LLDP

L3 Features

- ARP:
  - Max 16K ARP entries
  - Support 128 static ARP
- Support 8 IPv4 and 16 IPv6 interfaces
- Support IPv4 address 0.0.0.0 to prevent occupied IP address in the network
- Support IPv6 Neighbor Discovery:
  - Max 384 ND entries
  - Support up to 63 static ND entries
- Max. 64 IPv4 and 64 IPv6 static route entries
- Support secondary route
- Max. 768 IPv4 and 384 IPv6 host route

D-Link Green Technology

- Compliant with RoHS6.
- Support D-Link Green v3.0 power saving mode.
- D-Link Green Ethernet:
  - Power Saving by LED Shut-Off: Powered LEDs can be turned on/off by port or system through schedule
  - Power Saving by Port Shut-Off: Each port on the system can be turned on/off by schedule
  - Power Saving by System Hibernation: System enters hibernation by schedule. In this mode, switches get most power-saving figures since main chipsets (both MAC and PHY) are disabled for all ports.
- Energy Efficient Ethernet (EEE): EEE is disabled by default, user can enable EEE via Web GUI

VLAN

- 802.1Q VLAN standard (VLAN Tagging)
- Up to 4K VLAN groups
- Asymmetric VLAN

QoS (Quality of Service)

- Be able to classify packets according to follow contents:
  - 802.1p priority
  - VLAN
  - MAC address
  - Ether Type
  - IP address
  - DSCP
  - Protocol type
  - TCP/UDP port number
  - IPv6 traffic class
  - IPv6 flow label
- - TCP/UDP port number Up to 8 queues per port
- Supports Strict / WRR / WDRR / RR mode in queue handling
- Bandwidth Control

ACL

- Max 50 ingress ACL profile, 512 ingress ACL rules, 50 VLAN ACL rules.
- Each rule can be associated to a single port, multiple ports
- Supports following actions after analyzing packets:
  - Permit
  - Deny
- Support different ACL policy packet contents:
  - MAC address
  - Ethernet Type
  - IP address
  - ICMP
  - IGMP
  - TCP/UDP port number
  - 802.1p
  - DSCP
  - IPv6 traffic class
  - IPv6 flow label

Security

- Port Security: Support 64 MACs per port
- IP and MAC ACL
- Broadcast Storm Control
- D-Link Safeguard Engine

- DHCP Server Screening
- AAA (RADIUS/TACACS+)
- SSL: Support v1/v2/v3
- Support DHCP Snooping
- IP-MAC-Port Binding
- DoS Attack Prevention Settings

  - Supports ARP packet Inspection as default, ARP and IPv4 packet Inspection as option.

  - Supports IPv4 DHCP Snooping

- SSH
- SSL

Management

- Web-based GUI (IPv6 support)
- D-Link proprietary CLI
- Telnet Server: Max. 4 connections (IPv6 support)
- TFTP Client over IPv4 or IPv6
- SNMP v1/2c/3 over IPv4 or IPv6
- SNMP Trap
- DHCP client over IPv4 or IPv6
- RMON v1/v2
- Trap setting for destination IP, system events, fiber port events, twisted-pair port events
- Web-based configuration backup / restoration
- Web-based firmware backup/restore
- Firmware upgrade Web-based management
- Reset, Reboot


D-Link
Building Networks for People